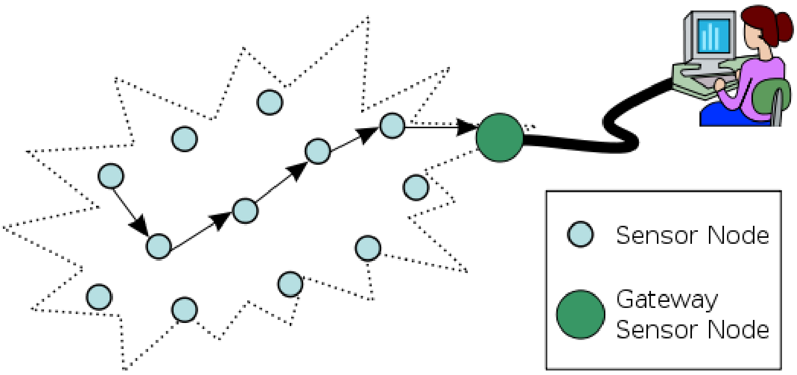
Wireless Sensor Network (WSN)

(da https://it.wikipedia.org/wiki/Wireless_sensor_network)

Con il termine ‘Wireless Sensor Network’ (o WSN) si indica una determinata tipologia di rete che è caratterizzata da una architettura distribuita, realizzata da un insieme di dispositivi elettronici autonomi in grado di prelevare dati dall’ambiente circostante e di comunicare tra loro.



L'utilizzo di una rete senza fili presenta vantaggi significativi per diversi motivi: economici, ambientali (difficoltà di cablare in ambiente), flessibilità della soluzione (spostamento dei nodi per esempio), scalabilità.

Una WSN può quindi essere definita come un insieme di nodi wireless interconnessi (anche detti mote, sensor node), aventi poca RAM e una CPU con prestazioni relativamente basse. La struttura di una Wireless Sensor Network prevede solitamente diversi nodi wireless sparsi in un’area, che inviano periodicamente dati rilevati tramite sensori (di posizione, temperatura, luminosità, …..) ad un punto di raccolta, detto sink (o base station o gateway, oppure coordinatore), il quale gestisce la rete (si pensi alle problematiche di routing), raccoglie i dati dei nodi, esegue un’elaborazione di primo livello e li inoltra ad un altro sistema remoto per ulteriori elaborazioni.

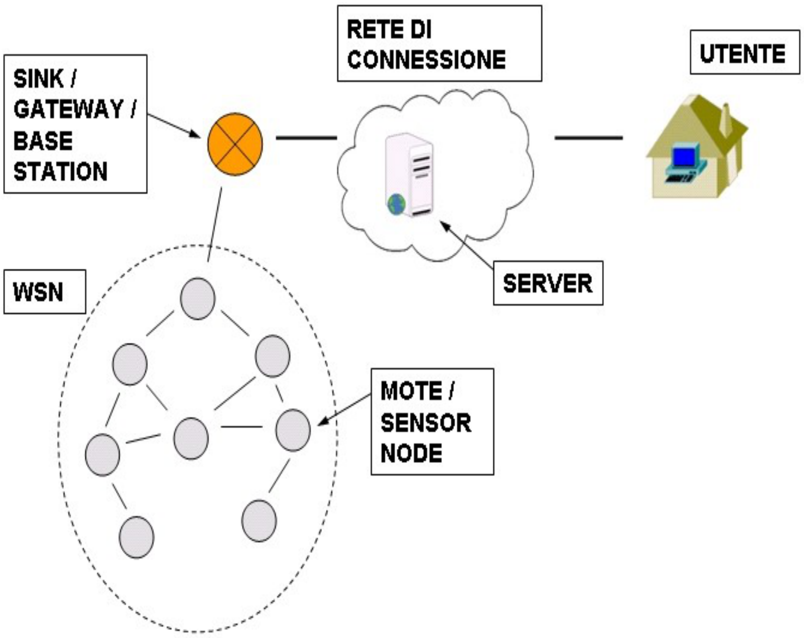
Una sensor network offre una vasta gamma di utilizzi che, per esempio, potrebbero essere :

- la raccolta dati in ambienti anche molto vasti (per esempio applicazioni nell’ambito dell’agricoltura, del controllo degli incendi, della gestione del traffico stradale)
- applicazioni in ambito medico/sanitario
- la domotica
- i sistemi di sorveglianza
- i sistemi di monitoraggio per il consumo energetico

Le componenti basilari di una rete per un sistema di questo tipo sono:

1. un insieme di sensori distribuiti (mote)
2. una rete di interconnessione (wireless nel caso in questione)
3. un punto di raccolta dei dati (sink, gateway)
4. un insieme di risorse computazionali con prestazioni medio elevate nel punto di arrivo dei dati della rete al fine di effettuare datalogging, correlazioni dei dati, elaborazione, monitoraggio dello stato ecc. . .

Uno schema esemplificativo della struttura di una rete di questo tipo è mostrato nella figura figura seguente:



Struttura tipica di una WSN

I sensori attualmente sul mercato possono rilevare una notevole varietà di parametri, i dati rilevati vengono spediti all'interno della rete tramite dei collegamenti wireless a bassa potenza al punto di raccolta, che spesso è connesso ad Internet e che a sua volta può inoltrare i dati ad un punto di analisi. Il meccanismo di accesso al canale wireless è solitamente di tipo contention-oriented ad accesso casuale, come definito nello standard IEEE 802.

