ITIC

UM
UNIVERSIDAD
DE MENDOZA

Wireless Sensor Network Protocols

Ing. Lucas Iacono

-2011-

lucas.iacono@um.edu.ar

Outline

1) What is WSN?

2) From point to point to mesh networks

3) Wireless Protocols

4) WSN. Which protocol can be used?

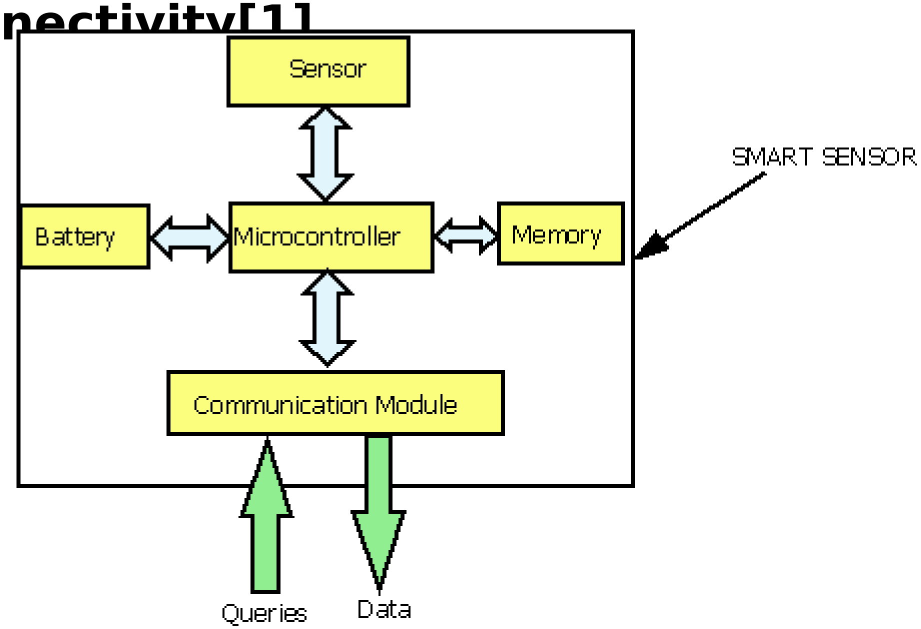
5) Expectations for the future of WSN protocols

1) What is WSN?

WSN: Definition, Hardware and Applications

Smart Sensors:

- **Replace** traditional analog sensor.
- Provide **improvements** in terms of **linearity, signal-to-noise ratio** and diagnostic features; **support network connectivity[1]**

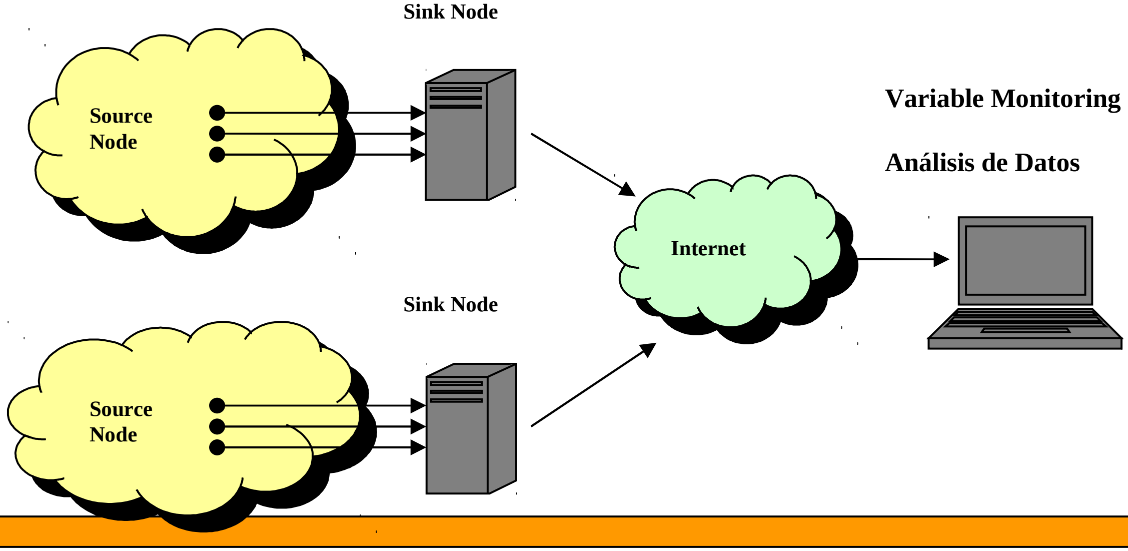


WSN: Definition, Hardware and Applications

- **Thanks** to the possibility of forming a **network**, the smart sensors can interact to **fulfill tasks** that usually, a single node is incapable to do.
- They use wired or wireless communication to enable this collaboration.
- The medium (wired or wireless) → depends on the application
- Healthcare sensor → hardware compactness and wireless comunications [2].
- Automotive and home automation → low cost [3].

WSN: Definition, Hardware and Applications

- In WSN the **data sensed** by the smart sensors **(nodes)** can be **transferred to a Gateway**, and **transmitted** through different **types of networks** (such as Internet) toward **computer systems**.
- Nodes can also have the **capacity to act on the environment**. WSNs are mostly used in, **low bandwidth and delay tolerant.**
- WSN nodes must meet requirements of **autonomy, low power consumption, low cost and robustness.**



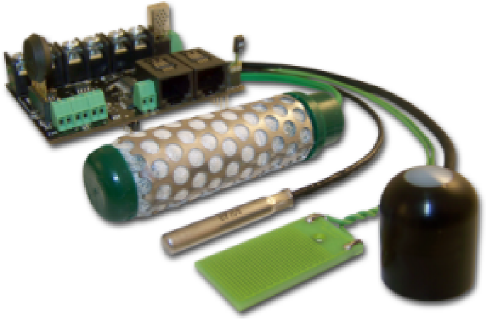
2) From point to point to mesh topologies networks

First Step: send data

- Large number of applications need to **send data acquired by sensors**, **to users** who are in a different place where the sensors are located.
- Due to this need, it was necessary to use **hardware and protocols that allow to send data to remote terminals.**
- Smart sensors, allow **remote reading** of measured parameters and to do **changes in the setup** of the sensor if it is required.
- The **first step** to do, is send **data from one node to a sink node**. The **simplest way** to establish a connection is the **point to point link**, where two nodes communicate directly.
- Limitation in WSN comes from the basics of radio communication and is the inherent power limitation of rf communication, which results in a limitation on the feasible distance between a sender and a receiver[6].

Why a network?

- **Event detection:** Sensor nodes should report to the sink(s) once they have detected the occurrence of a specified event.
- **Periodic measurements:** Sensors can be tasked with **periodically reporting** measured values. Often, these reports can be t**riggered** by a detected event.



Why a network?

- **Function approximation:** The way a physical value like **temperature** changes from one place to another can be regarded as a **function of location**. A WSN can be used to approximate this unknown function (to extract its spatial characteristics), using a **limited number of samples** taken at each individual sensor node.

- **Tracking:** The source of an **event can be mobile** (e.g. building security). The WSN can be used to report updates on the event source’s position to the sink(s).

Why a network?

- To carry out the interactions between nodes (which are common to most WSN applications), **it must comply with the next conditions:**

- **Type of service C**onventional communication **network service** is evident: it **moves bits** from one place to another. For a **WSN**, moving bits is only a **means to an end**, but not the actual purpose. **“People want answers, not numbers” (Steven Glaser, UC Berkeley, in [ ]).**

- **Quality of Service:** Some cases, only occasional **delivery of a packet** can be more than enough; In yet other cases, **delay** is important when actuators are to be controlled in a real-time fashion by the sensor network.

  Traditional **packet delivery ratio** is an **insufficient metric**.

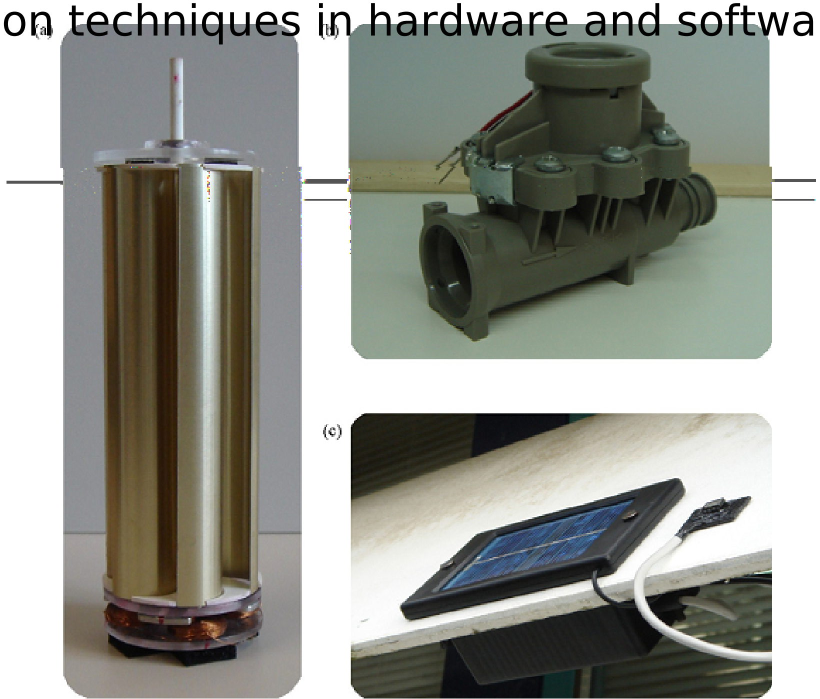
Why a network?

- **Fault tolerance:** Nodes may run out of energy, might be damaged, or the wireless communication between two nodes can be permanently interrupted.

  The WSN **must to be able to tolerate** such faults. To tolerate node failure, **redundant deployment** is necessary, using more nodes than would be strictly necessary if all nodes functioned correctly.

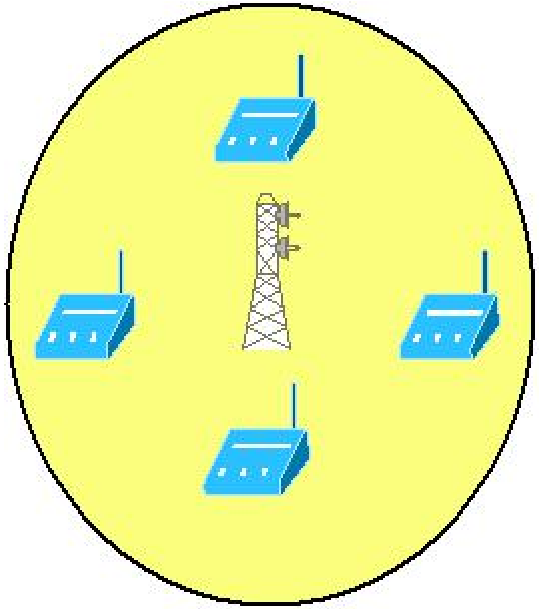
Why a network?

- **Lifetime:** In many scenarios, nodes will have to rely on a limited supply of energy (using batteries). Replacing these energy sources in the field is usually not practicable, and simultaneously, a WSN must operate at least for a given mission time or as long as possible.
- **Possible solutions:** Alternative power sources (solar, wind, etc), power consumption reduction techniques in hardware and software.



Why a network?

- **Scalability:** A WSN might include a **large number of nodes**, the employed architectures and protocols must be able scale to these numbers.



Why a network?

- **Programmability: Not only** will it be necessary for the nodes to **process information**, but also they will have to react flexibly on **changes in their tasks**.

  These nodes **should be programmable**, and their programming must be changeable during operation when new tasks become important.

- **Maintainability:** As both the environment of a WSN and the WSN itself change (depleted batteries, failing nodes, new tasks). **The system has to monitor its own health and status** to change operational parameters or to **choose different trade-offs** (e.g. to provide lower quality when energy resource become scarce).

Why a network?

- To **realize these requirements**, innovative mechanisms for a communication network have to be found, as well as new architectures, and protocol concepts.
- **Multihop wireless communication:** While wireless communication will be a core technique, a direct communication between a sender and a receiver is faced with limitations. In particular, communication over long distances is only possible using prohibitively high transmission power. The use of intermediate nodes as relays can reduce the total required power.
- **Energy-efficient operation:** To support long lifetimes, energy-efficient operation is a key technique.

  Options to look into include energy-efficient data transport between two nodes (measured in J/bit) or, more importantly, the energy-efficient determination of a requested information.

Why a network?

