Modern Wireless Technologies

Sommerakademie in Leysin
AG 2 – Effizientes Rechnen

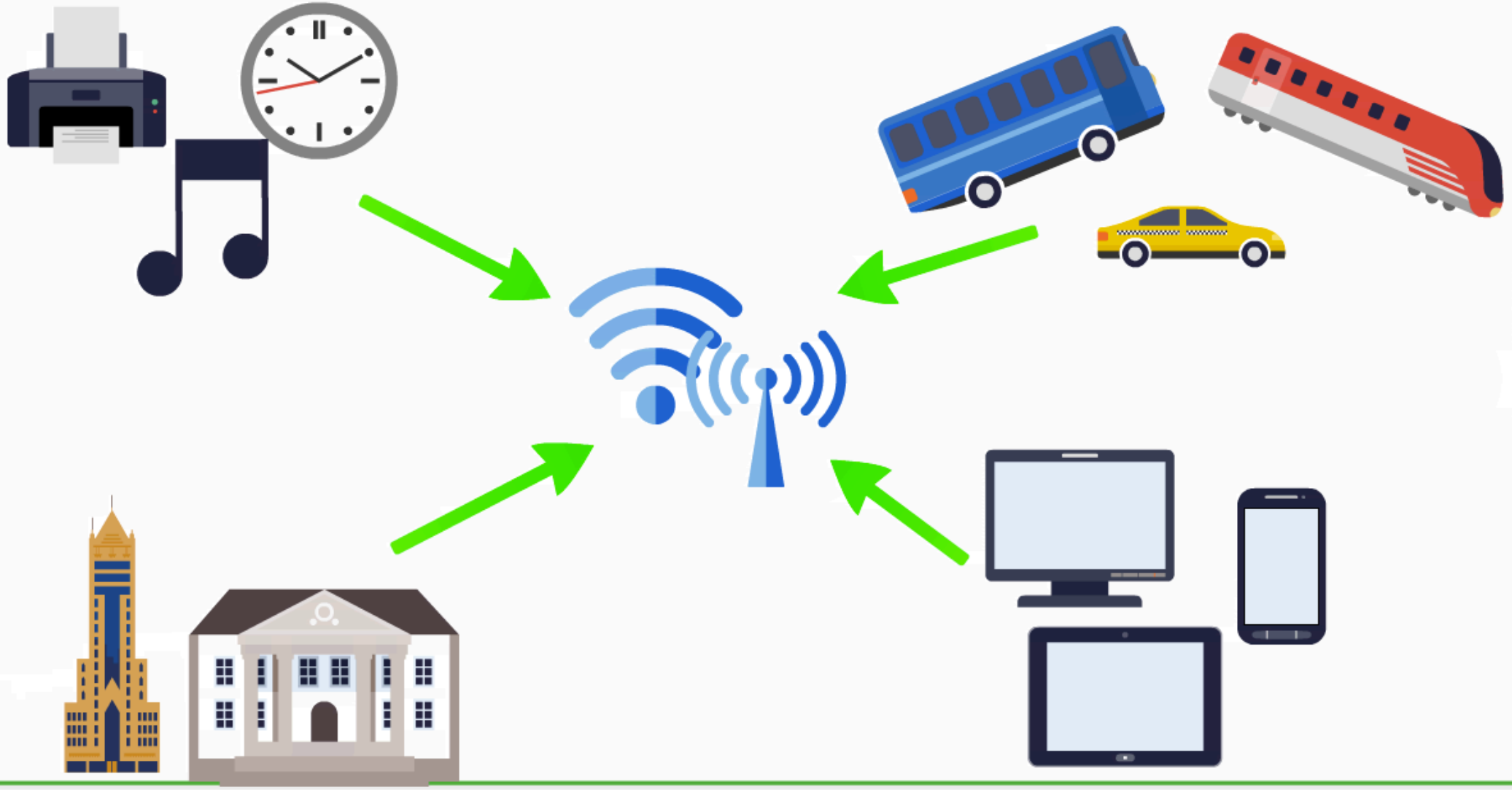
Matthias Kappeler

Goethe Universität Frankfurt

August 2016

Contents

Introduction



Different Types of Wireless Networks

PAN

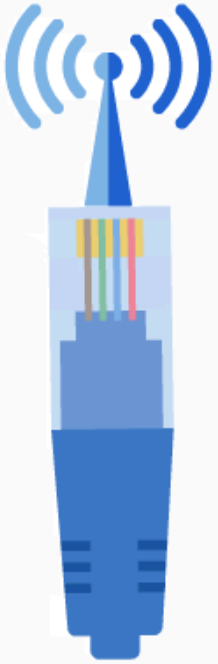
Personal Area Network

- Within the reach of a Person
- Cable replacement for Peripherals
- Standards: Bluetooth, ZigBee, NFC

LAN

Local Area Network

- Within a building or campus
- Wireless extension of wired networks
- Standards: IEEE 802.11 (WiFi)



MAN

Metropolitan Area Network

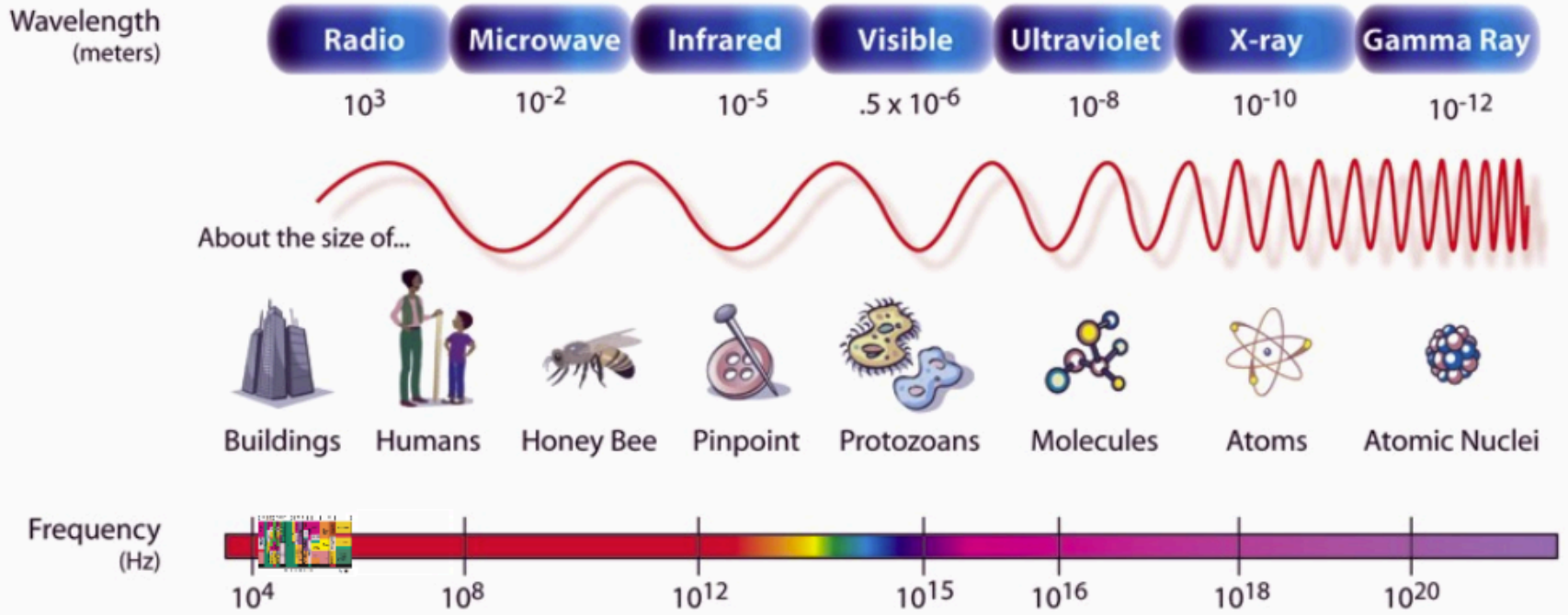
- Within a city
- Wireless inter-network connectivity
- Standards: IEEE 802.15 WiMAX

WAN

Wide Area Network

- Worldwide
- Wireless network access
- Standards: Cellular (UMTS, LTE, etc.)

