Università degli Studi di Padova

MIME

Master's degree ICT Internet Multimedia Engineering

Department of Information Engineering (DEI)
Master degree on ICT for Internet and Multimedia Engineering (MIME)

Internet of Things and Smart Cities
04 – Radio Frequency IDentification (RFID)

Marco Giordani (marco.giordani@unipd.it)
Department of Information Engineering (DEI) – SIGNET Research Group
University of Padova – Via Gradenigo 6/B, 35131, Padova (Italy)

UNIVERSITÀ DEGLI STUDI DI PADOVA

MIME

Master's degree ICT Internet Multimedia Engineering

04 – IoT technologies (short-range)
Introduction

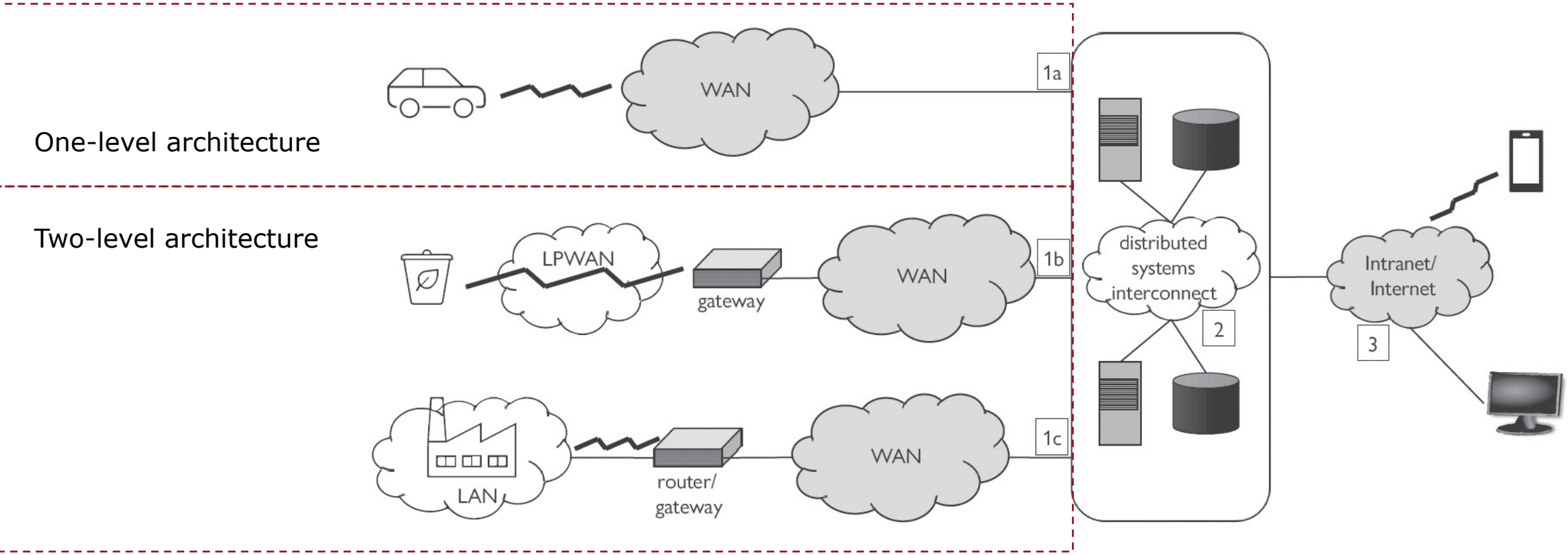
Marco Giordani (marco.giordani@unipd.it)
Department of Information Engineering (DEI) – SIGNET Research Group
University of Padova – Via Gradenigo 6/B, 35131, Padova (Italy)

Do you remember?

