European Commission

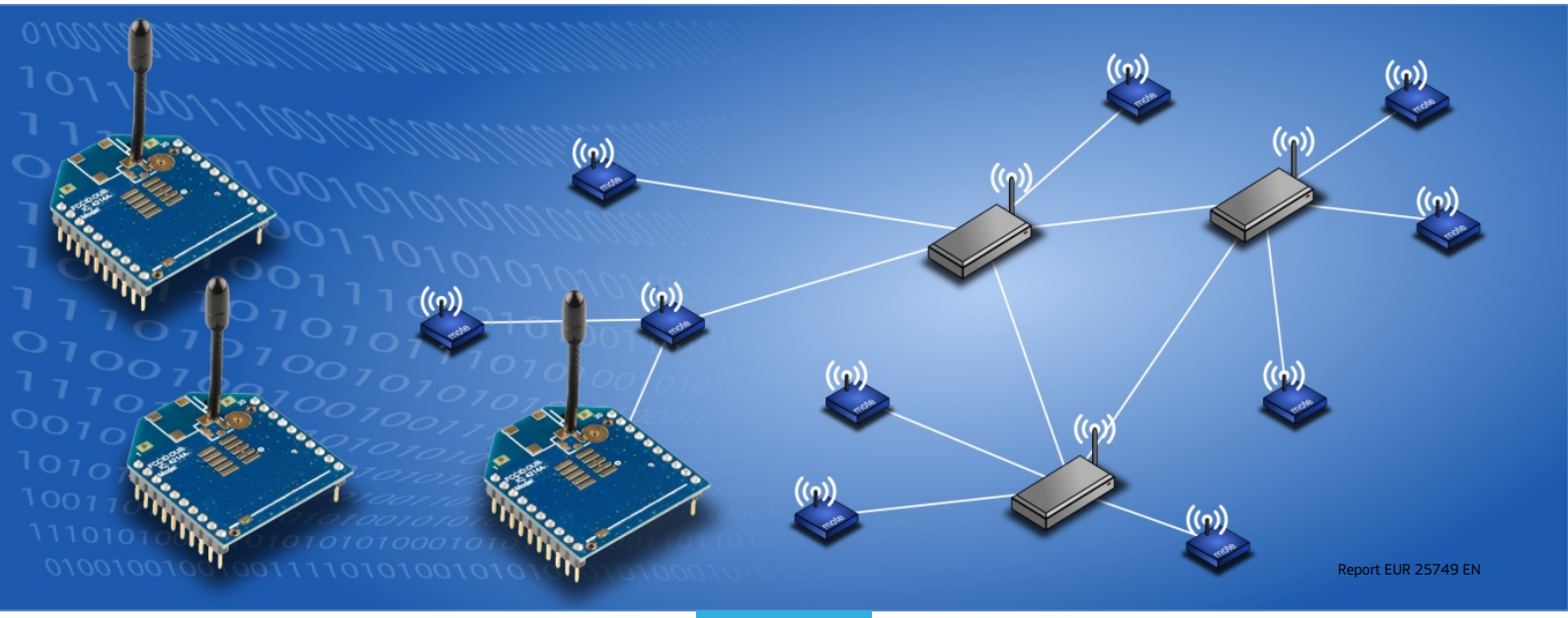
JRC SCIENTIFIC AND POLICY REPORTS

Analysis of current and potential sensor network technologies and their incorporation as embedded structural system

Deliverable 04.01

Flavio Bono, Graziano Renaldi (DG JRC)

2013



Joint Research Centre

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Eugenio Gutiérrez
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 480, 21027 Ispra (VA), Italy
E-mail: eugenio.gutierrez@jrc.ec.europa.eu
Tel.: +39 0332 78 5711
Fax: +30 0332 78 9049

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC77873

EUR 25749 EN

ISBN 978-92-79-28185-3

ISSN 1831-9424

doi: 10.2788/79382

Luxembourg: Publications Office of the European Union, 2013

Printed in Italy

Deliverable Administration & Summary		STEC		41999	
No & name	D04.01 Analysis of current and potential sensor network technologies and their incorporation as embedded structural system.				
Status	Final	Due	31/12/12	Date	14/12/2012
Author(s)	F.Bono, G.Renaldi (DG-JRC Unit G05)				
Compile/Edit	E.Gutiérrez (DG-JRC Unit G05)				

Cover Photo: Wireless Mesh Sensor Network representation.
(Flavio Bono)

Contents

Tables

Figures

1 SUMMARY

The recent and continuous improvement in the development of devices for monitoring and transmitting data is offering a broad range of possibilities in many different fields of applications, ranging from fire detection in wide forest areas, to surveillance systems, exchange of information in mobile networks, or infrastructures for medical care. This increasing interest and implementation in sensor networks is mainly due to the availability in recent years of ever cheaper and 'smarter' sensors.

A wireless sensor network, in general, is composed of spatially distributed smart devices capable of sensing, measuring, and gathering information from the environment and to eventually process the acquired information in order to take action and transmit data to the other nodes of the network towards a central gateway. The information can either be related to one single device (e.g. an alarm) or contribute to generate a spatially distributed measurement with the information provided by the other nodes of the system. Wireless sensor networks (WSNs) are therefore composed of possibly a large number of spatially distributed autonomous sensor devices equipped with wireless communication capabilities.

Many differences exist on the basis of the type of wireless communication, of the network organization and control and the functionality of the network nodes. Moreover, different communication protocols and frequency ranges are available so that different standards are used in different countries as frequency bands are often reserved for specific devices; this adds more constraints for devices that should be compliant to all the world standards. Moreover, in the case of wireless ad hoc networks, a group of communication nodes is capable of setting up and maintaining a network amongst the nodes, without the need of a base station. For this reason, wireless ad hoc networks are adopted in mobile networks where migrating nodes can join a network autonomously, whenever they are in the range of other signals, and exchange information with other nodes.

This report reviews the different types of wireless sensor network technologies available, especially in view of their possible implementation for ISO shipping container protection and monitoring within the framework of the JRC STEC Action.

The type of application of a WSN strongly affects the choice of the wireless technology to be adopted. Once application requirements are defined, the technology which allows satisfying these requirements can be identified. For this reason the knowledge of the different features, advantages and disadvantages of the existing technologies is crucial for an effective implementation of the network.

Whilst this report examines different communication protocols, the main focus is related to the IEEE 802.15.4 standard and, in particular, its *ZigBee* implementation for personal area networks (mostly employed by home automation services). The low energy consumption of these devices, and their usual adoption in ad hoc networks with low data exchange rate, makes them particularly interesting for short range information transmission and their coupling with energy harvesting systems.

2 CONTAINERS AND TERMINALS

The European Union has seen constant freight traffic growth over the latest few decades, only slowed down recently due to the global crisis. The European Freight Terminals (FT) are crucial key nodes of the commercial trade of the EU, with major ports accounting for the highest world shipping container traffic in terms of TEU (Twenty-foot ISO container Equivalent Unit)[1] like the Port of Rotterdam, for a long time the largest port of the world's and still one of the busiest.

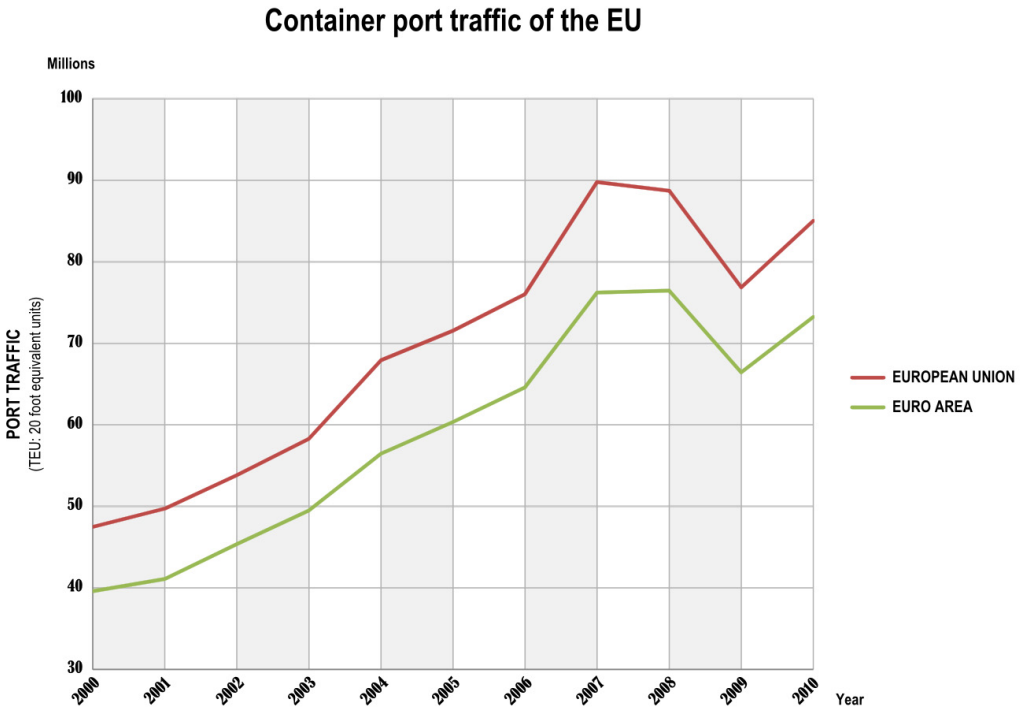


Figure 1 –EU container port traffic (source: the World Bank)

The multi-modality of the container transport contributed to the growth of this system, because ISO standardized container units are suitable to different means of transportation (i.e. by ship, train, plane and truck) this leading to a wide interconnected network both on land and sea.

2.1 CONTAINER TERMINALS

Container terminals are complex systems with tight logistic schedules for the loading and discharging of vessels or other container transport systems. A container terminal consists of at least three operational areas (Brinkmann 2011):

[1] Standard unit for describing a ship's cargo carrying capacity, or a shipping terminal's cargo handling capacity

- **Operational area**: between quay wall and container yard (apron or the area just behind the berth front)
- **Container yard** (terminal storage = stacking area)
- **Terminal area of landside operations** (including the gate, parking, office buildings, customs facilities, container freight station with an area for stuffing and stripping, empty container storage, container maintenance and repair area etc.)