The Electromagnetic Spectrum


Wavelength
(meters)
Radio
Microwave
Infrared
Visible
Ultraviolet
X-ray
Gamma Ray
10^{3}
10^{-2}
10^{-5}
$.5 \times 10^{-6}$
10^{-8}
10^{-10}
10^{-12}
About the size of...
Buildings
Humans
Honey Bee
Pinpoint
Protozoans
Molecules
Atoms
Atomic Nuclei
Frequency
(Hz)
10^{4}
10^{8}
10^{12}
10^{15}
10^{16}
10^{18}
10^{20}

2300.0 2305.0 2310.0 2320.0 2345.0 2360.0 2390.0 2395.0 2417.0 2450.0 2483.5 2495.0 2500.0 2655.0 2690.0 2700.0 2900.0 3000.0

FIXED
MOBILE**
SPACE RESEARCH (space-to-Earth) (deep space)
Amateur
RADIOLOCATION
Amateur
RADIOLOCATION
MOBILE
FIXED
BROADCASTING SATELLITE
MOBILE**
FIXED
Mobile
Radio-location
BROADCASTING - SATELLITE
Fixed
Radiolocation
MOBILE
RADIOLOCATION
Fixed
FIXED
BROADCASTING SATELLITE
Mobile
Radio-location
Fixed
RADIOLOCATION
AMATEUR
AMATEUR
Radiolocation
Amateur
Radiolocation
MOBILE
FIXED
MOBILE SATELLITE (space-to-Earth)
RADIODETERMINATION-SATELLITE (space-to-Earth)
MOBILE SATELLITE (space-to-Earth)
MOBILE**
FIXED
MOBILE**
FIXED
FIXED
MOBILE**
Radio astronomy
Space research (passive)
Earth exploration-satellite (passive)
EARTH EXPLORATION-SATELLITE (passive)
RADIO ASTRONOMY
SPACE RESEARCH (passive)
AERONAUTICAL RADIONAVIGATION
METEOROLOGICAL AIDS
Radiolocation
RADIOLOCATION
Radiolocation
MARITIME RADIO-NAVIGATION

ISM – 2450.0± .50 MHz

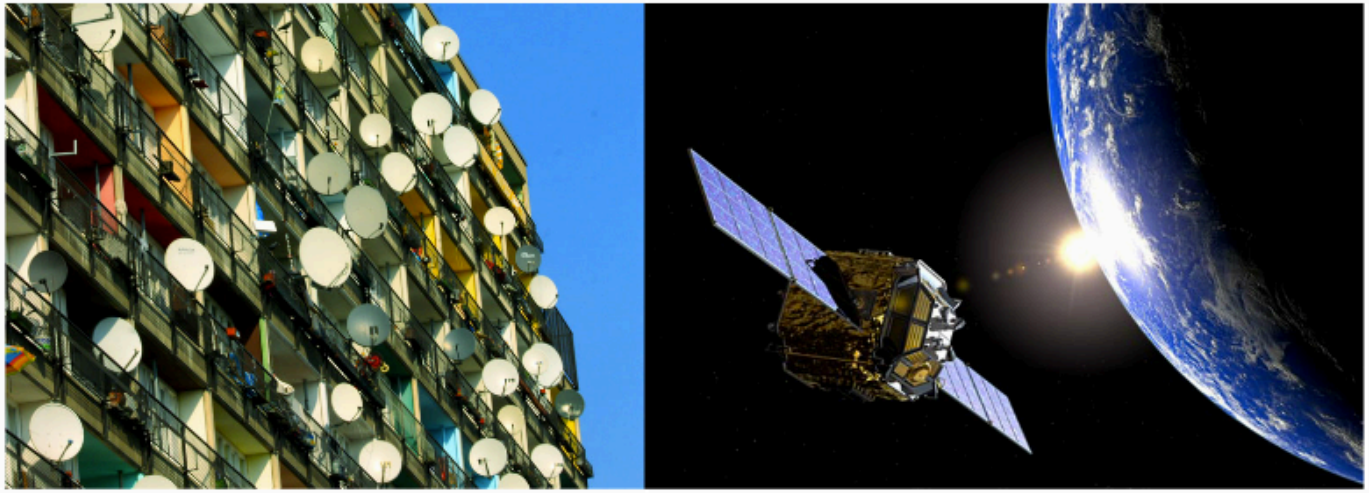
Industrial, Scientific, Medical

3 GHz

Limitation

$$C = BW \cdot log_2(1 + \frac{S}{N})$$

- C is the channel capacity and is measured in bits per second.
- BW is the available bandwidth, and is measured in hertz.
- S is signal and N is noise, and they are measured in watts.



Communication Satellites

GEO

- Latency: 270 ms
- Hight: 35000 km
- Sats needed: 3

MEO

- Latency: 35-85 ms
- Hight: 7000-15000 km
- Sats needed: 10

LEO

- Latency: 1-7 ms
- Hight: 200-2000 km
- Sats needed: 50

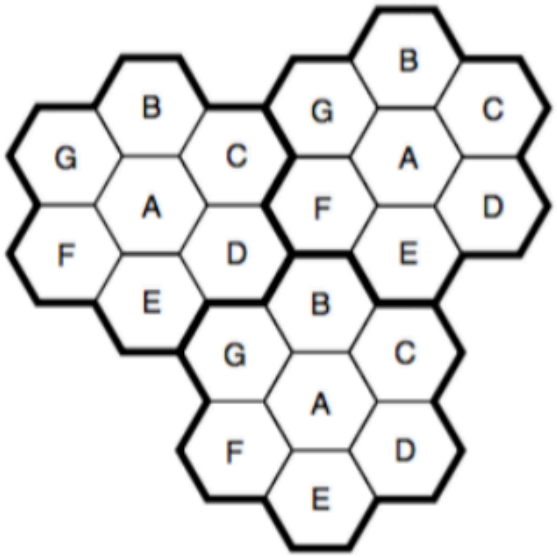
Television

Pay-TV

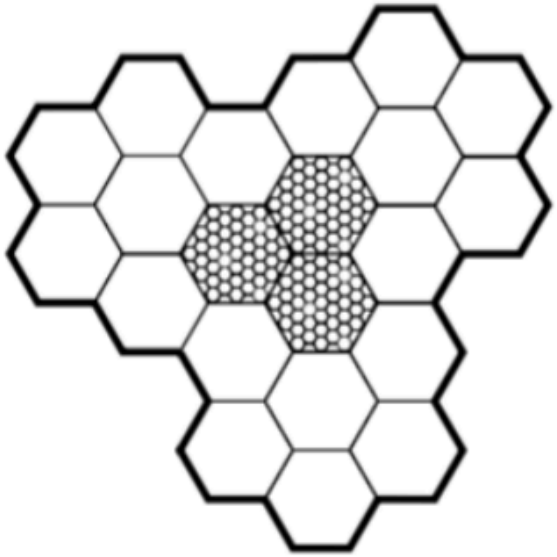
Military purposes

Communication

The Mobile Phone System



(a)



(b)

(a) (b) (c)

Generation	Organization	Release	
2G	3GPP	GSM	9,6 Kbit/s
	3GPP2	IS-95 (cdmaOne)	
2.5G, 2.75G	3GPP	GPRS, EDGE (EGPRS) ★	172 / 384 Kbit/s
	3GPP2	CDMA2000	
3G	3GPP	UMTS	
	3GPP2	CDMA 2000 1x EV-DO Release 0	
3.5G, 3.75G, 3.9G	3GPP	HSPA, HSPA+, LTE ★	
	3GPP2	EV-DO Revision A, EV-DO Revision B, EV-DO Advanced	
4G	3GPP	LTE-Advanced, HSPA+ Revision 11+ ?	

4G

- Interoperable with previous wireless standards (3G and 2G)
- 100 Mbit/s data rate for mobile clients and Gbit/s when stationary
- Dynamic allocation and sharing of network resources between users

	HSPA+	LTE	LTE-Advanced
Peak downlink speed (Mbit/s)	168	300	3,000
Peak uplink speed (Mbit/s)	22	75	1,500
Maximum MIMO streams	2	4	8
Idle to connected latency (ms)	< 100	< 100	< 50
Dormant to active latency (ms)	< 50	< 50	< 10
User-plane one-way latency (ms)	< 10	< 5	< 5

SMS and MMS

- distributed denial of service (DDoS)
- Virus via MMS

Attacks based on the GSM networks

Wireless Lan

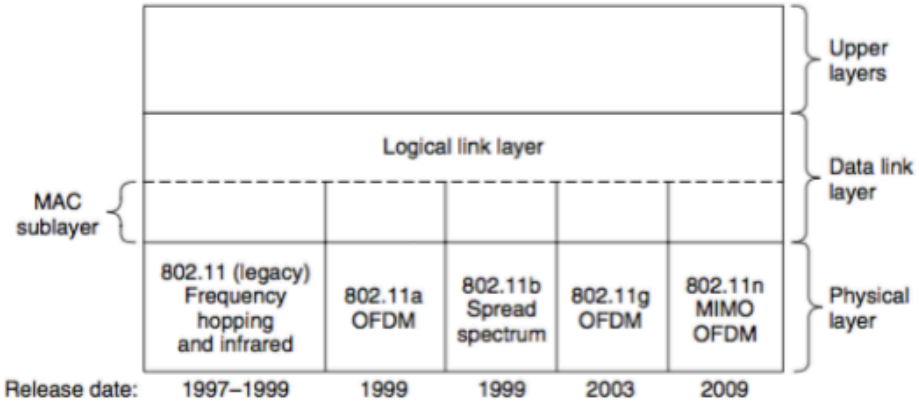
Facts:

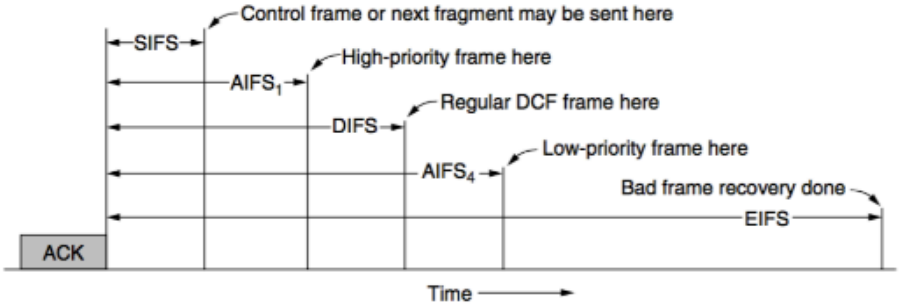
- WiFi provides no bandwidth or latency guarantees or assignment to its users.
- WiFi provides variable bandwidth based on signal-to-noise in its environment.
- WiFi transmit power is limited to 200 mW, and likely less in your region.
- WiFi has a limited amount of spectrum in 2.4 GHz and the newer 5 GHz bands.
- WiFi access points overlap in their channel assignment by design.
- WiFi access points and peers compete for access to the same radio channel.

