WSN'S AND SMART HOME AUTOMATION

Sai Krishna Kovi	Dharma bandreddi	Venkatesh poola	Sheshank R
Skovi0@frostburg.edu	dbandreddi0@frostburg.edu	vpoola0@frostburg.edu	srevani0@frostburg.edu
Dept. of comp. science	Dept. of comp. science	Dept. of comp. science	Dept. of comp. science
Frostburg state university	Frostburg state university	Frostburg state university	Frostburg state university

Abstract:

Wireless sensor networks now a day are widely used in various fields such as environmental control, smart home automation, agriculture, defence, healthcare etc. generally WirelessSensorNetworks are integrated with the Internet Protocol (IP) to develop the Internet of Things (IoT) for connecting objects which we use in everyday life to the internet. There are many technologies to integrate WSN's into smart home some of them are Z-Wave, Insteon, Wavenis, Bluetooth, Wi-Fi, and ZigBee. Among all these technologies the ZigBee based systems are popular due to their low cost and low power consumption. In this paper, we are going to discuss about how and why wireless sensor networks are to be integrated in to smart home automation, how ZigBee helps in smart home automation, and what are the security challenges and their measures involved.

Introduction:

The future Internet, outlined as a "Internet of Things" is predicted to be " a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" [1], Recognized by a different type of address, anything counting Personal Computers, sensors, RFID labels or cell phones will have the capacity to progressively join the system, team up furthermore, participate proficiently to accomplish total work. [1]. In a period of Internet of Things, more devices are connected to the web when contrasted with the populace—there were over 12.5 billion devices in 2010. Cisco predicts that 25 billion devices will come locally available in 2015 what's more, there will be 50 billion by 2020. [4]. The components of the Internet of Things are involved not only with those devices that are as of now profoundly established in the innovative world, (for example, cars or fridges), additionally protests remote to this condition (articles of clothing or, then again perishable sustenance), or not withstanding living creatures (estates, woods or then again domesticated animals) [2]. Indeed, a standout amongst the most imperative components in the Internet of Things worldview is wireless sensor systems (WSN). The advantages of associating both Wireless Sensor Network and other Internet of Things components go past remote access, as heterogeneous data frameworks can have the capacity to work together and give normal

administrations. A Wireless Sensor Network (WSN) is an arrangement of disseminated self-sufficient sensors, which are called nodes, that screen the status of the space in which they are working. [11]. Covering a wide application field, Wireless Sensor Networks can assume an essential part by gathering encompassing setting and condition data. [1]. A remote sensor organize comprises of three significant components: sensor unit (used to take estimations), computing unit (used to process information), and correspondence unit (used to empower correspondence among the remote nodes) [16]. Additionally, it is conceivable to interface the information created by the components of a Wireless Sensor Networks (sensor nodes) with web administrations in light of SOAP and REST [2], informing components, (for example, messages and SMS) or informal organizations (e.g. Twitter) and websites (e.g. WordPress) [2]. A Wireless Sensor Network can be depicted as a system of nodes that agreeably sense and may control nature, empowering association between people or PCs and the encompassing condition [3]. The Wireless Sensor Networks are progressively being utilized as a part of the home for vitality controlling administrations. Now-a-days Individuals need to live in smart living spaces outfitted with home automation networks, these frameworks not just give them comfort, comport, security additionally lessen their day by day living expense by vitality sparing arrangements. The interest for home computerization items have been expanded quickly, which guarantee a potential market incline in close future. [5]. A smart home is a space or a room which is given the capacity to get usual independent from anyone else to specific circumstances to make the tenants feel great [15]. Smart home appliances are the combination of innovation and administrations through home organizing for computerizing, enhancing, security, wellbeing, correspondence, solace and vitality sparing. In nowadays, smart home security has been turned into an imperative issue because of high rate of violations and everyone has proposed to get sensible measures to avoid interruption [12]. Wireless Home Automation Network (WHANs) empower monitoring and, control applications for user comfort. A few associations and organizations have created WHAN arrangements as indicated by various architectures and principles [8]. Home automation and wireless monitoring of houses. For instance, Liang et al built up an arrangement of remote smart home sensor organize in view of ZigBee and PSTN (Public Switched Telephone Network) advancements. [13]. ZigBee innovation has the most reduced vitality utilization and cost. [7]. Davide Merico et al have built up the Safe and IN-Dependent living (SINDI) framework, that spotlights on checking individuals personal satisfaction and raising caution under certain therapeutic conditions. It utilizes wireless sensor networks (WSN) for information gathering, and consistent strategies for setting translation and wellbeing evaluation [10]. “Engaging WSNs in home and industrial monitoring systems, medicine and healthcare systems, entertainment, education, and so forth, has enlightened and improved the concept of modern living” [14]. To this end, in this paper, we display the plan and usage of a keen home which expects to characterize structure for remote observing and control of smart home device by means of the web. The outline depends on remote sensor network framework.

