Simone Soderi

EVALUATION OF INDUSTRIAL WIRELESS COMMUNICATIONS SYSTEMS’ SECURITY
SIMONE SODERI

EVALUATION OF INDUSTRIAL WIRELESS COMMUNICATIONS SYSTEMS' SECURITY

Academic dissertation to be presented with the assent of the Doctoral Training Committee of Technology and Natural Sciences of the University of Oulu for public defence in the OP auditorium (L10), Linnanmaa, on 17 June 2016, at 12 noon

UNIVERSITY OF OULU, OULU 2016
Soderi, Simone, Evaluation of industrial wireless communications systems’ security.
University of Oulu Graduate School; University of Oulu, Faculty of Information Technology and Electrical Engineering; Centre for Wireless Communications
University of Oulu, P.O. Box 8000, FI-90014 University of Oulu, Finland

Abstract

The worldwide success of wireless communications was originally fueled by the possibility to replace existing cables with wireless solutions. This phenomenon imposed the development of security engineering as a multidisciplinary field. Although wireless solutions can reduce installation costs and allow introducing new services, the end–users expect it to have the same level of security as they would normally have with wired solutions. Secure communications is an important part of the overall security of industrial wireless communications systems (IWCS).

The aim of this thesis is to develop new security engineering methodologies for IWCS. The author develops countermeasures against confidentiality and integrity attacks and carries out a security analysis covering the protocol, electromagnetic and physical layer. In the first part of the thesis, Host Identity Protocol (HIP) is utilized to secure communication in an intra–vehicular network. Simulations and measurement campaigns are also conducted to evaluate the impact of the overhead on security in a tunnel, considering line–of–sight (LOS) and non–LOS (NLOS) scenarios.

Electromagnetic analysis (EMA) is an important step in the development of safety–related systems. Today, the increasing usage of smaller integrated circuit also increases the susceptibility to electromagnetic (EM) interference. From near–field (NF) to far–field (FF) transformation, a method for the evaluation of the emissions leakage is investigated. The virtual EM (VEM) interface of the device–under–test (DUT) is studied, and it is described how an adversary can exploit it for denial of service (DoS) attacks. An effective jamming attack model is studied, and the theoretical calculations are validated with experiment–based results.

Finally, focusing attention on physical layer security, two algorithms are developed. Active radio frequency fingerprinting (RFF) implements the exchange of a public key during the setup of secure communication. Afterwards, utilizing a jamming receiver in conjunction with the spread spectrum (SS) watermarking technique, the watermark–based blind physical layer security (WBPLSec) protocol is presented. The analysis and results indicate how the WBPLSec seems to be a valuable technique for deploying physical layer security by creating a secure region around the receiver.

Keywords: EMC, emulator, far–field, fingerprinting, HIP, jamming, near–field, physical layer security, railway, safety, secrecy capacity, secure region, sniffer, spread spectrum, vehicle, watermarking, wireless, wiretap channel
Soderi, Simone, Teollisuuden langattomien tietoliikennejärjestelmien turvallisuuden arviointi.
Oulun yliopiston tutkijakoulu; Oulun yliopisto, Tieto- ja sähköteknikan tiedekunta; Centre for Wireless Communications
*Acta Univ. Oul. C 572, 2016*
Oulun yliopisto, PL 8000, 90014 Oulun yliopisto

**Tiivistelmä**


Asiakasvirivierostuomioistuin liittyy sähkömagneettisiin menetelmiin, joiden tavoitteena on analysoi tietoliikennejärjestelmien turvallisuus ja kehittää menetelmiä ja teknisiä ratkaisuja sähkömagneettiselle harmoniselle EM–liitäntä sähkömagneettisen turvallisuuden suojeluun.
To Barbara, Greta, Matteo,
Massimo, Miriam and Stefano.
Preface

The research work presented in this thesis was carried out as a part of a doctoral study program of the University of Oulu Graduate School (UniOGS), Finland, while working at GE Transportation Systems\(^1\), in Florence, Italy, during the years 2010–2015. This was possible thanks to the support of people that I wish to acknowledge below.

My journey has its roots back in 2002 when I joined the Centre for Wireless Communications (CWC), University of Oulu, Finland in order to complete my Master’s degree. I remember the first meeting at CWC with Prof. Matti Latva–aho and Dr. Matti Hämäläinen when just within a few minutes they introduced me to the ultra–wideband (UWB) world. I was surprised about their trust in a young student but I immediately understood how exciting the research community in Finland was.

I want to express my deepest gratitude to my supervisor Prof. Jari Iinatti. He gave me the opportunity to start the Doctoral studies after eight years since I obtained my M.Sc. degree. Jari was the supervisor of my Master’s thesis and now for the Doctoral thesis. If I have grown up in the research field, it is thanks to his guidance and excellent example. His high standards in research together with his teachings helped me to achieve good results. He has molded my ways to work, encouraging to look always for the best technical solution without any trade–off.

I also wish to extend my eternal gratitude to Dr. Matti Hämäläinen. After more than 10 years in the industry, without a doubt he has been my best manager. Working to achieve a Doctoral degree has its ups and downs, and doing it remotely, in some cases, could be even harder, but Matti always pointed me to the right direction in my studies and showed me how to face difficulties. Furthermore, his valuable comments improved the quality of my papers and this manuscript. My warmest thanks also go to Matti’s family for welcoming me in their home. When I was in Oulu, you always made me feel at home!

Jari, Matti, you have taught me a lot and, in addition to the professional side, I am grateful for your sincere friendship. Thanks!

I also want to thank also pre–examiners of this manuscript, Prof. Sanjay Jha, head of the Networked Systems and Security Group (NetSyS) and Director of CySPri Laboratory at the School of Computer Science and Engineering at the University of New South

\(^1\)Since November 2015, GE Transportation’s Signalling business has been sold to Alstom that now is now fully focused only on transport.
Wales, Australia, and Dr. Alberto Rabbachin, Directorate General for Communications Networks, Content & Technology (DG CONNECT) at the European Commission, for their constructive criticism that helped me to improve the quality of this work.

I am also thankful to many people at CWC, and in particular to Jani Saloranta and Harri Viittala. I spent the first part of my Doctoral studies working with them. The technical discussions and meetings held with them during the three–year joint–research project between GE and CWC taught me a lot. I will never forget the measurement campaign inside the ski–tunnel in Vuokatti for the train wireless bus. It was awesome! Our relationship has gone beyond the work. Moreover, Jani, thanks for your support to survive in the bureaucracy and also for your support \LaTeX and Mathematica. My gratitude also goes to the CWC administrative staff that assisted me.

I am grateful to Prof. Andrei Gurtov for his teaching about network security. Furthermore, I would like to thank Prof. Lorenzo Mucchi and Prof. Alessandro Piva from the University of Florence for their useful support during my research on physical layer security. Combining wireless communication with watermarking has been really fascinating. My gratitude also goes to Dr. Ian Oppermann for providing energizing words from Australia. I also wish to thank Dr. Leonardo Goratti for his useful suggestions regarding doctoral studies. However, this research would not have been possible without the funding from both GE Transportation Systems and the Tuscany Region throughout the European Commission under the 2007–2013 POR CREO FESR2 program. GE is one of the largest company worldwide with great investment in R&D and continued efforts to improve employees’ knowledge. This environment facilitated the decision to begin my doctoral studies while working. I also want to thank Mr. Mario Luigi Papini because he supported my Doctoral studies when he was my manager at GE.

Last but not least, I would like to say something to my lovely wife Barbara. We met few months before my first trip to Finland and you know how CWC and Finland are important in my life. Thank you for your understanding and support during the difficult times encountered during the studies. Thank you also to my children, Greta and Matteo, because with you my life gets better and your energy lets me forget the problems at work!

A special thanks goes to my parents Massimo and Miriam for all the things that they taught me and for their valuable support during my studies. Finally, I thank my brother Stefano because without his encouragement to leave Florence back in 2002, perhaps I would have never started this journey.

Florence, Italy April 28, 2016 Simone Soderi
List of symbols and abbreviations

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A$</td>
<td>Area of circular antenna</td>
</tr>
<tr>
<td>$a$</td>
<td>Circular antenna radius</td>
</tr>
<tr>
<td>$A_{\Sigma}$</td>
<td>Cylindrical observation curve</td>
</tr>
<tr>
<td>$C_E$</td>
<td>Channel capacity from Alice to Eve</td>
</tr>
<tr>
<td>$C_M$</td>
<td>Channel capacity from Alice to Bob</td>
</tr>
<tr>
<td>$C_s$</td>
<td>Secrecy capacity</td>
</tr>
<tr>
<td>$c_N$</td>
<td>Pseudo–noise signal</td>
</tr>
<tr>
<td>$D$</td>
<td>Maximum dimension</td>
</tr>
<tr>
<td>$\Delta E_{ch}$</td>
<td>Sniffer characterization against biconical antenna</td>
</tr>
<tr>
<td>$E$</td>
<td>Electric field</td>
</tr>
<tr>
<td>$E_1$</td>
<td>Exponential integral</td>
</tr>
<tr>
<td>$\overrightarrow{E}^{NF}$</td>
<td>Measured electric near–field</td>
</tr>
<tr>
<td>$E_{NF}^{\text{meas}}$</td>
<td>Measured electric near–field</td>
</tr>
<tr>
<td>$E_{rms}$</td>
<td>Electric field root mean square</td>
</tr>
<tr>
<td>$E_{sim}^{NF}$</td>
<td>Simulated electric near–field</td>
</tr>
<tr>
<td>$\overrightarrow{E}^{FF}$</td>
<td>Measured electric far–field</td>
</tr>
<tr>
<td>$E_J$</td>
<td>Energy of jamming signal</td>
</tr>
<tr>
<td>$E_{err}^{FF}$</td>
<td>Maximum acceptable error in far–field</td>
</tr>
<tr>
<td>$E_S$</td>
<td>Energy of $x_S$</td>
</tr>
<tr>
<td>$E_W$</td>
<td>Energy of watermark signal</td>
</tr>
<tr>
<td>$E_{\text{iJAM}}^{\text{tot}}$</td>
<td>Total Energy of iJAM</td>
</tr>
<tr>
<td>$E_{\text{WBPLSec}}^{\text{tot}}$</td>
<td>Total Energy of WBPLSec</td>
</tr>
<tr>
<td>$G_p$</td>
<td>Processing gain</td>
</tr>
<tr>
<td>$g_J$</td>
<td>Jamming channel complex Gaussian fading coefficient</td>
</tr>
<tr>
<td>$H$</td>
<td>Magnetic field</td>
</tr>
<tr>
<td>$h$</td>
<td>Height of cylindrical observation curve</td>
</tr>
<tr>
<td>$\overrightarrow{H}^{NF}$</td>
<td>Measured magnetic near–field</td>
</tr>
<tr>
<td>$\overrightarrow{H}^{FF}$</td>
<td>Measured magnetic far–field</td>
</tr>
<tr>
<td>$h_M$</td>
<td>Main channel’s complex Gaussian fading coefficients</td>
</tr>
<tr>
<td>$h_E$</td>
<td>Wiretap channel’s complex Gaussian fading coefficient</td>
</tr>
<tr>
<td>$\overrightarrow{J}_1$</td>
<td>Electric source</td>
</tr>
</tbody>
</table>
$\vec{J}_{eq}$  Electrical current density  
$k_J$  Jamming channel’s complex Gaussian fading coefficients  
$M$  Number of jammed samples  
$\vec{M}_1$  Magnetic source  
$\vec{M}_{eq}$  Magnetic current density  
$m$  Dipole moment  
$N$  Number of samples  
$N_0$  AWGN power density  
$N_W$  Watermark signal’s samples  
$n_E$  Eavesdropper channel complex zero–mean Gaussian noise  
$n_M$  Main channel complex zero–mean Gaussian noise  
$P_{out}$  Outage probability of secrecy capacity  
$P_{tx}$  Transmitter power  
$\vec{r}$  Observation point  
$\vec{r}_1$  Observation point over the imaginary surface  
$R$  Radius of cylindrical observation curve  
$R_t$  Target secrecy rate  
$S_0$  Average power density  
$S^1$  Imaginary surface  
$S(r)$  Average Poynting vector  
$T_c$  Pseudo–noise chip length  
$T_{sa}$  Host signal symbol length  
$x_J$  Jamming signal  
$x_S$  Host transmitted signal  
$(x_S^N)_N$  Alice’s transmitted signal with $N$ samples  
$(x_W^N)_W$  Source message with $N_W$ samples  
$\hat{x}_W$  Estimated embedded bit  
$w$  Spread–spectrum watermark  
$y_M$  Received signal  
$\epsilon$  Permittivity of free–space  
$\gamma_E$  Eavesdropper’s signal–to–interference–plus–noise ratio  
$\gamma_M$  Legitimate receiver’s signal–to–interference–plus–noise ratio  
$\lambda$  Wavelength  
$\mu$  Permeability of free–space
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>APTA</td>
<td>American Public Transport Agency</td>
</tr>
<tr>
<td>ARIB</td>
<td>Association of Radio Industries and Businesses</td>
</tr>
<tr>
<td>ASK</td>
<td>Amplitude Shift Keying</td>
</tr>
<tr>
<td>AWGN</td>
<td>Additive White Gaussian Noise</td>
</tr>
<tr>
<td>BEX</td>
<td>Base Exchange</td>
</tr>
<tr>
<td>BCH</td>
<td>Bose–Chaudhuri–Hocquenghem</td>
</tr>
<tr>
<td>BITS</td>
<td>Bump In The Stack</td>
</tr>
<tr>
<td>BITW</td>
<td>Bump In The Wire</td>
</tr>
<tr>
<td>BT</td>
<td>Bluetooth</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CBTC</td>
<td>Communications Based Train Control</td>
</tr>
<tr>
<td>CC</td>
<td>Common Criteria</td>
</tr>
<tr>
<td>CCA</td>
<td>Clear Channel Assessment</td>
</tr>
<tr>
<td>CCC</td>
<td>Common–control–channel</td>
</tr>
<tr>
<td>CCMP</td>
<td>Counter Mode with Cipher Block Chaining MAC Protocol</td>
</tr>
<tr>
<td>CREO</td>
<td>Competitività Regionale e Occupazione</td>
</tr>
<tr>
<td>CORE</td>
<td>Common Open Research Emulator</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off–The–Shelf</td>
</tr>
<tr>
<td>CR</td>
<td>Cognitive Radio</td>
</tr>
<tr>
<td>CRM</td>
<td>Cognitive Radio Manager</td>
</tr>
<tr>
<td>CSI</td>
<td>Channel State Information</td>
</tr>
<tr>
<td>CSM</td>
<td>Common Safety Method</td>
</tr>
<tr>
<td>CSMS</td>
<td>Cyber Security Management System</td>
</tr>
<tr>
<td>CST</td>
<td>Computer Simulation Technology</td>
</tr>
<tr>
<td>DCS</td>
<td>Data Communication System</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DSSS</td>
<td>Direct Sequence Spread Spectrum</td>
</tr>
<tr>
<td>DUT</td>
<td>Device Under Test</td>
</tr>
<tr>
<td>EAL</td>
<td>Evaluation Assurance Level</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>EM</td>
<td>Electromagnetic</td>
</tr>
<tr>
<td>EMA</td>
<td>Electromagnetic Analysis</td>
</tr>
<tr>
<td>EMANE</td>
<td>Extendable Mobile Ad–hoc Network Emulator</td>
</tr>
<tr>
<td>EMC</td>
<td>Electromagnetic Compatibility</td>
</tr>
<tr>
<td>EMI</td>
<td>Electromagnetic Interference</td>
</tr>
<tr>
<td>EMP</td>
<td>Electromagnetic Pulse</td>
</tr>
<tr>
<td>EmSec</td>
<td>Emissions Security</td>
</tr>
<tr>
<td>ERTMS</td>
<td>European Rail Traffic Management Systems</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload</td>
</tr>
<tr>
<td>ETCS</td>
<td>European Train Control System</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FDA</td>
<td>Food and Drug Administration</td>
</tr>
<tr>
<td>FF</td>
<td>Far Field</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standard</td>
</tr>
<tr>
<td>FESR</td>
<td>Fondo Europeo di Svilappo</td>
</tr>
<tr>
<td>GSM–R</td>
<td>Global System for Mobile Communications – Railway</td>
</tr>
<tr>
<td>HFSS</td>
<td>High Frequency Structural Simulator</td>
</tr>
<tr>
<td>HIP</td>
<td>Host Identity Protocol</td>
</tr>
<tr>
<td>HIT</td>
<td>Host Identity Tag</td>
</tr>
<tr>
<td>IC</td>
<td>Integrated Circuit</td>
</tr>
<tr>
<td>ICT</td>
<td>Information Communications Technology</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>ISM</td>
<td>Industrial, Scientific and Medical</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITU–R</td>
<td>International Telecommunication Union Recommendation</td>
</tr>
<tr>
<td>IWCS</td>
<td>Industrial Wireless Communication System</td>
</tr>
<tr>
<td>LOS</td>
<td>Line of Sight</td>
</tr>
<tr>
<td>LPD</td>
<td>Low Probability of Detection</td>
</tr>
<tr>
<td>LPI</td>
<td>Low Probability of Interception</td>
</tr>
<tr>
<td>LTE</td>
<td>Long Term Evolution</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MIC</td>
<td>Message Integrity Code</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>MitM</td>
<td>Man in the Middle</td>
</tr>
<tr>
<td>MoM</td>
<td>Method of Moments</td>
</tr>
<tr>
<td>MPDU</td>
<td>MAC Protocol Data Unit</td>
</tr>
<tr>
<td>NEM</td>
<td>Network Emulation Modules</td>
</tr>
<tr>
<td>NEMP</td>
<td>Nuclear Electromagnetic Pulse</td>
</tr>
<tr>
<td>NF</td>
<td>Near Field</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NLOS</td>
<td>Non Line of Sight</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>NS3</td>
<td>Network Simulator 3</td>
</tr>
<tr>
<td>OFDM</td>
<td>Orthogonal Frequency Division Multiplexing</td>
</tr>
<tr>
<td>OMNET++</td>
<td>Objective Modular Network Testbed in C++</td>
</tr>
<tr>
<td>OPNET</td>
<td>Optimum Network Performance</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>OTA</td>
<td>Over–The–Air</td>
</tr>
<tr>
<td>PARC</td>
<td>Palo Alto Research Center</td>
</tr>
<tr>
<td>PHY</td>
<td>Physical</td>
</tr>
<tr>
<td>PN</td>
<td>Pseudo–Noise</td>
</tr>
<tr>
<td>POR</td>
<td>Programma Operativo Regionale</td>
</tr>
<tr>
<td>PP</td>
<td>Protection Profiles</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre–Shared Key</td>
</tr>
<tr>
<td>RC4</td>
<td>Rivest Cipher 4</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>Research and Development</td>
</tr>
<tr>
<td>RFF</td>
<td>Radio Frequency Fingerprinting</td>
</tr>
<tr>
<td>RV</td>
<td>Random Variable</td>
</tr>
<tr>
<td>RWG</td>
<td>Rao–Wilton–Glisson</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control And Data Acquisition</td>
</tr>
<tr>
<td>SDR</td>
<td>Software Defined Radio</td>
</tr>
<tr>
<td>SFR</td>
<td>Security Functional Requirement</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
</tr>
<tr>
<td>SINR</td>
<td>Signal–to–Interference–plus–Noise Ratio</td>
</tr>
<tr>
<td>SoC</td>
<td>System on Chip</td>
</tr>
<tr>
<td>SotA</td>
<td>State–of–the–Art</td>
</tr>
<tr>
<td>SRM</td>
<td>Source Reconstruction Method</td>
</tr>
<tr>
<td>SS</td>
<td>Spread Spectrum</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>ST</td>
<td>Security Target</td>
</tr>
<tr>
<td>SWOT</td>
<td>Strengths, Weaknesses, Opportunities, Threats</td>
</tr>
<tr>
<td>TCSEC</td>
<td>Trusted Computer System Evaluation Criteria</td>
</tr>
<tr>
<td>TETRA</td>
<td>TERrestrial Trunked RAdio</td>
</tr>
<tr>
<td>TOE</td>
<td>Target of Evaluation</td>
</tr>
<tr>
<td>TOSSIM</td>
<td>Tiny Operating System Simulator</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>UWB</td>
<td>Ultra–Wideband</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>V2I</td>
<td>Vehicle to Infrastructure</td>
</tr>
<tr>
<td>V2V</td>
<td>Vehicle to Vehicle</td>
</tr>
<tr>
<td>VC</td>
<td>Vehicle Communications</td>
</tr>
<tr>
<td>VEM</td>
<td>Virtual Electromagnetic</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WBPLSec</td>
<td>Watermark Blind Physical Layer Security</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WPA</td>
<td>Wi–Fi Protected Access</td>
</tr>
<tr>
<td>WPAN</td>
<td>Wireless Personal Area Network</td>
</tr>
<tr>
<td>WSN</td>
<td>Wireless Sensors Network</td>
</tr>
</tbody>
</table>
List of original publications