Network architectures

One-level architecture

Two-level architecture



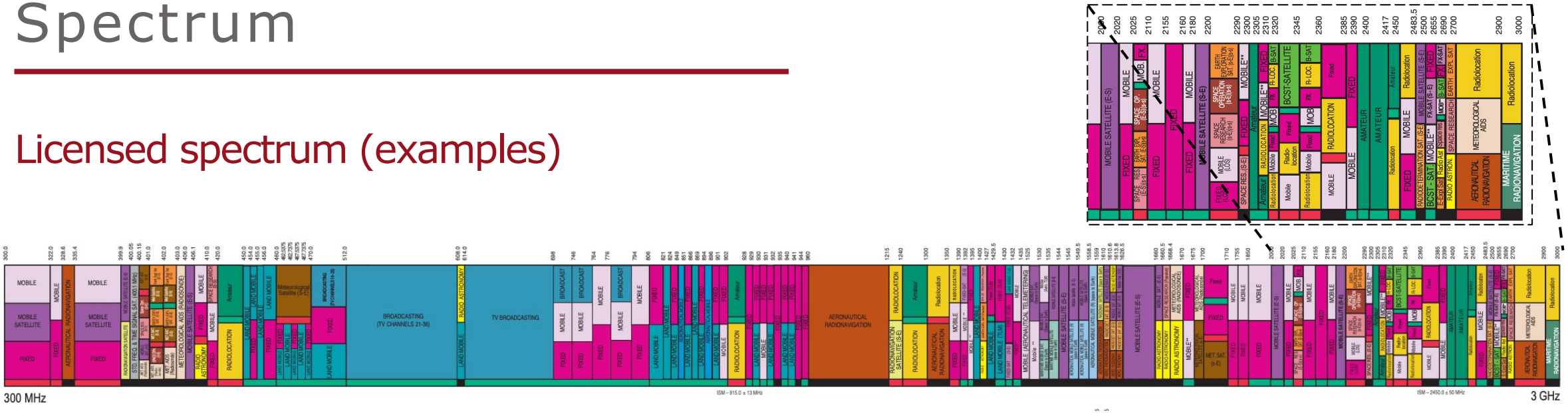
Spectrum

Introduction

- Spectrum is a **limited** resource (interference, collision, etc.).
- Necessary measures to ensure **efficient** and **fair** use of this resource.
- Controlled and owned by the State, that is responsible for these actions.
  - The State must provide geography-based **regulations** for the use of the spectrum.
  - **Licensed spectrum**: allocation of spectrum resources to private companies (e.g., cellular network operators) upon concession fees (auctions).
    - In Italy, 5G spectrum auction in 2018: 6.5B€: https://www.corrierecomunicazioni.it/telco/5g/chiusa-lasta-5g-incasso-oltre-i-65-miliardi/
    - It provides the best quality of service for end customers.
  - **Unlicensed spectrum**: free access to spectrum without any centralized control.
    - Unlicensed does not mean unregulated.
  - **"Reserved" spectrum**: spectrum for public safety, emergency forces, police, miliary.

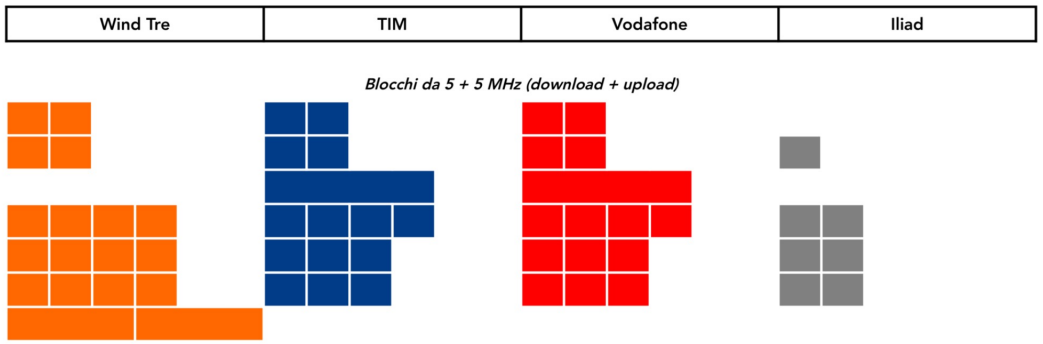
Spectrum

Licensed spectrum (examples)



Spectrum allocation in the US (from 300 MHz to 3 GHz): https://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf

Bande di frequenza italiane			
Frequenza	Banda	Tecnologia	Rete
800 MHz	20	FDD	4G
900 MHz	8	FDD	2G/3G
1500 MHz	32	SDL*	(4G)
1800 MHz	3	FDD	2G/4G
2100 MHz	1	FDD	3G/4G
2600 MHz	7	FDD	4G
2600 MHz	38	TDD*	(4G)



4G LTE frequency bands: https://www.sqimway.com/lte_band.php

LICENSED SPECTRUM

Spectrum

Unlicensed spectrum

- Also referred to as **Instrumental, Scientific, and Medical (ISM)** bands.
- It is available to **any number of customers**, but with no exclusive rights.
- Target: applications with are not lucrative enough to justify the cost of licence, but prove valuable if considered collectively.
  - Notable examples: Wi-Fi, Bluetooth, etc.
- Unlicensed does not mean unregulated → there are still some rules to avoid/minimize **interference**, and to promote **fair use** of resources.
  - **Some regulation mechanisms**: ERP limits, duty cycle, etc.
  - Regulations are not necessarily aligned in all the Regions of the world, but there are some levels of superimposition (e.g., 2.4 GHz ISM band for Wi-Fi).

