International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 10 Ver IV || Oct 2018 || PP 54-62

Iot Design To Support Wireless Sensor Networks And Data Transmission

M.Papoutsidakis[1], E.Symeonaki[1], A.Chatzopoulos[1]andD.Piromalis[1]
[1]*Department of Industrial Design and Production Engineering, University of West Attica, Greece*
Corresponding Author: M.Papoutsidakis

Abstract: *The purpose of writing this dissertation is to get acquainted with wireless sensor networks. By Wireless Sensor Network (WSN) we mean a set of scattered autonomous sensors with the main goal of monitoring natural or environmental conditions. First of all, we study the main features of these networks and the categories in which they are divided. Then, we compare them with ad hoc networks. Wireless Sensor Networks have a prominent place in environmental, residential, submarine and military but mainly in health applications. In the field of health, science has taken great strides in order to best serve chronic sufferers.*

Keywords *-Wireless Sensor Network (WSN), Internet of Things (IoT)*

Date of Submission: 17-10-2018 Date of acceptance: 03-11-2018

I. Introduction

Wireless communications is a kind of data communication that is made and the data delivered wirelessly. Generally speaking, it is a broad term that incorporates all processes and forms of connection and communication between two or more devices using a wireless signal through wireless communications technologies and devices.

Wireless communication is the transfer of information between two or more points not connected to an electrical cable.

The most common wireless technologies use the radio. As far as radio waves are concerned, distances may be small, as few measures as television or thousands of meters or even millions of kilometers for radio communications. It includes various types of fixed, mobile and portable applications, including two-way radios, mobile phones, personal digital assistants (PDAs), and wireless networking. Other examples of radio wireless technology applications include GPS units, garage door opening, wireless computer mice, keyboards and headphones, receivers, satellite TV, TV broadcasting and cordless phones.

Although all these communication technologies have different underlying architectures, they all have a physical or wired connection between their respective devices to initiate and perform communication.

A wireless network is any type of computer network that uses wireless data connections to connect network nodes.

Wireless networking is a method by which homes, telecommunication networks and business facilities avoid costly cable entry in a building, or as a connection between different equipment locations. Wireless telecommunication networks are generally implemented and licensed using radio communication. This application takes place at the physical level of the network model OSI.

Data Transmission

Data transmission, digital transmission, or digital communications is the physical transfer of data via a digital bit stream to a point-to-point or point-to-multipoint communication channel. Examples of these channels are copper wires, fiber optics, wireless communication channels, and computer storage media. The data is represented as an electromagnetic signal, such as an electric voltage, radio waves, microwaves and the infrared signal (Gupta, 2006: 29).

While analog transmission is the transmission of a continuously variable analogue signal, digital communications are the transmission of discrete messages. The messages are either represented by a pulse sequence by means of a line code (baseband transmission), or with a limited set of continuously variable waveforms (passband), using a digital modulation method. The configuration and the corresponding demodulation passage, also known as detection, is carried out with modem equipment. According to the most common digital signal definition, both the baseband and transit band signals representing bits are considered as digital transmission, while an alternative definition only considers the baseband signal as digital and digital data transit as a form of conversion digital to analog.

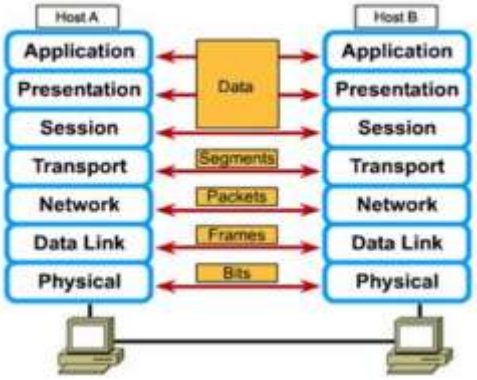

Figure 1: How to Transmit Data, Source: Kizza, 2005: 15

Data transmission is called "simple" if there are only two machines that communicate, or if only a part of the data is sent (Venier, 2012: 31). Otherwise, it is necessary to install multiple transmission lines or share the line between many different communication factors. This exchange is called multiplexing.

A protocol is a common language used by all communication vectors for data exchange. However, his role does not stop there. A protocol also allows:

- The commencement of communications
- Exchange of data
- Error detection
- A normal end of communications

The data transmission principles are also used on storage devices for detecting and correcting errors since 1951 (Tanenbaum, 2003: 25).