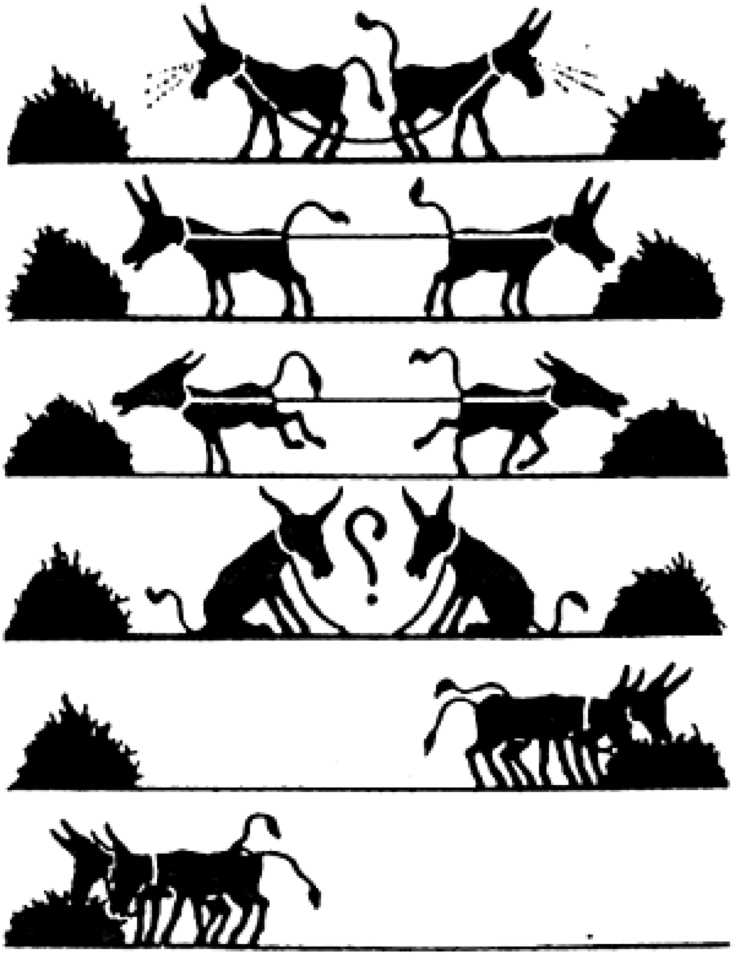
- **Locality** When nodes collect information at the moment to process the communication protocol. The node (which is primarily resource limited memory) should be treated just accumulate information of its neighbors. This allows the network to be composed of many nodes with limited resources.

  How to combine the locality principle with efficient protocol designs is still an open research topic.

Why a network?

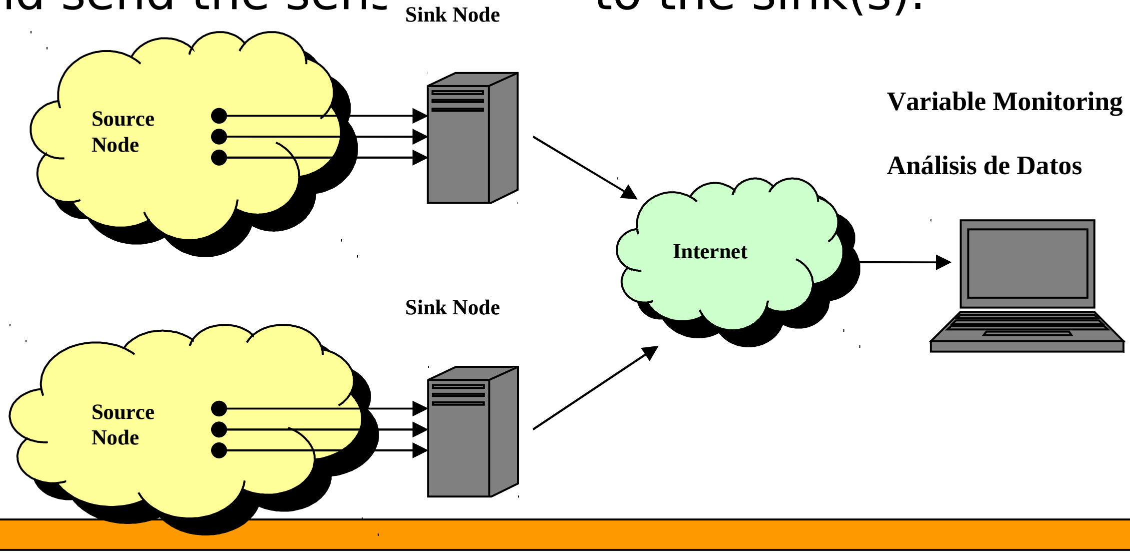
- **Exploit trade-offs** found the balance between different characteristics expected and at the same time contradictory, when designing the protocol and implementation.

- Example: A higher consumption of energy allows more accurate results.



Why of the different topologies in WSN:

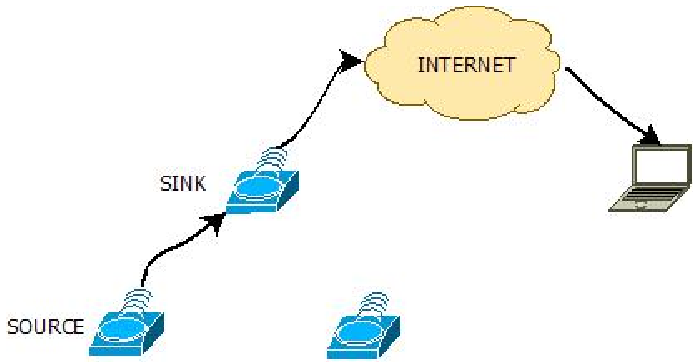
- **Two Types of Nodes Sink and Sources:**
- **Source:** Any component in the network that can provide information, that is, generally a sensor or actuator node.
- **Sink:** Component **where information is required**. The sink(s) sends queries or commands to the source nodes in the sensing region while the sensor nodes collaborate to accomplish the sensing task and send the sensed data to the sink(s).



Why of the different topologies in WSN:

- **SingleSink and Multisink Network.**

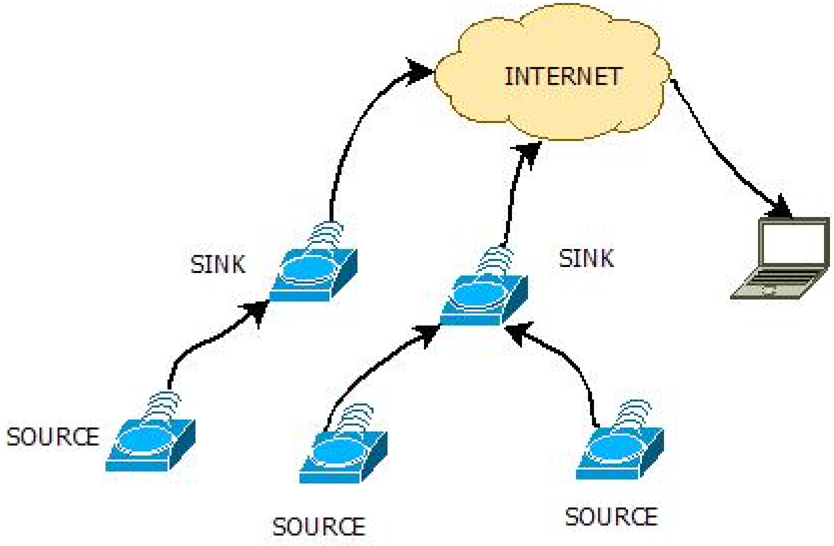
Single sink network: In this type of WSN there is only one sink located near or into the sensing region. All sensor nodes send their collected data to this sink.



Why of the different topologies in WSN:

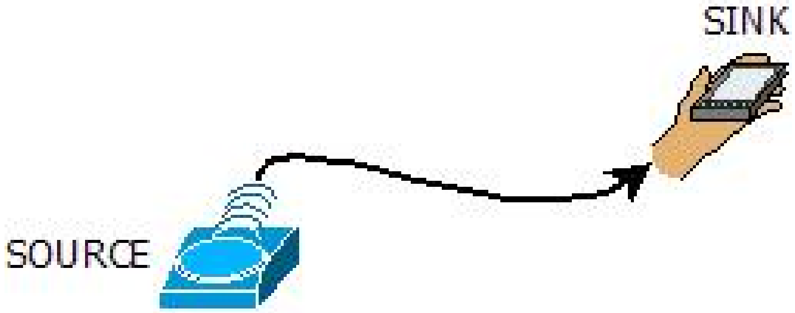
- **SingleSink and Multisink Network.**

Multisink network: in this case there may be many sinks located in different positions close to or inside the sensing region. Sensor nodes can send their data to the nearest sink, which can balance the traffic load of sensor nodes.



Why of the different topologies in WSN:

- **Single Hop and Multihop Network**
- **Single Hop[1]** all sensor nodes transmit their data directly to the sink, which makes **network control easy to implement**. This requires **long - range wireless communication**, which is costly in terms of energy consumption and hardware implementation.
- A single - hop network has simpler network architecture and thus is easier to control. It is suitable for applications in small sensing areas with sparsely deployed sensor nodes.

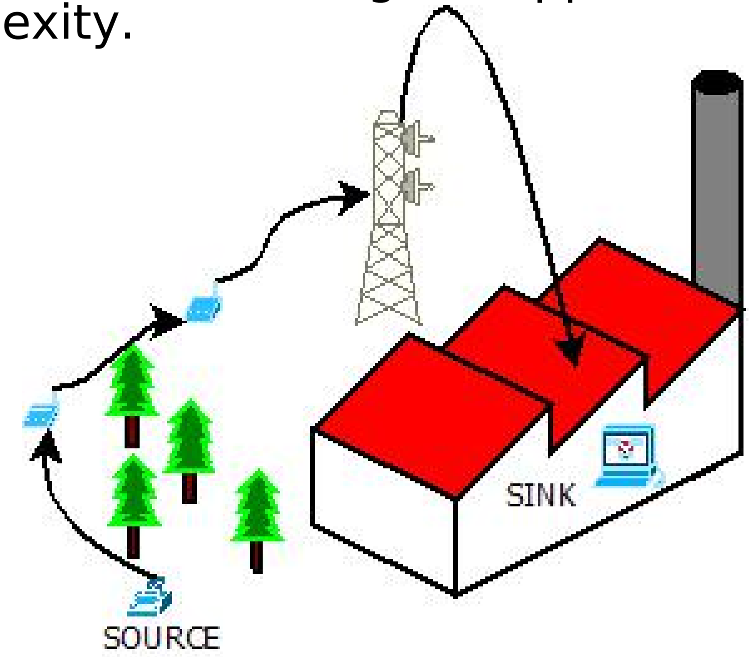


Why of the different topologies in WSN:

- **Multihop network[1]:** sensor nodes transmit their sensed data to the sink using short - range wireless communication via one or more intermediate nodes.

- Each intermediate node must perform routing and forward the data along a multihop path.

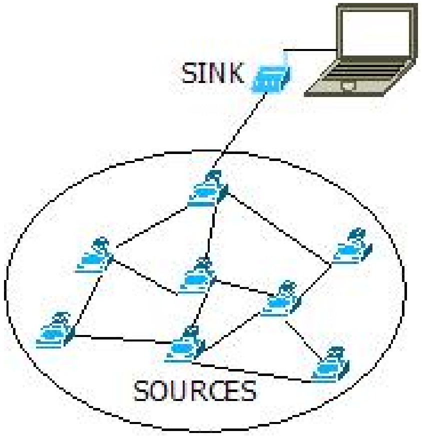
- Multihop networks have a wider range of applications at the cost of higher control complexity.



Why of the different topologies in WSN:

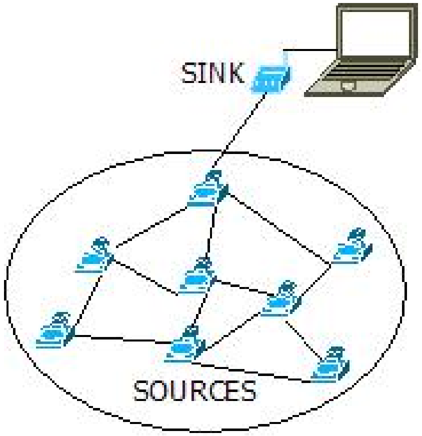
- **Multihop Network. Flat and Hierarchical Architecture.**

- **Flat Architecture[10].** Each node plays the same role in performing a sensing task and all sensor nodes are peers.



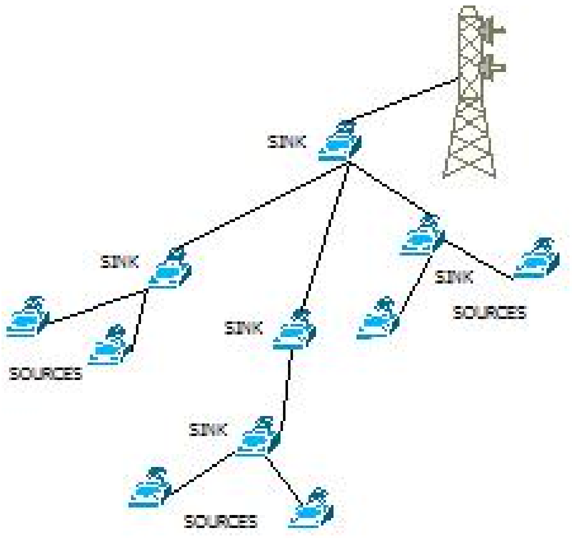
Why of the different topologies in WSN:

- Each sensor node communicates with the sink via a multihop path and uses its peer nodes as relays.