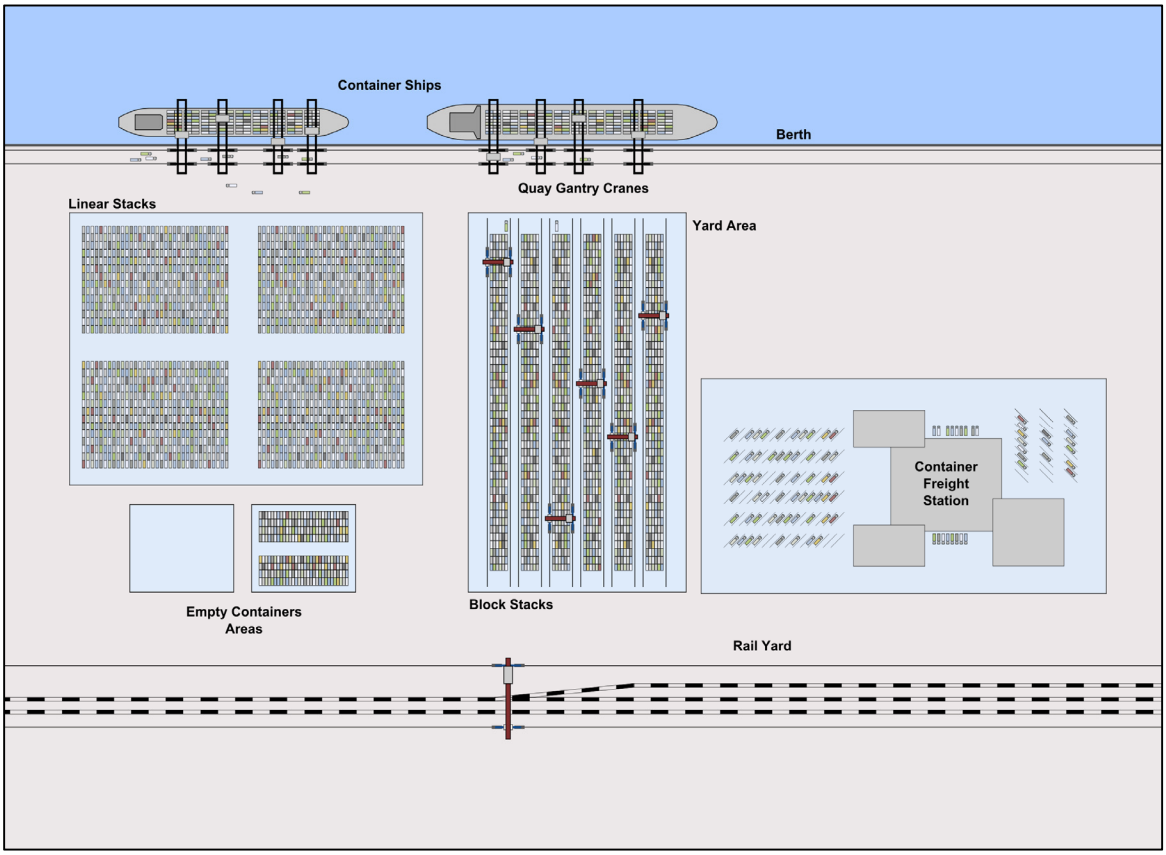


Figure 2 - General layout of a container terminal

Container Terminals are also a complex environment for wireless communications: steel containers are a barrier to radio waves, electric motors of gantry cranes may cause interference to transmissions and the existence of other radio signals is a critical aspect in relation to a WSN. Moreover, containers are moved all over the area of the terminal, either for loading and unloading operation, for their storage in waiting areas (as is the case of empty containers) or their blocks or linear stacking awaiting their management at the berth.

In Figure 2 the schematic layout of a container terminal with the different operational areas is shown. Containers are moved within the terminal by handling equipment for horizontal container transport. The operational system, composed by all the equipment used in a terminal for handling the containers (e.g. for loading and unloading the vessels, for transport tasks between quay and stacking yard or for container stacking) as well as the layout (e.g. the stacking of containers or the areas devoted to host empty containers) and choice of equipment for the above mentioned areas differs in every terminal (Vacca, Bierlaire and Salani 2007). These are defined mainly by the geographical area and the traffic and a wireless

sensor system targeted to work in such a peculiar environment therefore needs to be adaptable and capable to face all the different terminal scenarios and to cope with the possible interferences in the area of operations. Moreover, as terminals usually consist of large areas, coverage issues must be carefully taken into account when designing a WSN in this scenario.

2.2 WSN REQUIREMENTS FOR CONTAINERS

The design of a WSN significantly depends on the type of application, and it must consider factors such as the environment, costs, hardware, and system constraints. The implementation of a Wireless sensor networks in a container terminal scenario has the typical requirements of an environmental monitoring application:

- Energy efficiency
- Low data rate
- One-Way Communication
- Wireless backbone

Moreover, other requirements proper of an industrial application are also needed:

- Reliability
- Security

Apart from the specific requirements listed above, general common requirements are also needed:

- Self-organization
- Self-healing
- Sufficient degree of connectivity among nodes
- Low complexity
- Low cost
- Small size of node devices

The most critical requirement for the present application is related to the energy efficiency. Nodes in a container network are necessarily battery powered or have a limited power supply. This stringent limitation has a significant impact on all the remaining requirements as it poses different problems in all aspects of network implementation: from the hardware design targeted to minimal energy consumption, to network protocols (as nodes may be configured to a prevailing sleep mode with alternate awake intervals).

WSNs have many advantages over traditional wired systems:

- Low costs of devices
- Easy deployment, as cables are replaced by wireless communications
- Network Scalability
- Dynamic topology
- Ease of use

Some aspects of wireless standards are particularly important when designing a WSN; these same aspects also are the key characteristics that typically differentiate the various standards:

- **Connection model and topology:**
  the way in which devices discover each other, connect to the wireless network, establish connections with other nodes, manage and route data streams from other nodes, maintain connections in power-saving modes and disconnect from the network.
- **Latency, range and throughput**
  In contrast to wired networks, in wireless communications sent data does not reach the destination in a defined time; the wireless connection may act as a bottleneck, has variable delays and a limited range for the connection to be deterministically ensured.
- **Security**
  Security is a critical issue in wireless communications. A wireless standard must ensure that the information exchanged cannot be intercepted and read. However, security may affect the throughput and ease of connectivity.

3 WIRELESS SENSOR NETWORKS (WSNS)

Wireless Sensor Networks are gaining increasing attention in recent years thanks to the advances in the devices (in terms of size, power consumption, wireless communication performances and manufacturing costs) and standardization of new air interfaces both for infrastructure-less and infrastructure-based wireless networks progresses (e.g. *Wi-Fi*, *Bluetooth*, *Zigbee*), attracting both academic and commercial interest.

A *wireless sensor network* (WSN) is composed of *sensor nodes* for monitoring environmental physical conditions or variables such as temperature, humidity, vibrations, pressure, motion, and pollutants, among others, at different locations. Typically, a *sensor node* is a small autonomous device that includes three basic components: a *sensing system* for data acquisition from the physical environment, a *data management system* for local data storage and, eventually, processing, and *a wireless communication system* for data transmission.

Moreover, a power source supplies the energy needed by the device to perform the tasks. The power source of wireless sensor nodes is usually stored in a battery that may not be easily replaceable or rechargeable. Because the sensor network should be able to perform the monitoring operations of the environment for a sufficient time (which could be days or months), the battery lifetime may not be compatible with the expected performances of the node; it is therefore required to scavenge energy from the external environment.

3.1 WSNS ARCHITECTURE

Although WSNs can be considered as a special case of *wireless ad hoc networks*, they share several common aspects, but with substantial differences. Wireless ad hoc networks are formed dynamically by an autonomous self-organizing system of nodes communicating over a common wireless channel. Nodes establish link connections through ad-hoc topologies that, contrary to other networks (e.g. *Wi-Fi* or cellular networks) are not supported by any type of additional infrastructure such as base stations, a wired backbone or a central network controller.

The organization of a WSN is affected by factors such as scalability, fault tolerance, power consumption and environmental conditions.

In a *centralized topology network* (Toumpis and Toumpakaris 2006), such as the cellular network of mobile communication systems, a large number of users of mobile terminals (e.g. mobile phones) are wirelessly connected through an extensive infrastructure of base stations linked through high-speed links with a central network controller that manages the operation of the network (e.g. in a GSM network this entity is the Base Station Controller). Each node (e.g. a mobile phone) routes its data through a nearby base station, over a shared wireless medium. Given its architecture, the mobile network is to be considered as a *wireless access network* (where only the end nodes are connecting wirelessly, whereas the infrastructural network is typically wired) rather than a *wireless network*. Several different topologies have been applied to wireless self-organization networks, such as clustered sets, star, tree, grid and mesh-based topologies. Moreover, smart nodes in wireless ad-hoc networks usually have no energy limitation (e.g. laptop computers) and each node in the network is both a transmitter and a receiver.

There is a clear distinction between *ad-hoc networks* and WSNs due to the different complexity of the nodes, the power constraints of sensor nodes and the limited size of the information exchanged.

Contrary to a centralized network, nodes in a wireless ad hoc network are not managed by a centralized system but must autonomously organize themselves in the network. Furthermore, the transmitted data must follow a non-trivial multi-hop route through the shared wireless medium. The multi-hop transmission, while ensuring reduced power consumption in the transmission of the information to the final sink, has a limited capacity and is liable to frequent changes.

Nodes in WSNs can be *stationary*, if they maintain their position during time, or *dynamic* if they are moving. *Wireless Ad Hoc Networks* are those in which nodes discover their neighbors and self-organize to perform peer-to peer data routing with topologies that are generally dynamic and decentralized.

WSNs are composed of nodes that are at least of two different types, *sensor* and *sink* nodes, and in general deal with a limited amount of information to be transmitted.

Sensor nodes gather data from the environment and then forward the information to a controller connected to other networks (e.g., the Internet) through a gateway. The message forwarding can be performed via multiple-hop relaying so to minimize the maximum transmission distance for power saving as radio devices are one of the most power consuming elements of a sensor node.

The purpose of a WSN is to gather and process data originated by sensors, whereas sinks are in charge of collecting such data. The network's connectivity must ensure that any sensor node is able to reach at least one sink node, in order to successfully report the measurements, either with a direct connection to the sink or with multi-hop routing through other sensor nodes.

The network connectivity is crucial both in terms of scalability and reliability of the system. Considering the most basic type of WSN (see Figure 3), the capacity of a *single sink* network with end nodes directly connected to the sink, in terms of the maximum number of nodes within the transmission range that can be able to transmit data from sensors, is directly proportional to the maximum data throughput measured at the application layer and the time intervals of transmission (the longer the intervals, the higher the capacity). However, the capacity of the single sink decreases with the size of samples to be transmitted by the nodes. Therefore the capacity of a single-sink WSN is highly dependent on the requirements set by the application scenario.

To overcome transmission range limitations it is possible to increase the spatial density of nodes while enabling the possibility to forward the data samples through multiple hops (i.e. each node can transmit data to the nearest node that, in turn, will forward it to its neighbor towards the network's sink). This is

the case of a *single sink- multi hop* network as shown in Figure 3c where the nodes out of the sink's range can transmit their data through their neighbors within the range area. This coverage extension has a drawback in the reduced nodes capacity of this network configuration as a sample transmitted by means of *n* hops requires *n* transmissions. Considering an average number of hops per sample n_h in the system, without a smart reuse of the radio resources, then the capacity of the single-sink multi-hop WSN is reduced by a factor n_h (Verdone, et al. 2008).