Data transmission is used on computer networking equipment such as modems, LAN adapters, repeaters, hubs, microwave links, wireless access points, etc.

In the telecommunications sector, serial transmission is the sequential transfer of the signal elements from a group representing a character or other entity of the data. Digital serial transmissions are bits that are sent through a single cable, frequency, or optical path sequentially. Due to the fact that it requires less signal processing and less chance of errors than parallel transmission, the rate of transfer of each route may be faster. This can be used over longer distances as a control digit or parity bits can be sent along easily.

Asynchronous transmission uses start and stop bits to indicate that the start character bit character ASCII would be transmitted using 10 bits. This method of transmission is used when the data is sent from time to time, as opposed to a solid in current (Halsall, 2005: 36). The start and stop bits should be of opposite polarity. This allows the receiver to recognize when the second packet of information is being sent.

Synchronous transmission does not use start and stop bits, but instead synchronizes transmission speeds both in reception and sending of transmission termination using a terrestrial signal built into each cell. A continuous data stream is then sent between the two nodes. Because there are no start and stop bits, the data transfer rate is faster although more errors occur as the clocks eventually go out of sync and the receiving device will have the wrong time compared to the one agreed in the protocol for sending / receiving data, so some bytes could be destroyed by losing bits. Ways to resolve this issue include re-synchronizing clocks and using control digits to ensure that the byte is interpreted and taken correctly (Comer, 2009: 64).

Wireless Connection

Laptops, smartphones, tablets and many other types of consumer devices support wireless network connections. Wireless connections have become, as is understood, the preferred form of computer networks for many people due to its portability and ease of use.

Connecting two wireless devices directly to each other is a peer-to-peer network format. Peer-to-peer connections allow devices to share resources (files, printer, or an Internet connection). They can be done using the various wireless technologies, Bluetooth and Wi-Fi, which are the most popular options.

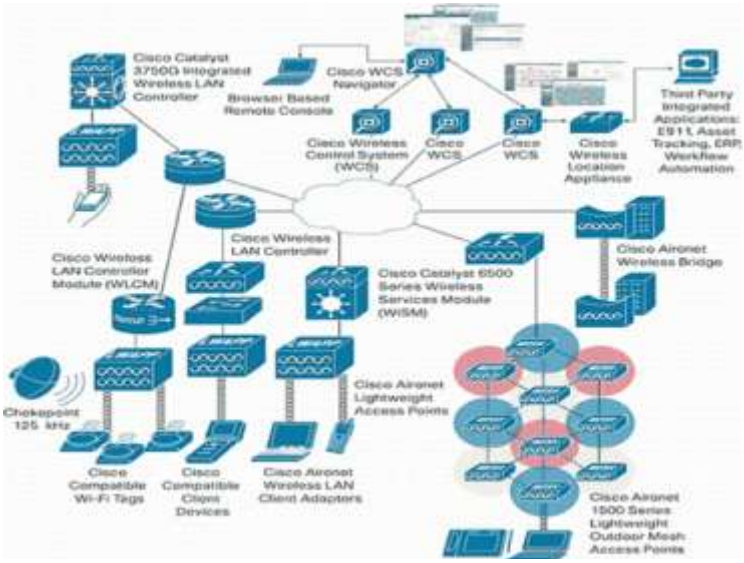

Figure 2: Complex interconnection system according to CISCO, Source: Stallings, 2007: 41

The process of creating peer-to-peer connections via Bluetooth is called matching. Bluetooth pairing often involves connecting a mobile phone to a hands-free headset, but the same procedure can also be used to connect two computers or a computer and a printer. To connect two Bluetooth devices, you first need to ensure that one of them is set to be detectable. Next, you have to find the detectable device on the other device and start the connection by providing a key (code), if necessary. The special menus and button names involved in the configuration vary depending on the type and model of the device.

Peer-to-peer connections over Wi-Fi are also called ad hoc wireless networks. Ad-hoc Wi-Fi supports a wireless local area network that contains two or more local devices.

Many home networks have a wireless broadband Wi-Fi router. Home routers simplify the process of managing wireless connections within a home. As an alternative to creating peer networking among devices, all devices are centrally connected to a router that in turn shares the connection of home Internet and other resources (Karagiannidis, 2009: 99).

To create wireless home network connections through a router, first configure a router's Wi-Fi user interface. This creates a local Wi-Fi network with the selected name and security settings. Then, each wireless user connects to this network.

