



PROGRAMA DE ASIGNATURA

Nombre del curso o actividad	SEGURIDAD DE CAPA FÍSICA DE COMUNICACIONES
Nombre del programa	Doctorado en Ciencias de la Ingeniería mención Automática
Descripción	<i>Código: 11311, Nivel: 2 o 3, Créditos SCT-Chile: 10, Tipo: Electiva, Plan de Estudios: Resolución N°1118 del 03/04/20.</i> Este curso explora técnicas de seguridad aplicadas a la capa física en sistemas de comunicaciones inalámbricas. A diferencia de los métodos tradicionales basados en criptografía en capas superiores, la seguridad en la capa física explota las características inherentes del canal inalámbrico para mejorar la confidencialidad y la integridad de la comunicación. Se abordarán temas como codificación segura, desvanecimiento del canal, modelos de ataque físico, y el diseño de sistemas robustos frente a eavesdropping y jamming.
Objetivos	• Comprender los principios y motivaciones detrás de la seguridad en la capa física. • Analizar modelos de amenaza relevantes para redes inalámbricas. • Aplicar técnicas como beamforming, codificación segura y ocultación de señales para fortalecer la seguridad. • Diseñar y evaluar esquemas de seguridad física bajo diferentes escenarios de canal y adversarios. • Simular sistemas seguros en la capa física y evaluar su rendimiento frente a ataques.
Contenidos	Unidad 1: Introducción a la Seguridad en Comunicaciones Inalámbricas • Modelos de seguridad tradicionales vs. seguridad en capa física • Vulnerabilidades inherentes en entornos inalámbricos • Motivación y casos de uso Unidad 2: Modelos de Canal y Fundamentos Teóricos • Canales con desvanecimiento (fading) • Información mutua y capacidad secreta • Modelo wiretap de Wyner • Secrecy capacity y secrecy outage Unidad 3: Técnicas de Seguridad en Capa Física • Codificación segura (secure channel coding) • Artificial noise generation • Beamforming y MIMO seguro • OFDM y técnicas de modulación seguras Unidad 4: Amenazas y Ataques • Eavesdropping pasivo vs. activo • Jamming selectivo y de banda ancha • Ataques de inyección de señales (spoofing físico) • Técnicas de detección y mitigación Unidad 5: Aplicaciones Prácticas y Nuevas Tendencias • IoT y redes de sensores seguras



	• Seguridad física en 5G y 6G
Modalidad de evaluación	Estrategias Metodológicas Clases expositivas para introducir conceptos fundamentales. Estudio de casos de vulnerabilidades en sistemas inalámbricos. Lectura de artículos de investigación recientes. El estudiante deberá desarrollar simulaciones computacionales de esquemas de seguridad física, analizar modelos matemáticos como el wiretap channel, medidas de información mutua y capacidad de canal secreta, entre otras, y resolver ejercicios en distintos escenarios de canal y ataques. Evaluación Analizar artículos sobre seguridad en la capa física, evaluando su contribución, metodología, resultados y limitaciones. Realizar presentaciones orales de casos de estudio.
Resultados de aprendizajes esperados	Resultado de Aprendizaje General: Aplicar los principios y técnicas de seguridad en la capa física para el diseño, análisis y simulación de sistemas de comunicación inalámbrica robustos frente a amenazas como eavesdropping y jamming, comprendiendo los fundamentos teóricos y prácticos del entorno físico del canal. Resultados de Aprendizaje Específicos: • Comprender los conceptos fundamentales y las diferencias entre la seguridad tradicional basada en criptografía y la seguridad en la capa física. • Analizar las propiedades estadísticas de los canales inalámbricos (como el desvanecimiento y el ruido) y su impacto en la seguridad. • Modelar escenarios de amenaza mediante el uso de modelos como el wiretap de Wyner y conceptos como la secrecy capacity. • Evaluar el desempeño de sistemas seguros ante ataques como eavesdropping, jamming, y explorando otros ataques físicos a través de la literatura. • Simular escenarios de seguridad en capa física utilizando herramientas computacionales y revisar el comportamiento de las métricas de desempeño. • Explorar aplicaciones de seguridad física en tecnologías emergentes.
Bibliografía	Básica: • X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, 2013. • [2] A. Jamalipour and Y. Bi, *Wireless Powered Communication Networks: From Security Challenges to IoT Applications*. Springer, 2019. • [3] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005 Recomendada: • Publicaciones disponibles en las Bases de datos IEEE Xplore, Springer Nature Link y ScienceDirect (Elsevier).