



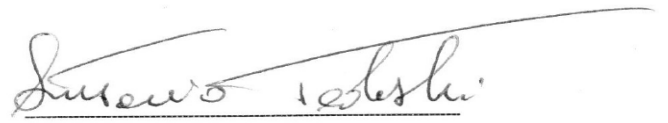
DOCTORATE IN APPLIED ELECTRONICS

Department of Engineering

XXIX DOCTORATE CYCLE

*Signal Processing Techniques for Cooperative
Spectrum Sensing in Trusted and Untrusted Networks*

*PhD student
Antonio Tedeschi*



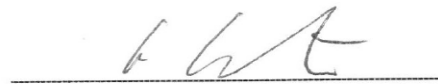
signature

*Tutor
Prof. Francesco Benedetto*



signature

*Co-Tutor
Prof. Gaetano Giunta*



signature

*Coordinator
Prof. Alessandro Salvini*



signature

Homo faber fortunae suae

Acknowledgements

*To my mother,
your strength will always serve as an example to me.*

*To Carlo and Sara,
my touchstones and the support team I can always count on.*

*To Mary,
for your love and for standing by me through thick and thin.*

*To my friends,
despite distance, work and random things that try to get in the way,
you have never ceased to be a constant in my life.*

*To my colleagues Angelo, Emanuela, Federico, Gabriel and Rig,
with whom I shared stress, breaks and laughs.*

*To Daniele, Antonio, Riccardo and Andrea,
your advice and your friendship helped me grow and better myself.*

*To my former students,
you made me love (and hate, at times) this short but intense career.*

Still, the teaching went both ways.

To Francesco,

a mentor, role model and friend.

I got this far guided by your advice and by what you taught me.

It made me a good researcher and a better person.

Thank you.

Table of Contents

| | |
|--|-------------|
| TABLE OF CONTENTS | 1 |
| LIST OF FIGURES | 4 |
| LIST OF ABBREVIATIONS | 9 |
| ABSTRACT | XIII |
| LIST OF PERSONAL PUBLICATIONS | XVII |
| 1 COGNITIVE RADIO TECHNOLOGY | 1 |
| 1.1. RADIO SPECTRUM MANAGEMENT | 1 |
| 1.1.1. <i>Spectrum Scarcity Problem</i> | 3 |
| 1.1.2. <i>Radio Spectrum Regulation and Shared Spectrum</i> | 6 |
| 1.1.2.1. <i>Licensed Spectrum</i> | 8 |
| 1.1.2.2. <i>Unlicensed Spectrum</i> | 8 |
| 1.2. DYNAMIC SPECTRUM ACCESS | 9 |
| 1.2.1. <i>Dynamic Exclusive Model</i> | 10 |
| 1.2.2. <i>Open Sharing Model</i> | 11 |
| 1.2.3. <i>Hierarchical Access Model</i> | 11 |
| 1.3. DEFINITION OF CR SYSTEMS..... | 11 |
| 1.3.1. <i>CRT's Benefits and Criteria</i> | 14 |
| 1.3.2. <i>Standardization Activities</i> | 17 |
| 1.4. COGNITIVE RADIO NETWORK..... | 18 |
| 2 COGNITIVE RADIO OPERATIONS & SPECTRUM AWARENESS | 21 |
| 2.1. COGNITIVE RADIO CYCLE | 21 |
| 2.1.1. <i>Spectrum Sharing</i> | 23 |
| 2.1.2. <i>Spectrum Mobility</i> | 23 |
| 2.1.3. <i>Spectrum Decision</i> | 25 |
| 2.2. SPECTRUM AWARENESS..... | 26 |
| 2.2.1. <i>Passive awareness</i> | 28 |
| 2.2.2. <i>Spectrum Sensing</i> | 31 |

| | | |
|----------|--|-----------|
| 2.2.2.1. | <i>Spectrum Sensing Algorithms</i> | 32 |
| 2.2.2.2. | <i>Spectrum Sensing challenges</i> | 37 |
| 2.2.2.3. | <i>Basic Framework for Spectrum Sensing</i> | 38 |
| 2.3. | COOPERATIVE SPECTRUM SENSING | 40 |
| 2.3.1. | <i>Cooperative strategies</i> | 43 |
| 2.3.2. | <i>Data fusion techniques for CSS</i> | 46 |
| 2.3.3. | <i>Basic Framework for CSS</i> | 48 |
| 2.3.4. | <i>CSS challenges</i> | 48 |
| 3 | SECURITY ISSUES OF CRT | 51 |
| 3.1. | A CLASSIFICATION OF THE MAIN COGNITIVE THREATS | 51 |
| 3.1.1. | <i>Security Requirements for CRNs</i> | 52 |
| 3.1.2. | <i>Classification of CR's security threats</i> | 53 |
| 3.1.2.1. | <i>Conventional Security Threats</i> | 58 |
| 3.1.2.2. | <i>CR-specific Security Threats</i> | 59 |
| 3.2. | PRIMARY USER EMULATION ATTACK | 62 |
| 3.2.1. | <i>PUE Attackers Classification</i> | 63 |
| 3.2.2. | <i>Effects of PUE attack in a CRN</i> | 64 |
| 3.2.3. | <i>CRN in Presence of PUE attackers</i> | 65 |
| 3.3. | COGNITIVE JAMMING ATTACK AND ITS EFFECT ON CCC | 67 |
| 3.3.1. | <i>Strategies of Cognitive Jammers</i> | 69 |
| 3.3.2. | <i>CCC vs Cognitive Jamming</i> | 70 |
| 3.4. | BYZANTINE ATTACK | 71 |
| 3.4.1. | <i>Attack's parameters</i> | 72 |
| 3.4.2. | <i>Attack strategies</i> | 74 |
| 4 | PERFORMANCE IMPROVEMENT OF CSS IN TRUSTED CNR | 78 |
| 4.1. | CSS IN PRESENCE OF CORRELATED SUs' OBSERVATIONS | 78 |
| 4.2. | MODIFIED TWIN TEST..... | 80 |
| 4.3. | SIMULATION RESULTS | 83 |
| 4.4. | EXTENDED MTT IN PRESENCE OF NOISE UNCERTAINTY | 87 |

| | | |
|----------|--|------------|
| 4.5. | EXPERIMENTAL RESULTS OF THE EMTT | 89 |
| 5 | FINE GRAINED ANALYSIS OF PACKETS LOSS IN CRSN | 93 |
| 5.1. | CRSN AND SECURITY THREATS | 93 |
| 5.2. | RELATED WORKS ON PACKET LOSSES INVESTIGATION | 96 |
| 5.3. | SYSTEM MODEL..... | 97 |
| 5.3.1. | <i>Conventional FGA method.....</i> | <i>99</i> |
| 5.4. | A STATISTICALLY-ENHANCED PROFILING TECHNIQUE | 100 |
| 5.4.1. | <i>Motivations.....</i> | <i>100</i> |
| 5.4.2. | <i>Rationale</i> | <i>101</i> |
| 5.4.3. | <i>Statistical Profiling Comparison Algorithm.....</i> | <i>103</i> |
| 5.5. | EVALUATION RESULTS | 104 |
| 5.5.1. | <i>Jamming Attack.....</i> | <i>105</i> |
| 5.5.2. | <i>Selective Forwarding</i> | <i>109</i> |
| 5.5.3. | <i>Sample Precision.....</i> | <i>109</i> |
| 5.5.4. | <i>Consideration about different path-loss models.....</i> | <i>111</i> |
| 6 | PERFORMANCE IMPROVEMENT OF CSS IN UNTRUSTED CRN | 112 |
| 6.1. | CONVENTIONAL METHOD AGAINST BYZANTINE ATTACKS..... | 113 |
| 6.2. | PROPOSED REPUTATION-BASED APPROACH | 116 |
| 6.3. | EXPERIMENTAL RESULTS | 119 |
| | CONCLUSIONS | 127 |
| | SUMMARY OF CONTRIBUTIONS..... | 127 |
| | DESIGN RECOMMENDATIONS AND FURTHER WORK | 129 |
| | REFERENCES..... | 131 |

List of Figures

| | |
|--|----|
| FIGURE 1. ITU’S FREQUENCY ALLOCATION MAP [2]..... | 2 |
| FIGURE 2. DYNAMIC SPECTRUM ACCESS MODELS. | 10 |
| FIGURE 3. BROWSE SPECTRUM FUNCTION OF GOOGLE SPECTRUM DATABASE WEBSITE. | 15 |
| FIGURE 4. IEEE SCC41 ORGANIZATION STRUCTURE..... | 17 |
| FIGURE 5. ARCHITECTURE OF A COGNITIVE RADIO NETWORK..... | 19 |
| FIGURE 6. COGNITIVE CYCLE OF COGNITIVE RADIO OPERATION. | 22 |
| FIGURE 7. SPECTRUM MANAGEMENT FRAMEWORK FOR COGNITIVE RADIO NETWORKS [16]..... | 24 |
| FIGURE 8. SPECTRUM AWARENESS CLASSIFICATION FOR COGNITIVE RADIO. | 26 |
| FIGURE 9. SPECTRUM DATABASE IN PASSIVE AWARENESS..... | 29 |
| FIGURE 10. ASPECT OF SPECTRUM SENSING FUNCTION FOR CRT..... | 31 |
| FIGURE 11. TEMPERATURE OF INTERFERENCE [23]..... | 33 |
| FIGURE 12. ACCURACY VS COMPLEXITY COMPARISON OF DIFFERENT SPECTRUM SENSING APPROACHES PERFORMED BY A SU | 36 |
| FIGURE 13. EXAMPLES OF HIDDEN PRIMARY USER PROBLEM, WHERE THE DASHED CIRCLES REPRESENT THE OPERATING RANGES OF THE PU TRANSMITTER AND THE SU, IN PRESENCE OF INTERFERENCE WITH PU RECEIVER. | 38 |
| FIGURE 14. ED-BASED SPECTRUM SENSING. | 40 |
| FIGURE 15. THREE-STATE-BASED PROCESS OF COOPERATIVE SENSING..... | 41 |
| FIGURE 16. FINE-GRAINED DEFINITION OF CSS CHARACTERIZED BY SEVEN ELEMENTS. | 42 |
| FIGURE 17. THE THREE MAIN COOPERATIVE MODELS: (A) CENTRALIZED, (B) DISTRIBUTED, AND (C) RELAY-ASSISTED. | 43 |
| FIGURE 18. CENTRALIZED CSS FRAMEWORK [97]..... | 45 |
| FIGURE 19. COGNITIVE CYCLE’S STAGES AFFECTED BY ATTACKERS..... | 54 |
| FIGURE 20. CATEGORIZATION OF DIFFERENT ATTACK SCENARIOS IN A CRN [142]..... | 56 |
| FIGURE 21. EFFECTS OF THE PUEA, BYZANTINE AND JAMMING ON THE COGNITIVE CYCLE. | 61 |
| FIGURE 22. CENTRALIZED CRN IN PRESENCE OF PUE ATTACKERS. | 66 |
| FIGURE 23. EXAMPLE OF A CRN IN PRESENCE OF A COGNITIVE JAMMER..... | 68 |
| FIGURE 24. CLASSIFICATION OF TYPICAL BYZANTINE ATTACK PARAMETERS [163]. | 72 |

| | |
|--|-----|
| FIGURE 25. PRINCIPAL STRATEGIES OF BYZANTINE ATTACK [163]..... | 75 |
| FIGURE 26. BLOCK DIAGRAM OF PROPOSED EMTT METHOD UNDER NOISE UNCERTAINTY CONSIDERING CORRELATED USERS. | 81 |
| FIGURE 27. SIMPLIFIED BLOCK SCHEME OF THE MTT METHODS. | 82 |
| FIGURE 28. PD OF ALL THE CONSIDERED METHODS FOR THREE CORRELATED OBSERVATIONS AND: A) $\rho = 0.1$; B) $\rho = 0.5$ | 84 |
| FIGURE 29. PD OF ALL THE CONSIDERED METHODS FOR FIVE CORRELATED OBSERVATIONS AND: A) $\rho = 0.1$; B) $\rho = 0.5$ | 84 |
| FIGURE 30. PD OF ALL THE CONSIDERED METHODS FOR TEN CORRELATED OBSERVATIONS AND: A) $\rho = 0.1$; B) $\rho = 0.5$ | 84 |
| FIGURE 31. DETECTION GAIN OF ALL THE CONSIDERED METHODS VERSUS THE CORRELATION COEFFICIENT FOR: A) $M = 5$ AND; B) $M = 10$ CORRELATED USERS. | 85 |
| FIGURE 32. MDT GAIN OF THE NEW TEST VERSUS THE CONVENTIONAL OR METHOD, FOR SEVERAL CORRELATION COEFFICIENTS, AND FOR A NUMBER OF SENSORS $M = 3, 5, 10$ | 86 |
| FIGURE 33. PERFORMANCE COMPARISON OF THE EMTT AMONG DIFFERENT VALUES OF ρ COEFFICIENT (I.E. $\rho \in [0.1 \ 0.6]$) AT 1 DB NOISE UNCERTAINTY. | 90 |
| FIGURE 34. PERFORMANCE COMPARISON OF THE EMTT AMONG DIFFERENT VALUES OF NOISE UNCERTAINTY (I.E. 0 DB, 0.1 DB, 0.5 DB, AND 1 DB) AT $\rho = 0.3$ | 91 |
| FIGURE 35. PD OF THE EMTT AND CONVENTIONAL METHODS AT $\rho = 0.3$ AND IN PRESENCE OF NOISE UNCERTAINTY: A) EQUAL TO 0.1 DB; B) EQUAL TO 1 DB. | 92 |
| FIGURE 36. SCHEME OF THE STATISTICAL PROFILE COMPARISON ALGORITHM..... | 104 |
| FIGURE 37. SNAPSHOT OF THE NETWORK PORTION (A) IN PRESENCE OF AN INTERFERENCE ATTACK GENERATED BY THE JAMMER NODE, J, (B) HIGHLIGHTING THE COMMUNICATION LINK AMONG THE NETWORK'S NODES. | 105 |
| FIGURE 38. VARIANCES OF THE TESTING VARIABLE VERSUS THE NUMBER OF SAMPLES AT DIFFERENT FALSE ALARM RATES. | 106 |
| FIGURE 39. THEORETICAL (THEOR.) AND EXPERIMENTAL (SIM.) PROBABILITY OF DETECTION OF THE PROPOSED METHOD FOR THE LINK 2-3 AND SEVERAL VALUES OF SNR AND DIFFERENT FALSE ALARM PROBABILITIES EXPLOITING: A) THE RSSI VARIANCE; B) THE LQI VARIANCE. SIMULATION (DOTTED LINES); THEORY (SOLID LINES). | 107 |
| FIGURE 40. THEORETICAL (THEOR.) AND EXPERIMENTAL (SIM.) PROBABILITY OF DETECTION OF THE PROPOSED METHOD FOR THE LINK 2-7 AND SEVERAL VALUES OF SNR AND DIFFERENT FALSE | |

| | |
|---|-----|
| ALARM PROBABILITIES EXPLOITING: A) THE RSSI VARIANCE; B) THE LQI VARIANCE. SIMULATION (DOTTED LINES); THEORY (SOLID LINES). | 107 |
| FIGURE 41. THEORETICAL (THEOR.) AND EXPERIMENTAL (SIM.) PROBABILITY OF DETECTION OF THE PROPOSED METHOD FOR THE LINK 4-5 AND SEVERAL VALUES OF SNR AND DIFFERENT FALSE ALARM PROBABILITIES EXPLOITING: A) THE RSSI VARIANCE; B) THE LQI VARIANCE. SIMULATION (DOTTED LINES); THEORY (SOLID LINES). | 107 |
| FIGURE 42. THEORETICAL ROC CURVES FOR SEVERAL VALUES OF SNR EXPLOITING: A) THE RSSI VARIANCE; B) THE LQI VARIANCE. | 108 |
| FIGURE 43. THEORETICAL (THEOR.) PROBABILITY OF DETECTION OF THE PROPOSED METHOD FOR THE TWO CONSIDERED DATASETS AND SEVERAL VALUES OF SNR AND DIFFERENT FALSE ALARM PROBABILITIES EXPLOITING: A) THE RSSI VARIANCE OF THE LINK 2-7; B) THE LQI VARIANCE OF THE LINK 2-7; C) THE RSSI VARIANCE OF THE LINK 4-5; B) THE LQI VARIANCE OF THE LINK 4-5. THEORETICAL PD OF THE DOUBLE PRECISION DATASET (DOTTED LINES); THEORETICAL PD OF THE TRUNCATED DATASET (SOLID LINES)..... | 110 |
| FIGURE 44. SIMPLIFIED FLOWCHART OF THE PROPOSED REPUTATION-BASED CSS. | 118 |
| FIGURE 45. THE ROC CURVES OF THE NEW AND CONV. METHODS (IN BLIND AND TNA MODES) IN PRESENCE OF 2 AF ATTACKERS FOR SNR = -11dB | 121 |
| FIGURE 46. THE ROC CURVES OF THE NEW AND CONV. METHODS (IN BLIND AND TNA MODES) IN PRESENCE OF 2 OPP. ATTACKERS FOR SNR = -11dB | 121 |
| FIGURE 47. THE ROC CURVES OF THE NEW AND CONV. METHODS (IN BLIND AND TNA MODES) IN PRESENCE OF 2 SAF ATTACKERS FOR SNR = -11dB | 121 |
| FIGURE 48. NUMBER OF: (RED) CORRECTLY IDENTIFIED MALICIOUS USERS; (BLUE) DISCARDED MISBEHAVED SUs IN PRESENCE OF AT LEAST 3 AB ATTACKERS (SNR = -11dB)..... | 123 |
| FIGURE 49. NUMBER OF: (RED) CORRECTLY IDENTIFIED MALICIOUS USERS; (BLUE) DISCARDED MISBEHAVED SUs IN PRESENCE OF AT LEAST 3 OPP. ATTACKERS (SNR = -11dB)..... | 123 |
| FIGURE 50. NUMBER OF: (RED) CORRECTLY IDENTIFIED MALICIOUS USERS; (BLUE) DISCARDED MISBEHAVED SUs IN PRESENCE OF AT LEAST 3 SAF ATTACKERS (SNR = -11dB)..... | 123 |
| FIGURE 51. PD OF THE NEW AND CONV. METHODS (IN BLIND AND TNA MODES) IN PRESENCE OF THE AF ATTACK VERSUS THE NUMBER OF SUs IN PRESENCE OF 10% OF MALICIOUS USERS (SNR = -11dB). | 124 |
| FIGURE 52. PD OF THE NEW AND CONV. METHODS (IN BLIND AND TNA MODES) IN PRESENCE OF THE OPP. ATTACK VERSUS THE NUMBER OF SUs IN PRESENCE OF 10% OF MALICIOUS USERS (SNR = -11dB)..... | 124 |

| | |
|---|-----|
| FIGURE 53. <i>PD</i> OF THE NEW AND CONV. METHODS (IN BLIND AND TNA MODES) IN PRESENCE OF THE SAF ATTACK VERSUS THE NUMBER OF SUS IN PRESENCE OF 10% OF MALICIOUS USERS (<i>SNR</i> = <i>-11dB</i>)..... | 125 |
| FIGURE 54. NUMBER OF: (BLUE) DISCARDED MISBEHAVED SUS; (RED) CORRECTLY IDENTIFIED MALICIOUS SUS AND (GRAY) MISBEHAVED SUS IN PENDING STATE WITH 10% OF THE THREE ATTACKERS (<i>SNR</i> = <i>-11 dB</i>). | 125 |

List of Tables

| | |
|---|-----|
| TABLE 1. FREQUENCY RANGE FOR EACH ITU'S REGION [1] - [2]..... | 1 |
| TABLE 2. REGULATORY AND STANDARDIZATION BODIES IN EUROPE. | 3 |
| TABLE 3. POLICY OPTIONS FOR PRIMARY AND SECONDARY USERS [26]..... | 7 |
| TABLE 4. CR'S FEATURES IDENTIFIED BY FCC..... | 12 |
| TABLE 5. CRITERIA FOR TARGETING PROMISING CR SCENARIOS. | 16 |
| TABLE 6. COMPARISON OF NON-COOPERATIVE SPECTRUM SENSING TECHNIQUES. | 36 |
| TABLE 7. COMPARISON BETWEEN CENTRALIZED AND DISTRIBUTED CSS..... | 45 |
| TABLE 8. EXTENDED SECURITY REQUIREMENTS OF ITU [131]. | 53 |
| TABLE 9. SUMMARY OF THE COGNITIVE THREATS [131]..... | 57 |
| TABLE 10. ATTACKERS CHARACTERIZATION. | 58 |
| TABLE 11. SUMMARIZATION OF THE MAIN INFRASTRUCTURE-BASED CRN ATTACKS. | 62 |
| TABLE 12. IMPACT OF JAMMING ATTACKS. | 70 |
| TABLE 13. SUMMARY OF THE BYZANTINE STRATEGIES BASED ON [163]. | 76 |
| TABLE 14. THE THEORETICAL PROBABILITY OF DETECTION OF THE PROPOSED METHOD IN PRESENCE OF A SELECTIVE FORWARDING ATTACKS FOR SEVERAL RELEVANT LINKS. | 109 |

List of Abbreviations

| Name | Acronym |
|---|---------|
| Access Point | AP |
| Additive White Gaussian Noise | AWGN |
| Advance Metering Infrastructures | AMI |
| Always Busy | AB |
| Always Free | AF |
| Authorization and Authentication | A&A |
| Base Station | BS |
| Bit Error Rate | BER |
| Black | B |
| CR Technology | CRT |
| CR ad-hoc network | CRAHN |
| Centralized Dependent Non-Probabilistic Small-Scale | CDNS |
| Centralized Dependent Probabilistic Small-Scale | CDPS |
| Centralized Independent Probabilistic Small-Scale | CIPS |
| Cognitive Jammers | CJs |
| Cognitive Radio Networks | CRNs |
| Cognitive Radio Wireless Sensor Networks | CR-WSNs |
| Cognitive Radio sensor network | CRSN |
| Cognitive Radio | CR |
| Common Control Channel | CCC |
| Compounded Average Growth Rate | CAGR |
| Concurrent Spectrum Access | CSA |
| Cooperative spectrum sensing | CSS |
| Decentralized Independent Probabilistic Small-Scale | DIPS |
| Denial of Service | DoS |
| Detection Gain | D_G |
| Digital Signal Processor | DSP |

| | |
|---|------------|
| Digital Television | DTV |
| Direct Sequence | DS |
| Dynamic Frequency Selection | DFS |
| Dynamic Spectrum Access | DSA |
| Energy Detection | ED |
| Energy with Min Eigenvalue | EME |
| European Commission | EC |
| European Communication Office | ECO |
| European Conference of Postal and Telecommunication Administrations | ECPT |
| European Conference of Postal and Telecommunications Administrations | ECPT |
| European Telecommunications Standards Institute | ETSI |
| European Union | EU |
| Extended MTT | EMTT |
| Extended Modified Generalized-Q | EMGQ |
| Federal Communication Commission | FCC |
| Field Area Networks | FAN |
| Field Programmable Gate Array | FPGA |
| Fifth Generation | 5G |
| Fine-Grained Analysis | FGA |
| Frequency Modulation | FM |
| Frequency hopping | FH |
| Fusion center | FC |
| Gray | G |
| Hostile Jamming | HJ |
| Industrial | Scientific |
| Information Assurance | IA |
| Information | I_i |
| Institute of Electrical and Electronics Engineers | IEEE |
| International Telecommunication Union | ITU |
| Intrusion Detection Systems | IDSes |

| | |
|---|-----------------|
| Language Laboratory Virtual Instrument Engineering Workbench | LabVIEW |
| Likelihood Ratio Test | LRT |
| Link Quality Indicator | LQI |
| Long Term Evolution | LTE |
| Majority | MAJ fusion rule |
| Max Eigenvalue detection | MED |
| Max-Min Eigenvalue detection | MME |
| Maximum Ratio Combining | MRC |
| Mean Detection Time | MDT |
| Medium Access Control | MAC |
| Mobile Ad-Hoc Networks | MANET |
| Modified Twin Test | MTT |
| Narrowband | NB |
| Opportunistic Spectrum Access | OSA |
| Opposite | Opp |
| Over-The-Air | OTA |
| PUE attack | PUEA |
| Physical | PHY |
| Primary Base-Station | PBS |
| Primary User Emulation | PUE |
| Primary Users | PU |
| Probability of Detection | P_D |
| Probability of False alarm P_FA | |
| Pseudo-Random Number | PN |
| Quality of Service | QoS |
| Radio Frequency | RF |
| Radio Spectrum Committee | RSC |
| Radio Spectrum Policy Group | RSPG |
| Radio Spectrum Policy Group | RSPG |
| Received Signal Strength Indicator | RSSI |

| | |
|---|-------|
| Received Signal Strength | RSS |
| Receiver Operating Characteristic | ROC |
| Secondary Users | SU |
| Secondary base station | SBS |
| Selection Combining | SC |
| Service Level Agreements | SLA |
| Signal-to-Noise Ratio | SNR |
| Smart Always Free | SAF |
| Software Defined Radio | SDR |
| Spectrum Brokers | SB |
| Spectrum Databases | SDs |
| Spectrum Sensing Data Falsification | SSDF |
| Square Low Combining | SLC |
| Standards Coordinating Committee 41 | SSC41 |
| Start Frame Delimiter | SFD |
| System Inherent Interference | SII |
| Telecommunications Conformity Assessment and Market Surveillance | TCAM |
| Transmit Power Control | TPC |
| Trusted Node Assistance | TNA |
| Ultra-High Frequency | UHF |
| Universal Software Radio Peripheral | USRP |
| Weighted Sequential Probability Ratio Test | WSPRT |
| White | W |
| Wideband | WB |
| Wireless Local Area Networks | WLANs |
| Wireless Regional Area Networks | WRAN |
| Wireless Sensor Network | WSN |
| Working Groups | WGs |

Abstract

The rapid growth in the demand for wireless broadband applications in both licensed and unlicensed frequency bands has led to an ever-increasing need for radio spectrum. As confirmed by several measurements about spectrum occupancy, the fixed policy adopted by Governments and regulatory Agencies concerning the assignment of the spectrum results in an under-utilization of its usage below 1GHz. This behaviour severely reduces the number of available (i.e., vacant) frequency bands viable to deploy new communication services or to enhance the existing ones. In addition, the continuous development of new technologies requires a more flexible and efficient management of the spectrum to satisfy the goals of the EU Digital Agenda and the future market demands for mobile and broadband services.

A new emerging technology, namely Cognitive Radio (CR), addresses the issue of spectrum scarcity and aims at improving the efficiency of the spectrum. CR-based devices are indeed able to gather information about the surrounding radio environment to dynamically adjust their operational parameters and improve their performance. CR Technology (CRT) promises several benefits such as: the interoperability with new and legacy radio systems; the ability to implement on each radio networking tasks that are transparent to users; the possibility to implement reconfigurable and cost-effective architectures for wireless devices. In addition, CRT paves the way for broadband usage in secure communications – which is currently restricted to only a few available technologies – harmonizing the needs of commercial, public, safety and military users. As a matter fact, CRT can also coexist with the current telecommunication technologies and licensed legacy users, namely Primary Users (PU), allowing unlicensed users, namely Secondary Users (SU), to opportunistically access the unused frequency bands (i.e., the spectrum holes or white spaces). SUs can employ both cooperative and non-cooperative techniques to sense the spectrum. As a matter of fact, spectrum sensing is the main task of SUs, given their ability to detect a PU signal in a certain frequency band. However, in a non-cooperative scenario, with each SU performing the spectrum sensing independently, it might be hard to obtain a reliable decision about the spectrum occupancy. For this reason, several approaches suggest sensing the spectrum through the exploitation of a cooperative scheme that

combines the local decisions of SUs in order to make a global decision about spectrum occupancy.

Cooperative spectrum sensing (CSS) can be classified in three categories: centralized, distributed, and relay assisted. In particular, the centralized CSS is widely considered the conventional solution. In such approach, SUs perform the spectrum sensing independently, sending their decisions to a cognitive base station, namely fusion center (FC), which is responsible for combining them and then reaching the global decision about the spectrum occupancy. This behaviour allows SUs to create cognitive radio networks (CRNs) to communicate without interfering with the primary communications, therefore fulfilling the main constraint of the CRT. Implementing CRNs, however, requires knowledge in different fields of expertise related not only to scientific and technological capabilities for the physical deployment of such networks, but also to marketing and management for the regulation of the coexistence of primary and secondary users.

Even though CSS ensures improvements in terms of performance and spectrum utilization, it poses several challenges that are not to be overlooked in the design and implementation of a cooperative environment. Two typical challenges are: the cooperative sensing in presence of correlated SUs' observations, and the security of CRNs. In particular, when the proximity among SUs results in correlated observations, the performance of the cooperative sensing degrades if the correlated observations are under the conventional threshold of techniques based on the Energy Detection (ED), which leads SUs to interfere with primary communications and to discourage PUs from sharing their licensed spectrum. In addition, the openness of low layers protocol stacks makes CRT vulnerable to different kind of attacks that aim to destroy the typical cognitive operations of legitimate SUs and to allow malicious users to join in the CRN to exploit the available spectrum holes. Then, malicious users can act as the relay nodes of the network accessing the transmitted information, and affect the efficiency of the spectrum, interfering with primary communications. Therefore, the definition of an efficient, secure CRN is a critical challenge that requires not only the definition of techniques to improve the performance of the spectrum sensing (both cooperative and non-cooperative), but also the definition of ad-hoc countermeasures to identify all malicious users, discarding them from the cooperative sensing and the CRN.

The proposed doctoral dissertation aims at addressing the problem of spectrum scarcity by proposing novel signal processing techniques for the performance improvement of CSS in both trusted and untrusted networks (i.e. without and with the presence of attackers).

The remainder of this doctoral thesis is organized as follows.

The first chapter introduces the fundamental concepts behind the CRT. In particular, the current allocation spectrum framework is discussed in detail, highlighting its main drawbacks. Then, the benefits provided by the CRT in overcoming the spectrum scarcity problem are presented, defining the main operating scenarios.

The second chapter describes the CR lifecycle, focusing the attention on the features of spectrum sensing. In particular, an analysis of the techniques and strategies of spectrum sensing (both cooperative and non-cooperative) are presented and discussed in detail, highlighting crucial issues, such as the security of the cooperative sensing and of the network itself.

The third chapter provides an in-depth analysis of the typical security issues affecting CRT. Ensuring the invulnerability of wireless networks is a major challenging task. As any other wireless network, a CRN is vulnerable not only to the well-known attacks used in conventional networks, but also to specific threats that take advantage of the drawbacks innate to CR's operations. A taxonomy of the most popular attacks that affect a cognitive network is provided, focusing, in particular, on three main categories of attacks: Primary User Emulation, Cognitive Jamming, and Byzantine attacks.

In the fourth chapter, a novel cooperative sensing approach is introduced to improve the detection performance in presence of correlated SUs' observations and in trusted CRNs. The proposed method exploits two tests at once to recover those correlated observations that are under the conventional threshold of ED-based techniques, and to

increase the cooperative performance, in the presence of a communication channel affected by additive white Gaussian noise (AWGN) and different levels of noise uncertainty.

The fifth chapter describes a statistical, fine-grained analysis framework for the identification of the root causes of packet losses to distinguish between packet drop and jamming attacks. In particular, the approach builds a statistical model for determining optimal thresholds and testing variables, and for setting an individual threshold for each link of the network by using the typical packet information provided by both CR-based and traditional wireless sensors networks.

Finally, the sixth chapter provides the definition of a new centralized reputation-based CSS in untrusted CRNs affected by Byzantine attackers. In particular, the proposed CSS scheme is based on two features (i.e. a new reputation method, and three dynamic lists) that state the reliability of CR users in a CRN and allow the FC to properly identify Byzantine attackers, without penalizing legitimate users that misbehave due to channel noise. Even though our method is completely blind (i.e. no need for any a-priori information), it can also involve trusted nodes to enhance the system's performance.

List of Personal Publications

Journal Papers

- [J1] F. Benedetto, **A. Tedeschi**, “Cognitive Radio: overview and security threats”, *Synthesis Lectures on Information Security, Privacy, and Trust*, Morgan & Claypool Publishers, submitted, 1st review round, 2016.
- [J2] **A. Tedeschi**, A. Iuliano, F. Benedetto, “StreetFlow: A cloud-based tool for the automatic videos making of visual routes using Google Street View and OpenCV”, *Advanced Engineering Informatics*, submitted, 1st review round, 2016.
- [J3] **A. Tedeschi**, S. Calcaterra, F. Benedetto, “Ultrasonic RADar System (URAS): Arduino and Virtual Reality for a light-free mapping of indoor environments”, *IEEE Sensors Journal*, submitted, 2nd review round, 2016.
- [J4] **A. Tedeschi**, F. Benedetto, “A Real-Time Automatic Pavement Crack and Pothole Recognition System for Mobile Android-based Devices”, *Advanced Engineering Informatics*, in press, 2017.
- [J5] **A. Tedeschi**, D. Midi, F. Benedetto, E. Bertino, “Statistically-enhanced Fine-Grained Diagnosis of Packet Losses”, Special issue on: “Signal Processing, Security and Privacy for Mobile/Wireless and Computer Networks”, *Int. J. of Mobile Network Design and Innovation*, 2016, (in press).
- [J6] **A. Tedeschi**, A. Liguori, F. Benedetto, “Information Security and Threats in Mobile Appliances”, *Recent Patents on Computer Science*, vol. 7, n. 1, 2014.

Editorials

- [E1] F. Benedetto, **A. Tedeschi**, Editorial, *International Journal of Interdisciplinary Telecommunications and Networking (IJITN)* (Special Issue on New Applications and Advanced Methodologies for road safety and simulation), vol. no. 1, 2014. DOI: 10.4018/IJITN, ISSN: 1941-8663, EISSN: 1941-8671.

Book Chapters

- [B1] F. Benedetto, **A. Tedeschi**, “Big Data Sentiment Analysis for Brand Monitoring in Social Media Streams by Cloud Computing”, pp. 341-377 in “Sentiment Analysis and Ontology Engineering: An Environment of Computational Intelligence” , Editors: Witold Pedrycz, Shyi-Ming Chen, published by Springer-Verlag, 2016. DOI: 10.1007/978-3-319-30319-2_14. ISBN 978-3-319-30319-2.
- [B2] F. Benedetto, **A. Tedeschi**, “Chapter 1. The Cognitive Radio Technology: Future Trends in the Spectrum Access of Next Generation Communication Systems”, pp. 1-32, in “Communication Systems: New Research”, Vyacheslav Tuzlukov editor, NOVA Science Publishers, 432 pp. USA, 2013. ISBN: 978-1-62618-654-5.

International Conferences

- [C1] F. Benedetto, G. Giunta, **A. Tedeschi**, P. Coronas, "Detecting Byzantine Attacks in Self-Organizable Networks by a Reputation-Based Cooperative Spectrum Sensing", 26th International Conference on Computer Communication and Networks (ICCCN), July 31-August 3, Vancouver, Canada, 2017.
- [C2] **A. Tedeschi**, S. Dikmese, F. Benedetto, M. Renfors, G. Giunta, “Novel Extended Modified Twin Test Based Sensing For Cooperative Communication Under Noise Uncertainty”, IEEE Global Conference on Signal and Information Processing (GlobalSIP), Greater Washington, D.C., USA, 7-9 December, 2016.
- [C3] F. Benedetto, **A. Tedeschi**, G. Giunta, “Automatic Blind Modulation Recognition of Analog and Digital Signals in Cognitive Radios”, IEEE 84th Vehicular Technology Conference: VTC2016-Fall, 18–21 September 2016, Montréal, Canada.
- [C4] F. Benedetto, G. Giunta, **A. Tedeschi**, “Optimizing The Performance Of Cooperative Spectrum Sensing In Cognitive Radio Communication

- Systems”, IEEE International Workshops on 'Optimization and Inverse Problems in Electromagnetism' (OIPE), Roma, Italy, 13-15 September 2016.
- [C5] F. Benedetto, A. Tedeschi, G. Giunta, P. Coronas, “Performance Improvements of Reputation-Based Cooperative Spectrum Sensing”, 27th IEEE International Symposium on Persona, Indoor and Mobile Radio Communications (PIMRC), Valencia, Spain, 4-7 September 2016. (**Award:** IEEE PIMRC'16 Student Travel Grant).
- [C6] D. Midi, **A. Tedeschi**, F. Benedetto, E. Bertino, “Statistically-enhanced Fine-Grained Diagnosis of Packet Losses”, 2015 IEEE International Conference on Future Internet of Things and Cloud (FiCloud), August 2015, Rome, Italy, pp. 748-753.
- [C7] **A. Tedeschi**, F. Benedetto, “A Cloud-based Big Data Sentiment Analysis Application for Enterprises' Brand Monitoring in Social Media Streams”, 2015 1st IEEE International Forum on Research and Technologies for Society and Industry: Leveraging a better tomorrow (RTSI-2015), September 2015, Torino, Italy, pp. 186-191.
- [C8] F. Benedetto, **A. Tedeschi**, “Moisture Content Evaluation For Road-Surfaces Monitoring By GPR Image And Data Processing On Mobile Platforms”, 2015 IEEE International Conference on Future Internet of Things and Cloud (FiCloud), August 2015, Rome, Italy , pp. 602-607.
- [C9] **A. Tedeschi**, F. Riganti Fulginei, A. Laudani, “PV Panel Modeling: a mobile application for modeling photovoltaic panels using datasheets information”, 2015 IEEE International Conference on Future Internet of Things and Cloud (FiCloud), August 2015, Rome, Italy, pp. 608-613.
- [C10] **A. Tedeschi**, F. Benedetto, L. Paglione, “A Blind Signal Processing Method for Assessing Users' Movements in Indoor Wi-Fi Communications by Android-based Smartphones”, 38th IEEE Int. Conf. on Telecommunications and Signal Processing (TSP 2015), 9-11 July 2015, Prague, Czech Republic , pp. 149-153.
- [C11] F. Benedetto, G. Giunta, **A. Tedeschi**, E. Guzzon, “Performance Improvements of Cooperative Spectrum Sensing in Cognitive Radio Networks with Correlated Cognitive Users”, 38th IEEE Int. Conf. on

Telecommunications and Signal Processing (TSP 2015), 9-11 July 2015, Prague, Czech Republic , pp. 1-5.

- [C12] F. Benedetto, **A. Tedeschi**, “GPR Image and Signal Processing for Pavement and Road Monitoring on Android Smartphones and Tablets” - EGU 2014 General Assembly Conference Abstracts.
- [C13] F. Benedetto, **A. Tedeschi**, G. Giunta, “Cooperative Spectrum Sensing for Positioning in Cognitive Radios”, 11th International Symposium on Wireless Communication Systems, ISWCS, 2014, pp. 670-674.
- [C14] **A. Tedeschi**, F. Benedetto, “A cloud-based tool for brand monitoring in social networks”, 1st International Workshop on Social Networks Analysis, Management and Security, SNAMS, Aug., 2014, pp. 541-546.
- [C15] F. Benedetto, **A. Tedeschi**, G. Giunta, “Brand Monitoring in the Twitter Social Network for Electronic Commerce”, Networking and Electronic Commerce Research Conference, Aug., 2014, pp. 1-16.
- [C16] F. Benedetto, **A. Tedeschi**, “A Mobile Android Application for Road and Pavement Inspection by GPR Data Processing”, 15th International Conference on Ground Penetrating Radar, GPR, July, 2014, pp. 842-846.

1 Cognitive Radio Technology

This first chapter introduces the fundamental concepts of the Cognitive Radio Technology (CRT), highlighting its benefits in overcoming the spectrum scarcity problem.

1.1. Radio Spectrum Management

Radio spectrum is an important and natural resource shared by various types of wireless services. It can be re-used, if certain technical conditions are met, and can simultaneously accommodate a limited number of users.

Nowadays, a large portion of the radio spectrum is assigned by the different governments to authorized user through a spectrum regulatory framework, which helps to carefully manage the spectrum, while maximizing its value for all users. The current regulatory framework is based on static spectrum allocation and on an assignment policy that refers to command and control mechanisms, specifying technologies and services for spectrum uses. As described in the Radio Regulations [1], published by the International Telecommunication Union (ITU) and containing the services' definitions and the allocations' table for the three ITU regions, the radio spectrum is allocated to the radio services on a primary or secondary basis. For the frequency allocation, the ITU divides the world in three regions (see Figure 1) assigning them three different ranges of frequency bands, as depicted in Table 1.

Table 1. Frequency Range for each ITU's region [1] - [2].

| Region | Frequency Range |
|-----------------|--|
| Region 1 | 380-470 MHz |
| Region 2 | 746-806 MHz, 806-869 MHz, 4 940-4 990 MHz |
| Region 3 | 406.1-430 MHz, 440-470 MHz, 806-824/851-869 MHz, 4 940-4 990 MHz and 5 850-5 925 MHz |

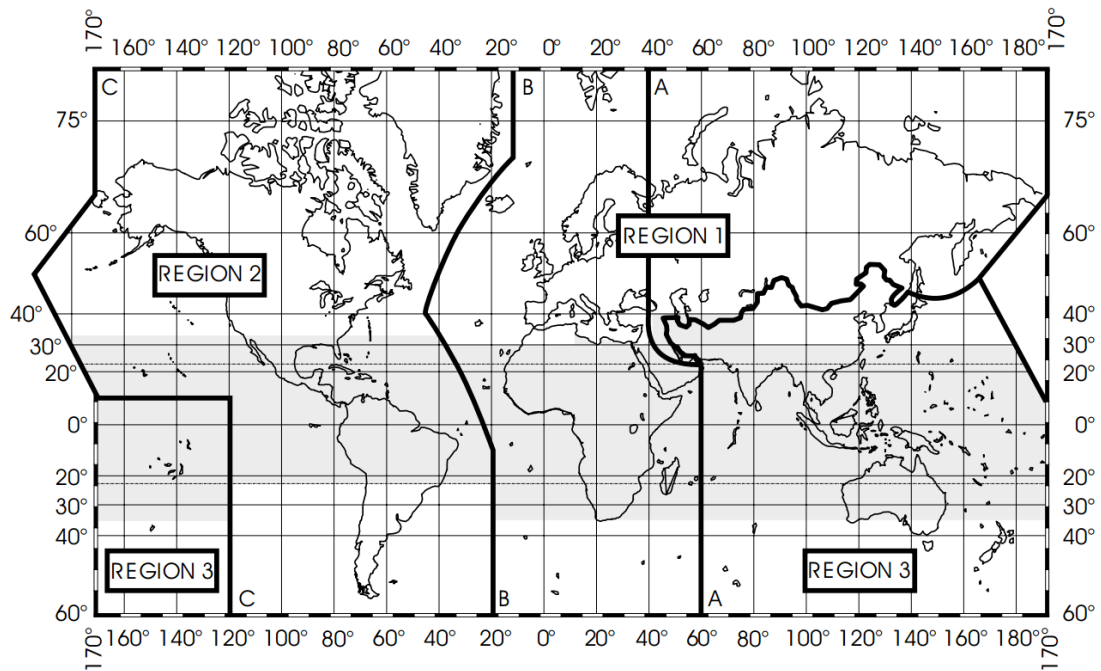


Figure 1. ITU's frequency allocation map [2].

The radio spectrum is managed through a regulatory body that varies for each country. For example, in USA, radio spectrum is managed by the Federal Communication Commission (FCC) and the National Telecommunications and Information Administration (NTIA), which regulate radio, television, wire, satellite, and cable communications taking place among the states or internationally [3]. In particular, the FCC defines and maintains a database listing of Frequency Modulation (FM) and Digital Television (DTV) frequencies, namely Table of Allotments, currently not assigned [4]. In Europe, the European Union (EU) governs the spectrum through several entities such as the European Conference of Postal and Telecommunications Administrations (ECPT), the Radio Spectrum Policy Group (RSPG) and the Radio Spectrum Committee (RSC) [5]. These entities not only aid the EU in the spectrum regulation, they also participate in the standardization process as described in Table 2. For a proper, country-specific disposal of the radio spectrum, the regulatory bodies delegate its management to national regulatory agencies, which define their own allocation tables and assign frequency bands to users on a long term, exclusive basis and for large geographical regions. Therefore, the only way for users to gain exclusive access to a portion of the radio spectrum, is to own an individual license issued by the national regulatory agency itself. This mechanism is crucial in improving the design of mobile communication systems, since it is easier to develop

Table 2. Regulatory and standardization bodies in Europe.

| Regulatory and standardization body | Description |
|---|--|
| European Conference of Postal and Telecommunication Administrations (ECPT) | It allows the European policy makers and regulators to collaborate in order to improve the radio spectrum and postal regulation [6]. |
| European Communication Office (ECO) | It is the Secretariat of the CEPT and aids it to develop and deliver its policies and decisions in an effective and transparent way. |
| European Telecommunications Standards Institute (ETSI) | It is responsible for most of the European telecommunication standardization activities |
| Radio Spectrum Policy Group (RSPG) | It is a high-level advisory group that assists the European Commission (EC) |
| Telecommunications Conformity Assessment and Market Surveillance (TCAM) | It is a regulatory committee that assists the EC in matters regarding conformity assessment and market surveillance |

a system that operates in a dedicated band than a system forced to rely on several. Moreover, spectrum licensing provides an effective way to guarantee adequate quality of service (QoS) and to prevent interferences. Through a detailed analysis of the Article 5 of the ITU's Radio Regulation, it can be assessed that most of the radio spectrum available to each Region is already assigned to specific services. For instance, all three of them exploit the frequency range 495-505 kHz for maritime mobile services, which allows communications between coast and ship stations. In addition, most of the frequency bands for commercial and public services are already licensed, as shown by the analysis of the national spectrum assignment database. Current predictions of further growth of demand for wireless communication services show a substantial increase in the demand for radio spectrum. These circumstances raise serious concerns about future radio spectrum shortages.

