Wireless Sensor Networks

Paulo Leal
Faculdade de Ciências
Universidade do Porto
Email: up201101503@fc.up.pt

António Carvalho
Faculdade de Ciências
Universidade do Porto
Email: up200801471@fc.up.pt

Inês Maia
Faculdade de Ciências
Universidade do Porto
Email: up201101593@fc.up.pt

***Abstract*—In the recent years, a lot of research has been done concerning Wireless sensor network (WSN) technologies. The development of new protocols, algorithms, and the availability of smarter, cheaper and smaller sensors culminated into real-world applications such as disaster prevention, agriculture monitoring, health tracking, etc. In comparison to the traditional wireless networks, WSNs need to be implemented with different design goals particularly energy efficiency and network reliability. In this paper we intend to give an outline about WSN mentioning: its different types and applications; its topologies and protocols and the adopted standards. Lastly we found that there is still room for improvements in the WSN ecosystem namely efficient battery usage and self-repairing networks.**

I. Introduction

Nowadays everything around us is connected to the internet which provides us with smart houses, smart grids, smart cities, and intelligent transportation - all these systems can be incorporated into a single concept, the Internet of Things (IoT).

One of the most important elements of the IoT is the WSN, which is gradually receiving more attention due to its wide range of potential applications in areas like industry, transportation, science, security, and civil infrastructure. A WSN is a network formed by a large number of sensor nodes that have the purpose of monitoring and collecting data, which, despite several challenges, is a promising technology.

In the section II we give an overview of WSN, its types and applications. We also describe the multiple topologies and its characteristics in section III. Furthermore, we present WSN architecture (section IV), its communication protocols (sections: V,VI,VII), and its standards(section VIII). Lastly we discuss the current research issues and design goals in sectionIX.

II. Wireless Sensor Networks

WSN, also referred to as Wireless Sensor and Actuator Networks (WSAN) are a group of sensors that collect and monitor information about their environment, like multiple detection stations - it works by having its sensor nodes pass the data through the network to a main point (See Fig.1). Sensors gather the environmental conditions, such as temperature, pressure, and humidity, which are of use to a lot of applications such as automated smart homes, traffic, and medical device monitoring.[1].

There are two ways of developing sensor nodes: Ad-hoc, and Preplanned. For large uncovered regions, the best is the Ad-hoc deployment - a large number of nodes in a network deployed in order to perform monitoring and reporting. Consequently, for limited coverage, the preferred way is the pre-planned deployment - a lesser number of nodes implemented in certain locations.

There are some challenges and corresponding requirements that have to be fulfilled in order to be used in a large number of expected applications. For example, sensor nodes have resource constraints, more precisely, limited memory, limited energy, and limited computational capacities - to make up for that, it is important to efficiently use resources; sensor node failures may occur, caused by dynamic network topologies and harsh environment conditions - WSN may have adaptive network operation, algorithms and protocols to deal with those conditions; other challenges like data redundancy, prone to node failures and large scale deployment are also important aspects that require some mechanisms to improve the deployment.

The types of networks used are decided depending on the environment.

A. Terrestrial WSN

In this type of WSN, sensor nodes are capable of communicating data to the base station and are deployed on land both in the Ad-hoc or Preplanned manner.

In order to solve the limited battery power issue, these sensors can have a secondary power source - a battery equipped with solar cells.

The most common applications of this type of WSN are industrial, environmental monitoring and surface.

B. Underground WSN

Consists of sensor nodes deployed underground, in mines or caves, in order to monitor conditions. Given the fact that the communication is done through rocks and water, used equipment must ensure communication reliability, which makes this environment a greater challenge, and more expensive, than the terrestrial type. Sensor battery nodes also have a limited battery power and underground WSNs are not easy to recharge. The most common applications are water , soil, or mineral, agriculture, and military border monitoring.

C. Underwater WSN

Sensors are deployed underwater and use acoustic waves which have a long propagation delay, limited bandwidth and

signal fading. There is also a limited battery, which can not be recharged or replaced, and this involves development of underwater communication and networking techniques. Underwater WSNs have applications like undersea surveillance, disaster prevention and monitoring (seismic and pollution).