Le reti di sensori sono dunque delle reti wireless "ad hoc", ma rispetto ad una tradizionale rete "ad hoc" presentano alcune peculiarità che hanno richiesto nuove soluzioni. Infatti ,le WSN hanno le seguenti caratteristiche:

- il numero di nodi che compongono una rete di sensori può essere di alcuni ordini di grandezza maggiore rispetto al numero di nodi in una rete ad hoc;
- i nodi possono essere disposti con un'alta densità;
- i nodi sono soggetti a guasti;
- la topologia di una rete di sensori può cambiare frequentemente a causa di guasti ai nodi o della loro mobilità;
- i nodi utilizzano un paradigma di comunicazione broadcast mentre la maggior parte delle reti ad hoc sono basate su una comunicazione di tipo punto-punto;
- i nodi sono limitati rispetto ad alimentazione, capacità di calcolo e memoria;

- i nodi non sono alimentati (ad eccezione delle soluzioni di home automation in cui lo possono essere o in cui comunque la batteria è facilmente sostituibile) e il loro funzionamento deve essere garantito per periodi di tempo molto lunghi (mesi/anni)

- I nodi solitamente non possiedono un identificatore globale (come l'indirizzo IP nei computer);

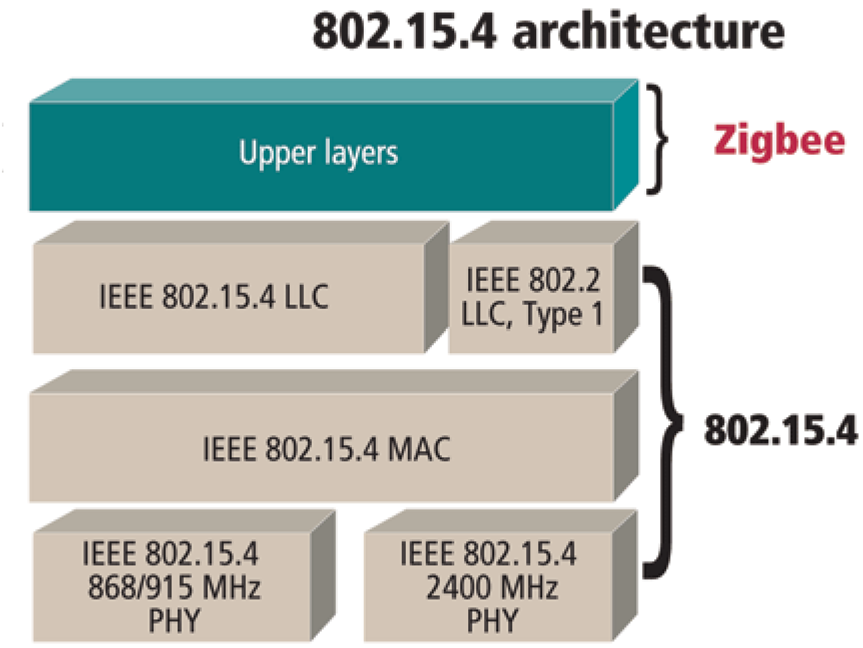
Lo stack protocollare delle WSN deve essere quanto più leggero possibile, per poter soddisfare i vincoli imposti dai limiti hardware dei nodi. A partire dai primi anni del 2000 furono definiti degli standard, che tuttavia erano proprietari, solamente in seguito si è cercato di definirne uno aperto.

Dapprima sono stati esaminati quelli già disponibili ma sono risultati non adatti a tale scopo, in particolare:

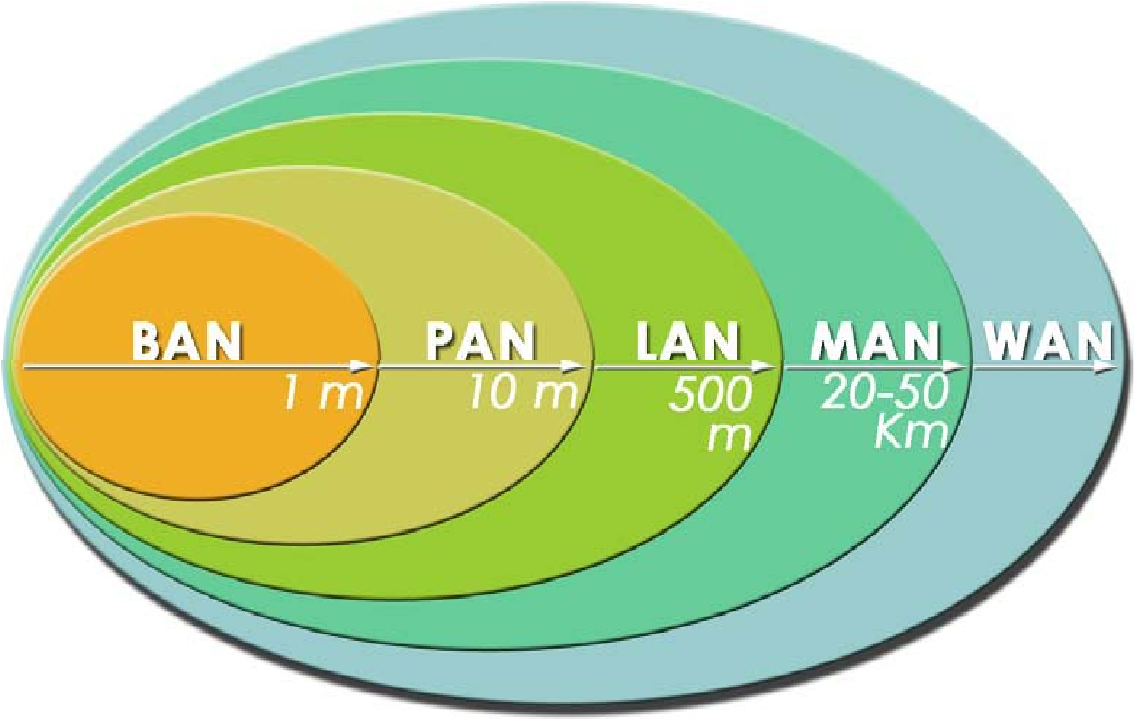
- IEEE 802.11: richiede troppe risorse hardware e offre una banda ben oltre le necessità di un nodo della WSN (che trasmette pochissimi byte alla volta) .
- Sistemi ad infrarossi: richiedono un allineamento visivo tra i nodi.
- IEEE 802.15.1 (WPAN/Bluetooth): emanato nel 2002 per dispositivi portabili e mobili all'interno di uno spazio "personale" risulta troppo complesso, costoso, oneroso in termini di consumo energetico. Nel 2010 è stato emanato lo standard Bluetooth 4.0 + BLE (Bluetooth Low Energy) che sta determinando lo sviluppo di reti WSN BLE