This thesis is based on the following original papers, which are referred to as follows by their Roman numerals (I–VII). The publications and appendices are reproduced with permission from the publishers.


Contents

Abstract
Tīivistelmä
Preface
List of symbols and abbreviations
List of original publications
Contents
1 Introduction
   1.1 Background
   1.2 Motivation
   1.3 Author’s Contribution
   1.4 Outline of this thesis
2 State–of–the–art security solutions for industrial wireless communications systems
   2.1 Security in mainline and urban–transit railway applications
   2.2 Wireless technology in industrial applications
   2.3 Security in railway safety–related systems
      2.3.1 Protocol level
      2.3.2 Electromagnetic level
      2.3.3 Physical layer level
3 Security for IWCS a multilevel analysis
   3.1 Security threats in the TWB
   3.2 Protocol level analysis
      3.2.1 WPA2–PSK
      3.2.2 HIP
      3.2.3 Validation of intra–vehicular secure communication architecture
   3.3 EM theoretical analysis
      3.3.1 VEM interface analysis through NF–FF transformation
      3.3.2 Jamming attack model
   3.4 Physical layer security analysis
      3.4.1 WBPLSec system model and secrecy capacity
9
10
17
19
21
24
25
28
29
31
35
38
42
43
46
49
51
51
52
53
55
60
62
66
68
70
4 Summary of the Original Publications
   4.1 Protocol level contributions ........................................ 81
   4.2 Electromagnetic level contributions ............................ 82
   4.3 Physical layer contributions ....................................... 83

5 Discussions and conclusions
   5.1 Main findings ....................................................... 85
   5.2 Future work ........................................................ 87

References ................................................................. 89
Appendices ............................................................... 99
Original publications .................................................. 103
1 Introduction

“The best way to predict the future is to invent it.”
— Alan Kay
Xerox PARC, 1971

1.1 Background

Over the past years, the industrial sectors has changed even more than the digital market. More and more systems get connected to wireless networks, and it is driving technical challenges in many sectors. Wireless local area networks (WLANs) usually provide the needed connectivity in public transportation systems, automotive, healthcare and energy sectors. One of the most attractive advantage provided by the WLAN technology is replacement of cables because it provides an immediate return on the wireless investment. However, even if wireless communications provides new opportunities and support for new services, many of these systems require a high level of safety. Greater dependence on wireless technologies increases the complexity during development and exposes wireless systems to security threats. First of all, the difference between safety and security should be made clear: the first refers to avoiding physical harm to people or property, whereas the second term refers to applying defenses against malicious attacks [1, 2].

Any system that implements security needs to assure that the system works, and to also provide an evaluation of that. As long as assurance is based on processes, formal methods and technical assessments, evaluation is a process that gives the evidence that the system meets the relevant security requirements [3].

By the late 1960s, the United States Department of Defense (DoD) had created the Trusted Computer System Evaluation Criteria (TCSEC), or the Orange Book, for the evaluation of commercial products selected to store and process classified information2. Although this process took a long time, the US National Security Agency (NSA) replaced it in 1999 with the Common Criteria for Information Technology Security

2After the Second World War, the North Atlantic Treaty Organization (NATO) governments created a scheme for labeling sensitive information: Top Secret, Secret, Confidential and Unclassified, from higher to lower sensitivity [3].
Evaluation (CC) [4]. The commercial products evaluated using the TCSEC process had become mostly obsolete and thus TCSEC had also become unsuitable for the needs of most markets. Furthermore, TCSEC was very expensive.

CC [5] has been approved as an international standard (ISO/IEC 15408) [6–8] and it aims to become a global standard for the Information Technology (IT) security certification [9]. CC is more flexible than TCSEC, because rather than evaluating the whole system, the product is evaluated against protection profiles (PPs), such as operating systems, intrusion detection systems, smart cards, etc. In this process, PPs comprise several security targets (STs) that are a combination of a security objective and security functional requirements (SFRs). During the certification, the target of evaluation (TOE), i.e., the product, is rated using the evaluation assurance level (EAL) rank. EAL ranges from EAL1 to EAL7 and it does not measure the system's security but only how rigorous the verification process is. Currently the members of CC, who authorize these certificates, only consist of the 28 NATO members and some additional countries because the world has a variety of different groups that share an interest and outlook on economic events. In the past few years, cyberwarfare has been growing and CC might survive as a global certification standard only if the international security outlook is aligned with political interests [9].

By 2001, the US National Institute of Standards and Technology (NIST) had developed another evaluation criteria, known as the Federal Information Processing Standard (FIPS) publication 140–2 (FIPS 140–2) [10]. This standard defines four security levels for cryptographic modules in particular security areas, such as cryptographic module specifications, finite state machines, physical security, electromagnetic interference/ electromagnetic compatibility (EMI/EMC), etc. Each level has predefined security functions and test requirements. The FIPS certification is not permanent and any further vulnerability can lead to a module’s de-certiﬁcation. Certainly, the module can be re-certified but in the meanwhile the company seeking the certification would not have any certified products to ship.

In order to reduce certiﬁcation costs and the time needed for security evaluation, some manufacturers decided to implement modular architectures in which they can reuse modules which are already certiﬁed. In any case, security evaluations and certiﬁcations have signiﬁcantly increased due to the various terrorist and cyberattacks that have occurred in the 21st century.

By June 2010, after the identiﬁcation of Stuxnet, the security landscape changed deﬁnitively. Stuxnet is a malicious computer worm that infected supervisory control
and data acquisition (SCADA) computers at 14 industrial sites in Iran, including a uranium–enrichment plant. The Stuxnet attack comprised three phases. First, it infected Microsoft Windows machines. Then, the worm checked if the machine run the Siemens Step7 software used to program industrial control systems, such as centrifuges. Finally, Stuxnet took control over the centrifuges [11]. The lesson that Stuxnet taught to the research community, companies and governments is that malware is not only restricted to personal computers and that isolation from the Internet is not an effective defense. According to some experts, Stuxnet is the first real cyberwarfare weapon developed with immense resources and financial government backing [12]. Duqu in 2011 [13] and Flame in 2012 [11] had a similar infection and propagation mechanism (e.g., USB dongle, Bluetooth and Internet) as Stuxnet but a different purpose. Duqu and Flame were developed to steal information. After the discovery of these types of cybertools, with an estimated investment of some billions of dollars, the security scenario has changed because now hackers can use malware codes that are available online. Stuxnet is far more sophisticated than its predecessors, and thus a number of countries have decided to improve their cyberwarfare capabilities [12].

New technologies have brought prosperity and progress for populations, but in some cases they have also created new security and privacy challenges. In fact, malwares can affect the critical national infrastructure. Typically, each country has its own network of critical infrastructures, which makes it important to thoroughly analyze the network vulnerability. Since 2001, the US has established the electromagnetic pulse (EMP) Commission to assess the threat of nuclear Electromagnetic Pulse (NEMP) attacks [14]. The burst of high EM field intensities, i.e. NEMP, generated by a nuclear explosion at a high altitude could cover several million square kilometers of Earth. The nation–wide infrastructures built in the US and the European Union (EU), which are based on a network of systems controlled by computers, and the increasing use of electronics in civilian systems are highly vulnerable to NEMP attacks. Unfortunately, today the only mitigation against NEMP attacks is the agreements between countries for mutual destruction of weapons. The EMP Commission issued a report where they analyzed the impact of possible NEMP attacks on US infrastructures such as power grid, telecommunications systems, petroleum and natural gas distribution systems, transportation network, water supply system, space system and the government [15].
1.2 Motivation

In this scenario, each system could become exposed to new vulnerabilities, and therefore manufacturers must continuously develop new security capabilities. Railway and urban transit systems are typical examples of critical transportation infrastructures where the use of electronics is continuously increased.

The research for this thesis was carried out at GE Transportation Systems, located in Italy, in collaboration with the University of Oulu in Finland. The objective of this joint research project was to develop new techniques for future systems increasing railroad security. This work was co-funded by the Tuscany Region and the European Community under the 2007–2013 POR CREO FESR program.

Today, WLANs provide the needed connectivity in public transportation systems and in vehicle communication networks. This wide utilization imposed the development of security engineering as a multidisciplinary field ranging from cryptography and computer science to hardware and embedded systems [3]. The goal of this thesis is to provide a multilevel analysis of the level of security of industrial wireless communications systems and to develop solutions that manufactures could utilize during their product development. Currently, wireless technologies evolve faster than the systems where they are utilized, and, as written above, obtaining, for example, a CC or FIPS–140–2, certification for a new technology may take a long time. In addition and increasingly more frequently, new security processes have to be modified in order to quickly fix new vulnerabilities.

This thesis focuses on railway safety–related electronic equipment, but the concepts and results presented can be utilized in any industrial use case that has the similar wireless architecture. The cybersecurity threat landscape is wide and is becoming increasingly more sophisticated. Hacking a safety system, in the best case, could lead only to a fail safe state, compromising the system availability [2]. In the worst case, fatal accidents could occur to people. With reference to the open systems interconnection (OSI), the explored scenarios concerned the protocol and physical layers, but deeper investigations into the other layers were excluded from the scope of the research, although the author has always kept in mind the overall system.

Since WLANs are vulnerable to malicious attacks against standard encryption protocols, such as WPA (Wi–Fi Protected Access) and WPA2–PSK (Pre–Shared...
Key), in this thesis the host identity protocol (HIP) was utilized to secure wireless communications in public transport systems and was also compared against other protocols [16]. HIP implements end-to-end security immunes against Man in the Middle (MitM) and Denial of Service (DoS) attacks. The simulations of these protocols, presented in Paper II, were aimed to be extended and verified with measurements in order to develop a network emulator that might be used as a new tool to evaluate security solutions.

On the other hand, in addition to the OSI model, electromagnetic (EM) emissions were studied as an additional device virtual interface. These emissions could be utilized by an attacker to build particular attacks. With regard to the system EM analysis (EMA), it should be noted that an attacker could exploit EM leakage even if these emissions were lower than the radiated limits defined by the standard. In the field of EMI/EMC, the EU has issued Directive 2004/108/EC [17]. Unfortunately, the EMC requirements defined by the current standards do not cover EM attack details or their countermeasures.

Typically, security is implemented using cryptography at upper layers [18]. However, in the past few years, several techniques based on signal processing have been utilized to secure communications at the physical layer, and they have been shown to be promising methods where standalone security solution is needed. The author has focused his attention to watermarking, which is a process to hide or embed a signal into another signal [19]. Watermarking is a form of communication. In this thesis, the combination of signal watermarking and jamming was studied in order to provide an attractive solution for mobile devices with multiple air interfaces, e.g. cognitive radio, in terms of security with effective energy costs.

1.3 Author’s Contribution

Modern IWCSs use information communications technology (ICT)-based systems to control electromechanical-based systems and automate operations of industrial processes. In many industries, IWCSs interconnect different systems and security receives particular attention due to the increasing number of Internet connections of these systems. The research community investigates cyber-attacks against critical infrastructure domains where IWCSs are widely applied. Due to the systems complexity, the discussion of security attacks and related defenses is carried out at various levels, such as software, hardware and even processes. The general architecture of an IWCS
consists of layers, and for each layer different vulnerabilities can be identified as follows [20]:

- **Hardware layer**: fault injection and backdoors are attacks that an adversary can implement to gain access to stored information or to create a DoS;
- **Software/Firmware layer**: firmware includes data and instructions to control the hardware, and any malicious firmware can cause an irregular behavior of the IWCS;
- **Network layer**: quite often network devices, such as firewalls, routers, modems and access points, are not properly configured and an adversary can exploit these vulnerabilities to disrupt network communication;
- **Process layer**: in industrial systems, it is important to determine whether a variation in the system process is a consequence of an expected operation or not. An attacker can disturb the process by injecting irregular data into the system process, creating a DoS.