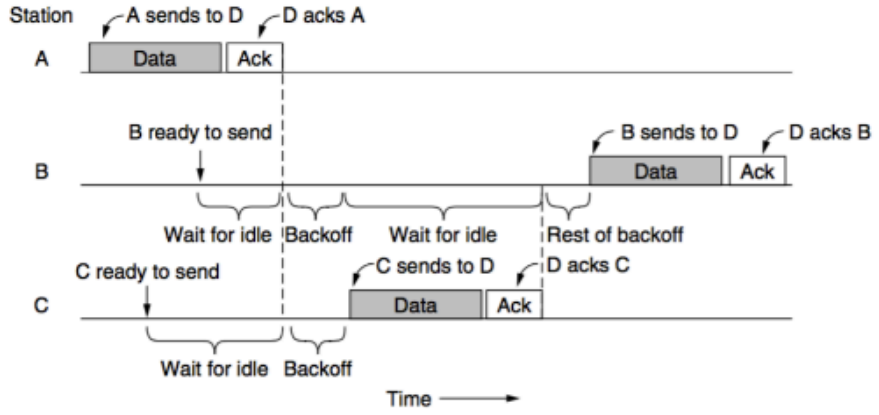
802.11 protocol	Release	Freq (GHz)	Bandwidth (MHz)	Data rate per stream (Mbit/s)	Max MIMO streams
b	Sep 1999	2.4	20	1, 2, 5.5, 11	1
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1
n	Oct 2009	2.4	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	4
n	Oct 2009	5	40	15, 30, 45, 60, 90, 120, 135, 150	4
ac	~2014	5	20, 40, 80, 160	up to 866.7	8

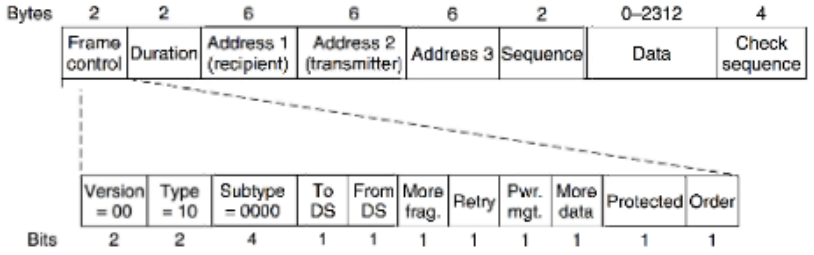
802.11 protocol	Release	Freq (GHz)	Bandwidth (MHz)	Data rate per stream (Mbit/s)	Max MIMO streams
b	Sep 1999	2.4	20	1, 2, 5.5, 11	1
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1
n	Oct 2009	2.4	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	4
n	Oct 2009	5	40	15, 30, 45, 60, 90, 120, 135, 150	4
ac	~2014	5	20, 40, 80, 160	up to 866.7	8

WiFi-Protocol



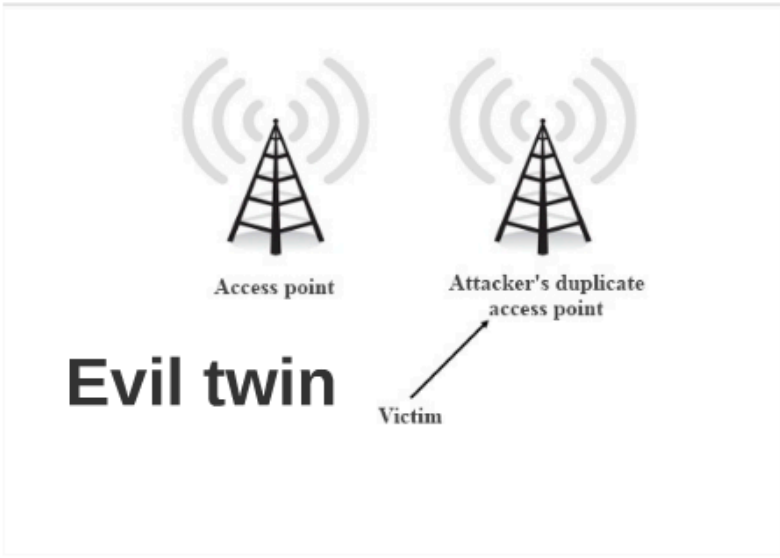




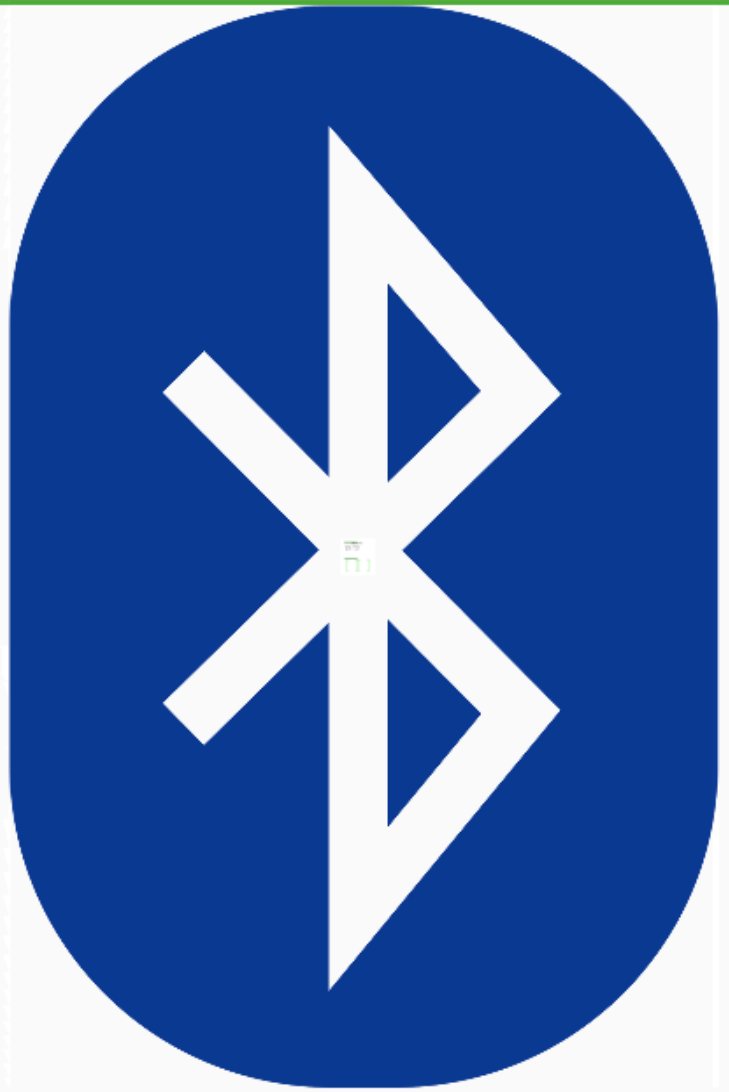


WEP

WPA / WPA2


Access point
Attacker's duplicate access point
Evil twin
Victim

Bluetooth



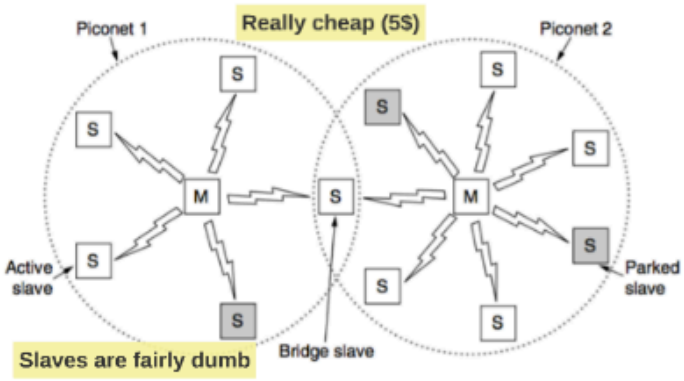
IEEE 802.15.1

Bluetooth v4

- Speed: 25 Mbit/s
- Range: 200 feet (60.96 m)