Wireless sensor networks in smart homes:

Now a day’s smart home is a dream for every individual. Smart homes are nothing but homes which are equipped with smart meters, smart appliances, smart power outlets and sensing devices which helps in designing energy efficient smart homes as shown in the figure

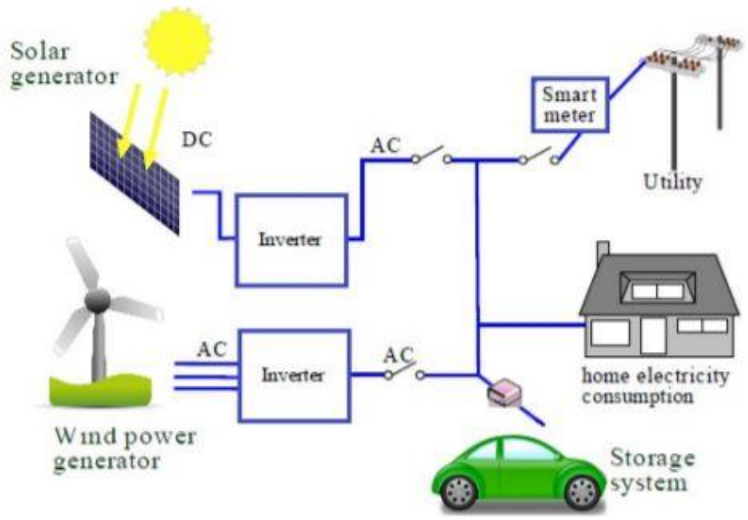

FIGURE1. Energy efficient smart homes

Wireless home automation networks(WHAN) Finds their applications in lot of ways some of the use cases are

Light control:

In WHAN light can be controlled through wireless networks which results in the reduction of need for the new wired connections.light can also be controlled remotely by using luminance sensors so that sensors detect peoples and lights starts glowing[8].

Remote control: Generally infrared technologies are used before for wireless communications in home devices such as t.v's air conditioners e.t.c,but infrared rays are only limited to shorter distances.so Radio frequecies are employed in WHAN's instead of infrared technologies which overcomes all the limitations[8]

Smart energy:

In whan's energy can be smartly and efficiently utilised by the control of HVAC(Heating,Ventilation and Air conditioning) and central heating systems.All these can be controlled by utilising the information collected by various sensors which monitors Temperature,Humidity,Light and presence of people, Hence unwanted usage of energy can be limited[8].

Health care:

Patient monitoring would be easy by the usage of wearable wireless sensors,so that the timely reports of body parameters such as temperature,blood pressure,insulin e.t.c of the patients and eledrly people who can't move can be monitored[8].

Security:

Several sensors which can detect smoke,breaking glasses, and motion are used to achieve advanced security systems,for example if there is lot of smoke in home smoke detectors alert the fire department[8].