In order to decrease the probability of isolated cluster of nodes in a WSN, it is possible to increase the number of sinks in the system (Figure 3b). In this configuration two different cases are possible:

- sinks are connected to a separate network
- sinks are disconnected

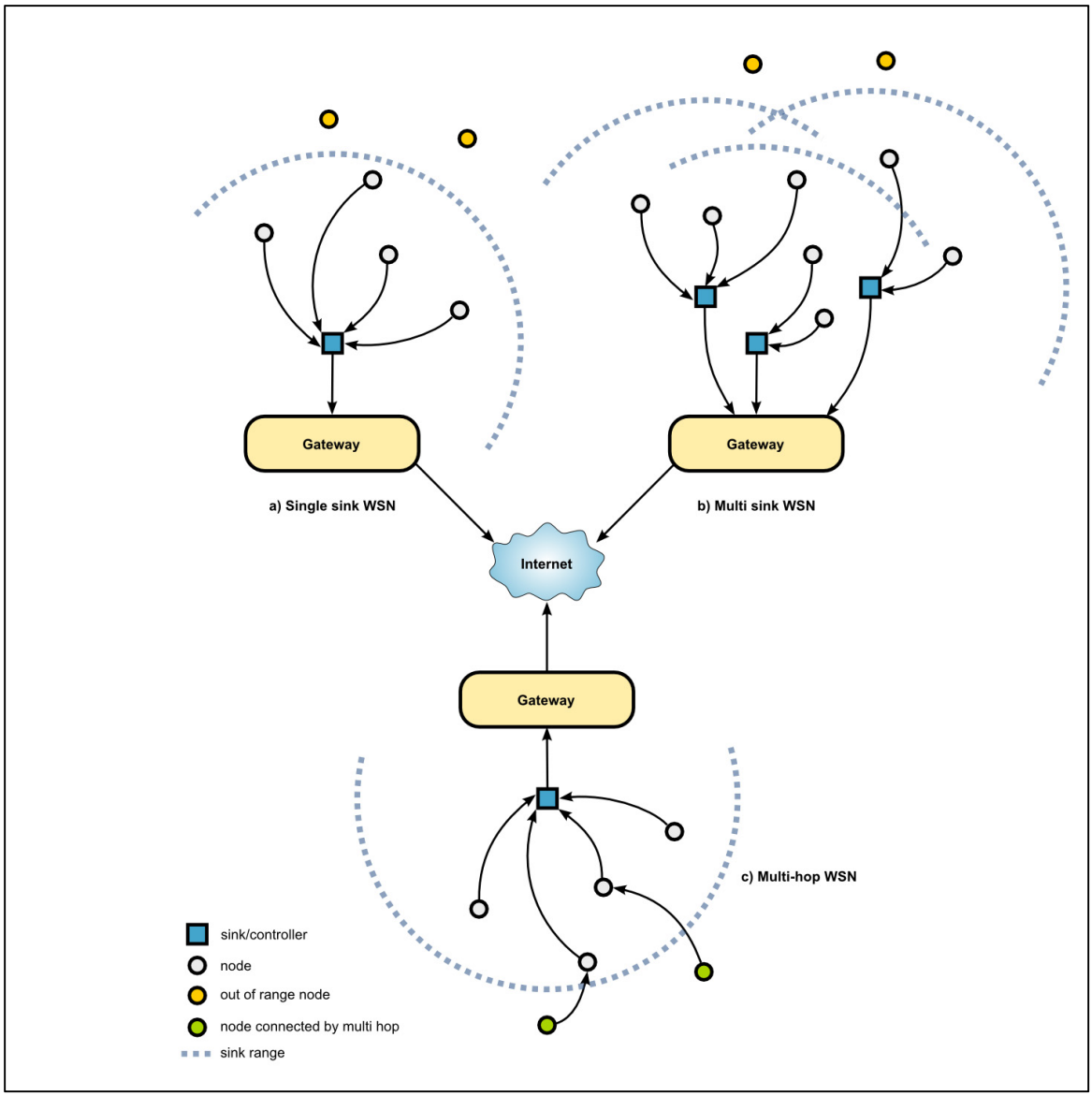


Figure 3 – WSN architectures

In the *first case* all the sinks are connected through a separate network over a mesh network or via direct links with a common gateway; a node needs to forward the data collected to any element in the set of

sinks. To enhance the performance of this network the node's protocol must perform a selection of the sink node on the basis of a suitable criterion (e.g., minimum delay, maximum throughput or minimum number of hops). The presence of multiple sinks allows better network performance provided that the communication protocols are properly designed according to suitable criteria. This increases the protocols' complexity but offers the possibility of achieving better performances.

In the *second case*, with multiple disconnected sinks, the nodes tend to be partitioned into smaller network components as they connect to different sinks; however, the complexity of the communication protocols is not increased but, in order to successfully reach a sink node, sink discovery mechanisms must be included to effectively route the information to the desired sink.

3.2 Sensor Nodes (motes)

A sensor node (or mote) is a device in a WSN that gathers information from the external environment, can process the acquired information and perform decisional tasks, and communicates with other connected nodes in the network.

WSN nodes have specific hardware characteristics and limitations. Most WSN nodes have limited available energy: some rely on batteries and some implement environmental energy harvesting techniques (e.g. solar panels or vibration-powered generators). Therefore WSN nodes tend to be small embedded systems with few processing resources and low bit rate capable of establishing limited low range radio links. Cost and size restrictions impose similar constraints.

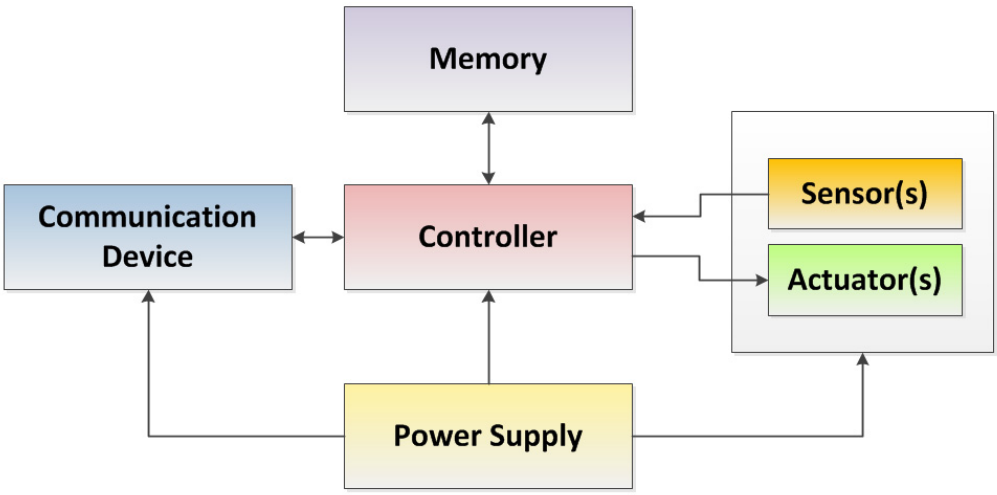


Figure 4 - Architecture of a sensor node

A typical architecture of a WSN sensor node consists of the following main components as shown in Figure 4:

- Controller
- Sensor/Actuators
- Memory

- Communication device
- Power Supply

The *controller* in a WSN is responsible for a node's main tasks of running analysis and computational tasks and for processing data. In order to minimize energy consumption, different running modes are available (i.e. active, idle, sleep modes) and the controller can decide upon the transmission of signals. When the node is part of a network, the controller also keeps information about its neighboring nodes and can decide the routing path and communicates the routing information to the other nodes.

Sensors are used to collect data from the environment (e.g. light, accelerations, vibrations, temperature, or radiations) and they may provide signals to wake up the controller from sleep mode when a predefined threshold is exceeded. Conversely to sensors, *actuators* are means of the nodes' devices to manipulate the environment rather than observing it. They are meant to take action following local measurements or centralized decision processes (e.g. activating an alarm or closing valves in a plant system). Sensing units are usually composed of two subunits: *sensors* and *analog-to-digital converters* (ADCs). The analog signals produced by the sensors are converted to digital signals by the ADC, and then fed into the processing unit.

Memory is used to store temporary data, or during data processing.

Power supply is a critical aspect as motes are generally geographically distributed and may have difficult access. For this reason replacing discharged batteries can be difficult and the possibility to power the hardware of a sensor node for a long period of time can significantly improve the possibility of implementation of a wireless sensor network. On the one hand, the design of a mote must be targeted to maximize the overall energy efficiency of the device to ensure its operability during the network's lifetime; on the other hand the possibility to recharge the battery with energy scavenging systems can offer improved flexibility to the system. For these reasons sensor nodes can be coupled to energy harvesting solutions from ambient energy sources such as:

- Light
- Temperature gradients
- Vibrations
- Pressure variation
- Air/liquid flow

Finally, the *communication devices* ensure the information exchange with the other nodes of the network or with the sink. Wireless radio transceivers can be the major power consuming subsystem of a sensor node. If the node is part of a network, data can be transmitted from the node to the destination using *single hop* or *multiple hops* communication between source-destination pairs that significantly reduces the transmission power necessary to deliver packets in wireless ad hoc networks. Power control techniques may be adopted to further reduce energy consumption by setting the transmit power at the minimum level needed to allow signal correct detection at the receiver end. However, setting a transmitter into sleep mode prevents a data burst sent to the node to be detected. For this reason the management of sleep mode in transceivers is a complex task in WSNs.

3.3 WSN APPLICATIONS

WSNs can be applied to a broad range of possible applications in the real world, from environmental monitoring, health care, positioning and tracking, to logistic. WSNs application can be divided in three

main groups (Buratti, et al. 2009): event detection (ED), spatial process estimation (SPE) and mixed ED and SPE.

ED applications use sensors to detect event (e.g. forest fire early detection or flood warning systems) or customer behavior surveillance are among many sensor network applications. Signal processing of Sensor nodes in ED applications is very simple as a single device has to compare the measured quantity with a given threshold to decide whether to send the information to the sinks. The density of nodes must ensure that the event is detected and that the information can be routed successfully within the network. Decisions can be performed by single nodes, or they can be decentralized and managed cooperatively by multiple nodes in more complex scenarios.

In SPE applications, sensor nodes capture geographical local information and all together contribute to the estimation of a spatially distributed process. The single measurements are analyzed either with a distributed process by the nodes, or centrally by a supervisor. Being spatially distributed, measurements at nodes are sampling the environment and the accuracy of the estimation is necessarily dependent on the nodes' density and their geographical distribution in relation to the phenomenon to be observed.

3.3.1 Environmental monitoring

The use of WSN for reliable environmental monitoring solutions can significantly improve the effectiveness and feasibility of systems thanks to the wireless and ad-hoc network capabilities of sensor nodes. Usually, geographically distributed sensors can be located in wide areas and in remote site environments. Power is a critical issue as well as nodes distance and density in order to ensure the connectivity of all the nodes and to gather sufficient information representative of the phenomenon of interest.