Bluetooth v5

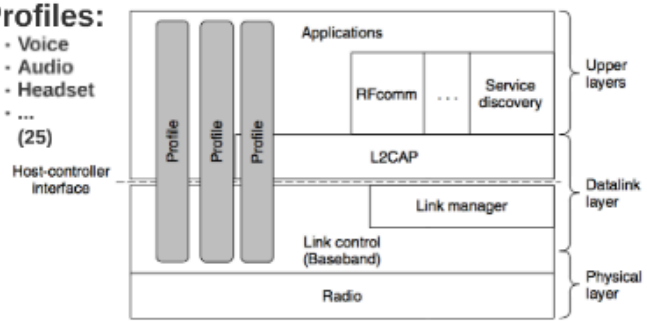
- Speed: 50 Mbit/s
- Range: 800 feet (243.84 m)



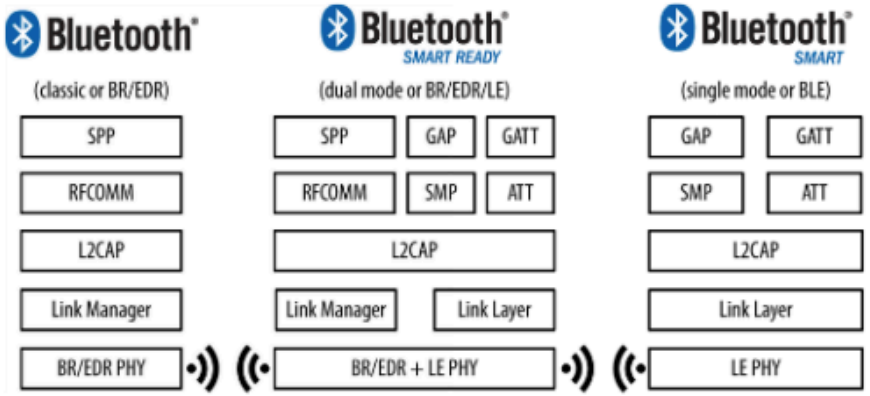
Version 1-3
Bluetooth

Profiles:
- Voice
- Audio
- Headset
- ...

(25)



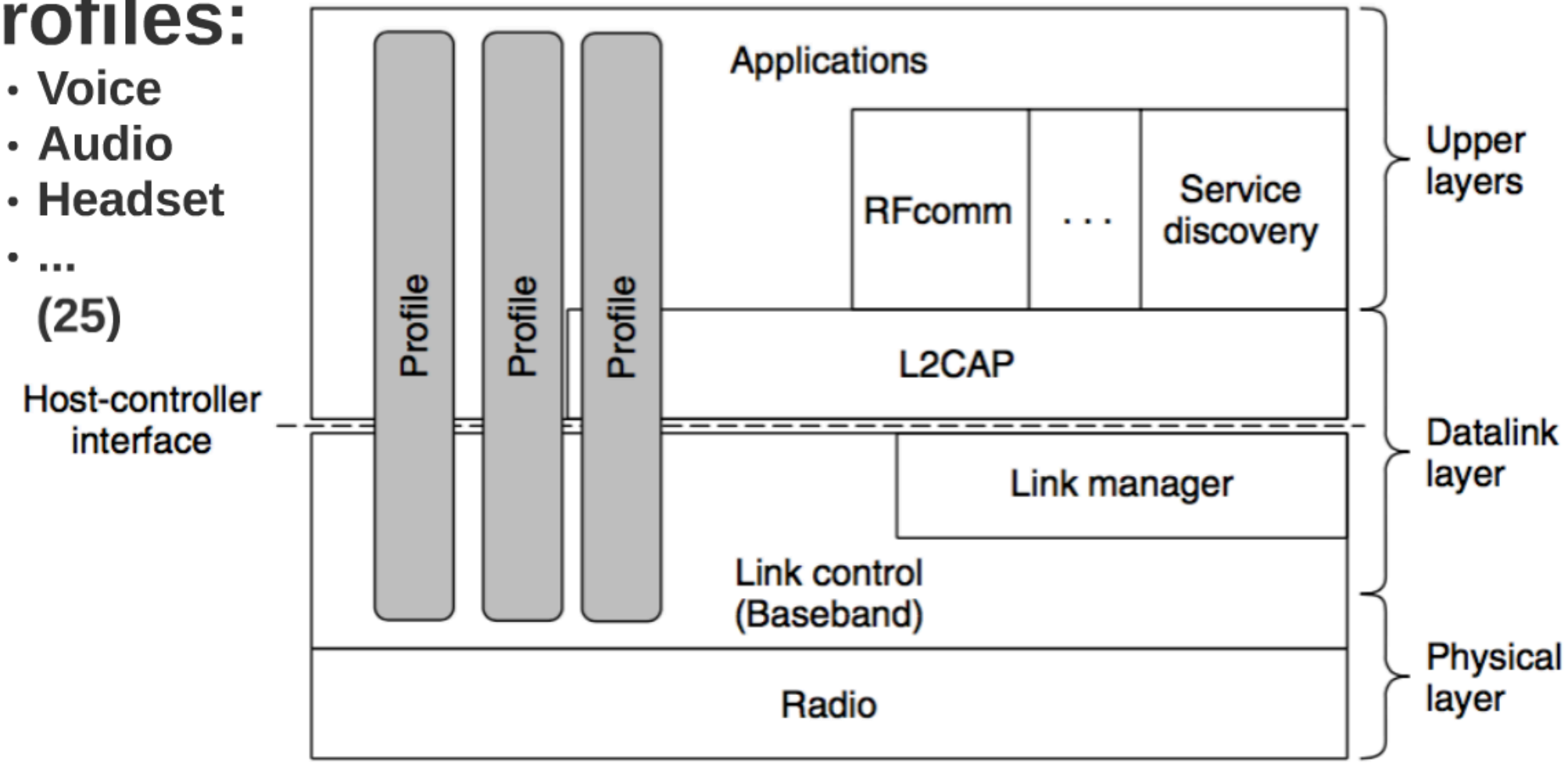
Version 4
Bluetooth LE
Low Energy

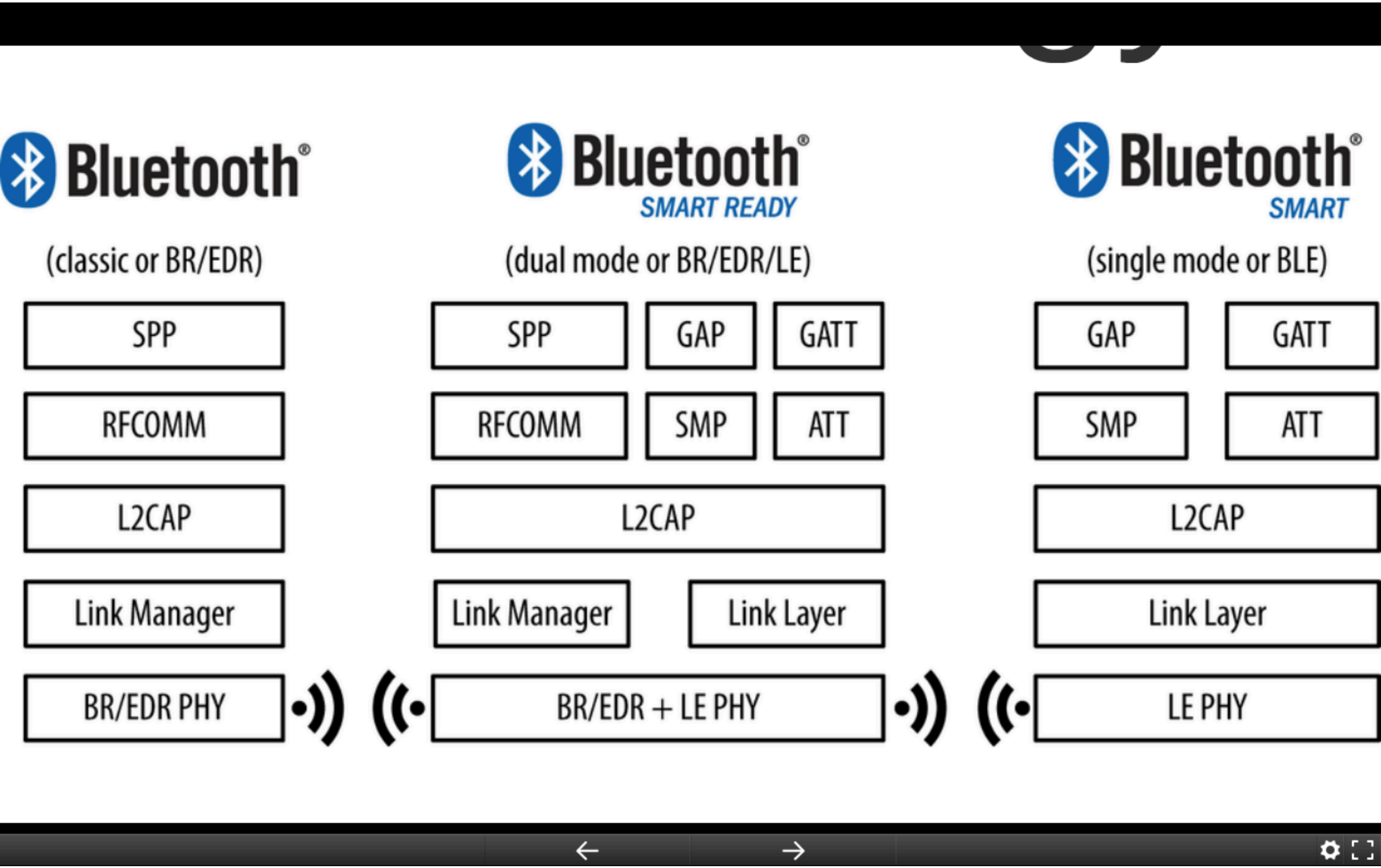


Profiles:

- Voice
- Audio
- Headset
- ...

