ISSN: 2456 – 3137
International Journal of Computational Research and Development
Impact Factor 5.015, Special Issue, February 2019 - Conference Proceedings
International Conference on Management 4.0: Disruptions in Business and Millennials at the Workplace (KRUPACON 2018) On 12th & 13th October 2018 Organized By
Krupanidhi Group of Institutions, Bangalore, Karnataka

WSN AND IOT: A COMPARATIVE STUDY

Jissy Thomas* & Roopini J**
* Krupanidhi Group of Institutions, Bangalore, Karnataka
** Krupanidhi Degree College, Bangalore, Karnataka

Cite This Article: Jissy Thomas & Roopini J, "WSN and IoT: A Comparative Study", International Journal of Computational Research and Development, Special Issue, February, Page Number 17-20, 2019.

Abstract:

Over the years, the Internet of Things has grown much more quickly and is one of the research areas that is most supported. As a consequence of the need for expanded, integrated Wi-Fi sensor networks of different kinds, the Internet of Things has increased. This provides an overview of the numerous wireless sensor networks that enable the improvement of the Internet of Things through protocols and organized bureaucracy. Outlined here are Wireless HART, ZigBee, and ISA. Chanting is one of the criteria of conversation. In addition, this finding helps the contrast and similarity between the most powerful wireless sensor networks and the Internet of Things (IoT) to be addressed.

Key Words: WSN, Zigbee, IoT, Internet of Things

Introduction:

A sensor network is defined by the International Standards Organization (ISO) as a unit of distributed sensor nodes and other environments that interact to collect, process, modify and provide recordings extracted from the physical world [1]. These networks have been developed for cutting-edge machinery and automation in the fields of industry [2], medicine [3], agriculture and households [4], as well as numerous other automation tasks. WSN (Wireless Networks Sensor) is a spatially dispersed autonomous static system used to gather data in a Wi-Fi environment and is capable of jointly tracking and sensing physical or environmental factors, including noise, stress, humidity, vibration, and emissions. Uh, may. Yeah, or draw. In a single location (5). Many of the world's standard wireless networks, including ZigBee, ISA, and Wireless HART. To offer a quick overview of the hierarchical structure for protocol execution, 100 follows the stack structure [6]. As a result of the need for remote sensing network administration, the Internet of Things (IoT) has increased. The Internet of Things (IoT) is characterized as the interconnection of physical and digital objects to provide advanced goods by building a global infrastructure based on current and emerging real-world and interaction technologies for an evidence-based society [7]. WSN is a catalyst for the growth of the Internet of Things (IoT). This is because an infrastructure that can replace the computing and technical systems of today is required by the IoT. Although wireless networks have made substantial advancements in device, control and voice functions, a set of globally proven and long-standing protocols can use existing warehouse systems to provide networking and routing capabilities.

Standards WSN:

There are several simple network architectures with wireless sensors that can be classified by improvements and upgrades. During implementation and communication, the outstanding criteria you should pay attention to are latency, range of Wi-Fi connectivity, cost of updating sensor data, power usage, stability, environmental performance, etc. Here is a general conversation on WSN requirements accepted.

A. Wireless HART:

This generation of the network utilizes DSSS radios compatible with IEEE 802.15.4 and facilitates pack transition. The contemporary counter-piece fits the medium-sized HART thread. The 16 famous IEEE802.15 are customized by Wireless HART. Using the Hopping Frequency Propagation Spectrum, 4 channels (FHSS). This includes Wireless HART's optional Clean Channel Evaluation (CCA) features that can be run prior to sending a message [8]. Power conversion is another feature of Wireless HART, which prohibits the use of some specified channels. It prohibits Wireless HART [9] from interfering with other concurrent Wi-Fi networks.

Technology: All peripherals of Wireless HART have a routing feature [9]. For routing, scripting and routing sources, Wireless HART has plans. For contacts in the group, the initial path is chosen because it uses on-call links and there are no alternate paths. In order to deliver messages and send them using predetermined paths, visual routing is used. Relevant Wireless HART Architecture Additions:

- Gateway-A tool for linking the host network to the gateway-sensor network. Wireless HART's key interface uses Modbus-Profibus-Ethernet. Gateway tools maintain confidentiality and monitoring of networks [10].
- Network Manager-Mesh is deployed by Network Manager. His task is to determine high-quality routes and track access times (10ms for every Wireless HART game). Access to slot machines depends on the method's preferred levelling fee and [10] multiple receivers.
- The Compliance Advisor provides encryption protection keys. Gadget permissions [10] are also dealt.
- Repeater-used to extend the reach of the culture. Text route for Wireless HART, not a dedicated link. Routing [11] is sponsored by the Wireless HART network as a whole.
- Adapters are used to relay information to Wireless HART community hosts who are already linked to HART support resources. Across the 4-20mA system cable, the adapters are placed. Driven by a battery or cable of 20mA. [11].
- Terminal-connects the portal with the diagnosis resources available. The new tool makes it easy to connect to an established Wireless HART network [11].