D. Multimedia WSN

Consists in storing, processing, and retrieving multimedia events, like video, images or audio. There are sensor nodes equipped with multimedia material (microphones, cameras) connected in a wireless communication. As expected, there are issues such as bandwidth requirements, data processing and compressing techniques, and high energy consumption. Tracking and monitoring are the main uses.

E. Mobile WSN

Mobile WSNs consist of sensor nodes that can be moved and have interaction with the physical environment. The nodes have the ability to self-reconfigure themselves in order to communicate, which bring us advantages such as greater channel capacity and better energy efficiency

Mobile WSN applications are military surveillance, target tracking and monitoring.

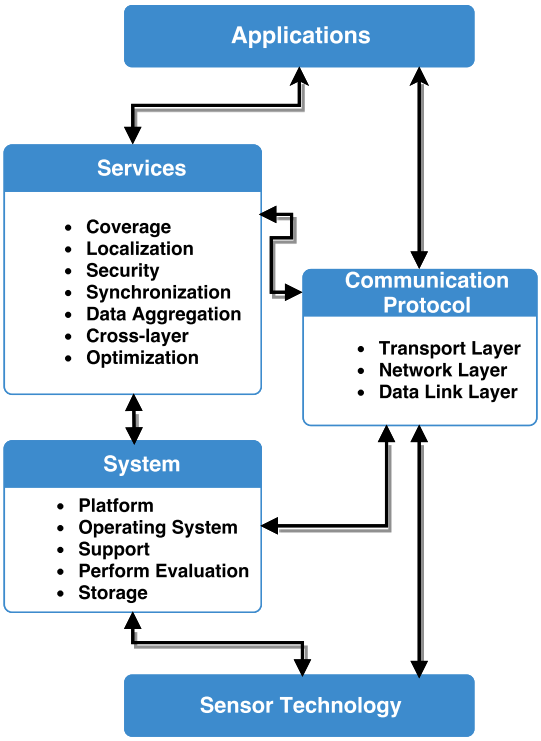

Fig. 1. Wireless Sensor Network overview: components and requirements

III. Topologies

A network topology is the manner in which the several components of the network are arranged. It is, simply put, its topological structure and may be represented in a physically or logically. A physical topology consists of the physical devices, their location and connections. A logical topology indicates the connections at an information level; how data/information flows in the network[2][3].

A. Fully Connected

As more nodes are added there's an exponential grow in the amount of links existing which means that it's of NP-Complexity, thus, for bigger networks, even with great computing power this network configuration isn't viable(Fig.2).

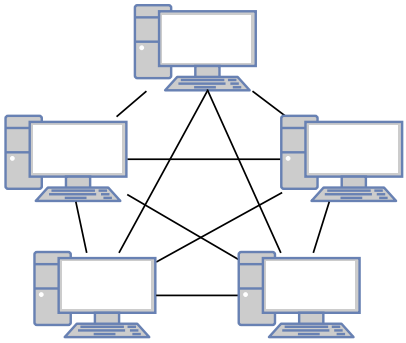

Fig. 2. Fully Connected Topology

B. Mesh

Nodes that belong to this network configuration are usually of identical priorities and information is transmitted between neighbors. The structure of the network doesn't necessarily imply a physical mesh as it only reflects it's topology, which means that this network can be applied in a large range of uses, the majority of them being in larger scale options, eg: Vehicle and Personnel security systems. Although, as referred, there is a sort of equality between nodes some of them can be designated group leaders that perform additional functions; if this group leader happens to become inactive another node can take its place as a new leader(Fig.3).

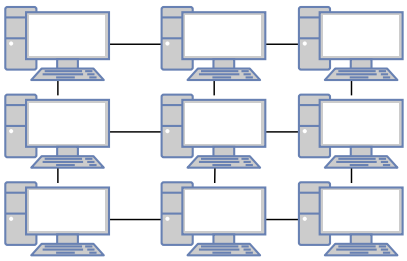

Fig. 3. Mesh Topology

C. Star

This topology has all of its nodes connected to a single hub which requires that the hub has good capabilities in message handling, decision-making, and routing. In the event that communication happens to be disabled only the node that pertains to that link will cease to have a connection to the network, yet, if the hub is destroyed the whole network is lost(Fig.4).