  (25)




Bluetooth
(classic or BR/EDR)
SPP
RFCOMM
L2CAP
Link Manager
BR/EDR PHY
Bluetooth
SMART READY
(dual mode or BR/EDR/LE)
SPP
GAP
GATT
RFCOMM
SMP
ATT
L2CAP
Link Manager
Link Layer
BR/EDR + LE PHY
Bluetooth
SMART
(single mode or BLE)
GAP
GATT
SMP
ATT
L2CAP
Link Layer
LE PHY

Bluejacking

Bluesnarfing

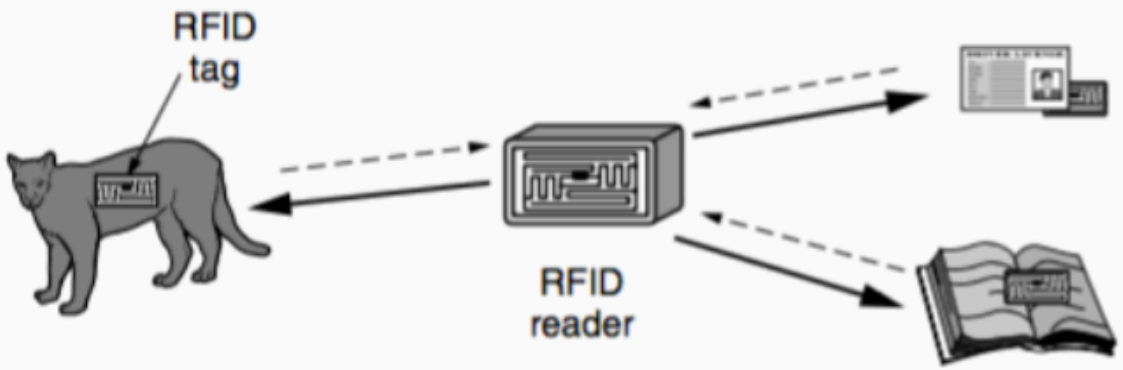
Bluebugging

Options to mitigate against Bluetooth security attacks include:

- Enable Bluetooth only when required
- Enable Bluetooth discovery only when necessary, and disable discovery when finished
- Do not enter link keys or PINs when unexpectedly prompted to do so
- Remove paired devices when not in use
- Regularly update firmware on Bluetooth-enabled devices

RFID

Passive



Active

UHF RFID
Ultra-High Frequency

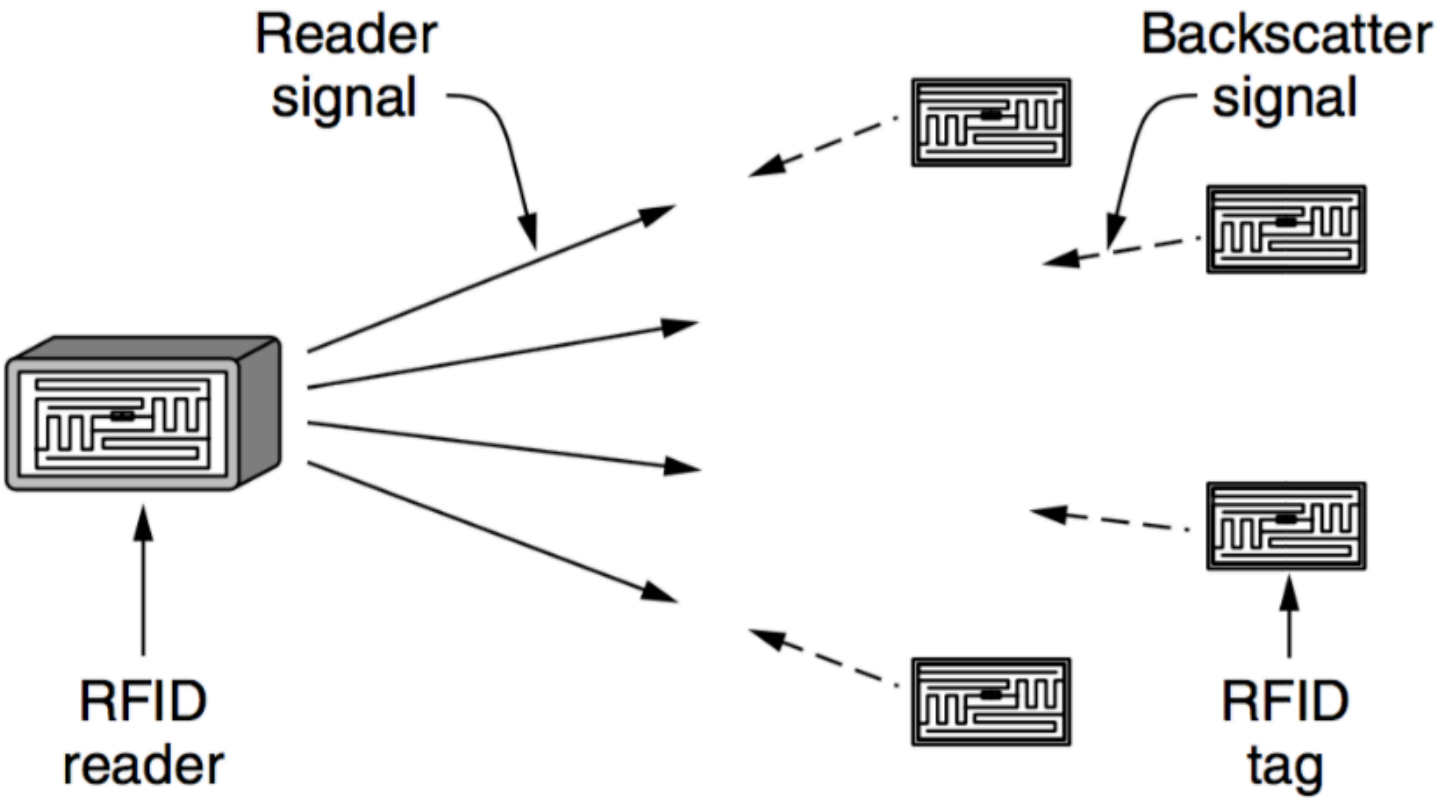
- Range: several meters
- Technology: backscatter
- Frequency: 902-928 MHz
- Application: shopping pallets and some drivers licenses

HF RFID
High Frequency

- Range: less than a meter
- Technology: induction
- Frequency: 13.56 MHz
- Application: Passports, credit cards and noncontact payment systems

LF RFID
Low Frequency

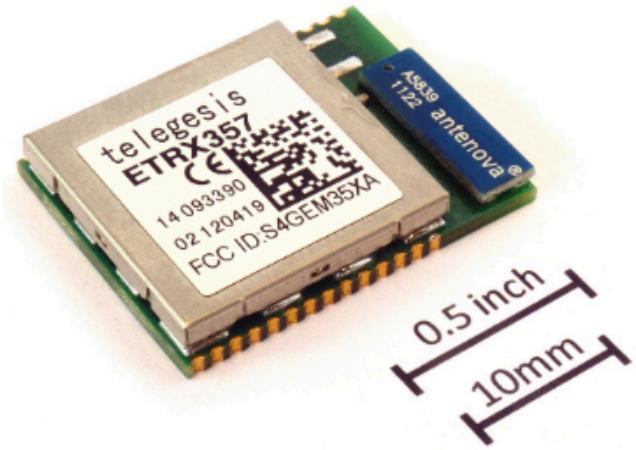
- Range: really short
- Technology: induction
- Frequency: 30–500 kHz
- Application: animal tracking

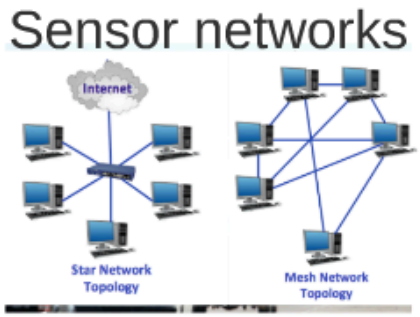

Reader
signal
Backscatter
signal
RFID
reader
RFID
tag

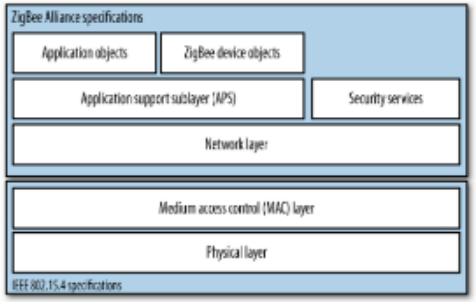
- Password Protection on Tag Memory
- Physical Locking of Tag Memory
- Authentication of the “Author” in Tag Memory
-
- Reader Protection
- Read Detectors
-
- Kill Tag
- Faraday Cage
- Active Jamming
-
-
-