Wi-Fi hotspots allow people to access the Internet while away from home, ie in the workplace, on a trip or in other public places. Creating a hotspot connection works in a similar way as links to home router connections.

First, it should be determined whether the hotspot is open, ie free of charge for public use or whether it requires registration. Wi-Fi hotspot tracking services maintain databases containing information about publicly accessible hotspots. Then the registration process should be completed if necessary (Preves, 2008: 93). For public hotspots, this may involve emailing, possibly with a payment that may be required. Businesses may need pre-configured software installed on their devices to register.

Next, the name of the hotspot network and the required security settings should be specified. Business system hotspots managers provide this information to employees and visitors while business owners provide it for free to their customers.

Finally, entering a hotspot takes place exactly as it will on a wireless home router. However, you should take all network security measures, especially in public hotspots that are more prone to attack (Kurose, 2013: 135).

1.1 WIRELESS PAN

Wireless Personal Area Networks (WPANs) interconnect devices within a relatively small area that is generally feasible for an individual of the tests. The format of the report should be structured in an understandable way for all the persons involved.

1.2 WIRELESS LAN

A wireless local area network (WLAN) connects two or more devices a short distance using a wireless distribution method, usually providing a connection through an access point for Internet access. The use of

spectrum spreading or OFDM technologies can allow users to move within a coverage area, and still remain connected to the network (Stallings, 2011: 88).

1.3 WIRELESS GRID NETWORKS

A wireless grid is a wireless network that consists of the radio nodes arranged in a grid topology. Each node sends messages on behalf of other nodes. Grid networks "self-healing" automatically re-routing around a node that has lost its power (Peterson & Davie, 2011: 116).

1.4 WIRELESS MAN

Metropolitan area wireless networks are a type of wireless network that connects various wireless local area networks.

1.5 WIRELESS WAN

Wide area wireless networks are wireless networks that cover large areas, such as between neighboring cities, or city and suburban areas. These networks can be used to link business branches or as a public internet access system. Wireless links between access points usually point to point microwave links use 2.4 GHz parabolic plates instead of directional antennas used with smaller networks. A typical system includes base station gates, access points and wireless relay bridging (Mir, 2006: 89). When combined with renewable energy systems, autonomous systems can be built.

1.6 CELLULAR NETWORKS

A cellular network or cellular network is a radio network distributed over areas called cells, and each is served by at least one stationary transceiver, known as a cell site or base station. In a cellular network, each cell typically uses a different set of radio frequencies from all direct cell locations to avoid interference.

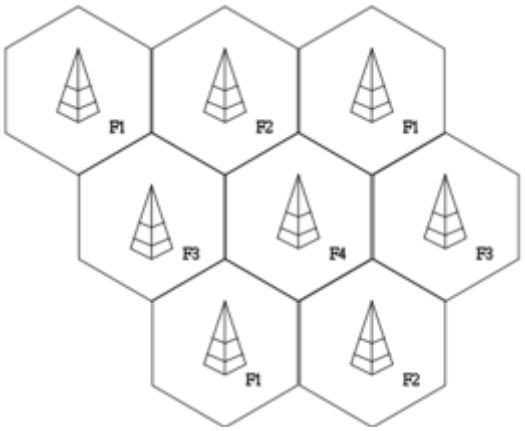

Figure 3: Example of honeycomb connection, Source: Venieris, 2012: 61

When these cells are joined together, they provide radio coverage over a wide geographical area. This allows a large number of portable transceivers such as mobile phones or pagers to communicate with each other and with fixed transceiver phones and anywhere in the network via base stations even if some of the transceivers move through more than one cell during the transmission.

1.7 WI-FI NETWORKS

Wi-Fi essentially comes from the term Wireless Fidelity. Wi-Fi technology was developed in 1991 at NCR Corporation, which was acquired by AT & T in the same year. The first Wi-Fi product was named "WaveLAN" and its data rate was 1 to 2 Mbit / s only (Gupta, 2006: 133).

Now with the continued development of Wi-Fi technology, IEEE 802.11n is growing faster, up to 600 Mbit / s and IEEE 802.11g at speeds of up to 54 Mbit / s.

Many people also use wireless networking, also called WiFi or 802.11 networking, to connect their computers to home, and some cities are trying to use technology to provide free or low-cost Internet access for residents. In the near future, wireless networking can become so widespread that Internet access can be accessed from anywhere at any time without the use of cables.