Spectrum

Unlicensed spectrum in Europe

- At the European level, spectrum is regulated by the European Commission (EC), Electronic Communications Committee (ECC), and the **European Telecommunications Standard Institute (ETSI)**.
- Different rules/limitations are defined, especially:
  - **Effective Radiated Power (ERP)**: it evaluates the emissions of a device.
    - It is related to the Effective Isotropic Radiated Power (EIRP), defined as the power that would have to be used on an isotropic antenna in order to get the same field strength that the tested device produces at the same distance.
    - We have that ERP = EIRP – 2.15.
  - **Duty Cycle (DC)**: it is defined as the ratio, expressed as a percentage, of the maximum transmitter "on" time over one hour, relative to a one hour period.
    - These limitations apply to every receiver, excluding those with LBT capabilities.
    - *1% DC: the max. transmission time of any device is 1% of an hour (i.e., 36 seconds in an hour).*

Spectrum

Unlicensed spectrum in Europe

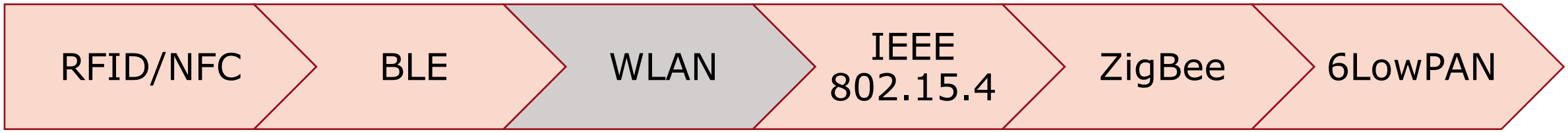
- Some of the most important ISM sub-bands in Europe (focus on IoT use cases).

Range [MHz]	Max. power	Duty cycle	Example	Example IoT scenario
169.4-169.8125	10 mW 500 mW (169.4-169.475)	1% or 0.1% 10% (169.4-169.475)	Wireless M-Bus	Water and gas metering
433.050-434.790	10 mW	10%	RFID, NFC	Metering
863-870	25 mW 500 mW (869.4-869.650)	1% or 0.1% 10% (869.4-869.650)	LoRa, Zigbee	Metering, Smart city, environmental control
2400-2483.5	100 mW	N/A	Bluetooth, Wi-Fi	Smart home
5150-5350	200 mW	Transmission power control	Wi-Fi (802.11)	Smart home
5470-5725	1000 mW	Transmission power control	Wi-Fi (802.11)	Smart home

Short-range

Introduction

- **Short-range**: (generally) cell diameter smaller than 100 m.
- Does not support mobility/handover.
- Can be classified according to the reach of the radio link:
  - Vicinity and proximity networks, from a few cm to ~2-3 m.
  - Wireless Personal Area Networks (WPANs), up to ~10 m.
  - Wireless Local Area Networks (WLANs), up to ~100 m.
- Are sometimes referred to as **Low-Rate WPAN**.



UNIVERSITÀ DEGLI STUDI DI PADOVA

MIME

Master's degree ICT Internet Multimedia Engineering

04 – IoT technologies (short-range)
RFID and NFC

Marco Giordani (marco.giordani@unipd.it)
Department of Information Engineering (DEI) – SIGNET Research Group
University of Padova – Via Gradenigo 6/B, 35131, Padova (Italy)