1.1.1. Spectrum Scarcity Problem

Radio spectrum is a limited resource and the current static policy has brought to a highly inefficient use of its capabilities by introducing an artificial spectrum scarcity. Several observation surveys about radio spectrum occupancy have proved that most of

the allocated spectrum is not fully used [7]-[13]. In particular, the measurements provided by the FCC in several American cities show large variations in the intensity of spectrum use below 1 GHz [7]-[8]. As a matter of fact, observing two non-adjacent 7 MHz spectrum bands with a sliding 30-second window, the measurements showed that most of the frequencies on one band were fully idle, while on the second one only a fraction of the considered frequency were idle during the observation period. Additional measurements were conducted by the Shared Spectrum Company in the USA on the bands between 30 MHz and 3 GHz [9]. The analyses assessed an average occupancy in the observed locations around 5.2% with a maximum occupancy of 13.1% in New York City and a minimum occupancy of 1% in rural areas. In Europe, several measurements conducted in Germany, Spain, Netherlands, Ireland, France, and Czech Republic [10]-[13] depict a better scenario, ascertaining a higher spectrum occupancy if compared to USA, but still rather low if considered alone. For instance, in the Aachen area (Germany) spectrum occupancy is estimated to take up 32% of the range between 20 and 3000 MHz. This means that spectrum occupancy is moderate below 1 GHz and is very low above 1 GHz. Such discrepancies between spectrum allocation and actual usage prove how the current spectrum management policy has helped creating an artificial shortage of frequency bands, which does not reflect the actual availability of usable radio spectrum.

This near-sighted approach also damages the efforts and investments of manufacturers and telecommunications providers towards the improvement of the spectrum efficiency in terms of bit/s/Hz [5], coverage and traffic capacity. These investments led to the definition of new technologies, such as Long Term Evolution (LTE) and the Fifth Generation (5G). Due to the development of new communication technologies and services, the mobile data traffic is expected to grow at a Compounded Average Growth Rate (CAGR) of 57% between 2014 and 2019, reaching 24.2 Exabyte per month by 2019 [14], while the theoretical and technical limits for spectrum efficiency and coverage are close to being reached [15].

The issues currently hindering a proper management of the spectrum can be summarized in the following points [5]:

- underutilization of the radio spectrum, which is not fully and efficiently exploited in time or space as proved by several measurements campaigns;
- the large amount of time required to introduce a new radio communication service or a new spectrum management approach due to the fragmented nature of the regulatory bodies, especially in Europe;
- financial barriers that prevent small and medium enterprises from accessing the market;
- investments in existing wireless communication infrastructures and spectrum licenses.

In addition, the continuous development of new technologies requires a more flexible and efficient spectrum management that should satisfy the EU Digital Agenda goals and the future market demand for mobile and broadband services. For such reasons, a rapid and more flexible access to the radio spectrum in the ultra-high frequency (UHF) band is required.

To deal with the spectrum allocation congestion and spectrum scarcity problems, the Cognitive Radio Technology (CTR) has been proposed, a technology that allows unlicensed users, namely Secondary Users (SUs), to opportunistically utilize already licensed bands left unused by licensed users [16]-[21]. Such frequency bands are named spectrum holes (or white spaces) and are defined as multidimensional regions within time, space, and frequency [22]. A spectrum hole in space can be described as the area around a primary Base Station (BS) that a SU can adopt for its transmissions at the same frequency. Conversely, a spectrum hole in time is the time slot in which a frequency band can be used by a SU. Lastly, a spectrum hole in frequency is defined as a frequency band in which a SU can transmit without interfering with a PU across different adjacent frequencies.

Through the opportunistic access provided by this technology, it is possible to improve the efficiency of the spectrum utilization and, in perspective, to allow next generations of mobile networks to access radio spectrum bands. A pre-requisite of CRT is the coexistence with current telecommunication technologies and licensed legacy users, namely Primary Users (PU), in the shared spectrum. In spite of being a

promising technology, though, CRT is still an emerging one and faces several research challenges, from concept to practical implementation in everyday use.

1.1.2. Radio Spectrum Regulation and Shared Spectrum

Since the beginning of the 19th century, communication services like radio and television have been regulated to provide a public service on a non-discriminatory basis and with fair and reasonable prices and conditions [23], with the aim of increasing public welfare while reflecting the public interest. In particular, regulators carry out the spectrum regulation based on the following aspects:

- the determination of usable spectrum bands;
- the provision of rights to licensed and/or unlicensed users;
- the definition of rules to constrain the access to the available spectrum.

In the context of radio spectrum regulation, it is necessary to distinguish between *trading*, as a transfer of spectrum usage rights, and *liberalization*, as a weakening of the restrictions and limitations associated with spectrum usage rights related to technologies and services.

The report of the Spectrum Policy Task Force of the FCC defines spectrum regulatory mechanisms, highlighting three different models [24]: a *command-and-control* model; an *exclusive use* model; an *open access* model. The most used one is the *command-and-control* model, which refers to the licensed spectrum for shared usage and unlicensed spectrum.

Radio spectrum regulation has also to take into account the development of access protocols and standards to balance the following goals [25]:

- an adequate QoS should be possible to all radios based on the supported applications;
- no radio should be blocked from spectrum access and transmission for extended periods of time;
- spectrum management policies and standards should not slow down innovations in the economically significant, but rapidly changing, communication sector;

- the limited available spectrum should be used efficiently, including possibilities for a special re-use of the spectrum;
- spectrum can be used in a dynamically adaptive way, taking into account the local communication environment like spectrum usage policies;
- the costs of devices should be not increased significantly through techniques prescribed by regulation.

In addition, for primary and secondary users of the radio spectrum, it possible to identify different regulatory options as summarized in the following Table 3.

Table 3. Policy options for primary and secondary users [26].

| | Application requirements | Regulator controls access | Licensee controls access |
|------------------------|--|--|---|
| Primary Users | Guaranteed QoS | Traditional licensing | Band manager makes guarantees |
| | No guarantee, coexist with other primary devices | Unlicensed band; regulator sets etiquette | Band manager sets etiquette; no guarantees |
| | No guarantee, cooperate with other primary devices | Cooperative mesh network; regulator sets protocol | Cooperative mesh network; licensee sets protocol |
| | Application requirements | Regulator controls access | Primary Licensee controls access (secondary market) |
| Secondary Users | Guaranteed QoS | Not possible | Licensee guarantees QoS (static or dynamic) |
| | No guarantee, coexist with primary devices | Unlicensed underlay with opportunistic access | Secondary market with opportunistic access |
| | No guarantee, cooperate with primary devices | Interruptible secondary operation; regulator sets cooperation protocol | Interruptible secondary operation; licensee sets cooperation protocol |

In particular, focusing on the SUs, they:

- should defer the provided and shared spectrum whenever the primary demands it;

- might attempt to coexist and cooperate with the PU without interfering with its communication;
- should be able to access the spectrum opportunistically, when the channel is free from the PU's communications;
- can learn when it is possible to start and interrupt communication through explicit signalling. Generally, regulators grant permission for secondary access and define the signalling protocol.

It is interesting to note that if a PU has enough flexibility, it may choose to grant secondary access instead, by creating a secondary market to rent the unused portion of the spectrum. This approach can guarantee an adequate QoS for the SUs [27].

1.1.2.1. Licensed Spectrum

As mentioned above, most of the radio spectrum is allocated to licensed radio services following the command-and-control model. These licenses provide spectrum users with an exclusive access to the radio spectrum and allow sharing it through strictly regulated devices. For such privilege, PUs pay a fee that also grants them several advantages, such as the possibility to prevent potential interference, avoiding potential dangers for reliable and chargeable communications.

Due to the spectrum scarcity, licensed spectrum becomes a valuable, leading resource for economic profits since consumers must to pay to use it. Because of this commercial impact, several requirements must be met to gain spectrum licenses (e.g. the network must be able to reach a certain percentage of the population when purchasing the spectrum for wireless communication).

Nowadays, the spectrum is for shared usage and it is restricted only to specific technologies through the regulation of emission parameters, such as transmission power and interference to neighbouring frequencies like out of band emissions.

1.1.2.2. Unlicensed Spectrum

Access to unlicensed spectrum is unrestricted and, currently, several users are sharing the same unlicensed portion of the spectrum. Its utilization, however, is strictly

regulated and, in order to mitigate potential interference, it is allowed solely to devices that satisfy specific requirements, standards and technical rules, such as limitation of transmission power and advanced coexistence capabilities. The usage rights for unlicensed spectrum are flexible and no concrete methods to access it are specified [25].

In 2004, the under-utilization of TV bands in the USA, led the FCC to allow unlicensed systems (i.e. SUs) to use such frequency bands [28]. In addition, the FCC extended the use of the new spectrum to wireless broadband communication in the range of 3.65-3.7 GHz for mobile and fixed devices transmitting at a higher power [28].

It is envisaged that multiple users share this spectrum minimizing interference between fixed and mobile operation through the use of contention-based protocols, which will help to reduce the chances of interference from co-frequency operations by managing each station's access to the spectrum.

1.2. Dynamic Spectrum Access

According to the definition of the IEEE Standard 1900.5 [29], the Dynamic Spectrum Access (DSA) is:

“The real-time adjustment of spectrum utilization in response to changing circumstances and objectives.”

In particular, the term *changing circumstances* includes (but it is not limited to) energy consumption, interface avoidance, spectrum usage efficiency and changes in the radio device. Through the DSA, it is possible to efficiently and effectively allocate the unused bandwidth and to overcome, in combination with the CRT, the current spectrum management problem, reducing the unused spectrum bands [30]. Through the CRT, a radio device can exploit the unused frequency bands in time and space without interfering with a PU's transmission. Such behaviour allows CR to dynamically access the unused bands for their own communications [31].

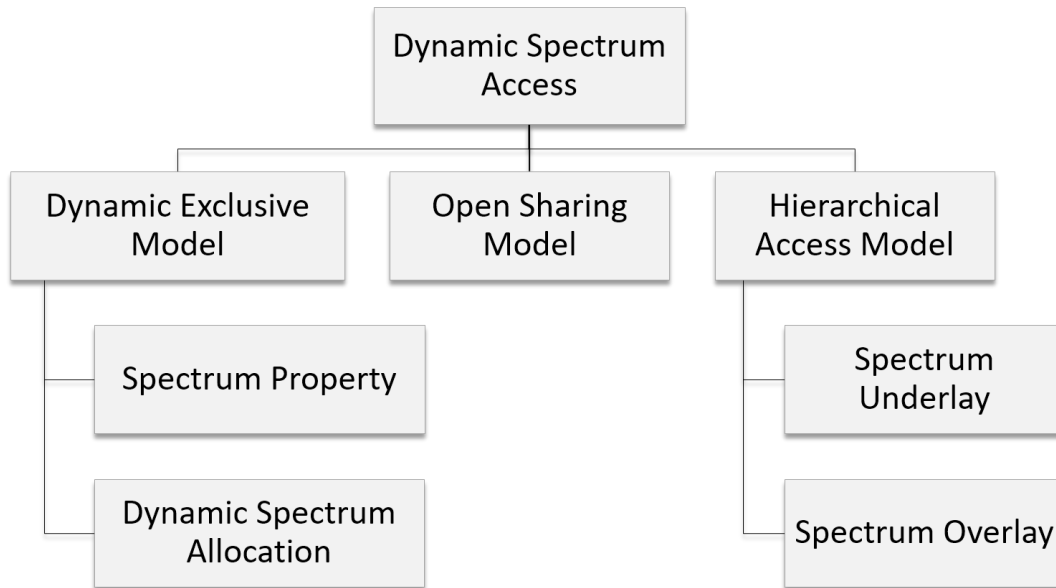


Figure 2. Dynamic Spectrum Access Models.

As shown in Figure 2, several strategies have been proposed in literature for the DSA, distinguishing among three different models:

- Dynamic Exclusive Model;
- Open Sharing Model;
- Hierarchical Access Model.

1.2.1. Dynamic Exclusive Model

The Dynamic Exclusive Model allows regulators to allocate spectrum bands following the current fixed spectrum regulation policy and dynamically assigning the spectrum. The main rationale behind this model is to provide flexibility in spectrum allocation and to improve spectrum efficiency by proposing two different approaches:

- the spectrum property rights allow licensed users to sell or trade the spectrum with unlicensed ones [32]-[33]. The main benefits are related to the market opportunities that will play an important role in driving toward a more profitable use of the radio spectrum;
- the DSA aims to improve the spectrum efficiency by exploiting both the spatial and the temporal variation of the communication traffic [34].

Even though this model allows service providers to efficiently use the available spectrum, it is based on the current regulatory policy and it does not decrease spectrum holes related to the bursting nature of wireless traffic.

1.2.2. Open Sharing Model

The open sharing model is based on the same approach used for the Industrial, Scientific, and Medical (ISM) radio bands, like WiFi. Through this model, users can share the same frequency band at the same time and in the same geographic location avoiding interference among them [35].

1.2.3. Hierarchical Access Model

This model exploits a hierarchical access structure with PUs and Sus, defining two different models:

- the Opportunistic Spectrum Access (OSA) model, which allows SUs to access a licensed band only if the PUs are not using it for their own communication. In addition, PUs have the absolute priority on the available spectrum and if they need to use it, then the SUs must yield to them;
- the Concurrent Spectrum Access (CSA) model, which allows SUs and PUs to coexist together at the same time and in the same geographic region if the SUs' interference with a PU is below a tolerable threshold [36]-[37]. To reach this goal, two approaches have been proposed. In the first approach a SU can spread its transmit power over a wide range of frequency bands to reduce the interference level and to stay below the established interference threshold. This approach is typically used for short range communications. The second approach, namely interference temperature, allows SUs to transmit with a higher power than the first approach if the total interference caused by SUs is below the interference temperature limit [38].

1.3. Definition of CR systems

According to American Heritage [39] and Collins English [40] dictionaries, the term *cognition* is referred to:

- the mental process of knowing, including aspects such as awareness, perception, reasoning, and judgment;
- something comes to be known, as through perception, reasoning, or intuition; knowledge;
- the mental act or process by which knowledge is acquired, including perception, intuition, and reasoning;
- the knowledge that results from such an act or process.

According to this definition, it is possible to describe a CR device as a self-aware communication system that is able to efficiently exploit the radio spectrum adopting adequate approaches. In particular, a CR device can autonomously detect unused frequency bands by observing the radio spectrum.

CR concept was first introduced by Mitola and Maguire in [24]. The authors presented it as an evolution and extension of the software defined radio (SDR) technology meant to improve the flexibility of personal wireless services. In particular, the architecture of a CR device can be described as an integrate agent for SDR in the intersection of personal wireless technology and computational intelligence [25]. A CR is an intelligent wireless communication system and it is a fully re-configurable radio device that can *cognitively* adapt itself to:

- the communications requirements of its user;
- the radio frequency environment in which it is operating;
- the different kinds of network and regulatory policies [20].

A CR is aware of its surrounding environment and, by learning from it, it can adapt its internal states to statistical variations in the incoming radio frequency stimuli by making corresponding changes in certain operating parameters in real time with two primary objectives: granting highly reliable communications whenever and wherever needed and ensuring an efficient utilization of the radio spectrum [41].

Table 4. CR's features identified by FCC.

| Features | Description |
|-------------------|--|
| Frequency Agility | a SU can change its operating frequency to optimize its use in its adaptation to the environment |

| | |
|-----------------------------------|--|
| Dynamic Frequency Selection (DFS) | a SU senses signals from nearby transmitters to choose an optimal operation environment |
| Adaptive Modulation | the transmission characteristics and waveforms can be reconfigured to exploit every spectrum opportunity. In particular, the modulation scheme should be dynamically adapted to the user's requirements and to the channel conditions |
| Transmit Power Control (TPC) | the transmission power is adapted to full power limits when necessary, and/or to lower levels to allow a better sharing of the spectrum. For instance, if any high-power operation is required, the radio device should transmit with low power to decrease the interference and allow other radios to share the spectrum hole |
| Location Awareness | a SU is able to determine its location and that of other devices operating in the same spectrum to optimize transmission parameters |
| Communication Technology | a SU should be able to provide interoperability among different communication systems. The transmission parameters of a SU should be re-configured at the beginning and during the transmissions. In addition, in case the CR switches to another spectrum band, its operational parameters should change accordingly |
| Negotiated Use | a SU should have algorithms enabling the sharing of spectrum in terms of prearranged agreements |

Even though CRT is achieving great goals, this technology is unlikely to create a fully capable CR device in the next years and it requires a gradual development of certain cognitive features which are to be integrated in radio equipment in the near future. As reported in Table 4, the FCC has identified many features that CRs should possess in order to improve the spectrum's usage and its flexibility.

Considering such requirements, modern Wireless Local Area Networks (WLANs) can already be regarded as cognitive radios. IEEE 802.11 systems operate with a listen-before-talk spectrum access, dynamically changing their operation frequencies and controlling their transmission power. Recently, CRs are also referred to as *spectrum agile radios* to put an emphasis on the dynamic use of the spectrum [42]-[43]. Mangold *et al.*, in [42], focus thereby on IEEE 802.11k for radio resource measurements as a technique to facilitate the development of spectrum agile radios, while Mangold *et al.* in [43] introduce spectrum agile radios as a society of value-oriented machines. Basic

concepts taken from social science are used to classify the social action of independent decision-makers.

This understanding of cognitive radios is summarized in the following definition of cognitive radio from Haykin [17]:

“Cognitive radio is an intelligent wireless communication system that is aware of its surrounding environment (i.e., outside world), and uses the methodology of understanding-by-building to learn from the environment and adapt its internal states to statistical variations in the incoming radio frequency stimuli by making corresponding changes in certain operating parameters (e.g., transmit power; carrier frequency, and modulation strategy) in real-time, with two primary objectives in mind: (i) highly reliable communication whenever and wherever needed and (ii) efficient utilization of the radio spectrum”.

1.3.1. CRT’s Benefits and Criteria

CRT is becoming increasingly attractive for several actors in the wireless and ICT industry, since it provides significant benefits if compared to what is possible with today’s and tomorrow’s mainstream wireless technology. For instance, the FCC has certified Google Inc. to create a database (Spectrum Database [44]) of USA’s unlicensed television spectrum bands for broadband access and to collect information from protected entities and fixed base station operators. In addition, Google cooperates with other database administrators, designed by the FCC, to provide TV spectrum holes services and to share this information with the FCC, with certified database operators and with the public. In fact, Google provides information about TV spectrum holes and allows users to browse the spectrum (Figure 3) and to use it through ad-hoc API, obtaining information about TV-band spectrum availability.

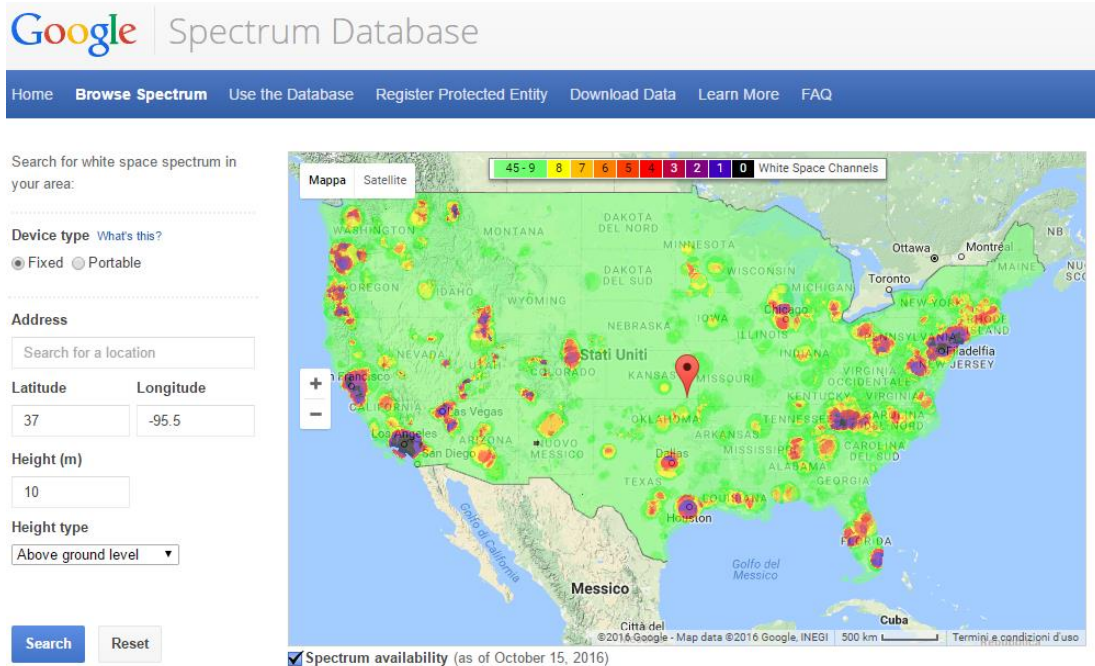


Figure 3. Browse spectrum function of Google Spectrum Database website.

In addition, devices' manufacturers can choose to sign up for a commercial agreement in order to use the Spectrum Database API in their white space devices. Cellular service providers and telecommunications equipment companies (e.g. Verizon, T-Mobile, and Qualcomm) argued that shifting some of their LTE traffic over to unlicensed spectrum during busy periods would add extra capacity to their networks aiding them to provide faster coverage for their customers [45].

The evolution towards LTE-Advanced and Wi-Fi has given mainstream technology, such as 3GPP's Long Term Evolution (LTE), a great momentum in the market and, in the next years, it will bring about significant improvements in performance as well as in cost. Three are main criteria defined to select feasible deployment scenarios for a CRT providing both managed QoS and high mobility [23], [46]:

- *Benefit from CRT technology*
 CRT should provide a significantly better performance than the existing conventional systems in order to be attractive for customers;
- *Benefit for actors*
 Exploiting the CRT in certain scenarios should provide a potentially significant benefit for users and industrial actors (i.e. service, network and database

providers), reaching a joint, maximized benefit. A successful solution based on CRT should also be commercially attractive, addressing the commercial side of the CRT. In addition, the selected scenarios should provide a better business case than conventional systems;

- *Managed QoS and mobility*
Adopting the CRT for certain scenarios should cover a range of QoS and/or mobility demands where the QoS requirements are based on the traffic classes to be served.

In addition, as presented in Table 5, other seven criteria, such as market potential and ecosystem feasibility, have been identified to target the promising scenarios for business case studies [23], [46].

Table 5. Criteria for targeting promising CR scenarios.

| Criteria | Description |
|--------------------------|---|
| Market Potential | The scenario should have a large market potential, e.g. with respect to the number of user terminals or expected revenue for the service. This potential could actually come from reduced costs, e.g. reduced spectrum costs or lower power requirements |
| Best Solution | No other solution should appear as a better solution for the given scenario |
| Technical Feasibility | It must be probable that this system can be implemented with current state of the art technology, or beyond state of the art technology achievable within a reasonable time frame |
| Economic Feasibility | It must be probable that within a period of 3-10 years it will be possible to produce equipment and services to a cost that match the users' willingness to pay. The scenario must offer profitability for all major actors in its ecosystem |
| Regulatory Feasibility | If the solution requires regulatory changes in order to be deployed, the changes should be such that it is reasonable to expect that they can be realized within a reasonable time frame |
| Ecosystem Feasibility | The ecosystem may consist of customers, partners, suppliers, competitors and local and national authorities. If the scenario imposes great changes in the ecosystem (e.g. roles that disappear), it will be much harder to get acceptance for the solution in the industry. |
| Benefits for the society | Local or national authorities may be willing to support deployment of a system if the social benefits it represents are large. Political support can also make it much easier to get acceptance for regulatory changes. |

1.3.2. Standardization Activities

The Institute of Electrical and Electronics Engineers (IEEE) together with the Standards Coordinating Committee 41 (SSC41) is working on the standardization of the CRT in the wake of the IEEE P1900 Standard Committee's efforts to develop supporting standards dealing with new technologies for the next-generation of radio management [47]-[49]. The IEEE SCC41 is focusing on the improvement of the spectrum utilization by using the DSA, and its activities are supported by the IEEE Communication Society's technical committees.

As shown in Figure 4, the IEEE SCC41 is organized in seven working groups (WGs) responsible for advancing the standardization processes for several aspects of DSA [47]. Each WG is identified as IEEE 1900.x, where x represents a specific group.

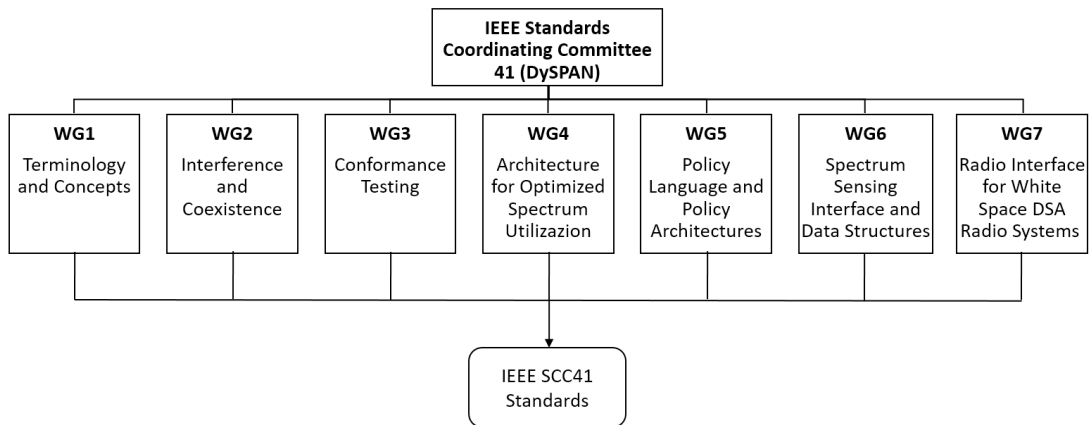


Figure 4. IEEE SCC41 organization structure.

Let us briefly introduce each group and its aims:

- the IEEE 1900.1 provides the standard definitions and concepts for spectrum management and advanced radio system technologies and it is responsible for creating a glossary (which is currently under review [50]) aimed at providing technically precise definitions related to CR;
- the IEEE 1900.2 recommends the interference analysis criteria and establishes a well-thought-out framework for measuring and analysing the interference between radio systems;
- the IEEE 1900.3 aims to define a set of recommendations to help in ensuring the coexistence and compliance of the software modules of CR devices before

the certification. Through these practices, it should be possible to create radio devices based on multiple layers of software;

- The IEEE 1900.4 defines the overall system's architecture, dividing the functionality between the terminals and the network, and managing the information exchange between coordinating entities. In addition, it aims to enhance the spectrum utilization while increasing the QoS;
- The IEEE 1900.5 provides a definition of policy language and architectures to manage CRs for DSA;
- The IEEE 1900.6 aims to define the information exchange between spectrum sensors and their clients;
- The IEEE 1900.7 is the most recent WG related to radio interface for white space DSA radio systems supporting fixed and mobile operations and is currently under development [51].

The IEEE 1900.x standards provided by IEEE SCC41 are not the only ones defined for the standardization of the CRT. In particular, the IEEE SCC41 started a collaboration with the FCC, the SDR Forum and other organizations to define the IEEE 802.22 standard for TV white space. As mentioned early in this chapter, the FCC has noticed that TV bands are often under-utilized. To overcome such issues, the FCC has allowed the utilization of white spaces in TV spectrum for wireless regional area networks (WRAN) regulated by the IEEE 802.22 standard [47], [52]. This standard allows the sharing of geographically unused frequency bands allocated to the TV broadcast service in order to widen broadband access to rural environments, avoiding interferences with the PU's operations (e.g. digital TV).

1.4. Cognitive Radio Network

A CR network (CRN) is a new generation of networks in which SUs communicate among them exploiting the spectrum holes. A CRN can be defined as follows [53]:

“A type of network in which the behaviour of each radio is controlled by a cognitive control mechanism to adapt to changes in topology, operating condition or users' needs”.

A CRN is composed of two different networks that coexist at the same time: the primary and the secondary network (Figure 5).

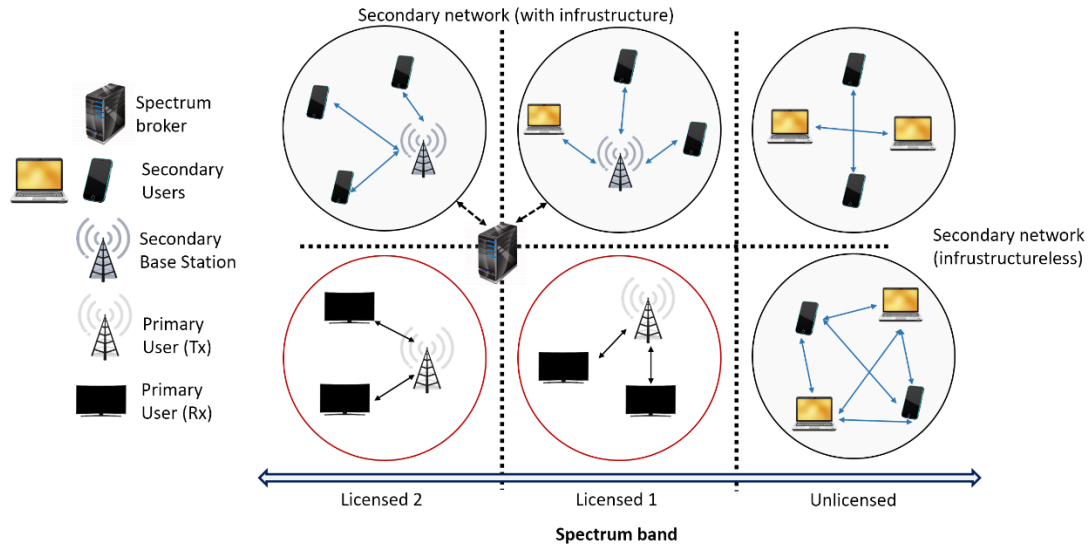


Figure 5. Architecture of a Cognitive Radio Network.

The primary network is an existing network infrastructure that has exclusive rights to a specific licensed spectrum band, like a cellular or TV broadcast network. It is composed of two main actors [54]:

- the Primary Base-Station (PBS), namely licensed base-station, is a fixed infrastructure network component with spectrum licenses. This actor does not possess any cognitive capability and is unable to share the spectrum with SUs, but it may have legacy and DSA protocols for managing the access of PUs and SUs;
- the PU has a license to operate in the assigned spectrum band. Its access can only be controlled by the PBS and its operations should not be affected by any SU's communication. In addition, it does not require any additional functions and behavioural features to coexist with SUs and secondary base-station.

The secondary network, namely DAS network or unlicensed network, is a network that does not have a license to operate in a spectrum band, but it can opportunistically access the spectrum licensed to a primary network. A secondary network is composed of:

- the Secondary base station (SBS), namely unlicensed base-station, which is a fixed infrastructure with cognitive capabilities and provides single-hop connection to SUs so they can opportunistically access other networks without a spectrum license;
- the SUs, namely CR users, do not possess a licence to operate in spectrum bands, but their cognitive capabilities allow them to share the licensed spectrum of PUs, avoiding any possible interference.
- the spectrum broker is the main actor of this network because it is responsible for the dynamic assignment of spectrum access rights. It can be connected to both the primary and secondary network, playing the role of spectrum information manager to enable the coexistence of multiple CRNs.

The possibility to access and communicate with such networks relies on whether the spectrum band is licensed or not. For instance, in a licensed band, a SU can access the spectrum only if the PU is not using it. In such scenario, a SU should sense the radio spectrum to detect the presence of a primary communication and to select the best available channel for its own communication. In addition, if a PU needs to exploit the spectrum, the SU should immediately vacate the occupied spectrum and switch to another available band, avoiding any possible interference with the PU.

By contrast, in unlicensed bands, such as ISM bands, all users have the same rights of access to the spectrum due to the absence of PUs. In such scenario, sophisticated spectrum sharing methods must be adopted in order to manage interference among users.

2 Cognitive Radio Operations & Spectrum Awareness

This chapter will provide a deep analysis of the CR lifecycle, focusing the attention on the Spectrum Sensing (both cooperative and non-cooperative) features provided by this technology. In particular, the most common sensing technique, namely energy detection, will be introduced highlighting its main drawbacks that we will address in this dissertation by providing novel solutions. In addition, the centralized strategy of the cooperative spectrum sensing will be addressed in this dissertation analysing the current performance limits and the security issues that will be considered in designing new cooperative, secure approaches.

2.1. Cognitive Radio Cycle

In order to recognize the available spectrum opportunities and efficiently use them for adaptive transmission, a CR-based device should be able to acquire, measure, sense, learn and be aware of its radio's operating environment. To do so, a CR should adaptively modify its characteristics in real-time and access radio spectrum bands without generating interference with the PU's communications.

The operations of a secondary radio device can be summarized by the cognitive cycle shown in Figure 6 [19]-[20].

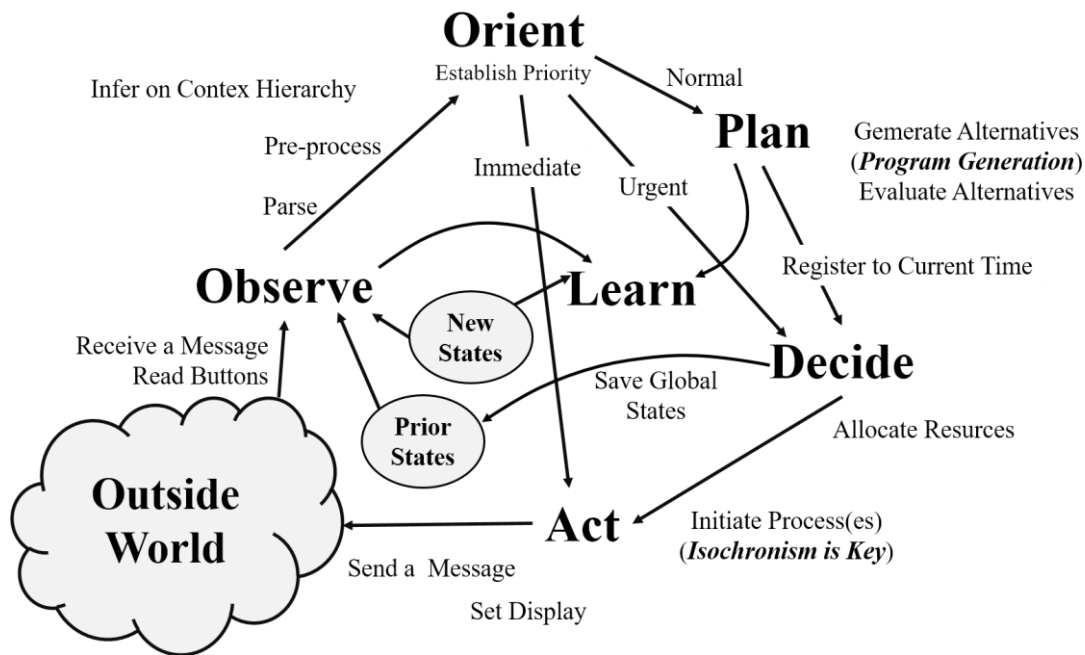


Figure 6. Cognitive cycle of cognitive radio operation.

Through an analysis of the figure, it is possible to identify the main building blocks of the cognitive cycle and of the spectrum awareness process in the following four major functions [55]:

- *Spectrum sharing*: as mentioned in the previous chapter, multiple SUs may try to access the spectrum bands to create a CRN. The access to the created network should be coordinated in order to prevent multiple collisions in overlapping portions of the spectrum;
- *Spectrum mobility*: SUs can dynamically change the frequency band used for their own communications if it is required by a PU. This allows SUs to continue their communication in other vacant and available (under appropriate incentives) portions of the spectrum;
- *Spectrum decision*: exploiting the information about the spectrum availability, SUs can allocate a channel for their own communications. Such allocation depends also on internal and (possibly) external policies;
- *Spectrum sensing*: in order to identify the available spectrum holes in a certain spectrum band, SUs should be able to monitor the spectrum bands to acquire the information about its occupancy and to allocate only the unused and detected portion of the spectrum. A detailed description of this operation is provided in section 2.2.2.

The operations presented above will be discussed in detail in the following sections focusing the attention on the Spectrum Sensing function and highlighting how to perform it in both a cooperative and non-cooperative way [23], [16], [46], [56]-[57].

2.1.1. Spectrum Sharing

Since spectrum holes can be exploited by a considerable number of SUs, each user has to achieve balance between two goals: transferring information in an efficient way, and altruistically allowing other users (both cognitive and non-cognitive) to utilize the available resources. This is achieved through spectrum sharing, which is disciplined by specific policies and regulations. Even though such rules differ according to the country and to the communication system involved, they still allow determining users' behaviour in a radio environment. A huge research interest has stemmed from this topic in the recent past [58]-[61].

There are multiple and active research issues regarding the realization of efficient and seamless open spectrum operations in CR networks, such as:

- common control channel (CCC). The CCC facilitates many spectrum sharing functionalities. However, a fixed CCC cannot be implemented since the CRT does not allow SUs to interfere with PU's communications. In addition, a CCC is highly related to the CRN topology and varies over time [62]. For such reasons, CCC mitigation techniques must be devised;
- communication channel assessment. In most spectrum sharing techniques, a communication channel is considered as a basic spectrum unit, posing as a crucial aspect to consider in the design and development of new algorithms;
- available CRN information. According to several studies, interference with PU's communication could be easily computed with SUs aware of the transmit power and of a PU's current location in the considered radio. Unfortunately, though such information is not always available in a CRN.

2.1.2. Spectrum Mobility

In a scenario in which a PU starts operating on a channel used by a SU's transmission, the latter has to promptly cease its transmission and vacate the used radio

spectrum changing frequency. This operation, namely spectrum mobility, has to be performed in real-time in order to guarantee SUs a smooth transition in terms of associated latency and to avoid interference with a PU's transmission. Switching to another channel characterized by different features requires SUs to quickly adapt their operating parameters such as operating frequency, modulation scheme and adequate associated source/channel coding. In particular, information about the transition latency between two channels allows a SU to improve mobility performances by providing a time estimation of the transition process. To do so, communication is necessary among all the network communication components of a CR radio (Figure 7) device, minimizing the performance degradation during transition.

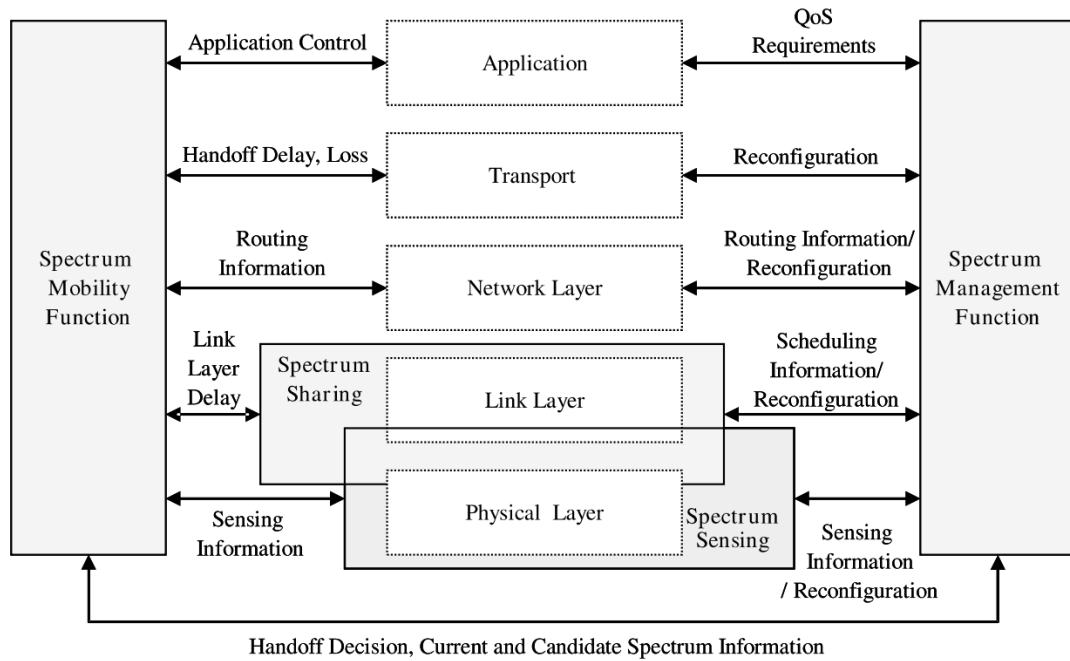


Figure 7. Spectrum management framework for cognitive radio networks [16].

In addition, SUs have to constantly investigate alternative spectrum holes [61], [63], facing several challenges that can be summarized in the following two points:

- the spectrum mobility in the time domain requires CRNs to adapt their wireless spectrum considering the available channels, which change over time. Consequently, the CRNs may not guarantee the required QoS for the services;
- the spectrum mobility in space requires a continuous allocation of the spectrum because SUs move from one place to another.

2.1.3. Spectrum Decision

Each CR application requires a certain class of QoS which provides for a specific operating channel the minimum requirements needed by SUs for their communication. For instance, real-time applications are based on high QoS, small delay and large bandwidth in order to guarantee a good service to end-users. As a matter of fact, a primary objective of a CR device is to satisfy the QoS requirements avoiding interference with the PU's communications. To achieve this goal, SUs can exploit a spectrum decision protocol that allows them to define the minimum acceptable parameters for each application and enabling them to compare such parameters to the available choices generated by the spectrum sensing. Using such information, a CR device can select the operating frequency and the corresponding technical parameters meeting the requirements [19]-[22] and, then, start its operation. Finally, SUs may use information provided by regulatory and policy databases [64]-[65] to improve their operations and outage statistics.

Several challenges should be considered in the development of the spectrum decision functions [57]:

- in a CRN, it is not possible to characterize spectrum bands by using only Signal-to-Noise Ratio (SNR) without taking into account the QoS of applications. For such reasons, the design of a spectrum/application-adaptive decision model is still a challenging task;
- the utilization of a spectrum hole requires SUs to adapt their operational parameters to meet the ones required for it and provide optimal transmissions. For instance, even though new a spectrum hole has a different SNR, it may be possible to maintain the bit rate and bit error rate (BER) through adaptive modulation. Hence, a cooperative framework with reconfiguration is required in spectrum decision;
- in a CRN, spectrum decision operations should be supported on both licensed and unlicensed channels to permit spectrum decision operation over heterogeneous spectrum bands.

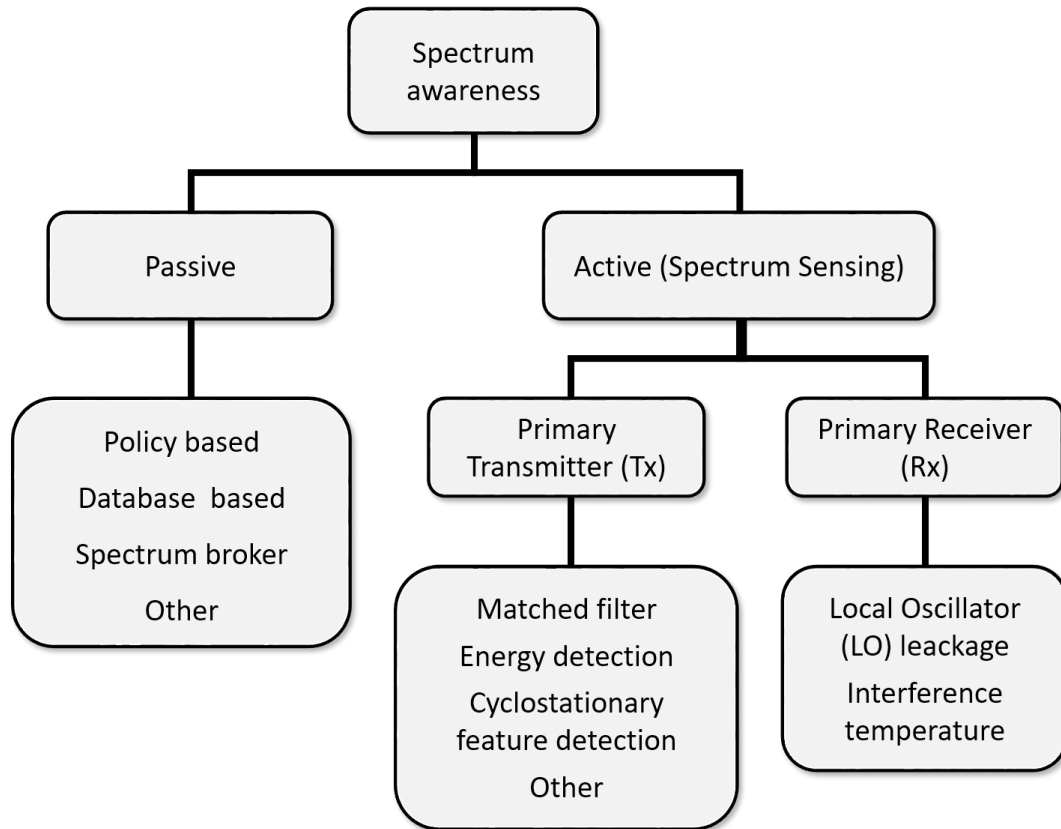


Figure 8. Spectrum awareness classification for cognitive radio.