Così si è arrivati a definire un nuovo standard, l'**IEEE 802.15.4** e lo ZigBee (ZigBee definisce solo i layer software sopra l'802.15.4 e supporta diverse applicazioni). L'IEEE 802.15.4 opera nella banda radio ISM a 2.4 Ghz, permette data rate fino a 250 kbps e un range tipico tra i 10 e i 75 metri.

Lo standard **IEEE 802.15.4** è stato concepito per regolamentare il livello fisico ed il livello MAC (*Media Access Control*) di reti in area personale che lavorano con basse velocità di trasferimento dati (LR-WPAN, *Low-Rate Wireless Personal Area Networks*). Questo standard è gestito dal gruppo IEEE 802.15. Le specifiche ZigBee, WirelessHART, e MiWi sono basate su questo standard: esse sviluppano i livelli superiori del modello ISO/OSI, non coperti dallo standard, per offrire una soluzione completa di rete di trasmissione dati.



Riassumiamo la classificazione delle reti in funzione dell’area coperta:



Questo tipo di classificazione viene in genere ricondotto alla definizione di reti cablate, anche se in generale potremo costruire un modello molto simile in cui inserire le diverse tipologie di rete wireless ad oggi presenti sul mercato, quest’ultima classificazione però risulterà essere meno precisa per la continua evoluzione del mercato del wireless.

In corrispondenza delle reti locali locali LAN possiamo individuare il corrispondente wireless all’interno dello standard IEEE 802.11 che descrive le WLAN, reti pensate per poter sostituire la corrispondente cablata, quindi in grado di sostenere i flussi di informazioni richiesti dai personal computer, raggiungendo velocità di trasmissione comprese fra gli 11Mbit/s (IEEE 802.11b), i 500Mbit/s (IEEE 802.11ac).
Esistono reti wireless anche nel campo delle MAN dando origine alle Wireless Metropolitan Area Network, in grado di coprire aree superiori al chilometro (WMAN IEEE 802.16).

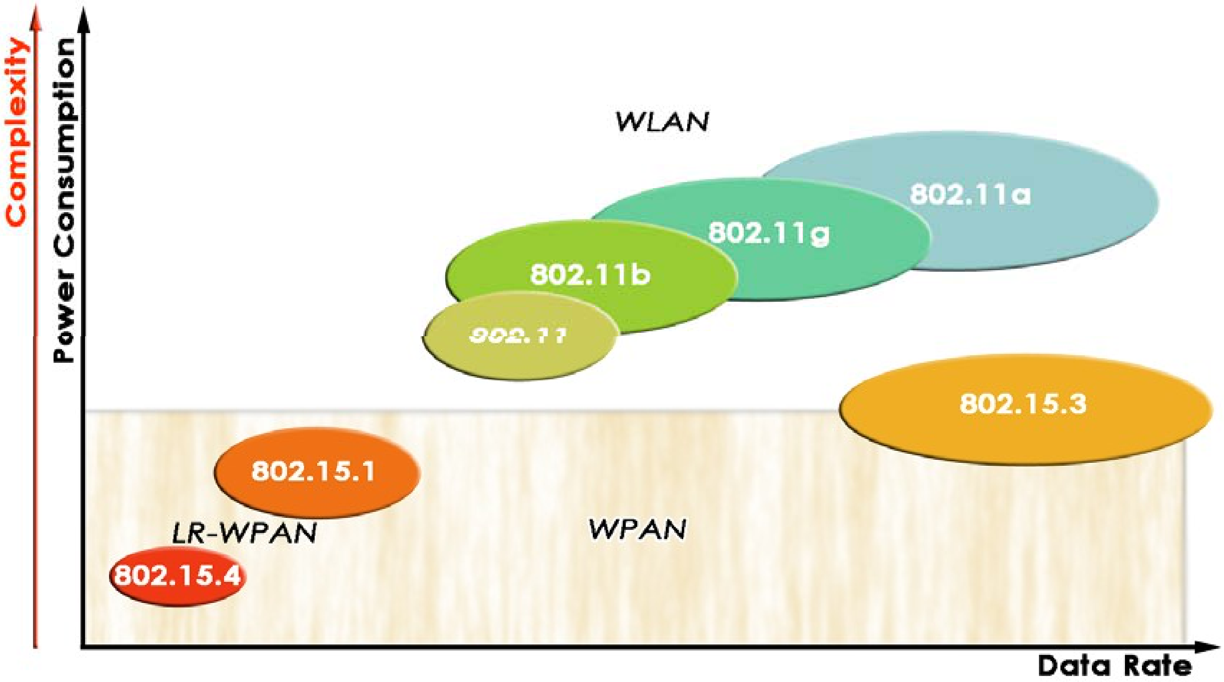
Per quanto concerne le PAN sono state definite tre diverse classi di WPAN caratterizzate da diversi data rate, consumi e QoS:

- WPAN ad elevati data rate
  Vengono descritte dall’IEEE 802.15.3, all’interno di questa famiglia si trovano tecnologie pensate per applicazioni di tipo multimediale e che richiedano un elevato QoS (WiMedia);

- WPAN a medi data rate
  Sono tecnologie descritte dall’IEEE 802.15.1 (Bluetooth);

- WPAN a bassi data rate
  Vengono indicate come LR-WPAN (Low Rate WPAN IEEE 802.15.4, ZigBee), intendono rispondere alle esigenze di reti che richiedano bassi consumi e bassi costi che non possano essere implementate con altre WPAN.