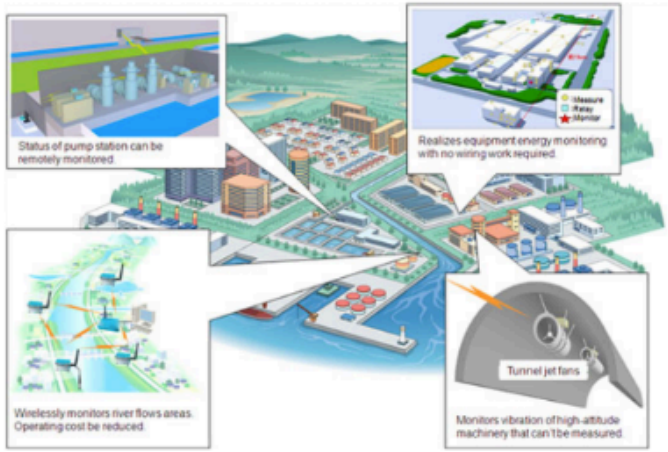
ZigBee

It is based on IEEE 802.15.4 which specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs).

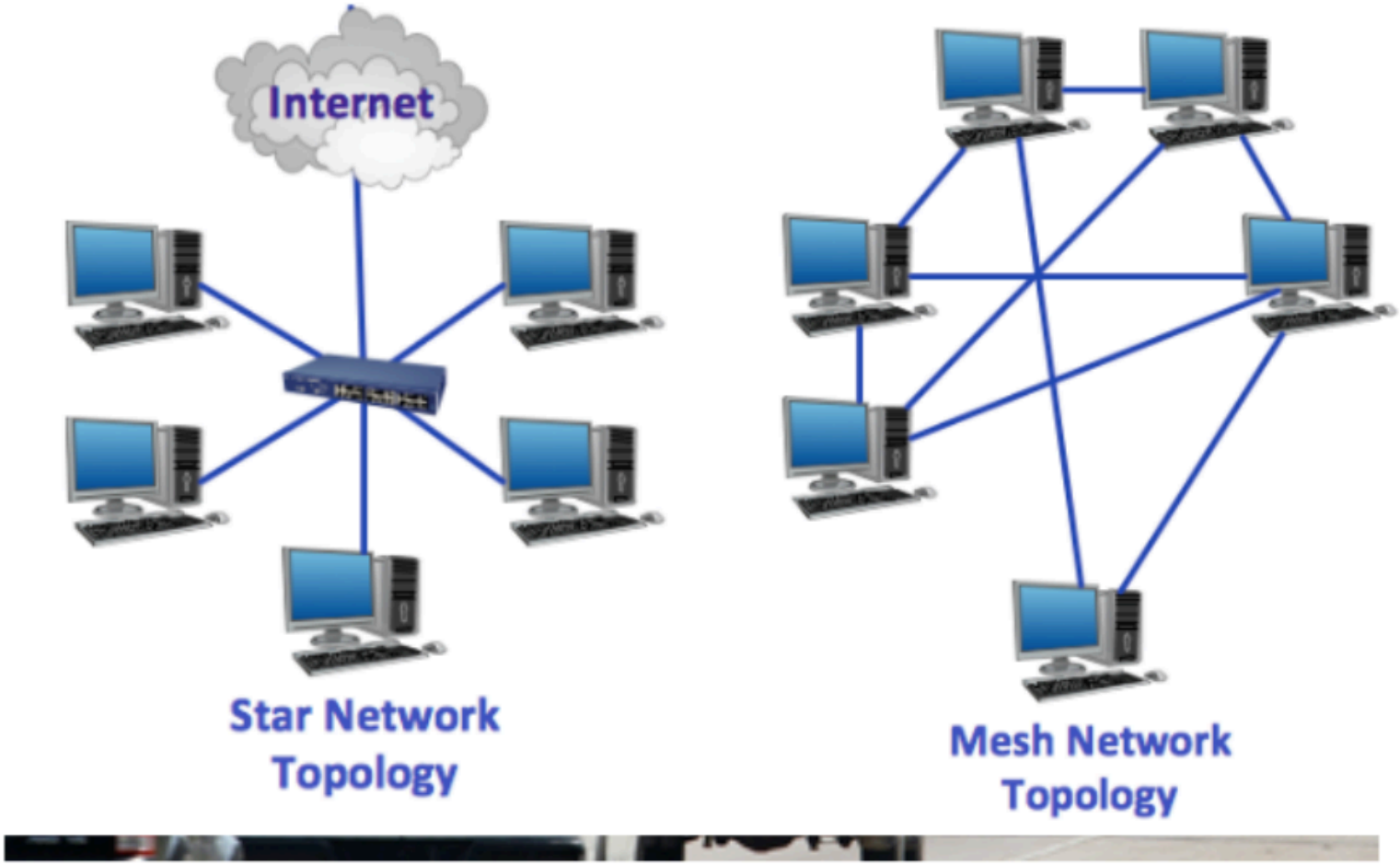


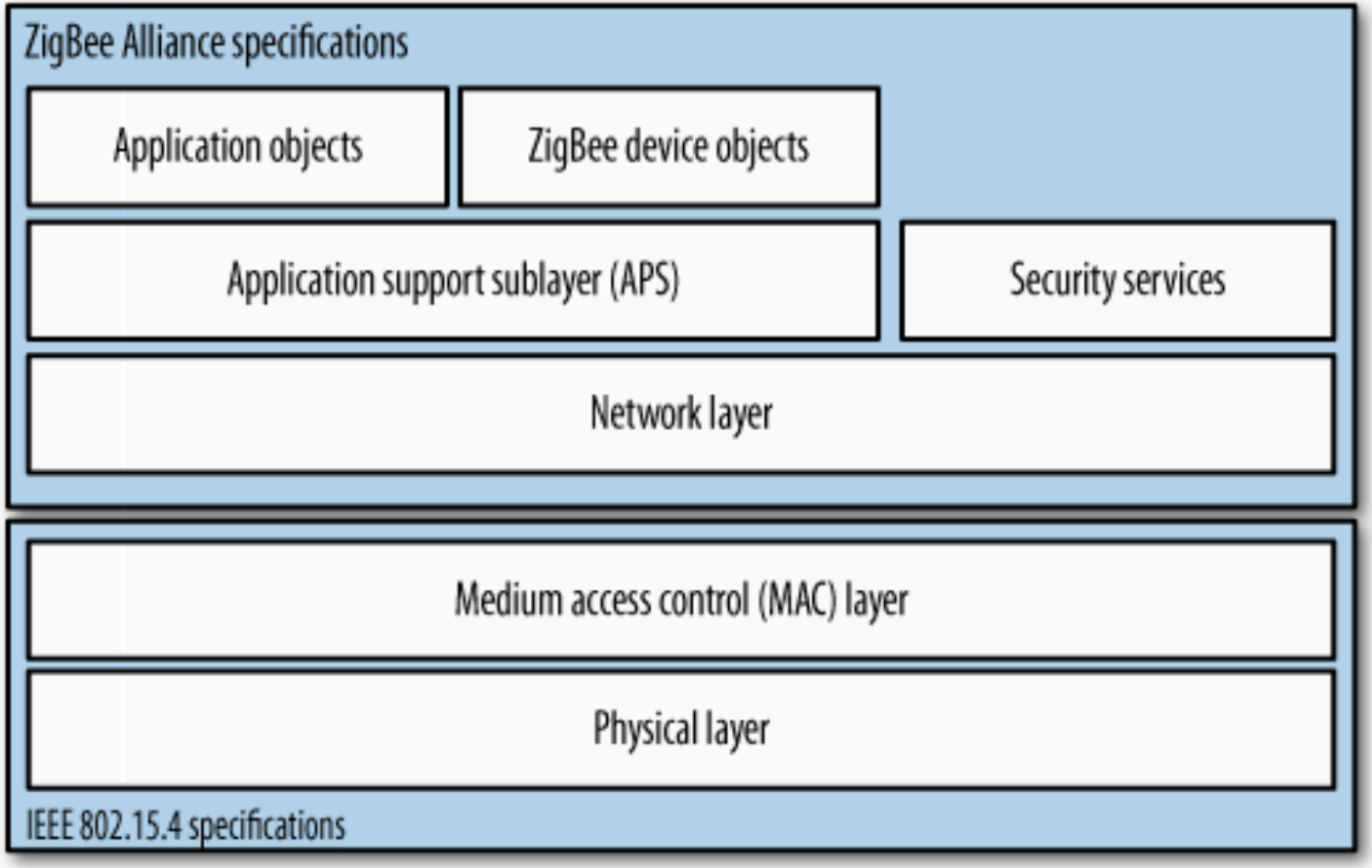






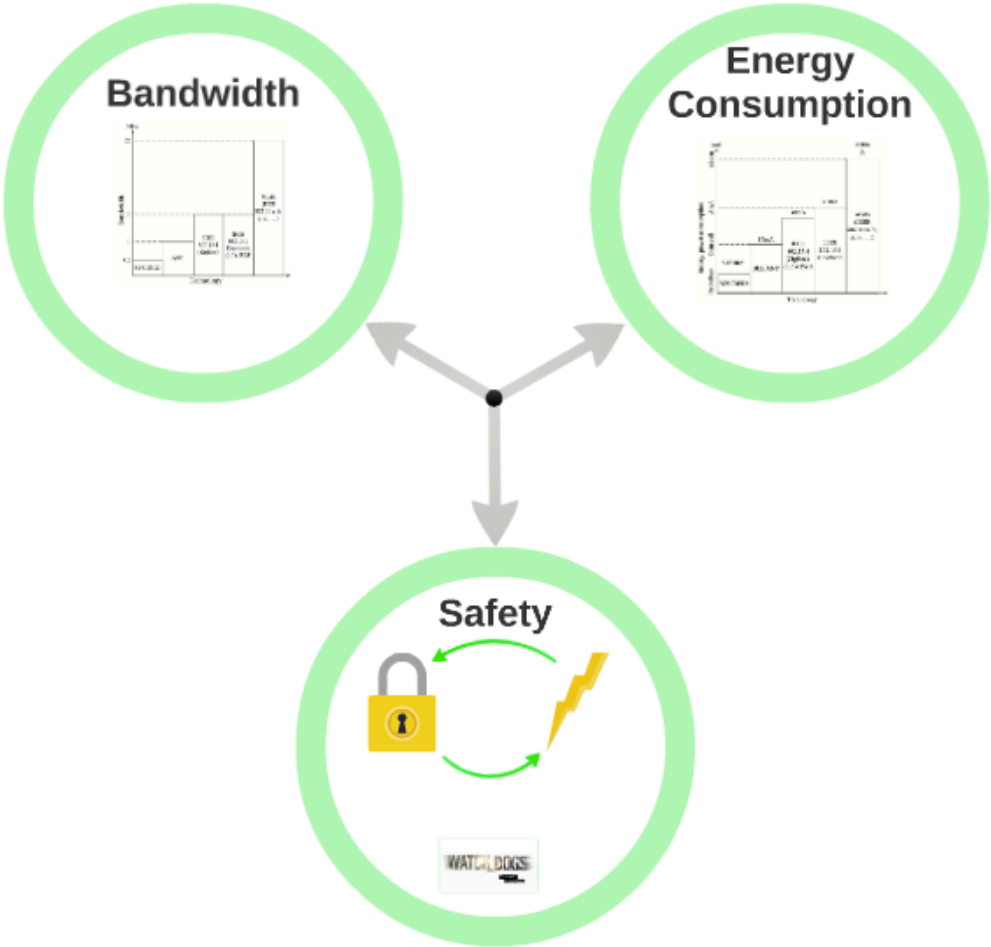
Sensor networks



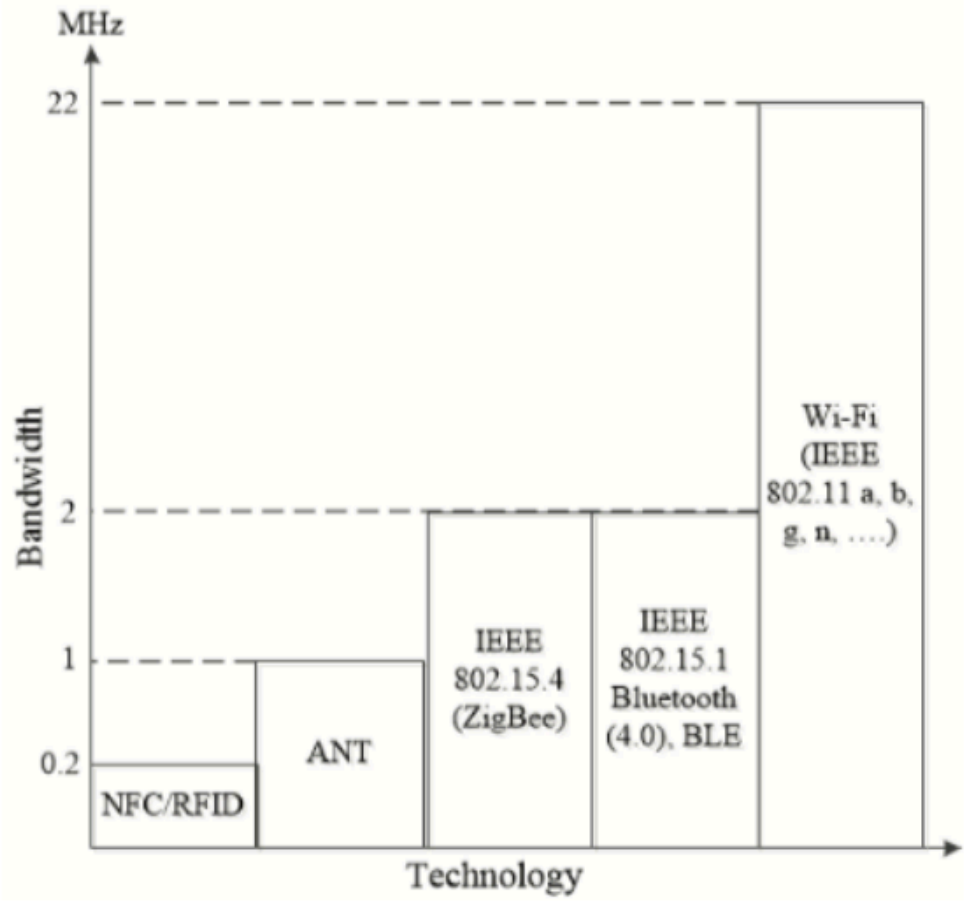

ZigBee Alliance specifications
Application objects
ZigBee device objects
Application support sublayer (APS)
Security services
Network layer
Medium access control (MAC) layer
Physical layer
IEEE 802.15.4 specifications


Communication Satellites
The Mobile Phone System
ZigBee
ZigBee
Control your world
Wireless Lan
RFID
Bluetooth