Security: Wireless HART enforces security as a must and offers errors and host protection. Security is implemented using an AES-128 symmetric block encryption key [9] by encrypting facts and authenticating messages at the data and network hyperlink

level. To protect the adhesion of modern devices created and managed by security administrators [9], a series of security keys is used. The network administrator offers keys and suggestions to the network for more contact. The session key provides permission to pass and permission to pass [9] is provided by the communal key.

B. Zigbee:

A series of organizations called the ZigBee partnership typically endorse ZigBee. A collection of high-level networking protocols using IEEE is the most current ZigBee specification. 802.15.4 mostly depends on low-energy radio. ZigBee is useful for local RF programming with low bitrate, low energy consumption and ease of use.

Technology: ZigBee specifically uses the 802.15.4 protocol, which is based on all on-demand advertisement vector guidelines (AODV). For P2P communications, this protocol loads, allowing follow-up and detection [12]. The ZigBee group is helping to deploy the mesh topology using the same frequency channel on all connected devices as there is no frequency break available [9]. Total Focus Devices (FFD) and Minimal Function Devices are known as ZigBee gizmos (RFD). Using any network topology, FFD will attach to another complete FFD, and RFD links to the handiest FFD. In Beaconed and Non-Beaconed modes, Zigbee features. Both nodes are synced in light mode. Super Frame Signal Frame is broken into 16 slots, there is an alternative to use seven dedicated map slots that allow contact more deterministic, generally referred to as GTSS (Time Guaranteed Slot). [9]. The units of zig-zag are defined as follows:

- Coordinator-Initiates the analysis and oversees the network. This unit has all group information and operates with a security key [13] as a trust center and archive.
- The Router-Coordinator binds to other endpoints and routers. It offers information about how the reach of public insurance can be broadened and hurdles avoided. In the event of infrastructure loss or network bottle necks [13], it also protects evacuation routes.
- A final system, primarily a sensor/actuator collection that collects or transmits data (messages) but no longer performs a routing function [13]. The coordinator or router should be attached to the computer.

Security: ZigBee can use any IEEE 802.15.4 supplied security framework, but protection is optional. ZigBee has a security and verification handbook. With AES-128 encryption, ZigBee runs on CBC-MAC (CCM). Although Zigbee is a feature that offers maximum integrity or protection, 802.15.4[14] addresses the MAC layer's protection indirectly. With three types of keys, ZigBee encryption is implemented: main key, network key and reference key. The key is to connect to the network, and the contact key offers the maximum security standard, but includes higher garage standards for non-interference encryption. Network keys provide a low degree of protection but require considerably less memory and are standard for all devices [14]. To defend computers from replay attacks, Zigbee uses a serial numbering strategy [9].

C. ISA.100:

In order to incorporate industrial Wi-Fi technology networks, ISA (Instrumentation, Systems and Automation Association) proposed a new WSN ISA 100 for industrial automation and management [15]. ISA.100 pursues a policy of coexistence and gives the ability for a Wi-Fi network to do its job in an environment where other network-based Wi-Fi networks are equally recognized" or "[October 16] physical ISA .100 Networks can cover an increasing area of several square kilometres, and each network can have thousands of units [16]."

Technology: ISA.100 operates with the TDMA mechanism and accepts intrusion prevention networks from multiple devices [15]. The ISA.100 uses a default 6 LoWPAN compatible codec on the network layer, unlike other wireless sensor networks. ISA.100 tries to keep healing safe and is utterly useless [15].

Security: ISA100 enforces security protocols that will apply to all records that are encrypted. Modify the default model as follows: on the data link layer, the sub-controller uses the same rules and a key is used at once, but for a brief key transfer period [15]. This implies versatility and simplicity of scale. Flexibility and simple scalability are what this entails. [This architecture uses session keys for both symmetrical and asymmetrical key updates that are periodically updated with time assured. The computer initiates the main upgrade process and is sent by the security monitor to make it possible to resume the detection [18].

The first two is distinguished by linking individuals via personal computer systems and mobile devices to the Internet, and things need to be more linked to individuals in this Internet age [19]. Therefore, an assortment of elements of modern life are expected by the Internet of Things. As a consequence, a toolbox of real life elements is needed by the Internet of Things. The Internet of Things is much more common than networks with wireless sensors. Since it contains not only the simplest detection feature, it also contains measurements of the sensor node and has quite a few tactics. Compared to wireless sensor networks, this can be achieved at the software level which makes it a network [20] and thus provides much more advantages. This can be done at the software level, making it a network [24] and consequently offers far more advantages over wireless sensor networks.

