Wireless Security

Prof. Marco Mellia
Dr. Andrea Nardin

Course Outline

- **Course Outline**
  - Review of basic concepts for digital communications
  - **<u>Security at the physical layer</u>**
  - Global Navigation Satellite Systems (GNSS) and positioning
  - Security in WiFi Networks
  - Bluetooth security
  - Security of Cellular Networks - 3G/4G/5G Network Structure and Architectures
  - Security of Near Field Communications (NFCs) and RFIDs

Security at the Physical Layer

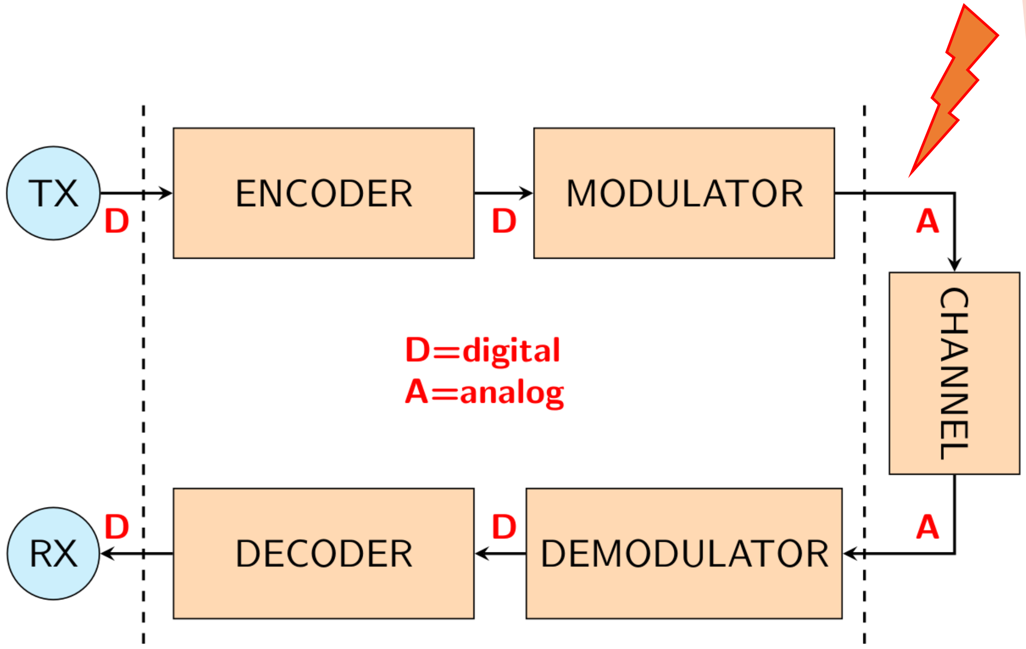
Andrea Nardin

Wireless Channel and Security Threat

- When signals are transmitted over the **wireless channel**, security is more of a concern

- Why?
  - No inherent physical protection
    - physical connections between devices are replaced by logical associations
    - sending and receiving messages do not need physical access to the network infrastructure (cables, hubs, routers, etc.)

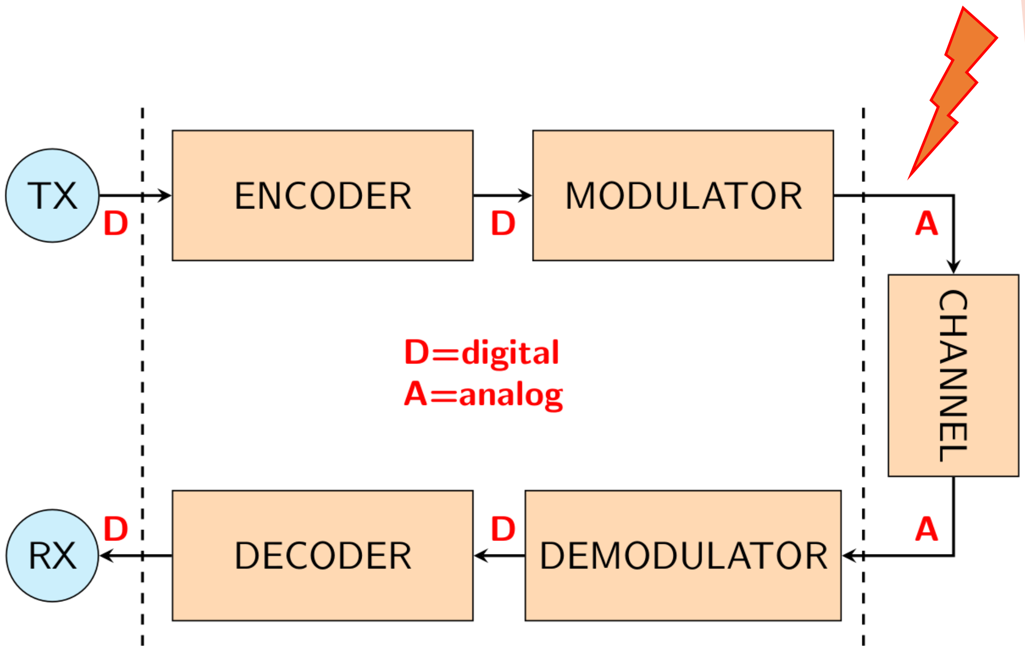
Security threat!



