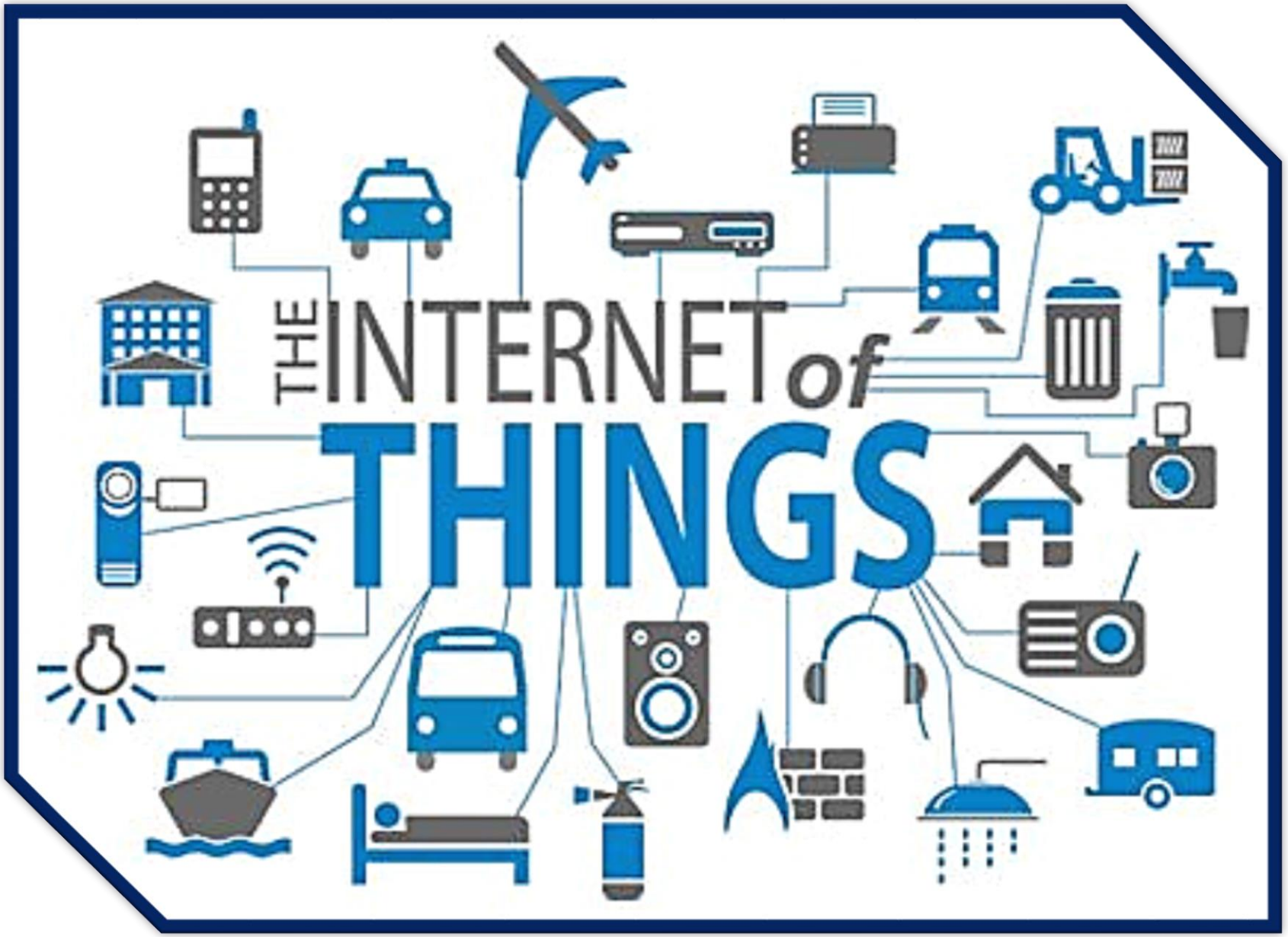

THE INTERNET of THINGS

3EC32D303
Internet of Things

L	T	P	C
2	-	2	3

Course Outcomes (COs):

At the end of the course, students will be able to -

1. Design framework for Internet of Things (IoT) for given applications using suitable sensor, microcontroller, and communication protocol and cloud architecture.
2. Comprehend sensor types, power management, IP based and non-IP based WLAN, WPAN and WWAN communication protocols and cloud messaging protocols related to IoT.
3. Evaluate the performance of cloud service models for the given IoT based applications.

SYLLBUS

UNIT I: Introduction of IoT

Definition, Growth, Architecture Overview, Building an architecture, Application areas, Characteristics, Threats and security, design principles and needed capabilities, standard considerations, Machine to Machine and IoT Technology Fundamentals - Devices and gateways, Local and Wide Area Networking.

UNIT II: Sensor, Microcontroller and Power Management

Sensors for temperature, light, pressure, humidity; LiDAR, Hall effect sensor, PIR sensor, MEMS sensors, Vision system – CCD and CMOS, Sensor fusion, Case study – Sensor tag energy harvesting, batteries and super capacitors, interfacing of sensors with microcontroller

UNIT III: Communication Protocols

Non-IP based WPAN – IEEE 802. 15. 1 Bluetooth, Bluetooth low energy (BLE 4.0), Beacon Technology, Bluetooth Mesh, Bluetooth Smart 5.0, IEEE 802.15.4 WPAN, Zigbee, Z-wave, Internet Protocol (IP) based WPAN and WLAN – 6LoPAN, WPAN with IP-thread

SYLLBUS

UNIT IV: IoT Edge to Cloud Protocols

Message Queuing Telemetry Transport (MQTT)- Publish-Subscribe Operation, Packet Structure, MQTT-SN, Transport Layer (TCP, MPTCP, UDP, DCCP, SCTP)-(TLS, DTLS) – Session Layer-HTTP, *Constrained Application Protocol* (CoAP), Extensible Messaging and Presence Protocol (XMPP), Advanced Message Queuing Protocol (AMQP).

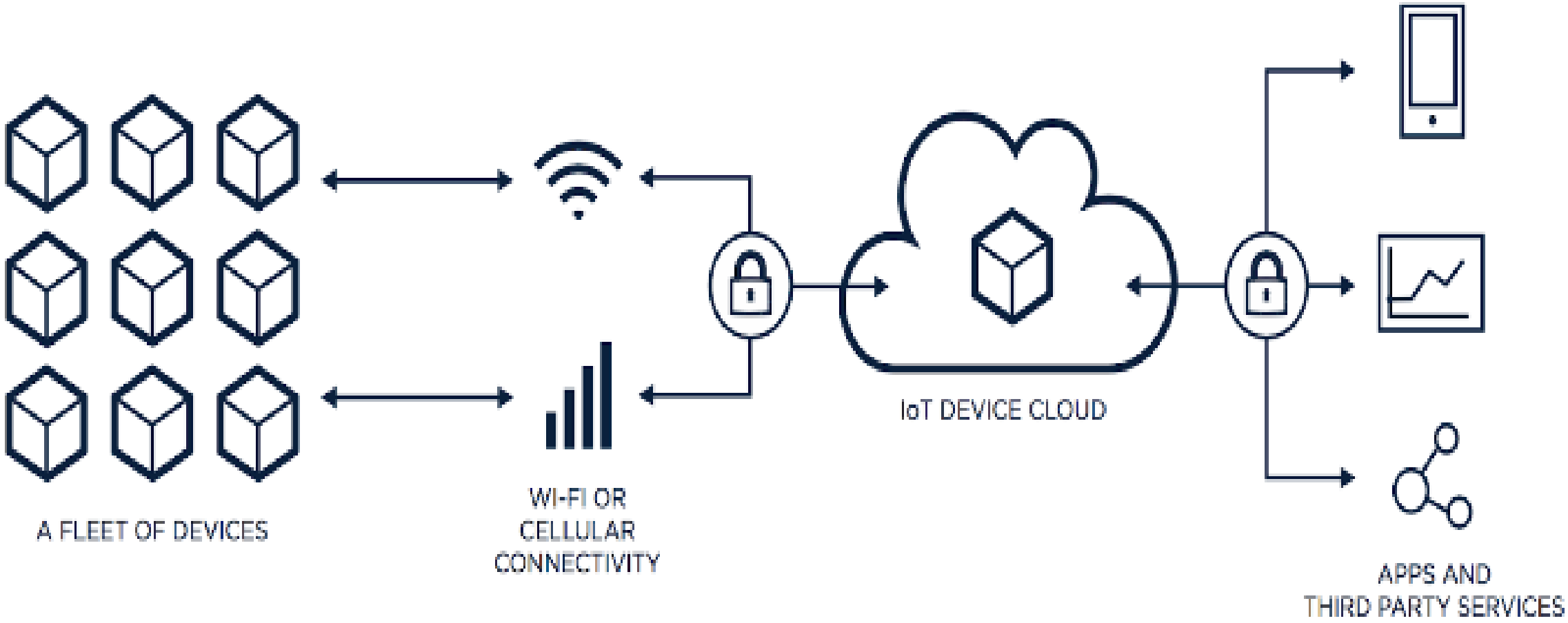
UNIT V: Cloud Computing

Cloud service models – Network as a Service (NaaS), Software as a Service (SaaS), Platform as a Service (PaaS), Internet as a Service (IaaS), Public, private and hybrid cloud, OpenStack cloud architecture.

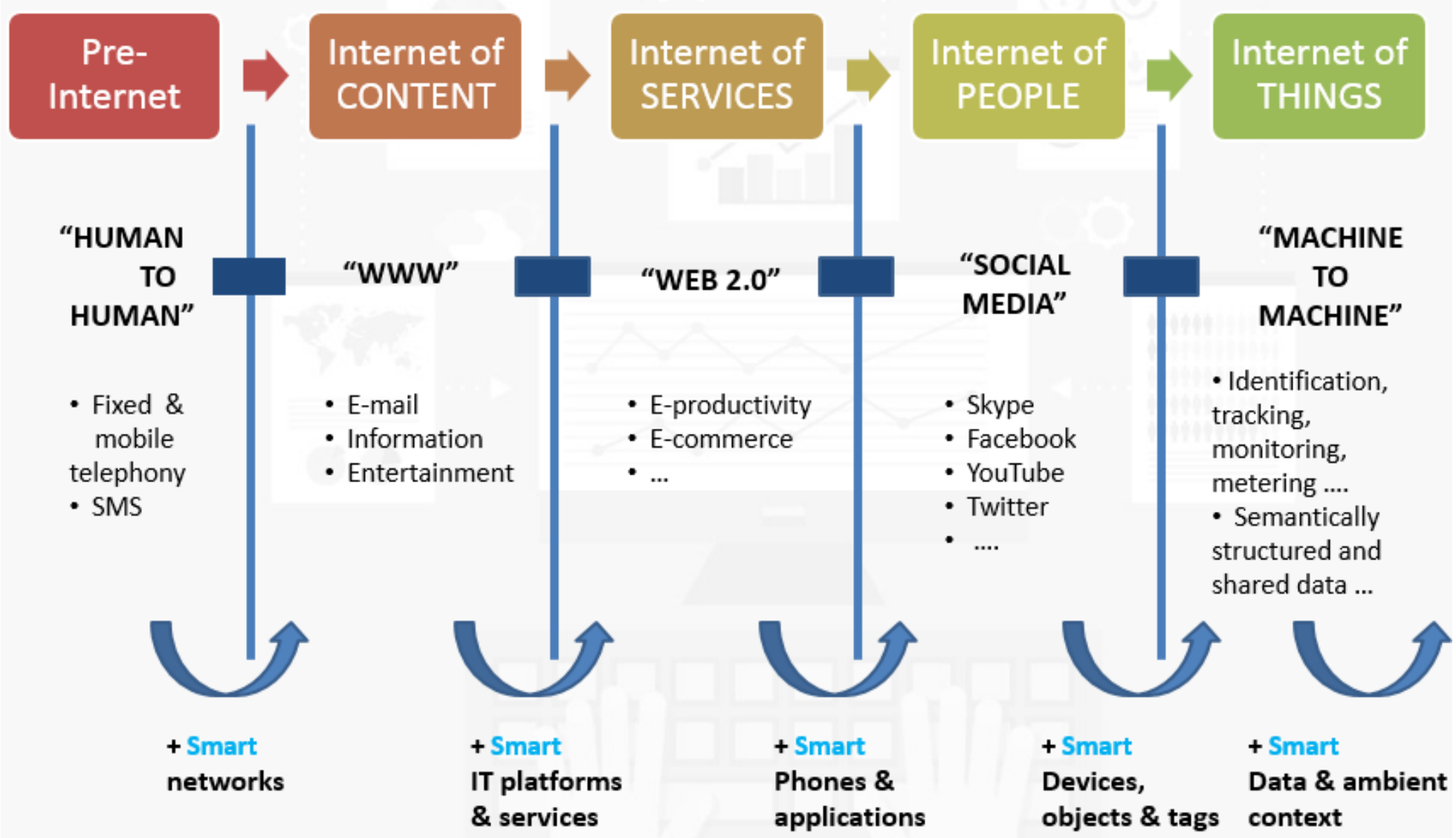
UNIT VI: Case Study

IoT for Healthcare domain, IoT for Smart City applications.

What is Internet of Things __(over) Simplified View



Evolution of Internet of Things



Various Definitions .....

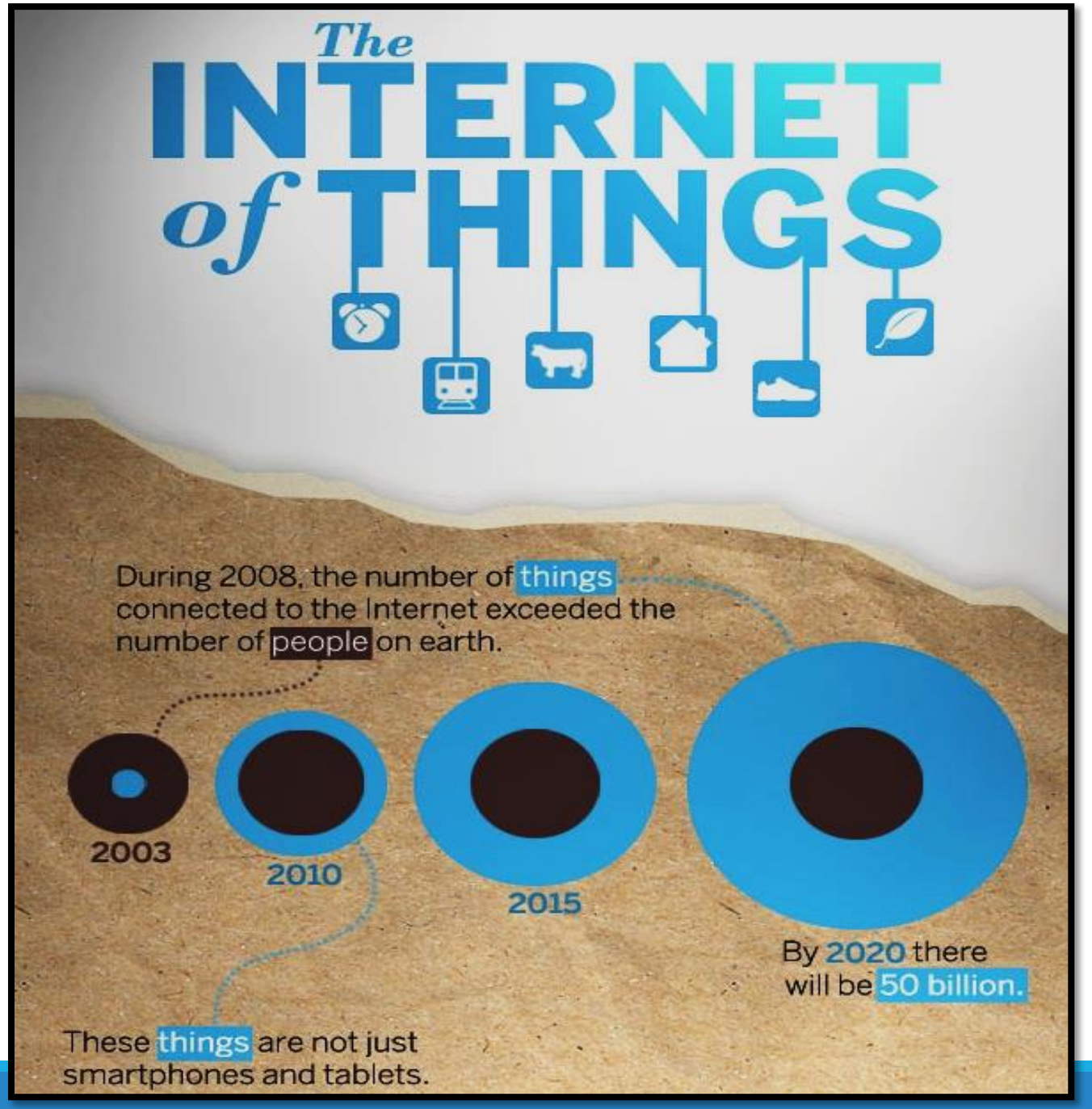
*"the interconnection of **uniquely identifiable embedded computing devices** within the existing **Internet infrastructure***

is defined as a paradigm in which objects equipped with sensors, actuators, and processors
communicate with each other to serve a meaningful purpose.

Interconnection of Things or Objects or Machines, e.g., sensors, actuators, mobile phones, electronic devices, home appliances, any existing items and interact with each other via Internet.

the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.

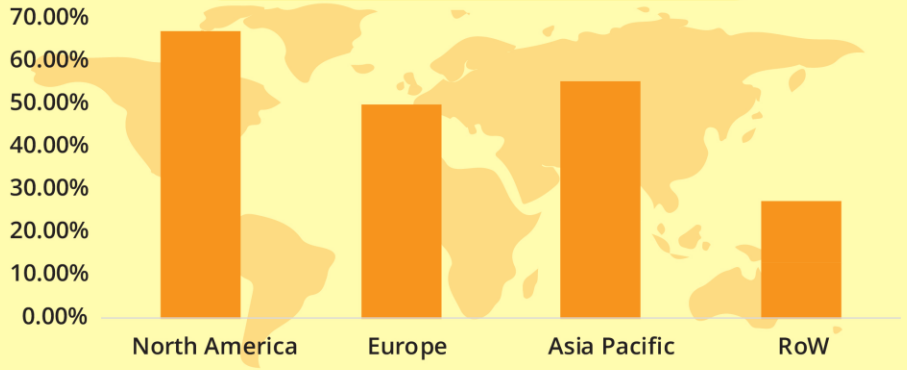
"Advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications".



Source: Cisco

GLOBAL INTERNET OF THINGS (IoT) MARKET FORECAST 2017-2025

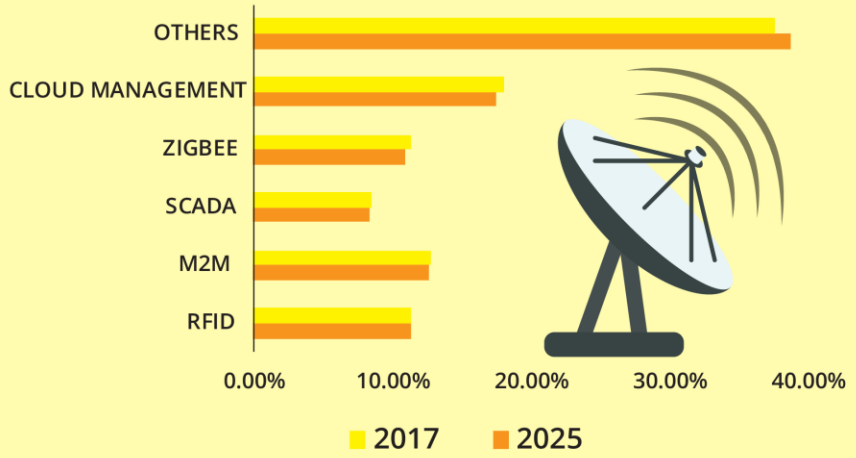
MARKET BY REGION



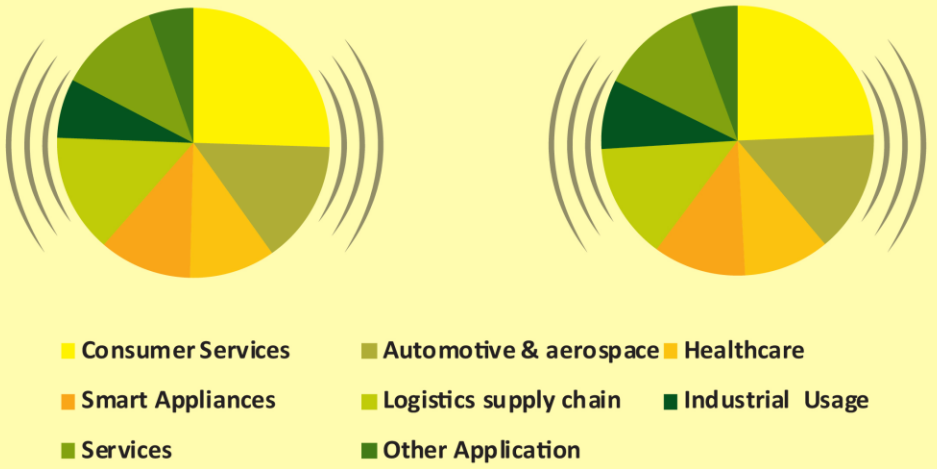
TOP COMPANIES

- SAP
- Oracle Corporation
- Texas Instruments
- Microsoft

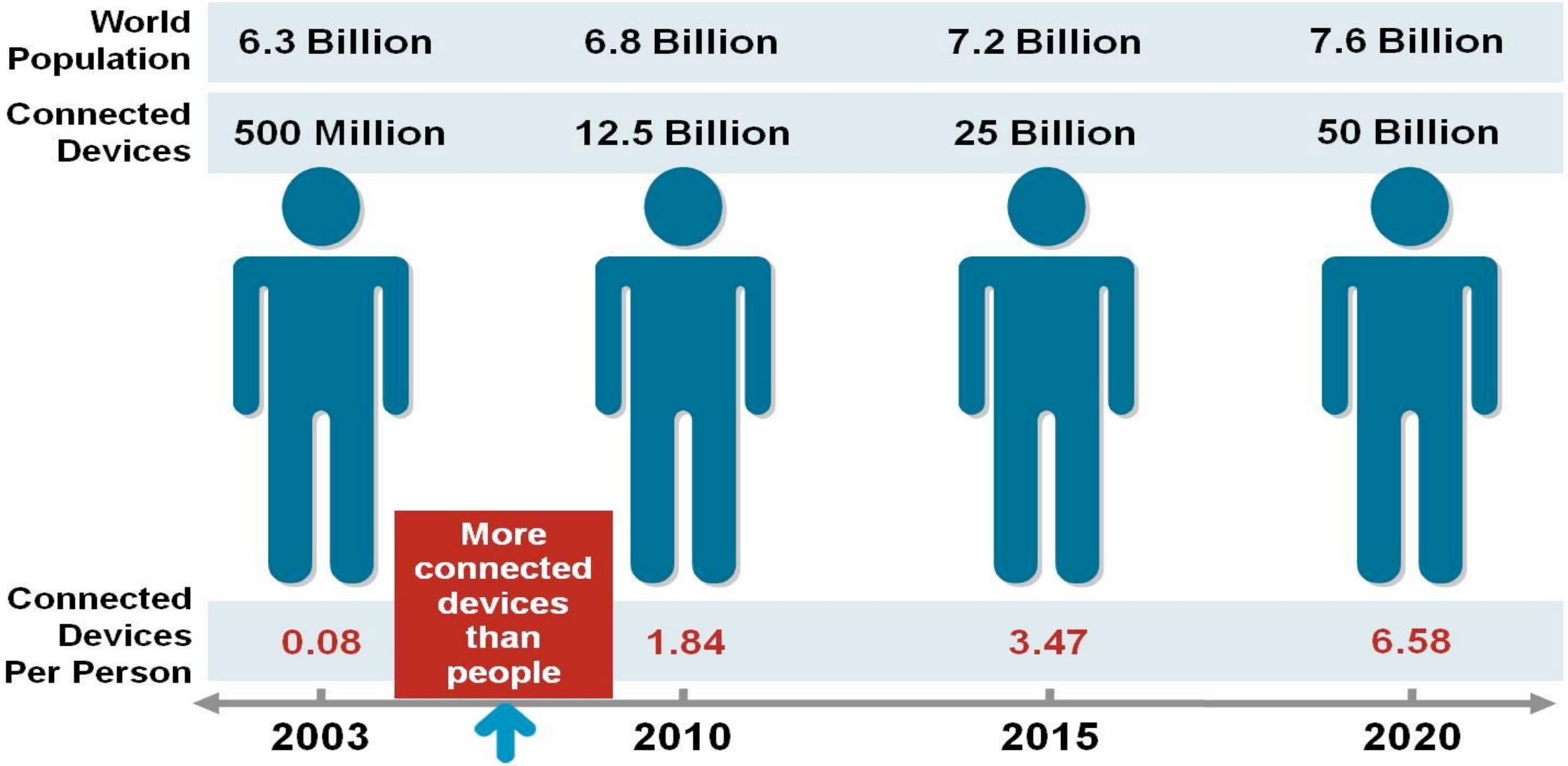
MARKET BY TECHNOLOGY



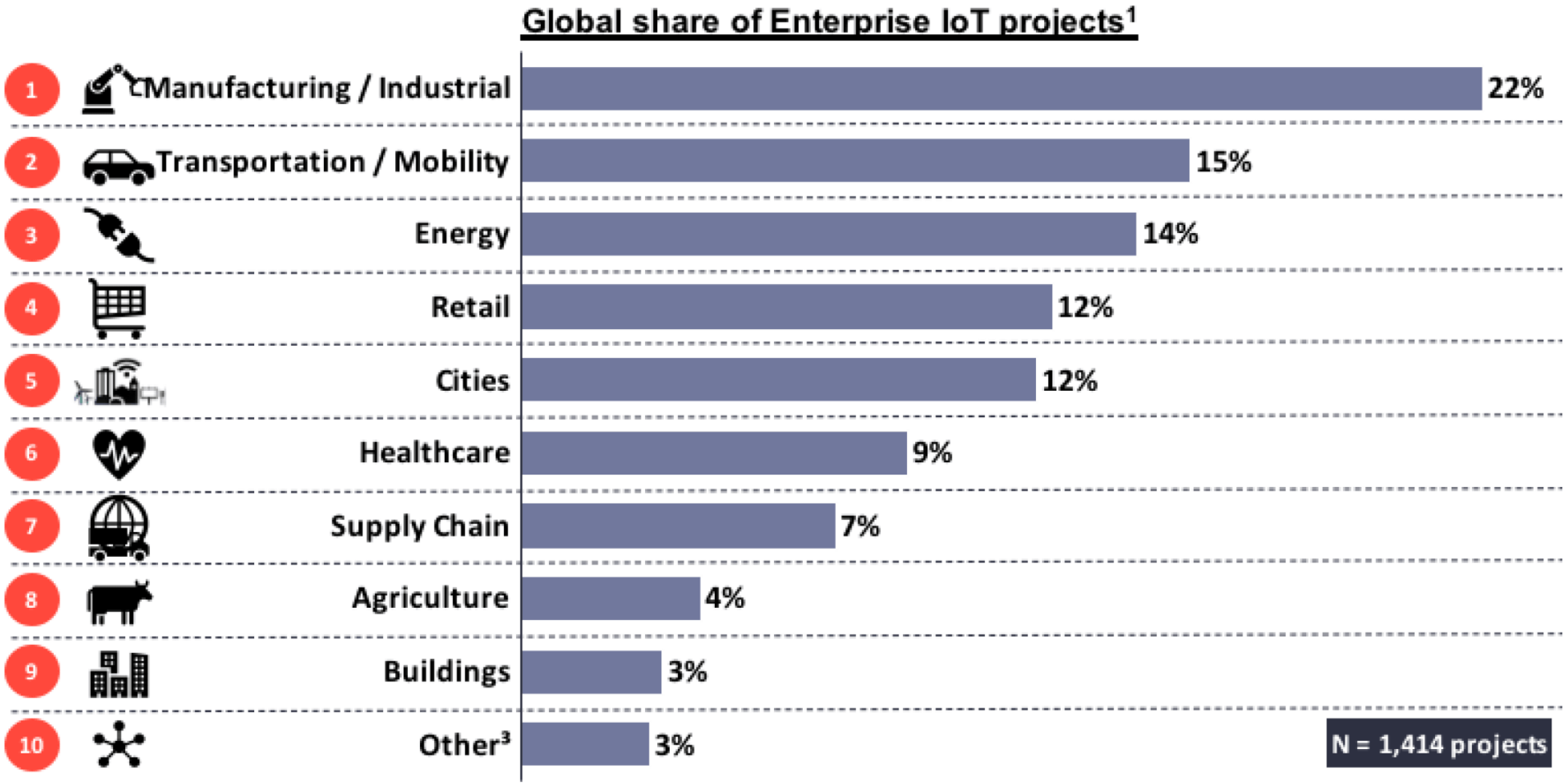
MARKET BY APPLICATIONS



www.inkwoodresearch.com


World Population
6.3 Billion
6.8 Billion
7.2 Billion
7.6 Billion
Connected Devices
500 Million
12.5 Billion
25 Billion
50 Billion
More connected devices than people
Connected Devices Per Person
0.08
1.84
3.47
6.58
2003
2010
2015
2020

Top 10 IoT Application areas 2020



Scenario before and after IoT

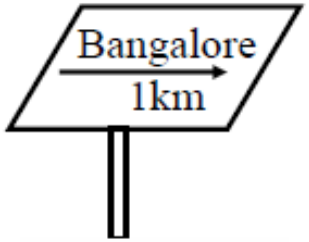
Before IoT		Enabled by IoT
Delivery schedule set based on distances and historical traffic patterns	→	Real-time adjustments to routes and proactive customer alerts of delays based on actual truck locations and traffic
Equipment maintenance performed every 12 months or at time of failure (downtime)	→	Maintenance performed when a failure is predicted based on real-time performance
Sell replacement parts and provide repair service	→	Customers pay maintenance subscription for services people to proactively visit when a failure is predicted
Service people visit every vending machine once a week even though some products were sold out for days or no products are out	→	Service people are dispatched to vending machines only when a threshold of products are predicted to be sold out
Static advertisement replaced monthly	→	Digital advertisement changes based on demographics of closest shopper

What is ‘SMART’?

Old: Smart = Can think , Can compute

Now: Smart = Can find quickly, Can Delegate, Communicate, Networking

1. **Passive**: Communicate only when queried.
   Passive RFID, QR codes (*Nirjeeva*)



2. **Active**: Communicate when needed.
   Sensors. Home automation (*1-4 sense*)

3. **Aware**: Action based on simple computation. E.g., tele-health (*5-sense*)

4. **Autonomous**: Can make decisions based on rules. E.g., autonomous cars, smart grid (*Human*)

courtesy: ©2014 Raj Jain

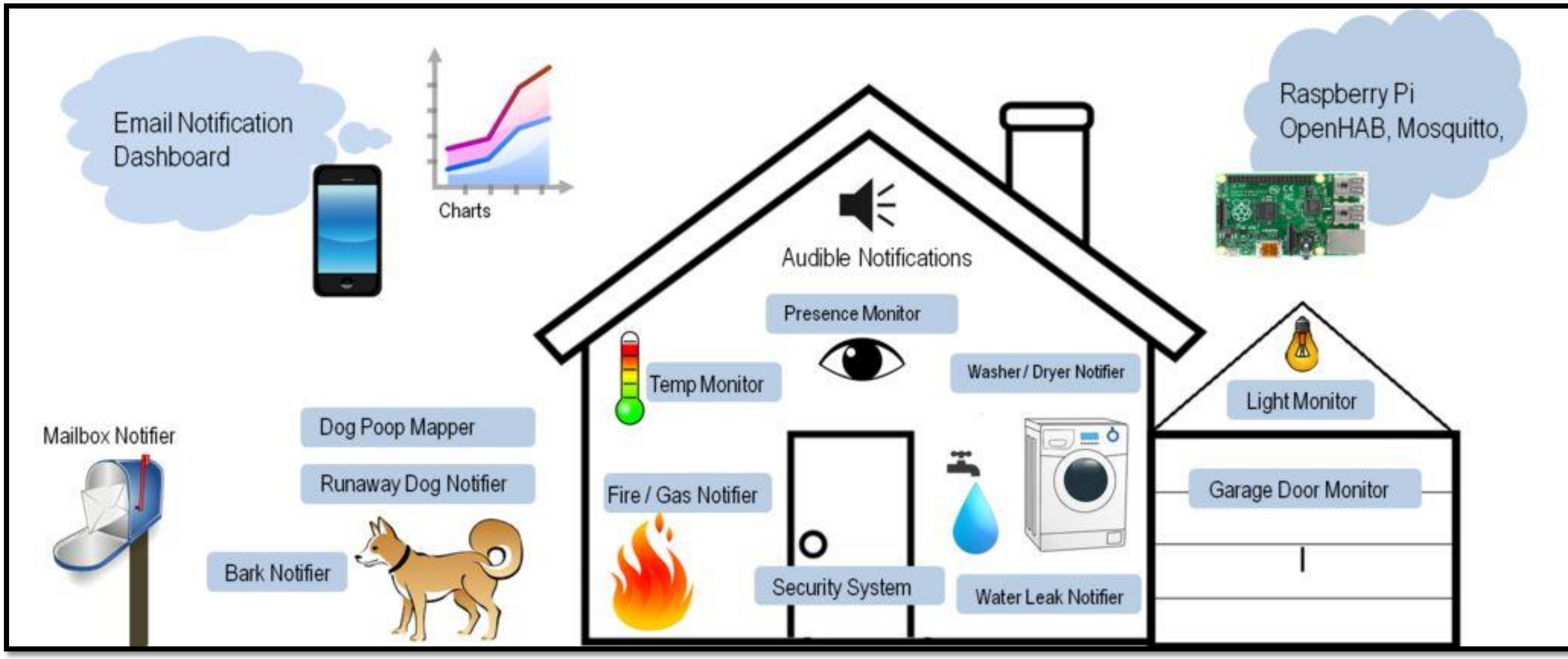
Application sphere of IoT

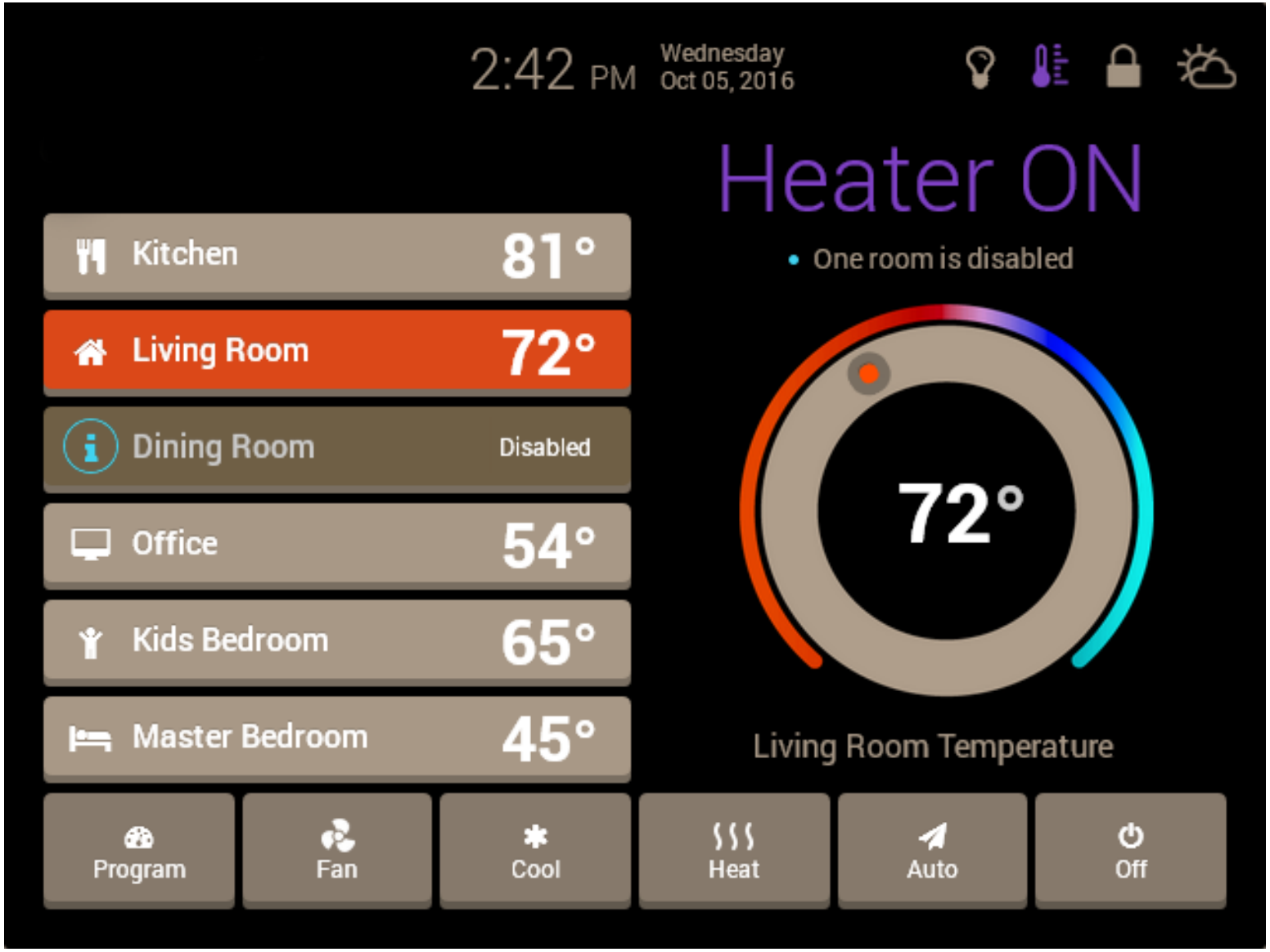
- ✓Building and Home automation
- ✓Manufacturing
- ✓Medical and Healthcare systems
- ✓Media
- ✓Environmental monitoring
- ✓Infrastructure management
- ✓Energy management
- ✓Transportation
- ✓… … …

https://data-flair.training/blogs/iot

You name it, and you will have it in IoT!

Home Monitoring & Automation




2:42 PM
Wednesday
Oct 05, 2016
Heater ON
One room is disabled
Kitchen 81°
Living Room 72°
Dining Room Disabled
Office 54°
Kids Bedroom 65°
Master Bedroom 45°
72°
Living Room Temperature
Program
Fan
Cool
Heat
Auto
Off

IoT in Industry

The 4th Industrial Revolution Is Upon Us.

FROM INDUSTRY 1.0 TO INDUSTRY 4.0

PRODUCTIVITY

FIRST
INDUSTRIAL REVOLUTION

Introduction of mechanical production facilities with the help of water and steam power

1784

First mechanical loom

SECOND
INDUSTRIAL REVOLUTION

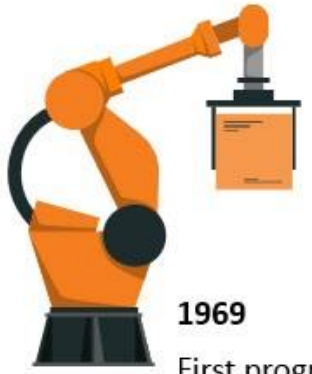
Introduction of a division of labor and mass production with the help of electrical energy

1870

First assembly line

THIRD
INDUSTRIAL REVOLUTION

Use of electronic and IT systems that further automate production

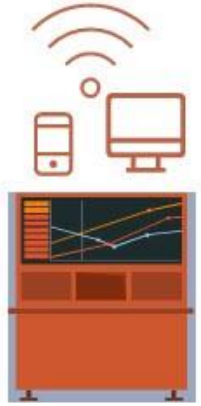


1969

First programmable (PC)

FOURTH
INDUSTRIAL REVOLUTION

The Digital Connected World



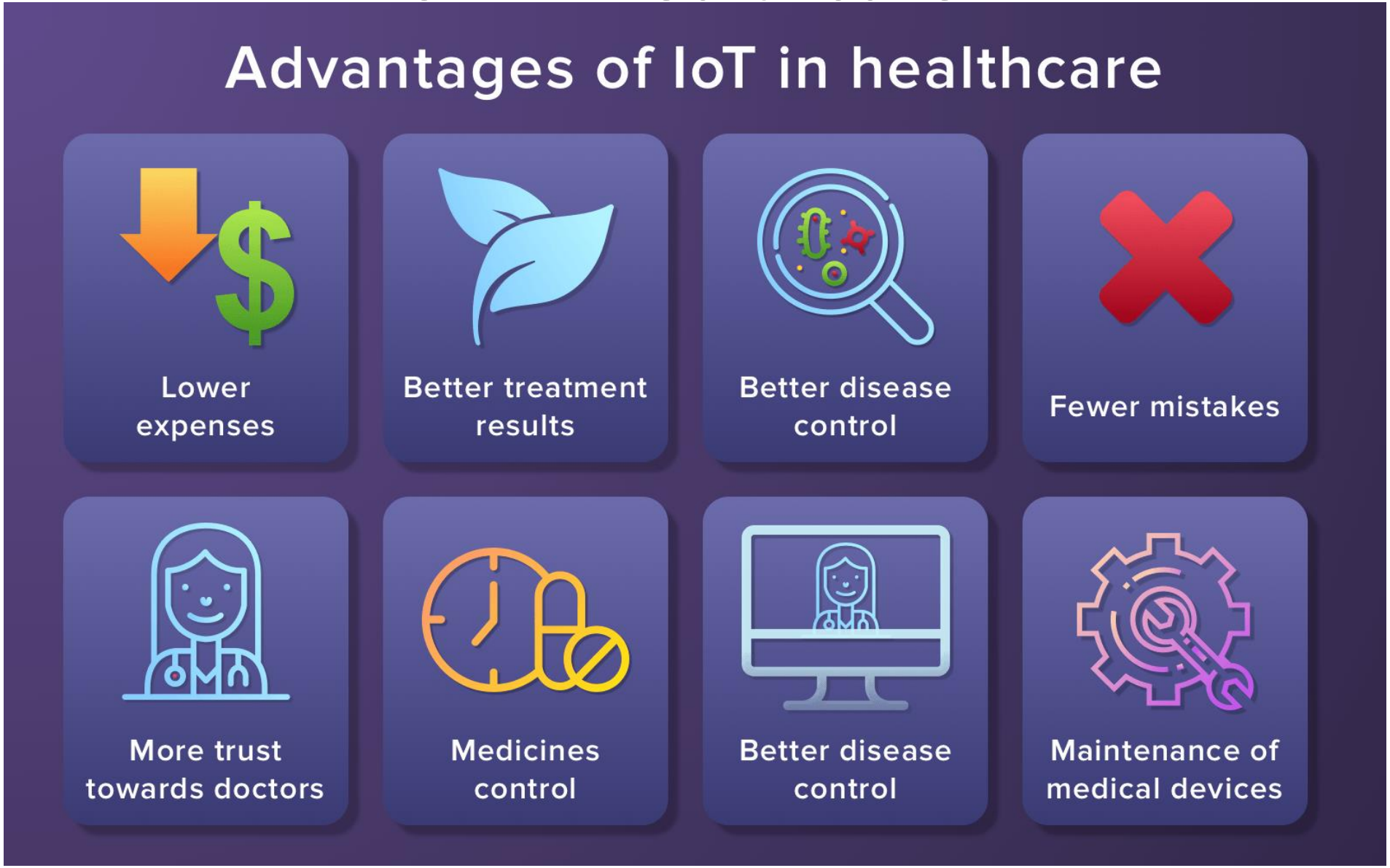
1800 — 1900 — 2000

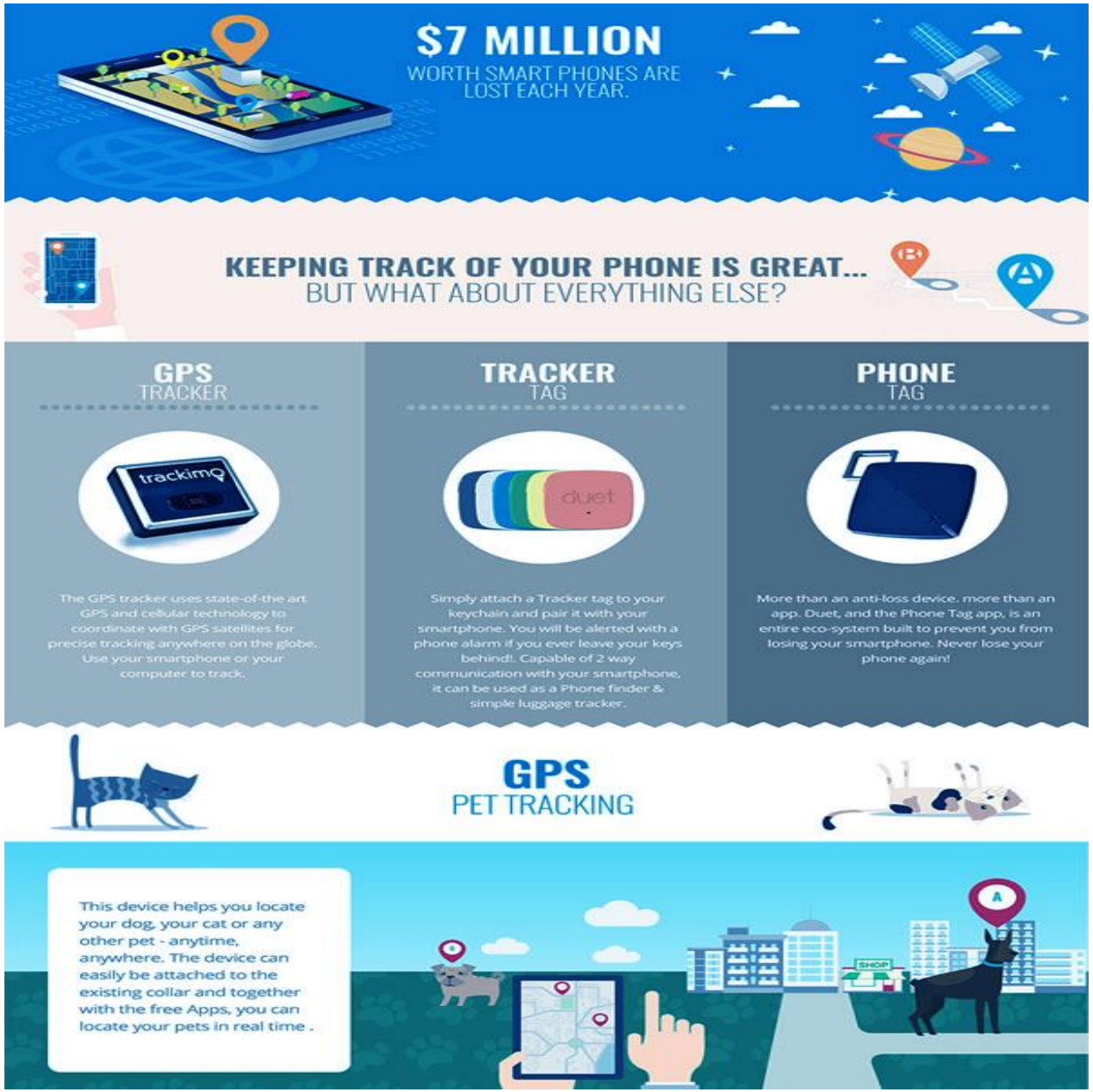
Principles of Scientific Management

TQM

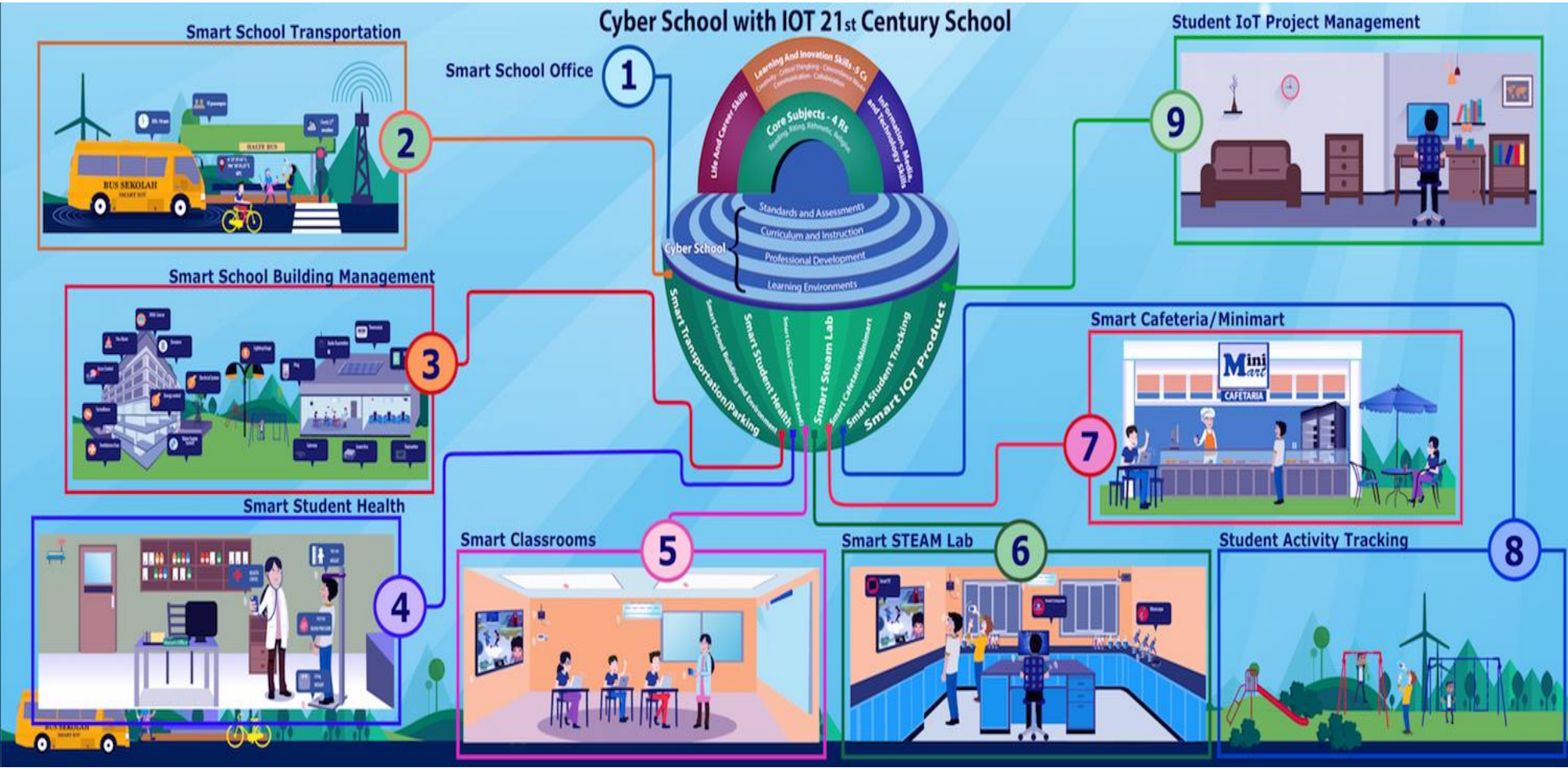
- *Lean*
- *Six Sigma*

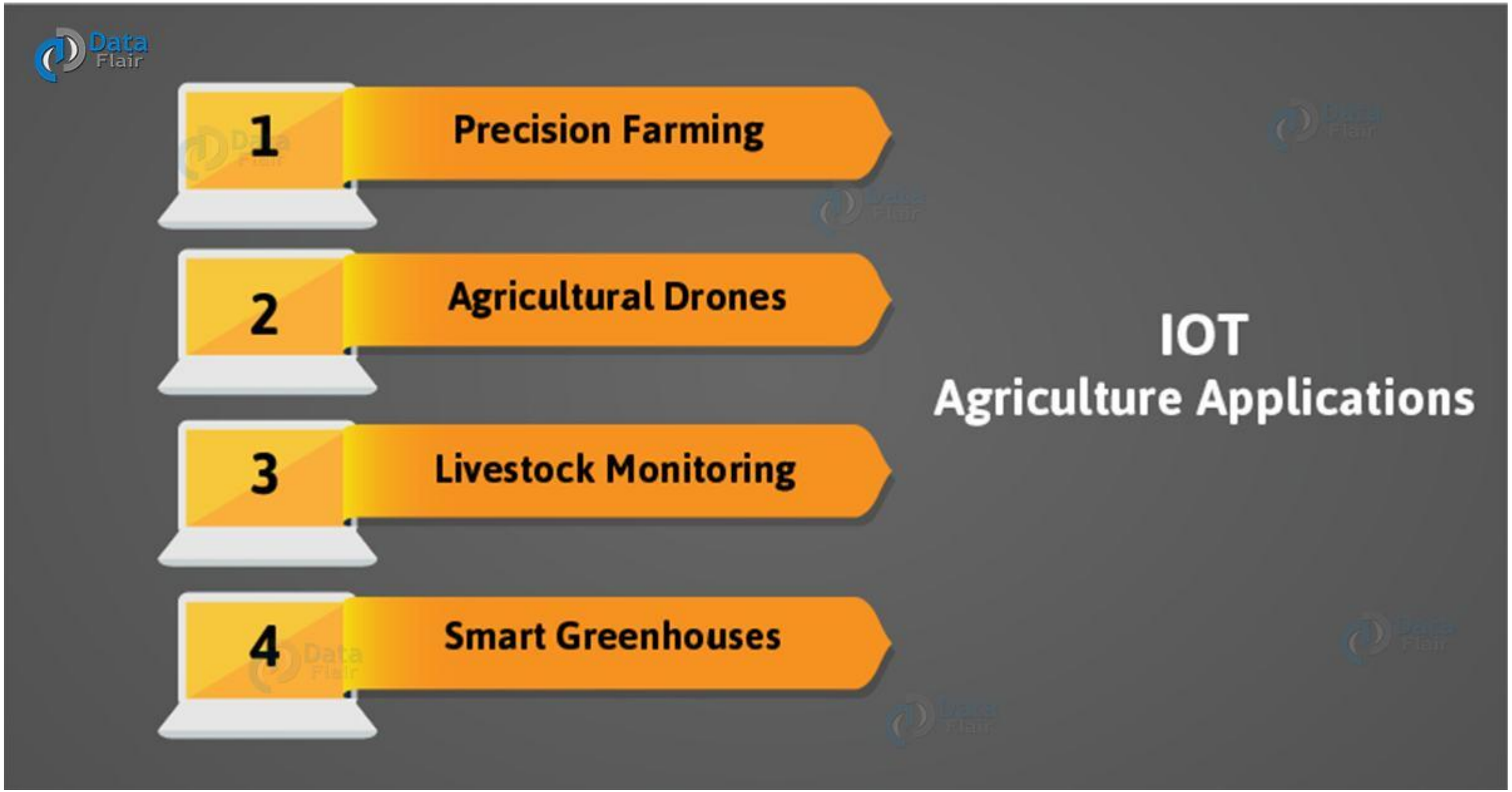
IoT in Healthcare





IoT for Tracking


Cyber School with IOT 21st Century School
Smart School Transportation
BUS SEKOLAH
2
Smart School Office
1
Learning And Inovation Skills - 5 Cs
Life And Career Skills
Information, Media and Technology Skills
Core Subjects - 4 Rs
Standards and Assessments
Curriculum and Instruction
Professional Development
Learning Environments
Cyber School
Smart Transportation/Parking
Smart Student Health
Smart Steam Lab
Smart Student Tracking
Smart IOT Product
Student IoT Project Management
9
Smart School Building Management
3
Smart Cafeteria/Minimart
Mini Mart
CAFETARIA
7
Smart Student Health
4
Smart Classrooms
5
Smart STEAM Lab
6
Student Activity Tracking
8


1
Precision Farming
2
Agricultural Drones
3
Livestock Monitoring
4
Smart Greenhouses
IOT
Agriculture Applications

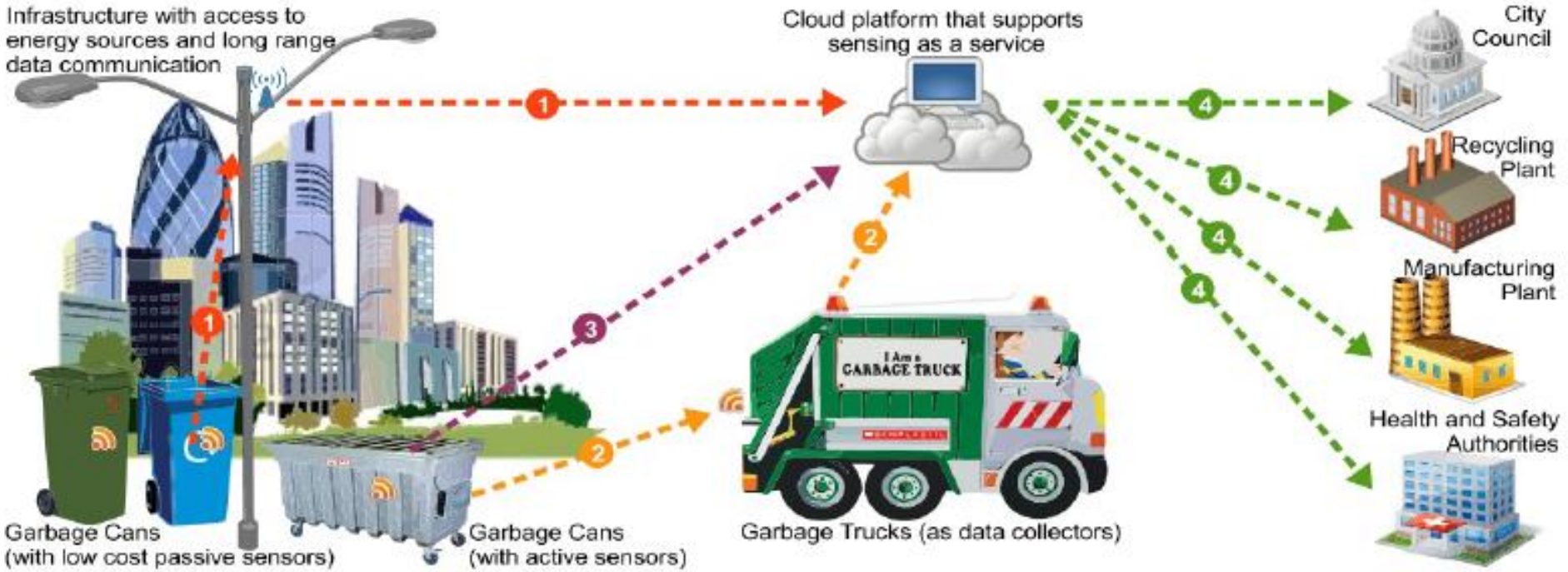
Smart Parking

Create **USD 41Billion** by providing visibility into the availability of parking spaces across the city.

Residents can identify and reserve the closest available space, traffic wardens can identify non-compliant usage, and municipalities can introduce demand-based pricing.

[Source: http://www.telecomreseller.com/2014/01/11/cisco-study-says-ioe-can-create-savings/]

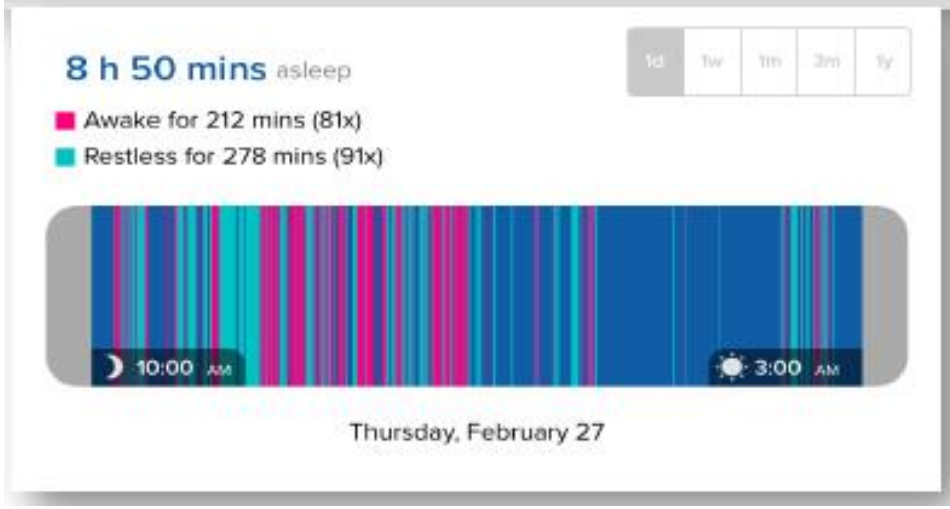
Efficient Waste Management in Smart Cities Supported by the Sensing-as-a-Service



[Source: "Sensing as a Service Model for Smart Cities Supported by Internet of Things", Charith Perera et. al., Transactions on Emerging Telecommunications Technology, 2014]

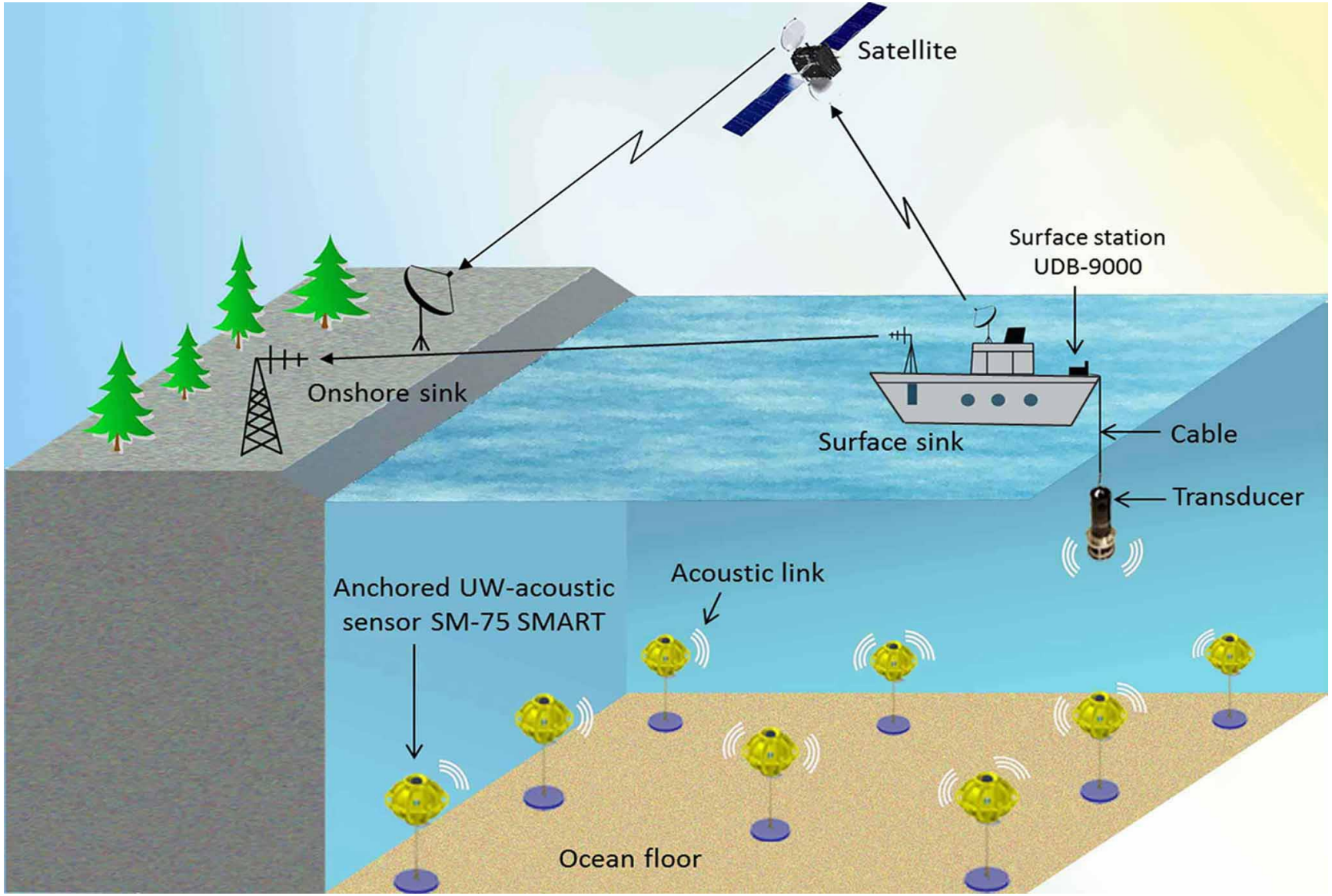
How Well Do I Sleep?

Sleep

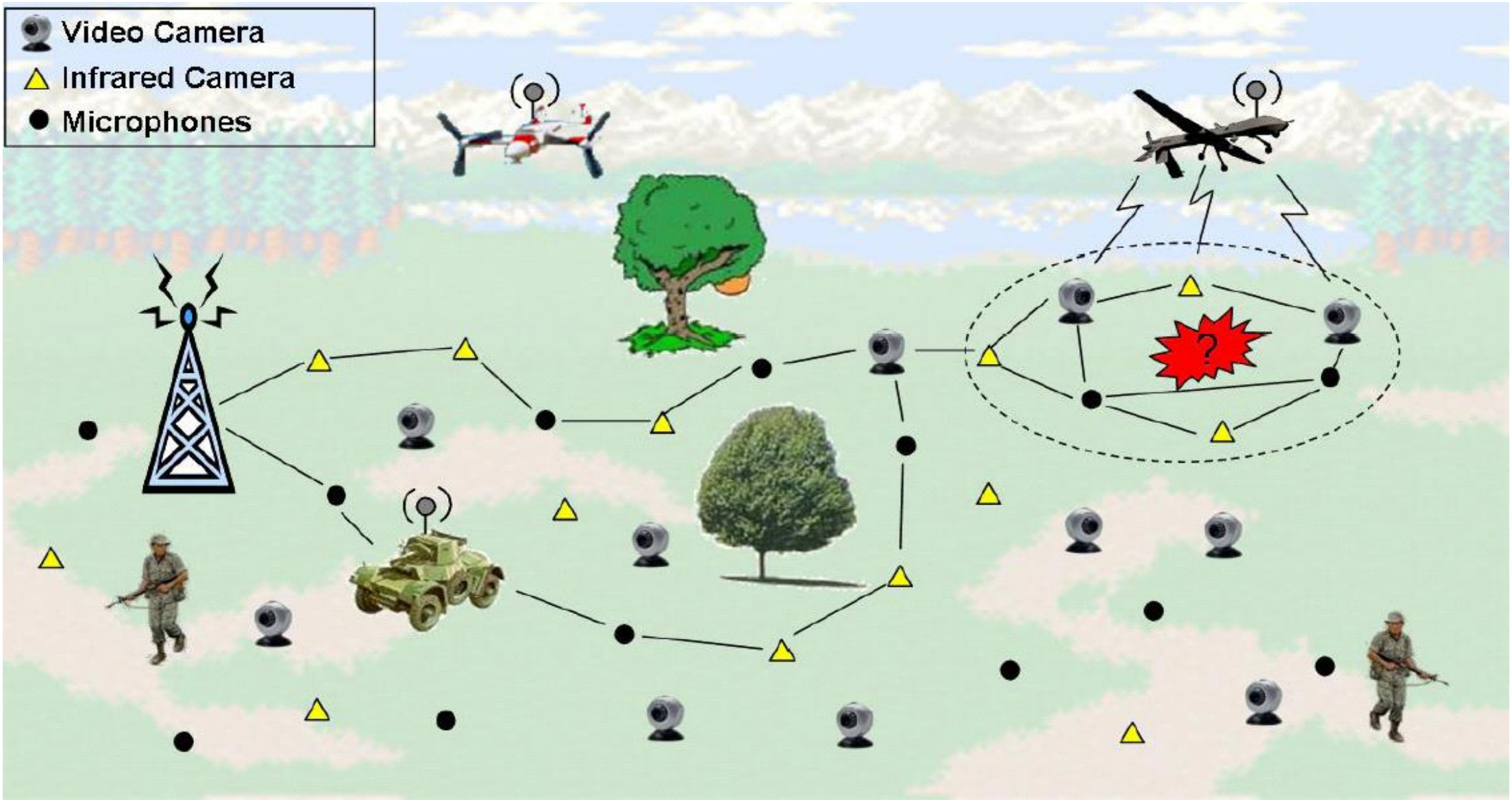


Sleep Stats

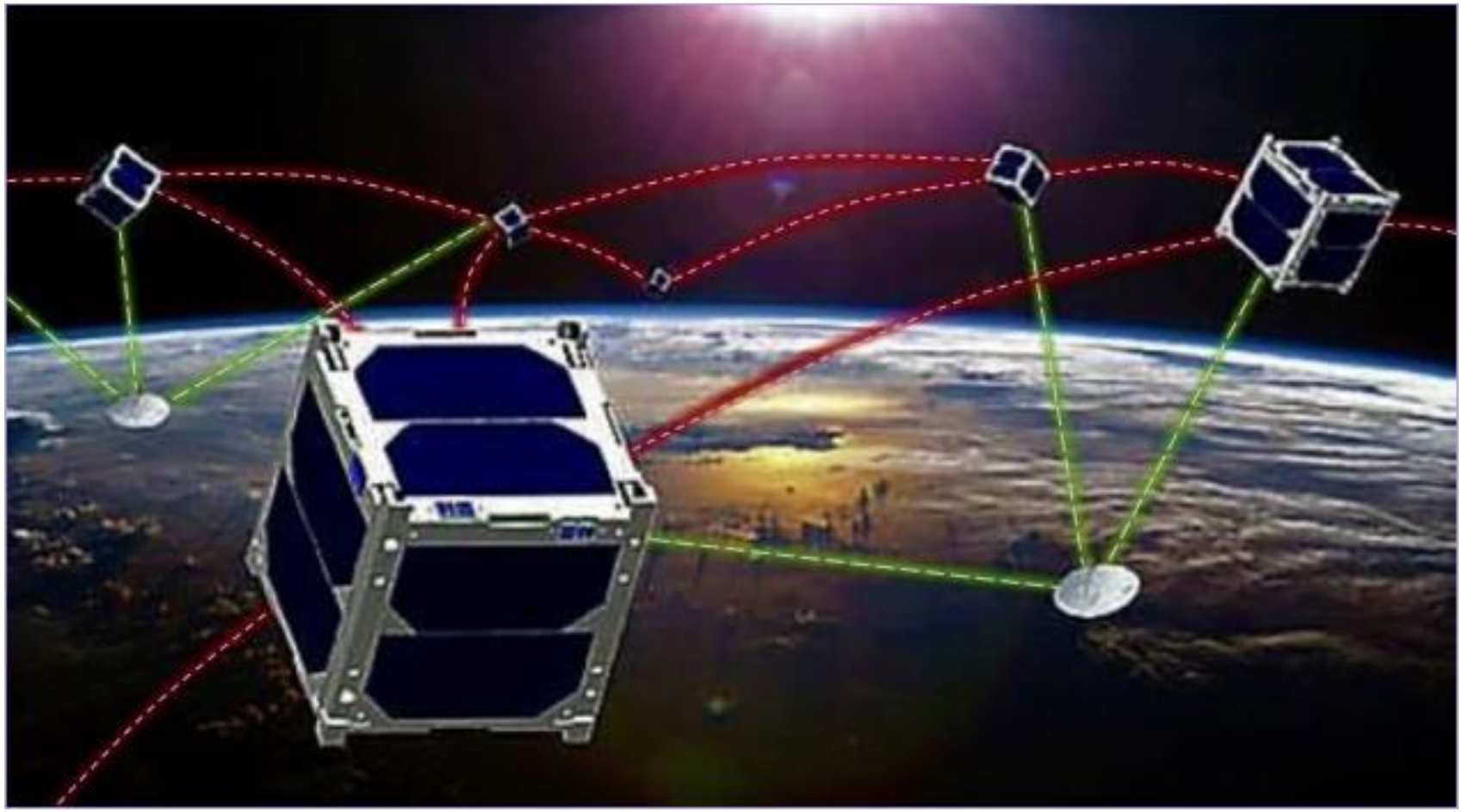
INTERNET OF UNDERWATER THINGS



Internet of Battlefield Things



INTERNET OF SPACE THINGS



Advantages of IoT

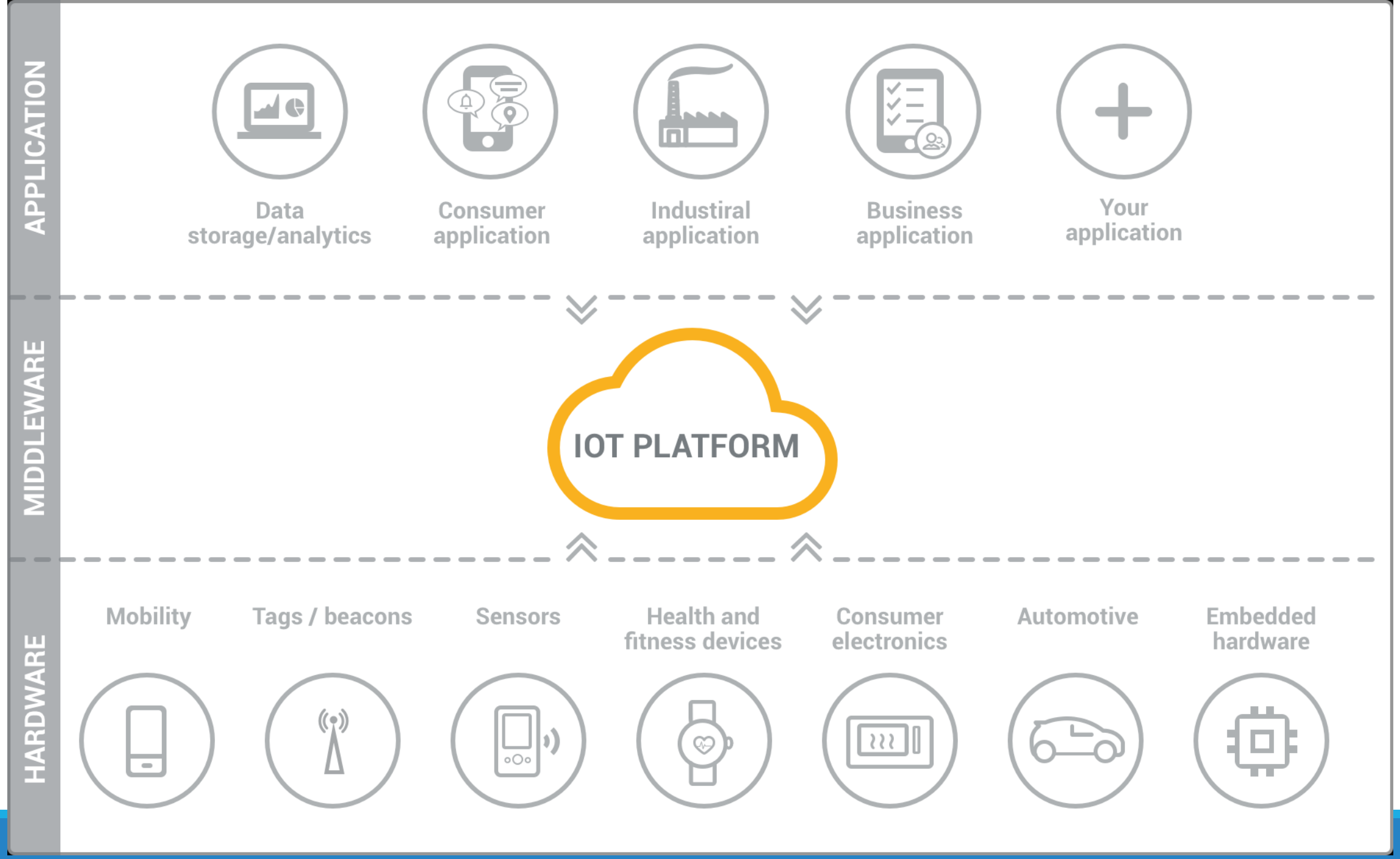
- **Efficient resource utilization**
- **Minimize human effort**
- **Save time**
- **Enhance Data Collection**
- **Improve security**

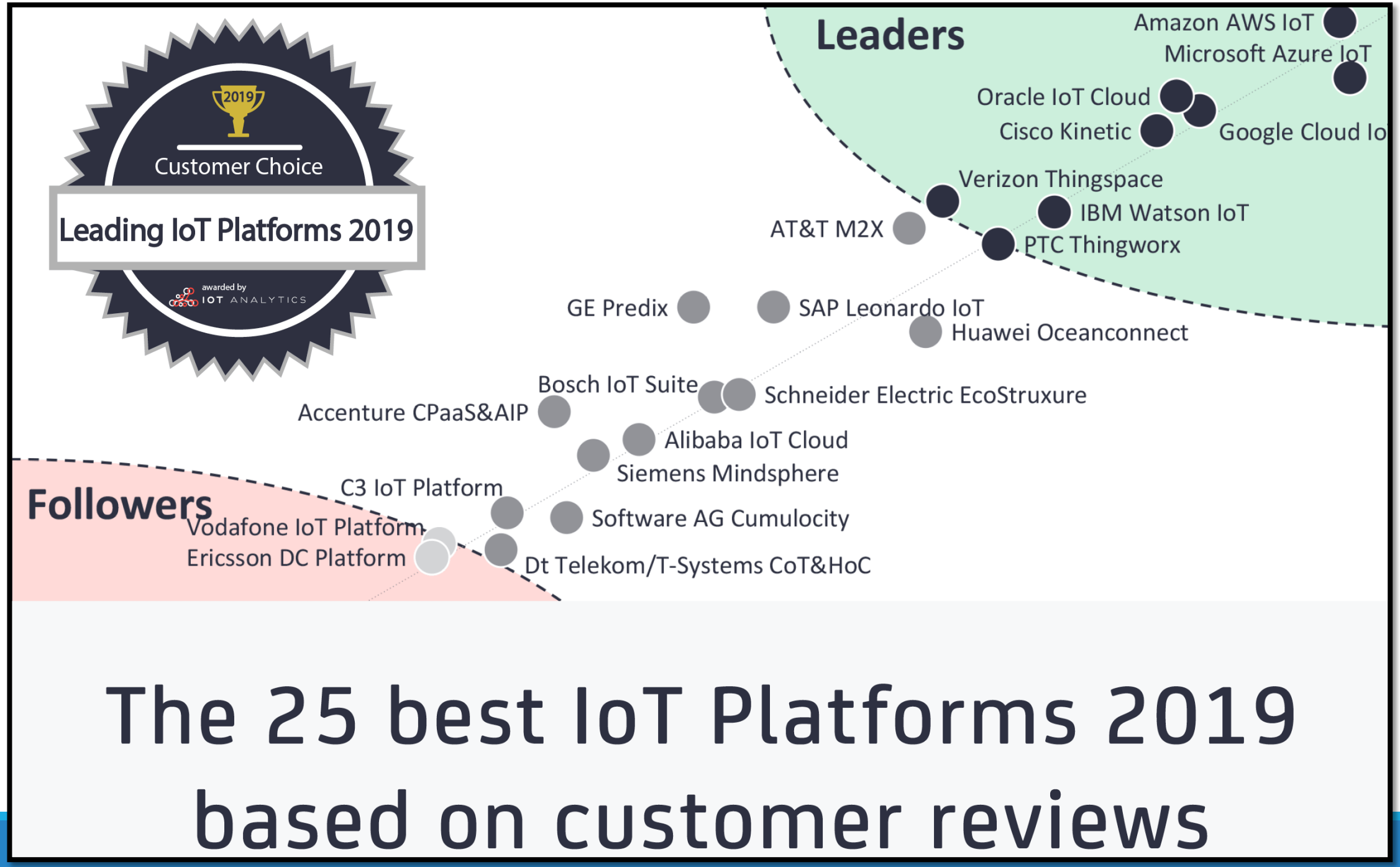
Challenges of IoT

- **Security:** As the IoT systems are interconnected and communicate over networks. The system offers little control despite any security measures, and it can be lead the various kinds of network attacks.