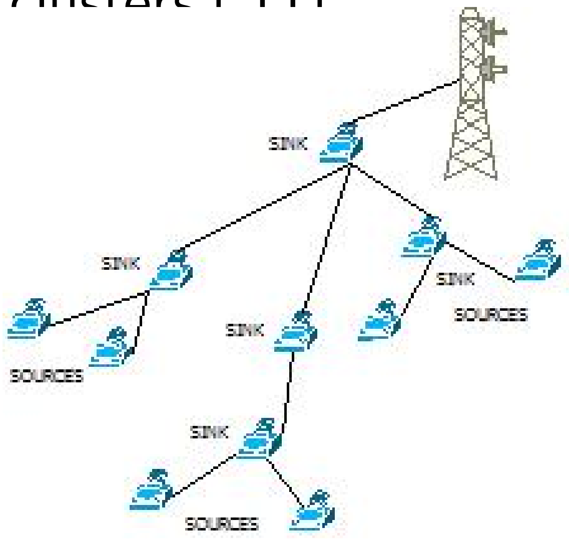
Why of the different topologies in WSN:

- **Hierarchical Architecture.** In a hierarchical network, sensor nodes are arranged in groups called clusters. The cluster members send their data to the cluster heads. The cluster heads forwards the data to the sink.
- A node with **lower energy** can be used to perform the **sensing task** and send the collected data to its cluster head at short distance.
- A node with **higher energy** can be selected as a **cluster head** to process the data from its cluster members and **transmit the processed data to the sink.**



Why of the different topologies in WSN:

- This process reduce the energy consumption for communication, balance trafic load and improve scalability when the network size grows.
- The problem with clustering is how to select the cluster heads and how to organize the clusters [11]



3) Wireless Protocols

MAC Protocols

- Medium Access Control (MAC) protocols solve a seemingly simple task: they **coordinate the times where a number of nodes access a shared communication medium.**

- For the case of **WSNs**, the balance of requirements is different from traditional (wireless) networks. Additional requirements come up, first and foremost, the need to conserve energy.

MAC Protocols

- **Reasons of Energy Waste:**

- **First reason:** When a receiver node receives more than one packet at the same time, these packets are called **“collided packets”.** All packets that cause the collision have to be discarded and the re-transmissions of these packets are required which increase the energy consumption.
- **Second reason: overhearing**, meaning that a node receives **packets that are destined to other nodes.**

MAC Protocols

- **Third reason:** energy waste occurs as a result of **control packet overhead**. Minimal number of control packets should be used to make a data transmission.

- **Fourth reason: Overemitting**, is caused by the transmission of a message when the **destination node is not ready.**

- **Conclusion:** A correctly-designed MAC protocol should prevent these energy wastes.

IEEE 802.15.4 Family Protocols

- The Institute of Electrical and Electronics Engineers (IEEE) finalized the IEEE 802.15.4 standard in October 2003 . The standard covers the physical layer and the MAC layer of a low-rate Wireless Personal Area Network (WPAN).

- The targeted applications for IEEE 802.15.4 are in the area of wireless sensor networks, home automation, home security, etc.

IEEE 802.15.4 Family Protocols

- **802.15.4 Types of nodes:** The standard distinguishes on the MAC layer two types of nodes:

- **Full Function Device (FFD):** can operate in three different roles: it can be a PAN coordinator (PAN = Personal Area Network), a simple coordinator or a device.

- **Reduced Function Device (RFD):** can operate only as a device.

IEEE 802.15.4 Family Protocols

- **Coordinator function:**

- **Manages a list of associated devices:** Devices are required to explicitly associate and disassociate with a coordinator using certain signaling packets.

- **Allocates short addresses to its devices:** All IEEE 802.15.4 nodes have a 64-bit device address.

  When a device associates with a coordinator, it may request assignment of a 16-bit short address to be used later in all communications between device and coordinator.

IEEE 802.15.4 Family Protocols

- In the beaconed mode of IEEE 802.15.4, it transmits regularly frame beacon packets announcing the PAN identifier, a list of outstanding frames, and other parameters.
- It exchanges data packets with devices and with peer coordinators.

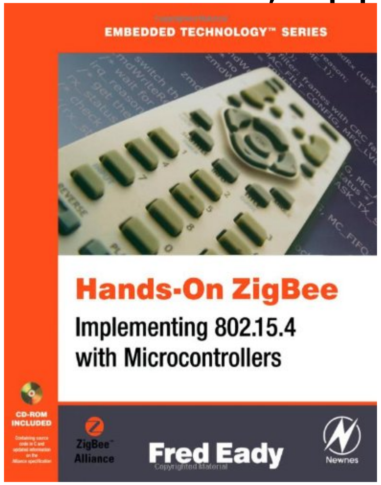
Zigbee

- **First:**

  ZigBee is not IEEE 802.15.4 and IEEE 802.15.4 is not ZigBee. ZigBee is a standards-based network protocol supported solely by the ZigBee Alliance that uses the transport services of the IEEE 802.15.4 network specification and adds more functionalities (full peer-to-peer/ mesh networks, application services, etc).

Source:

.


EMBEDDED TECHNOLOGY™ SERIES
Hands-On ZigBee
Implementing 802.15.4 with Microcontrollers
CD-ROM INCLUDED
ZigBee™ Alliance
Fred Eady
Newnes

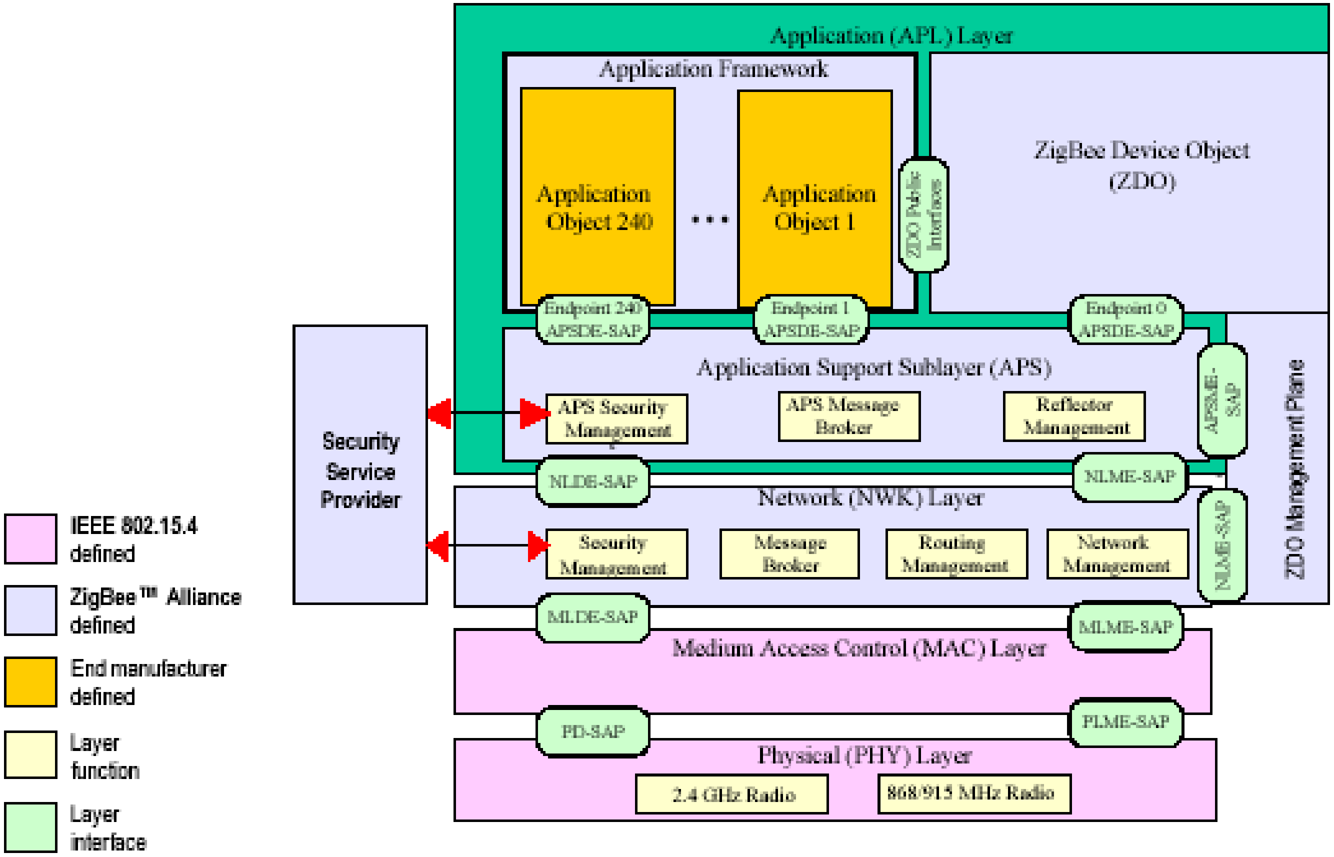
Zigbee

- The IEEE 802.15.4 MAC sublayer is in control of what is happening on the radio link.

- Acknowledgment, retransmission, flow control, and network synchronization tasks are managed by the IEEE 802.15.4 MAC sublayer .

- IEEE 802.15.4 MAC is in control of the access to the radio channel and employs the services of CSMA-CA (Carrier Sense Multiple Access - Collision Avoidance) to avoid packet collisions on the RF link.

Zigbee



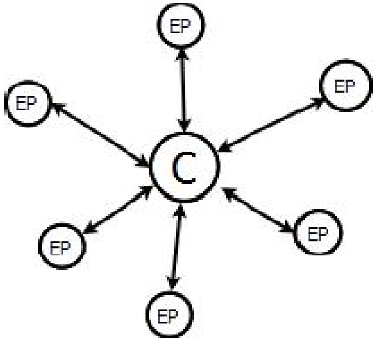
Outline of the ZigBee Stack Architecture (Source: Zigbee Alliance)

Zigbee

- **Zigbee Network topologies:** The ZigBee network layer (NWK) supports star, tree, and mesh topologies.

- **Star topology:** the network is controlled by one single device called the ZigBee coordinator. The ZigBee coordinator is responsible for initiating and maintaining the devices on the network. All other devices, known as end devices, directly communicate with the ZigBee coordinator.

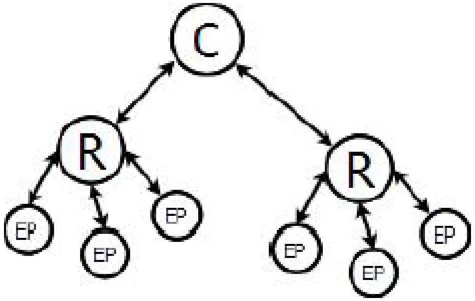
Star Network



Zigbee

- **Mesh and Tree topologies:** the ZigBee coordinator is responsible for starting the network and for choosing certain key network parameters, but the network may be extended through the use of **ZigBee routers**.
- In **tree networks**, routers move data and control messages through the network using a **hierarchical routing strategy.**

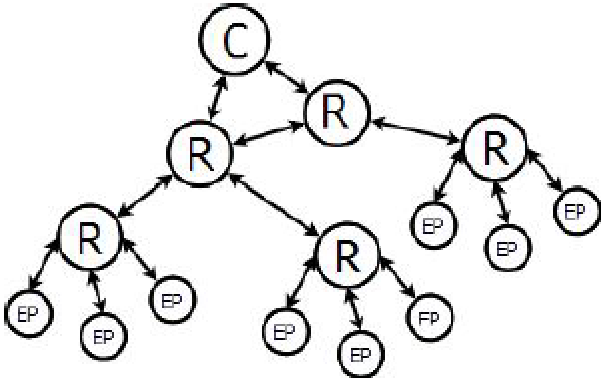
Tree Network



Zigbee

- **Mesh networks:** allow full peer-to-peer communication.