The author’s contribution to this dissertation can be categorized under three topics concerning the security of the system under investigation. On each topic, papers as
first-author have been published in order to highlight results achieved. Figure 1 depicts
the topics addressed in this thesis and how these are linked to the other layers as follows:

- Protocol → network layer;
- Electromagnetic → hardware layer;
- Physical Layer → firmware and software layers.

Each topic has its own dedicated section, which starts with a literature review pointing
out the most important concepts concerning the topic. These concepts are then discussed
at a more detailed level. The investigation begins from the protocol level and then moves
to the lower layers of the OSI model, including the discussion on the electromagnetic
aspects.

The protocol analysis focuses on the overhead from the utilization of security
for outdoor vehicular communication and is divided into two parts. First, the author
performed an investigation on Wi-Fi on-board vehicle networks in which an attacker
on-board the vehicle could launch an intentional attack in order to take control over
the brakes, lighting, steering, or entertainment subsystems. The author carried out a
measurement campaign where the WPA2-PSK protocol was compared against HIP in
two scenarios: line-of-sight (LOS) and non-LOS (NLOS). The author developed the
test equipment needed for the trials. Then, with the other team members, he planned and
carried out measurements inside a ski-tunnel to study the performance of the wireless
security protocol. Then the author post-processed the collected data and analyzed
the results achieved. At a later stage, the Common Open Research Emulator (CORE) [21]
with the Extendable Mobile Ad-hoc Network Emulator (EMANE) [22] framework was
modified to include the HIP protocol and then evaluated in the same scenario of the
ski-tunnel in a virtual test-bed. The results achieved by the author are presented in
Papers I and II.

In the past few years, EM analysis has increasingly been used in the filed of crypto-
analysis and emissions security (EmSec) [23]. The author developed an EMA for the
assembled safety-related systems based on near-field (NF) to far-field (FF) transforma-
tion. This thesis comprises theoretical and algorithmic contributions developed by the
author. Simulation results, as well as laboratory measurements, validated this technique
to analyze EM weaknesses starting from NF information. Furthermore, a new jamming
model was developed and utilized to improve the system design. The results achieved by
the author, are presented in Papers III and IV.

Finally, this thesis deals with physical layer security analysis, which has recently
received wide attention in the literature because, due to its nature, wireless commu-
nication might be vulnerable to eavesdropping attacks. Both theoretical analysis and experimental results support the validity of the proposed method, which for the first time combines watermarking techniques with a jamming receiver to develop a standalone physical layer security solution. The results, achieved by the author, are presented in Papers V, VI and VII.

1.4 Outline of this thesis

This thesis investigates novel security engineering techniques and particularly their application to safety–related systems utilized in railways. Chapter 2 discusses the state–of–the–art security solutions for industrial wireless communications systems (IWCS). In the chapter, different levels of the system, i.e., the protocol, EM emissions and physical layer are analyzed. The analysis follows closely the structure of this study.

Chapter 3 is devoted to a multilevel analysis of the IWCS. The first part of the chapter focuses on simulations of the protocol selected for intra–vehicular communications, such as outdoor wireless bus installed on–board trains. The simulation results are then validated with a dedicated measurement campaign. The chapter continues with an EMA of safety–related systems, with the aim of developing a novel EM model based on NF–FF transformation. At the time of writing, there was no literature describing similar techniques in which an EM leakage could be analyzed with an NF to FF model. Finally, the chapter ends with the physical layer security study. An extensive theoretical analysis is presented to support watermarking techniques to improve the physical layer security. The simulation results have validated the novel architecture that combines watermarking with jamming receiver to develop a standalone security solution. Chapter 4 provides a summary of the original papers. Chapter 5 concludes the thesis, discussing the main results achieved and possible topics for future research.

The original papers are provided in the appendices, and they are divided into three groups according to their topics; protocols (I, II), EM analysis (III, IV) and physical layer study (V–VII).
2 State–of–the–art security solutions for industrial wireless communications systems

Products in ICT store, manipulate, transmit and receive data in a digital form. Over the recent years, the amount of ICT applications has increased and now include, e.g., energy, navigation, education, medical and public transport (railway and urban–transit) solutions, as shown in Figure 2. Basically, ICT devices are utilized to combine audio–video data and communications. In particular, the ICT infrastructure continues to evolve to meet new customer’s requirements [24]. Furthermore, as we will see later on in this chapter, this technological evolution changes the wireless scenario of safety–related systems where these radios are applied. For instance, CENELEC\(^4\) defined a risk assessment process for safety–related railway systems to mitigate any possible safety issues. In particular, the standard EN50159 [25] states requirements to mitigate malicious attacks against communication systems utilized in railways. Obviously, any changes to the radio systems installed on trains drive security updates as well as reviews of previously completed assessments.

The \textit{maritime industry} is a life–critical and almost autonomous environment. ICT introduced many advantages to real–time cargo tracking, a computer–based radar system that supports ocean–going vessels, and data–centers that implement crew and passengers management applications [26]. Although ICT supports autonomous ship operations, it also creates security problems because in the worst scenario, an attacker could take control over a vessel [27].

\textit{Medical ICT} is an interesting research area for both academia and industries, and in the last years it created innovative solutions in the health–care sector that was isolated for many years. Results that combine wireless technologies and medical research are achieved by, e.g., the University of Oulu’s research units established to provide sights of future wireless health care [28]. Medical systems are safety–critical and any malfunction could damage the infrastructure or even the patients. This scenario can be attractive for hackers and regulatory authorities, such as the US Food and Drug Administration (FDA), which are investigating argumentation that support the development of safe and secure medical devices [29].

\(^4\)The organization responsible for European standardization in the area of electrical engineering.
Today, the electrical infrastructure implements smart grid solutions to create the next generation of the power distribution system. The introduction of renewable energies has imposed the utilization of ICT to enhance efficiency, reliability, and safety of the existing power grid as well as security [30]. Smart grids require a reliable communication infrastructure for monitoring real–time capacity limitations and making a rapid diagnosis in equipment failure situations. Recently, smart grid gained support from wireless sensors networks (WSNs) for collecting equipment data with built–in security since the beginning [31]. The utilization of ICT in smart grid system scenarios bring additional security concerns in this field [32], [33]. Recently, the International Electrotechnical Commission (IEC) defined in IEC 62351[34] security for communication protocols in power systems.

The research presented in this thesis was motivated by the author’s work at GE Transportation Systems. The company is one of the founders research which aims at developing new security mechanisms. The rest of the chapter gives a general overview of the common wireless communication architecture for mainline and urban–transit railways scenarios and of the role of ICT in it.
2.1 Security in mainline and urban–transit railway applications

Since the late 1800s, electric railroads are indispensable to the movement of people. Over the past years, railway operators have managed a higher traffic capacity and more stringent performance requirements without compromising the safety. Mainline and urban–transit railways are the two main railway applications and they differ in terms of both operations and structure. Mainline railway vehicles are heavier than those used in urban–transit systems, i.e., on tram and metro networks. In the case of high–speed trains, mainlines move people from city to city cities at a speed up to 500 km/h. Moreover, mainlines railways are for both passenger and freight transport. Metros and trams are slower and their typical top speed does not exceed 100 km/h [35–38].

The worldwide population growth is driving major investments in rail infrastructures. Building new inter–city rail routes and new metros are increasing the existing rail capacity, and the introduction of ICT–based train systems supports this development while also fulfilling the applicable safety requirements [25, 39, 40]. In the past years, awareness of cybersecurity has also impacted the public transport market, raising security as one of the new challenges for the rail sector. At present, the European Rail Traffic Management System (ERTMS) and the Communications Based Train Control (CBTC) are the prevailing radio-based control systems [41].

ERTMS is a European standard that enhances the interoperability of the signaling equipment on mainline railways. It is composed of the European Train Control System (ETCS) for on–board train control and a vehicle–to–infrastructure communication system implemented utilizing the Global System for Mobile Communications – Railway (GSM–R) for exchanging information with Movement Authorities. ERTMS has three operating levels and it implements a standard solution jointly created by different manufacturers at each of those levels [42].

The CBTC system makes use of RF–based data communication systems (DCSs) for train control and traffic management purposes [43]. CBTC’s DCS, includes both vehicle–to–infrastructure (V2I) and vehicle–to–vehicle (V2V) radio communications. This is a typical urban railway solution that collects information from the line and consequently adapts the train speed in order to get the shortest time interval, i.e., headway, between those [41]. Since the 1990s, CBTC increased its popularity among railway operators because the performance of these systems, with headways' values of even shorter than 60 s, allows the maximization of the railway capacity [44].

\[5\] 60 seconds is a typical headway value for CBTC.
Even though ERTMS and CBTC have different origins, both make use of DCSs, and the rapid evolution of wireless technologies and the development of secure communications are generating interesting results in railway scenario. This thesis focuses on IWCSs, which of course also include DCSs. The wayside network, e.g. the Ethernet, optical fiber and field–buses, with interlocking\(^6\) are outside the scope of this research and are thus not discussed here.

In its wider understanding, a DCS is composed of V2I and V2V, as shown in Figure 3. TErrestrial Trunked RA dio (TETRA) [45] is utilized in railway DCSs for both data and voice communication allowing group calls as well as the walkie talkie mode. Moreover, the reliability and flexibility of urban–transit systems can be improved utilizing a dedicated IP-based TETRA dispatcher able to combine multiple users to work together and meet the application needs in different situations [46]. In the context of mobile networks, GSM–R is only used for railway signaling and additional on–board Internet services are provided through the 4G UMTS Long Term Evolution (LTE), implementing load balancing and installing directional antennas on trains [47]. Recently, 5G systems have been proposed as viable fast communication means for high–speed

\(^6\)Interlocking is a control system responsible for the supervision of trains with respect to track setting and releasing railway signals [38].
trains, and novel algorithms for the implementation of a better Internet connection have been developed [48]. IEEE 802.11 is another technology with high data rates but with lower development costs than mobile networks and, when industrial, scientific and medical (ISM) bands are selected, without frequency license fees [49]. This standard is utilized in DCSs [50], [51] but also in ICT–based on–board control systems [52] and distributed Wi-Fi services inside metro trains [37].

Figure 4 shows the technological evolution of railway systems. Whereas many years ago, the safety of railway systems was dependent on electromechanical devices and isolated from the external environment, nowadays commercial off–the–shelf (COTS) devices are commonly utilized to implement railway control systems and new products are fully connected across rail networks. This scenario makes the railway market vulnerable to hackers and a fertile ground for researches to develop new and improved security mechanisms [53]. Table 1 lists some security attacks against railway systems that have occurred over the last years. Most of these attacks affected the railway traffic but as a result of the one that took place in Poland in 2008, twelve people were injured, which drove doubts about safety of railway into the public opinion.

In order to reduce costs, COTS devices, inherently insecure operating systems with vulnerable protocols, are widely adopted in railway networks. In these cases, any responsible manufacturer should provide a cybersecurity management system (CSMS) to understand the real security threats. Unfortunately, even though most of the
contracts have strong security requirements, due to the lack of adequate expertise inside the railway sector companies and the need to limit costs, most of the manufacturers tend to implement only a general security solution [58]. However, taking the security aspects into account right from the start of the design phase is a good practice that some companies have already adopted.

Over the past years, security attacks against business ICT systems have increased, and it is relatively easy to find instructions or tools to replicate these attacks. As mentioned above, in railway communications, ICT technologies such as IEEE 802.11 are utilized in DCSs but also on–board trains to remotely control programmable devices. For example, the introduction of a wireless link to a driver–machine interface (DMI) in a train can make the maintenance process simpler but, on the other hand, it could create security problems to the entire system [59], [60]. Another evolution in railway systems embraced networking devices, such as SCADA, but they make rail systems vulnerable to cyber–attacks like viruses. The impact is similar to the ones listed in Table 1, and any cyber event against a safety–related system could be catastrophic [61].

Transportation organizations have to cope with the risk of physical and cyber–attacks against their infrastructure. In Europe, several companies from the rail sector formed a consortium and implemented joint projects funded by the EU. Projects like PROTECTRAIL [62], SECUREMETRO [63] and SECRET-PROJECT [64] identify critical scenarios in railway systems and provide, providing technical specifications for prevention and crisis management. Fields investigated range from terrorist attacks by firebombs or explosives to electromagnetic attacks against rail infrastructures. In the US, the American Public Transport Agency (APTA) issued several reports to provide

<table>
<thead>
<tr>
<th>When</th>
<th>Description of the attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>August, 2003</td>
<td>A virus infected the computer systems of the international transportation company CSX Corp. in Jacksonville (Florida, US) and then disrupted train signals [54].</td>
</tr>
<tr>
<td>January, 2008</td>
<td>A Polish teenager derails four tram vehicles after hacking a train network (Lodz, Poland) [55].</td>
</tr>
<tr>
<td>March, 2010</td>
<td>A breakdown in communications affected the high–speed Airport Express Train in Oslo (Norway) and freight trains. The trains stood still nationwide for one night [56].</td>
</tr>
<tr>
<td>December, 2011</td>
<td>Hackers attacked computers at an unidentified railway company in Pacific Northwest (US), disrupting railway signals for two days [57].</td>
</tr>
</tbody>
</table>

Table 1. Security attacks against railway systems.
information and considerations about cybersecurity within the public transit enterprises [65], [66], [67], [68]. These documents are not a substitute to any security program but they do support managers and designers to become aware of the risks introduced by new technologies and the right mitigating actions against each threat.

### 2.2 Wireless technology in industrial applications

Today, wireless solutions range from cellular networks to WLANs, wireless personal area networks (WPANs), wireless body area networks (WBANs), WSNs, and also satellite communications. The first requires licensed bands, whereas the IEEE 802.11 WLAN family standard [69],[70], Bluetooth (BT) [71] and WPAN systems [72], such as IEEE 802.15.4 [73], can work in a portion of the spectrum reserved internationally for ISM purposes. ISM bands are defined by the International Telecommunication Union Radiocommunication Sector (ITU–R) and governed with some modifications by the Federal Communications Commission (FCC) in the US, by the European Telecommunications Standards Institute (ETSI) in Europe and the Association of Radio Industries and Businesses (ARIB) in Japan. Figure 5 shows an example of ISM bands between 900 MHz and 60 GHz. Unlicensed communications are permitted in ISM bands, but on the other hand, each device shall tolerate interference generated by other ISM devices [74].

The success of wireless equipment that operate in ISM bands requires analyzing the situation in terms of radio coexistence, when these technologies are selected for industrial applications. The strengths, weaknesses, opportunities and threats (SWOT) analysis is extensively used in the industry to identify internal and external factors that are favorable or unfavorable to achieve a specific function. Table 2 summarizes the SWOT analysis for utilization of wireless technologies in industrial applications and it is also briefly described below [75].

![Fig. 5. Example of ISM bands between 900 MHz and 60 GHz.](image)
Table 2. SWOT of wireless technology in industrial applications.

<table>
<thead>
<tr>
<th></th>
<th>Helpful</th>
<th>Harmful</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal Origin</strong></td>
<td><strong>Strengths</strong></td>
<td><strong>Weaknesses</strong></td>
</tr>
<tr>
<td></td>
<td>– Wireless technology standardization;</td>
<td>– Challenging for field–bus requirements;</td>
</tr>
<tr>
<td></td>
<td>– No frequency licensing;</td>
<td>– Wireless channel’s characteristics.</td>
</tr>
<tr>
<td></td>
<td>– Transient errors.</td>
<td></td>
</tr>
<tr>
<td><strong>External Origin</strong></td>
<td><strong>Opportunities</strong></td>
<td><strong>Threats</strong></td>
</tr>
<tr>
<td></td>
<td>– Cable replacement;</td>
<td>– Security;</td>
</tr>
<tr>
<td></td>
<td>– Cost and time reduction;</td>
<td>– Industrial applications are affected</td>
</tr>
<tr>
<td></td>
<td>– Plant flexibility.</td>
<td>by the wireless channel.</td>
</tr>
</tbody>
</table>

1. **Strengths**:  
   – The deployment of COTS devices in the industrial environment is driven by the general tendency towards wireless technology standardization;  
   – The industrial environment does not require any frequency licensing;  
   – Wireless channels have transient transmission errors, for example, due to fading. On the other hand, errors in wired channels can be permanent due to faults of cables.