2.2. Spectrum Awareness

A classification of the spectrum awareness in two categories (i.e. passive and active) is provided in Figure 8, as described in [16], [66]–[69]. Through such classification, it is possible to define the main approaches defined in literature to obtain the information about the available spectrum bands.

By exploiting the passive awareness, a CR device receives spectrum information from third-party sources like: servers, centralized databases, primary communication systems, or predefined policy sets [66], [69]. Through such approach, an additional communication channel is required for information acquisition. In addition, data relevance in space and time becomes a strict and critical requirement.

Providing this class of methods on simplified secondary transceivers, it is necessary to modify several aspects, such as:

- the legacy primary system;
- additional data acquisition;

- data storage resources;
- data management system;
- additional network capacity.

Clear examples of passive awareness approaches are: *(i)* Policy based approaches, which are based on information provided by the regulatory agency that can define rules and constraints to access and use the available spectrum; *(ii)* Spectrum databases, which provide several data about spectrum occupancy in specific geographical locations provided by primary systems or regulatory agencies; *(iii)* Spectrum brokers (SB), which enable spectrum management and should implement decision and control algorithms.

Even though passive awareness can increase spectrum utilization, it does not provide an optimal usage of the available spectrum resulting in rather static secondary usage. Conversely, active awareness adopts spectrum sensing techniques to analyse the spectrum in both a cooperative and non-cooperative manner in order to identify the unused bands. Through the spectrum sensing, the SUs analyse the radio environment to adapt their operational parameters to the available spectrum holes. In particular, by using a non-cooperative model, SUs independently perform the analysis of the spectrum, making their own decisions about spectrum occupancy based on the observations about the spectrum environment.

Active awareness provides different approaches that can be classified in two categories:

- Primary transmitter (Tx). This category groups all the approaches used by CRs to sense the spectrum in order to detect primary Tx in real-time. The popular ones are: *(i)* Matched filtering, which allows detecting the primary communications with a high level of accuracy if the primary signal is known. Unfortunately, this method requires significant power consumption; *(ii)* Cyclostationary feature detection, which allows detecting the primary user's transmissions by exploiting the cyclostationarity features of the received signals. The main drawback of this technique is that the noise may not be stationary and its variance may be unknown; *(iii)* Energy detection is the simplest approach to detect primary communications by analysing the energy

of the received signal. Even though this method has a low computational complexity, its performance decreases in presence of noise uncertainty and fading.

- Primary receiver (Rx). This category defines the method used by a CR device to locate the primary Rx. Typical approaches are: (i) Local Oscillator leakage power, which all RF receivers emit enabling CRs to locate these receivers; (ii) Interference temperature, which is used as a decision metric in CRNs to state whether SUs can access the spectrum without interfering with PUs.

In the Cooperative Spectrum Sensing (CSS), the local decision of each SU in the network is combined through data fusion techniques in order to make the final decision about the spectrum occupancy. The final decision is then signalled to all SUs. The CSS is becoming a popular approach to significantly improve the sensing of the spectrum by decreasing error statistics even with a small number of non-correlated sensing entities [70]-[71].

By comparing passive and active awareness, some benefits and disadvantages emerge. Unlike active awareness, passive awareness does not require complex hardware, but it results in a static usage of the spectrum and fails to improve it. Active awareness, on the other hand, can enhance spectrum usage statistics of SUs [66]-[68]. However, since CR systems may employ either one or both forms of awareness, the discussed approaches should not be viewed as mutually exclusive.

In the following section, a discussion about passive and active awareness will be presented focusing the attention on the main approaches provided by these categories.

2.2.1. Passive awareness

Several approaches are defined in literature for passive awareness. Examples are systems based on: negotiated spectrum use; policy; utilization of a spectrum broker; spectrum databases.

The system based on negotiated spectrum utilization allows PUs to inform SUs about the allocated frequencies and the available spectrum holes through the exploitation of spectrum beacons [66], [69]. In this scenario, negotiation management

is centralized and provides information such as determination of geographical, temporal, technical, service quality, and interference constraints and conditions.

The policy based approach uses information provided by the national regulatory agency that identifies licensed bands of the spectrum with low usage or characterized by a deterministic usage pattern [66], [69]. Through this approach, regulators provide rules and constraints to manage the access and the usage of the available spectrum holes for SUs, which constantly update their information bases and the stored policy. Such updates allow SUs to adapt their operational parameters (e.g. power and frequency) to meet the policies.

The approach based on spectrum broker exploits a server to enable a coexistence between primary and secondary users in a shared environment, which can be managed in a centralized fashion [66], [69]. The information managed by the centralized spectrum server are provided by different terminals and allow the server to provide suggestions for an efficient use of the spectrum. Both network users and service providers gain time-bound rights to a part of the spectrum from a regional spectrum broker, and then they configure the obtained portion of the spectrum to supply network services.

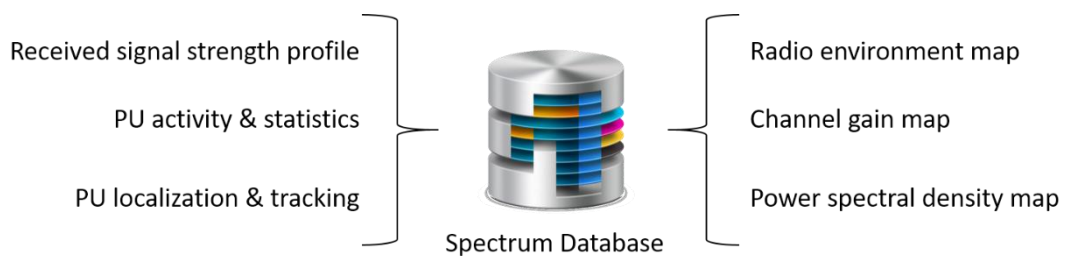


Figure 9. Spectrum database in passive awareness

The approach based on spectrum databases (SDs) can overcome typical issues and limitations of spectrum sensing [72]. As shown in Figure 9, this kind of database can provide information about available frequency bands, geographical locations, power in dBm and additional details such as channel number, the time interval to use it, the radio environment and channel gain maps and an estimate of the interference range of SUs. Generally, these databases are maintained by a primary system or by a regulatory authority. Given the amount of information available to a cognitive device through this approach, the device's only task is to query the database proving its current location

[73]. The database service provides a list of available channels and the related information. Once the channel is occupied by a SU's transmission, the other users are warned that the channel is busy and can select other spectral resources that meet their requirements. When a primary or secondary user stops transmitting, the associated channel is released and it becomes available to other users [23].

Although the approaches based on spectrum databases are quite simple and efficient, they have some drawbacks and limitations that are similar to the ones related to active awareness (i.e. the spectrum sensing):

- the CR device has to be equipped with location awareness devices or sensors, increasing the cost of the system;
- the geo-location information needs to be accurate to correctly determine the available channel. Unfortunately, it is not possible to obtain the exact position of a CR device, so the spectrum database should be developed in order to consider low level of accuracy and to avoid interference with PU's communications by returning conservative inquiry results;
- the impossibility to detect incoming PU's signals in the considered frequency band;
- the need to provide SUs with a fast, secure, scalable, and energy efficient access to remote spectrum databases;
- Security and Privacy mechanism are required to avoid information leakage and to isolate the system from potential attacks. Moreover, the database should include further knowledge, such as the behaviour model of SUs and the model for jammer identification.

Nevertheless, spectrum databases are increasingly being used in both spectrum sharing and network optimization, leading to very interesting results in the increment of spectrum utilization. In particular, SDs are effective and reactive, and often it is required that they are exploited in conjunction with spectrum sensing, especially if their operations require automation [74]. As a matter of fact, a SU can obtain a list of available spectrum from the spectrum database, perform the spectrum sensing and then combine the sensing results with the ones from the database, selecting the best channel for its transmissions [75]. Even though spectrum sensing is a promising approach to

detect the PUs' transmissions, as of today, it is not mature enough to guarantee the highly demanding requirements for the detection threshold defined by the FCC, and other regulatory agencies. For such reasons, the current focus is on the improvements of SD-based solutions through the definition of a new IEEE standard project, IEEE 1900.6b, on spectrum sensing support for spectrum database [76]. Such project aims to enhance the 1900.6 baseline standard for the purpose of spectrum sensing information to assist spectrum databases, considering different realization options. Consequently, a spectrum database may be an embedded function of a larger system as well as a large distributed spectrum authorization system [74].

2.2.2. Spectrum Sensing

Since interference actually takes place at the receiver location, active awareness should be focused on detecting the receiving activities of PUs but, without a cooperation between primary and secondary users, SUs hardly detect PU's communication. Due to the dynamism of the spectrum utilization, it is not possible to adopt solely the approaches provided by passive awareness and, in general, those based on active awareness and spectrum sensing are preferred.

As shown in Figure 10, there are several aspects (i.e. algorithms, challenges, etc.) to be taken into account for the spectrum sensing operation deployed on a CR device. In the following sections, a description of the main approaches and challenges of the Spectrum Sensing operation will be discussed [67].

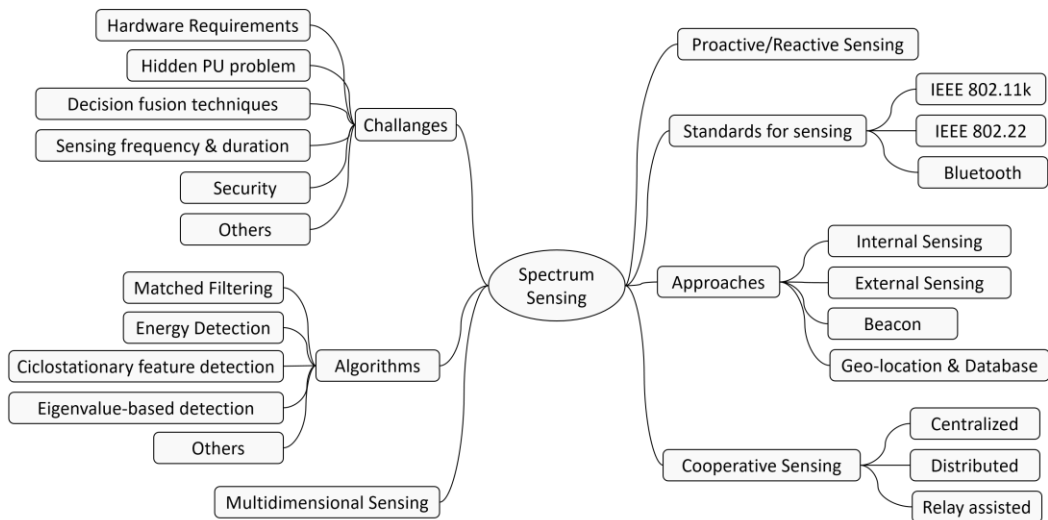


Figure 10. Aspect of Spectrum Sensing function for CRT.

2.2.2.1. Spectrum Sensing Algorithms

Several techniques have been developed to allow SUs to sense the radio environment and detect primary receivers and transmitters. In particular, for the detection of primary receivers, it is possible to exploit:

- the local oscillator leakage power;
- the interference temperature.

The detection of primary transmitters, instead, requires different kind of algorithms based on the processing of the signal received by a CR user:

- the matched filter detection;
- the cyclostationary feature detection;
- the eigenvalue-based detection;
- the energy detection.

Let us now focus on the first group of techniques.

In [62], the authors propose an approach based on the measurements of the local oscillator leakage power emitted by RF receivers that allows SUs to locate them. The drawback of this technique, used in several countries to detect TV viewers not paying for TV subscription, is the considerable detection time needed for good level of accuracy and the short detection range. Due to such limitations, this approach requires building a large network of passive sensors assisting SUs in the cognitive cycle.

The interference temperature is further receiver-centric method proposed by the FCC to measure the interference power in SUs' environment [16], [37], [77]-[78]. Generally, the interference temperature is used as a decision metric in CRNs to state whether SUs can access the spectrum without interfering with PUs. As for the noise temperate, its value is obtained as a measurement of the power and bandwidth occupied by the interference. A SU can characterize both the interference and the noise by taking only one measurement. The interference temperature constraint is computed as the sum of the receiver's noise floor level at the primary system service range and the interference gap, which can be identified as the maximum positive variation of noise level, as shown in Figure 11.

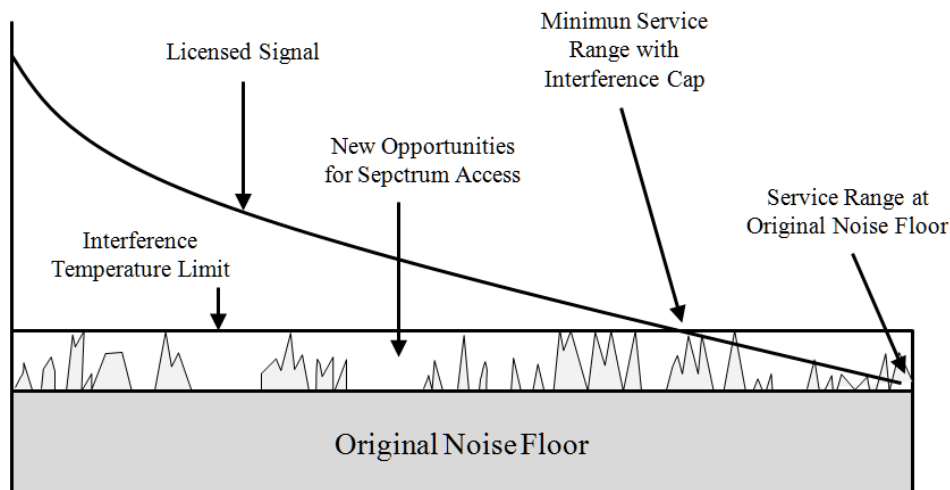


Figure 11. Temperature of interference [23].

The comparison between the measured interference temperature and the interference temperature constraint determines the interference temperature gap. This gap sets up a measure of cumulative interference that can be tolerated by a PU without reduction in service area and that can be exploited by SUs for their own short-range transmissions. The second category of active awareness approaches switches the focus of the detection from primary receivers to primary transmitters. Popular methods are: matched filter detection, cyclostationary feature detection, energy detection, waveform based sensing, and others (e.g. Eigen-value based detection) [16], [66]–[71].

Matched filtering detection can be considered as the optimal solution that a SU should use, if it has a priori information about the PU's signal in stationary Gaussian noise channel since it maximizes received SNR comparing to other detection methods [16], [67]–[68]. The main advantage of this method is the short time and the low number of samples required to achieve a required level of false alarm. Unfortunately, to use this method, a SU requires many information about the primary signal at both physical and medium access control (MAC) layers (i.e. modulation, coding, packet format, etc.). If this information is not accurate, the SU cannot achieve coherency and demodulate primary user signal. Additional drawbacks are:

- the requirement of a dedicated receiver for each PU signal in the CRN;
- large power consumption that makes the matched filter impracticable for wider implementation.

In CRN, the possibility for a SU to have a priori knowledge of the PU information is very low and, as consequence, the matched filter detection is rarely used. However, in some scenarios (e.g. the DTV system) the primary signal is known allowing SUs to sense the radio environment through the matched filter detection.

Another interesting approach is the cyclostationary feature detection method that exploits the inherent redundancy in the signals transmitted by a PU [16], [67]–[68]. In particular, it is possible to model any signal as a cyclostationary random process since it has a built-in periodicity in its samples or statistics. Moreover, the modern communication systems adopt modulated signals characterized by sine wave carriers, frequency hopping or repeated digital spreading sequences. Cyclostationary signals have a correlation between widely separated spectral components that can be considered as a distinctive feature used for detecting primary transmission since modulated signals have nonzero correlation components. The main benefit of this detection approach is the possibility to distinguish the wanted signal from the noise because modulated signals are cyclostationary with spectral correlation and noise is in wide-sense stationary process with no correlation. The detection of PU transmissions can be performed with cyclostationary detection even with low and negative SNR. However, the computational complexity of this method is high and it is necessary a large observation window to collect all the samples necessary for a correct detection.

Eigenvalue-based detection centres on the computing of the eigenvalues of the covariance matrix of the received signal [79]–[80]. Several studies have proved that the ratio of the maximum or average eigenvalue to the minimum eigenvalue allows detecting the presence of PU's signal [81]. Through such approach, no a priori information about the PU signal and the communication channel is required, avoiding any issue related to noise uncertainty [82]. In addition, correlation among signal samples has been incorporated by covariance matrix. Several approaches have been defined to improve the detection of the PU's signal using eigenvalues, and they can be classified in the following three categories:

- Max Eigenvalue detection (MED), which defines the maximum eigenvalue of the covariance matrix as test statistics;

- Max-Min Eigenvalue detection (MME), which defines the ratio of maximum and minimum eigenvalue of covariance matrix as test statistics;
- Energy with Min Eigenvalue (EME), which defines the ratio of average power of received signal and minimum eigenvalue as test statistics.

Finally, the energy detection (ED) method is widely used in radiometry and is one of the most popular spectrum sensing techniques for the detection of a PU's transmission thanks to its low computational and implementation complexity [16], [67]–[68]. Its detection of the primary transmissions is based on the computing of the received signal energy and does not require any a priori knowledge about the primary signal and its statistics. The energy of the received signal is computed by integrating the received signal with the observation time interval and the receiver's bandwidth. To assess the presence or absence of the PU, the method compares the energy of the received signal with a preselected threshold level that is related to the noise floor and the required level of false alarm. Generally, ED is used because of its low complexity, but it has major drawbacks. As a matter of fact, this method is highly susceptible to uncertainty in noise power or in-band interference, and it does not allow SUs to distinguish between primary signal, noise or interference. In addition, it performs poorly under low SNR and it is not appropriate for detecting spread spectrum signals, for which more sophisticated signal-processing algorithms are needed. To overcome some of these issues and to improve spectrum decision's accuracy, it is necessary to adopt advanced approaches such as the cooperative spectrum sensing.

As shown in Figure 12, each method provides a different level of accuracy and complexity. In particular, at an increase in the level of accuracy corresponds an increase in the computational complexity of the considered method and of the time required to perform a reliable detection. Match filtering detection is the most accurate approach but also the most complex one, since it requires a priori knowledge about primary communication signals. Eigenvalue-based detection is a further interesting method that provides good performances in term of detection probability and proves to be robust to the typical challenges of the spectrum sensing operation. Unfortunately, though, its computational complexity is considerably high due to the eigenvalue decomposition. In CRT, information about past and current spectrum usage offers a foundation for opportunistic spectrum space access.

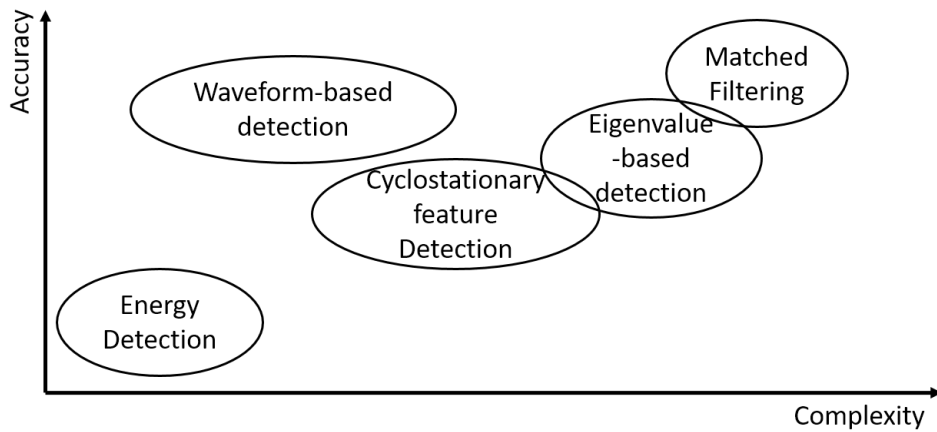


Figure 12. Accuracy vs Complexity comparison of different spectrum sensing approaches performed by a SU

In CR systems, spectrum management’s functions allow to access, assign and use radio spectrum efficiently without causing excessive interference to PU. For the sake of compactness, a summary comparison among the above-mentioned approaches is provided in Table 6.

Table 6. Comparison of non-cooperative spectrum sensing techniques.

| Sensing technique | Energy Detection | Cyclostationary feature based Detection | Matched filter Detection | Waveform based Detection | Eigenvalue-based Detection |
|--|------------------|---|--------------------------|--------------------------|----------------------------|
| Narrowband (NB) - Wideband (WB) sensing | NB/WB | NB | WB | NB | NB |
| Prior signal information | No | Yes | Yes | Yes | Yes |
| Reliability & accuracy | Poor | Good | Very Good | Good | Medium |
| Computational complexity | Very Low | High | High | Medium | High |
| Sensing time | Less | Large | Less | Medium | Less |
| Cost | Very Low | Very High | Very High | Low | Very High |
| Power consumption | Very Low | Medium | High | Low | Medium |

2.2.2.2. Spectrum Sensing challenges

Several challenges should be considered in the development of the spectrum sensing operation performed by a SU. Some of the main issues for non-cooperative sensing [67], for instance, are hardware requirements, the problems posed by hidden PUs, spread spectrum users, and frequency and duration of the sensing.

Particularly important aspects of the spectrum sensing operation are the hardware requirements related to the sampling rate, the speed of the signal processors, and the A/D converter. A CR device should be able to process narrowband and wideband signals transmitted over a certain bandwidth to exploit any possible spectrum opportunity with reasonably low complexity and low power processors. However, to work properly with wideband signals, cognitive devices need additional components, such as power amplifiers, and they have to operate over a range of wideband operating frequencies by using high-speed processors such as Digital Signal Processor (DSP) or Field Programmable Gate Array (FPGA). These processing units allow radio devices to perform computationally demanding signal processing tasks with low delay. Currently, there are several hardware and software platforms available for CR and able to perform the cognitive cycle described in this chapter. Some examples are the GNU Radio [83], the Shared Spectrum's XG Radio [84], and the Universal Software Radio Peripheral (USRP) [85]. At the beginning, these platforms were only able to perform ED-based spectrum sensing due to their limited computational resources. Currently, especially the National Instrument's USRP [86] allows developing more sophisticated techniques through the visual programming language Laboratory Virtual Instrument Engineering Workbench (LabVIEW) [87].

Hidden primary users pose a further interesting challenge in the non-cooperative spectrum sensing. In such scenario, the PUs' transmission can be hidden due to unintentional interferences generated by other SUs and to the presence of severe multipath fading (and/or shadowing) affecting a channel and observable during the spectrum sensing operation. In addition, a SU may fail to detect a primary communication due to the presence of buildings or constructions, which can hide PUs. An example of hidden primary user is shown in Figure 13, where a SU causes unwanted interference to the primary receiver, as the primary transmitter's signal could

not be detected due to the SU's location. To overcome this problem, the CRN should provide a cooperative sensing framework as proposed in several works [88]–[90].

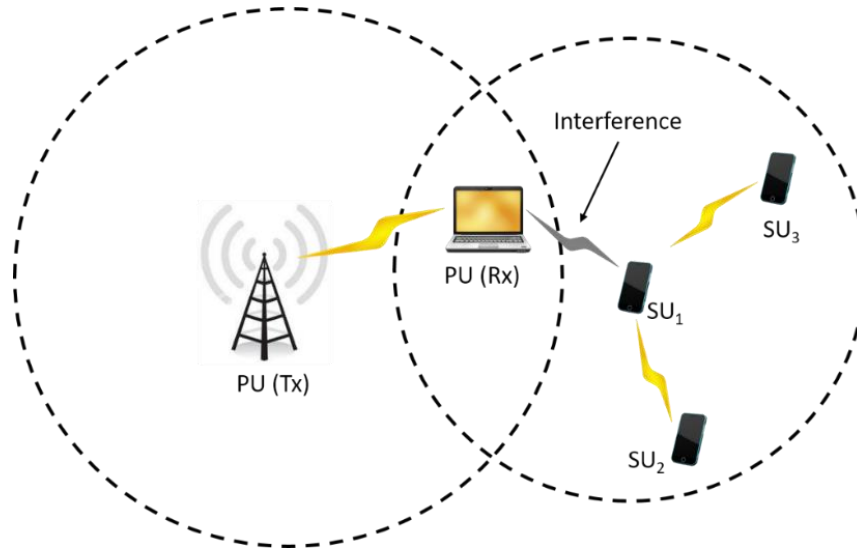


Figure 13. Examples of Hidden Primary User problem, where the dashed circles represent the operating ranges of the PU transmitter and the SU, in presence of interference with PU receiver.

Finally, the last but not least spectrum sensing challenge is presented by the sensing frequency and duration. In order to avoid the interference to and from the PU while exploiting the possible spectrum holes, SUs should be able to identify the presence of a PU's transmission in a certain duration. For such reason, a trade-off between the sensing time, the accuracy and reliability of the spectrum sensing is to be found. The sensing frequency is also a crucial design parameter and has to be carefully chosen, since its optimal value is related to the temporal characteristic of the PU in the environment [91]. Additional parameters, which also affect spectrum sensing, are channel detection and moving time, together with further timing parameters as defined in [92].

2.2.2.3. Basic Framework for Spectrum Sensing

The decision about the absence or presence of a PU's communication in a given channel can generally be described as a binary hypothesis test that allows SUs to discriminate between two testing hypotheses (equation 1).

$$\begin{aligned}
 \text{Hypothesis } H_0: & \text{ absence of a PU signal} \\
 \text{Hypothesis } H_1: & \text{ presence of a PU signal}
 \end{aligned}
 \tag{1}$$

In particular, the null hypothesis, H_0 , states the absence of a PU signal in the considered sensing channel (i.e. a spectrum hole is detected), while the alternate hypothesis, H_1 , states the presence of the PU's signal (i.e. any spectrum hole in the considered channel).

The two hypotheses can be formulated as follows:

$$r(n) = \begin{cases} w(n) & \text{Hypothesis } H_0 \\ s(n) + w(n) & \text{Hypothesis } H_1 \end{cases} \quad (2)$$

where $r(n)$ is the PU's signal (with $n = 0, \dots, N - 1$ sensed samples), which is assumed to be affected by additive white Gaussian noise (AWGN) $w(n)$, with zero-mean and variance $2\sigma_w^2$. Finally, $r(n)$ is the signal received in a certain frequency band, and it is possible to assume that $s(n)$ and $w(n)$ are zero-mean and mutually independent random processes.

In order to perform the test and to distinguish between these two hypotheses, it is necessary to compare a testing (or decision) variable with a properly chosen threshold [93]. For instance, in the ED approach, the energy of the received signal is used as testing variable, and it is computed as follows:

$$T = \frac{1}{N} \sum_{n=0}^{N-1} |r(n)|^2 \quad (3)$$

In order to perform effective tests, the constant false alarm rate (CFAR) criterion is exploited as an optimality criterion and adopted to determine the threshold [94]. In particular, the CFAR procedure refers to a common form of adaptive algorithm used in telecommunications systems to discriminate between the presence and absence of something (e.g. unknown user's communication), against a background of noise and interference [95]. In CRT, the CFAR is exploited to discriminate between the presence and the absence of a PU's communication through the definition of a proper threshold:

$$\gamma = 2\sigma_w^2 + Q^{-1}(P_{FA}) \sqrt{\frac{1}{N} 4\sigma_w^4} \quad (4)$$

where $Q^{-1}(\cdot)$ is the inverse of the Marcum Q -function, and P_{FA} is the desired probability of false alarm that represents the probability of our technique to declare the presence of the PU's communication when it is actually not present. Conversely, it is possible to define as probability of detection (P_D) the probability of a SU to correctly detect the presence of a primary transmission, when it is actually performed.

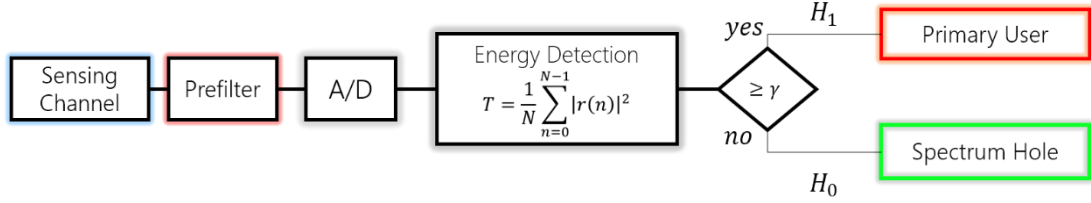


Figure 14. ED-based Spectrum Sensing.

As shown in Figure 14, a SU senses the channel of interest to acquire the current information about the channel, i.e. the signal transmitted over it. Then, the user applies some pre-filtering to improve the signal quality and to convert it in a digital signal composed of complex samples. Finally, the energy detection is performed and the testing variable T is computed and compared with the threshold expressed by the equation (4). In particular, the testing hypotheses in (2) result in:

$$\begin{aligned} H_0: T < \gamma & \quad (PU \text{ absent}) \\ H_1: T \geq \gamma & \quad (PU \text{ present}) \end{aligned} \quad (5)$$

where if the testing variable T is lower than the pre-determined threshold γ then a spectrum hole is identified and the SU can use it for its own communication. Otherwise, a primary communication is detected.

2.3. Cooperative Spectrum Sensing

Cooperative spectrum sensing has been recently proposed as a possible solution for the typical spectrum sensing challenges arising in presence of noise uncertainty, fading, shadowing and hidden primary users [96]. The idea behind this approach is to provide a cooperation among SUs so that they can sense the radio environment and then combine their sensing results according to a specific scheme. The CSS ensures several benefits, such as:

- the improvement of the CR's sensitivity;
- the improvement of the sensing performance, namely cooperative gain, through the spatial diversity in the SUs' observations;
- the mitigation of the hidden primary user problem;
- the possibility to decrease the time required for a correct detection.

As shown in Figure 15, the conventional CSS can be considered as a process based on three main states:

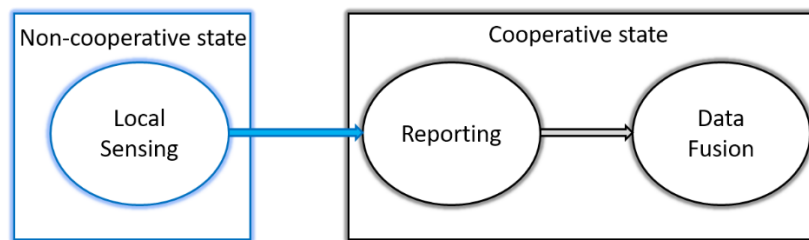


Figure 15. Three-state-based process of cooperative sensing.

- the Local Sensing state, in which each SU performs the spectrum sensing independently, making its local decision about the spectrum occupancy;
- the Reporting state, in which each SU communicates with the other users in the radio environment or with a central unit in order to collect the sensing results of the other SUs;
- Data Fusion state, which allows SUs or a specific central unit to combine the local sensing results of all the users in the radio environment and make the global decision about the spectrum occupancy.

The Local Sensing is the only state performed independently by each SU in the cooperative scenario, while the other two states require a cooperation among such users.

A fine-grained definition of CSS based on seven different elements is proposed by Akyildiz *et al.* [97] (see Figure 16). In detail, the authors identify the following elements:

- *Cooperation models* (or strategies), which provide the cooperative configuration for SUs which know how to communicate among them to make the global decision;

- *Sensing techniques*, which are exploited in the cooperative scenario to allow SUs to monitor the spectrum and detect the primary transmission. The choice of the sensing technique affects the cooperation among SUs;
- *Hypothesis testing*, which is the statistical test that can be performed by each SU independently or by a central unit that will collect the information acquired by SUs (e.g. testing variables like the energy of the received signal);
- *Control and reporting channels*, which are two important channels used by SUs to reliably report the sensing results to a central unit or to other users. These channels have standards to be met in terms of reliability and bandwidth [98]. In particular, the information shared among SUs or with the central unit is limited by the bandwidth of the common control channel [99] that determines the cooperation level;

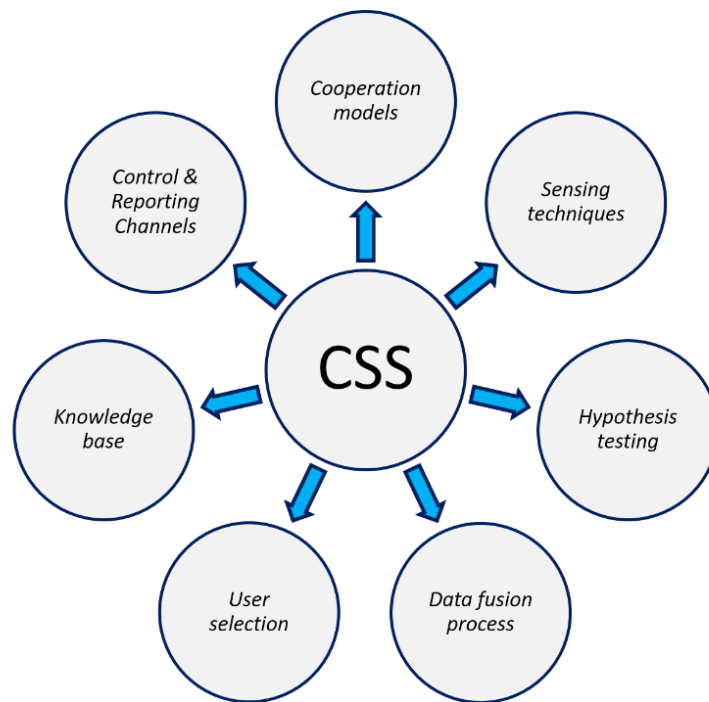


Figure 16. Fine-grained definition of CSS characterized by seven elements.

- *Data fusion process*, which is the main aspect of the CSS since it concerns the methods (i.e. decision fusion rules, or a signal combining techniques) used to combine the local sensing results of the SUs to make the global decision about the spectrum occupancy;

- *User selection*, which allows the selection of certain SUs for the cooperation in order to address the issues related to the shadowing effects. It plays a key role in the improvement of the cooperative gain and in the minimization of the overhead issue. The selection can be: centralized, when performed by a central unit [100]; cluster-based, when in presence of a high number of SUs that may cause high overhead [101];
- *Knowledge base*, which is the remote spectrum database that stores useful information about PUs' communication and location, as described in section 2.2.1. The presence of a spectrum database can improve the cooperative gain but it is an optional feature.

The definition of such elements allows to design a cooperative framework that improves the performance of the spectrum sensing and overcomes most of the challenges effecting the non-cooperative sensing. The main elements that to be taken into consideration in designing a cooperative framework are the cooperative strategy and the data fusion process.

2.3.1. Cooperative strategies

As shown in Figure 17, it is possible to divide the cooperative strategies in three main categories: centralized [102]-[103], distributed [104]-[105], and Relay-assisted CSS [106]-[107].

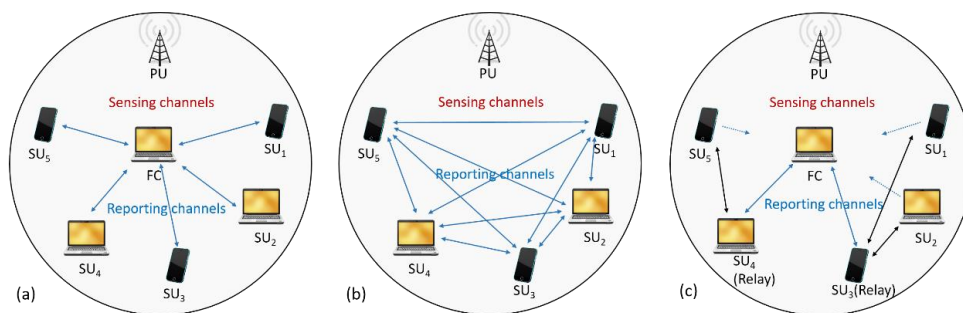


Figure 17. The three main cooperative models: (a) centralized, (b) distributed, and (c) relay-assisted.

The centralized CSS (Figure 17.a) is characterized by the combined presence of SUs and of a central unit, namely Fusion Center (FC), that can be represented by a cognitive base station in a cellular network, an access point (AP) in a wireless local area network (WLAN), or a cognitive device in an ad-hoc CRN. The FC aims at

controlling the cooperation among SUs as follows: it selects a given channel, namely sensing channel, for the sensing operation and forwards the information to all SUs, allowing them to perform the spectrum sensing on that channel. Then, each SU performs the sensing and sends its local sensing results to the FC through a secondary channel, namely reporting channel, which allows the communication between SUs and the FC. Finally, the FC combines the SUs' local sensing results and makes the global decision about the presence or absence of a PU's communication in the considered channel. In this strategy, the FC can select the SUs that will be taken into account during the cooperative sensing by broadcasting them a message to join [108].

Unlike the centralized strategy, the distributed CSS does not adopt a central unit like the FC to manage the cooperation and SUs are left to communicate directly among themselves. In particular, as in a peer-to-peer network, each SU is directly connected to the others (see Figure 17.b) through the reporting channel, so that a sensing channel can be established and the local sensing results exchanged by using a distributed algorithm. Once each SU has received all the sensing results, it combines them with its own result using some local criterion. If such criterion is not satisfied, the users send their combined results until the algorithm is converged.

Finally, the last strategy for the cooperative sensing is the relay-assisted CSS, which is an alternate version of the centralized CSS. It requires the presence of the FC to combine SUs' sensing results, but it is characterized by a number of SUs with a weak reporting channel and a strong sensing channel and by other users with a weak sensing channel and a strong reporting channel (Figure 17.c). To overcome such issue, this strategy allows SUs to communicate among them. In particular, the SUs with a strong reporting channel are used by those with a strong sensing channel as relay-nodes in order to forward the sensing results to the FC. This strategy can be considered as a multi-hop cooperative sensing due to the presence of the relay-node.

The choice of the cooperative strategy is strictly influenced by the radio environment and the kind of operating scenario to be implemented. Table 7 provides a comparison between the two main strategies of CSS (i.e. centralized and distributed CSS), highlighting the main pro and cons. The most used between the two, is the centralized CSS thanks to the reliability provided by the presence of the FC, which

Table 7. Comparison between centralized and distributed CSS.

| CSS Strategy | Pro | Cons |
|--------------------|--|--|
| Centralized | Bandwidth-efficient for same number of SUs in the cooperative scenario | FC becomes a critical node as well as the management of all SUs Requires a backbone to manage the cooperation |
| Distributed | Low design and implementation cost No need for a backbone to manage the cooperation | Large control bandwidth required for information exchange among all SUs Large sensing time due to iterative nature of distributed algorithm |

allows selecting the SUs that can participate to the cooperative sensing, improving the CRN's security. Moreover, the centralized approach allows to implement all the characterizing elements of the CSS, as shown in Figure 18.

A CR is composed by a radio frequency (RF) frontend, the processing unit that elaborates the data acquired from the channel, and the hypothesis testing to make the local decision about the spectrum occupancy. In detail, the RF frontend is used for the sensing and/or data transmission and requires a MAC scheme to access the control channel and to report the local decision or the raw sensing result to the FC.

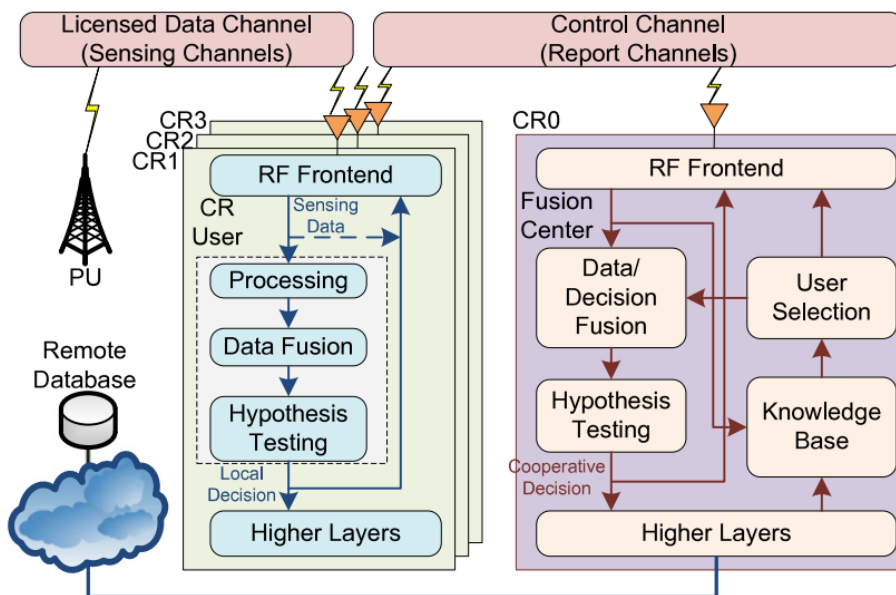


Figure 18. Centralized CSS framework [97].

For instance, a cognitive user can send the raw sensing data to the FC by using the RF Frontend. Conversely, the FC can be considered as an advanced cognitive device that provides all the features of a CR plus additional functions, such as user selection, connection to a remote spectrum database, and data/decision fusion techniques.

2.3.2. Data fusion techniques for CSS

The data or decision fusion technique is of crucial importance in the CSS, since it allows the FC to combine the data sent through the reporting channel via the RF frontend and to make the global decision about the spectrum occupancy. As mentioned in the previous section, the FC aims to combine the local decision or raw sensing results by exploiting different kinds of data fusion techniques with different bandwidth requirements. Ordering these techniques by increasing demand of bandwidth, it is possible to identify three categories: (i) hard combining voting rules; (ii) quantized soft combining; (iii) soft combining.

The hard combining voting rules is based on the idea that each SU makes a local decision about the spectrum occupancy sending a one-bit information to the FC. If the SU has detected a primary communication in the channel, then the local decision is equal to 1. Otherwise, it will be equal to 0. Once the FC has collected all the local decisions, it combines them by exploiting one of the following fusion rules:

- OR fusion rule, which allows the FC to declare that the sensing channel is not empty if at least one SU declares the presence of a PU;
- AND fusion rule, which allows the FC to state that the sensing channel is vacant if all the SUs state the absence of a PU;
- Majority (MAJ) voting fusion rule, which allows the FC to identify the sensing channel as a spectrum hole, if more than half of the SUs decide for the absence of a PU.

In particular, the OR, AND, and MAJ fusion rules can be considered as special cases of the general k -out-of- N rule when k is 1, N or $\frac{N}{2} + 1$, respectively [109]. This method helps the system's designer to decide the number of the nodes that will cause the system to consider the primary user as present. Through a comparison among these rules, it can be assessed that the OR fusion rule provides a better performance in terms

of detection probability in presence of a high number of SUs, while the AND rule proves to be the worst since all SUs should provide the same sensing results. It should be noted, however, that the AND rule works well in presence of few users. Finally, the MAJ voting fusion rule is the more robust and provides good results thanks to the majority criterion.

The quantized soft combining technique requires that SUs quantize their local results sending to the FC only the quantized data. For instance, SUs can send two-bit instead of the raw sensing result as depicted in [110]. Through this technique, the FC can exploit a soft combining approach together with the quantized data received by SUs, therefore decreasing the bandwidth requirement of soft combining techniques.

Finally, the soft combining techniques requires that SUs send the raw sensing results, such as the energy of the received signal, to the FC, which combines them by using some soft approach. This technique provides better performance and accuracy if compared to the hard combining voting rules, although its bandwidth requirement is high.

It is possible to identify three main soft fusion approaches [111]:

- Square law combining (SLC), which is the simplest soft combining approach based on the computing of the received signal's energy. In such approach, the energy information is sent to the FC, which sums all the received energies and compares the values with a pre-selected threshold in order to make the global decision;
- Maximum ratio combining (MRC) approach, which allows the FC to combine the energy information with a normalized weight related to the SNR's information of each SU;
- Selection combining (SC) approach, which allows the FC to select the SU with the best SNR and to exploit its sensing results to make the global decision.

Other approaches can be based on statistical approaches such as the Likelihood Ratio Test (LRT) [112]-[114] providing reliable detections. However, their drawbacks are related to the high computational complexity of LRT and the communication overhead generated during the reporting stage.

2.3.3. Basic Framework for CSS

Section 2.2.2.3 introduces a basic framework for the non-cooperative spectrum sensing based on the ED method, a framework that can be extended to cooperative scenarios. In particular, considering an ED-based centralized cooperative scenario composed of M cognitive users, the users can cooperate among them to identify the presence or the absence of the PU in the sensing channel and make the global decision.

At each time k , each i -th SU performs spectrum sensing independently using the ED technique and makes a one-bit decision, namely local decision $d_i(k)$, as follows [115]:

$$d_i(k) = \begin{cases} 1, & T_i \geq \gamma_i \\ 0, & T_i < \gamma_i \end{cases} \quad (6)$$

where T_i and γ_i are the testing variable and the threshold evaluated for the i -th SU as expressed in (3) and (4) respectively.

Once the FC has received all the local decisions through the reporting channels, it makes the global decision, $d(k)$, about the occupancy of the sensing channel at the time k [89]. To make the global decision, the FC can combine the local observations of the SUs through one of the approaches described in the previous sections. In particular, the conventional, basic framework is based on the application of one or more hard combining voting rules, such as the Majority (MAJ) fusion rule [116], [117]. However, to improve the reliability and the accuracy of the sensing results provided by the CSS approach, more sophisticated techniques should be considered.

