International Journal on Emerging Technologies **11**(3): 1015-1021(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

A Comparative Survey on Wireless Sensor Networks based Internet of Things (IoT)

***Akansha Sarad*[1]*, Apurv Verma*[2] *and Abhishek Badholia*[3]**
[1]Research Scholar, Department of Computer Science & Engineering,
School of Engineering & IT, MATS University, Raipur, Chhattisgarh, India.
[2]Assistant Professor, Department of Computer Science & Engineering,
School of Engineering & IT, MATS University, Raipur, Chhattisgarh, India.
[3]Associate Professor, Department of Computer Science & Engineering,
School of Engineering & IT, MATS University, Raipur, Chhattisgarh, India.

(Corresponding author: Akansha Sarad)

(Received 23 March 2020, Revised 16 May 2020, Accepted 18 May 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Internet of Things has been evolving at a much faster pace from the past few years, as it is being one of the most funded research areas. The development of varied sorts of wireless sensor networks and therefore the requirement of their being interconnected led to the event of the Internet of Things. This work provides an insight of varied Wireless Sensor Networks whose protocols and architecture forms a boon to the event of the existing Internet of Things. This study discusses Wireless HART, ZigBee, and ISA.100 which are some of these communication standards. Further, the purpose of the study is to represent a discussion of contrast and similarities of the Internet of Things (IoT) with the most effective wireless sensor networks. The comparison is made based on different work accomplished by different researchers in the field of the Internet of things. In this, application requirements such as quality of service, security, scalability etc. for WSN and IOT are compared.

Keywords: IoT; WSN Standards; Wireless HART; ZigBee; ISA 100.

Abbreviations: IoT, Internet of Things; *WSN*, Wireless Sensor Networks; ISO, International Standardization Organization; AODV, Ad-hoc On Demand Distance Vector; FHSS, Frequency Hopping Spread Spectrum ; CCA, Clear Channel Assessment; FFD, Full Function Devices; RFD, Reduced Function Devices; GTS, Guaranteed Slot Time; ISA, Instrumentation, Systems, and Automation Society; DSSS, Direct Sequence Spread Spectrum; TDMA, Time-Division Multiple Access; CSS, Chrip Spread Spectrum; EDRS, Energy-efficient Distributed Retransmission Selection.

I. INTRODUCTION

The International Standardization Organization (ISO) defines a sensor network as a system of distributed sensor nodes interacting with each other *et al.* environments to accumulate, process, transfer, and supply information extracted from the physical world [1]. These networks were developed to usher in control mechanisms and automation to Industries [2], Medical [3], Home, and Agriculture [4] and various other automation operations. WSNs (Wireless Sensor Network's) are a group of spatially distributed autonomous devices wont to collect data employing a wireless medium and should cooperatively control and monitor environmental or physical conditions, like sound, pressure, temperature, vibration, pollutants, or motion at different locations [5]. Most Internationally Standardized Wireless Networks like ZigBee, WirelessHART, and ISA.100 follow a stacked structure to supply a layered architecture with abstract description for implementation of protocols [6]. The need for Sensor Networks to be far-remotely controlled drove the event of the Internet of Things (IoT). Internet of Things (IoT) defined as the interconnection of physical and virtual things referred to as Nodes to make a worldwide infrastructure for the knowledge society supported existing and evolving interoperable information and communication technologies for enabling advanced services [7]. WSN's formed a boon to the event of the Internet of Things (IoTs) as IoT needed an architecture that could enter lieu with the architecture of existing computing, and communication technologies. IoT as if a way advancement of WSNs in terms of computing, controlling and communicating capabilities could use the prevailing stacked-layer architecture of varied internationally accepted Wireless Network Standards to implement its physical connectivity and routing functionalities. This study would be useful for developing the basic application requirements for the IoT as it is becoming a specific area of research of interest for WSN. There are only a few researchers who work on the field of internet of things and still, research work is going on to improve the quality standards and design requirements of IoT. Hence, this paper is tried to initiate the consideration factors which should be adopted to design and analyze the Internet of things based on wireless sensor networks. The rest of the paper is arranged as follows: section II describes the WSN standard of WirelessHART, Zigbee, and ISA.100 networks and compares them on different feature sets. Section III and IV gives an overview of the internet of things and related works done by different authors till the year 2019. Section V and VI summarized the discussion and future work of the study.