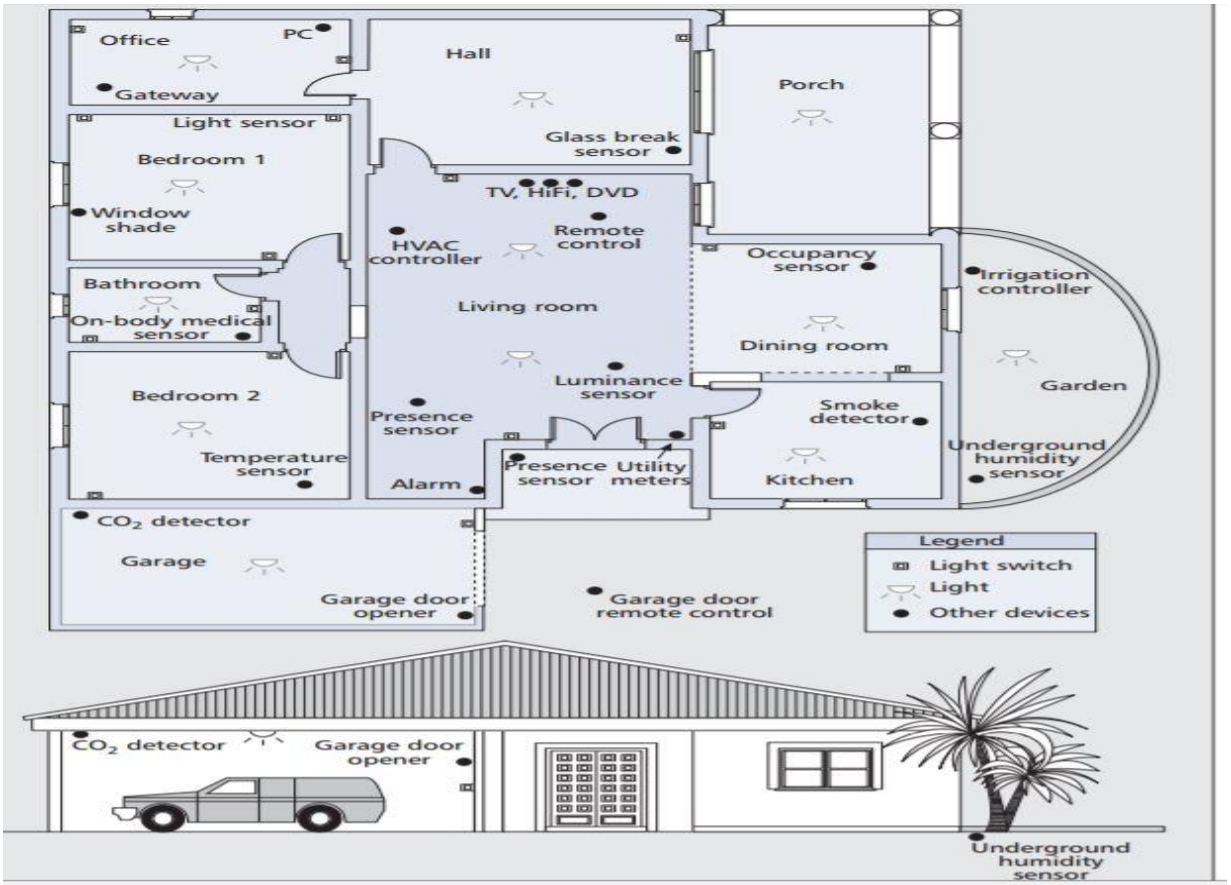

FIGURE2. WIRELESS SENSOR ENABLES SMARTHOME

Different technologies used in smart home automation using wsn:

Z-wave:

The Z-wave technology is a wireless technology which is created by Sigma Design and it advanced by the Z-wave ALLIANCE [23]. Z-wave find its fundamental usage in residential and commercial conditions. The Main Motive of the Z-Wave is to support a reliable transmission of short messages from a control unit to one or more nodes in a network [17]. The Z-Wave network works in the 900 MHz ISM band. It can help data rate to reach up to 64 kbps by utilizing Binary Frequency Shift Keying (BFSK) modulation [17].

Insteon:

Insteon is one of the Home Automation technology created by Smart Labs and advanced by the Insteon Alliance [17]. The Insteon technology works by utilizing radio frequency (RF) link and power line link [17]. The nodes inside the insteon can help either RF connections or power line cable connections. They can likewise assist both the communications. Insteon works in the 904 MHz frequency band. It can assist an data rate up to 38.4 kbps by utilizing Frequency Shift Keying (FSK) balance. Insteon technology uses a dual-mesh networking topology [17].

Waveins:

Waveins is a low power remote convention created for controlling and checking smart home appliances. It is at present overseen and advanced by Wavenis Open Standard Alliance [18]. This convention characterizes physical, link, and network layers. Wavenis services can be accessed from the upper layer through an application programming interface [17]. The working frequencies of Waveins are in the ISM Band (i.e., 433 MHz, 868 MHz, and 915 MHz in Asia, Europe, and United States individually) [17]. The most extreme information rate offered by Waveins is 100 kbps. Gaussian Frequency Shift Keying (GFSK) and Fast Frequency Hopping Spread Spectrum (FHSS) radio technologies are utilized as a part of Waveins.

Bluetooth, a standard kept up by Bluetooth Special Interest Group (SIG), basically intended for short range Personal Area Network (PAN) applications. It utilizes low power. Bluetooth utilizes Frequency Hopping Spread Spectrum (FHSS), which utilizes something like 79 frequencies amid the hopping. Bluetooth gives an approach to associate and trade data among gadgets including cell phones, phones, tablets, PCs, computerized cameras, and computer game consoles [17].

Wi-Fi:

Wi-Fi was presented by Wi-Fi Alliance [21]. The fundamental focus of Wi-Fi was to overthrow Local Area network (LAN) and thus to decrease the network operation and support costs. All

confirmed items that have a place with a wireless LAN might be associated with a Wi-Fi. The constantly dropping expense of remote chip sets for Wi-Fi network has helped this innovation to possess a mass market division of the wireless industry. The Wi-Fi technology is backward compatible and it is a global set of standard [17]. The operating range of Wi-Fi network is very limited (i.e., 32 meter indoors and 95-meter outdoors) [17]. The range of Wi-Fi system is the primary driver of its limited applications [17].

Integration of wireless sensor networks in to smart homes:

- The technology that can be used in integrating wireless sensor networks into smart homes is ZigBee. This technology is introduced by ZigBee alliance. ZigBee Technology is built on layers. This technology has unique features which results in low cost, easy implementation, low power consumption and high scale security. The ZigBee alliance built ZigBee on the top of IEEE 802.15.4 standard. This ZigBee technology is introduced in many applications such as

Industrial Automation:

Through ZigBee Technology we can assemble enterprises and control cost of correspondence. It also results in improved reliability.

Home Automation:

Similar to Industrial automation, this technology can be applied to Home automation by controlling home machines remotely such as apparatus control, warming and cooling frame work control, ventilation etc.

Smart Metering:

ZigBee remote operations can be applied to Sharp metering which include energy consumption response, estimating support, monitoring power theft issues etc.

Smart Grid monitoring:

ZigBee Technology can be applied to smart grid monitoring. It can be applied to remote temperature observing, blame finding, receptive power administration etc.