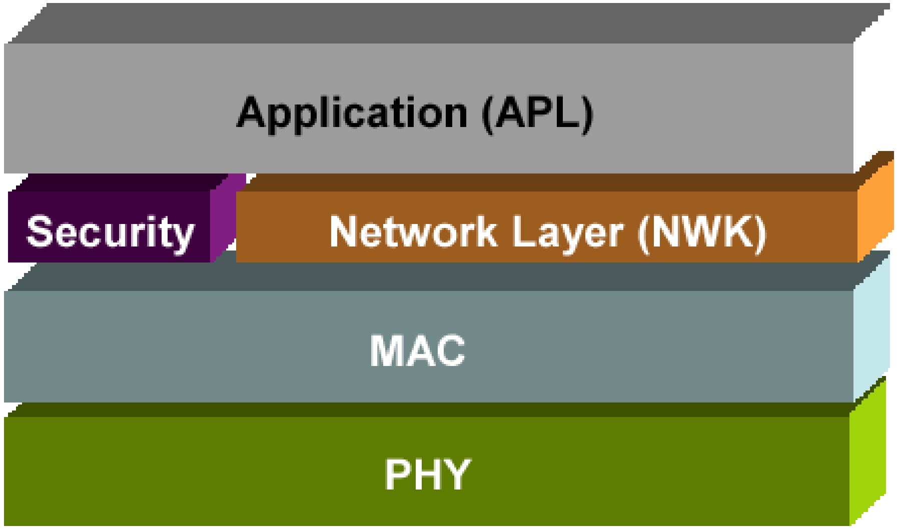
Mesh Network



The manufacturer's solution: Microchip MiWi

- The **MiWi™** protocol is based on the MAC and PHY layers of the IEEE 802.15.4 specification. It is designed in order to develop simple networks in the 2.4 GHz band.
- A network using the MiWi™ protocol is capable of having a **maximum of 1024 nodes** on a network.
- Each coordinator is only capable of having **127 children**, with a **maximum of 8 coordinators** in a network.
- Packets can travel a maximum of **4 hops in the network and 2 hops** maximum from the **PAN coordinator.**

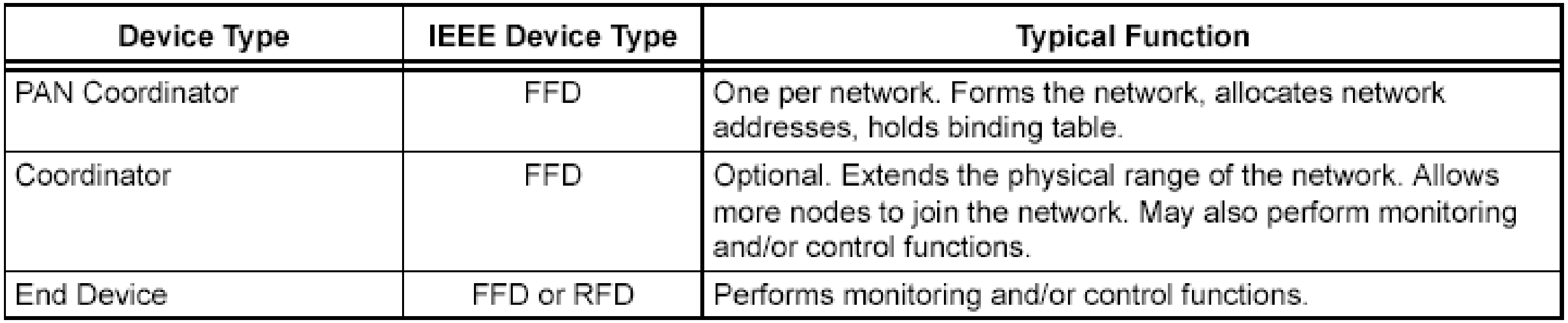
The manufacturer's solution: Microchip MiWi



- MiWi Protocol Stack *(Source: www.tecnoimprese.it)*

The manufacturer's solution: Microchip MiWi

- **MiWi™ devices:**



Device Type	IEEE Device Type	Typical Function
PAN Coordinator	FFD	One per network. Forms the network, allocates network addresses, holds binding table.
Coordinator	FFD	Optional. Extends the physical range of the network. Allows more nodes to join the network. May also perform monitoring and/or control functions.
End Device	FFD or RFD	Performs monitoring and/or control functions.

MiWi protocol Devices Type *(Source Microchip)*

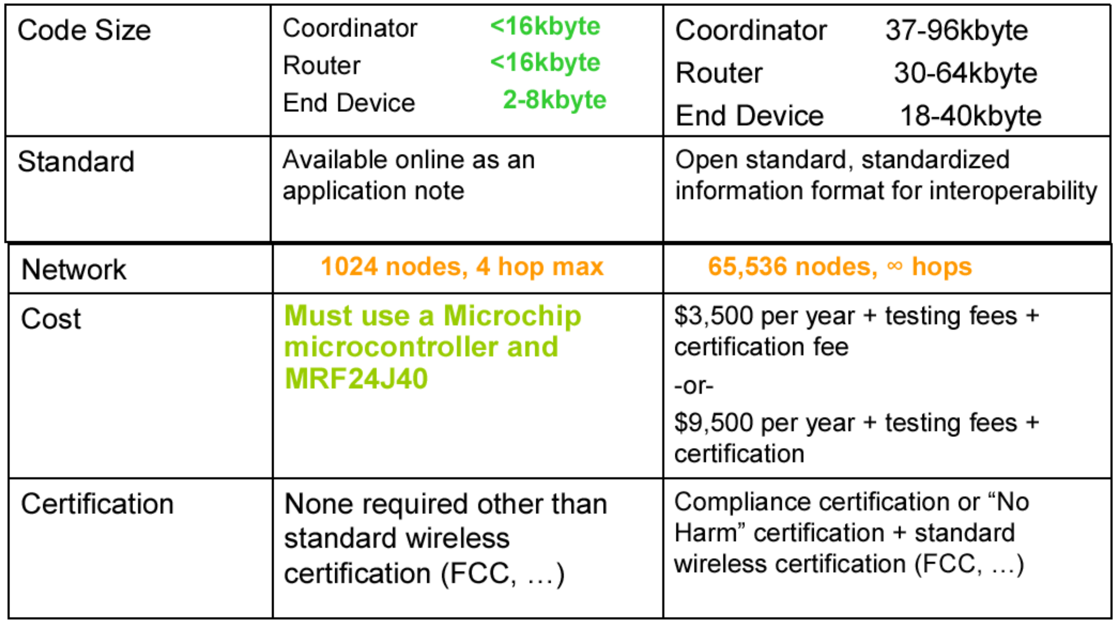
The manufacturer's solution: Microchip MiWi

- **Star Network Configuration:** End devices communicate only with the PAN coordinator.

- **Cluster Tree Network Configuration:** One PAN coordinator; and other coordinators are allowed to join in to the network. This forms a tree-like structure, where the PAN coordinator is the root of the tree, the coordinators are the branches of the tree and the end devices are the leaves of the tree.

- **Mesh Network Configuration:** Is similar to a cluster tree configuration, except that Full Function Device (FFDs) can route messages directly to other FFDs instead of following the tree structure.

The manufacturer's solution: Microchip MiWi



Code Size	Coordinator <16kbyte Router <16kbyte End Device 2-8kbyte	Coordinator 37-96kbyte Router 30-64kbyte End Device 18-40kbyte
Standard	Available online as an application note	Open standard, standardized information format for interoperability
Network	1024 nodes, 4 hop max	65,536 nodes, ∞ hops
Cost	**Must use a Microchip microcontroller and MRF24J40**	$3,500 per year + testing fees + certification fee -or- $9,500 per year + testing fees + certification
Certification	None required other than standard wireless certification (FCC, …)	Compliance certification or “No Harm” certification + standard wireless certification (FCC, …)

MiWi vs Zigbee (Source: www.tecnoimprese.it)

RF4CE

- The ZigBee RF4CE specification defines a simple, robust and low-cost communication network that allows wireless connectivity in consumer electronics applications.

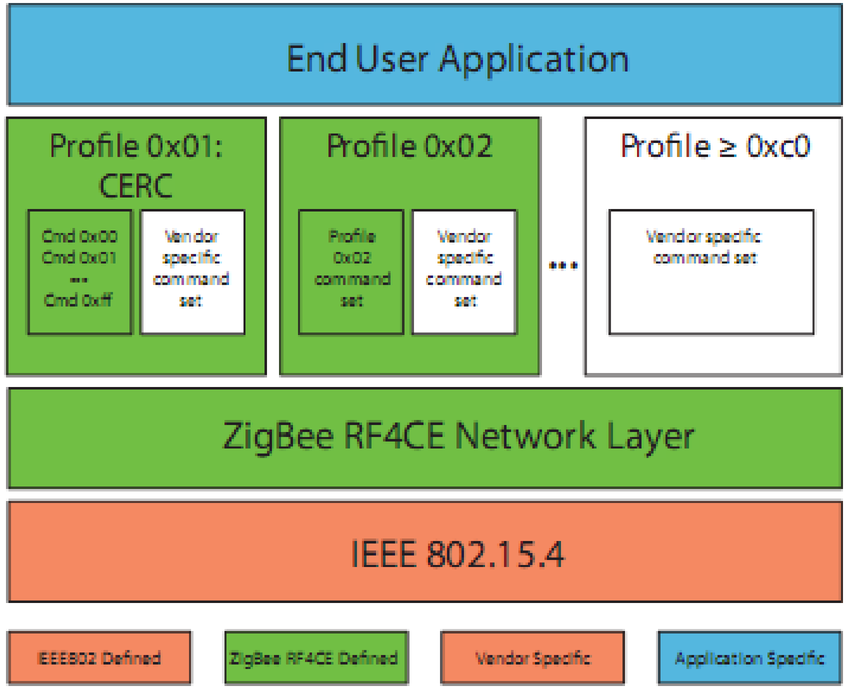
- ZigBee RF4CE is based on the IEEE 802.15.4 standard MAC and PHY layers and provides networking functionality and standard application profiles which can interface to the end user application.

RF4CE

- **Characteristics of a ZigBee RF4CE:**
- Operation in 2.4GHz frequency band
- Three RF channels.
- Discovery and Pairing mechanism with full application confirmation.
- Multiple star topology with inter-PAN communication.
- Various transmission options including unicast, broadcast, acknowledged, unacknowledged, secured and un-secured.
- Apply standard AES-128 **security scheme**.
- First public application profile targeted towards remote control applications.
- Allows for manufacturer specific profiles to be added.

RF4CE

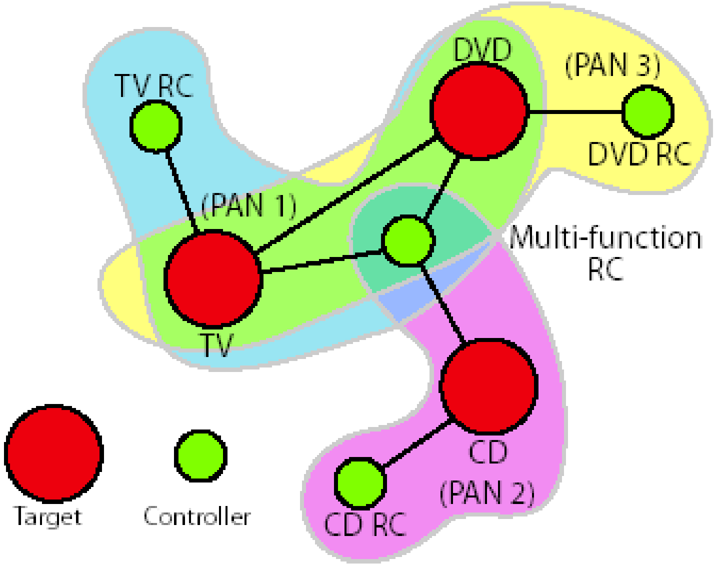
- **Types of devices:**
- **Target node:** This device has full PAN coordinator capabilities and is responsible for start the network.
- **Controller device:** It can join to the networks started by target devices by making a connection with the target node.



RF4CE Arquitecture *(Source Zigbee Alliance)*

RF4CE

- **Network topology:** ZigBee RF4CE uses a star topology and includes inter-PAN communication.

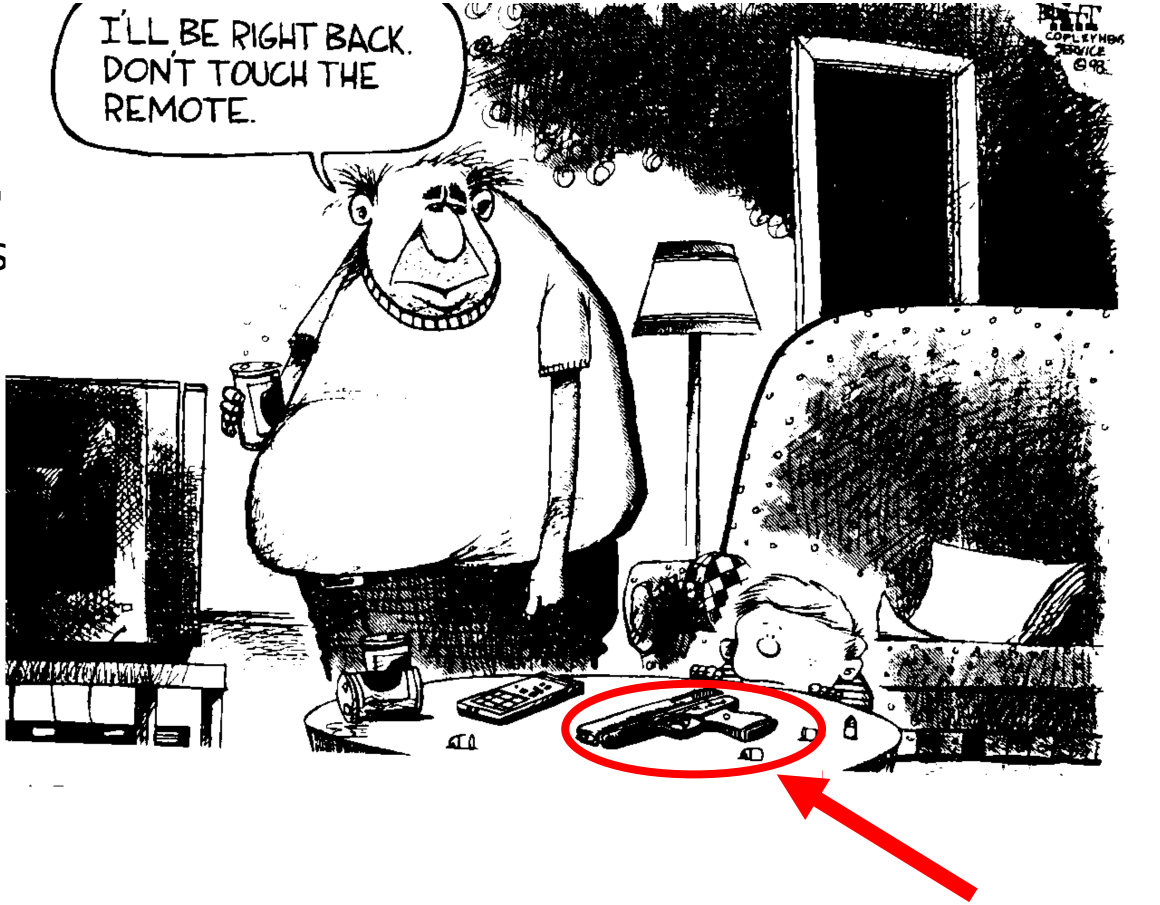


RF4CE Star Network *(Source Zigbee Alliance)*

RF4CE

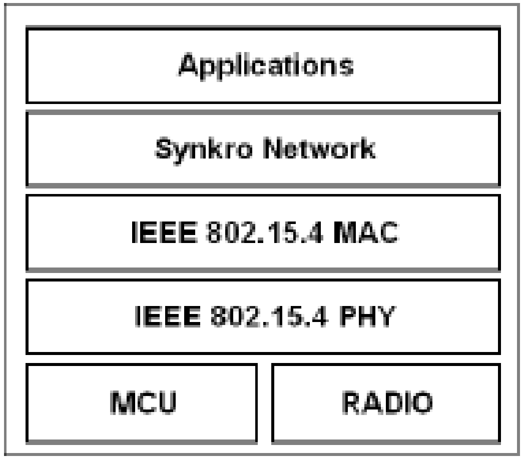
- **Why RF4CE?**

- **Advantage:** Low Cost**.**
- **Weakness:** 32 devices Maximum per target Node.
- **Applications:** RF Remote Control, Home Automation, Home Entertainment and Control.