Le reti di sensori sono dunque delle WPAN a basso data rate



Classificazione delle reti wireless in funzione del Data Rate, della complessità e dei consumi

	802.11	**802.15.1/Bluetooth**	**802.15.4/ZigBee**
Copertura(metri)	100	10-100	10-75
Throughput(Mbps	2-30	1-2	0.25
Consumo Energetico	Medio	Basso	Molto Basso
Autonomia	Minuti/poche ore	Diverse ore/ pochi giorni	Giorni/Pochi anni
Dimensioni	Medie	Piccole	Molto piccole
Rapporto costo/ complessità	Alto	Medio	Basso

Tecnologie Wireless a confronto

A Survey of ZigBee Wireless Sensor Network Technology: Topology, Applications and Challenges

Omojokun G. Aju
Adekunle Ajasin University, Department of Computer Science
Akungba-Akoko, Ondo-State, Nigeria

ABSTRACT

ZigBee technology as a wireless sensor and control network is one of the most popularly deployed wireless technologies in recent years. This is because ZigBee is an open standard lightweight, low-cost, low-speed, low-power protocol that allows true operability between systems. It is built on existing IEEE 802.15.4 protocol and therefore combines the IEEE 802.15.4 features and newly added 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 ZigBee 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 ZigBee as a wireless sensor network based technology which provides the readers with the general overview of ZigBee network technology including its topology, applications and challenges.

General Terms

Wireless Sensor Network, Mobile Network.

Keywords

ZigBee, IEEE 802.14.5, Wireless Sensor Network (WSN), topology, application, wireless technology.

1. INTRODUCTION

Wireless sensor networking is one of the most popular and active research areas in networking and communication field in recent years. Consequently, numerous workshops and conferences are being arranged annually on this emerging technology. This attraction resulted from the fact that the technology is exciting with unlimited potential for numerous applications that are been implemented based on wireless sensor networks (WSNs). Application areas include environmental, military, telecommunication, transportation, entertainment, crisis management, health, retail services and smart homes. The wireless technology deployed for a particular sensor network depends on the type of application. Common wireless technologies include Infrared, Bluetooth, WiFi, WiMax, ZigBee etc. However, this paper survey ZigBee technology as a Wireless Sensor Network with emphasis on its topology, application, and challenges.

Wireless sensor network (WSN) is a large number of nodes with sensing capabilities which gather information from physical processes/events (e.g. temperature, sound, vibration, pressure, motion, or pollutants) and communicate the processed data (information) cooperatively and wirelessly to the base station. The network is formed when the same or different types or group of sensors jointly monitor (and/or control) one or more physical environments [15]. Although, wired sensor networks are more reliable and secured in addition to having stable communication systems. However, the greatest advantage of wireless sensor devices is that they make installations possible where cabling is impractical, such as in large concrete structures and cargoes [17].

When ideal wireless sensors are networked, they perform smartly and are scalable. They consume very little power, software programmable, capable of fast data acquisition, reliable and accurate. Also, wireless sensors are relatively cheap and WSNs largely reduce long term maintenance cost, eases installation, eliminate the use of bundle of wires and fiber optic tails.

In WSN, the protocol stack helps to promote cooperative efforts of sensor nodes, enhance power efficiency and integrates data with networking protocols. The protocol stack is made up of the task management plane, mobility management plane, power management plane, application layer, transport layer, network layer, data link layer and physical layer. Although, some modifications may be applicable to the protocol depending on the wireless standard and technology used in designing the WSN. ZigBee, Bluetooth, WiFi, WiMax, ANT, WirelessHART, Z-Wave and 6LowPAN are some of the most popular technologies that are currently being deployed in WSNs.

Unlike LAN sensor network where sensors, controllers and processing stations are connected directly, in WSN, sensors interact wirelessly with central based (processing) stations [11]. The base station (can be a sink node) otherwise known as the gateway, communicates with the wireless sensors via radio link. Data from wireless sensor nodes is transmitted to the gateway (the sink node) directly or through other wireless sensor nodes using multi-hop communication system. Therefore, WSN enables information (data) to be obtained from remote and inaccessible locations for processing. A simple schematic diagram of a WSN is shown *in figure* 1.1.

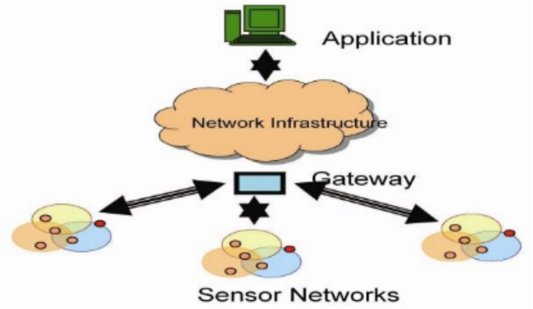


Fig. 1.1 A Wireless Sensor Network

Unlike other popular WSNs, ZigBee is an open standard protocol developed by ZigBee alliance using IEEE 802.15.4 wireless standard. It allows true operability between systems [1]. ZigBee is simpler, requires smaller power, more robust, less expensive, more reliable and secure, and has lower latency, energy efficiency with efficient wireless connectivity infrastructure. This accounts for its wide range of applications in wireless personal area networks and hence ZigBee WSN is one of the most popularly deployed technologies for home automation and monitoring systems.