• Personal health care: Tolerant checking, Fitness observing,

• Industrial control: administration, Process control, Energy administration, Environmental,

• **Building automation:** Automatic Meter Reading (AMR), Security, HVAC, Lighting control, Access control

• **Environment:** ZigBee is used in monitoring Environment changes.

To achieve the similar benefits of ZigBee there are other technologies. Below is the comparison table of those various technologies:

Technology	Z-Wave	Insteon	Waveins	Bluetooth	WiFi	ZigBee
Frequency	868 MHz 908MH 2.4 GHz	904 MHz	433 MHz 868 MHz 915 MHz	2.4 GHz	2.4 GHz 5 GHz	868 MHz 915 MHz 2.4 GHz
Modulation	FSK/GFSK	FSK	GFSK/PSK	FHSS	QPSK COFDM QAM	BPSK O-QPSK
Error Control	CRC(8-bit)	CHECKSUM	BCH	CRC (16- bit)	CRC(32-bit)	CRC(16-bit)
Range	30-100m	45m	200-1000m	10m	100m	10m-100m
Network size	232	256	unknown	8	2007	64000
Power Consumption	Low power	NA	Ultra-low	Medium	High	Very Low

TABLE1. Comparision of Different Wireless Technologies with ZIGBEE

ZigBee:

The below figure depicts the actual process of ZigBee in home automation

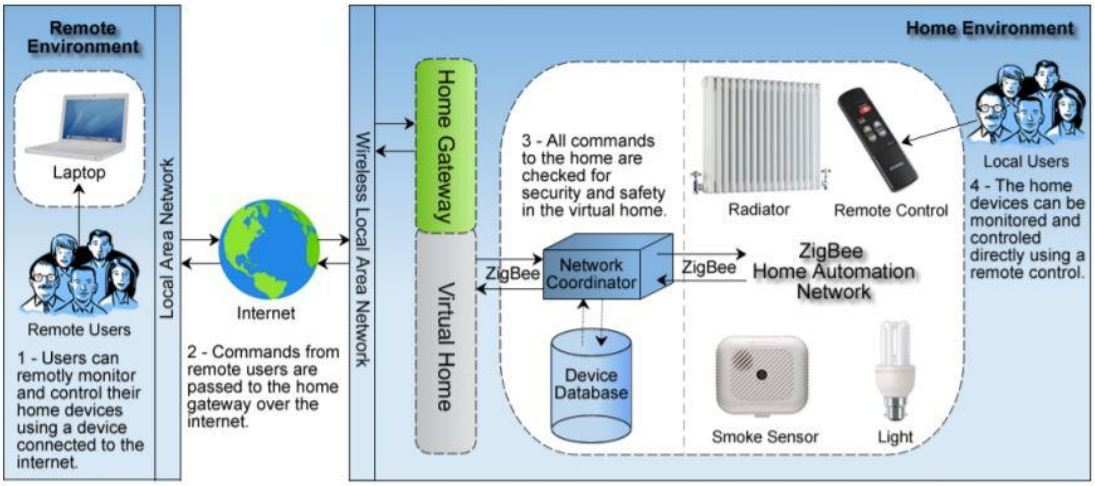

FIGURE4.Conceptual overview of ZigBee based smart home automation

ZigBee is a new technology with short distance, low complexity, low energy consumption, slow data rate and low cost. ZigBee network is built with elements such as Coordinator, routers and various end devices. Coordinator responsibility is to start the ZigBee network. Network elements to be used varies as per the application of ZigBee technology-The ZigBee technology applied in Home network includes a light switch, radiator valve, safety sensor and ZigBee remote control. Generally, ZigBee end node is integrated these end devices. Once the coordinator initiates the technology, the node scans for available channels and sends request to the network it wishes to join.