Wireless Channel and Security Threat

- When signals are transmitted over the **wireless channel**, security is more of a concern

- Why?
  - Broadcast communications
    - wireless usually means radio, which has a broadcast nature
    - transmissions can be overheard by anyone in range
    - anyone can generate transmissions
      - received by other devices in range
      - interfere with other nearby transmissions and may prevent their correct reception (*jamming*)

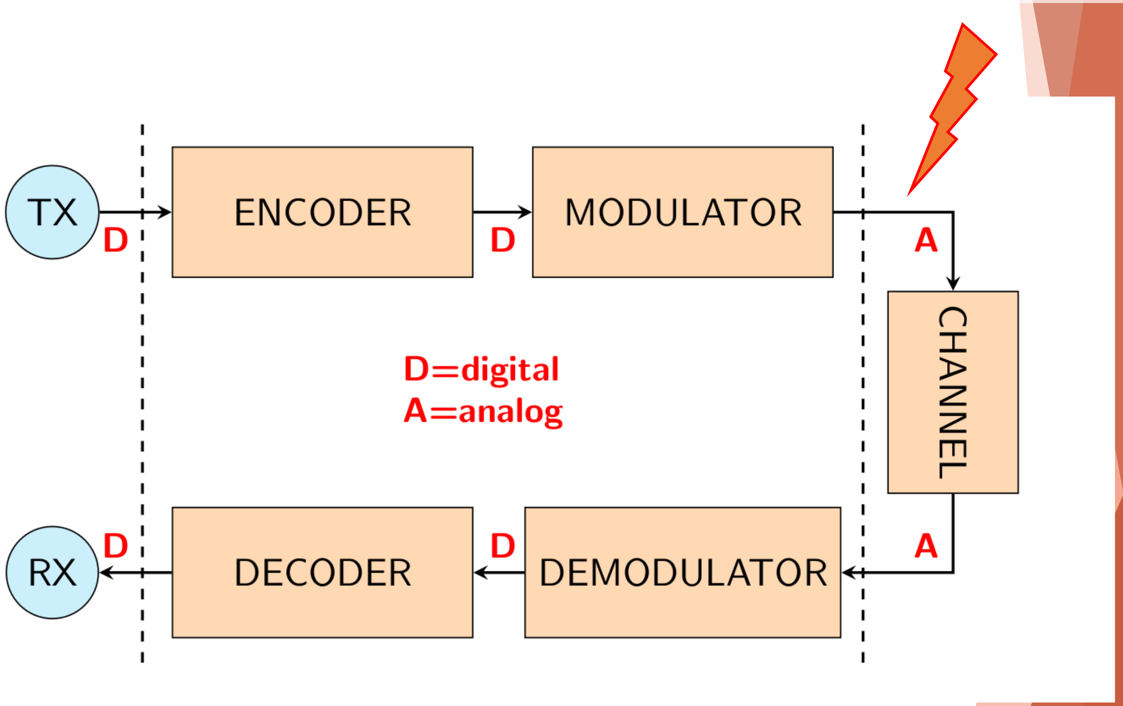


Wireless Channel and Security Threat

- When signals are transmitted over the **wireless channel**, security is more of a concern