- **Privacy:** Even without the active participation on the user, the IoT system provides substantial personal data in maximum detail.

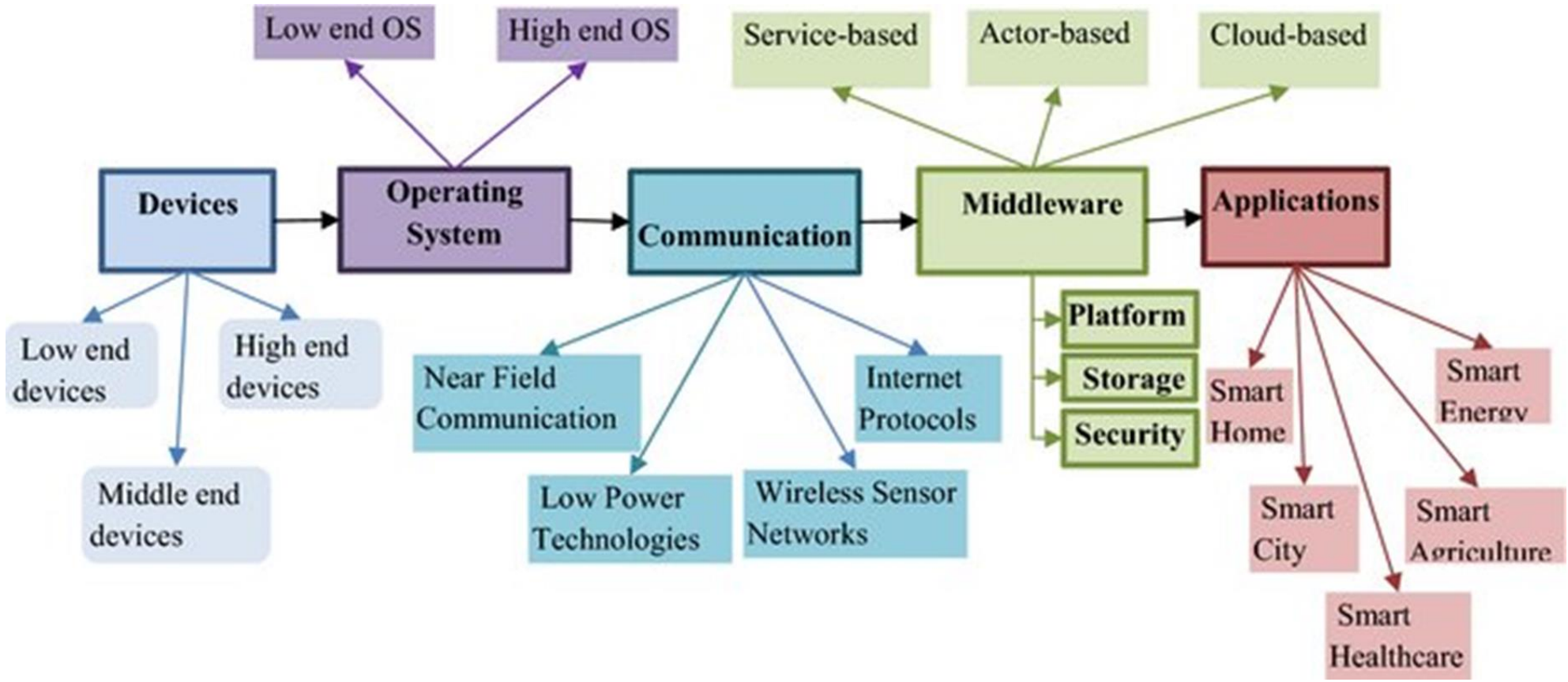
- **Complexity:** The designing, developing, and maintaining and enabling the large technology to IoT system is quite complicated.


APPLICATION
Data storage/analytics
Consumer application
Industiral application
Business application
Your application
MIDDLEWARE
IOT PLATFORM
HARDWARE
Mobility
Tags / beacons
Sensors
Health and fitness devices
Consumer electronics
Automotive
Embedded hardware



The 25 best IoT Platforms 2019 based on customer reviews

Summary _ Introduction



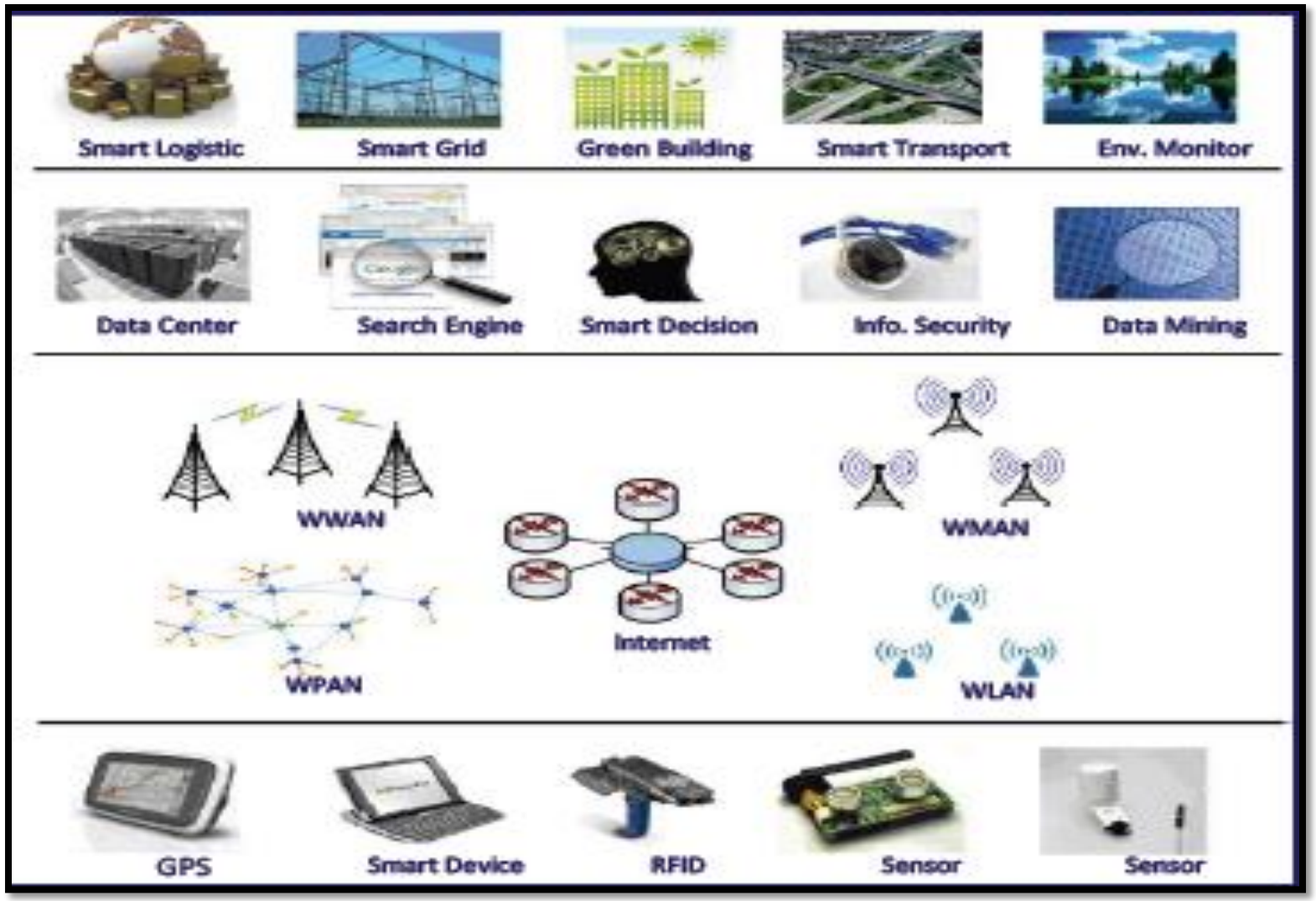
IoT Model

Integrated Application

Information Processing

Network Construction

Sensing and Identification



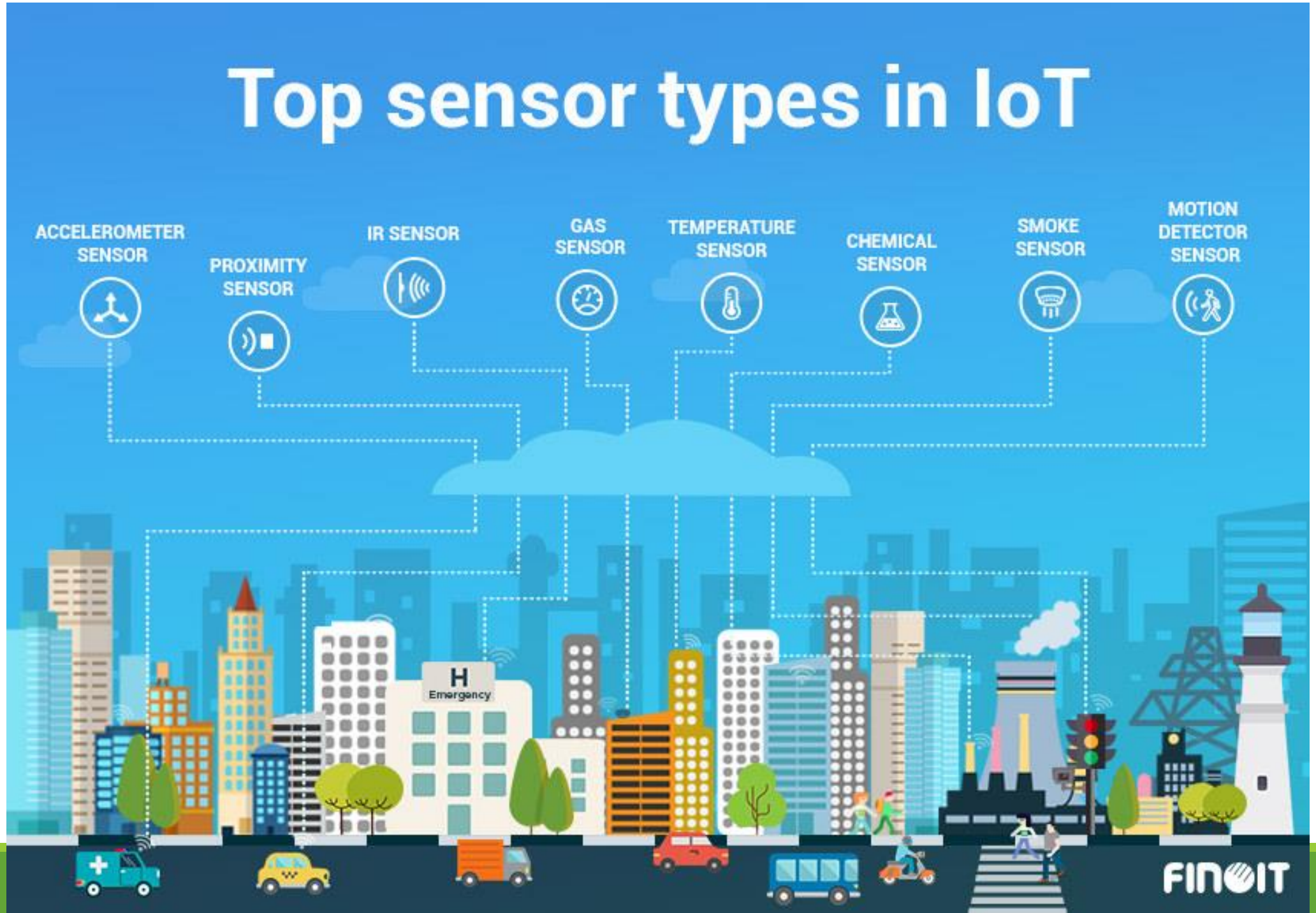
IoT Endpoints (‘Things’)

Contents

- Sensing & Actuator devices
- Energy generation systems
- Energy storage systems

Importance

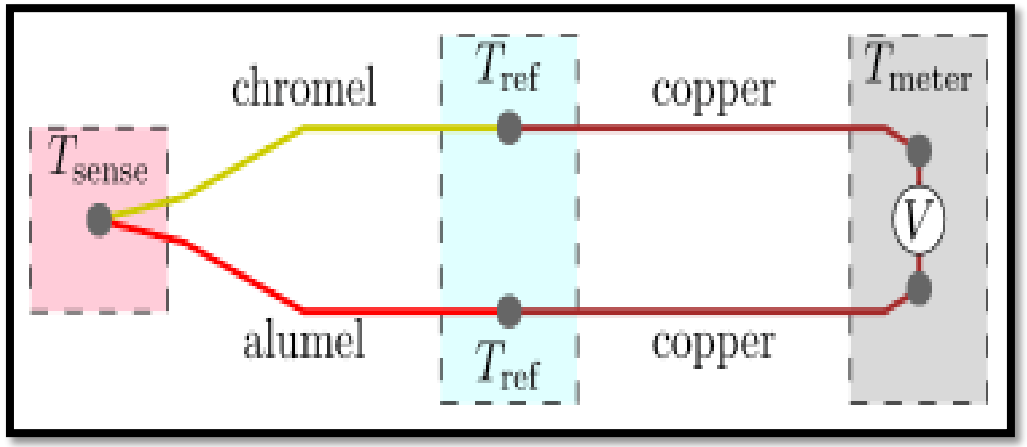
- Sensors output a stream of time-correlated data that must be transmitted securely / analysed/ stored
- Issues:
  - Type of data
  - Interpretation of data
  - Accuracy of data
  - Erroneous data
  - Failure of sensor
- Aspects - Cost, features, size, usable life, precision, power dissipation, energy generation


Top sensor types in IoT
ACCELEROMETER SENSOR
PROXIMITY SENSOR
IR SENSOR
GAS SENSOR
TEMPERATURE SENSOR
CHEMICAL SENSOR
SMOKE SENSOR
MOTION DETECTOR SENSOR
H
Emergency
FINOIT

Temperature Sensors

- **Thermocouples:** Measure temperature as a change in voltage
- **Resistor temperature detectors (RTD):** The resistance of the device is directly proportional to the temperature.
- **Thermistors:** It is a temperature sensitive resistor that changes its physical resistance with the change in temperature.
- **IC (Semiconductor):** Conductivity of the semiconductor increases linearly with temperature.
- **Infrared sensors:** It detects temperature by sensing the intensity of emitted infrared energy of the object. It can be used to measure temperature of solids and liquids only.

Thermocouple



- Junction of two wires of two different materials
- Each metal develops a voltage differential independently of each other.
- **Seebeck electromotive effect** - the difference between the voltage of the two metals has a nonlinear relationship to the temperature
- The magnitude of the voltage depends on the metal material chosen.
- It is critical that the ends of the wires are thermally isolated from the system
- **cold junction compensation**

Thermocouple ….

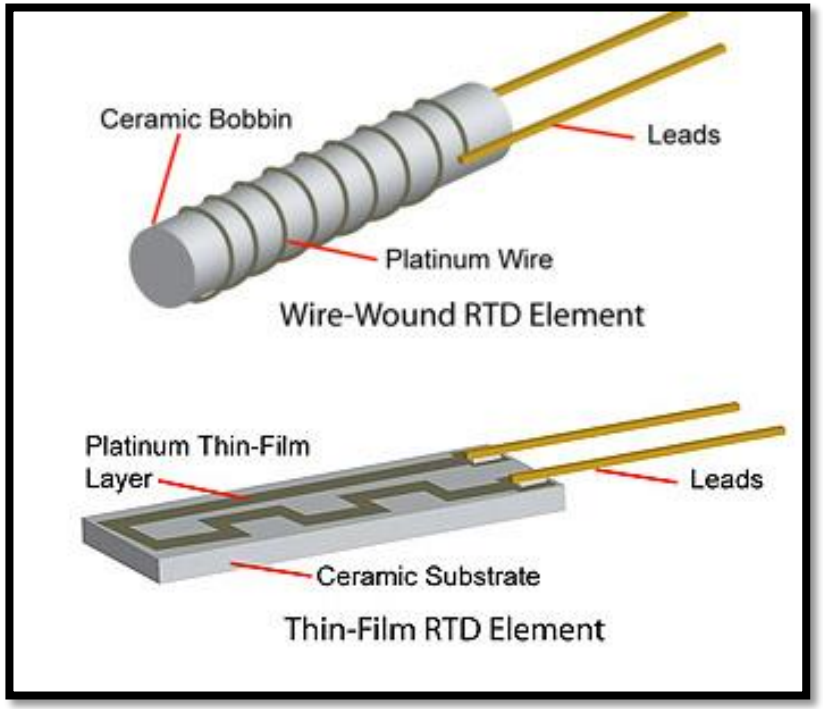
- Used for simple measurements – less accuracy
- More aging in Industrial environment
- Colour coded, different metal combinations
- Can measure high temperature
- Having long leads for long distance measurement

ANSI Code	Alloy Combination		Color Coding		Maximum Useful Temperature Range ++	Maximum Thermocouple Grade Temperature Range	EMF (mV) Over Max. Temperature Range
	+ Lead	- Lead	Thermocouple Grade	Extension Grade			
J	IRON Fe (magnetic)	CONSTANTAN COPPER-NICKEL Cu-Ni			Thermocouple Grade: 32 to 1382°F 0 to 750°C Extension Grade: 32 to 392°F 0 to 200°C	-346 to 2193°F -210 to 1200°C	-8.095 to 69.553
K	CHROMEGA® NICKELCHROMIUM Ni-Cr	ALOMEGA® NICKEL-ALUMINUM Ni-AI (magnetic)			Thermocouple Grade: -328 to 2282°F -200 to 1250°C Extension Grade: 32 to 392°F 0 to 200°C	-454 to 2501°F -270 to 1372°C	-6.458 to 54.886

https://www.omega.com/techref/colorcodes.html

Resistance Temperature Detectors (RTD)

- Constructed with very fine platinum wire tightly wrapped around ceramic or glass
- As it is a resistance-based measurement, an excitation current is needed to operate an RTD (1 mA)
- Operates within a narrow range of temperatures
- Have much better accuracy than thermocouples (below 600 degrees Celsius)…Limited industrial application
- Often used with bridge circuits to increase resolution

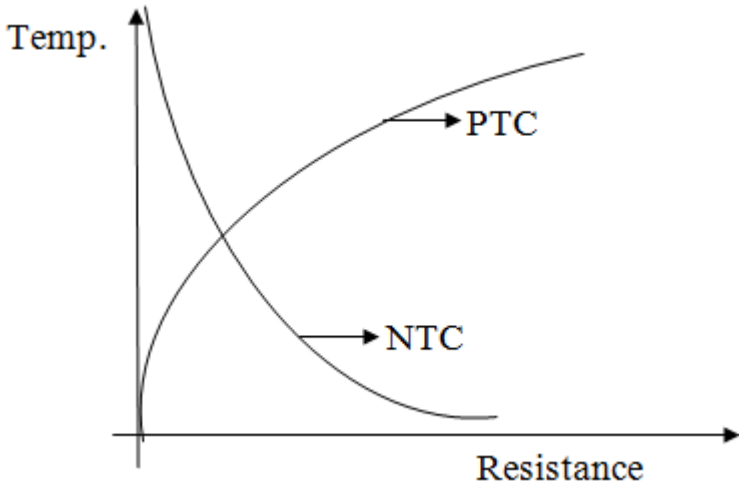


Comparison- Thermocouple and RTD

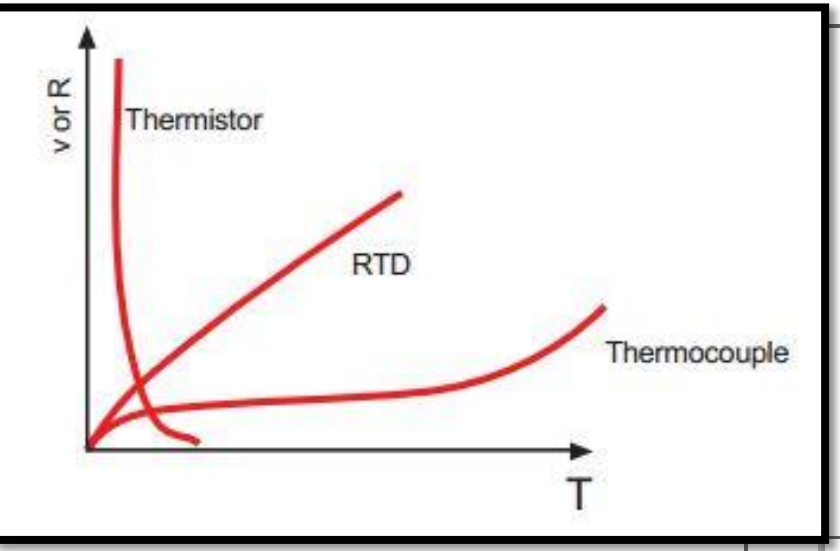
Attributes of the Temperature Sensor		
Parameter/Criteria	**Thermocouple**	**RTD**
Typical Measurement Range	-450 ºF (-267 ºC) to +4200 ºF (2316 ºC)	-400 ºF (-240 ºC) to +1200 ºF (649 ºC)
Interchangeability	Good	Excellent
Long-term Stability	Poor to Fair	Excellent
Accuracy	Medium	High
Repeatability	Poor to Fair	Excellent
Sensitivity (output)	Low	Good
Response	Medium to Fast	Good
Linearity	Fair	Good
Self Heating	No	Low
Tip (end) Sensitivity	Excellent	Fair
Lead Effect	High	Medium
Size/Packaging	Small to Large	Medium to Small

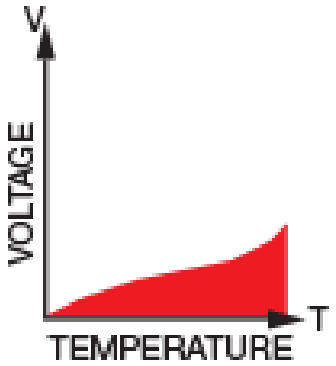
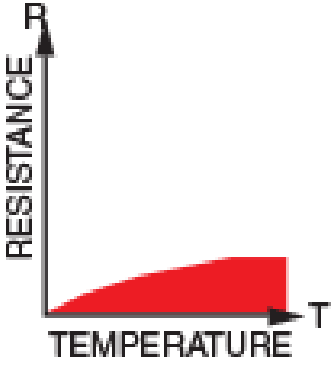
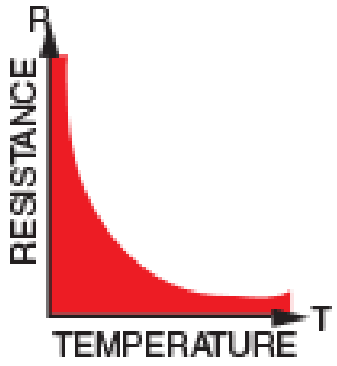
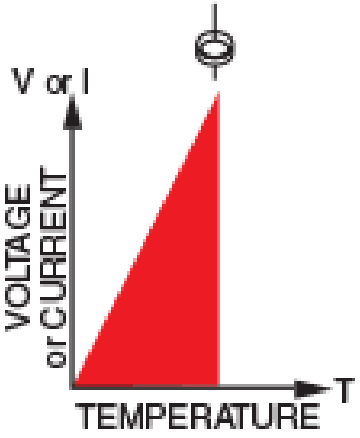
Advantages and Disadvantages		
Sensor	**Advantages**	**Disadvantages**
Thermocouple	• Inexpensive • No resistance leadwire problems • Fastest response • Simple and rugged • High temperature operation • Tip (end) temperature sensing	• Least sensitive • Non-linear • Low voltage • Least stable, repeatable
RTD	• Good stability • Excellent accuracy • Contamination resistant • Good linearity • Area temperature sensing • Very repeatable temperature measurement	• Marginally higher cost • Current source required • Self-heating • Slower response time • Medium sensitivity to small temperature changes

Thermistors

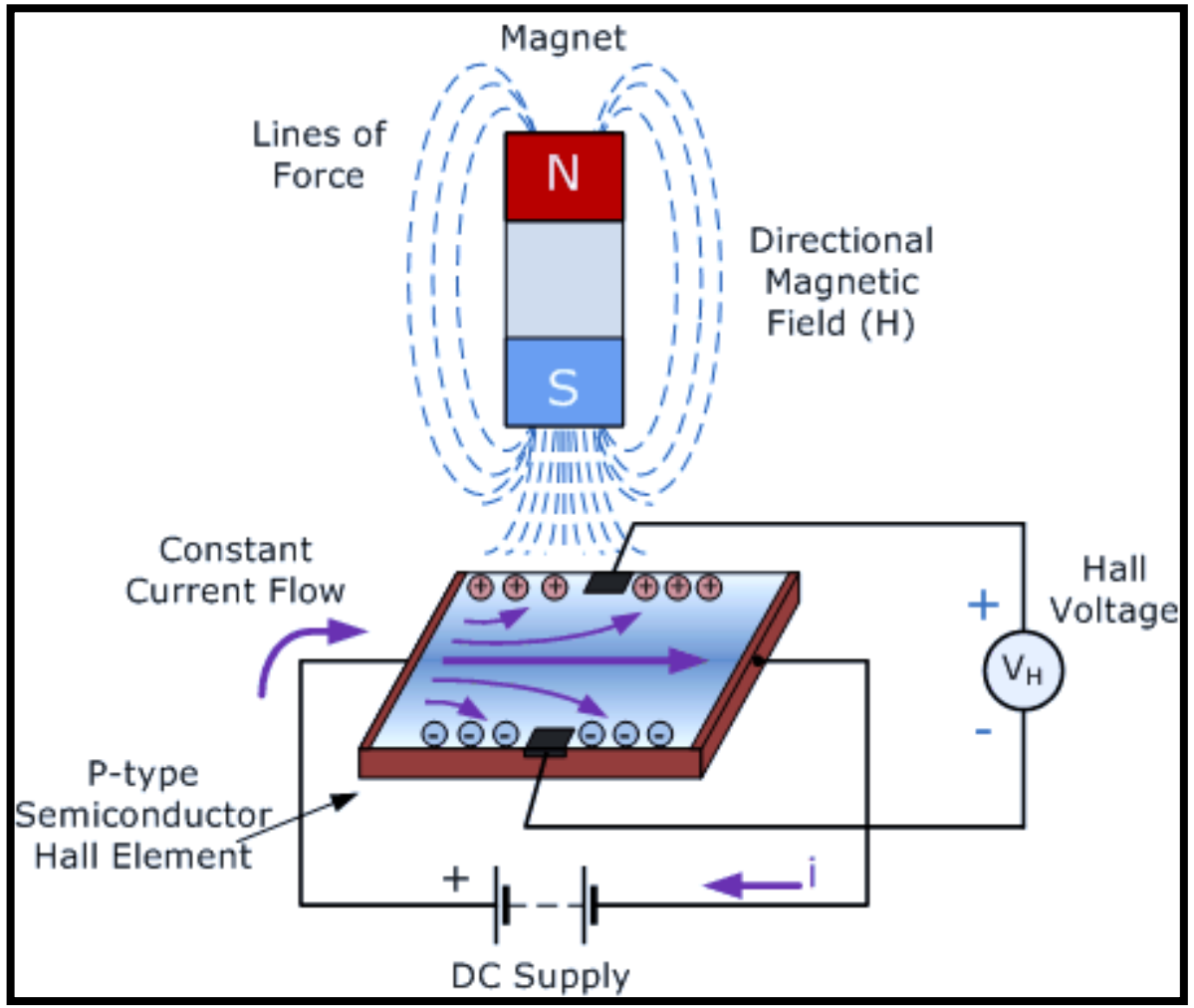


- Resistors that vary with temperature
- Two Types:
  - PTC (resistance increases as temperatures rise)
  - NTC (resistance decreases as temperatures rise)
- Produce a higher degree of change for a given temperature than an RTD
- Have a highly nonlinear relationship
- Suitable where high resolution is needed for a narrow temperature range
- Found in medical devices, scientific equipment, food handling equipment, incubators, and home appliances such are thermostats.



	Thermocouple	RTD	Thermistor	I. C. Sensor
				
Advantages	☒ Self-powered ☒ Simple ☒ Rugged ☒ Inexpensive ☒ Wide variety ☒ Wide temperature range	☒ Most stable ☒ Most accurate ☒ More linear than thermocouple	☒ High output ☒ Fast ☒ Two-wire ohms measurement	☒ Most linear ☒ Highest output ☒ Inexpensive
Disadvantages	☒ Non-linear ☒ Low voltage ☒ Reference required ☒ Least stable ☒ Least sensitive	☒ Expensive ☒ Current source required ☒ Small Δ R ☒ Low absolute resistance ☒ Self-heating	☒ Non-linear ☒ Limited temperature range ☒ Fragile ☒ Current source required ☒ Self-heating	☒ T<200°C ☒ Power supply required ☒ Slow ☒ Self-heating ☒ Limited configurations

Hall effect sensors



- Used to measure the magnitude of a magnetic field
- Output voltage is directly proportional to the magnetic field strength
- Used for proximity sensing, positioning, speed detection, and current sensing applications.

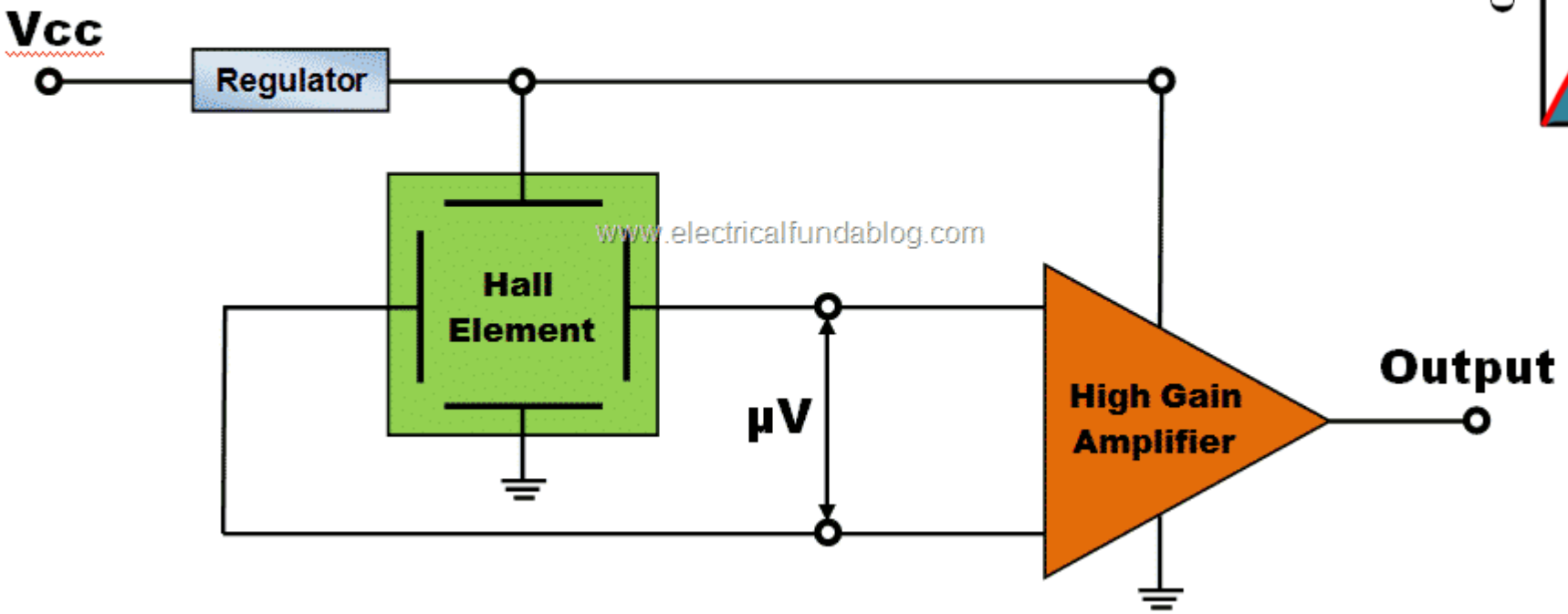
- Used for ….
  - position sensing
  - magnetometers,
  - highly reliable switches
  - to measure the rotational velocity of different machines and motors

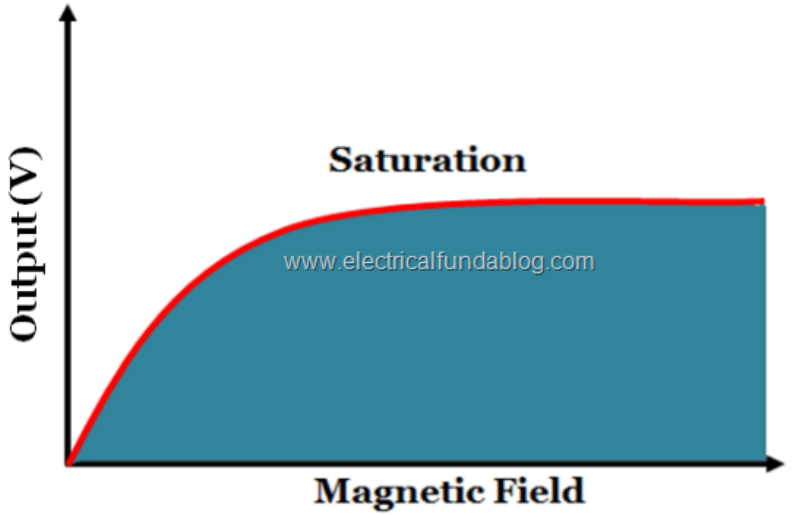
- Advantage:
  - inexpensive
  - tolerate harsh environmental conditions
  - Maintenance free, robust
  - immune to vibration, dust and water.

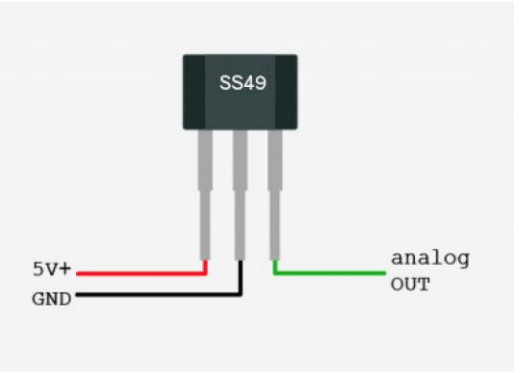
- On the basis of Output, the Hall Effect Sensors can be classified into two types:
  - Analog Output Hall Effect Sensors
  - Digital Output Hall Effect Sensors

- On the basis of Operation, the Hall Effect Sensors can be classified into two types:
  - Bipolar Hall Effect Sensor
  - Unipolar Hall Effect Sensor

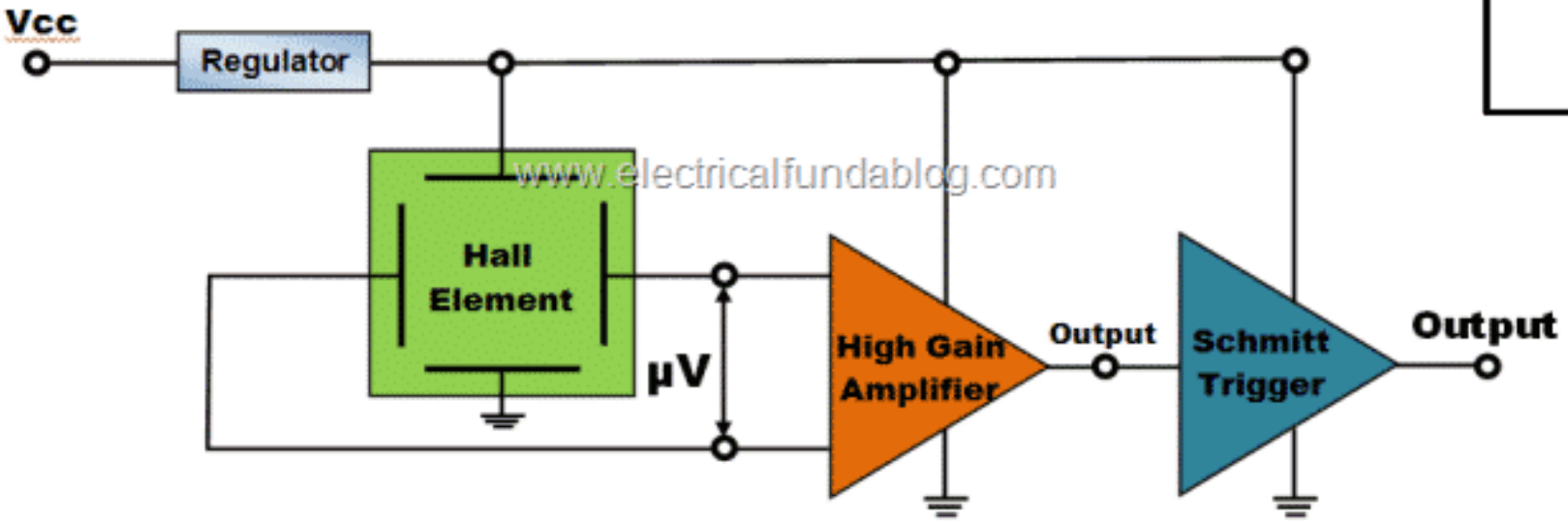
Analog Output Hall Effect Sensor



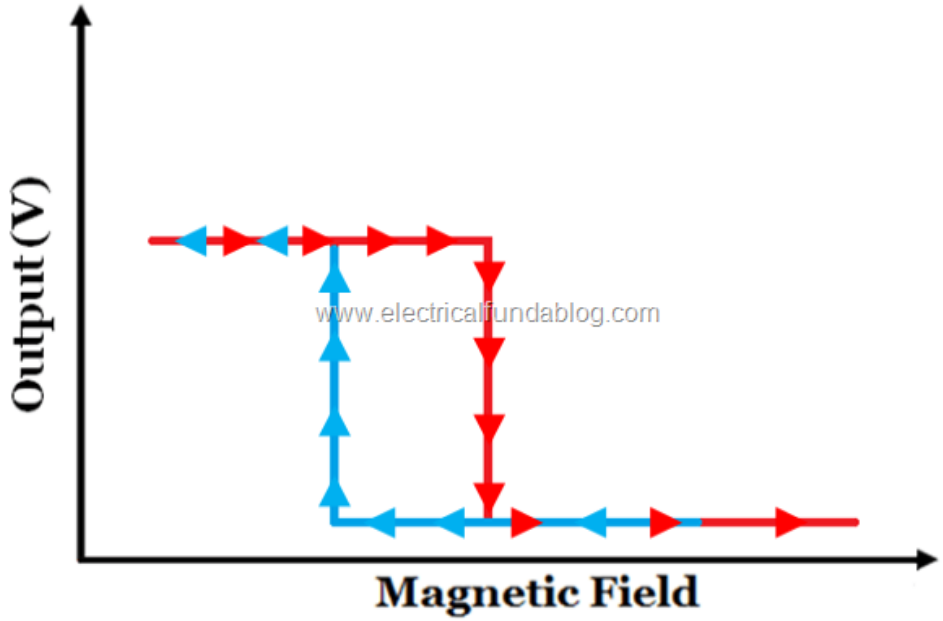




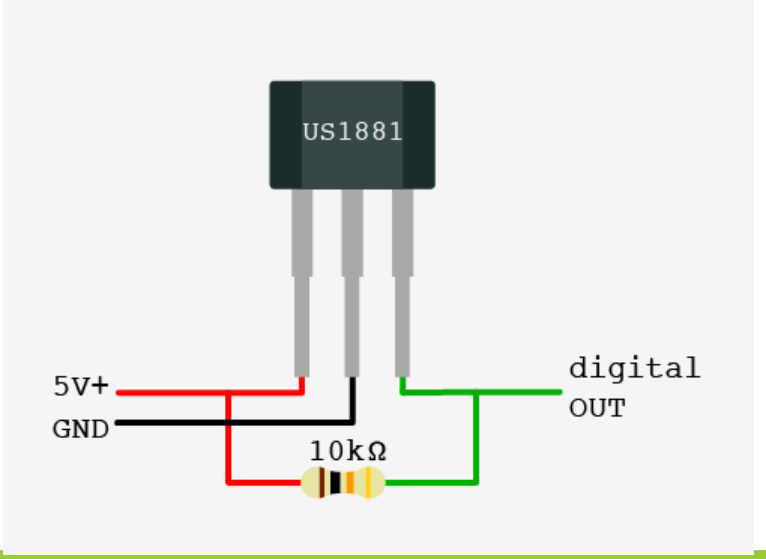
Digital Output Hall Effect Sensor



www.electricalfundablog.com



www.electricalfundablog.com

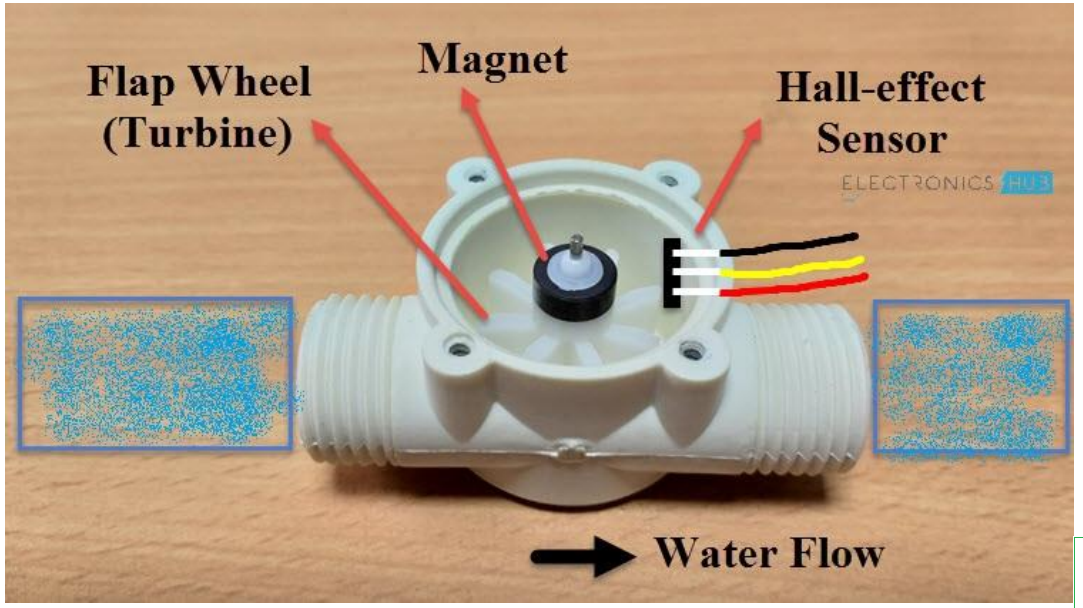


Application of Analog Hall Effect Sensors:

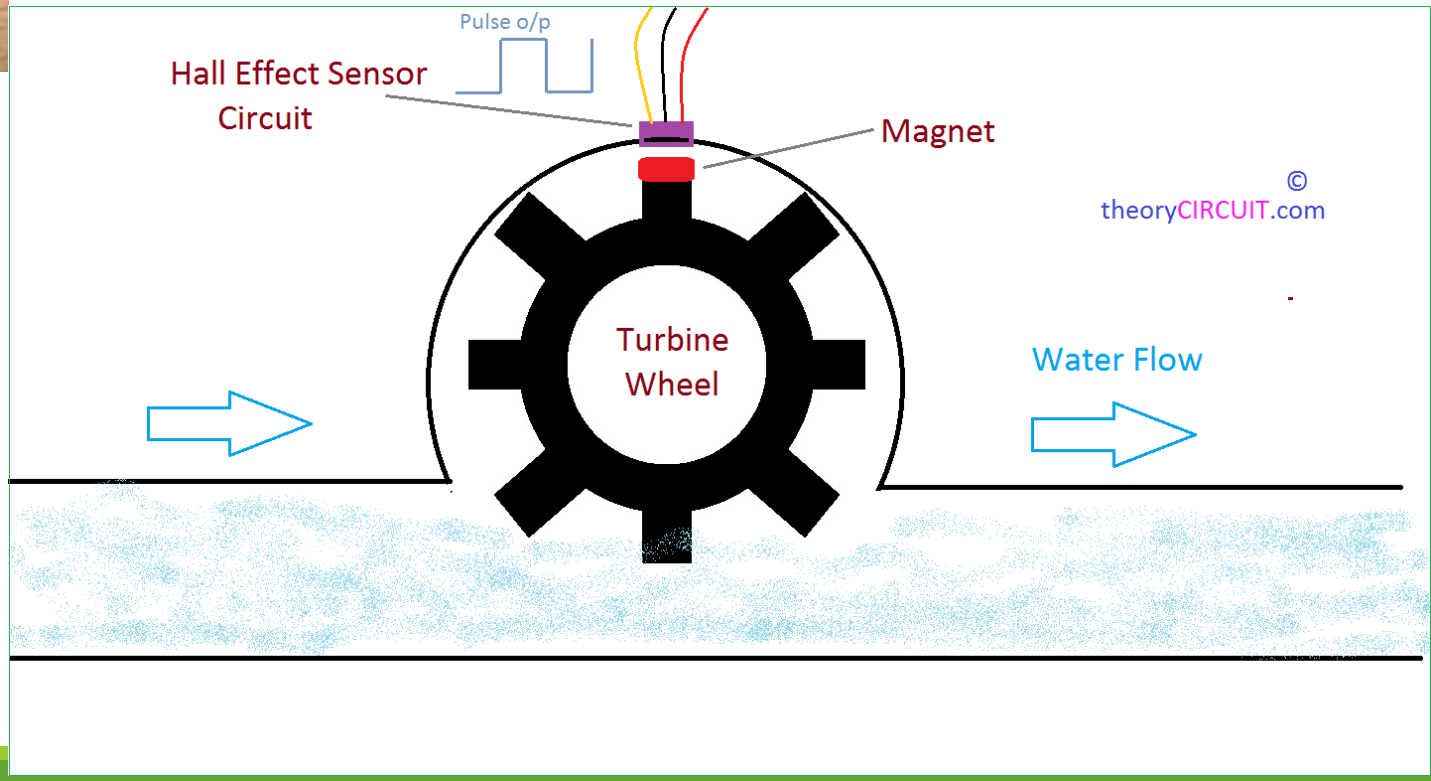
- Direct Current sensing in Clamp meters
- Wheel speed detection for the anti-lock braking system, (ABS)
- Motor control devices for protection and indications
- Sensing the availability of Power supply
- Motion Sensing
- Sensing the rate of flow
- Sensing Diaphragm pressure in Diaphragm pressure gauge
- Sensing Vibration
- Sensing Ferrous Metal in Ferrous Metal Detectors
- Voltage Regulation

Application of Digital Hall Effect Sensors:

- Sensing the angular position of the crank shaft for the firing angle of the spark plugs
- Sensing the position of the car seats and seat belts for air-bag control
- Wireless Communications
- Sensing Pressure
- Sensing Proximity
- Sensing rate of flow
- Sensing position of Valves
- Sensing position of Lens



Sensing the rate of flow using Hall effect sensor

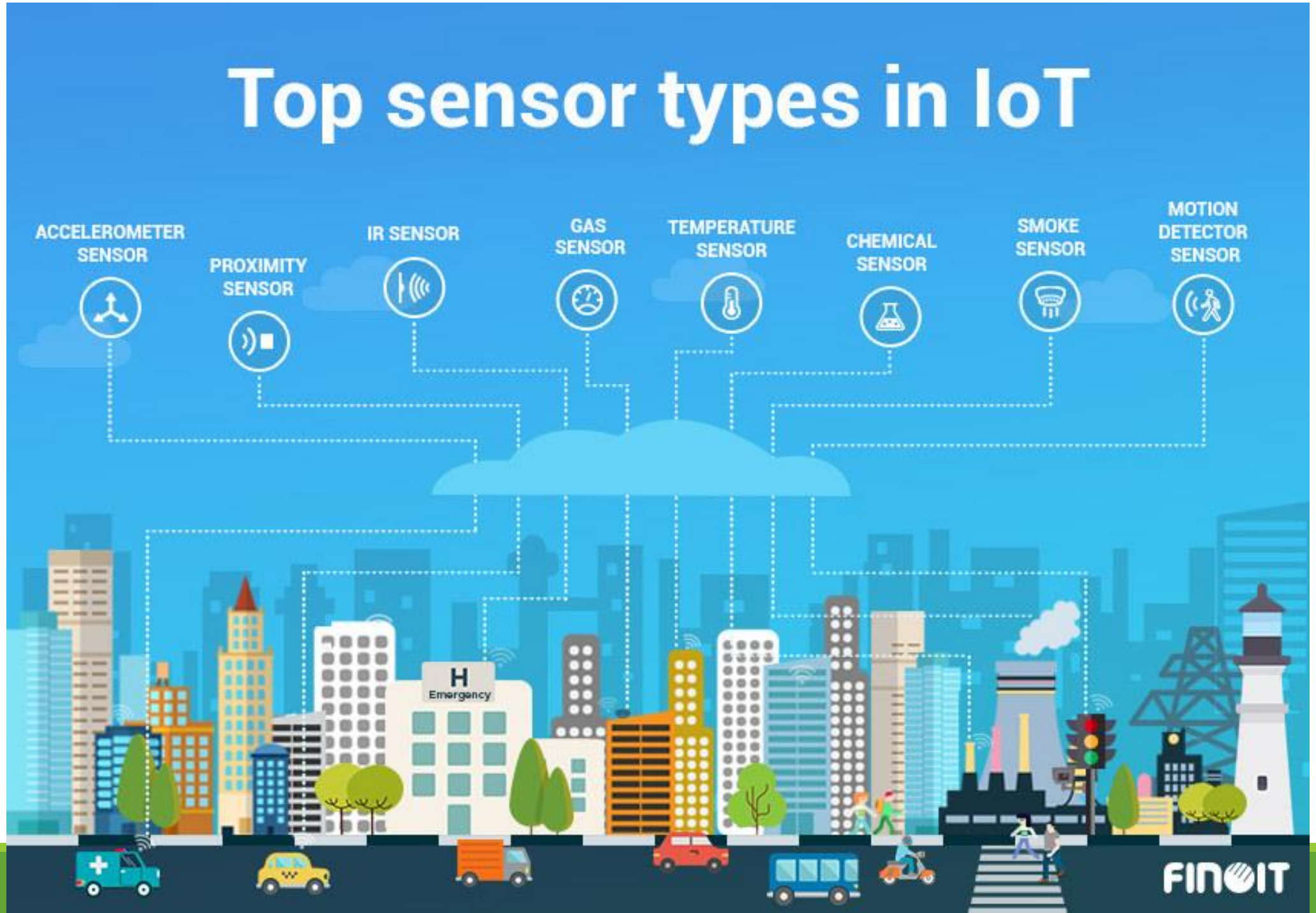


Limitations:

•They are not capable to measure current flow at a distance more than 10 cm. The only solution to overcome this issue is to use a very strong magnet that can generate a wide magnetic field.

•Accuracy of the measured value is always a concern as external magnetic fields may affect the values.

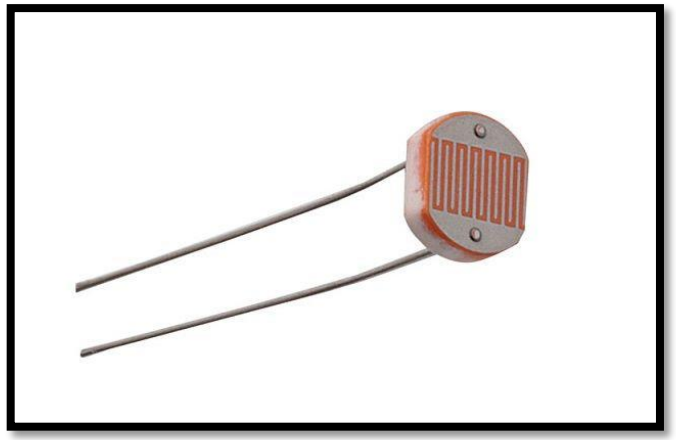
•High Temperature affects the conductor resistance. This will in turn affect the charge carrier's mobility and sensitivity of Hall Effect Sensors.


Top sensor types in IoT
ACCELEROMETER SENSOR
PROXIMITY SENSOR
IR SENSOR
GAS SENSOR
TEMPERATURE SENSOR
CHEMICAL SENSOR
SMOKE SENSOR
MOTION DETECTOR SENSOR
H
Emergency
FINOIT

Photoelectric sensors

Two principles:

- Photo-resistor varies in resistance depending on light intensity
- Photodiodes convert light into an electrical current.

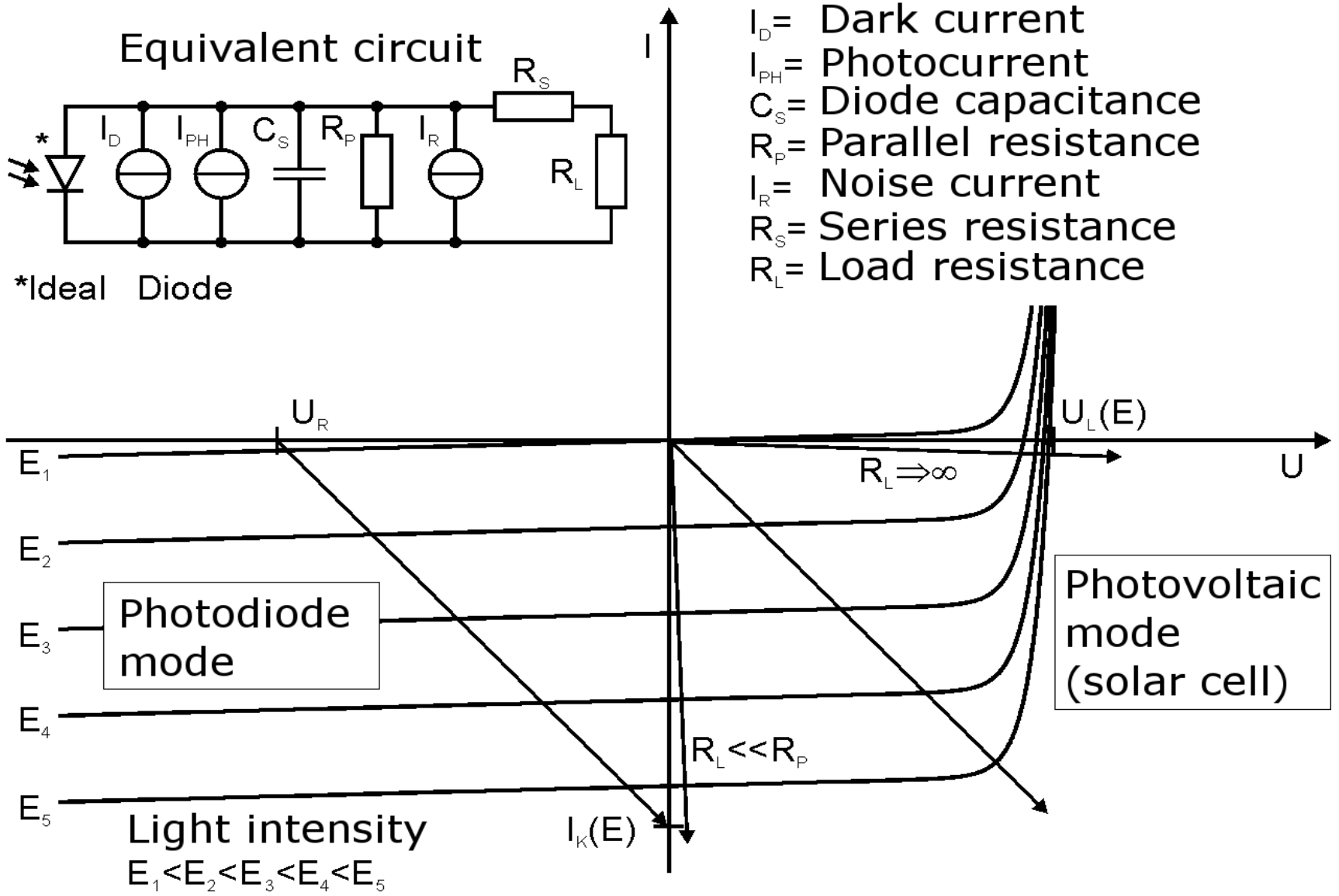


- In the dark, a photoresistor can have quite a high resistance (in the megaohm range).
- Photons absorbed by the semiconductor allow electrons to jump to the conduction band and conduct electricity.
- Photoresistors are wavelength Sensitive

- Photodiodes are semiconductors with a p-n junction.
- The device responds to light by creating an electron-hole pair which produces current
- Solar cells operate in this photovoltaic mode
- Photo diode in reverse bias can be used to improve the latency and response time

Photodiodes are optimized for light detection while solar cells are optimized for energy conversion efficiency

Photo diode and Solar cell operation modes

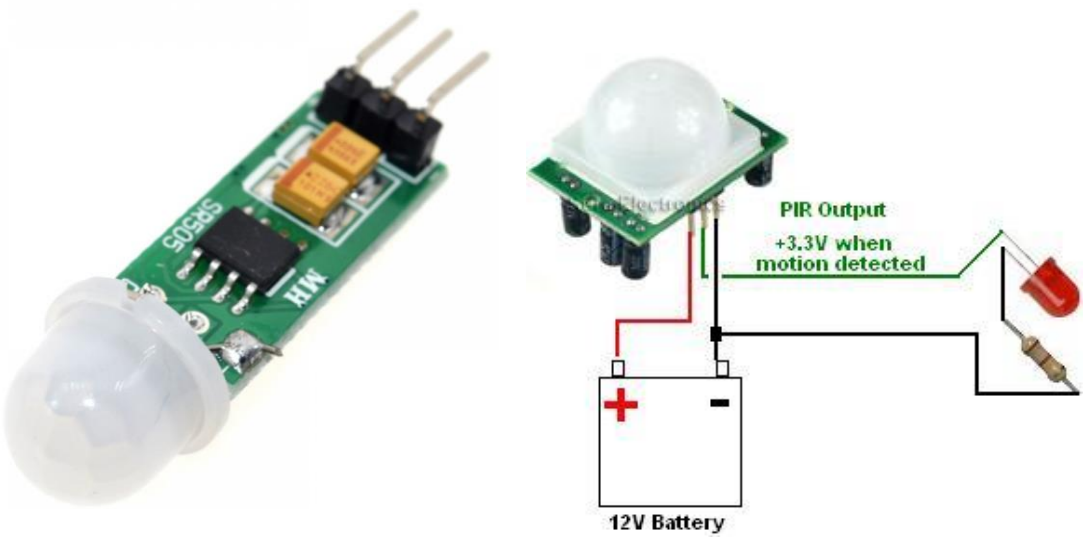


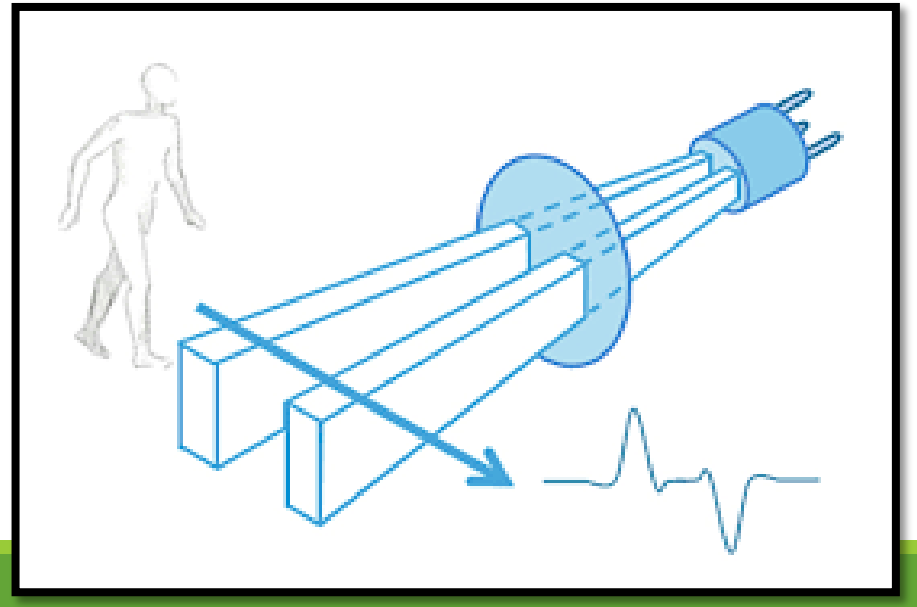
Parameter	Photo Resistor	Photo Diode
Light Sensitivity	Low	High
Active/passive	Passive	Active
Temp. Sensitivity	High	Low
Response time to light change	Long	Short

PIR sensors

Pyroelectric Infrared or Passive Infrared sensors

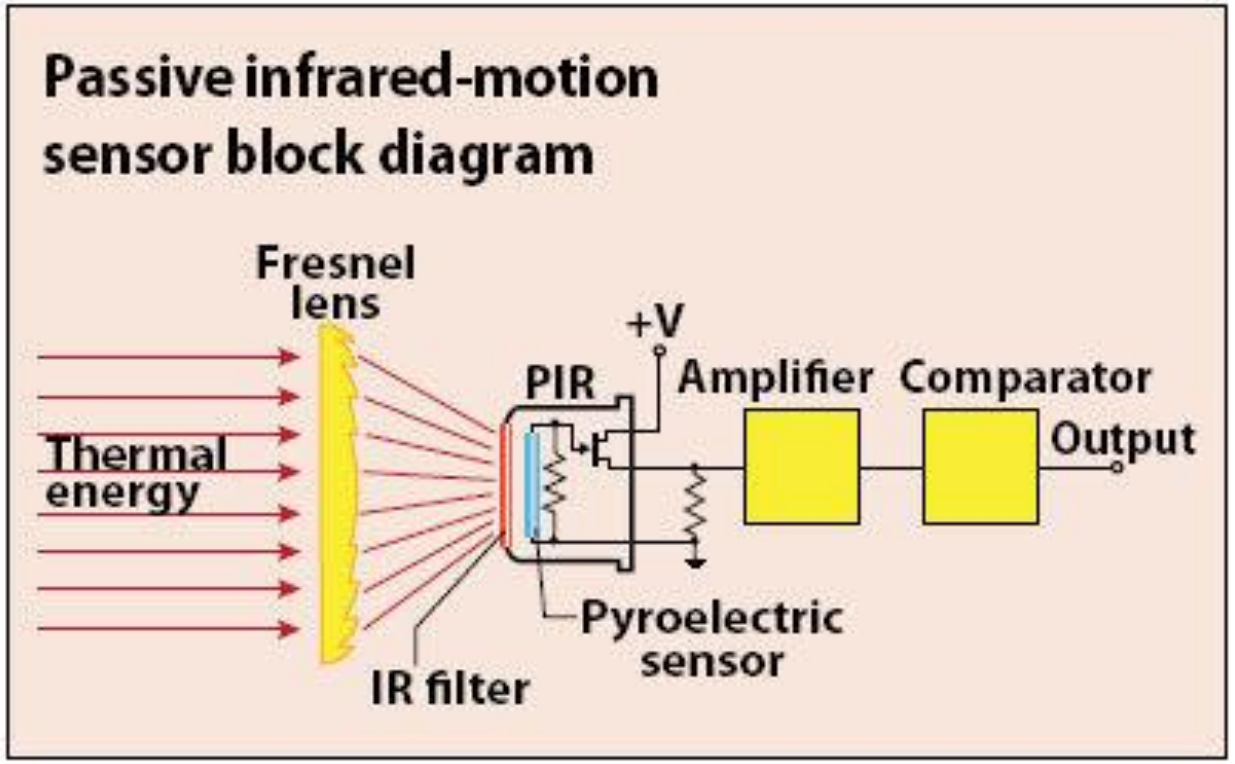
- All objects with a temperature above absolute zero emit heat energy in the form of radiation. Not visible to human eye as it is in Infrared band
- The PIR sensors use a crystalline material that generates current when subjected to IR radiation





- To scan a larger area with a single sensor requires multiple Fresnel lenses that condense light from regions of the room to create distinct regions on the PIR array.

- The hold time specifies for how long to output a motion event after an object has been detected moving across the path of the PIR.
- The shorter the hold time, the more events may be output.

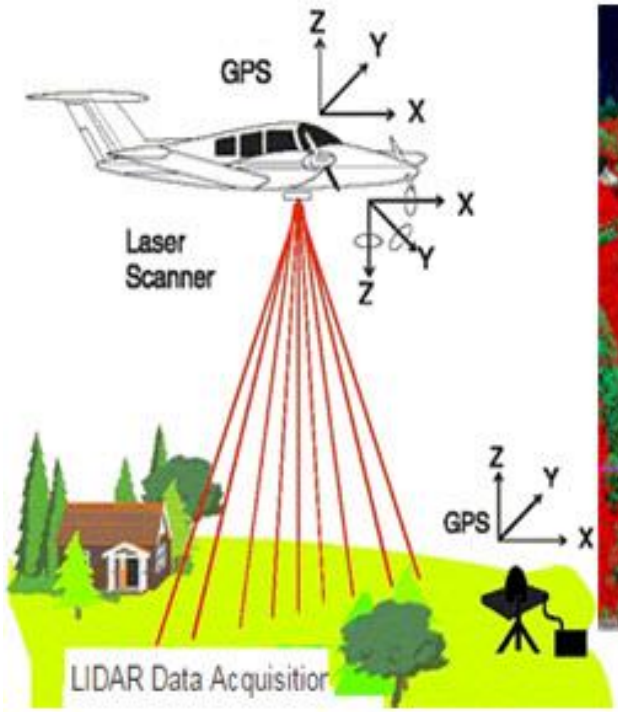


LiDAR and active sensing systems

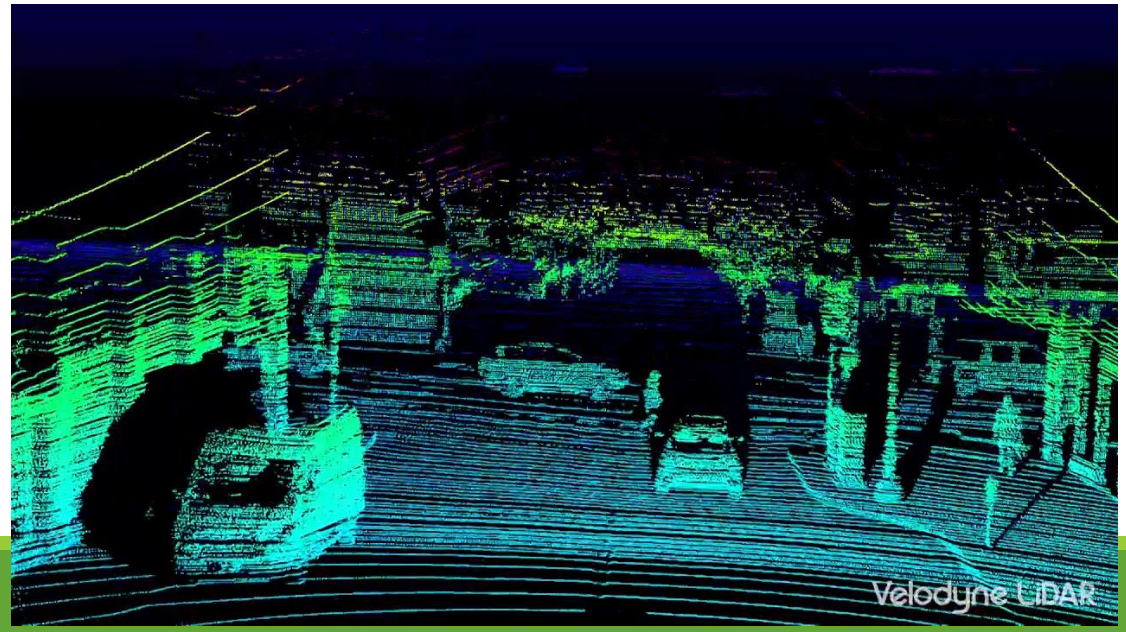
Light Detection And Ranging

- LiDAR is an active sensor technology, and broadcasts laser energy.
- As a laser hits an object, some of the energy will be reflected back towards the LiDAR emitter
- LiDAR systems are capable of very long ranging and scanning, even from satellites.
- The laser will pulse up to 150,000 pulses per second, which can reflect off an object back to a photodiode array.
- LiDAR is used in automated and self-driving vehicles, robotics, surveillance, and environmental studies.
- It is also used to analyze gases, atmospheres, cloud formations and compositions, particulates, the speed of moving objects etc….

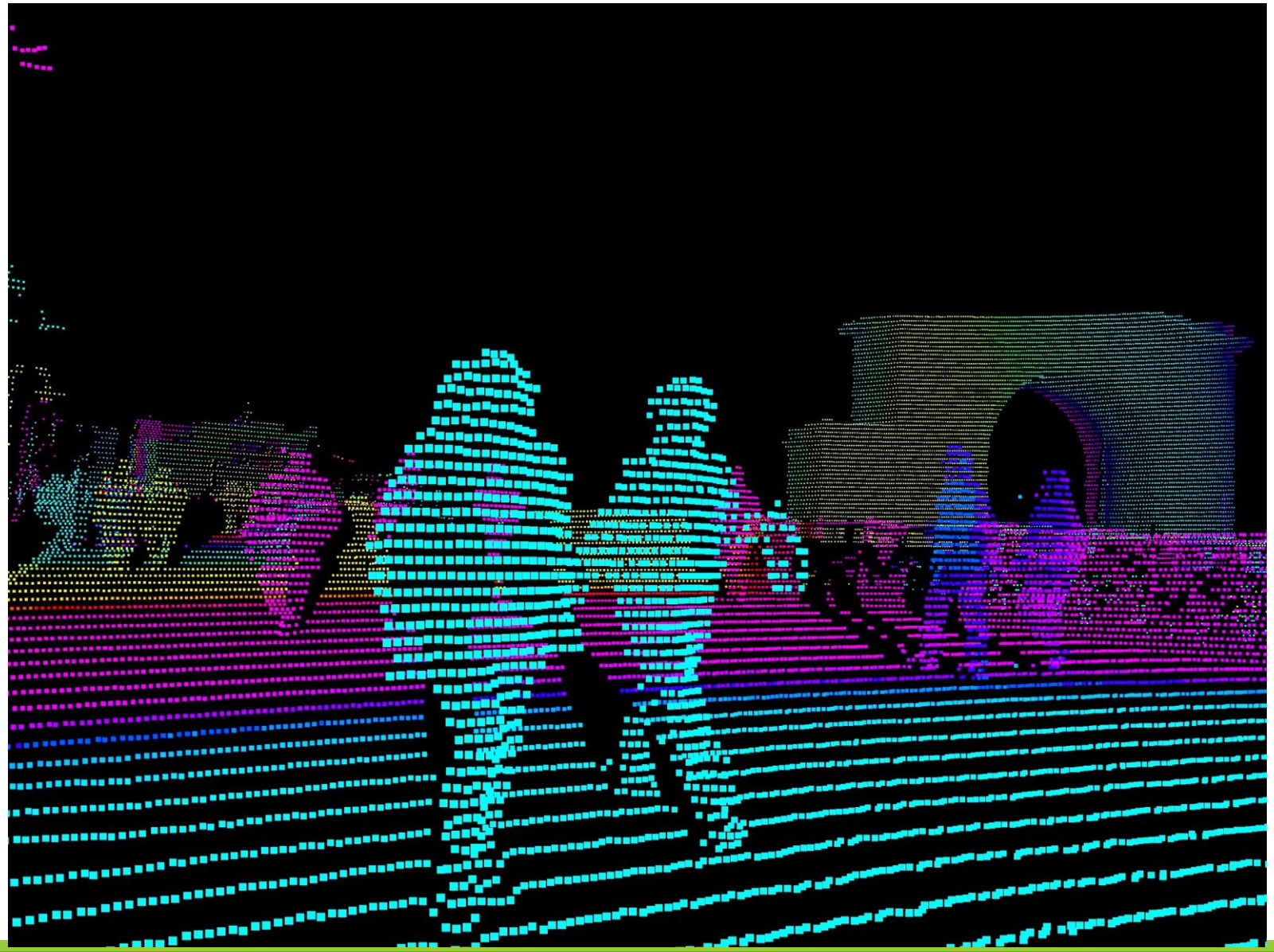
- The lasers wavelength is between the 600 to 1000 nm
- Relatively inexpensive
- Power is constrained for safety reasons to prevent eye damage.
- The laser apparatus can also sweep the scene via a rotating mirror to build a comprehensive 3D image of the environment.



Aerial LIDAR Range Scan



VW's self-driving division picked Luminar's system from a crowded field



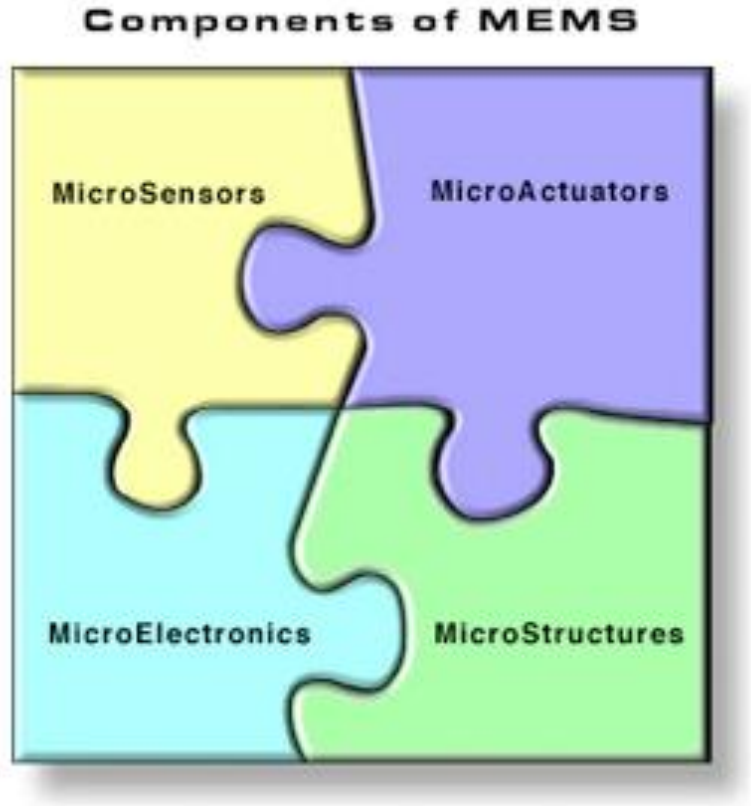
MEMS sensors

Micro-electromechanical systems

MEMS mechanical structures can spin, stretch, bend, move, or alter form, which in turn affects an electrical signal.

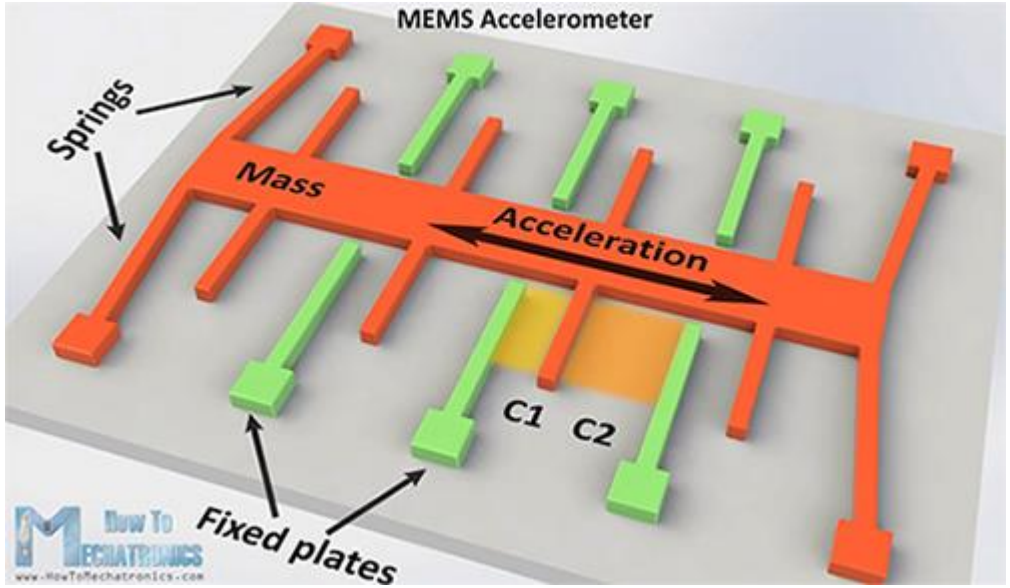
MEMS devices are manufactured in a typical silicon fabrication process using multiple masks, lithography, deposition, and etching processes.

MEMS silicon dies are then packaged with other components such as operational amplifiers, analog to digital converters, and support circuitry.



MEMS accelerometers and gyroscopes

- Accelerometers and gyroscopes are common in many mobile devices
- They are used in positioning and movement tracking, such as with pedometers and fitness trackers.
- Gyroscopes detect rotational motion, and accelerometers respond to changes in linear motion.
- Both gyroscopes and accelerometers require power supplies and an op-amp for signal conditioning.
- After conditioning, the output is ready to be sampled by a digital signal processor.