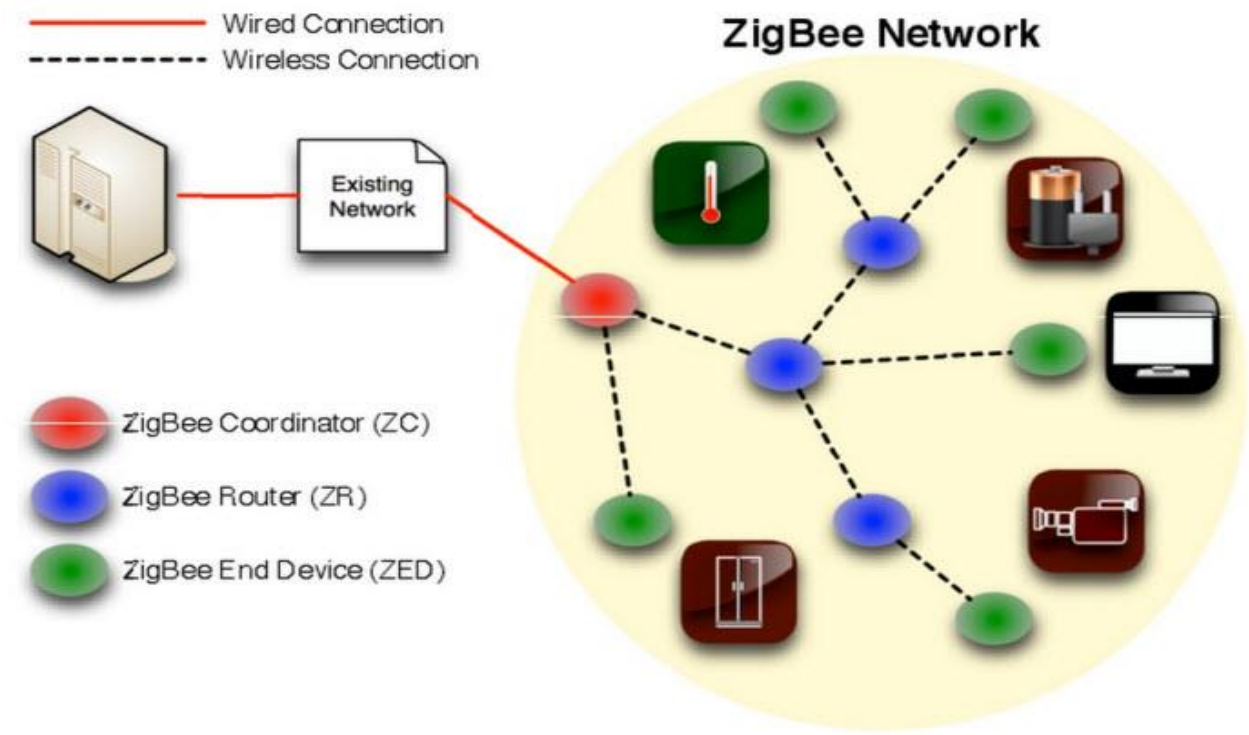

FIG5.ZIGBEE system Architecture

Once the coordinator of the receiving network receives the request, coordinator checks for the genuinity of the request initiating network [5]. ZigBee technology implementation prevents unauthorized devices to join the network. ZigBee data transmission rates vary from
Kbps in the 868MHz frequency to 250kbps in the 2.4GHz frequency. [14]. One of the ZigBee's benefits is low power consumption, it+ uses a variety of power saving modes in such a way that it could run at least from 6 months to 2 years by using 2 AA batteries. For avoiding collision mechanism ZigBee uses CSMA/CA mechanism and presets a time slot for a fixed bandwidth communications.

ZigBee protocol architecture is developed based on IEEE 802.15.4 standards. It consists of IEEE 802.15.4 physical and MAC layers while this protocol is completed by accumulating ZigBee's own network and application layers.

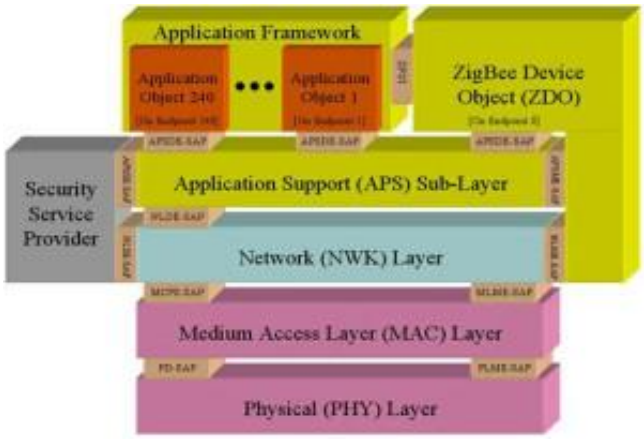

FIGURE 6. ZigBee protocol architecture

Physical Layer:

Physical layers responsibility is to modulate and demodulate operations up on transmitting and receiving signals. Below figure depicts physical layers' frequency, data rate and number of channels [21].

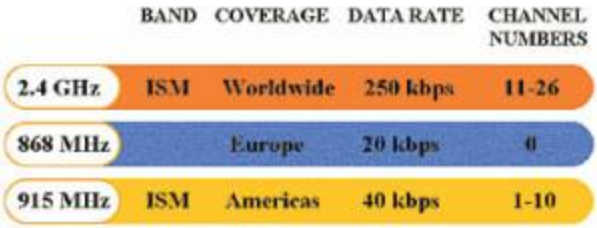

FIGURE7.Physical Layer of ZigBee Protocol

MAC Layer:

ZigBee technology uses CSMA technology to prevent collisions.MAC layers is responsible for implementing this CSMA technology and takes responsibility for reliable transmission [22].

Network Layer:

Network Layer is responsible for Network set up, Network connection initiation and Network disconnection, routing, device configurations etc[22].

Application Support Sub-Layer:

This layer enables the services necessary for ZigBee device object and application objects to interface with the network layers for data managing services. This layer is responsible for matching two devices according to their services and needs [22].