II. WSN STANDARDS

There are a number of ordinary Wireless Sensor Networks architectures, which are further classified by versions of amendments and upgrades. The various parameters for consideration for his or her use and discussion are latency, wireless transmission range; sensor data update rates, power consumption, reliability, environment efficiency. A general discussion of most prominent WSN Standards is as follows.

A. WirelessHART

WirelessHART operates in 2.4GHz ISM radio. It a mesh networking technology uses IEEE 802.15.4 compatible DSSS radios and supports channel hopping on a packet basis. The quality is backward compatible with its core wired technology - HART. WirelessHART optimizes all the 16 channels of the IEEE802.15.4 standard by employing Frequency Hopping Spread Spectrum (FHSS). Its optional feature of CCA (Clear Channel Assessment) is an optional feature in WirelessHART which will be performed before transmitting a message [8]. Another feature of WirelessHART is transmitting power, which disallows the use of few channels termed as Blacklisting. This feature prevents other co-existing real-time constrained wireless systems from interfering with WirelessHART [9].

1. Technology: All WirelessHART devices have the capability of routing [9]. WirelessHART has two routing schemes, Graph routing, and Source routing. Source routing is employed for network diagnostics because it uses ad-hoc created routes and has no diverse paths. Graph routing is employed for message transmission and uses pre-determined paths to send messages. Key components of WirelessHART architecture are:

•Gateway – The device which connects the sensor network to its host network. The interface between WirelessHART and therefore the main is using Modbus - Profibus - Ethernet. The Gateway device provides the safety and network manager [10].

•Network Manager – The mesh networking is implemented by Network Manager. Its role is to spot the simplest paths and manage the distribution of your time slots access (Each squeeze WirelessHART is of 10msec) Slot access depends upon the specified process value refresh rate and other access [10].

•Security Manager – It distributes keys for security encryption. It also manages device authorization [10].

•Repeater – It is wont to extend the range of a network. It routes WirelessHART messages and should not have any process connection of its own. All WirelessHART network is capable of routing [11].

•Adapter – It is wont to pass data to the host, during a WirelessHART network by plugging into an existing HART-enabled instrument. The adapter might be located anywhere along the instrument 4-20Ma cable. it's either battery-powered or obtains its power from the 4-20Ma cable. [11].

•Terminal – It connects the gateway and an instrument that will be used for diagnostics. It's wont to join a replacement instrument to an existing WirelessHART network [11].

2. Security: WirelessHART implements security as mandatory and provides hop-to-hop and end-to-end security. Security is implemented by encoding and message authentication in Data-link and Network layers using AES-128 block cipher symmetric keys [9]. A group of security keys is wont to provision the joining of the latest devices, which are generated and managed by the Security manager [9]. The network manager provides network and session keys for further communication. Session keys provide end-to-end authentication and network keys provide hop-to-hop authentication [9].

B. ZigBee

ZigBee standard is maintained by a gaggle of companies referred to as ZigBee Alliance. ZigBee standard specifications are a set of high-level communication protocols using IEEE based low power radios. ZigBee is beneficial for the low rate, low power, and secure network RF applications.

1. Technology: ZigBee uses the 802.15.4 protocol which is predicated on the ad-hoc on-demand distance vector algorithm (AODV). This protocol is liable for peer-to-peer communication thus making routing and discovery possible [12]. ZigBee network supports mesh with all devices connected using the same frequency channel as no frequency hopping is out there [9]. ZigBee devices are classified as FFD (Full Function Devices) and RFD (Reduced Function Devices). An FFD can connect to a different full FFD using any networking topology whereas an RFD connects to an FFD only. Zigbee operates in two modes- Beaconed and Non-beaconed. Beaconed mode has all nodes synchronized. A superframe in beaconed mode is split into 16 slots, having an option of using seven dedicated slots out of those for creating communication more deterministic and it's called GTS (Guaranteed Slot Time) [9]. Zigbee devices are classified as:

•***Coordinator –*** Starts and controls the network. This device has all the knowledge of the network and it acts as a Trust Centre and security keys repository [13].