Internet of Things (IoT):

At the software stage, this can be achieved, rendering it a network [24] and thereby having even more benefits over wireless sensor networks.

Technology: IoT equipment should promote the five procedures for detection, identification, activation, contact and tracking [21]. The following curriculum modules support these competencies. A system for the identification, triggering, supervision, and tracking of athletic activities.

- The IoT tools cover data analysis and data transfer and can provide a range of interfaces for speech communication [22]. Communication-This block carries out verbal communication to a remote server from the computer.
- Many protocols, such as the data channel layer, the network layer and the implementation of various IoT models [22], are built for different layers. Many forms of tool modelling, device control, transparency and information security software are offered by Service IoT systems [22].

- Administration-This block includes different functions for IoT system management.
- Authentication, consent, secrecy, message accuracy, physical integrity and factual protection include IoT security issues [22].
- From the point of view of the user, the application layer is the most significant layer since it acts as a processor and display interface.
- Dynamic and self-adapted, self-replicable, interoperable and transparent protocols of recognition built into sensitive statistical and contextual networks [23] and efficient smart choices [21] will characterize IoT systems.

The operation of IoT machines includes a number of hardware devices, such as a processor, EEPROM memory, specific low-power capabilities, and the ability to link I/O to arbitrary networks, and Wi-Fi 802, which supports multiple protocols for wireless communication. Even), LR-WAN (802.15.4), WiMAX (802.16), Smartphone (2G/3G/4G), Low Energy Bluetooth (802.15.1) and LoRAWAN (R1.0-LoRa). A robust cloud response can be provided by IoT engines, allowing you to connect into the cloud and use frameworks and apps as goods. Multiple architectures, primarily service-driven, are leased by IoT instruments. For IEEE 802.15, the ITU has specified a five-level framework called the IEEE P2413 framework. Yeah, LoWPAN and ROLL with data connection and network layer, and COAP, DTLS, MQTT and XMPP with device layer [24]. Yeah, on the network and data link layer, LoWPAN and ROLL, and on the device layer, COAP, DTLS, MQTT and XMPP [24].

Security: The Internet of Things (IoT) can be different when it supports multiple architectures or when certain protocols are introduced at different levels by such systems. Protection can be regarded at different levels within the ITU standard architecture for general discussion. Supporting 16 lines, the IEEE 802.15.4 protocol, which fits the 2.4 GHz band in the physical layer, is a special encryption since it is DSSS (Direct Series Spread Spectrum), PCB (Ultra Broadband Direct Serial) and Crip Spread Spectrum (CSS) for low power operations. Non-implementation of defence mechanisms [24]. Peer protocols at the MAC level use 64-bit or 16-bit IEEE EUI high-speed identifiers to recognise gizmos and use AES-CBC-MAC32/64/128 data authentication encryption specifications [24]. The available AES CTR protection mode guarantees secrecy. The Replay Attack Protection Guide [24] is another case. IETF 6LoWPAN is an Internet access standard that has no security controls, but a different security tactic is offered by features with unique communication protocols [25]. CoAP (Limited Application Protocol) supports Pre Shared Key, Raw Public Key and certificate authentication modes at the application level [24].

Discussion and Conclusion:

Sensory nodes such as SNWs, however, vary from those used by IoT nodes [26] [27]. IoT nodes, like field machining, are in fact surface machining. IoT nodes are a special expression of a WSN tool's computational power. As most WSN chat specifications including IEEE 802.14.5, LoRa, and Bluetooth Low Energy (BLE) are commonly used for communicating in different IoT architectures, there is a similar collection of chat generating functions between IoT and WSN. The IoT Evaluation WSN does not however, describe the direct link of sensor nodes to the Internet for the purpose of reading and transmitting information. For IoT and WSN, looking at WSN as a subdomain or crude IoT, there are several parameters discussed. In the table below, each demand for use is compared. IoT technology discussions may need to cite equipment protocols, characteristics, and multilevel connections, but they can no longer substitute wireless sensor network comparisons.

The Wi-Fi sensor software layer no longer has to process Internet Protocol records and no longer requires the requirements and modules needed for the network or device layer to process the details in order to comply with the specifications. R Current world on the Internet. The aim is to compare the wireless sensor network and the Internet of Things in this figure, and we explored the easiest technological and security settings that can provide both technologies with comparative details.