The manufacturer's solution: Freescale SyncroRF

- **Freescale's Syncro RF:** The main difference of Synkro RF with RF4CE is that can not be implemented public profiles, so this aimed to developing low cost, ad-hoc applications.



RF4CE Arquitecture *(Source Freescale Semiconductors)*

The manufacturer's solution: Freescale SyncroRF

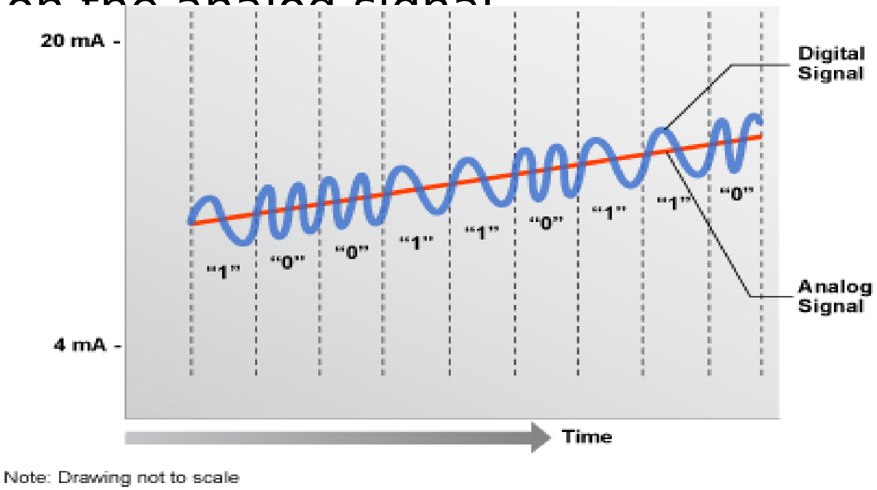
- **Characteristics:**
- An over the air data rate of 250 kbit/s in the 2.4 GHz band.
- 3 independent communication channels in the 2.4 GHz band.
- 2 network node types, controller and controlled nodes.
- Applications: Cable replacement, wireless control (toys)
- Advantage: Low Cost for Ad Hoc applications.
- Weakness: 32 devices Maximum per controlled Node, Public network profiles can´t be implemented

WirelessHart

- **What is Hart:** HART (Highway Addressable Remote Transducer) is a digital protocol for two-way communication between a **host application** and **smart field instruments**, providing access to diagnostics, configuration and process data[ ].
- “Smart” devices are field instruments with enhanced computing and communication capabilities that permit them to perform situational analysis not previously possible.
- A host can be any software application from technician's laptop, to a plant's process control, safety or other system using any control platform.
- **HART** specified a **physical layer** which used frequency-shift keying **(FSK)** to superimpose digital communication signals at a low level on top of the 4-20mA.

WirelessHart

- Two simultaneous communication channels: the 4-20mA analog signal and a digital signal.
- The 4-20mA signal communicates the primary measured value (in the case of a field instrument) using the 4-20mA current loop.
- Other device information (e.g. device status, diagnostics, additional, calculated values, etc.) is communicated using a digital signal that is superimposed on the analog signal.

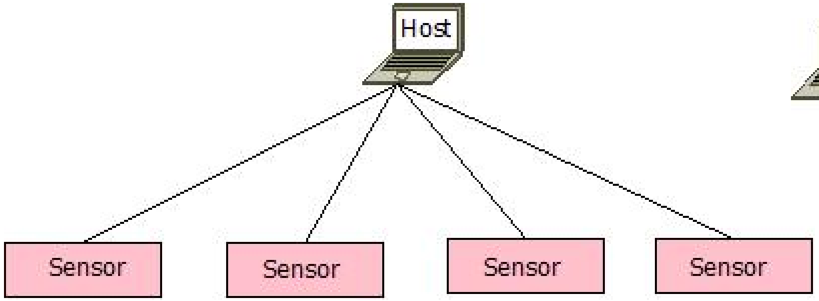


Note: Drawing not to scale

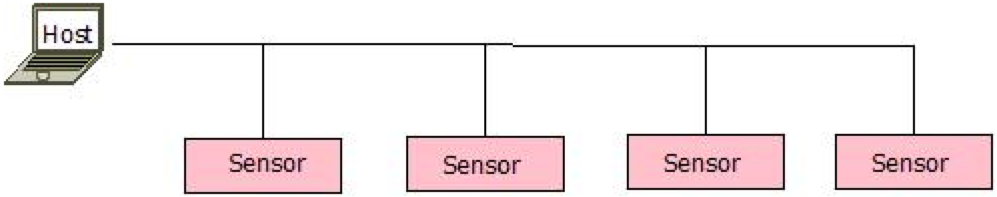
Digital over Analog

WirelessHart

- **Types of networks**
- **Point to Point:** In this type of networks, the host has one wire for each sensor. It minimizes the chance of failure because there is only one wire per sensor, but it increases the complexity of wiring.
- **Multidrop Network:** To the late 70's and early 80's, appeared on the market the first multidrop buses. (e.g. Modbus.). Multidrop networks (buses) reduced the number of wires required to connect field devices to the host, but they also introduced another single point of failure—the cable. (solution: redundance, cost: more cabling complexity).



Point to point Network.



Multidrop Network.

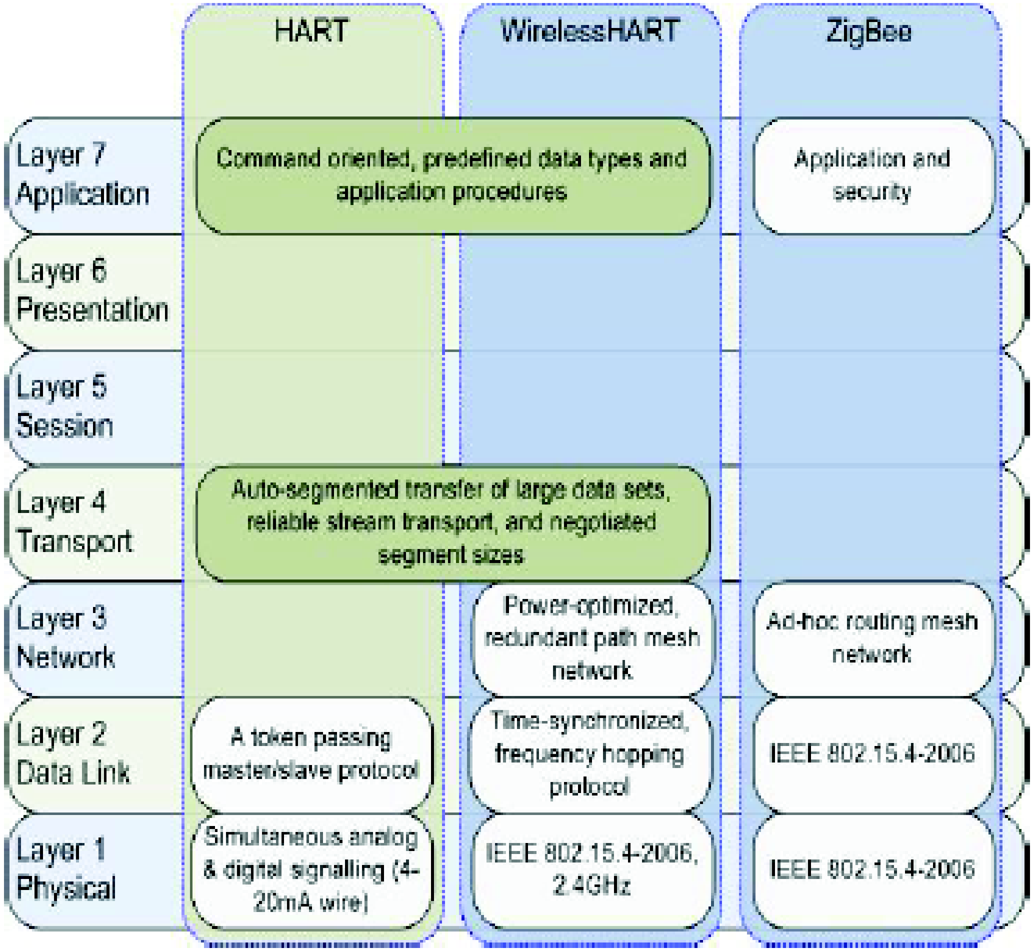
WirelessHart

- **Wireless Hart:** Since version 7, HART also incorporates an IEEE 802.15.4-based wireless mesh network as an option for the physical layer. Is a Wireless Mesh Network Communications Protocol and its aim is solve the needs for process automation applications.

- WirelessHART is **backward compatible** with existing HART devices and applications. Existing HART applications (e.g., control systems, PLCs, etc.) can utilize WirelessHART without the need for software upgrades.

WirelessHart

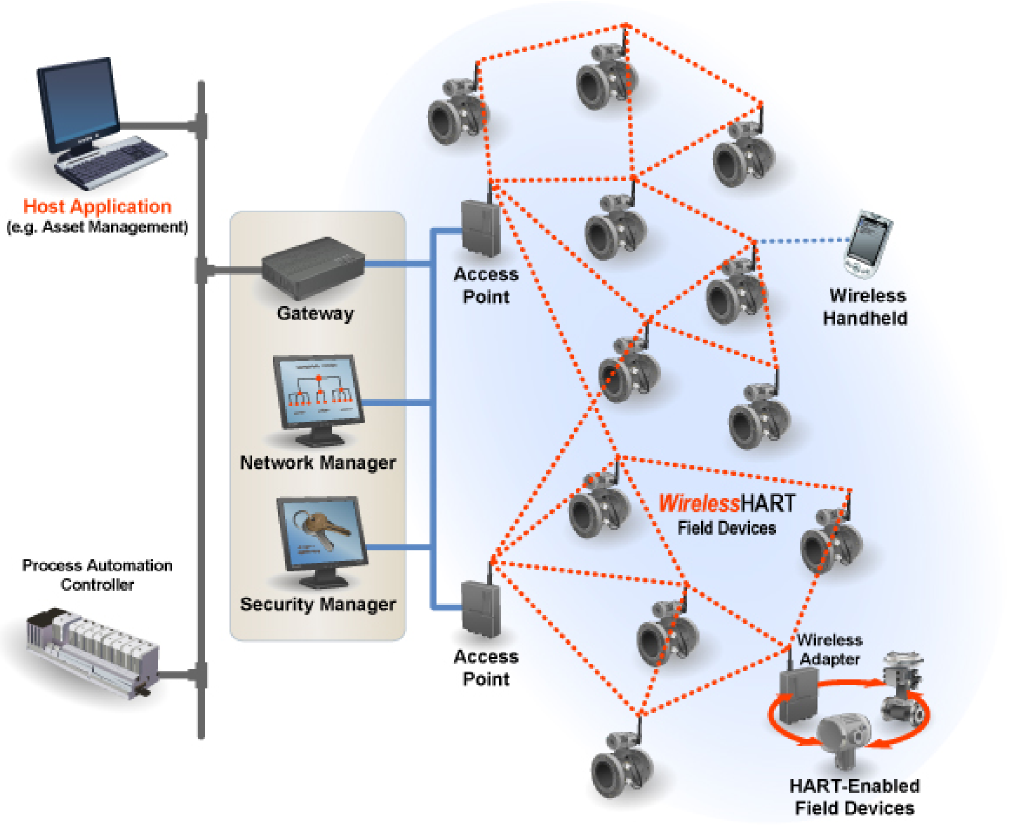
- Figure *(Source: ABB Corporate Research)* shows that WirelessHART is based on the PHY layer specified in the IEEE 802.15.4-2006 standard, but specifies new Data-link (including MAC), Network, Transport, and Application layers.