• ***Router –*** Connects coordinator other routers and end devices. It extends the network coverage area and routes data around obstacles. It also manages backup routes just in case of device failure or network congestion [13].

• ***End Device –*** These are mainly sensor/actuator nodes, which receive or transmit data (messages) but don't perform any routing functionality [13]. An End Device must necessarily hook up with either a coordinator or a router.

2. Security: ZigBee can use all the safety mechanisms available in IEEE 802.15.4, but security isn't mandatory. ZigBee has support for integrity and authentication. ZigBee uses CBC-MAC (CCM) with AES-128 encryption. Zigbee provides an option for implementing integrity only or encryption only but MAC layer security is implicitly addressed by 802.15.4 [14]. ZigBee security is implemented by three sorts of keys: passkey, Network key, and Link key. Passkey is for joining the network and Link keys for end-to-end encryption, which provides the highest level of security but requires higher storage requirements. Network keys provide low-security levels but use less storage requirements and are shared between all devices [14]. Zigbee uses sequential numbering techniques to guard devices from Replay attacks [9].

C. ISA.100

Instrumentation, Systems, and Automation Society (ISA) proposed ISA.100 WSN standard for automation and control of industries, aimed to integrate wireless infrastructure platform for industries [15]. ISA.100 adheres to its coexistence strategy providing “the ability of wireless networks to perform their tasks in an environment where there are other wireless networks which will or might not be supported an equivalent standard" [16]. The physical span of ISA.100 networks can extend over a neighborhood of multi-sq.-km plant and every network can have thousands of devices [16].

1. Technology: ISA.100 works on TDMA mechanism and supports channel hopping to avoid interference from other devices [15]. ISA.100 uses 6LoWPAN compatible header formats in the network layer and thus making it different from the remainder of Wireless Sensor Networks. ISA.100 supports end-to-end reliability and is self-healing and fully redundant [15].

2. Security: ISA.100 implements security by policies, which are distributed with each cryptographic material. Change the default, adjust the template as follows. A subnetwork uses the same policies at the link layer and one key's used at a time, apart from a quick period of key handover [15]. ISA.100 provides security against major industrial threats by leveraging IEEE 802.15.4-2006 security thus simple flexible and scalable [17]. This architecture uses both symmetric and asymmetric key variants with session keys having a time-bound periodic updating. A tool initiates a key updating process and is pushed by the security manager to make sure a session is kept alive [18].

A featured listing of the above discussed Wireless Network Standards is providing in Table 1, to summarize:

Table 1: Feature Set of Wireless Networks.

Feature Set	Zig Bee	WirelessHART	ISA 1OO
Topology	Mesh	Mesh, Star, Combined, Mesh and Star	Mesh, Star, combined, Mesh and Star
Scalability	Yes	Yes	Yes
Radio Channel	CSMA-CD	TDMA	TDMA/CDMA
RF Channel Change	Yes	Yes	Yes
Keys	Symmetric	Symmetric	Symmetric/ Asymmetric
Interface Control/ Noise	Yes	Yes	Yes
Interoperability to other Systems	Yes	Yes	Yes
Application Context	Commercial	Industrial	Industrial
Reliability Determinism	No	Yes	Yes
Latency Determinism	No	Yes	Yes
Implementation	Easy	Challenging	Challenging

III. INTERNET OF THINGS

Internet of Things marks the third age of the Internet with the first two being characterized as connecting people through personal computers and mobile devices to the Internet and this age of Internet demands connecting of objects additionally to people [19]. The age of IoT thus involves the instrumentation of real-world objects. These objects referred to as things, belonging to the real/physical world make use of existing and new demanded technology to link to cyberspace [20]. Internet of Things may be a much bigger domain in comparison to Wireless Sensor networks because it encompasses not only sensing but also involves of computing at the sensor node and more thereto, it's an honest number of processes to be carried at application layer [24], which is to form it internet-oriented and thus puts it at a way greater advantage of operation than Wireless Sensor Networks.