RFID

Overview

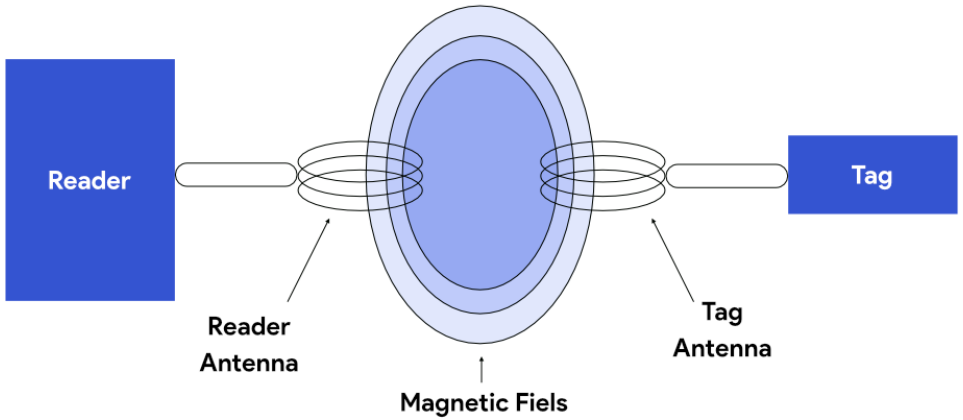
- **Radio Frequency IDentification (RFID)** is a method of remotely storing and retrieving data using devices called RFID tags and RFID readers.
- **Tags** store information, that can be retrieved wirelessly in an automated fashion.
- **Readers** can read/write information from/to the tags.
- Many advantages:
  - Data can be stored and retrieved from the tag automatically with a Reader.
  - Tags can be read without line-of-sight restrictions.
  - Tags can be write-once-read-many (WORM) or rewritable.
  - Other sensors can be combined with RFID.
- Comes with strict critics, e.g., privacy concerns.

RFID

How does it work

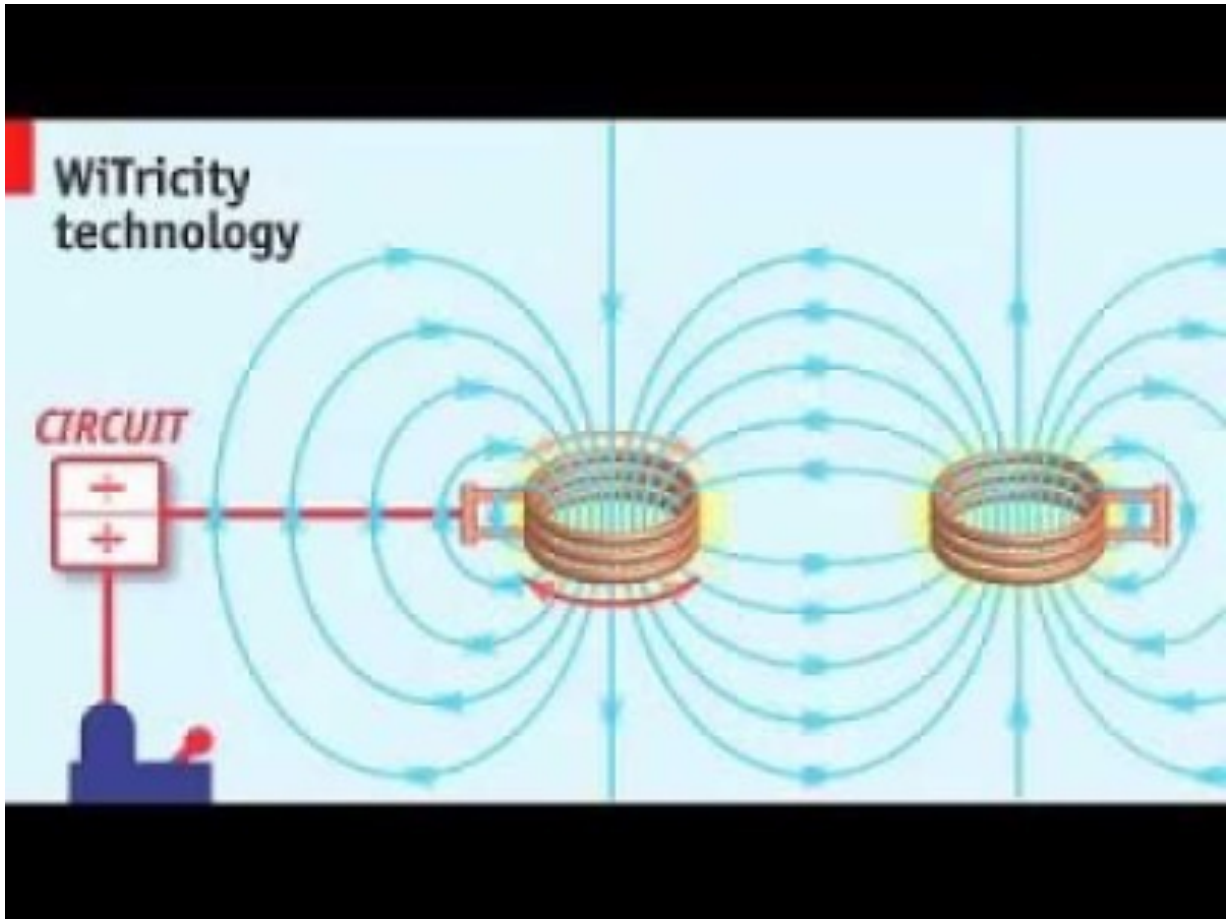
- RFID tags are affixed to objects and stored **information may be written and rewritten to an embedded chip in the tag**.
- Tags can be read remotely when they receive a radio frequency signal from a reader via **inductive (or magnetic) coupling**.
  - Coils in the tag and the reader are coupled together through a magnetic field.
  - It is a sort of Wireless Power Transfer.
- Tags can use this energy to respond.
- Can operate over a range of distances.

