International Journal of Scientific Research in Computer Science, Engineering and Information Technology
 | Volume 3 | Issue 1 | ISSN : 2456-3307

A Survey of Z-wave Wireless Sensor Network Technology

Pavan A C

Lecturer, Department of Computer Science, KLE Society's S. Nijalingappa College, Bangalore, Karnataka, India

ABSTRACT

Z-wave technology as a wireless sensor and control network is one of the most popularly deployed wireless technologies that too in recent years; this is because Z-wave is an open standard lightweight, low-cost, low-speed, low-power protocol that allows true operability between systems. It features to meet required functionalities thereby finding applications in wide variety of wireless personal area networked systems such as home/industrial automation and monitoring systems. Although the Z-wave design specification includes security features to protect data communication confidentiality and integrity, however, when simplicity and low-cost are the major goals, security suffers. This paper gives the general survey of the Z-wave as a wireless sensor network based technology, which provides the readers with the general overview of Z-wave network technology.

Keywords: Z-wave, Wireless Sensor Network (WSN), Topology, Wireless technology.

I. INTRODUCTION

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

How the Next Evolution of the Internet Is Changing Everything

The Internet of Things (IoT), sometimes referred to as the Internet of Objects, will change everything—including ourselves. This may seem like a bold statement, but consider the impact the Internet already has had on education, communication, business, science, government, and humanity. Clearly, the Internet is one of the most important and powerful creations in all of human history. Now consider that IoT[3-6] represents the next evolution of the Internet, taking a huge leap in its ability to gather, analyze, and distribute data that we can turn into information, knowledge, and, ultimately, wisdom. In this context, IoT becomes immensely important.

Already, IoT projects are under way that promise to close the gap between poor and rich, improve distribution of the world's resources to those who need them most, and help us understand our planet so we can be more proactive and less reactive. Even so, several barriers exist that threaten to slow IoT development, including the transition to IPv6, having a common set of standards, and developing energy sources for millions—even billions—of minute sensors. However, as businesses, governments, standards bodies, and academia work together to solve these challenges, IoT will continue to progress. The goal of this paper, therefore, is to educate you in plain and simple terms so you can be well versed in IoT and understand its potential to change everything we know to be true today.

Characteristics of the IoT:

Interconnectivity: With regard to the IoT, anything can be interconnected with the global information and communication infrastructure.

Heterogeneity: The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.

Dynamic changes: The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.

Safety: As we gain benefits from the IoT, we must not forget about safety. As both the creators and recipients of the IoT, we must design for safety. This includes the safety of our personal data and the safety of our physical well-being. Securing the endpoints, the networks, and the data moving across all of it means creating a security paradigm that will scale.

Connectivity: Connectivity enables network accessibility and compatibility. Accessibility is getting on a network while compatibility provides the common ability to consume and produce data.

In general, what IoT can do is, in future consumer applications envisioned for IoT sound like science fiction, but some of the more practical and realistic sounding possibilities for the technology include:

- receiving warnings on your phone or wearable device when IoT networks detect some physical danger is detected nearby
- self-parking automobiles
- automatic ordering of groceries and other home supplies
- automatic tracking of exercise habits and other day-to-day personal activity including goal tracking and regular progress reports

Potential benefits of IoT in the business world include:

- location tracking for individual pieces of manufacturing inventory
- fuel savings from intelligent environmental modeling of gas-powered engines
- new and improved safety controls for people working in hazardous environments

II. Z-wave Technology

Z-wave (or Z wave or Z-wave)[9] is a protocol for communication among devices used for home automation. Z-Wave enables smart home products like locks, lights and thermostats to talk to each other. This creates the backbone of your smart home and enables you to use your smartphone or tablet to create one-touch scenes that help with daily activities like: saving energy, keeping your home secure, looking after your loved ones and being more comfortable.