A. Technology

An IoT system is to facilitate five processes- Sensing, Identification, Actuation, Communication, and Management [21]. These processes are facilitated by the following functional blocks:

• ***Device*** – is to supply sensing, actuation, control, and monitoring activities. An IoT device is involved in the processing of knowledge and transmitting of knowledge and should contain several communication interfaces [22].

•***Communication–*** This block performs the communication between devices and remote servers. There are several protocols functional at various layers link, Network, and Application Layers of various IoT models [22].

•***Service –*** An IoT system serves various sorts of services for device modeling, device control, data publishing and data security [22].

•***Management –*** This block is to supply different functioning to control an IoT system.

• ***Security –*** concerns of IoT system are authentication, authorization, privacy, message integrity, content integrity and data security [22].

• ***Application Layer –*** it's the foremost important layer in the user’s terms because it acts as an interface to regulate and monitor.

An IoT system could also be characterized as dynamic and self- adapting, self-configuring, interoperable communication protocols, unique identity, integrated into information networks, context-aware [23], and intelligent deciding capable [21]. IoT system requires a spread of hardware platforms for his or her operation like Processors, Memories EEPROMs, I/O connectivity with specific characteristics of low power and low resource and are compatible with numerous wireless communication protocols – Wi-Fi (802.11), WiMAX (802.16), LR-WAN (802.15.4), Mobile Communication (2G/3G/4G), Low Power Bluetooth (802.15.1) and LoRAWAN (R1.0 – LoRa). An IoT system could also be capable of providing a cloud-based solution thus integrating to cloud and use platform and application as services thereto. The IoT system employs numerous architecture and most of them are service-oriented architectures. ITU has defined a five-layer architecture referred to as IEEE P2413 architecture and has applicability to protocols IEEE 802.15.4, LoWPAN, and ROLL at its Networking and link layer and COAP, DTLS, MQTT and XMPP at its application layer [24].

B. Security

Internet of Things (IoT) supports a varied number of architectures and even a specific architecture may then vary in the implementation of various protocols at various layers. Thus, the safety of an IoT system may vary as per its architecture and protocols implemented. Security at various layers of ITU standardized architecture could also be considered for generalized discussion. At the physical layer, IEEE 802.15.4 protocol, which works at 2.4GHz band supports 16 channels, employs Direct Sequence Spread Spectrum (DSSS), Direct Sequence Ultra-Wideband (UWB) and Chrip Spread Spectrum (CSS) for low power transmission, and thus implements no specific security mechanism of encryption [24]. At the MAC layer, an equivalent protocol uses the IEEE EUI-64 identifier or 16-bit short identifier for identification of devices and employs AES-CBC- MAC32/64/128 encryption standards for data authentication [24]. Confidentiality is provided by using AES_CTR security mode which is optional to be used. It's also support for Replay attack protection [24]. IETF 6LoWPAN as an internet-connected standard has no security implementation as in itself but devices employing different communication protocols offer various security approaches [25]. At the Application layer, CoAP (Constrained Application Protocol) supports PreSharedKey, RawPublicKey, and Certificate Security mode [24].

IV. SOME OTHER WORKS ON IOT

This Mohamed Riduan Abid *et al.*, [27] presented the architecture of a real test bank for smart micro-networks to be distributed on a university campus. They highlighted their main components with an emphasis on the ICT component. They presented that SG will use the Internet of Things (IoT) to get all kinds of data and, in this way, bring the whole system into the Big Data field. To manage the large amount of data that will be collected, they recommended the implementation of a private local cloud using an open-source platform for High Performance Computing (HPC) along with Hadoop/MapReduce as an underlying model of data storage and processing. They considered that this project is an ideal model that can be easily adapted for similar testbeds of the intelligent micro-network in the real world in Africa and the world.

Andrea Zanella *et al.*, [28] specifically focused on urban IoT systems which, despite being a fairly large category, are characterized by their specific application domain. Urban IoT is designed to support the vision of Smart City, which aims to exploit the most advanced communication technologies to support value-added services for city administration and citizens. Therefore, this document provides a complete overview of enabling technologies, protocols, and architecture for an urban IoT. Also besides, the document will present and discuss the technical solutions and best practices adopted in the Smart City project in Padua, a proof-of-concept demonstration of an IoT island in the city of Padua, realized in collaboration with the city council.

