ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/299982390

Use of Wireless Sensor Networks in Smart Homes

Chapter · April 2016

DOI: 10.1201/b20085-13

CITATIONS
5

READS
2,415

2 authors:

Oktay Çetinkaya
The University of Sheffield
31 PUBLICATIONS **485** CITATIONS
SEE PROFILE

Ozgur B. Akan
Koc University
259 PUBLICATIONS **9,878** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

MINERVA: Communication Theoretical Foundations of Nervous System Towards Bio-Inspired Nanonetworks and ICT-Inspired Neuro-Treatment View project

MINERVA: Communication Theoretical Foundations of Nervous System Towards Bio-Inspired Nanonetworks and ICT-Inspired Neuro-Treatment View project

All content following this page was uploaded by Oktay Çetinkaya on 25 March 2020.

The user has requested enhancement of the downloaded file.

Use of Wireless Sensor Networks in Smart Homes

Oktay Cetinkaya
Research & Teaching Assistant, Next-generation and Wireless Communications Laboratory, Koc University, Turkey

Prof. Dr. Ozgur Baris Akan
Faculty Member, Director of Next-generation and Wireless Communications Laboratory, Koc University, Turkey

1. Introduction

Wireless sensor networks (WSNs) have come into prominence and started to attract certain environments' interest such as academia, industry and standard developing organizations, recently [1]. With the improvements of advanced sensory structures, flexible and reliable communication technologies, and also offering extended application diversity, WSNs are getting more feasible and preferable day by day. In general, a WSN can be defined as a bunch of spatially distributed autonomous sensors to sense, measure and monitor the physical and environmental parameters of a medium and to carry the gathered information through the network to a coordinator or an access point over wireless links [2], [3]. WSNs provide numerous advantages in terms of cost, flexibility, installation, monitoring, management, and reliable data collection. Typical applications focus on environment, traffic and health-care monitoring, process management, military surveillance, transportation, logistics, disaster assessment -earth sensing, and building automation [2], [3]. WSNs are formed by sensor nodes as getting together in tens to hundreds or even thousands. Each node consists of collaboratively working four units to sense, evaluate and transfer the needed physical parameter of the environment. In a WSN, node deployment varies depending on the application specific. As an example, for a military operation, nodes are organized as uniformly distributed by dropping randomly from an aircraft. However, when a particular measurement is needed to gather from a specific area similar to home automation applications; nodes are placed as fixed in well planned points which called as regular deployment. For a tracking system, such as logistics transportations, mobile sensor nodes are utilized to compensate the negative effects of deployment oriented problems.

Since the existing power plants and systems fail to satisfy the energy demand and scarcely keep up with the constantly improving technology nowadays, planning and management of energy have undoubtedly

become rather important. To maintain the energy need of existing systems, researches are aimed to improve the usage and savings of available resources and power plants, more effectively. Smart grid, an integrated infrastructure of electrical grid, is one the best possible candidate to use energy in an efficient way to overcome the existing utilization induced problems by providing enhancements in production, transmission and distribution of the electricity. Smart grid can be also described as a modernized communication system between supplier and consumer which is built by integrated circuits, smart meters, controlling units and monitoring systems embedded to current power grids in order to track and update the grid data by providing more sustainable, reliable and qualified transmission, and advanced user privacy. In lower levels, smart cities and smart homes take place to sustain the operations of smart grids as extensively.

Information and communication technologies are utilized by smart cities in order to analyze and bring together the vital information of core systems in running cities. A smart city can also respond logically to a variety of needs such as environment protection, public safety and city services, daily livelihood, industrial and commercial activities [4].

A home and/or any quasi-residential area can be referred as the simplest element of a smart grid due to being the last chain on the transmission line. A smart home is a dwelling of ubiquitous or pervasive computing with automated and controlled components. There are several synonyms used for referring a smart home, i.e., intelligent or adaptive home, home automation, and smart or aware house [5]. To illustrate, smart systems can be assumed as a triangular where the smart homes lie down at the lowest level to construct the base, the smart cities place at middleware between smart homes and grids, and the smart grids complete the triangular shape by filling the top corner.

Smart systems require an exchange and transmission of control and sensor information between all components, systems, and the related peripheral units. To enable that, a network of collaboratively working devices should be utilized. Even if it is possible to constitute this network as wired, wireless technologies have been mostly preferred to satisfy today's needs. To measure, monitor and control the environment, sensing and actuation equipped gadgets, i.e., nodes, are deployed in the dwellings as fixed or mobile those communicate over a wireless protocol and compose of the network with the integration of other devices. From this point, it is obvious to say that, smart homes and WSNs are interdependent systems to regulate the energy utilization, measure the physical environmental conditions, control the usage of electrical appliances and resources, and monitor a subject's movements, motions and vital signs.

This chapter surveys existing studies and research opportunities of wireless sensor networks in smart home applications from the perspective of node and network structures, routing and communication technologies, and privacy considerations. We examine the state-of-the art approaches related to energy and communication constraints, and the requirements of wireless home sensor network technologies. We clearly indicate the emerging and promising technologies for the future homes and finalize this part of the book with concluding remarks.

2. Smart Home Scenario

As it is introduced, smart homes and/or home automation systems are one of the first application fields of developing wireless sensor networking technologies. These networks provide easiness and flexibility to users in terms of monitoring, managing and control of the appliances, environmental parameters and previously arranged scenarios. Small battery powered embedded devices which have low power radio frequency (RF) transceivers, low computation capable processors, and compact designed sensing circuitries, are typical components of WSNs in a severely constrained form. RF communication enables adjustable device movement -removal or addition in the network and lower installation expenses due to not requiring any extra wiring unlike the wired counterparts. As the sensing parts are the entities where the required physical parameters gathered, the processor is in charge of evaluating this received information and managing both the system and communication duties. To provide proper system working, every component sustains their operation in an efficient manner. When the overall efficiency is concerned, each part of system should work correspondingly which necessitates the construction of homes as 'smart', and a home requires to equip with exactly three things to turn into smart, namely internal network, intelligent control and automation system [5]. Since the smart home networking is utilized over wireless links and corresponding devices, intelligent control is handled by advanced gateways like smart meters. In addition to that, the automation part refers to internal and external system and service connections. Smart home applications are generally focused on comfort, healthcare and security operations where some WSNs enabled use cases and corresponding examples are given below [1], [5], and [6].

Lighting control: Lighting management which refers to switch or dimmer a light from any user outlet placed on the walls, decreases the necessity of new wired connections while providing both ease of use and flexibility. Remote control option is also available for activation of the lights via wired or wireless systems. Moreover, due to the luminance sensors' ability to detect people presence in an inadequately illuminated environment, lights can be turned on or off automatically without the influence of human beings.

Remote control: Infrared (IR) technology was used as a form of wireless communication in household appliance management. Nevertheless, short distanced coverage and line-of-sight necessity has resulted in the development of radio frequency (RF) operative communication protocols. There are several related technologies that enable remote control of connected devices over wireless links.

Energy management: As the sensors are able to collect and process the parameters of temperature, humidity, light and presence, and correspondingly control the utilization of window shades, doors, heating, ventilating, and air conditioning (HVAC) systems, energy usage is directly linked to these gadgets. Power metering and managing units, i.e., smart plugs, can be used in smart home applications for demand

responsive regulations, energy consumption monitoring, and prevention of stand-by derived redundant energy usage by informing user or any other related institutions [7].

Remote care: In-home medical systems can provide aids to patients, disabled and/or elderly citizens. In this matter, various body and health related parameters such as blood pressure, hormone and/or sugar level, body temperature or heart rate values can be reported by wireless sensors for diagnosis and decision making procedures. In any circumstance where the sensors inform of an abnormal value, alarms can be triggered instantly to call for help from hospitals and/or health centers.

Security and safety: High level security systems may include several sensors, such as glass brake, motion, presence and smoke, to identify the potential risks and control of trigger mechanisms for proper action management. There are such systems which directly connect with fire departments, police stations and/or private security services.

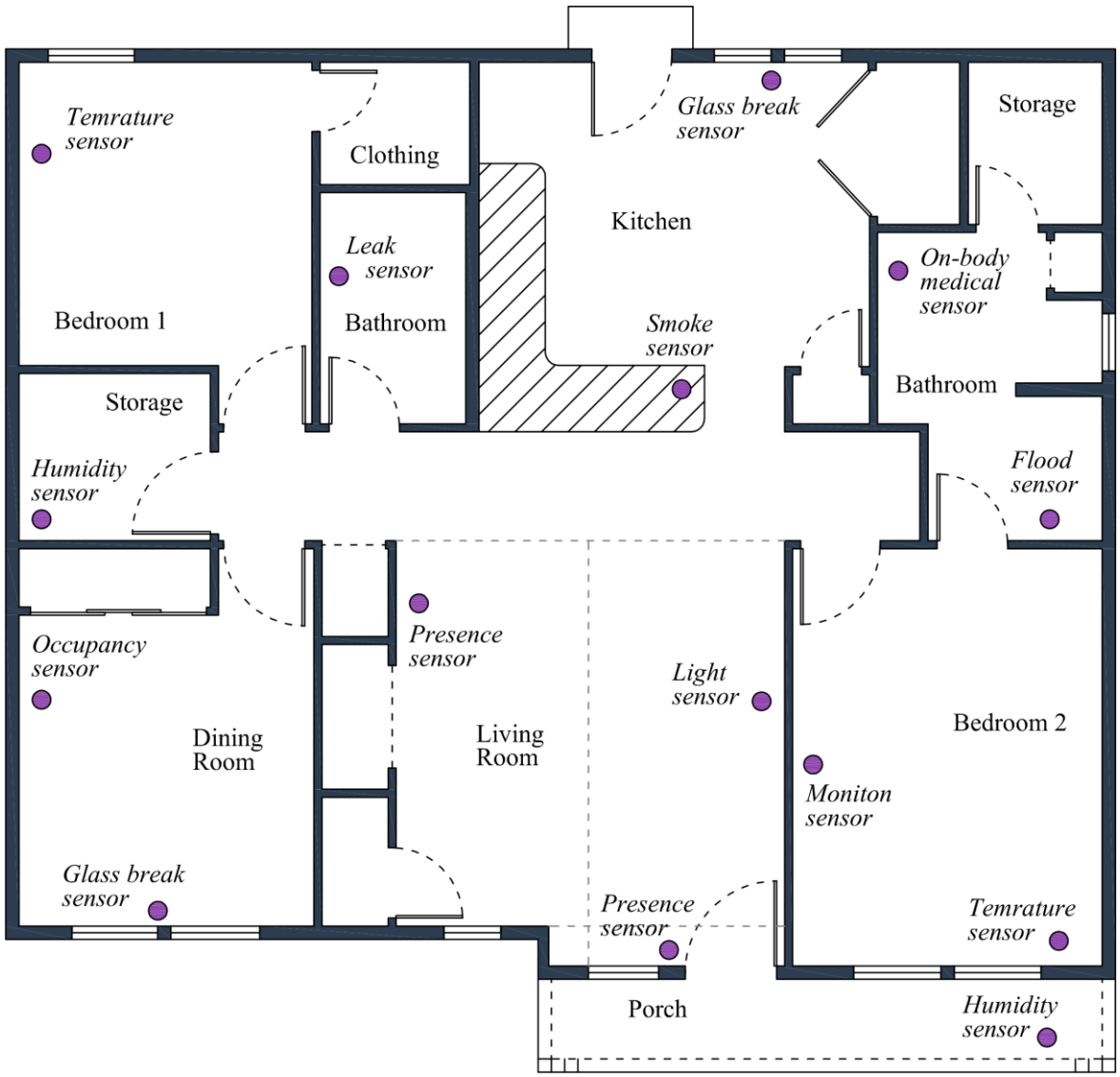

Fig. 1. An illustrative example of a WSN-enabled Smart Home -node types and deployment

