POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	Bezpieczeństwo warstwy fizycznej, PG_00069756		
Kierunek studiów	Informatyka, Technologie wodorowe i elektromobilność		
Data rozpoczęcia studiów	luty 2026 r.	Rok akademicki realizacji przedmiotu	2026/2027
Poziom kształcenia	II stopnia	Grupa zajęć	
Forma studiów	stacjonarne	Sposób realizacji	na uczelni
Rok studiów	1	Język wykładowy	polski
Semestr studiów	2	Liczba punktów ECTS	1.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	zaliczenie
Jednostka prowadząca	Wydziały Politechniki Gdańskiej -> Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Systemów i Sieci Radiokomunikacyjnych		
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr inż. Jarosław Magiera	
	Prowadzący zajęcia z przedmiotu	dr inż. Jarosław Magiera	

Formy zajęć

Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
Liczba godzin zajęć	15.0	0.0	0.0	0.0	0.0	15

W tym liczba godzin zajęć na odległość: 0.0

Adres kursu na platformie eNauczanie: https://enauczanie.pg.edu.pl/2025/course/view.php?id=1809

Moodle ID: 5695 Bezpieczeństwo warstwy fizycznej (2026/2027) https://enauczanie.pg.edu.pl/2025/course/view.php?id=5695

Aktywność studenta i liczba godzin pracy

Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów	Udział w konsultacjach	Praca własna studenta	RAZEM
Liczba godzin pracy studenta	15	1.0	9.0	25

Cel przedmiotu

Celem przedmiotu jest zapoznanie studentów z zagadnieniami szeroko pojętego bezpieczeństwa cyfrowej transmisji bezprzewodowej, nie tylko w zakresie bezpieczeństwa danych, ale przede wszystkim w kontekście ataków realizowanych na poziomie warstwy fizycznej łącza radiowego.

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[K7_W03] zna i rozumie w pogłębionym stopniu budowę i zasady działania komponentów i systemów związanych z kierunkiem studiów, w tym teorie, metody i złożone zależności między nimi oraz wybrane zagadnienia szczegółowe – właściwe dla programu kształcenia	Zna i rozumie metody i techniki zabezpieczania transmisji radiowej przed zakłócaniem, manipulacją i podsłuchem. Zna i rozumie techniki wykorzystania właściwości warstwy fizycznej dla potrzeb zabezpieczenia poufności transmisji.	[SW1] Ocena wiedzy faktograficznej
[K7_W02] zna i rozumie w pogłębionym stopniu wybrane prawa i zjawiska fizyczne oraz metody i teorie wyjaśniające złożone zależności między nimi, stanowiące zaawansowaną wiedzę ogólną z dziedziny nauk technicznych, związaną z kierunkiem studiów	Zna i rozumie zjawiska fizyczne zachodzące w kanale radiowym w zakresie możliwości realizacji ataków radioelektronicznych i przeciwdziałania im, jak również wykorzystania tych zjawisk dla potrzeb uwierzytelniania transmisji.	[SW1] Ocena wiedzy faktograficznej
[K7_W101] identyfikuje w pogłębionym stopniu kluczowe obiekty i zjawiska związane ze studiowanym kierunkiem oraz opisujące je teorie i możliwe do zastosowania metody analityczne i projektowe	Identyfikuje obiekty stanowiące elementy scenariuszy ataków elektronicznych w warstwie fizycznej łącza bezprzewodowego oraz analizuje zjawiska warunkujące realizowalność takich ataków i ochrony przed nimi. Rozumie opis bezpieczeństwa warstwy fizycznej z punktu widzenia teorii informacji i zna metody projektowania systemów o podwyższonej odporności na ataki w warstwie fizycznej.	[SW1] Ocena wiedzy faktograficznej