Wireless Connection

Sensors are sophisticated devices that are often used to detect and respond to electrical or visual signals. A sensor converts the physical parameter (for example: temperature, blood pressure, humidity, speed, etc.) into a signal that can be measured electrically. Let's explain the example of temperature. Mercury in the glass thermometer dilates and shrinks the liquid to convert the measured temperature that can be read by an atom to the calibrated glass tube

A good sensor obeys the following rules:

• It is sensitive to the measured property alone
• It is not sensitive to any other property it may encounter when it is applied
• Does not affect the measured property

Ideal sensors are designed to be linear or linear to a simple mathematical measurement function, typically logarithmic. The output of such a sensor is an analog signal and linearly proportional to the value or simple function of the measured property (Kalavrektis & Katevas, 2012: 78). The sensitivity is then defined as the ratio between the output signal and the measured property. For example, if a sensor measures the temperature and has a voltage output, the sensitivity is a constant with a V / K unit. This sensor is linear because the ratio is constant at all measuring points.

Figure 4: Different types of sensors

In order to process or use in digital equipment an analog signal sensor, it should be converted to a digital signal using an analog to digital converter.

Sensor resolution is the smallest change it can detect in the quantity it counts. Often on a digital screen, the less significant digit will show fluctuations, indicating that changes of this size have just been analyzed. The analysis relates to the accuracy with which the measurement is made. For example, a tunnel scanner (a thin edge near a surface collects a stream of tunnel electrons) can analyze atoms and molecules (Lutrid, 2008: 92).

In this phase we can mention the main categories of sensors and then we can refer to some indicative types.The main categories are:

• Temperature
• Acceleration / Vibration
• Acoustic / Ultrasonic
• Chemists / Gas
• Electrical / Magnetic
• Flow
• Strength / Load / Torque / Stress
• Humidity
• Leakage / Flatness
• Artificial Vision
• Opticians
• Motion / Speed / Cubic
• Position / Presence / Proximity
• Pressure.

Wireless Sensor Networks

The wireless nodes are dispersed in one field. Each of them collects data, processes them, and sends them back to a central location and ends up with the relevant users.

The protocol stack used by the central point and all nodes. It appears to be composed of the following levels: physical, data link, network, transport and implementation, as well as the following management planes of energy, motion and target.

The three latest levels of management help sensory nodes work better together with each other in order to accomplish the purpose for which they were established by consuming as little energy as possible. The remaining levels work according to the OSI standard. Three existing designs using these levels are WINS, smart dust motes, and μAMPS.

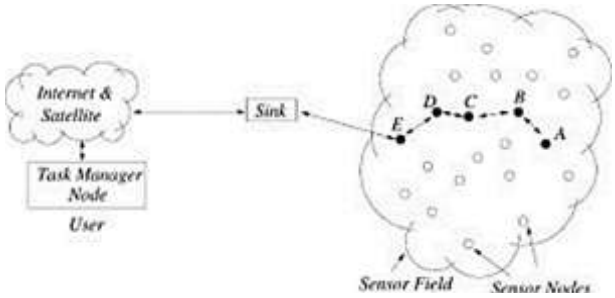

Figure 5: Dispersion of wireless nodes in a monitoring area

1.8 NATURAL LEVEL

The physical level is responsible for frequency selection, carrier creation, signal detection, configuration and encryption of data. A major factor in level design remains the energy consumed in communication. Of course, due to the densely spatial development of the sensors and the multi-hop communication capability, we have significant energy savings and small signal losses, thus enabling less energy to be emitted.

1.9 NATURAL LEVEL

This level is responsible for data multiplexing, data frame detection, media access and error control.The data link level must achieve two purposes: a) construct the network structure in order to have point-to-point communication and give the network a self-organizing capacity; and b) share the transmission medium equally and effectively between of sensory nodes.

1.10NETWORK LEVEL

In order to observe a phenomenon, specific routing protocols are required in order for information from the phenomenon to reach end users. Existing protocols are inadequate and others need to be used. The principles according to which the network layer of a wireless sensor network must be designed are:

- Effective use of energy.
- Sensor networks are usually given-centrally
- Reunion of data is useful when it does not impede the collaborative effort of wireless nodes.
- An ideal sensor network is addressing based on attributes and position knowledge.