3. Sensor Networks

3.1. Node Structure

As its name suggests, sensor nodes are the main constituents of WSNs. They come together to compose a network where the communication and management tasks are handled over a wireless medium. A typical wireless sensor node comprises of four main systems and/or components as shown in Figure 2, and these can be classified as sensing, processing, communication and energizing units [8]. In certain cases like when the processor does not contain any internal memory, sensor needs to be equipped with an external storage which changes the total number of systems as five. A sensor node may include multiple sensors and/or actuators depending on application, and can communicate over wired, wireless or combination of these systems. A sensor node stores and executes the communication protocols as well as data processing algorithms. As the received data could be directly transferred to the upper level components, it is also possible to evaluate them with in network processing mechanisms [3]. All these features vary according to the application needs and requirements with certain tradeoffs. As the total number of the connected devices varies between hundreds, some nodes need to be organized as coordinator to manage the data flow and conduct the assigned tasks in the network. For the small indoor environments like homes, buildings, offices, and/or subway stations, sensor nodes are purposed for well-defined tasks to probe the area, and inform the user itself or any other authenticated people. So, a wise deployment becomes crucial to increase the reliable data gathering. Typically, the process starts with the measurement of the environmental parameters. Then, these analog inputs are converted into digital bits by an analog-to-digital converter (ADC). The received useful and more comprehensible data are evaluated by the processor for the further transactions. As the processor can store the output in a memory as temporarily while waiting the other related measurements for the evaluation before sending them to their destination over the communication device, the data could be stored as permanently for the future usage. All the operations conducted on a sensor node are managed and pursued by the processor with the energy provided from power supply. Considering the certain constraints, all the units of a sensor node should work collaboratively to sustain the operation as long as possible. As a result of that, design efforts are focused on how to build a more robust, efficient and flexible node to increase the overall system reliability [8], [9].

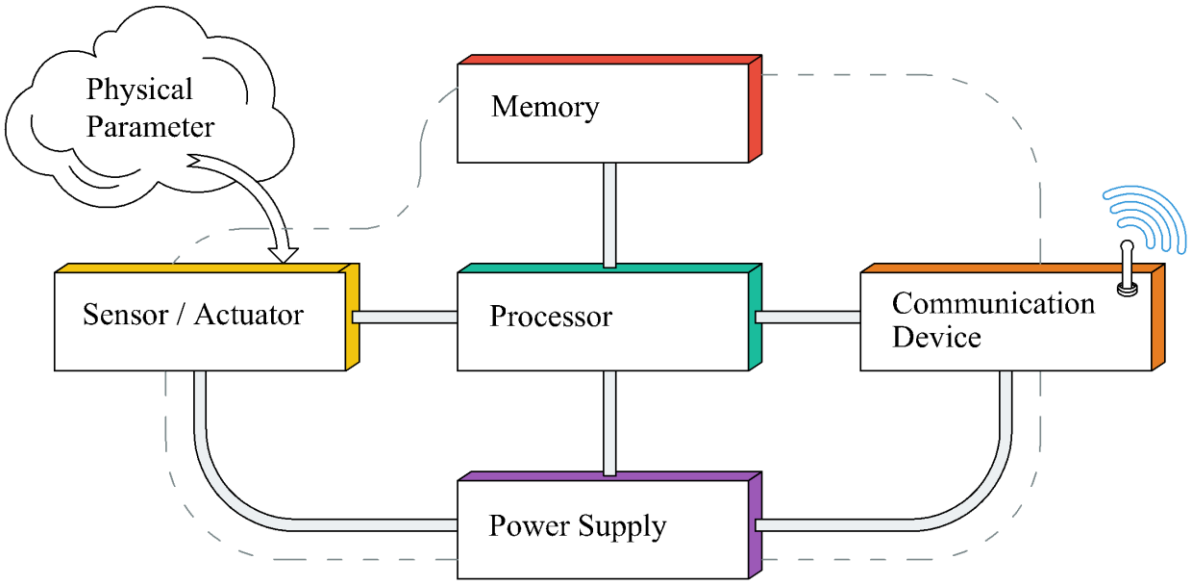

Fig. 2. Typical schematic of a sensor node

3.1.1. Sensing

To observe and control the physical parameters of the environment, sensors and cognate devices - actuators are utilized. Sensing circuitries can be categorized into three groups as passive, omnidirectional; passive, narrow-beam; and active sensors [2]. Omnidirectional sensors do not manipulate the environment during the measurement, and the information is gathered regardless of the direction. They operate with tiny batteries to amplify the generated analog signals. Light, temperature, and humidity levels or any other related physical condition is sensed with this type of sensory circuits. The notion of direction is well defined in passive narrow-beam sensors. The sensor interacts with a previously stated particular area to obtain the needed information. Camera is the simplest example to narrow-beam sensors. Active sensors continuously probe the environment where the measurement occurs. This type of sensors require more energy in contrast with other sensor classes, therefore they need to be energized with external sources in some cases. Sonar sensors and/or radars can be counted as the members of this group. As may be noticed from the definitions, passive sensors best fit to home automation applications. For an indoor environment commonly lux -for the level of light, humidity, temperature, motion -for occupancy and/or presence, glass break, dry contact -for flood and/or leak detection, open/close, smoke or gas, and passive infrared (PIR) sensors are deployed [9]. ADC is responsible for the conversion of the analog signals into the digital equivalents through two steps, namely quantization and sampling. After this process, any information representing a physical parameter related to environment becomes more logical and perceptible by the rest of the node which will be conveyed to the processing part.

3.1.2. Processing

When the processor is considered, there are a variety of options to implement. Microcontrollers, Digital Signal Processors (DSPs), Application Specific Integrated Circuits (ASICs), and Field Programmable Gate Arrays (FPGAs) can be counted as the best known types of it [3]. A processor is basically responsible for executing the node, performing tasks, collecting and processing data, and deciding where and when to send these gathered or generated information. It should be general purposed, flexible to interconnect different systems, devices and peripherals, easily programmable and low power consumptive. The processing unit of the sensor node includes a nonvolatile and an active-temporary memory to store the program instructions and sensed data, respectively, a processing chip, and an internal clock to synchronization and timing operations. Microcontrollers or microcontroller units (MCUs) are frequently preferred for processing, computing and managing duties of sensor nodes when the design goal is focused to achieve flexibility. Besides being compact -constructed, low cost and low power consumptive, debugging and programming easiness as a result of using high-level programming languages make MCUs more preferable. However; when the application requires more powerful and cost and/or energy efficient capabilities, custom made processors like FPGAs and DSPs become more likely to implement. Texas Instruments' MSP430 and Atmel's Atmega series are the well-known types of the microcontrollers.

As the name suggests, DSPs are used for processing discrete signals with the help of digital filters to minimize the negative sides of hardware and/or circuitry oriented noises and modify the spectral characteristics of signals. As mentioned before, the analog data gathered by sensory measurements from the environment are converted into digital signals with the help of ADCs and transferred to the DSP for evaluation. After processing, the meaningful information can be transmitted to another node, an access point (AP) or directly to the coordinator/supervisor over a communication module. The simple and easily implementable structure of control and flow components like adders and multipliers make DSPs more applicable for this type of constituent required applications, and also with the addition of specific algorithms, DSPs become the most suitable candidate for signal processing required applications. However many benefits DSPs possess, there are some drawbacks as well. Being relatively expensive, having inflexible structure, and ongoing deployment complications both restrict the capabilities and so decrease the number of possible applications of DSPs.

ASICs are customized for specific tasks and applications in general. Rather than manage the whole circuit, they work as a complement of mentioned processors to handle low level duties. Being small, having higher bandwidths, performing much better and consuming low power can be denoted as the main good benefits of ASICs. The only drawback they hold is having relatively higher production costs as a corollary of being the final product of a complex design process.

FPGAs perform better in terms of programmability. This flexible and relatively complex-constructed hardware class has higher bandwidths than DSPs, is faster than both microcontrollers and again DSPs -in general, and able to support parallel programming. Besides these good specifications, costly and complex structure of it restricts the application suitability.

All in all, microcontrollers stand as the best candidates to meet the requirements of wireless indoor networking applications as being low cost, low power consumptive and flexible, thus they mostly preferred in home energy management, controlling, and monitoring operations.