2. **Weaknesses**  
   – Running wireless field–bus systems is challenging for real–time and reliable applications. E.g., in a wireless network, packets delivery or re–transmissions can affect real–time requirements because channel errors could cause that the packet misses the protocol’s deadlines;  
   – In the industrial environment, there are many sources of noise that can interfere the transceivers and the wireless communication. Wireless channel’s characteristics, such as pathloss and multipath, must be taken into account during the utilization of the wireless media.

3. **Opportunities**  
   – Cable replacement aims to provide an effortless field–bus implementation;  
   – Field–bus installations normally connect many devices with lots of cables in harsh environments. Connecting of devices without wires can reduce

---

Footnote: Field–bus represents the family of industrial wired computer networks standardized by IEC 61158 [76].
costs and time in terms of installation, maintenance and also plant network reconfiguration;

- Full wireless solutions and also hybrid wired/wireless field–bus implementations provide plant flexibility for new expansions, as well as connections to mobile systems.

4. Threats

- Security: the wireless medium is open and without any countermeasure against adversary attacks;
- Wireless channels can affect industrial applications or at most they can influence their design, forcing decisions at the protocol, physical layer or installation stage.

The SWOT matrix identifies security a threat to IWCSs. As a rule, adversaries exploit vulnerabilities accidentally left by manufacturers in their products. In the case of software bugs, major vendors issue periodical updates in order to fix security issues and keep up with these malicious activities. In its broad sense, hacking includes hardware and software techniques designed for creating legal or illegal access to system networks [3]. However, it is important to note that hacking could be legal when utilized during the design phase, and in some cases it provides important contributions to product research and development (R&D). There are case studies that demonstrate how a design team can expedite product development by hacking COTS devices [77]. After selecting a set of key requirements, these have been implemented through the modifications of COTS and avoiding to build any prototype with dedicated hardware and software. Moreover, if these changes do not infringe EMC or radio certifications, the manufacturers can quickly perform field trials and collect data that can be used for the final design.

Today, technology is more pervasive in our lives and security is an area that can be viewed from multidisciplinary perspectives. If, on the one hand, influence from many disciplines stimulate ground-breaking ideas, on the other hand, systems can no longer be seen as only technical machines [78]. In the same way, it is important to understand the context in which the security technology will be utilized and to learn from applications of other disciplines, because this can inspire important new insights [79]. For instance, the development of embedded products shows an imbalance between software and hardware in terms of costs, size of teams and maintenance. In particular, recently companies focused on the software and software security aspects.

This technique has been utilized in Paper I, in which the author carried out a measurement campaign to test the security protocol overhead.
Motivated by this observation, manufacturers have started to continuously improve their software processes. In this respect, we can see similarities between industrial product supply chains and the software supply chain insofar as they both try to identify security problems that are caused by poor coordination between suppliers and customers regarding security measures implemented in different systems [80].

If we can observe the multidisciplinary influence on security, we might also notice that security engineering needs cross-disciplinary expertise. The skills required today range from software, hardware and processes to economics and law. Getting protection differs from one system to another, and sometimes devices fail because designers protect wrong things. For instance, in order to mitigate failures, a framework for security engineering implementation has been developed. It consists of a policy that defines the goals in terms of security and a mechanism that includes hardware and software techniques. This framework assures an amount of effort for each mechanism, and finally, includes incentives to efficiently maintain the process. This systematic analysis has been developed to develop realistic security implementations rather than creating just a feeling of security [3].

It is important to note that changes in the environment could modify the security scenarios, invalidating solutions and, in some cases, requiring new mitigations. For instance, a wireless scenario could change as follows:
- a new node joins the wireless network;
- a third-party apparatus creates an unwanted interference;
- new radio regulations liberalize frequencies where the system emits information making the frequencies vulnerable to attacks.

Moreover, technological evolution and new radio regulations drive designers to flexibly adapt the available security techniques. Motivated by this observation, the author next investigates unconventional and innovative methods developed to improve security in IWCSs, with a particular focus on railway systems.

2.3 Security in railway safety-related systems

Public transportation systems, such as railways, require a high level of safety with complex development and testing processes. When wireless communications are selected for safety-related applications, urban-transit and mainline railways, the new technical elements should be investigated during the product design. Safety-related systems are identified as devices, consisting of hardware and software, able to prevent
dangerous situations by taking appropriate actions, i.e., safety functions, on detection of a condition which may lead to a hazardous event [81]. First of all, the difference between safety and security should be made clear: safety implements methods to avoid physical harm to people or property whereas security mitigates possible malicious attacks [1, 2]. In other events, they reduce the risk to a tolerable level. In particular, safety prevents accidents by identifying potential hazards and applying appropriate mitigations, while security prevents violations by identifying potential threats and applying appropriate controls [68]. The European Commission (EC) in its Regulation EC N.352/2009 [82] defined a Common Safety Method (CSM) on risk assessment and evaluation for railways. The CSM set out in this Regulation is an iterative risk management framework where, after the system hazard identification, the safety requirements are derived. The process ends once a tolerable risk level is achieved. In accordance to the Regulation, specific standards have to be applied to the design of safe systems. The IEC 61508 [81] requires a hazard and risk analysis in order to reduce or mitigate issues making the residual risk acceptable. This standard defines four safety integrity levels (SILs). Each level states the amount of risk reduction in order to guarantee a degree of reliability of the system. Both safety and security implement some kind of system protections, and under the risk management approach, they have to identify hazards or threats, analyze accidents or security violations and, finally, implement mitigations or controls to obtain the acceptable lower risk.

Security services included in wireless communications can be grouped in categories such as authentication, confidentiality, integrity and availability. Table 3 provides a description for each category.

Each of these services has different importance, and it depends on the context where they are applied. Figure 6 shows the different approaches to cybersecurity between the ICT business and public transportation sectors. The first sector is more concerned about confidentiality because in ICT, users do not want to share their private information such as credit card numbers or medical data. In the second sector, availability has the higher priority because in the transportation sector, rail control system, for example, needs information from wayside systems to carry out calculations and appropriately control the position of trains along the railroad [66].

For this scenario, some possible attacks are describe below as an example [83].
Table 3. Security services categories.

<table>
<thead>
<tr>
<th>Security Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Service maintains privacy and protects proprietary information between the two machines involved in the communication by implementing mathematical algorithms to transform data into a form that is not readily intelligible.</td>
</tr>
<tr>
<td>Integrity</td>
<td>Two categories of integrity service: the connection–oriented integrity service assures that messages are received as sent without duplication, insertion, modification, reordering, or replays, and the connection–less integrity service provides protection only against messages’ modifications. Moreover, it provides protections against improper information destruction.</td>
</tr>
<tr>
<td>Authentication</td>
<td>This security service is concerned with assuring that communication is authentic. At the time of connection initialization, the service assures that the two communicating entities are who they claim to be, and during the communication, it assures that the exchange of messages is not interfered by a third–party device that can masquerade itself as one of the two entities.</td>
</tr>
<tr>
<td>Availability</td>
<td>Ensuring timely and reliable access and use of correct information. This service deals with resource accessibility because resources should be accessible and usable upon demand and by an authorized party according to the system specifications relating to the performance.</td>
</tr>
</tbody>
</table>

Fig. 6. Different approaches to cybersecurity.
Confidentiality attack: Unauthorized interception of private information. This attack invades privacy but leaves the confidential data intact. Examples

- Eavesdropping: Capturing and decoding data sent over a WLAN to obtain sensitive information.
- Man in the Middle (MitM): A form of active eavesdropping. The attacker intercepts the communication between the victims and injects new messages. Each endpoint is not able to detect the intruder.

Integrity attack: Modification of data in transit over a wireless network in order to mislead the receiver or facilitate another attack. Examples include:

- Denial of Service (DoS).
- 802.11 data replay: The attacker captures, modifies and later injects 802.11 data.
- Frame injection: The attacker injects frames in the wireless communication in the transit to display malicious content on a legitimate outer web page.

Authentication attack: Stealing of users identities and credentials in order to gain access to a network. Examples include:

- WPA/WPA2–PSK cracking: The attacker could recover PSK information by running a dictionary tool attack on previously captured packets.
- Application log–in theft: Clear–text application protocols could be exploited to capture user credentials.

Availability attack: Denying legitimate users to access WLAN resources. Examples include:

- Queensland DoS: The attacker exploits the CSMA/CA Clear Channel Assessment (CCA). Using CCA–jamming, he injects an interference on the channel triggering the carrier busy state. Each node in the network is blocked.
- 802.11 beacon flood: Malicious generation of thousands of false 802.11 beacons could make it more difficult for a new user the pairing to the network mechanism.

The idea proposed in this thesis addresses countermeasures against confidentiality and integrity attacks. The author developed controls against some of these attacks and carried out a related investigation at multiple levels, i.e., at the protocol, electromagnetic and physical layer. Next, in this chapter, the author continues listing the most important technologies for each level that he selected during his research. These technologies have been selected due to their popularity in the industrial sector.
2.3.1 Protocol level

The protocol level analysis addressed the viability of IEEE 802.11 wireless technology as a mean to implement V2V, V2I, and on-board communications in a railway scenario. In Europe, CENELEC defines the related standards to assure quality, safety, and health of European citizens. The standard EN50159 deals with safety-related communications in railway transmission systems. It classifies Wi-Fi as an open communication, i.e., category 3 in EN50159, which requires a cryptographic defense in order to resist malicious attacks.

Current security protocols, such as wired equivalent privacy (WEP), WPA and WPA2-PSK, developed for Wi-Fi, provide only weak security services, and thus WLAN users are vulnerable to malicious attacks against the standard encryption protocol. Since 1997, when Wi-Fi was released, WEP has been the first widely used security protocol [84]. WEP implements Rivest Cipher 4 (RC4) cryptography with only 40-bit key length, and over the years, researchers have been able to develop effective attacks against it. Now there are publicly available tools to extract WEP keys in just a few minutes, and thus WEP cannot be considered as an effective security solution [84–86]. WPA was issued to solve the security problems of the WEP protocol. It still uses RC4 and therefore has similar cipher security issues as found in WEP. Moreover, in 2003 it was discovered that WPA is prone to dictionary brute-force attacks, and since 2004, an on-line tool for cracking the WPA protocol has been publicly available [88, 89]. WPA2 solves the cipher problems and provides user authentication and a key distribution mechanism. However, it is prone to DoS, de-authentication and de-association attacks [85]. As said above, well-known Wi-Fi security protocols have weakness and there are many contributions in literature on this topic. Things are different in businesses because environment and application scenario changes are driving different sets of attacks. Chapter 3 presents a proposal to secure a wireless communication protocol for railways.

The results presented later on in this thesis have been simulated and then compared with data collected during the measurement campaign. Simulators and emulators are both useful tools for wireless networks' development [90, 91]. A simulator behaves similarly to the original system with a completely different implementation. Models implemented to simulations are not as accurate as real implementations. Today, there are many general-purpose network simulators, of which the most popular are:

Aircrack-ng is an IEEE802.11 WEP and WPA-PSK keys' cracking program [87].
– OPNET (Optimum Network Performance) is a computer software to simulate communication networks [92];
– OMNET++ (Objective Modular Network Testbed in C++) is a discrete event simulation tool designed to simulate computer networks [93];
– TOSSIM (Tiny Operating System Simulator) simulates entire TinyOS applications [94]. TinyOS is an open source operating system for low–power wireless devices;
– NS–2 (Network Simulator 2) and NS–3 (Network Simulator 3) are discrete event network simulators [95].

However, whereas a simulator behaves similarly to the original system with a completely different implementation, an emulator reproduces exactly the system’s external behavior. Furthermore, an emulator is binary compatible with the emulated system but it works in a different environment [91].

2.3.2 Electromagnetic level

As we have seen in Table 1, due to its inherent easy access and openness, railways are attractive for security attacks [64]. Railway systems consist of much electronic equipment as well as various telecommunications, electronic control and computer networks, therefore an EM attack could cause serious issues. EM threats can act against wireless communications systems, such as WLAN, GSM–R or TETRA, preventing the link between two end–nodes, or the interference could modify information to enable or disable railway control system functions [64]. The European project SECRET aims to analyze the real risk produced by these kind of attacks and to provide suitable defenses [64]. Depending on the attacked system, i.e., an on–board train or a wayside system, consequences to people and infrastructure differ. The ERTMS standardization applied in the railway sector distributes same technology in multiple countries but the downside is that it has also a homogeneous vulnerability. In other words, any attacker can design an EM threat to a ERTMS and then apply the threat to each ERTMS installation, wherever it may be located. Again, the wide utilization of COTS, also in railway systems, increases the risks of vulnerabilities because anyone could exploit applications and frequencies available on the market to create their own attack. SECRET addresses low–level EM interference generated using a COTS jammer or home–made devices, i.e., publicly available.

The author of this thesis has addressed in his research EM emissions radiated from a railway system and has developed a new methodology to control and mitigate
weaknesses in EM devices. The investigation began with the state–of–the–art (SotA) solutions for EM emissions, defined in standards and regulations. In the field of Electromagnetic Compatibility (EMC) and Electromagnetic Immunity (EMI), the EU has issued Directive 2004/108/EC [17]. Pursuant to the Directive, there are harmonized standards for EMC for different markets, the information technology, industrial, medical and railway sectors. The EU issued the EMC Directive with the declared intention to create a single European market between the EU Member States [96]. Unfortunately, these standards do not address specific rules on EM security hazards that could occur in safety–related systems [97]. The EMC requirements refer to immunity and radiated aspects. Each apparatus should be built in order to avoid unintentional emissions exceeding the predefined limits. Moreover, the final product should be immune to both intentional and unintentional EM disturbances. In most cases, applying electronic design rules to a single board design does not guarantee compliance with the EM emissions levels. The research developed by the author at the EM level aims to improve system’s emissions security starting from the radiated emissions allowed by the EMC standards.

On the other hand, the same principle can be utilized by an attacker to detect EM weaknesses.

From the EMC point of view, there are two types of EM emissions [98]:

- **Differential mode** radiations generated by small loops, components or printed circuit traces that act as small antennas;
- **Common mode** radiations are the result of an undesired voltage difference between two points of the circuits connected to the ground. Any external cable connected to the ground acts as an antenna.

From an attacker’s point of view, EM emanations can be split into two categories [99]:

- **Direct emanations** come from active circuits where there are intentional current flows, such as short burst of currents;
- **Unintentional emanations** are due to a high integration of electronic parts and come from EM coupling of devices in proximity. Typically, these emissions are modulated signals, such as amplitude, frequency or phase modulated signals.

This thesis proposes an unconventional model to analyze radiated emission levels using a system model developed by the author. The research utilized a dedicated software tool and measurement instruments developed by the author. On the other hand, the SotA EM simulators include CST [100], ANSYS HFSS [101] and COMSOL.
RF module [102]. These are useful tools during EM design. Some of these software packages, such as CST and ANSYS, were included in the EMC analysis as well.

The difference between EM and EMC models should be clarified. EM models only consider interactions between metallic structures and EM fields. EMC models also take account of functional performance. The increasing system complexity leads to more and more elaborate EM and EMC models where specific skills are required, and quite often the finalization of the numerical results become difficult in practice [103]. Based on this observation, the author developed his own numerical model to simulate an EM field. The author’s model is based on the equivalent theorem in which the field radiation by electronic devices can be reproduced from a surface–under–test (SUT) distribution of electric and magnetic equivalent currents. To solve the equations, the Method of Moments (MoM) is used [104]. MoM is based on Rao–Wilton–Glisson (RWG) edge elements where the surface currents are represented via the so called dipole model, as shown in Figure 7 [104]. With this representation, the metallic SUT can be divided in small triangles, i.e., $T_{m}^{±}$, adjacent to the edge of length $L_{m}$ and each pair of these create a dipole moment, i.e., $m$. The DUT NF and FF can be expressed as the overall contribution of the elementary dipole shown in Figure 7, where $r_{m}^{c±}$ and $r_{m}^{c−}$ are the centre of triangles in vector notations.