Ala Al-Fuqaha *et al.,* [29] provides an overview of the Internet of Things (IoT) with emphasis on enabling technologies, protocols and application problems. The IoT is enabled by the latest developments in RFID, smart sensors, communication technologies, and Internet protocols. The basic premise is that intelligent sensors collaborate directly without human participation to offer a new class of applications. The current revolution in Internet technologies, mobile devices, and machine to machine (M2M) can be seen as the first phase of the IoT. In the coming years, the IoT should connect various technologies to enable new applications by linking physical objects to support intelligent decision-making. This document begins by providing a horizontal overview of the IoT. Then, they provide a general description of some technical details that belong to the IoT's technologies, protocols and enabling applications. Compared to other fieldwork surveys, its purpose is to provide a more complete summary of the most relevant protocols and application problems to allow researchers and application developers to quickly understand how different protocols are combined to provide the desired functionality without having to go through the RFCs and the specifications of the standards. They also provide an overview of some of the main IoT challenges presented in the recent literature and provide a summary of related research work. Also besides, they explore the relationship between IoT and other emerging technologies, including big data analysis and cloud computing and cloud computing. They also present the need for better horizontal integration between IoT services. Finally, they present detailed cases of use of the service to illustrate how the different protocols presented in the document are adapted to offer the desired IoT services.

John A. Stankovic [30], many technical communities are actively looking for research topics that contribute to the Internet of Things (IoT). Nowadays, when the detection, action, communication, and control become even more sophisticated and omnipresent, there is a significant overlap in these communities, sometimes from slightly different perspectives. Greater cooperation between communities is encouraged. To provide a basis for the discussion of open research problems in the IoT, a vision of how the IoT could change the world in the distant future is presented for the first time. Then, eight key search topics are listed and search problems are discussed within these topics.

Wu He *et al.*, [31], introduced an innovative multilayer data platform for vehicles through the use of cloud computing and IoT technologies. There are also two innovative services offered in the vehicle data cloud, an intelligent cloud parking service, and a data mining cloud service for vehicle assurance analysis in the IoT environment. Two modified mining models are presented in detail for the vehicle data mining cloud service, a Naïve Bayes model, and a logistic regression model. Challenges and instructions for future work are also provided.

Muhammad Abrar *et al.,* [32], in research work, a device is installed between users of mobile phones and devices that will act as gateways between the two. To communicate, the devices must overcome different quality limits of service and system conditions. We have proposed a bidirectional approach. The first devices must become candidates for re-use by the mobile user, so the optimal resource allocation method will be used. In the optimal resource allocation method, the maximum bipartite coincidence graph theory is used. The results of the simulation showed the validity of the system.

Prianka Agrawal; Gaurav Chitranshi [33] presented the Web server design using the ATmega328 based Internet and the W5100 Shield Shield Ethernet chip with some I / O devices. To create an HTML Web page for which a server-side IP address is required. enter your browser as an Internet browser, Firefox and Google Chrome on the client-side. The input/output devices are LM35 temperature sensors, rain sensors, BMP180 pressure. The conditions of temperature, pressure, altitude, and precipitation are controlled and a system is developed and tested in which, in emergencies, different devices are controlled in real-time.

The communicative gap between teachers and students is one of the predominant factors for students' lower grades. There are cases in which students are unaware of the allocation periods and tests that lead to degrading scores. To fill this gap, the Internet of Things (IoT) can be used to provide academic information about students. This feature would help achieve the goal of verbal zero communication between the student and the teacher. The teacher can load tasks and deadlines that will be retrieved from the mobile phone when the student enters the range of the device. To achieve this, they used Beacon technology, which allows mobile applications to listen to beacon signals in the physical world and react accordingly. The strategic and creative implementation of location-based technology has great potential to reduce the hassles a student faces. They aim to use IoT in the field of education to reduce communication barriers in the student-teacher relationship [34].