https://rfid4u.com/inductive-and-backscatter-coupling/



RFID

How does it work



How Wireless Energy Transfer Works
https://youtu.be/-Wf7aadxBkE?si=e7GMOLnfuQ8he80f

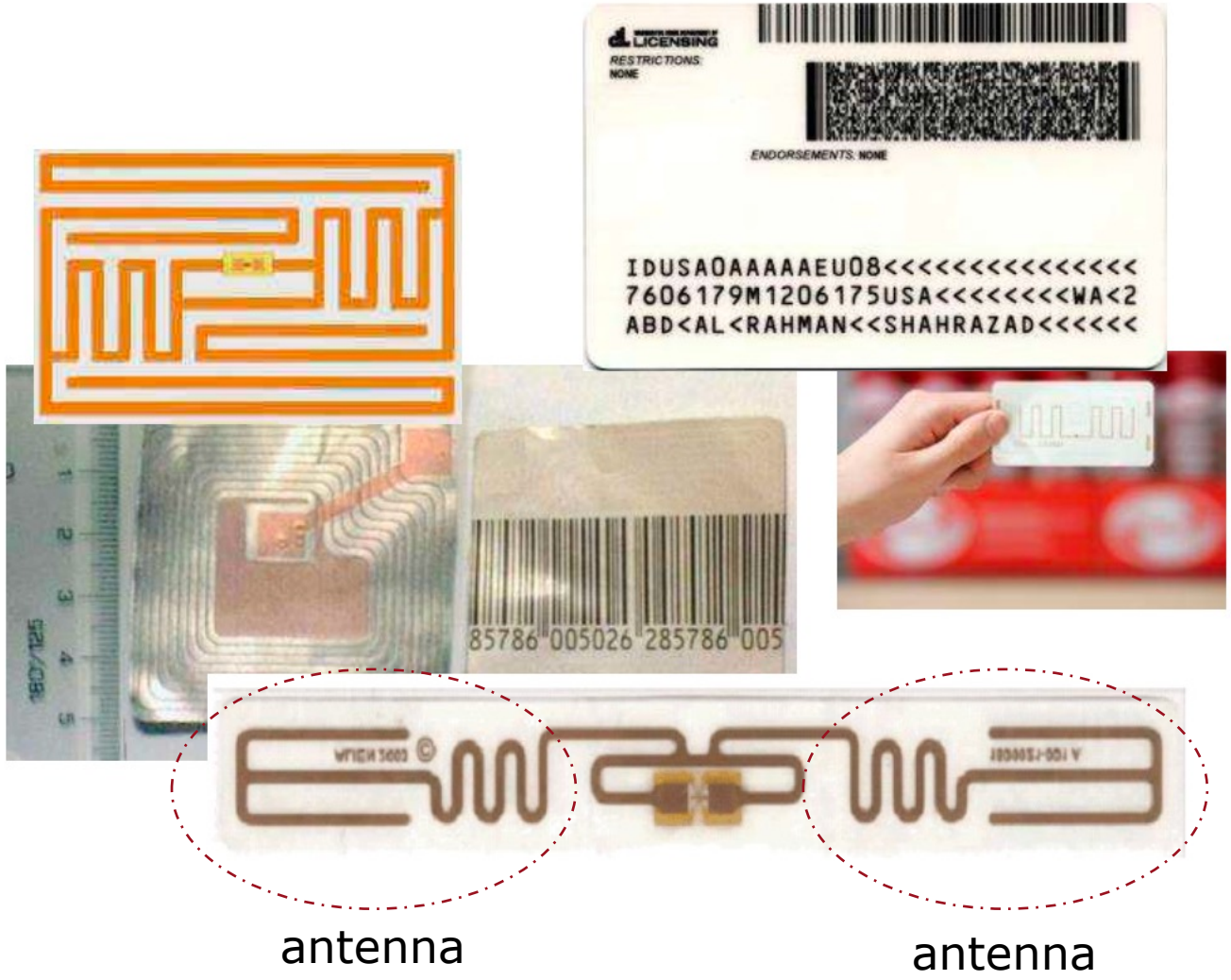
RFID

How does it work

- The coupling occurs in the near-field region.
- Therefore, **the distance between the tag and the reader must be much smaller than the signal wavelength**.
  - Rule of thumb: distance shall be around 15% of the wavelength.
  - It is convenient to operate at low frequency (so the wavelength – and the operational distance – can be larger).
  - At 2.4 GHz (~Wi-Fi), the wavelength is ~0.13 m, so the range would be up to 2 **cm**.
  - At 13.56 MHz, the wavelength is ~22 m, so the range would be up to 3 **m**.

RFID

Tags visualized



RFID

Applications

- Readers monitoring entering and exiting a closed region.
  - Security (RFID in identification cards and/or passports).
  - Access control (e.g., Telepass).
  - Merchandise in stores.
  - Logistics.
  - Ticketing.
  - NFC in phones (more on this later).
- Readers tracking an RFID-tagged object.
  - Business process monitoring (RFID tags on pallets).
- Tags marking a spatial location.
  - Sport match/competition.

RFID

Applications: Passport

- RFID tags are used in passports.
- RFID tags have been used in new British and American passports since 2006.
- **The tags will store the same information printed in the passport** and will also include a digital photograph of the owner.
- To this day, RFID tags consist of the following elements:
  - A microchip that contains information RFID readers can interpret.
  - A tag antenna to send and receive signals.
  - A substrate to hold all components together.

US «biometric» passport with RFID tag

RFID

Applications: Metro card

- Balance is maintained on the card → Cryptographically secured.
- The "reader" updates the balance as you enter/leave the metro station.