Fig. 7. Dipole model interpretation (Paper III, published by permission of IEEE).
2.3.3 Physical layer level

Historically, secrecy in communications has been achieved through cryptography at upper layers of the OSI model, while recent results have identified physical layer opportunities for security design. Since 1949, Shannon developed a metric for the information theory for secrecy systems [5] and proved the perfect secrecy condition where the eavesdropper cannot pull out any information from the transmitted signal. Afterwards, the wiretap channel model introduced by Wyner assumed that a secure communication can be achieved when the eavesdropper receives a degraded version of the transmitted signal [105]. The secrecy capacity defined by Wyner is the maximum transmission rate achievable whenever the eavesdropper has a more noisy channel than the legitimate user [106]. Finally, Csiszár et al. extended Wyner’s results to non–zero secrecy capacity when a non–degraded wiretap channel is utilized [107]. Figure 8 shows a non–degraded wiretap channel model that includes a transmitter, i.e., Alice, a legitimate receiver Bob and a passive eavesdropper named Eve. This model has been used in this thesis as a baseline for the research, as described in Chapter 3.

![Fig. 8. Wireless non–degraded wiretap channel.](image)

It is important to note that the classic cryptographic approach is in contrast to the mechanism introduced by the physical layer security. Typically, cryptography security mechanism solidity is based on the rigorousness of the mathematics and how users maintain the secret keys. On the other hand, physical layer security provides secure...
communications against an eavesdropper exploiting wireless channel imperfections, such as fading, multipath and interference. An important result in the area of physical layer security is the implementation that exploits imperfect channel state information (CSI) to secure communications at the first layer of the OSI model [108].

Coding for secrecy is another way to enhance security. It provides a standalone security solution utilizing signaling models and error correction codes. Actually, a low–power sensor network is an area where physical layer security can provide awesome advantages in terms of energy cost due to the lower number of computations than required in cryptography [18]. Moreover, implementation of security at a lower level can greatly simplify the management of secret keys.

Theoretical results have also shown that the secrecy capacity can be improved by exploiting channel variations [109–111], and in particular fading fluctuations [108]. It has also been proven how adding artificial noise to information can yield significant improvements to the secrecy capacity [112].

It is well known that spread-spectrum technologies have a low probability of detection (LPD) and low probability of interception (LPI) [113], but the messages transmitted with SS techniques are still encrypted with a pseudo–noise (PN) signal to protect their secrecy. Exploiting physical layer properties of ultra–wideband (UWB), in combination with a signaling model to share a secret key can enhance the security of a cryptographic scheme [114]. Furthermore, orthogonal frequency division multiplexing (OFDM) has been proposed as effective system to secure communication between Alice and Bob over multipath fading channels [115].

Finally, the author points out that physical layer security can be implemented utilizing jamming schemes. In literature, there are several contributions that also deals with jamming because it can be used to damage wireless communications [116] or exploited as a fundamental part in original ideas for security in cooperative networks [117]. Recently, researchers have developed a powerful tool based on friendly jamming to increase the secrecy of wireless systems [118].
3 Security for IWCS a multilevel analysis

Wireless network technologies are rooted in many systems and touch several aspects of our lives. Against this context, it is becoming even more important that we are protected from security attacks. Security solutions continuously improve with new algorithms and new mathematics, but hackers normally exploit weaknesses in how these technologies are applied. This leads to a new security mindset where security experts must understand many different topics because the adversaries look for any vulnerabilities in the system [119].

The central idea of this thesis is to investigate security in the IWCS scenario. The cross-disciplinary skills required by security engineering suggested a multilevel investigation. As stated in the previous chapter, the author identified three major levels for his investigation: the protocol, electromagnetic and physical layer. This selection, which will be expanded in further research, was made based on an evaluation of the development process of an industrial product. As a general assumption, any embedded system could have wireless protocols. The system must comply with the EMC emissions standard and, in the case of new products, it should be able to implement physical layer security.

While protocol design may correlate with network security issues, IWCSs can also have physical vulnerabilities that could lead to a DoS or a reduction in the quality of communications due to a legitimate user’s traffic disruption [120]. Unfortunately, physical layer attacks, such as jamming or similar, cannot be avoided, but on the other hand, the impact of those shall be well understood. In this chapter, the author describes security controls developed throughout his research to support the security risk reduction.

When vehicular communications (VC) was developed, security played a key role in its success. Over the years, the network architecture design was further improved to control possible threats. Today, VC enables several applications, such as safety, traffic control, infotainment and driver assistance, but on the other hand, it has become vulnerable to a formidable set of abuses and attacks. Hence, without security services, VC could not be deployed to the market, otherwise there would be social risks [121]. Furthermore, the utilization of COTS in VC implementations makes secure communications even more difficult to achieve because security solutions require the
involvement of governments, academia and authorities. VC is prone to protocol and physical vulnerabilities. An attacker, even with limited powers, could steal information from protocols or chop the vehicular network with jamming. Another important aspect in service-oriented vehicular networks, such as real-time traffic, video streaming and Internet services, deals with authentication certificates management. In fact, MitM attacks can be prevented in VC systems with the utilization of public-key certificates issued by a certification authority (CA). The CA maintains the link between public-key and the user identity and is responsible for issuing and revoking certificates inside the network [122].

The scenario of a VC system can include intra-vehicular communication in long vehicles applications, which can bring benefits but also new challenges. Throughout this study, the author was involved in the development of the train wireless bus (TWB) system. This system was developed to replace wires in legacy on-board train networks using a wireless solution. The TWB implements an end-to-end wireless connection between the head and the tail of the train, exchanging both signaling data, i.e., safety-related data, and non-signaling data, such as passenger information and diagnostics data. Figure 9 depicts a TWB security scenario where the adversary is on-board a train and during the train mission he can perform various attacks against the wireless link, i.e., the protocol or the physical layer, or against an on-board unit by exploiting EM emissions.

![Train wireless bus use case](image-url)
3.1 Security threats in the TWB

The massive usage of wireless communications in industrial safety–related applications, such as the TWB in public transportation, has introduced advantages but, on the other hand, has also required carrying out network architecture analyses in order to consider security attacks. An attacker on–board the train with a high configuration laptop can intentionally perform various attacks on the TWB system and he can disturb the operation of the vehicle, if the wireless communication does not implement any countermeasures such as cryptography.

The TWB system can be very sensitive to [16]
- **Eavesdropping attacks**: Wireless intra–vehicular communication is not confined outside the vehicle, as shown in Figure 9, but it could be accessible by an adversary for eavesdropping open air messages. The attacker can steal information and then generate fake warnings into the passenger information system.
- **MitM attacks**: In a MitM attack, the adversary acts as a middle person between head–to–tail train wireless communication. He can generate and inject false messages into the TWB system and replay them until an undesirable event occurs, while the crew remains unaware of the true state of the vehicle.
- **Flooding attacks**: An attacker can generate and inject an huge amount of fake messages into the TWB consuming all the network resources. He breaks down the wireless communication, also interrupting also the safety–related signaling data and consequently emergency braking occurs.
- **Jamming attacks**: TWB electronic equipment could have EM emissions that are not confined into the locker in which the system is installed because most of the time these signaling systems are installed close to the passenger saloon. An adversary can detect the frequencies emitted by the TWB and set up a jammer to these frequencies for a more effective attack. Once the TWB is jammed, it can become unresponsive, and again emergency braking occurs.

3.2 Protocol level analysis

The TWB reflects a general security model where an information is exchanged between two parties through a communication channel. As shown in Figure 9, the adversary in the middle might create malicious attacks against security services, the categories of which, i.e., confidentiality, integrity, availability, and authentication, have been defined
in Table 3 in the previous chapter. The X.800 ITU Recommendation defines the security service as a layer in the communication system to secure data transfers [123]. Protocols adopted in the TWB must secure communication in order to mitigate malicious attacks against sensitive information, such as signaling data.

IEEE 802.11 was selected for the TWB implementation, and in Section 2.3.1, the author reviewed the StoA solutions relating to the common protocols utilized for security in standard Wi–Fi solutions. Due to some technical weaknesses of WEP, WPA and WPA2, the author decided against the utilization of these protocols for the development of a safety–related application and implemented the host identity protocol (HIP), which is based on the Internet Protocol Security (IPSec) technology. Since the above Wi–Fi security protocols have some major weaknesses and are not secure against several security attacks, these security protocols are advocated for the TWB project [16]. However, in this study, the author investigated a layered security solution that combines the WPA2–PSK and HIP protocols. The performance of this solution was evaluated adopting the protocol overhead as a metric for this comparison. The rest of the chapter first gives a summary of the overhead introduced by the chosen protocols and then continues with the results achieved from the measurements and simulations.

### 3.2.1 WPA2–PSK

As we have seen in Section 2.3.1, since 2001, the Wi–Fi Alliance have formed the IEEE 802.11i Committee to increase the MAC–layer security, and since 2004 they have included WPA2 in the standard [124]. In particular, WPA2 replaced WPA and introduced the Counter mode with Cipher Block Chaining MAC Protocol (CCMP) [69] as an enhanced encryption encapsulation mechanism based on the advanced encryption standard (AES). CCMP protects the integrity of the MAC Protocol Data Unit (MPDU) utilizing the message integrity code (MIC) section, as shown in Figure 10, and provides services for data confidentiality and authentication [69]. WPA2–PSK is typically adopted to implement a security protection at layer 2 of the OSI model. In the pre–shared mode, this protocol requires that each end–node uses a key, such as pass–phrase or hexadecimal digits, for the encryption.

Figure 10 shows that CCMP MPDU comprises five sections and the packet size overhead introduced by WPA2–PSK is 16 B, including the CCMP header and MIC.
3.2.2 HIP

Since 1999, when HIP was proposed, the protocol has been under continuous development in the IETF (Internet Engineering Task Force). Its current specifications are provided in protocol RFC5201 [125]. The most important innovation provided by HIP is the separation between the identification and localization information that normally comes with the IP–address. This property makes HIP robust against DoS attacks, supporting end–to–end encryption where IP information is bound to host identity only for routing purposes.

Indeed, HIP introduces the host identity layer in the TCP/IP stack between network and transport layers, and unlike WPA2–PSK, it implements a layer 3 tunneling solution, as shown in Figure 11.

However, Figure 12 depicts how the host identity consists of the public key component of a private–public key pair, providing a strong authentication, a feature which is useful against MitM attacks. Furthermore, with this mechanism, any user or end–node can implement multiple identities exporting this feature to the application layer.

HIP starts with the Base Exchange (BEX) stage. BEX consists of a four–way handshake in order to establish a Security Association (SA) between the initiator and the responder. Each host has to generate its Host Identity Tag (HIT) used in BEX with a one–way hash starting from a Public Key. After the SA is established, both hosts use IP Security (IPSec) Encapsulating Security Payload (ESP). When the pairing is completed, HIP uses IPSec in order to exchange data via a secure tunnel.

IPSec is a suite of protocols that uses cryptographic security services and protects communications over IP networks [126]. It provides three different implementations:

1. IPSec protocol and its capabilities are directly integrated into the IP protocol, without any extra hardware or additional layers;
2. Bump In The Stack (BITS) inserts an extra layer (i.e., IPSec) between the IP and Data–link layer with the intent to provide security for each packet;

Fig. 10. MAC Protocol Data Unit (MPDU) when using CCMP (Paper I, published by permission of IEEE).
3. Bump In The Wire (BITW) architecture adds an external device that provides IPSec services intercepting outgoing datagrams. These architectures are supported by IPSec with two basic modes of operation: the transport mode for an IPSec–integrated solution and the tunnel mode for BITS or BITW.

The author implemented HIP with IPSec in the transport mode to secure communication over the TWB. The overhead added by the HIP BEX phase with the four control packets in two round-trip times is a little less than 2 kB [125]. This amount of bytes have to be taken into account only once, when the SA is established. Then, the protocol...
packetization due to ESP security consists of fixed–size fields (i.e., 8 B + 12 B) and an ESP Tailer of a variable length (i.e., 2 B + (min 0 B, max 255 B)), as shown in Figure 13.

![IPSec: ESP transport mode](Paper I, published by permission of IEEE)

### 3.2.3 Validation of intra–vehicular secure communication architecture

The EN50159 is the specific CENELEC standard that regulates communications in safety–related electronic solutions for railway applications. TWB is a RF system that uses Wi–Fi operating at 2.4 GHz and 5.8 GHz ISM bands for its implementation. EN 50159 classifies Wi–Fi as an open communication (i.e., category 3 in [127]), requiring a cryptographic defense in order to resist malicious attacks.

The author implemented in a real system an HIP with IPSec architecture for the TWB application. Figure 14 represents the network topology and the protocol stack where each end–point is a secure zone that communicates with the other end–points through an HIP–secured channel. As shown in Paper I, thanks to the abstraction layer provided by HIP, the security is completely transparent to each device arranged as end–point.

Upon the start–up, the end–points authenticate each other by exchanging public keys, following the BEX mechanism, and then establish a secure communication channel, i.e., IPSec. With this architecture, the two security zones identified by end-points, i.e., the head and tail of the train, implement a virtual private network (VPN) and can exchange user datagram protocol (UDP) traffic safely. It must be noted that UDP data are tunneled at the Open Systems Interconnection (OSI) layer 2 and it imposes that each end–point learns the source MAC address.

Furthermore, as a security observation, the architecture selected for the TWB assumed that end–points do not have additional wireless interface that could threaten the overall system security. In any case, HIP supports multiple virtual interfaces and if a
node needed an additional secure communication we should allocate one more HIP protocol.

In this thesis, the impact of the security overhead yielded by the solution selected for the TWB in a real tunnel scenario has been studied in Paper I. A tunnel was selected due to its challenging multipath radio channel that makes it harder to achieve usable WLAN connections. A railway tunnel can be considered as a waveguide where many parameters impact the radio wave propagation. In particular, in each tunnel, the main cutoff frequency and field distribution are affected by the cross section shape and the size of the tunnel. It is also important to note that the radio channel is different when a train is loading a tunnel, thus having an impact on the field cutoff frequency, field distribution and wave propagation [128, 129]. However, at the time of the research the author had no access to a railway tunnel and so he had to selected another tunnel with a shape closer to subway tunnels, as shown in Figure 15. The measurement campaign was carried out in a ski–tunnel located in Vuokatti (Finland). The measurements were performed using a kit for each node composed of a Wi–Fi module with two antennas and an embedded PC as a controller. The embedded PC was driven by an external laptop used to run an Iperf [130] server and client. The Iperf tool was needed for communication profiling and it sent and received UDP traffic. During the field trials in Vuokatti, an open source HIP implementation (i.e., OpenHIP [131]) was used with the IPSec ESP transport mode. The transport mode was used to protect end–to–end communication [132], encrypting
only the IP payload (Figure 13). The OpenHIP ran as a software library at the user space level on a Linux PC. This library created a new virtual network tap, i.e., hip0 in Figure 14, that was used to send/receive packets with the Iperf tool [130].

During the experiments inside the tunnel, throughput, jitter and packet loss in a NLOS scenario that could happen in head–to–tail on–board wireless communication for long vehicles were measured. Figure 16 presents the results obtained using the OpenHIP in combination with WPA2–PSK at different distances. HIP and its combinations introduce an acceptable overhead in terms of mean throughput loss, jitter and packet loss up to 300 m in NLOS configurations. The acceptance criteria and the requirement for TWB in the 200 m NLOS scenario was to have at least 2 Mbps of mean throughput, jitter being less than 10 ms. This requirement was based on the type of traffic exchanged by the TWB.

Measurements showed that at 300 m, the throughput loss achieved with the combination of WPA2–PSK and OpenHIP is 54.2%, as shown in Table 4. It is also important to note that part of the loss was due to the NLOS communication. The second part of the protocol analysis deals with data post–processing and with the development of a software tool to reproduce the measurement scenarios. The increasing complexity

Fig. 15. Tunnel measurement campaign in Vuokatti, Finland.
of networks combined with services performed by WLANs, such as the TWB, need appropriate tools to get useful indications about the expected performances. In this study, the author selected a network emulator because it offers many benefits in terms of rapid network prototyping, giving also valid support to test unconventional security protocols. Then, the solution was validated against measurements over an end-to-end LOS outdoor wireless communication between two nodes.

Table 4. Throughput loss.

<table>
<thead>
<tr>
<th>Distance [m]</th>
<th>Security</th>
<th>Occurrence [kbps]</th>
<th>Loss [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>No</td>
<td>9999</td>
<td>-</td>
</tr>
<tr>
<td>300</td>
<td>WPA2-PSK + OpenHIP</td>
<td>4579</td>
<td>54.2</td>
</tr>
</tbody>
</table>

Because of the differences between emulators and simulators, already discussed in Section 2.3.1, for this thesis, the author combined CORE (Common Open Research Emulator) and EMANE (Extendable Mobile Ad–hoc Network Emulator) in a virtual test–bed for network emulations of security protocols, as shown in Paper II. CORE

10The measurement campaign was carried out near Oulu (Finland) in an open area selected in order to have LOS up to 800 m.
Fig. 17. CORE/EMANE Integrated Architecture.