ZigBee has a lot of perspective, ZigBee might be used in a couple of years inside the area of enterprise control, industrial wireless location, domestic network, building automation, medical gadget control, mine protection, and so on, especially home automation and enterprise control can be the main application fields. ZigBee wireless communication is implemented in households. With the change in the humans' lifestyles, the idea of smart home and home automation is widely known, but it must relate to the transmission of information and signal if it comes authentic, so it's far troublesome to wire cables. [8]. As compared to working expediently for workers, it's far the maximum essential to be used in safety. introduces an experimental home security monitoring and alarming gadget based totally on ZigBee generation, it's far able to monitoring door and smoke, fuel leak, water flooding, supplying easy controls which includes turning off the valves, and sending the alarms to the residential place security community and so forth. [7].

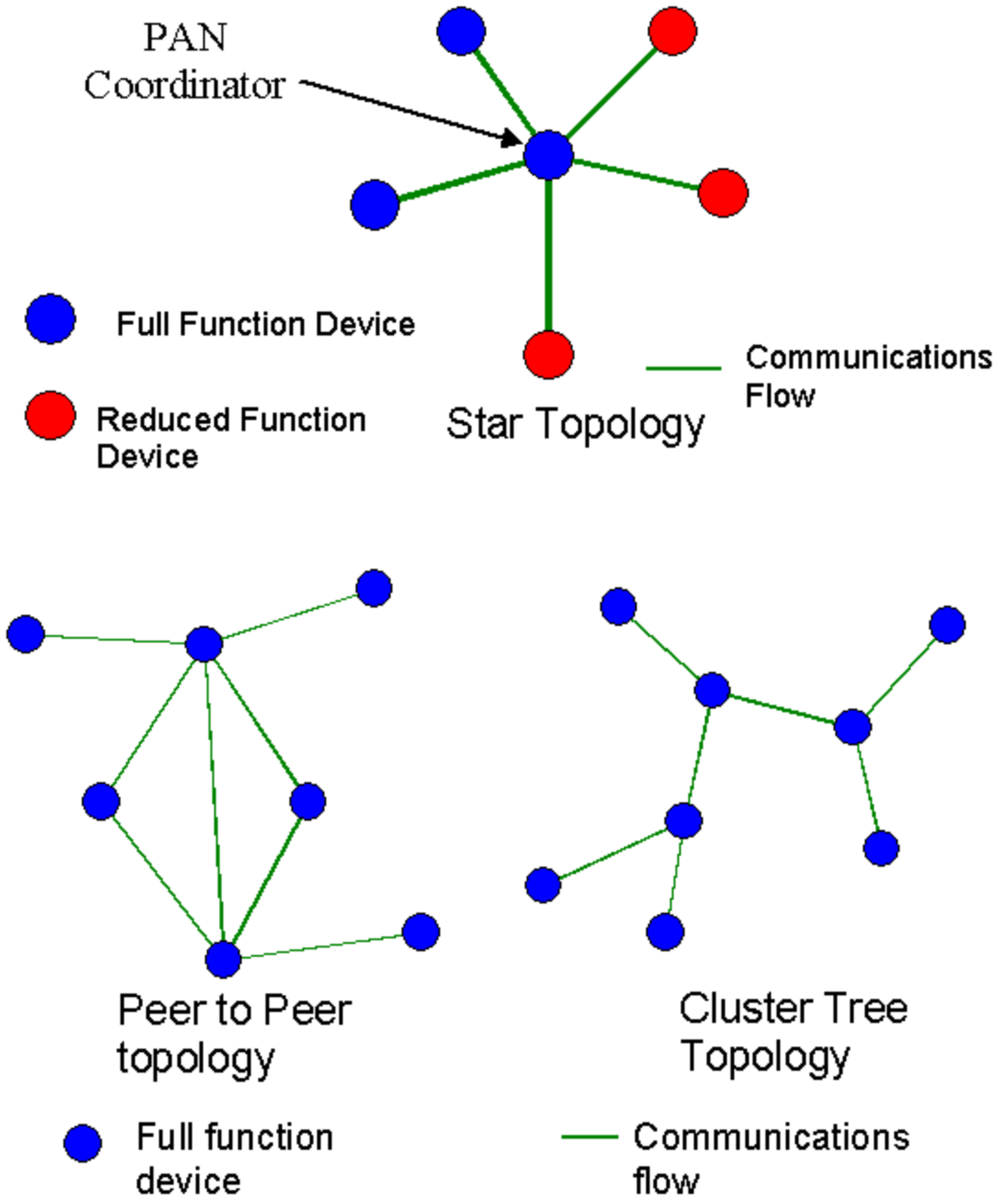

FIGURE8: ZIGBEE TOPOLOGY

* ZigBee is the key part in Baby Monitoring. (But, Spark fun's Wireless buying guide don't recommend ZigBee because of its steep learning curve.).

Comparison between ZIGBEE and WIFI:

1.IEEE Standard:

Wi-Fi has been institutionalized under IEEE 802.11.x standard. There are a few forms of the convention where x is replaced by a, b, g, n and so on which are diverse adaptations of Wi-Fi. ZigBee goes under 802.15.4 IEEE standard [5].

2. Caretaker Alliance:

Wi-Fi is overseen and its confirmation procedure is taken by Wi-Fi Alliance, a free gathering constituted by a few hardware and correspondence organizations. On comparative grounds, ZigBee additionally has a different organization together that takes of ZigBee based item advancement and affirmation forms [5].