ZigBee WSNs support three different network topologies, namely star, mesh and cluster tree, the cluster tree being a special case of mesh. Each of these topologies has its strengths and limitations which can be used to advantage in different situations. Although star is considered to be simpler, it has the limitation of ineffectiveness when multi-hop communication is required between nodes. In mesh, configuration of alternative paths is allowed in the network using the most cost effective path, thus allowing multi-hop communication. Hence, mesh connection is more secured, flexible, scalable and reliable.

Moreover, it should also be noted that the topology of a ZigBee network may change as a node moves from one point to another. Topology may also affect the correctness and accuracy of sensor readings, ease of network implementation and network security [19]. Therefore, this paper aims to evaluate these topologies and their corresponding trade-offs, while also looking at the various applications of the technology and the challenges facing the technology causing some constraints and limitations in its applications.

2. ZIGBEE TECHNOLOGY

ZigBee is a new open-standard wireless protocol developed by ZigBee Alliance (consisting of over 270 companies). ZigBee is particularly targeted at low-power, low-cost and low data rate wireless sensor and control networks, aimed at interoperability, it is easy to implement and can support up to 65,000 nodes depending on the type of topologies used [8].

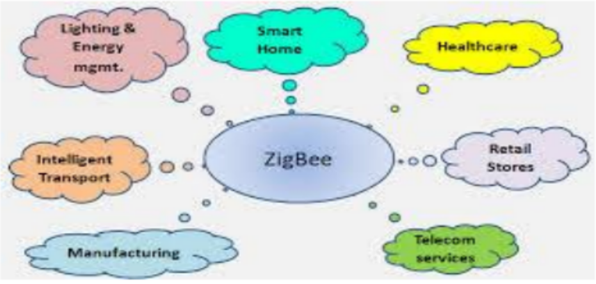


Fig. 1.2: ZigBee Technology Applications

ZigBee has a transmission range of 10 - 100metres. Comparing ZigBee with WiFi and Bluetooth, ZigBee stack is lighter weighted (about 120 KB). It has a maximum throughput of 250Kbps while Bluetooth (except 802.11n) and Wi-Fi transmit at 3Mbps and 54Mbps respectively. While WiFi devices (e.g. WiFi VoIP phones) are reported to have 8 – 12hours of battery lives and Bluetooth devices with a battery life of a few days, many ZigBee devices can boast of a battery life of up to 5years. The huge power saving resulted from relatively short-range of transmission, low data transfer rates and simple protocol stack of ZigBee. The characteristics of WiFi, Bluetooth and ZigBee are summarized and compare in table 1 [5]

Table 1. Characteristics of WiFi, Bluetooth and ZigBee

Features	**WiFi IEEE 802.11**	**Bluetooth IEEE 802.15.1**	**ZigBee IEEE 802.15.4**
Application	Wireless LAN	Cable Replacement	Control and Monitor
Frequency Bands	2.4GHz	2.4GHz	2.4GHz, 868MHz, 915MHz
Battery Life (Days)	0.1-5	1-7	100-7,000
Nodes Per Network	30	7	65,000
Bandwidth	2-100Mbps	1Mbps	20-250Kbps
Range (Metres)	1-100	1-10	1-75 and more
Topology	Tree	Tree	Star, Tree, Cluster Tree, and Mesh
Standby Current	20 * 10-3 amps	200 * 10-6 amps	3 * 10-6 amps
Memory	100KB	100KB	32-60KB

The history of ZigBee started back in 1998 when it was first conceived and supported from development perspective. Though, it was not until December 2004 that ZigBee Alliance published its first ratified specification. It only supported home control lighting [6]. However, ZigBee Alliance no longer supports 2004 specification. In 2006, the 2004 specification was modified to support group addressing, encryption and frame authenticity. In 2007, ZigBee 2007 and ZigBee Pro was published. ZigBee 2007 added new security model to ZigBee 2006 with "trust centre" while ZigBee-Pro has additional software features, more scalability, data fragmentation, stochastic addressing (automated address allocation mechanism) and enhanced security. ZigBee 2007 and ZigBee-Pro are interoperable [9].

2.1 ZigBee Device Types

The operation of a ZigBee node depends on whether it is a full-function device (FFD) or reduce-function device (RFD). The FFD performs all the tasks defined by ZigBee standard while the function performed by the RFD is limited. An FFD can form any type of network (such as star, tree or mesh) while a RFD can only connect to an FFD. With respect to these functionalities, ZigBee devices are classified as Coordinator, Router and End Devices [12].

i. ZigBee Coordinator (ZC)

It is an FFD and a network must contain only one. It starts the network and is responsible for the overall management of the network. In star topology, it is the central node while in tree or mesh topology, it is the root node. Its other functions include address allocation, granting permission to nodes to join or leave network, transfer application packets and keeping list of neighbours table. Because of it functions in the network, it must always be powered on.

ii. ZigBee Router (ZR)

It is also an FFD and can be absent in a network, a network can also contain just one or more depending on the size and topology of the network. It is not required in star topology (figure 2.1). It is often used to expand ZigBee network (in tree and mesh). Basically, it performs all the functions of the coordinator except network establishment (start-up). Constant power source must also be provided for a ZR.

iii. ZigBee End Devices (ZEDs)
They are RFDs and are usually located at the extremities of a network. Their main task is in sending and receiving packets. Other devices cannot connect to the network through a ZED and it cannot relay messages. ZEDs often *sleep* when they are not transmitting or receiving in order to conserve power. At this point in time, they are said to be in *sleep mode*. Therefore they can be battery powered for ease of mobility.

iv. ZigBee Trust Centre (ZTC)
It is a dedicated device (node) in the network whose function is to provide security management, device authentication and key distribution. Where this is not available in the network, the coordinator performs these roles.

v. ZigBee Gateway
The main function of the gateway is to connect the ZigBee network to external network e.g. LAN using protocol conversion.