(e.g.,[90], [21]) implements a virtual network stack and name-spaces for protocols and applications emulating a network layer (i.e., OSI layer 3) and upper OSI layers (i.e., transport, session, application). On the other hand, EMANE provides physical (PHY) and media-access-control (MAC) models in order to emulate OSI layers 1 and 2. As shown in Figure 17, EMANE consists of Network Emulation Modules (NEMs) connected through a bidirectional cross-layer communication to Over-The-Air (OTA) manager that emulates the multicast communications between NEMs. In the virtual test-bed, NEMs were configured to emulate TWB secure communication. Furthermore, EMANE provided a Universal PHY layer with some capabilities useful to mimic the real outdoor communication. In fact, EMANE supports pathloss calculation, received power calculation, custom antenna pattern and noise processing.

The author worked on the porting of the OpenHIP protocol into the emulator and then compared throughput, jitter and packet loss performance against outdoor measurements. Figure 18 shows the results achieved, which demonstrate that CORE/EMANE is a suitable tool to study security protocol performances. The OpenHIP porting developed by the author for the emulator introduced a slight increase of jitter caused by packet processing on the path through the network. In particular with this contribution, the author was able to validate the software developed for the emulator by utilizing the measurement campaign data.
3.3 EM theoretical analysis

As we have seen in Figure 9, the TWB consists of electric equipment installed inside rail vehicles, e.g. the head and tail of the train, with its antennas on the roof in order to provide wireless secure communication outside the train. An opponent could exploit EM leakage by intercepting information carried by EM emanations. Electronic devices emit different EM waves due to current flows within microprocessors, input–output devices and other parts. Over the last decades, EMC fields at the component level have grown significantly. The evolution of integrated circuits (ICs), even denser, have highlighted new issues regarding low–emission design techniques, high–immunity guidelines and extremely high–frequency [133]. Today, the semiconductor industry advances in several sectors, (e.g., automotive, railway and avionics) and most of the electromechanical actuators are replaced by electronic units which include power integrated system–on–chips (SoCs) drivers. Depending on the control signals, SoCs drive the power actuators generating switching noise and consequently EM emissions [134]. Even if these emissions are allowed by the relevant standards, an attacker could use the EM information radiated for his malicious purposes.

Today, radiated emissions are considered as an additional virtual interface and the EmSec’s purpose is to prevent attacks that utilize unwanted EM emanations.
Measurements performed during the EmSec analysis are closely related to the EMC aspects and RF interferences that can disrupt the system. Among the attacks against cryptoprocessor there is the technique known as Tempest, in which EM signals are monitored even when other RF signals are injected utilizing directive antennas by recording visible effects, the attacker can decode particular functions generated by victim equipment [3, 135–137]. Military organizations have many concerns regarding this issue and have invested a lot on Tempest defenses and improving shielding of sensitive equipments. Motivated by these observations, the author analyzed a generic on–board rail equipment’s emissions by developing an EM model of this device–under–test and validating the model with a measurement campaign performed in a laboratory. Furthermore, based on the radiated information achieved from the EM model, the author developed a technique to improve the system strength of a jamming attack, as shown in Papers III and IV.

Fig. 19. Block diagram of the proposed approach to analyze and attack the VEM interface (Paper IV, published by permission of Electromagnetics Academy).

In summary, as shown in Figure 19, the EM analysis was developed in two steps as follows:

1. **VEM interface analysis**: Development of an EM model to study radiated NF emissions even if these produce FF emanations that are lower than defined in the applicable standard, as presented in Section 3.3.1;
(II) **VEM interface attack**: Implementation of a jamming attack benchmarking against radiated immunity levels defined in the applicable standard, as presented in Section 3.3.2.

The VEM interface FF characteristics were developed starting from NF measurements and validated with a model developed by the author. To the best of the author’s knowledge, there is no existing solution that incorporates NF to FF transformation into emissions analysis and uses these EM leakages to improve the effectiveness of a jamming attack.

### 3.3.1 VEM interface analysis through NF–FF transformation

CENELEC produces several standards in the area of electrical engineering, including the EN 55011 [138] applied to in railways. This standard defines the acceptable radiated emissions limits generated by the railway equipment at 10 m. These limits vary in intensity from 40 dBμV/m to 47 dBμV/m between 30 MHz and 1 GHz. As we have seen in Section 2.3.2, the European EMC Directive regulates the requirements and tests for EMC within the EU. These tests are split between *full–compliance* and *pre–compliance* [17]. The former adheres to specific methods, limits and test setups. The latter utilizes the same limits but with some compromises with respect to the test setups and instruments. The method presented here is based on the evaluation of the far–field pattern measuring the near–field amplitude and it can be used to sketch the VEM interface of the DUT, as also shown in Papers III and IV. In accordance with the current EMC Directive, this can be classified as a pre–compliance test, useful for any manufactures to produce the needed documentation for the EMC assessment but also to support cybersecurity process development of the product, because EMC standards do not cover EM attacks in detail or their countermeasures. The EM field generated by the DUT, with maximum dimension $D$ and wavelength $\lambda$, can be divided into three regions from NF, i.e. the Fresnel region, to FF, i.e. the Fraunhofer region, and a gradual transition region between those, as shown in Figure 20 [139].

The DUT considered here is a rack–mounted railway system, sketched as a cube–shaped box in Figure 21. It represents only the electronic on–board equipment used in the TWB. The antenna was intentionally left out from this model because we are interested of unwanted emissions that can be exploited by an adversary on–board the train. As shown in Figure 21, the DUT’s flat metallic surfaces were approximated with only one active surface at the time known, as surface–under–test. The author formulated
the problem utilizing the Source Reconstruction Method (SRM), originally developed for antenna design [140–142]. It is based on the equivalence principle, according to which the actual electric and magnetic sources (i.e., $J_1$, $M_1$) of the DUT are replaced by their equivalent sources (i.e., electrical current density $J_{eq}$ and magnetic current density $M_{eq}$) distributed on an imaginary surface SUT, i.e., $S^1$. It represents the equivalent problem in terms of FF (i.e., $\overrightarrow{E^{FF}}$ and $\overrightarrow{H^{FF}}$) in the observation point $\overrightarrow{r}$ starting from the measured radiated NF (i.e., $\overrightarrow{E^{NF}}$ and $\overrightarrow{H^{NF}}$) when sources are in a point $\overrightarrow{r}_1$ of $S^1$.

The author implemented a modified version of the SRM depicted in Figure 22. The $\overrightarrow{E}$ and $\overrightarrow{H}$ near–fields’ amplitudes were measured with sniffers in both polarization

![Diagram](image-url)
with a cylindrical scan. In accordance with the Nyquist sampling rate in the NF–FF transformation, the NF measurements are typically performed on a discrete surface and the number of samples, \( N \), on the extended observation surface that encloses the sources is [143]

\[
N \approx \frac{A_{\Sigma}}{\left(\frac{\lambda}{2}\right)^2},
\]

where \( A_{\Sigma} = 2\pi Rh \) is the cylindrical observation curve and \( R \) and \( h \) are its radius and height, respectively. First, the electric field is measured, and after a complete cylindrical scan, its amplitude is selected along the direction of the DUT’s maximum radiated emission. Actually, the method is not utilized for radiation diagram reconstruction but for radiated emissions detection and analysis. The cost function proposed does not need any information about the phase [141, 144] and utilizes \( E_{\text{NF,meas}} \) measured to minimize the difference against the E–field simulated, i.e., \( E_{\text{NF,sim}} \), in NF via MoM varying the electrical surface currents as depicted in Figure 22. Assuming that in NF, \( \vec{E} \) and \( \vec{H} \) are independent and can be measured separately, a second block of iterations refine
the previous near E–field estimation using the near H–field independently measured with a magnetic sniffer. The process ends for NF when the maximum error constraint is verified. The achieved equivalent current distribution, i.e., \( \vec{J}_eq \), is then utilized to simulate the E–field in FF. Finally, as shown in Paper IV, this value is compensated with the sniffer characterization against biconical antenna, i.e., \( \Delta E_{ch} \), and with a maximum acceptable error in FF, i.e., \( Err_{FF} \). The algorithm used the NF peak detected information minimizing the cost function, as described above, for each peak.

![Power Near-Field E probe Vert. Polarization](image)

![E Far-Field and Peak Estimation Vert. Polarization](image)

Fig. 23. NF peak detection and FF peak estimation (Paper IV, published by permission of Electromagnetics Academy).

Figure 23 shows how the algorithm detects peaks in FF, and Table 5 lists the average error in decibels for each peak. The average error in the frequency range simulated is not higher than 0.5 dB.

**Table 5. Comparison of predicted and measured \( |E| \) in FF.**

<table>
<thead>
<tr>
<th>Number of Triangles</th>
<th>Error [dB]</th>
<th>Average Error [dB]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1st</td>
<td>2nd</td>
</tr>
<tr>
<td>16</td>
<td>0.85</td>
<td>0.1</td>
</tr>
</tbody>
</table>

65
3.3.2 Jamming attack model

Undoubtedly, jamming is a common attack against wireless networks and can produce a DoS. In Paper IV, a technique to improve the effectiveness of an electronic attack, i.e. jamming, against a safety–related system such as the train’s on–board equipment is presented. Figure 24 shows how the adversary’s primary goal is to produce a DoS attack utilizing a directional antenna. It is assumed that the attacker knows the direction of the maximum emissions, as described above in Section 3.3.1. Obviously, this method can also be utilized by any manufacturer during product development in order to improve the overall EM security of the system.

![Fig. 24. Jamming attack using a circular aperture antenna (Paper IV, published by permission of Electromagnetics Academy).](image)

Today, safety engineering concepts, such as hazard and risk assessments, have been utilized as a baseline for good EMI practices and to control EM disturbances that can affect safety–related systems [145]. Military applications suggest the usage of a safety margin on top of the immunity level. In its final draft, IEC 61000–6–7 [146], the IEC has recently issued new immunity requirements for safety related systems. This standard extends the utilization of the safety margin to safety–related systems. Basically, a safety margin of 6 dB is applied for safety–related applications, such as railway systems [147], [146]. This margin increases by a factor of 2 when the immunity level is measured in V/m.

In the case of a circular aperture antenna and carrying out simple calculations, the time average Poynting vector (average power density), at the axial observation point, is given by [148]

\[
S(r) = \frac{1}{2} \text{Re}[\mathbf{E} \times \mathbf{H}^*] = \frac{1}{2\eta}|\mathbf{E}|^2 = \frac{1}{\eta}|E_{rms}|^2 = S_0 \cdot 4 \sin^2 \left( \frac{A}{2\lambda r} \right),
\]

(2)
where $S(r)$ is expressed in $\frac{W}{m^2}$. $\eta = \sqrt{\frac{\mu}{\epsilon}}$ is the impedance of free–space, $\mu$ and $\epsilon$ are the permeability and the permittivity of free–space, respectively, $E$ and $H$ represent the peak values and $E_{\text{rms}}$ the RMS value [139], and $S_0 = \frac{P_{\text{tx}}}{A}$ is the average power density provided by the circular antenna and $A$ is its area.

Moving the adversary’s antenna closer, the rapid fluctuations in the field strength should be considered, as shown in Figure 25. It can be demonstrated that the distance from the DUT that causes the maximum error between the normalized version of $S(r)$, i.e., $\frac{S(r)}{S_0}$, and far–field trend, i.e., $\frac{\pi D^2}{8 \lambda}$, is

$$r = \frac{\pi D^2}{8 \lambda},$$

(3)

where $D = 2a$, is the circular aperture diameter.

Comparing the lower limit of the FF region depicted in Figure 20, i.e., $r < \frac{2D^2}{\lambda}$, with (3), the attacker can be moved five times closer to the DUT and he still goes on with his antenna in FF. Figure 25 shows the average of DUT power density trend against two distance conditions. In this scenario, a jamming attack at the distance indicated with (3) increases in 13 dB its power (see Appendix 1). In other words, this power increase is equivalent to the increase of the electric field, measured in V/m, by a factor of 4.5.

Fig. 25. Average DUT power density (Paper IV, published by permission of Electromagnetics Academy).
and it is *significantly higher* than the level tested with the safety margin proposed in IEC 61000–6–7.

### 3.4 Physical layer security analysis

Today, mobile devices, as well as IWCSs, are equipped with several air interfaces where the upward trend can include *multi-modality solutions* with multiple different chipsets for each apparatus or a *software defined radio (SDR)* with a flexible and re-configurable air interface implementation. In this section, the author describes his research to improve the TWB’s security by utilizing the physical layer security, as also shown in Paper V. Since the 1990s, the SDR has progressed into the cognitive radio (CR), and in the past years CRs have become very popular due to their capacity to improve spectral efficiency throughout a mechanism that sense, understand, decide and then adapt the radio to the environment. This flexibility in combination with *watermarking* inspired the development of an active *jamming receiver* for security purposes.

Although jamming can be utilized to damage wireless communications [116], the author focused his attention on jamming applications to enhance security [117], such as friendly jamming generated from third-party nodes to increase the secrecy of the wireless system [118]. Recently, a channel-independent protocol called iJAM was introduced [149]. It needs two replicas for each symbol to effectively implement a secure communication channel because the receiver randomly jams samples in the original transmission, as shown in Figure 26. In the iJAM, the receiver uses two antennas because it needs to receive and transmit simultaneously. Later, the legitimate receiver is able to get a clean signal by discarding all corrupted complementary samples in the

![Fig. 26. iJAM’s operating principle (Paper VI, published by permission of IEEE).](image-url)
original signal and its repetition. On the other hand, the eavesdropper cannot remove the interference because he does not have any information about the jamming characteristics.

Motivated by this observation, a ground-breaking full-rate watermarked blind physical layer security (WBPLSec) protocol was developed here (also presented in Papers VI and VII). The author exploited a jamming receiver with two antennas, as is done in the iJAM. In addition, the author implemented a watermarking concept to enhance system performance in terms of outage probability of the secrecy capacity, data-rate and energy cost by utilizing one spreading code between Alice and Bob in addition to a jamming receiver. We assume that Alice and Bob have perfect channel side information (CSI) about the main and jamming channels, while Eve has CSI about the wiretap channel. The WBPLSec protocol was then benchmarked against the iJAM protocol. Figure 27 shows how the iJAM effectively implements physical layer security but halves the data-rate when compared with the WBPLSec proposed in this thesis. In particular, the iJAM has to transmit twice the same symbol to get a clean signal whereas the WBPLSec does not. On the other hand, Figure 27 depicts how, in the protocol developed by the author, a watermark is added into the transmitted signal.

Fig. 27. Comparison between iJAM and WBPLSec.

Traditional communications have lots of similarities with the watermarking process that is typically utilized to hide or embed informations, e.g., pictures or videos, into another signal. In the literature, there are several contributions in which spread-spectrum watermarking techniques are utilized to implement physical layer security [150]. The author has adopted here the second paradigm for watermarking described by Cox et al.
The truly innovative process for deploying physical layer security consists of the spread–spectrum watermarking, jamming receiver, selective jamming and data decomposition method. As shown in Figure 27, the host signal transmitted by Alice embeds a message that is first modulated with a spreading sequence. The jamming receiver, i.e., Bob, jams only part of the received signal, and knowing which samples are jammed, he is able to rebuild a clean symbol. The WBPLSec transmits the information via two independent paths but implementing a data decomposition policy. With that policy, the information is sent via a narrow–band signal and a spread–spectrum signal. The transmitter embeds a SS watermark into the original modulated signal, i.e., the narrow–band signal. The watermarked narrow–band signal is partially jammed by Bob, but the SS watermark signal rejects jamming interference, after which it is utilized to re–compose the entire information.

### 3.4.1 WBPLSec system model and secrecy capacity

The WBPLSec addresses the general problem of physical layer security presented in [108], according to which any secure communications shall handle secrecy to avoid confidentiality attacks. With reference to the wiretap channel model presented in Section 2.3.3, a modified version of the non–degraded wiretap channel model [107] is implemented here. It includes the, so–called, jamming channel utilized to jam the received signal and also the eavesdropper, as shown in Figure 28. In the WBPLSec model, the jamming receiver provides secrecy and the selected watermarking technique provides the required information, which is destroyed due to the jamming.