Adi Candra Swastika *et al.*, [35] - proposed the design of an intelligent network system based on IoT for the smart home. The architecture of the proposed protocols to be used, the functioning of the system, and the challenge in the design of the system are analyzed in such a way that the proposed design can improve the optimization of the Smart system itself.

Sheikh Tahir Bakhsh [36] is proposed, an energy-efficient distributed retransmission selection (EDRS) technique for multi-use WSN networks. Power consumption is reduced by selecting a stable relay and an influence assignment for collaboration. Additionally, the EDRS proposal selects a relay node with optimal power levels to increase the lifetime of the network. The results of the simulation show that EDRS reduces energy consumption and increases the useful lifetime of the network.

Abdul Salam *et al.*, [38] presented an IoT technology research and innovation roadmap for the field of precision agriculture (PA). Many recent practical trends and the challenges have been highlighted. Some important objectives for integrated technology research and education in precision agriculture are described. Effective IoT based communications and sensing approaches to mitigate challenges in the area of precision agriculture are presented.

The basic underlying workflow of IoT is discussed and the architecture of IoT is explained. The paper also highlights the most useful technologies of these days, which employ IoT for their functioning. Further, the applications and features of IoT are mentioned in the paper. Lastly, the issues and challenges in implementing the IoT are briefly discussed [39].

Luca Turchet *et al.,* [40], reviewed the state of the art of this field, then presented a vision for the IoAuT and its motivations. In the proposed vision, the IoAuT enables the connection of digital and physical domains using appropriate information and communication technologies, fostering novel applications and services based on auditory information. The ecosystems associated with the IoAuT include interoperable devices and services that connect humans and machines to support human-human and human-machine interactions. They discussed the challenges and implications of this field, which lead to future research directions on the topics of privacy, security, design of Audio Things, and methods for the analysis and representation of audio-related information.

V. CONCLUSION

Internet of Things is integrating a variety of technologies with primitive being sensor networks. However, a sensor node as in WSN isn't almost like one utilized in IoT node [26, 27]. IoT nodes use edge computing, which involves the processing of knowledge at the node itself. IoT nodes are much different in terms of computational capabilities to a WSN device. There exists a standard feature set about communication technology between IoT and WSN as most of WSN communication standards like IEEE 802.14.5, LoRa, and BLE (Bluetooth Low Energy) are actively used for communication in various IoT architectures. Still, WSN in contrast to IoT, doesn't specify an immediate connection of the sensor nodes to the web for sensing and data collection. There are certain parameters we will concede to discuss IoT and WSN taking in regard to WSN as a subdomain or primitive of IoT. Application requirements of both are compared within the table given below:

Table 2: Comparison of WSN and IoT.

Requirement	WSN	IoT
Security and Privacy	Medium	High
Robustness	High	High
Scalability	Medium	High
Quality of Service	Medium	High
Heterogeneity	Medium	High
Deployment and Coverage	High	Null
Mobility	Medium	High
Power/Energy Management	High	Medium
Identification of Things	Null	High
Autonomy	High	High
Data Processing	Null	High
Communication and Internet Connection	High	High

VI. FUTURE SCOPE

The technological discussion of the Internet of Things would require mentioning the protocols at various layers, their function, and interaction with hardware but it might be not in lieu with contrast to Wireless Sensor Networks. The appliance layer of wireless sensor networks doesn't require the info to be processed for Internet Protocol and doesn't include those specifications and modularities required to form the process of data at the Networking or Application layer to satisfy specifications of existing Internet architecture.

The scope of this work intends to form a comparative of Wireless Sensor Networks and Internet of Things, thus discussion of only those technological and security parameters has been made, which might provide relative information of the 2 technologies. This work presents an idea of Wireless Sensor Networks by discussing the most prominent Wireless Standards and discusses about the Internet of Things in similar terminology to present awareness of similarities and therefore the differences between them. WSN and IoT are two fields of study with both having its origins common to computer networks and Machine to Machine Communications. However, both of them have a special approach to practice. It's concluded from the above discussion that IoT integrates several technologies that exist already with WSN together of them. Further, its worth saying that IoT and WSN have similar application requirements but the degree of relevance is different. WSN on one end focuses on the management of limited resources whereas, on the opposite security, assurance, scalability, and heterogeneity are of equal concern in the Internet of Things.