3.1.3. Communication

Sensed, processed and evaluated data are sent or received by communication devices and/or modules. Time and energy effective transmission of the information between these devices and linked subsystems is getting crucial; especially for the limited capable sensor node derived tiny gadgets and the huge networks formed by themselves. There are various communication types and corresponding mediums to transfer the information, such as electromagnetic propagation -at radio frequencies (RF), optical, ultrasound and so on. Optical medium needs line-of-sight (LoS) for communication and tend to be affected by weather conditions. Small amount of energy is enough for both generation and detection of the light and sending it through the kilometers with high speeds. Ultrasound signals are preferred when a long distanced coverage area is needed to be handled with consuming low power where RF and optical systems are not applicable. As might be expected from this definition, it suits best for the underwater communication. Electromagnetic radiation at radio frequencies serves the best service to employ a sensor network for indoor environments. RF provides high data rate and long distance communication in non-line-of-sight (n-LoS). There are four possible operational states for the RF transceivers decided and managed by the protocol stack, namely transmit, receive, idle and sleep which are diversified with respect to energy consumption, active parts and operation requirements. When a transceiver is put into the transmit state, the antenna continuously radiates energy, the transmitting circuitry becomes active and the total power consumption fluctuates in the order of microwatts. In receive state; only the receiving part is activated to collect information from other nodes or transmitters, and the level of power consumption is close to transmit state. For the idle mode, the transceiver is ready to receive; however, not willing to do something. Although some parts of receive circuitry are deactivated, transceiver consumes considerable amount of power. In sleep mode, significant parts of the transceiver are switched off, and as an expected result of that, it is not able to receive something immediately. Power consumption is limited with milliwats for this state. To leave the sleep mode, recovery time and startup energy terms become sufficient [2]. In addition to being time and energy costly operation, the major problem for the state switching stands as the tradeoff between energy consumption and packet transmission

reliability. Interface, channel capacity, supported frequency band, communication range and data rates can be denoted as the main evaluative capabilities for the RF transceivers.

3.1.4. Powering

The main idea of node powering is providing as much energy as possible by using tiny batteries that satisfies the minimal needs to operate the node with least cost and recharge time, smallest volume and weight, maximum longevity and robustness. However, node sizes restrict both the capabilities and the design goals of WSNs harshly, and energy becomes a scarce resource as a direct result of that. Wireless sensor nodes are so tiny to accommodate high-capacity power supplies considering the complexity of the tasks they carry out. Being small sized is also a constraining factor for the deployment of renewable energy and recharging mechanisms. Therefore, provided batteries have to durable, and stand as long as possible to prevent the possible failures. In parallel to that, sensory nodes have to sustain their operation in an energy efficient manner, because replacing and/or recharging the batteries may or may not be possible for all the time [2]. When considering the requirements of an energy supply, under load capacity, self-discharge time, voltage stability, shelf life and recharging efficiency terms take the attention. A source should be adequate to meet these requirements, and there are two practical energy suppliers for a wireless sensor node, referred as primary and secondary batteries. Primary ones are generally known as non-rechargeable, while the secondary equivalents are equipped with this capability. However, it only makes sense in combination with some form of energy harvesting operations. Benefitting from the freely available resources of the environment to tray the batteries becomes more logical, feasible and applicable in parallel to ongoing developments in advanced systems and material science. Scavenging energy is a good way to enable node's sustainability for long periods. Light with solar cells, vibration, noise, temperature gradient, and pressure with piezo-electric materials are among the best known types of converting ambient dynamics into energy sources.

In addition to energy harvesting, some power management operations may be applied for obtaining the longevity by increasing the efficiency of energy usage as discussed previously. To illustrate, it is not essential to operate the sensors all the time as fully functional if there is nothing to do. In these cases, the node can be switched to the power safe mode in order to prevent the redundant energy consumption. However, at this point a problem comes up with the question of when and how to wake up and turn back to active mode again. That results in a tradeoff between the energy efficiency and quality of service (QoS). To manage the power usage, some operation modes such as; active, idle and sleep for the instruction execution, turn on/off for both data transmission and sampling are implemented to the energy consumptive parts of the sensor nodes. But, as it is known, saved energy should be bigger than the overhead to handle the power

management, when the operation performance is also acceptable enough. Instead of sending and carrying every sensed data through the network, evaluating the same type of information about a particular parameter then conveying the gathered final one to the destination can help to reduce the energy consumption. That operation is called as in network processing which based on the idea of transmitting is much more costly than the evaluation.

3.2. Networking

3.2.1. Networking Types, Topologies, and Components

A wireless sensor network is formed by the combination of numerous nodes. These units are able to undertake there different tasks during the operation, and can be accordingly categorized as gateways, endpoints and routers [3]. In other words, there are three types of devices for a typical WSN, namely source, sink and relay. Source nodes are the entities where the sensing and data collection operations are carried out. The needed information regarding to a physical parameter of the environment is firstly sensed and then transferred by these types of devices. A source node is not sufficiently measure only one kind of a metric, it can be equipped with multiple sensors to sense several parameters from the related area depending on the application. For conveying the data to the required place or device, relay nodes are utilized. These nodes are responsible for the transportation of the useful information through the network till it reaches to its destination. Sink nodes are the entities where the gathered data is actually needed and used. Actuators are the specialized sinks for the particular tasks. The sinks can be formed by three different modes. A sink may belong and connect to the network directly; it may be an external entity, but still connected to the WSN; or may be a member of another external network; however, somehow connected to the WSN over a gateway.

These mentioned device classes come together and compose the network in different topologies, namely star, mesh, and cluster/tree [10], where the typical distribution of each structure can be shown in Figure 3. In star topology, each node is directly connected to the coordinator. Even though this connection serves a simple communication, it restricts the overall achievable network range. To overcome this problem, the topology of tree, i.e., cluster, can be utilized. For this architecture, each node maintains a single communication path to the coordinator similar to star topology; however, it uses the other nodes as relay to form this path. The common drawback of this topology is possible connection losses when a relay node expires or shuts down. To handle this shortcoming, mesh structures are constructed. For the mesh topology, the nodes have different paths to connect the coordinator which enables rerouting of the data in case of communication failures. This attempt helps to extend the lifetime and increase the robustness of network simultaneously as being quite reliable; however, it suffers from the increasing level of in network latency as a direct result of multi-hopping caused by the data during the travel to destination.

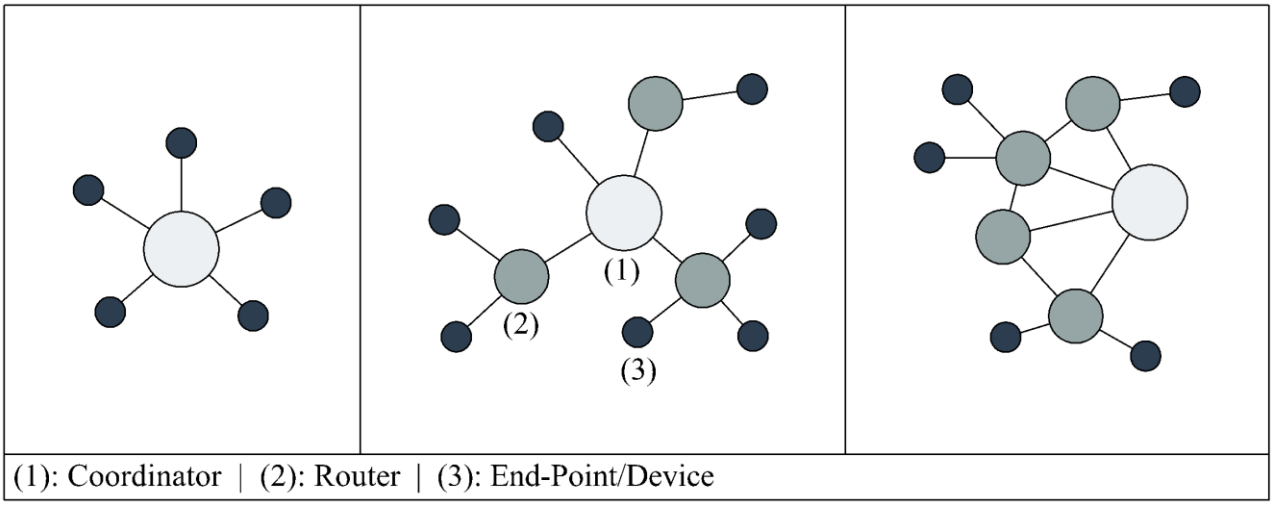

Fig. 3. Typical device connections of Star, Tree and Mesh topologies, respectively

For an indoor environment, all these mentioned topologies are applicable depending on the area where needs to be covered, application requirements and node specifications. In addition to these wireless networking structures, wired system can be also used to constitute a sensor network especially in indoor environments like homes, offices, and buildings. To explore these areas, sensing and actuation capable gadgets, i.e., nodes, are deployed as fixed or semi-mobile that connected to each other with cables, wires, and/or derivatives of these forms to communicate over a protocol, and compose of a network with the integration of other sub-devices. Network topologies are similar in some respects to its wireless counterparts. Mostly, peer-to-peer (P2P), line and/or bus topologies are utilized for data flow in wired networks. X10, Universal Power-line Bus (UPB), KNX and INSTEON technologies can be referred as the typical examples to these systems. A more illustrative comparison is detailed in upcoming sections.

3.2.2. Communication Protocols for WSNs in Smart Homes

There are several standardization bodies in the field of WSNs. With regard to this, communication protocols operated in smart homes are developed in huge numbers as wired, wireless or the combination of these systems. As the IEEE focuses on the physical (PHY) and medium access control (MAC) layer definitions, interest groups, alliances or more specifically, Internet Engineering Task Force (IETF) derived institutions try to develop higher level technologies. As a result of that, there exists several communication opportunities which collaboratively driven by the different industrial consortiums. The PHY and MAC layer parameters, characteristic specifications, and both advantages and disadvantages of the related existing wired and wireless communication technologies are discussed below, and comparatively scrutinized in Table I and Table II.

3.2.2.1. Wired Technologies

3.2.2.1.1. X10

X10 can be accepted as the initial general purpose communication and networking standard for home management and controlling. Although it launched as power line (PL)-based firstly, it has been evolved to a hybrid technology through time with the addition of an RF protocol. As the X10-PL operates in 120 kHz; the carrier frequency of supportive RF protocol varies between 310 to 433 MHz depending on the region that actualizes the connectivity of wireless appliances or components to the control system. Besides the RF extension, some INSTEON-based wireless gateways are also applicable to the existing X10 systems compatibly which increase the number of possible scenarios and range of applications [5].

The communication of X10 technology can be detailed as follows; data are transmitted through the AC power line as a series of 1 ms bursts of 120 kHz when the each half-wave reached at the zero point of 50/60Hz sine signal. A burst indicates logic 0 if it is absent, or inversely, in the case of presence it signifies logic 1. A standard transmission means 44 bits message spreading over 22 cycles of 50/60Hz waveform. 9 data bits which are carried in complimentary, follows a 4 bits 1110 initial pattern in this design. The remaining 22-bit pattern is then sent again with the second half of the command [12].