The legitimate user, i.e., Alice, transmits \((x_S')^N\) to Bob through the main channel, which in this case is assumed to be a discrete–time Rayleigh fading channel. The source message \((x_S)^N\) of length \(N\) is encoded into the codeword \((x_S')^N\) of length \(N\). In particular, the encoder embeds the watermark \((x_W)^{NW}\) of length \(NW\) into the host signal \((x_S)^N\). In accordance with the framework presented by Cox et al. [151], the transmitter architecture implements an embedding rule defined as

\[
x_S'(i) = x_S(i) + \mu w(i),
\]

where \(x_S(i)\) is the \(i\)–th sample of the amplitude shift keying (ASK) host transmitted signal, \(\mu\) is the scaling parameter and \(w(i)\) is the direct sequence spread spectrum.
(DSSS) watermark. Over the jamming channel, assuming $N$ samples for symbol, Bob jams $M$ samples over $N$ with $M < N$, and the energy of the jamming signal is given by

$$E_J = \frac{M}{N} E_S, \quad \text{(5)}$$

where $E_S = \sum_{i=1}^{N} |x_S(i)|^2$ is the energy of $x_S$ signal. The jamming receiver implemented in the WBPLSec requires symbol synchronization between Alice and Bob. The utilization of SS techniques in the WBPLSec supports naturally symbol synchronization and the detection of symbol boundaries.

On the other hand, if the source message for the watermark $(x_W)^{N_W}$ utilizes only $N_W$ samples over $N$, with $N_W < N$, the energy of the watermark is given by

$$E_W = \frac{N_W}{N} E_S. \quad \text{(6)}$$

Fig. 28. Non–degraded wiretap channel model with a jamming receiver (Paper VI, published by permission of IEEE).
Therefore, the instantaneous signal–to–interference–plus–noise ratio (SINR) at the legitimate receiver, i.e. $\gamma_M$, and at the eavesdropper, i.e. $\gamma_E$, are given by

$$\gamma_M = \frac{|h_M|^2E_s}{N_0' + |k_J|^2E_J} = \frac{\alpha'_{tr}}{1 + \alpha'_{tr}}$$ (7)

$$\gamma_E = \frac{|h_E|^2E_s}{N_0' + |g_J|^2E_J} = \frac{\beta'_{je}}{1 + \beta'_{je}}$$ (8)

where

$$N_0' = N_0 + E'_W, \quad \gamma_{tr} = \frac{E'_S}{N_0' d^2_{tr}}, \quad \gamma_{je} = \frac{E_J}{N_0' d^2_{je}},$$

and $h_M(i)$ and $k_J(i)$ represent the main channel’s and the jamming channel’s complex Gaussian fading coefficients, $n_M(i)$ is the complex zero–mean Gaussian noise, and $x_J(i)$ denotes the jamming signal, which is generated by Bob. $h_E(i)$ is the wiretap channel’s complex Gaussian fading coefficient between Alice and Eve, $n_E(i)$ is the complex zero–mean Gaussian noise, and $g_J(i)$ is the jamming channel complex Gaussian fading coefficient\textsuperscript{11}. It is assumed that all channels are quasi–static fading channels, which means that, the channel gain coefficients remain constant during the transmission of a codeword: $h_M(i) = h_M$, $h_E(i) = h_E$, $k_J(i) = k_J$ and $g_J(i) = g_J, \forall i = 1, ..., N$. Due to the proposed jamming receiver architecture, $E_J$ does not undergo any attenuation at the legitimate receiver. Moreover, it is assumed that $n_M$ and $n_E$ have the same noise spectral density, i.e., $N_0$.

When Bob has a better channel realization than Eve, i.e., $\gamma_M > \gamma_E$, the secrecy capacity ($C_s$) of the legitimate link is defined for a non–degraded Gaussian wiretap channel [107]

$$C_s = \max\{C_M - C_E, 0\}, \quad \text{where}$$

$$C_M = \frac{1}{2} \log_2\left(1 + \gamma_M\right) \text{ bit/transmission}$$

$$C_E = \frac{1}{2} \log_2\left(1 + \gamma_E\right) \text{ bit/transmission}$$

and $C_M$ is the channel capacity from Alice to Bob, i.e., main channel, and $C_E$ is the channel capacity from Alice to Eve, i.e., wiretap channel exploited by the eavesdropper.

\textsuperscript{11}$\alpha = |h_M|^2, \ \alpha = |k_J|^2, \ \beta = |h_E|^2$ and $\tilde{\beta} = |g_J|^2$ follow an exponential distribution as shown in Appendix 2.
Otherwise, if Eve has a better SINR than Bob, $C_s$ is set to 0. In (9), the author assumed that the noise plus the interference is still Gaussian.

In the presence of Rayleigh fading, the secrecy capacity is conditioned to $h_M$, $h_E$, $k_J$, $g_J$, and without loss in generality in the rest of the paper we impose $E[h_M^2] = E[h_E^2] = 1$ and $E[k_J^2] = E[g_J^2] = 1$. [152].

The outage probability of the secrecy capacity was defined by Bloch et al. [108] as

\[ P_{\text{out}} = P[C_s < R_s] = \] 
\[ = P \left[ \frac{1}{2} \log_2 \left( \frac{1 + \gamma_M}{1 + \gamma_E} \right) < R_s \right] = \] 
\[ = P \left[ \alpha < p(1 + \tilde{\alpha} \gamma_M) + q \beta \left( \frac{1 + \tilde{\alpha} \gamma_M}{1 + \tilde{\beta} \gamma_E} \right) \right], \] 

(10)

where $R_s$ is the target secrecy rate, $p = (2^{R_s} - 1)/\gamma'_E$, and $q = (2^{R_s} \gamma_M)/\gamma'_M$. In Appendix 2, the author proves the exact formula of the outage probability ($P_{\text{out}}$) of $C_s$ for the WBPLSec and Figure 29 plots it versus $\gamma_M$ for different Eve’s positions. The eavesdropper moves along the line that connects Alice to Bob. The selected wireless propagation model takes

![Outage probability versus $\gamma_M$ when Eve moves from Bob to Alice](image-url)
account of far-field propagation [105, 153]. We considered the near-field region limit at 1 m around Alice and Bob [152] as shown in Figure 29. In other words, with this model Eve, cannot be closer than 1 m to Alice or Bob.

With this architecture, part of the information is conveyed by means of the watermarking technique, and the error probability to recover the wrong bit from the watermarked signal has been selected as a metric to measure the watermark extraction process. The author has utilized the same detector introduced with the traditional spread spectrum watermarking [154], and the estimation of the embedded bit is given by

$$\hat{x}_W = \text{sign}(\frac{\langle y_M, c_W \rangle}{\langle c_W, c_W \rangle}) = \text{sign}(r),$$  \hspace{1cm} (11)

where $y_M$ is the received signal and $c_W$ is the PN signal. Let us consider the case when $x_W = -1$. Then, an error occurs when $r > 0$ and the same error probability can be achieved when $x_W = 1$. Therefore, the total error probability is given by

$$P_e = \frac{2}{1 + \left(\frac{\sqrt{E_J}}{\sqrt{E_S}} - 1\right)},$$  \hspace{1cm} (12)

where $G_p = T_{sa}/T_c$ is the processing gain, $T_{sa}$ is the host signal symbol length, and $T_c$ is the PN chip length utilized in the watermarking SS signal. Without loss of generality we have imposed $E[h_M^2] = 1$ and $E[k_J^2] = 1$.

Figure 30 shows the error probability as a function of the ratio $E_J/E_S$ and it shows that the watermark detection is more robust for higher values of $G_p$ and $\mu$.

### 3.4.2 Energy cost

As already mentioned, physical layer techniques are promising for low-power applications where the battery life is a key driver and, for instance, on-board train systems can be included in this scenario. Comparing the WBPLSec with the iJAM protocol, the total energy consumption is given, respectively, as

$$E_{\text{tot}}^{\text{WBPLSec}} = E_S \left(1 + \frac{N_W}{N} + \frac{M}{N}\right),$$

$$E_{\text{tot}}^{\text{iJAM}} = \frac{3}{2} E_S.$$  \hspace{1cm} (13, 14)

As shown in Table 6, in the WBPLSec’s worst case, i.e., when $E_i/E_S = 1/4$ with $M = 1024$, the same system energy as with the iJAM is spent. In all other cases, the WBPLSec has lower energy consumption compared to the iJAM.
Fig. 30. Error probability for a watermark signal as a function of $\frac{E_S}{E_J}$.

Table 6. Energy Cost Comparison.

<table>
<thead>
<tr>
<th>Jammed Samples$^1$</th>
<th>Energy Consumption $E_{WBPLSec}$</th>
<th>Energy Consumption $iJAM$</th>
<th>Energy Saving</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M = 256$</td>
<td>$1.3125 \cdot E_S$</td>
<td>$1.5 \cdot E_S$</td>
<td>12.6%</td>
</tr>
<tr>
<td>$M = 512$</td>
<td>$1.375 \cdot E_S$</td>
<td>$1.5 \cdot E_S$</td>
<td>9%</td>
</tr>
<tr>
<td>$M = 1024$</td>
<td>$1.5 \cdot E_S$</td>
<td>$1.5 \cdot E_S$</td>
<td>0%$^2$</td>
</tr>
</tbody>
</table>

$^1$ $N_w = 1024$ and $N = 4096$

$^2$ Worst case for WBPLSec

3.5 Use case: cybersecurity considerations on CBTC

As mentioned in Section 2.1, CBTC typically uses V2V and V2I radio communications to collect information about the train position and consequently to adapt the train speed. On the other hand, urban–transit systems make also use of the European Train Control System as a signaling train protection system. ETCS is a state–of–the–art signaling systems and is specified at four levels. In this thesis, the author focused only on the spot transmission between train and wayside balises implemented at ETCS Level 1 and Level 2. The on–board balise transmission module (BTM) communicates with balises via an
antenna placed under the vehicle. Balises are inductive transponders installed on the railway track. When the train passes over a balise, it energizes this passive transponder throughout with a telepowering signal at 27.095 MHz. When activated, each balise sends back to the train a telegram via the up–link signal at 4.234 MHz [155].

3.5.1 CBTC security scenario

The author has already explained how railway systems require high safety levels, which increases the complexity of design and test. Safety depends on computer systems, and with the evolution of the wireless technology, railway products are fully connected throughout DCSs to each other but also to additional computer networks. Today, Wi–Fi systems based on the IEEE 802.11 standard are often selected for safety–related applications such as V2V and V2I in CBTC systems. Furthermore, CBTC systems employ ETCS radio balises to get the exact train position and then implement accurate vehicle positioning close passengers platforms. The ETCS was designed in the 1990s based on the security mechanisms available at that time and these need to be updated to face the current security threats [156]. This scenario makes the railway market vulnerable to hackers and fertile ground for researches to develop new and improved security mechanisms.

Figure 31 shows the CBTC cybersecurity scenario analyzed in this study. The author assumed two adversaries. The first jams balises close the passengers platform, whereas the second embarks the train to attack Wi–Fi based networks, such as V2V or intra–vehicular wireless communication.

3.5.2 Attack against Wi-Fi based DCSs

An adversary on–board the train can eavesdrop intra–vehicular Wi–Fi communication to obtain confidential information. For instance, an attacker can circumvent the mutual authentication and using a MitM attack, he can impersonate each end-point. For unified communications in rail systems, CENELEC EN 50159 requires cryptographic defense in order to resist these security threats. In Section 3.2.3, the author has explained how an HIP with IPSec architecture can mitigate malicious attacks against V2V/V2I and intra–vehicular Wi-Fi based communications systems. HIP protects the wireless link implementing end–point encryption, as shown in Figure 14, and if each end–node does
not have any additional communication interface it is an effective technique to secure the on–board DCS.

Table 7. Summary of potential attacks in CBTC to V2V or V2I.

<table>
<thead>
<tr>
<th>Security Threats</th>
<th>Consequences</th>
<th>Risks</th>
<th>Occurrence Likelihood</th>
<th>Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eavesdropping</td>
<td>Loss of Information</td>
<td>Medium</td>
<td>Likely</td>
<td>HIP/IPSec</td>
</tr>
<tr>
<td>MitM</td>
<td>False Information</td>
<td>High</td>
<td>Likely</td>
<td>HIP/IPSec</td>
</tr>
<tr>
<td>Flooding attack</td>
<td>DCS DoS</td>
<td>High</td>
<td>Likely</td>
<td>HIP/IPSec</td>
</tr>
</tbody>
</table>

Table 7 lists potential attacks Wi–Fi based DCSs in the CBTC system, considering the risks and the mitigations proposed, i.e., the HIP/IPSec.

### 3.5.3 Jamming attack against BTM/balises

During the coupling between the ETCS on–board system, i.e., BTM, and balises, these send to the train telegrams through the up–link signal. It is a narrow–band signal modulated by Frequency Shift Keying (FSK) with characteristics as follows:

- frequency: 4.234 MHz ± 5 kHz;
- data-rate: 564.48 kbps;
- telegram coding: Bose-Chaudhuri-Hocquenghem (BCH);
- telegram length: 341/1023 bits.

The ERTMS standard does not take jamming into consideration as a security threat that can interrupt communication between the BTM and balises [156]. The author reproduced the attack in a laboratory with a real railway equipment and one balise.

Figure 32 shows a single–tone jamming swept over 1 ms in the range of one frequency utilized by FSK modulation, i.e., the tone swept between 3.92 MHz and 3.98 MHz. We assumed that adversary without particular knowledge of the system can jam balises close the passengers platform at a metro station interfering with the train stop.

At a later stage, a single–tone jamming at 3.85 MHz was generated to perturb the balise to BTM communication and, as shown in Figure 33, this second experiment confirms the vulnerability of the ETCS to a jamming attack. Table 8 lists possible security attacks in CBTC systems against vehicular communications and balises. Furthermore, if the adversary exploited the jamming attack model described in Section 3.3.2, he could even improve the effectiveness of his attack.

The ETCS was designed in the 1990s, and based on the conducted experiments, the author proves that the system needs a reform because new risks have emerged. The author also recommends the inclusion of jamming detection and its cancellation as a valid system countermeasure against this security threat to mitigate the ETCS standard’s weaknesses.
Fig. 33. Single-tone jamming attack against a balise.

Table 8. Potential attacks in a CBTC systems against BTM/balise.

<table>
<thead>
<tr>
<th>Security Threats</th>
<th>Consequences</th>
<th>Risks</th>
<th>Occurrence Likelihood</th>
<th>Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jamming</td>
<td>Train DoS, Error in Train Stop</td>
<td>High</td>
<td>Possible</td>
<td>Real–time interference detection</td>
</tr>
</tbody>
</table>
4 Summary of the Original Publications

The thesis includes the author’s original publications as a contribution from results achieved. The common theme of this work is the security of IWCSs with particular focus on safety–related systems in railway networks. The security analysis conducted in this research was divided into three categories: the protocol (PROTO), electromagnetic (EM) and physical layer (PHY). Table 9 lists the classification of the papers in each of these categories. Furthermore, for each publication, it has been indicated what security issue is addressed in the corresponding contribution. The research methods utilized for these studies comprised theoretical analysis, simulations/emulations and, in some cases, measurement campaigns, which verified the assumptions presented.

Table 9. Analyses conducted in the original publications and mitigations developed against security attacks.

<table>
<thead>
<tr>
<th>Paper</th>
<th>Analysis Level</th>
<th>Security Mitigation for</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROTO</td>
<td>EM</td>
<td>PHY</td>
</tr>
<tr>
<td>I</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>II</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>III</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>IV</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>V</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VI</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VII</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

4.1 Protocol level contributions

Wireless communications are increasingly often selected to replace cables in on–board vehicular networks. However, the introduction of wireless interfaces to safety–related applications, such as railways, requires carrying out communication protocol analyses, and the introduction of a security layer is indispensable to implement defenses from malicious attacks. Papers I and II analyze secure intra–vehicular communication for safety–related systems at the protocol level in a railway scenario. At the time of the publications of these papers published, the author was involved with the development of the TWB. It implements an end–to–end wireless connection between the head and the
tail of the train, exchanging both signaling data, i.e., safety–related, and non–signaling
data. IEEE 802.11 was selected for the implementation of the TWB and HIP was
selected to secure the wireless communication.