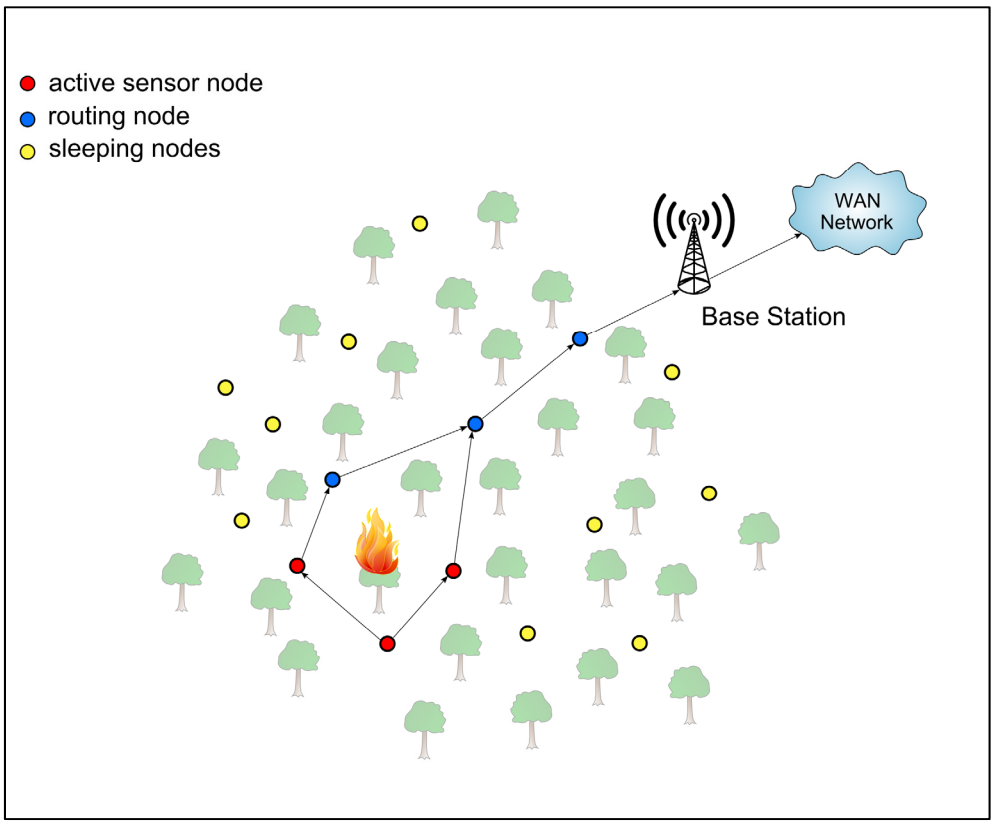


Figure 5 - WSN for forest fire detection and alarm activation

WSN have been successfully applied to examine subglacial processes (Hart, et al. 2006) by inserting *sensor probes* into the ice; the sensor nodes send their information to a base station on the ice surface that subsequently forward them to a fixed reference gateway station of the system (Martinez 2004).

Several research works have investigated the possibility to implement WSN for forest fire detection (Li, Wang and Song 2006) either with ad-hoc networks (Figure 4) or centralized wireless networks (Doolin and Sitar 2005) with sensors ranging from humidity and temperature sensors to more sophisticated fire detection systems based on image processing.

3.3.2 Structural Health Monitoring – Smart Structures

WSNs are being investigated as possible low cost systems for the monitoring and detection of structural integrity in civil engineering structures. A structural health monitoring (SHM) sensing systems assesses the integrity of structures such as buildings, bridges, aerospace structures and the operating conditions with various types of sensors. The collected information is at the basis of the evaluation of the safety of the monitored structure using damage diagnosis or prognosis methods. The advantage of a WSN for structural monitoring is the possibility of eliminating lengthy cables, thus offering a low-cost alternative to traditional cable-based structural health monitoring systems. Another advantage of a WSN is the ease of relocating sensors, thus providing flexible and easily reconfigurable system architecture.

SHM applications usually have specific requirements that differ from the usual one in WSNs applications. They can generate high data rates, whereas typical WSNs implementations tend to transfer minimal samples and several popular SHM algorithms require centralized implementations. In fact traditional SHM systems are essentially high end wired data acquisition systems that collect structural response data from several sensors and a central unit processes all the information.

In the case of civil structures, powering the devices can be an issue when the sensor nodes are in inaccessible locations. On the other hand the devices are usually external to the structure thus giving an ease of access when compared to embedded sensors nodes. Moreover, sensor nodes can be assigned with computational analysis tasks to analyze the measured values to autonomously evaluate the possible damage level.

There are many attempts in using sensor nodes as structural monitoring systems: these implement sensors like dual-axis accelerometers for three-dimensional vibration and tilt sensing embedded in bricks (Engel, et al. 2004); the University of California at Berkeley installed 64 nodes distributed over the main span and the tower of the Golden Gate bridge (Kim, et al. 2007) to collect ambient vibrations synchronously at 1kHz rate over a 46-hop network.

The monitoring of heritage buildings of artistic interest is performed to control both vibrations and deformations with Fiber Optic Sensors (Ceriotti, et al. 2009).

Another example of the implementation of WSN monitoring in real civil structures is the structural monitoring system of the Alamosa Canyon Bridge in New Mexico (Lynch, et al. 2002) consisting of wireless sensing unit prototypes. The monitoring system was used to record the bridge response to excitations applied during forced vibration testing. The wireless sensing unit also performed fast Fourier transforms (FFT) to identify the primary modal frequencies of the bridge during testing.

3.3.3 Industrial and Building Automation, Logistics

WSNs are gradually adopted in industrial applications thanks to their advantages over wired networks; however security and quality of service concerns are still limiting their widespread use. Moreover, WSNs

adding sensing and acting capabilities to objects in the physical world widen the realm of applications. Node to node communications also add increased flexibility in their adoption in industrial manufacturing and control systems where automation has been successfully introduced (e.g. in car, household appliances or food industries) helping in reducing the problems associated with traditional cabling.

WSNs have been applied to many industrial automation applications such as pressure/flow/temperature monitoring, precision instrumentation, quality measurements, overlay monitoring, supervisory control and data acquisition (SCADA) systems, tank monitoring, utility power-line or oil and gas pipelines monitoring (e.g. to control oil pipeline temperatures in harsh environments.).

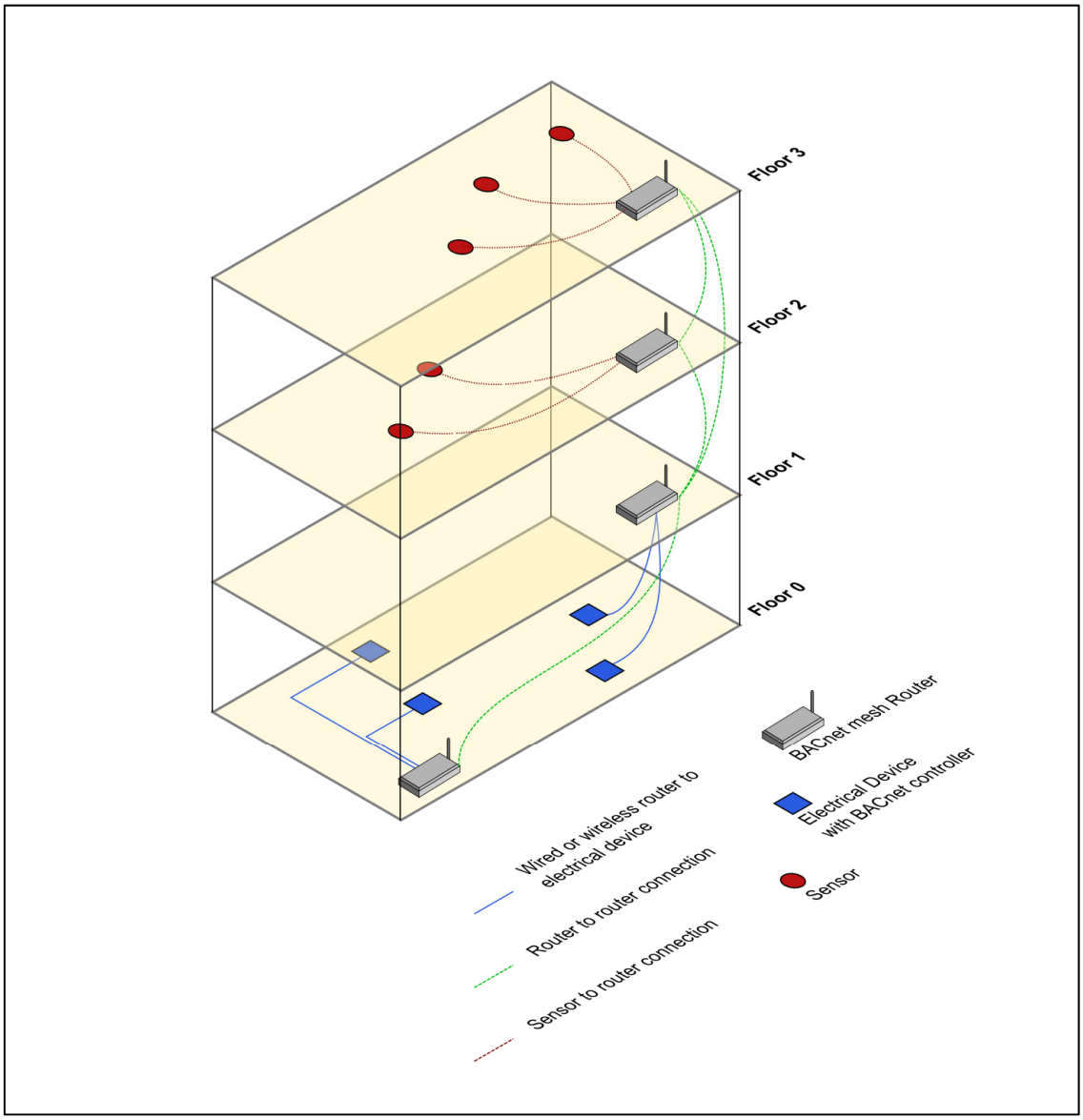


Figure 6 - Example of building automation integration with a WSN

Zigbee based industrial automation networks are implemented to achieve control, efficiency, and safety, in existing manufacturing and process control systems, with continuous monitoring of critical equipment. Sensor nodes collect data on the performances of the equipment, and for the automation of processes for reducing user intervention and to improve the preventive maintenance of the machines (Huang, Hsieh and Sandnes 2008).

Commercial applications are available to detect threats to security and safety in logistics such as the wireless chemical and radiation detection for shipping containers as during transportation. In this case wireless systems, using ZigBee-ready technology, communicate sensor readings to a central network node of a shipping vessel. There, relevant information is uploaded by satellite and read by the US coastguard so that they can deal with any threat before it reaches the coastline (Egan 2005).

