GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	Physical Layer Security, PG_00069756						
Field of study	Informatics, Electronics and Telecommunications, Biomedical Engineering, Biomedical Engineering, Biomedical Engineering, Space and Satellite Technologies, Automatic Control, Cybernetics and Robotics						
Date of commencement of studies	February 2025		Academic year of realisation of subject	2025/2026			
Education level	second-cycle studies		Subject group				
Mode of study	Full-time studies		Mode of delivery	at the university			
Year of study	1		Language of instruction	Polish			
Semester of study	2		ECTS credits	1.0			
Learning profile	general academic profile		Assessment form	assessment			
Conducting unit	Department of Radiocommunication Systems and Networks -> Faculty of Electronics Telecommunications and Informatics -> Faculties of Gdańsk University of Technology						
Name and surname of lecturer (lecturers)	Subject supervisor	dr inż. Jarosław Magiera					
	Teachers	dr inż. Jarosław Magiera					
Lesson types	Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
	Number of study hours	15.0	0.0	0.0	0.0	0.0	15
	E-learning hours included: 0.0						
	eNauczanie source address: https://enauczanie.pg.edu.pl/2025/course/view.php?id=1809						
Learning activity and number of study hours	Learning activity	Participation in didactic classes included in study plan		Participation in consultation hours	Self-study	SUM	
	Number of study hours	15		1.0	9.0	25	
Subject objectives	The aim of the course is to familiarise students with issues related to the broadly understood security of digital wireless transmission, not only in terms of data security, but above all in the context of attacks carried out at the physical layer of the radio link.						

Learning outcomes

Course outcome	Subject outcome	Method of verification
[K7_W03] knows and understands, to an increased extent, the construction and operating principles of components and systems related to the field of study, including theories, methods and complex relationships between them and selected specific issues - appropriate for the curriculum	Knows and understands methods and techniques for securing radio transmissions against interference, manipulation and eavesdropping. Knows and understands techniques for using the properties of the physical layer to secure the confidentiality of transmissions.	[SW1] Assessment of factual knowledge
[K7_W02] knows and understands, to an increased extent, selected laws of physics and physical phenomena, as well as methods and theories explaining the complex relationships between them, constituting advanced general knowledge in the field of technical sciences related to the field of study	Knows and understands the physical phenomena occurring in the radio channel in terms of the possibility of carrying out radio-electronic attacks and counteracting them, as well as the use of these phenomena for the purposes of transmission authentication.	[SW1] Assessment of factual knowledge
[K7_W101] is able to make an in-depth identification of key objects and phenomena related to the field of study, as well as theories that describe them and applicable analytical and design methods	Identifies objects that constitute elements of electronic attack scenarios in the physical layer of a wireless link and analyses phenomena that determine the feasibility of such attacks and protection against them. Understands the description of physical layer security from the point of view of information theory and knows methods for designing systems with increased resistance to attacks in the physical layer.	[SW1] Assessment of factual knowledge

Subject contents

Course content – lecture
Definition of physical layer security and its differences from cryptography.
PLS from the perspective of information theory.
Main types of threats in the physical layer.
Jamming characteristics, detection and countermeasures.
Spoofing characteristics, detection and countermeasures.
Passive and active eavesdropping characteristics and countermeasures.
Use of unique radio channel characteristics to ensure transmission confidentiality.
Authentication mechanisms in the physical layer.
Cooperative techniques in the field of PLS.
Possibilities of applying PLS techniques in various wireless communication standards, e.g. 5G, WiFi, GNSS.
Linking PLS with elements of modern radio communication, including millimetre waves, massive MIMO, full duplex, reconfigurable reflective surfaces.
Use of artificial intelligence and context awareness methods in PLS.

Prerequisites and co-requisites

Assessment methods and criteria

Subject passing criteria	Passing threshold	Percentage of the final grade
Assessment test	50.0%	100.0%

Recommended reading

Basic literature	1. Zhou, X., Song, L., & Zhang, Y. (Eds.). (2016). Physical layer security in wireless communications. CRC Press. 2. Bloch, M., & Barros, J. (2011). Physical-layer security: from information theory to security engineering. Cambridge University Press. 3. Arslan, H., & Furqan, H. M. (Eds.). (2023). Physical layer security for wireless sensing and communication (Vol. 18). IET.
Supplementary literature	---
eResources addresses	

Example issues/ example questions/ tasks being completed	Principles of the Physical Layer Security (PLS) concept Classification of threats in the physical layer in the context of attacks on communication systems PLS and information theory: • Shannon and Wyner model diagrams and their differences • The meaning of channel secrecy capacity • Model for key generation in the physical layer (scheme, assumptions, procedure) • The meaning of key generation rate Jamming • Attacker's objectives • Classification of jammers • Types of jamming signals • Smart jammer • Measures of jamming effectiveness • Methods of detection and countermeasures against jamming Spoofing • Overview of spoofing • Attacker's objectives • Methods of detecting and counteracting spoofing Eavesdropping • Attacker's objectives • Passive and active eavesdropping • Transmission secrecy metrics • Methods of counteracting eavesdropping PLS from the perspective of wireless channel • Criteria for the suitability of channel features for PLS (with an explanation of the meaning of each criterion) • Examples of channel features for use in PLS applications (RSS, impulse response, frequency response) Generating secret key based on channel features • Key generation procedure stages (with a brief explanation of each stage) • Key generation performance measures Physical Layer Authentication • General description / assumptions • Radio transmitter scheme, including blocks relevant to PLS • Features used to identify the local oscillator (phase noise, carrier frequency offset + meaning of these parameters) • Features used to identify the quadrature modulator • Classifier training modes (supervised/unsupervised) Cooperative techniques for PLS • Types of cooperation and their characteristics (cooperative communication, coordinated multipoint) • Types of relays • Applications of cooperative communication in PLS (coordinated: jamming, protection against jamming, protection against spoofing) • Coordinated multipoint (types of cooperation, methods of counteracting eavesdropping/jamming/ spoofing) PLS from the perspective of modern radio communication • Elements of current and future radio communication (millimeter waves, massive MIMO, full duplex, reconfigurable intelligent surfaces) • Emerging channel features (large scale fading, atmospheric effects, sparsity, antenna array non-stationarity, temporal/frequency/spatial non-stationarity) • Possibilities and benefits of using RIS surfaces for PLS
Practical activites within the subject	Not applicable