Paper I describes the impact of security on the TWB in a real tunnel scenario where,
in accordance to EN50159, issued by CENELEC, security is mandatory in order to
maintain the system safety. The objective of this paper was to evaluate throughput
loss due to security for intra–vehicular (i.e., inside the same vehicle) Wi–Fi based
communication in a tunnel using COTS devices. The calculations were validated
throughout a measurement campaign that was carried out inside a sport ski–tunnel
located in Vuokatti (Finland) using COTS Wi–Fi modules. These field trials showed that
wireless security is feasible up to a few hundreds of meters in NLOS without repeaters.
Finally, the experiment presented confirms the effectiveness of HIP when used as a
standalone solution or in combination with other security solutions.

Paper II provided a comparison between an emulated TWB representation and
its outdoor implementation throughout an end–to–end WLAN outdoor link. The
measurement campaign was carried out outdoors near Oulu (Finland) using the same
COTS Wi–Fi devices utilized in Paper I. In addition, the virtual test–bed that comprises
the CORE/EMANE frameworks was selected and modified for this research. The results
indicate that the end–to–end secure wireless communication built in the emulator works
similarly to an intra–vehicular on–board network.

4.2 Electromagnetic level contributions

Today, modern vehicles are controlled using complex distributed systems with a large
number of processors and electronic components able to emit electromagnetic (EM)
waves. By exploiting unwanted emissions, an attacker, on–board the target vehicle,
could launch intentional EM attacks against an electronic on–board network system,
such as the TWB.

Motivated by this observation, another approach for studying security was presented
in Paper III, where a method based on NF to FF transformation was developed in order
to evaluate the radiated emission leakage. At the time of writing that paper, it became
clear that the solution provides a novel approach to analyzing electromagnetic issues in
the case of safety–related systems.

Paper IV extended Paper III with a detailed explanation of the system model utilized
to sketch the VEM interface of the DUT in terms of emissions amplitude, frequency and
direction. The problem formulation was based on the equivalent theorem principle, in which FF radiations of the DUT can be reproduced from a SUT distribution of electric and magnetic equivalent currents. The author also developed a MoM simulator to solve integral equations. The results indicated that it is feasible to use this methodology to analyze EM radiated emissions starting from NF information. Furthermore, the method developed here can help the product design to avoid unwanted EM leakages and to mitigate EM attacks. Finally, Paper IV takes also into account a jamming attack model and how to increase its effectiveness by utilizing a directional antenna. The solution developed analyzed the average power density of a circular aperture antenna and increased its electric field, measured in V/m, by a factor of 4.5.

4.3 Physical layer contributions

The physical layer security, introduced in Chapter 3, is based on the research results developed in Papers V, VI and VII.

In Paper V, the opportunistic behavior of a cognitive radio for providing an efficient usage of radio spectrum and an easier wireless network setup were analyzed from the security perspective. Even more frequently, CR features can be exploited to implement malicious attacks, such as DoSs. This paper introduces active radio frequency fingerprinting (RFF) as a technique to encapsulate additional data in a host wireless communication. Active RFF can have a double application scenario. CRs could encapsulate common–control–channel (CCC) information in an existing channel using active RFF and by avoiding any additional or dedicated links. On the other hand, the same technique developed here could be implemented at the physical layer inside a device in order to exchange a public key during the setup of secure communication channel. The results achieved indicated that active RFF can be a valuable part of a cognitive radio manager (CRM) framework facilitating data exchange between CRs without any dedicated channel or additional radio resources.

The initial idea to fingerprint the radio signal at the physical layer was extended in Papers VI and VII. These papers propose a watermark–based blind physical layer security (WBPLSec) protocol that utilizes a jamming receiver in conjunction with spread spectrum watermarking technique. The author was motivated by the similarities between the watermarking process for multimedia data and wireless communications and selected the right paradigm to add SS watermarking into the host signal. The theoretical analysis and simulation results indicate that the WBPLSec seems to be a
valuable technique for deploying physical layer security by creating a secure region around the receiver. The author utilized two performance metrics, the outage probability of the secrecy capacity for assessing the secure communication effectiveness and the error probability for evaluating the watermark extraction process. Finally, the proposed protocol was shown to improve the secrecy capacity performance compared to other protocols, such as the iJAM. Moreover, it also has a lower energy consumption.
5 Discussions and conclusions

5.1 Main findings

Today, security has become a very hot topic, and its multidisciplinary nature motivated the author to carry out a multilevel investigation (protocol, electromagnetic and physical layer). On each level, the author conducted a theoretical analysis, the results of which were verified simulations or measurement campaigns. This approach reinforced the research results achieved in this doctoral study. The thesis focuses on the security of IWCSs, placing the emphasis on railway safety–related systems. Due to technological advances, the application scenarios where systems are installed can change, which in turn requires also changing the system design methods. Even if during the product development the best available security solutions are implemented, we cannot assume that it will remain valid forever.

In order to provide concrete results, the TWB was selected as an applicable scenario for this research. Certainly, security is an immensely vast research area and it addresses requirements for hardware and software development processes. The author introduced the TWB in Chapter 3 and identified possible attacks in situations where an adversary is on–board the train. This thesis provides a solution for each of these pre–defined attacks. On the other hand, this work could be extended in the future by taking into account other scenarios as well. The state–of–the–art review, provided in Chapter 2, highlighted the need to conduct further security investigations on public transport systems, such as railway and urban–transit networks, because these systems can be vulnerable to malicious attacks. Figure 34 shows the security mitigations implemented for the TWB. These were further discussed in Chapter 3. The HIP with IPSec architecture was introduced as a promising protocol for intra–vehicular communications, such as the TWB application. This security solution would mitigate attacks against the wireless on–board network that can come from an attacker boarded on the same vehicle. Furthermore, the security architecture proposed maintains the separation between the security technology and the radio selected, and it is useful in railway projects where very often the wireless technology is imposed based on the customer needs. The author tested the HIP solution in a NLOS scenario that can occur in head–to–tail on–board wireless communication for long vehicles. The experiment was implemented through a measurement campaign carried out inside a ski–tunnel. The results have shown that HIP
Fig. 34. TWB security mitigations developed in this thesis.

introduces an acceptable overhead in terms of throughput loss, jitter and packet loss up to 300 m. In the second experiment, the HIP architecture was emulated utilizing the CORE and EMANE frameworks proposed as a virtual test–bed, and its performance was compared with a real outdoor end–to–end LOS scenario. This experiment demonstrated the reliability of CORE/EMANE as an important tool to develop security without any additional measurement campaign. One limitation of the aforementioned technique is that the results, in terms of simulations and the measurements campaign, are valid for Wi–Fi because the TWB utilizes IEEE 802.11. Furthermore, as shown in Figure 11, HIP implements a layer 3 tunneling solution. The author expects the results to be similar with the same technologies but in the different application scenario, such as point–to–point wireless communications.

In Chapter 3, the author first developed an innovative use of NF to FF transformation to describe emissions of a railway on–board equipment. Characteristics of these emissions, such as frequencies and direction, assemble the VEM interface of the DUT, and they can be exploited by an adversary to plan a jamming attack. The proposed theoretical approach is based on the SRM method and was verified with an EM MoM simulator developed by the author. A measurement campaign was carried out to validate the numerical results in a laboratory. The algorithm represents a useful tool for the design and post–installation phases in order to identify EM emissions leakage. Knowledge of the EM vulnerabilities will drive new processes to improve emissions security for safety–related apparatus. Furthermore, the EM analysis continued with the development of a method to improve the effectiveness of the jamming model proposed. In particular, an attacker with limited resources might exploit VEM interface characteristics by
increasing the signal power by up to 13 dB when he moves along the maximum radiated emission direction, five times closer to the victim. The attack can be deemed efficient against safety–related systems even if these are tested utilizing a safety margin on top of the radiated immunity levels. The jamming model can be used to test the DUT by exploiting the frequencies detected by the algorithm and to improve the system design. Whereas the NF to FF technique is always valid, the results achieved with the jamming attack model sound only when a circular aperture antenna is utilized.

Finally, the author tackled the physical layer security by developing the WBPLSec, the combat information disclosure attacks, such as eavesdropping. Both the theoretical analysis and the simulation results proved the validity of the proposed method, which for the first time combines watermarking techniques with a jamming receiver to develop a standalone physical layer security solution. Furthermore, the combination of signal watermarking and jamming provides an attractive solution for mobile devices with multiple air interfaces, cognitive radios, in terms of security with effective energy cost. In terms of realism, the WBPLSec is a trade–off between security and communication reliability because for a fixed symbol energy, $E_S$, increasing the jamming energy, $E_J$, a wider security area is achieved with a lower $P_{out}$. On the other hand, when $E_J$ increases, the watermark extraction is getting worse with higher $P_e$. The WBPLSec offers some advantages when compared with the iJAM because it is a full–rate protocol, it has a better $P_{out}$ and a lower energy consumption. On the other hand, one spreading code is utilized to implement the SS watermarking. The wide utilization of SS communications in these days makes the sharing of one PN code acceptable for this implementation. The WBPLSec shares the same information in terms of spreading code when compared with SS communication. The WBPLSec deals with one limitation, namely this protocol requires symbol synchronization. However, the assumption is reasonable for SS techniques that support naturally the detection of symbol boundaries.

5.2 Future work

The aim of this thesis was to investigate cybersecurity in IWCSs with a particular focus on safety–related systems. The author discussed the development of new methodologies for security engineering from multiple perspectives, i.e., from the viewpoint of the protocol, electromagnetic and physical layer. At the time of writing this thesis, the importance of security in safety–related systems like railway is emphasized by many European projects that assess the impact of different types of malicious attacks against
rail infrastructure and equipment [62–64]. This dissertation provides one perspective to this wide scenario. The research was steered by the author’s knowledge about the development process of wireless apparatuses for railways and and the need to investigate their security aspects and how these can impact the entire system.

Certainly, this doctoral study can be extended to other disciplines, such as software security and network security, and other use cases as well. The author is certain that further investigation on cybersecurity is needed to evaluate wireless technology evolution and other safety–related system operating scenarios. Wireless communications beyond 2020 becomes pervasive, introducing the Internet of everything in which many small devices interact with each other and with users. In this scenario, large volumes of data with low latency requirement will be transmitted and processed [157]. 5G systems will encompass different radio providing ultra–high capacity, energy efficiency and new spectrum management solutions [158–160]. This evolution and prospective further security engineering methodologies mean that appropriate mitigations must be developed because it is likely that safety–related systems will have different wireless interfaces and their operating scenarios will include an extensive utilization of wireless links. The utilization of networking devices in railway systems makes them vulnerable to cyberattacks, and designers must address these threats with a particular focus on the perimeter of the safety related system.

Finally, software has become a key part of any product. Against that context, it is important to take account the security requirements in software development and deployment right from the beginning. Even more frequently, hackers will look at the victim system in its entirety; e.g., they can attack public transport systems by exploiting weaknesses in the software maintenance process. This prospective requires that the software must also include mechanisms to mitigate possible malicious attacks that could occur during over–the–air updates.
References

25. (2012). CENELEC EN 50159 - Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems.
55. Polish teen derails tram after hacking train network. URI: http://www.theregister.co.uk/2008/01/11/tram_hack/.
63. SECUREMETRO Project. URI: http://www.securemetro.com/.
64. SECRET Project. URI: http://www.secret-project.eu/.
73. IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirement Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications
93. OMNET++. URI: http://www.omnetpp.org/.
94. TOSSIM. URI: http://docs.tinyos.net/tinywiki/index.php/TOSSIM.
95. NS-3. URI: http://www.nsnam.org/.


127. (2012). CENELEC EN 50159 - Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems.
146. (2014). Electromagnetic compatibility (EMC) - Part 6-7: Generic standards - Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations. IEC 61000-6-7.


Appendix 1
Increasing power over jamming

When the circular aperture antenna moved closer to the DUT, the incident power increase. It can be easily verified that

\[ \Delta S = 10 \log \left( 4 \sin^2 \left( \frac{A}{2r} \right) \right) - 10 \log \left( \frac{1}{\lambda} \right)^2 \right|_{r_2} = 12.64 \approx 13 \text{ dB}, \]

where \( r_1 = \frac{\pi D^2}{8 \lambda} \), \( r_2 = \frac{2D^2}{\lambda} \) and \( \Delta S \) is the power increment in decibels.
Appendix 2
Outage probability of secrecy capacity
for WBPLSec

In the case of WBPLSec, $P_{out}$ results from simple algebra and can be expressed as [118]

$$P_{out} = 1 - \int_{0}^{\infty} e^{-p(1+\bar{\alpha}_{jr})-q\bar{\beta}} \left( \frac{1+\bar{\alpha}_{je}}{1+\bar{\beta}_{je}} \right) .$$

$$e^{-\bar{\alpha}} e^{-\bar{\beta}} d\bar{\alpha} d\bar{\beta} =$$

$$= 1 - \frac{1}{(\gamma_{jr} \gamma_{jr} P + \gamma_{je} - \gamma_{jr} q)^2} .$$

$$e^{-p} \left( -q \Omega \left( \frac{q+1}{\gamma_{je}} \right) (\gamma_{je} (\gamma_{jr} P + \gamma_{jr} + 1) - \gamma_{jr} q) -$$

$$\Omega \left( \frac{(q+1)(\gamma_{je} P + 1)}{\gamma_{jr} q} \right) \left( \gamma_{je} (\gamma_{jr} P - (\gamma_{je} + 1) \gamma_{jr} q +$$

$$\gamma_{je}) + \gamma_{je} (\gamma_{je} \gamma_{jr} P + \gamma_{je} - \gamma_{jr} q) \right) \right) .$$

(16)

where $\Omega(x) = e^{x} E_{1}(x), E_{1} = \int_{0}^{\infty} (e^{-t}) dt$ is the exponential integral. It is assumed that the fading channels’ coefficients are zero–mean complex Gaussian random variables (RVs). The proof that $\alpha, \bar{\alpha}, \beta$ and $\bar{\beta}$ are exponential distributed is given below.

$h = h_{I} + jh_{Q}$ denotes the channel complex Gaussian fading coefficients where $h_{I}$ and $h_{Q}$ are both Gaussian variables. $|h| = \sqrt{h_{I}^{2} + h_{Q}^{2}}$ is RV that follows Rayleigh distribution

$$f_{h}(h) = \frac{2h}{E[h^2]} e^{-\frac{h^2}{2E[h^2]}},$$

(17)

where $|h|$ is RV that follow Rayleigh distribution. The instantaneous SINR is $\propto \alpha = |h|^2$ and in accordance to the fundamental theorem [161] its probability density function is given by

$$f_{\alpha}(\alpha) = \frac{1}{E[\alpha]} e^{-\frac{\alpha}{E[\alpha]}},$$

(18)

it follows that $\alpha$ is exponentially distributed.
Original publications


Reprinted with permission from the IEEE (I, II, III, V, VI) and the Electromagnetics Academy (IV).

Original publications are not included in the electronic version of the dissertation.
556. Omran, Mandy (2015) Microwave dephosphorisation of high phosphorus iron ores of the Aswan region, Egypt: developing a novel process for high phosphorus iron ore utilization
558. Aula, Matti (2016) Optical emission from electric arc furnaces
559. Ferdinand, Nuwan Suresh (2016) Low complexity lattice codes for communication networks
560. Xue, Qiang (2016) Analysis of near-optimal relaying schemes for wireless tandem and multicast relay networks
563. Huuskko, Jarlko (2016) Communication performance prediction and link adaptation based on a statistical radio channel model
564. Nguyen, Vu Thuy Dan (2016) Transmission strategies for full-duplex multiuser MIMO communications systems
565. Keränen, Pekka (2016) High precision time-to-digital converters for applications requiring a wide measurement range
566. Koivuranta, Elisa (2016) Optical monitoring of flocs and filaments in the activated sludge process
567. Lohikoski, Päivi (2016) Information processing in global virtual NPD projects
568. Kauppila, Osmo (2016) Integrated quality evaluation in higher education
569. Kisko, Anna (2016) Microstructure and properties of reversion treated low-Ni high-Mn austenitic stainless steels
570. Postila, Heini (2016) Peat extraction runoff water purification in treatment wetlands constructed on drained peatlands in a cold climate
571. Happonen, Tuomas (2016) Reliability studies on printed conductors on flexible substrates under cyclic bending

Book orders:
Granum: Virtual book store
http://granum.uta.fi/granum/
Simone Soderi

EVALUATION OF INDUSTRIAL WIRELESS COMMUNICATIONS SYSTEMS’ SECURITY