Treści przedmiotu	Treści przedmiotu - wykład • Definicja bezpieczeństwa warstwy fizycznej oraz jej odmienności względem kryptografii. • BWF z punktu widzenia teorii informacji. • Główne rodzaje zagrożeń w warstwie fizycznej. • Zakłócanie (jamming) charakterystyka, metody detekcji i przeciwdziałania • Podszywanie (spoofing) charakterystyka, metody detekcji i przeciwdziałania • Podsłuch pasywny i aktywny charakterystyka i metody przeciwdziałania. • Wykorzystanie unikalnych cech kanału radiowego dla zapewnienia poufności transmisji. • Mechanizmy uwierzytelniania w warstwie fizycznej. • Techniki kooperacyjne z zakresie BWF. • Możliwości zastosowania technik BWF w różnych standardach komunikacji bezprzewodowej, np. 5G, WiFi, GNSS. • Powiązanie BWF z elementami współczesnej radiokomunikacji, m.in. fale milimetrowe, massive MIMO, full duplex, rekonfigurowalne powierzchnie odbijające. • Wykorzystanie metod sztucznej inteligencji i świadomości kontekstu w zakresie BWF.
Wymagania wstępne i dodatkowe	

Sposoby i kryteria oceniania osiąganych efektów uczenia się

Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
Zaliczenie	50.0%	100.0%

Zalecana lista lektur	
Podstawowa lista lektur	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.
Uzupełniająca lista lektur	---
Adresy eZasobów	

Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania	Założenia koncepcji Bezpieczeństwa Warstwy Fizycznej (BWF) Klasyfikacja zagrożeń w warstwie fizycznej w kontekście ataków na systemy komunikacyjne BWF a teoria informacji: • Schematy modeli Shannona, Wynera i ich różnice • Pojęcie pojemności sekretności kanału (secrecy capacity) • Model do generowania klucza w warstwie fizycznej (schemat, założenia, procedura) • Pojęcie szybkości generowania klucza (key generation rate) Zagłuszanie (jamming) • Dążenia atakującego • Klasyfikacja jammerów • Rodzaje sygnałów zagłuszających • Smart jammer • Miary skuteczności jammingu • Metody detekcji i przeciwdziałania zagłuszaniu Spoofing • Charakterystyka ogólna • Dążenia atakującego • Metody detekcji i przeciwdziałania spoofingowi Podsłuch • Dążenia atakującego • Podsłuch pasywny i aktywny • Metryki tajności transmisji • Metody przeciwdziałania podsłuchowi BWF z punktu widzenia kanału bezprzewodowego • Kryteria przydatności cech kanału dla BWF (z wyjaśnieniem znaczenia każdego kryterium) • Przykładowe cechy kanału do użycia w zastosowaniach BWF (RSS, odpowiedź impulsowa, charakterystyka częstotliwościowa) Generowanie klucza z użyciem cech kanału • Etapy procedury generowania klucza (z krótkim objaśnieniem każdego etapu) • Miary jakości generowania klucza Uwierzytelnianie w warstwie fizycznej • Opis ogólny / założenia • Schemat nadajnika radiowego z uwzględnieniem bloków istotnych dla BWF • Cechy służące identyfikacji oscylatora lokalnego (szum fazowy, przesunięcie częstotliwości nośnej + znaczenie tych parametrów) • Cechy służące identyfikacji modulatora kwadraturowego • Metody uczenia klasyfikatora (nadzorowane/nienadzorowane) Techniki kooperacyjne w zakresie BWF • Rodzaje kooperacji i ich charakterystyka (komunikacja kooperacyjna, skoordynowany wielopunkt) • Rodzaje przekaźników • Zastosowania komunikacji kooperacyjnej w BWF (skoordynowane: zagłuszanie, ochrona przed zagłuszaniem, ochrona przed spoofingiem) • Skoordynowany wielopunkt (rodzaje kooperacji, sposoby przeciwdziałania podsłuchowi/zagłuszaniu/ spoofingowi) BWF a współczesna radiokomunikacja • Elementy współczesnej i przyszłej radiokomunikacji (fale mm, massive MIMO, full duplex, powierzchnie rekonfigurowalne) • Dodatkowe cechy kanału radiowego (zaniki wolne, efekty atmosferyczne, rzadkość, niestacjonarność układu antenowego, niestacjonarność czasowa/częstotliwościowa/przestrzenna) • Możliwości i korzyści z wykorzystania powierzchni RIS dla BWF
Zajęcia praktyczne w ramach przedmiotu	Nie dotyczy

Dokument wygenerowany elektronicznie. Nie wymaga pieczęci ani podpisu.