Communicating over existing wires makes X10 easily implementable and cost effective. However, there also exist some drawbacks which limit X10 employability, such as being relatively slower -data rate can reach up to 20 bit/s, limited function diversity, wiring complexity, incompatibility, absence of encryption, inevitable noises, interferences, command losses and so on [17].

3.2.2.1.2. UPB

Universal Power-line Bus (UPB) is a home automation protocol for communication among devices which uses AC power line as the medium [13]. Although it takes its basis from X10, UPB uses higher voltage and stronger signals to communicate, also has an improved data rate and considerable reliability in comparison with its ancestor. As not requiring extra wiring, hardware, and power supply makes UPB appealing, depending only on an embedded wired system restricts both operation area and application range inevitably as a result of non-upgradable and inflexible structure.

The communication method of UPB consists of transmitting digitally encoded information over the electrical power line as a series of precisely timed electrical pulses called as UPB Pulses that are superimposed on top of the normal AC power waveform.

Regarding the long distanced communication, UPB is less responsive to AC line noises and signal reductions. Data rate is four times faster than its ancestor -X10, and by the peer-to-peer connections a UPB network can support nearly 64000 devices in operation. Similar to X10 technology, UPB suffers from the security issues as a result of being not containing data encryption mechanisms [14].

Protocol / Feature	*X10*	*UPB*	*KNX*	*INSTEON*
Operating Frequency	120 kHz; 310-433.92 MHz	4-40 kHz	110/132 kHz; 868.3 MHz	131.65 kHz; 868-924 Mhz
Maximum Data Rate	20-60 bit/s; 9.6 kbit/s	480 bit/s	1200/2400 kbit/s; 16.384 kbit/s	13.165 kbit/s; 38.4 kbit/s
Nominal Range	500-1000 m	80-500 m	~1000 m; 100 m	~500 m; 40 m
Modulation Type	N/A	PPM	S-FSK; FSK	BPSK; FSK
Network Topology	N/A; Star	Peer-to-peer	Tree, Line, Star	P2P; Mesh; dual-mesh/band
Network Size	256	~64000	255; 65536	65536
Encryption	N/A	N/A	N/A; 128-bit AES	Rolling Code Encryption
Complexity	Complex	Complex	Simple; Less Complex	Less Complex

Table 1. Summary of the main features of X10, UPB, KNX, and INSTEON technologies

3.2.2.1.3. KNX

KNX can be denoted as ISO/IEC 14543-3 based low-cost, flexible, secure and compatible network communication protocol for smart buildings [11]. Instead of directly using the existing AC power line, KNX requires its own wired network, and there are three forms of it; namely star, line and tree. A bus topology is able to support up to 256 KNX-oriented products, such as system devices, control units, sensors, detectors, and actuators. KNX enables the remote control of lighting, heating and cooling systems; gate entrance, security and authorization transactions; curtain/shutter-derived home appliances, and supports fault or malfunction tracking like central monitoring, managing and controlling operations. With the 16.384 kbit/s data rate, KNX provides relatively faster, flexible and energy efficient solutions for home and building automation. The protocol defines several physical communication media, such as twisted pair wiring

(KNX-TP), power line narrowband networking (KNX-PL) -PL110 and PL132, radio communication (KNX-RF) -ZigBee, Z-Wave, and Wi-Fi, and Ethernet (KNX-IP) to expand the application range [15]. Besides these good specifications, KNX systems have some inevitable restrictions like installation costs which are non-negligible, the complexity increased by multi-protocol participation, and the relatively embedded structure beclouded the system upgrades.

3.2.2.1.4. INSTEON

INSTEON is a dual-band mesh home networking technology to bridge and connect the wireless and power line-based protocols and/or devices to each other [16]. It enables sensors, switches, lightening tools, remote controls, and any other electrical gadgets to communicate over power lines, radio frequencies or both of these technologies. INSTEON is compatible with X10 standard operative devices where the commands are conducted on AC lines, but the actions take place in needed areas notwithstanding wires and/or cables thanks to the RF support of INSTEON. Today, there are nearly 200 INSTEON-to-X10 enabled devices on the market. All the INSTEON enabled devices are constructed as same, and they can transmit, receive, or repeat any message of the corresponding protocol, without requiring a network controller or a special routing algorithm. The only negative side of INSTEON technology is having considerably low data rates for the communication [17].

3.2.2.1.5. The Other Wired Systems

It is also possible to build an automation system over the traditional telephone line, DSL, ISDN or Ethernet; however, these methods are not adequate to satisfy today's needs.

3.2.2.2. Wireless Technologies

3.2.2.2.1. Wi-Fi

Wi-Fi or Wireless Fidelity is an IEEE 802.11 standard-based, low cost, unlicensed wireless local area network (WLAN) technology [11]. It operates in Industrial, Scientific and Medical (ISM) band with the carrier frequency of 2.4 - 5 GHz. Wi-Fi can be classified as a long range solution for local area networking with 45 m indoor and 90 m outdoor coverage capabilities [14]. The majority of wireless communication required products, such as laptops, cellphones, and internet access devices -routers, modems, etc. are equipped with Wi-Fi chipsets in parallel to ongoing decrease of their unit price and ease of use. As the

protocol was evolving to 802.11n from 802.11a/b/g in time, the number of hotspots, throughput and data rate increased, so Wi-Fi became more feasible to serve high bandwidth solutions for human oriented applications. Wi-Fi supports point-to-multipoint (access point), point-to-point (Ad-Hoc) and multipoint-to-multipoint (mesh) networking structures. The major limitations of Wi-Fi technology can be listed as high power requirements, interference from other devices as a result of using relatively crowded bandwidth, security, serious communication losses caused by obstacles, and lack of inter-operability.

3.2.2.2.2. ZigBee

ZigBee is an IEEE 802.15.4-based high-reliable and low cost wireless communication protocol which has low power consumption characteristics under operation [1]. It supports 3 different network structures; namely, generic mesh, star and cluster tree that varies depending on the application specific. Mesh networking enables routing protocols to reach the desired sensor nodes and/or devices by using intermediate network components as relay. That increases communication range while making the medium more reliable. ZigBee operates in 784, 868, 915 and 2400 MHz globally available ISM bands with the adaptive data rates varied between 20 and 250 Kbit/sec [10], [14]. This relatively low transfer rate implicitly provides multi-year battery life as requiring low energy. ZigBee reaches up to 70 m in LoS depending on frequency, output power and module characteristics. It is easier to utilize and/or implement a wireless personal area network in contrast with Wi-Fi and Bluetooth.

ZigBee uses the physical and medium access control layer definitions of IEEE 802.15.4 specification as a basis for higher layer communications as seen in Figure 4. IEEE 802.15.4 comprises various PHY opportunities for different regions in the world which operate in 868 and 2400 MHz frequencies of ISM band [11]. For the first one that assigned to Europe, the data are spreading by using direct-sequence-spread-spectrum (DSSS) at a rate of 20 Kbit/s with the carrier frequency of 868 MHz. One differential encoded data bit is spread to 15 chips. The chips are then physically transmitted with Binary Phase Shift Keying (BPSK) modulation. Maximum transmission power for this specification is limited with 25 mW and the effective bandwidth is stated as 600 kHz. The second PHY alternative operates in the 2.4 GHz ISM band with the rate of 20 Kbit/s and can be used worldwide. Spreading method is again DSSS similar to the first one, and 4 data bits are spread to 32 chips with the help of 16 quasi-orthogonal sequences. These chips are then transmitted with Offset Quadrature Phase Shift Keying (O-QPSK) modulation with half sine pulse shaping. Maximum transmission power for this specification is limited with 20 mW and the effective bandwidth is stated as 2 MHz. The MAC layer uses the physical channel to transmit the MAC frames and handles the channel access over a CSMA/CA procedure.

Due to the small duty cycles, low data transfer rates, leading into less energy consumptive small gadgets, power save mode deployment, and energy efficient modulation techniques, a ZigBee module serves longer process life with tiny batteries preventing the unnecessary usage of external supplies [18]. Therefore, it becomes a cost and energy effective solution for monitoring, managing and controlling duties. In addition to these advantages, fast and easy employability, flexibility, extra node capability and manufacturer supplier independence make ZigBee more preferable. However many benefits ZigBee possesses, there are some drawbacks as well. Low data rate, license requirements, limited distance, and low data processing speed can be counted as well-known restrictions of ZigBee technology.