Logistics need to track the travelling items with efficient processes and RFID tags are commonly used along with WSNs both by carriers and hub sites for location, cargo storage register in warehouses and management of the shipping goods all along their route to destination. Satellite and GPS are used to track fleets of vehicles and ships that can be constantly monitored. A wireless network in logistics can link directly to the RFID systems (i.e. optical bar code readers, portable and handheld devices) and a central systems process and manages the information to check the goods, update records and displays the list of goods stored. WSN in logistics aim at boosting quality of the distribution process and minimize human errors (e.g. packages sent to the wrong destination or stored in wrong locations leading to missing items).

Building automation (BA) has already progressed in the past years with wired devices enabling the monitoring and control of non-critical functions in the area of residential and commercial applications (Figure 6) eventually based on BACnet (an ISO standard communications protocol that allows communication of building automation and control systems). BA comprises a set of functions that includes lighting control, energy conservation, environment control and safety and security (Gutiérrez 2007) and the interest in WSNs for building automation applications is driven by non-invasive installation thanks to the absence of cabling that consists in reduced labor, materials, testing, and verification.

3.3.4 MANETs AND VANETs

Wireless ad-hoc architectures can also be implemented in networks of mobile devices (MANET). The MANET consists of a dynamical network that frequently changes as sensor nodes enter the transmission area or move away losing the connection. In MANETs sensor nodes are capable of routing the data received from the other nodes and, for this reason, the complexity of the transmission protocols is increased. A particular case of MANET is the vehicular ad-hoc network (VANET) specifically related to the implementation of sensor nodes in vehicles.

- Active safety (collision warning)
- Traffic efficiency (active traffic management, enhanced route guidance and navigation, green light optimal speed advisory)
- Environmental friendliness

Car navigator devices have spread in the last years with availability of low-cost GPS receivers and wireless local area network transceivers. The researchers are aiming to equip every vehicle with a radio communication system for vehicle-to-vehicle and vehicle-to-roadside communication.

The intelligent co-operative systems are the next big challenge in automotive electronics and Intelligent Transportation Systems (ITS). The communication based on ad-hoc network structures allow moving devices on board of vehicles to communicate with fixed based stations (e.g. for the traffic management or pollution recordings) or communicate in real-time with other vehicles for a collaborative distributed system (e.g. for the implementation of alert systems to obtain local traffic information to detect dangerous situations).

The EC-funded (7th Framework Programme) *PRE-DRIVE: C2X project* (Preparation for driving implementation and evaluation of C2X communication technology) main goal was to develop a detailed

system specification and a functionally verified prototype to be used in future field operational tests. Another EU project, iTETRIS (Krajzewicz, et al. 2010), investigates communication technologies (Bauza, Gozalvez and Sanchez-Soriano 2010) to improve traffic management through Real-Time exchange of Traffic Information (RTTI) for road traffic congestion detection through cooperative vehicle-to-vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications.

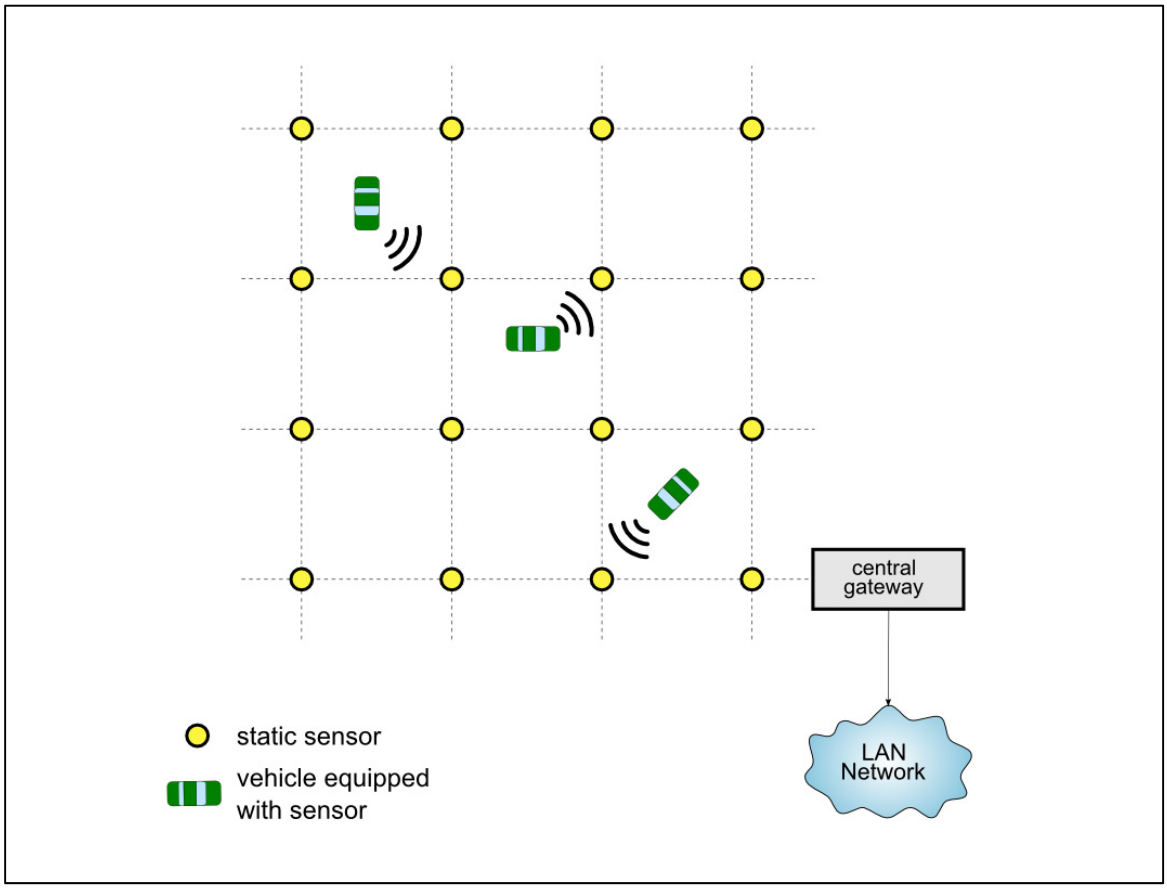


Figure 7 - Architecture of the mixed static and mobile sensor nodes for air traffic pollution monitoring (Ma, et al. 2008)

Air quality or air pollution monitoring is another application that benefits from of the WSN architecture to collect spatially distributed data to overcome the limitations of the existing fixed monitoring stations: the later one are usually located so as to measure ambient background concentrations or at potential hotspot locations, typically they are several kilometers apart and may therefore miss in capturing the real situation because pollution levels and hot spots change with time. Therefore, due to the limitations of the conventional environmental data monitoring systems, it may not be possible to achieve a sufficient temporal or spatial detail to represent credible models.

In London, a hierarchical network architecture formed by the mobile sensors and stationary sensors has been designed with the mixed use of roadside stationary sensor nodes and mobile devices installed on public vehicles (Ma, et al. 2008).

Here the sensors connect to the main Grid network by several Sensor Gateways (SGs) with different wireless access protocols. The sensors collect air pollution data and send the values to the remote grid with a multi-hop transmission. This capability enables the sensors to exchange their raw data locally and

then the data analysis and data mining is then performed in a distributed way. Finally, the SGs connect the wireless sensor network to the IP backbone, which can be either wired or wireless.

Another example of a MANET is the *ZebraNet* project (Juang, et al. 2002): an ad-hoc sensor network was developed with sensor nodes embedded in collars applied to zebras in the wild for the collection of data and the monitoring placed on sampled set of zebras. The ad-hoc network has the advantage to overcome the limit of no cellular coverage for the study area and has the advantage of reduced costs over.

Nodes (i.e. the tracking collars) collect logs of GPS position and other information. Researchers' base station collected data from the collars on the basis of node to node links (peer-to-peer communication) to aggregate data back. The sensor nodes are composed of a short-range power efficient radio for peer transfer among the collar nodes, a long range radio necessary to communicate with the base station, a microcontroller unit, a GPS device and power supply with the support of solar charging cells. The geographical position is periodically retrieved from the GPS and stored into the on-board flash RAM. As not all the collars can be within the range of the base station, data must be routed with multi-hop towards the network's sink. Moreover, not only collar nodes are moving, but also the base station is only active intermittently as researchers are driving to approach distant herds. Due to the dynamical network, the *ZebraNET* protocol is designed so that the node's data are flooded to all neighbors whenever they are discovered.

4 Wireless Systems

Different methods and standards of wireless communication exist across the world. These technologies can be classified into individual categories, based on their transmission range and specific application as shown in the Figure 8.