Reasons why Z-wave is trending:

- **Easy** to install and does not require any rewiring of your home's current electrical.
- **Trusted:** The biggest brand names on the market use Z-Wave in their smart home products.
- **Affordable:** You can get started with a minimal investment and easily add more smart products.
- **Experienced:** There are already 50 million products in smart homes worldwide.
- **Reliable:** Having been on the market for over 10 years, Z-Wave has proven to be the top home automation solution on the market.
- **The Smart Home Leader:** 9 out of 10 leading security companies use Z-Wave.
- **Secure:** Z-Wave technology uses the same encryption as online banking making it the safe choice for your smart home.
- **Provides Choices:** With over 2100 smart home automation products on the market, Z-Wave products provide many choices to suit your needs - styles, price points, colors, functionality, etc.

Z-wave Devices types

In Z-Wave terminology controlling devices are called controllers, reporting devices are called sensors and controlled devices are called actuators and they can be categorized into one of these function groups:

- **Controllers** - devices that control other Z-Wave[10] devices
- Remote Controls - universal remote control (with IR) or dedicated Z-Wave Remote Control with special keys for network functions, group and/or scene control
- USB sticks and IP gateways to allow PC software to access Z-Wave networks. Gateways also allow remote access via the internet
- **Sensors** - devices that report information by sending a digital or analogue signal
- Analogue Sensors - measure parameters like temperature, humidity and gas concentration
- Digital Sensors - door/glass breaking, motion detector and flood warning
- **Actuators** - devices that switch digital (on/off for an electrical switch) or analogue signals (dimmer or blind control)
- Electrical Switches - plug-in modules for wall outlets or direct replacements for traditional wall switches (digital)
- Electrical Dimmers - plug-in modules or replacements for traditional wall switches/dimmers (analogue)
- Motor Control - open or close a door, window or blind or a venetian blind (analogue or digital)
- Electrical Display - provide visual feedback or an alert such as a siren, LCD panel, etc (digital)
- Thermostats controls - TRVs (Thermostat Radiator Valves) or floor heating controls (analogue or digital)

Z-wave Network Topology

Z-Wave [7] uses a wireless mesh network topology. A wireless mesh network (WMN)[1] is a communications network made up of radio nodes organized in a mesh topology. It is also a form of wireless ad hoc network.

A mesh refers to rich interconnection among devices or nodes. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. Mobility of nodes is less frequent. If nodes were to constantly or frequently move, the mesh will spend more time updating routes than delivering data. In a wireless mesh network, topology tends to be more static, so that routes computation can converge and delivery of data to their destinations can occur. Hence, this is a low-mobility centralized form of wireless ad hoc network.

III. Some Other WSN Standards and Technologies

As the applications of WSNs are increasing, different protocols and standards are being researched and created to enhance the efficiency of the network. The decision to select a particular standard/protocol over the other is determined by the target application requirements and some other factors such as network size, network environment and network duration. Once the application requirements are set, then the engineer will select the technology which satisfies these requirements. The following are overview of the features of other popular WSN technologies.

i. Bluetooth Technology

Bluetooth [2] is a robust, low power, low cost, short-range wireless communication technology intended to replace cables in wireless personal area networks (WPANs). Initially created by Ericsson Microelectronics in 1994, its specifications are driven by a consortium that was founded by Ericsson, Nokia, Toshiba, IBM and Intel. The IEEE standard for Bluetooth (WPAN) is called The IEEE Project 802.15.1 and is based on the Bluetooth v 1.1 Foundation (BluetoothTM, 2004). It allows product differentiations because some of its core specifications are optional. It can communicate (pass and synchronize data) between up to seven devices using 868MHz, 915MHz and 2.4GHz radio bands at 1GHz per second using frequency-hopping spread-spectrum (FHSS) and up to a range of 10 meters. Bluetooth only supports star topology, uses master-slave based MAC protocol and full duplex transmission through the use of time-division duplexing.

ii. Wi-Fi

Based on IEEE 802.11 standards, Wi-Fi is a WLAN technology that allows electronic devices to exchange data over a network such as internet and uses a radio band of 2.4GHz. Wi-Fi is robust, easily expandable and cost effective. Wi-Fi data transfer rate is up to 300Mbps depending on the standard and has about 100 to 150Mbps through-put.