	HART	WirelessHART	ZigBee
Layer 7 Application	Command oriented, predefined data types and application procedures		Application and security
Layer 6 Presentation			
Layer 5 Session			
Layer 4 Transport	Auto-segmented transfer of large data sets, reliable stream transport, and negotiated segment sizes		
Layer 3 Network		Power-optimized, redundant path mesh network	Ad-hoc routing mesh network
Layer 2 Data Link	A token passing master/slave protocol	Time-synchronized, frequency hopping protocol	IEEE 802.15.4-2006
Layer 1 Physical	Simultaneous analog & digital signalling (4-20mA wire)	IEEE 802.15.4-2006, 2.4GHz	IEEE 802.15.4-2006

WirelessHart

- **Wireless Hart types of Networks:** Star, Cluster, Mesh.



WirelessHart

- **Wireless Hart types of Devices:**

- **Wireless field devices :** This device could be a device with WirelessHART built in or an existing installed HART-enabled device with a WirelessHART adapter attached to it.

- **Gateways:** enable communication between these devices and host applications connected to a high-speed backbone or other existing plant communications network.

- **Network Manager**: Can be integrated into the gateway, host application, or process automation controller. It identifies the best paths and manages distribution of slot time access (WirelessHART divides each second into 10msec slots)

- **All WirelessHART devices must have routing capability, there are no reduced function devices like in ZigBee.**

WirelessHart

- **Why Wireless Hart [ ]**

- **Mesh Advantage:** Industrial applicattions need redundant paths which allows messages to be routed around physical obstacles, broken links, and interference.

- **Robustness:** It’s designed from start to be a robust and secure communications protocol.

- **Avoids Interference:** Frequency hopping and retransmissions limits the effects of temporal and frequency interference.

- **Industrial Applications:** Although ZigBee has had very limited success in industral applications, the robustness of WirelessHART opens up the possibility for wireless control, at least for slow and non-critical processes.

WirelessHart

- **TDMA:** Prevents message collisions and allows devices to increase their power savings because the device only needs to keep the radio on during the required timeslots.

- **Weakness:**

  “The enhancements offered by industrial standards can also be advantageous in commercial building automation, but are generally not essential. Meanwhile, they add substantial cost that limits their feasibility for many residential and commercial applications.” [13]

- Requires a **Network Manager device**.

Freescale SMAC

- The SMAC is used for developing **proprietary RF transceiver** applications using a Freescale 802.15.4 transceiver. The SMAC was built to work with an HCS08 based MCU with an SPI, but it can easily be adapted to almost any processor core.

- **Network Topologies:** Point to point, Star (option: repeater)

- **Security:** The security module is a software component that allows the ciphering and deciphering of messages.

- Special for low-cost ad-hoc applications (toys, cable replacement, etc).

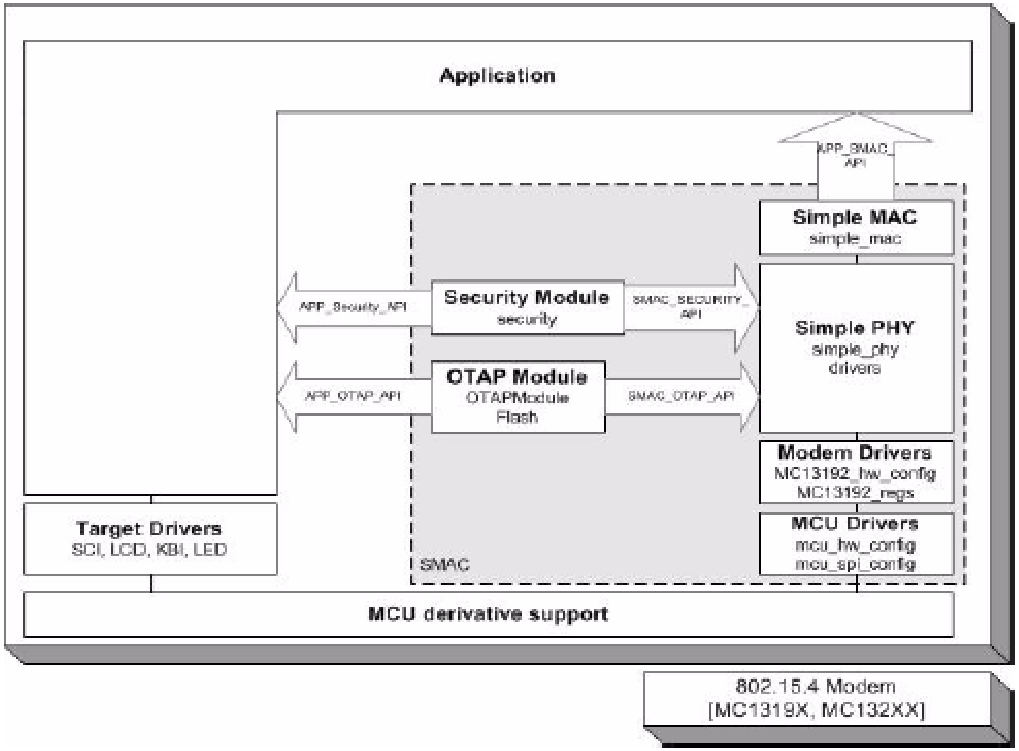
- Very-low power, proprietary, bi-directional RF communication link

Freescale SMAC

- **SMAC types of messages:** Reception (RX), Transmission (TX), Energy Detect (ED) Time out (TO).

- The **OTAP** (Over the air programming) module allows users to update device firmware without wires.

- Number of nodes 2-100



Bluetooth

- Bluetooth wireless technology is a short-range communication system intended to replace the cables in WPAN.

- The name Bluetooth is from the 10th century Danish King Harald Blatand (Harold Bluetooth in English) who was instrumental in uniting warring factions in parts of what is now Norway, Sweden, and Denmark; just as Bluetooth technology is designed to allow collaboration between differing industries such as the computing, mobile phone, and automotive markets.

- Bluetooth devices are expected to work in the presence of interference caused by other devices (e.g., IEEE802.11 WLAN)

- Bluetooth wireless technology is focused on voice and data applications.

Bluetooth

- **Communication Range:** depending on the type of device, goes up to 10 meters, for the less powerful to 100 meters for the most powerful.
- Maximum data rate with EDR for Bluetooth 2.0 is 3 Mbps.
- Antenna Conditions: Omni-directional and in some cases can work also in NLOS.
- Multi-vendor interoperability

- **Physical Layer:**
- The Bluetooth RF operates in the unlicensed ISM band, around 2.4 GHz [2400, 2483.5 MHz].
- The system employs a frequency hopping (FH) transceiver (the nominal hop rate is 1600 hops/s) to combat interference and fading.

Bluetooth

- **Physical Layer:**

- The Bluetooth RF operates in the unlicensed ISM band, around 2.4 GHz [2400, 2483.5 MHz].
- The system employs a frequency hopping (FH) transceiver (the nominal hop rate is 1600 hops/s) to combat interference and fading.

Bluetooth

- **Bluetooth Devices Power Classes:**
- **Class 1** with maximum output power of 20 dBm. (Power control required)
- **Class 2** with maximum output power of 4 dBm.
- **Class 3** with maximum output power of 0 dBm. (Power control capability under 0 dBm is optional and could be used for optimizing the power consumption and overall interference level)

Bluetooth

- **Bluetooth Network Architecture:**

- **Piconet:** Bluetooth devices can form small networks called “piconets” and information is exchanged seamlessly among devices in the piconet.[14]

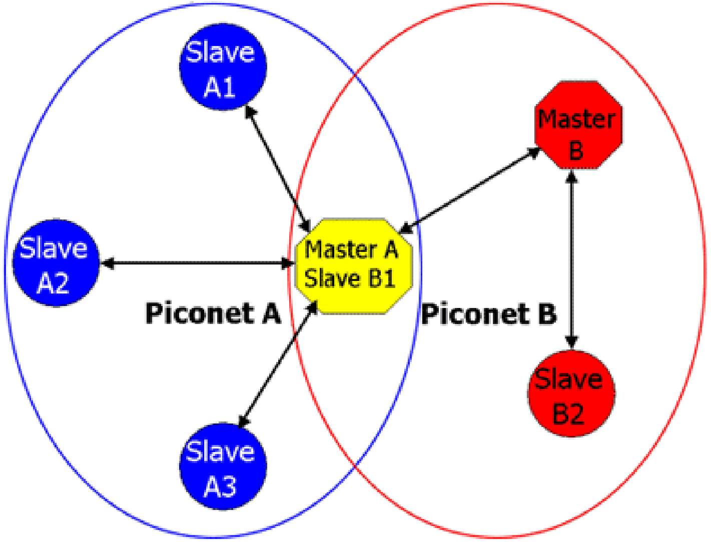
- A piconet is a **WPAN** formed by a Bluetooth device serving as a **master** in the piconet and one or more Bluetooth devices **serving as slaves**. A **frequency-hopping channel** based on the address of the master defines each piconet.

- Slaves communicate only with their master in a **point-to-point** fashion under the control of the master.

- Can be **8 maximum number** of devices in a Piconet.

Bluetooth

- **Scatternet:** Bluetooth piconets may be inter-connected to form larger networks called scatternets.
- This requires some devices, called **gateways**, to time–division their **presence among the piconets** they belong to lifetime.
- Gateway participation in multiple piconets has to be on a timedivision multiplexing basis.



. Bluetooth Scatternet. (Source: EETimes)

ferent ways to create a Scatternet: http://www.cse.buffalo.edu/tech-reports/2004-06.p

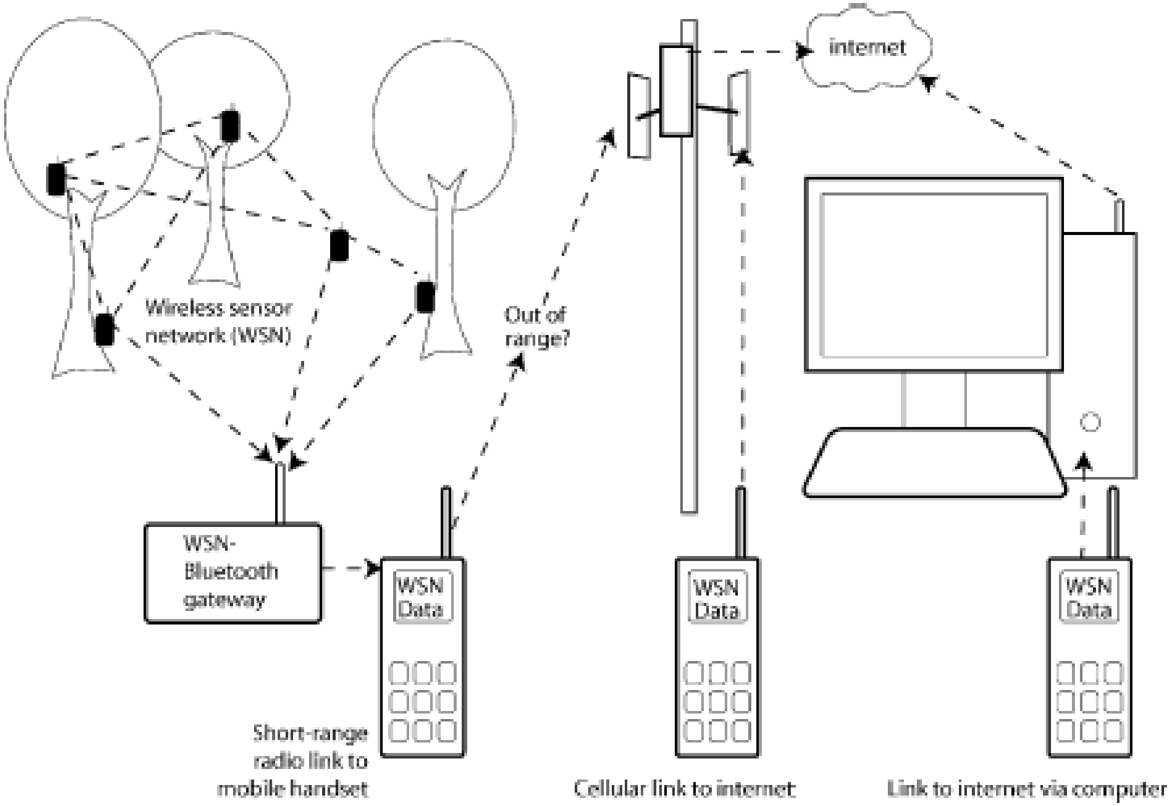
Bluetooth

- **Bluetooth in WSN:**

- Authors like Baker [15] have studied the strengths and weaknesses of bluetooth and zigbee for industrial applications, and claimed that ZigBee over 802.15.4 protocol can meet a wider variety of real industrial needs than Bluetooth, **due to its long-term battery operation, greater useful range,** flexibility in a number of dimensions, and reliability of the **mesh networking architecture.**

- Bluetooth is a protocol with **188 primitives** and events in total. ZigBee is more simple with only **48 primitives** defined in 802.15.4.