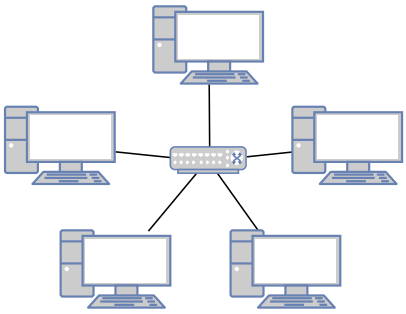

Fig. 4. Star Topology

D. Ring

All members of this topology have the same function and there are no leaders, all information travels in the same direction which means that if a link is cut the whole network is lost.(Fig.5)

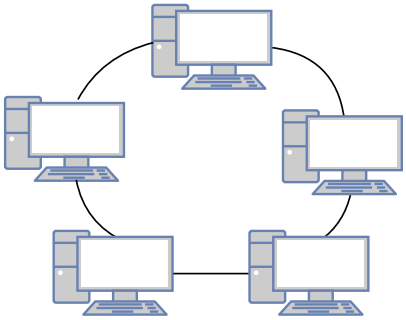

Fig. 5. Ring Topology

1) Self Healing Ring: An ”improvement” to the regular Ring topology, here two rings exist instead of one which make this style of network more tolerant to faults.

E. Bus

Messages are broadcast to all nodes via a central bus, being that each node checks the header for it’s destination and processes, in case of him being the destination, the information within the package. This is different style of network to all others being that it’s passive: nodes only listen for messages instead of transmitting and do not re-transmit any of them(Fig.6).

IV. Architecture

A general model exists, being it the OSI model, and most WSNs follow it. It consists of five layers: Application, Transport, Network, Data Link, and Physical. Three cross layers also exist: Power Management, Mobility Management, and Task Management (see Fig.7); their job is to manage the network and assure a healthy collaboration between sensors in order to maintain a high network efficiency[4].

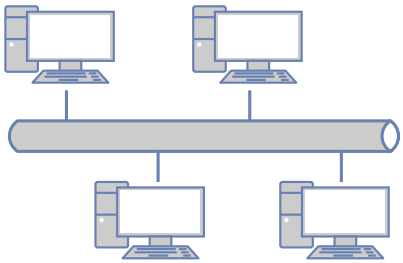

Fig. 6. Bus Topology

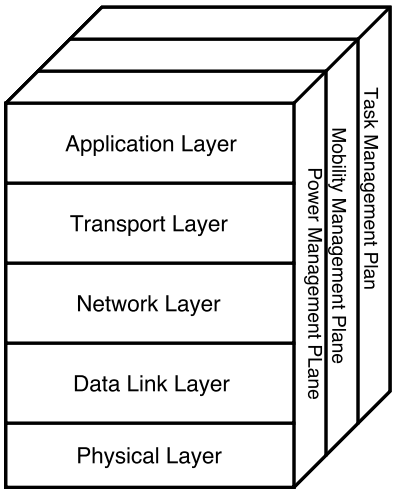

Fig. 7. WSN Architecture

A. Application Layer

Has software that allows a multitude of applications to translate data to an understandable form or obtain information via queries. WSN in several fields can be used as an example: medical, military, or even agriculture fields.

B. Transport Layer

Serves as a mean to provide both reliability and congestion avoidance where a number of protocols are applied as user to server and server to user; loss detection and recovery are different among these protocols. This layer is most needed when access between multiple networks is required. For WSN the suitability of TCP can be questioned as it’s more efficient to provide more reliable hops than it end to end. Usually downstream is considered UDP and a multi-cast transmission and upstream a TCP/UDP mono-cast transmission. Transport protocols are then Packet or Event driven. Packet driven means that all packets that are sent must reach their destination, and Event driven that the event itself must be acknowledged but only one packet has to reach the destination.