2.3.4. CSS challenges

Even though CSS ensures improvements in terms of cooperative gain and spectrum utilization, it poses several challenges that should not be overlooked in the design and implementation of a cooperative environment, such as [67], [97], and [118]:

- the synchronization among the SUs and cooperative sensing delay. To make the global decision, it is assumed that SUs are synchronized and send their sensing results not only instantly but also concurrently, which requires to consider the synchronization delay and also the cooperative sensing delay, that

- can be influenced by different factors (i.e. the amount of reporting data, the number of SUs, and the reporting channel access scheme) [118]. Several approaches are proposed in order to decrease the cooperative sensing delays [119] or to avoid the synchronization delay through asynchronous CSS [120];
- the spatially correlated shadowing, which can increase the probability of miss-detection of PU's communications, decreasing the cooperative gain [118], [121]. To mitigate such issue, several works [100]-[122] propose approaches based on user selection techniques, improving the reliability and increasing the network efficiency;
 - the energy consumption, which is further crucial aspect to consider since it is proportional to the amount of sensing data exchanged among SUs and to their number in the cooperative scenario. To tackle this issue and improve the energy efficiency, user selection techniques must be adopted in combination with a data fusion approach, allowing only the selected cognitive users to sense the spectrum and report their local sensing results [123];
 - the PU's and SU's mobility, which can affect the cooperative gain of the CSS [124]. For instance, it is possible to consider a CRN composed of M mobile and static SUs that can observe independent and correlated shadowing at a different time and based on their current location. As a consequence, cooperation throughput changes with the movement of SUs in time [11];
 - it may be required to use additional sensors, such as location awareness sensors, to communicate with a remote spectrum database, obtaining additional information about the current spectrum occupancy and improving the detection accuracy of primary communications. Moreover, several CSS approaches are based on the definition of SUs clusters that can be created by exploiting the distance among SUs;
 - the security of a CRN, which is a critical challenge and is becoming an increasingly popular and actual topic. Without ad-hoc countermeasures against attacks such as Primary User Emulation (PUE) or Spectrum Sensing Data Falsification (SSDF), the cooperative gain and the improvement of the spectrum utilization decrease, allowing malicious SUs to join in the CRN and to opportunistically exploit the available spectrum holes.

Considering the above-mentioned challenges, in this dissertation we will focus our attention on the performance improvement of the centralized CSS based on the ED. Finally, in the next chapter, a detailed analysis of the security issues of CRT will be discussed in detail, highlighting the main vector attacks and how they affect the dynamics of a CRN.

3 Security Issues of CRT

Ensuring the invulnerability of wireless networks is a challenging task. As every other wireless network, a CRN is vulnerable not only to the well-known attacks used against conventional networks, but also to specific threats that take advantage of the drawbacks innate in CR's operations. In this chapter, a deep understanding of the typical security issues affecting CRT is provided, focusing, in particular, on three main categories of attacks: Primary User Emulation, Cognitive Jamming, and Byzantine attacks.

3.1. A Classification of the Main Cognitive Threats

Trust is the most important feature to consider in the design and development of secure distribution systems. Security and trust are always correlated and mutually inclusive for any kind of network [125]-[126].

Due to their open nature, wireless networks are affected by several security threats that target different layers of the ISO/OSI stack, such as the physical (PHY) and the MAC layers [127]. The RF jamming attacks, for example, target the physical layer in order to severely interfere and destroy the network's operations [128], while different kind of attacks which target the MAC layers are related to the spoofing of the MAC address's device or to greedy behaviours [129].

CRN, however, are vulnerable not only to the common security threats that affect traditional networks, but also to specific types of attacks based on the mechanisms proposed by the CRT. Due to the operations and features characterizing CR systems (i.e. dynamic analysis of the radio environments, opportunistic channel utilization, etc.), the issue of their security demands the definition of new approaches, necessarily different from those applied to traditional wireless networks [130].

There are several and diverse security challenges, which can potentially undermine the benefits provided by CRT and disrupt its functionalities, that need to be properly addressed with the definition of apt countermeasures. Security threats to a CRN can occur in different layers of its architecture and through different patterns. The radio environment, for example, can be controlled by malicious users [131] by:

- creating false detection and misdetection of primary communication due to denial of service (DoS) or emulation of the PU;
- exploiting available spectrum holes by denying access to legitimate SUs (selfish behaviour);
- obtaining an unauthorized access to sensing data or falsifying and introducing fake sensing results in the network.

Given the threat they pose, CRT security issues have recently aroused a great interest from Academia and Industries [132]-[133].

In the following sub-sections, an analysis of the security requirements and a classification of the main CR's threats is provided.

3.1.1. Security Requirements for CRNs

The term Information Assurance (IA) refers to the modalities adopted to protect and secure information systems, like wireless networks, against security threats. It is possible to define the IA as [131]:

“the set of measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation”.

In the wake of this definition, studies like [127], and [134] define confidentiality, integrity, availability, and access control as main requirements for the security of wireless network. In particular, confidentiality denies unauthorized users to access and read network data, while integrity allows control units to detect intentional or unintentional data changes. Availability allows entities (i.e. devices or individuals) to access the network's resources when needed, while access control restricts network's resources to authorized entities only. However, as defined by ITU [135], security requirements should be based on the following concepts:

- stakeholders may be users of the communication system, like network providers or the public;
- assets should be composed of several data and services, such as the data stored or transmitted and the network's services;

- threats can be considered as a security violation and they can be intentional (i.e. a malicious user is performing an attack) or unintentional (i.e. an internal failure or a misbehaviour of the device). An example is the modification or disruption of the data stored and transmitted;
- risks refer to the impact of the threat on the network and asset and they can be addressed through the design and implementation of security countermeasures.

Baldini *et al.* [131] extend the definition of security requirements proposed by ITU [136] as defined in Table 8. To meet these requirements, a CR-based system should be able to address security threats by exploiting specific security countermeasures.

Table 8. Extended Security Requirements of ITU [131].

| Security Requirements | Characteristics |
|------------------------------------|--|
| Controlled access to resources | a system should guarantee that unauthorized actors gain access to specific information and services |
| Robustness | a system should provide the required communication services as described in specific service level agreements (SLA). In particular the system should be robust against threats |
| Protection of confidentiality | a system should provide the capabilities to ensure the confidentiality of the managed data |
| Protection of system integrity | a system should ensure the integrity of its components |
| Protection of data integrity | a system should ensure the integrity of the managed data |
| Compliance to regulatory framework | a system should ensure compliance to the regulations valid in the area |
| Non-Repudiation | a system should guarantee that an entity is in no position to deny responsibility for its actions |
| Verification of identities | a network should provide the capabilities to verify the identity claimed by its actors |

3.1.2. Classification of CR's security threats

Section 2.1 introduced the cognitive cycle performed by a CR device by defining the typical cognitive operations (i.e. spectrum sensing and sharing) run to detect and use a spectrum hole. Through such operations, a cognitive user can enter four different stages [16], [19]:

1. the observation stage, which represents the spectrum sensing and decision operations;
2. the reasoning stage, which is related to the learning and prediction process of a SU, allowing it to make an effective decision. If the learning is not properly performed then it might result in a negative impact for the SU;
3. the adaptation stage, which allows SUs to switch to the best transmit parameter;
4. the act stage, which represents the SU's communications based on the previous stage.

As noticed in [137], these four stages can be targeted by different kind of attacks. However, as far as security issues are concerned, the most important ones are observation, reasoning, and act, due to their vulnerabilities (Figure 19) [138].

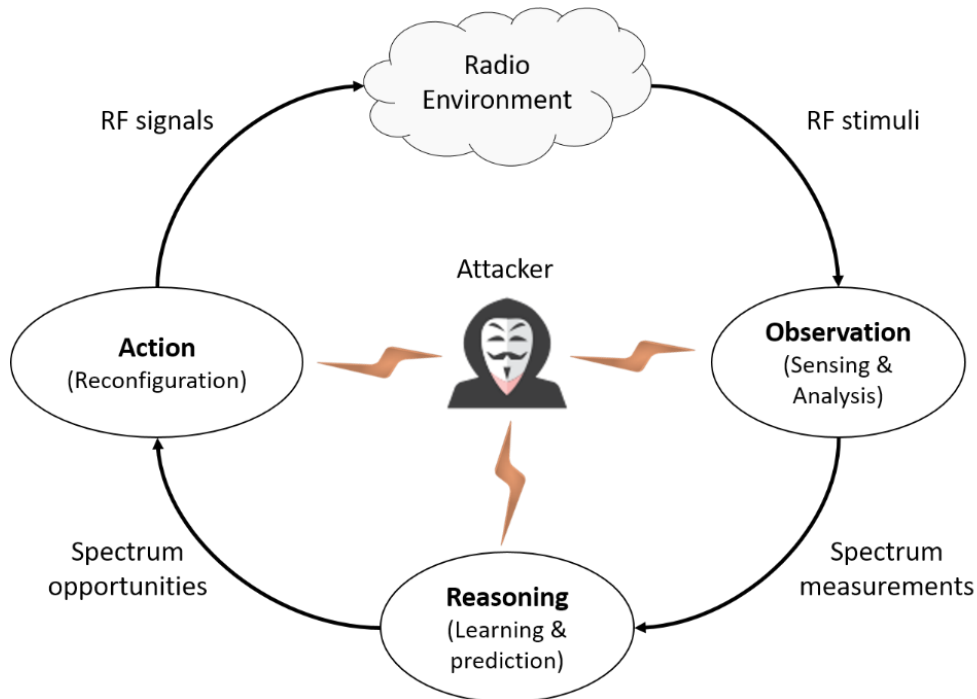


Figure 19. Cognitive Cycle's stages affected by attackers.

For instance, malicious users can attack SUs during the observation stage by emulating the characteristics of a PU and/or providing falsified sensing results to legitimate users. Moreover, a malicious user may interfere with SUs' channel utilization through a traditional jamming attack aimed at blocking legitimate transmissions [139]. Conversely, the reasoning stage may be altered by malware downloaded and installed on cognitive devices to alter the learning and prediction

process and to cause vulnerability to other attacks. In addition, to successfully deploy a CRN, it is necessary to carefully plan and coordinate the function of communication layers, such as the PHY and Data Link. The first one is a layer that enables the communication among CR devices while dealing with the transmit power, the modulation schemes, etc., and enabling the main cognitive operations [140]. For such reason, the operating parameters used for this layer must be chosen carefully in order to enable a dynamic utilization of the radio spectrum.

The dynamism of SUs and CRN does not allow the application of conventional security mechanisms, since they are designed and developed for systems and networks based on the current static spectrum allocation policy. In addition, in a scenario featuring a distributed CRN, things get more complicated and the threats double, since malicious users can exploit the drawbacks of both the distributed network and CRT to launch powerful and elaborate attacks. Hence, CRNs can be targeted by the conventional threats [139] of wireless networks and by more sophisticated attacks designed and launched to focus on two pivotal cognitive features [127]: the re-configurability and capability.

In [131], Baldini *et al.* identify several security threats related to CRT:

1. the jamming of the CCC;
2. the alteration of the messages exchanged in the CRN;
3. the emulation of PUs like digital TV broadcasters. This attack allows malicious users to disguise as PUs to obtain exclusive access to spectrum holes or to perform a DoS denying the available spectrum holes to legitimate SUs;
4. the alteration of cognitive devices in order to modify their behaviour and support other attacks;
5. the internal failure (e.g. memory fault and physical failure) of SUs in order to impact on the CRN;
6. the malicious collaboration with legitimate SUs during the execution of the main cognitive operations. For instance, an attacker may send fake sensing results to the other users during the cooperative decision process;
7. the unauthorized occupation of spectrum bands for selfish use, in order to gain more traffic capacity. This threats can be related to the PU emulation;

8. the unauthorized use of spectrum bands to generate a DoS for PUs by emitting power in unauthorized spectrum bands;
9. the saturation of the CCC to generate a DoS attack. In particular, the attackers send a high number of cognitive messages on the control channel to deny its service to the CR network. To prevent this attack, the CCC must be carefully designed [141];
10. the eavesdropping of cognitive messages coming from the CCC by malicious user that can later exploit the acquired information for further attacks;
11. the disruption of the MAC, network layer, or cognitive engine of the cognitive radio network.

Each threat affects specific operations and stages of the cognitive cycle and proper defence mechanisms are required to deal with and overcome such attacks, as depicted in Table 9.

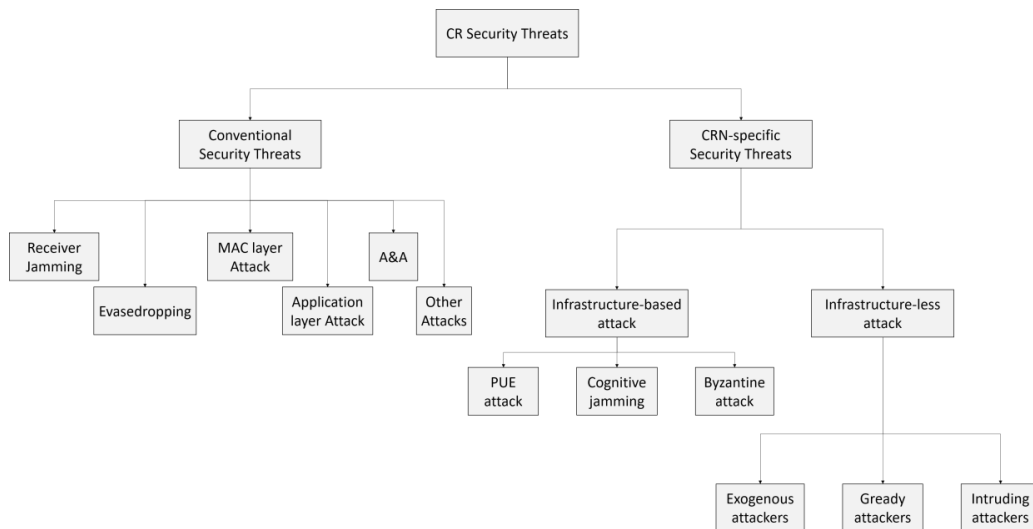


Figure 20. Categorization of different attack scenarios in a CRN [142].

An extensive and rigorous classification, which improves the one proposed by Baldini *et al.*, is provided by Attar *et al.* in [142]. Through a fine-grained analysis of the most common threats (both conventional and specific) that can affect a CRN, the authors trace not only a distinction between conventional and CR-specific threats, but also a classification of such threats in infrastructure-based (e.g. networks based on the IEEE 802.22 standard) and infrastructure-less (e.g. ad-hoc networks) CRN attacks (Figure 20). This classification will be discussed in the next sections.

Table 9. Summary of the Cognitive Threats [131].

| Security Threats | Security Requirement | Affected cognitive cycle operations or stages | Addressed in this dissertation |
|--|---|--|---------------------------------------|
| Jamming of the CCC | Robustness, Protection of system integrity | Spectrum sensing & sharing | X |
| Alteration of the messages exchanged in the CRN | Protection of data integrity, Verification of identities | Spectrum sensing & sharing | |
| Emulation of PUs | Verification of identities, Accountability | Spectrum sensing & mobility | |
| Alteration of cognitive devices | Protection of system integrity, Compliance to regulatory framework | Spectrum management, sharing & mobility | |
| Internal failure | Protection of system integrity, Robustness | Spectrum sensing & mobility | |
| Malicious collaboration with honest SUs | Verification of identities, Accountability, Protection of confidentiality, Controlled access to resources | Spectrum sensing, mobility & management | X |
| Unauthorized use of spectrum bands for selfish use | Compliance to regulatory framework | Spectrum sensing & mobility | X |
| Unauthorized use of spectrum bands to generate a DoS for PUs | Compliance to regulatory framework | Spectrum sharing | X |
| Saturation of the CCC to generate a DoS attack | Robustness, Protection of system integrity | Spectrum sensing & sharing | |
| Eavesdropping of cognitive messages | Protection of confidentiality | Spectrum sensing & sharing | |
| Disruption of the MAC, network layer, or cognitive engine | Verification of identities, Controlled access to resources, Protection of system integrity | Resource management & Data management | |

Following the attacks' identification and classification proposed by [128] and [139], respectively, it is possible to identify two types of behaviours in the attackers: greedy

(or selfish), and malicious. The first one aims to maximize its communication performances and to gain exclusive access to the spectral resources, affecting spectrum sharing and usage fairness. Conversely, a malicious user aims to disrupt the performances and the cognitive operations of both SUs and PUs through DoS attacks, and affects the efficiency of the spectrum usage and the SUs' performance. In addition, this kind of attacker may allow legitimate SUs to unintentionally interfere with the PU's communications. A characterization of these two categories of attackers is proposed in Table 10.

Table 10. Attackers Characterization.

| Behaviour Category | Goals | Approaches | Effects |
|---------------------|--|---|---|
| Greedy (or selfish) | Maximize the attackers' communication performance Gain exclusive access to spectral resources | Induction of false alarms through falsifications of sensing results or emulation of primary communications Creation of DoS | Spectrum sharing efficiency Usage fairness |
| Malicious | Destroy or damage performances and operations of SUs and/or PUs | Creation of DoS Falsifications of sensing results | Spectrum usage efficiency Performance of the affected SUs Interference with PUs |

3.1.2.1. Conventional Security Threats

Being wireless networks, CRNs can be affected by different conventional security threats that can destroy the typical mechanism of the network (i.e. the cognitive cycle operation and stages) and modify the behaviour of honest SUs. These conventional threats can be classified in the following categories:

- Receiver Jamming attack, which aims to interfere with the users' communication through the generation of noise signal over the target channel by decreasing the SNR below the required threshold;
- Eavesdropping attack, which allows attackers to exploit weaknesses in the network's security in order to intercept the messages (i.e. the cognitive messages in a CRN) exchanged among network's users over the

communication channel (i.e. the CCC). To prevent this threat, the SU's communications should exploit the cryptography of the cognitive messages;

- MAC-Layer attack, which takes into account the capability of SUs to modify their operational parameters. In particular, this kind of attack can be performed in a distributed ad-hoc network where attackers create malicious messages to saturate the CCC of the network and generate a DoS. In addition, the attack can be performed by greedy nodes reporting that the channel is not available and using it for its own communications;
- Application-Layer attack, which is based on the re-configurability of cognitive devices that need to download over-the-air (OTA) software to update their capabilities and behaviour. Such aspect addresses a challenging issue, since the cognitive device may download malware, viruses, and other malicious code that force SUs to misbehave unpredictably.
- Authorization and Authentication (A&A) attack, which, as the name says, focuses on two crucial aspects of a CRN (both centralized and distributed). If the network is not able to identify a SU, it allows attackers to enter and attack it. For such reason, a CRN should be based on robust authorization and authentication mechanisms in order to deny intruders access to secondary spectral resources.

The attacks above mentioned are only a small fraction of the possible wireless network attacks to which a CRN can be vulnerable. Others may be the blackhole and selective forwarding attacks, which aim at discarding all the packets transmitted during the communication or only a selection of them, respectively [143]. Other examples are the wormhole and acknowledgment spoofing attacks [141], which can drastically affect not only infrastructure-based networks but also mobile ad-hoc networks (MANET) [142].

3.1.2.2. CR-specific Security Threats

As noticed in [127], [131], [137]-[139] and [146] attackers can exploit typical CR behaviours and operations to create innovative and disruptive attacks with different

goals. In particular, Attar *et al.* [142] have identified two main categories of CR-specific threats: the CR infrastructure-based and infrastructure-less attacks.

The CR infrastructure-based attacks are:

- the primary emulation attack, also known as Incumbent attack, which poses a major threat to the spectrum sensing operations [125]. SUs should be able to distinguish between primary signals, secondary signals and interference. An attacker, however, may disguise as a PU, emulating its signal and characteristics to gain spectrum holes and deny SUs access to them. In particular, the PUE attack (or PUEA) may lead to DoS, in order to prevent SUs from acquiring useful communications, or to harmful interference, in order to prevent SUs from detecting the presence of PUs (additional cause of hidden PU problem). Attackers can also launch a PUEA simultaneously to prevent SUs from identifying new available spectrum holes for their own communications. Additional details about the PUEA are provided in section 3.2;
- the CCC Jamming attack, which aims to generate intentional interference over the CCC by emitting a radio signal with a sufficient amount of power. Performers of this attack are called jammers, since they can jam any ongoing communications in order to destroy them and generate a DoS in the CRN. In addition, the jamming attack impacts on the BER, the received signal strength (RSS) and its indicator (RSSI) as experienced at the desired destination. Finally, to be more effective, jammers can also launch a simultaneous attack over the communication channels. A brief introduction to this attack is provided in section 3.2;
- the Byzantine attack, which is also known as Spectrum Sensing Data Falsification attack, allows malicious users to falsify their own sensing results to decrease the cooperative gain of a CRN (both centralized and distributed). The falsification of the sensing results can aim at: (i) tricking the FC into supposing the PU is present when it is not (selfish aim and DoS); (ii) falsely declaring the absence of the PU to create a harmful interference (vandalism). A detailed description of the Byzantine attack is provided in section 3.4.

The CR infrastructure-less attacks are:

- Exogenous attack, which aims to damage the cognitive operations of CRNs through the exploitation of intentional interferences (i.e. jamming) affecting the CCC, or through the emulation of a primary communication;
- Intruding Attack, which allows attackers to penetrate the cognitive network posing as legitimate users. In particular, they aim to influence the behaviour of SUs by reporting falsified information during the different stages of the cognitive cycle. This attack can be associated to the byzantine attack in the infrastructure-based network;
- Greedy SU attack is a selfish attack where the authenticated and authorized user of the network misbehave to increase their chances of reserving the spectrum hole [147]. This attack produces a dramatic performance degradation and it may occur when the number of available spectrum holes is lower than the number of legitimate SUs and there is a queue to access them.

The infrastructure-less attacks use the strategies and the attacks defined for the infrastructure-based ones. For this reason, it is useful to focus the attention on infrastructure-based attacks and on how they affect the cognitive cycle.

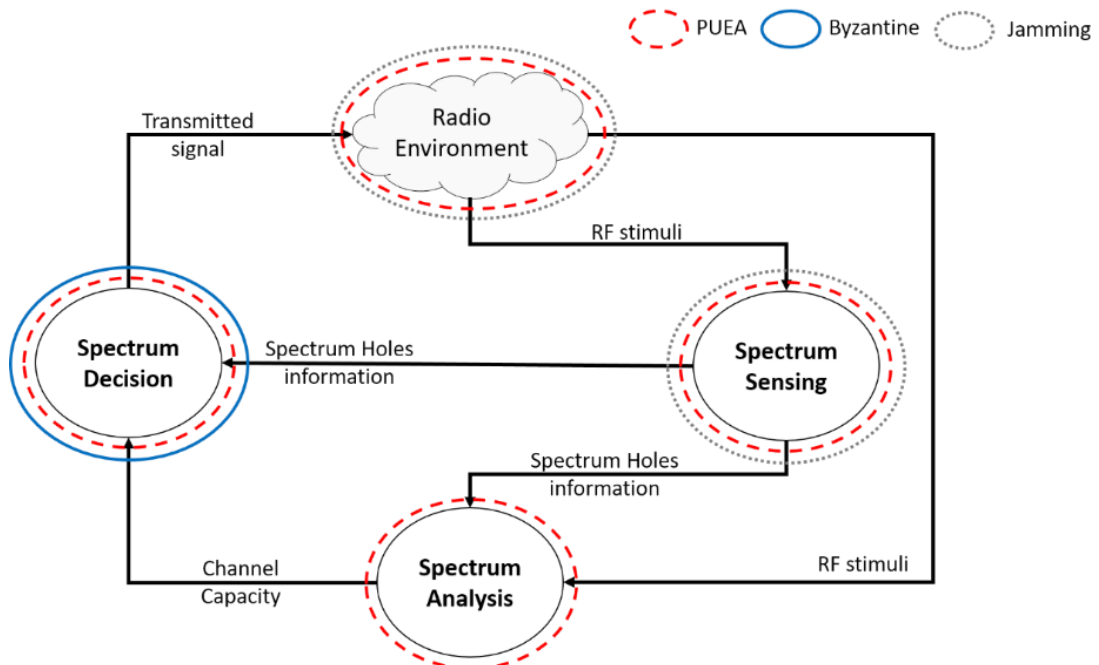


Figure 21. Effects of the PUEA, Byzantine and Jamming on the Cognitive Cycle.

As shown in Figure 21, each attack targets a specific operation of the cognitive cycle, having a different impact and probability to be performed.

Table 11 provides a comparison among these three infrastructure-based CRN attacks through an analysis of their impact on the operations of the cognitive cycle.

Table 11. Summarization of the main Infrastructure-based CRN attacks.

| CR infrastructure-based PHY Threats | PUE attack | Byzantine attack | Jamming |
|--|---|---|---|
| Cognitive Cycle operations | Spectrum Sensing, Analysis, Decision & Radio Environment | Spectrum Decision | Spectrum Sensing & Sharing |
| Impact | High | Moderate | High |
| Probability | Low | Moderate | Low |
| Time of Impact | Short and Long term | Short and Long term | Short term |
| Characteristics | Emulation of PU through the emission of radio signals with same characteristics as PU | Falsification of sensing results to interfere with PU's communications and/or to deny legitimate users access to available spectrum holes | Disruption of legitimate cognitive communication through the emission of radio interference |
| Effects | False alarms due to fake signals Decreased Performance | DoS Decreased Performance | DoS Decreased Performance |

The following sections provide a detailed analysis of PUE, Jamming and Byzantine attacks, analysing their behaviours and possible performing strategies.

3.2. Primary User Emulation attack

CRT allows SUs to opportunistically exploit and use the available spectrum holes and to promptly vacate them if PUs begin transmissions. This behaviour avoids any interference with primary communication and improves spectrum utilization through a spectrum handoff seeking for different, unused channels. To do so, SUs sense the spectrum and distinguish between primary and secondary signals: if the SU recognizes the detected signal, it is assumed to belong to another SU. Otherwise, said signal is classified as primary. This naïve trust model, adopted for sensing techniques like the

ED, is not robust to greedy and malicious users, since they can emulate PUs' features and transmit a signal in a licensed band that may be not recognized by SUs, denying them access to said band.

In the following sub-sections, a definition of the main attacker's behaviours and their related effects on the CRN will be discussed.

3.2.1. PUE Attackers Classification

In several works such as [131] and [148], the PUE attackers are divided in two categories that reflect the general attackers' categorization depicted in Table 10. In particular:

- Greedy attackers aim to gain exclusive use of the available spectral resources by transmitting fake primary signals that force all SUs to vacate said resources. To do so, attackers must monitor the spectrum to identify the frequency bands used by legitimate SUs. Once a busy channel is found, attackers disguise as PUs and force legitimate SUs to leave it;
- Malicious attackers do not aim for exclusive access to channels used by legitimate SUs. They disguise as PUs to launch a DoS attack in the CRN and to interfere with the DSA of legitimate SUs. In addition, to perform a more extensive attack, they can transmit the emulated primary signal on both available bands and the ones used by legitimate users.

The proposed classification is not exhaustive and it does not reflect all the possible behaviours of PUE attackers. Yu *et al.* [149], indeed, identify other two categories:

- Power-based attackers emulate the power level of a PU's signal to perform a PUE attack and deceive legitimate SUs that use ED as sensing technique. In particular, there are two types of power-based attackers, Power-Fixed and Power-Adaptive attackers. The first ones rely solely on a predefined power level, without taking into account the power level of a PU's signal. Conversely, the latter may dynamically adjust the power level of their signals according to the actual transmitting power of the PU and the radio environment;
- Location-based attackers are divided in two categories, static and mobile attackers. Static attackers have a fixed location during the attack process. For

such reason, they can be easily detected with positioning techniques (e.g. the Time of Arrival) and through a comparison with the PU's location, which is known by legitimate SUs. Conversely, mobile attackers can dynamically change their location during the attack, being therefore more difficult to detect.

One of the major drawbacks of the PUE attack is that legitimate SUs may not be able to detect the emulated signal due to a faulty performance of the spectrum sensing technique exploited, causing an interference with the attacker's communications. For the attack to be successful, further conditions should also be met. For instance, communication between SUs and PUs is to be prevented, since it may lead to the detection of the attacker. Also, the attacker must distinguish and learn to emulate the different features characterizing the primary and secondary signal (e.g. the signal modulation). Finally, to hide its presence in the CRN, the PUE attacker has to carefully monitor the radio environment in order to avoid any interference with the PU's communications.

3.2.2. Effects of PUE attack in a CRN

The PUE attack can hinder and affect a CRN and the cognitive operations of its users in different ways. In particular, it affects the spectrum sensing, the analysis and the decisions of a cognitive user, disrupting its performances and behaviour [139]. In addition, as identified in [150]-[151], the potential consequences of a PUE attack are:

- *Bandwidth waste.* The presence of a greedy or malicious user in the CRN causes a waste of the spectral resources, affecting spectrum usage efficiency. In fact, attackers may steal spectrum holes from legitimate SUs and deny them access to the available frequencies;
- *QoS degradation.* Due to a PUE attack, the QoS of a CRN can be severely deteriorated. SUs' operations are interrupted and disrupted by the attackers and SUs are forced to repeatedly vacate the spectral resources to seek for new spectrum opportunities. This behaviour can lead to unsatisfying delays and jitters in SUs' operations;
- *Connection unreliability.* As a result of a successful PUE attack, SUs may fail to identify other spectrum opportunities to use for their services, causing the

drop of real-time services. Even though, because of the nature of the DSA, CRT itself does not guarantee SUs stable spectral resources, PUE attackers can significantly increase the unreliability of a CRN's connection;

- *DoS*. The DoS is the major goal of malicious attackers aiming to interrupt SUs' services. For a successful and powerful DoS, attackers have to cooperate to transmit emulated primary signals over all the available spectrum holes. In this scenario, SUs can be left with no channel to use as CCC for the transmission of control messages and so the CRN has to be suspended;
- *Interference with the Primary Network*. This scenario takes place when the PUE attacker fails to correctly detect a PU's occurrence, causing interference with a primary communication. There is still the possibility, however, that SUs can incorrectly identify the real PU and, as consequence, interfere with its communication.

3.2.3. CRN in Presence of PUE attackers

Figure 22 shows an example of centralized CRN in presence of PUE attackers. In the considered scenario, the licensed band is represented by six channels (i.e. f_1, \dots, f_6) and the primary BS exploits only the frequencies f_1, f_3 , and f_5 for its communication with the primary receivers, while the SUs can exploit the idle frequencies (i.e. f_2, f_4 and f_6) for their transmissions. However, the presence of a PUE attacker (i.e. the $PUEA_1$) may prevent SUs from using idle channels. For instance, the PUEA mimics the primary signal in channel f_2 and, if it succeeds, then SU_1 and SU_2 have to evacuate channel f_2 . Consequently, the link between these users is interrupted and the channel becomes idle again. In this scenario, assuming the communication channel is affected only by AWGN, it is possible to define four different testing hypotheses that describe the possible states of the CRN.

These hypotheses can be expressed as follows:

$$\begin{cases} H_{s0} : & \text{Noise only} \\ H_{s1} : & \text{PU + Noise} \\ H_{s2} : & \text{PUEA + Noise} \\ H_{s3} : & \text{PU + PUEA + Noise} \end{cases} \quad (7)$$

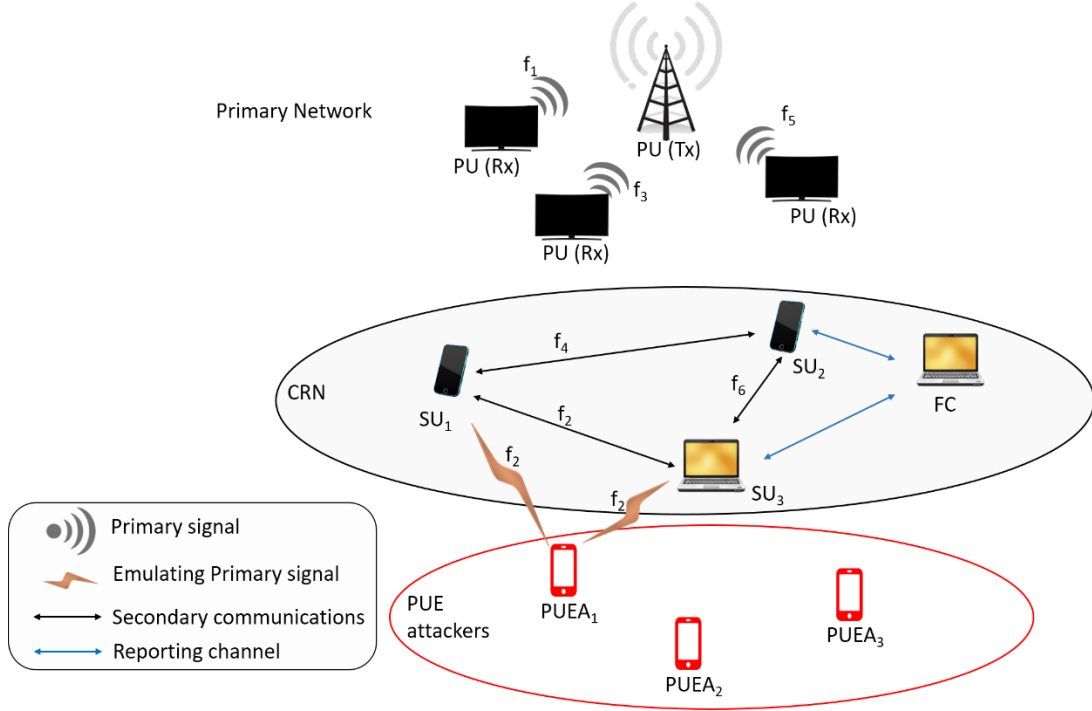


Figure 22. Centralized CRN in presence of PUE attackers.

where, in the first hypothesis, the signal received by i -th SUs will be composed only by the Gaussian noise that affects the channel, while the second hypothesis states the presence of a true PU's signal transmitted over the channel. Conversely, the third and the fourth hypotheses take into account the presence of a PUE attacker that tries to deceive SUs by sending a signal emulating the one transmitted by a PU. In particular, the third hypothesis indicates only the presence of a PUE attacker's signal affected by the noise, while the fourth one considers the simultaneous presence of both the PU's and the PUEA's signals.

The signal received by the i -th SU at the k -th time is:

$$y_i(k) = \alpha \sqrt{P_{PU}} x_{PU}(k) + \beta \sqrt{P_{PUEA}} x_{PUEA}(k) + w_i(k) \quad (8)$$

where $x_{PU}(k)$ and $x_{PUE}(k)$ are the signal transmitted by the PU and the PUE attacker with a power P_{PU} and P_{PUEA} , respectively. Conversely, $w_i(k)$ is the Gaussian noise that affects the channel, while the noise and the signals of the PU and the attacker are zero-mean and mutually independent random processes. Finally, α and β are two binary indicators that indicate the presence or the absence of the PU and the PUE attacker, respectively. In particular, the above hypothesis results in:

$$y_i(k) = \begin{cases} w_i(k) & H_{s0}, if \alpha = 0, \beta = 0 \\ \sqrt{P_{PU}} x_{PU}(k) + w_i(k) & H_{s1}, if \alpha = 1, \beta = 0 \\ \sqrt{P_{PUEA}} x_{PUEA}(k) + w_i(k) & H_{s2}, if \alpha = 0, \beta = 1 \\ \sqrt{P_{PU}} x_{PU}(k) + \sqrt{P_{PUEA}} x_{PUEA}(k) + w_i(k) & H_{s3}, if \alpha = 1, \beta = 1 \end{cases} \quad (9)$$

In order to properly perform the CSS and detect a PUE attack and the attacker, it is necessary to define a defence mechanism that is able to distinguish among these four testing hypotheses without decreasing the sensing performance of the users.

3.3. Cognitive Jamming attack and its effect on CCC

In communication systems, interference can be divided into two categories: the System Inherent Interference (SII) and the Hostile Jamming (HJ). In the SII scenario, the interference is caused by signals emitted from different active, transmitting users (i.e. multi-path propagation), while in the HJ scenario, the interference is introduced by attackers that intentionally transmit signals to deteriorate or destroy users' communications. While the SII can be easily dealt with through the design of a multi-user communication protocol, the HJ is harder to mitigate because the attackers, namely jammers, aim to saturate communication channels like the CCC with noise or false messages so that it is hard to detect them. Furthermore, jammers do not obey to the communication protocol, which makes them unpredictable, allowing adversaries to carry out DoS attacks [152].

In a conventional jamming attack, jammers use a fixed-strategy, performing the same activity for all the duration of the attack. This behaviour, however, is not effective in a CRN, since SUs can dynamically switch communication channels and identify those reflecting the desired QoS [153]. In addition, valid solutions to tackle conventional jamming are the Direct Sequence (DS) and Frequency hopping (FH) techniques, thanks to which the network is affected by the malicious activity only for a short time. However, recent studies [138], [154] have introduced the definition of a new, CRT-based generation of jammers, namely cognitive jammers (CJs), which are able to adapt their attack strategies in real-time by analysing the current radio environment dynamics. To do so, CJs have to sense the radio spectrum, analyse the

acquired data, decide the best attack strategy, and finally adapt their malicious transmissions to the conditions of target channel [153]. This is why CJs can easily cause inefficient transmissions of data or total failures of the CRN.

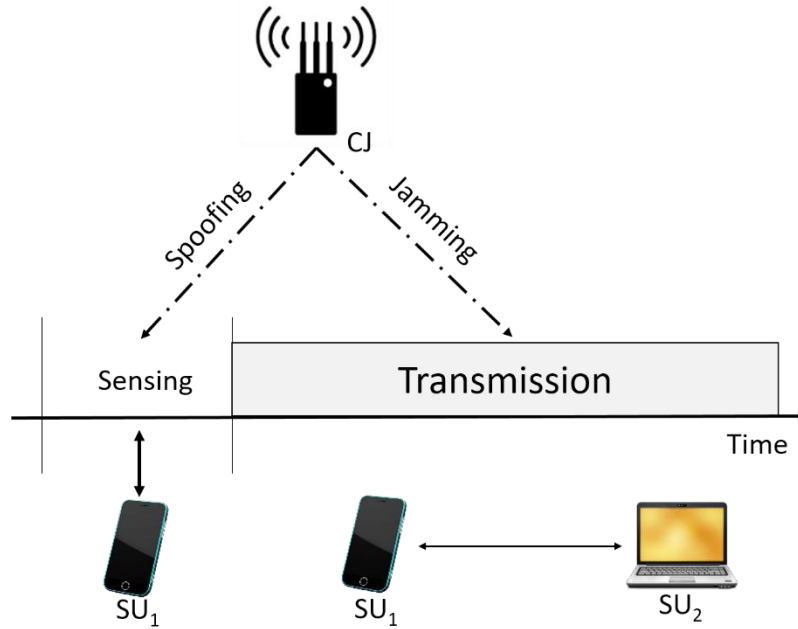


Figure 23. Example of a CRN in presence of a Cognitive Jammer.

As shown in Figure 23, a CJ aims to jam only SUs' communications. In order to target them, it has to sense the radio environment frequently, jumping among the various spectrum holes and discriminating between primary and secondary communications. The Cognitive Jamming attack is a fundamental category of security threats that can severely influence the behaviour and mechanisms of a CRN, due to its critical application in tactical communication networks [155]. The goals of a CJ can be summarized as follows:

- maximization of jamming gain, defined as the ratio between the power used by the model for jamming and the power of the constant jammer;
- success of the jamming attack targeting specific legitimate users or channels;
- minimization of the probability of being detected in the network.

As mentioned in the previous sections, jamming is a well-known attack in wireless networks and it has been introduced in military scenarios to prevent adversaries' communications [153], [155].

3.3.1. Strategies of Cognitive Jammers

To interrupt users' communications, CJs can deploy different attack strategies targeting both the PHY layer or the higher layers, in order to make the jamming attack as effective as possible [156].

In wireless networks, several jammer's attack strategies have been identified, most aimed at creating harmful interference. In particular, the most effective cognitive jamming attacks are [156]-[157]:

- Constant jammer, which generates noise signals continuously without following any MAC protocol. It denies legitimate SUs access to the channel and prevents them from using it, disguising it as busy;
Random jammer, which can be considered as an improvement of the constant jammer since it decreases the power usage by switching between two states: sleep and jamming. During the jamming state, the attacker sends a signal (both a noise and an emulated PU signal) over the target channel for a certain time, and then it stops, switching to the sleep state and becoming inactive. The sleeping and jamming periods are either fixed or random, and they can be modified in order to maximize the attack gain. Such behaviour also decreases the probability of being detected;
- Deceptive jammer, which continually injects signals with characteristics similar to those of a PU's transmission (instead of noise signal used in the constant jammer) in order to deceive SUs into believing that a PU is occupying the channel. Compared with the constant jammer, this attacker is harder to detect but it is inefficient in terms of the power used because of the continuous transmissions;
- Reactive jammer, which is the smartest attacker since it launches the attack only if it detects some activity on the target channel. It aims to compromise the reception of messages by disrupting both small and large packets. To do so, the attacker has to sense the radio environment continuously, which increases the power usage even more than in a random jammer scenario, but with the crucial difference that a reactive jammer is considerably harder to detect.

Several studies have analysed the impact of these strategies on a CRN. For instance, Balogun *et al.* [158] focus on the impact of jamming strategies from two different point of views (i.e. jammers and defenders) considering different metrics, such as power usage and cost. In Table 12, a comparison among the considered strategies is provided, showing how constant jamming can be considered the less effective one in terms of power usage.

Table 12. Impact of Jamming Attacks.

| Point of View | Metrics | Jamming strategies | | | |
|-----------------|--------------------------|--------------------|--------|-----------|----------|
| | | Constant | Random | Deceptive | Reactive |
| Jammer | Power usage | High | Low | High | Medium |
| | Throughput | Low | Medium | Low | Low |
| | SNR | High | Medium | High | Medium |
| | Cost | Low | Medium | Medium | Medium |
| | Scalability | High | High | High | High |
| | Level of DoS | Low | Medium | Low | Low |
| | Tech. Complexity | Low | Medium | Medium | Medium |
| | Intelligence Required | Low | Medium | Medium | Medium |
| Defender | Cost | Low | Medium | Medium | Medium |
| | Scalability | High | High | High | High |
| | Probability of Detection | High | Medium | Low | Medium |
| | Intelligence Required | Low | Medium | Medium | Medium |

3.3.2. CCC vs Cognitive Jamming

A new kind of jammer that attacks CCCs (crucial channels for the CRN) has been identified and modelled in [153], [159]. In fact, even though CCCs allow SUs to

cooperate among them, they remain exposed to jamming attacks that aim to destroy network operations. The introduction of high interference over a CCC can prevent SUs from receiving valid control messages, causing a DoS. A CCC jammer can cause a severe degradation in the network's performance exploiting compromised SUs in the CRN. These compromised users can reveal the pseudo-random number (PN) sequences used by spread spectrum techniques to mitigate jamming attacks. Such kind of jammer is more power-efficient and more effective since it aims to attack only the CCCs of the CRNs with harmful attacks [160].

3.4. Byzantine attack

Despite the improvement granted by the cooperative sensing, the openness of low-layers protocol stacks makes CSS vulnerable to Byzantine attacks [161], which falsify the sensing results to damage the reliability of CSS and to increase the attackers' gain [162]-[163]. As a matter of fact, attackers launch a Byzantine attack to interfere with a PU's communications and obtain exclusive access to the detected spectrum hole, increasing the false alarm probability [163]. These aspects are summarized by Fatemeh *et al.* [164]-[165] in two objectives: exploitation and vandalism.

When an attacker's objective is exploitation, it aims at preventing legitimate SUs from accessing idle channels. In a centralized CSS, for example, malicious users inform the FC that a given channel is busy when it is actually free. Consequently, the FC can declare the presence of a primary transmission, denying access to honest SUs, while the malicious ones can exploit the idle channel exclusively. Conversely, if malicious users have vandalism as objective, then they try to create a massive interference attack by sending to the FC a falsified sensing result that declares the absence of the PU in the sensing channel. Therefore, the FC unintentionally increases the probability of false alarm and allows legitimate SUs to use the busy channel and interfere with the primary communication. This category of malicious users wants to discourage PUs from sharing their unused licensed bands by creating interference with primary transmissions, which is against the assumption of CRT.

Malicious users can also attack a CRN with both the above-mentioned objectives (i.e. a mixed objective) if they aim at destroying the network maximizing their attack utility.

Based on this twofold, objective-oriented classification, it is possible to identify different kinds of behaviours in byzantine users [166]:

- *Always Busy* (AB) attackers state the presence of a PU’s communication in the sensing channel while it is free (exploitation objective);
- *Always Free* (AF) attackers report to the FC the absence of the PU in the considered channel while it is busy (vandalism objective);
- *Opposite* (Opp) attackers always declare the opposite of their local results (mixed objective);
- *Smart Always Free* (SAF) attackers randomly report to the FC the opposite of their sensing result (mixed objective).

In the following sections, a description of the main parameters of a Byzantine attack and of its strategies will be provided.

3.4.1. Attack’s parameters

To answer the question of where, who, how, and when to launch a Byzantine attack, Zhang *et al.* [163] identify the following four parameters (Figure 24): attack scenario, population, opportunity, and basis.