2.2 ZigBee Network Topologies

Three network topologies are specified for ZigBee network; star, tree and mesh. The depth of a network depends on the network topology and is determined by the number of routers (hops) in the network from the coordinator to the farthest node [8].

i. **Star Topology**
This topology consists of a coordinator and several end devices as shown *in figure* 2.1. It has no router and therefore a star network has a depth of one (1). End devices communicate with each other in the network only through the coordinator. Instead of end devices (*in figure* 2.1), routers can be used. However, router message relay functions will not be used, only its application functions will be used. The end devices or routers now become children to the coordinator

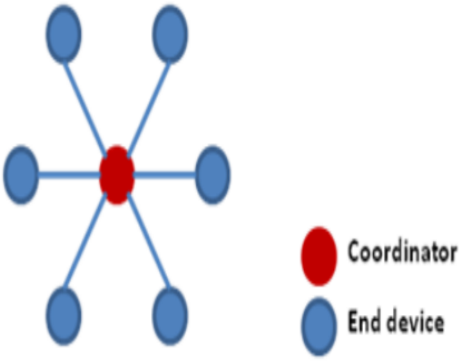


Fig. 2.1 ZigBee Star Topology

The major advantage of a ZigBee star network is its simplicity. The main disadvantage is that it does not provide alternative route for packet transmission and reception. All transmission and reception go through the coordinator. This may increase the burden on the coordinator and hence cause congestion in the network.

ii. **Tree Topology**

In the tree topology, the coordinator (at the top) is connected to several routers and end devices. In this case, the routers and the end devices are coordinator's children. The router is used to extend the network; a router can therefore connect to several other routers and/or end devices to form the router's children as shown *in figure* 2.2. Only the coordinator and the routers can have children and hence can become parents in a tree topology. The end devices cannot have children and therefore cannot become parents.

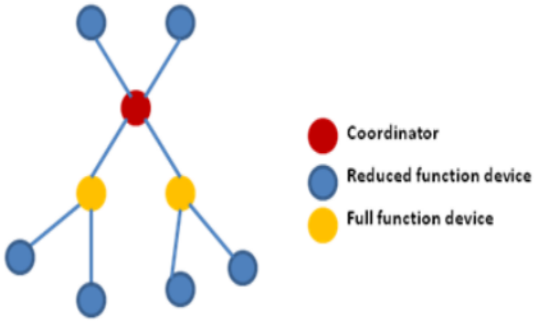


Fig. 2.2 ZigBee Tree Topology

A child is only permitted to communicate directly with its parent and not with any other nodes. Parents can communicate directly with their parents and children.

Like in star, there are no alternative paths to destinations. If a parent is down, its children cannot communicate with other nodes in the network. And even if two nodes in the network are geographically close, their direct communication is not guarantee.

iii. **Mesh Topology**
In mesh, the coordinator is also at the top like that of tree. It consists of a coordinator, several routers and end devices connected as shown *in figure* 2.3. Routers are used to extend network range like in tree. As shown, packets pass through multiple hops to reach destinations and communication between any source and destination in the network is realistic. Hence it is also called a peer-to-peer multi-hop network.

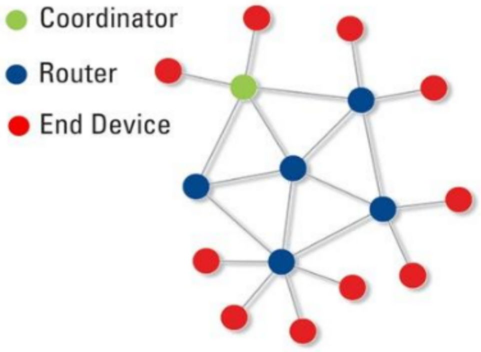


Fig. 2.3 ZigBee Mesh Topology

Moreover, a mesh network provides alternative paths for packet to reach its destination if a path fails. With reference to this, mesh network is usually also being described as a "self-healing" network. Thus adding or removing a node is made easier.

Compared to star and tree ZigBee network configurations, mesh network is more complex and therefore requires more overhead and uses more complex routing protocols.

2.3 ZigBee Protocol Stack

Two types of addresses are in use in ZigBee network; *IEEE address* and *network address*. The IEEE address is a unique 64-bit long address used to identify a ZigBee device. It is assigned to the device by the manufacturer and is also called MAC address or extended address. No two devices can have the same IEEE address in the entire world [12].

The network address (otherwise known as short address) is a 16-bit address that identifies a node locally in the network. It is assigned by a parent to a node when the node joins the network. The advantage of using the 16-bit address is that it extends battery life. A 16-bit address reduces frame size compared to a 64-bit address size and hence reduces transmission time and consequently, increases battery life. The disadvantage is that it is possible for two nodes on different networks to have the same short address.

The ZigBee stack is formed on top of the IEEE 802.15.4 standard. The IEEE 802.15.4 consists of the Physical (PHY) and Media Access Control (MAC) layers while the ZigBee layer is made up of the Network (NWK) layer, the Application Support Sublayer (APS), the ZigBee Device Object (ZDO) and the Security Service as shown in figure 2.4 [20].