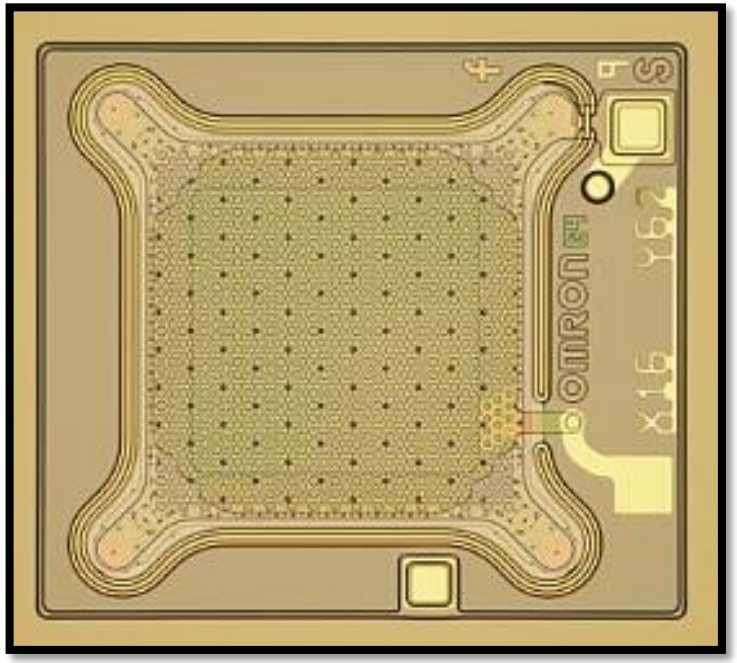


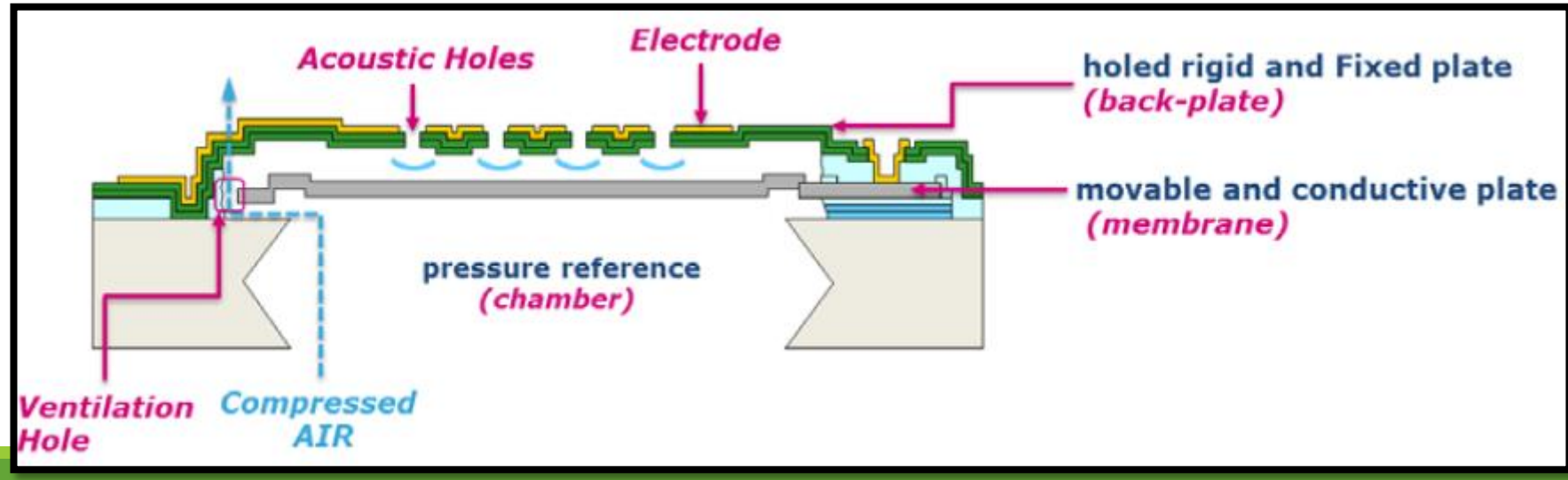
MEMS microphones

Sound and vibration measurements are common in the industrial IoT and predictive maintenance applications

This type of sensor will require an analog-to-digital converter of sufficient sampling frequency and amplifier to strengthen the signal

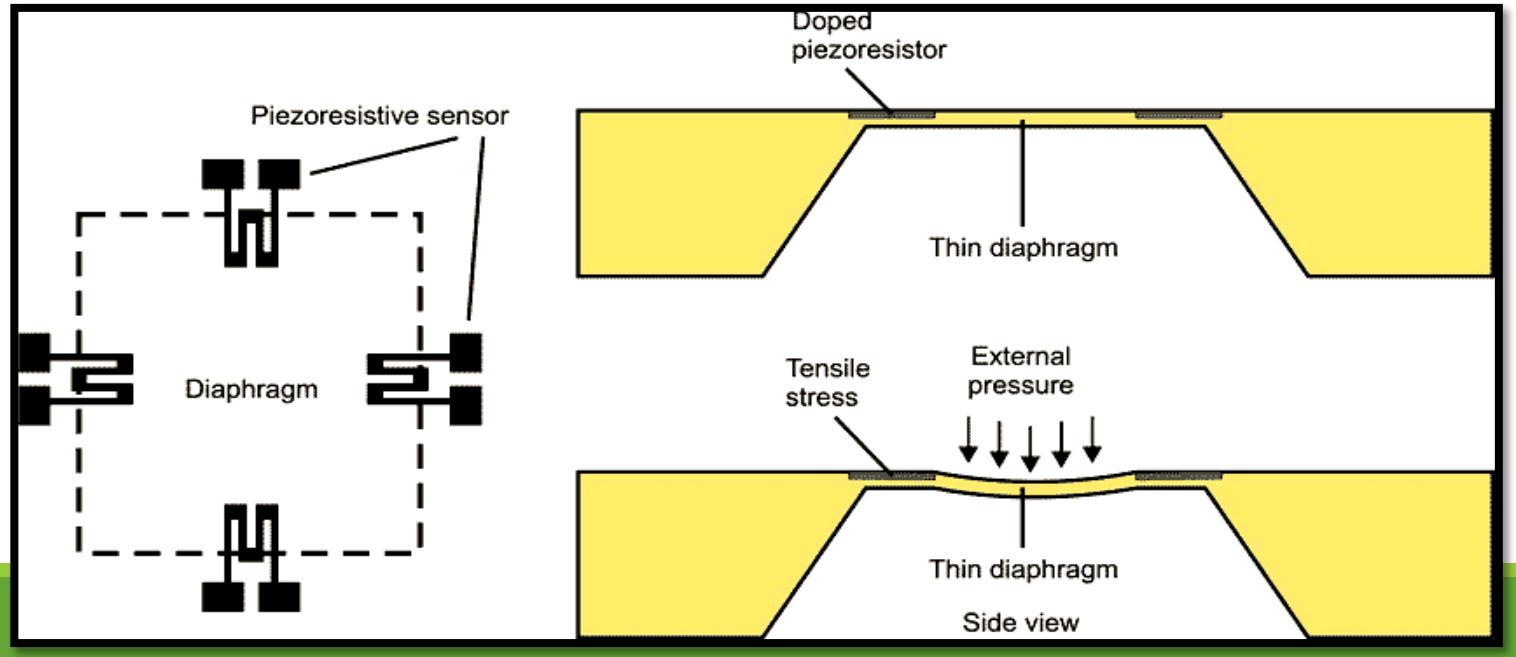
It can be analog or digital.





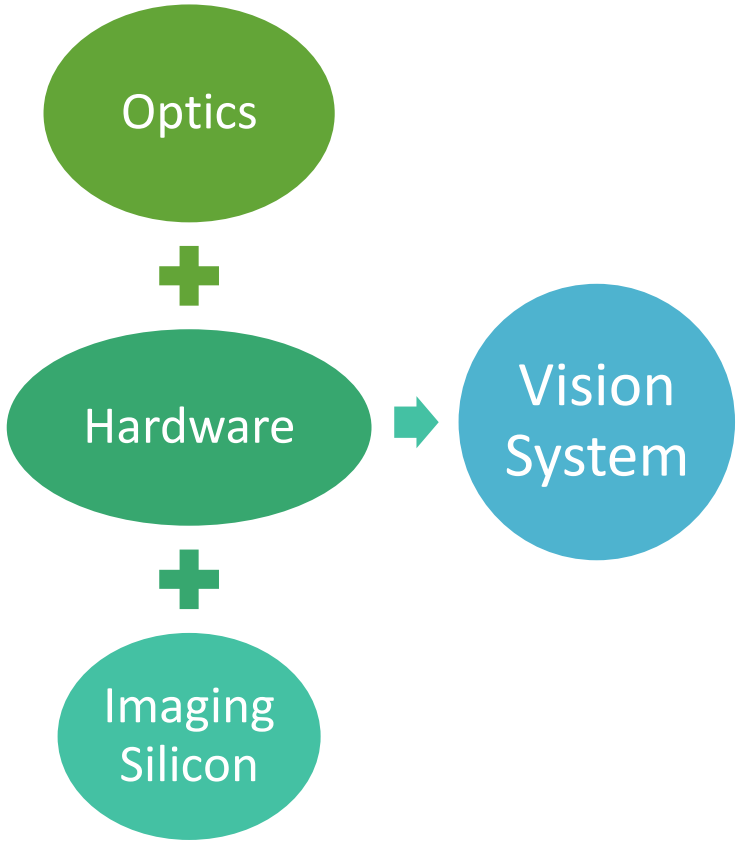
MEMS pressure sensors

- Pressure and strain gauges are used in a variety of IoT deployments, from smart cities monitoring infrastructure to industrial manufacturing
- These are used to measure fluid and gas pressures
- The heart of the sensor is a piezoelectric circuit
- A diaphragm is placed above or below a cavity on the piezoelectric substrate.
- The substrate is flexible, and allows the piezo crystals to change shape.
- This change in shape results in a directly correlated resistance change in the material



IoT Vision Systems

Smart sensors include devices such as video cameras and vision systems along with high-end processors, digital signal processors, FPGAs, and custom ASICs.



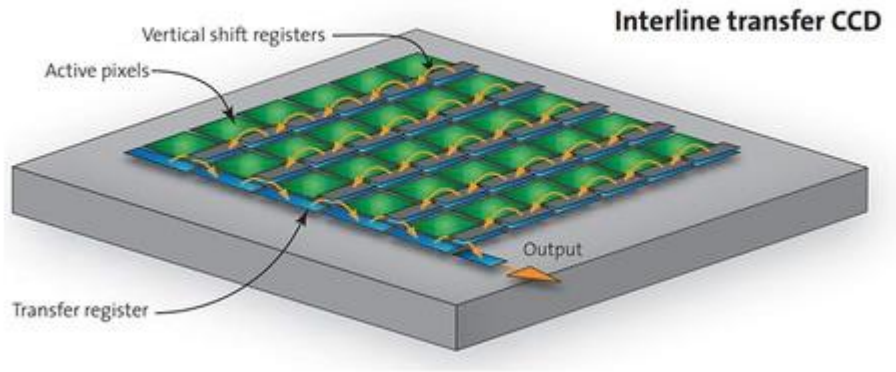
Sensing element in Vision System

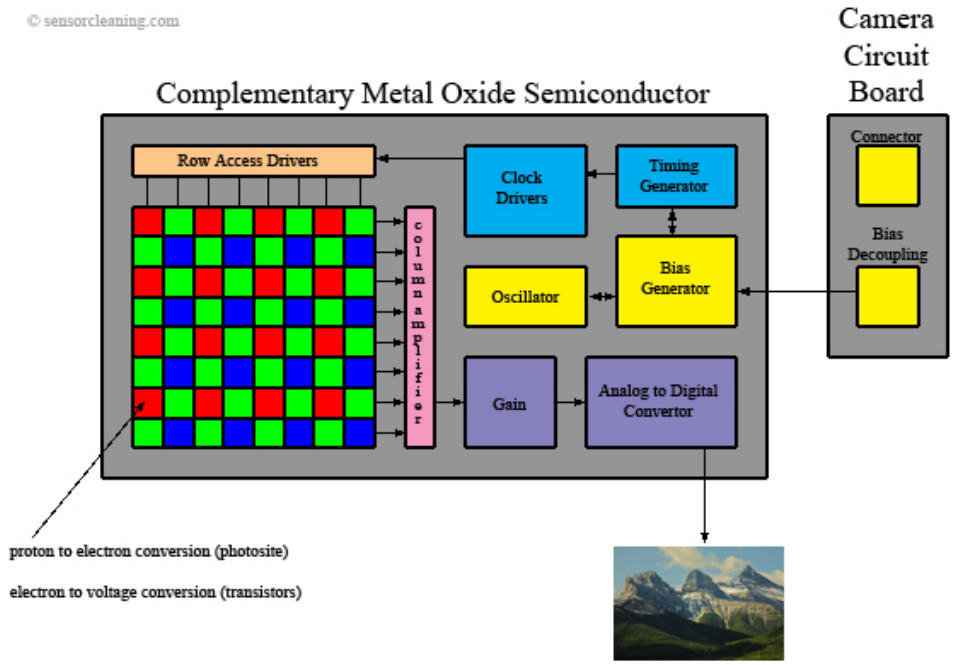
Charge Coupled Devices:

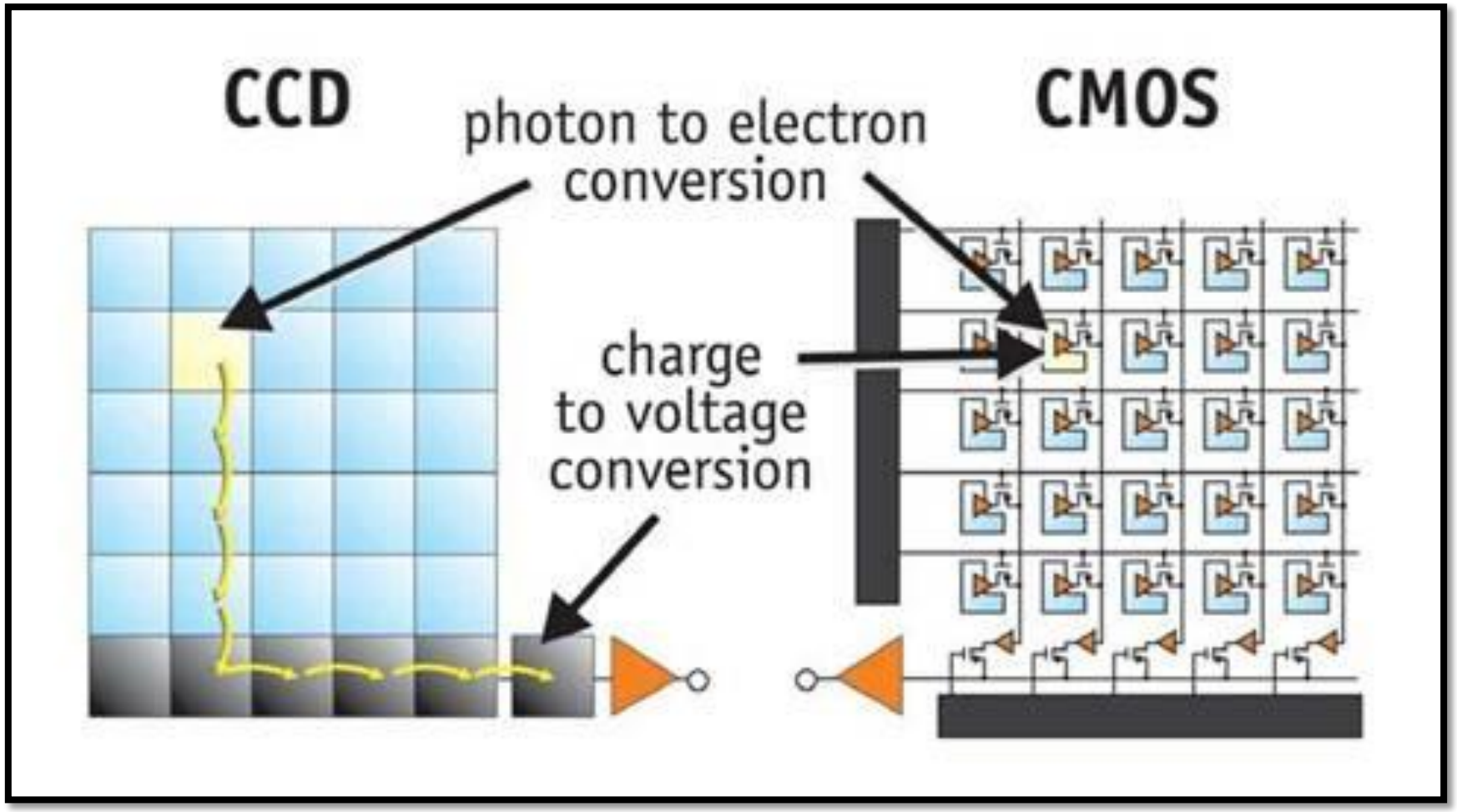
- Charge is transported from the sensor to the edge of the chip to be sampled sequentially via an analog-to-digital converter.
- CCDs create high-resolution and low-noise images.
- They consume considerable power (100x that of CMOS).
- They also require a unique manufacturing process.

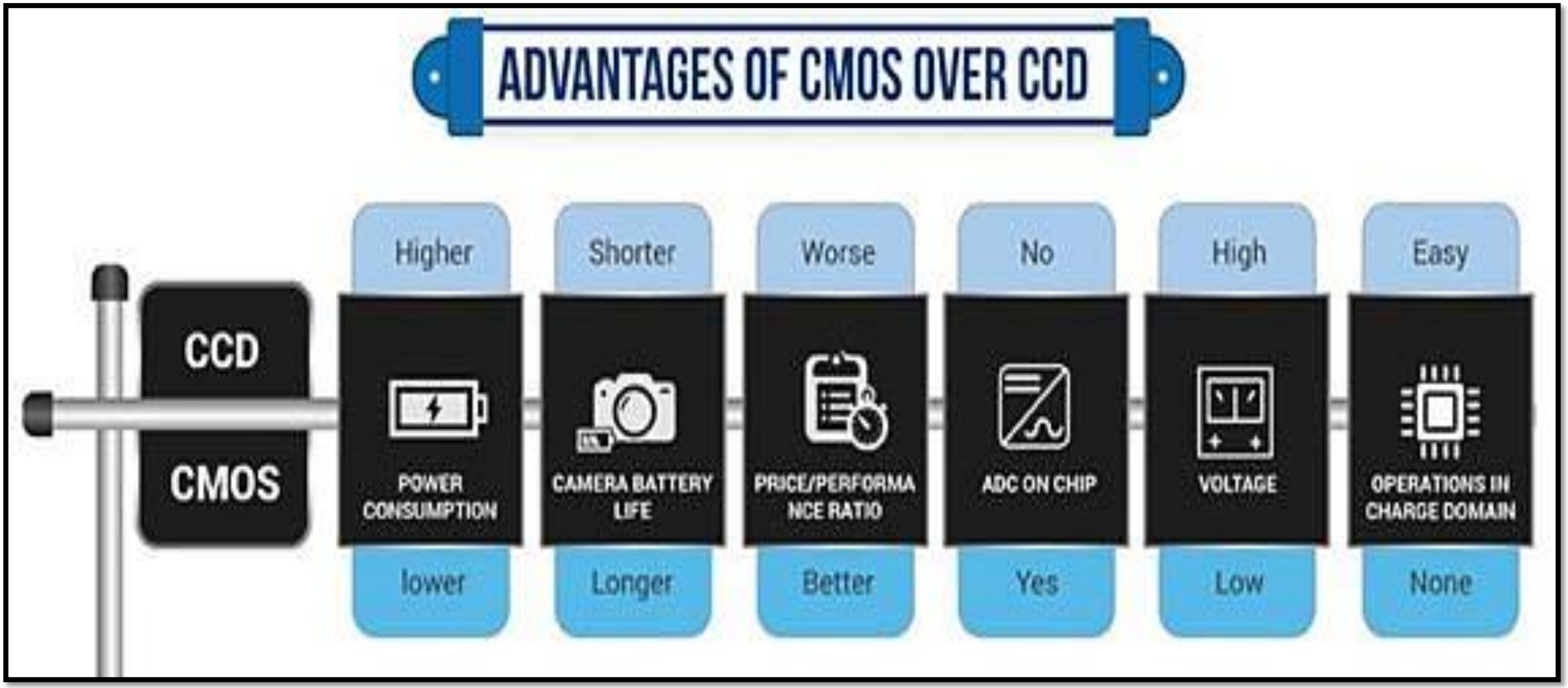
CMOS:

- Individual pixels contain transistors to sample the charge and allow each pixel to be read individually.
- CMOS is more susceptible to noise, but uses little power.



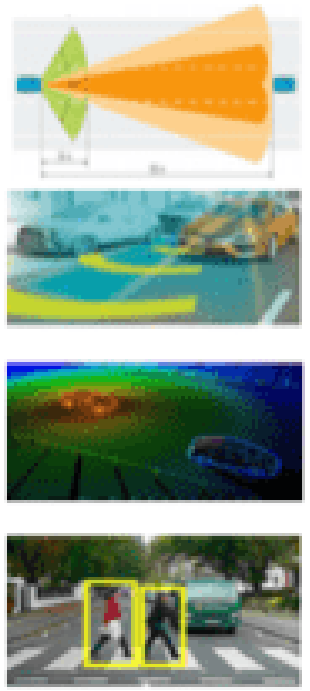


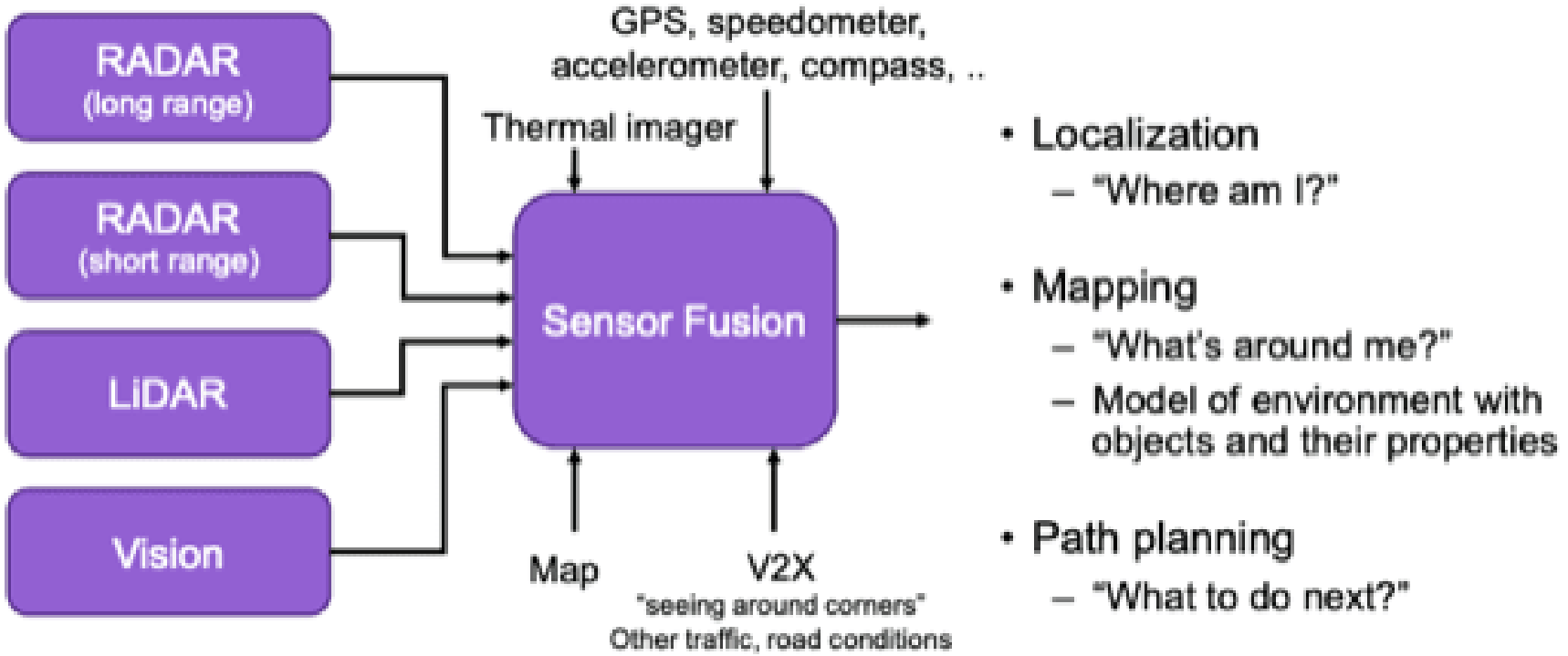

CCD
photon to electron conversion
CMOS
charge to voltage conversion


ADVANTAGES OF CMOS OVER CCD
CCD
CMOS
Higher
lower
POWER CONSUMPTION
Shorter
Longer
CAMERA BATTERY LIFE
Worse
Better
PRICE/PERFORMANCE RATIO
No
Yes
ADC ON CHIP
High
Low
VOLTAGE
Easy
None
OPERATIONS IN CHARGE DOMAIN

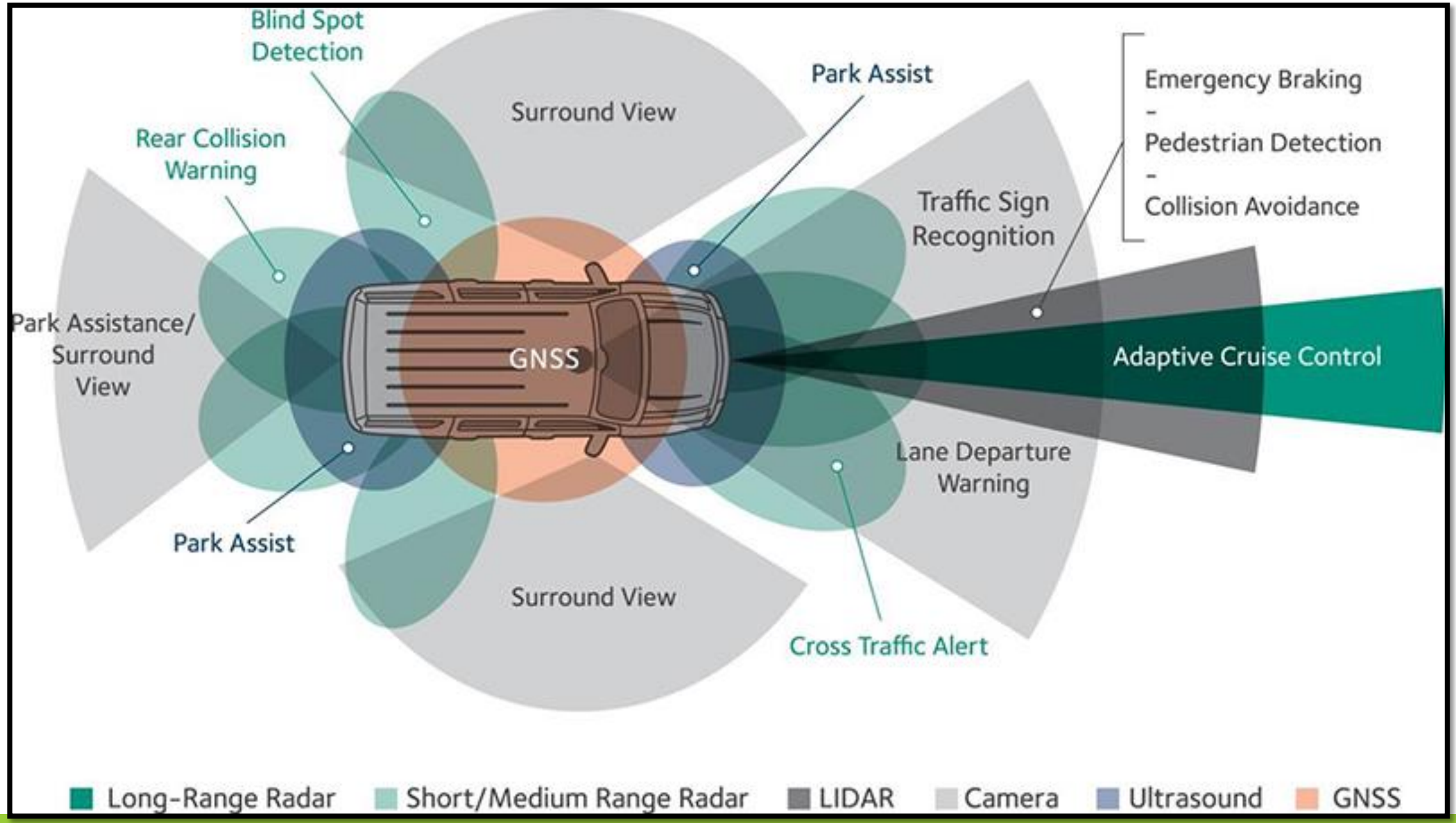
Sensor fusion

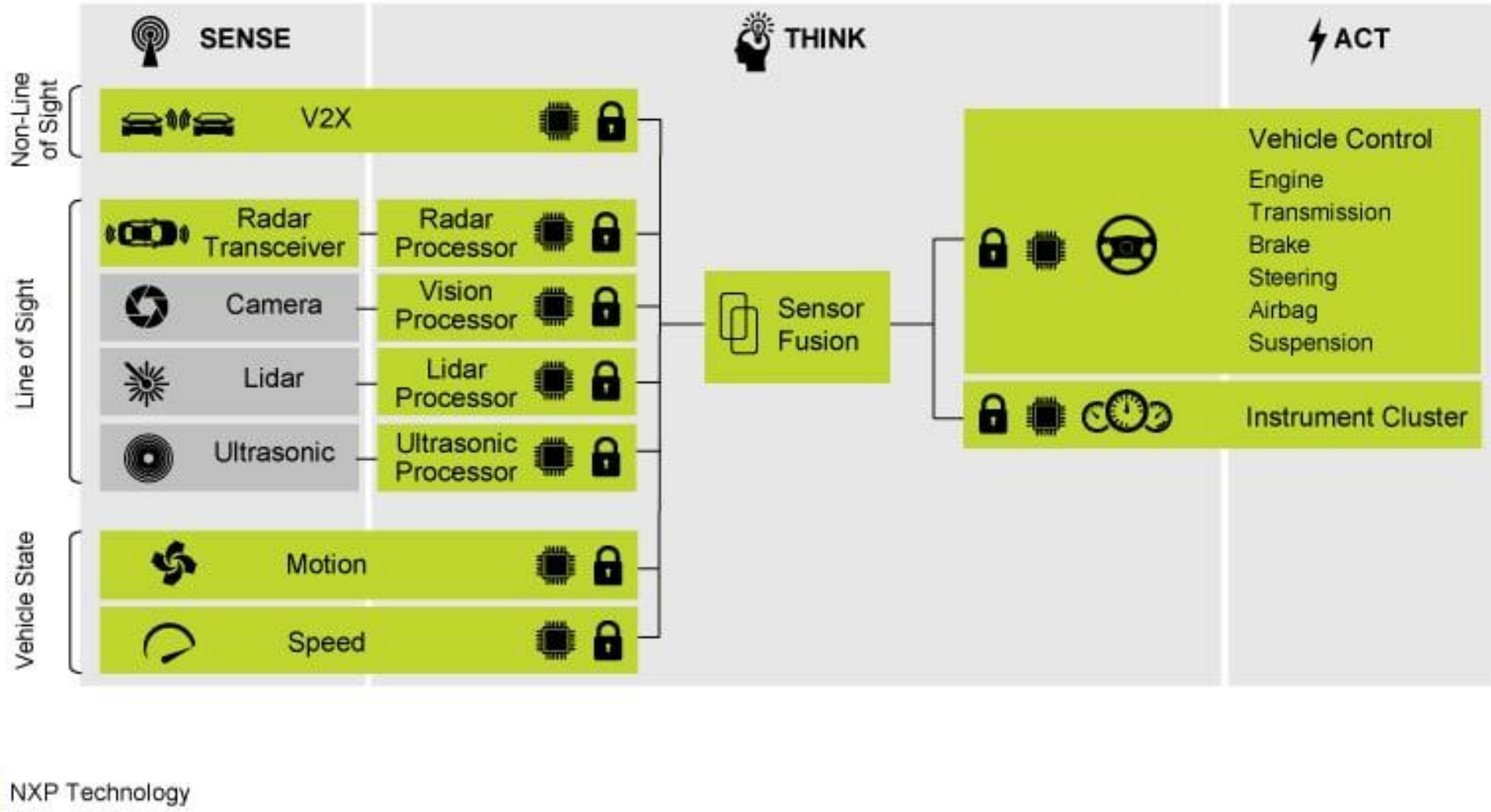
Sensor fusion is the process of combining several different kinds of sensor data to reveal more about context than a single sensor can provide.





- Localization
  - "Where am I?"
- Mapping
  - "What's around me?"
  - Model of environment with objects and their properties
- Path planning
  - "What to do next?"


Blind Spot Detection
Surround View
Park Assist
Rear Collision Warning
Emergency Braking
-
Pedestrian Detection
-
Collision Avoidance
Traffic Sign Recognition
Park Assistance/ Surround View
GNSS
Adaptive Cruise Control
Lane Departure Warning
Park Assist
Surround View
Cross Traffic Alert
Long-Range Radar
Short/Medium Range Radar
LIDAR
Camera
Ultrasound
GNSS

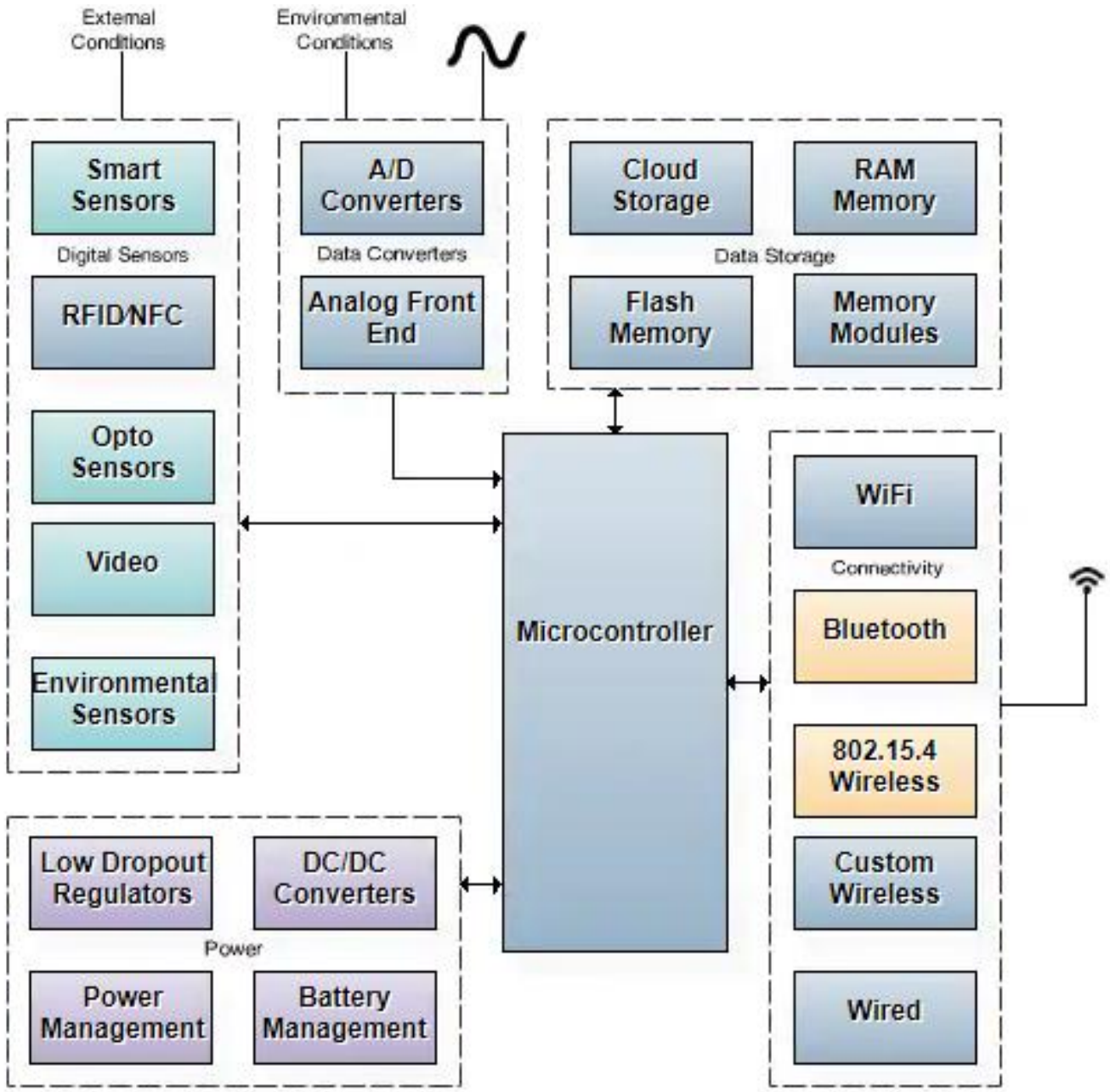

SENSE
THINK
ACT
Non-Line of Sight
Line of Sight
Vehicle State
V2X
Radar Transceiver
Camera
Lidar
Ultrasonic
Motion
Speed
Radar Processor
Vision Processor
Lidar Processor
Ultrasonic Processor
Sensor Fusion
Vehicle Control
Engine
Transmission
Brake
Steering
Airbag
Suspension
Instrument Cluster
NXP Technology


Proximity sensor
Ambient Light Sensor
CMOS Imager sensors
GPS sensor
Accelerometer
Humidity sensor
Microphone
Temperature sensor
Pressure sensor
Fingerprint sensor
Magnetometer
Gyroscope
Touch sensor

Sensors…..

- gas sensors
- humidity sensors
- radiation sensors
- smoke sensors
- ultrasonic sensors
- So on….

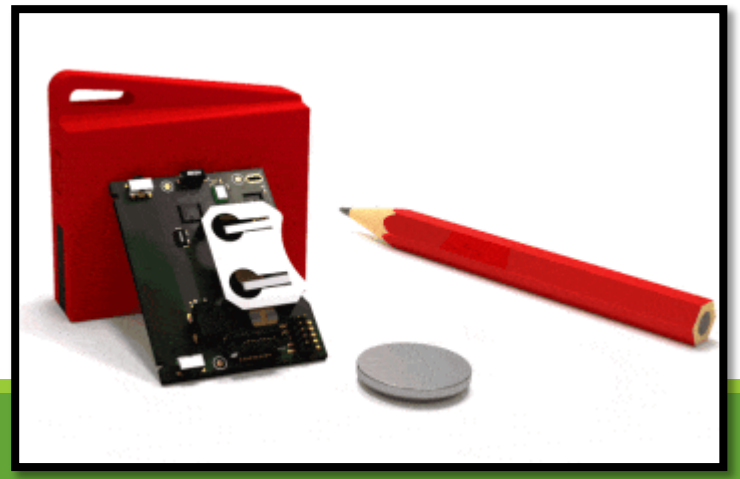
Typical IoT Node



Case Study - Texas Instruments CC2650 SensorTag

Sensor input

- Ambient light sensor (TI Light Sensor OPT3001)
- Infrared temperature sensor (TI Thermopile infrared TMP007)
- Ambient temperature sensor (TI light sensor OPT3001)
- Accelerometer (Invensense MPU-9250)
- Gyroscope (Invensense MPU-9250)
- Magnetometer (Bosch SensorTec BMP280)
- Altimeter/Pressure sensor (Bosch SensorTec BMP280)
- Humidity sensor (TI HDC1000)
- MEMS microphone (Knowles SPH0641LU4H)
- Magnetic sensor (Bosch SensorTec BMP280)
- 2 Push-button GPIOs
- Reed relay (Meder MK24)



Output devices

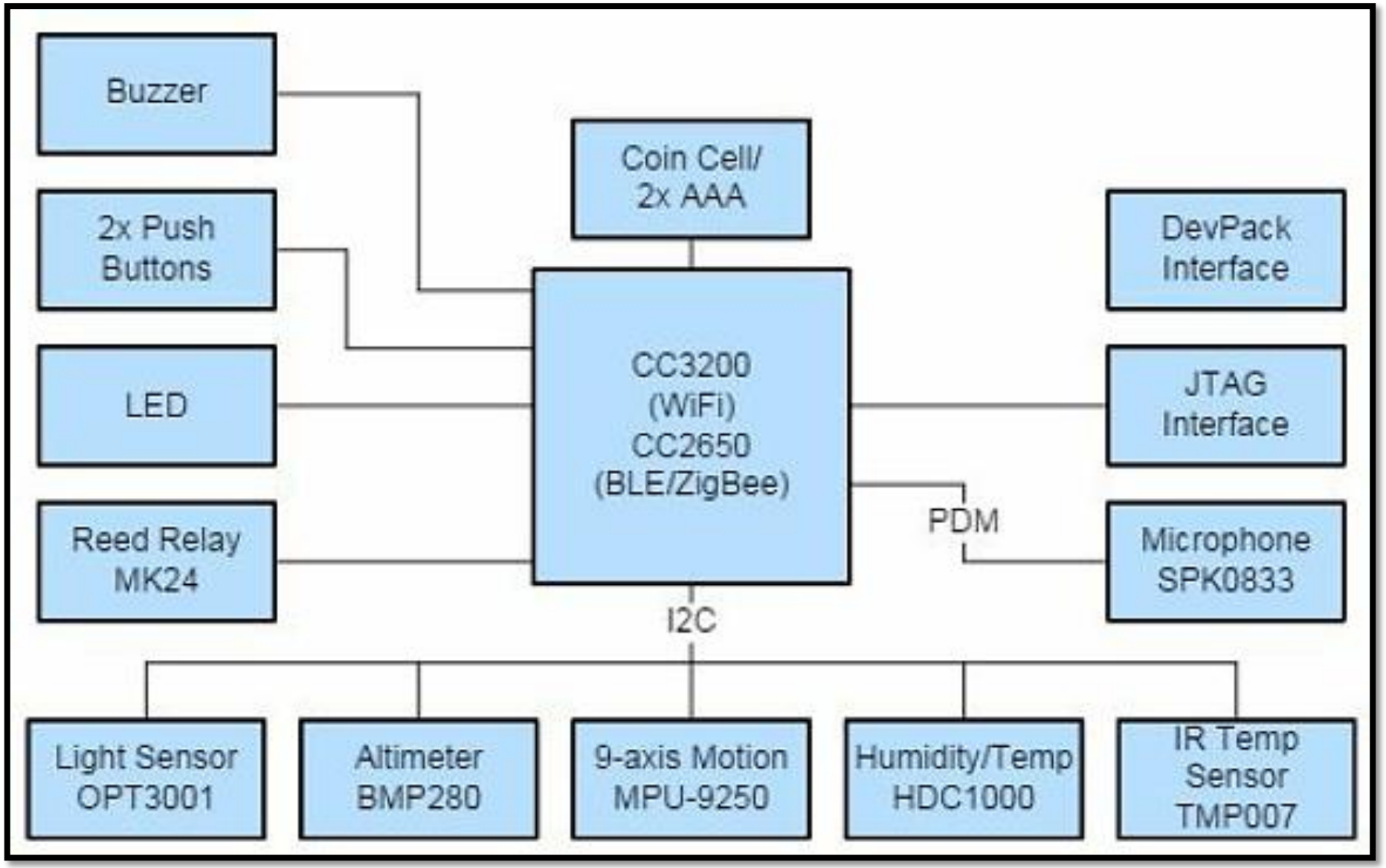
- Buzzer/speaker
- 2 LEDs

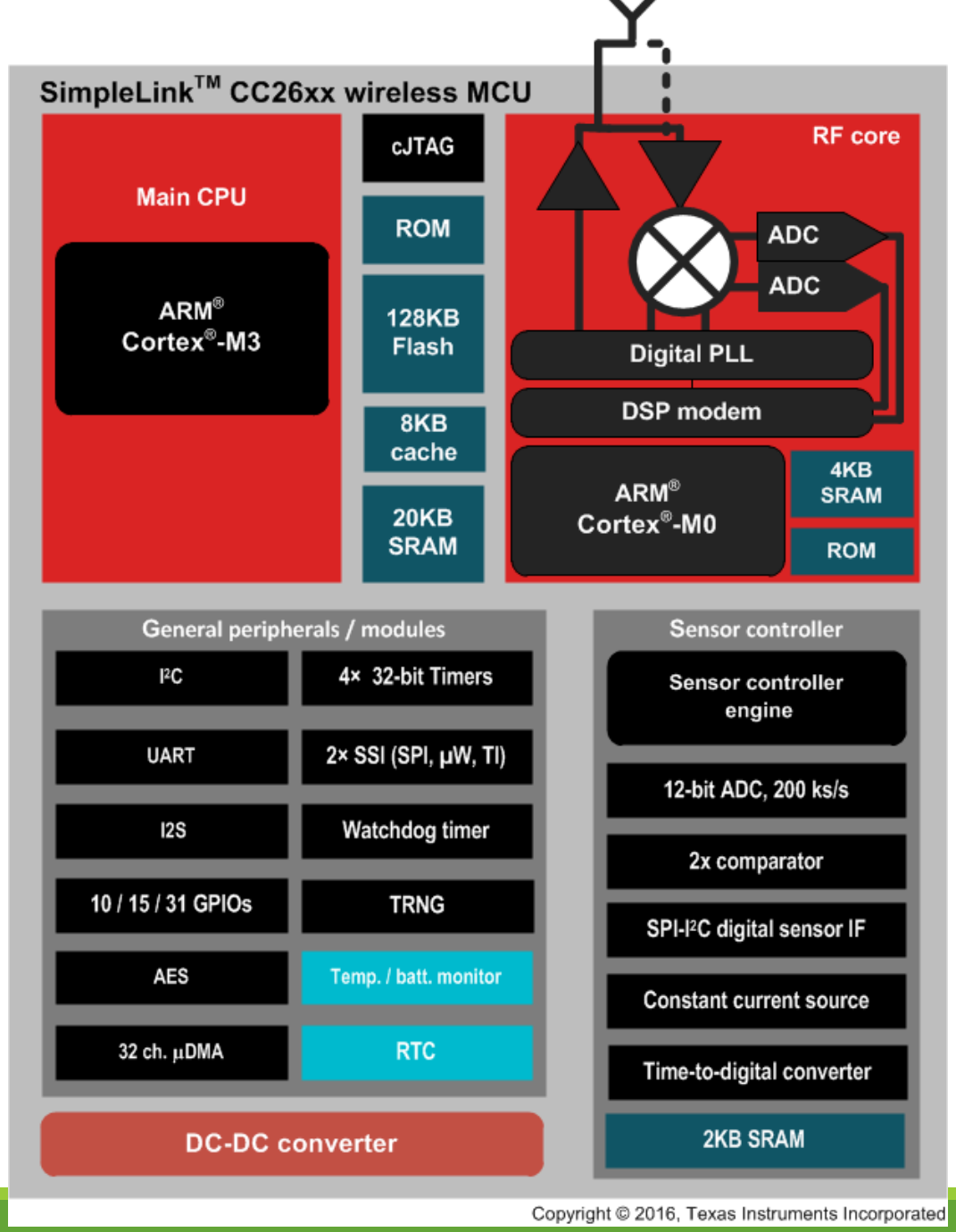
Communications

- Bluetooth Low Energy (Bluetooth Smart)
- Zigbee
- 6LoWPAN

This package is powered by a single CR2032 coin cell battery.

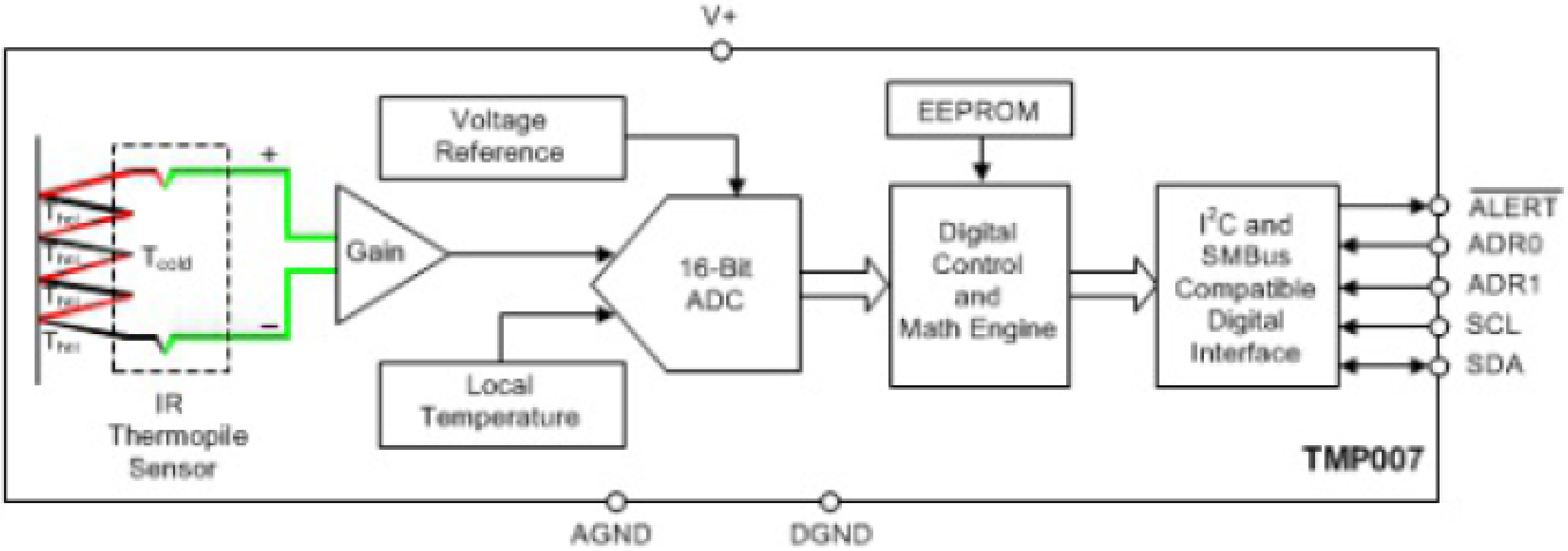
@ INR 3000/-


Buzzer
2x Push Buttons
LED
Reed Relay MK24
Coin Cell/ 2x AAA
CC3200 (WiFi) CC2650 (BLE/ZigBee)
DevPack Interface
JTAG Interface
PDM
Microphone SPK0833
I2C
Light Sensor OPT3001
Altimeter BMP280
9-axis Motion MPU-9250
Humidity/Temp HDC1000
IR Temp Sensor TMP007



Copyright © 2016, Texas Instruments Incorporated

Sensor to Controller



Microcontroller

- Programming flexibility
- Compact construction, small size, low power consumption, and low cost
- Less powerful and less efficient as not optimized for the given task
- Not preferred for large-scale deployments

Digital Signal Processor

- Powerful and complex digital filters can be realized
- Preferred for multimedia WSN applications in which in-network audio and video signal processing is required to compress or aggregate large size data
- Useful for applications that require the deployment of nodes in harsh physical settings where signal transmission may suffer corruption due to noise and interference
- Not suitable for tasks like network management, self-organization, multi-hop communication, topology control etc.
- Not suitable for operations with does not involve numerical operations (like protocols) may require periodical upgrade or modifications

ASIC

- Can be full customized or semi-customised
- Full customized includes features which are not defined by the standard cell library
  - expensive and long design time
- Semi-customized ASICs are built with logic cells that are available in the standard library
- In both cases, the final logic structure is configured by the end user
- Optimized for a specific application
- Difficulties in designing, the lack of re-configurability, and the usually high development costs

Interfaces

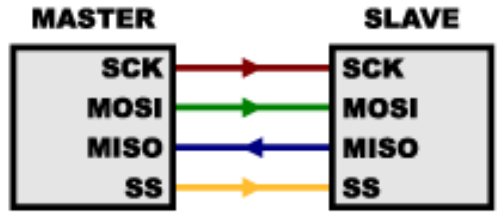
Interfaces

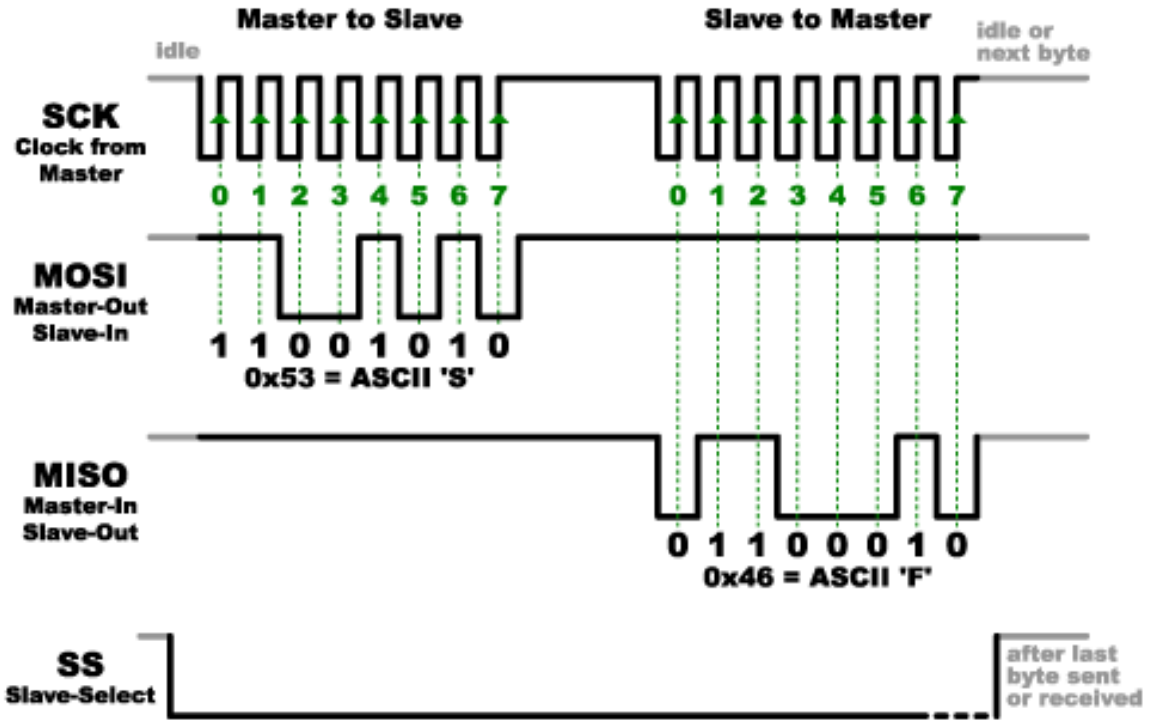
Serial is preferred to parallel interface

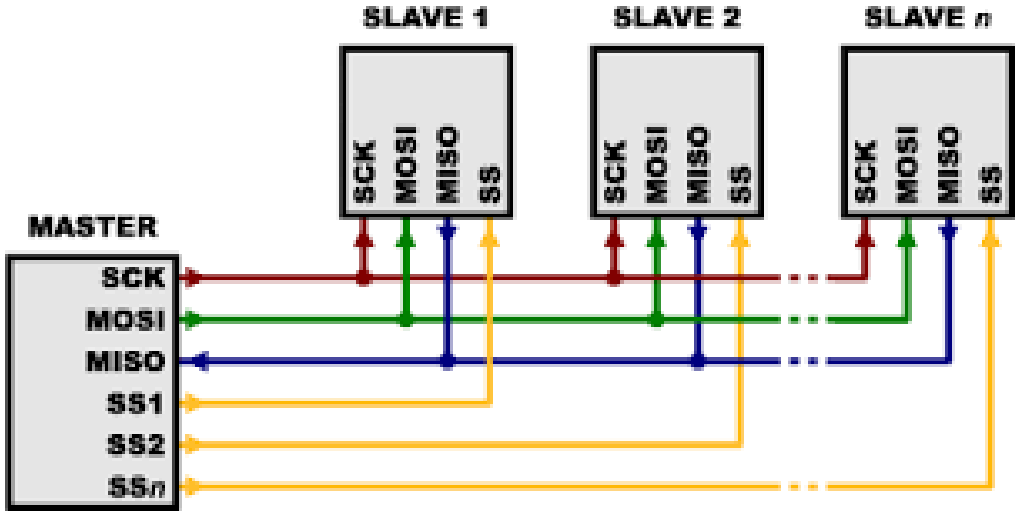
- serial peripheral interface (SPI)
- general purpose input/output (GPIO)
- secure data input/output (SDIO)
- inter-integrated circuit (I^2C)
- Universal Serial Bus (USB)

Among these, the most commonly used buses are the SPI and the I^2C

Serial Peripheral Interface







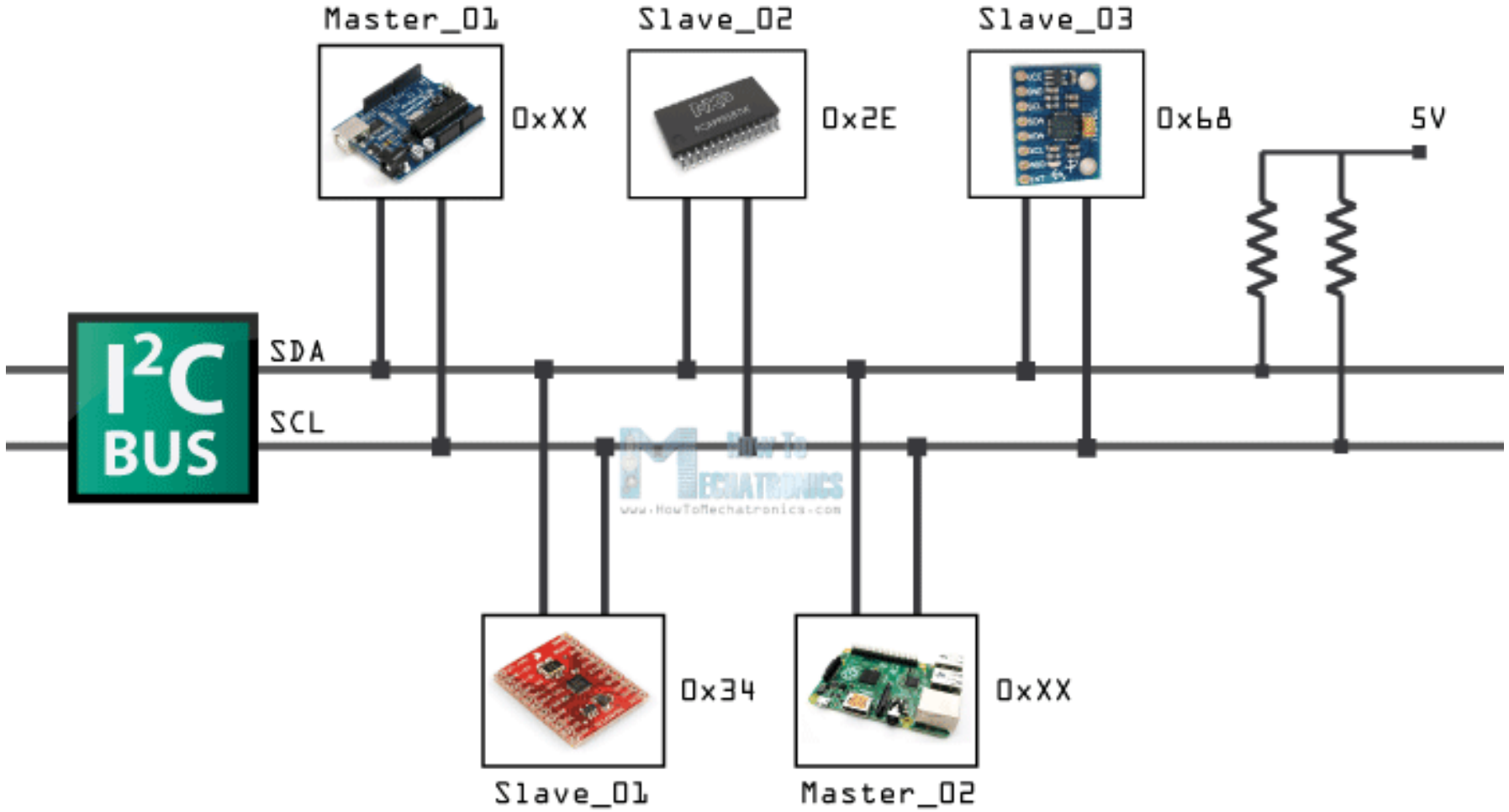
Advantage – Disadvantage

Advantages of SPI:

- It is faster than asynchronous serial
- The receive hardware can be a simple shift register
- It supports multiple slaves

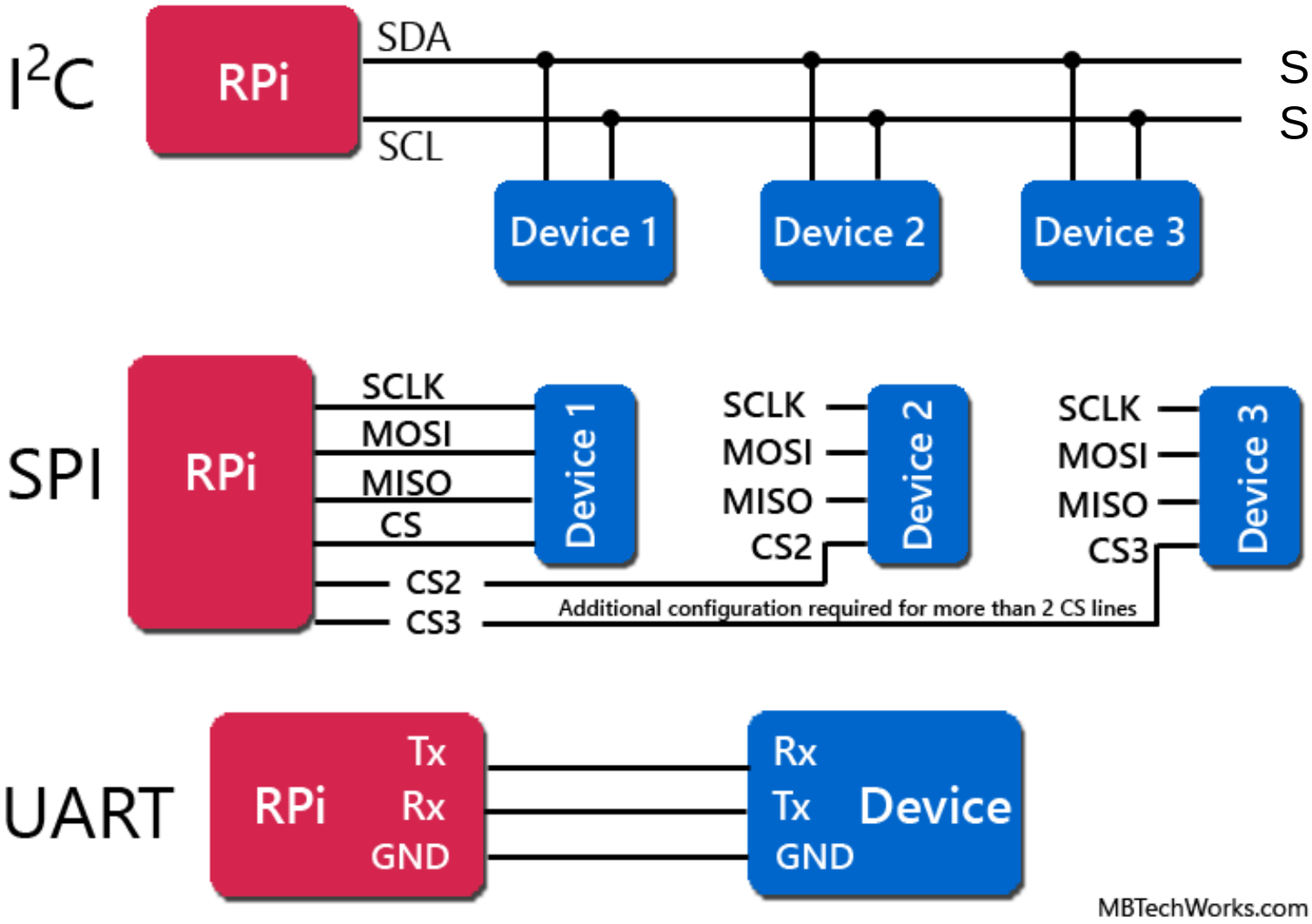
Disadvantages of SPI:

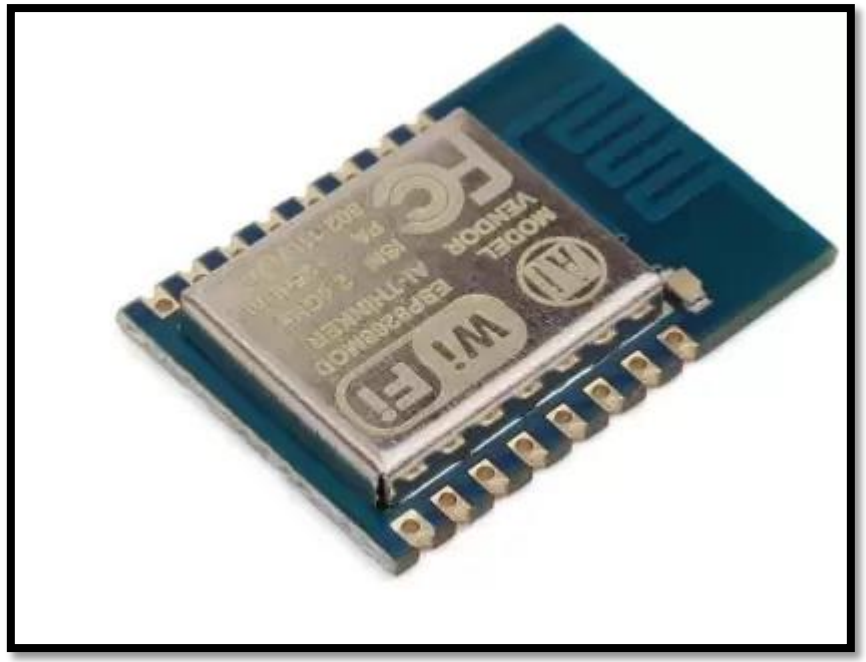
- It requires more signal lines (wires) than other communications methods
- The communications must be well-defined in advance
- The master must control all communications (slaves can't talk directly to each other)
- It usually requires separate SS lines to each slave, which can be problematic if numerous slaves are needed.

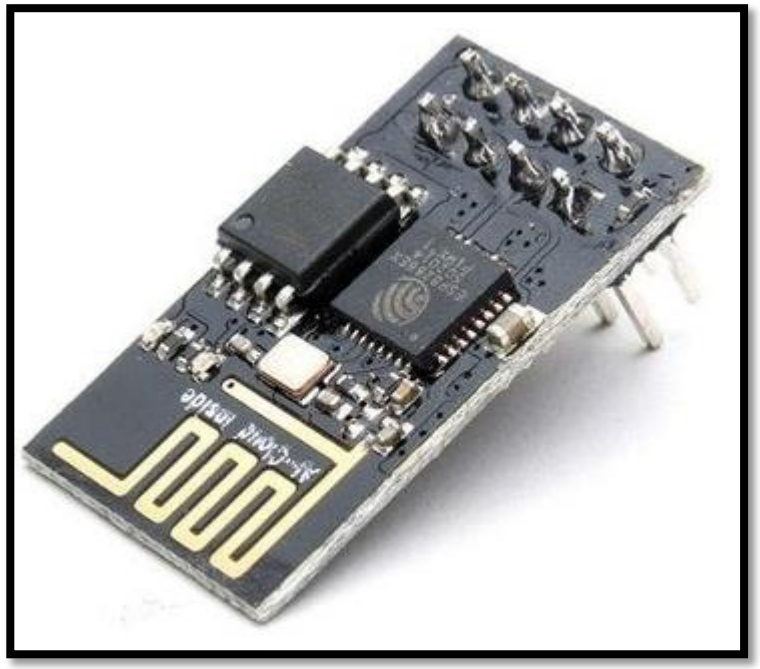


SDA- Serial Data
SCL – Serial Clock

SPI, I²C & UART interface







Transceiver

Transmission medium

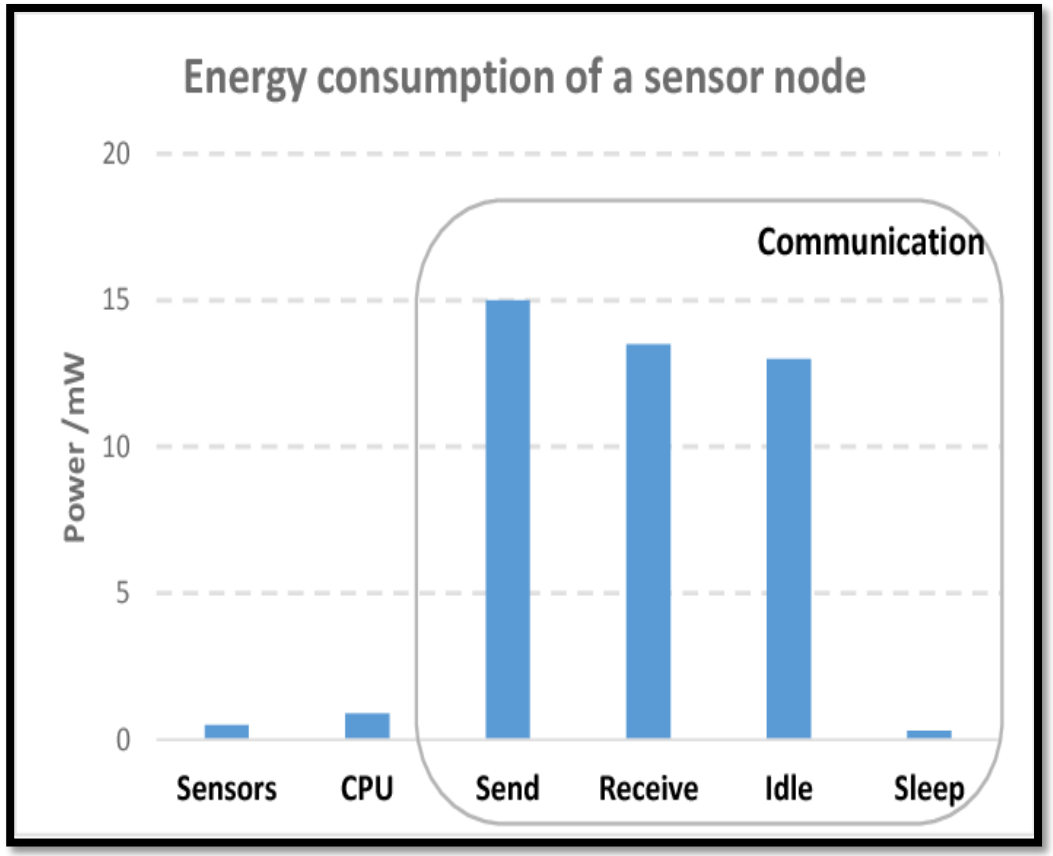
- Radio frequencies (RF/MW)
  - Long range
  - High data rates
  - Acceptable error rates at reasonable energy expenditure
  - Does not require line of sight between sender and receiver
  - Example: 433 MHz and 2.4 GHz, 5GHz
- Light
- Sonar/ Sound

Transceiver characteristics

- Data rate – few tens of kilo bits is sufficient (typically)
- Modulation technique – on-off keying (ASK) or FSK
- Coding scheme – trade off between energy and performance
- Transmission power control – usually discrete, max is regulated
- Noise figure, gain, power efficiency
- Receiver sensitivity (dBm) – better sensitivity-more range
- Range – decided by standard and depends on application
- Out of band emission – must be controlled
- Carrier sense and Radio Signal Strength Indicator (RSSI)

Tradeoff active-sleep mode

- ***Idle*** – ready to receive, but not doing so
- Some functions in hardware can be switched off, reducing energy consumption a little
- ***Sleep*** – significant parts of the transceiver are switched off
- Not able to immediately receive something
- ***Recovery time*** and ***startup energy*** to leave sleep state can be significant



TRADE-OFF - State change times and energy saving

Case Study - Radio Transceivers

RFM TR1000 family

- 916 or 868 MHz
- 400 kHz bandwidth
- Up to 115,2 kbps
- On/off keying or ASK
- Dynamically tuneable output power
- Maximum power about 1.4 mW
- Low power consumption

Chipcon CC1000

- Range 300 to 1000 MHz, programmable in 250 Hz steps
- FSK modulation
- Provides RSSI

Chipcon CC 2400

- Implements 802.15.4 (low data rate PAN)
- 2.4 GHz, DSSS modem
- 250 kbps
- Higher power consumption than above transceivers

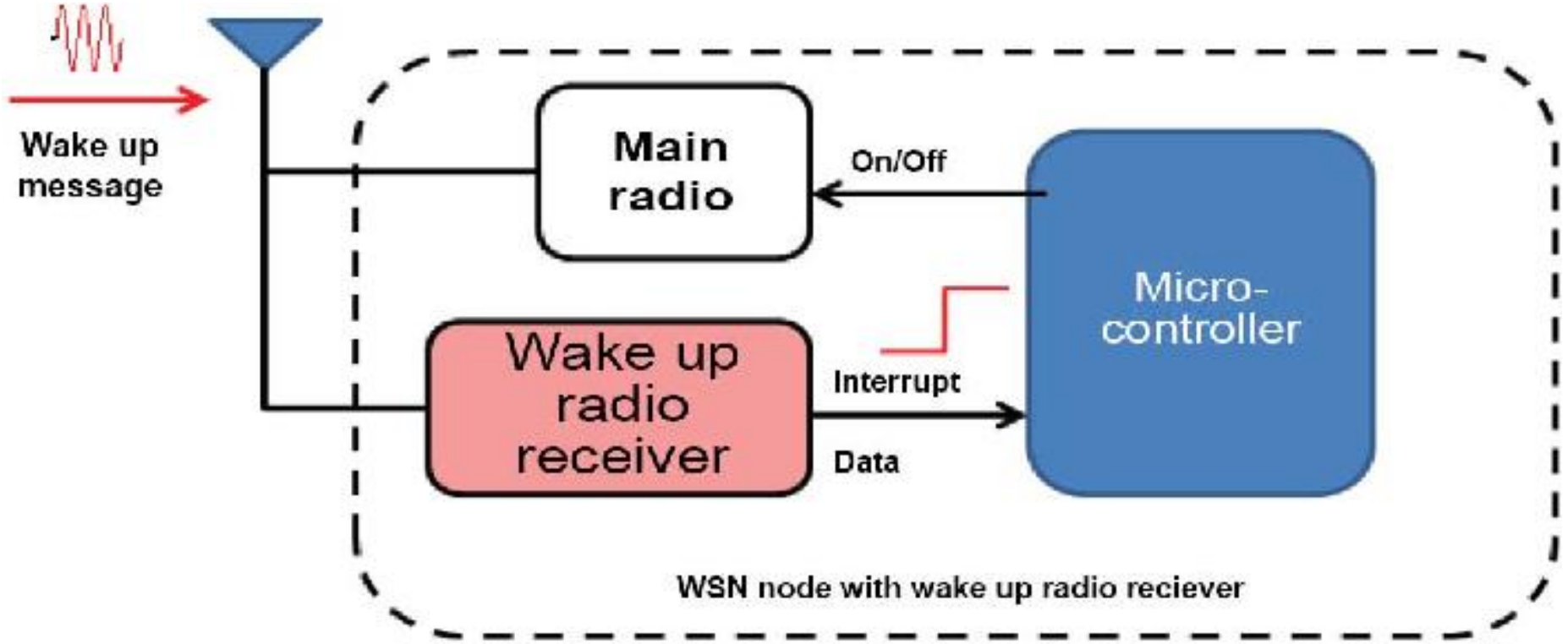
Infineon TDA 525x family

- E.g., 5250: 868 MHz
- ASK or FSK modulation
- RSSI, highly efficient power amplifier
- Intelligent power down
- Excellent blocking performance

Advance design concepts

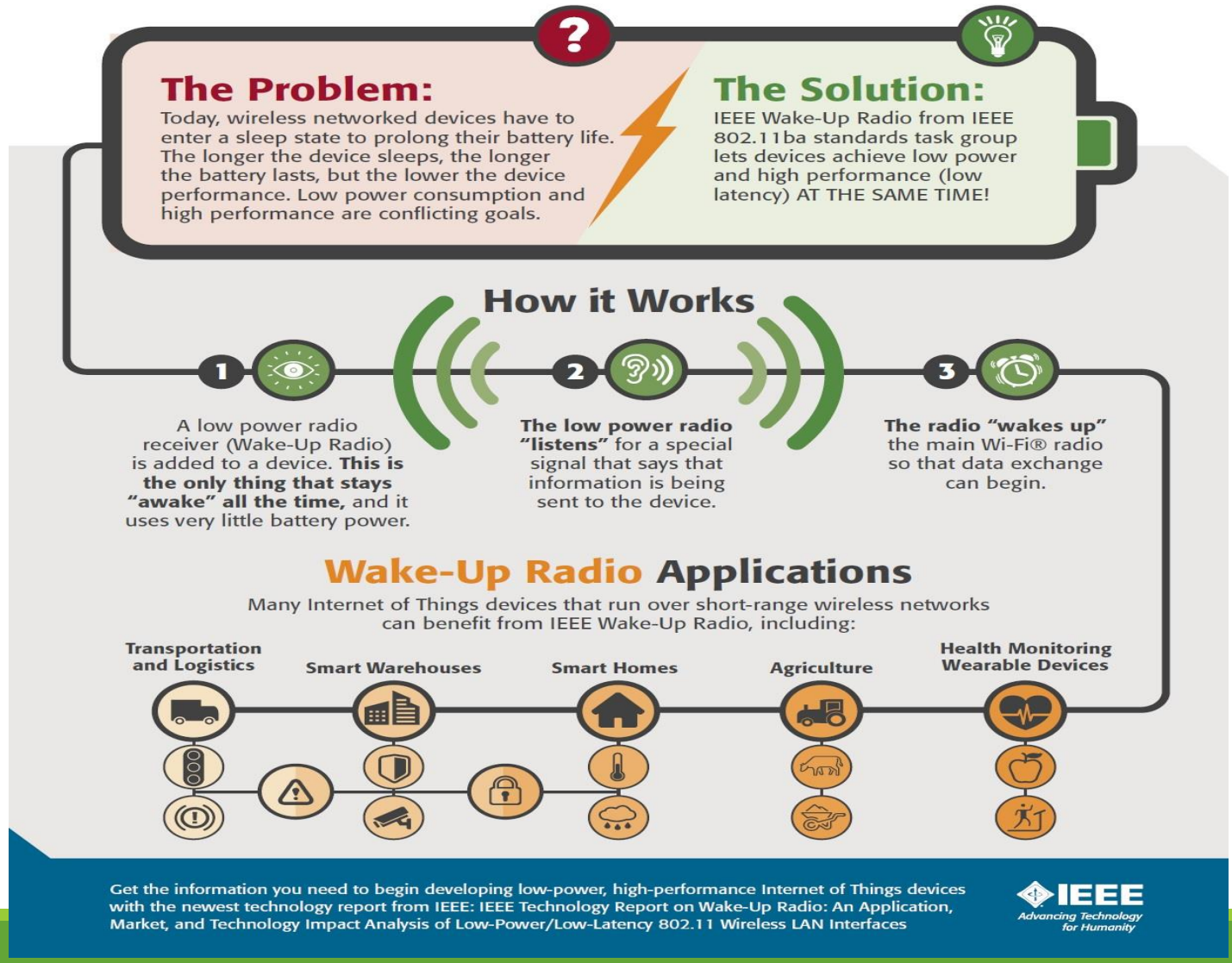
- Wake up receivers
- Spread-spectrum transceivers
- Ultra wide band communication
- Non – radio frequency based transmission
  - Optical
  - Ultrasound

Wake up receivers

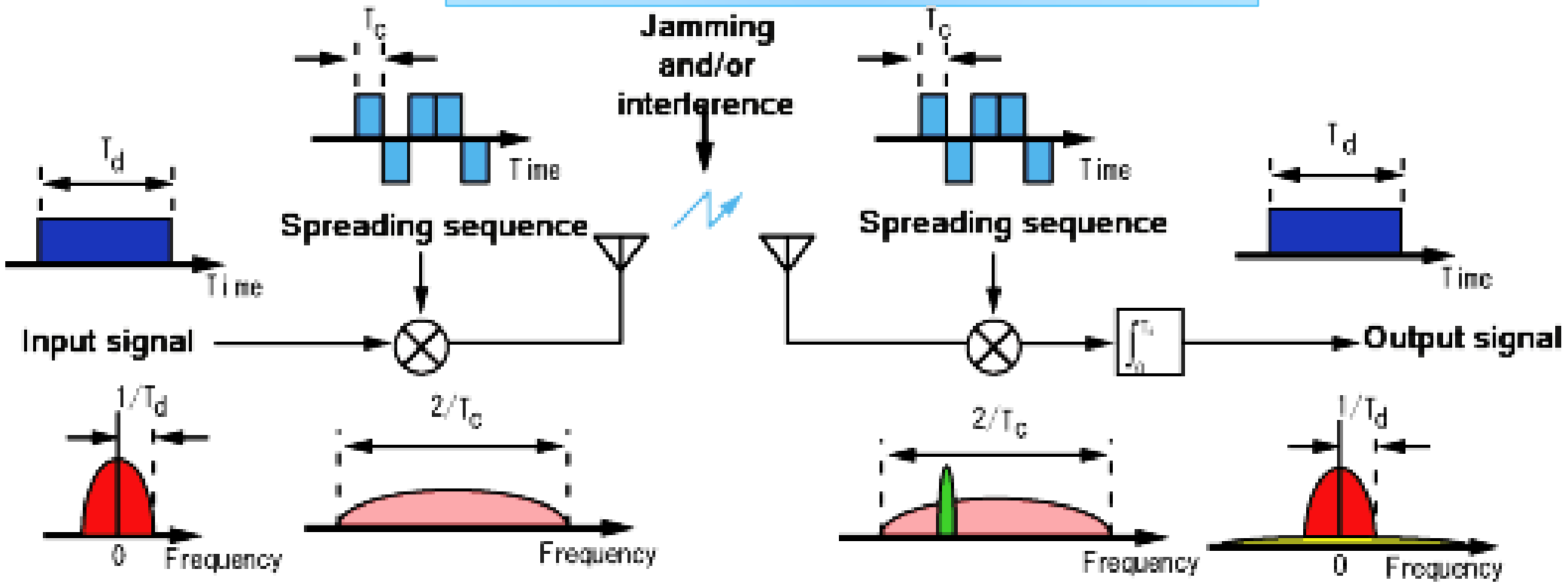


IEEE Wake-Up Radio

Prolong the battery life of Internet of Things devices with this low-power, high-performance solution.