- As a result:
  - eavesdropping is easy
  - injecting bogus messages into the network is easy
  - replaying previously recorded messages is easy (e.g. *meaconing*)
  - illegitimate access to the network and its services is easy
  - denial of service is easily achieved by jamming

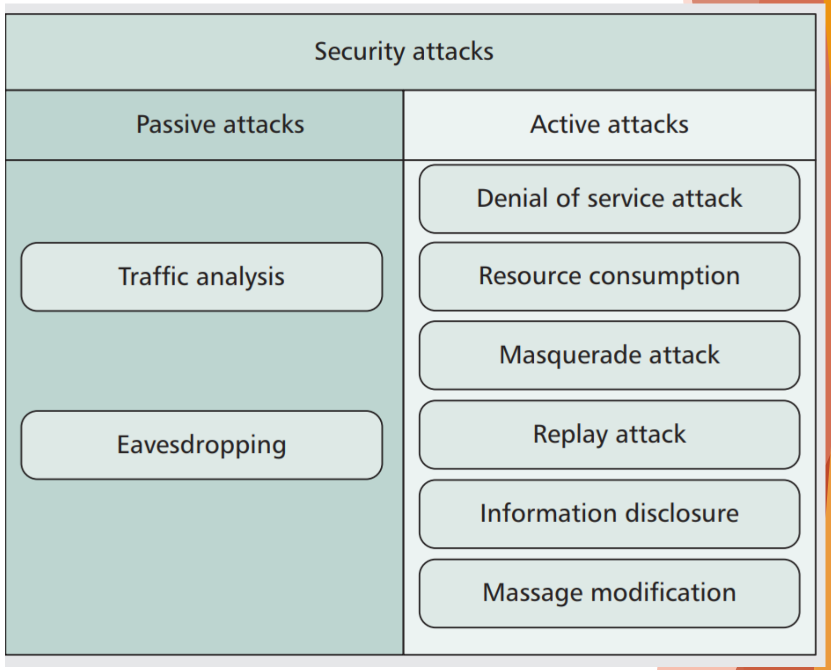
Security threat!



Security Attacks in Wireless Networks

- The wireless communication medium is open to **jamming** (or interference) and **eavesdropping** attacks from intruders.

- **Passive attacks**
  - do not disrupt network operation, and the adversary’s objective is to **steal** transmitted information
- **Active attacks**
  - active attacks can significantly **interfere** with normal network operations because an adversary often tries to alter the network data
  - ***Jamming*** is also widely used to launch DoS attacks at the physical layer. Radio frequency jamming can be employed to invade the transmitted signal band. An adversary can utilize jamming signals (thereby disrupting the communications) to make the attacked nodes suffer from DoS in a specific region



Security attacks

Passive attacks

Traffic analysis

Eavesdropping

Active attacks

Denial of service attack

Resource consumption

Masquerade attack

Replay attack

Information disclosure

Massage modification

Classification of the commonly used security attacks in wireless communications. From [1].

[1] Y. -S. Shiu, S. Y. Chang, H. -C. Wu, S. C. . -H. Huang and H. -H. Chen, "Physical layer security in wireless networks: a tutorial," in IEEE Wireless Communications, vol. 18, no. 2, pp. 66-74, April 2011, doi: 10.1109/MWC.2011.5751298.

Jamming (DoS)

- A simple strategy to disrupt wireless communications is to interfere with communications directly by *jamming* the communication channel
- A jammer may broadcast an **interference signal** on a **broad spectral band** to disrupt legitimate signal reception.
- They can be classified into two types:
  - **Active** (constant) jammers send out a radio signal **continuously** into the channel and therefore block the communications of users, making the prevention of such interference a big challenge.
  - A **reactive** jammer is idle until it senses transmission activities occurring in the channel; then it transmits jamming signals to interrupt the ongoing transmission. Since the jammer must detect transmission activities before issuing its jamming signal, the transceiver may improve its own low probability of detection to avoid jamming attacks
- A persistent and powerful adversary **can always jam** all data transmissions by transmitting **high-power white noise** over the entire frequency spectrum. Although such availability threats are powerful, they can be addressed through many physical layer security schemes