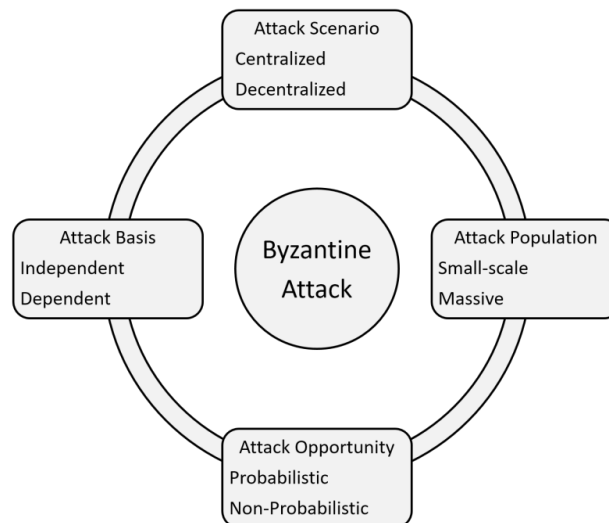


Figure 24. Classification of typical Byzantine attack parameters [163].

The attack scenario identifies where the attackers may act in the network. It cannot be considered as a parameter of Byzantine attackers since it refers to those circumstances to which attackers must adapt in order to launch a successful attack. Byzantine attackers operate based on the two main CSS's strategies (i.e. centralized and distributed), affecting the cooperative scenario in different ways. In fact, the attacker's behaviour changes according to the cooperative strategy.

Several studies, such as [167]-[168], have proved that the centralized cooperative sensing is robust to this attack vector thanks to the presence of the FC. In particular, the FC can be equipped with an ad-hoc function that allows tracking and monitoring the behaviour of every SU (both honest and malicious) in the radio environment, identifying the malicious ones. Conversely, the distributed CSS requires a strict cooperation among SUs, which are expected to exchange their local results and make a global decision together [168]-[170]. Consequently, malicious users can gather sensitive information (i.e. the sensing results of the honest users and the detection algorithm used in the CRN) to support the attack. They can also integrate fake sensing results into their neighbours' decision process and stealthily forward them to other users due to the nature of distributed decision algorithms.

The attack basis identifies how Byzantine attackers perform the attack. It can be performed in independent and dependent ways. In the first case, which is the most common, a malicious user performs the attack independently relying solely on its sensing capabilities, therefore significantly reducing the range of possible attack strategies. Conversely, the dependent strategy allows malicious users to cooperate in order to attack the CRN and to obtain useful information, such as data fusion techniques or defence strategies [171]. In this approach, attackers create a distributed sub-network and share sensing results to coordinate the attacks and increase the success rate probability. A dependent strategy is also very effective in distributed scenarios since it allows attackers to support each other in a possible trust verification scheme. However, this attack vector is based on a multi-hop communication that can create issues during the malicious cooperation, ultimately exposing the attack behaviour.

The attack opportunity specifies when an attack should be launched in order to maximize its gain and decrease the risk of detection. Attackers can decide whether to attack or not with a certain probability, while taking into account information such as its own sensing results and attack expectation [172]. As a matter of fact, sending falsified results to the FC at each sensing time, can be counterproductive for malicious users, since it increases the probability to be detected by a defence mechanism released on the FC. A probabilistic attack model [163], [173] is therefore required to improve the attack stealthiness. However, probabilistic attacks ignore current observation slots and can be detected over time through a statistical analysis.

Finally, the attack population refers to the actors of the attack and indicates the severity of the damages suffered by the targeted network. An increase in the attack population corresponds to an increase in its gain, causing a DoS in the targeted CRN. Hence, based on this parameter, two different attacks can be distinguished:

- Small-scale attack, with a number of attackers lower than a given value;
- Massive attack, with a number of attackers greater than or equal to a given value.

According to [163], [174], this discriminating value is named *blind point*.

Finally, it is interesting to notice that the effects of attack population are strictly related to the data fusion techniques exploited by the FC [175].

Malicious users launching a Byzantine attack need to accurately evaluate these four parameters in order to avoid detection and exclusion from the CRN.

3.4.2. Attack strategies

The Byzantine attack can be performed by adversaries through different strategies based on the above-mentioned parameters [163]. Such strategies are:

- the Centralized Independent Probabilistic Small-Scale (CIPS) strategy (Figure 25.a), which is widely considered in related literatures for the analysis of the robustness of centralized CSS. In this strategy, the Byzantine attack is based on a small group of malicious users that sense the target channel independently and randomly send falsified sensing results with a certain probability to the FC.

Due to the simplicity of this strategy, attackers can be easily identified by several defence algorithms released on the FC [176];

- the Centralized Dependent Probabilistic Small-Scale (CDPS) strategy (Figure 25.b), which allows attackers to cooperate and coordinate the attack by exploiting additional information such as: the knowledge of the data fusion technique used by the FC and/or the defence strategy [177]-[178]. Malicious users sense the spectrum independently and then exchange their results in order to consistently falsify the data with a certain probability and to enhance the attack's potency. The effects of this strategy on the centralized CRN are severe, but it is still possible to detect such attack thanks to the probabilistic approach and to the high correlation of the attackers;
- the Centralized Dependent Non-Probabilistic Small-Scale (CDNS) strategy (Figure 25.c), which poses as an alternative to the previous one. The CDNS is based on a non-probabilistic approach that allows attackers to consider the current state (i.e. attack expectancy) of the network and to adjust their attack behaviour with a certain flexibility. Therefore, the attackers aim to cleverly select attack opportunities and decrease potential risks by avoiding unprofitable attacks [179];

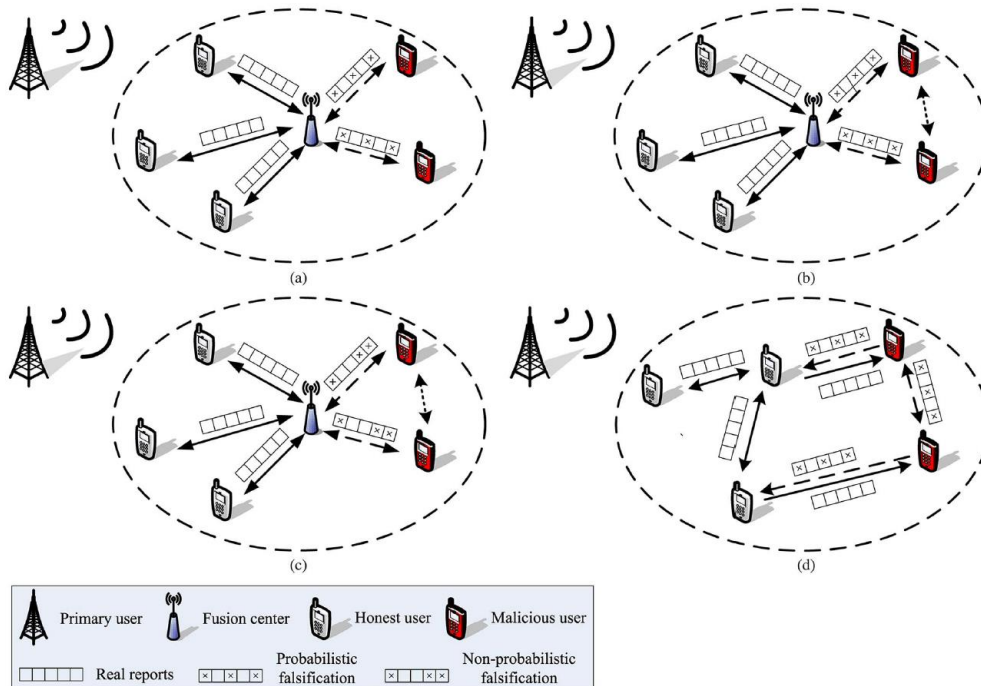


Figure 25. Principal strategies of Byzantine attack [163].

- the Decentralized Independent Probabilistic Small-Scale (DIPS) strategy (Figure 25.d), which aims to attack a CRN based on distributed CSS by using the sensing results of legitimate users. The additional knowledge acquired provides attackers with a deep understanding of the state of the targeted channel and allows them to inject falsified observation in the iteration stage of the distributed decision algorithm [180].

A summary comparison among these strategies is proposed in Table 13.

Table 13. Summary of the Byzantine strategies based on [163].

| Attack Strategy | Attack Parameters | | | | Characteristics |
|-----------------|-------------------|-------------|-------------------|-------------|--|
| | Scenario | Basis | Opportunity | Population | |
| CIPS | Centralized | Independent | Probabilistic | Small-scale | The most common attack strategy Byzantine users are vulnerable to detection |
| CDPS | Centralized | Dependent | Probabilistic | Small-scale | Additional information about the CSS' cooperative strategy and defence strategy improves the attack's effectiveness High similarity between attackers accelerates attackers' exposure |
| CDNS | Centralized | Dependent | Non-Probabilistic | Small-scale | Flexible and furtive Hard to perform |
| DIPS | Distributer | Independent | Probabilistic | Small-scale | Enriched attack basis and enlarged range of attack opportunities Convergence speed decreases |

The CIPS attack can be considered the most popular Byzantine strategy in literature thanks to its simplicity, which provides the basis for the other more advanced attacks. However, if malicious users can gather additional information, then a dependent-based strategy will be their first choice because it ensures a better management of the attack's

behaviour. It is interesting to notice that all the considered strategies are based on a small-scale population (i.e. the number of attackers is lower than the number of honest users) having a limited effect on the cooperation. In order to improve such effect and create a powerful DoS in a target CRN, a massive attack is required.

4 Performance improvement of CSS in Trusted CNR

Cooperative sensing is becoming a popular approach to improve spectrum efficiency and avoid interference with primary communications. As discussed in section 2.3, CSS is based on a collaboration (centralized or distributed) among SUs aimed at making a reliable decision on spectrum occupancy while overcoming the typical spectrum sensing issues [57], [67], such as: the hidden PUs problem, shadowing, noise uncertainty and fading.

Most of the approaches defined for the CSS consider the observations of the SUs as independent, in order to simplify the operating scenario. However, this assumption is not practical in those cases where the proximity among SUs results in correlated observations [181]-[182]: as the distance between the users decreases, the correlation between the users' observations increases, causing a decrease in the performance. Moreover, even if the PU is transmitting over a channel, most of the correlated observations may be under the conventional threshold of ED-based techniques. This results in a dramatic decrease of the cooperative gain and, hence, in an increase of the probability of interfering with the primary communications.

In this chapter, a new test for the performance improvement of CSS in trusted CRN is proposed assuming a correlation between SUs' observations. The proposed method exploits two tests at once to recover these unlucky cases and to increase the cooperative gain. In particular, a further threshold is introduced and the correlated observations are processed with two different fusion rules (the OR and MAJ voting rules) in order to improve the detection performance and enable a faster rejection of the occupied bands. Moreover, a preliminary analysis of the proposed method in a real communication channel affected by AWGN and by different levels of noise uncertainty is proposed and discussed.

4.1. CSS in presence of Correlated SUs' observations

In the CSS, each SU performs the spectrum sensing locally and independently using the conventional ED, as defined in section 2.3.3. However, if the distance among the SUs decreases, then the observations of SUs are correlated.

According to [181], let M be the number of SUs that make M correlated observations where the correlation coefficients are given by

$$\begin{aligned} E \left[\prod_{i \in I} d_i | H_j \right] &= E[d_{i,1}, d_{i,2}, \dots, d_{i,M} | H_j] \\ &= P(d_{i,1} = 1, d_{i,2} = 1, \dots, d_{i,M} = 1 | H_j) \end{aligned} \quad (10)$$

where $i, l \in \{1, \dots, M\}$, $i \neq l$, the $E[d_{i,l} | H_j]$ and $P(d_{i,l} = 1 | H_j)$ are the conditional expectation and conditional probability, given H_j with $j = 0, 1$, respectively.

$$\begin{aligned} E[d_i | H_1] &= P(d_i = 1 | H_1) = P_D^i \\ E[d_i | H_0] &= P(d_i = 1 | H_0) = P_{FA}^i \end{aligned} \quad (11)$$

where P_D^i and P_{FA}^i are the probability of detection and false alarm of the i -th SU, respectively. The correlation coefficient $\rho_{i,l}^j$ between the two local decisions d_i and d_l of the SUs i and l , respectively, under the testing hypothesis H_j is given by:

$$\rho_{i,l}^j = \frac{E[d_i d_l | H_j] - E[d_i | H_j] E[d_l | H_j]}{\sqrt{(E[d_i^2 | H_j] - (E[d_i | H_j])^2)(E[d_l^2 | H_j] - (E[d_l | H_j])^2)}} \quad (12)$$

Since $d_i \in \{0, 1\}$, it follows that $d_i = (d_i)^2$. Therefore:

$$\rho_{i,l}^j = \frac{E[d_i d_l | H_j] - E[d_i | H_j] E[d_l | H_j]}{\sqrt{(E[d_i^2 | H_j] E[d_l^2 | H_j])(1 - E[d_i | H_j])(1 - E[d_l | H_j])}} \quad (13)$$

Assuming that the distance between two SUs is short, if compared with the distance between them and the PU, the received signal at each SU will experience an almost identical path loss. Therefore, in case of an AWGN environment, it is possible to assume equal SNRs for the different users [183]. Assuming the same threshold for all SUs (i.e. $\gamma_i = \gamma$), then $P_{FA}^i = P_{FA}$. In case of an AWGN channel, as assumed in section 2.3.3, it is also possible to have $P_D^i = P_D$. Since $E[d_i | H_j] = E[d_l | H_j]$ from (11), $\rho_{i,l}^j$ is independent of i and l , and every pair of local detectors is equally correlated [184]. Therefore:

$$\rho^1 = \frac{P[d_i = 1, d_l = 1|H_1] - P_D^2}{P_D(1 - P_D)} \quad (14)$$

$$\rho^0 = \frac{P[d_i = 1, d_l = 1|H_0] - P_{FA}^2}{P_{FA}(1 - P_{FA})} \quad (15)$$

where ρ^1 and ρ^0 are the correlation coefficients under the hypotheses H_1 and H_0 , respectively. It is clear from (14) and (15) that ρ^j varies only with $P[d_i = 1, d_l = 1|H_j]$, which is a function of only P_D under H_1 and a function of only P_{FA} under H_0 .

Kalid *et al.* in [181] provide an analysis of the CSS' performance in presence of correlated observations by using the hard combining voting rules, i.e. the OR, AND, and MAJ voting rules. The obtained results show that, for all the fusion rules, the performance of the cooperative sensing degrades due to the presence of correlated users and with the increase in correlation between the correlated observations of the SUs. In addition, the OR and MAJ voting rules are always superior to the AND rule. As a matter of fact, in the AND rule all the observations must be under the threshold to declare the presence of a spectrum hole, and that is too strict a requirement to meet in presence of a large number M of SUs.

4.2. Modified Twin Test

In a CRN composed of a large number of SUs, the spectrum observation can be strongly correlated due to the proximity among SUs. In this scenario, the performance of the conventional ED-based CSS with independent observations drastically degrades. In addition, as shown in [181], with the increasing of the correlation degree among SUs' observations the cooperative gain decreases for all the Hard Combining Voting Rules.

In this section, a new test for the performance improvement of CSS in presence of correlated observations is designed. Recently, a method (namely twin test) for the performance improvement of code synchronization in wireless communications that takes into account correlated cells has been presented in [185]-[186]. Code synchronization is a task conceptually similar to spectrum sensing. In fact, a problem is modelled as a binary hypothesis testing, and the conventional method (the so-called power detector) compares the testing variable to a proper pre-selected threshold.

An improved and modified version of this procedure, namely the Modified Twin Test (MTT), is proposed for application to the CSS in presence of correlated observations. In particular, as shown in Figure 26, the MTT is performed by SUs that send their decision to the FC.

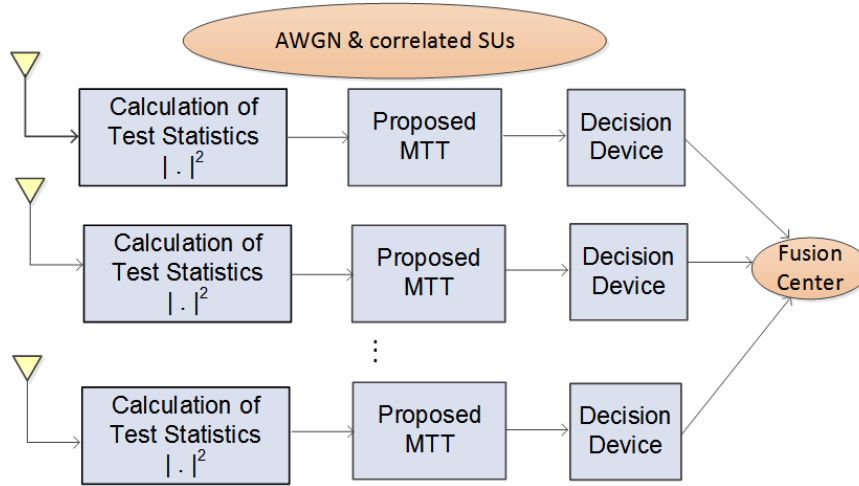


Figure 26. Block diagram of proposed EMTT method under noise uncertainty considering correlated users.

Taking into account the system model presented in section 2.3.3, the rationale of the new test is as follows. The MTT features an additional threshold γ_L (lower than conventional ED-based CSS) and an upper threshold γ_U (different from the conventional threshold γ) and employs two fusion rules (OR and MAJ) to process the correlated observations. In addition, the CFAR criterion is adopted for setting the threshold value of both the ED and the MTT methods. Each SU performs the spectrum sensing combining the ED and the new pair of thresholds. Then, if the testing variable T_i is lower than the γ_L threshold (H_0 hypothesis) or greater than or equal to the γ_U (H_1 hypothesis), then the i -th SU sends its local decision to the FC. Otherwise, if the testing variable is between the γ_L and γ_U thresholds, the FC receives the information about the energy of the received signal. From a practical point of view, the cognitive SUs can now send to the FC two information: their local decision and the received signal energy. In detail, let d'_i be the local decision of each i -th SU about the channel occupancy:

$$d'_i(k) = \begin{cases} 1, & T_i \geq \gamma_U \\ 0, & T_i \leq \gamma_L \end{cases} \quad (16)$$

Then, let I_i denote the information that each i -th SU sends to the fusion center:

$$I_i(k) = \begin{cases} T_i & \gamma_L < T_i < \gamma_U \\ d'_i(k) & \text{otherwise} \end{cases} \quad (17)$$

where T_i is not only the testing variable but also the value of the received signal energy evaluated by the i -th SU. The FC combines the correlated observations and makes the global decision as shown in Figure 27.

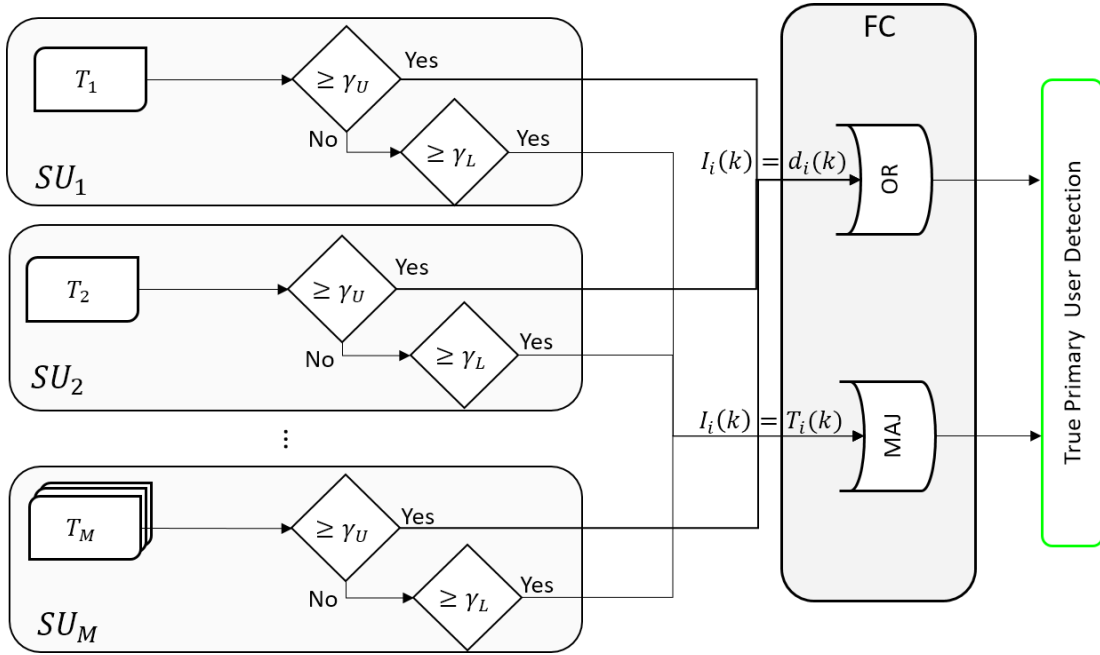


Figure 27. Simplified block scheme of the MTT methods.

The FC declares the presence of a PU's transmission if at least one correlated observation is greater than γ_U (i.e. $d'_i = 1$), in accordance with the OR fusion rule. Otherwise, if the majority of the information (I_i) sent to the FC is the energy of the signal received (i.e. the testing variable) by the i -th SU, then the MAJ rule can be applied to reliably detect the absence or presence of the PU's signal. Finally, if all the correlated decisions are under the lower threshold (i.e. $d'_i = 0$ for each i -th SU) or if the above-mentioned tests fail, the PU is declared absent.

A further novelty of our optimized MTT approach is the presence of more than one possible pair of thresholds (γ_L, γ_U) that meet the CFAR criterion, and the best one is chosen as the pair maximizing the P_D . In fact, fixing the P_{FA} to a desired target value,

the threshold evaluation step can be described as the following constrained-optimization problem: find the unique pair (γ_L, γ_U) that maximizes P_D , with the constraint that P_{FA} must be equal to the desired P_{FA} target value.

As opposed to the conventional ED-based CSS, which combines the local decisions of the SUs by using only one of the three fusion rules, the MTT is able to declare the presence of the PU employing two tests at once. In addition, the strong correlation among the testing variables makes it unlikely to detect a PU in one of them if they are jointly below the lower threshold.

4.3. Simulation Results

In this section, simulation results are presented and discussed to evaluate the performance of cooperative sensing in presence of correlated users. In addition, we consider a comparison with the results of the method proposed in [181] to state the effectiveness of the MTT. As in [181], we consider a network with M SUs, with all users participating in the final decision. The correlation between the M observations is represented by the correlation coefficient ρ , which is assumed to be equal under the two hypotheses H_0 and H_1 . The number of sensing symbols N of the constant modulus BPSK-modulated signal is set to 1000, the target P_{FA} is considered equal to 10^{-3} , and all the cooperating users have equal unitary noise variance. Finally, 10^4 Monte Carlo simulations to numerically compute the system's performance are used for each test.

Figures 28-30 show the detection probability of the system for the OR, AND, MAJ voting rules as well as for the MTT procedure versus SNR for $M = 3, 5, 10$. Figure 32.a represents the case of $\rho = 0.1$ while Figure 32.b depicts the cases of $\rho = 0.5$. As shown in the graphs, the highest P_D for all the methods is reached in correspondence of the lower correlation coefficient, i.e. in correspondence of a higher independence between sensors. In Figure 33 and 34, which illustrate $M = 5$ and $M = 10$ and again for a $\rho = 0.1, 0.5$., it is interesting to note that the P_D increases with the increasing of the number of SUs, as the observations become more and more correlated (i.e. with higher correlation coefficients). This happens because, in presence of correlated users, increasing the number of sensors means exploiting multi-user diversity, hence increasing the system performance.

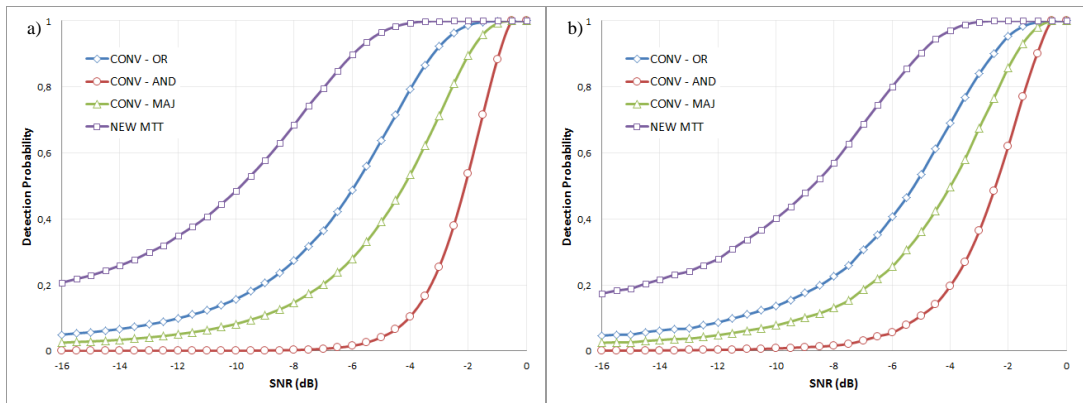


Figure 28. P_D of all the considered methods for three correlated observations and: a) $\rho = 0.1$; b) $\rho = 0.5$.

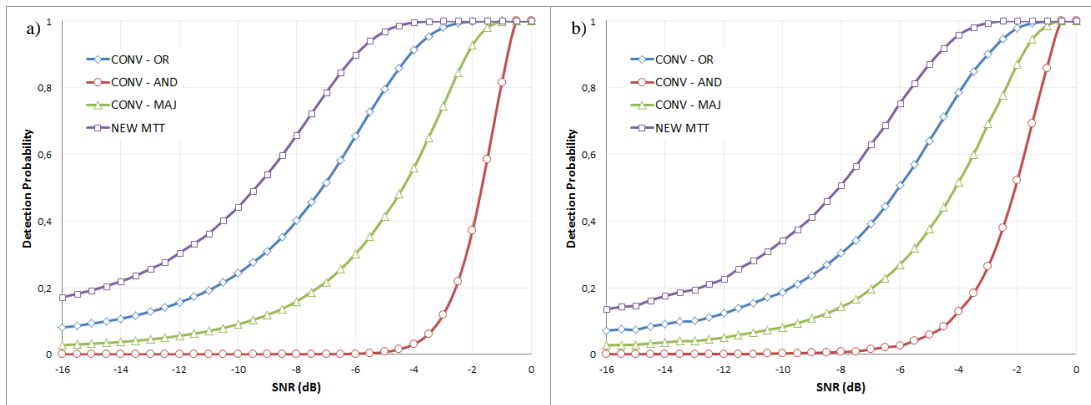


Figure 29. P_D of all the considered methods for five correlated observations and: a) $\rho = 0.1$; b) $\rho = 0.5$.

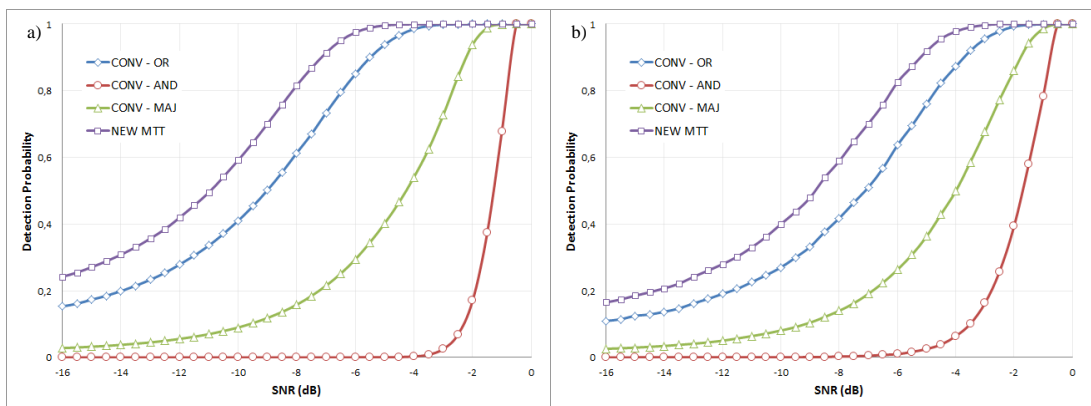


Figure 30. P_D of all the considered methods for ten correlated observations and: a) $\rho = 0.1$; b) $\rho = 0.5$.

In all the considered cases, the MTT always outperforms the conventional fusion rules, showing higher detection probabilities in correspondence of the same SNR. It has to be underlined that, for high SNR values – i.e. when the channel conditions improve to a point where the single user declares a correct decision on its own – the

effects of correlated observations become weaker and weaker, and all the methods provide the same performance. It is also to be noted that, for all the considered methods, as the correlation coefficient increases, it is necessary to increase the SNR of the system in order to reach the same probability of detection. For example, to maintain a $P_D = 0.9$, the MTT must increase the SNR of 2 dB (from $\rho = 0.1$ to $\rho = 0.5$), as must do all the other fusion rules.

Furthermore, we have analysed how the performance improvement obtained with the MTT procedure results in a detection gain, varying the correlation coefficient. In particular, we have defined as detection gain (D_G) the ratio between the P_D of the MTT and the P_D of the conventional approach.

Figure 31 shows the D_G in the cases of $M = 5, 10$ (Figure 31.a, and Figure 31.b, respectively). Once again, it is easy to see that the MTT method performs better – reaching detections of about 20% – if compared with the conventional OR fusion strategy, which provides better results than the AND and MAJ rules.

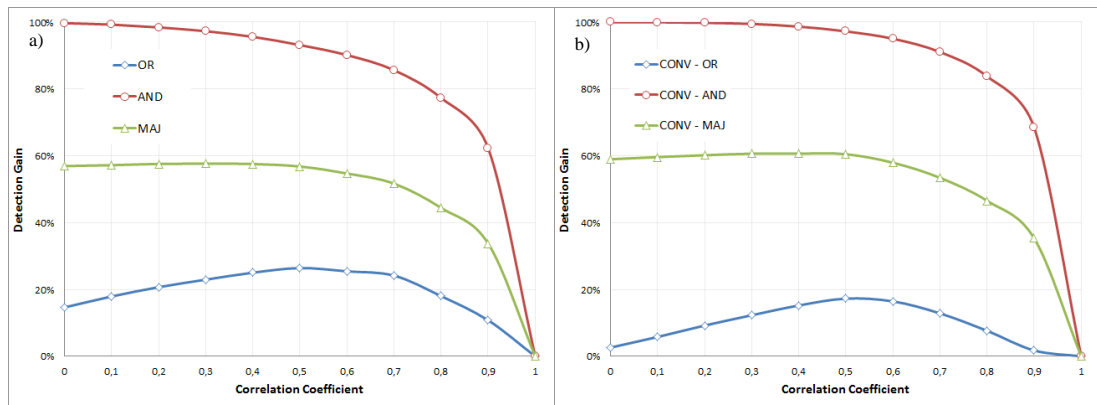


Figure 31. Detection Gain of all the considered methods versus the correlation coefficient for: a) $M = 5$ and; b) $M = 10$ correlated users.

Finally, we have evaluated the mean detection time (MDT) required by the two techniques to detect a primary signal. The MDT is defined as the time (i.e. the number of samples) needed on average before a correct detection is declared. The MDT can be expressed as follows [185]:

$$\text{MDT} = (N + P_{FA} \cdot T_P) \cdot \frac{2 - P_D}{P_D} \quad (18)$$

where N is the number of sensing samples and the penalty time T_p is the time needed to recover from a wrong decision (i.e. declaring the emptiness of a band where a primary user is actually transmitting). In addition, it is possible to define the MDT-gain as the ratio between the MDT of the conventional and of the new methods, respectively.

The MDT-gain between the conventional OR strategy versus the new method is shown in Figure 32, for several values of the correlation coefficient ($\rho = 0.2, 0.4, 0.6$) and for $M = 3, 5, 10$. In the figure, it is now visible how the increase in the P_D due to the new method results in a MDT gain. In fact, the curve of the MDT gain is always greater than 1, proving that the new method is always faster than the conventional OR fusion rule in detecting the primary user signal and rejecting occupied bands.

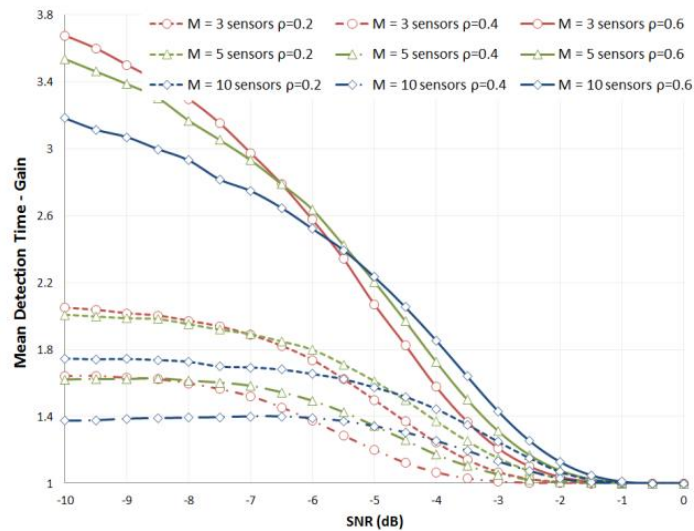


Figure 32. MDT Gain of the new test versus the conventional OR method, for several correlation coefficients, and for a number of sensors $M = 3, 5, 10$.

To conclude, it has to be noted that only negligible increasing of the system computational complexity is introduced by the new test. In fact, the threshold setting stage is usually performed offline since it is a time-consuming task; the thresholds are usually pre-computed and stored on lookup tables for several SNR values. The conventional procedure compares each testing variable to one threshold, while the new method tests each variable with two thresholds. Therefore, the new approach requires only one more comparison operated on the same testing variables, and followed by a Boolean operation.

4.4. Extended MTT in presence of Noise Uncertainty

Even though ED-based solutions, such as the MTT, offer a fairly simple and practical implementation and an acceptable performance, it is highly unlikely to gather an exact knowledge of the noise variance in a real communication scenario. As a matter of fact, noise is a combination of different elements, such as aliasing and thermal noise, which, influencing the estimation of its energy, lead to noise uncertainty [187]-[188]. The assumption is that the noise variance is expected to vary in the range:

$$[(1/\varepsilon) \cdot \sigma_w^2, \varepsilon \cdot \sigma_w^2] \quad (19)$$

where ε (with $\varepsilon > 1$) is a parameter related to the size of the uncertainty, while σ_w^2 is the noise variance. The noise uncertainty is usually expressed in dB units as:

$$x = 10 \log \varepsilon \quad (20)$$

Such uncertainty, however small, can heavily affect the detection performance due to the conventional ED's sensitivity to the knowledge of the noise variance, ultimately resulting in a lack of robustness of the detector [189]-[190]. Eigenvalue-based spectrum sensing techniques have been proposed to overcome the challenges of noise uncertainty [79], [81], and [191]–[192]. The main drawback of these methods is their high computational complexity, due to calculation of the covariance matrix of the received signal and its corresponding eigenvalues.

One of the fundamental blocks of the MTT's rationale is the computing of the thresholds, which allows to optimize the method's performance in presence of correlated observations. Despite the MTT's effectiveness, its major drawback is that its performance drastically decreases in presence of noise uncertainty, since the function used to compute the thresholds is not optimized to overcome such issue.

The effects of noise uncertainty and correlated users have been considered in addition to the conventional MTT. In particular, the thresholds computed in presence of noise uncertainty do not allow to reach the desired P_{FA} under the hypothesis H_0 and do not meet the CFAR criterion. For this reason, it is necessary to improve the MTT by optimizing the function used to compute the thresholds so that it takes into account

not only the correlated observations but also the information related to the variance of the noise uncertainty.

To properly set the two thresholds used in the extended version of the MTT, namely extended MTT (EMTT), we design a new recursive function based on the following parameters:

1. the correlation coefficient, ρ , among SUs' observations;
2. the desired probability of false alarm, P_{FA} ;
3. the mean (m_w) and variance (σ_w^2) in presence of different levels of noise uncertainty;
4. the number of trials required to compute the thresholds.

The thresholds are recursively computed, combining the extended modified generalized-Q (EMGQ) functions proposed in [185] with experimental values, which allow to set the thresholds at the desired P_{FA} . In addition, such function enables the EMTT to automatically find more than one pair of thresholds (γ_L, γ_U) that meet the CFAR criterion, and to choose the pair that maximizes the detection probability at the desired P_{FA} .

The value of the pair of thresholds, $[\gamma_L(j), \gamma_U(j)]$, at the j -th recursive step, is then modified by exploiting the experimental values as follows:

$$[\gamma_L(j), \gamma_U(j)] = [\gamma_L(j-1), \gamma_U(j-1)] - (\Delta_L, \Delta_U) \quad (21)$$

where (Δ_L, Δ_U) is the pair of experimental values used to modify the computed thresholds to obtain the final ones, while $[\gamma_L(j-1), \gamma_U(j-1)]$ are the threshold evaluated at the previous $(j-1)$ recursive step. Finally, the value of P_{FA} is computed by means of these new thresholds, and compared with the desired one given as input parameter. If the computed P_{FA} is equal to the desired one, then the pair of thresholds is employed in the test. Otherwise, the procedure continues its iteration, until the constraint related to the P_{FA} is satisfied. According to the rationale of the MTT, the threshold computing process can be defined as the following constrained-optimization problem: identify the unique pair (γ_L, γ_U) that maximizes the detection probability, with the constraint that P_{FA} must be equal to the desired P_{FA} .

Thanks to the proposed improvement process employed in the new recursive function and the improvement in the threshold-computing task, the EMTT is able to find the most suitable pair of thresholds at the desired P_{FA} even in presence of a given ρ coefficient and of different levels of noise uncertainty.

Since we are proposing enhancements to conventional ED using the EMTT approach, we deem it natural to compare the results against both basic ED and advanced eigenvalue based methods, demonstrating certain benefits. The main drawback of conventional ED is the performance degradation due to the noise uncertainty effects. Otherwise, ED offers a good performance versus complexity trade-off, which is also well recognized in the literature. While ED-based spectrum sensing techniques are quite simple and of low complexity, they are rather sensitive to noise uncertainty and the detection performance of these methods is significantly degraded under even small noise uncertainties, which are given in detail in the following section. On the contrary, advanced eigenvalue based sensing techniques are robust to noise uncertainty where the detection performance can still be adequate. However, eigenvalue-based approaches include huge computational complexity due to the calculation of the covariance matrix and its eigenvalues [81].

4.5. Experimental Results of the EMTT

This section reports some experimental results validating the better performance of the proposed EMTT when compared to the conventional CSS based on the hard combining voting rules in presence of correlated observations under noise uncertainty. In particular, we consider a centralized CR network of M cognitive users where the correlation among the M observations is represented by the correlation coefficient ρ . In the proposed tests, the number of sensors is $M = 8$ while the number of sensing symbols N of the constant modulus BPSK-modulated signal is set to 10000. The target P_{FA} for the FC is considered as 10^{-1} , and the ρ coefficient is in the range of [0.1, 0.6]. In the proposed scenario, an AWGN channel affected by different noise uncertainty values – which are assumed to be equal for all the SUs – is considered. Finally, 10^4 Monte Carlo simulations to numerically compute the system's performance are used for each test.

The first round of tests pertains the analysis of the performance of the EMTT in presence of correlated observations with different values of the correlation coefficient and under different levels of noise uncertainty. Figure 33 shows a comparison among different ρ coefficients at a high level of noise uncertainty, i.e. 1 dB. As expected, despite the high level of noise uncertainty, as the value of the ρ coefficient increases, the detection probability of the EMTT barely decreases. In addition, even though such level of noise uncertainty should heavily deteriorate the performance, the EMTT reaches a detection probability higher than 90% even in presence of very low SNR values (i.e. $SNR = -19 \text{ dB}$). Similar performances are reached for low and medium levels of noise uncertainty values as well but, for the sake of compactness, they are not reported here.

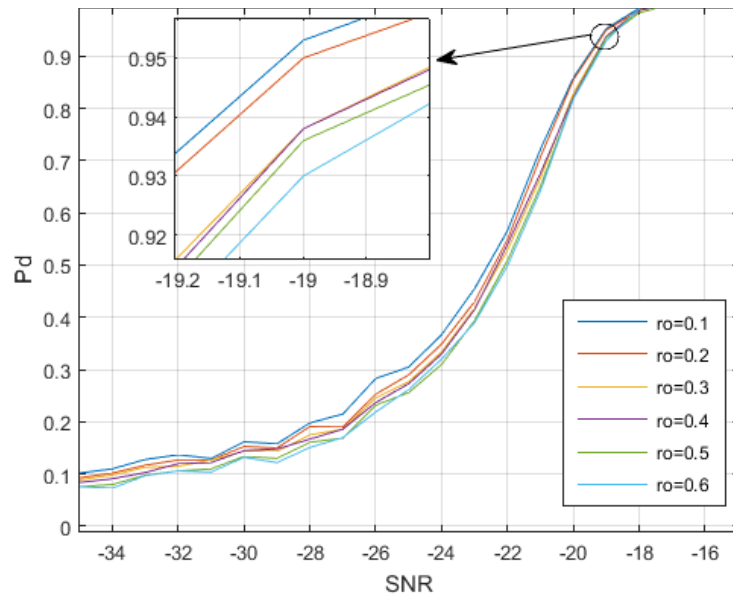


Figure 33. Performance comparison of the EMTT among different values of ρ coefficient (i.e. $\rho \in [0.1 \ 0.6]$) at 1 dB noise uncertainty.

Successively, we evaluated the performance of the EMTT in presence of different noise uncertainty values – i.e. 0 dB (no noise uncertainty), 0.1 dB, 0.5 dB, and 1 dB noise uncertainties – at a given value of the ρ coefficient, i.e. $\rho = 0.3$, which is considered as medium correlation. As shown in Figure 34, as the level of noise uncertainty increases, the detection probability of the EMTT barely decreases, stressing the robustness of the EMTT in presence of noise uncertainty.

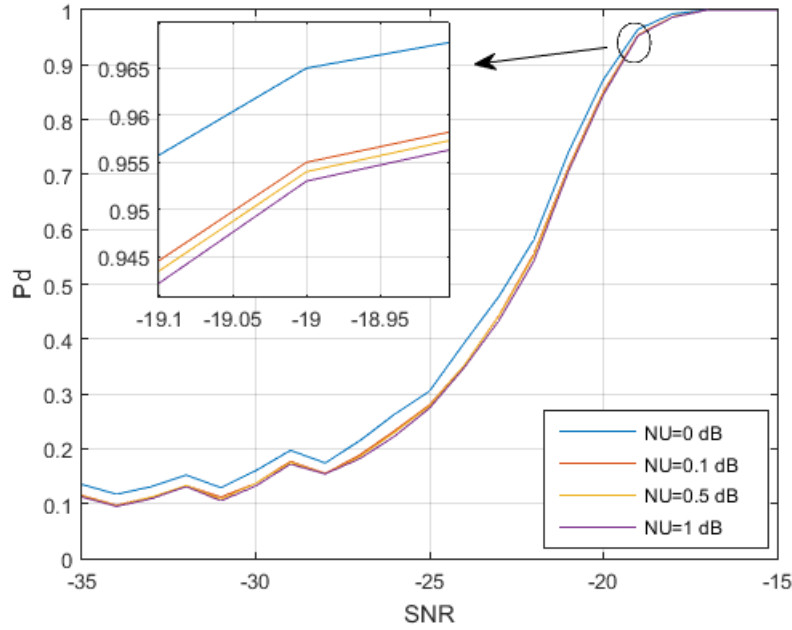


Figure 34. Performance comparison of the EMTT among different values of noise uncertainty (i.e. 0 dB, 0.1 dB, 0.5 dB, and 1 dB) at $\rho = 0.3$.

Finally, the proposed EMTT method is compared with the HCVR-based CSS methods and the MTT. Figure 35 shows the detection probabilities of both the EMTT and the conventional CSS methods versus the SNRs of interest for $\rho = 0.3$ and noise uncertainty equal to 0.1 (Figure 35.a) and 1 dB (Figure 35.b), respectively. It is possible to see how the EMTT clearly outperforms the conventional solutions and, in particular, the MTT in presence of noise uncertainty. As expected, the EMTT confirms the results previously shown (i.e. high detection probability, higher than 90%), reaching the desired P_{FA} even under low values of SNR.

The proposed results stress the robustness of the EMTT under noise uncertainty in presence of correlated observations, outperforming the conventional CSS approaches and the MTT, which performs poorly even in presence of low levels of noise uncertainty.