C. Network Layer

The definition of both reliant and redundant paths in order of a metric (which may differ from protocol to protocol) is the bare bone idea of routing and the overall goal of this layer. Many routing protocols are available which can be either Flat

TABLE I
COMPARISON BETWEEN OSI AND WSN

OSI Model	Wireless Sensor Network
Application layer	WSN Application
Presentation layer	WSN Middleware
Session layer	-
Transport layer	WSN Transport protocols
Network layer	WSN Routing protocols
Data link layer	WSN MAC protocols and error control
Physical layer	Transceiver

routing or hierarchical routing; they can further be divided as Time driven, Query driven, and Event driven.

As to cover a selected area fully we have to provide redundant sensors for deployment where the redundant ones supply data that is repeated, as well as sensors that send data via multi-hop (per times, flooding). Every sensor forwards its information to its neighbors and they to theirs, etc. As data processing consumes far less power then data transmission and this process provides a large amount or repeated data this is solved by aggregation and fusion being applied to the data. This is in a way the basics of flat routing.

D. Data Link Layer

Guarantees reliability between point to point or point to multipoint connections, also manages multiplexed data streams, data frame detection, MAC, and error controls. Issues between co-channel MAC layers are handled by MAC protocols and problems in the physical layer, multipath fading or shadowing, are solved by Forward Error Correction (FEC) and Automatic Repeat Requests (ARQ).

1) MAC Layer: Controls access policies for the channel, manages schedules, buffers, and error control. For WSN energy efficiency, low delays, high throughput, and reliability need to be considered in a MAC protocol.

E. Physical Layer

Serves as a mean of transmission for concurrent data bits on a physical medium, ie: an interface. Manages frequency generation and selection, signal detection, data encryption, and Modulation.

V. MAC PROTOCOLS(DATA LINK LAYER)

Every Ethernet message has a top section compromised of five sections: Preamble (8 bytes), Destination Address (6 bytes), Source Address (6 bytes), Length of Data field (2 byes), and Other Information (from 0 to 1500 bytes). This is referred to as a header and can be accompanied by the inclusion of a parity bit. In some networks, when they're based on packet routing, messages can be torn into several packets of a predisposed, fixed, length, which are then reassembled when they reach their target destination.[5]

A. Multiple Access Protocols

In a network in which multiple nodes transmit at the same time there's the need for protocols who control the network in order to avoid data collisions and even lost packets. An example of such a scheme would be: if the node receive an acknowledgment it proceeds if not the node waits a random time before re-transmitting the packet; this is known as ALOHA.

B. Frequency Division Access Protocols

Here different nodes have different frequencies and since frequency resources are being divided this implies that the bandwidth available for each node is diminished.

C. Code Division Multiple Access

Each node has its own code which is used to encode the respective nodes messages, this makes the communication and both the receiver and sender more complex.

D. Time Division Multiple Access

In Frequency Division Multiple Access (TDMA) each node has a predetermined amount of time it has for transmission, although this decreases the sweep rate it allows for TDMA to be applied in software (in which all nodes require a synchronized clock).

VI. ROUTING PROTOCOLS(NETWORK LAYER)

In computer networks, routing protocols are crucial to specify how nodes should communicate with each other. Particularly in WSNs, it is hard to find a routing protocol suitable for all applications. In WSNs, routing protocols can be classified into five different categories[6][7]:

1) Location-based: Nodes are addressed by their location information. Energy consumption can be estimated based on the calculated distance between two nodes. Examples: Geographic Adaptive Fidelity (GAF), Geographic and Energy-Aware Routing (GEAR), Span, Trajectory-Based Forwarding (TDF),Bounded Voronoi Forwarding (BVGF), Geographic Random Forwarding (GeRaF), Minimum Energy Communication Network (MECN), Small Minimum-Energy Communication Network (SMECN).
2) Data-centric: Intermediate nodes are used to aggregate data originating from multiple source sensors. This process can provide energy savings because of less transmission required to propagate data. Examples: SPIN, Directed Diffusion, Rumor Routing, Cougar, Energy-Aware Centric Routing.
3) Hierarchical: This category uses clusters formations to perform data aggregation and fusion in order to decrease the number of transmitted messages, thus reducing the energy consumption. Examples: Low-energy adaptive clustering hierarchy(LEACH), PEGASIS, TEEN, APTEEN, HEED.