ACKNOWLEDGEMENTS

The author thanks the other professors and friends of the college who help in planning, implementing, and developing the research work on wireless senor network-based internet of things.

Conflict of Interest. No.

REFERENCES

[1]. Vidyasagar Potdar ; Atif Sharif ; Elizabeth Chang, (2009). Wireless Sensor Networks: A Survey. IEEE transactions on *International Conference on Advanced Information Networking and Applications Workshops*, Bradford, 636-641.

[2]. Kruger, C.P. & Hancke, G.P. (2014). Implementing the Internet of Things vision in industrial wireless sensor networks.*12th IEEE International Conference on Industrial Informatics*, 627-632.

[3]. Hu, Fang & Xie, Dan & Shen, Shaowu. (2013). On the Application of the Internet of Things in the Field of Medical and Health Care. *IEEE International Conference on Cyber, Physical and Social Computing*, 2053-2058.

[4]. Zhang, F (2013).Research on applications of Internet of Things in agriculture. In Informatics and Management Science VI; Springer: London, UK, 69–75.

[5]. Zhang, Junqi & Varadharajan, Vijay, (2008). A New Security Scheme for Wireless Sensor Networks. *IEEE Proceedings of the Global Communications Conference*, Globecom, pp-128-132.

[6]. "WSN Security Project Overview and Scope-Internal Statoil Document " Statoil 2009.

[7]. "Recommendation ITU-T Y.2060 (06/2012)," 2012.

[8]. Du, Wenliang & Deng, Jing & Han, Young-Soo & Chen, Shigang & Varshney, P.K. (2004).A key management scheme for wireless sensor networks using deployment knowledge. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM, Volume: 1, pp-597.

[9]. Lennvall, T., Svensson, S., and Hekland, F. (2008) A comparison of WirelessHART and Zig-Bee for industrial applications. Proceedings of the IEEE International Workshop Factory Communication Systems, pp. 85-88.

[10]. "HART Communication Foundation," https://fieldcommgroup.org/

[11]. "The Components of WirelessHART Technology": https://fieldcommgroup.org/technologies/hart/hart-technology

[12]. Song, Tian-Wen & Yang, Chu-Sing, (2008). A Connectivity Improving Mechanism for ZigBee Wireless Sensor Networks. IEEE/IPIP International Conference on Embedded and Ubiquitous Computing (EUC 2008), Shanghai, China, *2*, pp- 495-500.

[13]. "Getting Started with ZigBee and IEEE 802.15.4," Daintree Networks, 2008.

[14]. Sun, Jing & Zhang, Xiaofen, (2009). Study of ZigBee Wireless Mesh Networks. DBLP Proceedings, 9th International Conference on Hybrid Intelligent Systems, HIS, 264-267.

[15]. "ISA 100: Wireless Systems for Industrial Automation-Developing a Reliable, Universal Family of Wireless Standards," ISA, Standard 2007.

[16]. "ISA I 00.11 a Release I Status," ISA 2008.

[17]. "ISA-I 00.11 a-2009 Wireless systems for industrial automation: Process control and related applications," ISA, 2009.

[18]. D. Sexton, "Understanding the unique nature of the universal family of ISAIOO Wireless Standards," ISA Aug. 28 2007.

[19]. Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Science Direct (Elsevier), Computer Communications*, *54*, 1-31.

[20]. R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, (2011).Key management systems for sensor networks in the context of the Internet of Things. *NICS Lab Publications, Computers & Electrical Engineering, 37*, 147-159.

[21]. S. Sebastian, P. P. Ray, (2015). Development of IoT invasive architecture for complying with health of home. In Proceedings of I3CS, Shillong, 79–83.

[22]. P.P. Ray, (2016).A survey on Internet of Things architectures. *Journal of King Saud University, Computer and Information Sciences,* 1-29.