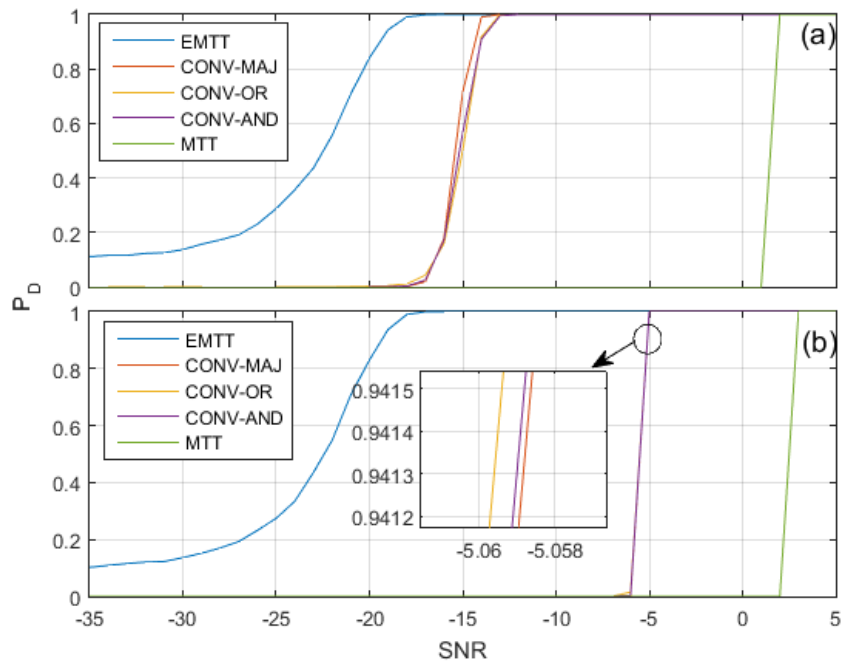


Figure 35. P_D of the EMTT and conventional methods at $\rho = 0.3$ and in presence of noise uncertainty: a) equal to 0.1 dB; b) equal to 1 dB.

5 Fine grained analysis of packets loss in CRSN

5.1. CRSN and security threats

Wireless Sensor Networks (WSNs) are employed in several critical fields, including power grids, agriculture, cyber-physical infrastructures, healthcare monitoring, and homeland protection [193]-[194]. Conventional WSNs, however, are based on fixed spectrum allocation and characterized by the communication and processing resource's constraints of low-end sensor nodes.

The synergy between WSN and other technologies (e.g. RFID, robotics, vehicular networks, cloud computing, CRT) has recently become a popular research topic, as ways to improve it and exploit it in other fields are the subject of numerous studies [195]. In particular, several critical activities are being monitored and observed using bandwidth-hungry multimedia WSNs. Exploiting CRT's features and behaviours allows WSNs to circumvent bandwidth limitations, enabling the detection and utilization of the available spectrum holes, thus providing a greater bandwidth. Moreover, through a network based on cognitive sensors, the WSN can benefit from several advantages such as [196]-[197]: (i) higher transmission range; (ii) fewer sensor nodes required to cover a specific area; (iii) better use of the spectrum; (iv) lower energy consumption; (v) better communication quality; (vi) fewer delays; (vii) noise mitigation; (viii) improved data reliability.

It is possible to design a new category of sensors networks, namely CR-WSN or CR sensor network (CRSN), which can be defined as [198]:

“a distributed network of wireless cognitive radio sensor nodes, which sense event signals and collaboratively communicate their readings dynamically over available spectrum bands in a multi-hop manner to ultimately satisfy the application-specific requirements”.

CRSN can be considered as a viable candidate for the next generation of WSN systems, especially in the fields of industry and healthcare. CRNs have already been proposed for smart grid applications and their performance had been evaluated in

different application domains [197]-[198], while the synergy between CR and healthcare WSN for emergency reporting is provided in [199].

Ensuring the security of this kind of wireless networks is of paramount importance [200]-[201]. In particular, CRSNs deployments cannot afford to lose service availability, while at the same time they must ensure reliable delivery of trustworthy data. However, the constrained and insecure nature of sensors (both cognitive and conventional), together with the fully-distributed design of applications, makes satisfying such requirements very challenging. As mentioned in the third chapter, attackers can exploit vulnerable nodes to disrupt network operations by altering data and hindering correct communication and delivery [202]-[204] in order to gain access to sensitive information and to spectrum opportunities. To detect such attacks at the time they are launched, sensor network applications are often deployed with advanced Intrusion Detection Systems (IDSes).

A particularly relevant class of attacks for both CRSNs and WSNs is that of packet losses, in which a malicious party hinders the correct delivery of one or more data packets to the intended recipient. This class of attacks is critical to these sensors networks as it may result in crucial information being lost. Packet drops may occur because of actions perpetrated by a misbehaving or compromised sensor or because of attacks on the wireless links [205]. Both types of attack can ultimately result in partial or total packet loss. Examples of node-related attacks are selective forwarding and blackhole attacks, while an example of a link-related attack is the introduction of interference (i.e. both intentional, such as jamming, and unintentional disruption of signal communication between sensor nodes).

While the two classes of packet loss attacks share the same symptoms, their root causes are significantly different. Correctly detecting the root causes for packet losses – whether link or node-related – is essential to the deployment of effective countermeasures, both manual or automated [206]. Current IDSes, however, are typically only able to detect the adverse event, but not to determine the actual causes of the losses, whether node- or link-related [207]-[210]. Thus, techniques to perform an accurate diagnosis of the underlying causes of packet losses in sensor networks are critical.

Most of the works focusing on the analysis of packet losses are based on conventional WSNs (see section 5.1.2), while there seems to be a lack of attention on this subject in research studies based on CRSNs, which tackle mainly energy efficient communication.

Midi and Bertino in [143] propose one of the most prominent works on the identification of the root causes of packet losses in a sensor network. In particular, the authors define an approach to fine-grained analysis (FGA) of packet losses, and implement and evaluate a tool based on it, using the typical packet metrics to profile all the network links. Upon the occurrence of a packet loss event, such profiles are used to carry out a thorough analysis and determine the underlying cause of the packet loss. Every parameter of the tool (e.g. detection thresholds) can be customized by the network's administrator based on the requirements of the network of interest. Setting incorrect parameters can obviously affect the accuracy of the analysis and the correct identification of the packet loss' causes in presence of subtle attacks. To address this issue, an automated guide for the proper setting of the system's parameters is of great importance. In fact, empirically-determined values, such as those proposed in [143], might not always prove optimal, causing a higher number of false alarms and thus reducing the accuracy of the tool. Moreover, the above-mentioned approach uses a single threshold for the whole network but, while such decision is aimed at reducing the workload of the network's administrator, it can also lead to a further increase in the number of false alarms. In fact, in a large-scale deployment, different parts of the network might experience different normality conditions, and a single, predefined threshold might be suitable for a network portion but inadequate for another. In addition, the previous approach does not allow any control on the false alarm rate for each link, meaning that a desired maximum rate of false detections cannot be required a priori.

The proposed work aims at addressing the shortcomings of [143] by designing an approach that builds and uses a statistical model for the determination of the optimal system thresholds. By collecting and analysing samples from the initial deployment of the network system, the proposed approach builds an accurate statistical model of each link, exploiting the variances of RSSI and LQI. Based on such model, the approach selects the optimal threshold for each link in the deployed network. One of the

advantages of the proposed model is, indeed, the possibility to support the setting of a different threshold for each link. Such task is manually unfeasible for a network administrator, but it can be effectively automated by the proposed model. Moreover, since each threshold is tuned according to an optimum criterion, it is always possible to choose a desired false alarm rate on a per-link basis and, if needed, exclude from the network all those links that will not be able to reach a satisfactory detection. Finally, the new statistically-enhanced FGA approach matches the typical behaviours and approaches of the CRT to perfection and it can be easily applied to a real CRSN, as shown in the experimental results.

5.2. Related works on Packet Losses Investigation

The use of forensic analysis for investigating packet losses in conventional WSNs has been addressed in few past research efforts. Ning *et al.* [211] propose a forensic technique that uses several network parameters (such as bitrate, packet size and node density) to determine the cause of forwarding misbehaviours. Yang *et al.* in [212] propose a more collaborative approach that leverages all nodes to monitor their neighbours and to ensure that data packets are forwarded correctly. These two approaches focus more on distinguishing natural and malicious packet losses, while the proposed approach addresses the identification of the root cause of packet drops relying on fewer parameters.

While the detection of packet dropping attacks has been the subject of several IDS-related works, the identification of the root cause of such adverse events by means of common network parameters has been investigated significantly less. In [213], the authors use an expected transmission time metric as weight for each link. In a similar fashion, an expected transmission count metric developed by De Couto *et al.* aims at estimating the packet delivery ratio of the various links [214]. Both metrics aim at assessing the packet loss rate, but neither of them investigates the cause of packet losses. Qiu *et al.* use trace-driven simulations to troubleshoot performance issues caused by link congestion, packet dropping, MAC misbehaviour, and external noise [215]. Ramach *et al.*, instead, propose a generic architecture to monitor numerous parameters of network devices and protocols [216]. While the goal of these approaches

is the diagnosis of performance problems, the proposed approach aims at determining the most likely cause of packet losses.

Several works use the RSSI and LQI metrics for purposes different from ours, mostly related to the localization of devices and sensor nodes. RSSI readings are used by Zâruba *et al.* for indoor positioning of wireless nodes using only a single access point [217]. However, Parameswaran *et al.* [218] show that, while the sole RSSI is sufficient for localization algorithms, the accuracy of inter-node distance measurements is often affected by factors such as interference. This further corroborates our findings on the effectiveness of those resident packet parameters in detecting interference. Srinivasan and Levis [219] prove that combining RSSI and LQI is effective for localization even in presence of obstacles or interference.

Even though these approaches can be exploited in both WSNs and CRSNs, none of them makes use of extensive statistical analyses of the metrics to reveal the presence of interference, as done in the proposed approach.

5.3. System Model

The radio chips based on the IEEE 802.15.4 standard [220] natively offer two main measurements for the link quality and estimation, namely RSSI and LQI.

A commonly used large scale model to predict attenuation over distances is the log-distance path loss model with log-normal shadowing (also known as log-normal path loss model [221]). According to this model, the RSSI represents an estimate of the received signal power for a packet, and it is measured in dBm. The RSSI value at the distance d from the base station is described by the following equation [222]:

$$RSSI = P_T - P_L(d_0) - 10\eta \log_{10} \frac{d}{d_0} + X_\sigma \quad (22)$$

where P_T is the transmitter power, $P_L(d_0)$ is the path loss at a specific distance d_0 , and η is the path loss exponent. The shadowing factor X_σ is a Gaussian random variable (with values in dB) and with standard deviation σ . The values of η and σ can be set depending on the propagation environment.

The LQI reflects the chip error rate of the received signal and measures the signal reception quality. As defined in [220], the LQI measurement is performed for each received packet and the obtained results are reported to the MAC sublayer of the radio chip. In addition, its value should be limited to the range [0, 255] with at least 8 unique values. Differently from the RSSI, literature does not provide an exact equation to compute the LQI, allowing manufacturers and vendors to define their own estimation methods.

In this work, the TelosB motes (TelosB) is the target hardware platform. Such platform uses a *CC2420* radio chip, but the proposed approach can be applied to any of the newer radios based on the IEEE 802.15.4 standard.

As indicated in [223], the *CC2420* radio chip calculates the RSSI value over an 8-symbol period, long on average $128 \mu s$. The dynamic range for the RSSI is between -50 and -100, with higher values (less negative) representing a stronger signal. It is worth noting that, on the *CC2420* chip, the manufacturer specifies that the read RSSI value is stored in the *RSSI_VAL* register of the chip, with a fixed offset of -45 dBm , as defined in (23).

$$RSSI_{power} = RSSI_{VAL} + RSSI_{OFFSET} \quad (23)$$

According to the specifications of the IEEE 802.11.4 standard, the RSSI value can be effectively used for both detecting noise on a channel, and estimating the quality of an incoming packet upon its reception. This property is leveraged by many protocols for optimal routing decisions [224], and validated by several research efforts on the accuracy of the RSSI measurements themselves [219], [225].

The specifications of the *CC2420* radio chip state that the measured LQI is actually the average correlation of each symbol, obtained by comparing the symbol that is supposed to be received with the symbol actually received (signal plus noise), based on the 8 bits after the start frame delimiter (SFD). The correlation values range between 110 and 50, corresponding respectively to maximum and minimum quality frames. Once the correlation value is computed, it must be converted to the range [0-255], [223].

Finally, another important metric for link quality estimation is the PRR. It is not a value natively computed by the radio chip, but instead an aggregated metric for each individual link, computed as the ratio between the number of packets successfully received and the number of packets sent. Higher values of PRR indicate a better link quality and therefore a healthier communication medium.

$$PRR = \frac{\# \text{ successfully received packets}}{\# \text{ sent packets}} \quad (24)$$

5.3.1. Conventional FGA method

In [143], the FGA approach is composed of two main phases: profiling and investigation. The profiling phase aims at understanding the quality of each link in the WSN under normal operating conditions, namely when there is no undergoing attack. Upon the initial deployment of the network and its setup, the FGA system collects resident metrics and aggregate statistics about each link. To do so, each node in the WSN broadcasts a configurable number of *dummy* packets. Upon receiving the dummy packets of its direct neighbours, each node records the RSSI and LQI values. At the end of this initial message exchange, each node averages the values for each incoming link, and computes the related PRR. The initial profiling phase, therefore, will terminate with every node having a profile in the form $P = \langle AVG_{RSSI}, AVG_{LQI}, PRR \rangle$ for each individual link.

When the IDS of a node detects that a packet drop attack has been carried out by a supposedly malicious node, say n_{bad} , the investigation phase of the FGA is triggered to determine whether n_{bad} is indeed a compromised node dropping packets, or if an interference is actually the cause for such loss. All the investigating nodes – that is, the direct neighbours of n_{bad} – will stealthily start to collect metrics from the overheard packets coming from n_{bad} . When a certain number of samples has been collected, the investigating nodes aggregate such data to obtain an *investigation profile* $P' = \langle AVG'_{RSSI}, AVG'_{LQI}, PRR' \rangle$. The assumption at the base of the diagnosis is that a node-related attack will not significantly alter the quality metrics of the link, whereas a link-related attack, such as the introduction of interference, will result in noticeable changes in these quality metrics. The FGA tool therefore compares the initial profile P with the investigation profile P' . If the difference in their components exceeds a predefined

threshold, it infers that the attack is link-related, otherwise it declares the attack as node-related.

5.4. A Statistically-Enhanced Profiling Technique

This section considers the motivations behind the new profiling approach, providing a formal definition of the rationale of the new procedure.

5.4.1. Motivations

The profiling technique proposed by Midi *et al.* [143] has proven to be very effective in discriminating between a network affected by intentional low/high interference (i.e. jamming attack) or by a packet drop attack (either selective forwarding or blackhole attack). However, an analysis of the technique has underlined two major drawbacks:

- the threshold is just one for the entire network and it is not computed observing the statistical trend of the RSSI and LQI for each link;
- the threshold is empirically evaluated (i.e. not tuned according to an optimum criterion).

To address these drawbacks, a new profiling technique is designed, defining an optimal threshold for each link in the network by exploiting the variances of the RSSI and LQI parameters. The problem is formulated as a conventional binary hypothesis test, where the two testing hypotheses H_0 and H_1 correspond to the absence or presence of the attack of interest, respectively. We define as P_D the probability of our system to correctly identify the presence of the attack when it is actually performed. Conversely, we define as probability of false alarm P_{FA} the probability of our technique to declare the presence of the attack when it is actually not present.

To limit the computational cost of the decision device, we choose one-dimensional testing variables that are compared to a pre-selected threshold in order to efficiently perform the test. The optimal threshold for each link is tuned according to an optimality criterion [226]. Here, the CFAR criterion is adopted as the optimal criterion to discriminate between the presence and absence of a given subject (e.g. an unknown user in hidden communications), against a background of noise and interference. The

CFAR criterion is executed, for each link, according to the following two steps. Firstly, a threshold is determined that limits the false alarm probability at a given reduced value (i.e. the *size* of the test) under the null hypothesis H_0 . Secondly, the P_D (i.e. the *power* of the test) is evaluated under the alternate hypothesis H_1 for the previously determined threshold .

The main idea behind the proposed procedure is that the variance of the received signal (and hence the variance of the RSSI and LQI of the received packets) is lower when the link is affected by a packet drop attack (H_0 hypothesis), and higher in the alternate H_1 hypothesis (i.e. when the link is affected by low/high interference). As noted by [143], packet drop attacks do not change the statistics of the received signal in terms of RSSI and LQI. In fact, the aim of this kind of DoS attack is to discard the incoming packet and damage the communication among links. Conversely, the same consideration is not valid any longer in the presence of links affected by low/high interference. Therefore, we can select the variances of the received RSSI and LQI as the one-dimensional testing variables to compare with the optimal thresholds. Hence, our variance-based test can be effective in discriminating between cases of a packet drop attack by nodes and cases of low/high interference. In addition, since these considerations apply to each link in the network, we can first identify the most appropriate threshold, and then evaluate the detection performance for each link.

5.4.2. Rationale

The rationale behind our method is as follows. The Intrusion Detection System (IDS) of a sensor has declared the presence of an anomaly (i.e. some kind of attack) in the network. This declaration is based on the observation of the PRR values, as done in [143], and it allows discriminating between the following two hypotheses:

$$\begin{aligned} H_0: & \text{ packet drop attack} \\ H_1: & \text{ jammin attack} \end{aligned} \quad (25)$$

The decision about the presence or absence of a jamming attack in a certain link of the WSN can be obtained by comparing the decision metric to the pre-selected threshold. In our case of interest, the testing variable is the variance of the RSSI and LQI of the received packets on that link. Let $u(n)$, $i(n)$ and $x(n)$ be the sequences (of

N samples) representing, respectively, the (useful) transmitted signal, the interference affecting the communication in the network, and the received signal. Since node-related packet-dropping attacks do not change the signal's statistics, the problem can be formulated as follows:

$$x(n) = \begin{cases} u(n) & H_0 \\ u(n) + i(n) & H_1 \end{cases} \quad (26)$$

Then, assuming that the signal and the interference are zero-mean, mutually independent random processes, the two hypotheses result in:

$$\sigma_x^2 = \begin{cases} \sigma_u^2 & H_0 \\ \sigma_u^2 + \sigma_i^2 & H_1 \end{cases} \quad (27)$$

where σ_u^2 and σ_i^2 are the variances of the useful signal and the interference respectively, while σ_x^2 is the variance of the received signal. The variance σ_x^2 can be the variance of either the received RSSI values or of the LQI values. For the sake of compactness, in what follows we refer only to the test in terms of RSSI variance. The same considerations apply to the LQI case. The estimation of the variance of the received RSSI values is now used as the testing variable to discriminating between the presence of a packet drop or an interference attack. The new testing variable is estimated according to the following expression:

$$\hat{Z} = \frac{1}{N} \sum_{n=1}^N \{x(n) - E[x]\}^2 \quad (28)$$

where $E[\cdot]$ stands for the expectation operator. Then, considering a threshold η , the test is finally formulated as follows:

$$\begin{aligned} H_0: \hat{Z} < \eta & \text{ packet drop attack} \\ H_1: \hat{Z} \geq \eta & \text{ jammin attack} \end{aligned} \quad (29)$$

This means that, if the testing variable is greater than the threshold value (η), then the algorithm decides for the hypothesis H_1 (i.e. jamming attack), otherwise the choice is for the hypothesis H_0 (i.e. packet drop attack). Finally, it has to be noted that the testing variable in (28) is asymptotically ($N \rightarrow \infty$) Gaussian as a direct consequence

of the central limit theorem. Hence, the test threshold can be asymptotically tuned from a straightforward evaluation of the Gaussian integral for a fixed probability of false alarm, under (i.e. conditioned to) the null-hypothesis [95]:

$$\eta = E[\hat{Z}]_{H_0} + \left(\sqrt{2 \cdot \text{var}[\hat{Z}]_{H_0}} \right) \cdot \text{erf}^{-1}(1 - 2P_{FA}) \quad (30)$$

where $E[\hat{Z}]_{H_0}$ and $\text{var}[\hat{Z}]_{H_0}$ denote the expectation and variance of the testing variable, respectively, conditioned to H_0 , while $\text{erf}^{-1}(\cdot)$ is the well-known (inverse of the) complementary error function. The time-consuming threshold setting stage is usually performed off-line (i.e. during the deployment of the network, when no attacks occur). Hence, the thresholds are pre-computed and stored on look-up tables for several SNR and P_{FA} values. Finally, the probability of detection P_D is determined under the H_1 hypothesis as:

$$P_D = \frac{1}{2} + \frac{1}{2} \cdot \text{erf} \left(-\eta + \frac{E[\hat{Z}]_{H_1}}{\sqrt{2 \cdot \text{var}[\hat{Z}]_{H_1}}} \right) \quad (31)$$

5.4.3. Statistical Profiling Comparison Algorithm

Figure 36 shows the new profile comparison algorithm that exploits the previously introduced rationale. The PRR_{curr} is set to the current PRR of the node under investigation by its neighbour and it is compared with a preselected threshold set by the administrator of the network. The PRR allows the method to differentiate the two cases of partial and total packet loss. Unlike the previous version, the new profiling technique requires to re-profile the links of the investigating nodes which are direct neighbours of n_{bad} .

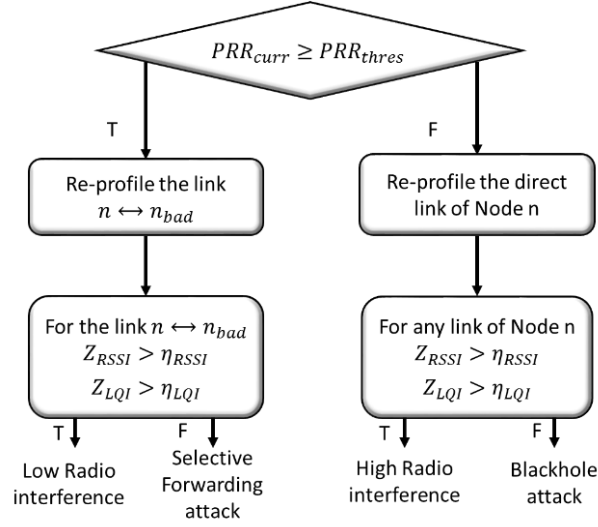


Figure 36. Scheme of the Statistical Profile Comparison Algorithm.

In this step, each node creates a new investigation profile $P' = \langle Z_{RSSI}, Z_{LQI}, PRR \rangle$, where Z_{RSSI} and Z_{LQI} are respectively the testing variable for the test based on RSSI and LQI. Finally, η_{RSSI} and η_{LQI} are the optimal thresholds computed during the deployment of the network, exploiting the CFAR criterion. Finally, when $PRR_{curr} \geq PRR_{thresh}$, the profile comparison algorithm of each neighbor node needs to re-profile the link that connects the node with n_{bad} . If $PRR_{curr} < PRR_{thresh}$, the profile comparison algorithm needs to re-profile all its links and compare the new profile with the pre-selected optimal thresholds.

5.5. Evaluation Results

To validate the theoretical approach and to assess the efficiency of the new profiling technique, several tests have been performed considering a network composed of 16 TelosB sensors placed in a 4x4 grid. These sensors are equipped with the CC2420 radio chip, natively providing the RSSI and LQI measurements for each received packet. In particular, through these experiments, it has been possible to evaluate the impact of the interference generated by a CJ and a Selective Forwarding attack. Unfortunately, it was not possible to compare the new approach with the one proposed by Midi et al. in [143] because their method does not work at the desired P_{FA} making the comparison unreliable and unfair. The following sections provide a brief discussion

about the performance of the proposed statistically-enhanced approach in cases of diverse levels of precision of the samples used for the analysis.

5.5.1. Jamming Attack

Figure 37 shows a snapshot of the network's portion under the attack of a Jammer node (J), highlighting the communication links among the network's sensors. The sensors also communicate with another node that acts as BS and is connected to a laptop. In order to conduct the experiments, a large amount of real data was collected during the deployment of the network – devoid of any interference and working properly (H_0 hypothesis). Then, the variances of the received RSSI and LQI parameters are estimated according to (26) to tune the optimal theoretical threshold using (28).

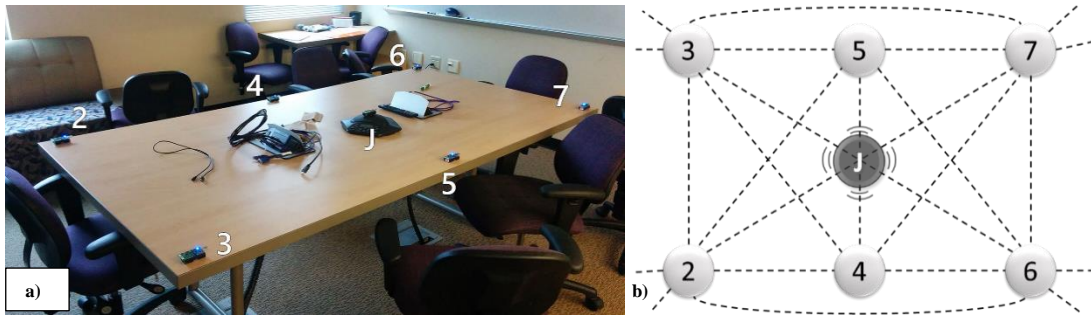


Figure 37. Snapshot of the network portion (a) in presence of an interference attack generated by the Jammer node, J, (b) highlighting the communication link among the network's nodes.

It is important to mention that the number of testing variables, used to estimate the mean and variance in (30), directly impacts on the threshold tuning. A high number of testing variables allows to set a finer threshold corresponding to the P_{FA} targets (complying with the CFAR procedure), while fewer testing variables result in a rougher threshold-setting with an actual P_{FA} that does not comply with the CFAR procedure.

A further important aspect is the number of samples used to compute the test variables, since it directly impacts on the P_D of the test. As show in Figure 38, increasing the number of samples enhances the system's performance, providing a higher accuracy in the estimation of the RSSI (and LQI) variance. Hence, in order to compute the optimal set of thresholds and estimate the testing variables, it is crucial to

find the appropriate trade-off between the number of samples and testing variables that ensures the maximum level of accuracy.

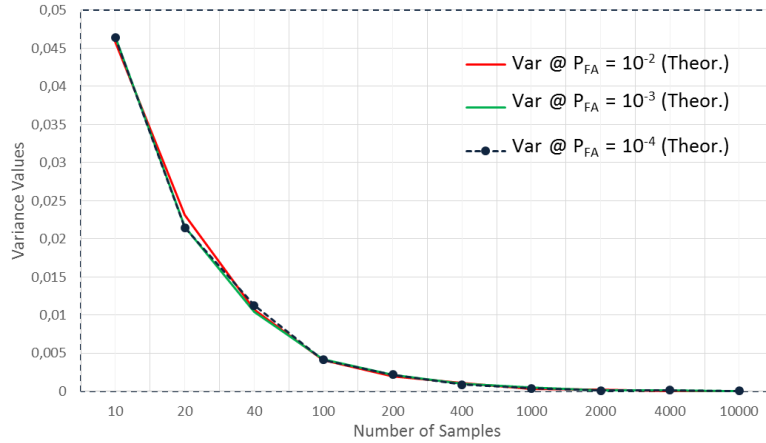


Figure 38. Variances of the testing variable versus the number of samples at different false alarm rates.

To properly compute the thresholds for each network's link at a given P_{FA} , 1000 testing variables have been considered, estimating the variance of the received RSSI/LQI values over $N = 100$ samples, since this value represents a reasonable trade-off between test performance and accuracy. The performance of the proposed test has been evaluated for three different false alarm probabilities (i.e. $P_{FA} = 10^{-2}$, $P_{FA} = 10^{-3}$, $P_{FA} = 10^{-4}$), evaluating P_D both analytically, i.e. using (31), and experimentally. In order to successfully conduct the experiments, a sensor acting as a jammer introduces different levels of interference in the network's communication; such sensor is located at the center of the network, as shown in Figure 42. The interference level varies from low, to medium and high values in order to collect the results at several SNR of practical interest. For the sake of compactness, only the results obtained for the links 2-3, 2-7, and 4-5 are here proposed in order to evaluate how the jammer impacts on the communication links that are close to the source of the interference (i.e. link 4-5) or far from it (link 2-3).

Figures 39-41 show the performance of our profiling technique in terms of the detection probability of an interference attack. In particular, Figures 39.a, 40.a and 41.a illustrate the observations of the RSSI variance, while Figures 39.b, 40.b and 41.b refer to the case of the LQI variance. In all the considered cases, the simulation results

(dotted lines) well match the theoretical ones (solid lines), thus validating the correctness of the mathematical analysis and assumptions.

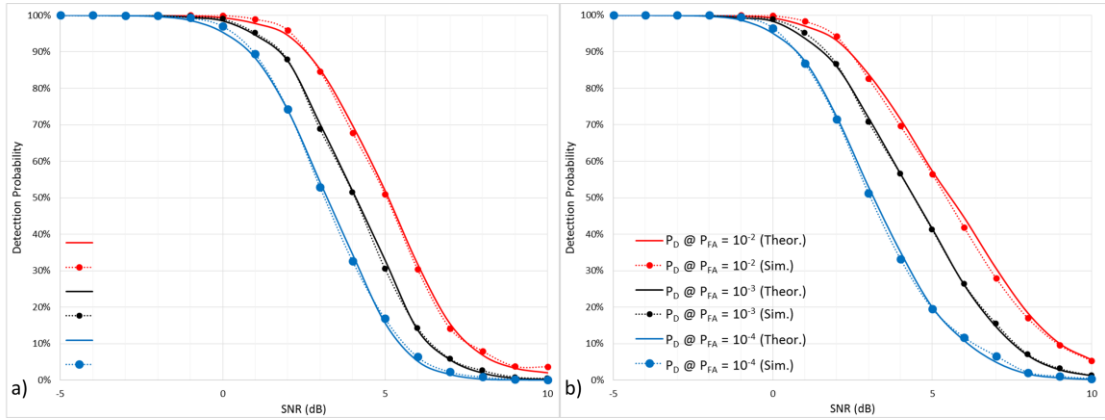


Figure 39. Theoretical (Theor.) and experimental (Sim.) probability of detection of the proposed method for the link 2-3 and several values of SNR and different false alarm probabilities exploiting: a) the RSSI variance; b) the LQI variance. Simulation (dotted lines); theory (solid lines).

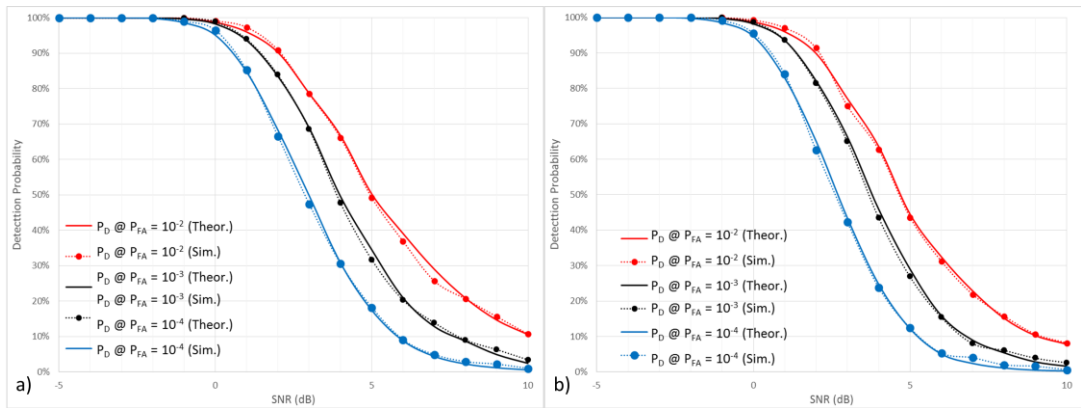


Figure 40. Theoretical (Theor.) and experimental (Sim.) probability of detection of the proposed method for the link 2-7 and several values of SNR and different false alarm probabilities exploiting: a) the RSSI variance; b) the LQI variance. Simulation (dotted lines); theory (solid lines).

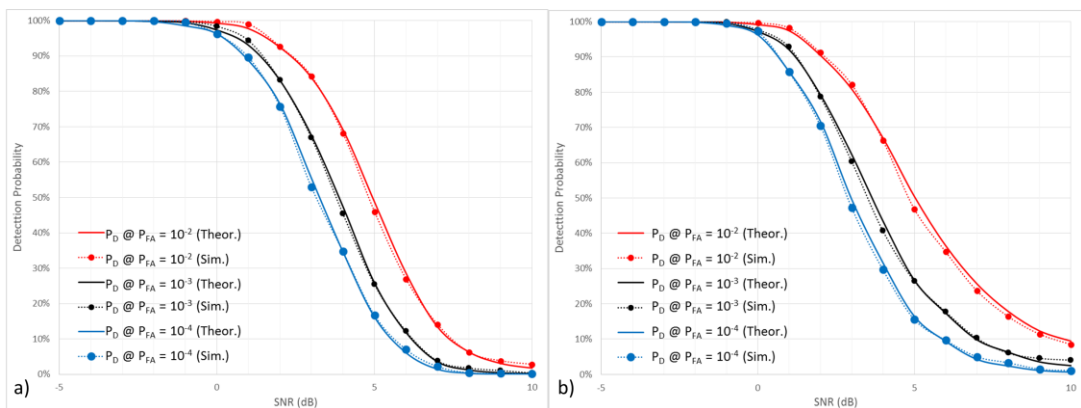


Figure 41. Theoretical (Theor.) and experimental (Sim.) probability of detection of the proposed method for the link 4-5 and several values of SNR and different false alarm probabilities exploiting: a) the RSSI variance; b) the LQI variance. Simulation (dotted lines); theory (solid lines).

As the SNR increases (from -5 dB to 10 dB, i.e. the attacker changes the interference level from high to medium-low), the performance of the proposed FGA technique decreases, as expected. In fact, if the level of the interference caused by the attacker (or jammer) is too low, the statistics of the received signals do not change in time and it becomes impossible for the sensor to discriminate between interference and a selective forwarding attack. However, a true detection (higher than 80%) is obtained in presence of low interference (at about $SNR = [0; 2]$ dB), even at a very low false alarm probability (i.e. $P_{FA} = 10^{-4}$).

To fully assess the performance of the profiling method, an analysis of how the detection and false alarm probabilities relate to each other has been performed. The receiver operating characteristic (ROC) curve illustrates the performance of the binary profiling method as its discrimination threshold varies. The ROC curve is created by plotting the detection probability against the false alarm probability at various threshold settings. Ideally, all the ROC curves must be above the line $P_D = P_{FA}$ (bisector) and concave downward. Paradoxically, if they were not, a randomized test would perform better. The *best* performing detector presents the minimum distance from the ideal point ($P_D = 100\%$ and $P_{FA} = 0\%$) in its ROC curve. An effective operating point is just the point of the curve near such an optimum case. Figure 42 shows the theoretical ROC curves, i.e. P_D vs. P_{FA} , of our profiling technique for several values of the SNR.

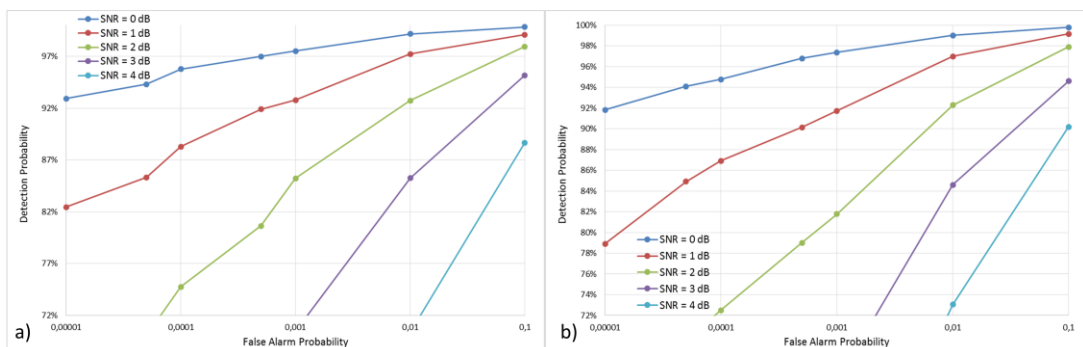


Figure 42. Theoretical ROC curves for several values of SNR exploiting: a) the RSSI variance; b) the LQI variance.

In particular, Figure 42.a refers to the use of the RSSI variance for the test, while Figure 42.b refers to the use of the LQI variance-based test. For the sake of simplicity, only the theoretical curves are reported in Figure 42, since the experimental data once

again perfectly overlap the theoretical ones. It is interesting to note that our method is able to identify a true detection (with a $P_D > 80\%$) even in presence of an interference attack with a SNR of 3 dB, allowing the target P_{FA} to increase from 10^{-4} to 10^{-2} . Hence, the proposed test needs to work with lower SNR values, to maintain the same level of detection, thus decreasing the false alarm rate. As it is possible to see from the previous graphs, larger detection probabilities are achieved also in presence of (low-power) interference attacks, thus demonstrating the effectiveness of the test for fine-grained diagnosis of packet losses in both conventional and cognitive radio wireless sensor networks.

5.5.2. Selective Forwarding

To test the proposed approach against Selective Forwarding attacks, we configured some nodes to act as compromised nodes, dropping the packets they were supposed to forward with a 20% probability. The experiments exploit 1000 testing variables for each link of the network, estimating the variance of the received RSSI/LQI values over $N = 100$ samples. For the sake of simplicity, we report only the theoretical probability of detection of the considered attack for some of the network's links. As shown in the results in Table 14, even in the case of Selective Forwarding attacks the probability of a correct detection provided by our algorithm is very effective, (i.e. always over 99%). These results underline the robustness of our approach in detecting the Selective Forwarding attacks that occur in the network.

Table 14. The Theoretical Probability of Detection of the proposed method in presence of a Selective Forwarding attacks for several relevant links.

| Links | $P_D @ P_{FA} = 10^{-2}$ | $P_D @ P_{FA} = 10^{-3}$ | $P_D @ P_{FA} = 10^{-4}$ |
|-----------|--------------------------|--------------------------|--------------------------|
| Link 2-13 | 99.3518% | 99.8791% | 99.996% |
| Link 6-10 | 99.2% | 99.8622% | 99.9905% |
| Link 3-15 | 98.461% | 99.9112% | 99.9832% |
| Link 4-16 | 99.2353% | 99.5314 % | 99.9808% |

5.5.3. Sample Precision

Statistical analysis approaches work at their best potential, as one would expect, when the precision of the samples used for the analysis is as high as possible.

Unfortunately, the RSSI and LQI values provided by the hardware platform to the software layer are truncated integer values. We evaluate how the accuracy of our statistical approach changes with the different precision of the collected samples. For this, we use MATLAB to generate sequences of samples (based on the mean and the variance of the data collected from our real testbed) with a precision of six decimal places. Then, we take the same data set and truncate all the samples to integer values. We then apply our approach to both the decimal and integer data set of samples to evaluate whether the loss in sample precision has repercussions on the accuracy of the analysis. For the sake of compactness, we report in Figure 43 the results of our simulation based on the two dataset – that is, both truncated and in double precision – of the links 2-7 and 4-5 at different values of P_{FA} , i.e. 10^{-2} and 10^{-3} .

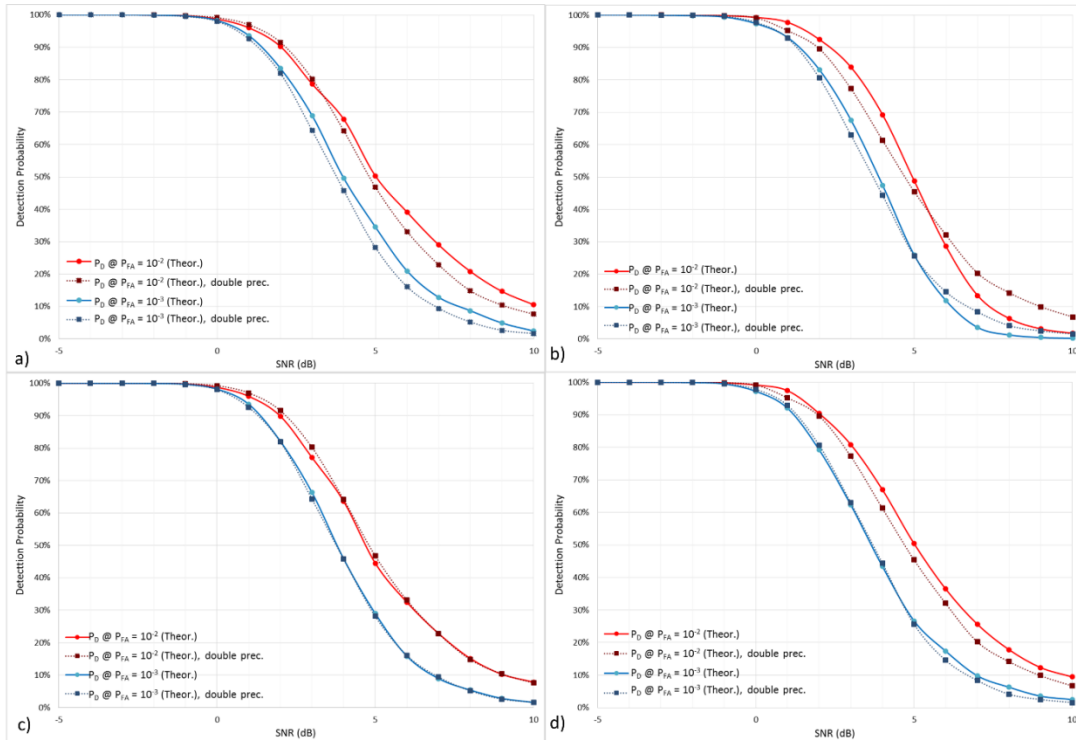


Figure 43. Theoretical (Theor.) probability of detection of the proposed method for the two considered datasets and several values of SNR and different false alarm probabilities exploiting: a) the RSSI variance of the link 2-7; b) the LQI variance of the link 2-7; c) the RSSI variance of the link 4-5; b) the LQI variance of the link 4-5. Theoretical P_D of the double precision dataset (dotted lines); Theoretical P_D of the truncated dataset (solid lines).

In particular, Figure 43.a and 43.c refer to the observations of the RSSI variance, while Figure 43.b and 43.d illustrate the case of the LQI variance for the considered link. A simple analysis of the experimental results shows that the proposed rationale based on variance is robust even for low-precision samples, i.e. the integer values, as

the detection rate is comparable for both the data sets. In particular, the analysis underlines that this similarity is stronger when the two nodes are close (e.g., link 4-5) and decreases of few percentage points when the distance separating the two nodes increases (e.g., link 2-7).

As a future research direction in the area of sensor hardware, we advocate that it could be useful to enable the sensor hardware and software layer to produce RSSI and LQI values with a higher precision, as this could potentially enable other statistical approaches that have better leverage decimal samples.

5.5.4. Consideration about different path-loss models

Propagation models are mainly focused on estimating both the average signal strength drop at different transmitter-receiver separations and signal strength variability in close proximity of specific transmitter-receiver separation [227]. The variation in signal strength is due to changes in the propagation path between transmitter and receiver. Furthermore signal strength can also change due to moving scatterers or shadowing objects which are affecting the propagation environment [228]. In this dissertation, the used model is the large-scale log-distance path loss model with log-normal shadowing. However, in outdoor scenarios other path loss models exist, such as COST, Okumura-Hata or multi-slope models. These models can affect several metrics of a WSN, such as the minimum hop routing to communicate the data to the BS, the PRR, the RSSI and the LQI. In this work, we focused our approach on the evaluation of the RSSI and LQI variances to properly discern a packet drop attack from a jamming attack. If a different kind of path-loss model occurs in the environment, this could probably produce a variation in the performance of the test as follows. If the network is under a known path-loss model during the deployment, then the proposed method will be able to tune the thresholds, by considering the path-loss, and to properly identify the attacks. Otherwise, it is possible that the effect of a different and unknown packet-loss model could heavily affect the system performance in the identification of the attacks, increasing the number of false alarms.

6 Performance Improvement of CSS in Untrusted CRN

Despite the improvement of the sensing performance, the openness of low layers protocol stacks makes CSS vulnerable to Byzantine attacks, which falsify the sensing results to damage the reliability of the CSS. As described in section 3.4, Byzantine attackers aim at generating a DoS of the CRN in order to destroy the legitimate primary and secondary communications and to obtain exclusive access to the spectrum opportunities, increasing the false alarm probability [162]. Attackers can also strike through different strategies, such as the CIPS, to launch a Byzantine attack independently, randomly sending falsified sensing results [163]. As a matter of fact, the presence of even a few Byzantine attackers can severely affect the performance of CSS [229], and a reliable defence mechanism is vital to identify malicious behaviours and perform effective data fusion [230].

To mitigate this kind of attack, several approaches have been proposed in literature with the purpose of detecting the attackers based on their different behaviours, of ignoring their sensing reports, and of discarding them not only from the cooperative sensing but also from the CRN. Zhu *et al.* [231] propose two enhanced schemes of the Weighted Sequential Probability Ratio Test (WSPRT) based on a credit evaluation system to restrict the damages caused by malicious users performing a Byzantine attack. The idea is the adoption of a new weight module and of a new test module requiring fewer samples of the WSPRT, which can be also exploited in distributed CRN [232]. An outlier detection scheme is used in [168] to identify attackers in the sensing process. According to this scheme, a CU is considered as an attacker if it sends results that are numerically distant from other users. This scheme, though, cannot be used to detect attackers when they are a majority in the network. Althunibat *et al.* [233] propose a cluster-based algorithm based on the report concerning the delivery of SUs' transmitted data. The delivery report is exploited by the FC to assess the local decision of each SU and to identify and remove attackers from the cooperation. Other approaches, such as [234] and [235], require that the FC knows one or more trusted nodes (TNs) that can provide reliable decisions about the spectrum occupancy. By exploiting the decisions of these nodes, the FC can then make a reliable decision. In particular, Zeng *et al.* [235] propose a reputation-based CSS with trusted node

assistance (TNA) to assess the reliability of CR users through three different states: reliable, pending and discarded. To move users among the three states, each user is given a reputation value used to weight the local decision. Finally, CR users in the discarded state are excluded from CSS with no chance of further reconsideration.