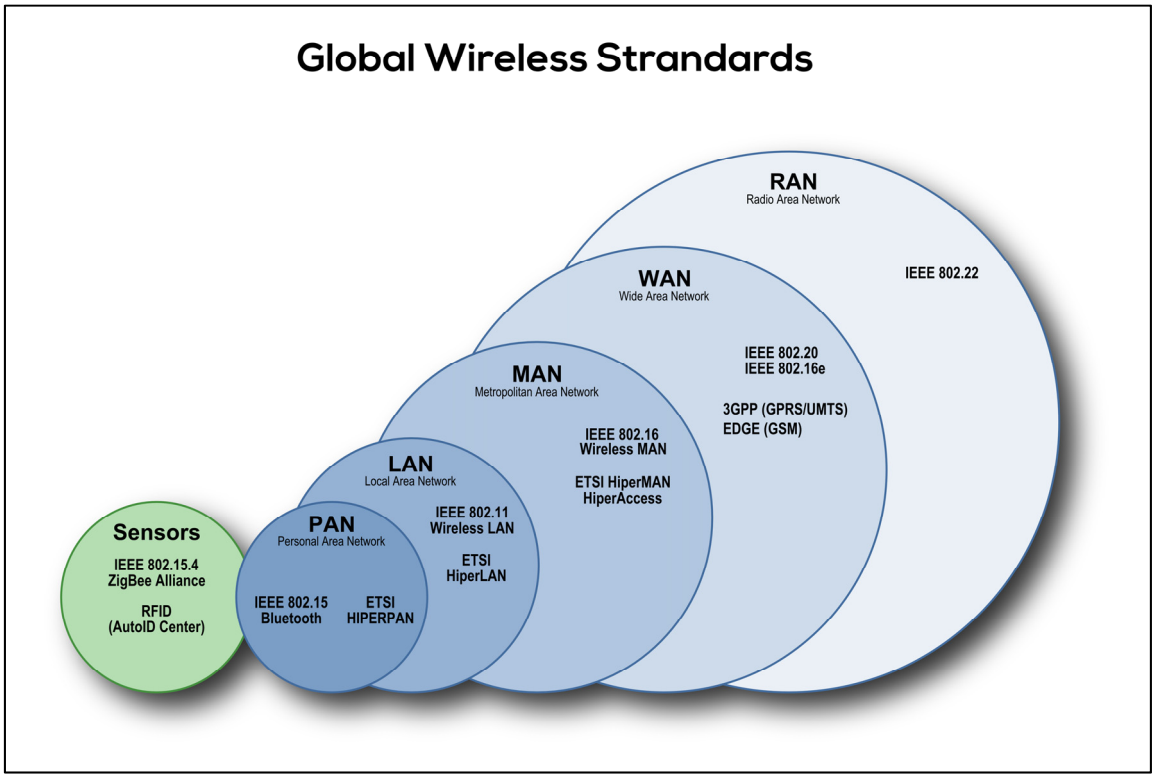


Figure 8 - Global Wireless Standards

- A *Personal Area Network* (PAN) is a localized computer network used for low-power short range communication among personal electronic devices (e.g. smart phones and wireless headphones) with Bluetooth as the most diffused industrial specification for wireless PANs. The typically range of a few meters of a PAN is used in the connection among personal devices themselves, or for connecting to a higher level network.
- A *Wireless Local Area Network* (WLAN) is a flexible data communication system that uses radio communication to accomplish the same functionality as LAN network and interconnects computers without using wires. WLAN uses radio waves to transmit data with spread-spectrum technology to enable the wireless communication between multiple devices in a limited area. This ensures the mobility of the connected devices within the coverage area while maintaining an active connection to the network. The IEEE 802.11 standard (Wi-Fi) denotes a set of Wireless LAN/WLAN standards developed by *working group 11* of the IEEE LAN/MAN Standards Committee (IEEE 802). The 802.11 standard includes six over-the-air modulation techniques all using the same protocol but with different performances in terms of both transmission rate and range within 100 meters.
- *Wireless Metropolitan Area Network* (MAN) is based to the standard IEEE 802. The WiMAX (Worldwide Interoperability for Microwave Access) IEEE standard is a technology of broadband wireless communication that was designed to complement DSL and cable lines and provide broadband Internet access to fixed or mobile devices. In a WiMAX network, subscriber stations communicate with the core-network connected base-stations to provide wireless access functions with an expected range of 6-8 Kilometers in non-line of sight capable frequencies and up to 16 Kilometers are very likely in line of sight applications. WIMAX networks are simple to build, relatively inexpensive and provide a good alternative to fixed line networks.
- A *Wide Area Network* or WAN is a network covering a broad geographical area (e.g. Internet). WAN's are used to connect local area networks (LAN's) together, so that computers in one location can communicate with computers in other locations. WAN's can belong to private organization or can be managed by Internet service providers. In addition, WAN's also refers to mobile data communications (e.g. GSM, GPRS and 3G).

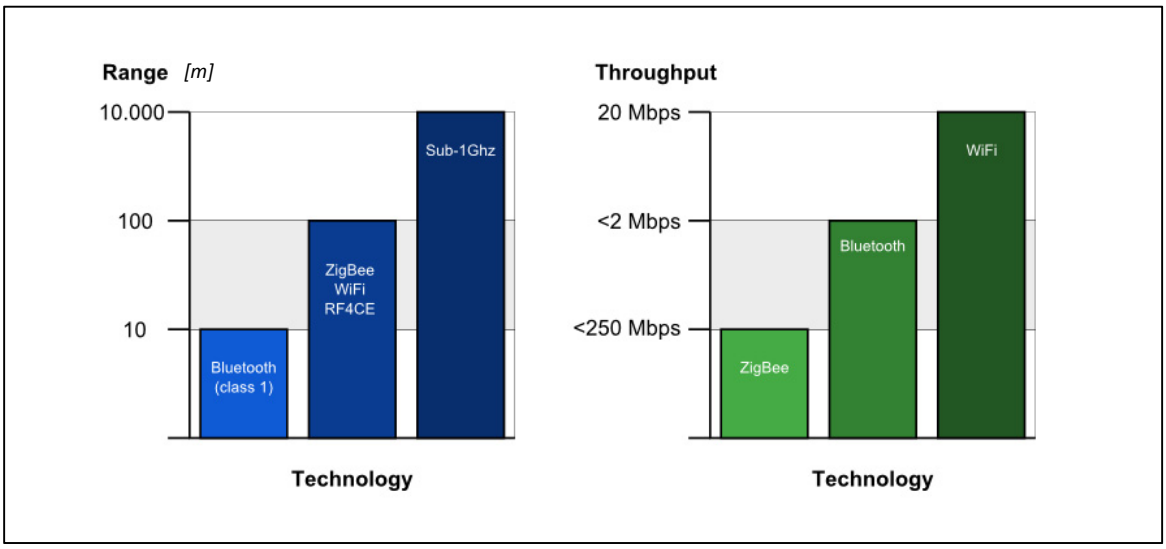


Figure 9 – Range and throughput of common wireless technologies

In contrast to the technologies described in the previous points, the standard IEEE 802.15.4 is specifically conceived for low rate, low range sensor nodes applications and is the usual choice in WSN applications.

All the different standards for wireless communications are targeted for specific applications and working conditions; because of this communication ranges and throughput vary significantly (Figure 9) ranging from the minimal distance of the Bluetooth standard to the high distance achieved with WAN Networks as reported in Table 1.

Table 1 - Comparison of Wireless technologies (source: www.zigbee.org)

	802.15.4 (ZigBee)	**GSM/GPRS CDMA/1xRTT**	**WiFi 802.11b**	**Bluetooth 802.15.1**
Application Focus	Monitoring and Control	Wide Area Voice and Data	Web, email, video	Cable replacement
System Resources	4Kb-32Kb	16MB+	1 MB+	250Kb+
Battery Life *(days)*	100-1000+	1-7	0.5-5	1-7
Network size	over 65000 for a ZigBee star network	1	32	7
Max Data Rate *(kbps)*	20-250	64-128+	11000+	720
Transmission Range *(meters)*	1-100+	1000+	1-100	1-10+
Success Metrics	• Reliability • Power • Cost	• Reach • Quality	• Speed • Flexibility	• Cost • Convenience

4.1 Wireless Networks Common Topologies

The topology of WSNs consists of the logical way the nodes are organized in the network to communicate. WSNs may implement different network topologies to improve performances such to reduce the cost, power consumption and complexity while improving the overall reliability.

Four main common topologies (Figure 10) are usually implemented in WSNs:

- **Peer-to-Peer networks**
  are based on a communication model in which each node has the same capabilities and can communicate directly with the other nodes without going through a centralized communications hub. Each *peer device* is able to function as both a client and a server.

- **Star networks**
  are one of the most common computer network topology in which all nodes are connected to a centralized hub or computer. Each node cannot communicate directly with the other nodes but all the communications are routed through the centralized node that is the common connection point of all the nodes in the network. Each node is defined as a *client* while the central hub is the *server*.
- **Tree networks**
  in these networks, nodes are hierarchically-organized with a top level central hub (root node) that is the main communications router. At the lower level, router nodes are connected to the root node forming a star network. For every child router, additional sub levels of more child routers can also be connected. End devices can connect to the network either by a router node or, eventually, directly to the root node.
  Messages are sent within the network following hierarchical routes: the source nodes transmit messages to the higher level parent nodes which then relay their messages higher up the tree and vice-versa. With respect to the other network topologies, the *tree network* can be considered a hybrid of both the Star and Peer-to-Peer topologies.

- **Mesh networks**
  these networks offer higher flexibility and reliability as they offer multiple paths for messages within the network. With this topology the network is self-healing and messages can be sent with multi-hops from node to node. Each node is then able to communicate with the other nodes as data are routed from node to node until the desired location. The flexibility and reliability of this topology is however associated to a greater complexity of the network and protocols.

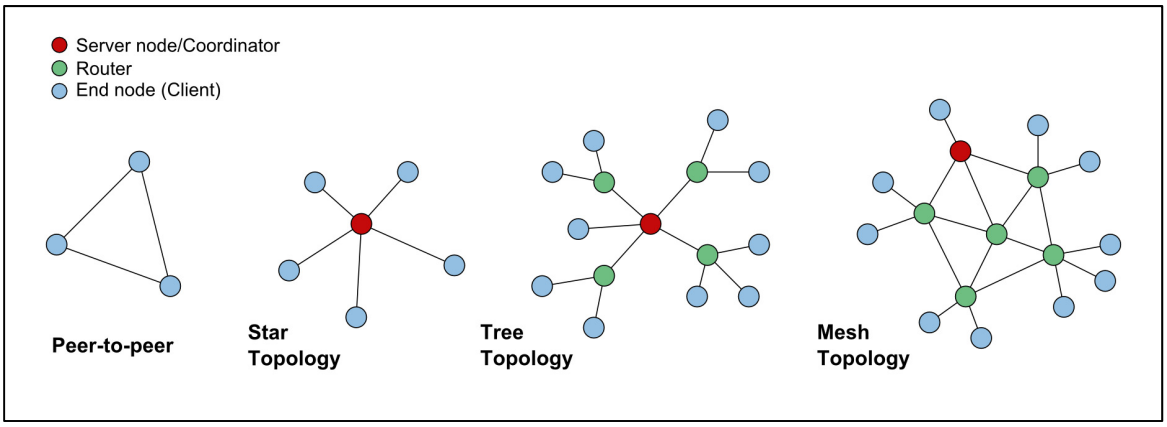


Figure 10 - Wireless Networks common topologies

5 Wireless Sensor Network Technologies

5.1 Wi-Fi

The IEEE 802.11 technology is designed to implement single-hop ad hoc networks with extreme simplicity. The *Wi-Fi* stations must be within the same transmission radius (about 100-200 meters) to be able to communicate. When the distance between a device and the router increases, the Wi-Fi range limitation

can be overcome by implementing multi-hop ad hoc networking with the addition of routing mechanisms at stations. Intermediate routers forward packets towards the final destination (Anastasi, et al. 2004).

5.2 Ultra Wide Band

Ultra-Wideband (UWB) is a radio technology used in wireless networking, developed to achieve high bandwidth connections with low power utilization.

Ultra-wideband technology differs substantially from other technologies (e.g. Bluetooth and 802.11a/b/g): it is based on short pulses using an extremely wide band of RF spectrum, on the order of several *GHz*, with low duty cycle and power spectral density with the main advantage of being able to transmit more data in a given period of time.

These characteristics provide UWB radio with important advantages:

- high-resolution ranging
- low processing complexity
- robustness to multi-path fading
- ability to penetrate obstacles
- large interference-resistance to other systems (e.g. GPS, radar and WLANs).

This technology is considered very interesting for many applications, including sensor networks, high accuracy localization, ground-penetrating radar, and through-the-wall imaging.

5.3 Bluetooth

The goal of Bluetooth technology is a short-range communication system to replace the cables in WPANs to enable users to connect, in a rapid or automatic way, a wide range of personal electronic devices (e.g. smartphones, speakers, GPS receivers, bar code scanners).

The initial idea, coming from an Ericsson project in 1994, was to replace wires. The project evolved and generated the Bluetooth Special Interest Group (SIG) and it was standardized by the IEEE as Wireless Personal Area Network (WPAN) specification IEEE 802.15.

The Bluetooth SIG is a trade association comprised of 17433 member companies (December 2012) and a small staff which is aimed to help the development and promotion of Bluetooth wireless technology.

Bluetooth is useful when transferring low-bandwidth information between two or more devices that are at a short distance and form a Personal Area Network (PAN). The key features of Bluetooth wireless technology consist of robustness, low power, and low cost.