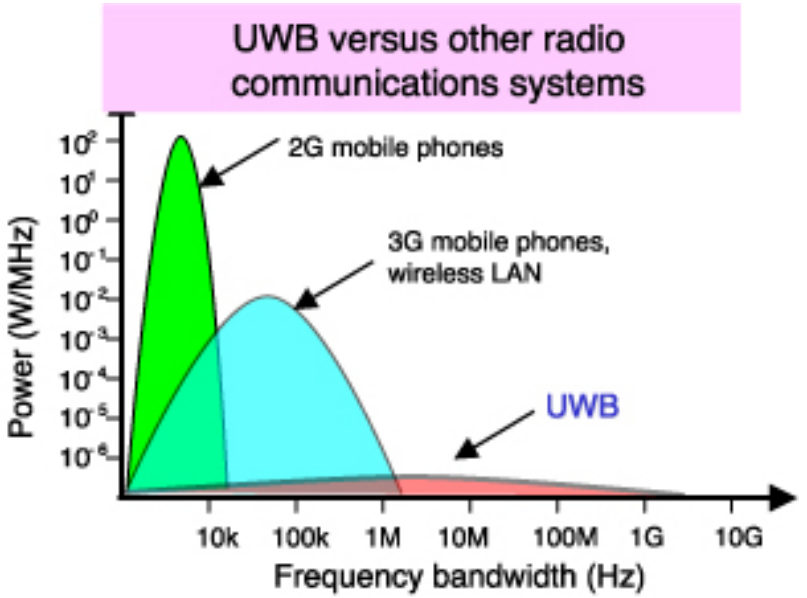
Spread-spectrum transceivers

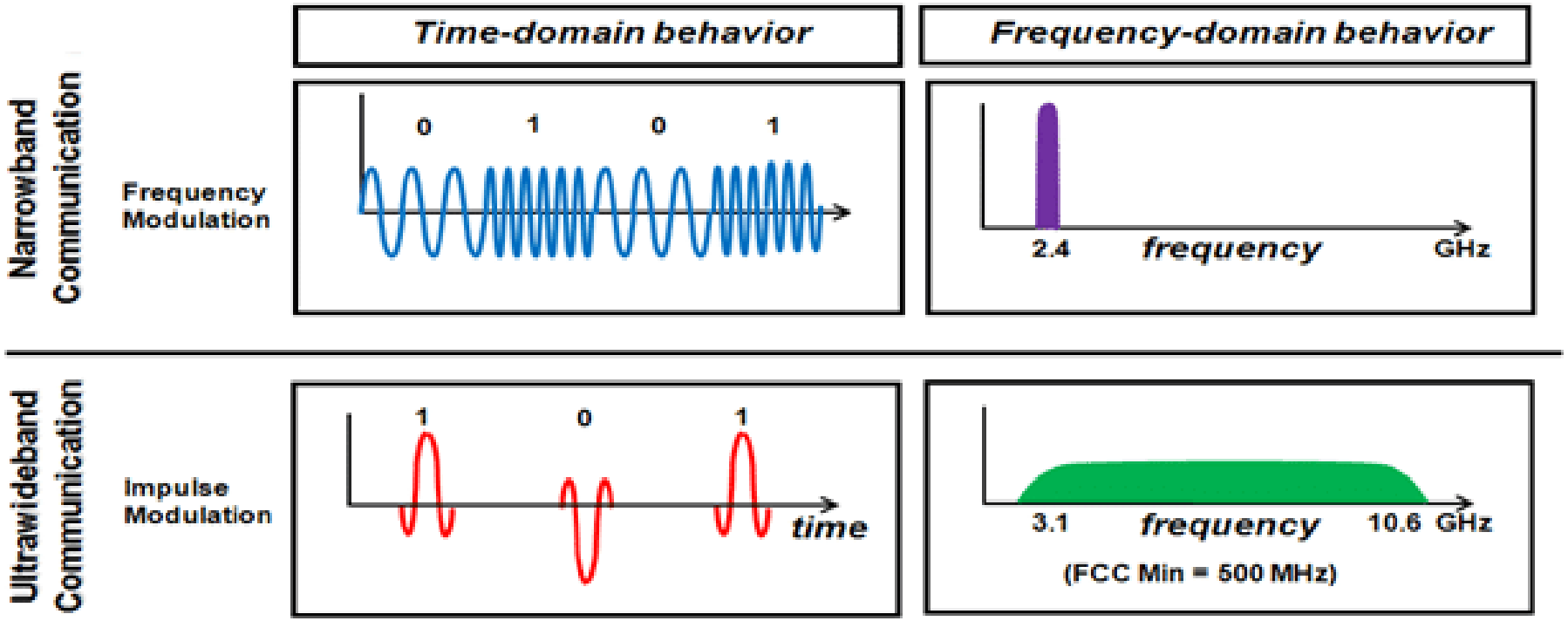


- Cross-talk elimination
- Better output with data integrity
- Reduced effect of multipath fading
- Better security
- Reduction in noise

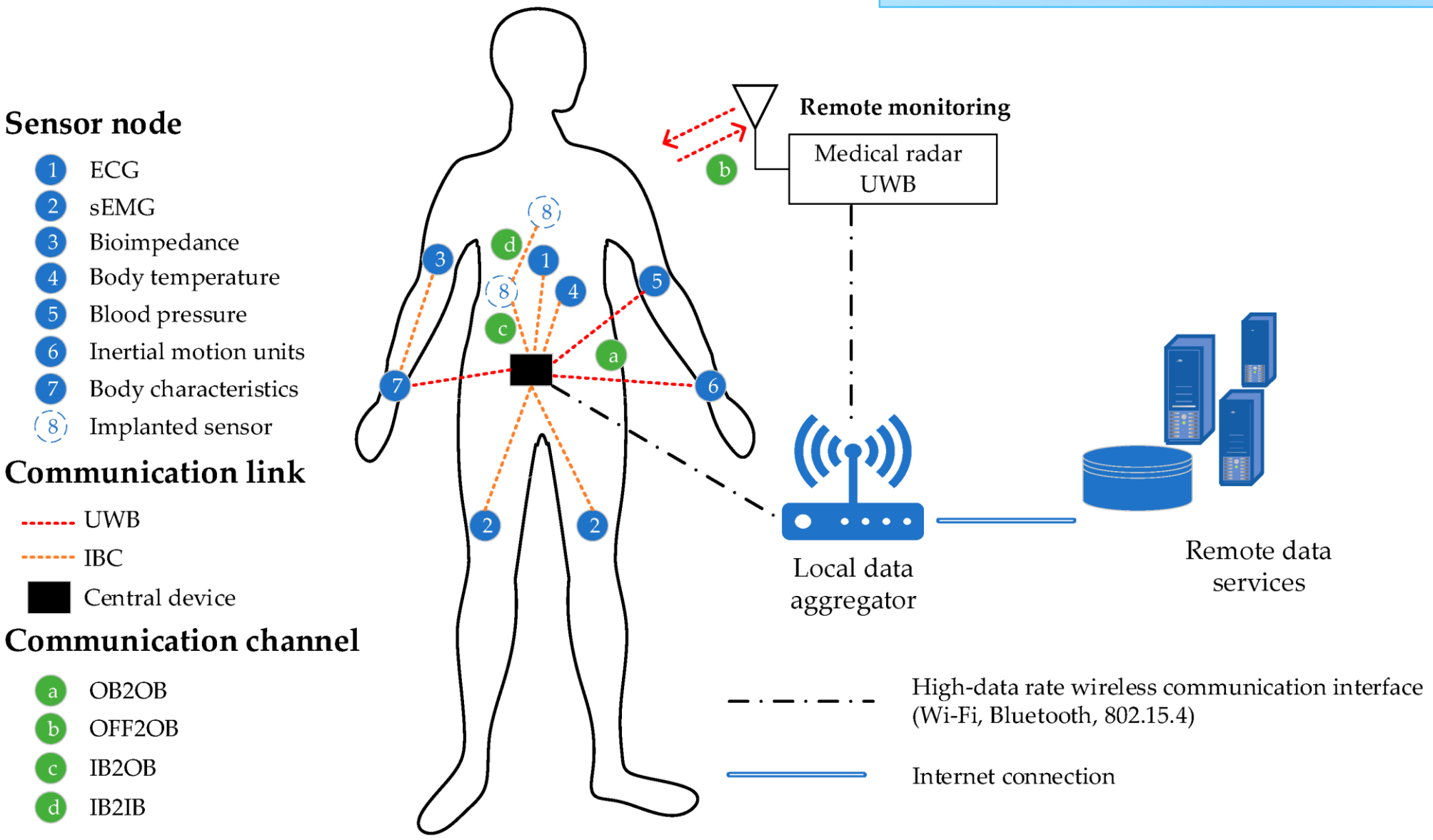
- Co-existence with other systems
- Longer operative distances
- Hard to detect
- Not easy to demodulate/decode
- Difficult to jam the signals

Ultra wide band Communication



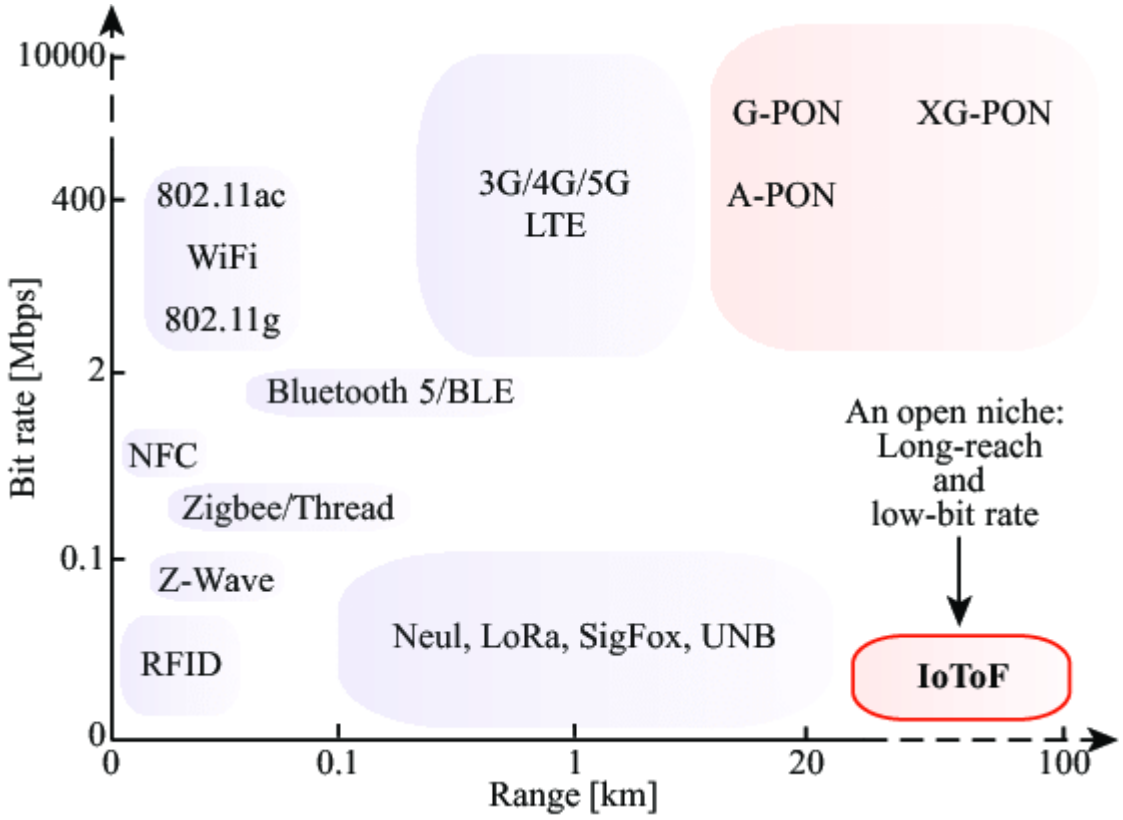


Ultra wide band Communication

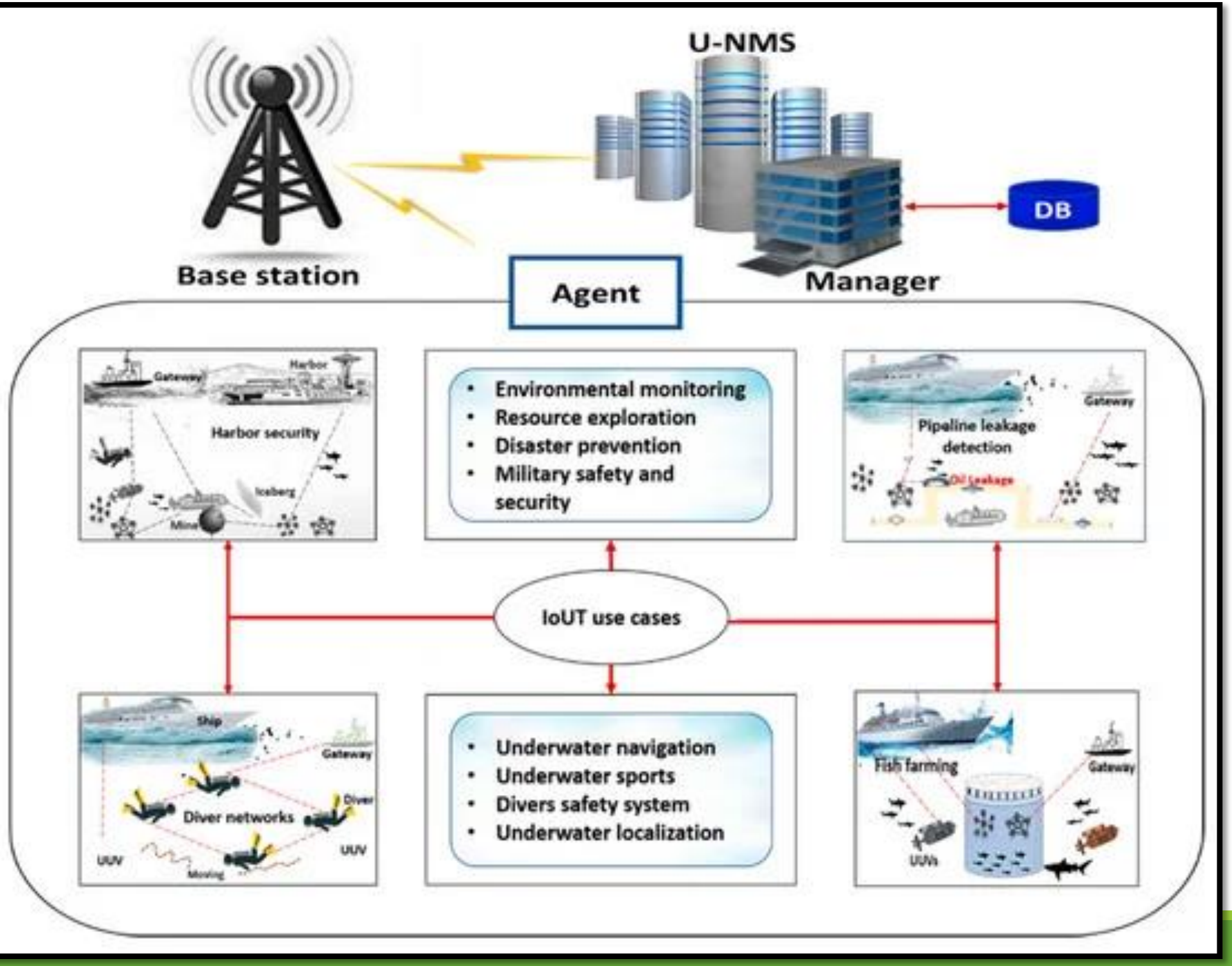


https://www.mdpi.com/1424-8220/20/12/3587/htm

IoT over fibre Optic



IoT over Sonar



Power Consumption and Data Rates for Various Wireless Technology for IoT

	100 bps		10K bps		40K bps	
1 m	BLE4 / Zigbee	0.15	BLE4 / Zigbee	7.5	Zigbee	30
	BLE Mesh	0.15	BLE Mesh	7.5	Bluetooth	25
	Bluetooth	25	Bluetooth	25	WiFi	50
	WiFi	50	WiFi	50	LoRA	20
	LoRA	0.5	LoRA	10		
50 m	Zigbee	20	Zigbee	30	WiFi	200
	WiFi	100	WiFi	100	NB-IoT, LTE-M	200
	LoRA	0.5	LoRA	20	LTE, 5G Cellular	200
	NB-IoT, LTE-M	1.0	LTE, 5G Cellular	150		
1 km	LoRa	30	NB-IoT, LTE-M	100	NB-IoT, LTE-M	400
	Sigfox	30	LTE, 5G Cellular	200	LTE, 5G Cellular	400
	NB-IoT, LTE-M	20				
	LTE, 5G Cellular	120				

All units in mW

https://www.embedded.com/making-energy-harvesting-work-for-edge-iot-devices/

Energy Sources & Power Managment

Need of Power

- Active sensor power
- Frequency and amount of data collection
- Wireless radio communication strength and power
- Microprocessor or microcontroller power
- Passive component power
- Energy loss from leakage or power supply inefficiency
- Power reserve for actuators and motor

Challenges

- Number of sensors and end devices in the billions
- Used in very remote areas
- Harsh environment, mobility
- Power usage pattern
- Sensors are buried undersea, or embedded into concrete infrastructures etc..

Power Management methods

- Reducing the clock rates of processors or microcontrollers
- Adjusting the sensing frequency and broadcast frequency
- Back-off strategies to reduce communication strength
- Various levels of sleep modes

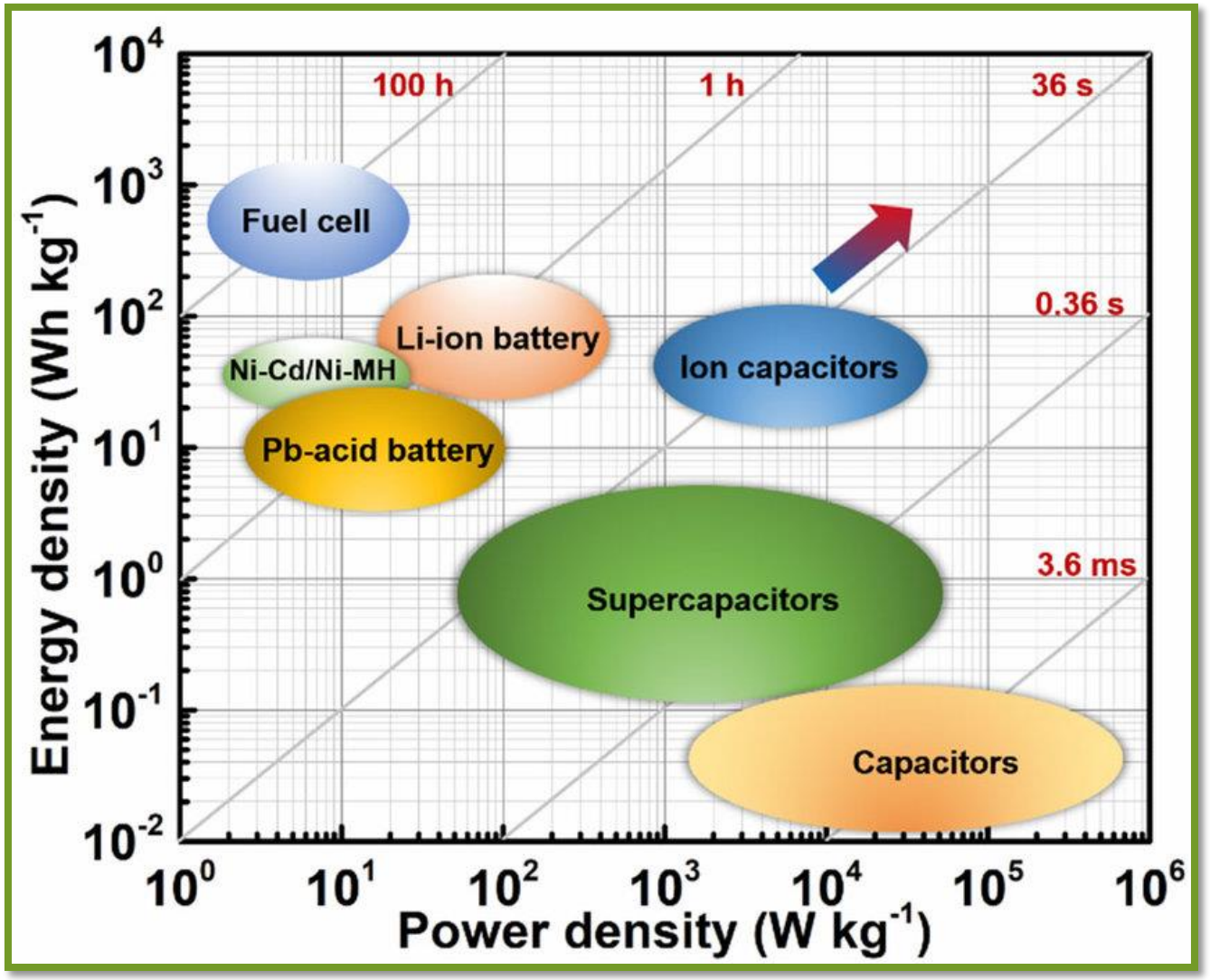
$(P = CV^2 f)$

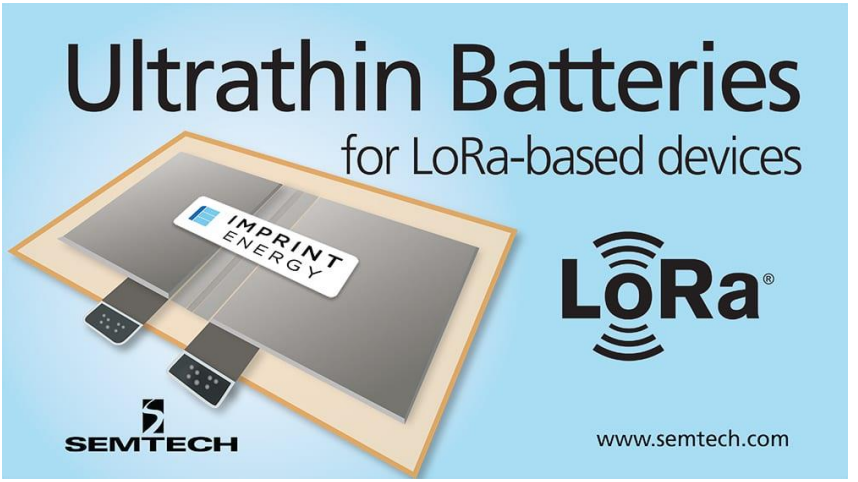
New methods:

- Approximate computing
- Probabilistic design

Energy density is the amount of energy that can be stored in a given mass of a substance or system

Power density is a measure of power output per unit volume.

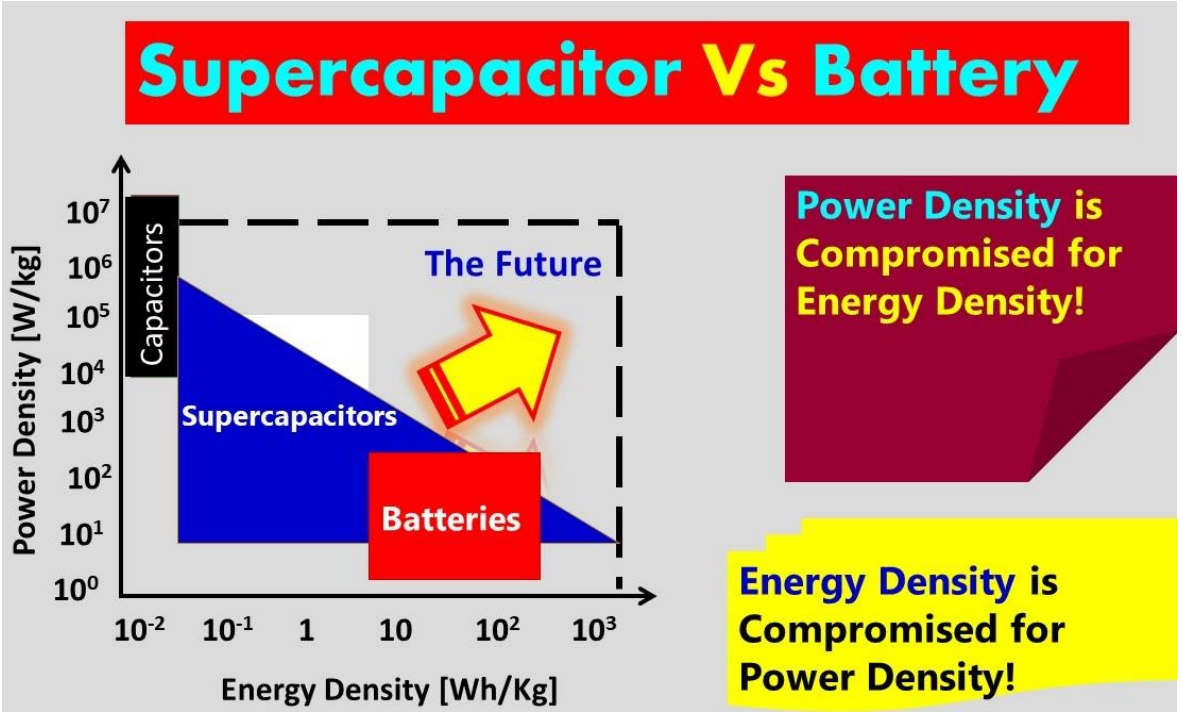




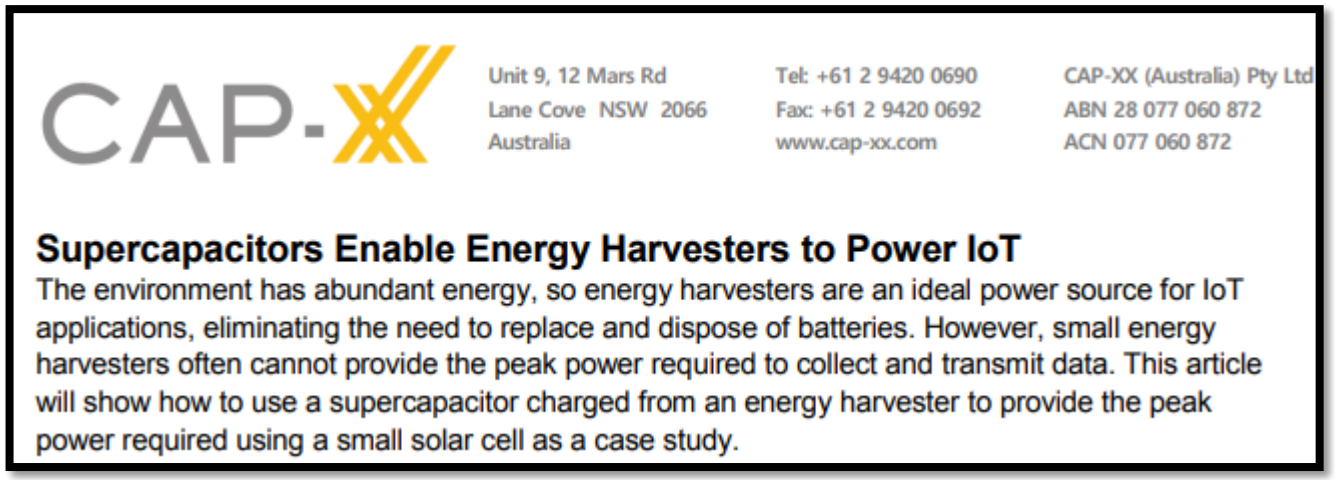
Super capacitors

Flexible Battery

	Battery	Supercapacitor
Recharge Cycle Life Time	$< 10^3$ cycles	$> 10^6$ cycles
Self-discharge Rate	5%	30%
Voltage	3.7V-4.2V	0V-2.7V
Energy Density (Wh/kg)	high (20-150)	low (0.8-10)
Power Density (W/kg)	low (50-300)	high (500-400)
Fastest charging time	hours	sec ~ min
Fastest discharging time	0.3~3 hours	< a few min
Charging Circuit	complex	simple

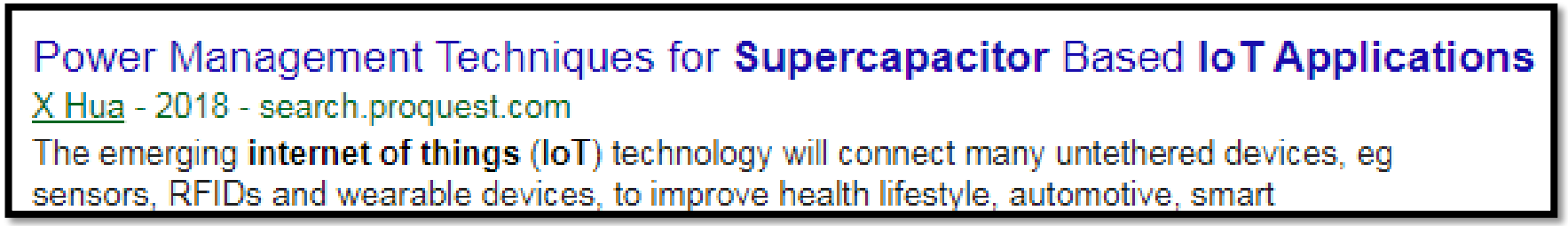


Wearable devices
Health monitoring patches
Smart watches


CAP-XX
Unit 9, 12 Mars Rd
Lane Cove NSW 2066
Australia
Tel: +61 2 9420 0690
Fax: +61 2 9420 0692
www.cap-xx.com
CAP-XX (Australia) Pty Ltd
ABN 28 077 060 872
ACN 077 060 872
Supercapacitors Enable Energy Harvesters to Power IoT
The environment has abundant energy, so energy harvesters are an ideal power source for IoT applications, eliminating the need to replace and dispose of batteries. However, small energy harvesters often cannot provide the peak power required to collect and transmit data. This article will show how to use a supercapacitor charged from an energy harvester to provide the peak power required using a small solar cell as a case study.


Mar 5 - Written By Joe Sleppy
Flexible Supercapacitors for Energy Harvesting Technologies in IoT

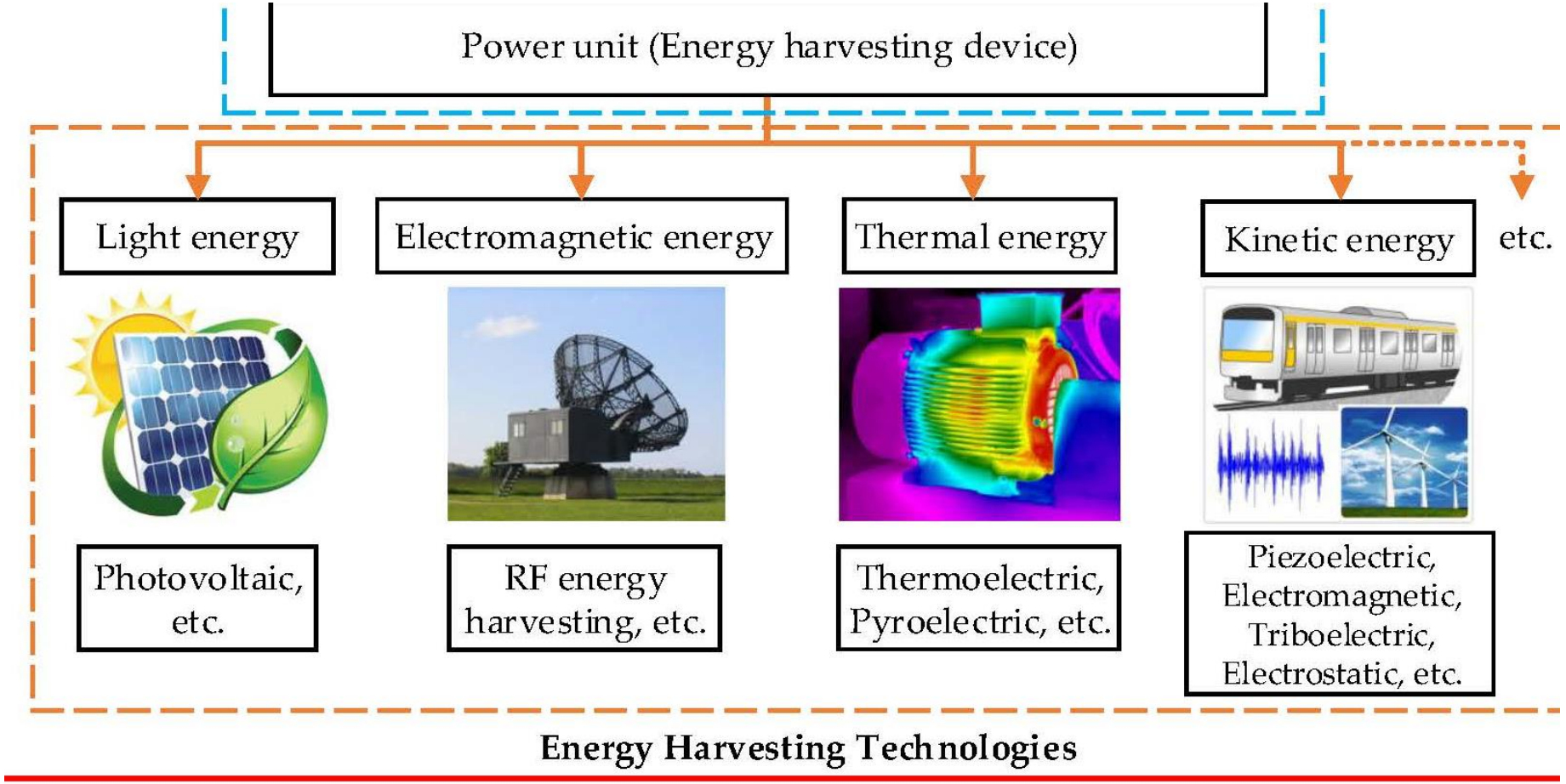

Challenges and prospects of 3D micro-supercapacitors for powering the internet of things
C Lethien, J Le Bideau, T Brousse - Energy & Environmental Science, 2019 - pubs.rsc.org

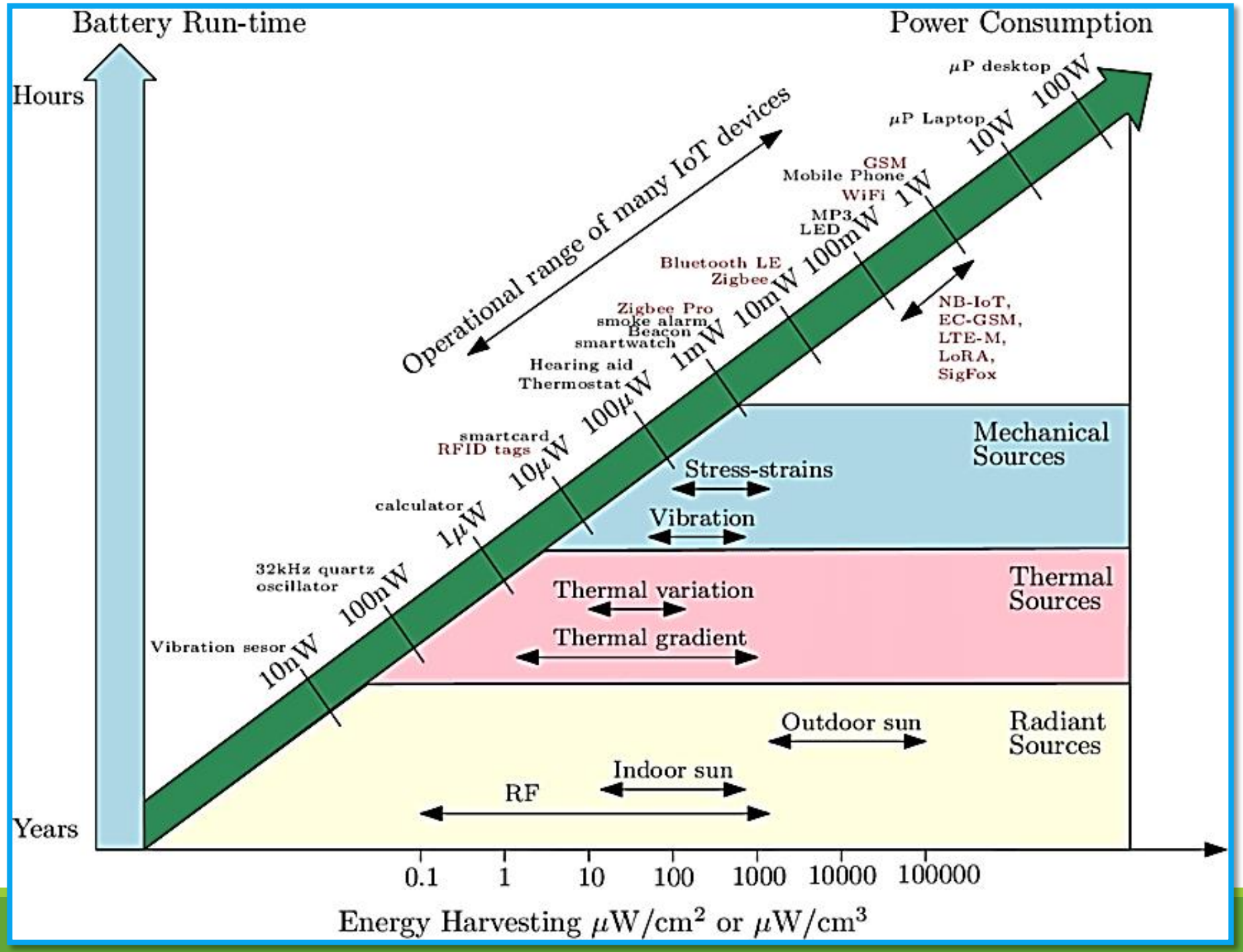

Power Management Techniques for Supercapacitor Based IoT Applications
X Hua - 2018 - search.proquest.com
The emerging internet of things (IoT) technology will connect many untethered devices, eg sensors, RFIDs and wearable devices, to improve health lifestyle, automotive, smart

Energy Harvesting

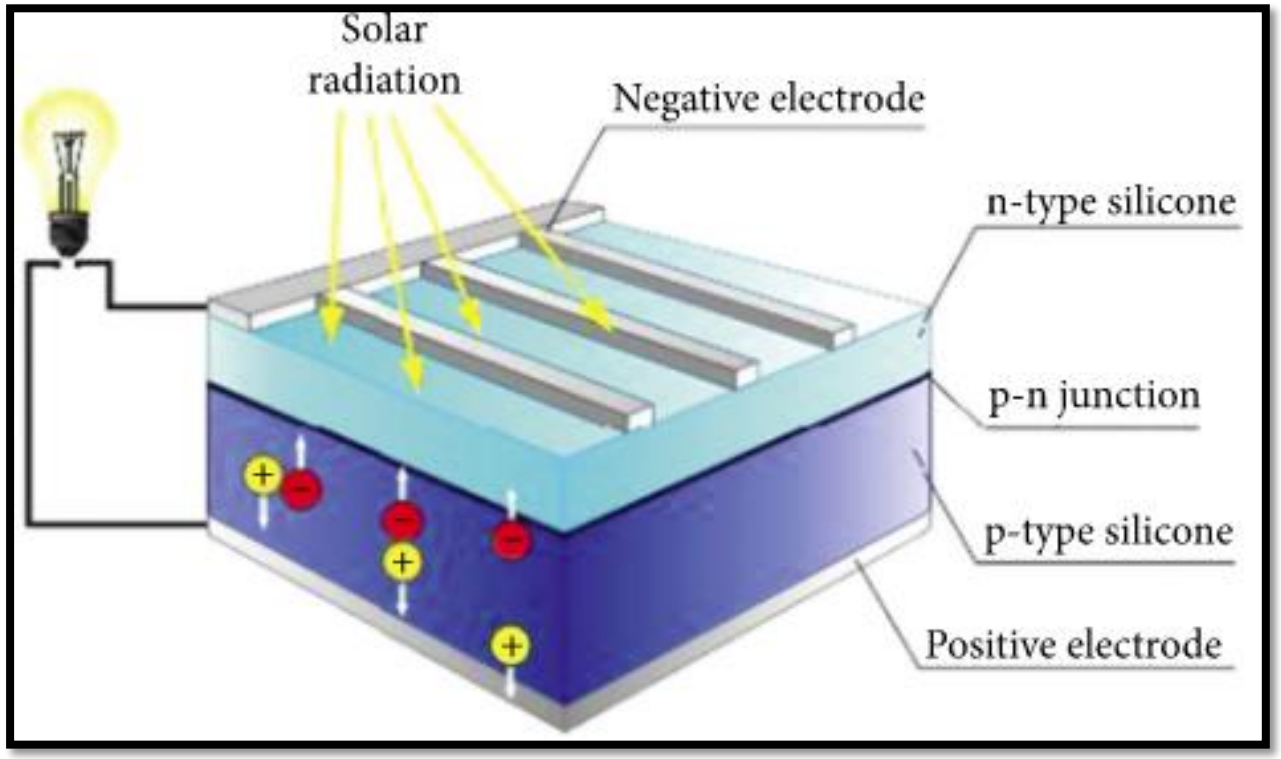
Energy harvesting

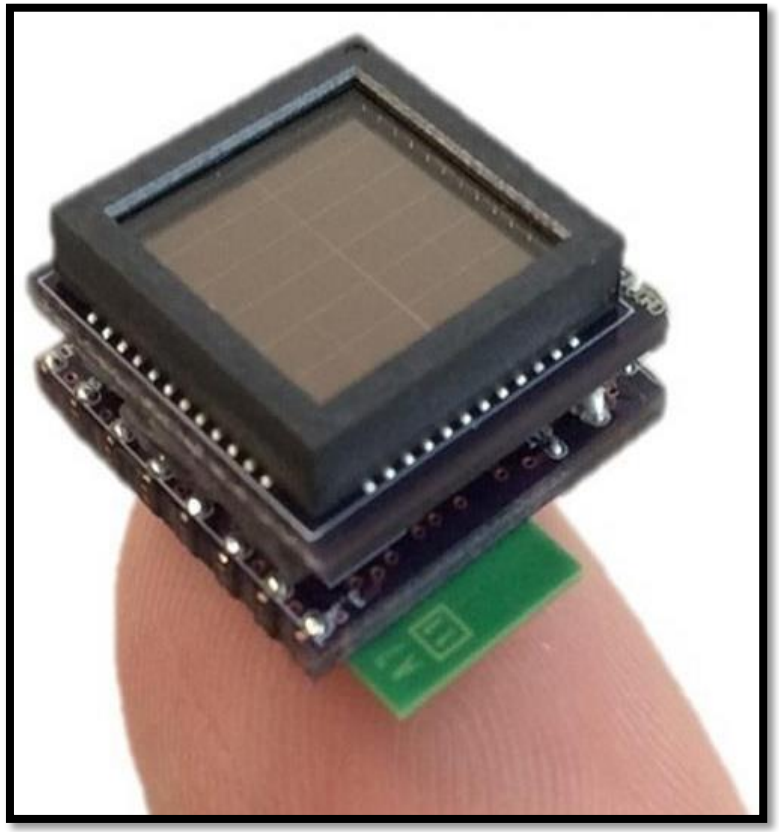
Harvesting systems have a low energy potential and low conversion efficiency




Battery Run-time
Power Consumption
Hours
Years
Operational range of many IoT devices
μP desktop
100W
μP Laptop
10W
GSM
Mobile Phone
WiFi
1W
MP3
LED
100mW
Bluetooth LE
Zigbee
10mW
Zigbee Pro
smoke alarm
Beacon
smartwatch
1mW
Hearing aid
Thermostat
100μW
smartcard
RFID tags
10μW
calculator
1μW
32kHz quartz
oscillator
100nW
Vibration sesor
10nW
NB-IoT,
EC-GSM,
LTE-M,
LoRA,
SigFox
Mechanical
Sources
Stress-strains
Vibration
Thermal
Sources
Thermal variation
Thermal gradient
Radiant
Sources
Outdoor sun
Indoor sun
RF
0.1
1
10
100
1000
10000
100000
Energy Harvesting μW/cm² or μW/cm³

Solar Harvesting

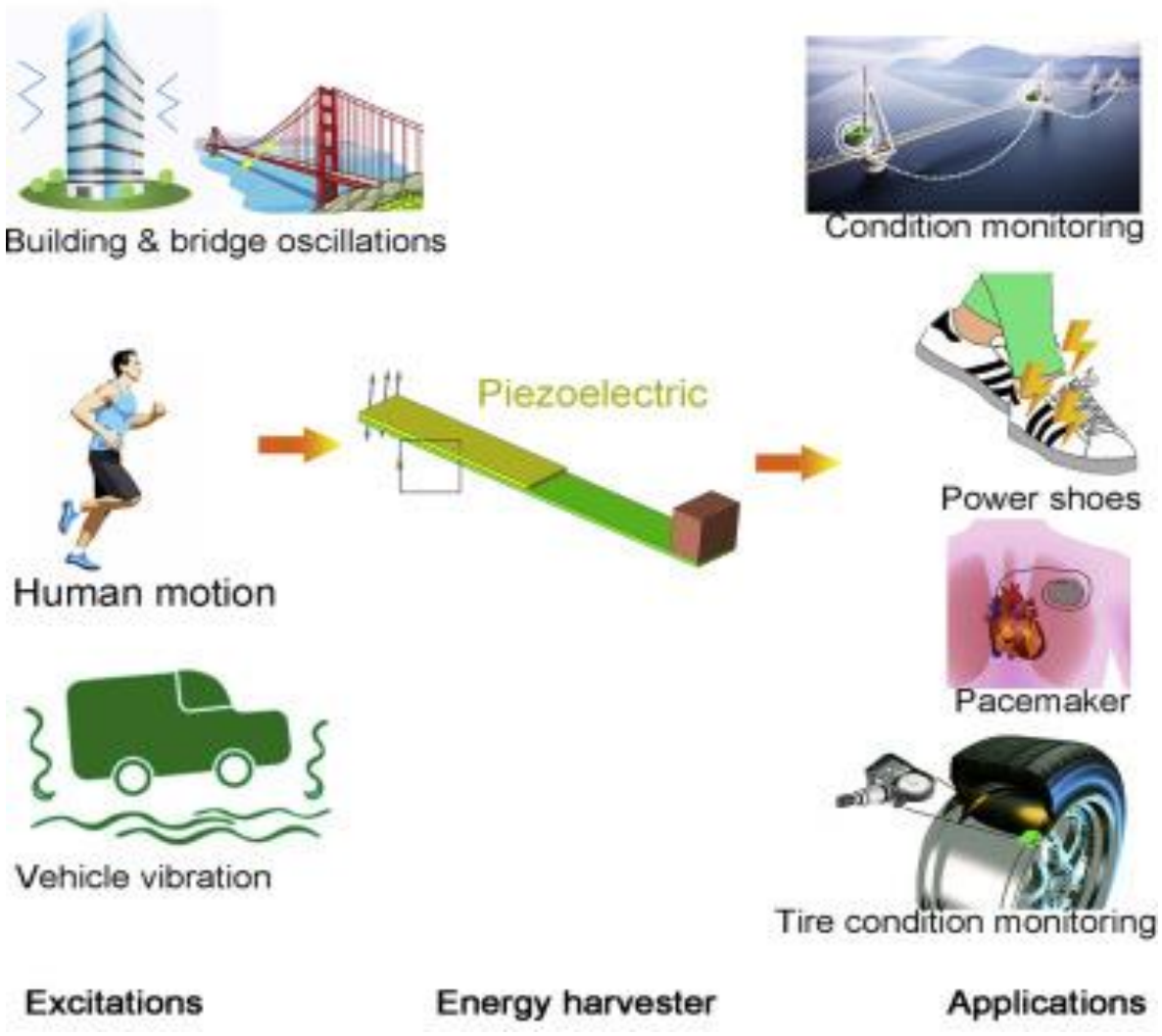


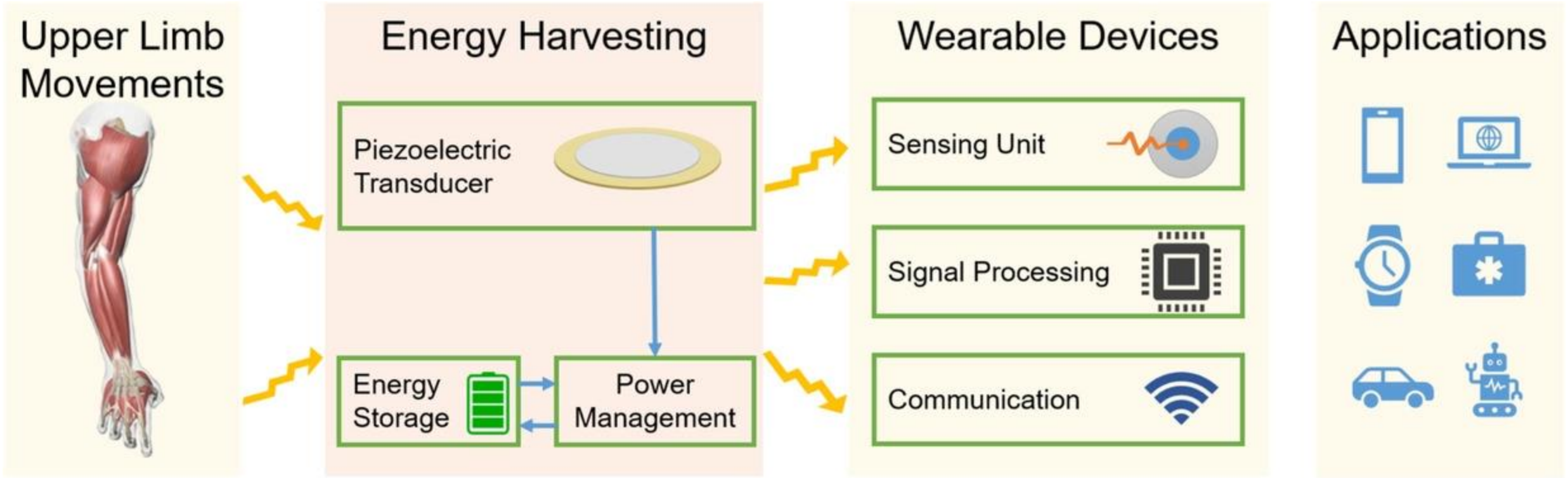


Piezo-mechanical Harvesting

Mechanical strains can be converted to energy through motion, vibration, and even sound.

These harvesters could be used in smart roadways and infrastructures to harvest and change systems based on traffic movement, even when embedded in concrete.




Upper Limb Movements
Energy Harvesting
Piezoelectric Transducer
Energy Storage
Power Management
Wearable Devices
Sensing Unit
Signal Processing
Communication
Applications

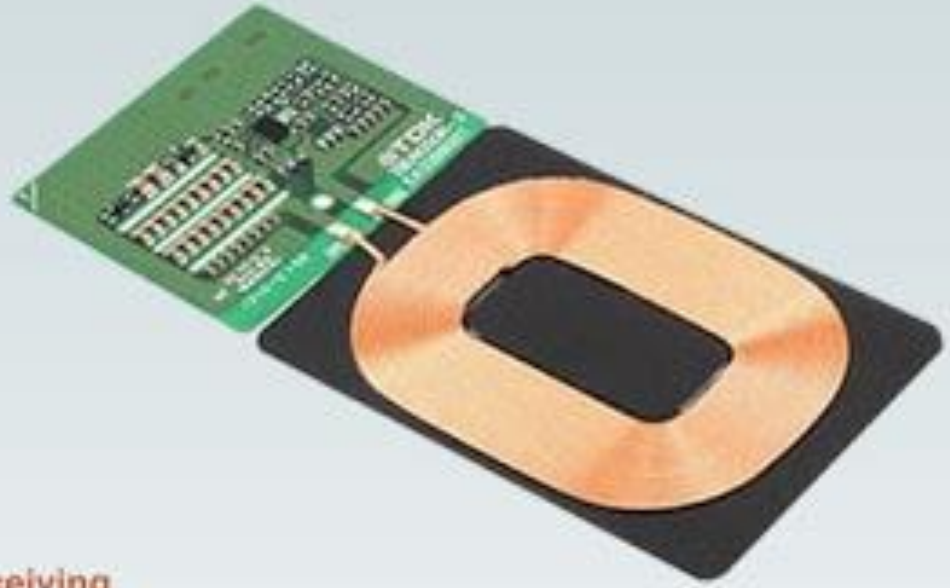
RF Harvesting

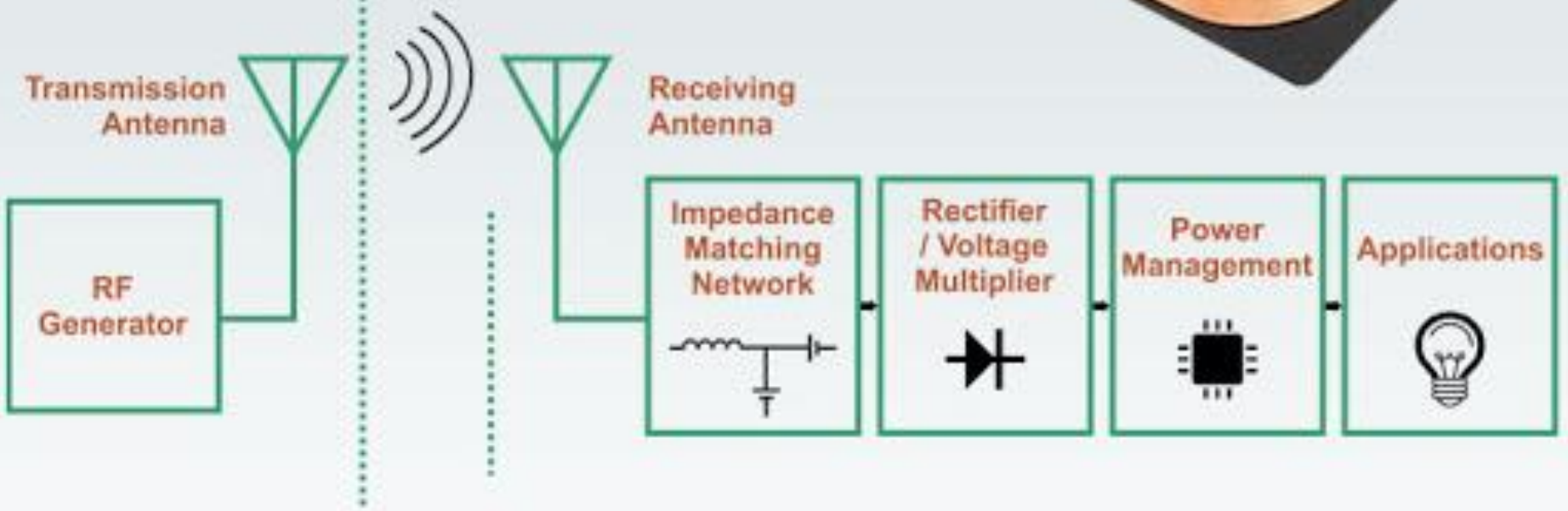
Radiofrequency (**RF**) energy harvesting is used in the form of RFID tags. RFID enjoys the benefit of being a near-field communication that uses a transceiver that essentially powers the RFID tag due to its close proximity.

For far-field applications, to harvest energy from broadcast transmissions. E.g. televisions, cell signals, and radio.

Capturing energy is difficult, as RF signals have the smallest energy density of all harvesting techniques.

RF Energy Harvesting

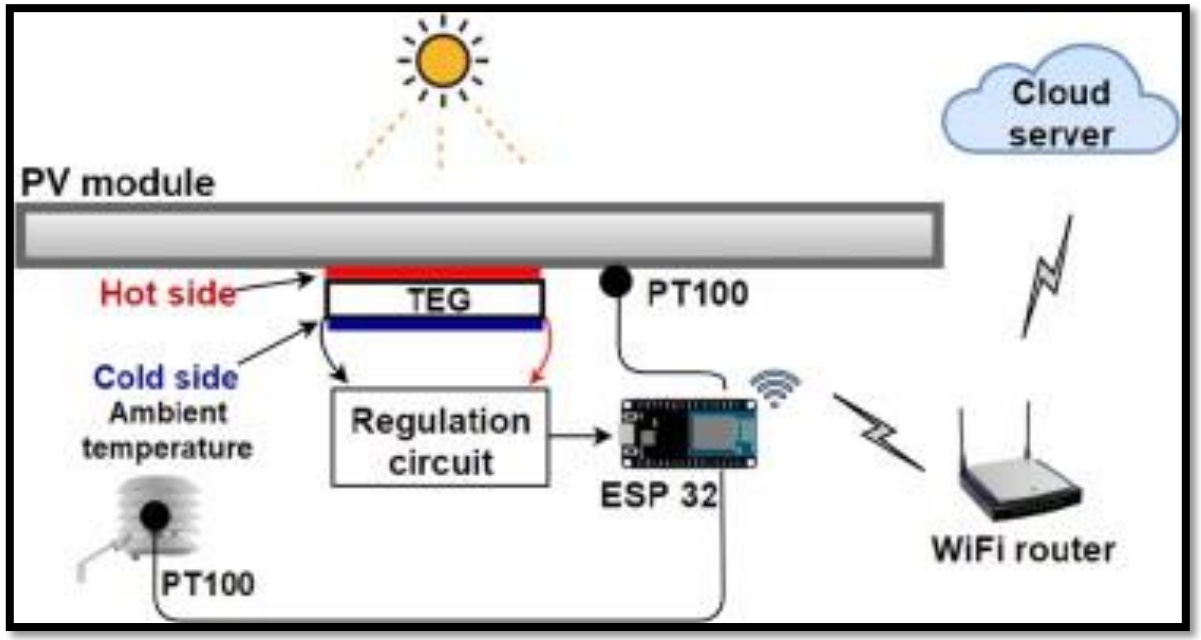


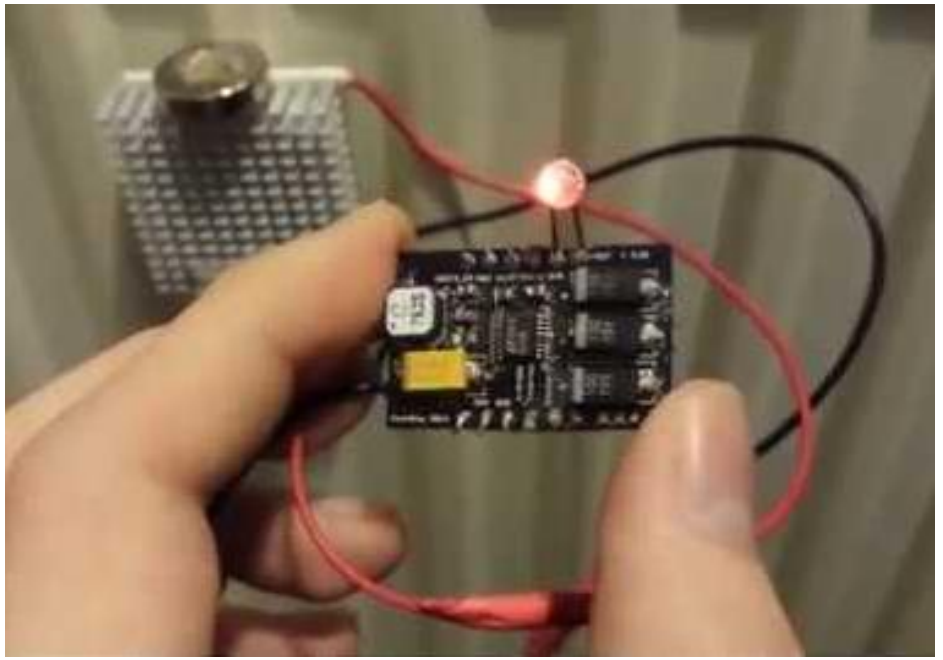


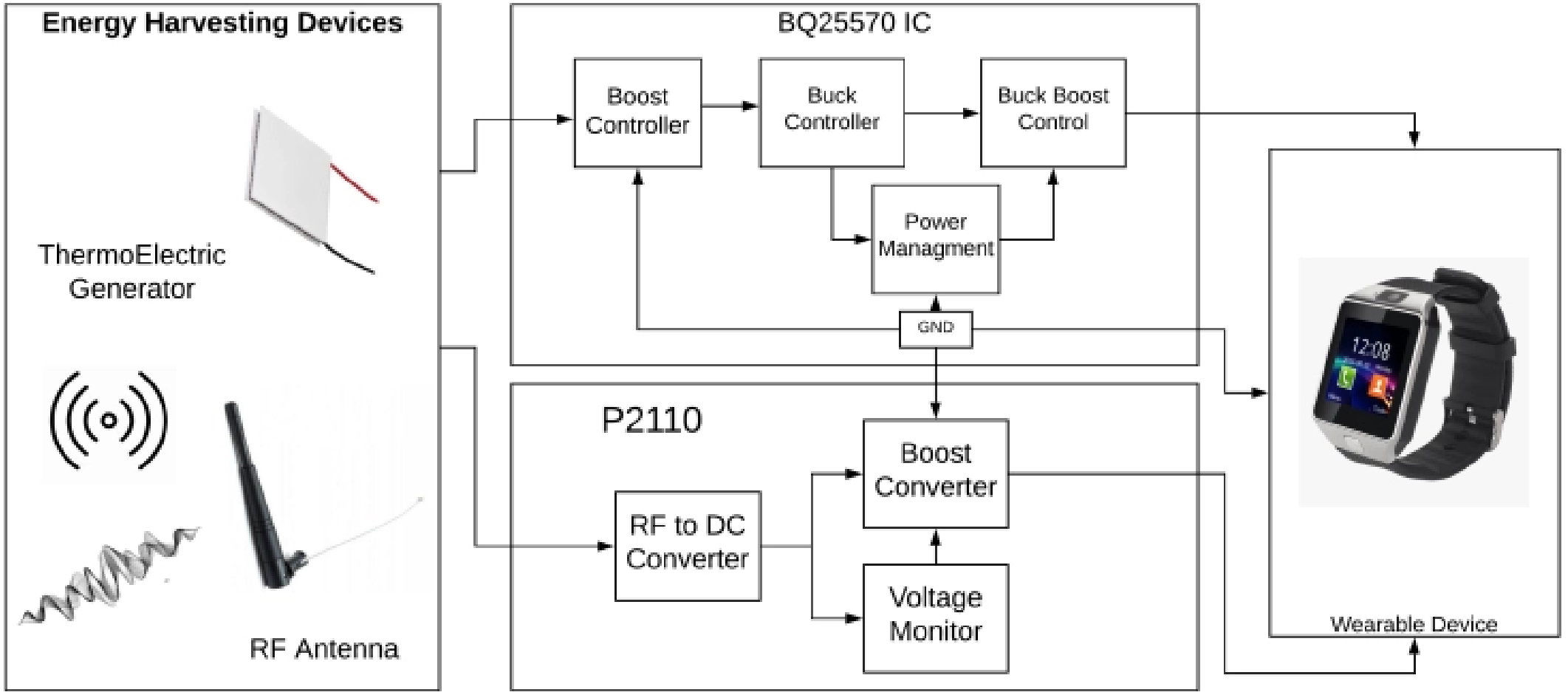
Thermal Harvesting

Thermal energy can be converted into electrical energy by two basic processes:

1. **Thermoelectric**: Direct conversion of thermal energy into electrical energy through the Seebeck effect.
2. **Thermionic**: Also known as thermos tunnelling where electrons are ejected from a hot electrode into a cold electrode


Cloud server
PV module
Hot side
TEG
PT100
Cold side
Ambient temperature
Regulation circuit
ESP 32
WiFi router
PT100





Ref: https://www.eetimes.eu/thermal-and-rf-energy-harvesting-circuit-for-ultra-low-power-applications/

IoT Communication Standards

2ECDE65 Internet of Things

Non-IP Based WPAN Protocols

- Bluetooth
- Zigbee
- Z-wave

IP-Based WPAN and WLAN Protocols

- TCP/IP
- WPAN with IP – 6LoWPAN
- WPAN with IP – thread™
- IEEE 802.11 protocols and WLAN (Wi-Fi)

802.15 standards

802.15.1: Original foundation of the Bluetooth PAN
802.15.2: Coexistence specifications for WPAN and WLAN for Bluetooth
802.15.3: High data rate (55 Mbps+) on WPAN for multimedia
- **802.15.3a**: High-speed PHY enhancements
- **802.15.3b**: High-speed MAC enhancements
- **802.15.3c**: High-Speed (>1 GBps) using mm-wave (millimeter wave) technology

802.15.4: Low data rate, simple design, multi-year battery life specifications (Zigbee)
- **802.15.4-2011**: Rollup (specifications a-c) includes UWB, China, and Japan PHYs
- **802.15.4-2015**: Rollup (specifications (d-p) includes RFID support, medical-band PHY, low energy, TV white spaces, rail communications

802.15 standards

802.15.5: Mesh networking
802.15.6: Body area networking for medical and entertainment
802.15.7: Visible light communications using structured lighting
- **802.15.7a**: Extends range to UV and near-IR, changed name to optical wireless

802.15.8: **Peer Aware Communications** (**PAC**) infrastructure-less peer to peer at 10 Kbps to 55 Mbps
802.15.9: **Key Management Protocol** (**KMP**), management standard for key security
802.15.10: Layer 2 mesh routing, recommend mesh routing for 802.15.4, multi PAN
802.15.12: Upper layer interface, attempts to make 802.15.4

BLUETOOTH

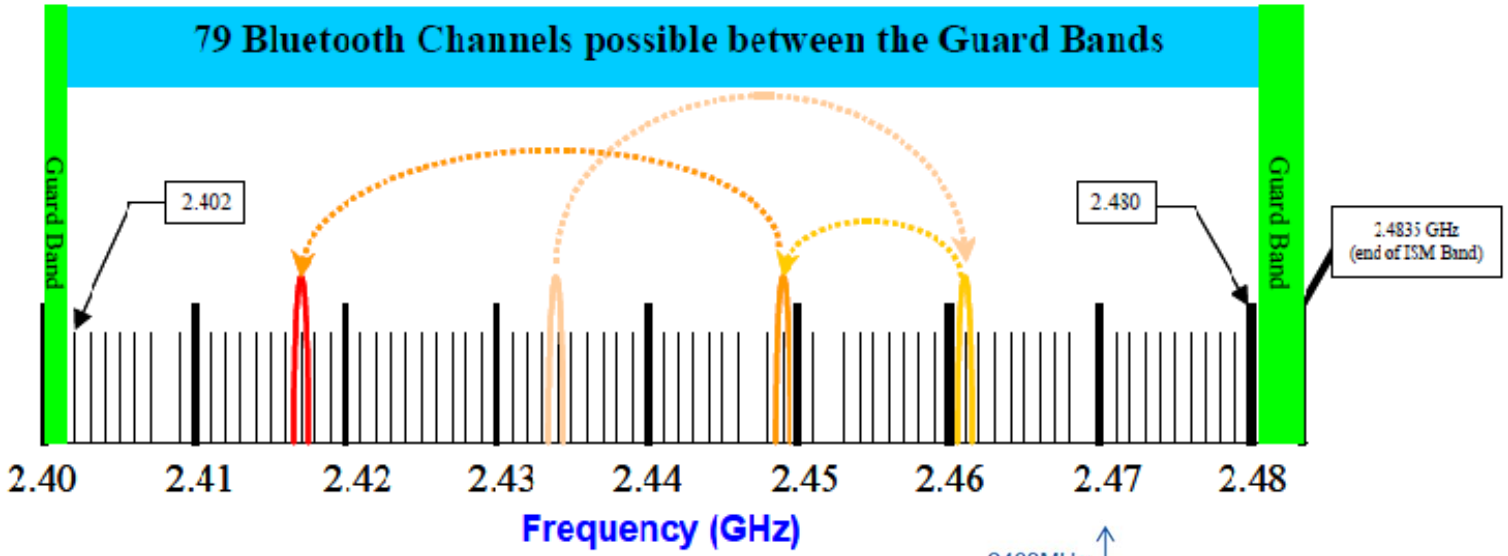
https://www.youtube.com/watch?v=1I1vxu5qIUM

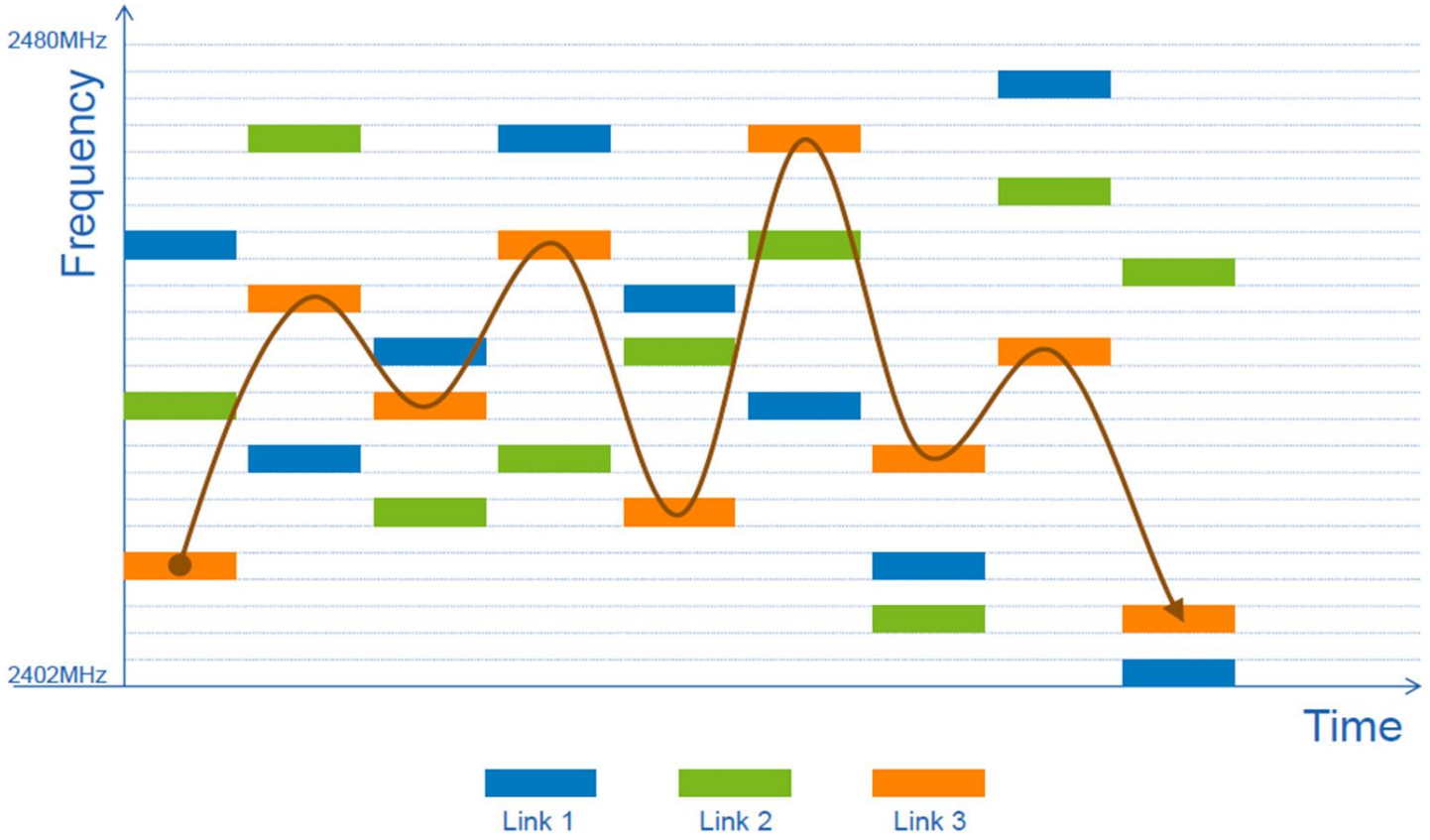
- Invention
  - 1994
  - Erission
  - a wireless alternative to RS-232 cable
- Development
  - 1997-1998
  - Erission, Nokia, Toshiba, IBM, Intel
  - Ver 0.7, 0.8 proposed
- Publish
  - 1999
  - SIG (Special Interest Group) is founded
  - Microsoft, Motorola, Samsung, Lucent with SIG
  - Bluetooth 1.0 published

Characteristics

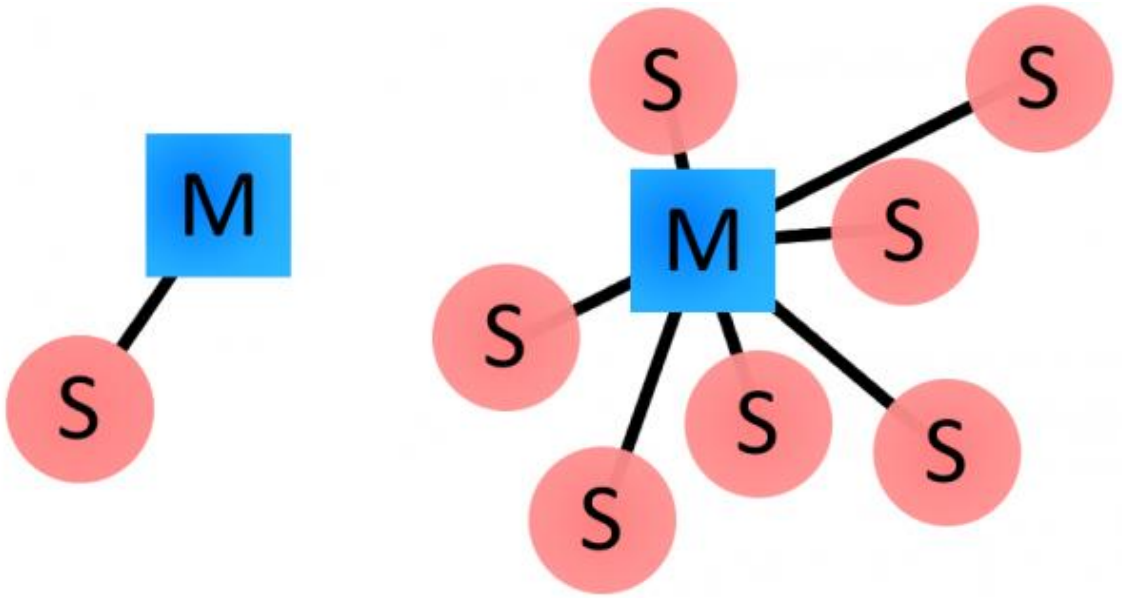
- Unlicensed 2.4GHz radio band
  - ISM (industrial, scientific,medical) band - Available worldwide
  - Also used by Microwave ovens, 802.11, HomeRF…
- Gross data rate of 1 Mbit/s
- Basic 10m range extended to 100m with amplifiers
- TDMA - TDD - Frequency hopping
- **Fast frequency hopping**
  - 1600 (or 3200) hops/s
  - 79 frequencies
  - 1 MHz spacing
  - 220 µs switching time

Frequency Hopping

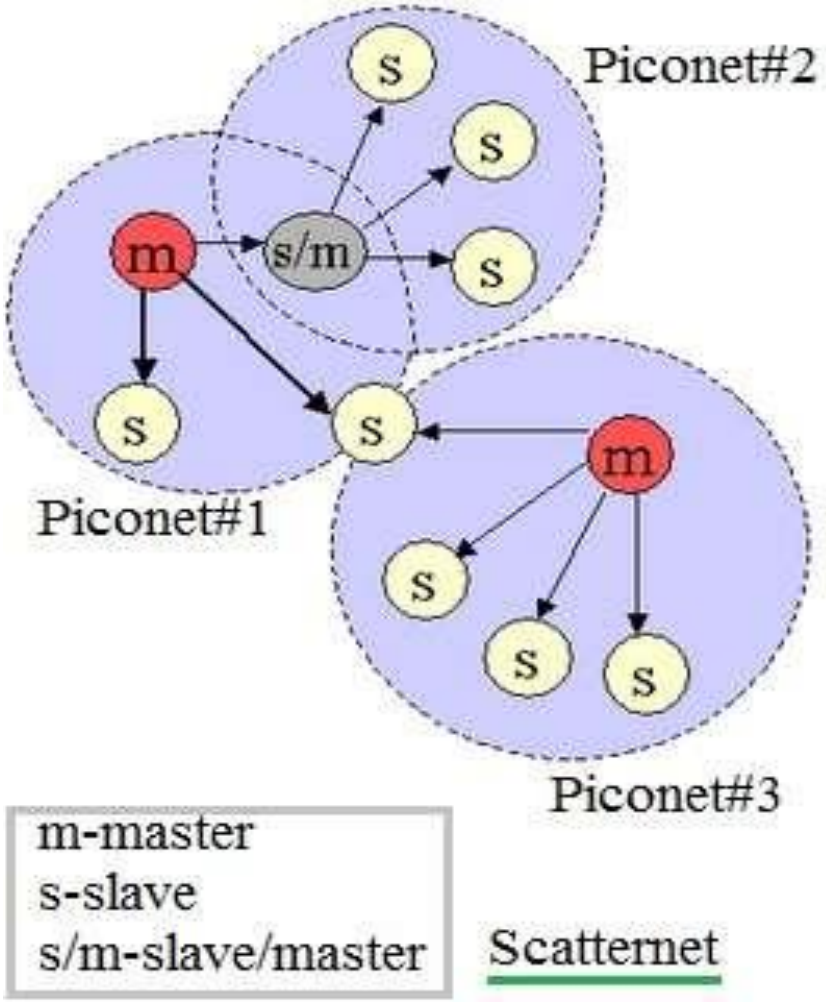




Bluetooth Network



Examples of Bluetooth master/slave piconet topologies.