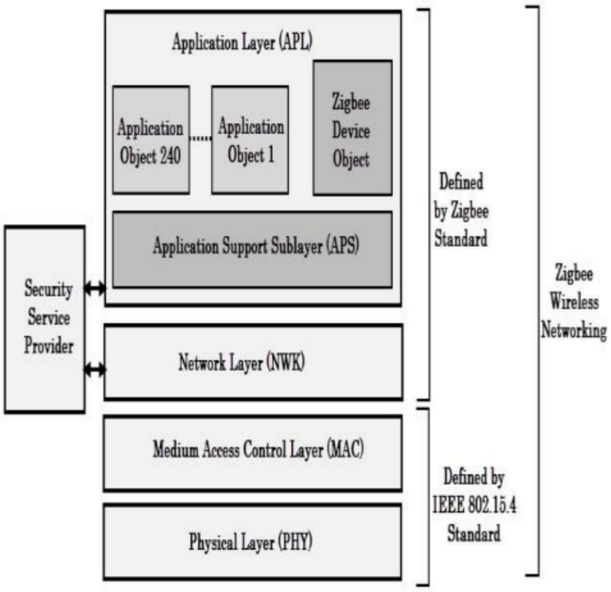

Application Layer (APL)
Application Object 240
Application Object 1
Zigbee Device Object
Application Support Sublayer (APS)
Security Service Provider
Network Layer (NWK)
Medium Access Control Layer (MAC)
Physical Layer (PHY)
Defined by Zigbee Standard
Defined by IEEE 802.15.4 Standard
Zigbee Wireless Networking

Fig. 2.4 ZigBee Protocol Architecture

ZigBee device manufacturers can use the ZigBee application profile to suite their design or they can develop their own application profile

i. ZigBee Physical Layer

The main function of the physical layer is to modulate outgoing signals and demodulates incoming signals. It also deals with transmission and reception of information from sources. The physical layer frequency band consists of 27 channels which are used worldwide [19]. How the bands are shared is shown in table 2.

Table 2. Physical Layer Frequency Band

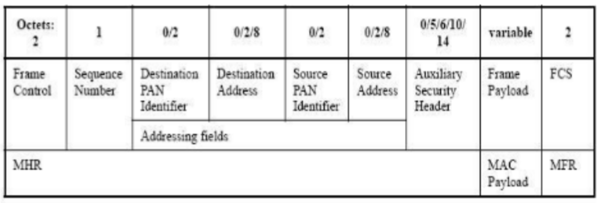
Country	Channel	Channel Width	Frequency Band	Data Rate
Europe	0	600KHz	868-868.6MHz	100Kbps
USA	1-10	2MHz	902-928MHz	250Kbps
Worldwide	11-26	5MHz	2.4-2.4835GHz	250Kbps

Like IEEE 802.11, ZigBee uses mandatory DSSS (Distributed Sequence Spread Spectrum) and optional PSSS (Parallel Sequence Spread Spectrum). And similar to WiFi, a ZigBee network remains on a single frequency picked up automatically by the coordinator when creating the network. However, it can be reconfigured into another frequency by an administrator.

i. ZigBee MAC layer

This layer access the network using CSMA/CA (carrier-sense multiple access with collision avoidance) to enable beacon transmission for synchronization and hence provide reliable transmission. Other functions of this layer include assigning device roles (into ZC, ZR, or ZED), topology design and network association and disassociation.

At MAC layer, ZigBee traffics are carried by frames, unlike WiFi and Bluetooth. The frames are beacon frames, data frames, acknowledge frames and command frames. A frame format of the IEEE 802.15.4 MAC layer is shown *in figure* 2.5. The frame format is not constant (stable). It can change depending on the options that are set in the frame control header bits [22].



Octets: 2	1	0/2	0/2/8	0/2	0/2/8	0/5/6/10/ 14	variable	2
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address	Auxiliary Security Header	Frame Payload	FCS
		Addressing fields						
MHR							MAC Payload	MFR

Fig. 2.5 ZigBee MAC Layer Frame Format

i. ZigBee Network Layer

As shown in *Figure 2.4*, this layer is located between MAC and Application layer. The main functions of the network layer includes network establishment, address assigning, routing and neighbour discovery, adding and removing devices from the network and applying security features to outgoing messages.

ii. ZigBee Application Layer

The application layer is the highest layer in the ZigBee protocol stack. It interfaces a ZigBee system (application object) with its end user. As shown *in Figure 2.4*, the application layer is made up of ZigBee Device Object (ZDO), Application Support Sublayer (APS) and Application Framework [14].

The ZDO Layer assigns functions to all ZigBee devices in the network. It determines whether a device is a coordinator, a router or an end device. It also performs security related functions (such as setting and removal of encryption key) and network management functions (such as network discovery).

The APS Layer enables the interfacing of ZigBee endpoints (application objects) and ZDO with the network layer for network services such as data and management services. This is achieved by receiving the required data (in the form of PDU) from either an application object or ZDO, add a header to create a data frame and then pass it down to the network layer. These services include *request*, *confirm* and *response*, which are provided to the objects for reliable and efficient data transfer [13].

The Application Framework enables different ZigBee devices from different manufacturers to interoperate. For interoperability to be achieved, ZigBee manufacturers must strictly adhere to the application profiles specified by ZigBee Alliance (2006). The two sets of data services specified in the application framework are Generic Message (GM) and Key Value Pair (KVP) services. Using KVP, object attributes can be configured through a simple XML interface. Unlike KVP, GM is more general and as such it uses arbitrary payloads and skips overheads. Exchange of actual data is achieved through ZDO interface using services such as *request*, *confirm* and *indicate*.

ii. Security Service

The security service plane spans and interacts with the NKW and APS layers. It is the security service provider layer of the stack. ZigBee security provides authentication, integrity, freshness and privacy in a ZigBee network. Security is provided using counter mode encryption and cipher block chaining message authentication code (CCM) at different levels with 128 bit Advanced Encryption Standard (AES) algorithm [21].

For all level of security, ZigBee uses symmetric key and applies cryptography and frame integrity to network and application layers. It is the responsibility of an application developer to decide the level of security to apply. A layer is also responsible to protect (secure) a frame that it generated.