5.3.1 Range

Bluetooth defines three power classes that determine the ranges:

- **Class 1 radio** has a maximum output power of 100*mW*, is capable of power control, in steps of 2 to 8 *dB*. The range is about 100 meters. It is most commonly found in industrial use cases.
- **Class 2 radio** has a maximum output power of 2.5*mW*, the power control is optional and the range is about 10 meters. It is most commonly found in mobile devices.
- **Class 3 radio** has a maximum output power of 1*mW*, the power control is optional and the range is about 1 meter.

The effective range varies due to many parameters such as battery conditions and propagation conditions. Manufacturers can tune their range to support the use case they are enabling.

5.3.2 SPECTRUM

Bluetooth operates at unlicensed 2.4 *GHz*, using 79 channels of 1-*MHz* bandwidth from 2.402 to 2.480 *GHz*, (with additional guard bands) using a spread spectrum, frequency hopping, full-duplex signal through the use of a time-division duplex (TDD) scheme, at a nominal rate of 1600 *hops/sec* to combat interference and fading. It can transmit data up to 1*Mbit/s*, can penetrate solid non-metal barriers, and has a nominal range of 10 *m* that can be extended to 100 *m* depending on the class range. Nodes are organized in star network topology *piconets*, managed by a master Bluetooth station that can service up to 7 simultaneous active slave links. A network of these *piconets* can allow one master to service up to 200 slaves (Lewis 2004).

5.3.3 BLUETOOTH CORE SPECIFICATION

Thanks to the Core System, Bluetooth devices can connect to each other and exchange a variety of classes of data. The last Bluetooth Core Specification is the version 4.0. This version provides Classic Bluetooth technology, Bluetooth low energy technology, and Bluetooth high speed technology. All three specifications can be combined or used separately in different devices according to their required functionality.

In particular, Bluetooth low energy technology (BLE) guarantees to consume only a fraction of the power of the more common Bluetooth radios. This solution enables the BLE technology to be used in devices powered by coin-cell batteries making it possible to ensure an operating up to more than a year. In order to save power different states are possible: BLE devices can normally be in a power saving connectionless state but still being aware of each other, and they can activate the communication link for as short a time as possible only when it is necessary. In addition, the last core Specification allows also an enhanced range and a lower cost.

Wireless sensors based on Bluetooth have not been met with wide acceptance due to limitations of the Bluetooth protocol including:

- Relatively high power for a short transmission range.
- Long time nodes synchronization to the network when returning from sleep mode
- Low number of nodes per network
- Complex medium access controller (MAC) layer if compared to that required for wireless sensor applications.

5.4 IEEE 802.15.4

IEEE 802.15.4 defines a low-power radio and media access controller (MAC). Although is the best-known higher-layer protocol stack using the 802.15.4 radio standard, is not the only one.

Other protocols have been developed but their limited diffusion has the consequence of a limited offer of devices on the market and their practical implementations.

Although communication standards generally have a consistent regulation around the world, each country still retains control of its own radio spectrum. Different working radio frequencies are assigned in different regions to the IEEE 802.15.4, with the 2.4 GHZ being common at a global level (see Table 2). The lower frequency bands have the advantage of a greater range and lower power consumption but are not global.

Table 2 - Radio frequencies defined by IEEE 802.15.4

Frequency	Channels	Throughput (kbs)	Region
868 MHz	1	20	Europe
915 MHz	10	30	USA
2.4 GHz	16	250	Global

Wireless standards using the unlicensed bands need to conform to national requirements for usage. These exist to ensure that the spectrum is used fairly.

In the following paragraphs the different protocols developed within the IEEE 802.15.4 specifications are reported:

- ZIGBEE
- WIRELESSHART
- 6LoWPAN

5.4.1 ZIGBEE/IEEE 802.15.4

Communication network protocols are structured as a stack of layers. Each layer provides the directly upper and lower layers with services according to well-defined interfaces. The layered model of network architecture protocols has many advantages, in particular the independence of one layer from the others, a greater flexibility and compatibility between devices, systems and networks.

ZigBee is a specification for a suite of high level communication protocols; in fact ZigBee defines only the networking, application and security layers. As shown in Figure 11, the two lowest layers NWK and PHY, are defined by IEEE 802.15.4 standard. ZigBee adopts IEEE 802.15.4 physical and medium layers as part of itself.

As IEEE 802.15.4 is a standalone protocol suite, it is possible to develop a wireless network completely different from *ZigBee*.

5.4.2 ZIGBEE PHYSICAL LAYER

The Physical layer specifies the physical parameters of the network such as data rate and receiver sensitivity requirements. At this level are also specified the frequencies of operation: 868-868.6 *MHz*, 902-928 *MHz* and 2400-2483.5 *MHz*.

The devices targeted at global applications must use the 2.4 *GHz* band because this is the only one authorized to be used worldwide. Unfortunately IEEE 802.11b operates also on this band and this could affect the connectivity where Wi-Fi network operates.

For the 2.4 GHz band, the PHY layer defines 16 channels, a chip rate of 2000 *Kchip/s*, a bit rate of *250 Kb/s* and a modulation O-QPSK.

Zigbee has many advantages over Bluetooth for WSN applications because of the former's features:

- **true low power** – sensor nodes can run for a long time from a single battery making them less prone to maintenance and user intervention. Low consumption coupled to energy scavenging systems can allow a truly independent energy system.
- **easy multi-hop networking** – the simplicity of the network stacks ensure easy configuration of the network with a reduced complexity of the protocols
- **low data rates** the *Zigbee* standard is adequate to low bandwidth applications like home and industrial automation

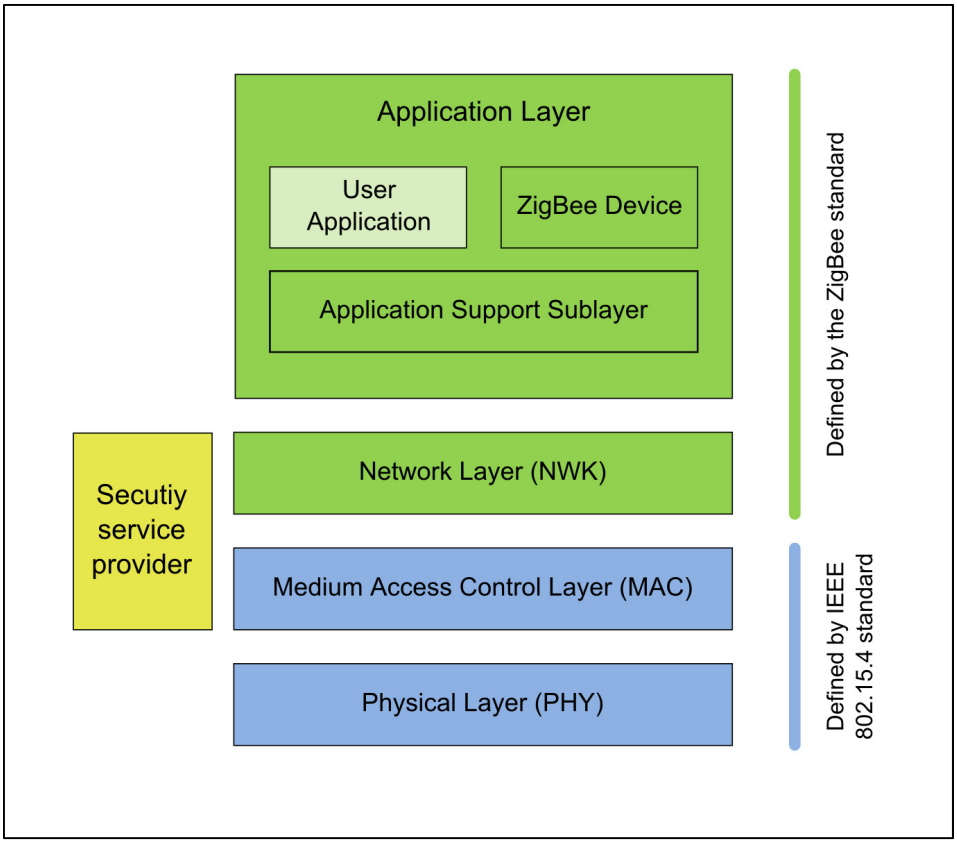


Figure 11 - Zigbee architecture

5.5 WIRELESSHART

WirelessHART is a wireless sensor networking technology designed to add wireless communication to the existing HART devices (Highway Addressable Remote Transducer), based on a specialized standard mostly used in factory and process control.

The *WirelessHART* protocol is capable of providing a wireless mesh topology where each device in the network can act as a router to forward messages from other nodes; this solution leads to an increased reliability of the wireless transmissions, thanks to the redundant communication routes and, at the same time, extends the range of the network without the need of additional infrastructure.

According to the HART Communication Foundation, more than 8000 WirelessHART networks are currently installed in major manufacturing sites around the globe (Allan 2012).

Three main elements are part of a *WirelessHART* network:

- **Wireless field device**
  connected to process or plant equipment, consists of a *WirelessHART* device or an existing HART-enabled device with a *WirelessHART* adapter attached to it.
- **Gateway**
  enables communication between field devices and host applications connected to a high-speed backbone or other existing plant communications network.
- **Network Manager**
  is responsible for configuring and maintaining the network, scheduling communications between devices, managing message routes, and monitoring the network status. The Network Manager can be integrated into the gateway, host application, or process automation controller.

Communications between devices are synchronized with transmissions occurring in pre-scheduled timeslots and channel hopping can be implemented to increase the system's immunity to interference.

The five key components of HART are:

- time-synchronized communication,
- frequency hopping,
- automatic node joining and network formation,
- fully redundant mesh routing,
- secure message transfer.

The *WirelessHART* nodes run the Time Synchronized Mesh Protocol (TSMP) of the standard and can discover neighbor nodes, measure the radio signal strength, acquire synchronization and frequency hopping information, and establish routes and links with the neighbor nodes.

5.6 6LoWPAN

6LoWPAN is an acronym for IPv6 over Low power Wireless Personal Area Networks; it is an open standard developed by the Internet Engineering Task Force (IETF). The 6LoWPAN protocol is raising considerable interest, particularly in relation with smart energy and smart grid applications, as it enables all the capabilities of IPv6 (Internet Protocol version 6) to individual sensor nodes. Internet Protocols (IP) addresses are required to be global and unique for each node of the network; with the advent of IPv6 increasing the availability of IP addresses networking appliances and assets are expected to outnumber the conventional computer hosts.

With the increasing demand for WSN applications the use of IP and especially IPv6 seems unavoidable in order to ensure direct accessibility of each node of a sensor network. The limited power calculation and the storage capabilities of sensor nodes have been a limit with classical IP stacks. 6LoWPAN has been designed to overcome these limitations. This protocol enables all the capabilities of IPv6 on a very constraint node and thus opens the gate to the Internet of Things.

The adaption of the IPv6 protocol to devices with limited characteristics is possible with the compression of the long IPv6 headers to 6 bytes with message routing adapted, for the WSNs, from meshed multi-hop

topology. Moreover, in order to have nodes with limited routing tables, the routing main capabilities are located at the border routers.