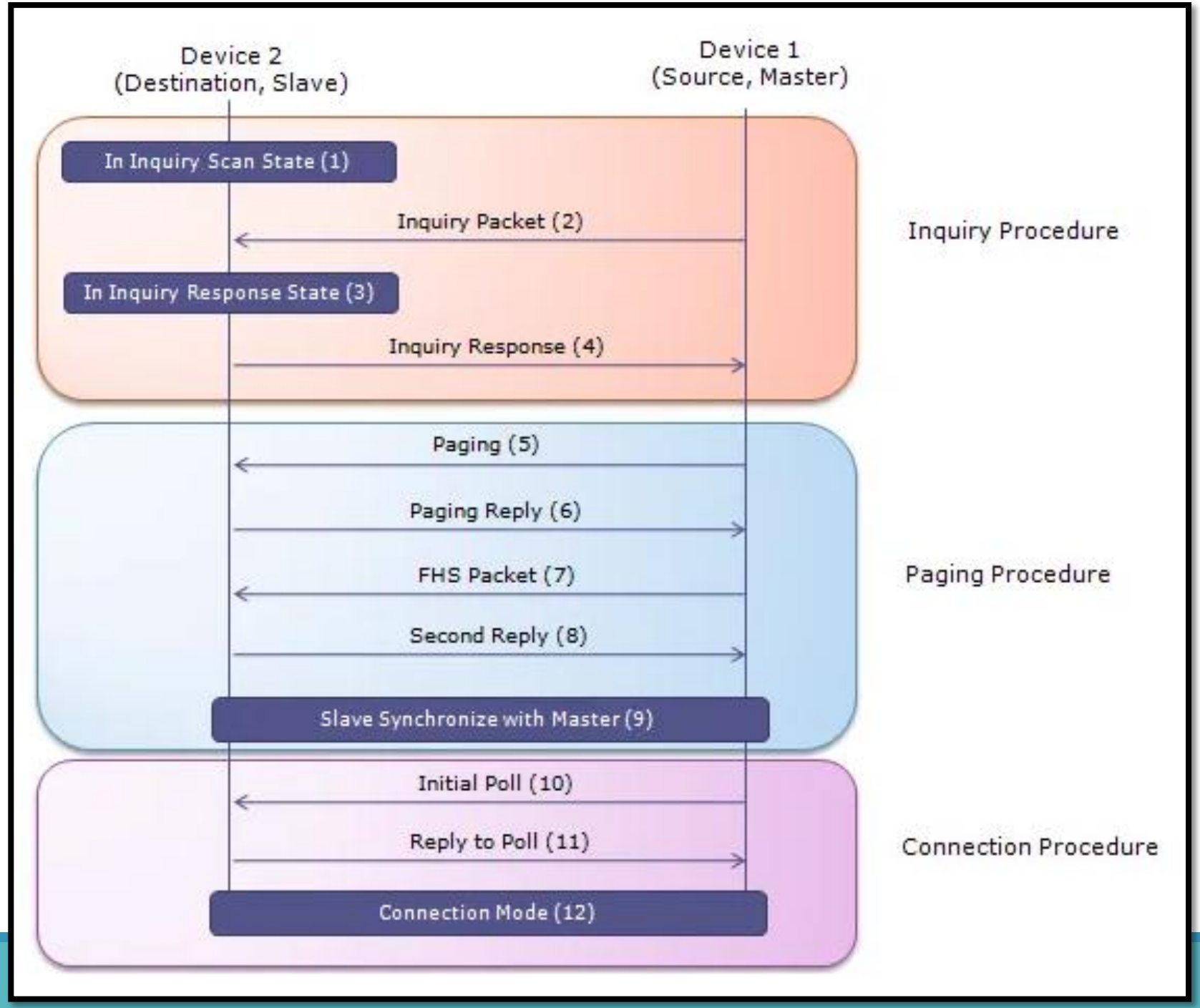
Bluetooth device has a unique 48-bit address, presented in the form of a 12-digit hexadecimal value.

Bluetooth Connection Procedure

- **Inquiry** -- One device sends out the inquiry request, and any device listening for such a request will respond with its address, and possibly its name and other information.
- **Paging** (Connecting) -- Paging is the process of forming a connection between two Bluetooth devices. Before this connection can be initiated, each device needs to know the address of the other.
- **Connection** -- After a device has completed the paging process, it enters the connection state. While connected, a device can either be actively participating or it can be put into a low power sleep mode.
  - Active Mode -- This is the regular connected mode, where the device is actively transmitting or receiving data.
  - Sniff Mode -- This is a power-saving mode, where the device is less active. It'll sleep and only listen for transmissions at a set interval (e.g. every 100ms).
  - Hold Mode -- Hold mode is a temporary, power-saving mode where a device sleeps for a defined period and then returns back to active mode when that interval has passed.
  - Park Mode -- Park is the deepest of sleep modes. A master can command a slave to "park", and that slave will become inactive until the master tells it to wake back up.

Ref:- https://lynxbee.com/understanding-bluetooth-basics-pairing-and-handshaking-process/

Bluetooth Connection Procedure

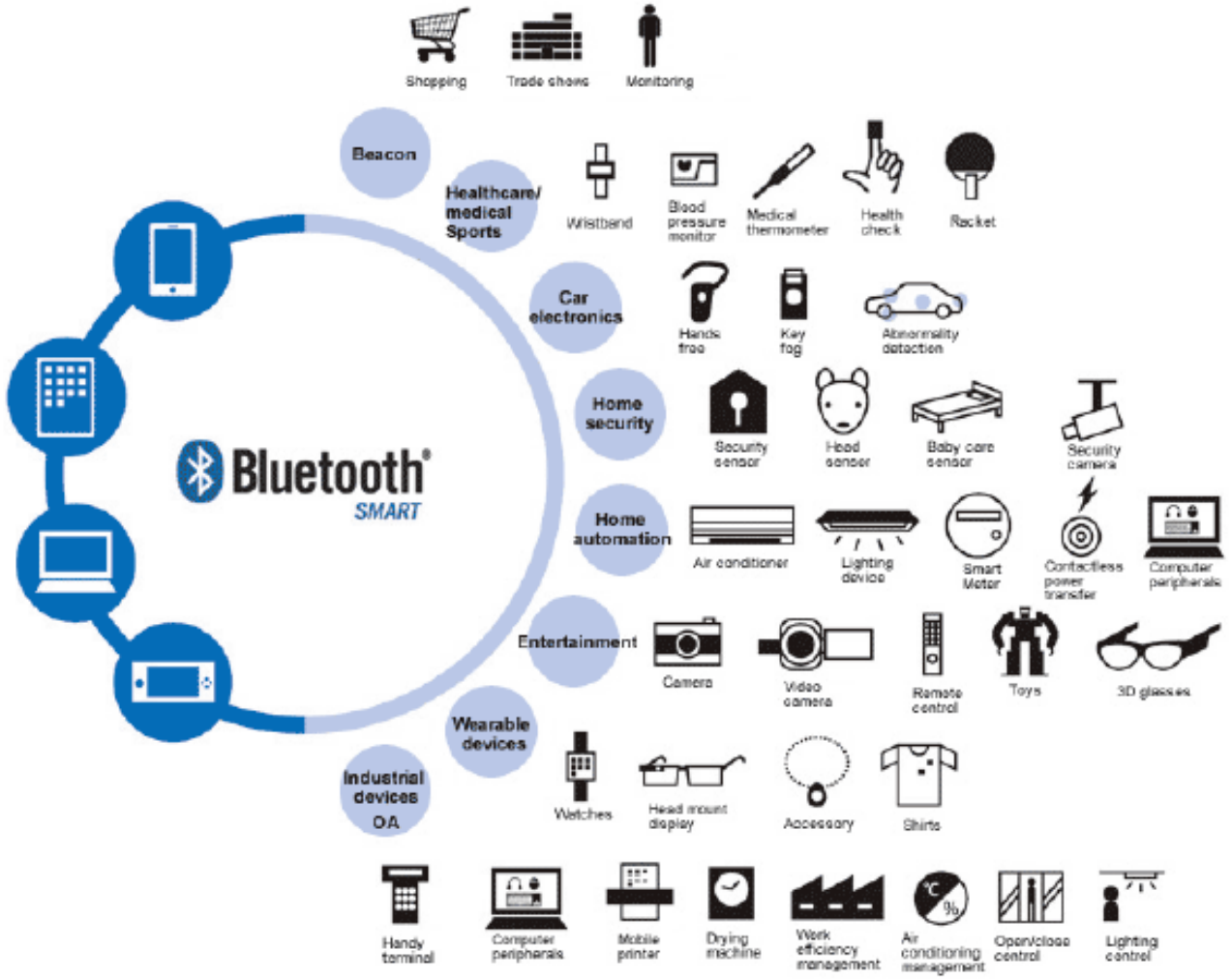


Bluetooth Versions

Year Introduced	Bluetooth Version	Feature
2004	2.0	Enhanced Data Rate
2007	2.1	Secure Simple Pairing
2009	3.0	High Speed with 802.11 Wi-Fi Radio
2010	4.0	Low-energy protocol
2013	4.1	Indirect IoT device connection
2014	4.2	IPv6 protocol for direct internet connection
2016	5.0	4x range, 2x speed, 8x message capacity + IoT

Bluetooth Low Energy (BLE) or Bluetooth smart

- What does IoT need?
  - An example: A sport bracelet
    - Small data packet
    - Burst transmission
    - Power consumption sensitive
- Similarities
  - Frequency band
  - Modulation
- Difference - Simplification
  - Smaller duty cycle
  - Shorter connecting time
  - Simpler packets
  - Connectionless advertising



	Bluetooth V2.1	Bluetooth Low Energy
Standardization Body	Bluetooth SIG	Bluetooth SIG
Range	~30 m (class 2)	~50 m
Frequency	2.4–2.5 GHz	2.4–2.5 GHz
Bit Rate	1–3 Mbit/s	~200 kbit/s
Set-Up Time	<6 s	<0.003 s
Voice Capable?	Yes	No
Max Output Power	+20 dBm	+10 dBm
Modulation Scheme	GFSK	GFSK
Modulation Index	0.35	0.5
Number of Channels	79	40
Channel Bandwidth	1 MHz	2 MHz

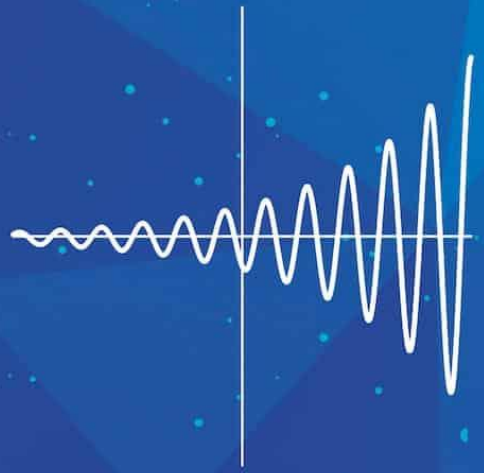
The emerging benefits of Bluetooth™ 5

Bluetooth 5 with mesh networking can technically support an **unlimited number of devices on a network**.

The range of **Bluetooth 5** is up to four times that of its predecessors, meaning you can cover larger areas using fewer devices. And with mesh **network topology enabling every device to connect to every other device, network sizes are technically limitless**.

Bluetooth 5 can deliver **up to 10 years' service from a single cell battery**.

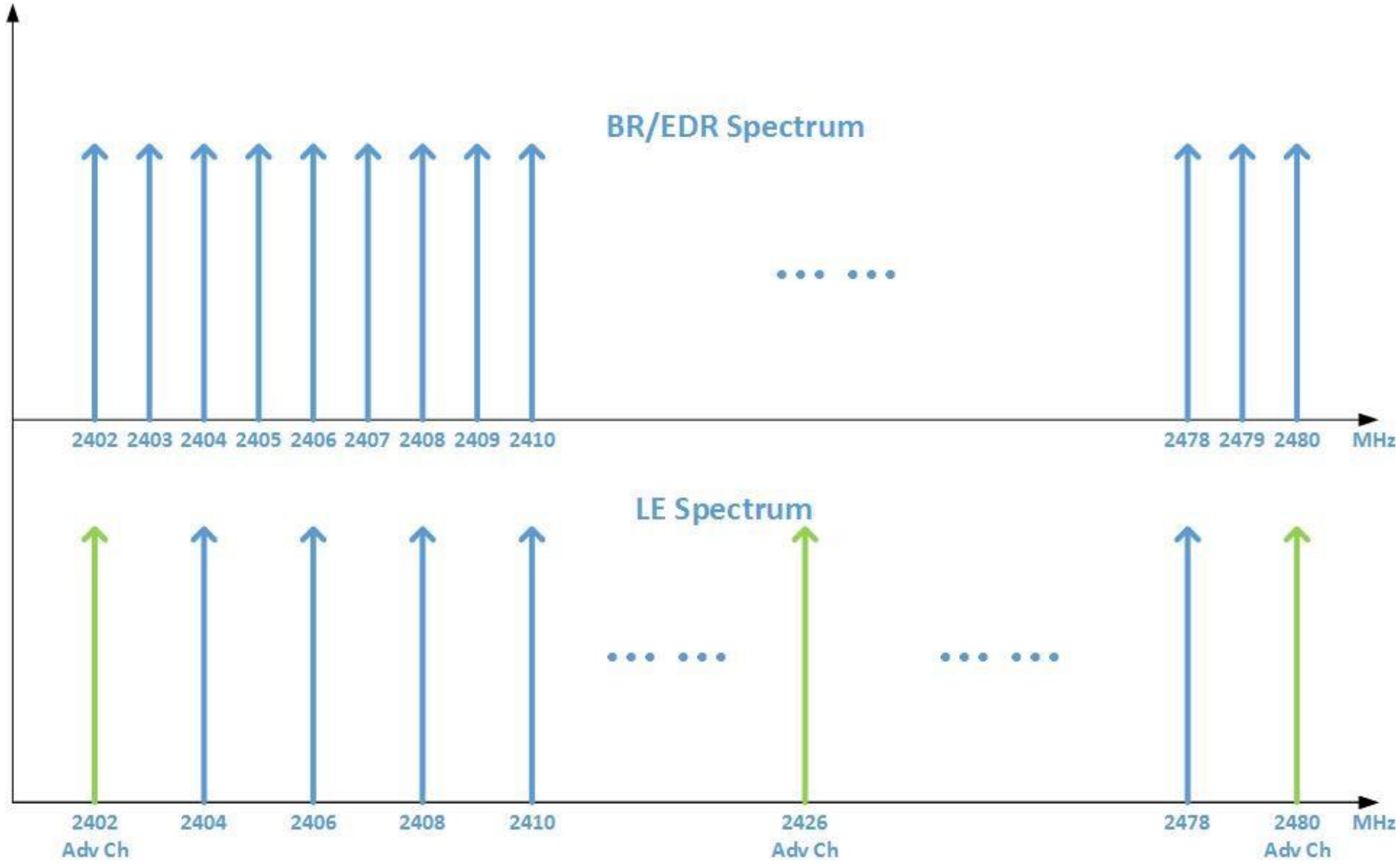
Bluetooth beacons will be greatly improved by **Bluetooth 5**, giving assets the ability to **transmit longer messages at higher data rates over greater distances**.



Thanks to techniques such as channel hopping and slot availability masks, **Bluetooth 5 has better interoperability and coexistence with other wireless technologies**.

MOUSER ELECTRONICS

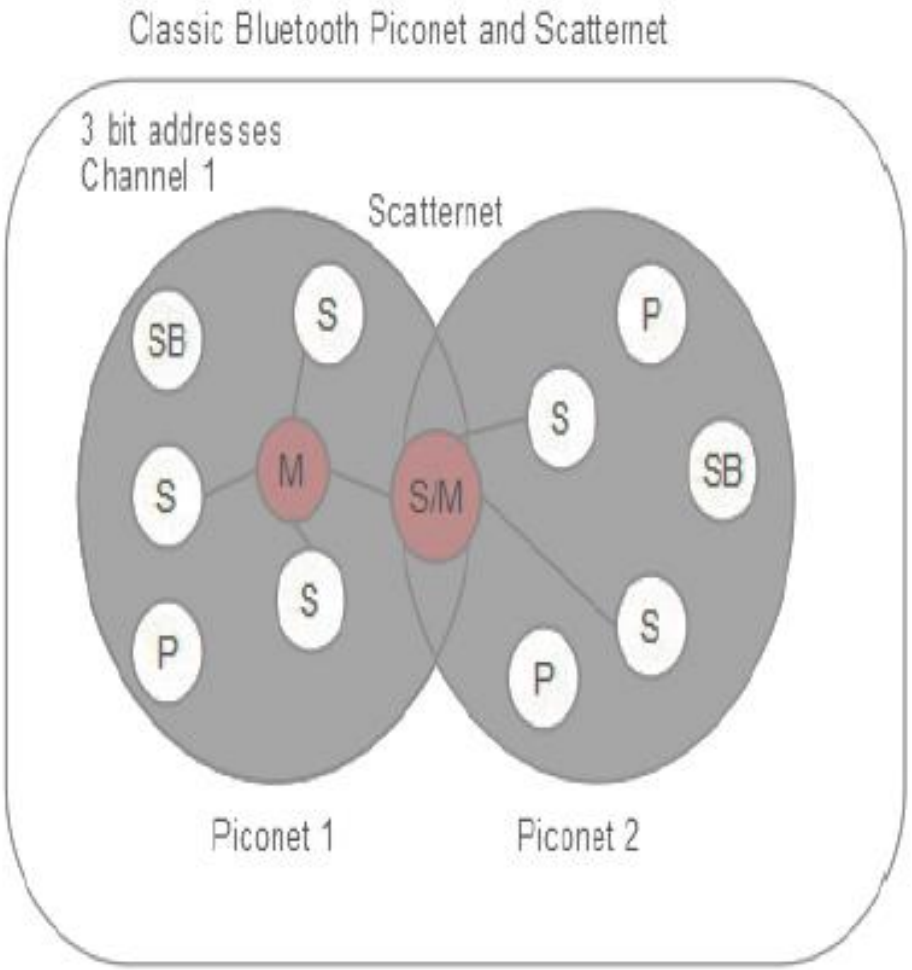
Link to webinar: **http://mou.sr/RFtechsolutions**

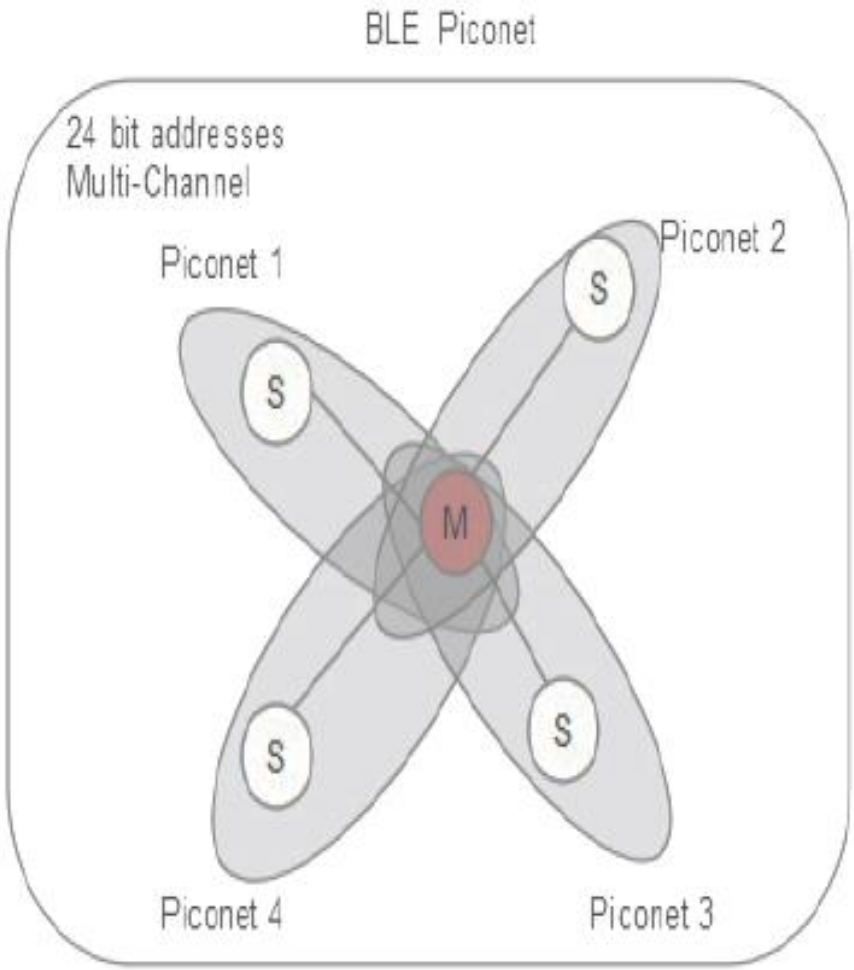

BR/EDR Spectrum
2402 2403 2404 2405 2406 2407 2408 2409 2410
2478 2479 2480
MHz
LE Spectrum
2402
Adv Ch
2404
2406
2408
2410
2426
Adv Ch
2478
2480
Adv Ch
MHz

Piconet and Scatternet

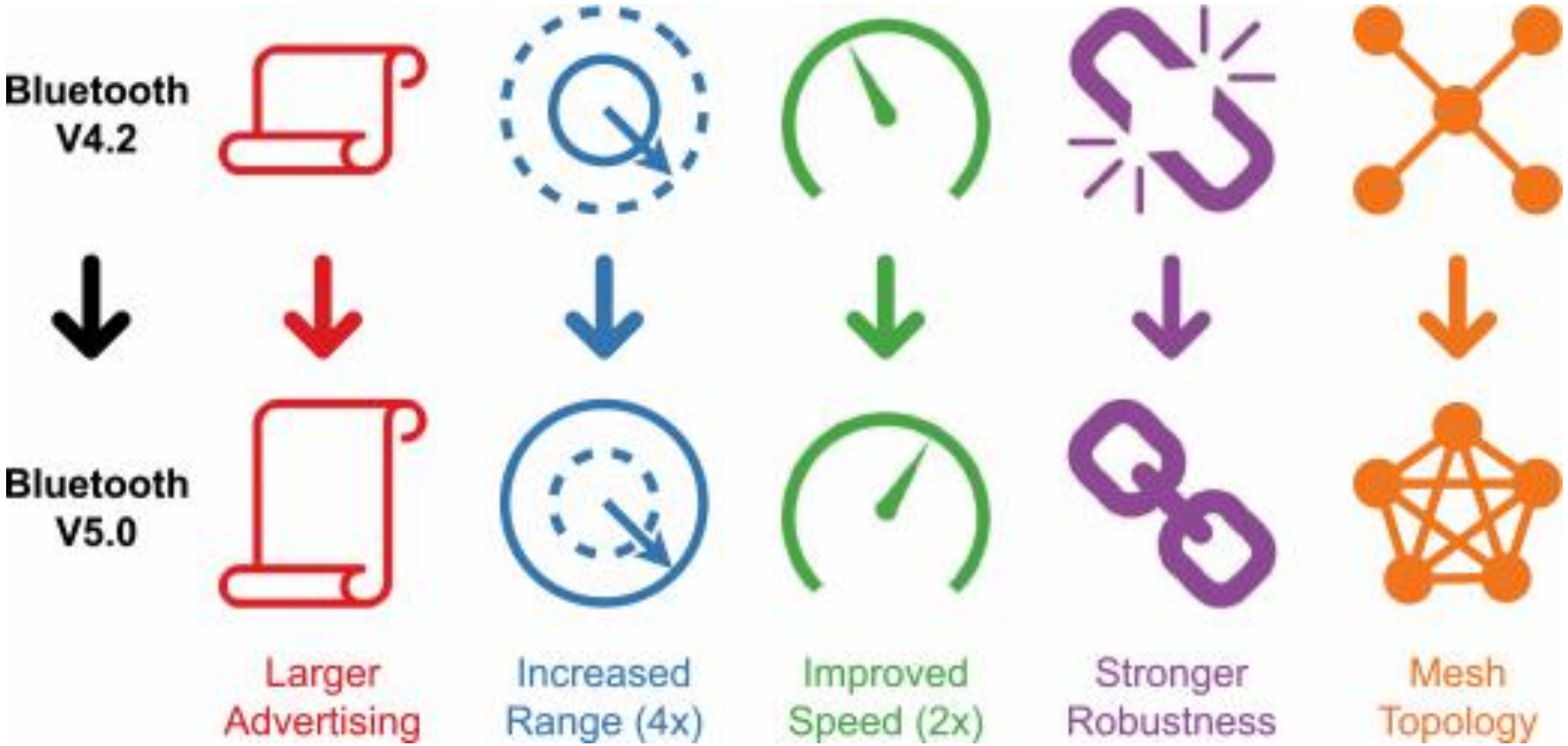
3 bit addressing
7 slaves with 1 master

SB- standby mode
P- Parked mode





7 bit addressing
1 slave/ piconet
Many piconets with 1 master


Bluetooth
V4.2
Bluetooth
V5.0
Larger
Advertising
Increased
Range (4x)
Improved
Speed (2x)
Stronger
Robustness
Mesh
Topology

Bluetooth 5
Long-range (Coded PHY)

How to Achieve Ranges of over 1 Km using Bluetooth Low Energy

By Mohammad Afaneh | January 6, 2020 | 1

Three PHYs in Bluetooth 5

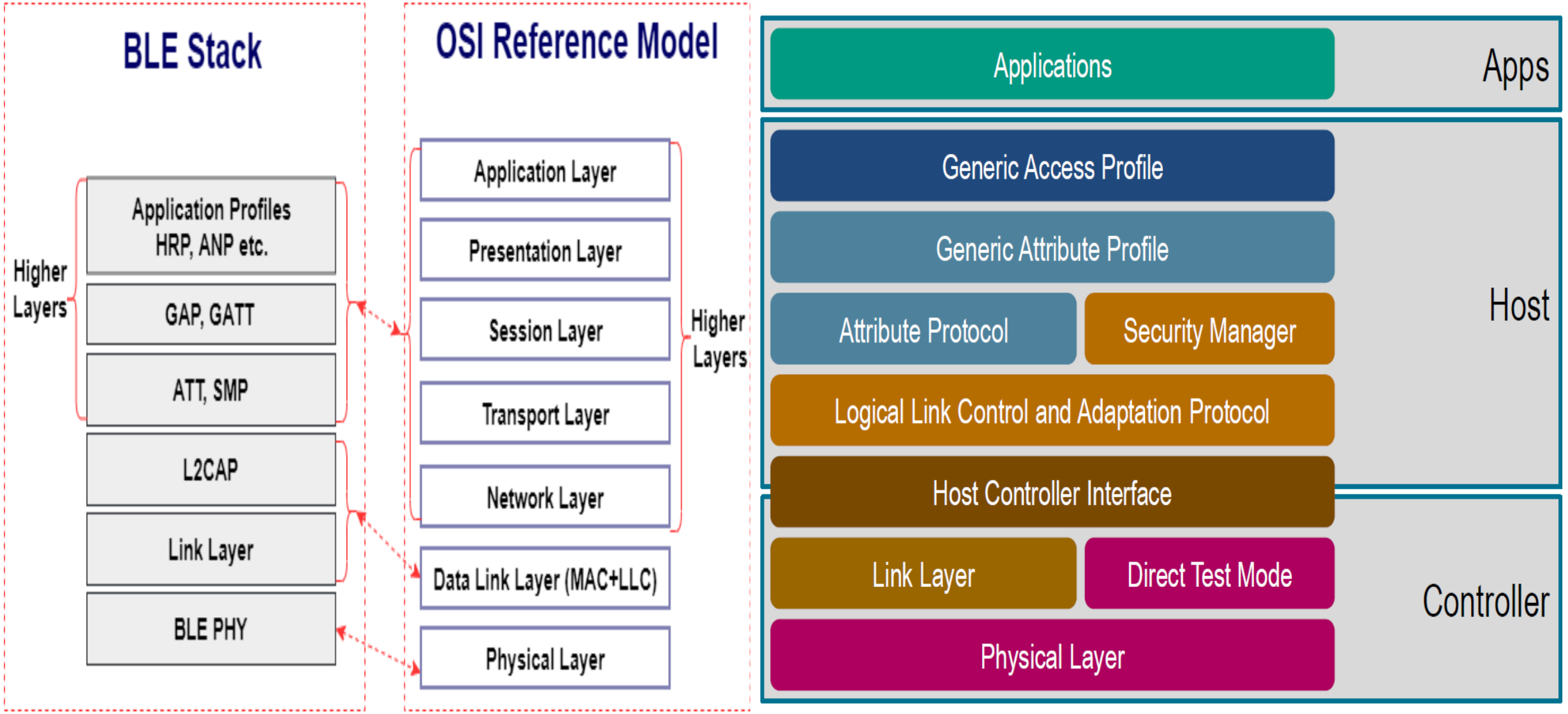
PHY	Modulation scheme	Coding scheme		Data rate
		Access Header	Payload	
LE 1M	1 Msym/s modulation	Uncoded	Uncoded	1 Mb/s
LE 2M	2 Msym/s modulation	Uncoded	Uncoded	2 Mb/s
LE Coded	1 Msym/s modulation	S=8	S=8	125 kb/s
			S=2	500 kb/s

4 times Range

LE 1M uses a frequency deviation of at least 185 kHz.
LE 2M uses a frequency deviation of at least 370 kHz.

https://www.novelbits.io/long-range-bluetooth-coded-phy/

Protocol Stack of Bluetooth LE



HCI layer provides communication between the host and controller through a standardized interface

L2CAP layer provides data encapsulation services to the upper layers, allowing for logical end-to-end communication of data

Security Manager layer defines the methods for pairing and key distribution, and provides functions for the other layers of the protocol stack to securely connect and exchange data with another device

Generic Access Profile (GAP) layer handles device discovery and connection-related services for the device

Generic Attribute Profile (GATT) layer is a service framework that defines the sub-procedures for using ATT.

ATT layer allows a device to expose certain pieces of data or *attributes*, to another device.

https://www.youtube.com/watch?v=8OfOwD8f2VI

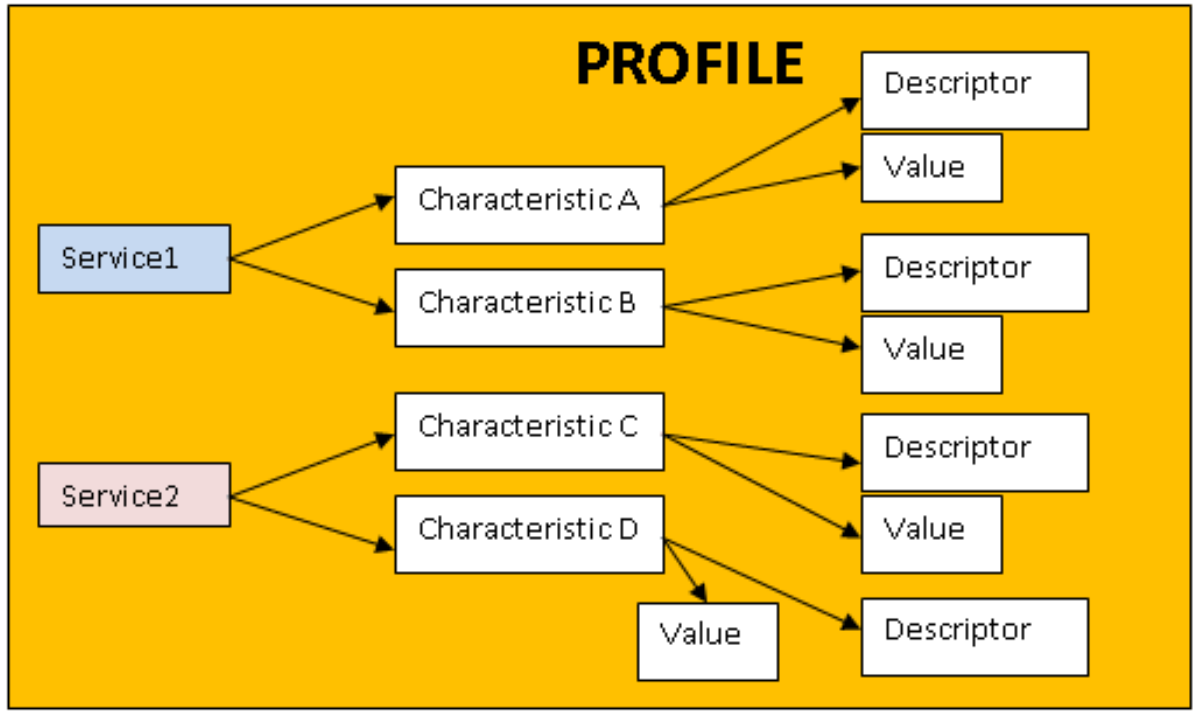
https://www.youtube.com/watch?v=eHqtiCMe4NA

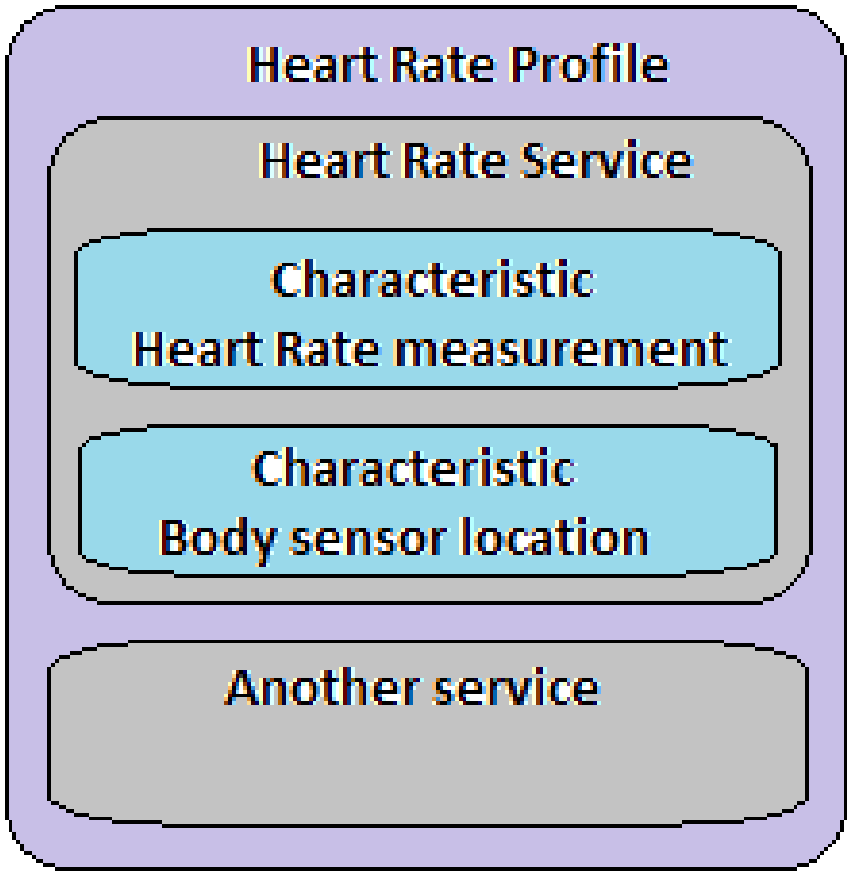
Generic Access Profile GAP

- **Broadcasting**: No connection
  - **Broadcaster**: A device that broadcasts public advertising data packets, such as how long a button has been pressed.
  - **Observer**: A devices that listens to the data in the advertising packets sent by the broadcaster. No connection happens between the broadcaster and observer.
- **Connecting**: Explicitly connect and handshake to transfer data.
  - **Peripheral**: A device that advertises its presence so central devices can establish a connection. After connecting, peripherals no longer broadcast data to other central devices and stay connected to the device that accepted connection request.
  - **Central**: A device that initiates a connection with a peripheral device by first listening to the advertising packets. A central device can connect to many other peripheral devices.

GAP Role	Connectionless	Connection-oriented
Active	**Broadcaster** • An Advertiser • Transmit only • Periodically sends advertising data packets • Does not allow connection • *Example: TILE/iBeacons broadcasting ID/ location data*	**Peripheral** • A Follower • Advertises to establish a connection • Allows single connection to central peer • *Example: Bluetooth headphones in pairing mode*
Passive	**Observer** • A Scanner • Receive only • Looks for advertising data packets • Does not initiate connection • *Example: Apps receiving ID/ location data for user display*	**Central** • An Initiator • Looks for advertising to initiate a connection • Allows multiple connections to peripheral peers • *Example: Smartphone Bluetooth settings app searching for connectable devices*

Generic Attribute Profile





https://www.bluetooth.com/specifications/gatt

Security in Bluetooth Low Energy

- No security for initial phase of pairing
- Key generation uses **long-term key** (**LTK**) based on an **elliptical-curve Diffie Hellman** (**ECDH**) public key cryptography.
- The master and slave generate ECDH public-private key pairs and exchange public portion of their respective pairs
- BLE randomizes 48-bit address:
  - **Random static private address**
  - **Random private resolvable - Identity Resolving Key** (**IRK**) is exchanged between the two devices.
  - **Random private non-resolvable**: The device address is simply a random number

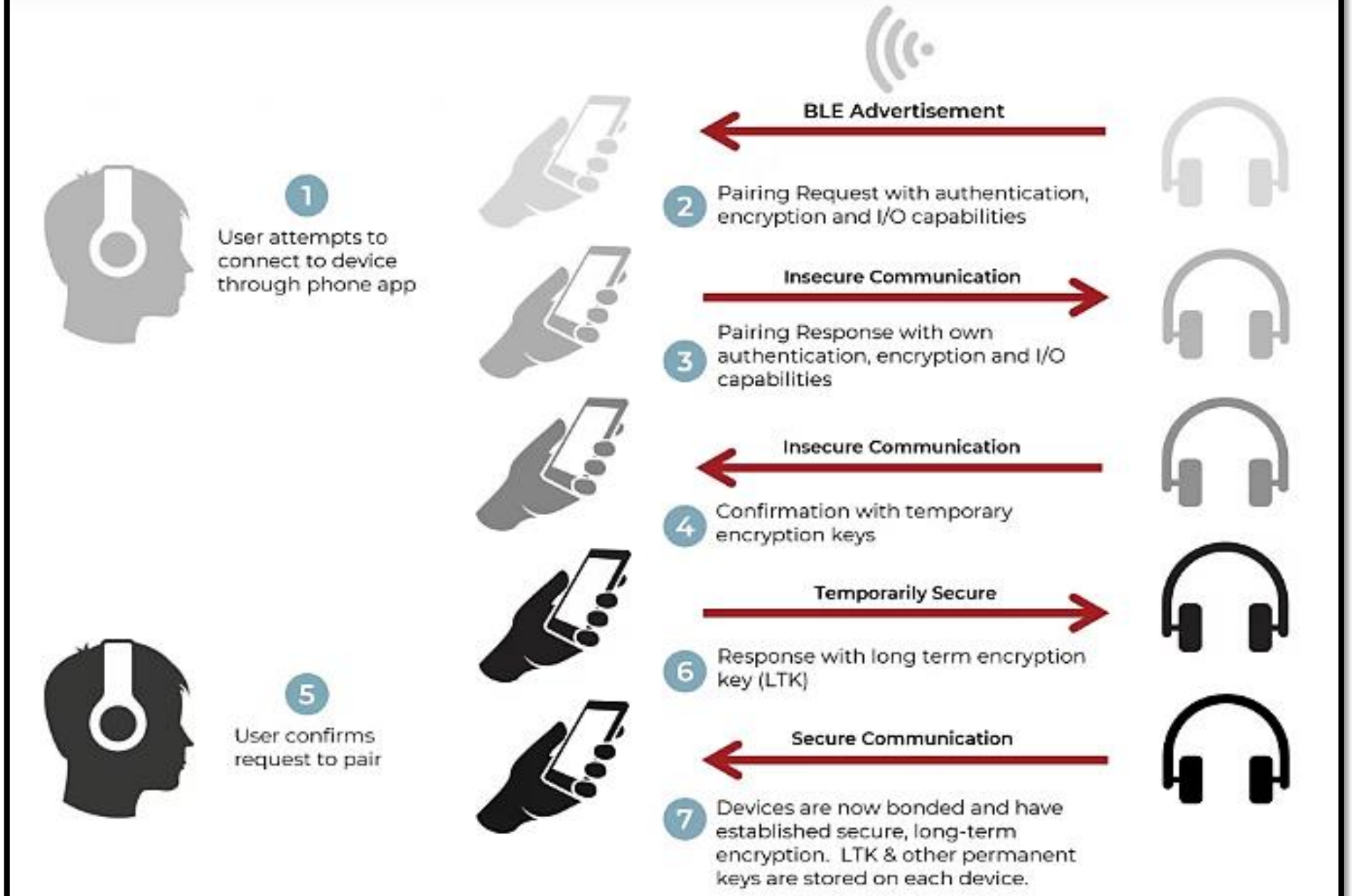


Figure 3: Establishing a secure Bluetooth Low Energy connection through the bonding process. This provides lasting encryption through the exchange of a long-term key (LTK).

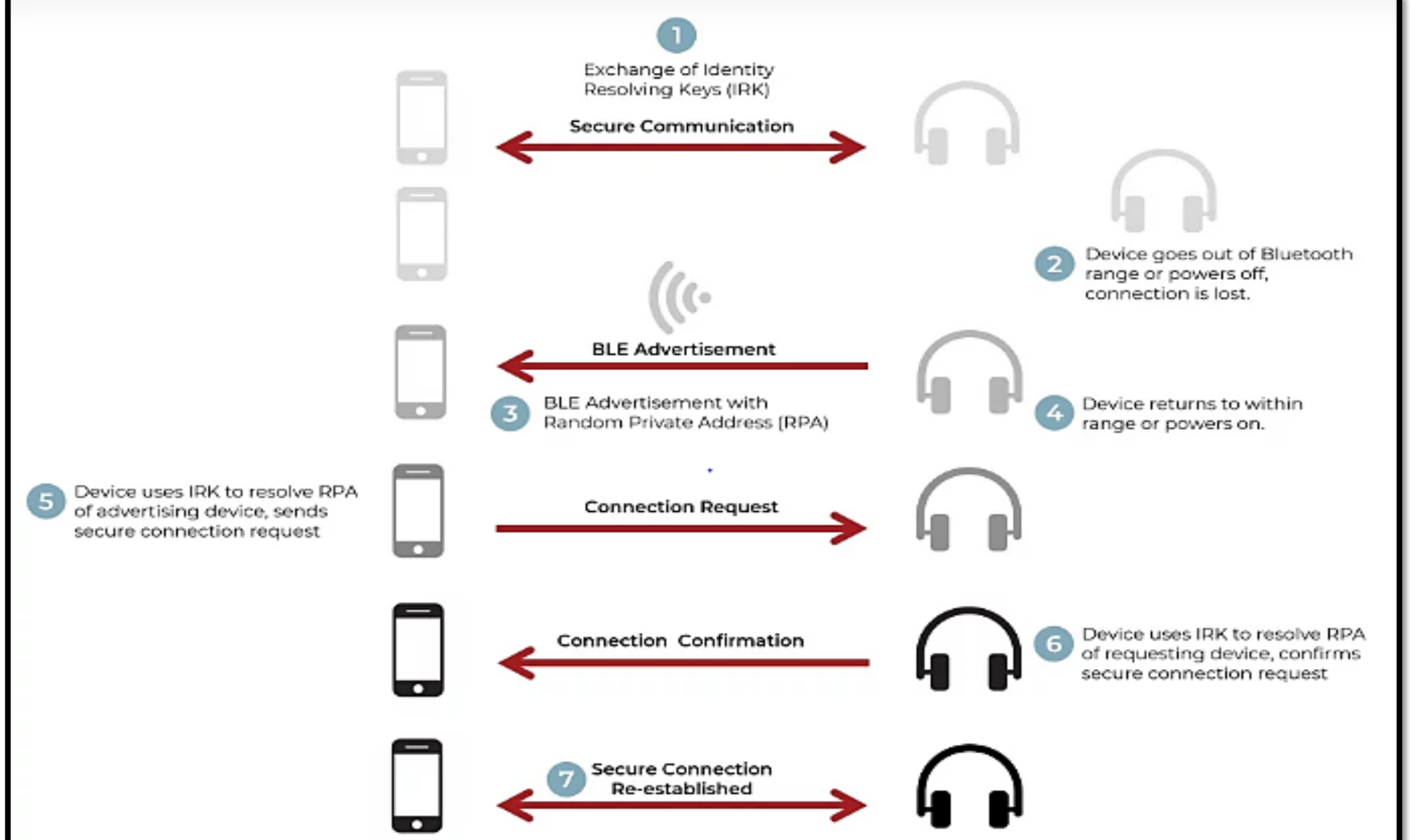


Figure 4: Establishing Bluetooth Low Energy privacy through the exchange and storage of an identity resolving key (IRK). The IRK is used to authenticate the devices upon resumption of a BLE connection.

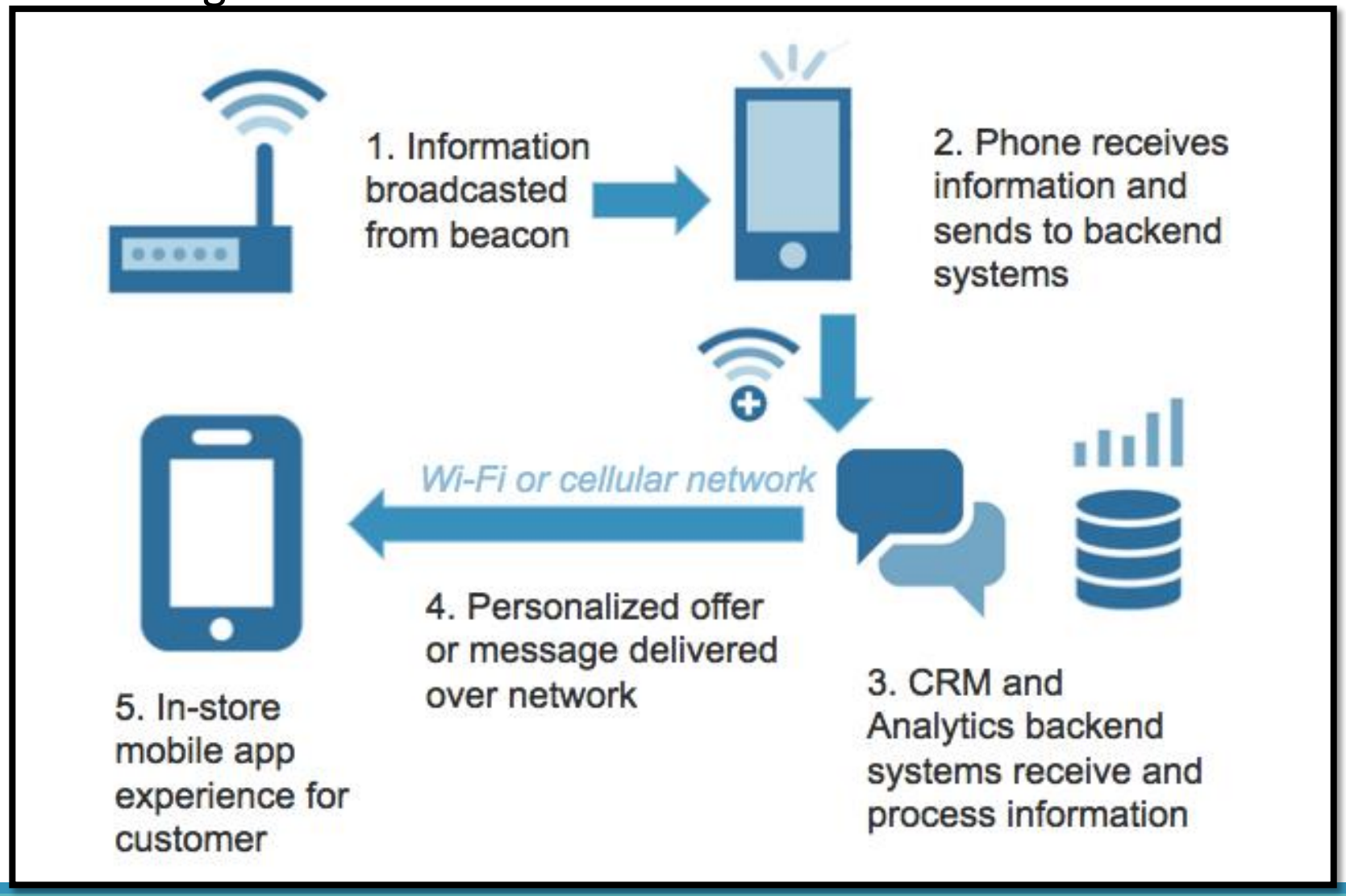
Ref: https://www.cardinalpeak.com/blog/bluetooth-le-security-and-privacy-in-wireless-audio-devices

Application scenario	**Audio stream application**	**Data transmission application**	**Location services application**	**Device network application**
	Wireless head-phones Wireless speaker Vehicle-mounted entertainment	Sports and fitness equipment Medical and health equipment Peripherals and accessories	Beacon services Indoor navigation service Asset tracking	Control system Monitoring system Automation system
Communication mode	One-to-one	One-to-one	One-to-many (broadcast)	Many-to-many (mesh)
Radio frequency mode	Classic Bluetooth BR/EDR	Bluetooth low energy (Bluetooth LE)		

Bluetooth Beacon

Eddystone by Google
iBeacon by Apple

Beaconing is Bluetooth devices in LE mode to advertise on some periodic basis.



Beacon Technology

https://www.youtube.com/watch?v=2YorsgulwdU

HOW BEACON TECHNOLOGY WORKS

Retailers strategically place beacons around their store.

The Beacons connect to a customer's Bluetooth enabled smartphone app.

It sends a signal to the phone and the app is opened.

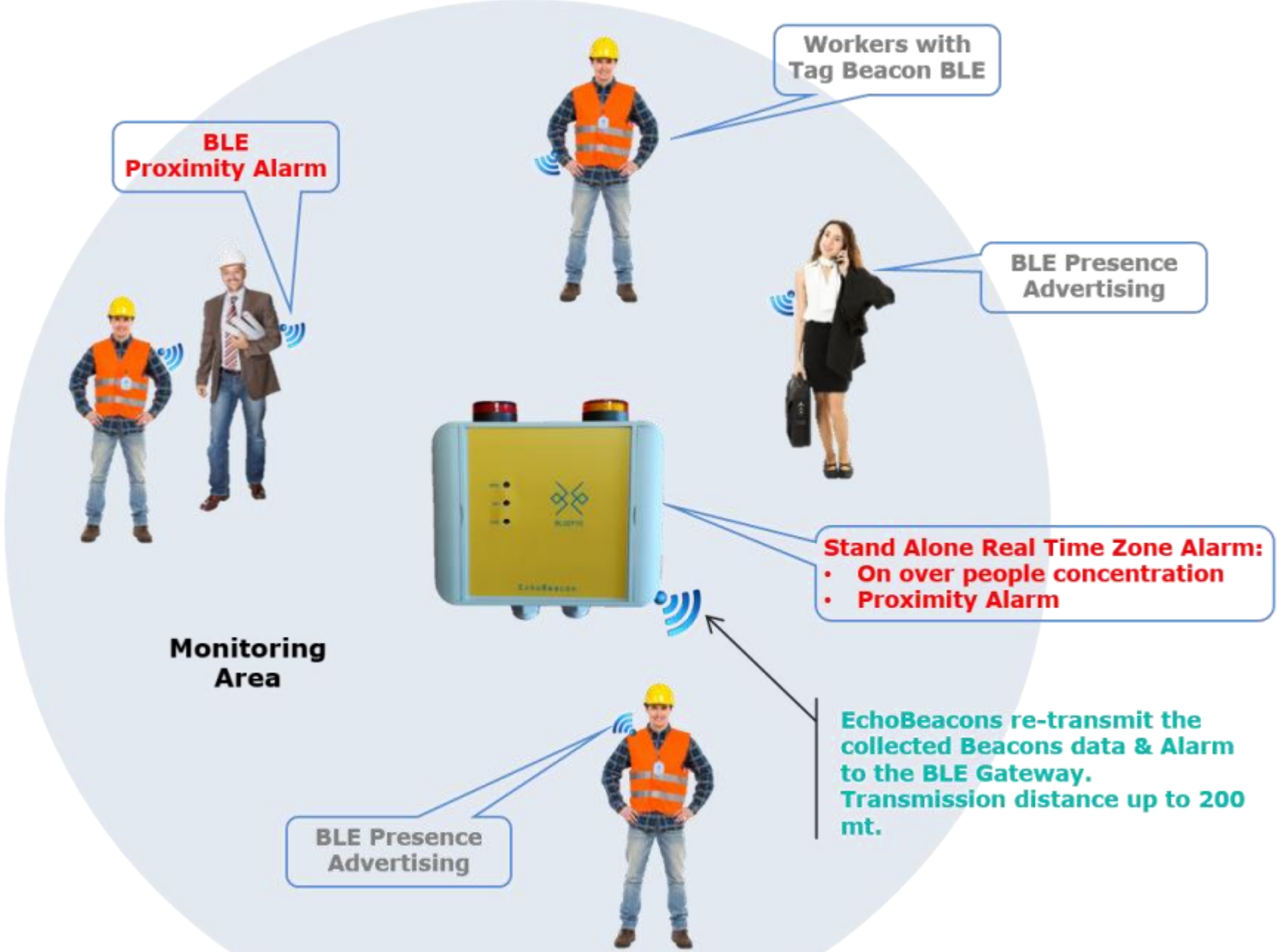
The retailer can provide the customer with a wealth of information.


Front Side
Led
Led
QRcode
MAC Address
Back Side
Push button
BluEpyc
bluepyc.com
cf:4b:0c:9e:51:32
Unique MAC Address
BE_A1900299
Friendy Name


Bluetooth 5.1
Temperature
Humidity
THINGSUP


41113
CR2450
3V

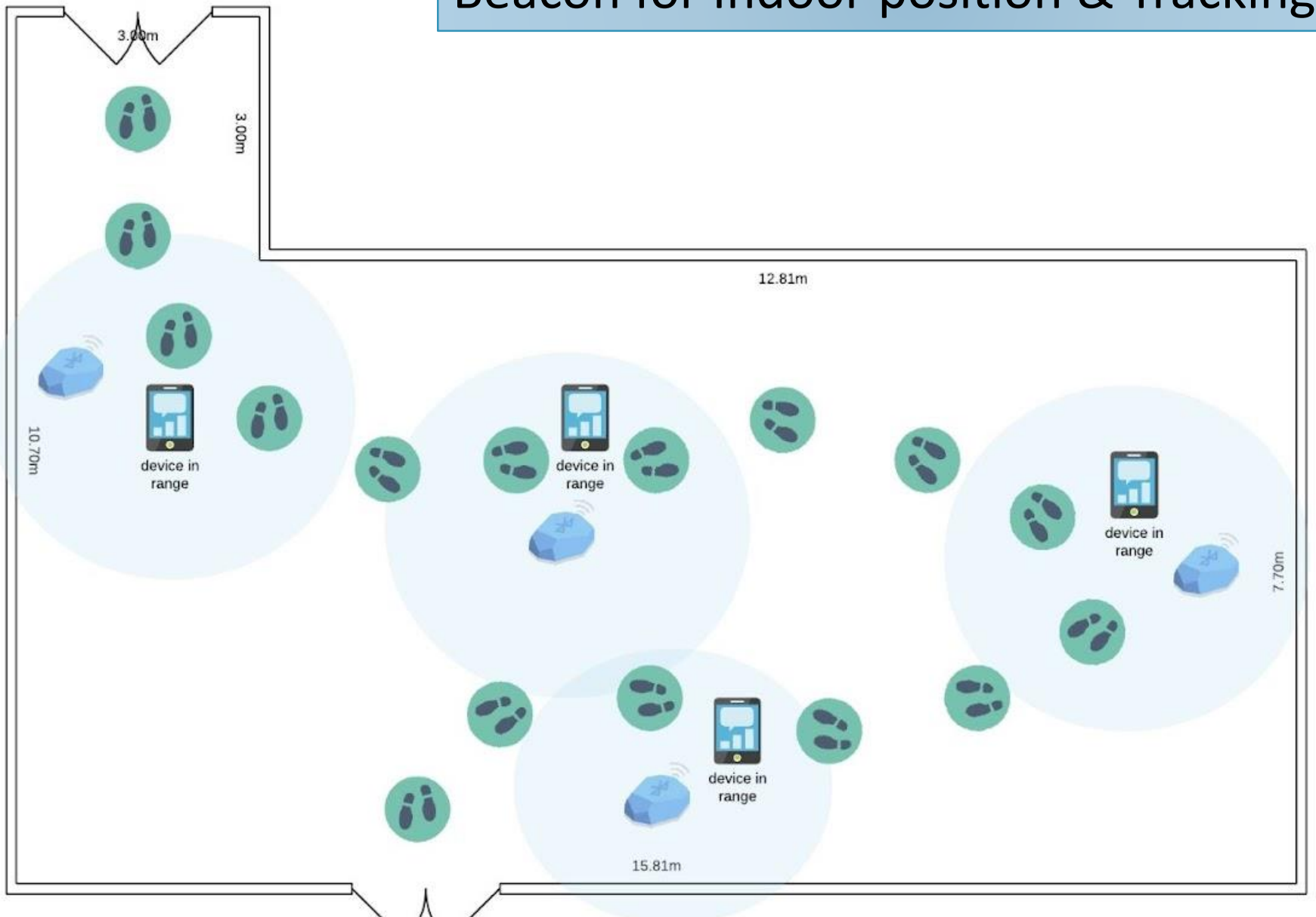

BlueSense
Estimote
Gimbal Series 10
Gliworm
Kontakt.io



Beacons for social distancing

https://www.bluepyc.com/application/blueye-ble-social-distancing-solution-covid/

Beacon for Indoor position & Tracking



Calculating Battery life _ A case study

Assume an iBeacon is advertised every 500 ms and the packet length is 31 bytes. The device uses a CR2032 coin cell battery rated at 220mAh at 3.7V. The beacon electronics consume 49uA at 3V. Use 0.7 factor or battery power decay. Find life of the battery.

Power consumption = 49uA x 3V = 0.147mW

Bytes per second = 31 x (1 second/500 ms) x 3 channels = 186 bytes/second

Bits per second = 186 bytes/second x 8 = 1488 bits/second

Energy per bit = 0.147 mW / (1488 bits/second) = 0.098 uJ/bit

Energy used for each advertisement = 0.098 uJ/bit x 31 bytes x 8 bits/byte = 24.30 uJ/advertisement

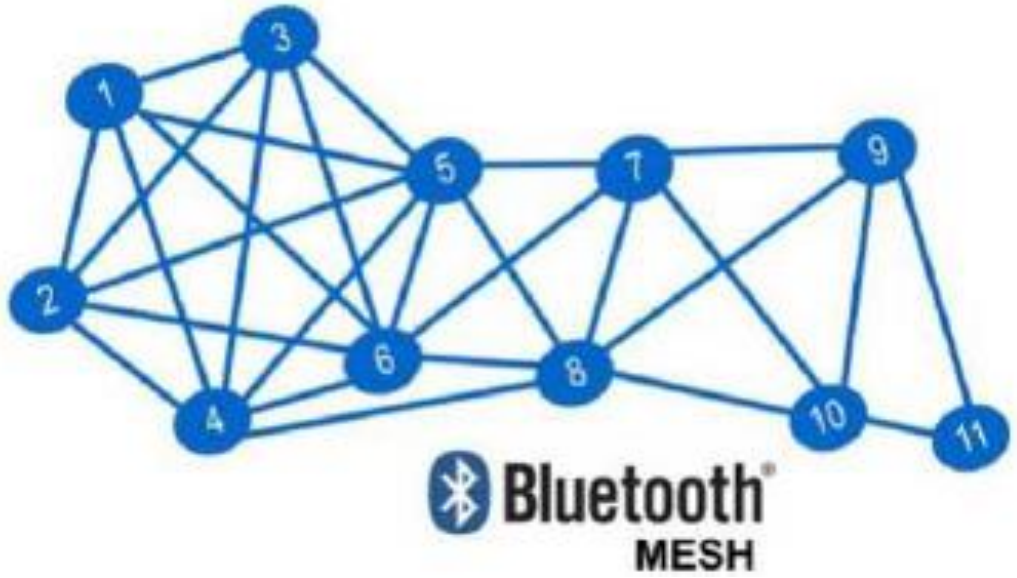
Energy stored in battery: 220mAh x 3.7V x 3.6 seconds = 2930 J

Life of battery = (2930 J x (1,000,000 uJ/J)) / ((24.30 uJ/advertisement) x (1 advertisement / 0.5 seconds)) x 0.7

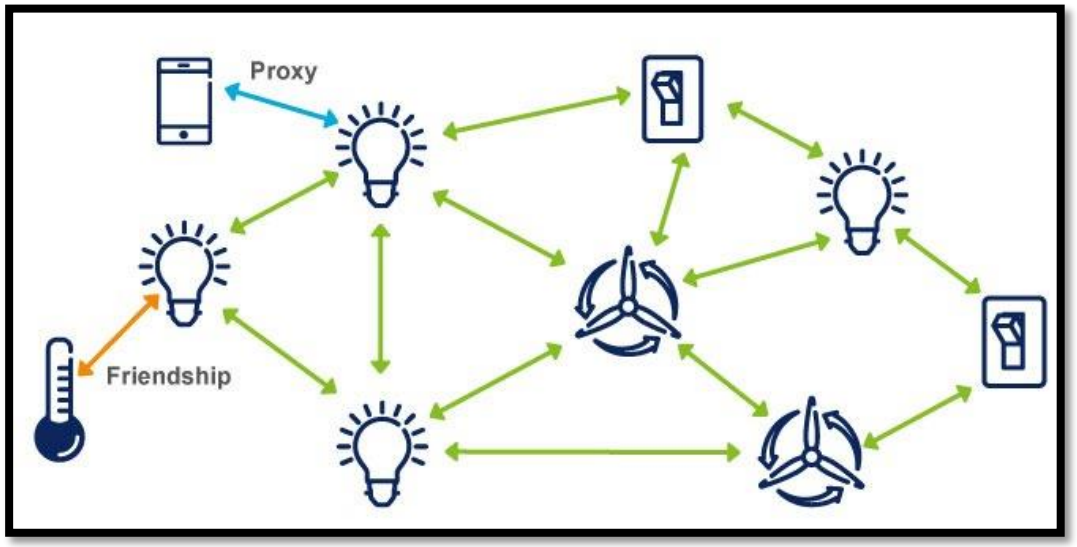
= 42,201,646 seconds = 488 days = 1.3 years

Bluetooth Mesh

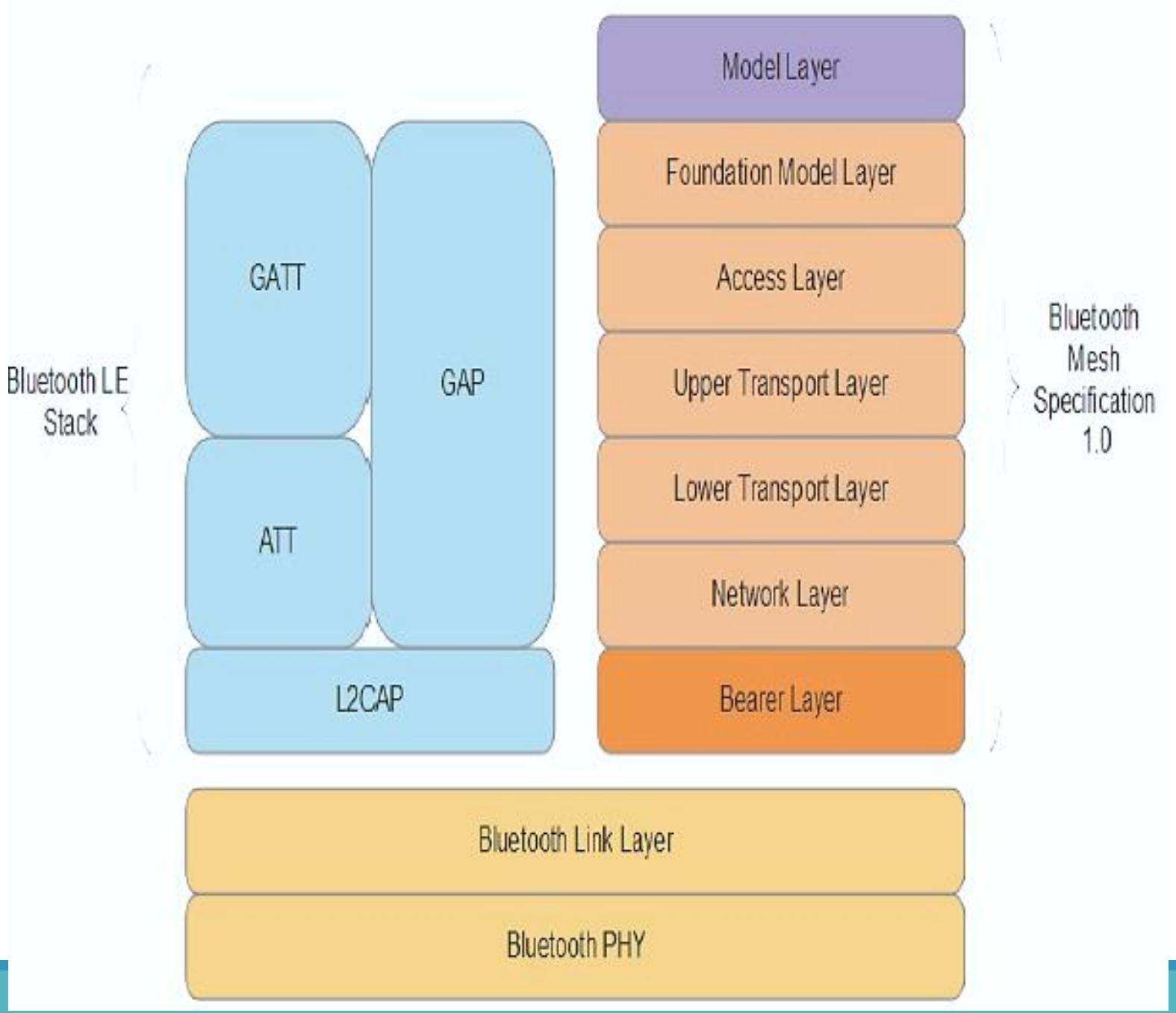
BLE – One to one communication
Bluetooth beacon – One to many
Bluetooth Mesh – Many to Many

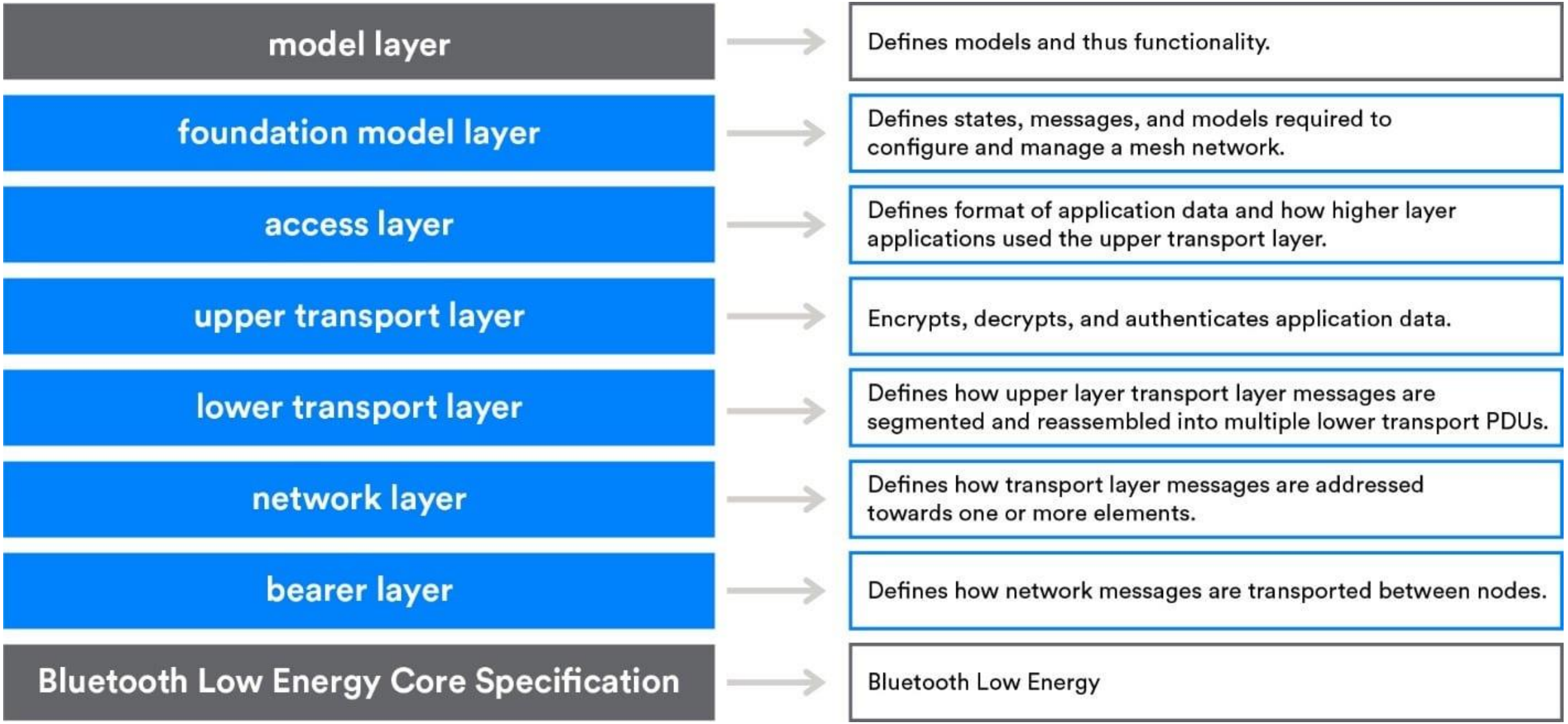


Mesh – The devices are able to relay messages to other devices so that the end-to-end communication range is extended far beyond the radio range of each individual node



https://www.novelbits.io/bluetooth-mesh-tutorial-part-2/


Model Layer
Foundation Model Layer
Access Layer
Upper Transport Layer
Lower Transport Layer
Network Layer
Bearer Layer
Bluetooth Mesh Specification 1.0
GATT
GAP
ATT
L2CAP
Bluetooth LE Stack
Bluetooth Link Layer
Bluetooth PHY

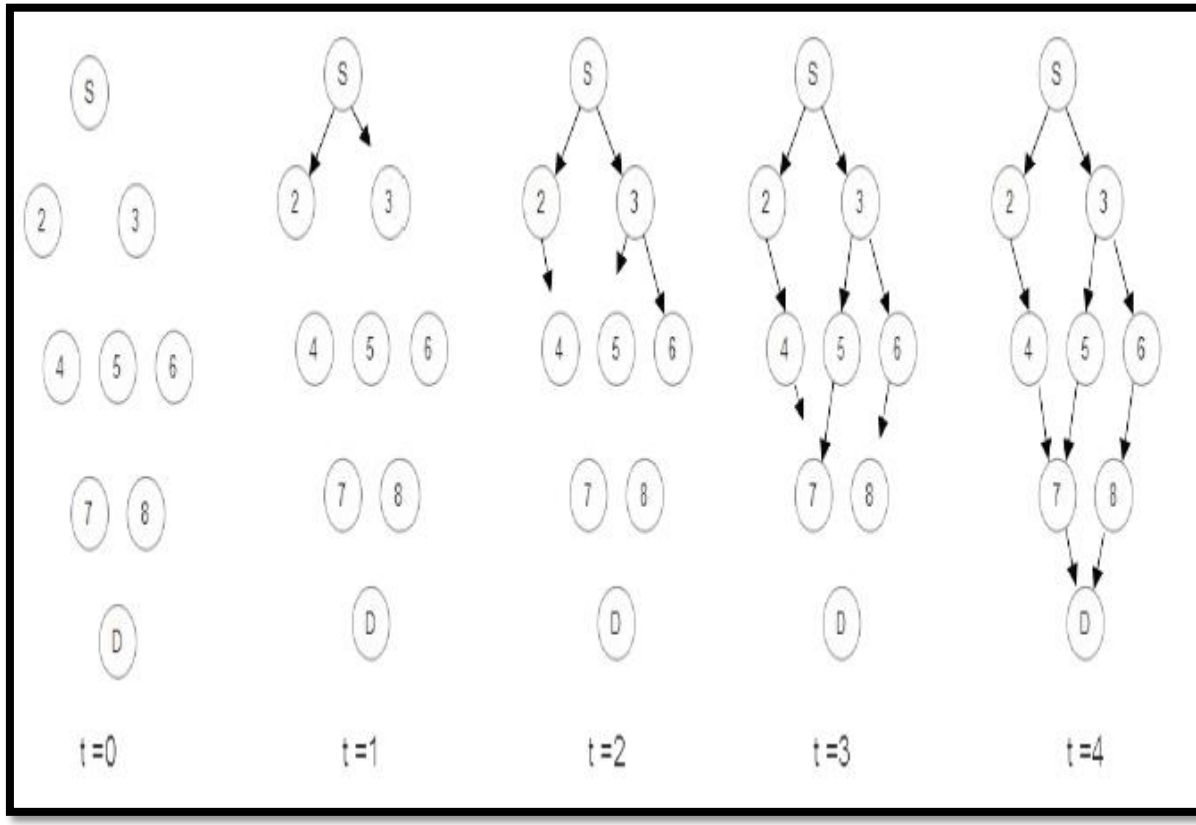

model layer
Defines models and thus functionality.
foundation model layer
Defines states, messages, and models required to configure and manage a mesh network.
access layer
Defines format of application data and how higher layer applications used the upper transport layer.
upper transport layer
Encrypts, decrypts, and authenticates application data.
lower transport layer
Defines how upper layer transport layer messages are segmented and reassembled into multiple lower transport PDUs.
network layer
Defines how transport layer messages are addressed towards one or more elements.
bearer layer
Defines how network messages are transported between nodes.
Bluetooth Low Energy Core Specification
Bluetooth Low Energy

Models: Implements behaviors, states, and bindings on one or more model specifications.
Foundation models: Configuration and management of the mesh network.
Access layer: Defines format of application data, encryption process, and data verification.
Upper transport layer: Manages the authentication, encryption, and decryption of data passing to and from the access layer. Transports control messages such as friendships and heartbeats.
Lower transport layer: Performs **segmentation and reassembly** (**SAR**) of fragmented PDUs if necessary.
Network layer: Manages the various address types and supports many bearers.
Bearer layer: Defines how mesh PDUs are handled.

Two types of PDUs are supported: advertising bearer and GATT bearer.
The advertising bearer handles the transmission and reception of mesh PDUs, while the GATT bearer provides a proxy for devices that don't support the advertising bearer.
BLE: The complete Bluetooth LE specification.

Bluetooth Mesh Topology

- Based Flooding network concept
- Flooding delivers the message based on routing table
- No central manager requires (compared to Wi-Fi)
- Tree based routing needs central controller
- Adaptive routing table - Proactive and reactive routing tables (Similar to WSN)
- Issues: bandwidth waste, congestion, duplication
- Time to live field in every packet



Bluetooth Mesh – Type of Nodes

Provisioning is a secure procedure which results in an unprovisioned device possessing a series of encryption keys and being known to the Provisioner device.

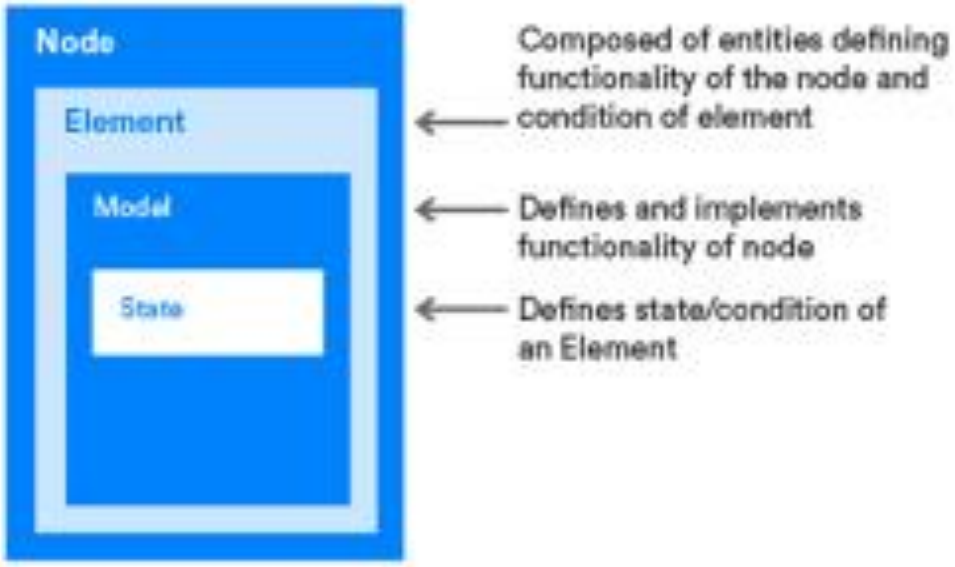
Nodes: These are Bluetooth devices that have been previously provisioned and are members of a mesh.

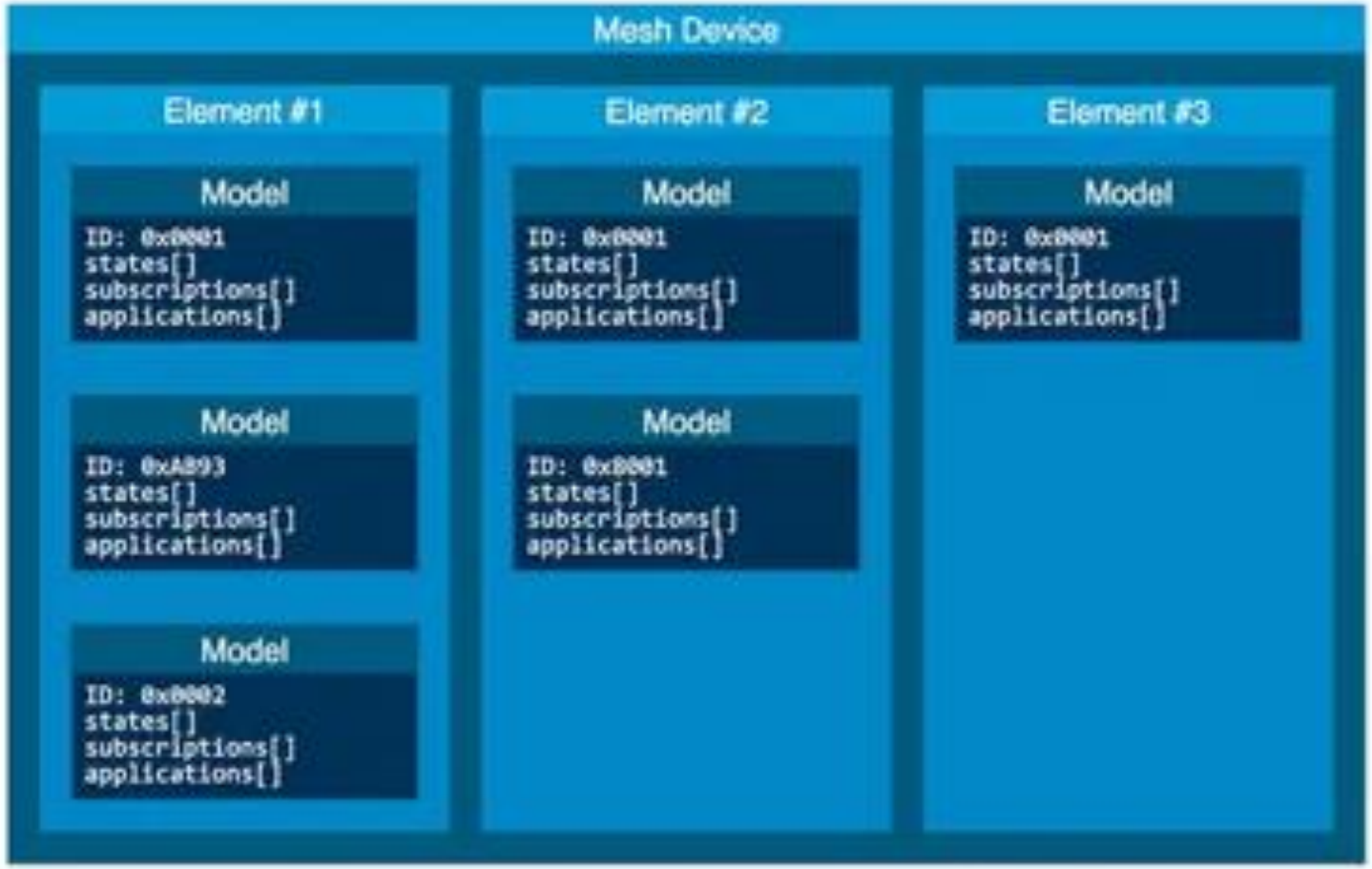
Unprovisioned devices: These are devices with the potential to join a mesh fabric that is not yet part of a mesh and has not been provisioned.