4) Multipath-based: In multipath routing, each source sensor finds the k shortest paths to the sink and distributes the load between them. Examples: Disjoint Paths, Braided Paths, N-to-1 Multipath Discovery.
5) Quality of Service (QoS)-based: Real-time applications have some critical requirements. In order to satisfy QoS demands (bandwidth, delay constraints), QoS routing becomes an important research issue. Examples: SAR(Sequential Assignment Routing), SPEED, Energy-aware routing.

VII. Transport Protocols(Transport layer)

The very basics of a Transport Protocol (TP) can be described as: data transfer in WSN starts by having the source capture from its sensors and, synchronously, send it to its neighbors, which will then repeat the process until the data has reached the destination. When the data reaches the final node the structure of the protocol can then be divided into three modules: Congestion, Reliability, Priority.[8]

A. Congestion

Congestion is when the rate at which packets are processed is superseded by the rate at which packets are transmitted or when the throughput exceeds the network bandwidth; this causes both drops in packet transmission and unnecessary retransmissions. Siphon, PCCP, CTCP, ESRT, STCP, TRCCIT, RT2, and PHTCCP are just some of the available protocols that can be used to control congestion, each being based on three sub-modules: Congestion Detection, Congestion Notification, and Congestion Avoidance.

B. Reliability

Successful continuous transmission from source to destination of each message is what defines reliability in the transport protocol. TRCCIT, CRRT, RT2, ESRT, ERTP, and GARUDA are some of the protocols that can be used to achieve reliability. The module itself is based on four sub-modules: Reliability Direction (Upstream, Downstream, Bidirectional), Reliability Level (Packet, Event, Destination), Loss and Notification, and Loss Recovery.

C. Priority

In WSN context Priority means to differentiate sensors by having levels of precedence added to different ones. This is important in order to support QoS standards and has been a much more prominent feature in later research. Bandwidth is divided in an effort for fairness by attributing more to sensors that handle critical applications (higher precedence), although it can, for simplicity, be attributed equally among all sensors (even though it is more important to be fair than to maintain simplicity). It stands as Priority Scheduler, being a lone module.

VIII. Standards and Technologies

In recent years, much effort has been made to standardize multiple wireless communication protocols. In comparison to IEEE 802.11(WLAN) and IEEE 802.15(WPAN), IEEE 802.15.4 is specifically designed for low power, low data-rate, and low-cost wireless sensor communication. Bluetooth Low Energy (BLE) is considered an alternative technology for WSN applications requiring both high data rates and short distances. WSN communication protocols operate in the ISM(Industrial, Scientific and Medical) radio band[9].

A. IEEE 802.15.4 standard

IEEE 802.15.4 is a standard for data communication devices operating in Low Rate Wireless Personal Area Networks (LR-WPANs). It targets wireless sensor applications, which need optimal battery usage and do not require high range communication. IEEE 802.15.4 standard specify two types of network nodes: Full-function devices (FFDs) and Reduced-function devices (RFDs). RFDs are nodes with limited processing and memory resources. They act as end-systems and communicate with FFDs. FFDs implement the standard and act as coordinators able to communicate with both FFDs and RFDs. This standard supports two topologies: star - preferred when coverage area is relatively small and low latency is required by the WSN applications - or peer-to-peer - designed to support a large coverage area and complex network formations such as mesh topology.

1) ZigBee: Maintained by ZigBee Alliance, it is a low-cost and low power wireless communication technology used in embedded applications. It provides mesh networking capabilities to the IEEE 802.15.4 applications. Furthermore ZigBee enhances IEEE 802.15.4 by adding security layers and an application framework. The latest ZigBee IP specification also provides support for IPv6-based communication.

2) 6LoWPAN: Defined by IETF to add IPV6 communication on top of IEEE 802.15.4 networks. It enables IPV6 packets communication over low power and low rate IEEE 802.15.4 links.

3) WirelessHART: A standard recommended for industrial applications such as process measurement and control applications. WirelessHART is designed to have reliability, security, energy efficiency, and compatibility with exiting devices. It also enables mesh networking.