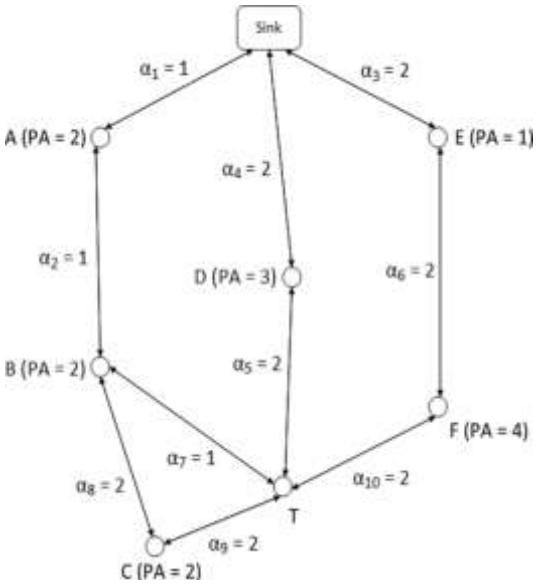

Figure 6: In order to observe a phenomenon, specific routing protocols are required in order for information from the phenomenon to reach end users

1.11 LEVEL OF TRANSMISSION

The level of transport is necessary when the system is to be accessible via the Internet or other external networks. Of course, this is quite common to happen because sensor networks are installed to watch events and transmit information.

At this time, the idea of "networking everywhere" prevails, information that can not be communicated to any interested person on time is considered obsolete and worthless. Therefore, the need to connect a network of wireless sensors to other networks is imperative.

The TCP protocol as it is designed can match the wireless sensor networks, with some change, such as terminating the protocol in the sink nodes, where the TCP connection will be terminated. Beyond that, a special transport protocol can take over the information between the wireless nodes and the sink node.

This differentiation is necessary due to the characteristics of the sensor networks as well as to the different addressing mode based on the information characteristics and not on specific sensors, as mentioned in the previous paragraphs.

1.12 APPLICATION LEVEL

Application level remains an unexplored area for wireless sensor networks, although many areas of application of these networks have been defined and proposed. Three possible levels of application are dealt with in the following paragraphs.

Wireless Sensor Network Applications

Sensor networks can consist of many different types of sensors such as seismic, magnetic low sampling rates, thermal, optical, infrared, acoustic and radar sensors that are capable of monitoring a wide variety of environmental conditions including the following

- Temperature
- Humidity
- Vehicle movement
- Light conditions.
- Pressure.
- Soil structure.
- Noise levels.
- The presence or absence of predetermined object types.
- Mechanical pressure levels in adherent objects and
- Current features such as the speed, direction and size of an object.

1.13 COMMERCIAL APPLICATIONS

Some of the commercial applications are the monitoring of material stress, vertical construction, inventory management, production quality monitoring, intelligent office space, environmental control in office complexes, robot control, and guidance to interactive fabrics, interactive museums, control of industrial processes and automations, monitoring of destruction areas, smart constructions with sensors angry nodes implanted in them, engine diagnostics, transport, installation of industrial instruments, local control actuators, detection and tracking car thieves, identification and detection of moving vehicles.

1.13.1 Home Automation

As technology evolves, intelligent sensing nodes and drive mechanisms can be implanted in devices such as vacuum cleaners, microwave ovens, refrigerators and video. These sensory nodes can interact with one another and with an external network via the Internet or a satellite. They allow end users to manage their home appliances from where they are located either locally or remotely.

1.13.2 Smart Environment

Designing an intelligent environment can have two different perspectives, ie human-centered and techno-centric. For a person-centered approach, a smart environment needs to be tailored to the needs of end-users in terms of entry and exit capabilities. For the techno-centric approach, new hardware technologies, network solutions and intermediate devices need to be developed. A scenario of how sensory nodes can be used to create a smart environment. Sensor nodes can be implanted in furnishings and home appliances and can communicate with each other as well as with the room server. The room server can also communicate with servers from other rooms to learn about the services they can offer e.g. print, scan, and send and receive faxes. These room servers can be integrated with existing implanted devices to become self-organizing, self-adjusting, and adaptable to theoretical models. Another example of a smart environment is the "lab house" at Georgia

Institute of Technology. Calculations and feelings in this environment must be reliable, consistent and transparent.