Many open source Operative Systems (OS) implementations and stacks are available for the 6LoWPAN standard such as the *TinyOS*, *Contiki*, *FreeRTOS* OSes. However, as stated in (Mazzer and Tourancheau 2009), the existing 6LoWPAN stacks are monolithic software and this does not allow for an easy modification of the networking strategies.

An example of 6LoWPAN implementation is given by the work on the development of a real-time positioning of manufacturing assets using 802.15.4 compliant wireless sensor network (Jaacán and Lastra 2011). The mobility of the assets makes a wired based positioning system insufficient; in this case the usage of a WSN is the optimal solution and the 6LoWPAN allows avoiding the increase of complexity of the system while allowing interoperability as well as reliability among different communication protocols.

5.7 RuBee

RuBee is an emerging IEEE 1902.1 based standard that should overcome the limitations of the actual RFID technology and provide additional features such as an increased read range, compared to passive RFID tags, simple set up and low cost.

The main difference between RuBee and ZigBee or Bluetooth is that RuBee works using magnetic field, whereas the others work with the electric field. This is a very important characteristic because it provides RuBee networks with the ability to work in harsh environment such as near steal or water and around corners, where other technologies are not applicable.

RuBee uses long wavelength transceiver mode under 450 *KHz* and can work with networks of many thousands of devices inside a range of 15 *m*. RuBee tags may be detected even if they are hidden in steel cases, as well as in vehicles through gates using antennas buried in the road.

RuBee is a two-way, on-demand, peer-to-peer network protocol that exchanges short data packets at the rate of 9.6 *Kb/s*. Two types of devices are defined: controllers and responders. The controller queries the responders by starting the communication and responders transmit back the information requested. The devices battery life can extend up to 10 years. RuBee is supported by many companies such as IBM, Motorola, Sony and Panasonic.

6 CONCLUDING REMARKS

Wireless technologies are constantly improving and many different applications are already successfully implemented in different application scenarios. However, some of the actual technologies are still limited to research projects and, despite the noticeable research activities, ad-hoc wireless sensor networks in real world applications are still relatively few. Commercial applications of sensor networks are still uncommon and WSN may still be considered a young technology.

Both closed and open protocols are available for WSNs communication, as energy saving performances requires improved and more efficient routing algorithms and commercial solutions are being designed to overcome open protocols limitations. The existence of different protocols leads to compatibility issues and open solutions are therefore preferable; WSN's that use different proprietary protocols are not able to interact amongst themselves unless through the use of application gateways (with the drawback of increasing design and management complexity).

From the vast number of research works on ad-hoc wireless networks it appears that the technology is ready for practical application, but each solution must be carefully designed and tailored to the specific implementation with preliminary laboratory tests to assess the feasibility of the chosen devices and protocols. Technical specifications of devices are usually referred to results in optimal conditions, whereas the real performances can differ significantly.

The main advantage of wireless sensor network solutions is the possibility to do away with cables and thus gain higher flexibility, especially when considering moving nodes that intermittently access the network. However, sending data wirelessly has some restrictions as wireless communication suffers from interference and does not guarantee wired-level transmission reliability. Moreover, wireless radio waves are damped, absorbed and mirrored by obstacles and therefore the environment may be a significant limit in the implementation of a WSN.

In spite of the aforementioned limits, WSNs offer a unique opportunity for large-area monitoring solutions that were impossible with previous technologies (e.g. in natural environments such as large forests and glaciers). However, when dealing with power resources of sensor nodes, the replaceability of batteries can be a technical obstacle if no efficient energy scavenging technique can provide sufficient energy to power the hardware. For this reason, WSN and energy harvesting techniques must be considered in the design of embedded structural solutions and the sensors; likewise, as any energy loss is critical, computational tasks and wireless communication protocols must be carefully considered (e.g. to avoid over dimensioning the radio capacity, one of the most energy consuming aspects of a sensor node).

Embedded solutions are feasible, and examples have been applied to structural health monitoring of structures or, considering mobility assets, to vehicles within an urban area or ecosystems (fauna tracking). However, the application of WSNs in the scenario of shipping containers pushes the actual technologies to their limits, both in terms of lifetime of energy supplies, network management and main infrastructural integration (i.e. the dispatching of information to the backbone).

7 WORKS CITED

Allan, Roger. "Energy harvesting powers industrial wireless sensor networks." *Electronic Design*, 9 2012.

Anastasi, G., E. Borgia, M. Conti, and E. Gregori. "Wi-Fi in Ad Hoc Mode: A Measurement Study." *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications, 2004. PerCom 2004.* . IEEE, 2004. 145- 154.

Bauza, R., J. Gozalvez, and J. Sanchez-Soriano. "Road Traffic Congestion Detection through Cooperative Vehicle-to-Vehicle Communications." *Local Computer Networks (LCN), 2010 IEEE 35th Conference on.* 2010. 606-612.

Brinkmann, Birgitt. *Operations Systems of Container Terminals: A Compendious Overview.* Vol. Operations Research/Computer Science Interfaces Series 49, in *Handbook of Terminal Planning*, by Birgitt Brinkmann, 25-39. New York: Springer, 2011.

Buratti, C., A. Conti, D. Dardari, and R. Verdone. "An Overview on Wireless Sensor Networks Technology and Evolution." *Sensors*, no. 9 (2009): 6869-6896.

Ceriotti, Matteo, et al. "Monitoring Heritage Buildings with Wireless Sensor Networks: The Torre Aquila Deployment." *Proc. of the 8th ACM/IEEE Int. Conf. on Information Processing in Sensor Networks (IPSN).* 2009.

Doolin, David M., and Nicholas Sitar. "Wireless sensors for wildfire monitoring." Edited by International Society for Optics and Photonics. *Smart Structures and Materials*, 2005: 477-484.

Egan, D. "The emergence of ZigBee in building automation and industrial control." *Computing & Control Engineering Journal* 16, no. 2 (2005): 14-19.

Engel, Jonathan M, Lianhan Zhao, Zhifang Fan, Jack Chen, and Chang Liu. "Smart brick - a low cost, modular wireless sensor for civil structure monitoring." *International Conference on Computing,Communications and Control Technologies (CCCT 2004).* Austin, TX USA, 2004.

Gutiérrez, José A. "On the Use of IEEE Std. 802.15.4 to Enable Wireless Sensor Networks in Building Automation." *International Journal of Wireless Information Networks* 14, no. 4 (2007): 295-301.

Hart, J. K., K Martinez, R Ong, A Riddoch, K.C . Rose, and P Padhy. "A wireless multi-sensor subglacial probe: design and preliminary results." *Journal of Glaciology* 52, no. 178 (2006).

Huang, Yueh-Min, Meng-Yen Hsieh, and Frode Eika Sandnes. "Wireless Sensor Networks and Applications." In *Wireless Sensor Networks and Applications*, edited by S.C. Mukhopadhyay and R.Y.M. Huang, 199-219. Berlin Heidelberg: Springer, 2008.

Jaacán, Martinez, and José LM Lastra. "Application of 6LoWPAN for the Real-Time Positioning of Manufacturing Assets." *Interconnecting Smart Objects with the Internet*, 2011.

Juang, Philo, Hidekazu Oki, Yong Wang, Margaret Martonosi, LiShiuan Peh, and Daniel Rubenstein. "nergy-Efficient Computing for Wildlife Tracking: Design Tradeoffs and Early Experiences with ZebraNet." *ACM Sigplan Notices* 37, no. 10 (2002): 96-107.

Kim, Sukun , et al. "Health Monitoring of Civil Infrastructures Using Wireless Sensor Networks." *IPSN '07: Proceedings of the 6th international conference on Information processing in sensor networks.* ACM Press, 2007. 254-263.

"iTETRIS - A System for the Evaluation of Cooperative Traffic Management Solutions." In *Advanced Microsystems for Automotive Applications 2010*, by Daniel Krajzewicz, et al., edited by Gereon Meyer and Jürgen Valldorf, 399-410. Berlin Heidelberg: Springer , 2010.

Lewis, F. "Wireless Sensor Networks." In *Smart Environments: Technology, Protocols and Applications*, by Wireless Sensor Networks. Wiley, 2004.

Li, Yanjun, Zhi Wang, and Yeqiong Song. "Wireless Sensor Network Design For Wildfire Monitoring." *Intelligent Control and Automation, 2006. WCICA 2006. The Sixth World Congress on.* 2006. 109-113.

Lynch, J. P., et al. "Laboratory and Field Validation of a Wireless Sensing Unit Design for." *Proceedings of US-Korea Workshop on Smart Structural Systems.* Pusan, Korea, 2002.

Ma, Y., M. Richards, M. Ghanem, Y. Guo, and J. & Hassard. "Air pollution monitoring and mining based on sensor grid in London." *Sensors* 8, no. 6 (2008): 3601-3623.

Martinez, Kirk, Jane K. Hart, and Royan Ong. "Environmental Sensor Networks." *Computer* 37, no. 8 (2004): 50-56.

Mazzer, Yannis, and Bernard Tourancheau. "Comparisons of 6LoWPAN Implementations on Wireless Sensor Networks." *Sensor Technologies and Applications, 2009. SENSORCOMM '09. Third International Conference on.* IEEE, 2009. 689-692.

Toumpis, S., and D. Toumpakaris. "Wireless ad hoc networks and related topologies: applications and research challenges." *e & i Elektrotechnik und Informationstechnik* 123, no. 6 (June 2006): 232-241.

Vacca, I., M. Bierlaire, and M. Salani. *Optimization at Container Terminals: Status, Trends and Perspectives.* Tech. Rep. TRANSP-OR 071204, Transport and Mobility Laboratory, Zurich: EPFL, 2007.

Verdone, R., D. Dardari, G. Mazzini, and Conti. *A. Wireless Sensor and Actuator Networks.* London, UK: Elsevier, 2008.

European Commission
EUR 25749 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: **Analysis of current and potential sensor network technologies and their incorporation as embedded structural system**

Authors: Flavio Bono, Graziano Renaldi

Luxembourg: Publications Office of the European Union

2013 – 34 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424

ISBN 978-92-79-28185-3

doi: 10.2788/79382

Abstract

This document provides a brief overview of the actual wireless ad hoc sensor networks technologies and standards available, especially in view of their possible implementation for shipping container protection and monitoring within the framework of the STEC Action aiming at analyzing possible technical solutions to improve the security of the millions of containers moving in and out of Europe. Examples of applications and research projects are reported from the literature to give insights on the possibility of implementation of wireless sensor networks in real world scenarios.

LB-NA-25749-EN-N

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new standards, methods and tools, and sharing and transferring its know-how to the Member States and international community.

Key policy areas include: environment and climate change; energy and transport; agriculture and food security; health and consumer protection; information society and digital agenda; safety and security including nuclear; all supported through a cross-cutting and multi-disciplinary approach.

Publications Office

ISBN 978-92-79-28185-3

9 789279 281853