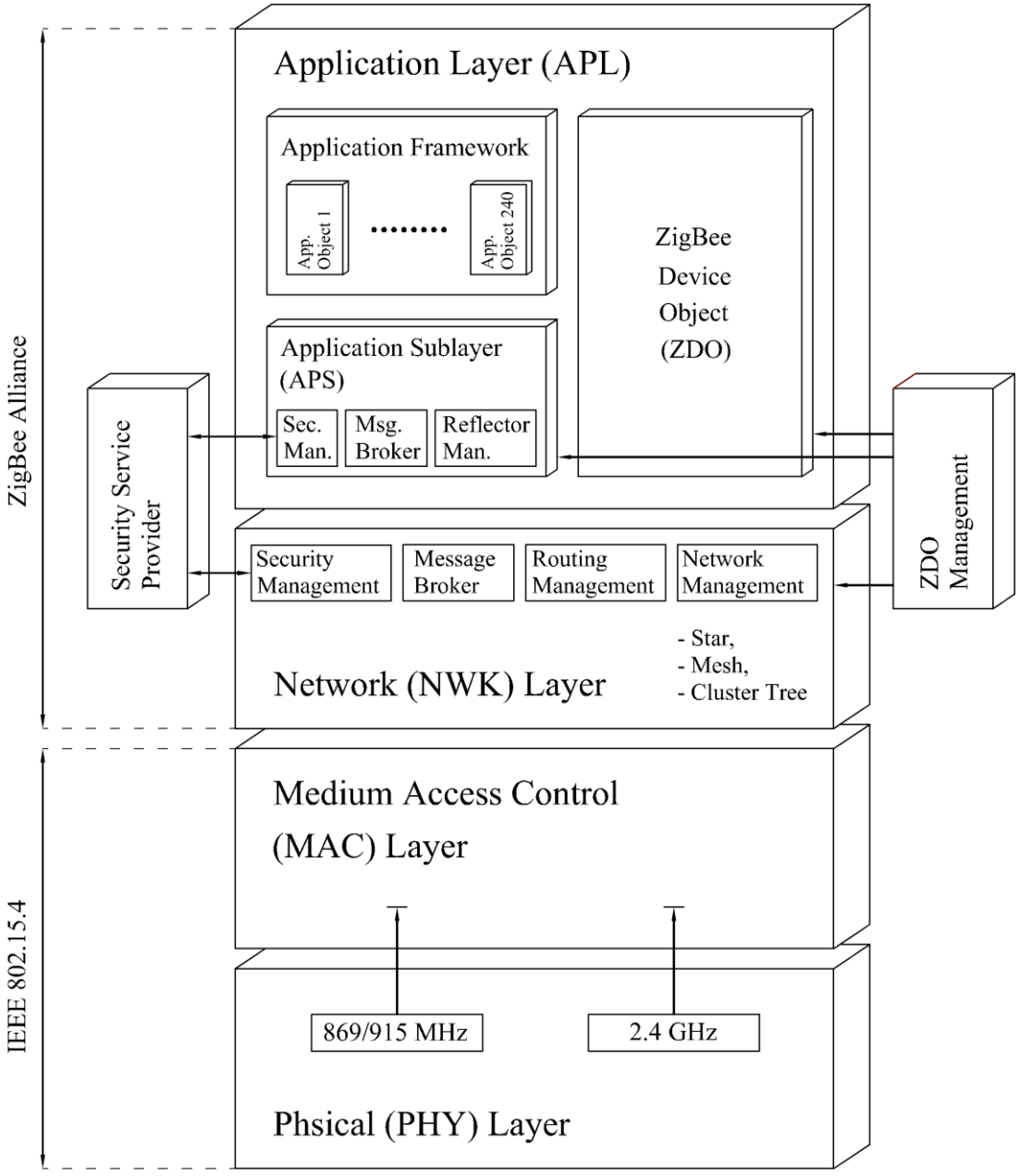

Fig. 4. Protocol architecture of ZigBee technology

3.2.2.2.3. Z-Wave

Z-Wave is a new wireless communication protocol which specialized for home automation [19]. In spite of coming out recently, it supports roughly 1000 different devices, and these can be controlled over a tablet, smartphone and/or personal computer. This extremely low power consumptive protocol makes any household product 'smart' as serving secure, energy efficient, convenient and reliable scenarios. It is easy to implement a Z-Wave network in a home environment, the corollary of wireless communication, because it doesn't require any additional wiring or construction. Operating frequency of Z-Wave varies from 862.2 to 921.42 MHz which helps to reduce the number of possible interferences from mostly preferred frequencies and protocols like 2.4 GHz operative Wi-Fi, Bluetooth and ZigBee. Unlike the collaboratively constructed technologies like 6LoWPAN, Z-Wave protocol is driven by Z-Wave Alliance, as shown in Figure 5.

Considering the huge data transfer is not essential to control the home appliances, Z-Wave has an adequate and acceptable data rates up to 100 Kbit/sec. It enables routing protocol utilization with supporting mesh network which increases the communication range, quality and reliability. Even if the mentioned specifications convince the user about it is a good option, there is still room for development. To illustrate; although the initial construction costs are low, Z-Wave enabled devices are relatively expensive. It is not license-free which means additional fees for commercial products have to be paid, and a network controller with an additional gateway must be provided to realize the connection between the end-devices.

3.2.2.2.4. Bluetooth and BLE

Bluetooth can be defined as IEEE 802.15.1-based wireless personal area networking technology. It uses short wavelength radio waves which limits the communication distance, and operates in the range of 2.4 to 2.485 GHz globally unlicensed ISM band [11]. There are 3 classes for Bluetooth, namely 1, 2 and 3; power requirements and typical ranges of them may vary depending on the application. Bluetooth is frequently used in mobile phones, personal computers, and gaming consoles. There exists a typical master-slave interaction between devices, and a master can manages/supports up to 7 slaves. The relation or behavior of these classes can change during the communication which means a master can turn into a slave and a slave can manage the communication as a master. This helps to carry a healthy and reliable communication out. Typical data rate of Bluetooth is 0.7 – 2.1 Mbit/sec and the range varies from 5 to 30 meters. The chipset expenditure of Bluetooth goes down day by day, and that makes it a cost effective solution for short distanced and low data rate required applications [14]. In recent years, an improved version of Bluetooth, namely Bluetooth Low Energy (BLE) or Bluetooth Smart has been announced and being used in smart phones, healthcare and fitness systems, beacons and home entertainments. As its name suggests, BLE

consumes considerably low power than Bluetooth without affecting the range; however the data rate reaches up to only 0.27 Mbit/sec. BLE has been used in home automation as being cheap and low power consumptive. Data spreading is realized with frequency hopping spread spectrum (FHSS) technology, and Gaussian Frequency Shift Keying (GFSK) modulation is preferred for the data transmission. Besides the mentioned advantages, limited range, low data rate, unsecure structure and using the battery of belonging device are the notable drawbacks of both Bluetooth and BLE.

Protocol / **Feature**	***Wi-Fi*** *IEEE 801.11.n*	***ZigBee*** *IEEE 802.15.4*	***Z-Wave*** *ISO/IEC 14543-3*	***Bluetooth*** *IEEE 802.15.1*	**BLE** *IEEE 802.15.1*	**6LoWPAN** *IETF RFC-6282*
Operating Frequency	120 kHz, 2.4-5 GHz	868/915 MHz, 2.4 GHz	868/915 MHz	2.402-2.482 GHz	2.402-2.482 GHz	868/921 MHz, 2.4-5 GHz
Maximum Data Rare	11-54 Mbps	20/40 kbps; 250 kbps	9.6-40 kbps	0.7-2.1 Mbps	0.27 Mbps	10-40 kbps, 250kbps
Nominal Range	10-100 m	10-1000 m	30-50 m	15-20 m	10-15 m	10-100 m
Modulation Type	BPSK, QPSK, OFDM, M-QAM	D-BPSK, O-QPSK, QPSK	FSK, GFSK, Narrowband	GFSK, CPFSK, 8-DPSK	GFSK	BPSK, O-QPSK, ASK
Network Topology	Star, Tree, P2P	Star, Mesh, Cluster Tree	Mesh	Star	Star	Star, Mesh, P2P
Network Size	32	65536	232	8	N/A	~100
Encryption	RC4 Stream & AES Block Cipher	128-bit AES	128-bit AES	AES Block Cipher	128-bit AES	128-bit AES
Coding	MC-DSSS, CCK, OFDM	DSSS(1→15) DSSS(4→32)	Manchester; NRZ	FHSS	Adaptive CCK	Header Compression, DSSS
Channel Bandwidth	20-25 MHz	0.3/0.6 MHz; 2-5 MHz	Fixed	1 MHz	8 MHz	2-5 MHz
Complexity	Complex	Simple	Complex	Complex	Simple	Less Complex
Applications	Monitoring, Internet, Data Network	Wireless Sensing, Monitoring	Home Automation, Security	Wireless Sensing, Monitoring	Health-care, Beacon, Fitness	Home, Automation, IoT

Table 2. Summary of the main features of Wi-Fi, ZigBee, Z-Wave, 6LoWPAN, Bluetooth and BLE

3.2.2.2.5. 6LoWPAN

6LoWPAN is a globally free and open standard to compose of low power wireless personal area networks (LoWPANs) over Internet Protocol version 6 (IPv6) which is defined in RFC 6282 by the Internet Engineering Task Force (IETF) [1]. As being based on IPv6 makes every device able to connect to the internet, due to having a unique IP address, over an open standard like TCP, UDP, HTTP, COAP and etc. In other words, 6LoWPAN is as a low cost, low power -battery operated- and low bandwidth wireless mesh networking technology that operates in 868, 915, and 2400 MHz frequencies of ISM band [20].