  - Enter: record when and where you boarded.
  - Leave: update balance on the card based on the trip.
  - These operations are entirely at the reader.
- Readers record all trips and send updates to a server about the balance of cards.
  - Auditing trail, lost cards, etc.
  - Riders can check their balance online.

Applications: Merchandise in stores (1/3)

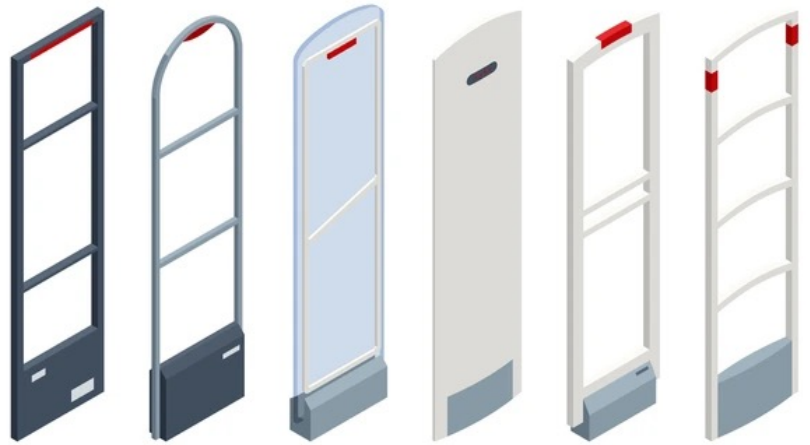
- **Data storage**: Store more data than barcode labels (can be changed at any time).
- **Improved quality**: Identify returned or counterfeit products by tracking goods from manufacture to storage.
- **Efficiency and speed**: Automatically read many tags from a distance.
- **Better stock control**: Locate product in a shop's stock. It allows the inventory to be taken as and when sales or returns.
- **Durability**: resistant to handling and external aggression.

Clothing RFID tag

Applications: Merchandise in stores (2/3)

- Tags and readers can serve for **anti-shoplifting** and **authenticity** verification.
  - If you walk through the doorway without paying for something, the radio waves from the transmitter (hidden in the door gates) are picked up by the coiled metal antenna in the tag. This generates a tiny electrical current that makes the label transmit a new radio signal of its own at a very specific frequency. The receiver (also hidden in the door gate) picks up the radio signal that the tag transmits and **sounds the alarm**.

QUESTION: Why are checkout alarm gates so «tall»?



Applications: Merchandise in stores (3/3)

- **Theft protection**: The RFID chips are automatically deactivated at the checkout and thus reduce the risk of theft or human error.
  - The checkout assistant passes your item over or through a deactivating device. This destroys or deactivates the electronic components in the tag so they no longer pick up or transmit a signal when you walk through the gates.