A Wi-Fi-based WSN is a combination of traditional Wi-Fi mesh network and WSN and hence possesses both the features of Wi-Fi mesh network and WSN. Therefore, it is both network-centered and data-centered. Wi-Fi-based WSNs are used in smart grid, smart agriculture and intelligent environment protection.

iii. ANT Technology

ANT is another proprietary wireless technology that is designed using microcontrollers and transceivers operating in the 2.4GHz ISM for reliable, flexible and adaptive data communication with ultra-low power consumption in WSN applications[8]. This technology is simply and efficiently designed to maximize battery life, simplify network design and minimize implementation cost. It has low latency, supports broadcast and burst with a data rate of up to 20 kbps. It also supports star, tree and mesh topologies and its nodes can act as slaves or masters in a network of tens to hundreds of nodes in personal area networks and practical WSNs. ANT also provides cross-talk immunity.

iv. Wireless HART

It is an open wireless industrial sensor network standard that is based on the Highway Addressable Remote Transducer (HART) Protocol using the 802.15.4 – 2006 standard. Officially released in 2007 and majorly used for industrial control process and monitoring, WirelessHART is a secure and TDMA-based (usng10*ms* time slot) mesh networking technology that operates in the 2.4 GHz ISM band. Other key features of Wireless HART includes network wide time synchronization, channel hopping, channel blacklisting, and industry standard AES-128 ciphers and keys.

IV.CONCLUSION

Z-wave technology [11] as a wireless sensor and control network is being considered as one of the most deployed wireless technologies in recent times as results of its attractive features to the users such as: open standard lightweight, low-cost, low-speed, low-power, interoperability protocol, among others. This paper has provided a general overview of the Z-wave sensor networking technology in which its definition, topology and challenges have been presented. Competing with Z-Wave are Thread and ZigBee network standards. Of the three, Z-Wave has the longest operating range at 300 feet (outdoor) and 80+ feet (indoor), ZigBee has the largest number of maximum device capability at 65,000 (to Z-Wave's 232) and Thread has the fastest data transmission rate at 250 kbps. Z-Wave has better interoperability than ZigBee, but ZigBee has a faster data transmission rate which is making Z-Wave highly accessible to Internet of Things developers.

V. REFERENCES

[1]. Abbagnale, A, Cipollone, E, Cuomo, F.: A case study for evaluating IEEE 802.15.4 wireless sensor network formation with mobile sinks, IEEE ICC, Rome. (2009)

[2]. Bluetooth T M.: Specification of the Bluetooth System; Bluetooth SIG Inc., Kirkland. (2005)

[3]. "Internet of Things: Science Fiction or Business Fact?" (PDF). Harvard Business Review. November 2014. Retrieved 23 October 2016

[4]. Alippi, C. (2014). Intelligence for Embedded Systems. Springer Verlag. ISBN 978-3-319-05278-6.

[5]. Internet of Things: The "Basket of Remotes" Problem". Monday Note. Retrieved 26 June 2015.

[6]. Kim, H, Caytiles, R.D, Kim, T.: Design of an Effective WSN-Based Interactive u-Learning Model. International Journal of Distributed Sensor Networks, (e-journal). (2012).

[7]. Knight, M.: Wireless security-How safe is Z-wave?. Computing & Control Engineering Journal, (e-journal). (2006). Vol. 17, No. 6. 18-23.

[8]. Ruiz-Garcia, L.: 2009. A review of wireless sensor technologies and applications in agriculture and food industry: state of the art and current trends. Sensors, Vol. 9, No. 6. 4728-4750. (2009)

[9]. Oliver Kaven, "Zensys' Z-Wave Technology", PC Magazine, January 8, 2005.

[10]. "Understanding Z-Wave Networks, Nodes & Devices". Vesternet.com. Retrieved 2012-11-19.

[11]. Brandon Lewis, "Z-Wave opens up as smart home connectivity battle closes in", Embedded Computing Design, September 2, 2016.