With a discussion of the most familiar wireless protocols, this trial presents the idea of wireless sensor networks and addresses the Internet of Things in similar terms. This is a good way to show the parallels and variations between the two. In computer networks and machine-to-machine communication, WSN and IoT are two fields of observation that have similar origins. Yet all of them have special ways of preparation. We may infer from the above conversation that the IoT incorporates many current systems, including one that is undoubtedly WSN. It should also be noticed that the IoT and WSN application specifications are identical, but the degree of significance is extraordinary. The security, scalability and heterogeneity of the Internet of Things, on the one hand, are difficult because on the other hand, SNW has limited resource management expertise. In the one side, the stability, security, scalability and heterogeneity of the Internet of Things, on the other hand, are complicated since WSNs have little knowledge resource management.

Acknowledgement:

The authors express gratitude towards the assistance provided by The Management, Krupanidhi Group of Institutions (KGI) and Krupanidhi Research Incubation Centre, KGI in completing the research. We also thank our Research Mentors who guided us throughout the research and helped us in achieving the desired results.

References:

1. I. J. I, “Study on Sensor Networks (Version 3),” Tech. Rep., 2009.
2. C. Kruger and G. P. Hancke, “Implementing the internet of things vision in industrial wireless sensor networks,” in 2014 12th IEEE International Conference on Industrial Informatics (INDIN). IEEE, 2014, pp. 627–632.
3. F. Hu, D. Xie, and S. Shen, “On the application of the internet of things in the field of medical and health care,” in Green Computing and Communications (Green Com), 2013 IEEE and Internet of Things (iThings / CPS Com), IEEE International Conference on and IEEE Cyber, Physical and Social Computing. IEEE, 2013, pp. 2053–2058.
4. F. Zhang, “Research on applications of internet of things in agriculture,” in Informatics and Management Science VI. Springer, 2013, pp. 69–75.

5. Zhang and V. Varadharajan, "A New Security Scheme for Wireless Sensor Networks," in IEEE Global Telec ommunications Conference, 2008, pp. 1-5.
6. "WSN Security Project Overview and Scope-Internal Statoil Document" Statoil 2009.
7. “Recommendation ITU-T Y.2060 (06/2012),” 2012.
8. D. Wenliang, D. Jing, Y. S. Han, C. Shigang, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, 2004, p. 597.
9. T. Lennvall, S. Svensson, and F. Hekland, "A comparison of Wireless HART and Zig Bee for industrial applications," in Factory Communication Systems, 2008. WFCS 2008. IEEE International Workshop on, 2008, pp. 85-88.
10. "HART Communication Foundation," http://www.hartcomm.org/index.htrnl, 2007.
11. "The Components of Wireless HART Technology": HART Communication Foundation, 2009.
12. S. Tian-Wen and Y. Chu-Sing, "A Connectivity Improving Mechanism for ZigBee Wireless Sensor Networks," in Embedded and Ubiquitous Computing, 2008. EUC '08. IEEEIIFIP International Conference on, 2008, pp. 495-500.
13. "Getting Started with ZigBee and IEEE 802.15.4," Daintree Networks, Feb 2008.
14. S. Jing and Z. Xiaofen, "Study of ZigBee Wireless Mesh Networks," in Hybrid Intelligent Systems, 2009. HIS '09. Ninth International Conference on, 2009, pp. 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. E. Borgia, “The internet of things vision: Key features, applications and open issues,” Computer Communications, vol. 54, pp. 1–31, 2014.
20. R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, “Key management systems for sensor networks in the context of the internet of things,” Computers & Electrical Engineering, vol. 37, no. 2, pp. 147–159, 2011.
21. S. Sebastian, P. P. Ray, “Development of IoT invasive architecture for complying with health of home,” In: Proceedings of I3CS, Shillong, pp. 79–83, 2015.
22. P.P. Ray, “A survey on Internet of Things architectures,” Journal of King Saud University – Computer and Information Sciences, 2016.
23. J. Granjal, E. Monteiro, and J. Sá Silva, “Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues,” IEEE communication surveys & tutorials, vol. 17, no. 3, pp. 1294-1312, 2015.
24. G. Yang, X. Li, M. Mantysalo, X. Zhou, Z. Pang, L. D. Xu, S. K. Walter, Q. Chen, L. Zheng, “A health-IoT platform based on the integration of intelligent packaging, unobtrusive biosensor and intelligent medicine box,”. IEEE Trans. Ind. Inf. 10 (4), pp.2180–2191, 2014.
25. D. Tr˘cek, “Lightweight protocols and privacy for all-in-silicon objects,” Ad Hoc Netw., vol. 11, no. 5, pp. 1619–1628, Jul. 2013.
26. S. G. on Sensor Networks (SGSN), “Study on sensor networks (version 3),” ISO/IEC JTC 1, Tech. Rep., 2009.
27. ITU-T, “F.748.0: Common requirements for internet of things (iot) applications,” ITU, Tech. Rep., 2014.