Example of an RFID checkpoint deactivation pad

RFID

RFID vs. barcode

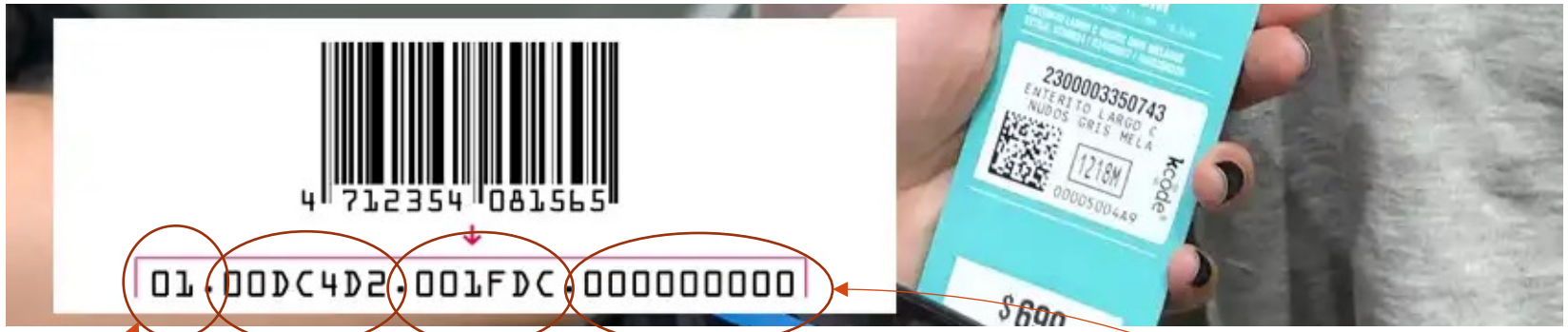
Feature	RFID	Barcode
Rate	Thousands	One at a time
Range	Up to a few meters	~6 meters
Speed	Very fast (ms)	Slow
Line-of-sight	Not necessary	Necessary
Identification	Can **uniquely** identify items	Only identifies the type of item

Electronic Product Code (EPC)

- In 2003 EPCGlobal was formed to promote RFID standards.
- It defined a standard for the **Electronic Product Code (EPC),** and standards for coding and modulation.
  - Designed to be unique across all physical objects in the world, over all time, and across all categories of objects.
  - Intended for use by business applications that need to track all diverse physical objects.
  - EPC data is stored on the RFID tag (can be accessed using reader).
  - Locate EPC Information Services (EPCIS), using Web Services like SOAP and WSDL.

RFID

Electronic Product Code (EPC)



Header (8 bits)
Partitioning scheme
256 instances

Object class (24 bits)
Product type
> 16M instances

EPC manager (28 bits)
Manufacturer ID
>268M instances

Serial number (36 bits)
Unique for each item
>68B instances

RFID

Types of tag

- **Passive**: rely on an external energy source to transmit.
  - In the form of a reader that transmits energy.
  - Relative short range.
  - Very cheap – used everywhere today!
- **Semi-passive**: have their own battery, but it is only activated when detecting the reader's field (expected lifetime duration: 3-5 years).
- **Active**: have a battery to transmit.
  - Has longer transmission range.
  - Can initiate transmissions and transmit more information (it is more like a sensor).

RFID

Passive tag

- **Operational frequency**
  - Low Frequency (LF): tag/readers at 120-140 kHZ.
  - High Frequency (HF): tag/readers in the 13.56 MHz ISM band.
  - Ultra-High Frequency (UHF): tag/readers at {433, 860, 960} MHz, based on the region.
  - "Microwave": tag/readers at 2.4 and 5.8 GHz, and millimeter wave.
- **Types of tag**
  - Vicinity: ISO/IEC 15693 standard, with distance up to 1-1.5 m.
  - Proximity: ISO/IEC14443, with distance up to 2-10 cm.
    - Inherent robustness against interception, interference, and unwanted readings.
    - Ticketing, access control, contactless payment, …
- Transmission consists of a **stream of bits** (plus CRC).
  - CRC allows reader to verify the value it reads

RFID

Passive tag (PHY Layer)

- Different modulations used by reader and tag.
  - Tags are cheap and dumb, so only **changes in amplitude of the reader signal** can be used (advanced modulations like PSK or QAM are not available).
  - Passive tag modulations differ from typical radio communications schemes because the reader signal also powers the tag, so it is **useful to have the signal be at its maximum value most of the time *(also, short-range high-quality links)*.**

1. The reader sends a series of sync pulses to help the tags set their clock.
2. A binary '0' is tx by turning the reader power down or off for a brief time, after which the power is turned back up for the rest of the symbol.
3. A binary '1' is tx by turning the power down for a longer time.
4. The “null” symbol is used to signal tags to change their state.