Elements: A node with multiple constituent parts. Each part can be independently controlled and addressed. An example could be a Bluetooth node with temperature, humidity, and lumens sensors. This would be a single node (sensor) with three elements.

Mesh gateway: A node that can translate messages between the mesh and a non-Bluetooth technology.

Node, Element, Model and State

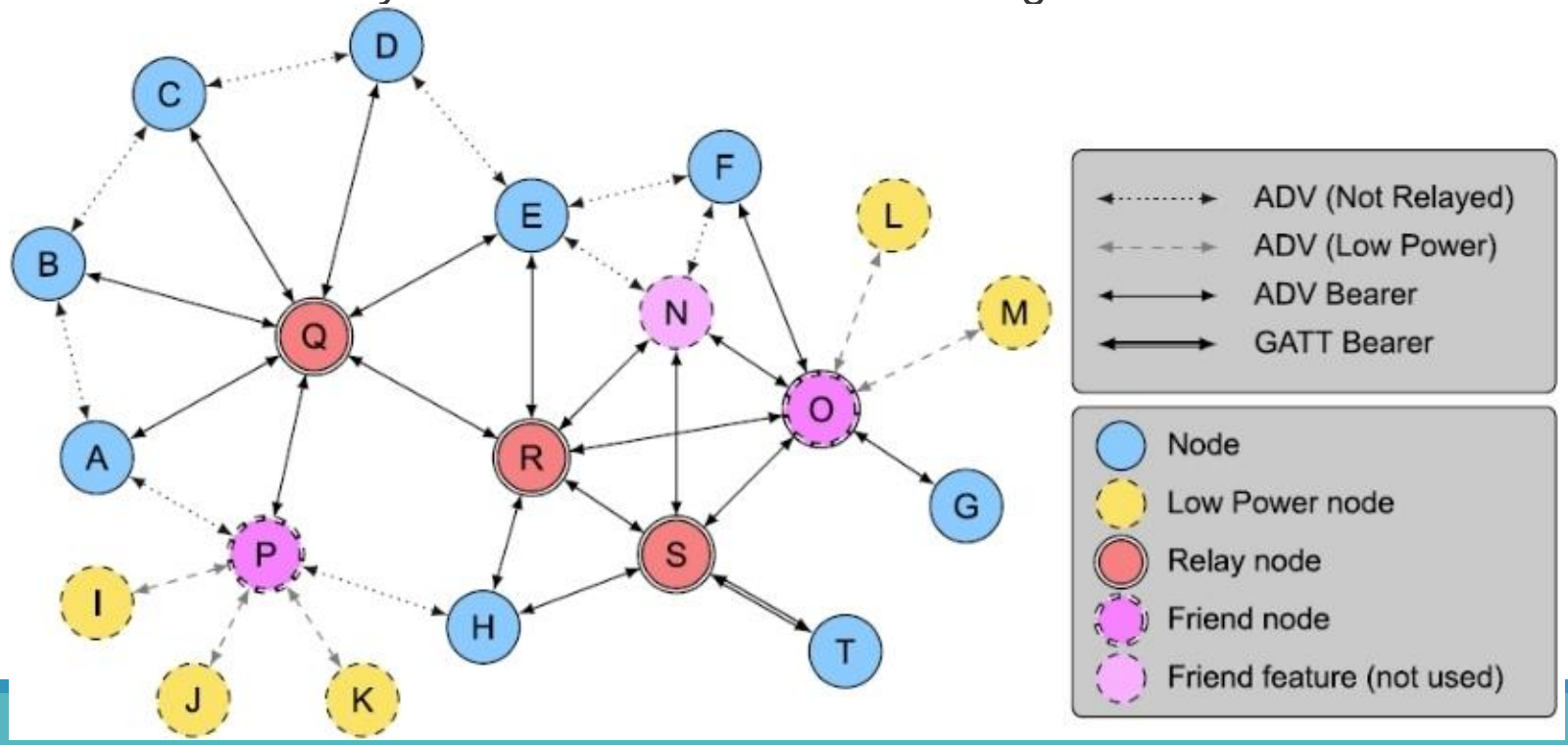




Bluetooth Mesh – Role of Nodes

Relay: A node that supports relay is termed a *relay node* and can retransmit messages received.
Proxy: Allows for Bluetooth LE devices that do not support Bluetooth mesh natively to interact with nodes on the mesh.
Low power: Some nodes on the mesh need to obtain extremely low levels of power consumption. That type of device cannot be placed in a listening mode. The node enters a role termed the **low power node** (**LPN**), which pairs it with a friend node. The LPN enters a deep sleep state and polls the associated friend for any messages that may have arrived while it was sleeping.
Friend: The friend node is associated with the LPN but is not necessarily power constrained like an LPN. A friend may use a dedicated circuit or wall power. The friend's duty is to store and buffer messages destined for the LPN until the LPN.

- Cache massages
- Time to Live field
- Heartbeat message



Bluetooth Mesh – Addressing

Unicast addressing: Uniquely identifies a single element in the mesh. The address is assigned during the provisioning process.

Group addressing: This is a form of multicast addressing that can represent one or more elements.

Virtual addressing: An address can be assigned to more than one node and more than one element. Virtual addressing uses a 128-bit UUID.

The Bluetooth mesh protocol starts with 384-byte long messages that are segmented into 11-byte parcels. All communication in a Bluetooth mesh is message-orientated.

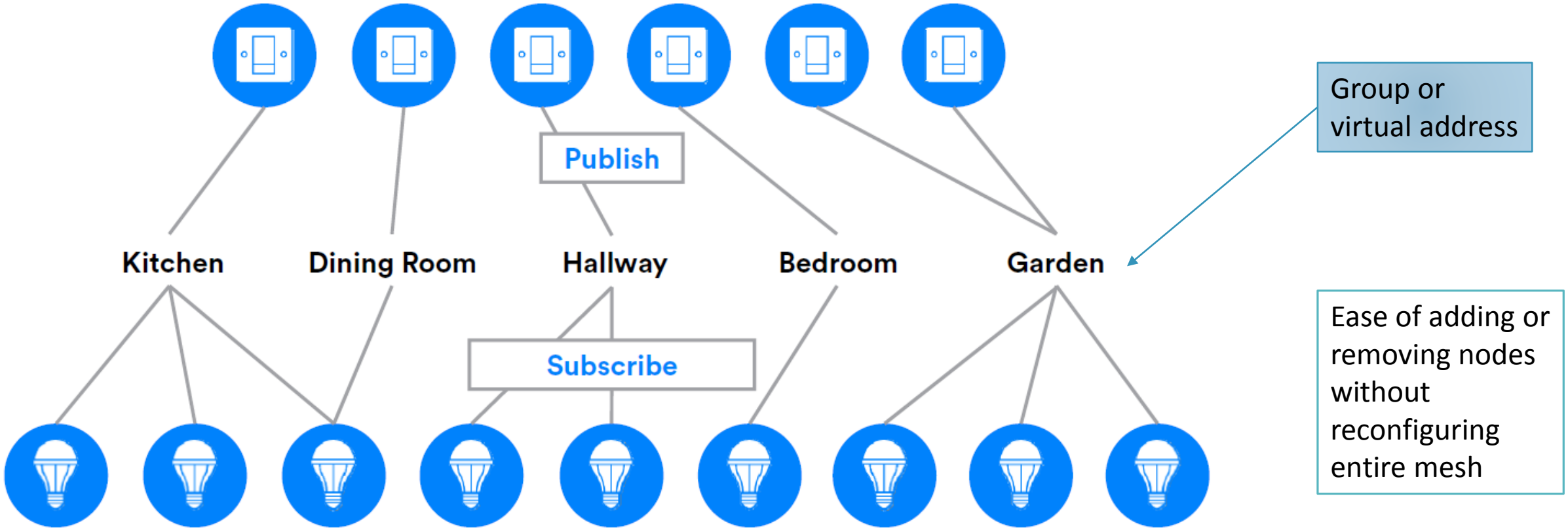
There are two forms of messages:

Acknowledged messages: These require a response from node(s) that receive the message. The acknowledgment also includes data that the originator requested in the original message. Therefore, this acknowledged message serves dual purposes.

Unacknowledged messages: These do not require a response from the receiver.

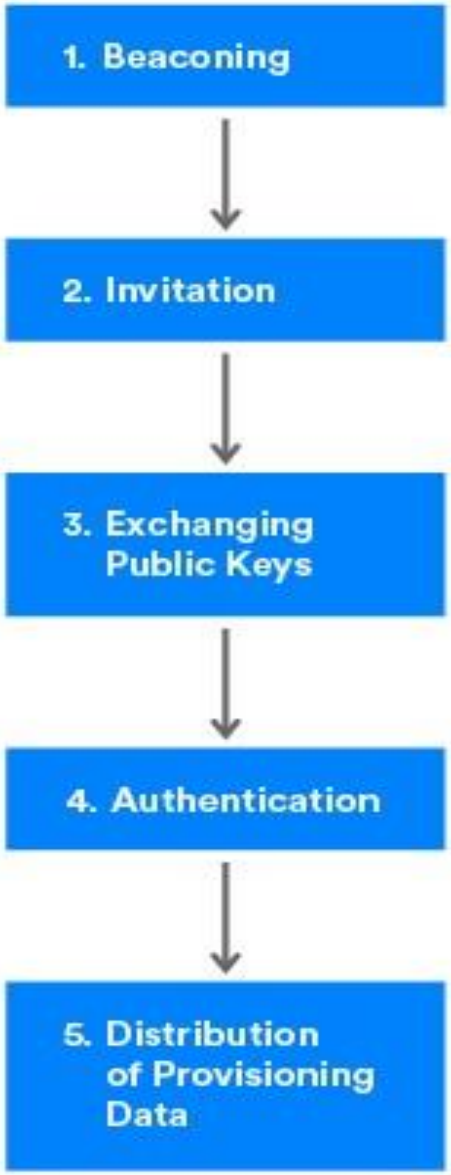
Bluetooth Mesh – Publish-Subscribe

- The act of sending a message is known as publishing.
- Nodes are configured to select messages sent to specific addresses for processing, and this is known as subscribing.



Bluetooth Mesh – Provisioning

- An unprovisioned device broadcasts a mesh beacon advertising packet.
- The provisioner sends an invitation to the device.
- The provisioner and device exchange public keys.
- The unprovisioned device outputs a random number to the user. The user enters the digits (or identity) into the provisioner and a cryptographic exchange starts to complete the authentication phase.
- A session key is derived by each of the two devices from the private key and the exchanged public keys.
- The device changes state from an unprovisioned device to a node and is now in possession of the NetKey, a unicast address, and a mesh security parameter called the IV index



Zigbee

ZigBee™ Alliance
Wireless Control That Simply Works

- ZigBee is a technological standard designed for control and sensor networks
- Based on the IEEE 802.15.4 Standard
- Created by the ZigBee Alliance –
  - Organization defining global standards for reliable, cost-effective, low power wireless applications
  - A consortium of end users and solution providers,
  - Developing applications and network capability utilizing the 802.15.4 packet delivery mechanism
- Zigbee is proprietary and closed standard. It requires a licensing fee and agreement provided by the Zigbee Alliance

ZIGBEE PROMOTERS

ZigBee and Bluetooth Comparison

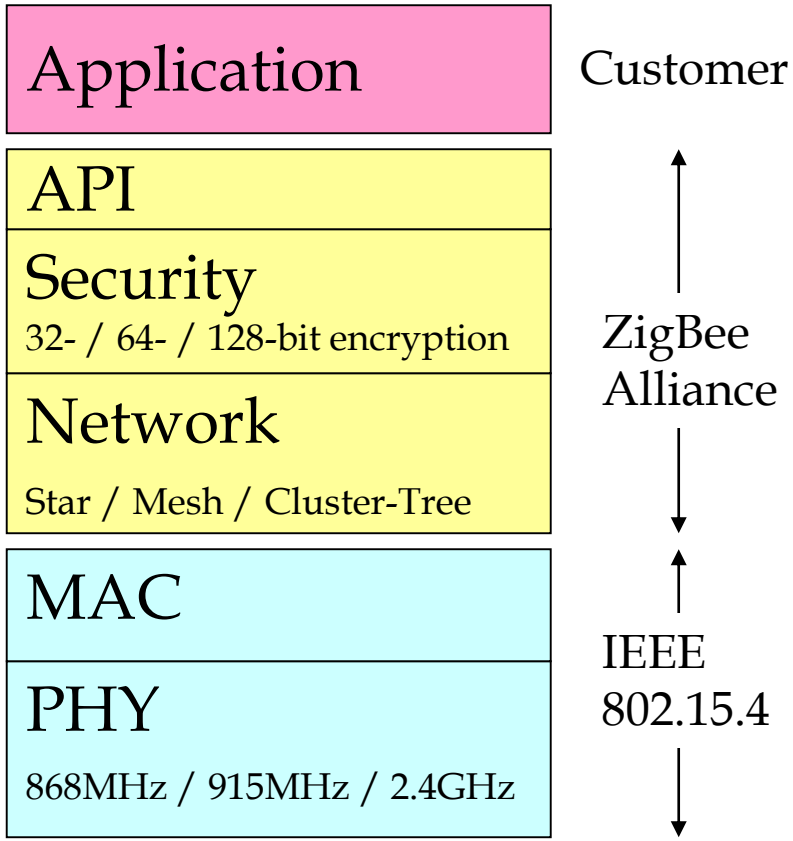
Feature(s)	Bluetooth	ZigBee
Power Profile	days	years
Complexity	Complex	Simple
Nodes/Master	7	64000
Latency	10 seconds	30 ms – 1s
Range	10m	70m ~ 300m
Extendibility	No	Yes
Data Rate	1 Mbps	250 Kbps
Security	64bit, 128bit	128bit AES and Application Layer
Optimizes for	Large packets over small network	Smaller packets over large network

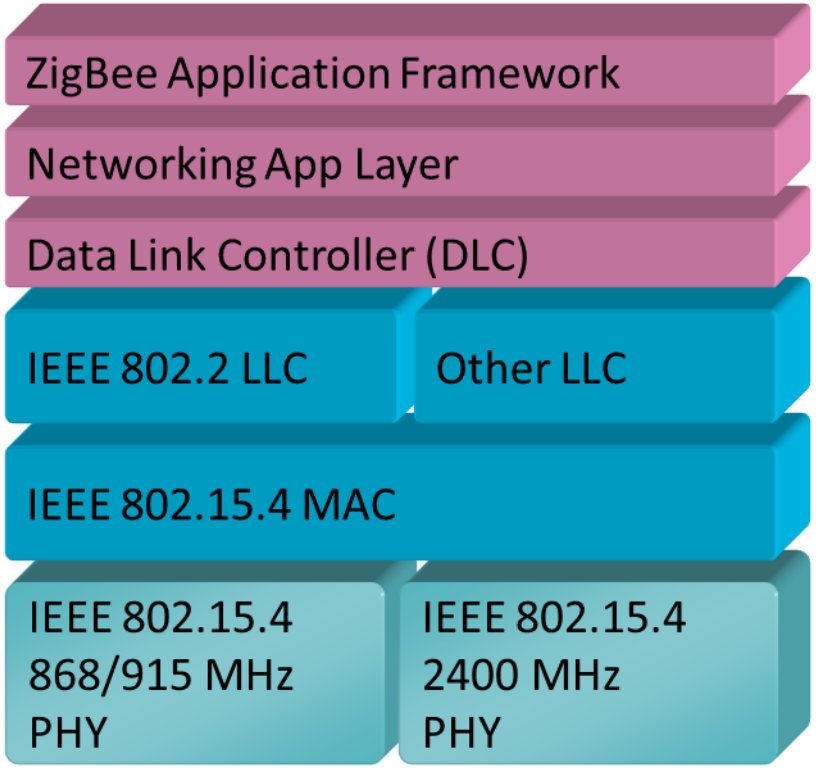
ZigBee and Bluetooth Comparison

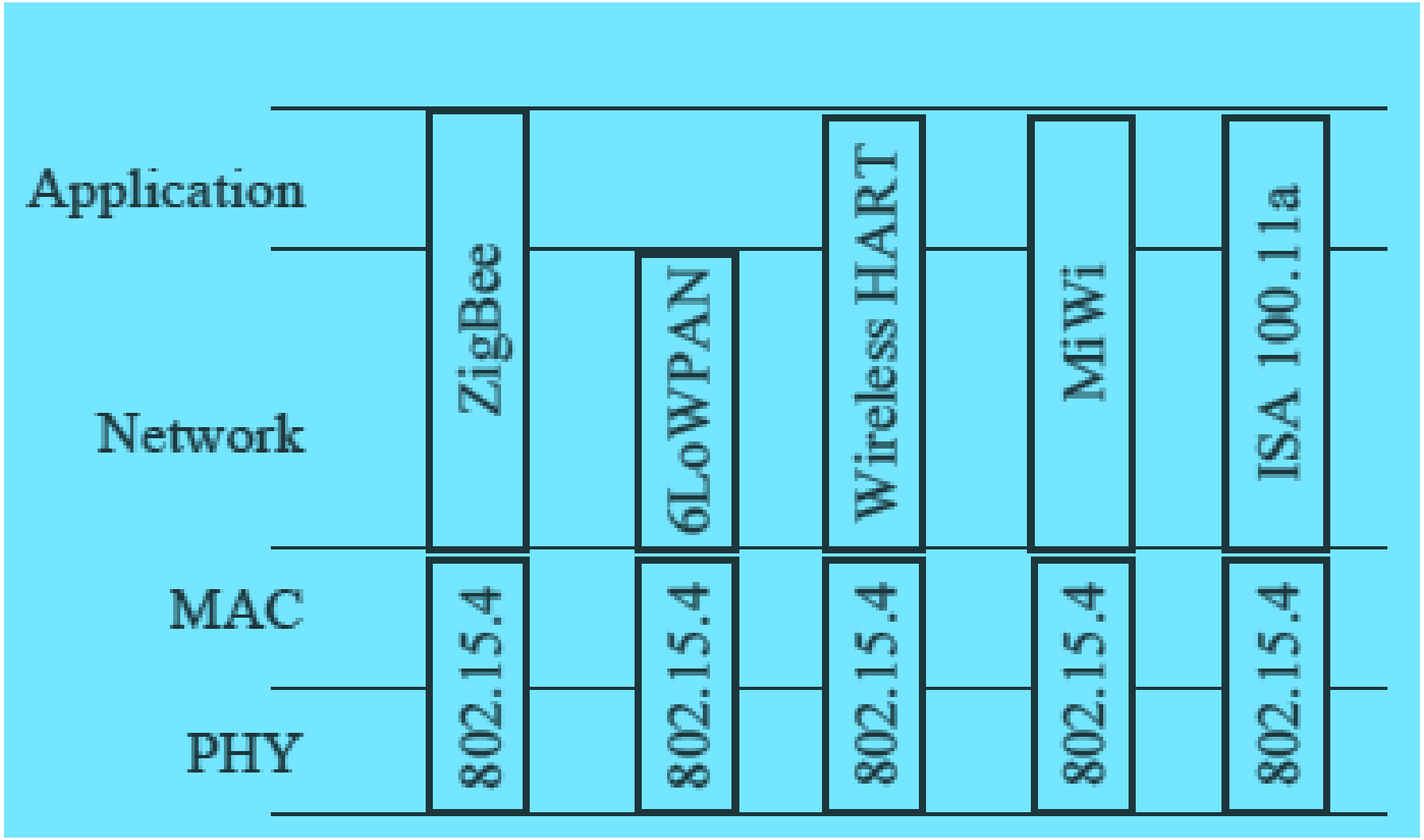
Optimized for different applications

- ZigBee
  - Smaller packets over large network
  - Mostly Static networks with many, infrequently used devices
  - Home automation, toys, remote controls, etc.
- Bluetooth
  - Larger packets over small network
  - Ad-hoc networks
  - File transfer
  - Screen graphics, pictures, hands-free audio, Mobile phones, headsets, PDAs, etc.

ZigBee/IEEE 802.15.4 Stack Architecture







Used by several “Internet of Things” protocols:
ZigBee, 6LowPAN, Wireless HART, MiWi, and ISA 100.11a

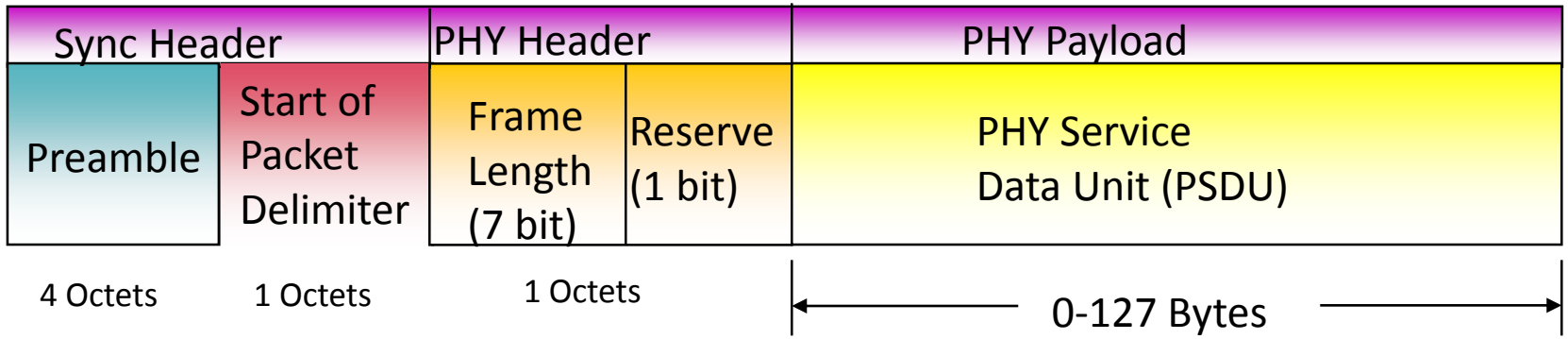
IEEE 802.15.4 Physical Layer

PHY functionalities:

- Activation and deactivation of the radio transceiver
- Energy detection within the current channel
- Link quality indication for received packets
- Clear channel assessment for CSMA-CA
- Channel frequency selection
- Data transmission and reception

PHY packet fields

- Preamble (32 bits) – synchronization
- Start of packet delimiter (8 bits) – shall be formatted as “11100101”
- PHY header (8 bits) –PSDU length
- PSDU (0 to 127 bytes) – data field

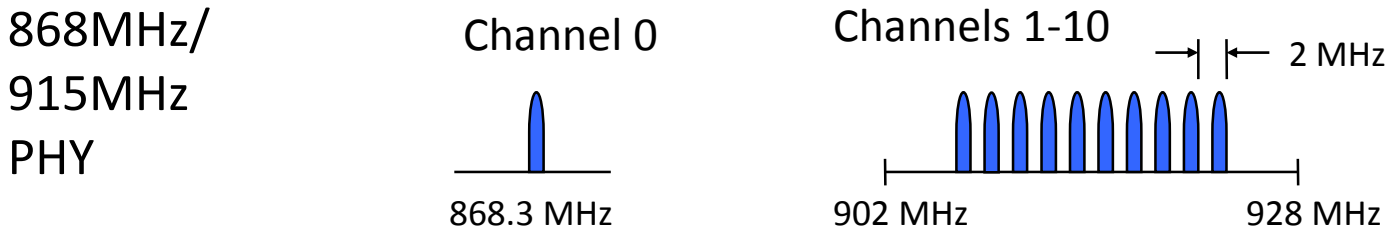


Operating frequency bands

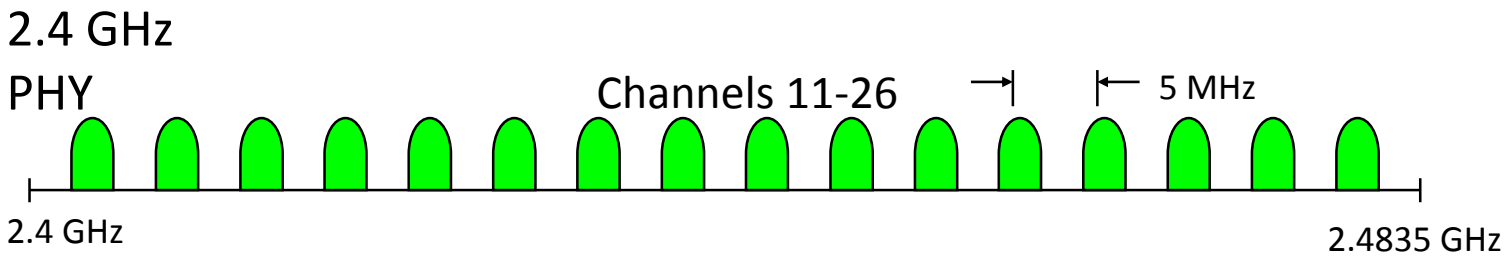
802.15.4 PHY

The standard specifies two PHYs :

- 868 MHz/915 MHz direct sequence spread spectrum (DSSS) PHY (11 channels)
  - 1 channel (20Kb/s) in European 868MHz band
  - 10 channels (40Kb/s) in 915 (902-928)MHz ISM band



- 2450 MHz direct sequence spread spectrum (DSSS) PHY (16 channels)
  - 16 channels (250Kb/s) in 2.4GHz band



802.15.4 PHY

OPTIONS FOR FREQUENCY ASSIGNMENTS

Geographical regions	Europe	Americas	Worldwide
Frequency assignment	868 to 868.6 MHz	902 to 928 MHz	2.4 to 2.4835 GHz
Number of channels	1	10	16
Channel bandwidth	600 kHz	2 MHz	5 MHz
Symbol rate	20 ksymbols/s	40 ksymbols/s	62.5 ksymbols/s
Data rate	20 kbits/s	40 kbits/s	250 kbits/s
Modulation	BPSK	BPSK	Q-QPSK

IEEE 802.15.4 MAC Layer

Traffic Type

- Periodic data
  - e.g. sensors
- Intermittent data
  - e.g. light switch
- Repetitive low latency data
  - e.g. mouse

Device Classes

Full function device (FFD)

Can function in any topology

Capable of being Network coordinator

Can talk to any other device (FFD/RFD)

Reduced function device (RFD)

Limited to star topology

Cannot become network coordinator

Talks only to FFDs

IEEE 802.15.4 MAC Layer

Frame Types

- Data Frame
  - used for all transfers of data
- Beacon Frame
  - used by a coordinator to transmit beacons
- Acknowledgment Frame
  - used for confirming successful frame reception
- MAC Command Frame
  - used for handling all MAC peer entity control transfers

Transmission Mode

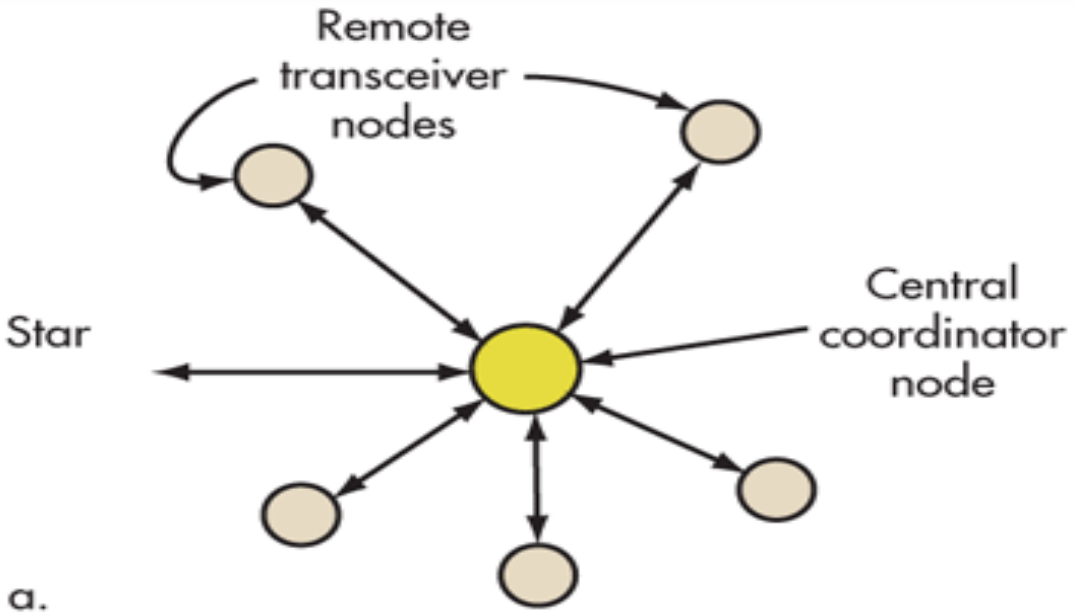
Slotted (Beacon enable mode)

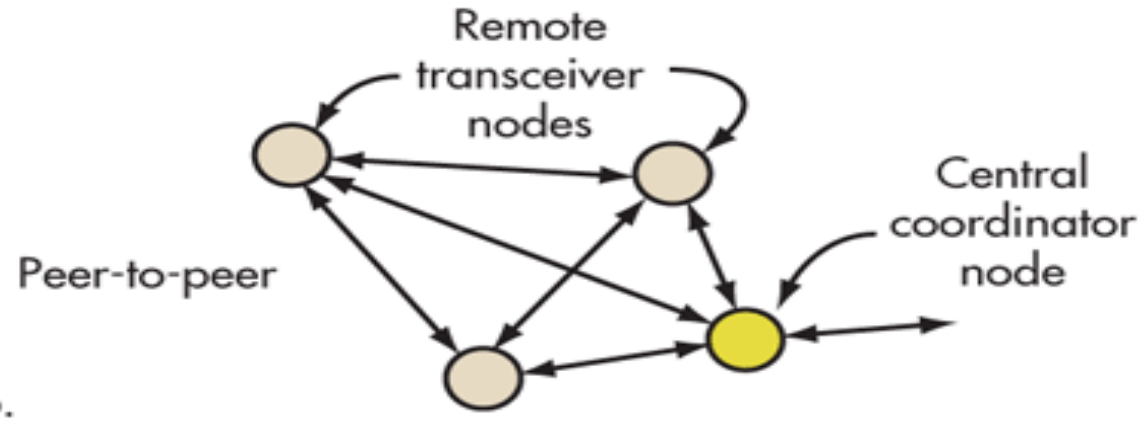
Periodic data and Repetitive low latency data

Un-slotted (Non-Beacon enable mode)

Intermittent data

802.15.4 – Network Topology





ZigBee Network Topologies

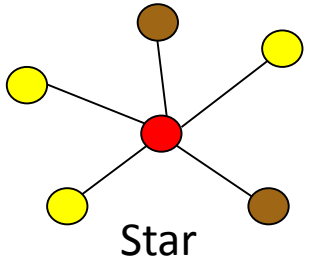
Star Topology

Advantage

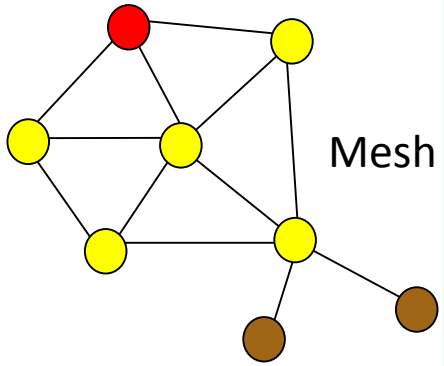
- Easy to synchronize
- Low latency

Disadvantage

- Small scale



Star



Mesh

Mesh Topology

Advantage

- Robust multihop communication
- Network is more flexible
- Lower latency

Disadvantage

- Route discovery is costly
- Needs storage for routing table

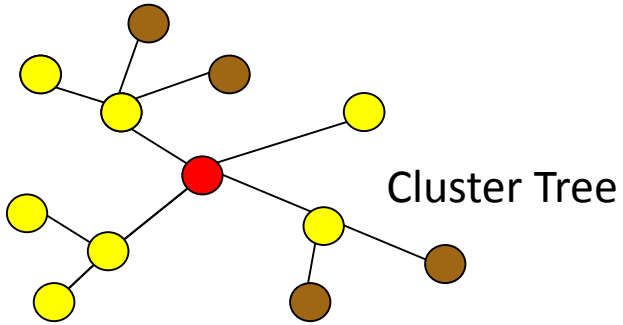
Cluster Tree

Advantage

- Low routing cost
- Allow multihop communication

Disadvantage

- Route reconstruction is costly
- Latency may be quite long



Cluster Tree

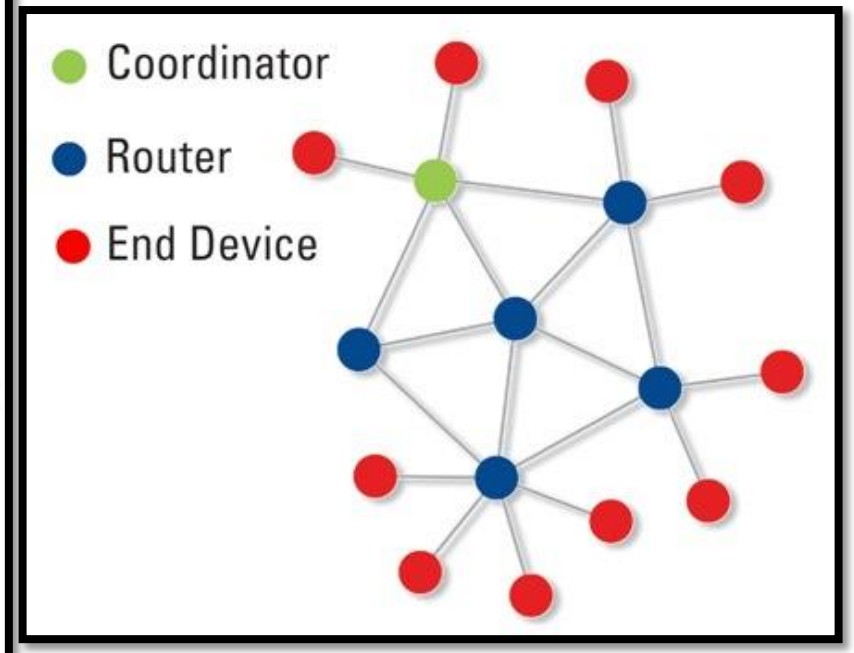
PAN coordinator

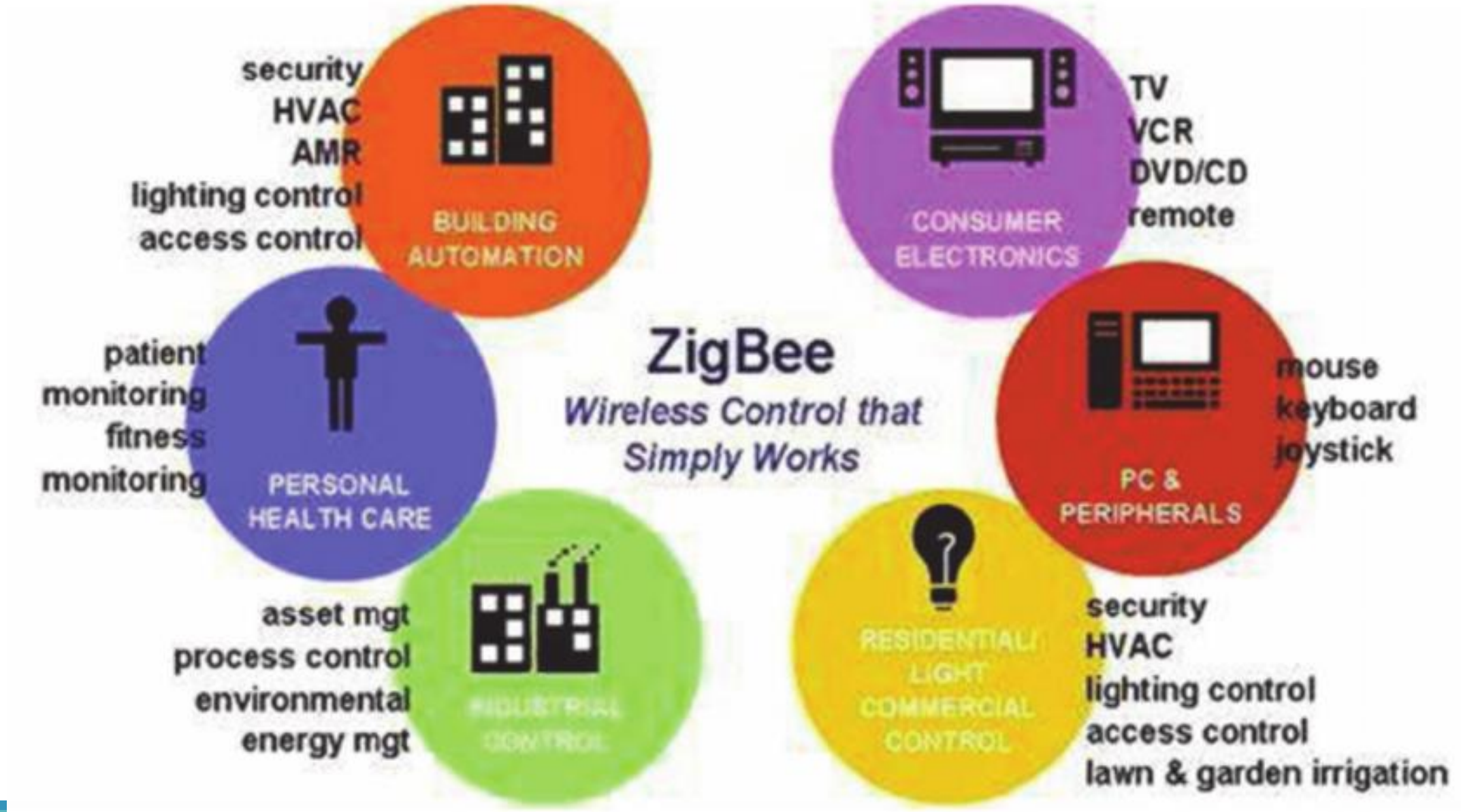
Full Function Device

Reduced Function Device

ZigBee Device Types

- ZigBee Coordinator (ZC)
  - One and only one required for each ZB network.
  - Initiates network formation.
  - Acts as 802.15.4 2003 PAN coordinator (FFD).
  - May act as router once network is formed.
- ZigBee Router (ZR or FFD)
  - Optional network component.
  - May associate with ZC or with previously associated ZR.
  - Acts as 802.15.4 2003 coordinator (FFD).
  - Participates in multihop routing of messages.
- ZigBee End Device (ZED or RFD)
  - Optional network component.
  - Shall not allow association.
  - Shall not participate in routing.




security
HVAC
AMR
lighting control
access control
BUILDING AUTOMATION
TV
VCR
DVD/CD
remote
CONSUMER ELECTRONICS
patient monitoring
fitness monitoring
PERSONAL HEALTH CARE
ZigBee
Wireless Control that Simply Works
mouse
keyboard
joystick
PC & PERIPHERALS
asset mgt
process control
environmental
energy mgt
INDUSTRIAL CONTROL
RESIDENTIAL/ LIGHT COMMERCIAL CONTROL
security
HVAC
lighting control
access control
lawn & garden irrigation

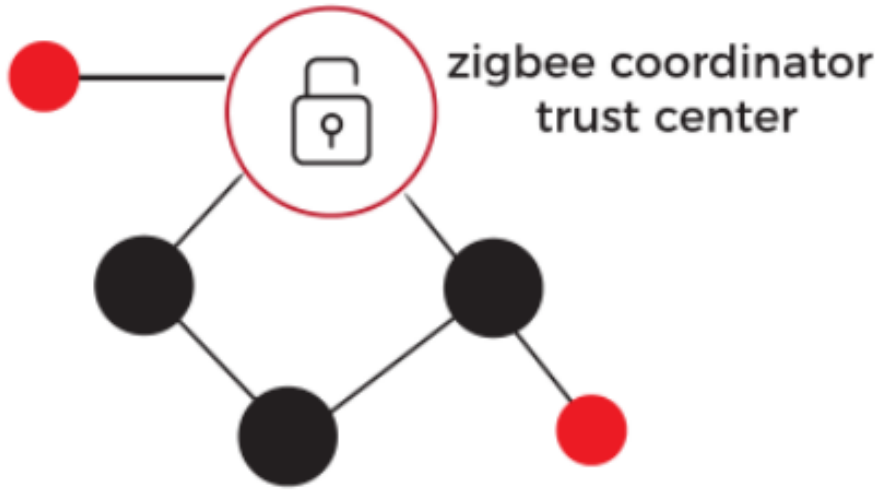
Security

- Zigbee provides three security mechanisms:
  - Access Control Lists (ACL)
  - 128-bit AES encryption
  - Message freshness timers
- Multiple keys:
  - **Master key**: The master key may be pre-installed by a manufacturer or entered by a manual process with the user.
  - **Network key**: This key will provide protection at a network level for outside attackers.
  - **Link key**: This forms a secure binding between two devices

Zigbee uses 128-bit keys as part of its specification within the MAC and NWK layers.

The MAC layer provides three modes of encryption - AES-CTR, AES-CBC-128, and AES-CCM-128

Centralized Security Model

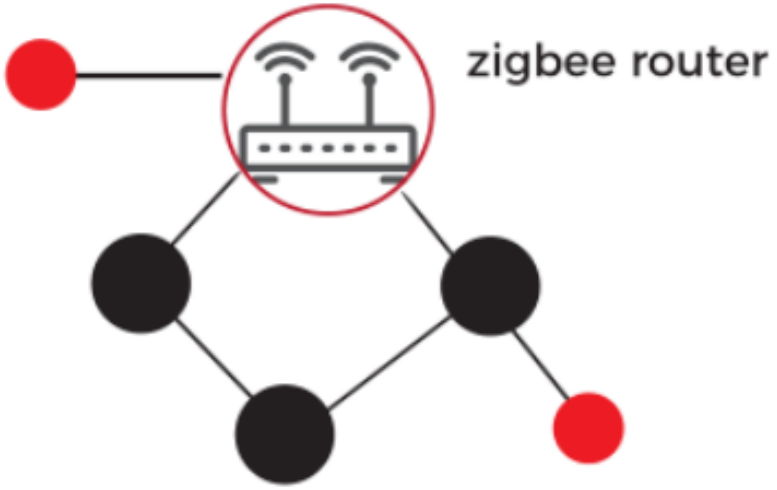


The TC establishes a unique TC Link Key for each device.

Node must support install codes (128 bits of random data + 16 bit CRC).

the Trust Center periodically creates, distributes, and then switches to a new network key.

Distributed Security Model



For easier-to-configure systems .

No Coordinator / Trust Center.

All devices must be pre-configured with a link key to encrypt the network key when a new node joining.

All the devices in the network encrypt messages with the same network key.

Z-Wave

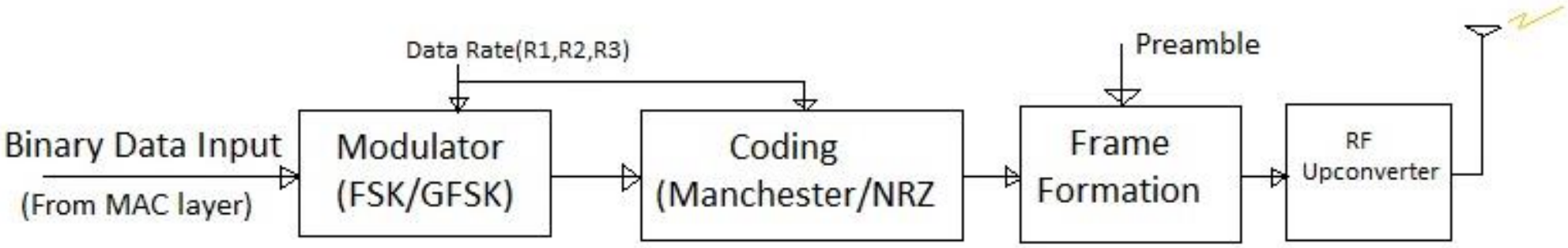
- Zensys a Danish-American company founded in 1999 invented the Z-wave technology.
- Mesh technology in the 900 MHz band.
- For wireless home automation CLOSED protocol
- Efficiency of the Z-Wave Network is because of the Routing Protocol
- More than one Z-Wave Network can co-exist.
- A Z-Wave network can consist of 232 nodes to the max
- Approximately 600 companies and 2200 certified devices


AEON LABS
ARRAYENT
blacksumac
ENERWAVE
Green Automation
FIBARO
Home intelligence
greenWAVE
HomeSeer
Honeywell
Kwikset
Linear
LEVITON
MCO HOME
mios
MITSUMI
NorthQ
poly-control
wireless locking the world
Radio Thermostat
RaZberry
RCS
TECHNOLOGY
Remotec
SCHLAGE
SIGMA
DESIGNS
SmartThings
somfy.
STRATTEC
SYSTECH
CORPORATION
Vera
VISION
WORTHINGTON
DISTRIBUTION
Wintop
Yale
zonoff

	ZigBee	Z-WAVE
TECHNICAL FOUNDATION	IEEE 8.02.15.4 ✓	No International Standard
FOUNDED UNION	Zigbee Alliance	Z-Wave Alliance
FIRST LAUNCHED IN	2013	2013
USE OF BAND	2.4 GHz	Sub 1G
IC PROVIDER	TI, Freescale	Sigma Designs
SENSITIVITY	-98 dBM	-101 dBM
OPERATING RANGE	35-65 ft	100-120 ft ✓
STANDARD DATA RATE	20 Kbps (868 MHz) , 40 Kbps (916 MHz) ✓	9.6 Kbps
MAX. DATA RATE	250 Kbps (2.4 GHz) ✓	100 Kbps
FREQUENCY	915 MHz / 2.4 GHz	908 MHz / 916 GHz ✓
RELIABILITY	BETTER ✓	GOOD
ENCRYPTION	AES 128'	AES 128 ✓

	ZigBee	Z-WAVE
COST TO BUILD DEVICES	LOWER ✓	HIGHER
WORKS IN ALL COUNTRIES	YES ✓	NO
INTEROPERABILITY	GOOD	BETTER ✓
SUBJECT TO WIFI INTER	YES	NO ✓
COMPATIBILE WITH STBS	YES ✓	NO
MAX. NO. OF NODES	65000 ✓	232
PRACTICLE NO. OF NODES	50 ✓	10
MAX. NO. OF HOPS	30 ✓	4
MODULATION	OQPSK	GFSK
TRANSMITTER POWER	8 dBm	0 dBm ✓
LINK BUDGET	106 DBs	101 DBs
NETWORK TYPE	Mesh	Mesh
NETWORK TYPE	UP TO 7 YEARS ✓	12-14 MONTHS

Z-wave PHY



R1= 9.6 Kbps, R2=40 Kbps, R3= 100 Kbps

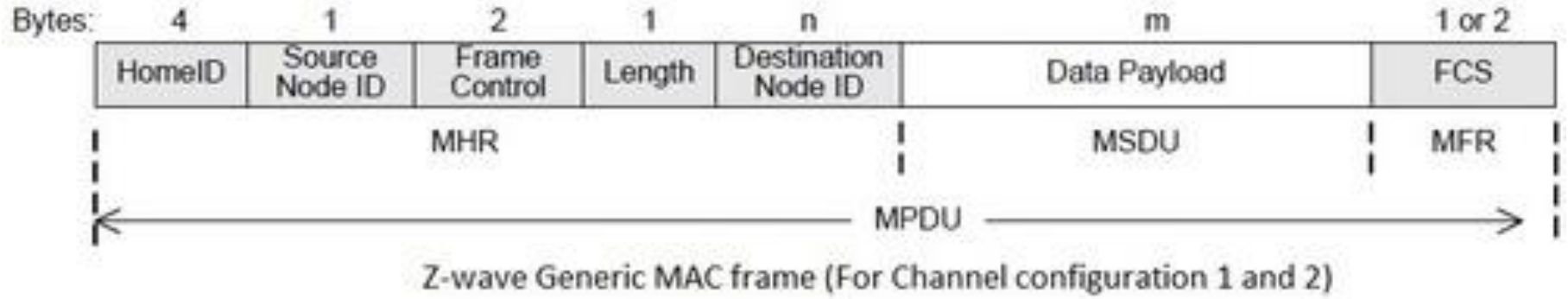
Z-wave Physical Layer Transmitter

Data Rate Designation	Modulation	Coding
R1	FSK	Manchester
R2	FSK	NRZ
R3	GFSK (BT=0.6)	NRZ

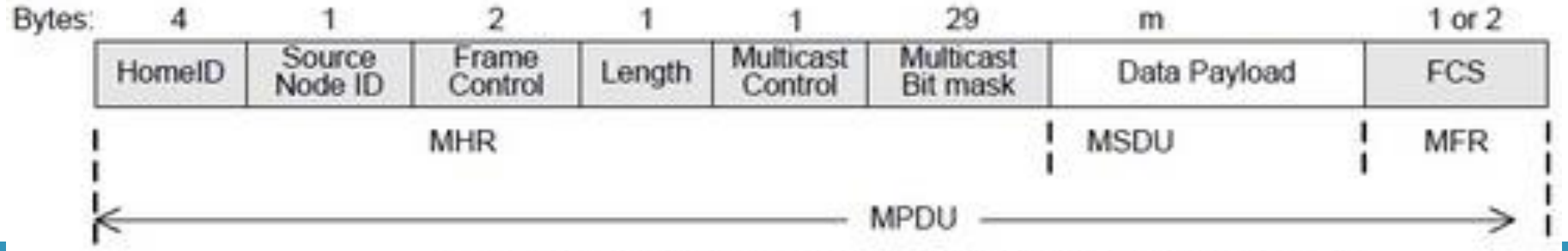
FEATURES

Z-wave MAC

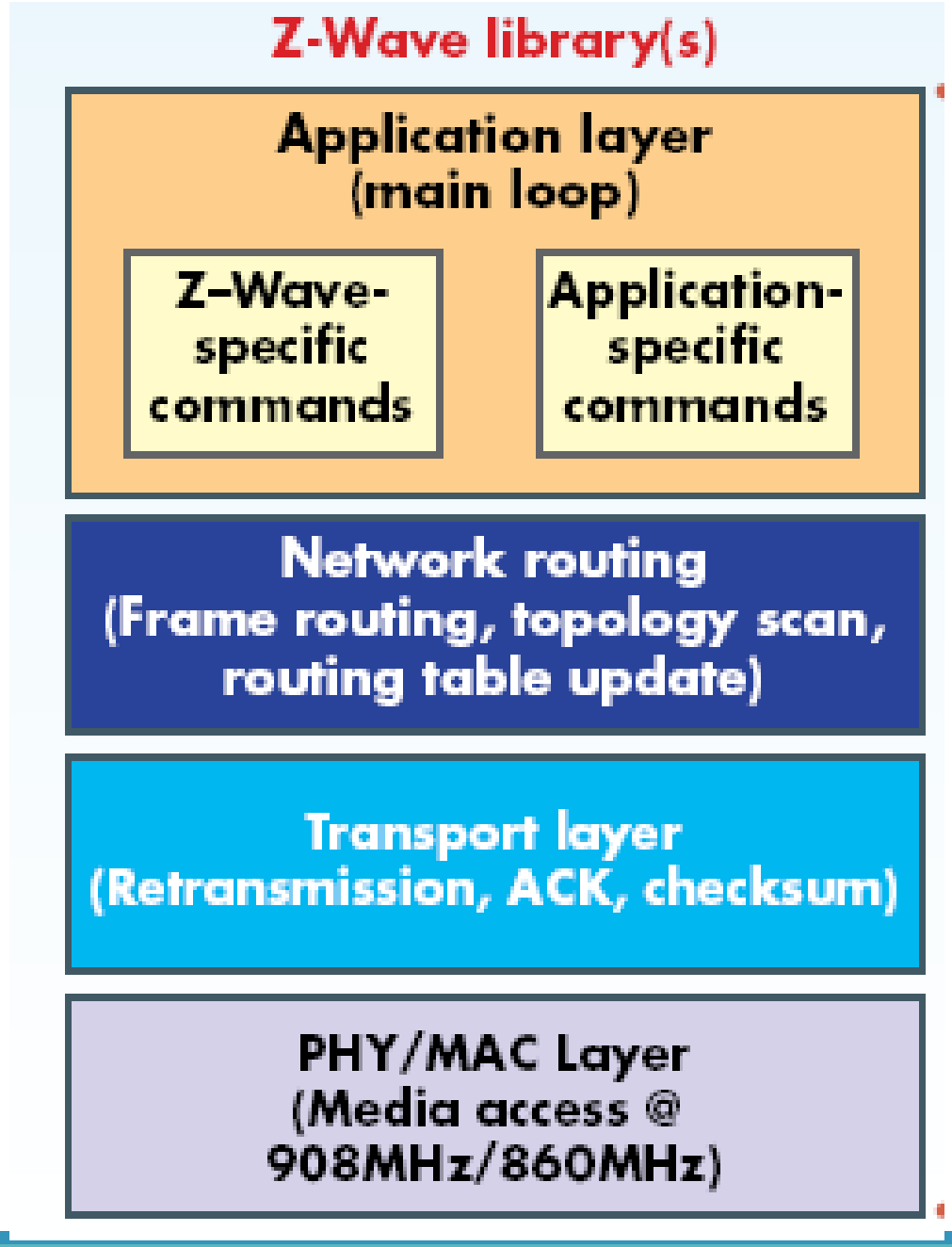
- unique network ID number (HomeID)
- up to 232 nodes in one network
- collision avoidance algorithm
- backoff algorithm
- automatic retransmission for reliable data transfer
- support for low-power operation via dedicated wakeup patterns.



Z-wave Generic MAC frame (For Channel configuration 1 and 2)



Z-wave Multicast MAC frame (For Channel configuration 1 and 2)



Application layer: Provides the user interface to applications and data.

Network layer: This provides routing services. Additionally, the network layer will perform a topology scan and update of the routing tables.

Transport layer: Manages the communication of Z-Wave frames.
Responsible for the retransmission of frames as needed. Additional tasks include acknowledgment of transmissions and checksum binding.

MAC layer: Manages the HomeID and NodeID fields. The MAC layer also uses a collision avoidance algorithm and backoff strategy to alleviate congestion and contention on the channel.

PHY layer: Manages the signal modulation, channel assignment, and preamble binding at the transmitter and preamble synchronization at the receiver.

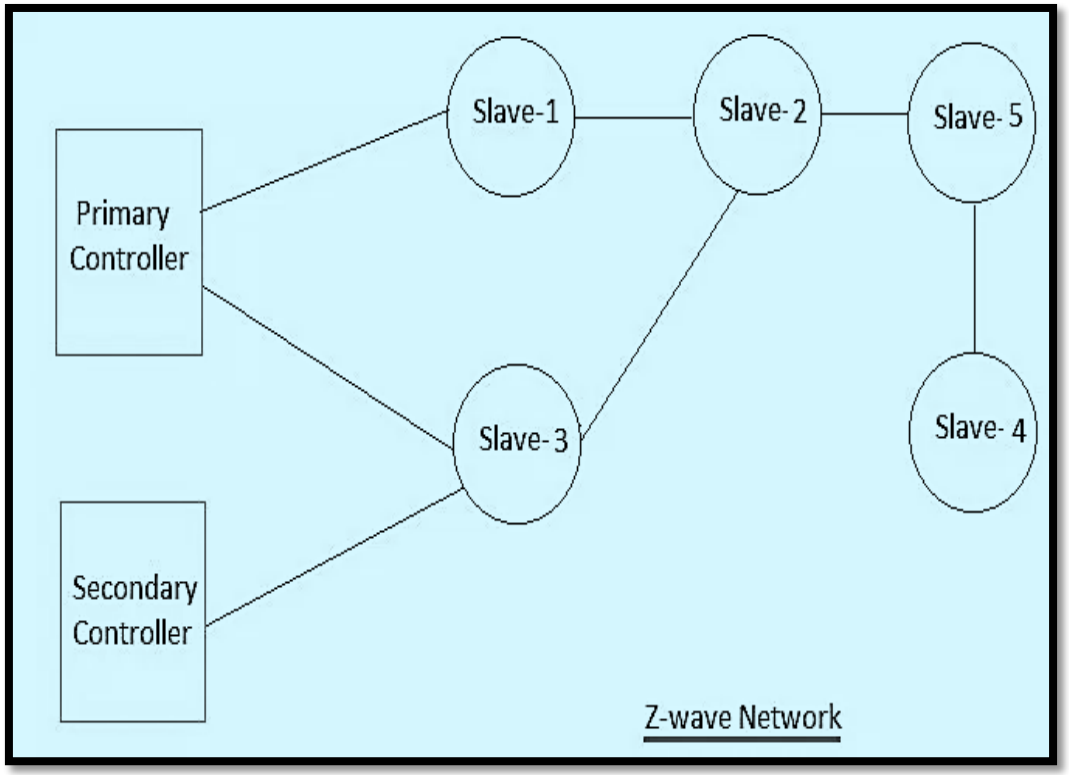
Type of Nodes

Controller device: This top-level device provides the routing table for the mesh network and is the host/master of the mesh under it.

- **Primary controller**: The primary controller is the master, and only a single master can exist in a network.
  - It has the ability to maintain the network topology and hierarchy.
  - It can also include or exclude nodes from the topology.
  - It allocates node IDs.
- **Secondary controller**: These nodes assist a primary controller with routing.

Slave device/node:

- These devices perform actions based on commands they receive.
- These devices cannot communicate with neighbour slave nodes unless instructed to do so via a command.
- Slaves can store routing information but do not compute or update routing tables.
- Acts as a repeater in a mesh.

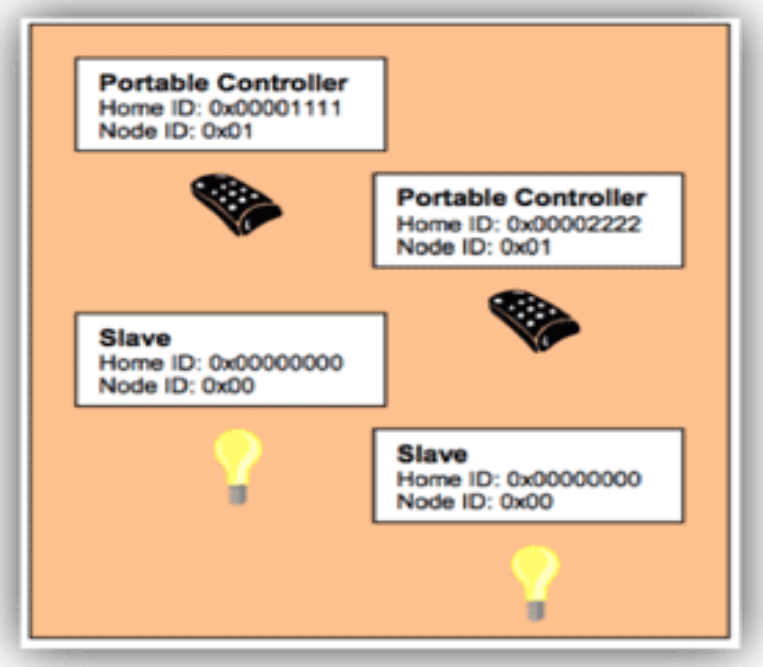


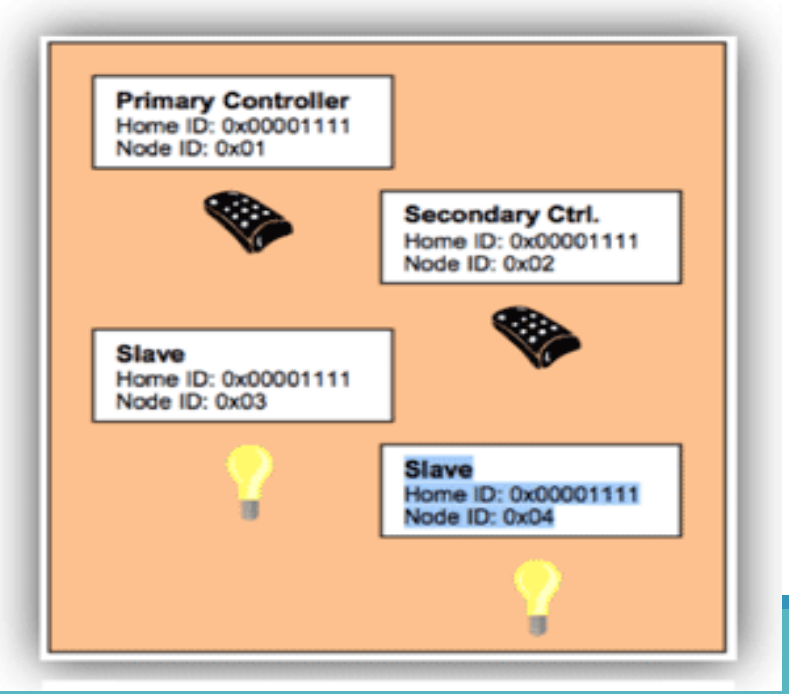
Z-Wave addressing

The addressing scheme is kept simple to minimize traffic and conserve power.

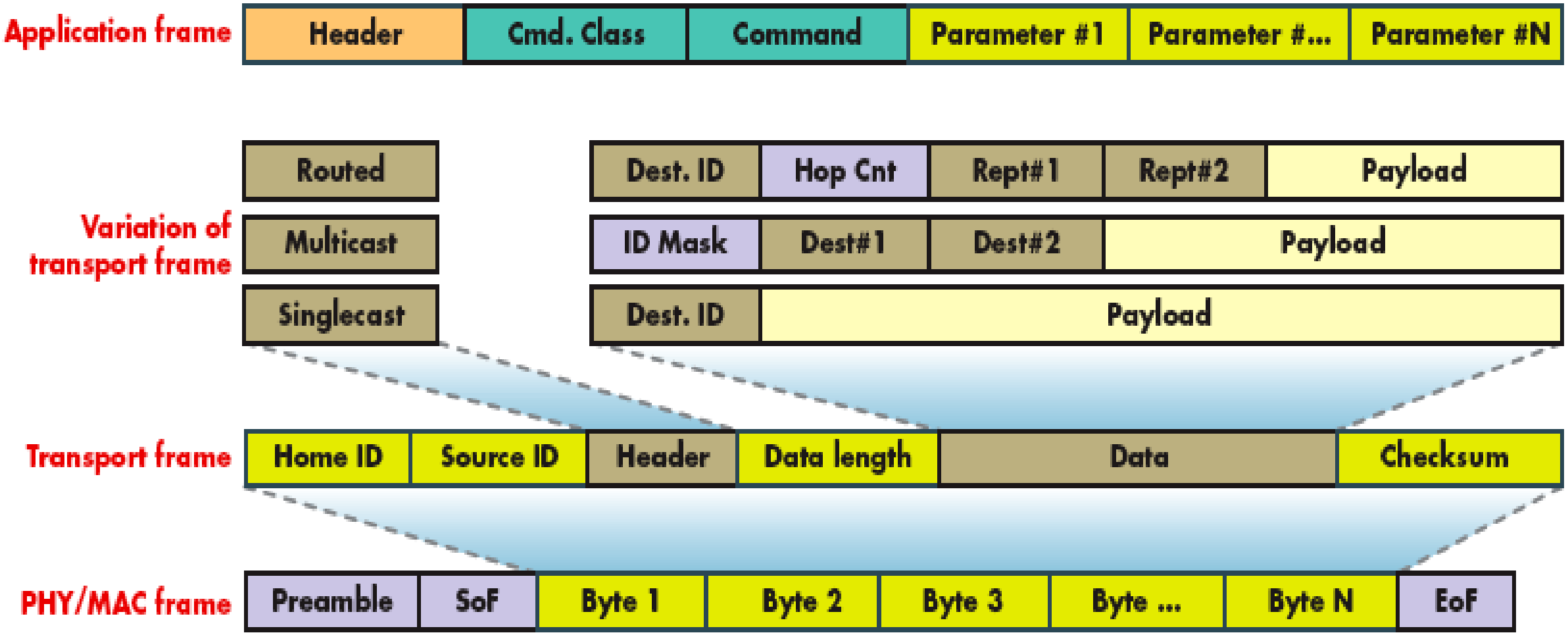
There are two fundamental addressing identifiers:

- **Home ID:**
  - This is a 32-bit unique identifier that is pre-programmed in controller devices to assist with identifying Z-Wave networks from each other.
  - During network start, all Z-wave slaves have a home ID of zero and the controller will systematically populate the slave nodes with the correct home ID.
- **Node ID:**
  - This is an 8-bit value that is assigned to each slave by the controller and provides addressing of slaves in the Z-wave network.





Z-Wave protocol frame structure




Home Control
Energy Conservation
Remote Home Management and Monitoring
Home Entertainment Control
Safety & Security
Comfort and Convenience
Z-WAVE

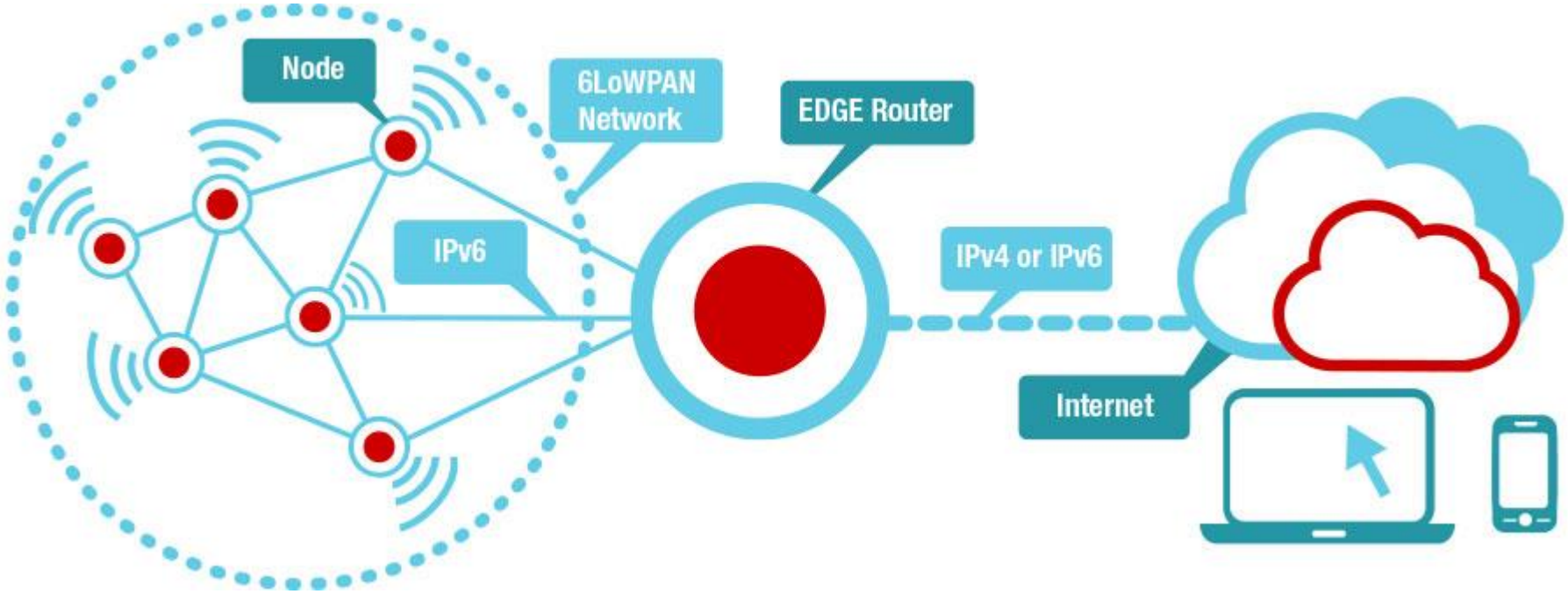

Z-WAVE®

IP-Based WPAN and WLAN

- Internet protocol and transmission control protocol (TCP/IP)
- WPAN with IP – 6LoWPAN
- WPAN with IP – thread
- IEEE 802.11 protocols and WLAN

6LowPAN

IPV6 over low power WPANs

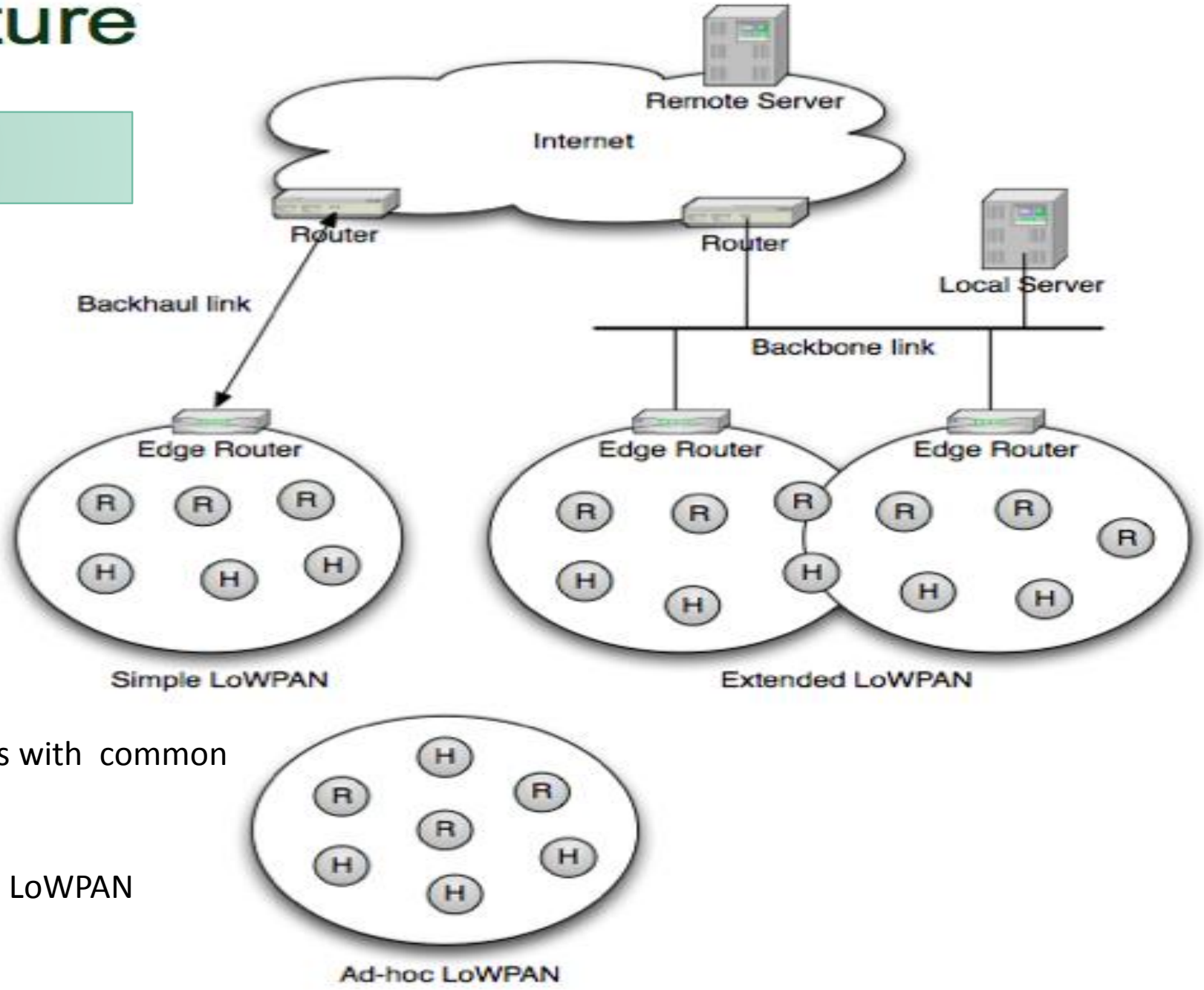


6LoWPAN-Characteristics

1. Small packet size
2. Support for both 16-bit short or IEEE 64-bit extended media access control addresses
3. Low bandwidth. Data rates of 250 kbps, 40 kbps, and 20 kbps for 2.4 GHz, 915 MHz, and 868 MHz, respectively
4. Topologies - star and mesh
5. Low power battery operated
6. Low cost
7. Large in numbers
8. No predefined location. Location keeps on changing
9. Device may sleep for longer time

Architecture

6LowPAN



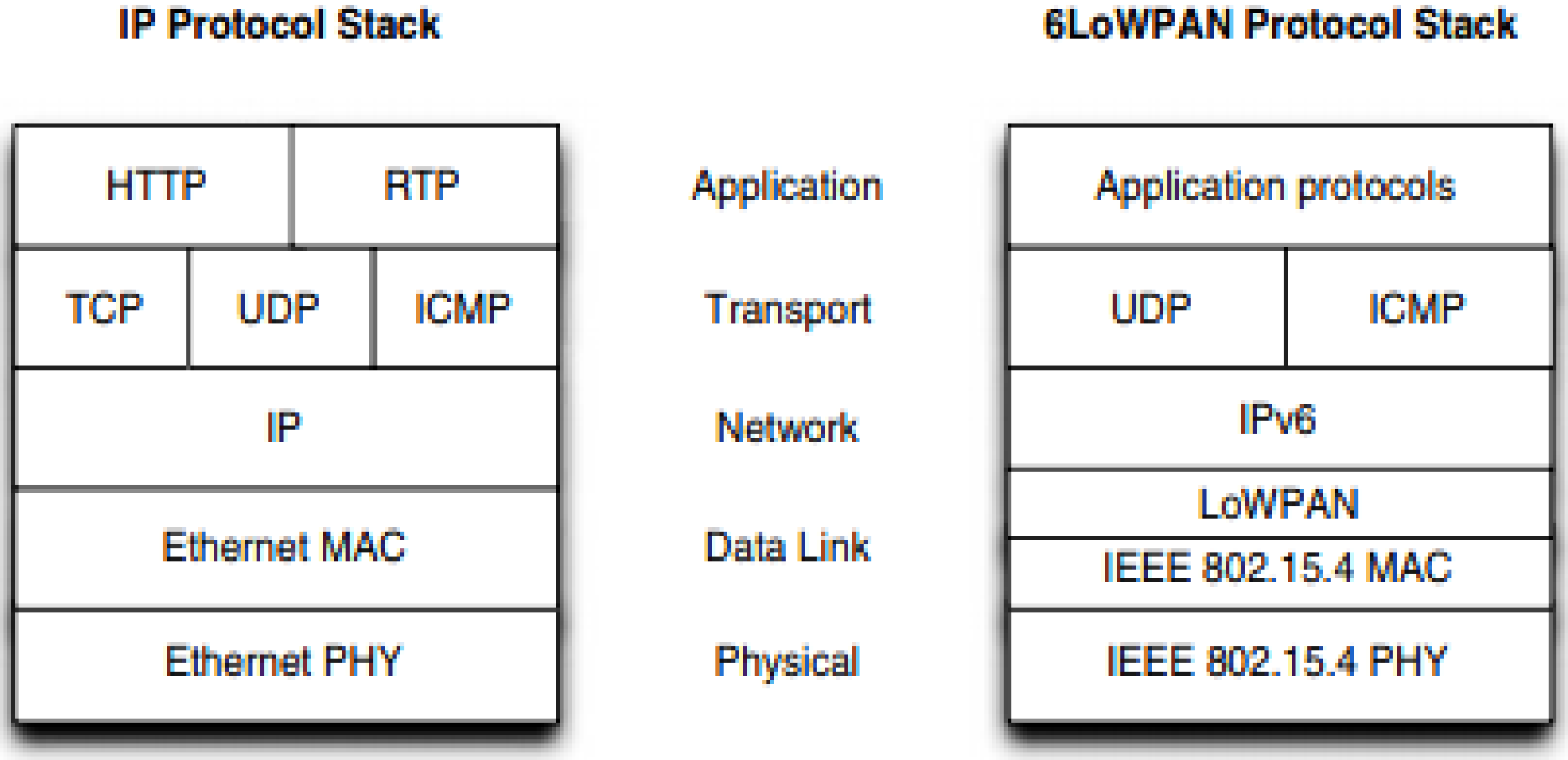
- Simple LoWPAN
  Single Edge Router
- Extended LoWPAN
  Multiple Edge Routers with common backbone link
- Ad-hoc LoWPAN
  No route outside the LoWPAN

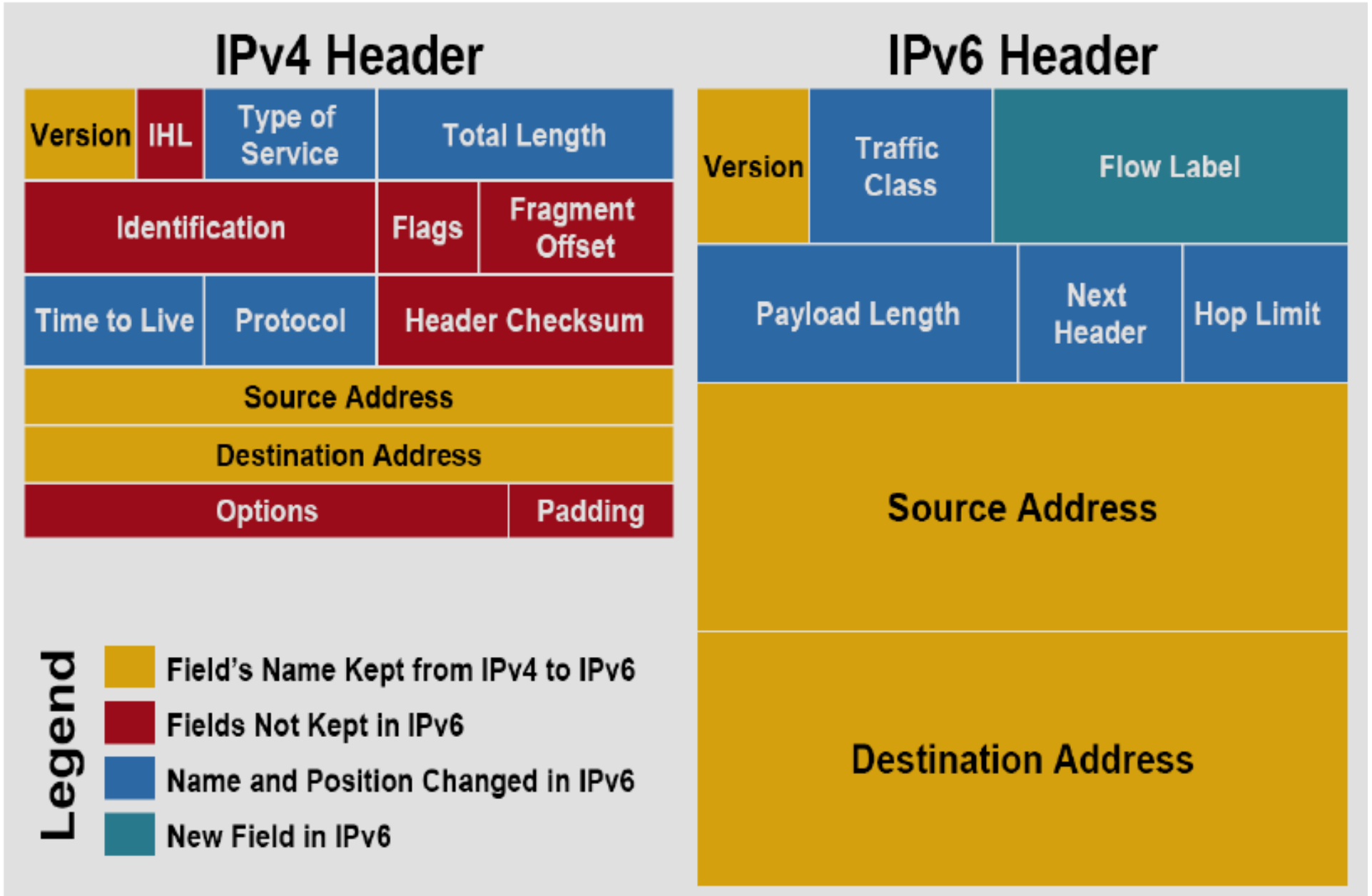
BY-NC-SA

- **Router nodes**: These nodes pass the data from one 6LoWPAN mesh node to another and communicate outward to the WAN and internet.
- **Host nodes**: Hosts are endpoints in Mesh. They cannot route. Hosts are allowed to be in sleep states, occasionally waking to produce data or receive data cached by their parent routers.
- **Edge routers**: An edge router (also known as border router) has four functions:
  1. Handles the communication to the 6LoWPAN devices and relays data to the internet.
  2. Performs compression of IPv6 headers by reducing a 40-byte IPv6 header and 8-byte UDP headers for efficiency in a sensor network. A typical 40-byte IPv6 header can compress to 2 to 20-bytes depending on usage.
  3. Initiates the 6LoWPAN network.
  4. Exchanges data between devices on the 6LoWPAN network.