Advantage: Bluetooth is everywere!!!


internet
Wireless sensor network (WSN)
Out of range?
WSN-Bluetooth gateway
WSN Data
WSN Data
WSN Data
Short-range radio link to mobile handset
Cellular link to internet
Link to internet via computer

- “Mobile phones carried by the public could enable a hybrid approach where data makes a low-power short distance hop to phones in the vicinity using Bluetooth or a similar short range protocol, then uses the phones’ long distance connectivity to upload to the Internet.”(C. K. Harnett, IEEE SENSORS JOURNAL, VOL. 10, NO. 6, JUNE 2010).

Wireless USB

- **Wireless USB RF Characteristics:**

- CWUSB (C is for certified) lets systems transmit USB wirelessly **via ultrawideband radio technology.**

- Has a theoretical maximum speed and range of from **480 Mbps at 3 meters** to **110 Mbps at 10 meters.**

Wireless USB

- Wireless USB is based on the WiMedia Alliance's **Ultra-WideBand (UWB)** common radio platform. The frecuency bands are in the range from **3.1 to 10.6 GHz** and uses Orthogonal frequency-division multiplexing modulation **(MB-OFDM)** metod (the same modulation metod than bluetooth 4.0).

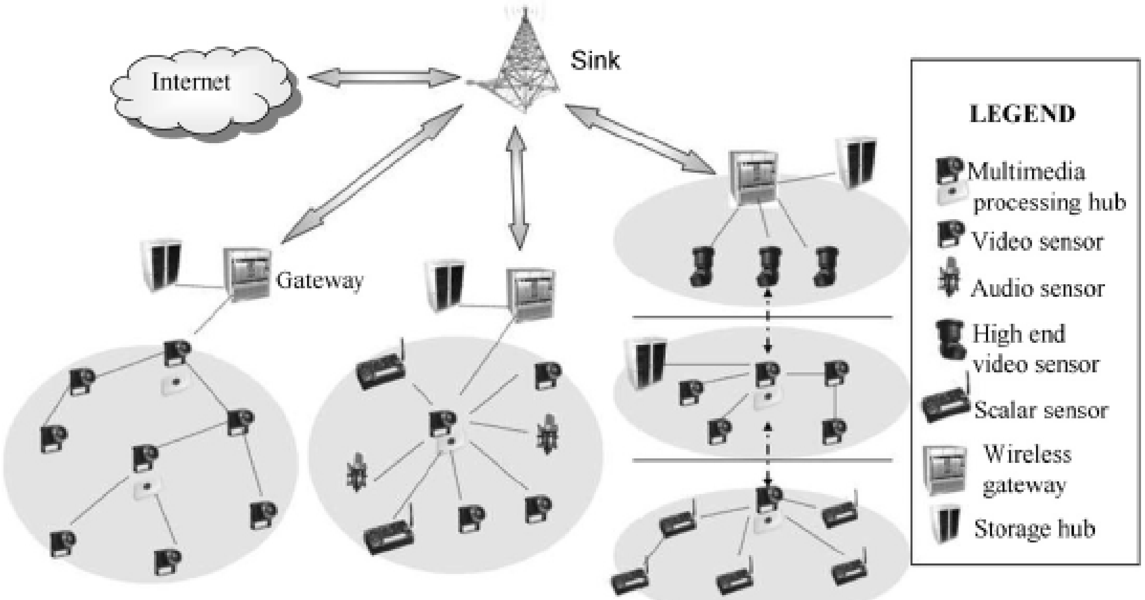
- MB-OFDM increases bandwidth by dividing a signal into **14 528-MHz-wide bands**, which can each **simultaneously carry signals**. The channels are **orthogonal** to their neighbors and thus can be packed close together **without interfering with one another**[17].

Wireless USB

- **Wireless USB Network Features**
- Security: WUSB provides 128-bit Advanced Encryption Standard Cryptography.
- Network Topology: Point to Point.
- In WUSB a **single host manages all data traffic, initiating communications and allocates time slots** to each connected device.
- WUSB allows up to **127 devices** to connect directly to a host.

Wireless USB

- **Wireless USB in Multimedia Wireless Sensor Network**
- The availability of low-cost hardware such as CMOS cameras and microphones has fostered the development of Wireless Multimedia Sensor Networks (WMSNs).



(a)
Single-tier flat,
homogeneous sensors,
distributed processing,
centralized storage

(b)
Single-tier clustered,
heterogeneous sensors,
centralized processing,
centralized storage

(c)
Multi-tier,
heterogeneous sensors,
distributed processing,
distributed storage

MWSN *(Source: Computer Networks 51 Pag. 926. Elsevier.2007*

Wireless USB

- The ultra wide band **(UWB)** technology has the potential to **enable low-power consumption, high data rate communications** within tens of meters, characteristics that make it an ideal choice for WMSNs.

- When **OFDM** is used, **high-speed FFT** processing is necessary, which requires significant processing power and leads to complex transceivers [18].

- In UWB **multi-hop** networks is still an **open issue.**

- More information see: S. Gezici, Z. Tian, G.B. Giannakis, H. Kobayashi, A.F.Molisch, H.V. Poor, Z. Sahinoglu, “Localization via ultrawideband radios”, IEEE Signal Process. Mag. 22 (4) (2005).70–84.

WiMAX

- WiMAX™ is based upon the IEEE 802.16. IEEE 802.16™ is an emerging suite of standards for **Broadband Wireless Access (BWA)** in licensed frequency bands under **6 GHz.**

- **WSNs** are scattered in various places and most of them are **located in remote areas**, WiMAX provides a better accessing mechanism with **greater coverage and cell capacity** for them. The possible use of **Wimax in WSN** is on the **gateway** between the WSN and the Internet.

- WiMax in contrast to other wireless technologies, **work in an acceptable way** under **NLOS (**non line of sight) conditions.

- WiMax gives **priority** to time sensitive traffic such as **VoIP and video**.

WiMAX

- **WiMax Network Architectures:**
- **Point to point:** This scenario is **typical for backhaul** or for the transport from **the data source** (data center, fiber POP, Central Office, etc) to the **broadband subscriber**.
- **Point to multipoint:** this type of network is applied largely in distribution. One base station can service hundreds of dissimilar subscribers in terms of bandwidth and services offered. **Omni directional ant** [illegible] rations.

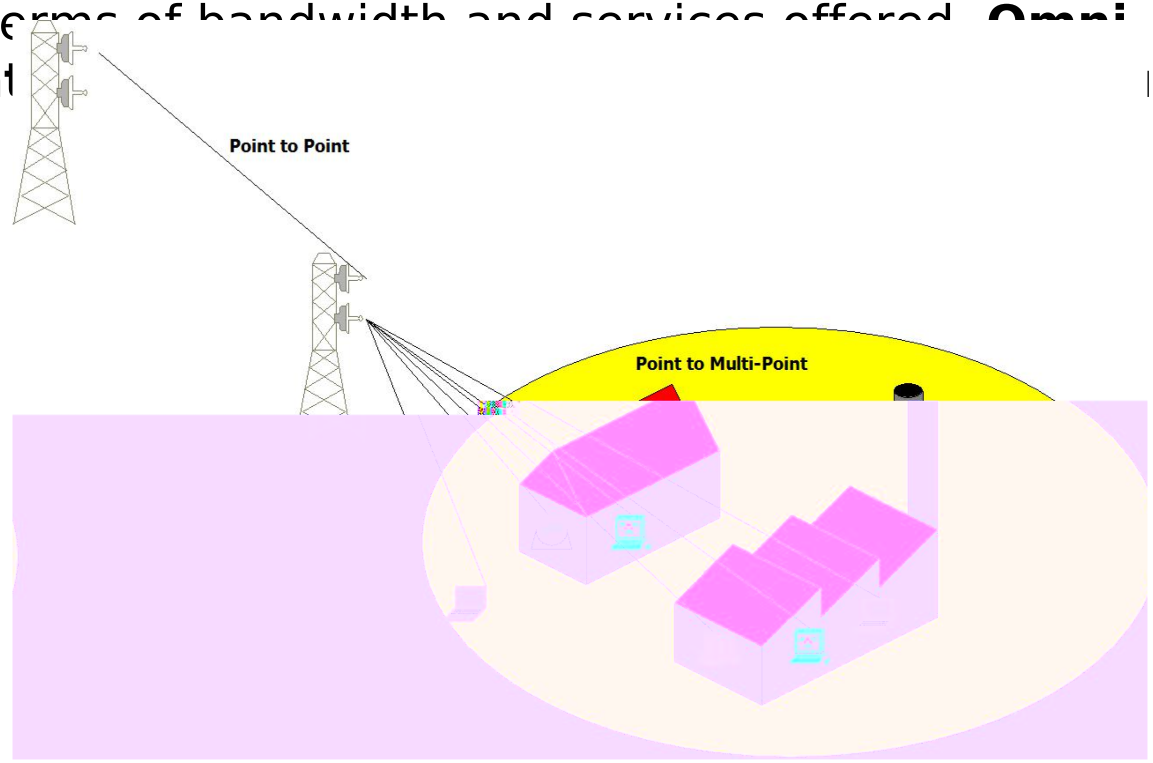


Figure X. WiMax Network

ISA100.11a

- ISA-100.11a is **meant to provide reliable and secure wireless operation** for non-critical monitoring, alerting, supervisory control, open loop control and closed loop control applications.(*Source: International Society of Automation*).

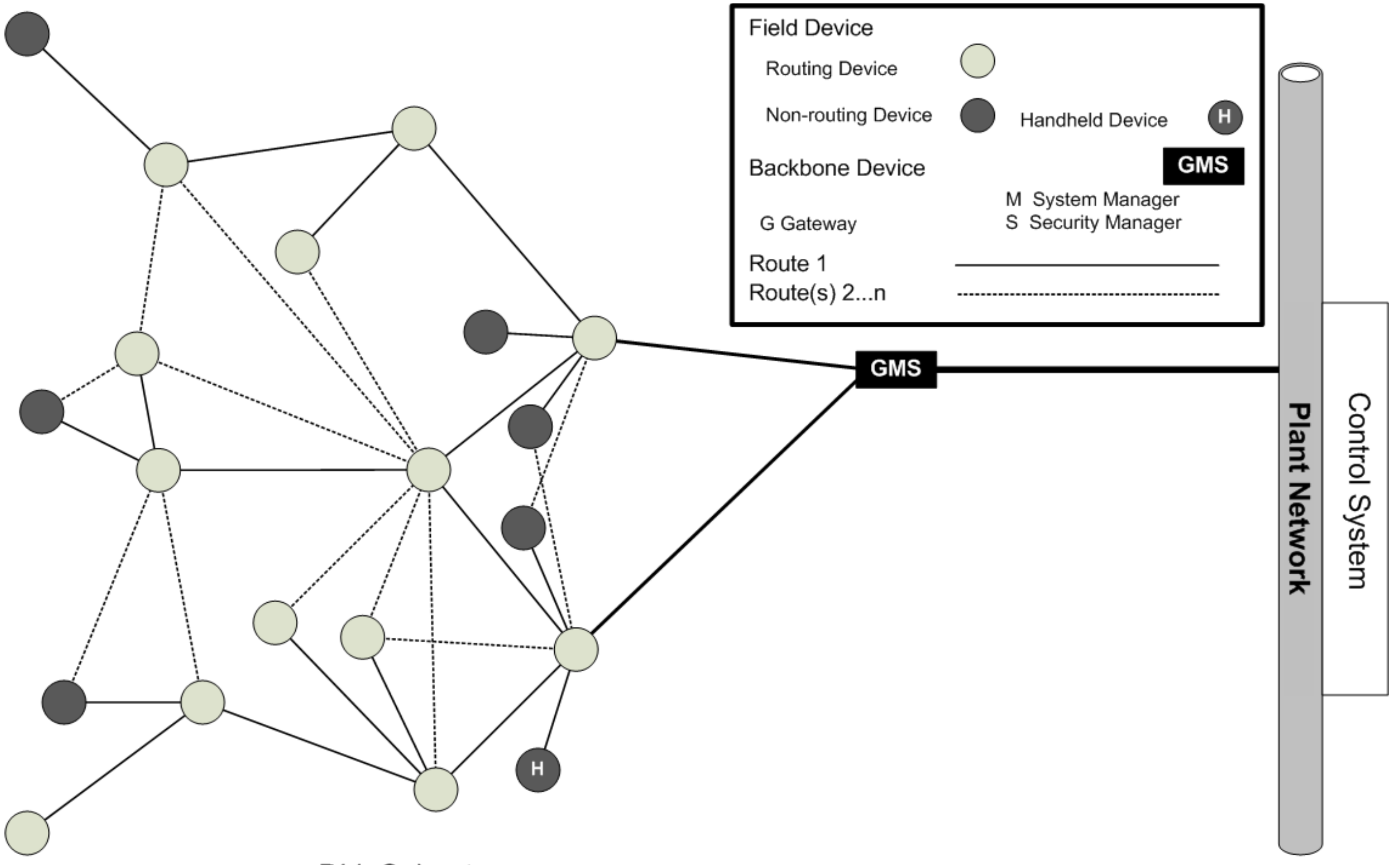
- **Key attributes** are **robustness to interference, low complexity, reasonable cost and low power consumption** while maintaining **interoperability** with wired plant infrastructure networks.