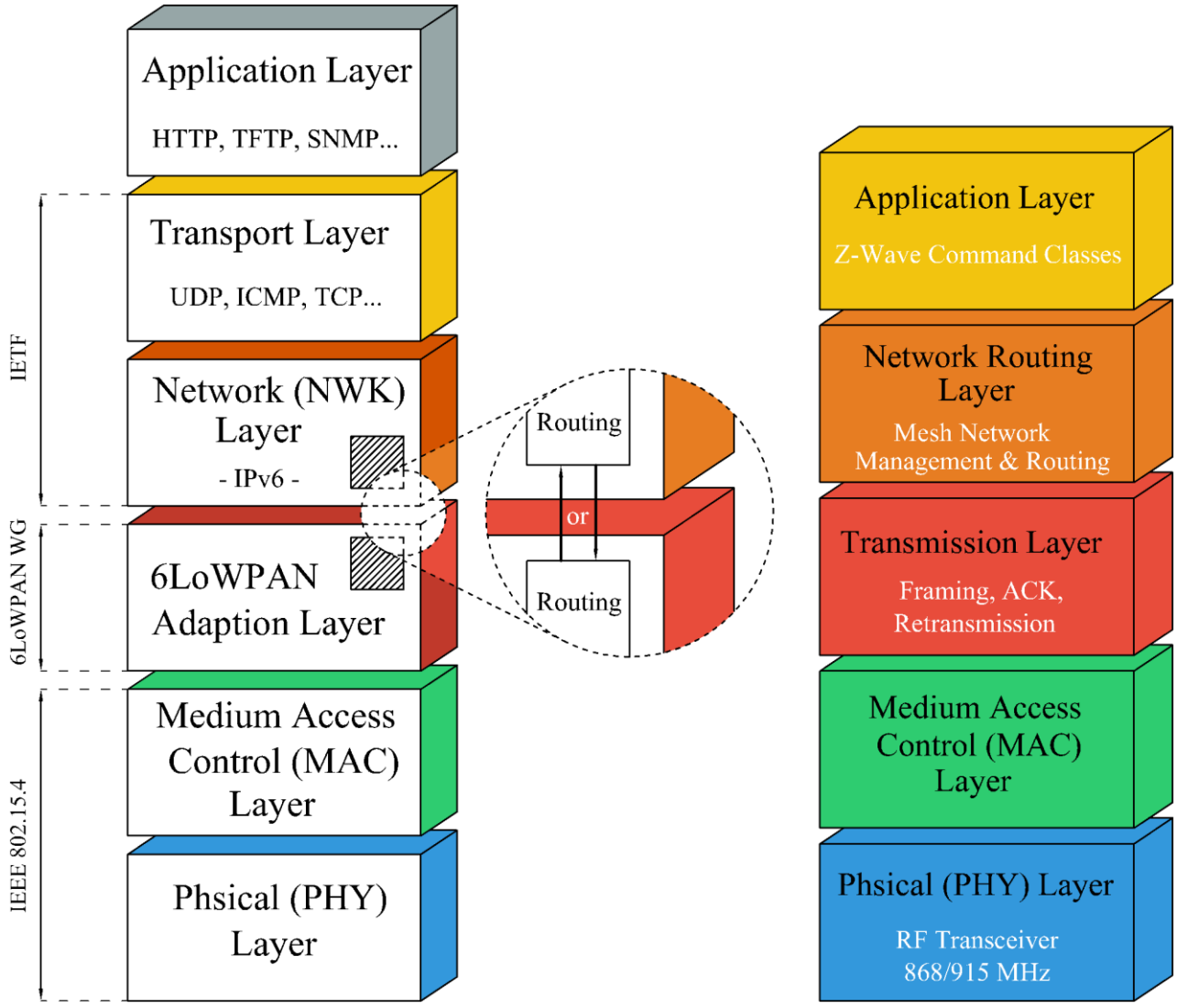

Fig. 5. Protocol architectures of 6LoWPAN and Z-Wave technologies, respectively

Data rates vary from 20 to 250 kb/s depending on the carrier frequency and mode specifications. It uses IEEE 802.15.4's PHY and MAC layer, i.e., OSI layer 1 and 2, definitions as a basis similar to ZigBee protocol. IETF is in charge with developing upper layer technologies as seen in Figure 5. As a natural consequence of that, data are spreading and encrypted by using DSSS, at 2.4 GHz, and AES-128 respectively, channel access is handled over a CSMA/CA procedure on MAC layer, and multi-hop/routing capable two types of devices similar to ZigBee technology, namely full and reduced function, are supported for mesh networking. A full function device (FFD) is able to communicate with all types of device classes in the network unlike a reduced function device (RFD), while supporting the full protocol. FFDs tend to consume more energy and require to equip with improved hardware like CPU/RAM in contrast with RFDs, because they are responsible for the overall network management, address allocation assignments, evaluation and conveying of the gathered information, and node/router joining and/or disjoining operations.

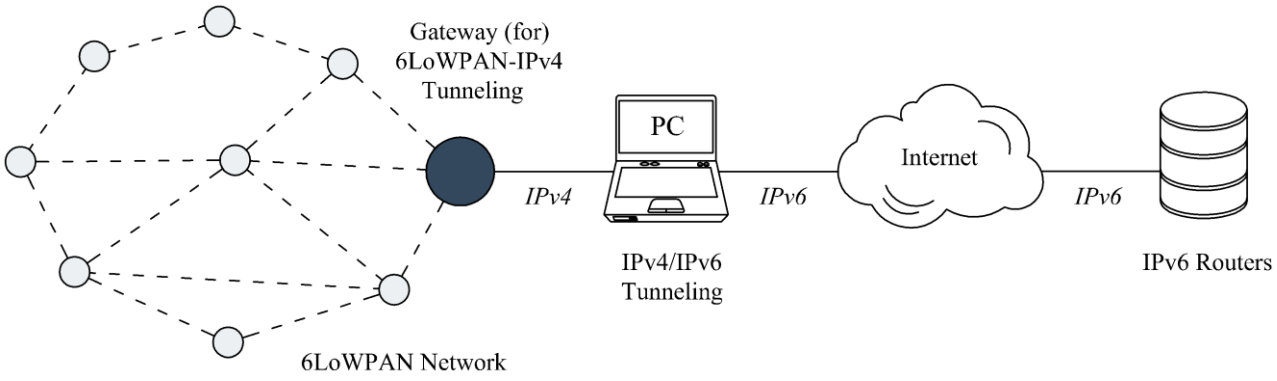

Fig. 6. The 6LoWPAN Protocol Network Model

The main idea which lies behind of this standard is the need of enabling the internet connectivity for even the smallest device. IPv6 is preferred for this goal, due to the ability of heterogeneous network connection, worldwide free-to-use infrastructure, globally scalability and perhaps most importantly having a great addressing space, numerically 2^{128} bits ~16 byte, what is enough for Internet of Things (IoT) [21]. Figure 6 shows both in network data flow and IPv4 to IPv6 packet conversion structure. Considering the massive expansion of web-enabled devices, today's frequently used protocol for Internet, IPv4 -which has only 2^{32} IP addresses, will be inadequate eventually. Therefore, IPv6 is developed to stay for decades while enabling the internet access to wireless operated devices. 6LoWPAN is now mostly preferred in health and environment monitoring, security, logistics, and building automation.

3.2.3. Requirements, Characteristics and Design Objectives of WSNs in Smart Homes

As mentioned before, WSNs enable numerous applications and scenarios for smart indoor areas. When considering these networks are formed by the combination of sensory nodes as getting together in huge numbers as collaboratively, there is no doubt to say that, building a 'healthy' WSN can be only obtained by constructing the nodes as good as possible [9]. In order to achieve that, some characteristic requirements; such as, scalability, self-configurability, mobility, responsiveness, energy efficient operation and QoS which compromise fault tolerance, programmability, reliability, maintainability, and longevity should be fulfilled [22]. Some of these metrics are detailed below.

3.2.3.1. Scalability

Scalability refers to the ability of supporting network enlargement in terms of node quantity. In other words, a network should be operational regardless of the increasing number of deployed sensors. However, as the network size grows, usable bandwidth detractive overheads can occur, and data packet & message loss causative communication link failures may increase; therefore, more control packets could be required to follow the routing path and make the communication feasible [22]. Where a typical WSN can be formed by 10s to 1000s sensor nodes, the average varies between two-digit numbers for an indoor environment. As the flexible structure of wireless home automation networks allow upgrading the system by adding extra sensors or any other related devices in certain quantities, they should be constructed as durable as possible even if the network size is enlarging constantly.

3.2.3.2. Reliability

Reliability is the ability of ensuring reliable data transmission regarding to continuously varying dynamics of networks. There is an inverse relation between scalability and reliability in WSNs; that means, while the number of node is increasing; it becomes more difficult to ensure the reliability as expected.

Since the structure diversifies, required number of control packets will increase, and the network eventually becomes unable to sustain the amount of overhead induced by the dynamics, which reduces the data transmission reliability. As expected, this braking point will be observed much earlier in a large-scaled network. Therefore, scalability and reliability metrics are firmly coupled and typically prone to act against each other [22].

3.2.3.3. Longevity

Longevity can be defined as the ability of fulfilling the previously assigned duties as long as possible. Since the definition of lifetime varies from the application, there are some keywords for denoting it. For example, as the time that elapsed until the first node dies can define the lifetime of the network, coverage loss of a particular area, failure of the first event notification, and the time until %50 of the nodes die -half time expressions are also usable for the definition of this metric. For especially the huge networks where the mesh topologies and routing algorithms are employed, longevity becomes more important for the overall network sustainability.

3.2.3.4. Robustness

Robustness is the ability of withstanding unpredictable node failures occurred by environmental variations or design based malfunctions. For a WSN, some nodes may expire in time due to the powering circumstances or any other restrictive characteristics of itself while the rests are trying to keep working under the coercive physical conditions of the operation area. The network should resist and sustain its operation with compensating the harmful effects of the system changing, and the level of this resistance roughly defines with robustness. In addition to that, ***fault tolerance*** or ***resilience*** can also be referred as a measure of how strong a network is. With regard to that, there are two failure models, namely nodes and communication links, for the precise evaluation of robustness.

3.2.3.5. Responsiveness

Responsiveness means the ability of the network to rapidly adapt itself to unexpected changes in the topology. To achieve high responsiveness, more control packets are exchanged, which will inevitably decrease the both scalability and reliability. Typically, the latency of packet delivery in dynamic environment reduces in the network with high responsiveness.

3.2.3.6. Mobility

Mobility can be defined as the ability of handling mobile nodes and changeable data paths in a network. Generally, a WSN that includes a bunch of mobile nodes should have high responsiveness to deal with the mobility. That means, it is not easy to design a large scaled and highly mobile wireless sensor network, without considering the system constraints.

3.2.3.7. Maintainability

Maintainability is the ability of adapting to changes by utilizing self-monitoring derived adaptive operations. For example, the system should provide lower operation quality when the energy source becomes scarce.

3.2.3.8. Programmability

Programmability refers to the ability to re-programming of nodes in the field when it becomes compulsory. This metric improves the flexibility of the network as enabling proper system working.

3.2.3.9. Energy Efficient Operation

As mentioned previously, energy can be the scarcest resource for WSNs in some cases. Therefore, it should be used as efficient as possible, and the energy efficient operation refers to this goal in terms of network requirements. To measure this metric, energy per correctly received bit or energy in transporting one bit of information from source to destination terms can be considered.

A low-power wireless sensor network can be achieved by reducing the duty cycle of each node. However, as the wireless sensor node operates in power save –sometimes called as sleep mode- much longer, the possibility of packet losses and communication failures increases. As mentioned before, although this mode saves considerable amount of power, recovery time and startup energy terms are getting crucial to maintain the efficient system work. This results in decreasing system responsiveness and also the reliability of network by the absence of control packets and increasing duration of packet delivery delays. At this point more sophisticated synchronization techniques should be utilized to keep more nodes in low duty cycle, without affecting the overall system responsiveness, scalability and reliability.

3.2.4. Routing Protocols for WSNs in Smart Homes

As the wireless systems deal with the drawbacks of their wired counterparts by providing satisfactory solutions in terms of simplification, QoS and energy efficient operation, there is still room for enhancements. To give an example, one common problem for the wireless technologies can be denoted as the limited range of the communication. This issue is essentially arisen due to the restricted transmitting power, path losses, and fixed or mobile obstacles. To overcome the lack of coverage-based transmission failures, multi-hop operations, i.e., routing protocols, can be utilized [10].