Features

- Efficient header compression - IPv6 base and extension headers, UDP header
- Fragmentation - 1280 byte IPv6 MTU -> 127 byte 802.15.4 frames
- Support for e.g. 64-bit and 16-bit 802.15.4 addressing
- Useful with low-power link layers such as IEEE 802.15.4, narrowband ISM and power-line communications
- Network auto-configuration using neighbour discovery
- Unicast, multicast and broadcast support
- Support for use of link-layer mesh (e.g. 802.15.5)


IP Protocol Stack
HTTP
RTP
TCP
UDP
ICMP
IP
Ethernet MAC
Ethernet PHY
Application
Transport
Network
Data Link
Physical
6LoWPAN Protocol Stack
Application protocols
UDP
ICMP
IPv6
LoWPAN
IEEE 802.15.4 MAC
IEEE 802.15.4 PHY


IPv4 Header
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding
IPv6 Header
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address
Legend
Field's Name Kept from IPv4 to IPv6
Fields Not Kept in IPv6
Name and Position Changed in IPv6
New Field in IPv6

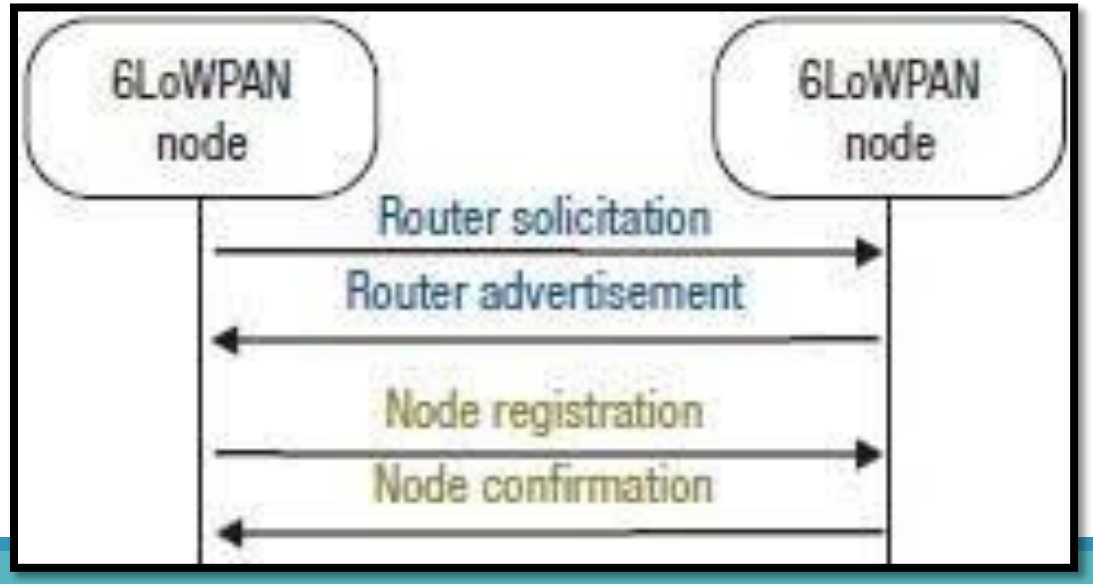
	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.149.0.0/24	3FFE:F200:0234::/48
Number of Addresses	2^{32} = ~4,294,967,296	2^{128} = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456

Neighbour discovery (ND)

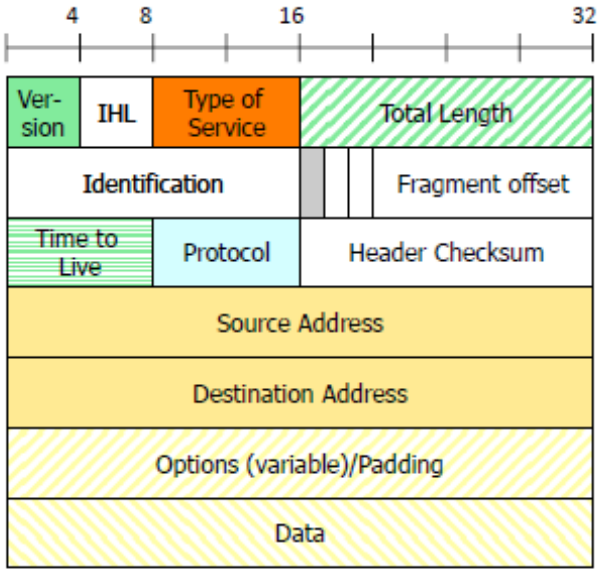
One hop routing protocol

ND is the process of discovering new neighbours, as a mesh can grow, shrink, and transform, resulting in new and changing neighbour relations.
There are two basic processes and four basic message types in ND:

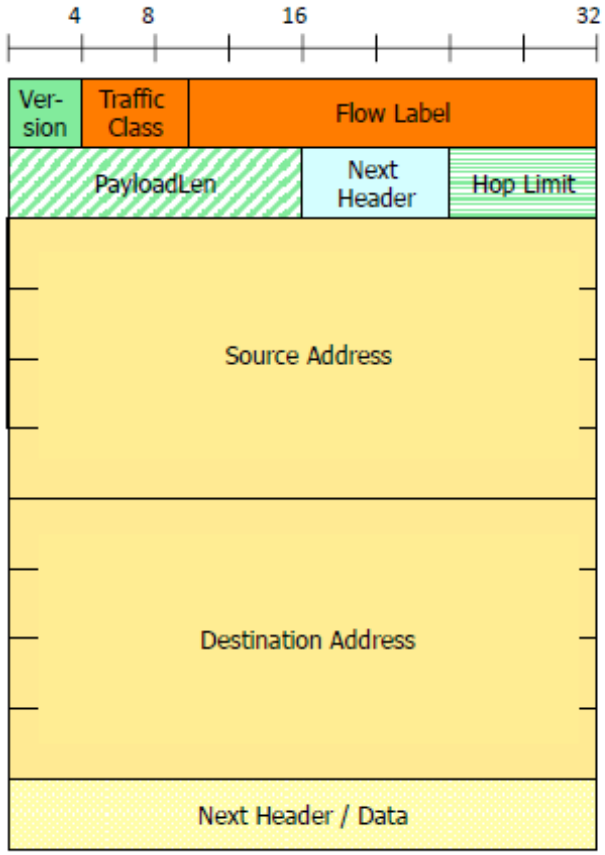
- Finding neighbors: Includes Neighbour Registration (NR) and Neighbour Confirmation (NC) phases
- Finding routers: Includes Router Solicitation (RS) and Router Advertisement (RA) phases



Header Compression



The IPv6 header is longer, but this is only caused by the longer addresses.



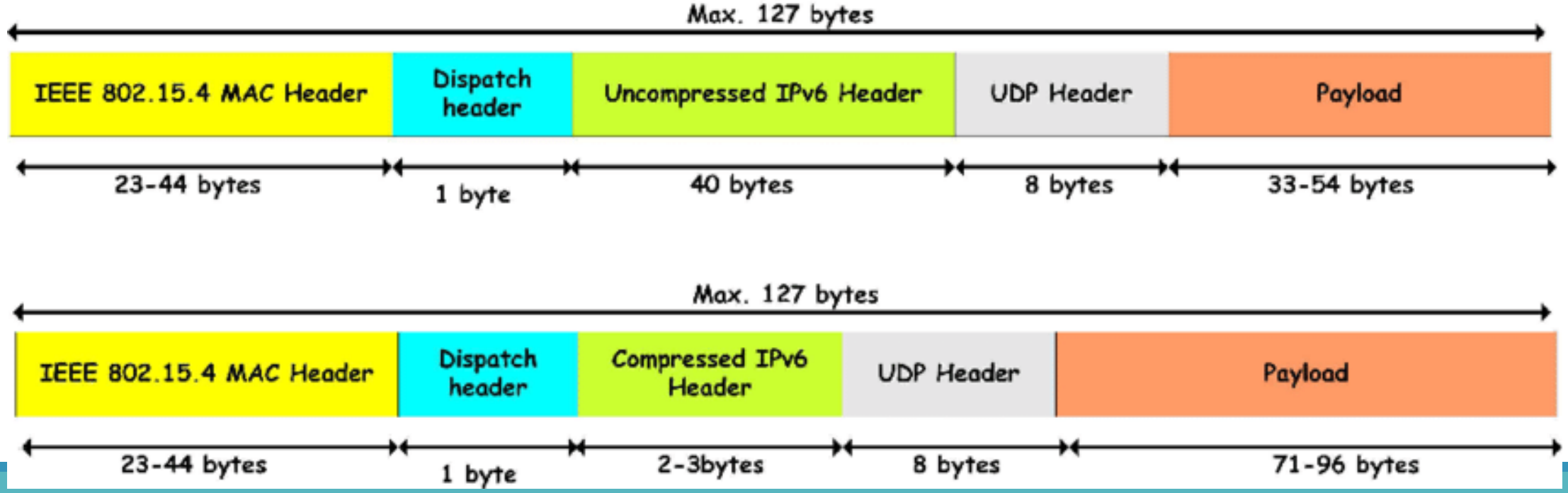
- 6LoWPAN = IPv6 on an 802.15.4 link
- IPv6 has a **Maximum Transmission Unit** (**MTU**) size of 1280 bytes, while 802.15.4 has a limit of 127 bytes
- Header compression in IPV6 is a means to compress and remove redundancy in
- But not suitable for a mesh network such
- as 6LoWPAN
  - Packets hop between nodes and would require compression/decompression on each hop.
  - The routes are dynamic and allowed to change and transmissions may not be present for long duration.
- 6LoWPAN adopted stateless and shared-context compression

Header compression:

- By assuming usage of common values
- From 802.15.4 frame or based on simple assumptions of shared context.
- 40Bytes of IPv6 header are compressed into 2 Bytes of 6LowPAN header.

Fragmentation:

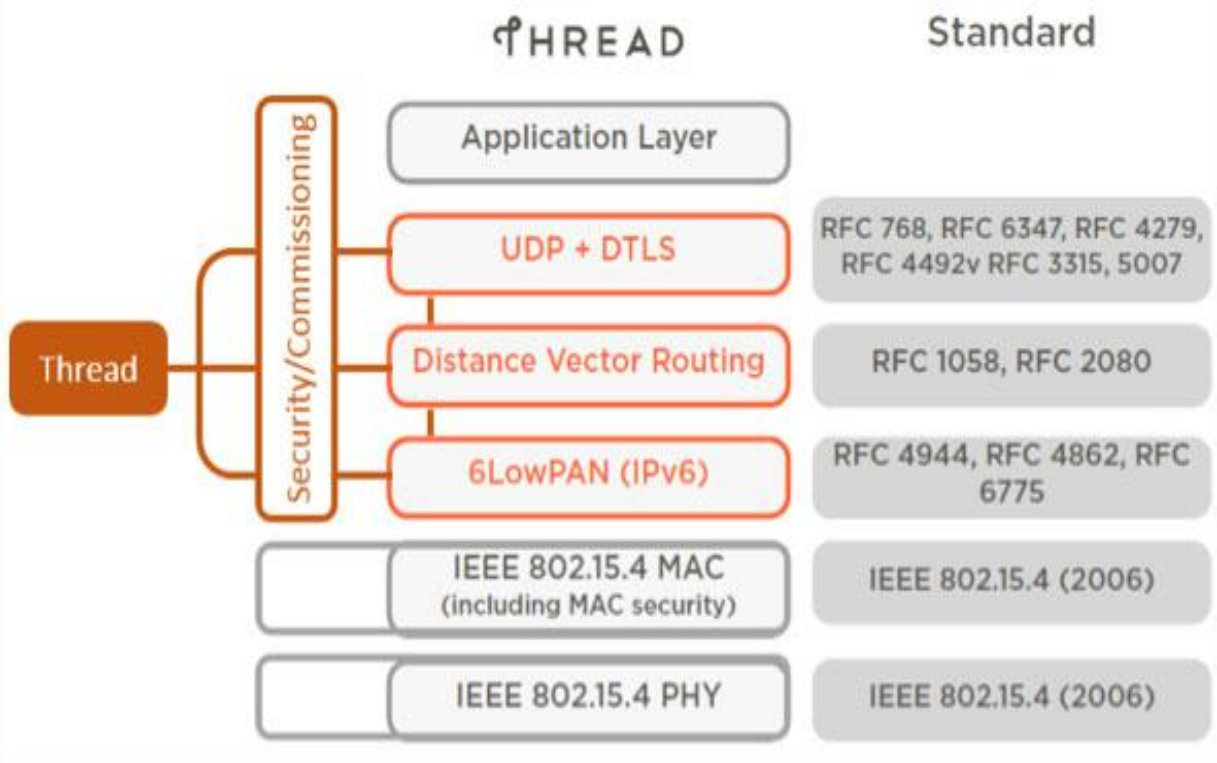
- IPv6 packets are fragmented into multiple link-level frames to accommodate the IPv6 minimum MTU requirement.
- 1280 Bytes of IPv6 frame (minimum IPv6 MTU) have been fragmented to 127Bytes, which is the 802.15.4 MTU.



WPAN – IP Thread

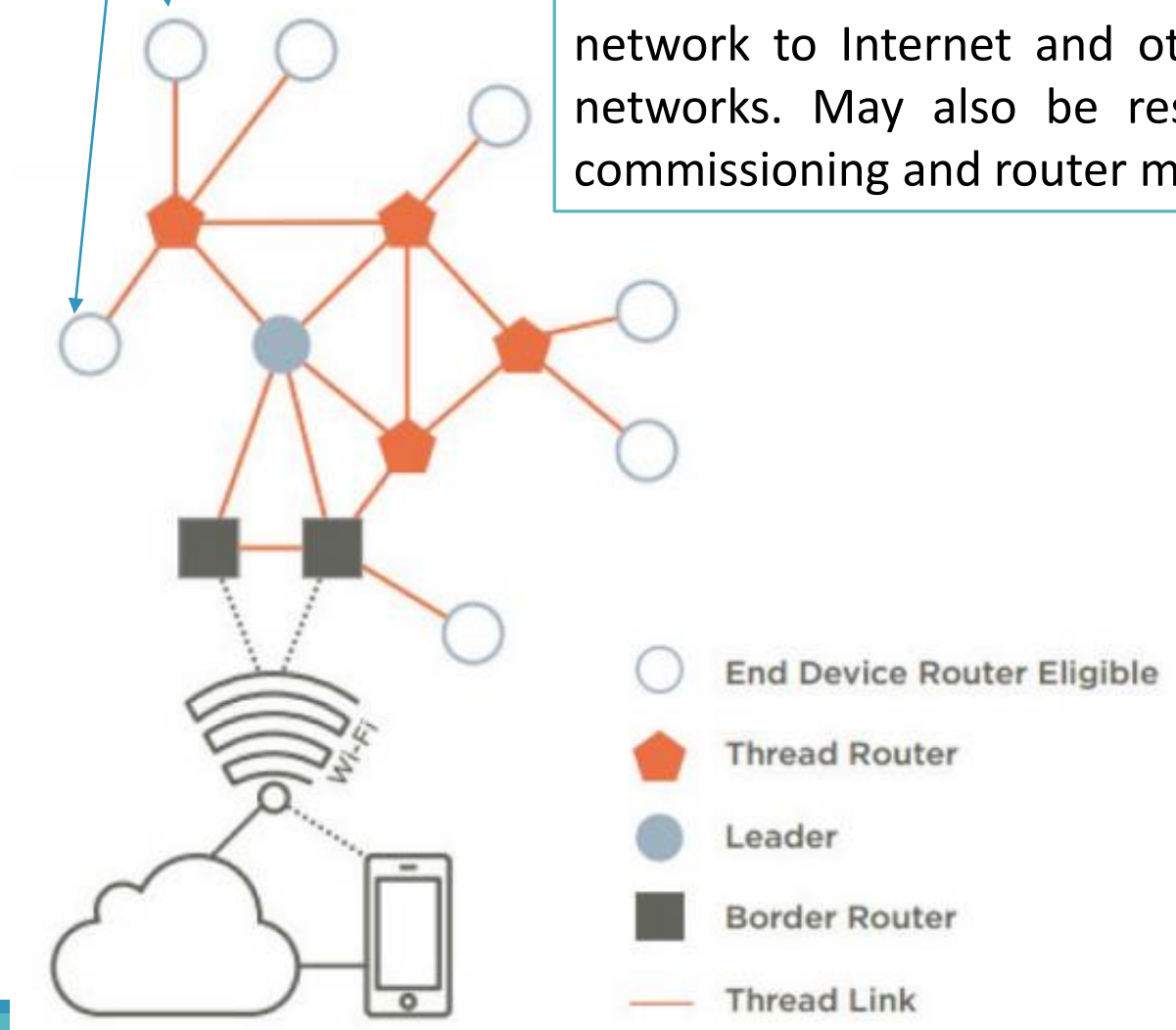
- The Thread IoT protocol is an IP-based wireless mesh network for the home and connected products.
- Utilising a mesh network means there's no single point of failure.
- Uses 6LoWPAN, which in turn uses the IEEE 802.15.4 wireless protocol
- Thread is IP-addressable, with cloud access and AES encryption.

An industry-wide IPv6 protocol suite for IoT



WPAN – IP Thread

REED



Border Router: Connects the Thread network to Internet and other adjacent networks. May also be responsible for commissioning and router management.

Router: Responsible for providing joining, routing and security services in the network.

Router Enabled End Devices (REED): Non-routers in the network who behave as end devices and are hardware-capable of upgrading to Routers when required by the network

Leader: The single distinguished device in any Thread Network Partition that currently acts as a central arbiter of network configuration state.

WPAN – IP Thread

- Open standard protocol – Thread is an IP based wireless networking protocol. It carries IPv6 packets natively through 6LowPAN.
- Simple for consumers to use – The installation of a Thread network is simple and intuitive for users. Users can add, authorize and remove devices onto the network using smart phones or computers through a few simple steps.
- Secure – Thread networks are secure and encrypted. Thread uses smartphone-era authentication schemes and AES encryption to close security holes that exist in other wireless protocols. Only authorized devices can join the network.

WPAN – IP Thread

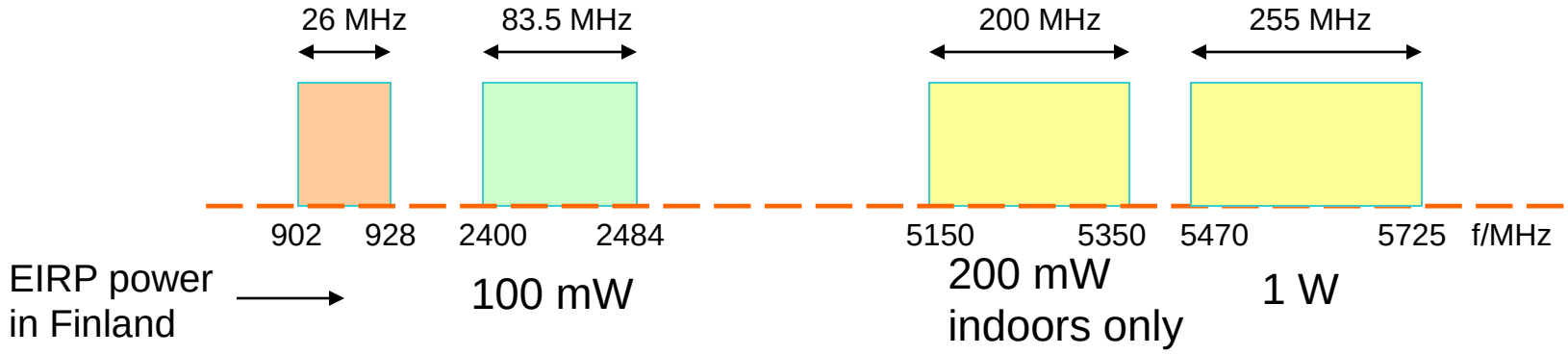
- Power-efficient – Thread is designed to be battery friendly and requires very little energy to operate. Devices efficiently communicate to deliver a great user experience, yet still run for years on the smallest of batteries.
- No single point of failure - Devices working in a Thread network create a mesh. This provides resiliency and removes any single point of failure.
- Designed to support a wide variety of products for the home: appliances, access control, climate control, energy management, safety, and security

IEEE 802.11 protocols

IEEE 802.11 standards and rates

- IEEE 802.11 (1997) 1 Mbps and 2 Mbps (2.4 GHz band)
- IEEE 802.11b (1999) 11 Mbps (2.4 GHz band) = Wi-Fi
- IEEE 802.11a (1999) 6, 9, 12, 18, 24, 36, 48, 54 Mbps (5 GHz band)
- IEEE 802.11g (2001 ... 2003) up to 54 Mbps (2.4 GHz) backward compatible to 802.11b

IEEE 802.11 networks work on license free industrial, science, medicine (ISM) bands:



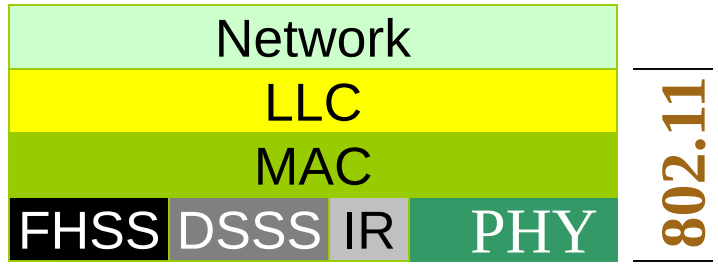
IEEE 802.11 Architecture

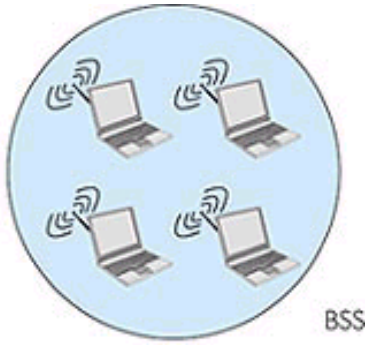
IEEE 802.11 defines the physical (PHY), logical link (LLC) and media access control (MAC) layers for a wireless local area network

802.11 networks can work as

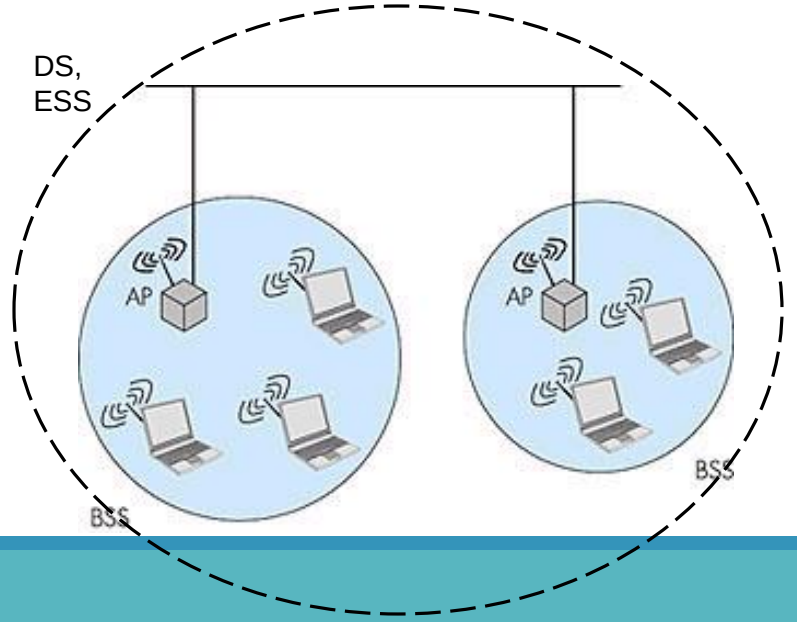
- basic service set (BSS)
- extended service set (ESS)

BSS can also be used in ad-hoc networking





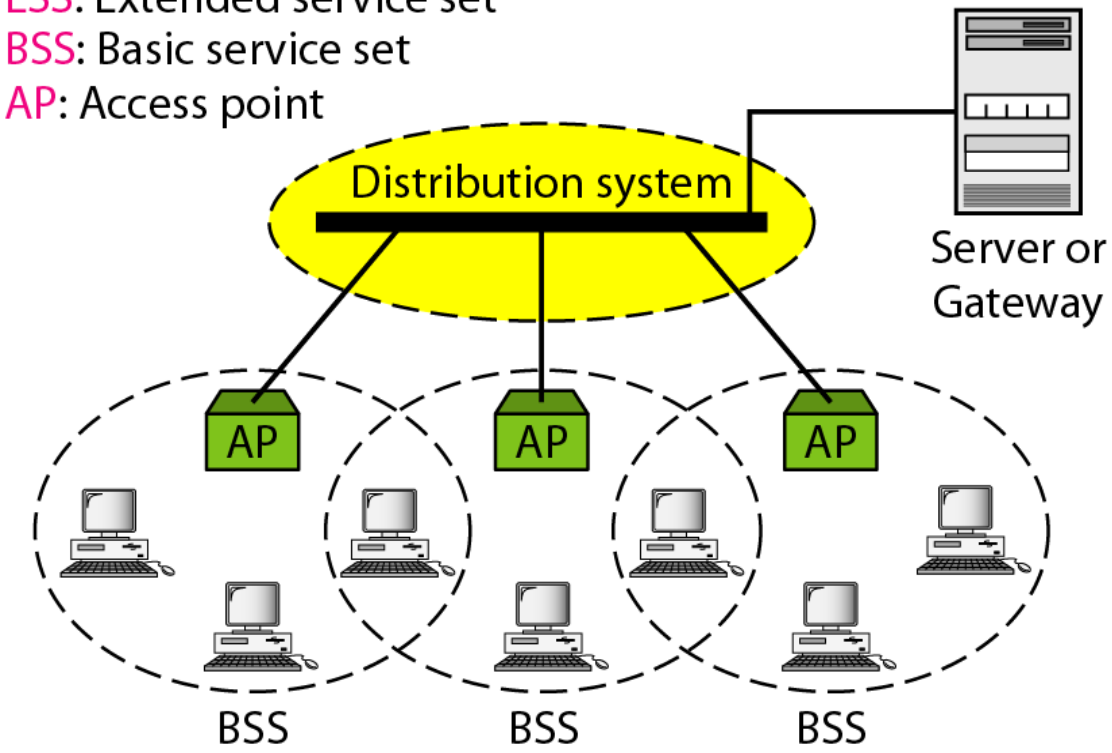
ad-hoc network



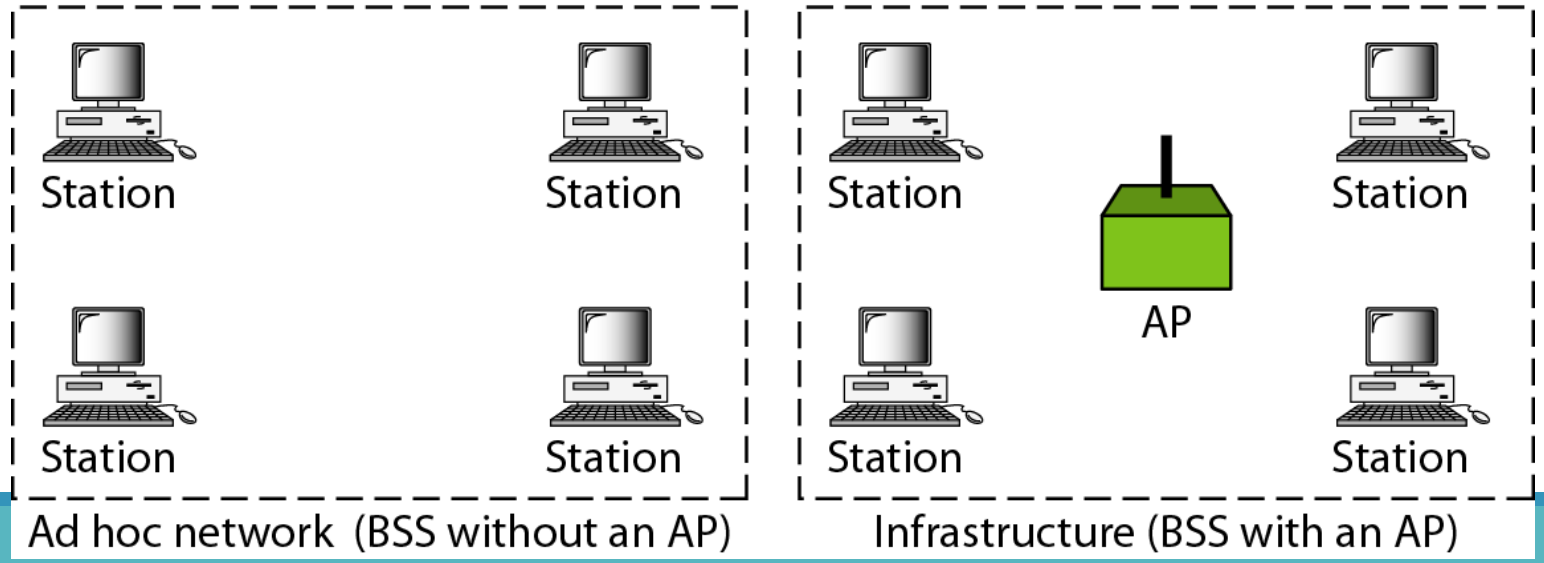
LLC: Logical Link Control Layer
MAC: Medium Access Control Layer
PHY: Physical Layer
FHSS: Frequency hopping SS
DSSS: Direct sequence SS
SS: Spread spectrum
IR: Infrared light
BSS: Basic Service Set
ESS: Extended Service Set
AP: Access Point
DS: Distribution System

BSS and ESS

ESS: Extended service set
BSS: Basic service set
AP: Access point



BSS: Basic service set
AP: Access point



802.11 Logical architecture

LLC provides addressing and data link control

MAC provides

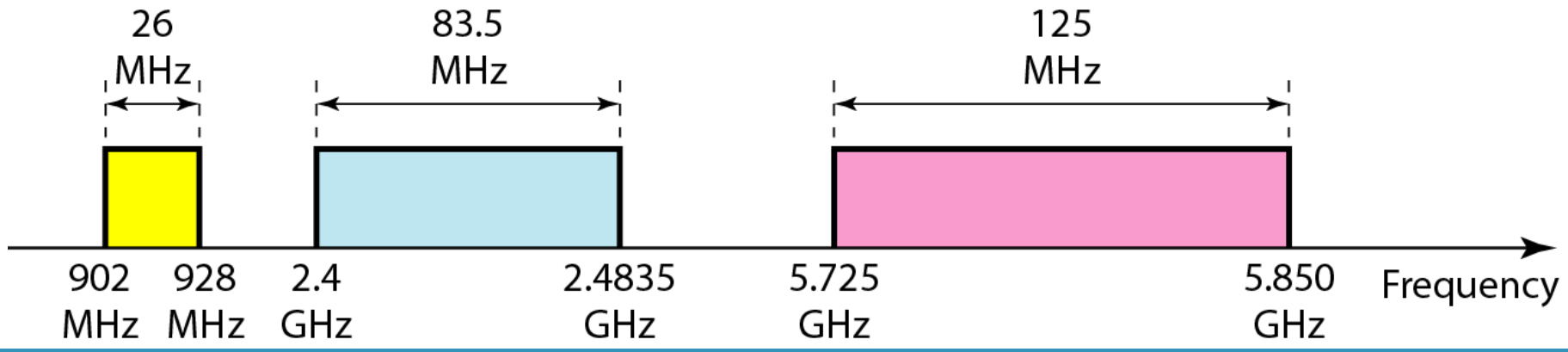
- access to wireless medium
  - CSMA/CA
  - Priority based access (802.12)
- joining the network
- authentication & privacy

Three physical layers (PHY)

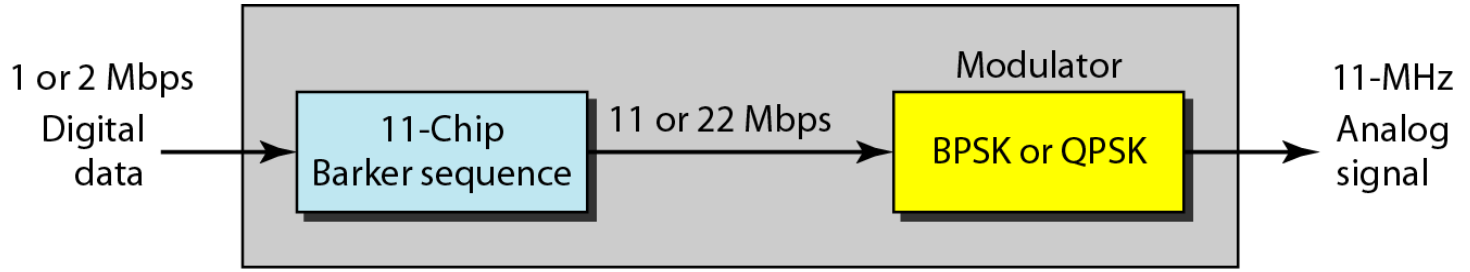
- FHSS: Frequency Hopping Spread Spectrum (SS)
- DSSS: Direct Sequence SS
- IR: Infrared transmission

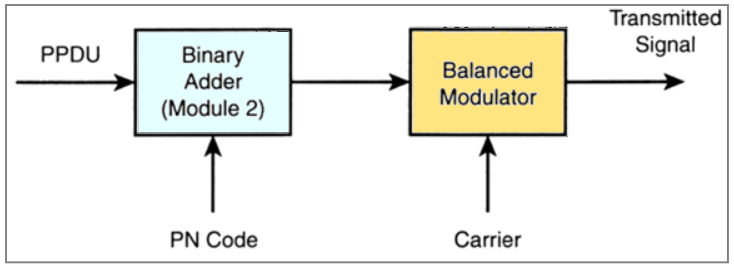
Physical Layer

IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	PSK	1 and 2
		Infrared	PPM	1 and 2
802.11a	OFDM	5.725 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.4 GHz	PSK	5.5 and 11
802.11g	OFDM	2.4 GHz	Different	22 and 54



802.11 DSSS



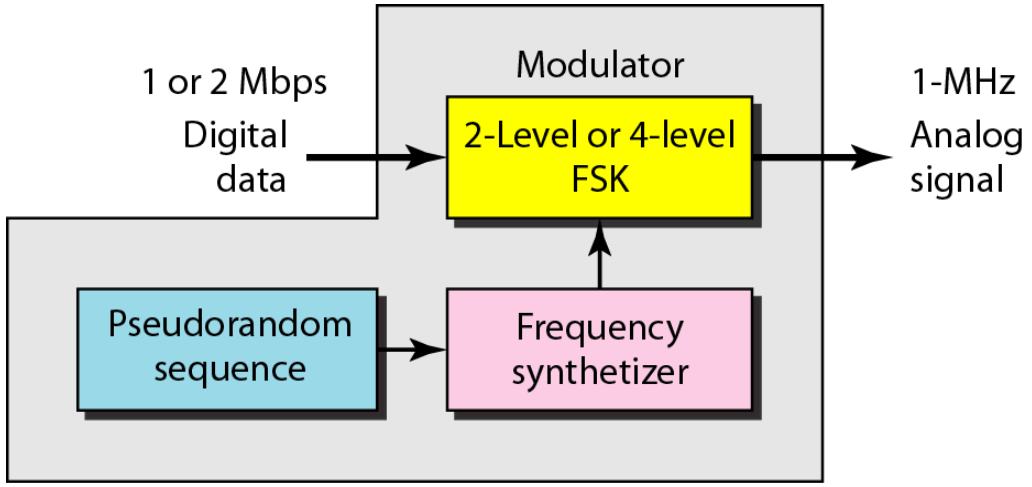


DS-transmitter

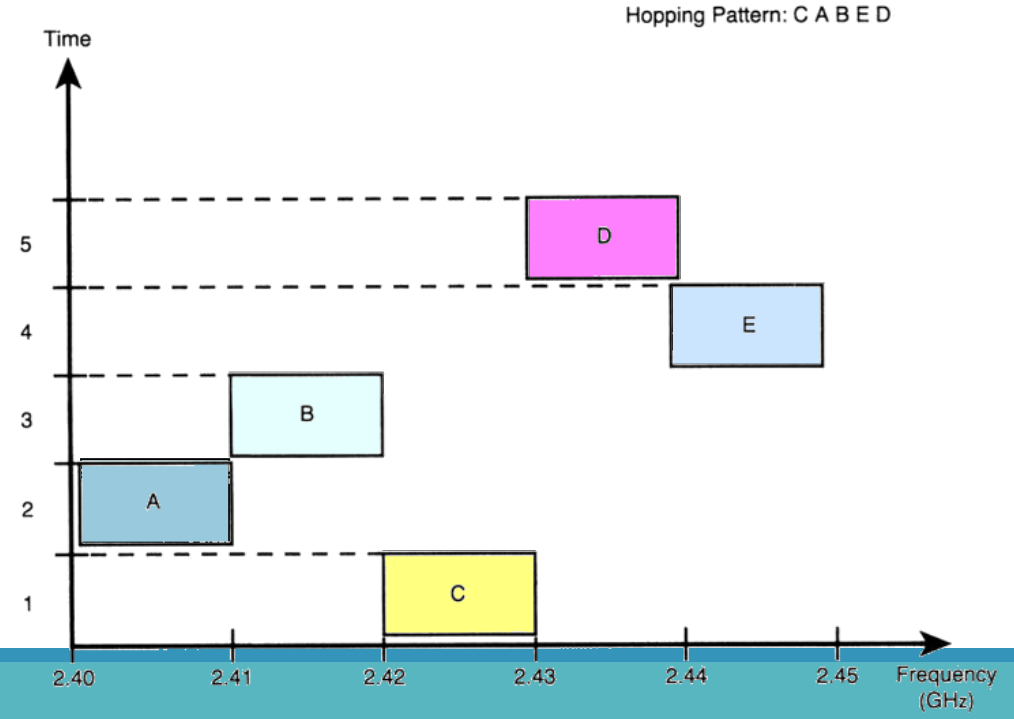
- Supports 1 and 2 Mbps data transport, uses BPSK and QPSK modulation
- Uses 11 chips Barker code for spreading - 10.4 dB processing gain
- Defines 14 overlapping channels, each having 22 MHz channel bandwidth, from 2.401 to 2.483 GHz
- Power limits 1000mW in US, 100mW in EU, 200mW in Japan
- Immune to narrow-band interference, cheaper hardware

PPDU:base band data frame

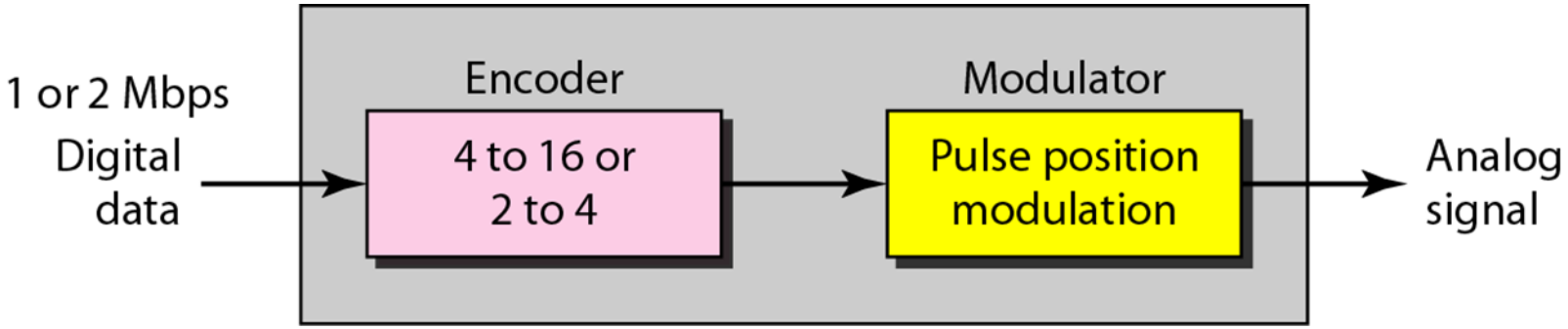
802.11 FHSS



- Supports 1 and 2 Mbps data transport and applies two level - GFSK modulation (Gaussian Frequency Shift Keying)
- 79 channels from 2.402 to 2.480 GHz (in U.S. and most of EU countries) with 1 MHz channel space
- 78 hopping sequences with minimum 6 MHz hopping space, each sequence uses every 79 frequency elements once
- Minimum hopping rate 2.5 hops/second
- Tolerance to multi-path, narrow band interference, security
- Low speed, small range due to FCC TX power regulation (10mW)



Physical layer of IEEE 802.11 infrared



802.11: Channels, association

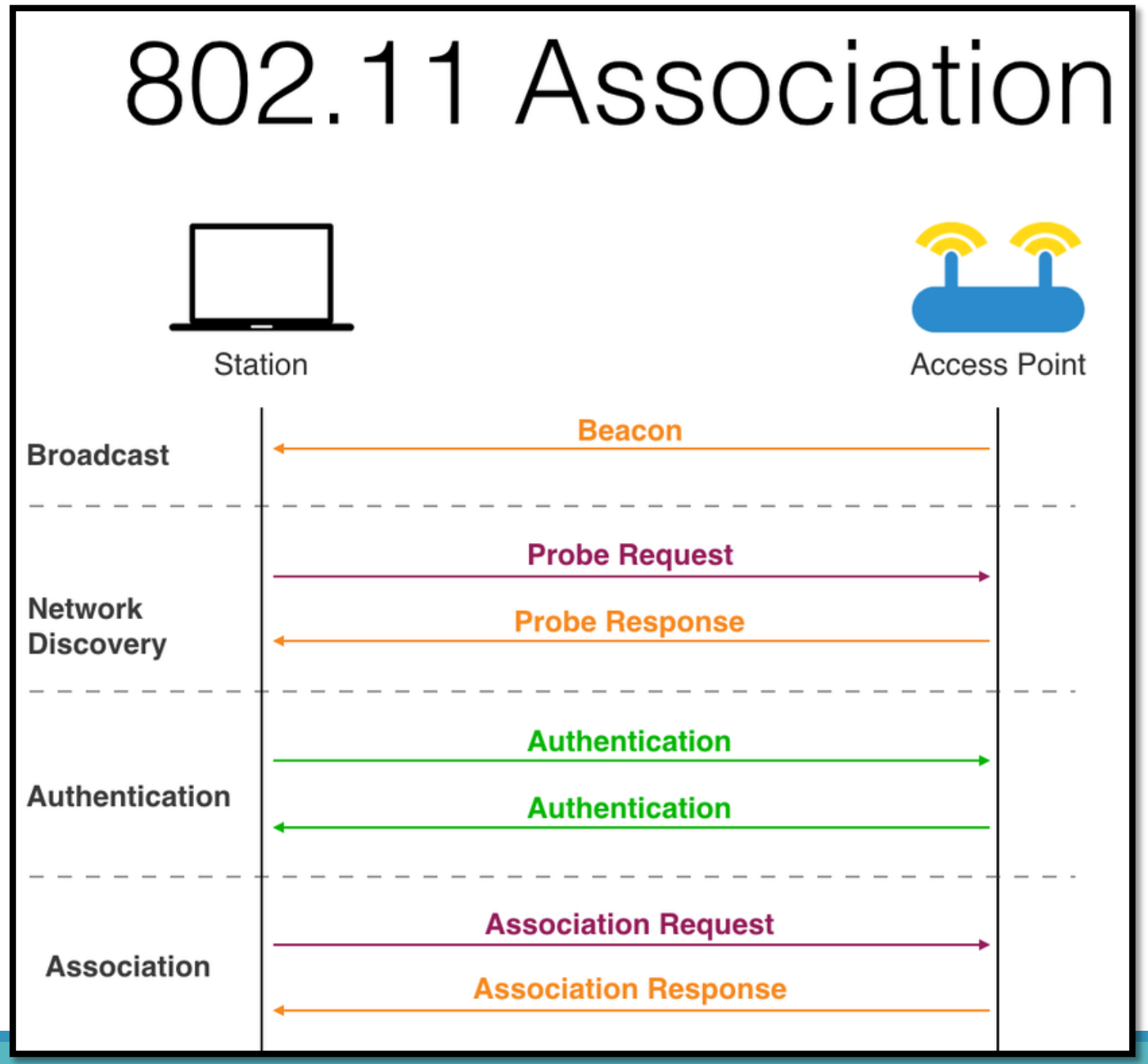
802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies

- AP admin chooses frequency for AP
- interference possible: channel can be same as that chosen by neighboring AP

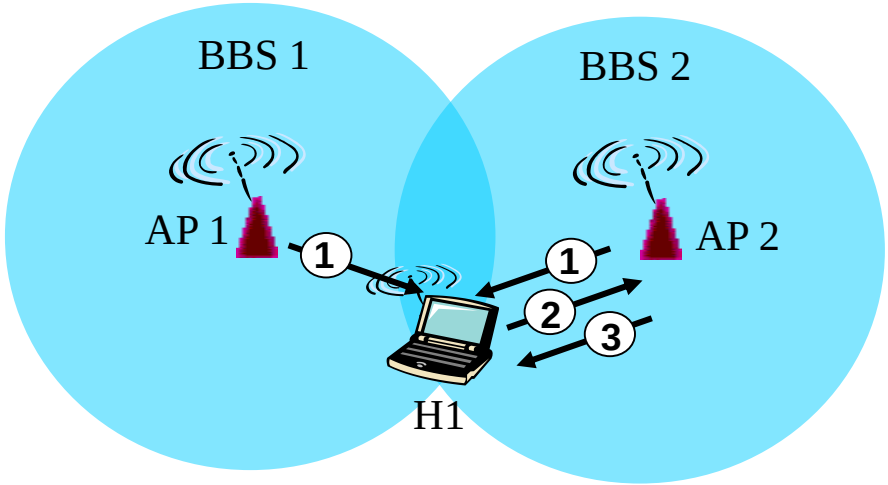
host: must *associate* with an AP

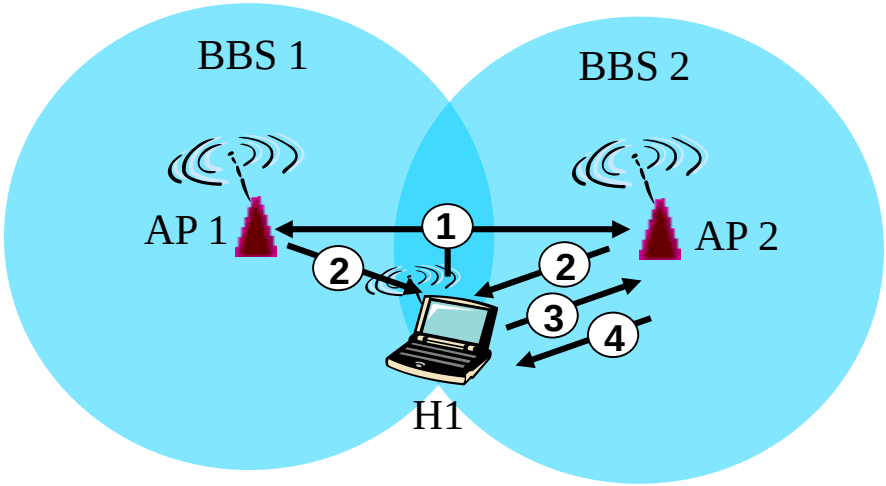
- Scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
- Selects AP to associate with
- May perform authentication

802.11 Association



802.11: passive/active scanning





Passive Scanning:

(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent: selected AP to H1

Active Scanning:

(1) Probe Request frame broadcast from H1
(2) Probes response frame sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent: H1 to selected AP

IEEE 802.11: Multiple Access

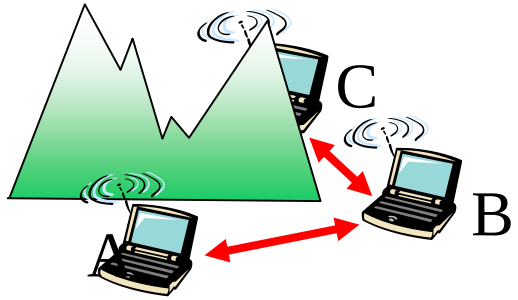
Avoid collisions: 2^+ nodes transmitting at same time

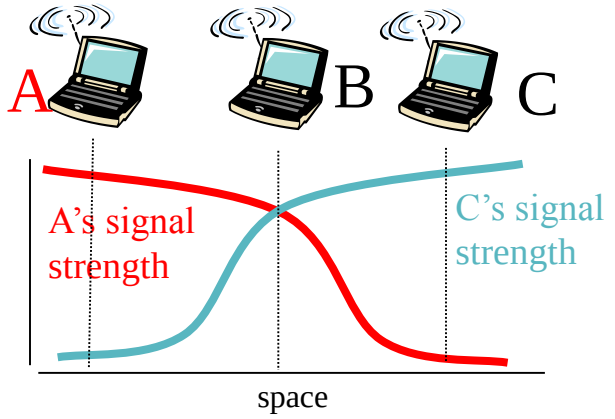
802.11: CSMA sense before transmitting

- Avoids collision with ongoing transmission by other node

802.11: Collision Avoidance, not Collision Detection

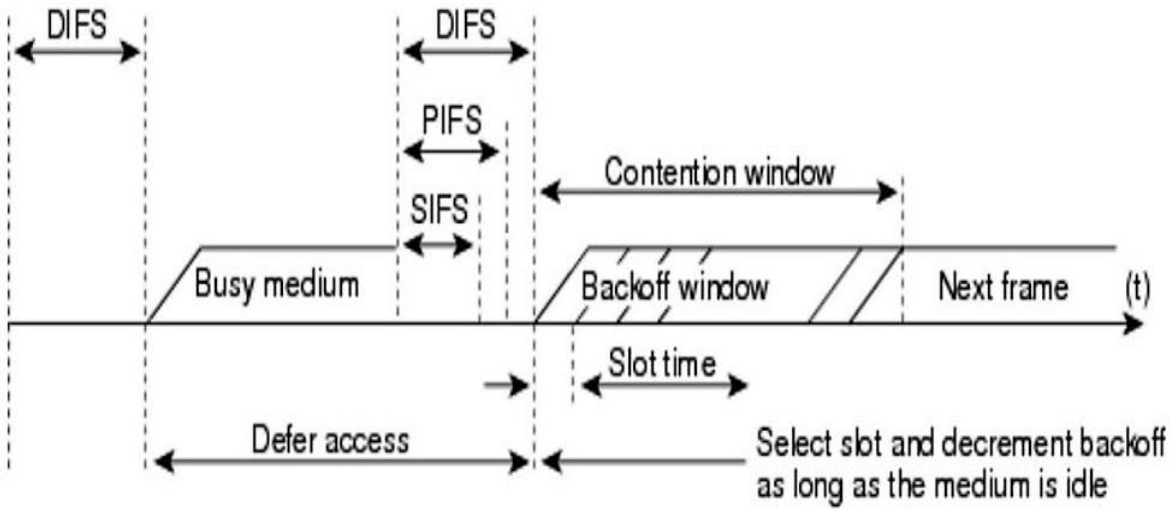
- Difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
- Cannot sense all collisions in any case: hidden terminal, fading





CSMA/CA flowchart

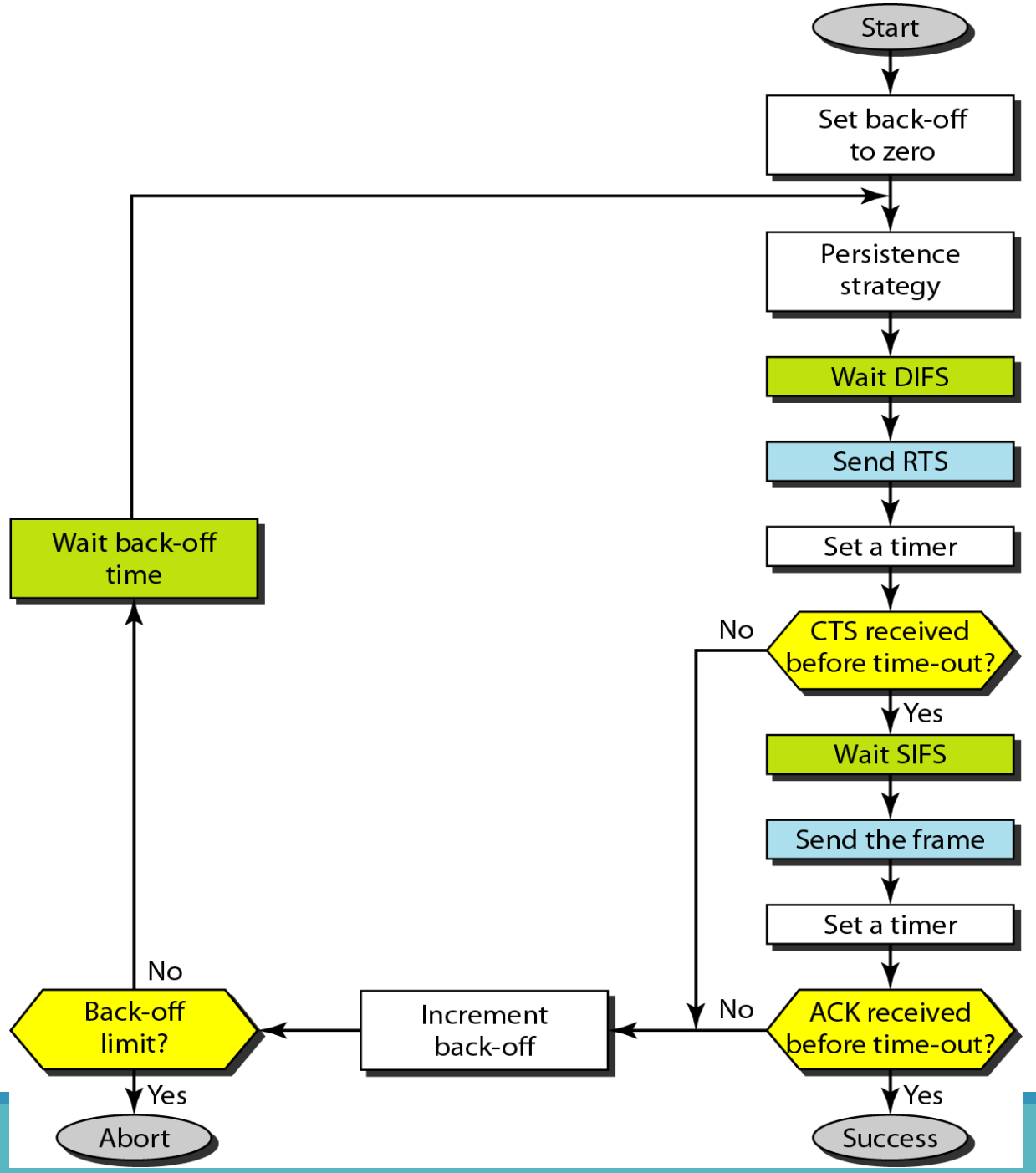
802.11 Inter Frame Space



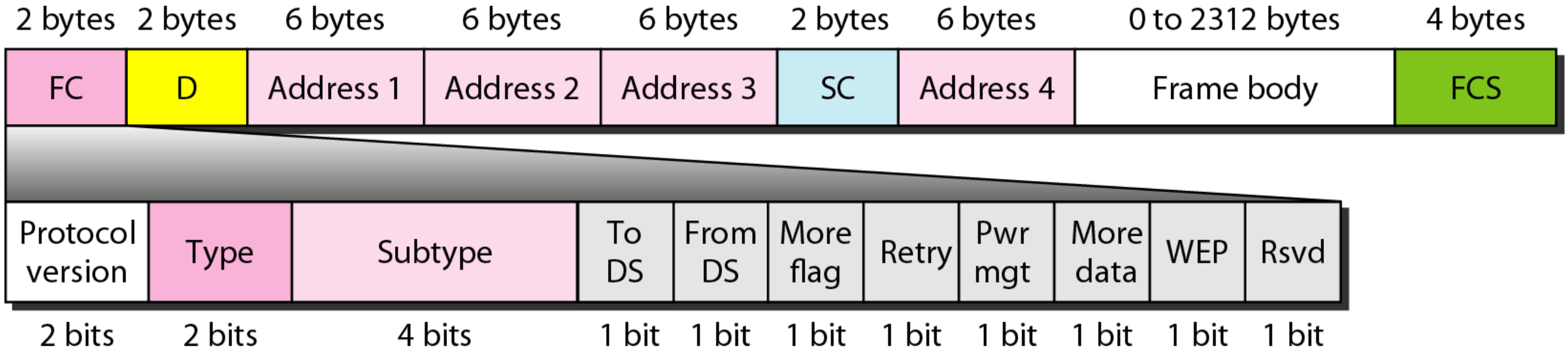
DIFS- Distributed Coordination Function Inter-frame Space

SIFS - Short Inter-Frame Space

PIFS- Point coordination Function IFS



802.11 frame



FC – Frame Control
SC – Sequence Control
FCS- Frame Check Sum

Pros and Cons of using standard 802.11a/b/g/n/ac for IoT

Pros	Cons
1. Low cost of infrastructure and devices	1. High power consumption
2. Ease of deployment	2. Moderate range
3. Points of presence	3. Spectrum congestion

Wi-Fi Standards for IoT

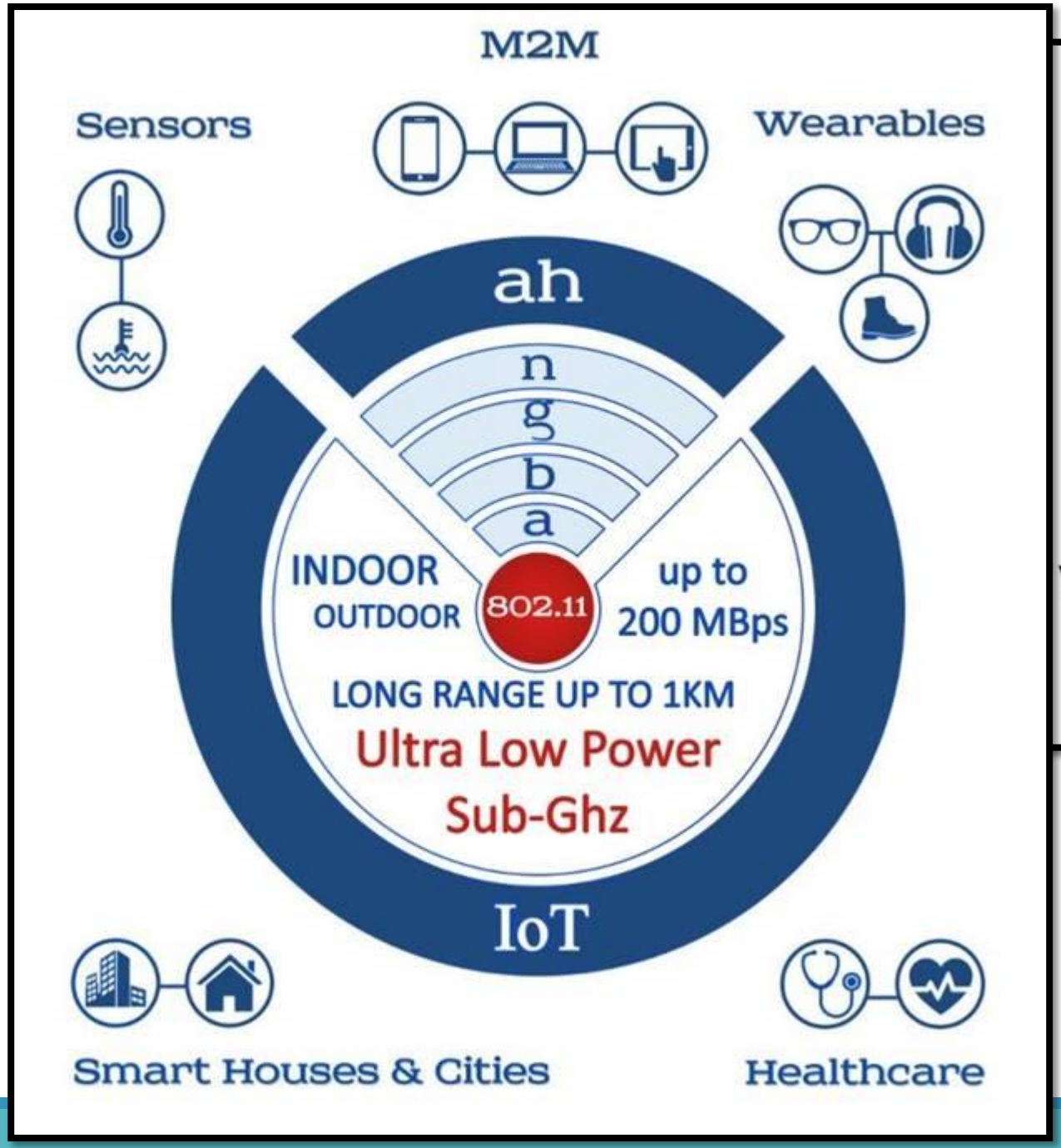
Low power/low bandwidth IoT interconnect **WiFi HaLow (802.11ah)**

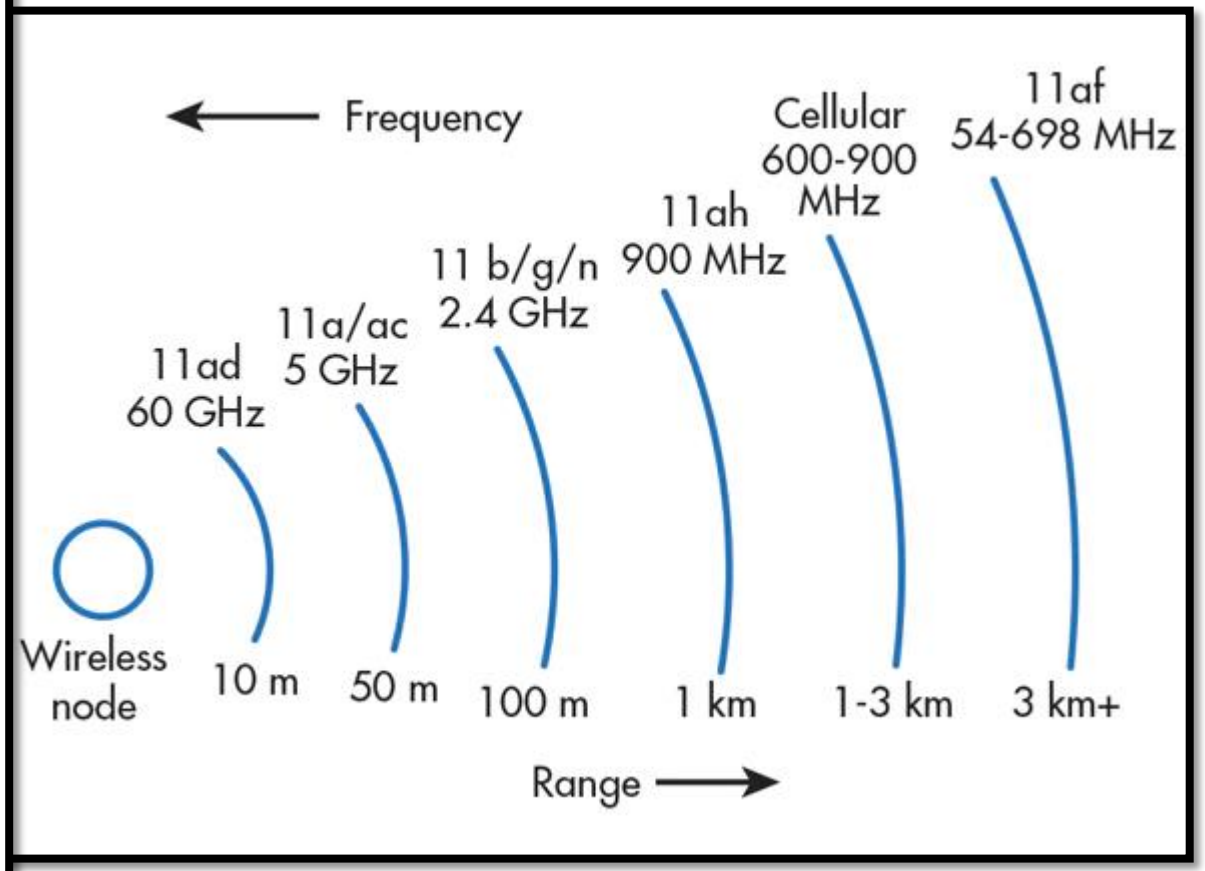
Based on 802.11ac standard **HEW (802.11ax)**

Extreme bandwidth near meter communication for audio/video (802.11ad)

Reuse of television analog RF space (802.11af)

Vehicle-to-Vehicle communication (802.11p)


M2M
Sensors
Wearables
ah
n
g
b
a
INDOOR
OUTDOOR
802.11
up to
200 MBps
LONG RANGE UP TO 1KM
Ultra Low Power
Sub-Ghz
IoT
Smart Houses & Cities
Healthcare

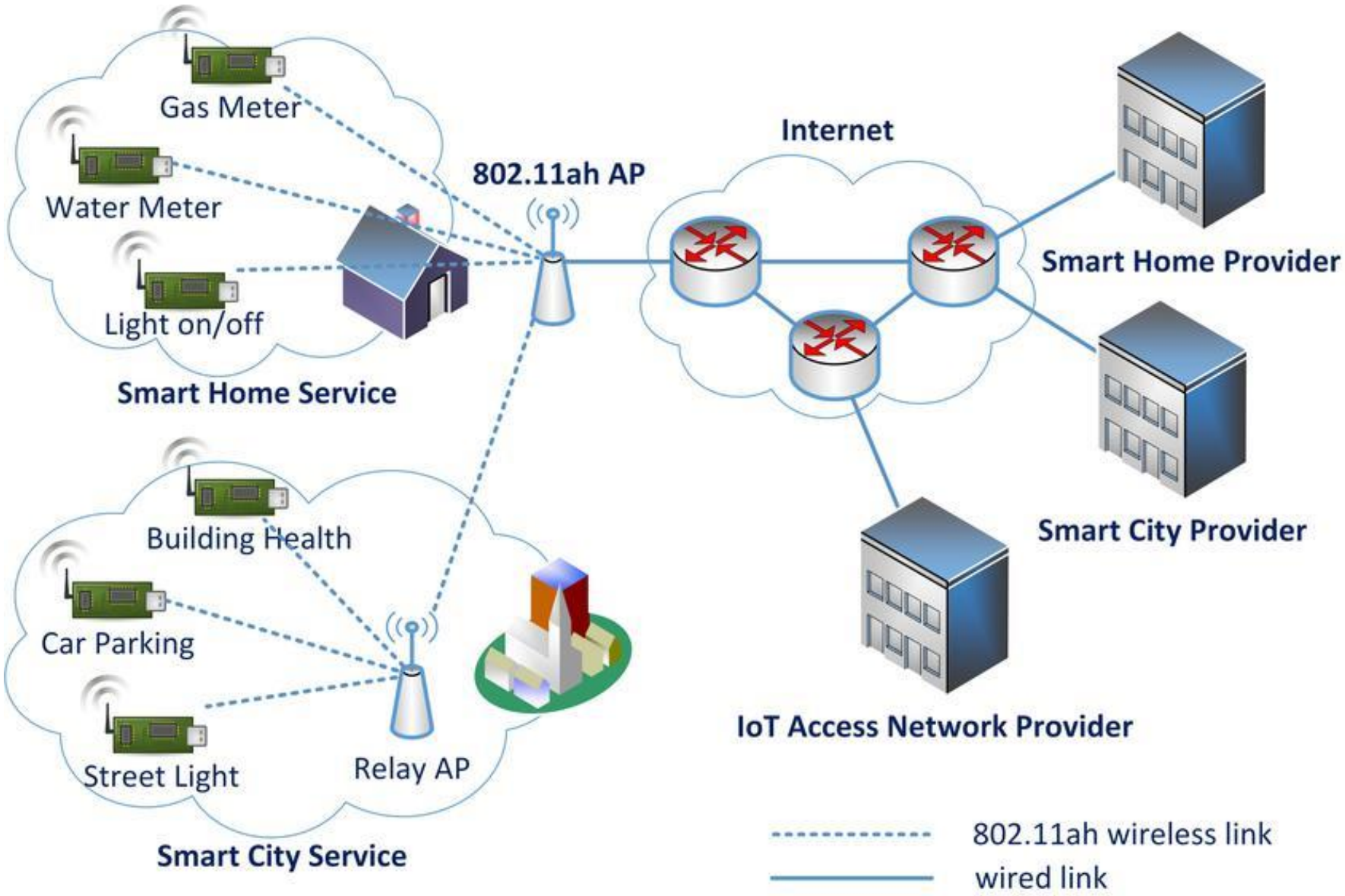

Frequency
11af
54-698 MHz
Cellular
600-900
MHz
11ah
900 MHz
11 b/g/n
2.4 GHz
11a/ac
5 GHz
11ad
60 GHz
Wireless
node
10 m
50 m
100 m
1 km
1-3 km
3 km+
Range

WiFi HaLow (802.11ah)

- Operates in 900 MHz spectrum. This allows for good propagation and penetration of materials and atmospheric conditions.
- Channel width varies and can be set to 2, 4, 8, or 16 MHz-wide channels.
- The available modulation methods are diverse and include BPSK, QPSK, 16-QAM, 64-QAM, and 256-QAM modulation techniques.
- Modulation based on 802.11ac standard with specific changes.
- A total of 56 OFDM subcarriers with 52 dedicated to data and four dedicated to pilot tones.
- Total symbol duration is 36 or 40 microseconds.
- Supports SU-MIMO beamforming.
- Fast association for networks of thousands of STAs using two different authentication methods to limit contention.
- Provides connectivity to thousands of devices under a single access point.

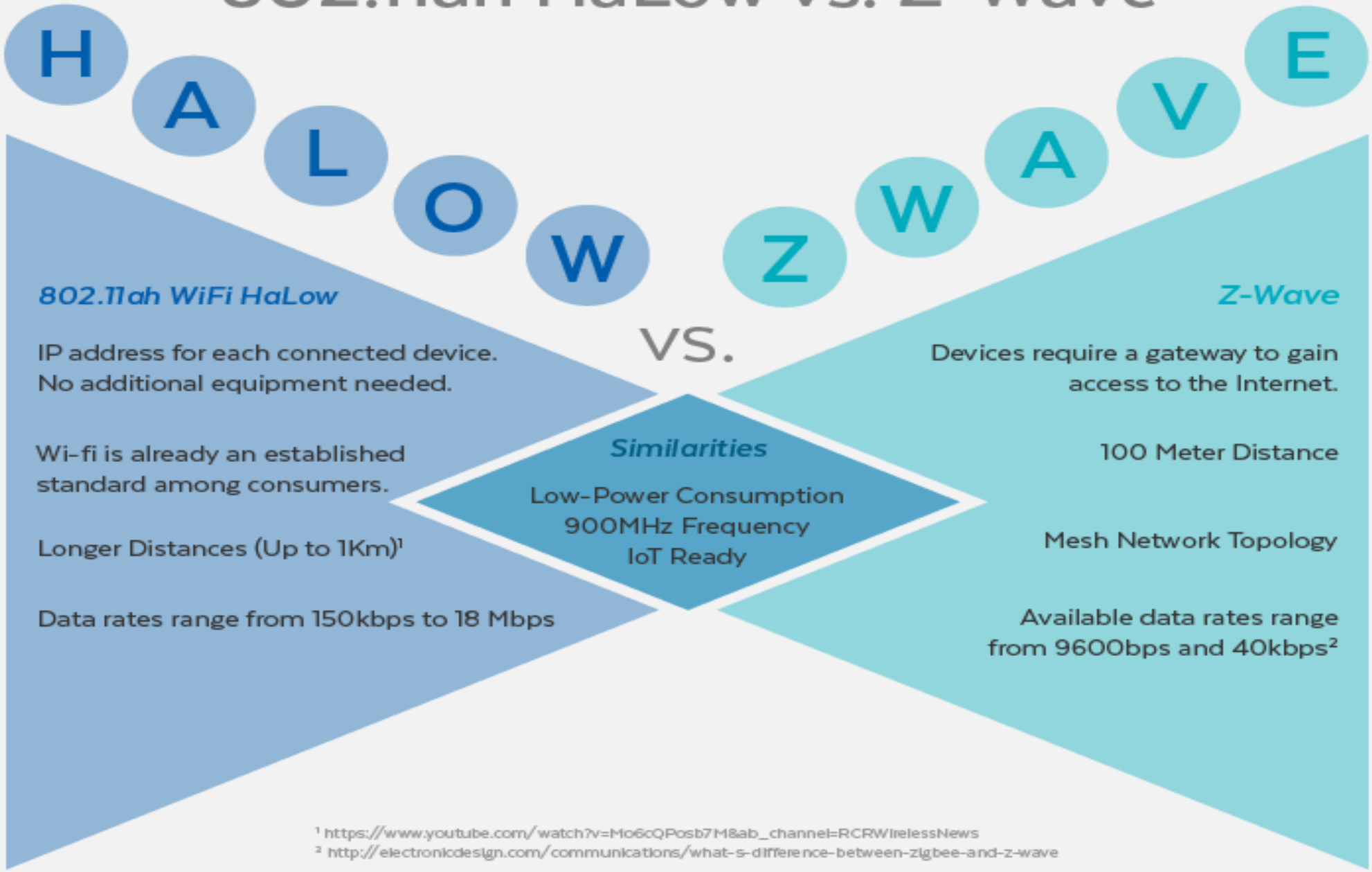
WiFi HaLow (802.11ah)

- Includes the ability to relay to reduce power on STAs and allow for mesh networking using a one-hop reach method.
- Allows for advanced power management on each 802.11ah node. (wake/doze periods)
- Allows for non-star topology communication through the use of Restricted Access Windows.
- Allows for sectorization, which enables antennas to be grouped to cover different regions of a BSS (called sectors). This is accomplished using beamforming adopted from other 802.11 protocols.
- The minimum throughput is 150 kbps, based on BPSK modulation on a single MIMO stream at 1 MHz channel bandwidth.
- The maximum theoretical throughput is 347 Mbps based on a 256-QAM modulation using 4 MIMO streams and 16 MHz channels.