ISA100.11a

- **ISA 100.11a RF Characteristics**
- Based on IEEE 802.15.4 radios in the 2.4 GHz ISM band.
- **TSCH** Time-synchronized channel-hopping to sidestep RF interference and minimize power consumption.
- Allows for FFD devices such as routers to sleep.
- Upper DLL provides: TDMA, Channel Hopping and Mesh routing

- **Network Topologies and Security**
- **Star Topology:** can provide very quick response times that are necessary for some types of critical applications.
- **Mesh networks:** can offer increased robustness, enhanced reliability, greater tolerance to interference, etc.
- **Security:** Messages protected with **AES128** block cipher**.**

ISA100.11a



- **ISA 100.11 Network (Source International Society of Automation).**

ISA100.11a

- **ISA 100.11 Gateway**

- Has **access to control/sensing devices** in the ISA 100.11a industrial network

- ISA100.11a **provides support for protocol translation.** The support includes a **tunneling object** that fits within the application layer structure and **provides generic services for protocol translation.**

- ISA100.11a does not provide the actual protocol translators, only the supporting mechanism.

ISA100.11a

- **ISA 100.11 Strenght and Weaknesses**

- Industrial applications that need increased **robustness to interference** and **multipath services.**

- Industrial environments with **multiple wired protocols** (Field Bus, HART, Profibus, etc).

- **Low power consumption:** Applications where battery operated routers are required (TDMA Allow sleeping routers)

- **Not suitable for low-cost** applications.

4) WSN. Which protocol can be used?

WSN. Which protocol can be used?

- **Since the point of view of topology**

	Point to Point	Star	Cluster Tree	Mesh
Wireless field measurements		🟨	🟩	🟩
Home automation		🟩	🟩	🟩
Remote Control	🟨	🟩		
Cable Replacement	🟩			
Industrial WSN		🟩	🟩	🟩
Multimedia WSN		🟩		
Automotive WSN		🟩		

Network Topologies and Applications

WSN. Which protocol can be used?

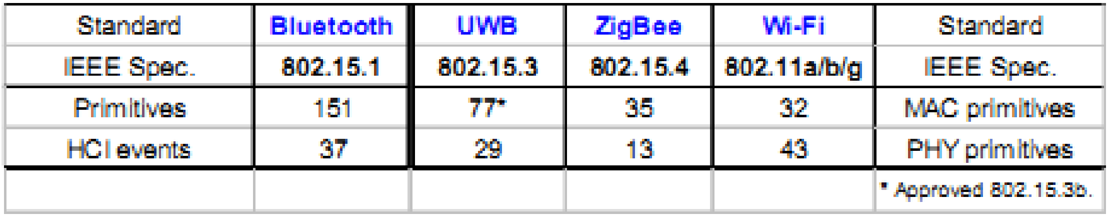
- **Since the point of view of Application**

	802.15.4 Family	Bluetooth	802.11	WiMax	UWB Technologies
Wireless in field measurements	🟨				
WSN for Home Automation	🟨				
Home Remote control	🟨				
Cable Replacement	🟨	🟨			
Industrial WSN	🟨				
Multimedia WSN					🟨
To Internet Gateway		🟨	🟨	🟨	
Mobile Networks		🟨		🟨	

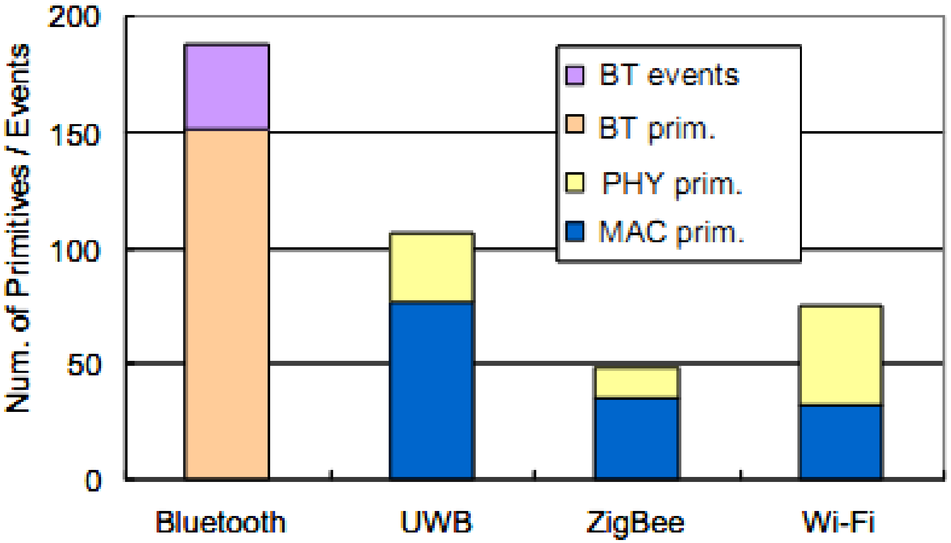
Protocols Family and Applications

WSN. Which protocol can be used?

- **Since the point of view of Hardware requeriments**



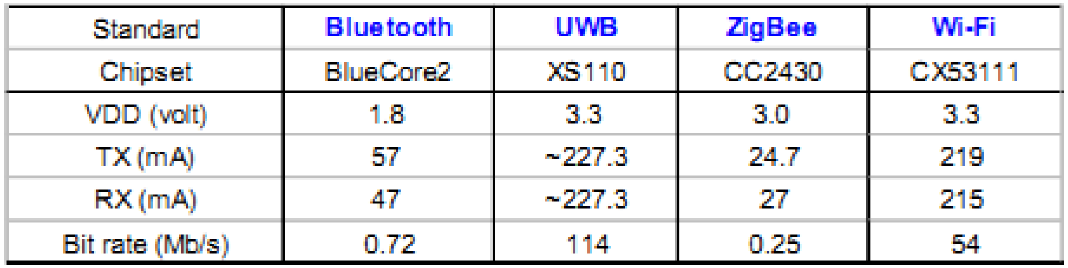
Standard	Bluetooth	UWB	ZigBee	Wi-Fi	Standard
IEEE Spec.	802.15.1	802.15.3	802.15.4	802.11a/b/g	IEEE Spec.
Primitives	151	77*	35	32	MAC primitives
HCI events	37	29	13	43	PHY primitives
					* Approved 802.15.3b.



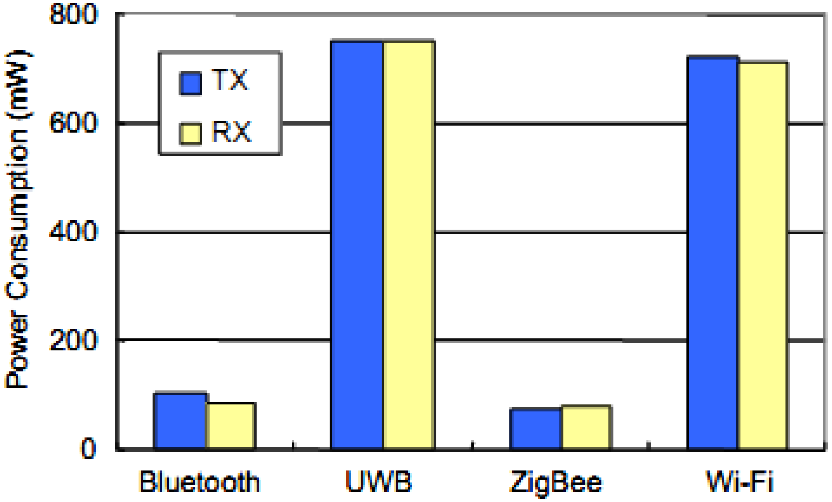
Number of primitives and events for each protocol

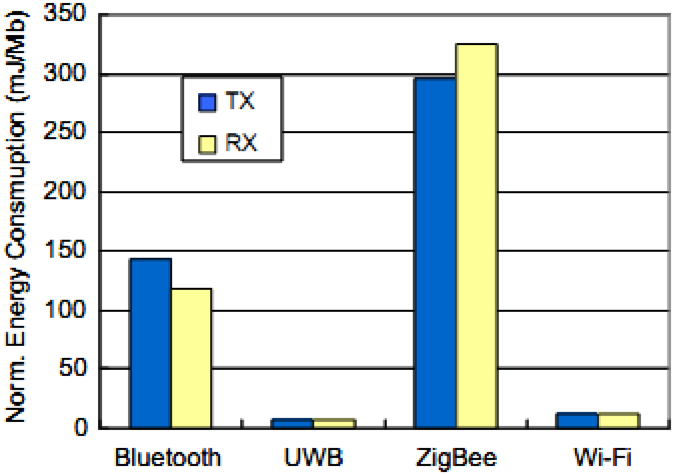
WSN. Which protocol can be used?

- **Since the point of view of Hardware requeriments**



Standard	Bluetooth	UWB	ZigBee	Wi-Fi
Chipset	BlueCore2	XS110	CC2430	CX53111
VDD (volt)	1.8	3.3	3.0	3.3
TX (mA)	57	~227.3	24.7	219
RX (mA)	47	~227.3	27	215
Bit rate (Mb/s)	0.72	114	0.25	54





Current consumption and N-current consumption of chipsets for each protocol

Source: Jin-Shyan Lee; Yu-Wei Su; Chung-Chou Shen; , "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE , vol., no., pp.46-51, 5-8 Nov. 2007

5) Expectations for the future of WSN protocols

Expectations for the future of WSN protocols

- **Real Time Specs:**

  Different applications (especially industrial type), require that measurements collected by the sensors are delivered immediately in order to take actions accordingly. By which progress is needed in the development of protocols to real-time applications

- **Power Management:**

  New researches in protocols must ensure the decrease of energy consumption in different types of WSN nodes without losing quality of service.

Expectations for the future of WSN protocols

- **Programming Abstractions:**

  The **growth of** technologies such as **WSN**, will be **greater** if the **programmers** are **independent** from **low-level details** such as sensing and communication node to node.

- **Security:**

  WSN interact with the enviroment and in many cases might be cause several troubles if an intruder attack the network. For this reasons if securitiy grows then WSN can be used to much in crittical applications

THE END
Metro-Goldwyn-Mayer
PICTURE

References

- [1]G. Smith, M. Bowen, Consideration for the utilization of smart sensors, Sensors Actuators A 46–47 (1995) 521–524.
- [2]A. Flammini, P. Ferrari, D. Marioli, E. Sisinni, A. Taroni, “Wired and wireless sensor networks for industrial applications”, Microelectronics Journal, Volume 40, Issue 9, Quality in Electronic Design; 2nd IEEE International Workshop on Advances in Sensors and Interfaces; Thermal Investigations of ICs and Systems, September 2009, Pages 1322-1336.
- [3] H.S. Ng, M.L. Sim, C.M. Tan, C.C. Wong, Wireless technologies for telemedicine, BT Technol. J. (Kluwer Academic Publishers) 24 (2) (2006) 130–137.
- [4] C. Gabriel, H. Horia, Integrating sensor devices in a LIN bus network, in: 26th International Spring Seminar on Electronics Technology: Integrated Management of Electronic Materials Production, 2003, pp. 150–153.
- [5] Potdar, V.; Sharif, A.; Chang, E.; , "Wireless Sensor Networks: A Survey," Advanced Information Networking and Applications Workshops, 2009. WAINA '09. International Conference on , vol., no., pp.636- 641, 26-29 May 2009.

References

- [6] H. Karl and A. Willig, Protocols and Architectures for Wireless Sensor Networks, Wiley, London, New York (2005).
- [9]J. Reed , Introduction to Ultra Wideband Communication Systems , Prentice Hall , Englewood Cliffs, J, June 2005.
- [10]Zheng, J.; Jamalipour, A.; , "A Networking Perspective," Wireless Sensor Networks , vol., no., pp.500,
- [11] M. Z. Win and R. A. Scholtz , “ Ultra-wide bandwidth time-hopping spread-spectrum impulse radio for wireless multiple - access communication ” , IEEE Transactions on Communications , vol. 48 , no. 4 , Apr. 2000 , pp. 679 – 689 .
- [12] HCF - HART Communication Foundation, “HART7 Specification”,
- September 2007.

References

- [13]Lennvall, T.; Svensson, S.; Hekland, F.; , "A comparison of WirelessHART and ZigBee for industrial applications," Factory Communication Systems, 2008. WFCS 2008. IEEE International Workshop on , vol., no., pp.85-88, 21-23 May 2008.
- [14]M. S. Rohit Kapoor and M. Gerla, “An Analysis of Bluetooth Scatternet Topologies,” ICC 2003, Anchorage, Alaska, vol. 1, pp. 266 –270, May 2003.
- [15]Baker, N. “ZigBee and Bluetooth: Strengths and weaknesses for industrial applications,” IEEE Computing & Control Engineering, vol. 16, no. 2, pp 20-25, April/May 2005.
- [16] Jin-Shyan Lee; Yu-Wei Su; Chung-Chou Shen; , "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE , vol., no., pp.46-51, 5-8 Nov. 2007
- [17] Leavitt, N.; , "For Wireless USB, the Future Starts Now," Computer , vol.40, no.7, pp.14-16, July 2007
- [18] Ian F. Akyildiz, Tommaso Melodia, Kaushik R. Chowdhury, A survey on wireless multimedia sensor networks, Computer Networks, Volume 51, Issue 4, 14 March 2007, Pages 921-960
- [19] http://www.wimax.com/wimax-tutorial/antenna-technologies-a-interference.