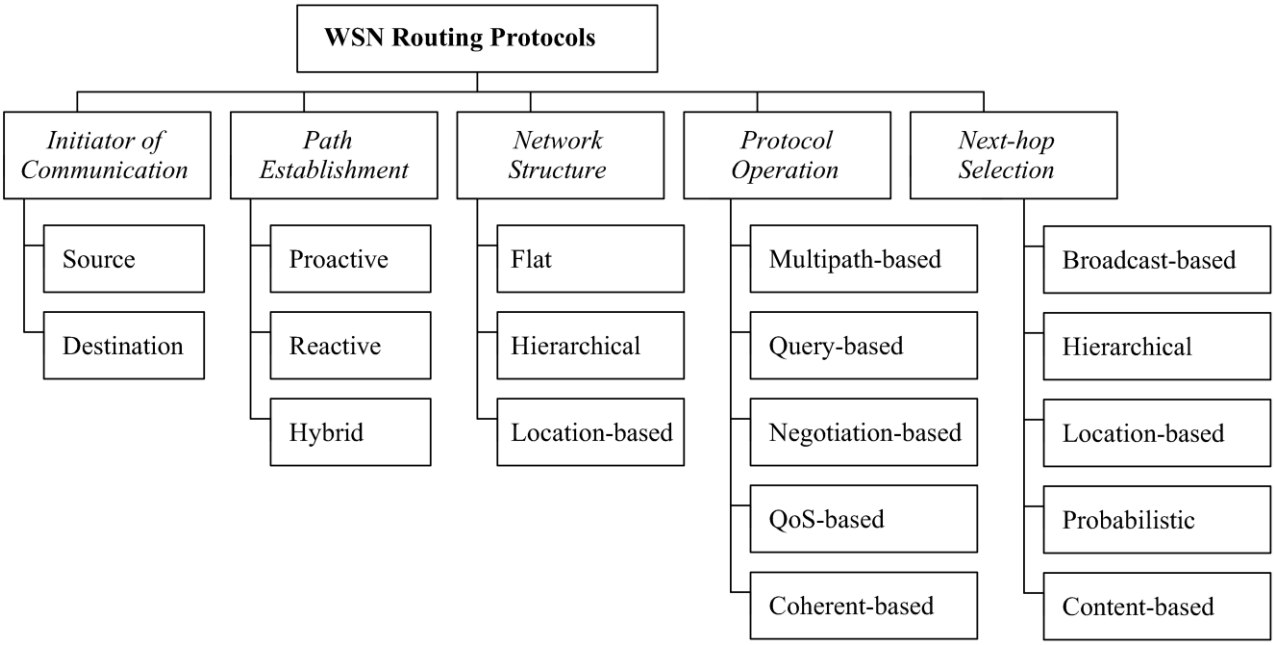

Table 3. The Classification of Routing Protocols in WSNs

These protocols are basically responsible for finding and maintaining the path from the sensors to sinks, access points or base stations. These architectures are based on the idea of using some intermediate nodes as relay to carry the sensor data from the source to destination. Intermediate nodes forward the received packets to their destination, which called as 'store and forward multi-hopping' or 'collaborative networking' [2]. Even though the routing protocols expand the reachable communication distances, they result in trade-offs between the system characteristics and requirements. Therefore, multi-hopping should be carefully applied to the networks as considering the possible energy consumptions in future, quality of the communication, total distance to be travelled till reaching the destination, and the robustness of the system. In general, the communication between the coordinator and the sensory nodes is handled through the direct links (with single-hop), when the operation area is small enough, thanks to star and/or point to point networking topologies. However, this may be not feasible or applicable due to constraint of energy, scale of network, and lack of unobstructed communication links. Although the area is limited and the nodes are deployed wisely, sometimes multi-hopping may become essential for the transmission. The schemes related to single and multi-hop communication can be found in Figure 7.

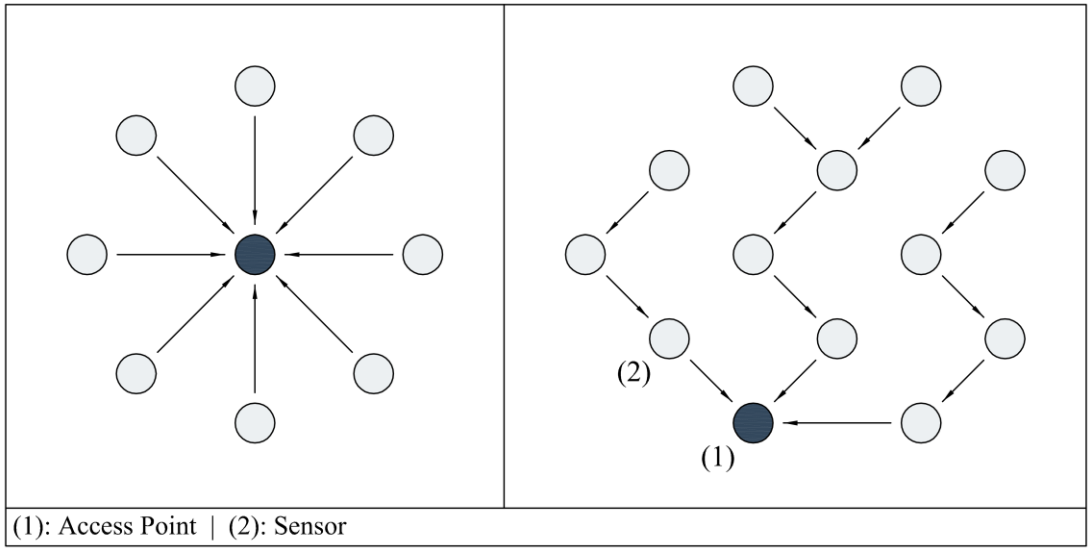

Fig. 7. Single and multi-hop communication schemes for sensor networks, respectively

There are several types of routing mechanisms which aim to minimize various cost functions such as distance -minimum hop (shortest path), QoS (latency, throughput, packet loss, and error rate), robustness (link quality and stability), and energy consumption [23]. For indoor environments, mostly minimum distance-based algorithms are utilized; however, this approach might yield in unsuccessful transmissions in the scenarios where moving obstacles exist in the area. In the case of crowded indoor areas such as offices, subway stations or supermarkets, human beings evolve to potential and inevitable obstacles for the sensors. Since nodes are fixed, they cannot reposition themselves to avoid the negative effects of human blockings. Therefore, that makes the sensors and so the networks more likely to prone the failures. Sensor networks provide the infrastructure for reliable transmission of data but routing based problems are likely to cause communication delay and increasing number of retransmissions, which are undesired for WSNs with efficient transmission capabilities. So the multi-hopping techniques should be wisely selected and effectively utilized depending on the specifications and the requirements of the application. Routing protocols in WSNs can be categorized into four groups -sometimes five, namely network structure or organization, the way of establishing routing paths, i.e., route discovery, the protocol operation, the initiator of communication, and (the fifth one) how a protocol selects the next-hop on the route of the forwarded message. Nowadays, more advanced technologies specialized for the specific requirements of application are preferred to transport the data through the network [24]. Table 3 and 4 are given to summarize the classification and the application distribution of the routing protocols conducted in WSNs.

Classification	Category	Protocol
Network Structure	Flat-based	EAR, DD, SAR, MCFA, SPIN, ACQUIRE
	Hierarchical-based	HPAR, TEEN, MECN, LEACH, PEGASIS, HEED
	Location-based	SAR, APS, GAP, GOAFR, GEAR, GEDIR, MECN
Protocol Operation	Multipath-based	MMSPEED, SPIN, Sensor, Disjoint, Braided
	Query-based	SPIN, DD, COUGAR
	Negotiation-based	SPAN, SAR, DD
	QoS-based	SAR, SPEED, MMSPEED

Table 4. Network Structure and Protocol Operation-based proposals

3.3. Operating Systems (OS) for WSNs in Smart Homes

Regarding the unavailability of supporting fully operative structures, WSNs utilize less complex operating systems (OS) rather than the general purposed equivalents. They are resemble to embedded systems by structured as application specific and equipped with less capable components in contrast with commonly used operating systems. Therefore, it is possible to utilize embedded systems such as eCos and/or uC/OS to the WSNs. TinyOS can be referred as the first and the most frequently preferred OS in WSNs which based on an event driven programming model instead of multithreading. It is designed for enabling capable, low cost and application focused sensory nodes with combining highly efficient execution and component models, and communication mechanisms. The components of TinyOS can be listed as command and event handlers, frame, and tasks. LiteOS is a relatively new OS that supports C programming language and UNIX derived systems. Contiki also takes its basis from C language which uses a simpler programming style. RIOT provides multithreading and enables internet connectivity for the nodes and/or related devices with supporting internet of things (IoT) protocols like 6LoWPAN, IPv6, TCP and so on, while implementing a microkernel structure. Lastly, ERIKA Enterprise can be defined as an open source and royalty-free OS derived in C programming language. These systems are in an ongoing improvement to achieve energy efficient operation, better harmonized execution, and simplified administration [2], [3].

Regarding to the need of graphical user interface (GUI) for smart home applications, smartphones are evolved to track, monitor and manage the environment over a communication technology. Considering the influence of these gadgets to human live, and also the usage intensity, smart home systems should be upgraded as compatible with the operating systems running in smartphones. With this attempt, ease of use and flexible management of household appliances could be achieved.

3.4. Security and Privacy Considerations for WSNs in Smart Homes

As introduced previously, WSNs are able to monitor, collect and analyze the essential data for the people, who live, work or situate in a smart environment, concerning their life-sustaining activities, movements, locations, device and utility usage information, and also the related physical parameters of the medium to control, manage and secure this particular area by informing the user's itself or any other authorized people and/or institutions for decision making operations. Interaction of this privacy including data is usually handled over the existing wireless networking technologies. When considering the communication is realized over the open air where numerous devices and networks are constantly transmitting through sharing and distributing information, smart environments become vulnerable to security threats, inevitably [5]. It could be easy to reach and probe the medium remotely by using powerful antennas to capture the sensors, tamper or modify the data with eavesdropping, jamming, or inserting malicious traffic [10]. To provide complete security, every sensor or any other sub-device of the network must be equipped with safety mechanisms to prevent the upcoming attacks might be occurred/targeted over an insecure component [25]. Without any protection, the whole system could suffer from threats or malfunctions caused by external attacks that disrupt the services provided by the sensor networks. As the security threats can be intended for physical layer, routing, position information and data aggregation, they can also be utilized for both eavesdropping and time synchronization affection. Security operations mostly focus on protecting environmental access, appliance usage, and users' privacy. There are two types of private information, namely data and context-oriented which are needed to be protected or preserved [25]. For the context-oriented privacy, mechanisms deal with the protection of the contextual information regarding location, and timing of both data generation and transmission processes. Data-oriented privacy can be treated by an external and/or internal adversary who is not an authorized member of the network. External attacks are generally intended for eavesdropping or listening to the data communication between sensory nodes since the internal ones are focused on node capturing and reprogramming for the private information collection. Internal attacks could be more dangerous in contrast with external adversaries, due to the fact that it is relatively harder to detect these kinds of assaults with traditional methods. Therefore, the main effort of data-oriented privacy is focused on protecting information from the internal adversaries. To rebuff the privacy-oriented interventions, generally cryptographic encryption with authentication, and end-to-end encryption (between the sensors and access points) methods are utilized, respectively. Potential applications in the smart environments like resource, appliance and utility usage; presence, identification and activity detection; vital sign, location and motion monitoring duties necessities the data-oriented protection rather than the context-oriented privacy. Therefore, when dealing with the security issues in smart

networks, the requirements; integrity confidence, freshness, availability, and authenticity, are observed to measure, compare and improve to provide more secure and private environments [25].