Gas Meter
Water Meter
Light on/off
Smart Home Service
802.11ah AP
Internet
Smart Home Provider
Smart City Provider
Building Health
Car Parking
Street Light
Relay AP
Smart City Service
IoT Access Network Provider
802.11ah wireless link
wired link

	Zigbee	*Bluetooth*	*IEEE 802.llah*
Standard	IEEE 802.15.4	IEEE 802.15.1	IEEE 802.11ah
Frequency band	EU: 868 MHz North America: 915 MHz Global: 2.4 GHz	2.4 GHz	Sub-1GHz
Data rate	868 MHz band: 20 kb/s 915 MHz band: 40 kb/s 2.4 GHz band: 250 kb/s	1 Mb/s	150kb/s - 347Mb/s
Typical range	2.4 GHz band: 10-100 m.	10-30 m.	100-1000 m.
TX power	1-100 mW	1-10 mW	10 mW<P_{tx}<1 W (depending on the country's regulations)

802.11ah HaLow vs. Z-Wave



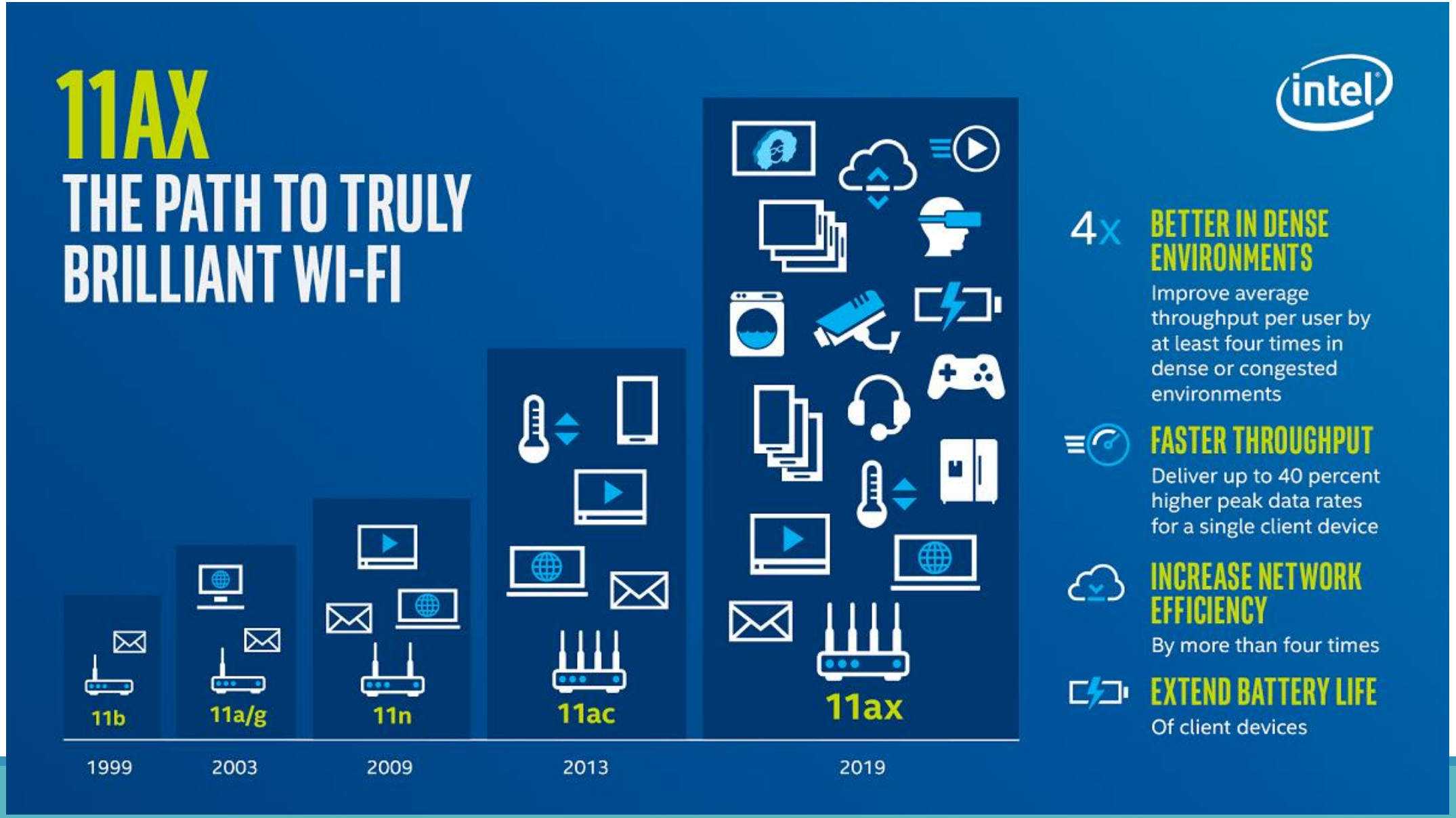
[1] https://www.youtube.com/watch?v=Mo6cQPosb7M&ab_channel=RCRWirelessNews
[2] http://electronicdesign.com/communications/what-s-difference-between-zigbee-and-z-wave

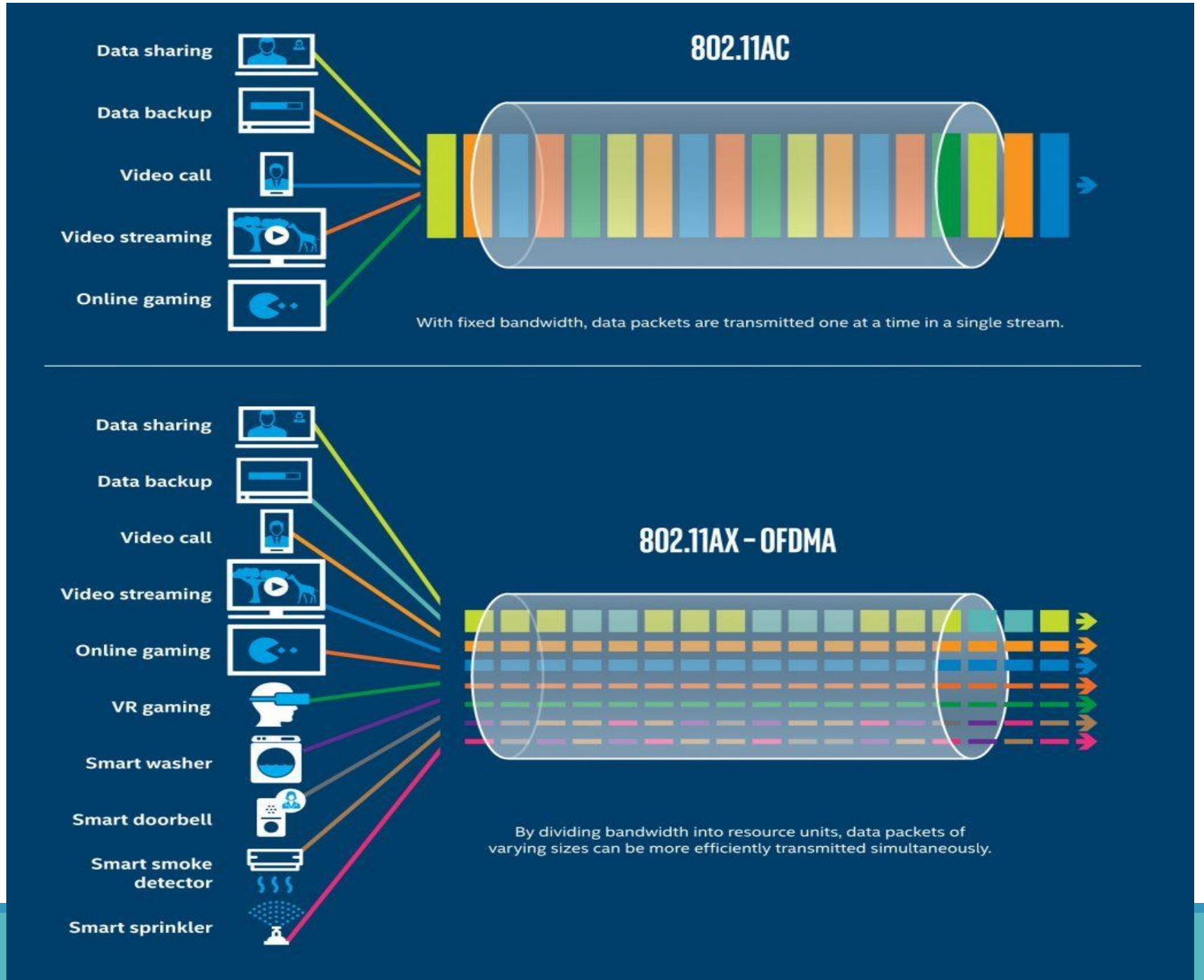
IEEE 802.11ax

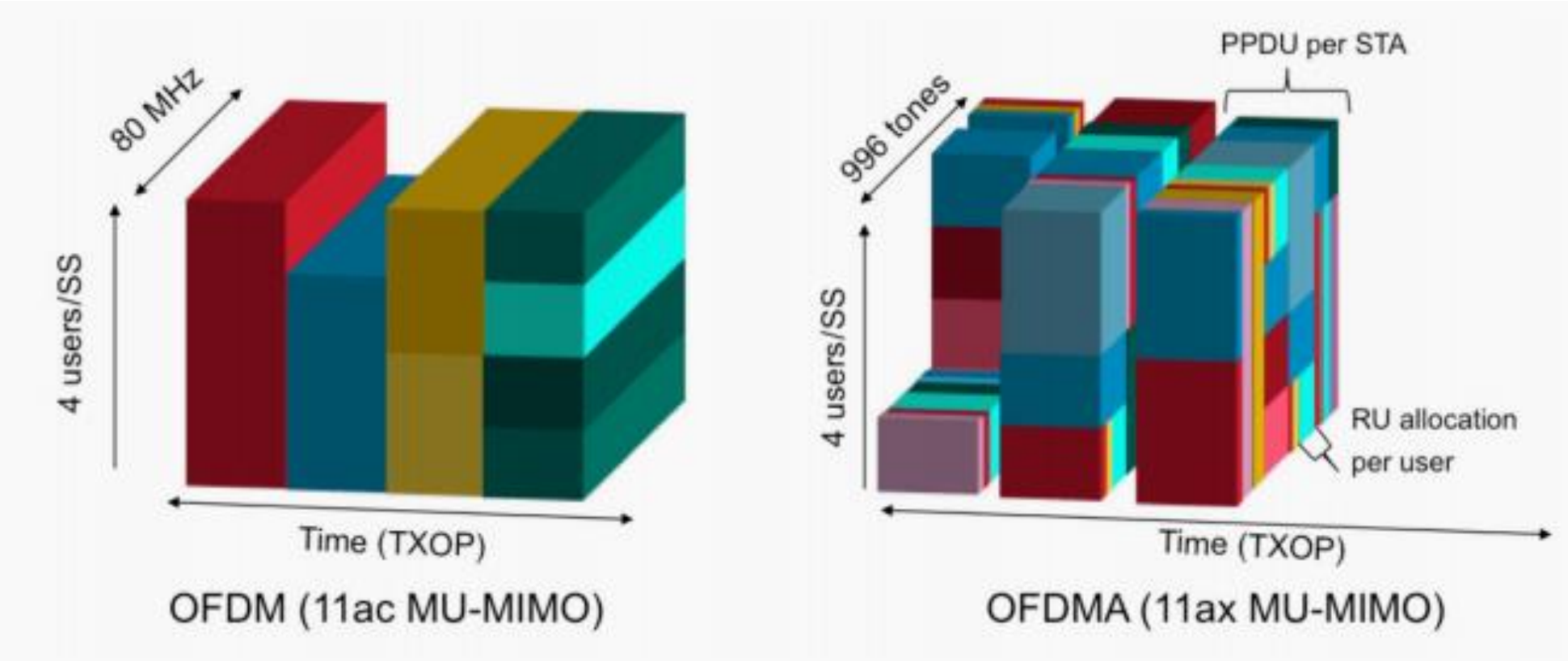
802.11ax major features

1. Downlink and uplink OFDMA
2. Downlink* and uplink multi-user MIMO
3. Higher order modulation
4. Advanced OFDM and coding
5. Outdoor operation
6. Reduced power consumption
7. Spatial re-use
8. Transmit beamforming*
9. Single-user operation*

802.11 ax


11AX
THE PATH TO TRULY BRILLIANT WI-FI
intel
11b
11a/g
11n
11ac
11ax
1999
2003
2009
2013
2019
4x BETTER IN DENSE ENVIRONMENTS
Improve average throughput per user by at least four times in dense or congested environments
FASTER THROUGHPUT
Deliver up to 40 percent higher peak data rates for a single client device
INCREASE NETWORK EFFICIENCY
By more than four times
EXTEND BATTERY LIFE
Of client devices

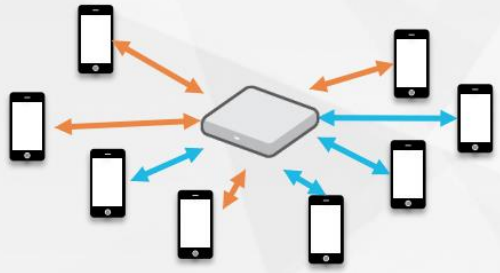

Data sharing
Data backup
Video call
Video streaming
Online gaming
802.11AC
With fixed bandwidth, data packets are transmitted one at a time in a single stream.
Data sharing
Data backup
Video call
Video streaming
Online gaming
VR gaming
Smart washer
Smart doorbell
Smart smoke detector
Smart sprinkler
802.11AX – OFDMA
By dividing bandwidth into resource units, data packets of varying sizes can be more efficiently transmitted simultaneously.


80 MHz
4 users/SS
Time (TXOP)
OFDM (11ac MU-MIMO)
PPDU per STA
996 tones
4 users/SS
RU allocation
per user
Time (TXOP)
OFDMA (11ax MU-MIMO)

802.11ax Building Blocks & Benefits

OFDMA

- Network Capacity

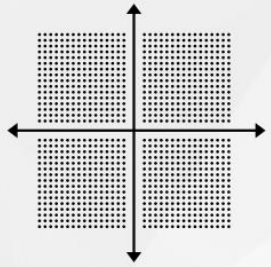


MU-MIMO

- Network Capacity

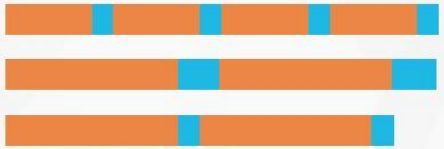
Power Efficiencies

- Device Battery Life



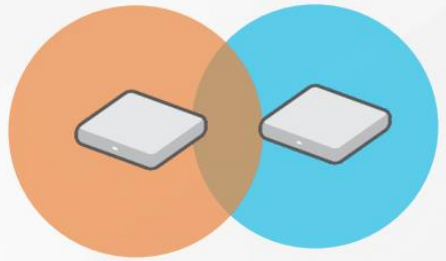
1024-QAM

- Peak throughout increase



Long OFDM Symbol

- Outdoor reliability
- Peak throughout increase



BSS Coloring

- Network Capacity
- Enhanced Wi-Fi Coexistence

Each BSS (access point) uses a different “color” (6 bits in the signal preamble)

Low Power WAN (LPWAN)

- ❑Cellular Standards
- ❑LoRa
- ❑Sigfox

Long range

Long range communications even in dense urban areas.

Low data rate

Star network

Unlike mesh networks (eg: Zigbee/802.15.4), star networks are more easily deployable and contribute to LPWA energy efficiency.

Low number of required base stations

Several thousands of sensors managed by a single base station.

Low Power

Batteries last up to 10 years.

Low subscription cost

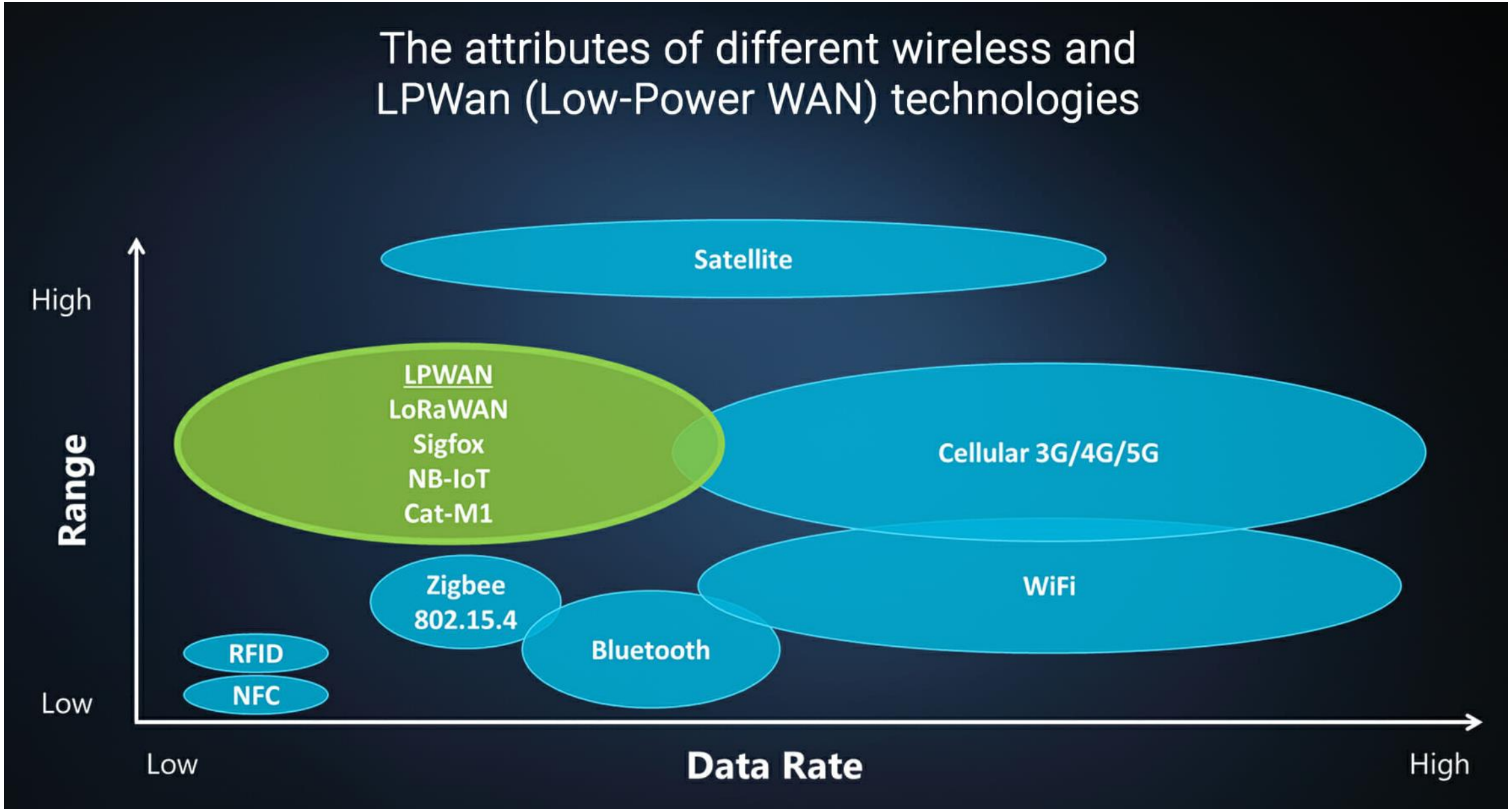
Useful Video Links for Low Power WAN Technologies

https://www.youtube.com/watch?v=grxnwoKDxAc&t=4s

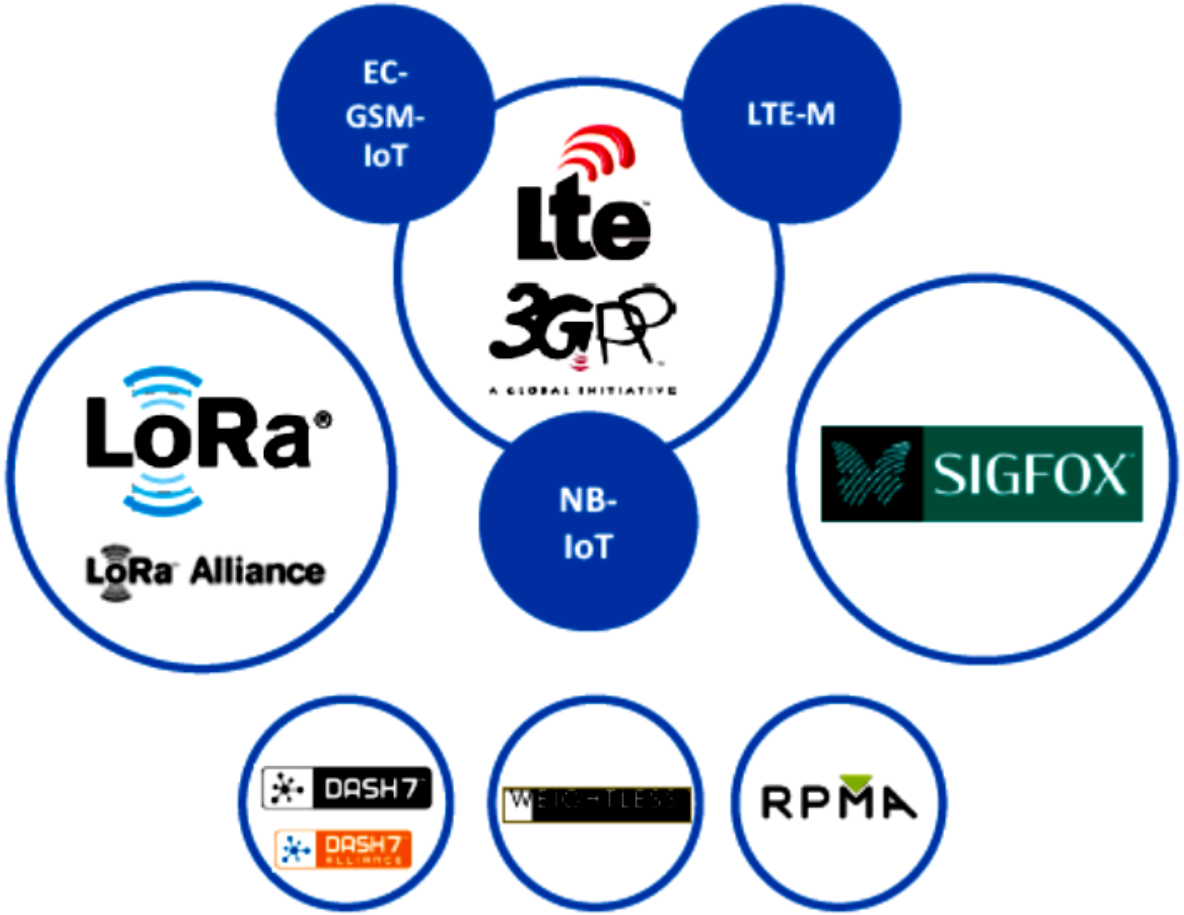
https://www.youtube.com/watch?v=vqHOyQK6jJ8

https://www.youtube.com/watch?v=hMOwbNUpDQA

https://www.youtube.com/watch?v=8Oxcp9wQQnk For LoRA practical implementation


The attributes of different wireless and LPWan (Low-Power WAN) technologies
Satellite
High
Range
LPWAN
LoRaWAN
Sigfox
NB-IoT
Cat-M1
Cellular 3G/4G/5G
Zigbee
802.15.4
WiFi
Bluetooth
RFID
NFC
Low
Low
Data Rate
High

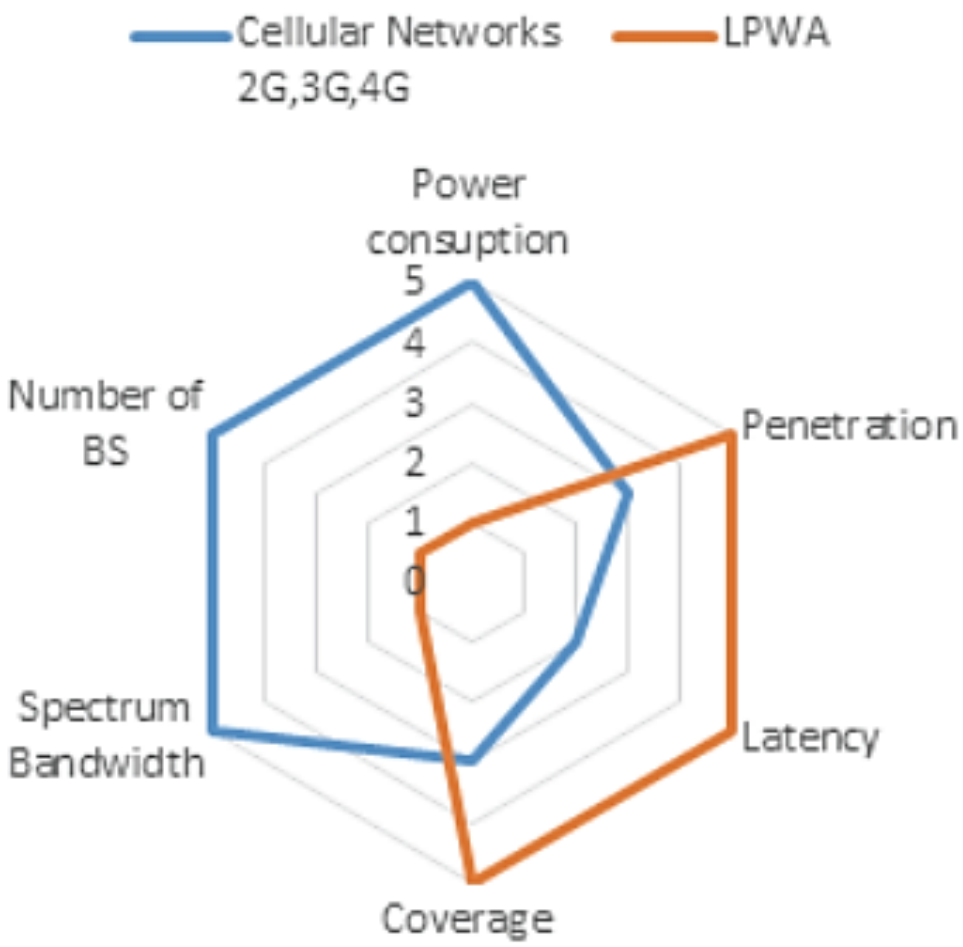
Technology landscape: LPWAN Technologies



- **LoRa** – proprietary / LoRaWAN open standard of LoRa Alliance, operate over ISM bands (5)
- **SIGFOX** – proprietary, developed by SigFox company, operate over ISM bands (6)
- **3GPP** - open standards, operate over LTE and GSM licensed bands:
  - **EC-GSM-IoT** - GSM enhanced technology to support low power wide area needs;
  - **LTE-M** (formally known as eMTC) - LTE evolution for IoT communications enabling a wide range of service;
  - **NB-IoT** – New LTE solution to support ultra-low bitrate applications.
- Other technologies: DASH7, Weightless, RPMA,…

Technology Comparative: Traditional Cellular vs LPWAN

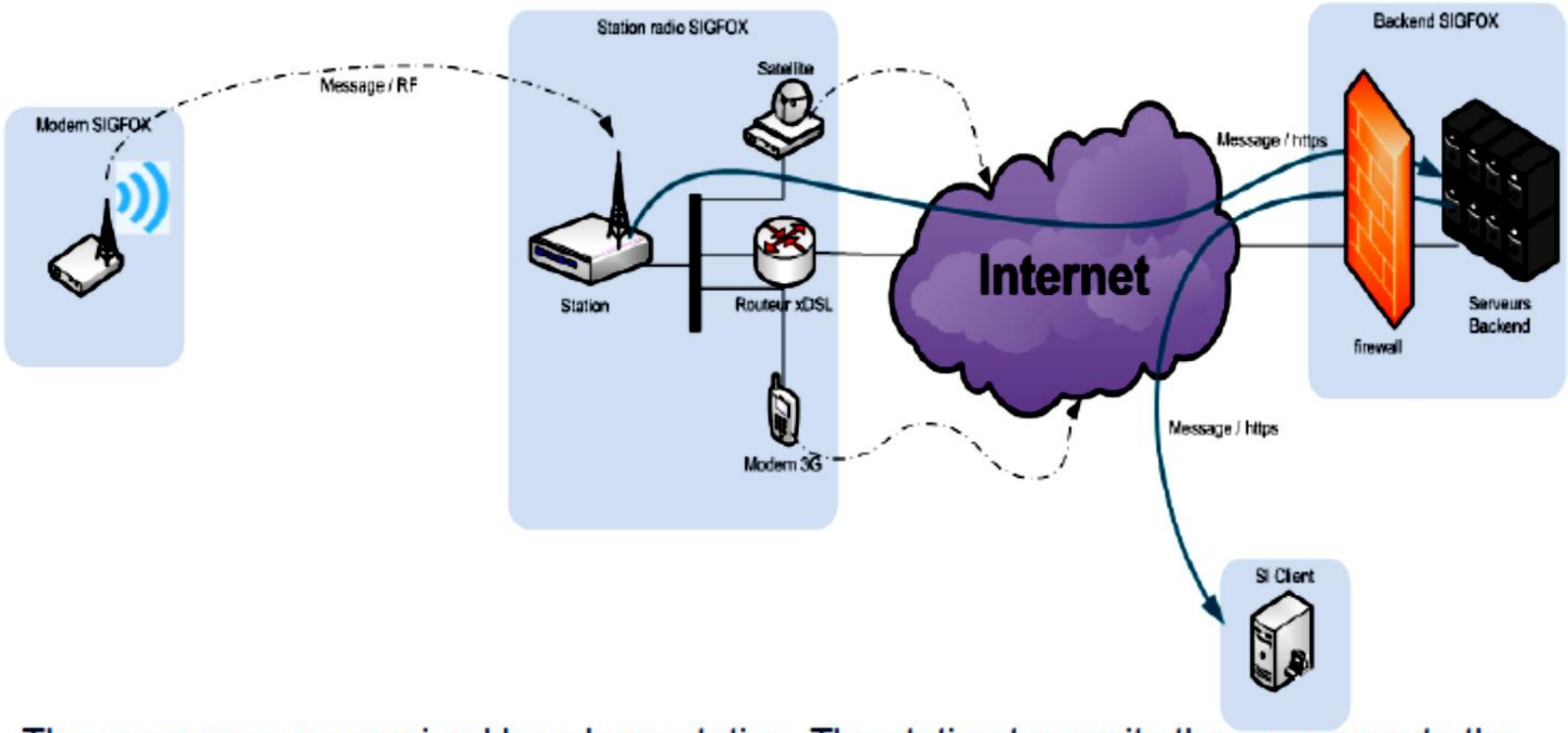
100 Mbit/s	4G				
10 Mbit/s	3G				
100 kbit/s		2G			LTE-M
10 kbit/s					NB-IoT EC-GSM LORA SIGFOX
Bit rate/ Battery life	Days	Weeks	Month	Years	Decades



(Qualitative Perspective Analysys)

- SIGFOX is a French start-up company founded in 2009
- Deploy long range infrastructure
- SIGFOX technology features modules able to send messages of **12 octets** maximum, with a maximum frequency of **140 transmissions per day**, and a data rate of **100 bits/s.**
- Network operator model only (annual subscriptions/connected object)
- Deployment outside France by selected SNOs(Sigfox Network Operator).
- The transmission uses public, open but regulated ISM radio band (ISM 868 MHz in Europe, 902 MHz in the US/FCC).
- A Sigfox modem cannot transmit more than overall 30s / hour (1% of time, i.e. roughly 6 messages max/hour).

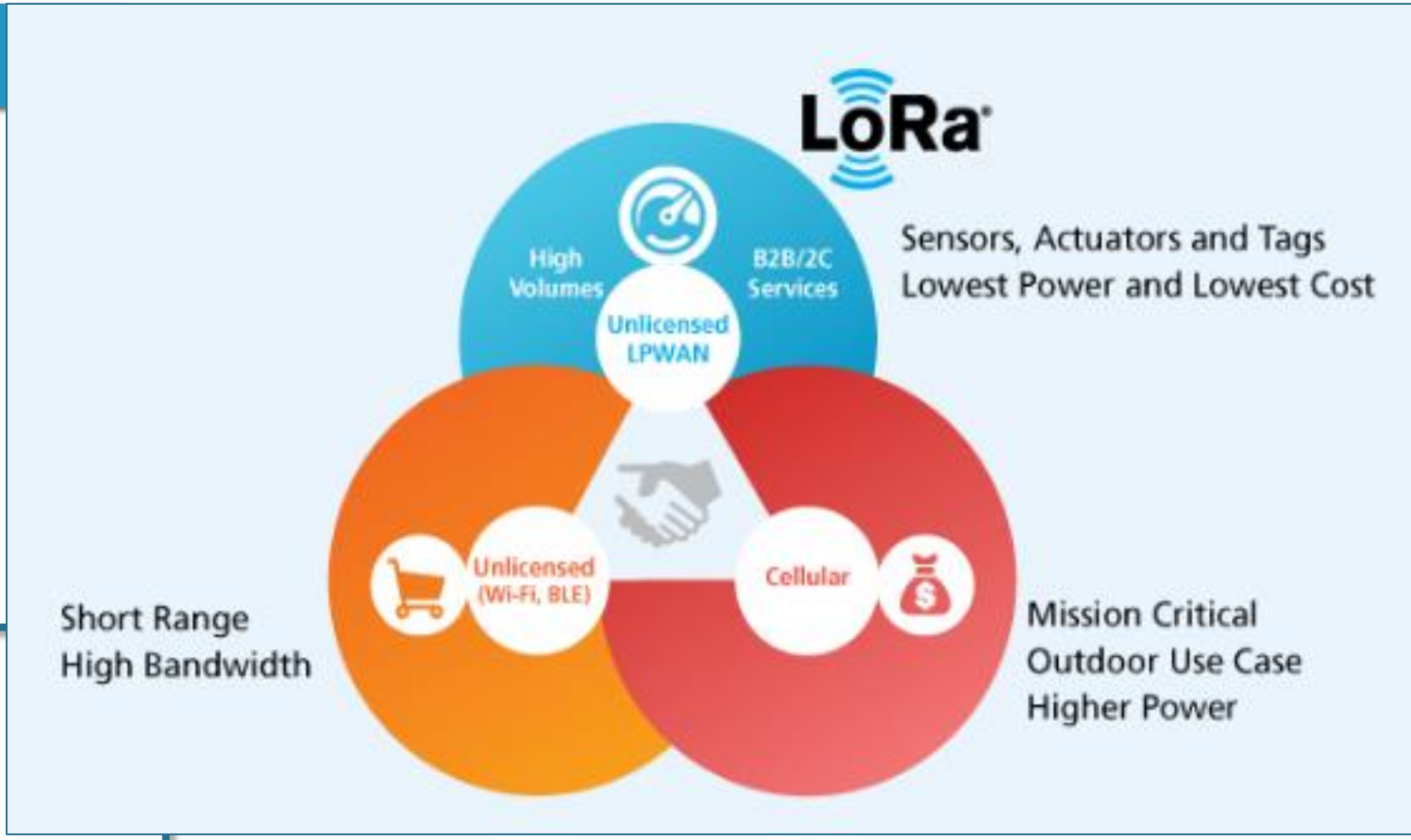
- Each device and each station have a unique Sigfox ID. The message are transmitted and signed with this ID. This signature authenticate the Sigfox device.
- Transmission mode is *fire and forget*: the modem does not wait for any acknowledgement from the base stations receiving the message. The modem has no awereness of the base station within its reach. Its missions are:
  - Multiple times transmission of messages (3 transmissions of the same message on 3 different canals)
  - The choice of transmission frequencies.
  - The choice of reception frequency which is calculated according to the frequency used for the last transmission

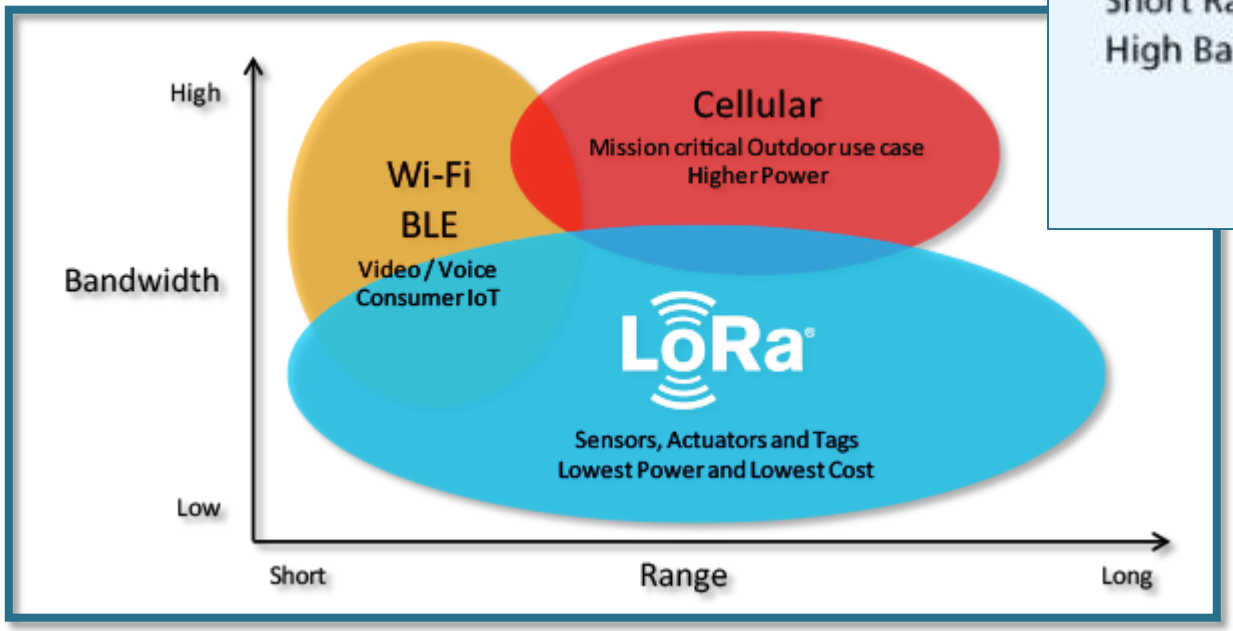


The messages are received by a base station. The station transmits the messages to the Backend (BE) through IP connectivity. The BE stores and sends the messages to the client Information System.

The BE can send messages to the base station and connect to it. Nonetheless neither the BE nor the base station can connect to the device.

LoRAWAN





https://lora-alliance.org/about-lorawan

https://youtu.be/WnrP5DRZGBU

LoRAWAN

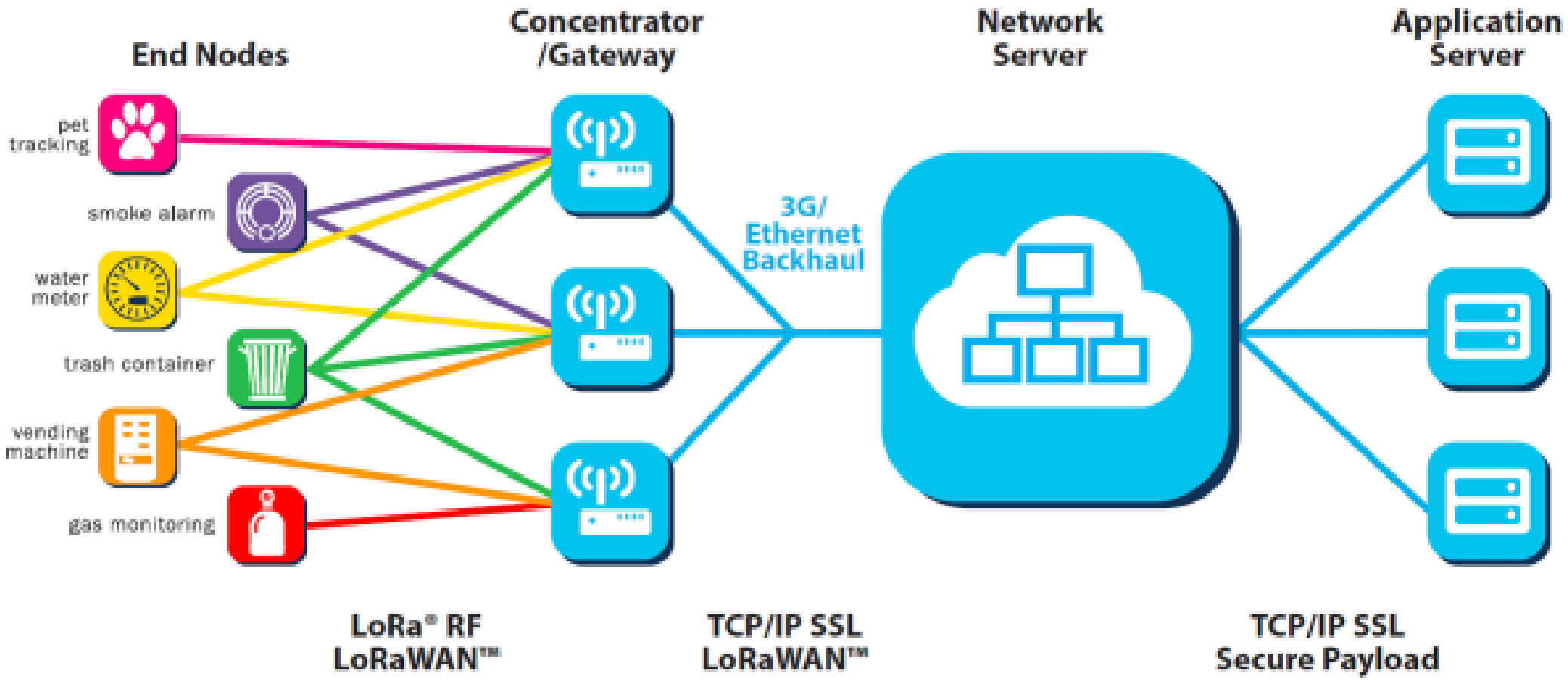
- Datarate of 0,3 to 50 Kb/s
- Encryption AES128 device – server & end-node – user app
- Stars of stars architecture
- 3 classes of devices (bidirectionnal communication)
  - A Class
  - B Class (beacon)
  - C Class (continuous)
- Uplink messages format

Preamble	PHDR	PHDR_CRC	PHYPayload	CRC

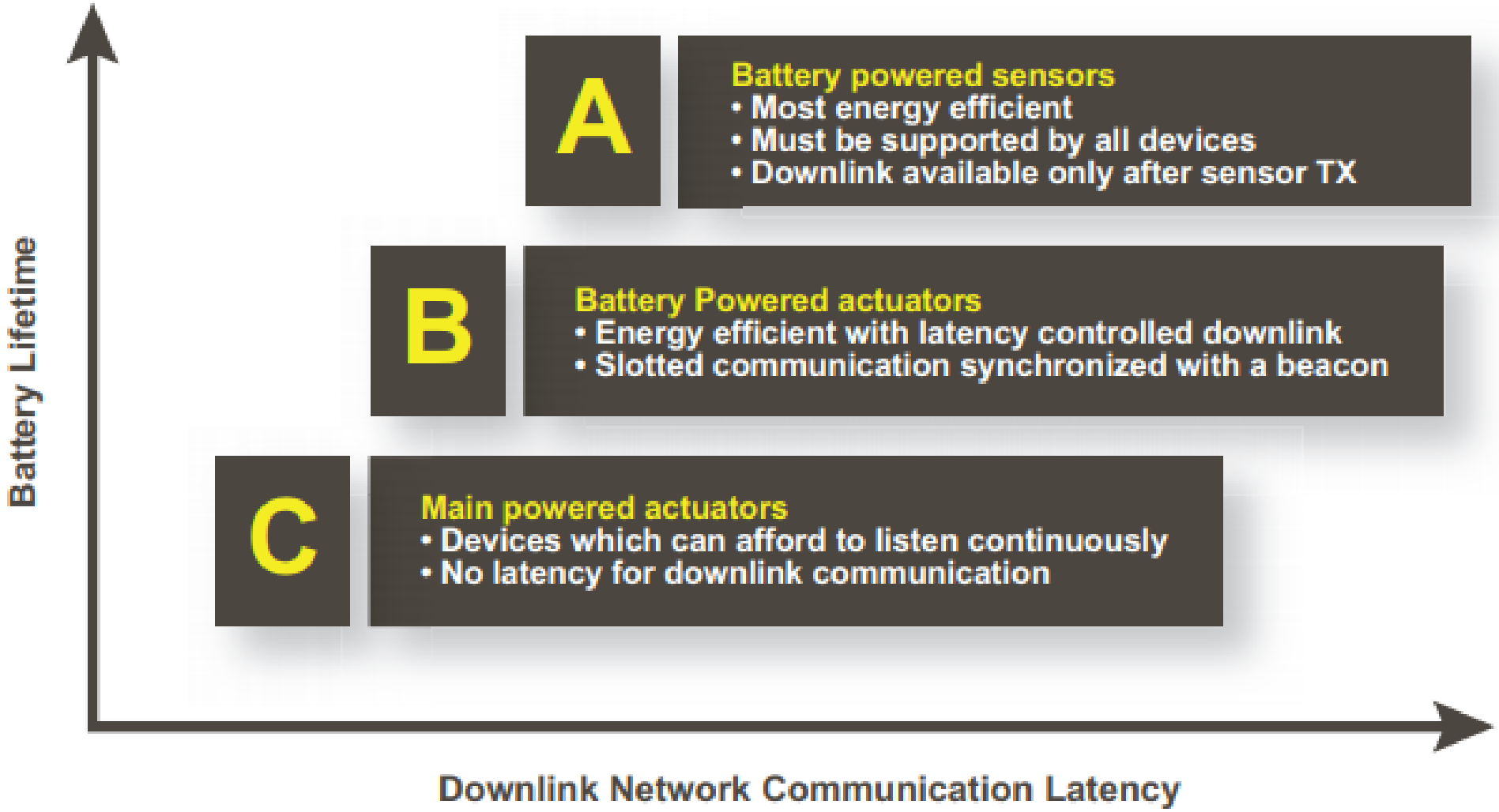
- Downlink messages format

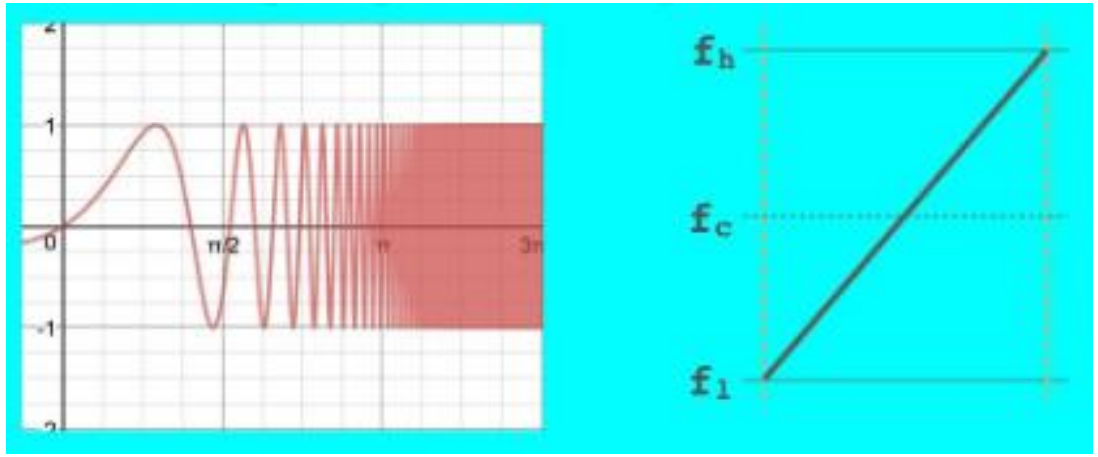
Preamble	PHDR	PHDR_CRC	PHYPayload

LoRA – Architecture

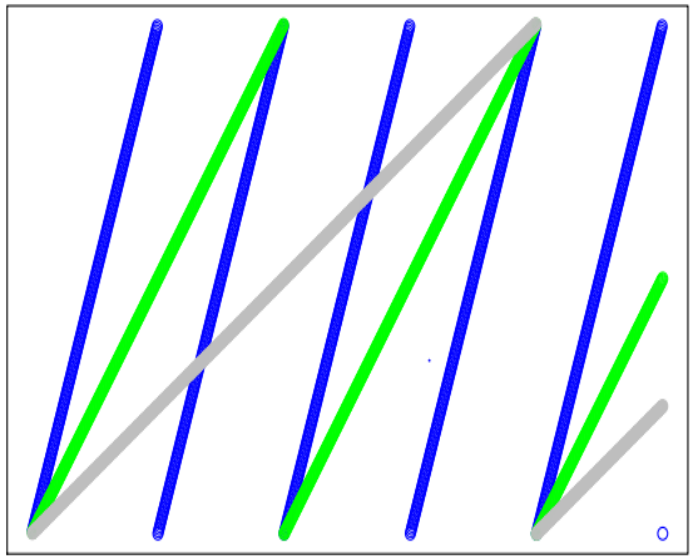


LoRA – Classes

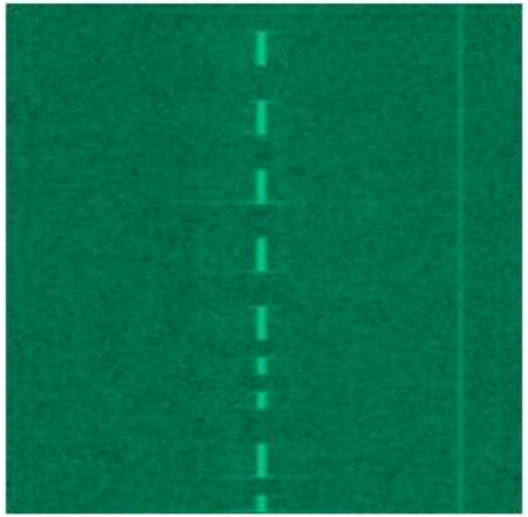




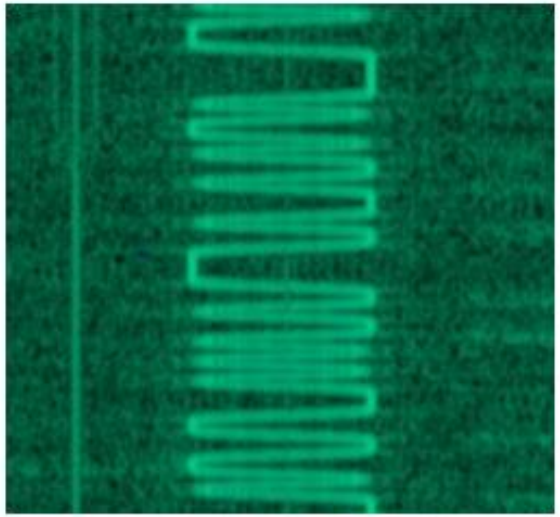
Chirp Spread Spectrum (CSS)



- SF7
- SF8
- SF9.



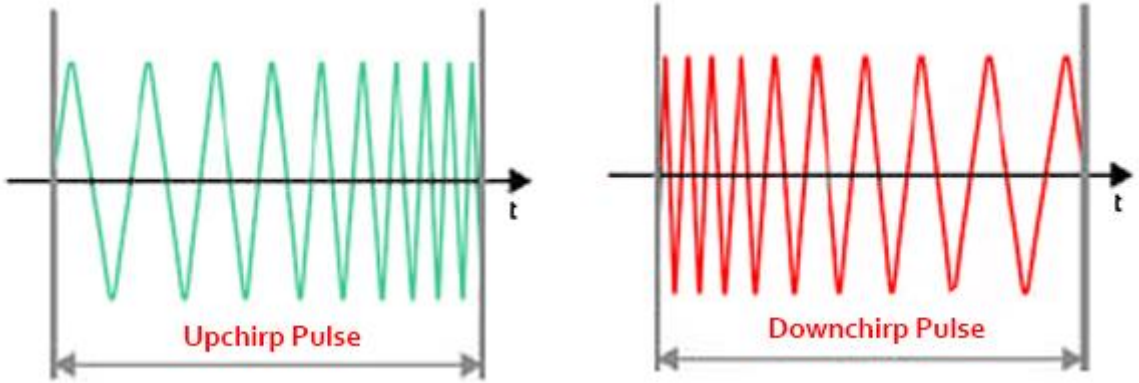
On-Off Keying

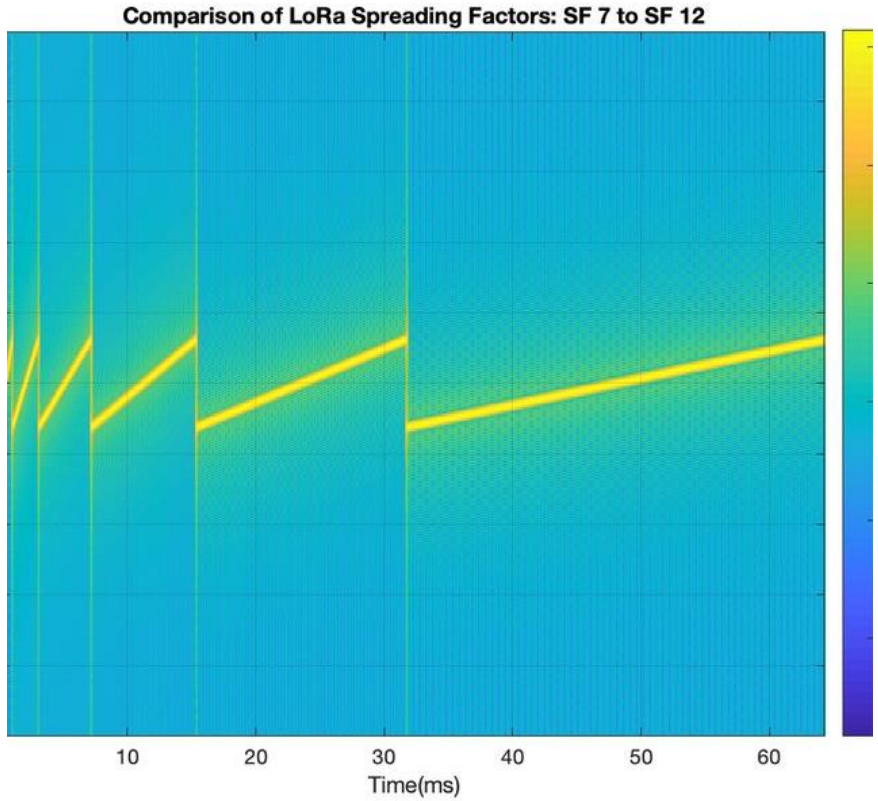


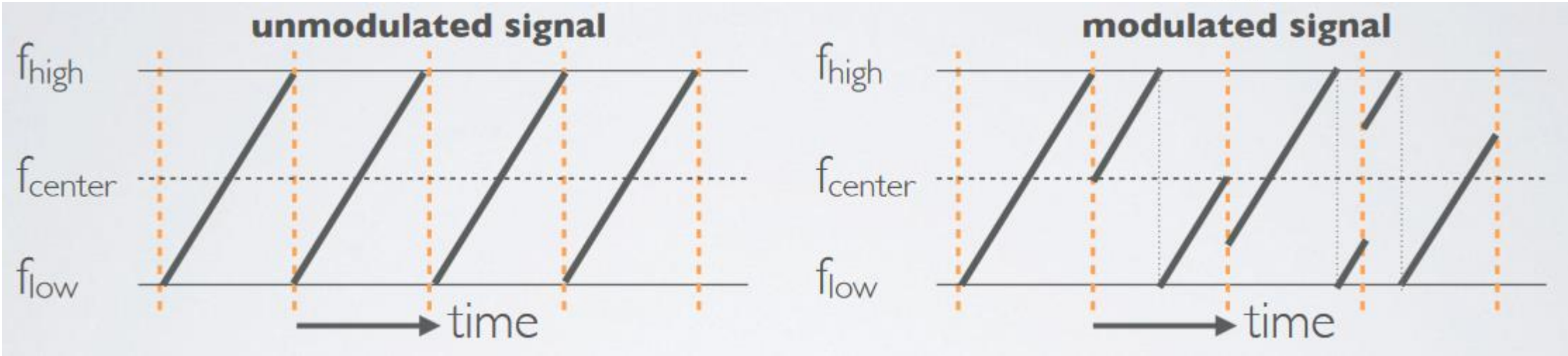
Frequency-shift Keying

LoRa

Chirp Spread Spectrum (CSS)

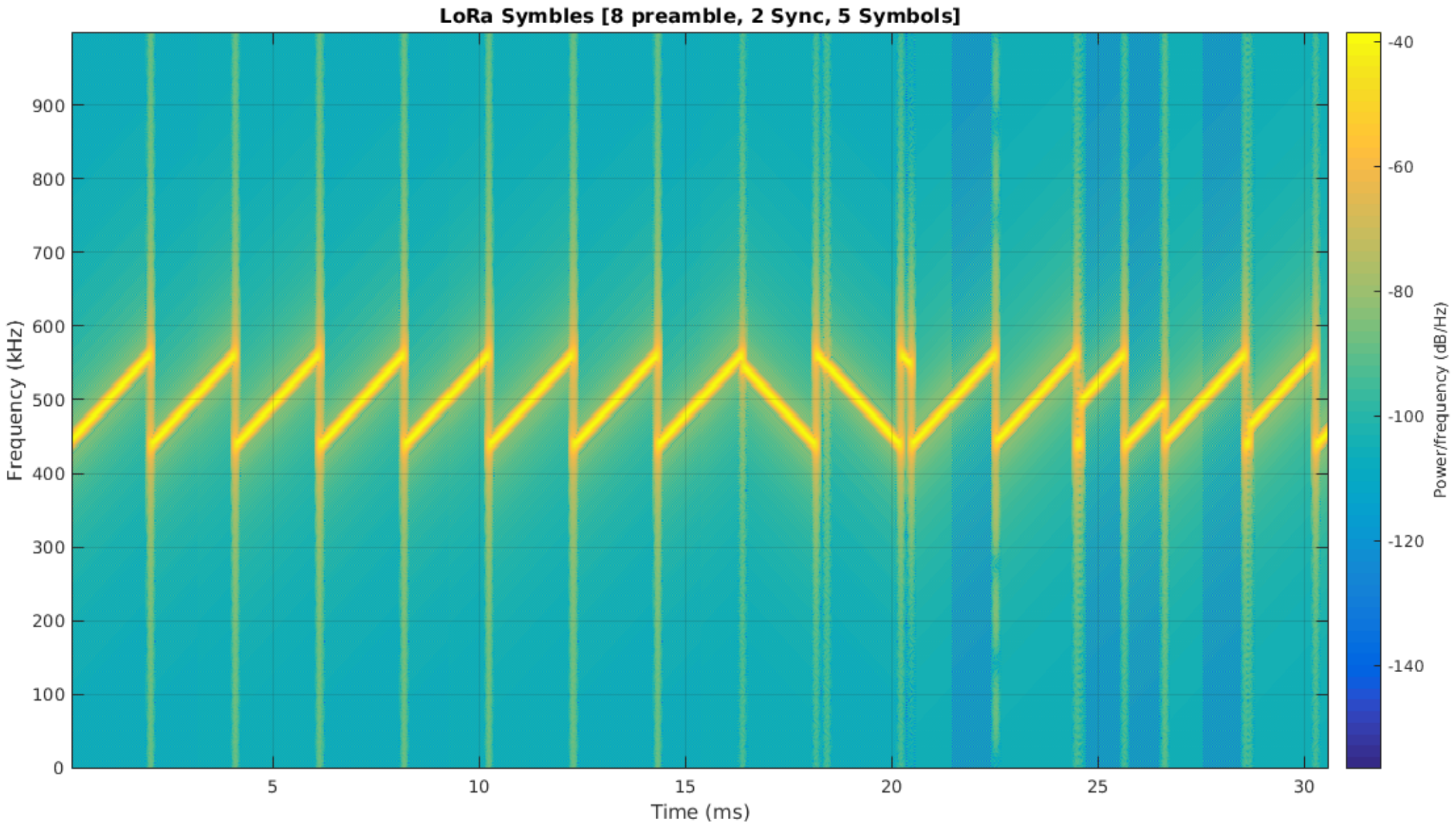






https://www.youtube.com/watch?v=dxYY097QNs0

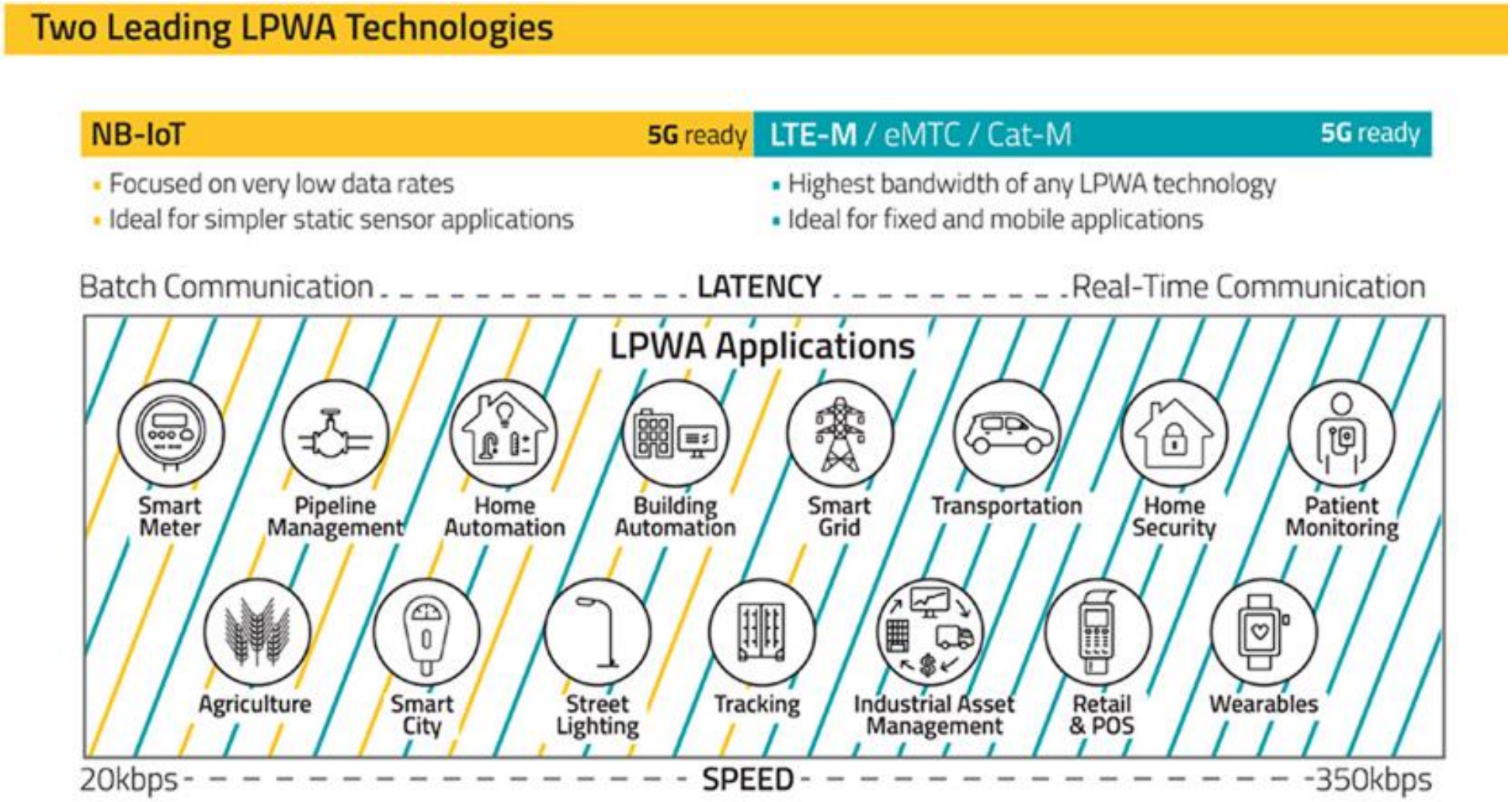
LoRA- Chirp Spread Spectrum (CSS)



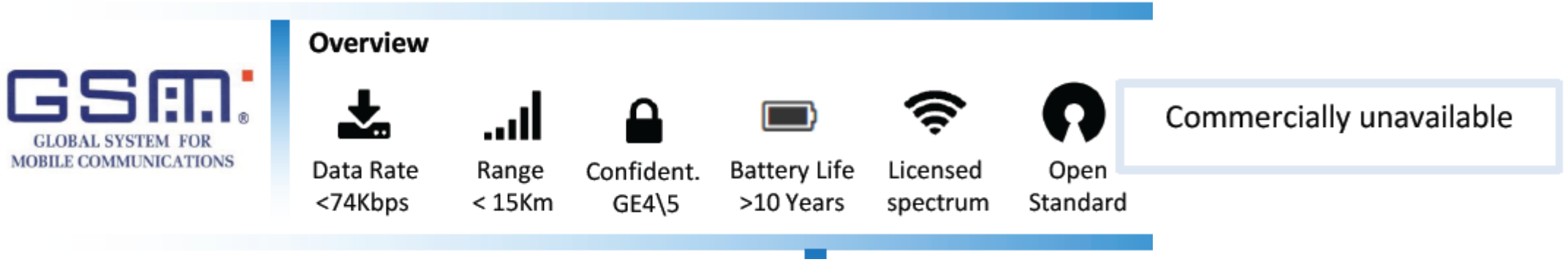
	SIGFOX	LORA
Frequency band	868/902 MHz (ISM)	433/868/780/915 MHz (ISM)
Urban range	3-10km	2-5km
Rural range	30-50km	15-20km
Packet size	12 bytes	Defined by user
Devices per access point	1M	100k
Status	In deployment	Spec released June 2015
Topology	Star	Star

	Sigfox	LoRa
Signal Bandwidth	on UNB (**Ultra narrowband**) — higher spectral efficiency and can mitigate the noise better	on CSS (**Chirp spread spectrum**)
Usage	is very practical for infrequent transmissions and offers longer battery life	uses more bandwidth
Business Model	is a network operator, so you wait for them to deploy, and you pay a subscription fee	can by deployed on your own to just cover your local area
Security	is better in preventing replay and man-in-the-middle attacks	weaker compared to Sigfox

Cellular IoT

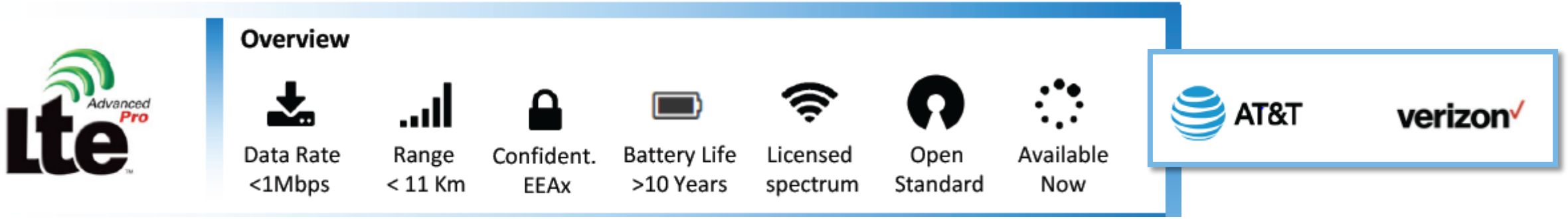


https://www.youtube.com/watch?v=csJWcz15MYY

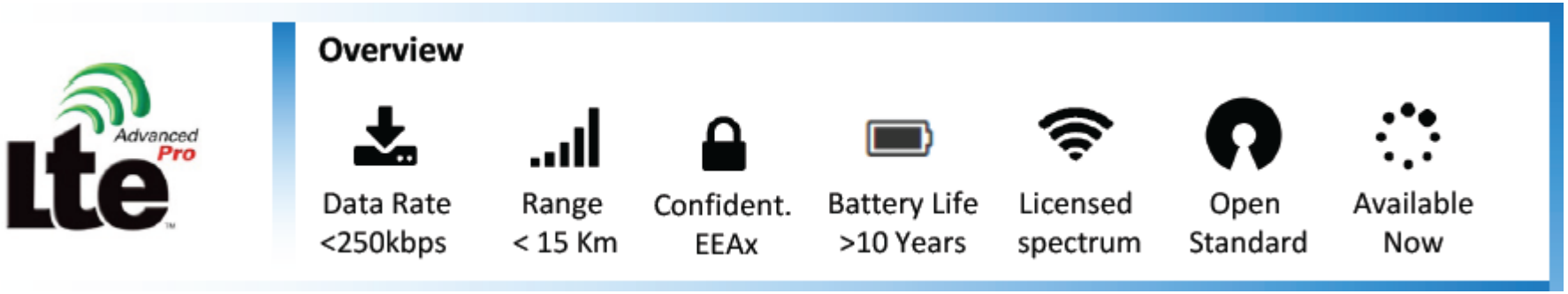


EC-GSM (Extended Coverage GSM) is a GSM enhanced technology to support low power wide area needs, operating in GSM bands.

- EC-GSM was standardized by 3GPP in Release 13 aiming at supporting long battery life, long range communications and high numbers of terminals per cell.
- EC-GSM is backwards-compatible to previous releases.
- EC-GSM adopts security and privacy features from mobile networks, including mutual authentication, confidentiality and data integrity.
- **Cat EC-GSM-IoT** user equipment was specified by 3GPP in Release 13 to work with EC-GSM-IoT networks



- eMTC (enhanced Machine-type communication) is a Release 13 LTE evolution for IoT communications enabling a wide range of services.
- LTE-M is the popular name for which **eMTC** is best known .
- LTE-M enables increased coverage, reduced complexity, lower cost and battery life of more than 10 years for a broad range of uses cases.
- LTE-M technology supports mobility, seamless handovers and low latency time intervals.
- It operates with a maximum channel bandwidth of 1.4 MHz within the 4G bands.
- To support LTE-M features, the existing LTE base stations only need a software update, keeping the hardware component unchanged.



- NB-IoT (Narrowband Internet of Things) is a new LTE solution, standardized in Release 13, to support ultra-low bit rate applications under licensed spectrum.
- NB-IoT aims to reduce terminal costs, being optimized for cheaper wireless modules, to enable very long battery life and to extend the radio coverage to support long range and deep indoor communications.
- NB-IoT may be deployed in a standalone mode by replacing a GSM carrier, it can be installed in the bandwidth reserved for LTE guard bands or may be deployed on LTE carriers of existing 4G networks.

- NB-IoT is answer for application requiring only limited data connections at low cost.
- LTE-M targets more advanced services allowing higher bandwidths, mobility and voice calls.
- EC-GSM and NB-IoT modules are less expensive than LTE-M ones.
- NB-IoT is the most flexible technology in terms of spectrum usage and can be deployed on LTE, GSM UMTS bands.
- EC-GSM can be deployed on existing GSM networks being a suitable option in the absence of 4G systems.
- EC-GSM is the system with lower traction and is not being adopted by the market.

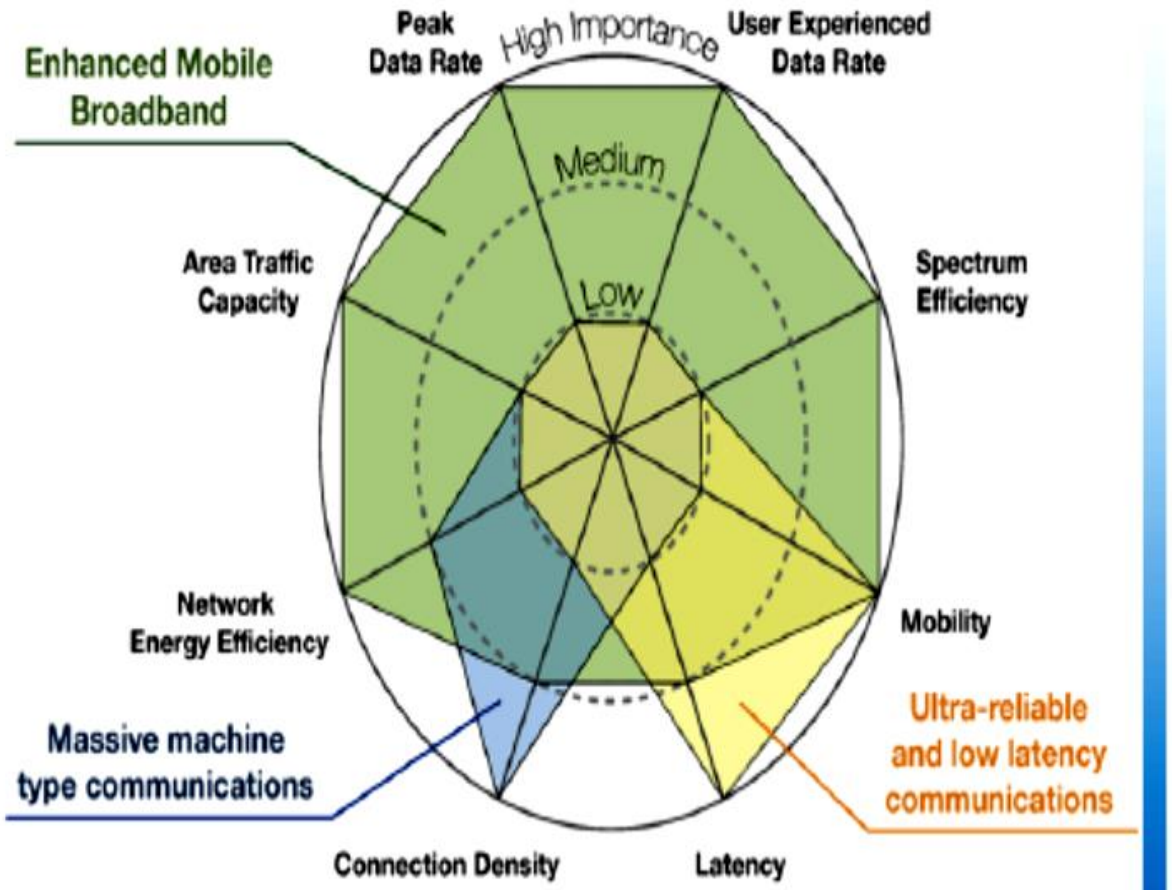
Parameter	EC-GSM	LTE-M	NB-IoT
Range	<15Km	<11Km	<15Km
Max peak data rate	74kbps	1Mbps	250Kbps
Spectrum	GSM bands	LTE bands	LTE in-band, guard bands, stand-alone
Voice	No	Yes	No
Typical module cost	Low	Medium	Low
Technology availability	On trial	Now	Now

	eMTC (LTE Cat M1)	NB-IOT	EC-GSM-IoT
Deployment	In-band LTE	In-band & Guard-band LTE, standalone	In-band GSM
Coverage*	155.7 dB	164 dB for standalone, FFS others	164 dB, with 33dBm power class 154 dB, with 23dBm power class
Downlink	OFDMA, 15 KHz tone spacing, Turbo Code, 16 QAM, 1 Rx	OFDMA, 15 KHz tone spacing, 1 Rx	TDMA/FDMA, GMSK and 8PSK (optional), 1 Rx
Uplink	SC-FDMA, 15 KHz tone spacing Turbo code, 16 QAM	Single tone, 15 KHz and 3.75 KHz spacing SC-FDMA, 15 KHz tone spacing, Turbo code	TDMA/FDMA, GMSK and 8PSK (optional)
Bandwidth	1.08 MHz	180 KHz	200kHz per channel. Typical system bandwidth of 2.4MHz [smaller bandwidth down to 600 kHz being studied within Rel-13]
Peak rate (DL/UL)	1 Mbps for DL and UL	DL: ~50 kbps UL: ~50 for multi-tone, ~20 kbps for single tone	For DL and UL (using 4 timeslots): ~70 kbps (GMSK), ~240kbps (8PSK)
Duplexing	FD & HD (type B), FDD & TDD	HD (type B), FDD	HD, FDD
Power saving	PSM, ext. I-DRX, C-DRX	PSM, ext. I-DRX, C-DRX	PSM, ext. I-DRX
Power class	23 dBm, 20 dBm	23 dBm, others TBD	33 dBm, 23 dBm

Parameter	LoRa	SigFox	EC-GSM	LTE-M	NB-IoT
Range (36)	<15Km	<50Km	<15Km	<11Km	<15Km
Maximum coupling loss (37)	157dB	153dB	164dB	160dB	164dB
Max peak data rate (37)	50kbps	100bps	74kbps	1Mbps	250Kbps
Spectrum	Unlicensed EU 868, 433MHz US 915MHz (41)	Unlicensed EU 868-869MHz US 902-928MHz (42)	GSM bands	LTE bands	LTE in-band, guard bands, stand-alone
Bandwidth	<500KHz (36)	100KHz (36)	200KHz per ch.(38)	1.08MHz (38)	180KHz (38)
Radio Tecnhology	Spread Spectrum (36)	Ultra Narrow Band (39)	TDMA/FDMA	OFDM	OFDM
Bidirectional modes (37)	Yes	Yes	Yes	Yes	Yes
Voice (Ericsson)	No	No	No	Yes	No
Device max transmitted power	14dBm	20dBm	23,33dBm (38)	20, 23dBm (38)	23dBm (38)
Autonomy (36)	>10years	>10years	>10years	>10years	>10years

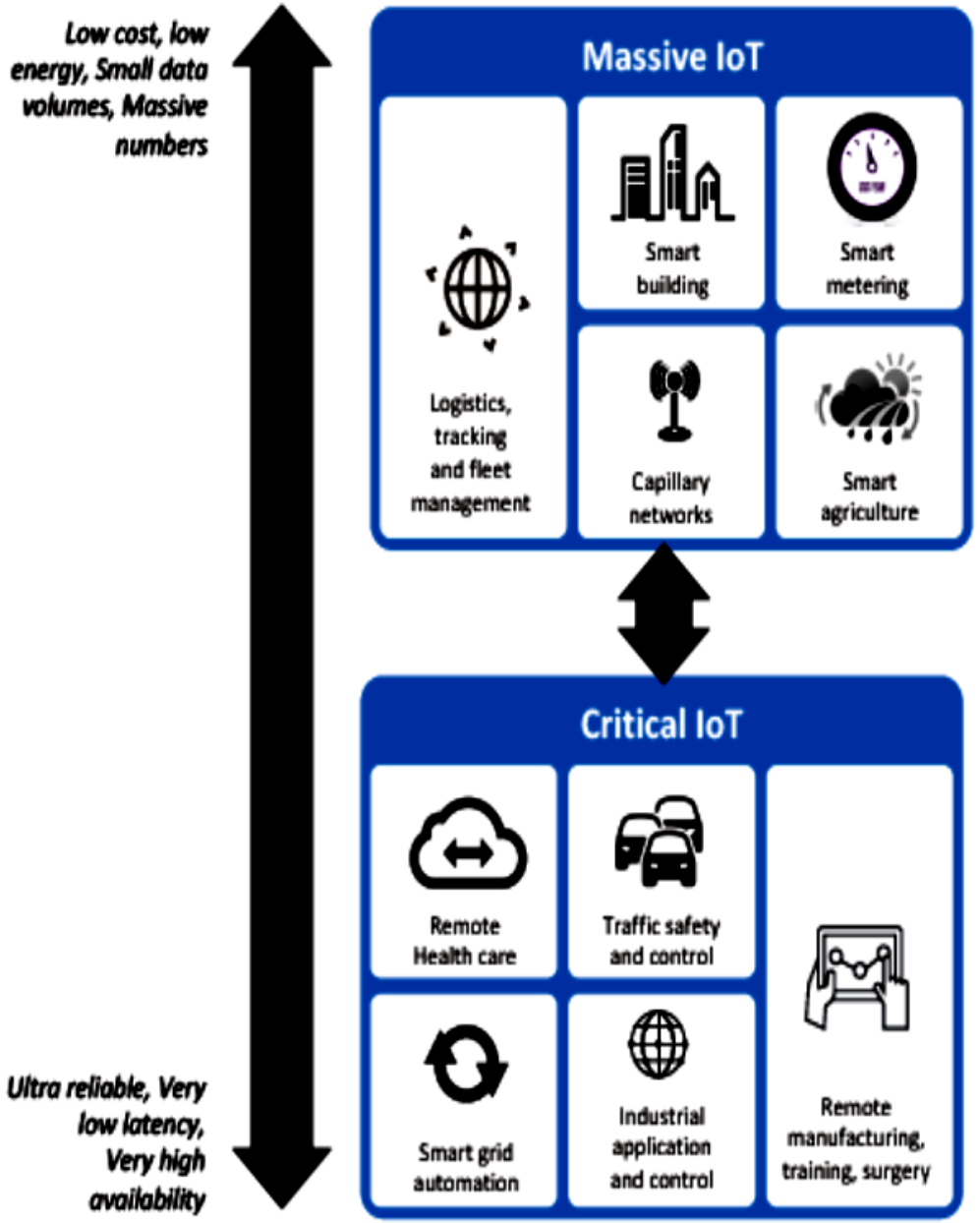
Parameter	LoRa	SigFox	EC-GSM	LTE-M	NB-IoT
Re-use existing cellular networks	No	No	yes	yes	yes
Link adaption	Yes	No	Yes	Yes	yes
Device categories	yes	No	yes	yes	yes
Operational mode	Public or private	Public	Public	Public	Public
Handover	No	No	Not seamless	yes	Not seamless
Data confidentiality (37)	Yes (AppSKey)	No	Partial (GEA4/5)	Yes (EEAx)	Yes (EEAx)
Network authentication (37)	Optional	No	UMTS AKA	LTE AKA	LTE AKA
Typical module cost (37)	Low	Very low	Low	Medium	Low
Technology availability	Now	Now	On trial	Now	Now

5G key capabilities in different usage scenarios



5G scenarios for IMT 2020 and beyond are centred on three core cases:

1. **Enhanced Mobile Broadband** – Focused on human-centric requirements for accessing multimedia content, services and data.
2. **Ultra-reliable and low latency communications** – Addresses mission-critical communications scenarios.
3. **Massive machine type communications** – Targets enormous deployments of low-cost devices typically with constrained capabilities.



- 3GPP is evolving its current standards to enable the Internet of Things market. The set of possible IoT use cases requires different connectivity characteristics and therefore different approaches are being taken.
- The first responses for massive IoT communications are already being defined on top of the existing cellular networks (EC-GSM, LTE-M, NB-IoT).
- 5G will be the answer for the majority of critical IoT communications requiring ultra-reliable and low latency features.