1.14 HEALTH APPLICATIONS

Some of the applications of sensor networks are: Providing interactive tools for people with disabilities, patient monitoring, diagnosis, drug management in hospitals, monitoring of movements and internal processes of insects and other small animals, remote monitoring of a person's physiological data, and tracking and tracking doctors and patients in a hospital.

1.15 ENVIRONMENTAL APPLICATIONS

Some environmental applications of sensor networks include tracking the movements of birds, small animals and insects, monitoring environmental conditions affecting flora and fauna, irrigation, ordering a series of actions to monitor large-scale land and explore the planet , chemical and biological detection, precision farming, biological and environmental monitoring of the sea, soil and air, monitoring for forest fires, meteorological and geophysical research, flood detection, the detection of complex living organisms in the environment, and the study of infections.

1.16 MILITARY APPLICATIONS

Wireless sensor networks can be an integral part of military command, control, communication, computation, intelligence, tracking, recognition and targeting systems. The features of sensor networks, such as rapid installation, self-organization and fault tolerance, rank them as a promising sensing device for the above systems. As the sensor networks are based on dense spatial installations, the destruction of some nodes by enemy forces does not affect a military operation to such an extent as the destruction of traditional sensors, making use of sensor networks ideal for battlefields. Some of the military applications of sensor networks are to monitor their friendly forces, their equipment and ammunition, track the battlefield, identify enemy forces and territory, target and assess the damage to the battle, and the detection and identification of a Radiobiological Chemical and Nuclear (PBX) threat.

1.17 USE OF INTERNET OF THINGS

Internet Of Things or "Internet of Things" is the upcoming evolution of the Internet of Services that exists today. It is a network not only of computers but also of interconnected objects. These items will contain embedded electronic systems and can be various household appliances, means of transport, telecommunication media, books, cars, and even food. In addition to ensuring the good functioning of these interconnected objects, an attempt will also be made to achieve co-operation between these systems. Each object will use radio frequency identification systems (known as RFID), a kind of sensor, that is. A prerequisite for the success of this new Internet is to make today's Internet safer.

The Internet of Things will be the culmination of the effort to integrate and automate the services provided by embedded systems of all kinds. The internet will become interactive, a huge hierarchically organized "nervous system" that will lead to devices with sensors and actuators that will work together for smart services for health, transportation, distribution and energy consumption, etc. Transport will soon be we have automated driving and organizing systems for more safety and economy. There are a number of innovations in the health sector, from interactive patient follow-up, to tele-surgery and intelligent medicines. The major challenge is the automation of resource management, for example in what is called smart grids, combined and efficient use of alternative forms of energy.

All of these will be some applications that will radically change the current lifestyle in the coming decades. The professor, however, stressed that the state of the Internet still remains very precarious and requires great action and mobilization to enable them to operate safely and effectively. The combination of the Internet, objects and mobile services opens the way to what we call "diffused intelligence." Ubiquitous and unimpeded access to pervasive services, effective resource control, interactivity and synergy to achieve integrated goals. Large corporations are no longer aiming at the individual sale of software or computers, but they study integrated solutions where IT systems are used to optimize natural resource management and develop intelligent services to create a 'smart planet'.

II. Conclusion

The Internet is undoubtedly the greatest discovery in the field of information dissemination since the time of Gutenberg and typography, radically altering the way people communicate and interact. At the heart of the Internet are technologies that have been developed to achieve communication between heterogeneous systems and networks.

In this way, while the Internet originally consisted exclusively of computer networks, other types of

networks such as fixed telephone networks, mobile networks, satellite networks, etc. were integrated into it.

Now the Internet is a network post-network that continues to expand and the respective supporting technologies continue to evolve. In the foreseeable future, the built-in control systems will be added to the Internet, thus realizing the Internet of Things vision.

The main supportive technology for the Internet of Objects is Wireless Sensor Networks (ADS). Wireless Sensor Networks are a special category of distributed and self-organized networks that promise to bridge the gap between the physical world and the digital world.

They consist of small autonomous devices, limited computing capabilities, equipped with digital sensors. These devices collect data and work collaboratively with each other, making routing via multi-step transmissions.

In this way, although each node in the network is characterized by significant limitations (in computing power, energy, wireless communication, etc.), the networks that are synthesized are able to solve difficult computer problems, producing and handling large amounts of information.

This work focused on the analysis of Sensor Network Wiring from all sides - primarily as a Wi-Fi network, with emphasis on the security issues that govern it.