Former jammer tower, used in the Soviet Union to jam western radio stations. Minsk, Belarus

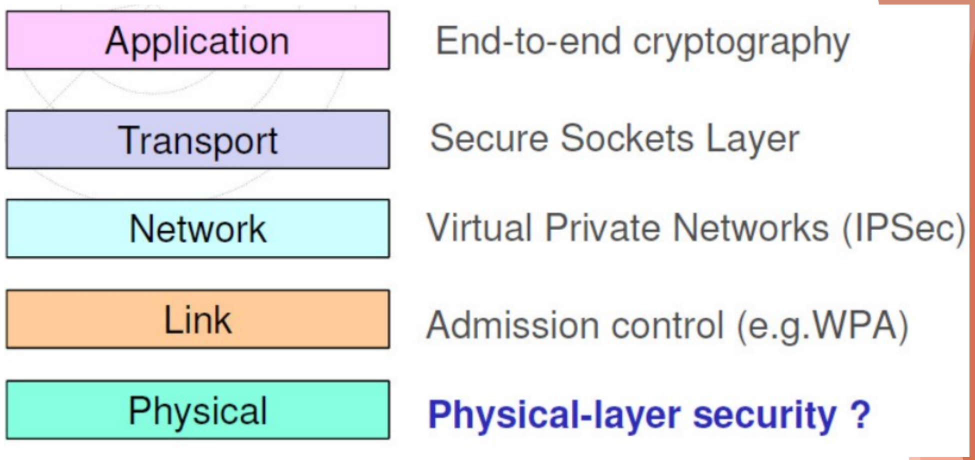
Eavesdropping

- The broadcast nature of the wireless medium makes it **hard to eliminate** unauthorized access to wireless networks
- The most common way to maintain confidentiality is to use **encryption**
- Another widely used approach to maintain confidentiality is to force the transmitter and receiver to adopt some **information hiding** measures
- Information hiding is a method to embed private messages into a background signal or noise process.

Cardinals eavesdropping in the Vatican. A painting by Henri Adolphe Laissement, 1895

Physical Layer Security

- In traditional systems, **reliability** is guaranteed by **channel coding** at the physical layer, while **security** is ensured by **encryption** protocols at the upper layers
- ***Physical layer security*** aims at exploiting the **randomness** inherent in **noisy** channels to provide an additional level of protection at the physical layer
  - *perfect secrecy* is achievable if the channel is unknown to unauthorized users, or the channel of the unauthorized users is more noisy than that of the authorized users [2]



Application	End-to-end cryptography
Transport	Secure Sockets Layer
Network	Virtual Private Networks (IPSec)
Link	Admission control (e.g.WPA)
Physical	**Physical-layer security ?**

[2] A. D. Wyner, "The Wiretap Channel," Bell System Tech. J., vol. 54, 1975, pp. 1355–87.

Cryptography VS Physical Layer Security

Crypto Vs PhySec

- Cryptography permits **demodulation**, but the message cannot be understood
- Physical Layer Security does not even allow demodulation
- Physical Layer Security does not rely on the assumption of limited computational power of the attacker
- Physical Layer Security can be measured

- Nowadays, many results from **information theory, signal processing, and cryptography** suggest that there is much security to be gained by accounting for the imperfections of the physical layer when designing secure systems