3. **Development Timeline**:

The thought for Wi-Fi turned out as another option to straightforwardness work of cashier machines in the year 1985.A community to standardize was set up in the year 1990 which propelled the standard in the year 1997. Then again, the idea of ZigBee was considered in the year 1999, when it was found that for some long running applications, Wi-Fi and Bluetooth were not readied. It was launched in the year 2004[5].

4. Operating Frequency:

Wi-Fi is known to work at 2.4GHz, 5GHz, however there have been late improvements where Wi-Fi is working at 60GHz recurrence. ZigBee works at 900-928 MHz and 2.4GHz. Other than that ZigBee convention has a recurrence of 868 MHz for European nations [5].

5.Channel Bandwidth: The protocols using ZigBee based correspondences have a channel transfer speed of 1MHz while Wi-Fi channels have a transmission capacity of 0.3, 0.6 or 2MHz [5].

6. Network Range:

ZigBee is confined only to Wireless Personal Area Networks (WPAN) with in a range of 10-30meter in normal applications. As of late, there have been a few applications which tend to achieve 100m as far as range. Wi-Fi serves up for PAN and WLAN territory systems with a normal range between 30 to 100 meters [5].

7. Data transfer speed: We know that Wi-Fi systems, however are quicker than ZigBee regarding information exchange, which demonstrates variety as far as speed. Wi-Fi systems are characterized under 802.11b standard have most extreme information exchange speed of 11mbps while a and c adaptations have 54mbps of greatest information exchange speed. Most extreme speed in ZigBee systems is just 250kbps, genuinely low than the least Wi-Fi offers [5].

8. Bit Time: It can be characterized as time taken to transmit one bit at a given data rate of transfer. Bit time in ZigBee is 4micro seconds while in Wi-Fi it is just 0.00185 micro seconds [5].

9. Network Elements: In ZigBee technology network elements, can be classified into three types:

1. ZigBee coordinator
2. ZigBee end router
3. ZigBee end device [5].

Security requirements in IOT based Home Automation using wsn's:

Each system requires security as a typical element. As WSN's uses remote transmission so there the system to get violate by outsiders, this can posture genuine security dangers to wsn's. Security must be considered as a major aspect amongst the most critical part of any system. The accompanying are a portion of the usage required to accomplish security.

Authentication:

In IOT based application authentication is the major requirement. It helps in protecting our system from unknown users. In IOT based applications which utilize wsn's convey their information through wireless medium, so it turns out to be simple for attacker to insert threats with no effort. So, it's the duty of the end node to confirm that the data used in any basic leadership method is started from the best possible source node or not. The authentication procedure offers authorization to the end node to check whether the data was transmitted from the suitable source node [20].

Trustworthiness:

The capacity of a system to trust the identity and guarantee access for third party is known as Trustworthiness. Third party trust is a circumstance in where the source node and the destination nodes in IoT-based application trusts each other despite the fact that they have not set up correspondent ways for information transmission previously [20].

Confidentiality and Privacy:

- In WSNs, it is required to protect the original data from any statement. A WSN need not reveal the original data from source node to the neighboring or even outside systems. In IoT-based home applications, the sensor nodes collect and transmits data to the server. An attacker can eavesdrop the information transmission, and can modify critical Sensors 2017, 17, 69 5 of 19 information.

  This phenomenon can prompt serious harm since the attacker can use the captured data for various unlawful purposes. In this way, confidentiality guarantees only verified users to access the information Along with that, privacy is also an important concern. Privacy guarantees all sensor nodes in the system to fulfill the privacy policies and help them to manage their specific data [20].

Integrity:

Similar to confidentiality and privacy, integrity is additionally an essential security factor during the transmission of information in WSNs. An attacker can simply change the data by embedding a few parts of fake data inside the transmitted to change the initial message. This modified information can be sent to the destination node. In this way, integrity is an essential mechanism to protect the original data from outsider attacks [20].

Non-Repudiation:

It is the capacity of a system to approve occurrence or non-occurrence of an activity from the source nodes. In IoT-based based home automation, the source nodes need should not deny their trustworthiness when sending the messages that are originated from them [20].

Availability:

Availability is a property which allows reliable access to system resources time to time to valid sensor nodes in a network. In IoT-based applications, it is extremely fundamental that network resources need to be accessible to the suitable nodes [20].

Access Control:

To keep away from attackers, it is very essential to recognize every client and every device in order to enforce security policies .noncompliant sensor nodes within the network need to be blocked or given only limited access. This process is known as network access control (NAC). To develop a secured IoT-based system, it is extremely crucial that the system should fulfill all the above-mentioned security requirements that could oppose different security attacks like replaying, data modification, impersonation, and eavesdropping among others.

Along these lines, noncompliant sensor nodes inside the network should be blocked or given limited access. This procedure is known as network access control (NAC). To build up a secured IoT-based system, it is very crucial that the system need to satisfy all the previously mentioned security prerequisites that could restrict distinctive security attacks like replaying, data modification, impersonation, and eavesdropping among others [20].