Acknowledgements

Authors would like to acknowledge the University of West Attica postgraduate program of studies "MSc in Industrial Automation" for supporting this research project.

References

[1] Alexopoulos, A., Lagogiannis, G., (2012), Telecommunications and Computer Networks, Publisher: Gialos
[2] Arsenis, S., (2009), Design and implementation of networks - From small office networks to large enterprise networks, Publisher: Klidarithmos
[3] Venieris, I., (2012), Broadband Networks, Publisher: Tziolas
[4] Karagiannidis, G., (2009), Telecommunication Systems, Publisher: Tziolas
[5] Margaritis, S., Stergiou, E., (2006), Local and Urban Networks (LAN-MAN), Publications: New Technologies Publishing
[6] Tanenbaum, A., (2003), Computer Networks, Publisher: Kleidarithmos
[7] Preves, N., (2008), Wireless Computer Networks, Publisher: New Technologies Publishing
[8] Kurose, R., (2013), Computer Networking, 6th Edition, Publisher: Giourdas
[9] Hallberg, B., (2011), Networks, Publisher: Giourdas
[10] Stallings, W., (2011), Computer and Data Communications, Publisher: Tziolas
[11] Ross, J., (2009), Introduction to Wireless Networking, Publisher: Kleidarithmos
[12] Stallings, W., (2007), Wireless communications and networks, Publisher: Tziolas
[13] Forouzan, B., (2005), Protocolo TCP / IP, Publisher: Giourdas
[14] White, C., (2012), Data Communications and Computer Networks: A Business User's Approach, Publisher: Cengage Learning
[15] Peterson, L., Davie, B., (2011), Computer Networks: A Systems Approach, Publisher: Elsevier
[16] Gupta, P., (2006), Data Communications and Computer Networks, Publisher: PHI Learning
[17] Kizza, J., (2005), Computer Network Security, Publisher: Springer
[18] Halsall, F., (2005), Computer Networking and the Internet, Publisher: Pearson Education
[19] Mansfield, K., Antonakos, J., (2009), Computer Networking for LANS to WANS: Hardware, Software and Security, Publisher: Cengage Learning
[20] Stewart, K., Adams, A., Reid, A., Lorenz, J., (2008), Designing and Supporting Computer Networks, Cisco Press
[21] Duck, M., Rea, R., (2003), Data Communications and Computer Networks: For Computer Scientists and Engineers, Publisher: Pearson Education
[22] Shinder, D., (2001), Computer Networking Essentials, Publisher: Cisco Press
[23] Comer, D., (2009), Computer Networks and Internets, Publisher: Prentice Hal
[24] Mir, N., (2006), Computer and Communication Networks, Publisher: Pearson Education
[25] Kalovrert, K., Katevas, N., (2012), Measurement and Control Sensors, Publisher: Tziola
[26] Kalaitzakis, K., Koutroulis, E., (2010), Electrical Measurements and Sensors: Principles of Operation and Design of Electronic Systems of Measurement, Publisher: Kleidarithmos
[27] Loutridis, S., (2008), Measurement and Sensor Technology, Publisher: Ion
[28] Gardner, J., (2000), Micro Sensors: Principles and Applications, Publisher: Tziola
[29] Vetelino, J., Reghu, A., (2010), Introduction to Sensors, Publisher: CRC Press
[30] Fraden, J., (2010), Handbook of Modern Sensors: Physics, Designs, and Applications, Publisher: Springer
[31] Sinclair, I., (2000), Sensors and Transducers, Publisher: Newnes
[32] Regtien, P., (2012), Sensors for Mechatronics, Publisher: Elsevier
[33] Eggins, B., (2008), Chemical Sensors and Biosensors, Publisher: John Wiley & Sons
[34] Janata, J., (2010), Principles of Chemical Sensors, Publisher: Springer
[35] Homola, J., (2006), Surface Plasmon Resonance Based Sensors, Publisher: Springer
[36] Webster, J., (1999), The Measurement, Instrumentation, and Sensors, Publisher: Springer
[37] Yamasaki, H., (1996), Intelligent Sensors, Publisher: Elsevier
[38] Nollet, L., De Gelder, L., (2007), Handbook of Water Analysis, Publisher: CRC Press

M.Papoutsidakis. " Iot Design To Support Wireless Sensor Networks And Data Transmission "International Journal of Engineering Science Invention (IJESI), vol. 07, no. 10, 2018, pp 54-62