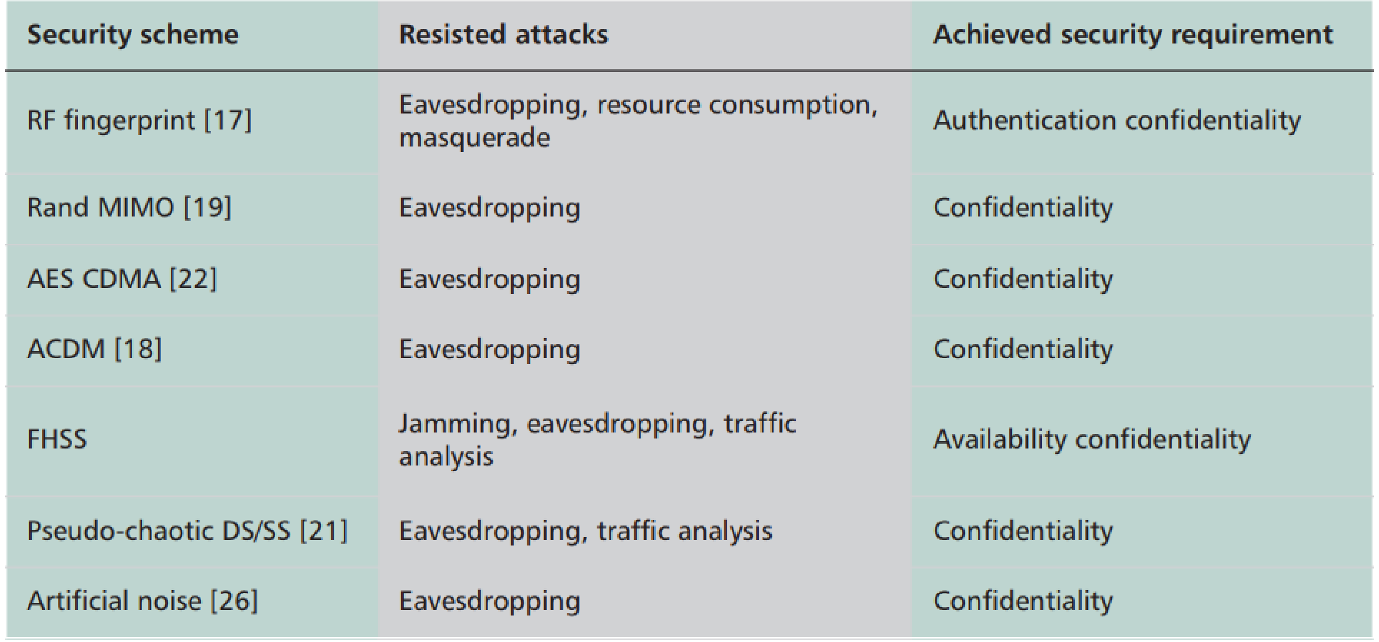
Physical Layer Security Methods

- Major categories of physical layer security methods: Channel Approaches, Coding Approaches, Power Approaches, and Signal Design Approaches.

- **Channel Approaches:**
  - *RF Fingerprinting:* Dynamic fingerprinting for intrusion detection.
  - *ACDM Precoding:* Use of singular value decomposition for generating transmitted code vectors.
  - *Randomization of MIMO Transmission Coefficients:* Achieving perfect secrecy by randomizing MIMO coefficients.
- **Code Approaches:**
  - *Error Correction Coding:* Advanced channel coding and AES cryptosystem for secure communication.
  - *Spread Spectrum Coding:* Direct-sequence CDMA and Frequency Hopping Spread Spectrum (FHSS).
- **Power Approaches:**
  - *Directional Antennas:* Improved spatial reuse and data availability using beamforming.
  - *Artificial Noise Scheme:* Generation of artificial noise to impair intruder's channel while maintaining secrecy for the legitimate receiver.
- **Signal Design Approaches:**
  - *Discriminatory Channel Estimation:* Use of artificial noise to degrade eavesdropper's channel estimation.
  - *Multistage Training-Based Channel Estimation:* Minimization of mean squared error subject to constraints using channel feedback.

Physical Layer Security Methods

- Each method addresses specific aspects of physical layer security, ranging from utilizing **channel characteristics** to employing artificial **noise** and **directional antennas**.
- Each method is effective against **various attacks** such as eavesdropping and jamming
- They are using a combination of information theory, coding techniques, and signal processing approaches



Security scheme	Resisted attacks	Achieved security requirement
RF fingerprint [17]	Eavesdropping, resource consumption, masquerade	Authentication confidentiality
Rand MIMO [19]	Eavesdropping	Confidentiality
AES CDMA [22]	Eavesdropping	Confidentiality
ACDM [18]	Eavesdropping	Confidentiality
FHSS	Jamming, eavesdropping, traffic analysis	Availability confidentiality
Pseudo-chaotic DS/SS [21]	Eavesdropping, traffic analysis	Confidentiality
Artificial noise [26]	Eavesdropping	Confidentiality

Comparison of different attack methods and their security scheme. From [1]