[23]. J. Granjal, E. Monteiro and J. Sá Silva, (2015).Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. Proceedings in *IEEE Communications Surveys & Tutorials, 17*(3, 1294-1312.

[24]. Yang, Geng & Xie, Li & Mäntysalo, Matti & Zhou, Xiaolin & Pang, Zhibo & Xu, Li & Kao-Walter, Sharon & Chen, Qiang & Zheng, Li-Rong. (2014). A Health-IoT Platform Based on the Integration of Intelligent Packaging, Unobtrusive Bio-Sensor and Intelligent Medicine Box. *IEEE Transactions on Industrial Informatics. 10* (4). 1-1.

[25]. D. Trˇcek,(2013). Lightweight protocols and privacy for all-in-silicon objects. Science Direct (Elsevier) Ad Hoc Networks, *11*(5), 1619–1628.

[26]. J. A. Manrique, J. S. Rueda-Rueda and J. M. T. Portocarrero (2016). Contrasting Internet of Things and Wireless Sensor Network from a Conceptual Overview. IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, *Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu*, 252-257.

[27]. M. R. Abid, R. Lghoul and D. Benhaddou, (2017). ICT for renewable energy integration into smart buildings: IoT and big data approach. *IEEE AFRICON, Cape Town,* 856-861.

[28]. A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, (2014). Internet of Things for Smart Cities. *Proceedings in IEEE Internet of Things Journal,* 1(1), 22-32.

[29]. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, (2015). Internet of Things: A

Survey on Enabling Technologies, Protocols, and Applications. *Proceedings in IEEE Communications Surveys & Tutorials, 17*(4), 2347-2376.

[30]. J. A. Stankovic, (2014).Research Directions for the Internet of Things. *Proceedings in IEEE Internet of Things Journal, 1*(1), 3-9.

[31]. W. He, G. Yan and L. D. Xu, (2014). Developing Vehicular Data Cloud Services in the IoT Environment. Proceedings in IEEE Transactions on Industrial Informatics, *10*(2), 1587-1595.

[32]. M. Abrar, R. Masroor, I. Masroor and A. Hussain, (2018). IOT based efficient D2D communication. M*oscow Workshop on Electronic and Networking Technologies (MWENT), Moscow,* 1-7.

[33]. P. Agrawal and G. Chitranshi, (2016). Internet of Things for monitoring the environmental parameters. IEEE International Conference on Information Technology (InCITe) - The Next Generation IT Summit on the Theme - Internet of Things: Connect your Worlds, Noida, pp. 48-52.

[34]. R. Koshy, N. Shah, M. Dhodi and A. Desai, (2017). Iot based information dissemination system in the field of education. *IEEE 2nd International Conference for Convergence in Technology (I2CT),* Mumbai, 2017, 217-221.

[35]. A. C. Swastika, R. Pramudita and R. Hakimi, (2017). IoT-based smart grid system design for smart home. *IEEE 3rd International Conference on Wireless and Telematics (ICWT), Palembang*, 49-53.

[36]. S. T. Bakhsh, (2017). Energy-efficient distributed relay selection in wireless sensor network for Internet of Things. *IEEE 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia,* 1802-1807.

[37]. N. Akhtar, M. A. Khan, A. Ullah and M. Y. Javed, (2019). Congestion Avoidance for Smart Devices by Caching Information in MANETS and IoT. *Proceedings in IEEE Access, 7*, 71459-71471.

[38]. A. Salam and S. Shah, (2019).Internet of Things in Smart Agriculture: Enabling Technologies. IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 692-695.

[39]. K. Chopra, K. Gupta and A. Lambora, (2019). Future Internet: The Internet of Things-A Literature Review. IEEE International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 135-139.

[40]. L. Turchet, G. Fazekas, M. Lagrange, H. S. Ghadikolaei and C. Fischione, 2019. The Internet of Audio Things: state-of-the-art, vision, and challenges. *Published in IEEE Internet of Things Journal*, 1-1.

How to cite this article: Sarad, A., Verma, A. and Badholia, A. (2020). A Comparative Survey on Wireless Sensor Networks based Internet of Things (IoT). *International Journal on Emerging Technologies*, *11*(3): 1015–1021.