More details: https://www.enigmatic-consulting.com/Communications_articles/RFID/Old_RFID_protocols.html

RFID

Passive tag (MAC Layer)

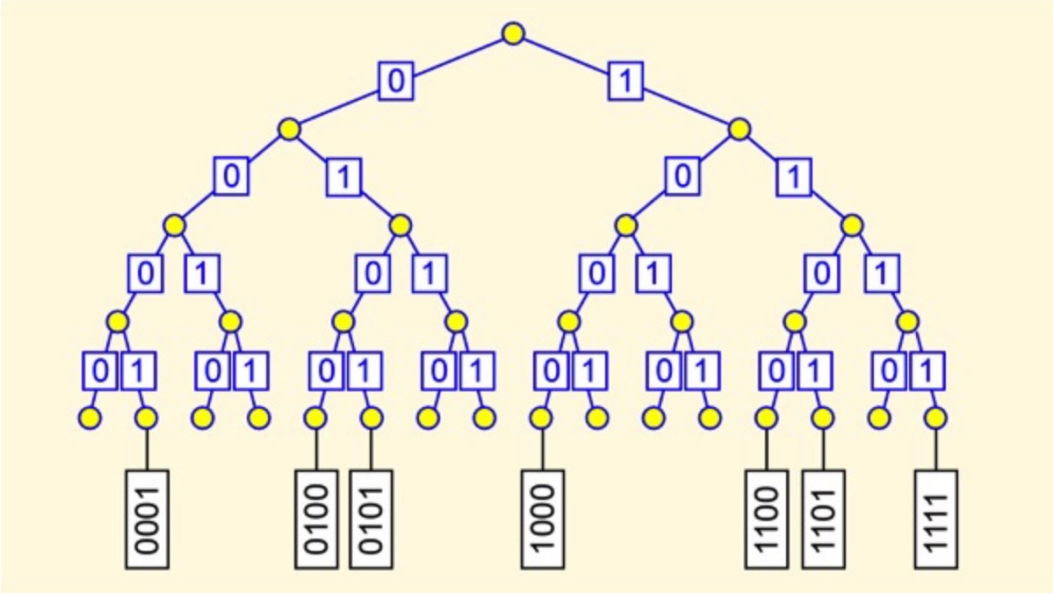
- MAC for tags is a challenge (very high concentrations of tags).
  - If only one reader is present: no need for MAC on the reader.
  - In case of multiple readers:
    - Tags are dumb, and cannot run sophisticated protocols (carrier sense, RTS/CTS, ..).
    - May also deal with multiple readers operating in the same environment.
- Two types of schemes used (standard):
  - **ALOHA**: tags transmit with a random backoff.
  - **Binary tree resolution**: reader explores a tree of tag values.
    - Send requests to tags with IDs that start with a certain string.
    - Narrow down search until one tag responds.

RFID

Passive tag (MAC Layer): Binary tree resolution

At each step:

- If no tags respond: skip the subtree (it does not contain any tags)
- If multiple tags respond, continue the breadth first search.
- If one tag responds: you have found a tag!



More details: https://www.enigmatic-consulting.com/Communications_articles/RFID/Old_RFID_protocols.html

NFC

Overview

- **Near Field Communication (NFC)** is a device that combines the functionality of an RFID reader and a tag.
  - Integral part of mobile devices (e.g., mobile phones reading tickets / bank cards).
  - Reader mode: NFC devices can access data from an object with an embedded RFID tag.
  - Peer-to-peer: Allows **two-way** communication between NFC devices, can act as smart tag.
  - Passive communication: one device acts as a reader and the other as a tag.
  - Active communication: both devices alternatively act as readers.
  - Since NFC devices can read and write, they must check for collisions.
- Operates at 13.56 MHz (HF), and is compatible to international standards.

RFID vs. NFC

Comparison

Feature	RFID	NFC
Network type	Point-to-point	Point-to-point
Communication	Unidirectional	Bidirectional (two-way)
Range	Up to 100 m	<0.2 m
Frequency	LF/HF/UHF/Microwave	HF (13.56 MHz)
Bitrate	Varies with frequency	Up to 424 KHz
Power consumption	Varies with frequency	<15 mA
Continuous sampling	No	Yes