4) ISA100.11a: Mainly used in industrial automation, supports network topologies such as star and mesh networking. It has interoperability with existing standards, such as WirelessHART. Its key features are low latency and fast response time.

B. Other technologies

1) IEEE 802.15.4a-ultra wideband: Ultra Wideband (UWB) is a communication technology in which information is transmitted through a series of very short impulses in periodic sequences. The advantages of UWB include its spectral efficiency, high data transmission rates with low power, high precision ranging and location capability, and the

ability to cope with multipath environments. It is not suitable for communication over long distances or measuring critical values because of high peak energy pulses.

2) Bluetooth low energy (BLE): Introduced in Bluetooth 4.0, it enables low-cost BLE compatible devices to operate for a long time (months or years) on coin-cell batteries. Its applications include healthcare, sports and fitness, security, and home entertainment. BLE allows 1Mbps data rates with 200m range.

IX. Research challenges

Wireless sensor networks face additional problems in comparison with regular wireless networks. In order to solve those problems, WSN researchers needed to create new protocols and algorithms to improve the WSN ecosystem. The main issue remains related to resource constraints, namely energy efficiency[9][10]. Other possible design goals related with algorithm and system design are:

1) Heterogeneity - There is a need to develop protocols which can handle multiple applications simultaneously.
2) Cross-layer solutions - The collaboration between all the layers (physical, data-link, network, and transport) can lead to higher energy saving, network performances, and longer network lifetime.
3) QoS models - Instead of using parameters like delay, packet loss, and jitter to specific application QoS, WSNs use parameters such as data accuracy, network sensing coverage, fault tolerance, and network lifetime. An appropriate QoS model should consider parameters like energy-sustainability, timeliness, reliability, security, mobility. and scalability.
4) Cooperation - Cooperative communication is a technique for efficient battery usage and enhanced network performance in WSNs.
5) Deployment - Deploying and managing multiple nodes is still complex. The ability to replace nodes without compromising the whole network is a current research issue.
6) Integration - WSN can act as a stand-alone network or be connected to other networks such as Internet, WiFi or cellular network. There has been a research interest in combining Cognitive Radio technology with WSNs.
7) Security - Focus on cryptography, key management, secure routing, secure data aggregation, and intrusion detection.

X. Conclusion

WSN consist of several sensors that respond to their environment (section II), collecting information through those sensors and propagating it until its destination is reached and consequently processed (section VII). Due to WSNs existing in several different topologies (section III) many distinct applications, from medical to home uses (section II), are possible, and even though several challenges exist regarding this technology (section IX) it continues to prosper as a promising tech which has had a high investment lately. Alternate technologies, such as BLE, are available but often have protocols operating in different radio bands which has WSNs pertain meaning within today's standards (section VIII).

References

[1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[2] F. L. Lewis *et al.*, "Wireless sensor networks," *Smart environments: technologies, protocols, and applications*, pp. 11–46, 2004.

[3] J. S. Wilson, *Sensor technology handbook*. Elsevier, 2004.

[4] A. A. A. Alkhatib and G. S. Baicher, "Wireless sensor network architecture," in *2012 International Conference on Computer Networks and Communication Systems (CNCS 2012)*, 2012.

[5] P. Huang, L. Xiao, S. Soltani, M. W. Mutka, and N. Xi, "The evolution of mac protocols in wireless sensor networks: A survey," *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 1, pp. 101–120, 2013.

[6] D. Goyal and M. R. Tripathy, "Routing protocols in wireless sensor networks: a survey," in *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on*. IEEE, 2012, pp. 474–480.

[7] A. Norouzi, A. H. Zaim *et al.*, "An integrative comparison of energy efficient routing protocols in wireless sensor network," *Wireless Sensor Network*, vol. 4, no. 03, p. 65, 2012.

[8] A. D. Rathnayaka and V. M. Potdar, "Wireless sensor network transport protocol: A critical review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 134–146, 2013.

[9] P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, "Wireless sensor networks: a survey on recent developments and potential synergies," *The Journal of supercomputing*, vol. 68, no. 1, pp. 1–48, 2014.

[10] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *Industrial Electronics, IEEE Transactions on*, vol. 56, no. 10, pp. 4258–4265, 2009.