These methods are reputation-based systems that assign lower reputations to SUs that provide inconsistent sensing results. However, one common drawback of such approaches is that they fail to decouple erroneous sensing reports, due to low sensing capabilities, from false reports due to attacks. The consequence is that benign SUs can be misidentified as attackers, which can cause severe performance degradation.

Here, a new centralized reputation-based CSS is presented. The proposed reputation system is based on two features:

- a new reputation method based on the number of consecutive correct decisions and the number of errors;
- three lists (*White*, *Gray* and *Black*) which state the reliability of CR users in a CRN.

Once a SU is in the *Black* list, it is no longer considered for the CSS, but since its reputation is constantly updated, it can still be promoted to the *Grey* list and, eventually, to the *White* one. Such behaviour allows us to properly identify Byzantine attackers without penalizing legitimate users that misbehave due to channel noise. Even though our method is completely blind (i.e. no need for any a priori information), it can also involve TNs (as in [235]) to enhance the system's performance. The results obtained with this method have also been compared with those presented in [235].

6.1. Conventional method against Byzantine attacks

To overcome the security issues posed by Byzantine attacks and to improve the sensing performance, Zeng *et al.* [235] propose two reputation-based CSS schemes, respectively with and without TNA. In particular, the authors define two major stages: identification and measurement of reliability.

The identification stage allows the FC to assign a reputation value $r_i(k)$ to the i -th SU. Such value represents a measurement of reliability and is updated at each time k

by comparing the local decision of the i -th SU to the global decision made by the FC. If the decision $d_i(k)$ is consistent with the global decision, then the reputation value is increased by one, otherwise it is decreased.

In the measurement combining stage, the FC defines the set of reliable users considered for the cooperative sensing, by comparing their reputation values with a pre-determined threshold. Once the set of reliable users is defined, the FC combines the reliable decisions exploiting the weighted function proposed in [236]:

$$w_j = \frac{w'_j(k)}{\sum_j w'_j(k)} \quad (32)$$

where

$$w'_j = \frac{r_j(k-1)}{\max(r_j(k-1))} \quad (33)$$

The main differences between the two reputation-based cooperative schemes proposed in [235] are the number of stages necessary to classify the reliability of SUs and the inclusion of the TNs.

In the blind approach (i.e. without TNA), the FC can classify SUs according to two states:

- *reliable state*. The SUs in this state show a reputation value $r_i(k)$ greater than or equal to a pre-selected threshold γ and the decision of the i -th SU is exploited to make the global decision;
- *discarded state*. If the reputation value, $r_i(k)$, of the i -th SU is lower than τ , the user is excluded from the cooperation since it is considered as a misbehaved user. In addition, the reputation of the discarded users is no longer updated.

At the time $k = 0$, all the cognitive users in the cooperative scenario are considered reliable and their reputation is set to

$$r_i(0) = \tau + \Delta \quad (34)$$

where the parameter Δ takes into account the uncertainty of the sensing environment.

In the TNA scheme (i.e. not blind), an additional state, namely the *pending state*, is provided to the FC. As seen for the discarded state, the SUs in pending state do not participate to the cooperative sensing. However, their reputation is properly updated

at each time k , allowing them to be included in the cooperative sensing once again if their reputation becomes greater than a pre-determined threshold. Adding this new state requires modifying the behaviour of the blind scheme by setting two new thresholds, τ_a and τ_b . According to [231], if $r_i(k)$ is lower than τ_a , the SU is excluded from the cooperation. Otherwise, if $\tau_a < r_i(k) < \tau_b$ the SU is in pending state. Conversely, if $r_i(k)$ is greater than τ_b , the i -th SU is considered reliable. In addition, at the time $k = 0$, the reputation of the i -th SU is $r_i(0) = \tau_a + \Delta$, while the reputation for the j -th TN is $r_j(0) = \tau_b + \Delta$, the parameter Δ is $\Delta = \frac{\tau_b - \tau_a}{2}$.

Finally, the FC considers only the TNs to be reliable at the initial time $k = 0$, while the remaining SUs are in pending state updating their reputations.

The approaches proposed in [235] are characterized by the following major drawbacks:

- some SUs may be temporarily unable to perform a local decision consistent with the global decision due to several issues, such as the hard condition of radio environment. Hence, discarding those SUs from the cooperative sensing without reconsidering their decisions penalizes not only the malicious users but also the legitimate, misbehaved SUs;
- discarding legitimate users that temporarily misbehaved decreases the set of available reliable users, forcing the FC to make the global decision exploiting only few SUs;
- the discarded legitimate SUs are permanently excluded from the exploitation of the spectrum opportunities and are forbidden access to the CRN, affecting the spectrum efficiency improvement proposed by the CRT;
- in the TNA-based scheme, there is a setup stage at time $k=0$ that denies SUs access to the CRN and to the detected spectrum holes in order to determine their reputations. This process may require time, wasting spectrum opportunities that can be used only by TNs, making the scheme unsuitable for potential market scenarios.

Designing and developing a new approach – both with and without TNA – able to address and overcome the above-mentioned drawbacks is therefore necessary.

6.2. Proposed reputation-based approach

The goal of this work is to provide a new reputation system to improve the performance of the centralized CSS, detecting both the misbehaved users and Byzantine attackers. To reach this goal, a new reputation method is defined as follows.

In the proposed method, the reputation of the i -th SU is composed of two parameters:

- the number of consecutive correct decisions ($Hits_i$);
- the number of detection errors ($Errors_i$).

The value of these two parameters is updated according to the equation (35).

$$r'_i(k) = \begin{cases} Hits_i(k) = (Hits_i(k-1) + 1) \cdot (1 - |d(k) - d_i(k)|) \\ Errors_i(k) = Errors_i(k-1) - (-1)^{d_i(k)+d(k)} \end{cases} \quad (35)$$

In particular, the parameter $Hits_i$ is set to zero when the local decision of the i -th SU is inconsistent with the global decision, otherwise it is increased. The parameter $Errors_i$ is increased by one when the local decision of the i -th SU is inconsistent with the global decision, otherwise it is decreased. Finally, to increase the security of the proposed reputation method, the FC is the only entity that knows and manages the reputation of each SU.

Through the exploitation of this new reputation method, we define a reputation system based on three lists: *White*, *Gray* and *Black*. These lists allow the FC to state the reliability of the cognitive users in the cooperative scenario and they can be defined as follows:

- *White* (W) list provides a reliable set of SUs, which are taken into account by the FC to make the global decision by weighting their decisions with a reputation weight, $w_{W,blind}$. At the time k , the list is defined as follows:

$$W(k) = \{SU_l : \text{if}(Hits_l(k) > N_{GW} \ || \ Errors_l(k) < K_{WG}) \\ \text{then } SU_l \in W, l \in \{1, \dots, L\}\} \quad (36)$$

If the reputation parameters of a SU satisfy the conditions to be in the list, then the user is eligible for the *White* list, otherwise its reputation will be compared with the conditions of the other lists;

- *Gray* (G) list is a set of SUs which participate to the cooperative sensing, but that are temporarily considered as misbehaved SUs and their decision is opportunely weighted with the reputation weight $w_{G,blind}$. The set of SUs belonging to this list is described by (37).

$$G(k) = \{SU_h : \text{if } (M_{BG} < Hits_h(k) \leq N_{GW} || K_{WG} \leq Errors(k) < L_{GB}) \\ \text{then } SU_h \in G, h \in \{1, \dots, H\}\} \quad (37)$$

- *Black* (B) list is composed of SUs that are considered by the FC as misbehaved and (probably) malicious users. The Black list is defined at the time k as follows:

$$B(k) = \{SU_j : \text{if } (Hits_j(k) \leq M_{BG} || Errors(k) \geq L_{GB}) \\ \text{then } SU_j \in B, j \in \{1, \dots, J\}\} \quad (38)$$

The decisions of the SUs in this list are not taken into account for the global decision, but they are considered to update their reputation at each time k .

To move SUs among the lists, the FC compares the reputation of each user with the defined thresholds of each list (i.e. K_{WG} , L_{GB} , M_{BG} , and N_{WG}). The thresholds should be tuned to detect all the misbehaved and malicious users and to have the highest number of reliable SUs in the *White* list. In addition, the thresholds are chosen to easily move the i -th misbehaved SU from the *White* list to the *Black* list, while making the change from the *Black* to the *White* list is harder. In particular, it is possible that some SUs might misbehave due to channel noise. Through the evaluation of their reputation, the FC states if they misbehave due to channel noise (in which case they can be moved from the *Black* to the *Gray* list and participate again to the cooperative sensing), or if they misbehave because they are malicious users (and hence must be excluded from the CSS and remain in the black list).

The MAJ voting fusion rule is more robust to the typical behaviour of Byzantine attackers than the OR and AND rules. As a matter of fact, using the OR or AND rule

as data fusion technique does not allow the FC to make a reliable decision in presence of Byzantine attackers, increasing the false alarm probability and causing a DoS for legitimate SUs and PUs. For instance, in a scenario where the sensing channel is free and the OR rule is used, an AB attacker can deceive the FC into making a wrong decision about the spectrum occupancy (i.e. the channel is busy while it is free). Using the AND rule as data fusion technique, instead, can allow an AF attacker to deceive the FC into declaring the absence of the PU while it is transmitting, allowing legitimate SUs to interfere with the PU's communication.

The MAJ fusion rule is indeed the optimal solution to minimize the effects of small-scale Byzantine attacks if any security mechanism is considered for mitigating them.

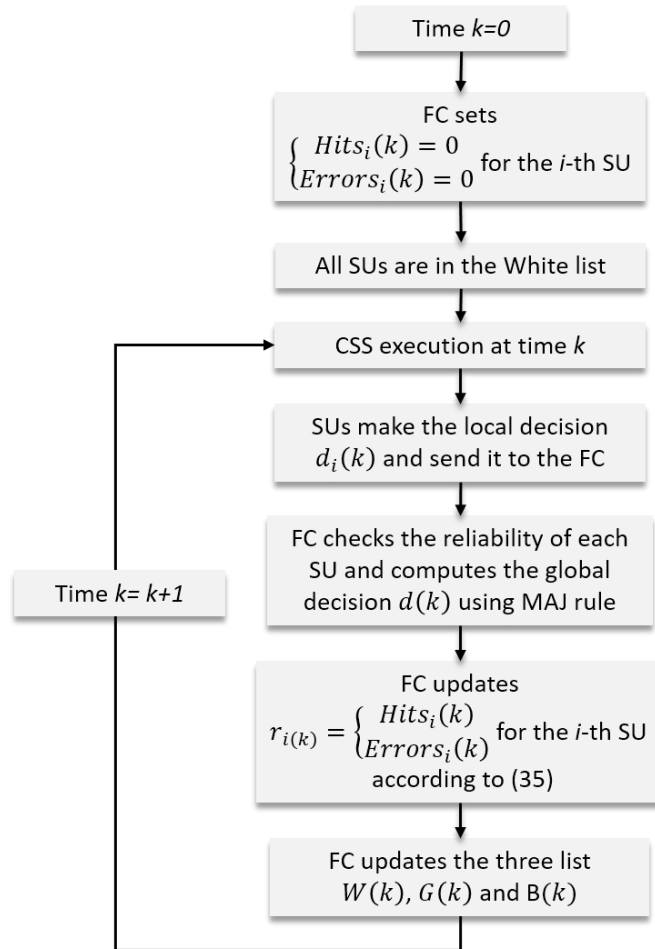


Figure 44. Simplified flowchart of the proposed reputation-based CSS.

As shown in Figure 44, at the time $k = 0$, all SUs (both legitimate and attackers) are considered reliable by the FC that sets their reputation parameters to 0 and moves them in the White list. Once the cooperative sensing starts, each SU makes the local

decision, $d_i(k)$, and sends it to the FC. The FC assesses the reliability of each SU based on the list it belongs to and defines the set of users that can participate to the CSS. Then, it makes the final decision, $d(k)$, and updates the reputation parameters of each SU according to (35). Finally, the FC updates the reliability of the SUs and moves them among the lists. Several factors (e.g. the hard propagation condition of the radio environment) could affect the ability of cognitive users to make a local decision consistent with the global one. Hence, omitting to reconsider the decisions of SUs discarded from the cooperative sensing, as in [235], penalizes the legitimate SUs. Therefore, contrary to the method presented in [235], the proposed approach evaluates the reputation of all users at the time k in order to move them among the three lists, meaning that SUs can go from the Black to the White list passing through the Gray one, and vice-versa.

To enhance the performance of proposed reputation system, it is necessary to involve TNs in a hostile CRN. As a matter of fact, the correctness of the global decision affects the performance of blind cooperative schemes. Hence, the presence of TNs, which provide reliable decisions to the FC, is useful to improve both the detection of malicious users and the cooperative gain. This is why the proposed approach can be improved by involving T TNs.

According to [235] and to underline the reliability of TNs, we increase the weight of the decision of such nodes by using a different reputation weight $w'_{W,TNA} = 2 * w_{W,TNA}$, where the $w_{W,TNA}$ is the reputation weight for the SUs in the *White* list. Furthermore, we change the weights for the White and the Gray list as follows:

- $w_{W,TNA} = 2 * w_{W,blind}$
- $w_{G,TNA} = 2 * w_{G,blind}$

Finally, the same rationale of the blind scheme is exploited to perform the new reputation system with TNA.

6.3. Experimental Results

The experimental results reported in this section show a performance comparison between the new schemes and the conventional ones proposed in [233]. Here, a CIPS

attack scenario is considered to test both the non-blind and blind approaches (i.e. with or without TNA), in presence of different types of malicious users (i.e. AB, AF, Opp, and SAF – see section 3.4). The CRN is composed of M users, M_0 malicious users and T trusted nodes. In detail:

- $M = 30$;
- $M_0 = [1, 2, 3]$;
- $T = 3$ in the TNA mode, while $T = 0$ in the blind mode.

The number of sensing symbols N is set to 1000, while the target P_{FA} is equal to 10^{-2} , and assumed equal unitary noise variance for all the SUs.

Finally, for the conventional methods, the remaining parameters are set as proposed in [231]: $\tau = 1$, $\tau_a = 1$, $\tau_b = 9$ and $\Delta = 4$, while for the proposed method they are set as follows: $w_{W,blind} = 1$, $w_{G,blind} = 0.5$, $w_{W,TNA} = 2$, $w'_{W,TNA} = 4$, $w_{G,TNA} = 1$, $K_{WG} = 8$, $L_{GB} = 10$, $M_{BG} = 28$, and $N_{WG} = 14$. The above parameters have been experimentally chosen by means of several trials and simulations, to maximize the performance of the proposed method, as done in [235].

For the sake of compactness, the results here reported are those implicating a scenario in which the network is under AF, Opp. and SAF attack at $SNR = -11dB$, which can be considered a typical working point for an ED-based CSS scenario.

Figures 45-47 show the receiver operating characteristic (ROC) curves (i.e. detection vs false alarm probabilities) of both the new and conventional methods (with and without TNA) in presence of two malicious users for each considered attack and for $SNR = -11dB$.

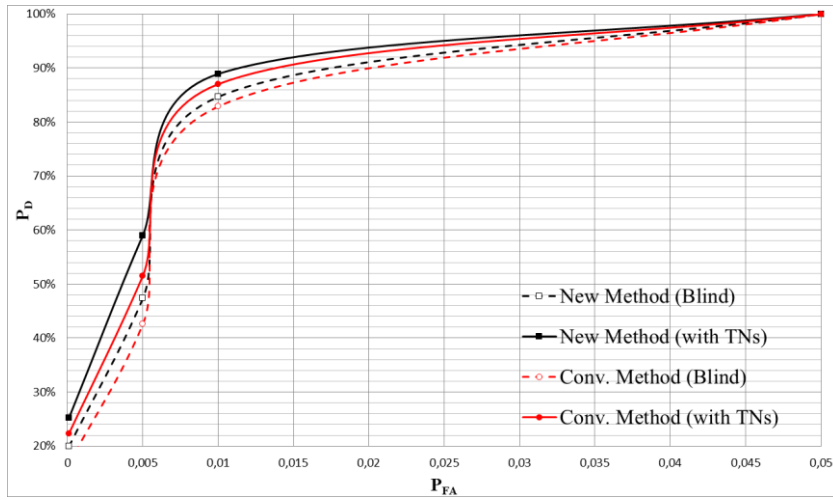


Figure 45. The ROC curves of the new and conv. methods (in blind and TNA modes) in presence of 2 AF attackers for $SNR = -11dB$.

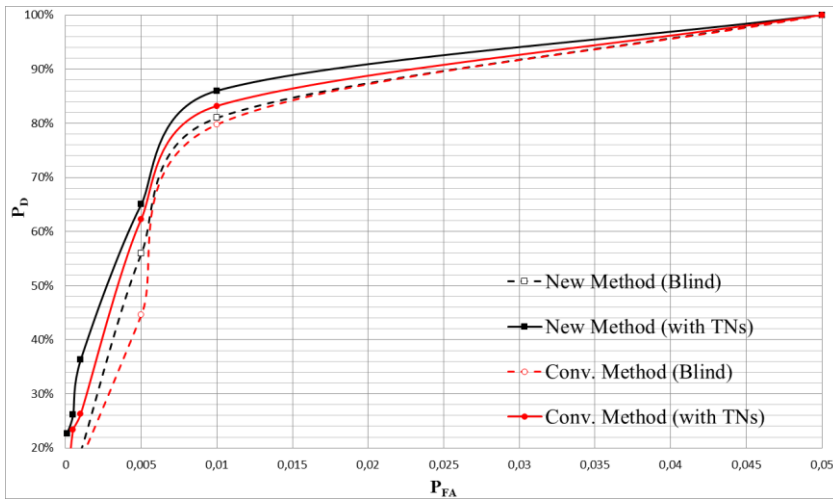


Figure 46. The ROC curves of the new and conv. methods (in blind and TNA modes) in presence of 2 Opp. attackers for $SNR = -11dB$.

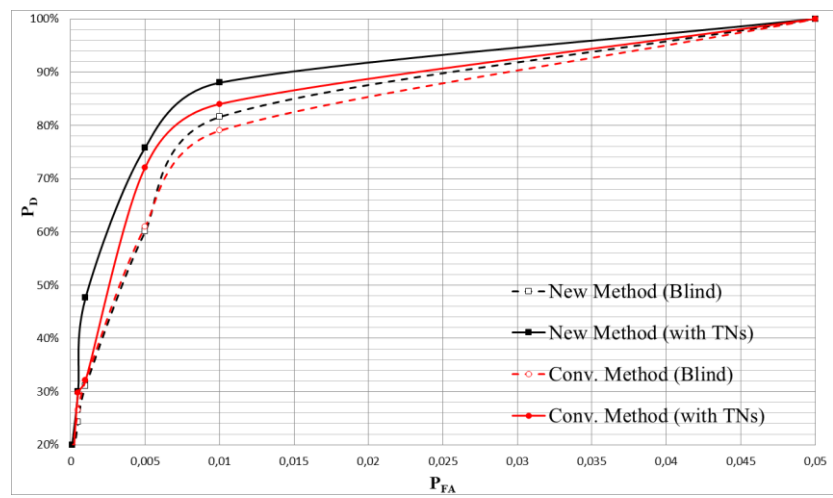


Figure 47. The ROC curves of the new and conv. methods (in blind and TNA modes) in presence of 2 SAF attackers for $SNR = -11dB$.

The obtained results show that our new blind method and the conventional blind method have similar performances in all the considered scenarios. In addition, the new method with TNA outperforms the conventional TNA method in all the considered scenarios. However, even if at a first glance it appears that our method shows only a minor performance increasing versus the methods in [233], it greatly outperforms these conventional methods in identifying the malicious users.

Figures 48-50 report the number of discarded SUs (misbehaved users, both malicious and honest) identified by the new and conventional methods in presence of three attacks with at least 10% of malicious users. From the analysis of the figures, the following advantages are provided by the proposed methods.

Firstly, our new methods (blind and with TNA) succeed in correctly identifying all the malicious users, while the blind method proposed in [235] is unable to detect all the AB and SAF attackers, as shown in Figure 48 and 50 (in presence of three and two attackers, respectively). In addition, the conventional approach fails to identify SAF malicious users in presence of one attacker acting in the cooperative scenario (see Figure 56).

Secondly, the proposed methods discard a number of honest (i.e. legitimate) but misbehaved SUs that is always lower than or at least equal to the number of users discarded by the conventional methods (both blind and with TNA). In particular, the proposed approach discards at least six honest but misbehaved users in presence of three SAF attackers, while the conventional methods (blind and with TNA) discard more than 12 misbehaved users (out of 30 total users). Such behaviour underlines how the conventional methods proposed in [233] allows the FC to make the global decision by using only a few local decisions, since a large amount of SUs is discarded from the cooperative sensing, and, hence, from the CRN.

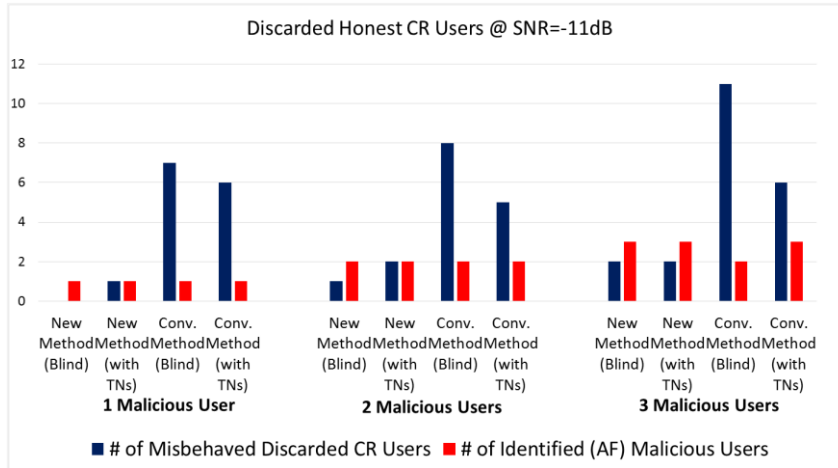


Figure 48. Number of: (red) correctly identified malicious users; (blue) discarded misbehaved SUs in presence of at least 3 AB attackers ($SNR = -11dB$).

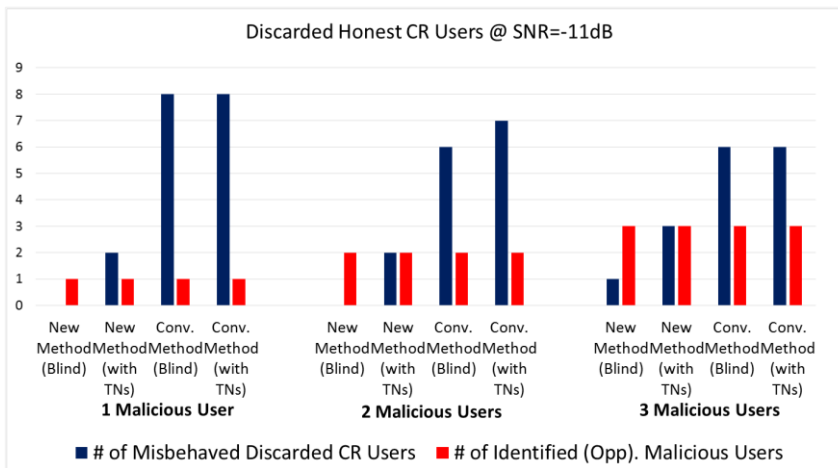


Figure 49. Number of: (red) correctly identified malicious users; (blue) discarded misbehaved SUs in presence of at least 3 Opp. attackers ($SNR = -11dB$).

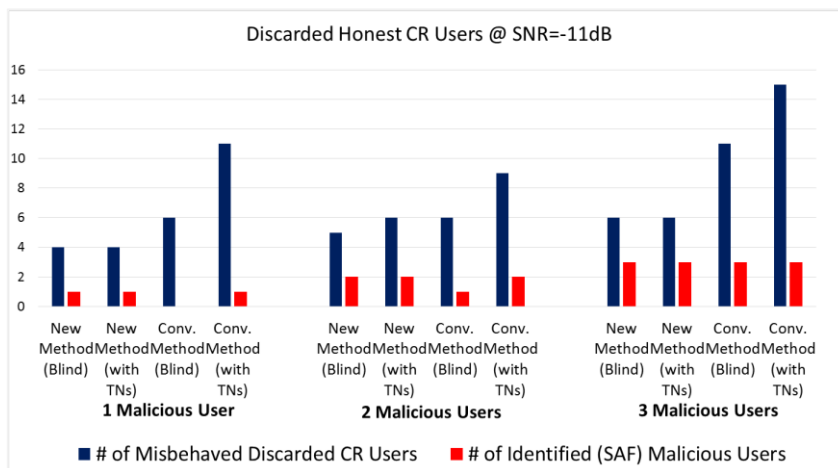


Figure 50. Number of: (red) correctly identified malicious users; (blue) discarded misbehaved SUs in presence of at least 3 SAF attackers ($SNR = -11dB$).

As a matter of fact, the conventional methods excessively penalize honest users that misbehave temporarily, for instance because of channel noise. Moreover, even if the excluded honest users start making decisions consistent with the global one after being discarded, they are no longer considered reliable by the FC and, hence, they are no longer taken into account in the cooperative scenario.

Figures 51-53 show the P_D of the new and conventional methods (both blind and TNA) in presence of the considered attack versus the number of SUs. In particular, we consider a cooperative scenario composed of M users (with $M = 10, \dots, 100$) and a number of TNs and malicious users equal to 10% of M , at the SNR value of $-11dB$ and P_{FA} value of 10^{-2} . In all the considered cases, the new TNA method outperforms the conventional approaches of [235].

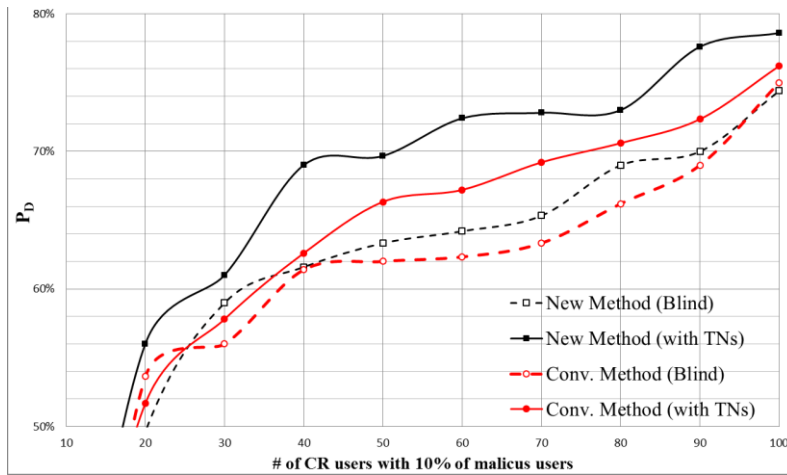


Figure 51. P_D of the new and conv. methods (in blind and TNA modes) in presence of the AF attack versus the number of SUs in presence of 10% of malicious users ($SNR = -11dB$).

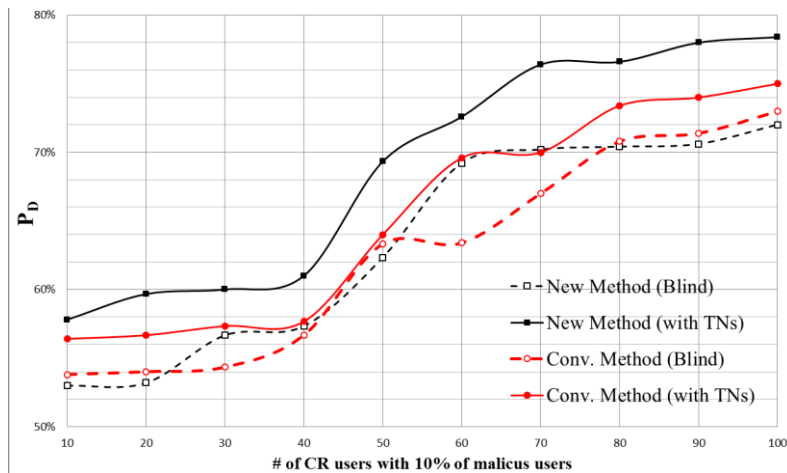


Figure 52. P_D of the new and conv. methods (in blind and TNA modes) in presence of the Opp. attack versus the number of SUs in presence of 10% of malicious users ($SNR = -11dB$).

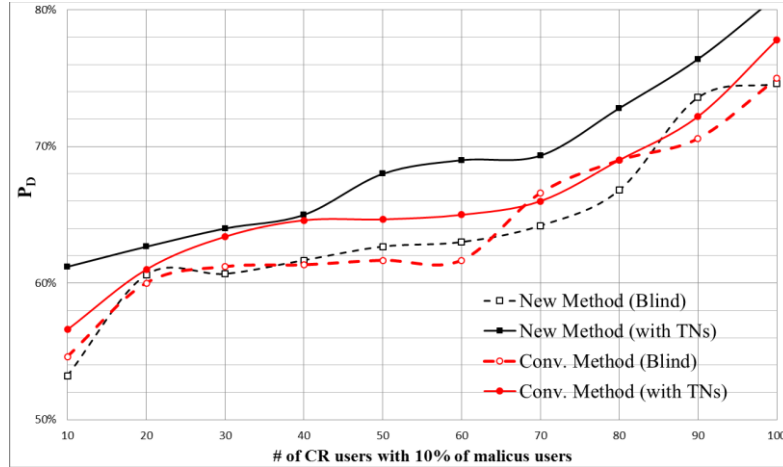


Figure 53. P_D of the new and conv. methods (in blind and TNA modes) in presence of the SAF attack versus the number of SUs in presence of 10% of malicious users ($SNR = -11dB$).

Finally, the performance of the approaches in presence of a higher number of malicious users, i.e. $M = 100$ and $M_0 = 10$, is evaluated, considering also the number of SUs in pending state for the conventional method with TNA. In particular, Figure 54 shows the number of both discarded SUs and attackers identified by the conventional and new methods in presence of the three considered attacks, with a SNR value of $-11 dB$.

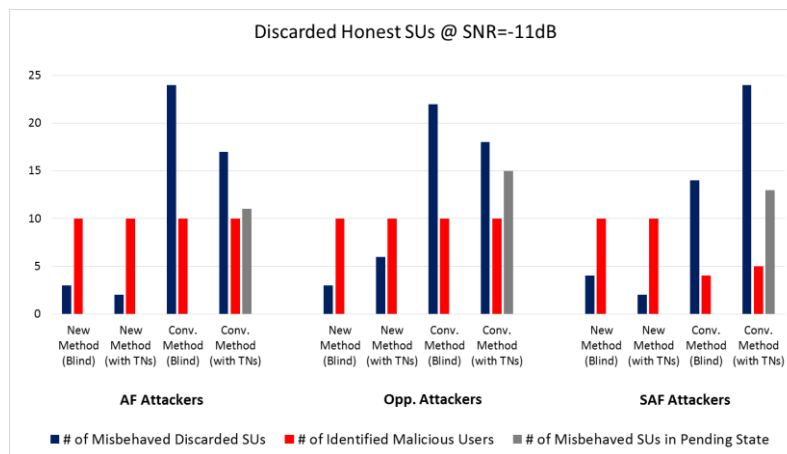


Figure 54. Number of: (blue) discarded misbehaved SUs; (red) correctly identified malicious SUs and (Gray) misbehaved SUs in pending state with 10% of the three attackers ($SNR = -11 dB$).

Once again, the obtained results assess the capability of the proposed approaches to identify all the attackers while discarding only a few honest users. As a matter of fact, in the worst-case scenario, our new methods discard at most 6 honest SUs in presence of the Opp. attackers, while both the conventional methods in blind and TNA modes

discard more than 20 honest users in presence of AF and SAF attackers, respectively. Moreover, the conventional method with TNA does not take into account the decision of the SUs in pending state, further decreasing the number of legitimate SUs that can participate to the cooperative scenario. The consequence of this behaviour is that the methods of [235] heavily penalize these misbehaving users (due to low SNR or high fading). If the channel's condition improves (e.g. due to the mobility of the users), they are not allowed to re-gain a reliable state and to participate to the CRN. In the worst-case scenario, the conventional method with TNA provides the final decision without taking into account 42 legitimate SUs, which are temporarily misbehaving according to the scheme proposed in [235], and includes in the decision process 6 misdetected SAF attackers, hence allowing these malicious users to join the CRN.

Conclusions

In the proposed doctoral dissertation, we discussed about the promising Cognitive Radio Technology (CRT) by defining its fundamentals concepts and behaviours. In particular, CRT aims at addressing the spectrum scarcity problem, improving the spectrum efficiency through a dynamic allocation of PUs' vacant frequency bands. It allows SUs to opportunistically access and use the radio spectrum without interfering with primary transmissions. A CRN should be efficient and secure to properly fulfil the constraints of CRT and to allow the interoperability with new and legacy radio systems. However, the creation of such a kind of network is a critical challenge that requires the definition of techniques for the performance improvement of the (cooperative and non-cooperative) spectrum sensing, and for the identification of attacks and, hence, attackers that affect the network. As a matter of fact, even though CRT promises several benefits in order to improve the spectrum utilization and to implement reconfigurable and cost-effective architectures for wireless devices, it poses several challenges that are not to be overlooked in the design and implementation of a cooperative environment.

In this dissertation, we highlighted the main issues of CRT and spectrum sensing, focusing on two challenging problems: the cooperative sensing in the presence of correlated SUs' observations, and the security of CRNs in the presence of packet loss and Byzantine attacks. In particular, we proposed novel signal processing techniques for the performance improvement of the centralized CSS in both trusted and untrusted CRNs.

Summary of contributions

The research activity related to trusted CRNs was focused on the improvement of the ED-based CSS in the presence of correlated SUs' observations. As a matter of fact, when the proximity among SUs results in correlated observations, the performance of the ED-based CSS degrades, increasing the probability to interfere with primary communications. To overcome such issues, we addressed the issue of CSS in presence of correlated observations by proposing the MTT method. The MTT defines an additional threshold that is lower than the one of the conventional ED and employs the

OR and MAJ fusion rules in order to reach reliable detection of the PUs. The obtained results demonstrate the effectiveness of the MTT method for application in CRNs in the presence of correlated users. Moreover, we have also evaluated the mean detection time, defined as the time required on average to perform a reliable detection of the PU. The simulation results show that the proposed method improves the detection performance, while reducing the mean detection time and enabling a faster rejection of occupied bands. However, in a real communication scenario, where the communication channel is affected by AWGN and noise uncertainty, the MTT performs poorly, since the function used to compute the thresholds is not optimized. To address such issues and to allow the MTT to still provide reliable detection, we proposed an extended version of the MTT (i.e. the EMTT) designing a new recursive function that allows the MTT to find the best pair of thresholds: the ones that meet the CFAR criterion and that maximize the detection probability of a PU's signal in the presence of noise uncertainty. Then, to validate the effectiveness of the EMTT, we considered an AWGN channel affected by different levels of noise uncertainty, which is assumed to be equal for all the SUs. The obtained results show that the EMTT outperforms the MTT and the CSS based on the hard combining voting rules and the ED, asserting its robustness in presence of noise uncertainty and correlated observations.

Successively, our research activity focused on the design and development of two novel signal processing techniques for the improvement of the security and reliability of CRNs. As a matter of fact, ensuring the security of this kind of wireless networks is of paramount importance to guarantee a reliable delivery of trustworthy data. In particular, this activity addressed two important security threats: (i) packet losses in sensor networks (both conventional and CR-based) caused by packet drop or jamming (i.e. intentional interference) attacks; (ii) Byzantine attacks in a cooperative scenario.

We provided an approach that builds a statistical model for an optimally-accurate fine-grained analysis of the underlying causes of packet losses in sensor networks (both conventional and CR-based), whether node- or link-related. The proposed model exploits the variances of both the RSSI and LQI to determine an individual, optimal detection threshold for each link. In addition, the proposed approach allows to have control on the P_{FA} through the CFAR criterion for the entire network's links. The

conducted experiments tested both the performance and the robustness of the model in presence of interference (i.e. the attacker changes the interference level from high to medium-low) and selective forwarding attacks. The experimental results validate the robustness of the proposed model in detecting the considered attacks and its performance.

Finally, we designed a new reputation-based CSS method for the detection of Byzantine attackers. The proposed approach is based on two features: a new reputation method based on the number of consecutive correct decisions and of errors; three lists (White, Gray and Black) which state the reliability of SUs in a CRN. Moreover, it can be applied with and without TNA, allowing the FC to assess the reliability of SUs through the exploitation of the three lists. In fact, the FC is able to move SUs (both legitimate and malicious) among said lists by evaluating their reputation vectors. The performance of the proposed method has been compared to another reputation-based approach proposed in [235], considering several kinds of Byzantine attacks. The experimental results highlight that the proposed approach outperforms the conventional one in the identification of all the considered categories of Byzantine attacker, while discarding only a few number of legitimate SUs and improving the security of the CRN.

Design recommendations and further work

The future developments and applications of the methods described in this doctoral thesis aim at sustaining the diffusion of efficient, secure CRNs. The proposed techniques improved the performance of the CSS in both trusted and untrusted networks, addressing the considered challenges. However, the proposed works require further improvements and investigations as follows.

In order to complete the current investigations of the EMTT, in future studies, we will consider quantifying, analytically and experimentally, the performance of EMTT-based CSS in different configurations, considering log-normal fading and frequency selective channels. The analysis of the computational complexity will also be investigated in detail to compare it with the advanced eigenvalue-based CSS methods, which are also robust to noise uncertainty with high computational complexity.

About the statistically-enhanced FGA approach, future developments will focus on an evaluation of the effectiveness of the proposed approach in more complex scenarios, as well as on a comparison between the system's performance and machine learning methods, such as neural networks and Naive Bayes classifiers.

Finally, we will focus future researches of the proposed reputation-based CSS schemes for the detection of Byzantine attackers on the (theoretical and experimental) relationship between the values of the parameters and the system's performance for several operating scenarios of interest. In addition, the integration of a soft-quantized approach in combination with dynamic reputation weight will be evaluated in order to improve the performance of the proposed reputation system.

References

- [1] ITU, “Radio Regulations. Articles”. 2012. [Online]. Available on: http://www.itu.int/dms_pub/itu-s/oth/02/02/S02020000244501PDFE.PDF. Last Access: 04/11/2016.
- [2] ITU. “Regionally harmonized bands”. [Online]. Available on: <http://www.itu.int/net/ITU-R/index.asp?category=information&mlink=emergency-bands&lang=en>. Last Access: 04/11/2016.
- [3] Federal Communications Commission, “What We Do”. [Online]. Available on: <https://www.fcc.gov/about-fcc/what-we-do>. Last Access: 04/11/2016.
- [4] Federal Communications Commission, “For New Visitors - Finding Broadcast Radio and Television Information on the FCC Website”. [Online]. Available on: <https://www.fcc.gov/media/radio/new-visitors>. Last Access: 04/11/2016.
- [5] G. Baldini, O. Holland, V. Stavroulaki, K. Tsagkaris, P. Demestichas, A. Polydoros, S. Karanasios, D. Allen, “The evolution of cognitive radio technology in Europe: Regulatory and standardization aspects”, *Telecommunications Policy*, vol.37, no. 2–3, March–April 2013, pp. 96-107, ISSN 0308-5961.
- [6] Electronic Communications Committee (ECC), European Conference of Postal and Telecommunications Administrations (ECPT), “Report C from CEPT to the European Commission in response to the mandate on: Technical considerations regarding harmonisation options for the digital dividend”. 2008.
- [7] Federal Communications Commission, “Facilitating Opportunities for Flexible, Efficient and Reliable Spectrum Use Employing Cognitive Radio Technologies”, notice of proposed rulemaking and order, FCC 03- 322, December 2003.
- [8] Federal Communications Commission Spectrum Policy Task Force, “Report of the Spectrum Efficiency Working Group”, November 2002.
- [9] Shared Spectrum Company, “Spectrum Occupancy Measurements”, 2005. [Online]. Available on : www.sharespectrum.com/measurements. Last Access: 04/11/2016.
- [10] K. N. Steadman, A. D. Rose, and T. T. N. Nguyen, “Dynamic Spectrum Sharing Detectors”, *In Proc. of IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2007)*, Dublin, Ireland, April 2007, pp. 276-282.
- [11] M. Wellens and P. Mähönen, “Lessons Learned from an Extensive Spectrum Occupancy Measurement Campaign and a Stochastic Duty Cycle Model”, *Proc. of TridentCom 2009*, Washington D.C., USA, April 2009, pp. 1-9.
- [12] M. Lopez-Benitez and F. Casadevall, “On the Spectrum Occupancy Perception of Cognitive Radio Terminals in Realistic Scenarios”, *International Workshop on Cognitive Information Processing*, Elba, June 2010, pp. 99-104.
- [13] V. Valenta, R. Maršalek, G. Baudoin, M. Villegas, M. Suarez and F. Robert, “Survey on Spectrum Utilization in Europe: Measurements, Analysis and Observations”, *in Proc. of ICST Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, Cannes, France, June 2010, pp. 1-5.
- [14] Cisco, “Cisco Visual Networking Index: Forecast and Methodology, 2014-2019 White Paper”. [Online]. Available on: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html. Last Access: 04/11/2016.
- [15] P. Rysavy, “Challenges and Considerations in Defining Spectrum Efficiency”, in *Proceedings of the IEEE*, vol. 102, no. 3, pp. 386-392, March 2014.

- [16] I. F. Akyildiz, W. Y. Lee, M. C. Vuran and S. Mohanty, "NeXt Generation / Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey", *Computer Networks*, 2006, pp. 2127-2159.
- [17] S. Haykin, "Cognitive Radio: Brain-empowered Wireless Communications", *IEEE Journal on Selected Areas in Commun.*, Vol. 23, No. 2, February 2005, pp. 201-220.
- [18] A. L. Drozd, I. P. Kasperovich, C. E. Carroll, A. C. Blackburn, "Computational Electromagnetics Applied to Analyzing the Efficient Utilization of the RF Transmission Hyperspace", In *Proc. of IEEE/ACES Conf. on Wireless Comm. and Applied Computational Electromagnetics*, Hawaii, USA, April 2000, pp. 1077-1085.
- [19] J. Mitola, G. Q. Maguire, "Cognitive radios: Making Software Radios More Personal", *IEEE Pers. Commun.*, vol. 6, no. 4, August 1999, pp. 13-18.
- [20] J. Mitola, "Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio", PhD thesis, KTH Royal Institute of Technology, Stockholm, Sweden, 2000.
- [21] L. Berlemann, G. Dimitrakopoulos, K. Moessner, J. Hoffmeyer, "Cognitive Radio and Management of Spectrum and Radio Resources in Reconfigurable Networks", *Wireless World Research Forum, Working Group 6 White Paper Cognitive Radio and Management of Spectrum and Radio Resources*, 2005.
- [22] R. Tandra, S. M. Mishra, A. Sahai, "What is a Spectrum Hole and What Does it Take to Recognize One?", in *Proceedings of the IEEE*, vol. 97, no. 5, pp. 824-848, May 2009.
- [23] F. Benedetto, A. Tedeschi, "Chapter 1. The Cognitive Radio Technology: Future Trends in the Spectrum Access of Next Generation Communication Systems", pp. 1-32, in "Communication Systems: New Research", Vyacheslav Tuzlukov editor, NOVA Science Publishers, 432 pp. USA, 2013. ISBN: 978-1-62618-654-5.
- [24] Federal Communications Commission - Spectrum Policy Task Force, "Report of the Spectrum Rights and Responsibilities Working Group", ET Docket No. 02-135, 15 November 2002.
- [25] J. M. Peha, "Wireless Communications and Coexistence for Smart Environments", *IEEE Personal Communications*, pp. 66-68, October 2000.
- [26] J. M. Peha, "Approaches to spectrum sharing", in *IEEE Communications Magazine*, vol. 43, no. 2, pp. 10-12, Feb. 2005.
- [27] J. M. Peha and S. Panichpapiboon, "RealTime Secondary Markets for Spectrum", *Telecommun. Policy*, Aug. 2004, pp. 603-18.
- [28] Federal Communications Commission, "Notice of Proposed Rulemaking (FCC 04-100): Unlicensed Operation in the Band 3650 - 3700 MHz", ET Docket No. 04-151, 23 April 2004.
- [29] IEEE Std 1900.5-2011, IEEE Standard Policy Language Requirements and System Architectures for Dynamic Spectrum Access Systems.
- [30] D. T. C. Wong, A. T. Hoang, Y.-C. Liang, F. P. S. Chin, "Dynamic Spectrum Access with Virtual Partitioning in Open Spectrum Wireless Networks", In *IEEE Vehicular Technology Conference*, 2008.
- [31] S. Sengupta, M. Chatterjee, K. Kwiat, "Dynamic Spectrum Access in Cognitive Radio Tactical Networks", In *IEEE Conference on Wireless Communications and Networking*, Budapest, 2009, pp. 1-6.
- [32] D. N. Hatfield, P. J. Weiser, "Property rights in spectrum: taking the next step", *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Baltimore, MD, USA, 2005, pp. 43-55.
- [33] O. Ileri, D. Samarzija, N. B. Mandayam, "Dynamic Property Rights Spectrum Access: Flexible Ownership Based Spectrum Management", *2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Dublin, 2007, pp. 254-265.