Conclusion:

In this paper the wireless sensor networks are used to control the appliances in a smart home. Applications and use cases of wsn's in smart homes are discussed. we provided an overview of all wireless technologies such as Z-wave, Waveins, Wi-Fi, ZigBee. The main features of the ZigBee technology have been highlighted in this paper. Comparison between Wi-Fi and ZigBee has been done in this paper, some limitations and challenges of the ZigBee based WirelessHomeAutomationSystem have also been listed in this paper. Moreover, security challenges regarding wsn's and smart home automation are discussed in this paper.

References:

[1] D. Christin, A. Reinhardt, P. S. Mogre, and R. Steinmetz, "Wireless Sensor Networks and the Internet of Things: Selected Challenges," *Multimedia Communications Lab, Technische Universitat Darmstadt ¨ Merckstr. 25, 64283 Darmstadt, Germany*.

[2] C. Alcaraz, P. Najera, J. Lopez, and R. Roman, "Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?," *Computer Science Department University of Malaga Malaga, Spain*.

[3] "Internet of Things: Wireless Sensor Networks," *IEC*.

[4]H. Ghayvat, S. Mukhopadhyay, X. Gui, and N. Suryadevara, "WSN- and IOT-Based Smart Homes and Their Extension to Smart Buildings," *Sensors*, vol. 15, no. 5, pp. 10350–10379, Apr. 2015.

[5] Ashwini.R and Mrs. Pooja Mohnani , "Application of Wireless Sensor Network in Home Automation," *International Journal of Computer & Organization Trends – Volume 9 Number 1 – Jun 2014*.

[6] USHAA ESWARAN and RAJITH R, "REAL TIME HOME AUTOMATION SYSTEM USING WSN WITH POWER OPTIMIZATION," *i-manager's Journal on Instrumentation & Control Engineering, Vol. 4 lNo. 3lMay - July 2016*.

[7] Aamir Shaikh and Siraj Pathan, "Research on Wireless Sensor Network Technology," *International Journal of Information and Education Technology, Vol. 2, No. 5, October 2012*.

[8] C. Gomez and J. Paradells, "Wireless home automation networks: A survey of architectures and technologies," *IEEE Communications Magazine*, vol. 48, no. 6, pp. 92–101, 2010.

[9] A. Bagula, "Applications of Wireless Sensor Networks," *Wireless Sensor Networks*.

[10] D. Basu, G. Moretti, G. S. Gupta, and S. Marsland, "Wireless sensor network based smart home: Sensor selection, deployment and monitoring," *2013 IEEE Sensors Applications Symposium Proceedings*, 2013.

[11] PRODROMOS-VASILEIOS MEKIKIS, "Design and Implementation of a Wireless Sensor Network for Smart Home Applications," *KTH electrical engineering*.

[12] F. Kausar, "Intelligent Home Monitoring Using RSSI in Wireless Sensor Networks," *International journal of Computer Networks & Communications*, vol. 4, no. 6, pp. 33–46, 2012.

[13] M. Xu, L. Ma, F. Xia, T. Yuan, J. Qian, and M. Shao, "Design and Implementation of a Wireless Sensor Network for Smart Homes," *2010 7th International Conference on Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing*, 2010.

[14] B. R. Stojkoska, A. P. Avramova, and P. Chatzimisios, "Application of Wireless Sensor Networks for Indoor Temperature Regulation," *International Journal of Distributed Sensor Networks*, vol. 10, no. 5, p. 502419, Aug. 2014.

[15] B. Jayashri and S. Arvind, "Energy efficient Smart home based on Wireless Sensor Network using LabVIEW," *American Journal of Engineering Research (AJER) e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-02, Issue-12, pp-409-413*.

[16]

[17] T. Obaid, H. Rashed, A. A. -Elnour, M. Rehan, M. M. Saleh, and M. Tarique, "Zigbee Technology and its Application in Wireless Home Automation Systems: A Survey," *International journal of Computer Networks & Communications*, vol. 6, no. 4, pp. 115–131, 2014.

[18] M. VARCHOLA and M. DRUTAROVSKÝ, "ZIGBEE BASED HOME AUTOMATION WIRELESS SENSOR NETWORK," *Acta Electrotechnica et Informatica No. 4, Vol. 7, 2007* .

http://www.radiocomms.com.au/products/42985-Wavenis-Open-Standard-Alliance

[19] Ahmed ElShafee and Karim Alaa Hamed "Design and Implementation of a WiFi Based Home Automation System," *World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:6, No:8, 2012* .

[20] PIRBHULAL, S., ZHANG, H., E ALAHI, M., GHAYVAT, H., MUKHOPADHYAY, S., ZHANG, Y. AND WU, W., "A Novel Secure IoT-Based Smart Home Automation System Using a Wireless Sensor Network," *Sensors*, vol. 17, no. 1, p. 69, 2016.

[21] https://www.wi-fi.org/

[22] https://www.elprocus.com/what-is-zigbee-technology-architecture-and-its-applications/)

[23] The Z-Wave technology available at http://www.z-wavealliance.org/technology