The data should be encrypted to becloud the content leaks since the processor of the system must be capable and intended for performing the required cryptographic operations itself or with the contribution of included cryptographic boosters. As an example, the IEEE 802.15.4 standard which provides physical and mac layer definitions to the ZigBee and 6LoWPAN derived technologies for the construction of higher level communication layers, serves three different security opportunities classified as no security, non-cryptographical access to control lists, and symmetric key security with employing AES-128 (Advanced Encryption Standard). These and the other quasi-enhancements contribute to build more secure systems in parallel to increasing sizes of the networks and the number of interaction diversity.

3.5. Emerging Technologies, Challenges and Requirements for the Future Smart Homes

When considering the total amount of spent time in the residential areas by the people, future homes will be formed with the all required services, such as entertainment, communication, energy planning, utility usage, medical monitoring, and security. The developers and the investors will play a key role collaboratively for this progress [5].

Recently, smart grid systems have been emerged for the intelligent control of the electricity, which provides bidirectional communication between the suppliers and the consumers. With this attempt, a supplier has been evolved to control home appliances indirectly to guarantee the proper system work by providing uninterrupted electricity supply. To make the intelligent energy control feasible, smart meters, i.e., smart plugs [26], are utilized as an integral part of the smart grids. These systems allow the users to control and manage the connected devices remotely, and monitor the energy usage to regulate the all kinds of consumptions with demand responsive and redundant energy preventive algorithms. Also, the negative effects of grid and/or threat induced malfunctions are reduced with employed mechanisms to obtain more reliable communication and operation. In the near future, the integration of smart grids, smart homes and smart plugs will play a crucial role for the regulation of the energy demand.

The other justification to deploy WSNs into the residential areas is enabling healthcare systems for the elderly and/or disabled people. As requiring less manpower in control and monitor the vital signs of patients, these systems became more preferable. The growing number of population will result in lack of servings and staffs for the care and treatment of illnesses in hospitals, therefore, WSN-based local healthcare services will be expected to receive more emphasis in the future, inevitably.

One of the compelling issue in the existing smart homes can be denoted as the lack of inter-compatibility. Although there are numerous communication and networking technologies employed so far,

these systems are not able to work in collaboratively except a small portion. That yields to problems when a combination of different protocols is needed to be utilized. To overcome this drawback, developers, institutes, interest groups and alliances have started to work together for the standardization. In the short run, more flexible and inter-compatible home automation standards will influence the market.

The other restrictive issue for the wireless home automation networks is the possible threats on the user privacy. Since the reliable data transmission may not be provided at every step of the communication, private information may be leaked. Especially with the integration of the IP-based protocols to the WSNs, the risk level of the violation has increased rapidly. To maintain the confidentiality, data encryption and cryptography mechanisms are currently being used to employ the security in communication systems.

To overcome the problem of energy scarcity in WSNs, energy harvesting operations may be maintained. Scavenging energy can provide longevity to the nodes while implicitly increasing the overall network sustainability. For an indoor environment, solar cells can be mounted where the places intensely exposed to sun, and for the crowded ambient like subway stations and/or hospitals piezo-electric materials may be furnished to the ground to gather energy from the pressure variations. Vibrations, noises, and temperature gradients are the other existing proposed methods for converting ambient dynamics into the energy sources [27]. Considering the efficiency of energy harvesting operations is increasing continuously, there is no doubt to say that the future smart homes will benefit heavily from the improvements of these technologies.

3.6. Conclusion

In this article, we surveyed the existing literature of sensor networking-based indoor automation systems. Detailed information is given about the current situation of the small scaled extension of smart grids, namely smart homes, and their applications. Besides the elderly wired proposals, the most relevant emerging communication protocols tailored to wireless smart home sensor networks have been investigated as comparatively. Node architectures, network types, topologies and requirements, design objectives, routing protocols, and restrictive issues are also discussed. After these, with the analysis of security and privacy considerations focused on WSNs in smart home implementations, and emerging & promising technologies for future smart indoor areas, the discussion part is finalized. All in all, this book chapter aims to survey the significant and recent papers on wireless sensor home networks and to highlight the research potential and possible approaches to the problems in smart home applications.

References

[1] C. Gomez,, and J. Paradells. Wireless home automation networks: A survey of architectures and technologies. *IEEE Communications Magazine*, pages 92-101, 2010.

[2] H. Karl and A. Willig. Protocols and architectures for wireless sensor networks. *John Wiley & Sons*, 2007.

[3] W. Dargie and C. Poellabauer. Fundamentals of wireless sensor networks: theory and practice. *John Wiley & Sons*, 2010.

[4] K. Su, J. Li, and H. Fu. Smart city and the applications. *Electronics, Communications and Control 2011. ICECC 2011. International Conference on*, IEEE, 2011.

[5] M.R. Alam, M.B.I. Reaz and M.A.M. Ali. A Review of Smart Homes—Past, Present, and Future. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, Vol.42, No.6, pages 1190-1203, 2012.

[6] F. Viani, F. Robol, A. Polo, P. Rocca, G. Oliveri and A. Massa. Wireless Architectures for Heterogeneous Sensing in Smart Home Applications: Concepts and Real Implementation. In *Proceedings of the IEEE* , Vol. 101, No. 11, pages 2381-2396, 2013.

[7] O. Cetinkaya and O. B. Akan. A DASH7-based Power Metering System. In *Proc the 13th Annual Consumer Communications & Networking Conference 2015. CCNC 2015.* IEEE, 2015.

[8] F. Karray, M.W. Jmal, M. Abid, M.S. BenSaleh and A.M. Obeid. A review on wireless sensor node architectures. *Reconfigurable and Communication-Centric Systems-on-Chip 2014. ReCoSoC 2014. 9th International Symposium on* , pages 1-8, 2014.

[9] D. Basu, G. Moretti, G.S. Gupta and S. Marsland. Wireless sensor network based smart home: Sensor selection, deployment and monitoring. *Sensors Applications Symposium 2013. SAS 2013, pages* 49-54, IEEE, 2013.

[10] S. Singhal, A.K. Gankotiya, S. Agarwal and T. Verma. An Investigation of Wireless Sensor Network: A Distributed Approach in Smart Environment. In *Advanced Computing & Communication Technologies 2012. ACCT 2012. Second International Conference on*, pages 522-529, 2012.

[11] N. Langhammer, and R. Kays. Performance evaluation of wireless home automation networks in indoor scenarios. *Smart Grid, IEEE Transactions on, 3*(4), pages 2252-2261, 2012.

[12] [Online], Simply Automated, Inc. "X-10 To UPB Migration Document," Version 1.1, 2003, http://www.simply-automated.com/documents/X10ToUPB%20V1.1a.pdf

[13] [Online], Simply Automated, Inc. "The UPB System Description," Version 1.2, 2005, http://www.simply-automated.com/documents/UpbDescriptionV1.2a.pdf

[14] C. Saad, B. Mostafa, El A. Cheikh and Hajraoui Abderrahmane. Comparative Performance Analysis of Wireless Communication Protocols for Intelligent Sensors and Their Applications. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 5(4), 2014.

[15] Y. Kyselytsya and T. Weinzierl. Implementation of the KNX Standard. In *KNX Scientific Conference*. 2006.

[16] [Online], INSTEON, "Whitepaper: The Details," Version 2.0, 2013, http://cache.insteon.com/pdf/insteondetails.pdf

[17] [Online], INSTEON, "Whitepaper: Compared," Version 2.0, 2013, http://cache.insteon.com/pdf/INSTEONCompared.pdf

[18] Z. Xiao-yan, H. Ting-lei, L. Pin and L. Zhao-lai. Research on smart living technology based on WSN. In *Intelligent Computing and Integrated Systems 2010. ICISS 2010. International Conference on*, pages 938-941, 2010.

[19] B. Fouladi and Sahand Ghanoun. Security Evaluation of the Z-Wave Wireless Protocol. *Black hat USA* 24, 2013.

[20] V. Kumar and S. Tiwari. Routing in IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN): A Survey. *Journal of Computer Networks and Communications*, 2012.

[21] G. Mulligan. The 6LoWPAN architecture. In *Proceedings of the 4th workshop on Embedded networked sensors*. *EmNets '07*, pages 78-82. ACM, 2007.

[22] S. Muthukarpagam, V. Niveditta, and S. Neduncheliyan. Design issues, topology issues, quality of service support for wireless sensor networks: Survey and research challenges. *International Journal of Computer Applications*, 2010.

[23] Y. Xu, S. Wu, R. Tan, Z. Chen, M. Zha, and T. Tsou. Architecture and Routing Protocols for Smart Wireless Home Sensor Networks. *International Journal of Distributed Sensor Networks*, 2013.

[24] Hussein Mohammed Salman. Survey of Routing Protocols in Wireless Sensor Networks. *International Journal of Sensors and Sensor Networks*, Vol. 2, No. 1, pages 1-6. 2014.

[25] K. Islam, W. Shen and X. Wang. Security and privacy considerations for Wireless Sensor Networks in smart home environments. In *Computer Supported Cooperative Work in Design, 2012. CSCW 2012. 16th International Conference on*, pages 626-633. IEEE, 2012.

[26] O. Cetinkaya and O. B. Akan. A ZigBee Based Reliable and Efficient Power Metering System for Energy Management and Controlling. In *Proc International Conference on Computing, Networking and Communications. ICNC 2015*. IEEE, 2015.

[27] V. C. Lee. Energy Harvesting for Wireless Sensor Network. *PhD diss., University of California, Berkeley*, 2012.

View publication stats