- [34] Lin Xu, R. Tonjes, T. Paila, W. Hansmann, M. Frank, M. Albrecht, "DRiVE-ing to the Internet: Dynamic Radio for IP services in Vehicular Environments", *Proceedings of 25th Annual IEEE Conference on Local Computer Networks.*, Tampa, FL, 2000, pp. 281-289.
- [35] W. Lehr, J. Crowcroft, "Managing shared access to a spectrum commons", *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005*, Baltimore, MD, USA, 2005, pp. 420-444.
- [36] M. Sharma, A. Sahoo, K. D. Nayak, "Channel modeling based on interference temperature in underlay cognitive wireless networks", *IEEE International Symposium on Wireless Communication Systems*, Reykjavik, 2008, pp. 224-228.
- [37] T. C. Clancy, "On The Use Of Interference Temperature For Dynamic Spectrum Access", *Ann. Telecomm. Springer*, vol. 64, no. 7, pp. 573-585. Aug. 2009.
- [38] J. S. Pang, G. Scutari, D. P. Palomar, F. Facchinei, "Design of cognitive radio systems under temperature-interference constraints: A variational inequality approach", *IEEE International Conference on Acoustics, Speech and Signal Processing*, Dallas, TX, 2010, pp. 2994-2997.
- [39] The American Heritage Dictionary. [Online]. Available on: <https://ahdictionary.com/>. Last access: 04/11/2016.
- [40] Collins English Dictionary. [Online]. Available on: <http://www.collinsdictionary.com/dictionary/english>. Last access: 04/11/2016.
- [41] M. Matinmikko, M. Mustonen, H. Sarvanko, M. Höyhty, A. Hekkala, A. Mämmelä, M. Katz and M. Kiviranta, "A Motivating Overview of Cognitive Radio: Foundations, Regulatory Issues and Key Concepts", *First International Workshop CogART*, Aalborg, February 2008, pp. 1-5.
- [42] S. Mangold, Z. Zhong, K. Challapali, and C. T. Chou, "Spectrum Agile Radio: Radio Resource Measurements for Opportunistic Spectrum Usage", in *Proc. of 47th annual IEEE Global Telecommunications Conference*, Globecom 2004, Dallas TX, USA, 29 Nov. - 3 Dec. 2004.
- [43] S. Mangold, S. Shankar, L. Berlemann, "Spectrum Agile Radio: A Society of Machines with Value-Oriented (invited paper)", in *Proc. of European Wireless Conference 2005, EW'05*, Nicosia, Cyprus, 10-13 April 2005.
- [44] Google Spectrum Database. [Online]. Available on: <https://www.google.com/get/spectrumdatabase/>. Last access: 04/11/2016.
- [45] Amy Nordrum, "How Cognitive Radio Can Help LTE-U and Wi-Fi Users Get Along", [Online]. Available on: [http://spectrum.ieee.org/tech-talk/telecom/wireless/how-cognitive-radio-can-help-lteu-and-wifi-users-get-along?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+IeeeSpectrum+\(IEEE+Spectrum\)](http://spectrum.ieee.org/tech-talk/telecom/wireless/how-cognitive-radio-can-help-lteu-and-wifi-users-get-along?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+IeeeSpectrum+(IEEE+Spectrum)). Last access 15/10/2016.
- [46] Per H. Lehne, Ole Grøndalen, Richard MacKenzie, Dominique Noguet, Vincent Berg, "Mapping cognitive radio system scenarios into the TVWS context", *Journal of Signal Processing Systems* 73, 2013, no. 3, 227-242.
- [47] P. Pawelczak, R. Venkatesha Prasad, "Chapter 13 - Defining cognitive radio, In Cognitive Radio Communications and Networks", edited by Alexander M. Wyglinski, Maziar Nekovee and Y. Thomas Hou, Academic Press, Oxford, 2010, pp. 367-386, ISBN 9780123747150.
- [48] L. M. Grande, "IEEE Dynamic Spectrum Access policy standards work", *MILCOM 2009 - 2009 IEEE Military Communications Conference*, Boston, MA, 2009, pp. 1-4.
- [49] S. Filin, H. Harada, H. Murakami and K. Ishizu, "International standardization of cognitive radio systems", in *IEEE Communications Magazine*, vol. 49, no. 3, pp. 82-89, March 2011.
- [50] IEEE 1900.1 Working Group on "Definitions and Concepts for Dynamic Spectrum Access: Terminology Relating to Emerging Wireless Networks, System Functionality, and Spectrum Management". [Online]. Available on: <http://grouper.ieee.org/groups/dyspan/1/>. Last access 04/11/2016

- [51] IEEE SCC41, "IEEE 1900.7 White Space Radio Working Group". [Online]. Available: <http://grouper.ieee.org/groups/dyspan/7/index.htm>. Last access 04/11/2016
- [52] Federal Communications Commission, "Second report and order and memorandum and order FCC 08-260: In the matter of unlicensed operation in the TV broadcast bands—ET Docket No. 04-186 and additional spectrum for unlicensed devices below 900 MHz and in the 3 GHz band—ET Docket No. 02-380", Nov. 2008.
- [53] IEEE, "IEEE Standard Definitions and Concepts for Dynamic Spectrum Access: Terminology Relating to Emerging Wireless Networks, System Functionality, and Spectrum Management", in *IEEE Std 1900.1-2008*, vol., no., pp.1-62, Oct. 3 2008
- [54] B. Wang, K. J. R. Liu, "Advances in cognitive radio networks: A survey", in *IEEE Journal of Selected Topics in Signal Processing*, vol. 5, no. 1, pp. 5-23, Feb. 2011.
- [55] I.F. Akyildiz, "Spectrum, network and operations management in cognitive radio networks", *IEEE Network Operations and Management Symposium*, 2008. NOMS 2008.
- [56] H. Elshafie, N. Fisal, M. Abbas, W.A. Hassan, H. Mohamad, N. Ramli, S. Jayavalan, S. Zubair, A survey of cognitive radio and tv white spaces in malaysia, *Transactions on Emerging Telecommunications Technologies* 26 (2015), no. 6, 975–991.
- [57] I. F. Akyildiz, W. y. Lee, M. C. Vuran, S. Mohanty, "A survey on spectrum management in cognitive radio networks", in *IEEE Communications Magazine*, vol. 46, no. 4, pp. 40-48, April 2008.
- [58] N. Nie, C. Comaniciu, "Adaptive Channel Allocation Spectrum Etiquette for Cognitive Radio Networks", *Springer Science Business Media*, 2006
- [59] Raul Etkin, Abhay K. Parekh, David Tse, "Spectrum Sharing for Unlicensed Bands", *IEEE Journal on Selected Areas in Communications*, vol. 25, pp. 517–528, April 2007.
- [60] Z. Bouida, K. Qaraqe, M. Abdallah, M. Alouini, "Performance Analysis of Joint Multi-Branch Switched Diversity and Adaptive Modulation Schemes for Spectrum Sharing Systems", *IEEE Trans. on Commun.*, early access, pp. 1 – 11, 2012.
- [61] D. Kalathil, R. Jain, "Spectrum Sharing through Contracts for Cognitive Radios", *IEEE Trans. on Mobile Computing*, early access, pp. 1-14, 2012
- [62] B. F. Lo, "A survey of common control channel design in cognitive radio networks", *Physical Communication*, Volume 4, Issue 1, March 2011, pp. 26-39, ISSN 1874-4907.
- [63] W. Y. Lee, I. F. Akyildiz, "Spectrum-Aware Mobility Management in Cognitive Radio Cellular Networks", in *IEEE Transactions on Mobile Computing*, vol. 11, no. 4, pp. 529-542, April 2012.
- [64] L. Won-Yeol, I.F. Akyildiz, "A Spectrum Decision Framework for Cognitive Radio Networks", *IEEE Trans. on Mobile Computing*, vol. 10, no. 2, pp. 161 – 174, 2011.
- [65] W. Li-Chun, W. Chung-Wei, F. Adachi, "Load-Balancing Spectrum Decision for Cognitive Radio Networks", *IEEE J. on Selected Areas in Commun.*, vol. 29, no. 4, pp. 757 – 769, 2011.
- [66] M. Matinmikko, M. Höyhty, M. Mustonen, H. Sarvanko, A. Hekkala, M. Katz, A. Mämmelä, M. Kiviranta, A. Kautio, "Channel State Estimation and Spectrum Management for Cognitive Radios, Cognitive Radio: An Intelligent Wireless Communication System", *VTT Research report*, No. VTT-R-02219-08, March 2008.
- [67] T. Yücek, H. Arslan, "A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications", *IEEE Communications Surveys and Tutorials*, Vol. 11, No.1, 1Q2009, pp. 116-130
- [68] D. Čabrić, S. M. Mishra, R. Brodersen, "Implementation Issues in Spectrum Sensing for Cognitive Radios", *Conference Record of the 38th Conference on Signals, Systems and Computers*, November 2004, pp. 772-776
- [69] A. Ghasemi, A. S. Sousa, "Spectrum Sensing in Cognitive Radio Networks: Requirements, Challenges and Design Trade-offs", *IEEE Communications Magazine*, April 2008, pp. 32-39

- [70] S. M. Mishra, A. Sahai, R. Brodersen, "Cooperative Sensing Among Cognitive Radios", in *Proc. of IEEE International Conference (ICC 2006)*, June 2006, pp. 1658-1663.
- [71] A. Ghasemi, E. S. Sousa, "Collaborative Spectrum Sensing for Opportunistic Access in Fading Environments", in *Proc. of IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2005)*, pp. 131-136.
- [72] R. Murty, R. Chandra, T. Moscibroda, P. Bahl, "SenseLess: A Database-Driven White Spaces Network", in *IEEE Transactions on Mobile Computing*, vol. 11, no. 2, pp. 189-203, Feb. 2012.
- [73] H. N. Tran, Y. D. Alemseged, C. Sun, H. Harada, "On the effect of local sensing database to cognitive radio systems", *Wireless Personal Multimedia Communications (WPMC), 2011 14th International Symposium on*, Brest, 2011, pp. 1-5.
- [74] B. Bochow, O. Holland and K. Katzis, "Spectrum sensing infrastructure support for IEEE 1900.6b sensing-assisted spectrum databases," *2016 IEEE Conference on Standards for Communications and Networking (CSCN)*, Berlin, 2016, pp. 1-6.
- [75] Li, Lingjie, Jung Yee. "System and method of implementing a cognitive radio device with enhanced spectrum sensing", U.S. Patent No. 8,928,759. 6 Jan. 2015.
- [76] O. Holland, B. Bochow and K. Katzis, "IEEE 1900.6b: Sensing support for spectrum databases," *2015 IEEE Conference on Standards for Communications and Networking (CSCN)*, Tokyo, 2015, pp. 199-205.
- [77] B. Wild, K. Ramchandran, "Detecting primary receivers for cognitive radio applications", *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005*. Baltimore, MD, USA, 2005, pp. 124-130.
- [78] T. C. Clancy, "Formalizing the interference temperature model". *Wireless Communications & Mobile Computing*, vol.7, no. 9, pp. 1077-1086. 2007.
- [79] S. Dikmese, M. Renfors, "Performance analysis of eigenvalue based spectrum sensing under frequency selective channels", *Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM), 7th International ICST Conference on*, Stockholm, 2012, pp. 356-361.
- [80] Y. Gao, Y. Chen, Y. Ma, C. He, L. Su, "Eigenvalue-Based Spectrum Sensing for Multiple Received Signals Under the Non-Reconstruction Framework of Compressed Sensing", in *IEEE Access*, vol. 4, no. , pp. 4891-4901, 2016.
- [81] Y. Zeng, Y. C. Liang, "Eigenvalue-based spectrum sensing algorithms for cognitive radio", in *IEEE Transactions on Communications*, vol. 57, no. 6, pp. 1784-1793, June 2009.
- [82] S.K.Sharma, S. Chatzinotas, B.Ottersten, "Eigenvalue based sensing and SNR estimation for Cognitive Radio in presence of noise correlation", *IEEE Trans. on Vehicular Technology*, vol. 62, no. 8, pp. 3671-3684, April 2013.
- [83] E. Blossom, "GNU radio: tools for exploring the radio frequency spectrum", *Linux Journal*, vol. 2004, no. 122, June 2004.
- [84] M. Ettus, "Universal software radio peripheral". [Online]. Available: www.ettus.com
- [85] M. McHenry, E. Livsics, T. Nguyen, N. Majumdar, "XG dynamic spectrum sharing field test results", in *Proc. IEEE Int. Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Dublin, Ireland, Apr. 2007, pp. 676-684
- [86] National Instrument, USRP. [Online]. Available on: <http://www.ni.com/sdr/usrp/>. Last Access: 04/11/2016.
- [87] National Instruments, LabVIEW System Design Software. [Online]. Available on: <http://www.ni.com/labview/>. Last access: 04/11/2016.
- [88] G. Ganesan, Y. Li, "Agility improvement through cooperative diversity in cognitive radio", in *Proc. IEEE Global Telecomm. Conf. (Globecom)*, vol. 5, St. Louis, Missouri, USA, Nov./Dec. 2005, pp. 2505-2509.

- [89] G. Ganesan, Y. Li, "Cooperative spectrum sensing in cognitive radio networks", *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*. Baltimore, MD, USA, 2005, pp. 137-143.
- [90] D. Cabric, A. Tkachenko, R. Brodersen, "Spectrum sensing measurements of pilot, energy, and collaborative detection", in *Proc. IEEE Military Commun. Conf.*, Washington, D.C., USA, Oct. 2006, pp. 1-7.
- [91] S. D. Jones, E. Jung, X. Liu, N. Merheb, I.-J. Wang, "Characterization of spectrum activities in the U.S. public safety band for opportunistic spectrum access", in *Proc. IEEE Int. Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Dublin, Ireland, Apr. 2007, pp. 137-146.
- [92] C. Cordeiro, K. Challapali, D. Birru, "IEEE 802.22: An introduction to the first wireless standard based on cognitive radios", *Journal of communications*, vol. 1, no. 1, Apr. 2006.
- [93] F. Benedetto, G. Giunta, E. Guzzon, M. Renfors, "Detection of Hidden Users in Cognitive Radio Networks", *24th IEEE Int. Symp. on Personal, Indoor and Mobile Radio Commun*, pp. 2296-2300, 2013.
- [94] F. F. Digham, M. S. Alouini, M. K. Simon, "On the energy detection of unknown signals over fading channels", *IEEE Trans. on Commun.*, vol. 55, no. 1, pp. 21-24, 2007.
- [95] F. Benedetto, G. Giunta, E. Guzzon, M. Renfors, "Effective Monitoring of Freeloading User in the Presence of Active User in Cognitive Radio Networks", *IEEE Trans. on Vehicular Technology*, vol. 63, no. 5, pp. 2443-2450.
- [96] Kaabouch, Naima, "Handbook of Research on Software-Defined and Cognitive Radio Technologies for Dynamic Spectrum Management". IGI Global, 2014.
- [97] I. F. Akyildiz, B. F. Lo, R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey", *Phys. Commun.*, Vol. 4, no. 1, pp. 40-62. 2011.
- [98] Wei Yang, "Energy efficient cooperative sensing in cognitive radio sensor networks", *Wireless Communications and Signal Processing (WCSP) 2014 Sixth International Conference on*, pp. 1-5, 2014.
- [99] B.F. Lo, I.F. Akyildiz, A.M. Al-Dhelaan, "Efficient recovery control channel design in cognitive radio ad hoc networks", *IEEE Transactions on Vehicular Technology*, vol. 59 no. 9 2010, pp. 4513-4526.
- [100] Y. Selen, H. Tullberg, J. Kronander, "Sensor selection for cooperative spectrum sensing", *Proc. of IEEE DySPAN*, 2008, pp. 1-11.
- [101] A. Malady, C. da Silva, "Clustering methods for distributed spectrum sensing in cognitive radio systems", in: *Proc. of IEEE MILCOM 2008*, 2008, pp. 1-5.
- [102] N. Janatian, M. M. Hashemi, S. Sun, Y. L. Guan, "Centralised cooperative spectrum sensing under correlated shadowing", in *IET Communications*, vol. 8, no. 11, pp. 1996-2007, July 24 2014.
- [103] N. Janatian, M. M. Hashemi, S. Sun and Y. L. Guan, "Centralised cooperative spectrum sensing under correlated shadowing", in *IET Communications*, vol. 8, no. 11, pp. 1996-2007, July 24 2014.
- [104] H. Lin, J. Hu, C. Huang, L. Xu, "A Secure Cooperative Spectrum Sensing Strategy for Distributed Cognitive Radio Networks", *IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, Liverpool, 2015, pp. 2198-2205.
- [105] J. Wei, C. Haixi, Y. Zhen, "Distributed cooperative spectrum sensing based on consensus among reliable secondary users", *International Conference on Wireless Communications & Signal Processing*, Nanjing, 2015, pp. 1-6.
- [106] S. A. Astaneh, S. Gazor, "Relay-assisted spectrum sensing", in *IET Communications*, vol. 8, no. 1, pp. 11-18, Jan. 3 2014.

- [107] A. El Shafie, T. Khattab, A. Sultan Salem, "Relay-Assisted Primary and Secondary Transmissions in Cognitive Radio Networks", in *IEEE Access*, vol. 4, no. , pp. 6386-6400, 2016.
- [108] Letaief, Khaled Ben, Wei Zhang. "Robust cooperative spectrum sensing for cognitive radios", U.S. Patent No. 7,965,641. 21 Jun. 2011.
- [109] S. Maleki, S. P. Chepuri and G. Leus, "Optimal hard fusion strategies for cognitive radio networks," *2011 IEEE Wireless Communications and Networking Conference*, Cancun, Quintana Roo, 2011, pp. 1926-1931.
- [110] M. Mustonen, M. Matinmikko, A. Mammela, "Cooperative spectrum sensing using quantized soft decision combining", *2009 4th International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, Hannover, 2009, pp. 1-5.
- [111] D. Teguig, B. Scheers, V. Le Nir, "Data fusion schemes for cooperative spectrum sensing in cognitive radio networks", *Communications and Information Systems Conference (MCC), 2012 Military*, Gdansk, 2012, pp. 1-7.
- [112] E. Axell, G. Leus, E. G. Larsson, H. V. Poor, "Spectrum Sensing for Cognitive Radio : State-of-the-Art and Recent Advances", in *IEEE Signal Processing Magazine*, vol. 29, no. 3, pp. 101-116, May 2012.
- [113] W. H. Chung, "Sequential Likelihood Ratio Test under Incomplete Signal Model for Spectrum Sensing", in *IEEE Transactions on Wireless Communications*, vol. 12, no. 2, pp. 494-503, February 2013.
- [114] N. Kundargi, A. Tewfik, "A performance study of novel sequential energy detection methods for spectrum sensing", in *Proc. IEEE International Conference on Acoustics Speech and Signal Processing*, pp. 3090–3093.
- [115] L. Khalid, A. Anpalagan, "Cooperative Sensing With Correlated Local Decisions in Cognitive Radio Networks", *IEEE Trans. on Vehic. Tech.*, vol. 61, no. 2, pp. 843-849, 2012.
- [116] F. Benedetto, G. Giunta, A. Tedeschi, E. Guzzon, "Performance Improvements of Cooperative Spectrum Sensing in Cognitive Radio Networks with Correlated Cognitive Users", *38th IEEE Int. Conf. on Telecommunications and Signal Processing (TSP 2015)*, 9-11 July 2015, Prague, Czech Republic , pp. 1-5.
- [117] F. Benedetto, A. Tedeschi, G. Giunta, "Cooperative Spectrum Sensing for Positioning in Cognitive Radios", *11th International Symposium on Wireless Communication Systems, ISWCS, 2014*, pp. 670-674.
- [118] Raza Umar, Asrar U.H. Sheikh, "A comparative study of spectrum awareness techniques for cognitive radio oriented wireless networks", *Physical Communication*, vol. 9, December 2013, pp. 148-170, ISSN 1874-4907.
- [119] C. Sun, Wei Zhang, K.B. Letaief, "Cooperative spectrum sensing for cognitive radios under bandwidth constraints", *Wireless Communications and Networking Conference*, 11–15 March 2007, pp. 1–5.
- [120] X. Zhou, J. Ma, G. Li, Y. Kwon, A. Soong, "Probability-based combination for cooperative spectrum sensing", *IEEE Transactions on Communications*, vol. 58, no. 2, 2010, pp. 463–466.
- [121] Trung Q. Duong, Thanh-Tan Le, Hans-Jürgen Zepernick, "Performance of cognitive radio networks with maximal ratio combining over correlated Rayleigh fading", *Third International Conference on Communications and Electronics*, pp. 65-69, 2010.
- [122] W. Xia, W. Yuan, W. Cheng, W. Liu, S. Wang, J. Xu, "Optimization of Cooperative Spectrum Sensing in Ad-Hoc Cognitive Radio Networks", *IEEE Global Telecommunications Conference*, 2010, Miami, FL, 2010, pp. 1-5.
- [123] S. Maleki, A. Pandharipande, G. Leus, "Energy-Efficient Distributed Spectrum Sensing for Cognitive Sensor Networks", in *IEEE Sensors Journal*, vol. 11, no. 3, pp. 565-573, March 2011.
- [124] A.W. Min, K.G. Shin, "Impact of mobility on spectrum sensing in cognitive radio networks", *ACM Cognitive Radio Networks*, 2009, pp. 13–18.

- [125] Y. Zhang, G. Xia, X. Creng, "Security threats in Cognitive Radio Networks", *10th IEEE International Conference on High Performance Computing and Processing*, Dalian, China, Sept.2008, pp.1036-1041.
- [126] S. Bhattacharjee, R. Rajkumari, N. Marchang. "Cognitive Radio Networks Security Threats and Attacks: A Review". *International Journal of Computer Applications, Proceedings on International Conference on Information and Communication Technologies ICICT*, no. 2, pp. 1-4, 16-19, October 2014.
- [127] A. G. Fragkiadakis, E. Z. Tragos and I. G. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks", in *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 428-445, First Quarter 2013.
- [128] A. Fragkiadakis, E. Tragos, T. Tryfonas, I. Askoxylakis, "Design and performance evaluation of a lightweight wireless early warning intrusion detection prototype", *EURASIP Journal on Wireless Communications and Networking*, to appear in 2012.
- [129] A. Cardenas, S. Radosavac, J. Baras, "Evaluation of detection algorithms for mac layer misbehavior: Theory and experiments", *IEEE/ACM Trans. Netw.*, vol. 17, pp. 605–617, 2009.
- [130] K. Ren, H. Zhu, Z. Han and R. Poovendran, "Security in cognitive radio networks", *IEEE Network*, vol. 27, no. 3, pp. 2-3, May-June 2013.
- [131] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Godor and M. Street, "Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead", in *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 355-379, Second Quarter 2012.
- [132] S. Roy, M. Conti, S. Setia, S. Jajodia, "Secure data aggregation in wireless sensor networks: Filtering out the attacker's impact", *IEEE Transactions on Information Forensics and Security*, 2014, pp. 681–694.
- [133] S. Alrabaei, M. Khasawneh, A. Agarwal, N. Goel, M. Zaman, "Towards Security Issues and Solutions in Cognitive Radio Networks", a book chapter, book name: *the Advances in Wireless Technologies and Telecommunication*, IGI Global, 2014.
- [134] S. Frankel, B. Eydt, L. Owens, K. Scarfone, 2007, *establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, NIST Special Publication 800-97.
- [135] International Telecommunication Union. "Security in Telecommunications and Information Technology. An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications".
- [136] International Telecommunication Union, "ITU-T E.408. Telecommunication networks security requirements".
- [137] Y. Zou, J. Zhu, L. Yang, Y.C. Liang, Y.D. Yao, "Securing physical-layer communications for cognitive radio networks", in *IEEE Communications Magazine*, vol. 53, no. 9, pp. 48-54, September 2015.
- [138] Q. Peng, P. C. Cosman, L. B. Milstein, "Spoofing or jamming: Performance analysis of a tactical cognitive radio adversary", *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 903–911, Apr. 2011.
- [139] A. Banerjee, S. Das, "A review on security threats in Cognitive Radio", *4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems*, Aalborg, 2014, pp. 1-5.
- [140] D. B. Rawat, B. B. Bista, Y. Gongjun, "Security, Privacy, Trust, Resource Management in Mobile and Wireless Communications". Hershey, PA, USA: IGI Global, 2013.
- [141] V. Stavroulaki et al., "Cognitive control channels: from concept to identification of implementation options", in *IEEE Communications Magazine*, vol. 50, no. 7, pp. 96-108, July 2012.
- [142] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, V. C. M. Leung, "A Survey of Security Challenges in Cognitive Radio Networks: Solutions and Future Research Directions", in *Proceedings of the IEEE*, vol. 100, no. 12, pp. 3172-3186, Dec. 2012.

- [143] D. Midi, E. Bertino, “Node or Link? Fine-Grained Analysis of Packet Loss Attacks in Wireless Sensor Networks.”. *ACM Transactions on Sensor Networks (TOSN)*, 2015.
- [144] C. Karlof, D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures”, *Ad Hoc Netw.*, vol. 1, no. 2/3, pp. 293–315, 2003.
- [145] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, “A survey of routing attacks in mobile ad hoc networks”, *IEEE Wireless Commun. Mag.*, vol. 14, no. 5, pp. 85–91, Oct. 2007.
- [146] T. Clancy, N. Goergen, “Security in Cognitive Radio Networks: Threats and Mitigation”, *Third International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, May 2008.
- [147] S. Ma *et al.*, “Detecting the greedy spectrum occupancy threat in cognitive radio networks”, *2014 IEEE International Conference on Communications (ICC)*, Sydney, NSW, 2014, pp. 4939-4944.
- [148] J. Marinho, J. Granjal, E. Monteiro, “A survey on security attacks and countermeasures with primary user detection in cognitive radio networks”, *EURASIP Journal on Information Security* 2015 (2015), no. 1, vol. 4.
- [149] R. Yu, Y. Zhang, Y. Liu, S. Gjessing and M. Guizani, “Securing cognitive radio networks against primary user emulation attacks”, in *IEEE Network*, vol. 29, no. 4, pp. 68-74, July-August 2015.
- [150] A. Mahmud, *et al.* “Physical Layer Security in Cognitive Radio Networks.” *International Conference on Artificial Intelligence, Energy and Manufacturing Engineering (ICAEME’2015)*, Dubai. 2015.
- [151] Z. Jin, S. Anand, K. P. Subbalakshmi, “Impact of Primary User Emulation Attacks on Dynamic Spectrum Access Networks”, *IEEE Trans. Commun.*, vol. 60, no. 9, 2012, pp. 2635–43.
- [152] K. Pelechrinis, M. Iliofotou, “Denial of service attacks in Wireless Networks: The case of Jammers”, *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, 2011
- [153] R. D. Pietro, G. Oligeri, “Jamming mitigation in cognitive radio networks”, in *IEEE Network*, vol. 27, no. 3, pp. 10-15, May-June 2013.
- [154] B. Wang *et al.*, “An Anti-Jamming Stochastic Game for Cognitive Radio Networks”, *IEEE JSAC*, vol. 29, no. 4, Apr. 2011, pp. 877–89.
- [155] K. Mourougayane, S. Srikanth, “Intelligent jamming threats to Cognitive Radio based strategic communication networks - A survey”, *Signal Processing, Communication and Networking (ICSCN), 2015 3rd International Conference on*, Chennai, 2015, pp. 1-6.
- [156] K. Grover, A. Lim, Q. Yang. “Jamming and anti-jamming techniques in wireless networks: a survey. *Int. J. Ad Hoc Ubiquitous Comput*, Vol. 17, no. 4, December 2014, pp. 197-215.
- [157] W. El-Hajj, H. Safa, M. Gizani, “Survey on Security Issues in Cognitive Radio Networks”, *Journal of Internet Technology*, vol. 12, no. 2, 2011
- [158] V. Balogun, A. Krings. “On the impact of jamming attacks on cooperative spectrum sensing in cognitive radio networks”. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, ACM, New York, NY, USA, pp. 1-4, 2013.
- [159] B. F. Lo, “A survey of common control channel design in cognitive radio networks”, *Physical Communication*, vol. 4, no. 1, March 2011, pp. 26-39, ISSN 1874-4907.
- [160] A. Chan, X. Liu, G. Noubir, B. Thapa, “Broadcast control channel jamming: resilience and identification of traitors”, *IEEE International Symposium on Information Theory*, 2007, pp. 2496–2500.
- [161] F. Yu, H. Tang, M. Huang, Z. Li, “Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios”, in *Proc. MILCOM*, Boston, MA, USA, Oct. 18–21, 2009, pp. 1–7.

- [162] G. Ding, Q. Wu, Y. Yao, J. Wang, Y. Chen, “Kernel-based learning for statistical signal processing in cognitive radio networks: Theoretical foundations, example applications, and future directions”, *IEEE Signal Process. Mag.*, vol. 30, no. 4, pp.126-136, 2013
- [163] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, J. Wang, “Byzantine Attack and Defense in Cognitive Radio Networks: A Survey”, *Commun. Surveys & Tuts, IEEE*, vol.17, no.3, pp.1342-1363, third quarter 2015.
- [164] O. Fatemieh, A. Farhadi, R. Chandra, C. A. Gunter, “Using classification to protect the integrity of spectrum measurements in white space networks”, *Proc. NDSS*, pp. 1-17, Feb. 2011.
- [165] O. Fatemieh, R. Chandra, C. A. Gunter, “Secure collaborative sensing for crowd sourcing spectrum data in white space networks”, *Proc. IEEE Symp. New Frontiers Dyn. Spectrum*, pp. 1-12, Apr. 2010.
- [166] S. Bhattacharjee, N. Marchang, “Attack-Resistant Trust-Based Weighted Majority Game Rule for Spectrum Sensing in Cognitive Radio Networks”. Information Systems Security, Springer International Publishing, 2015. p. 441-460.
- [167] M. Usman, I. Koo, “Secure Cooperative Spectrum Sensing for the Cognitive Radio Network Using Nonuniform Reliability”, *The Scientific World Journal*, vol. 2014, pp.1-10, 2014.
- [168] P. Kaligineedi, M. Khabbazian, V. K. Bhargava, “Secure cooperative sensing techniques for cognitive radio systems”, in *Proc. ICC*, Beijing, China, May 19–23, 2008, pp. 3406–3410.
- [169] B. Kailkhura, S. Brahma, P. Varshney, “On the performance analysis of data fusion schemes with Byzantines”, *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Florence, 2014, pp. 7411-7415.
- [170] Qiben Yan, Ming Li, T. Jiang, Wenjing Lou, Y. T. Hou, “Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks”, *INFOCOM, 2012 Proceedings IEEE*, Orlando, FL, 2012, pp. 900-908.
- [171] B. Kailkhura, Y. S. Han, S. Brahma and P. K. Varshney, “Distributed Bayesian Detection in the Presence of Byzantine Data”, in *IEEE Transactions on Signal Processing*, vol. 63, no. 19, pp. 5250-5263, Oct.1, 2015.
- [172] H. Li and Z. Han, “Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitive radio networks”, *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3554–3565, Nov. 2010.
- [173] F. Penna, Y. Sun, L. Dolecek, and D. Cabric, “Detecting and counteracting statistical attacks in cooperative spectrum sensing”, *IEEE Trans. On Signal Process.*, vol. 60, no. 4, pp. 1806–1822, Apr. 2012.
- [174] A. S. Rawat, P. Anand, H. Chen, P. K. Varshney, “Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks”, *IEEE Trans. Signal Process.*, vol. 59, no. 2, pp. 774–786, Feb. 2011.
- [175] M. Abdelhakim, L. Zhang, J. Ren, T. Li, “Cooperative sensing in cognitive networks under malicious attack”, in *Proc. IEEE ICASSP*, Prague, Czech Republic, May 22–27, 2011, pp. 3004–3007.
- [176] T. Peng, Y. Chen, J. Xiao, Y. Zheng, J. Yang, “Improved soft fusion-based cooperative spectrum sensing defense against SSDF attacks”, *2016 International Conference on Computer, Information and Telecommunication Systems*, Kunming, 2016, pp. 1-5.
- [177] Z. Qin, Q. Li, G. Hsieh, “Defending against cooperative attacks in cooperative spectrum sensing”, *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2680–2687, Jun. 2013.
- [178] J. Wang, J. Yao, Q. Wu, “Stealthy-attacker detection with a multidimensional feature vector for collaborative spectrum sensing”, *IEEE Trans. Veh. Technol.*, vol. 62, no. 8, pp. 3996–4009, Oct. 2013.
- [179] W. Wang, H. Li, Y. Sun, Z. Han, “CatchIt: detect malicious nodes in collaborative spectrum sensing”, in *Proc. GLOBECOM*, Honolulu, HI, USA, Nov. 30–Dec. 4, 2009, pp. 1–6.

- [180] S. Liu, H. Zhu, S. Li, Xu Li, C. Chen, X. Guan, “An adaptive deviation-tolerant secure scheme for distributed cooperative spectrum sensing”, in *Proc. IEEE GLOBECOM*, Anaheim, CA, USA, Dec. 3–7, 2012, pp. 603–608.
- [181] L. Khalid, A. Anpalagan, “Performance of cooperative spectrum sensing with correlated cognitive users' decisions”, in *proc. of the IEEE 22nd Int. Symp. on Personal Indoor and Mobile Radio Commun.* pp. 635-639, 2011.
- [182] R. Viswanathan, P. K. Varshney, “Distributed detection with multiple sensors I. Fundamentals”, in *Proceedings of the IEEE*, vol. 85, no. 1, pp. 54-63, Jan 1997.
- [183] W. Zhang, R. K. Mallik, K. B. Letaief, “Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks”, *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5761–5766, Dec. 2009.
- [184] M. W. Baidas, A. S. Ibrahim, K. G. Seddik, K. J. R. Liu, “On the impact of correlation on distributed detection in wireless sensor networks with relays deployment”, in *Proc. IEEE Conf. Commun.*, Jun. 2009, pp. 1–6.
- [185] E. Guzzon, F. Benedetto, G. Giunta, “A New Test for Initial Code Acquisition of Correlated Cells”, *IEEE Trans. on Vehic. Techn.*, vol. 62, no. 5, pp. 2349-2358, 2013.
- [186] F. Benedetto, G. Giunta, E. Guzzon, “Reducing mean acquisition time in code synchronization for wireless communications”, in *Proc. of the 24th Int. Symp. on Personal Indoor and Mobile Radio Commun.*, pp. 667-671, 2013.
- [187] H. Wang, Y. Xu, X. Su, J. Wang, “Cooperative spectrum sensing in cognitive radio under noise uncertainty”, in *Proc. IEEE VTC 2010*, May 2010, pp. 1-5.
- [188] H. M. Farag, E. M. Mohamed, “Hard decision cooperative spectrum sensing based on estimating the noise uncertainty factor”, Tenth International Conference on Computer Engineering & Systems (ICCES), 2015, Cairo, 2015, pp. 217-222.
- [189] R. Tandra, A. Sahai, “SNR walls for signal detection”, *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 4–17, Feb. 2008.
- [190] Y. F. Sharkasi, D. McLernon, M. Ghogho, S. Zaidi, “On spectrum sensing, secondary and primary throughput, under outage constraint with noise uncertainty and flat fading”, in *Proc. IEEE Personal Indoor and Mobile Radio Communications (PIMRC)*, London, UK, 8–11 Sep. 2013, pp. 927–931.
- [191] Y. Zeng, Y. C. Liang, “Spectrum-sensing algorithms for cognitive radio based on statistical covariances”, *IEEE Trans. Commun.*, vol. 58, no. 4, pp. 1804–1815, May 2009.
- [192] A. Kortun, T. Ratnarajah, M. Sellathurai, C. Zhong, C. B. Papadias, “On the performance of eigenvalue-based cooperative spectrum sensing for cognitive radio”, *IEEE J. Sel. Topics Signal Process.*, vol. 5, no. 1, pp. 49–55, Feb. 2011.
- [193] O. Chipara, C. Lu, T. C. Bailey, G.-C. Roman, “Reliable clinical monitoring using wireless sensor networks: experiences in a step-down hospital unit”. in *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*. New York, NY, pp. 155–168. 2010.
- [194] G. Virone, A. Wood, L. Selavo, Q. Cao, L. Fang, T. Doan, Z. He, R. Stoleru, S. Lin, J.A. Stankovic, “An advanced wireless sensor network for health monitoring”, *Transdisciplinary Conference on Distributed Diagnosis and Home Healthcare*. 2006.
- [195] P. Rawat, K. D. Singh, H. Chaouchi, J.M. Bonnin, “Wireless sensor networks: a survey on recent developments and potential synergies”, *The Journal of Supercomputing*, vol. 68, no. 1, pp. 1–48. 2014.
- [196] O. B. Akan, O. B. Karli, O. Ergul, “Cognitive radio sensor networks”, in *IEEE Network*, vol. 23, no. 4, pp. 34-40, July-August 2009.
- [197] G. A. Shah, O. B. Akan, “Cognitive Adaptive Medium Access Control in Cognitive Radio Sensor Networks”, in *IEEE Transactions on Vehicular Technology*, vol. 64, no. 2, pp. 757-767, Feb. 2015

- [198] A. O. Bicen, V. C. Gungor, O. B. Akan, "Spectrum-aware and cognitive sensor networks for smart grid applications", *IEEE Commun. Mag.*, vol. 50, no. 5, pp. 158-165, May 2012.
- [199] G. A. Shah, V. C. Gungor, O. B. Akan, "A cross-layer QoS-aware communication framework in cognitive radio sensor networks for smart grid applications", *IEEE Trans. Ind. Informat.*, vol. 9, no. 3, pp. 1477-1485, Aug. 2013.
- [200] M. Sousa, W. Lopes, F. Madeiro, M. Alencar, "Cognitive LF-Ant: A Novel Protocol for Healthcare Wireless Sensor Networks". *Sensors*, vol. 12, no. 8, pp. 10463–10486. 2012.
- [201] A. Araujo, J. Blesa, E. Romero, D. Villanueva, "Security in cognitive wireless sensor networks. challenges and open problems, EURASIP Journal on Wireless Communications and Networking", no. 1, vol. 48. 2012.
- [202] A. Fragkiadakis, V. Angelakis, E. Z. Tragos, "Securing Cognitive Wireless Sensor Networks: A Survey", *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 393248, 12 pages, 2014.
- [203] A. Francillon, C. Castelluccia, "Code injection attacks on harvard-architecture devices". In *Proceedings of the 15th ACM conference on Computer and communications security*. ACM, New York, NY, USA, pp. 15-26. 2008.
- [204] T. Giannetsos, T. Dimitriou, I. Krontiris, N. R. Prasad, "Arbitrary code injection through selfpropagating worms in von neumann architecture devices". *Comput. Journal*, vol. 53, no. 10, pp. 1576–1593. 2010.
- [205] J. Ko, C. Lu, M. B. Srivastava, J. A. Stankovic, A. Terzis, M. Welsh, "Wireless sensor networks for healthcare", *Proceedings of the IEEE*, vol. 98, no. 11, pp. 1947-1960. 2010.
- [206] H.-S. Lim, G. Ghinita, E. Bertino, M. Kantarcioglu, "A game-theoretic approach for high-assurance of data trustworthiness in sensor networks", *International Conference on Data Engineering*, pp. 1192–1203. 2012.
- [207] S. Sultana, D. Midi, E. Bertino, "Kinesis: a security incident response and prevention system for wireless sensor networks", In *Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems*. ACM, pp. 148-162. 2014.
- [208] A. S. K. Pathan, H. Lee, C. S. Hong, "Security in wireless sensor networks: issues and challenges". *The 8th International Conference on Advanced Communication Technology*. 2006.
- [209] Y. Wang, G. Attebury, B. Ramamurthy, "A survey of security issues in wireless sensor networks", *IEEE Communications Surveys and Tutorials*, vol. 8, pp. 2–23. 2007.
- [210] T. Zia, A. Zomaya, "Security issues in wireless sensor networks", in *International Conference on Systems and Networks Communications*. pp. 40. 2006.
- [211] J. R. Ning, S. Singh, K. Pelechrinis, B. Liu, S. V. Krishnamurthy, R. Govindan, "Forensic analysis of packet losses in wireless networks". *ICNP*, pp. 1-10. 2012.
- [212] S. Yang, S. Vasudevan, J. Kurose, "Witness based Witness-based Detection of Forwarding Misbehaviors in Wireless Networks". *UMass Computer Science Technical Report*. 2009.
- [213] R. Draves, J. Padhye, B. Zill, "Routing in multi-radio, multi-hop wireless mesh networks". *ACM MobiCom*, pp. 114-128. 2004.
- [214] D. D. Couto, D. Aguayo, J. Bicket, R. Morris, "A High-Throughput Path Metric for Multi-Hop Wireless Routing", *Proceedings of the 9th annual international conference on Mobile computing and networking*, pp. 134-146. 2003.
- [215] L. Qiu, P. Bahl, A. Rao, L. Zhou, "Troubleshooting wireless mesh networks". *ACM SIGCOMM Computer Communication Review*, vol. 36, no. 5, pp. 17-28. 2006.
- [216] K. N. Ramach, E. M. Belding-Royer, K. C. Almeroth, "DAMON: A distributed architecture for monitoring multi-hop mobile networks". *Proceedings of IEEE SECON*. 2004.
- [217] G. V. Záruba, M. Huber, F. Kamangar, I. Chlamtac, "Indoor location tracking using RSSI readings from a single Wi-Fi access point". *Wirel. Netw.*, vol. 13, no. 2, pp. 221--235. 2007.

- [218] A. T. Parameswaran, M. I. Husain, S. Upadhyaya, "Is RSSI a reliable parameter in Sensor Localization Algorithms: An experimental Study". *28th IEEE SRDS F2DA workshop*. 2009.
- [219] K. Srinivasan, P. Levis, "RSSI is Under Appreciated". 2006. [Online]. Available on: <https://sing.stanford.edu/pubs/rssi-emnets06.pdf>.
- [220] IEEE Standard. "Local and metropolitan area networks-- Specific requirements-- Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs)", in IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003), pp. 1-320. 2006.
- [221] T. S. Rappaport. "Wireless Communications: Principles & Practices". Prentice Hall, 1996.
- [222] A. Tedeschi, F. Benedetto, L. Paglione, "A Blind Signal Processing Method for Assessing Users' Movements in Indoor Wi-Fi Communications by Android-based Smartphones", 38th IEEE Int. Conf. on Telecommunications and Signal Processing (TSP 2015), 9-11 July 2015, Prague, Czech Republic , pp. 149-153.
- [223] CC2420, "CC2420 – Datasheet". [Online]. Available on: <http://www-mtl.mit.edu/Courses/6.111/labkit/datasheets/CC2420.pdf>.
- [224] O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, P. Levis, "Collection tree protocol". *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems*. ACM, pp. 1-14, New York, NY, USA. 2009.
- [225] Y. Chen, A. Terzis, "On the Mechanisms and Effects of Calibrating RSSI Measurements for 802.15.4 Radios". 2006. [Online]. Available on: <https://sing.stanford.edu/pubs/rssi-emnets06.pdf>.
- [226] E. Moulines, K. Choukri, "Time-domain procedures for testing that a stationary time series is Gaussian". *IEEE Trans. Signal Processing*, Volume 44, pp. 2010–2025. 1996.
- [227] L. Boithais, *Radio Wave Propagation*. New York: McGraw-Hill, 1987.
- [228] S. Kurt and B. Tavli, "Path-Loss Modeling for Wireless Sensor Networks: A review of models and comparative evaluations.," in *IEEE Antennas and Propagation Magazine*, vol. 59, no. 1, pp. 18-37, Feb. 2017.
- [229] S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among CRs," in *Proc. IEEE International Conf. Commun.*, vol. 4, pp. 1658-1663, June 2006.
- [230] L. Zhang, G. Ding, Q. Wu, F. Song, "Defending Against Byzantine Attack in Cooperative Spectrum Sensing: Defense Reference and Performance Analysis", in *IEEE Access*, vol. 4, no. , pp. 4011-4024, 2016.
- [231] F. Zhu, S.W. Seo, "Enhanced robust cooperative spectrum sensing in cognitive radio", *J. Commun. and Networks*, vol.11, no.2, pp.122-133, 2009.
- [232] R. Chen, J. M. Park, K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks", *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, Phoenix, AZ, 2008, pp.
- [233] S. Althunibat, B. J. Denise and F. Granelli, "Secure cluster-based cooperative spectrum sensing against malicious attackers", *IEEE Globecom Workshops (GC Wkshps)*, Austin, TX, 2014, pp. 1284-1289.
- [234] X. He, H. Dai, P. Ning, "A Byzantine attack defender in cognitive radio networks: The conditional frequency check", *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 2512-2523, May 2013.
- [235] K. Zeng, P. Paweczak, D. Čabrić, "Reputation-based cooperative spectrum sensing with trusted nodes assistance", *IEEE Commun Letters*, vol.14, no.3, pp.226-228, 2010.
- [236] Z. Quan, S. Cui, A. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks", *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 28–40. 2008.