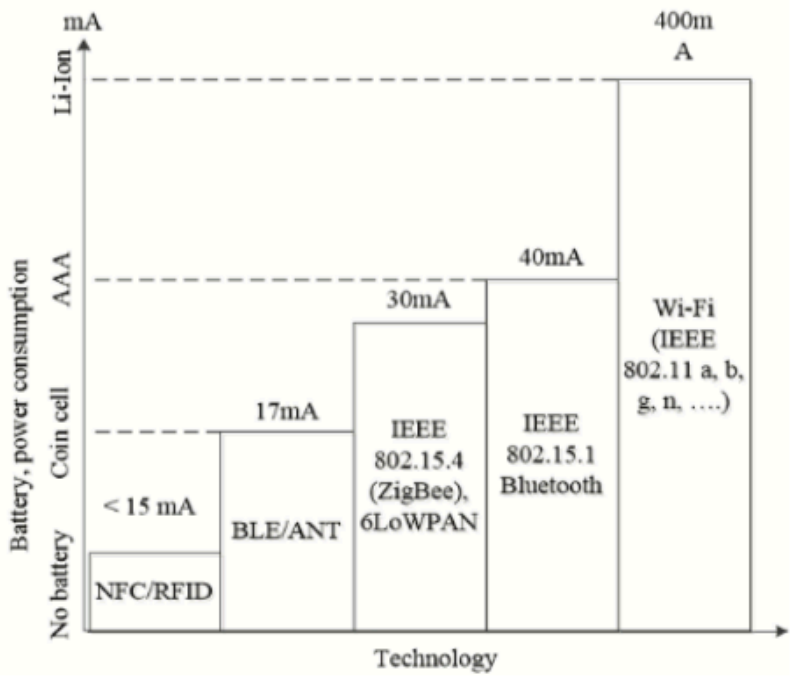
Comparison



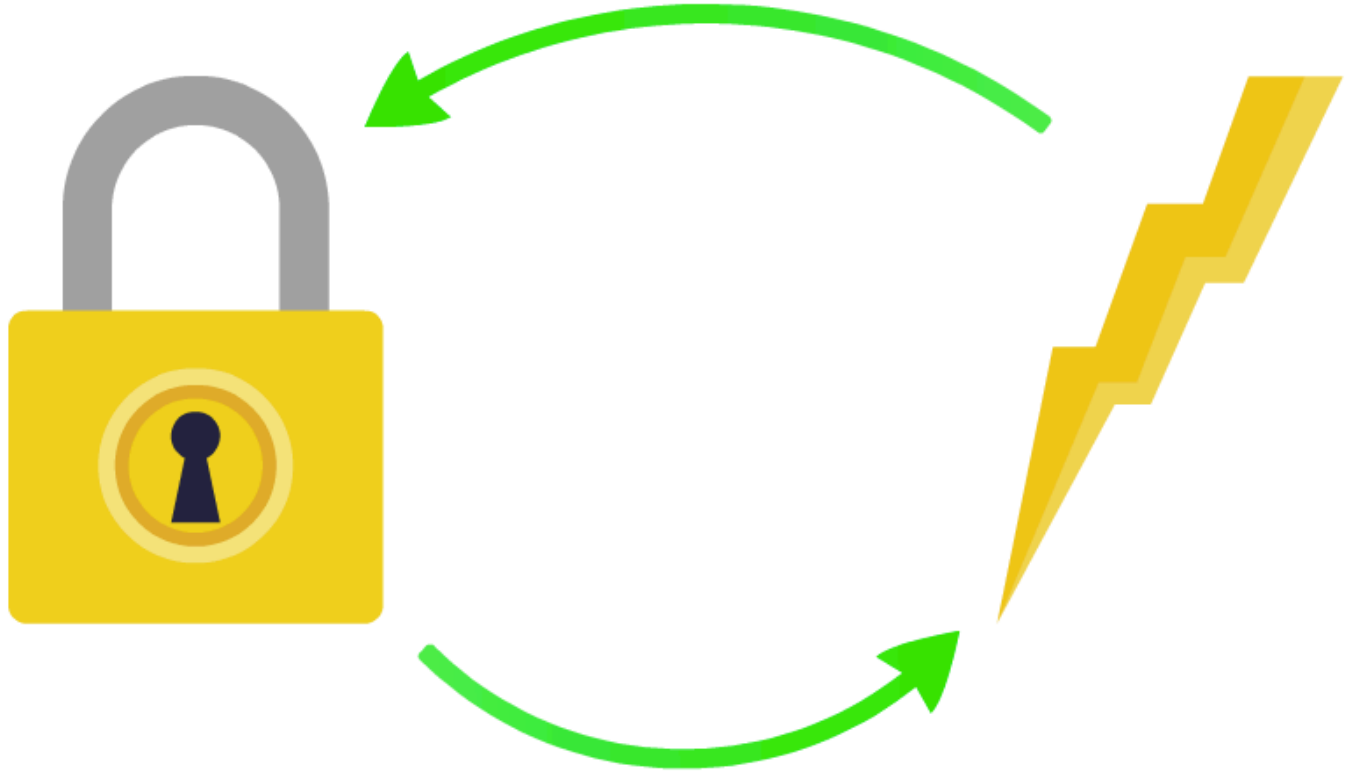
Bandwidth


MHz
22
2
1
0.2
Bandwidth
NFC/RFID
ANT
IEEE
802.15.4
(ZigBee)
IEEE
802.15.1
Bluetooth
(4.0), BLE
Wi-Fi
(IEEE
802.11 a, b,
g, n, ….)
Technology

Energy Consumption

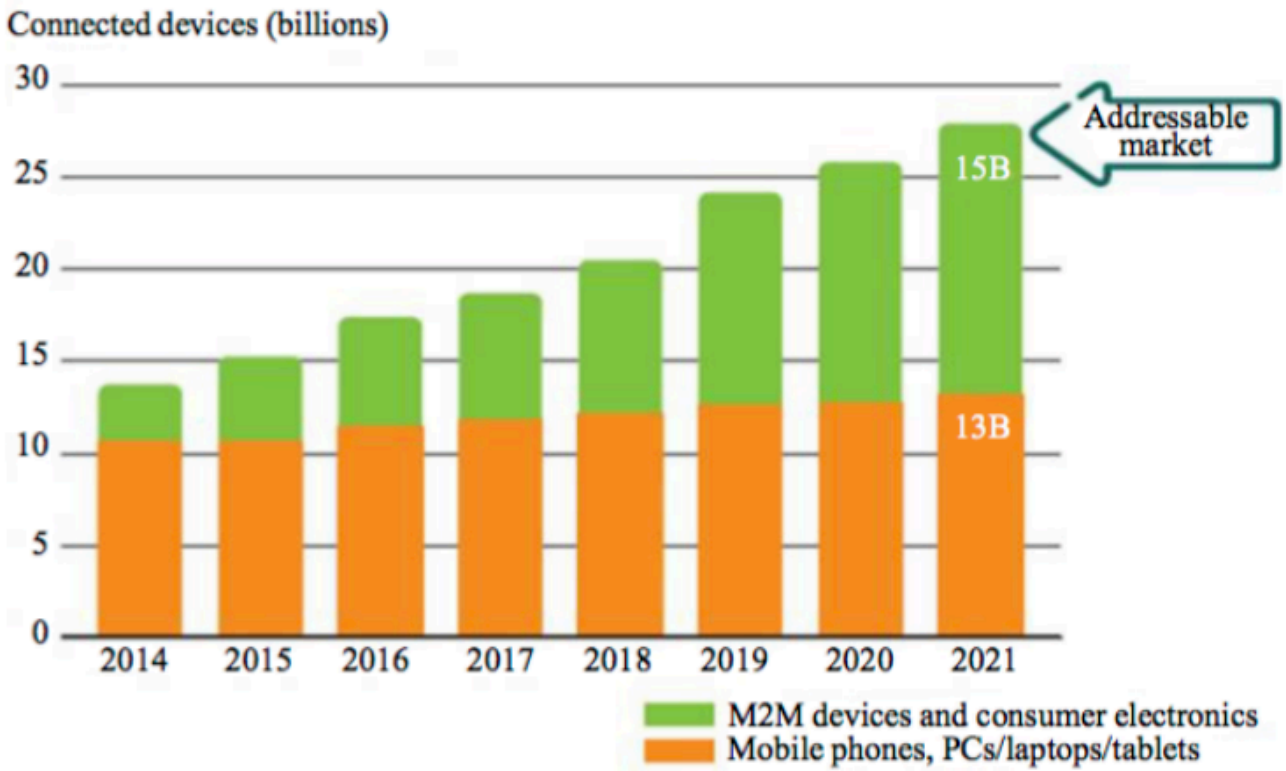


Safety




Max is koning ;)
knp. Almere
31 m
23 m


11. August 2016, 05:00 Uhr Funkfernbedienungen
Sicherheitslücke bei 100 Millionen Autos
Hier lauert die Gefahr: Funk-Schlüssel verschiedener VW-Modelle sind ein Einfallstor für Angreifer. (Foto: Collage SZ.de)


Connected devices (billions)
30
25
20
15
10
5
0
2014
2015
2016
2017
2018
2019
2020
2021
Addressable market
15B
13B
M2M devices and consumer electronics
Mobile phones, PCs/laptops/tablets


THANKS YOU FOR
YOUR ATTENTION !

Sources

Books/Papers:

William Stallings, *Wireless Communications & Networks, 2nd Edition*, Pearson, 2005
Mahmoud Shuker Mahmoud, Auday A. H. Mohamad, *A Study of Efficient Power Consumption Wireless Communication Techniques*, Scientific Research Publishing Inc., 2016
Artem Proskochylo, *Overview of wireless technologies for organizing sensor networks*, IEEE Xplore, 2015
Ilya Grigorik, *High Performance Browser Networking*, O'Reilly, 2013
A. Tanenbaum, *Computer Networks - 5th edition*, Pearson, 2011
Robert Davidson, Akiba, Carles Cufí, Kevin Townsend, *Getting Started with Bluetooth Low Energy*, O'Reilly Media, Inc. 2014

Pictures:

http://i.computer- bild.de/imgs/3/4/7/2/8/4/8/Satelliten-Schuesseln -an-Hauswand-745x559-27dd21d5c96145bc .jpg
http://newseastwest.co m/wp-content/uplo ads/2014/10 /India-to-launch-Canadian-M3M-satellite.jpg
https://upload.wikimedia. org/wikipedia/commons/thumb/d/da/Bluetooth.svg/2000px- Bluetooth.svg.png
http://www.nx-id. com/web/images/default/02.jpg
http://zigbee. org/wp-content/uploads/2014/08/zigbee_cntrlworld_vert_cmyk-273x300.png
By AutolycusQ - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=25179566
By Benjamin M. A'Lee - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=3554759
By User:sarysa - I derived this from Thomas.Baguette's work, using Paint.NET to edit the strings with similar fonts., CC BY-SA 3.0, https://en.wikipedia.org/w/index.php?curid=49590301
https://www.youtube. com/watch?v=KQdc5AdJqCg
http://www.newsline. dot.state.mn.us/images/14/July/9-TrafficTimeSign400.jpg
http://www.conceptdraw.c om/How-To-Guide/picture/Common-network-topologies.png
https://www.youtube.c om/watch?v=32JgSJYpL8o
http://www.hitachi.co m/businesses/infrastructure/product_solution/industry/electric/zignet/image/index_00.jpg
http://www.padtronix.c om/wp-content/uploads/2015/11/connected-house-main-image1.jpg