ZigBee uses 3 types of keys for security. They are: link, network and master keys.

a) ***Link Key:*** This is used by the APS layer to protect confidentiality and integrity of unicast traffic between two devices. Link key may be preconfigured by device manufacturer, distributed by trust centre, generated from master key or installed on devices using SKKE (Symmetric-Key Key Establishment). In standard security environments, the key can be distributed in plain text [22].

b) ***Network Key:*** This is used to protect and secure group or broadcast traffic in the network. The network key is shared by all network devices. The key can be preconfigured or transported by the trust centre. Over-the-air key transport is not recommended for security reasons. Like the link key, the network key can also be distributed in plain text, however, in a standard security environment.

c) ***Master Key:*** This key is optional. It can be preinstalled or installed by the trust centre. Where applicable, it can be used to generate other keys (network and link keys).

3. ZIGBEE APPLICATIONS

ZigBee technology has find its applications in wide variety of wireless personal area networked systems such as home/industrial automation and monitoring systems due to attracting features to various industries and sectors. Some of the areas in which its applications are found are:

i. ***Home Automation:*** This defines ZigBee applications for automated residential management. ZigBee can be used to remotely control doors, lightings, security alarm, heating, cooling and other residential applications.

ii. ***Commercial Building Automations:*** ZigBee provides means for easy management and maintenance of buildings. An example is found in the monitoring of fire-door positions and smoke detectors operation. With ZigBee all the smoke detectors in a building can be remotely monitored and managed from a central location [17].

iii. ***Smart Energy:*** ZigBee enables wireless communication between home area networks (HAN) and advanced metering infrastructure thereby enhancing quick reading of water, gas and electrical meters. It also helps utility companies to effectively manage services provided to their customers especially during peak demands.

iv. ***Health Care:*** This profile enables remote monitoring of patients in the hospitals and health care centres. Hence, mobility of patients does not affect monitoring. For example, patientsʼ blood pressure can be monitored remotely using ZigBee wireless sensor technology.

v. ***Industrial Process Monitoring and Control:*** With ZigBee, industrial processes are now being controlled and monitored wirelessly. An example is found in industrial inventory tracking where equipment are tagged with wireless sensors and can be located by a ZigBee node.

vi. ***Remote Control for Consumer Electronics:*** Most remote controllers for consumer electronics now uses radio frequency (RF) instead of infrared (IR) with the help of ZigBee RF4CE technology. The limitation of IR remote controller *line of sight* operation is therefore eliminated.

vii. ***Telecommunication Applications:*** Here, ZigBee devices are embedded in smart phones and PDAs thus enabling their communication with other ZigBee enabled devices

4. CHALLENGES OF ZIGBEE SENSOR NETWORK

Despite their countless practical applications in our modern society, however, because of their peculiarity in terms of their non-conventional protocol design, complexity, long network lifetime, bandwidth constraint of communication channel between nodes and fusion canter, balance between communication and data processing, signal processing techniques, etc., WSNs offer numerous and formidable challenges. In order to overcome these challenges, huge efforts are now being placed in research activities, standardization process and industrial investments of wireless sensor networking. The following are some of the challenges and constraints pose by WSNs when compared to other distributed (existing) systems especially in terms of design with respect to protocol and algorithms.

i. ***Energy Limitation***: Wireless sensor nodes are usually powered with batteries and replacing batteries in the field is often not practicable. Since a WSN must operate for a given network operation time or as long as possible, meeting the energy requirement with batteries becomes a challenge [3]. Energy limitation can be improved by the use of solar cells, which can be charged as the battery is being in use. However, this is only applicable to applications in light exposed environments. Also, sensor nodes are now been designed with improved energy efficiency and balanced energy harvesting techniques to enable them operate for several years without battery replacement [10].

ii. ***Self-Management*:** WSNs are usually deployed in remote and harsh environments (which may not be predetermined or engineered) and often without infrastructural support, repair and maintenance. Consequently, sensor nodes are exposed to system and environmental dynamics thus posing a significant challenge for building reliable sensor networks [11]. Therefore the need to build a self-managed WSN network in terms of self-organization, self-optimization, self-protection and self- healing becomes a necessity.

iii. ***Connectivity Challenge*:** The fact that WSNs use wireless communication system also poses a number of challenges to their design especially when maintaining a balance between signal strength, power (transmitted and received) and distance. Increasing the distance between a sensor node and a base station increases the required transmission power and decreases signal strength. For energy and connectivity efficiency, the need to split large distance into several shorter distances using multi hop communication and routing becomes essential. Moreover, in an attempt to conserve energy, some sensor nodes do switch off their radios when they are not in use (*duty cycling*) thereby preventing them from receiving message from neighbours during down time and creating synchronization and connectivity problems. Arbitrary long sleep periods can also reduce the responsiveness and effectiveness of a sensor. However, sensor nodes now use *wake up on demand* strategies and *adaptive duty cycling* to conserve power and still maintain connectivity in WSNs [2, 4]. In *adaptive duty cycling*, some nodes sleep while others are active to form network backbone.

iv. ***Decentralized Management:*** Another challenge to WSN is its infeasibility of centralized management functions such as topology management and routing. This resulted from the fact that WSNs are often large scaled and usually affected by energy constraints. Hence WSN management is usually decentralized to ensure that sensor nodes collaborate with neighbours to make localized decisions. Thus management overhead is consequently reduced although may lead to non-optimal routes.

v. ***Privacy and Security:*** The fact that information collected by a WSN is sensitive, of large scale and sensor nodes are often located in remote, unattended and hostile environments poses privacy and security challenges [21]. Therefore, they are prone to malicious intrusions and attacks such as Denial of Services (DoS), Interrogation, Sybil, Wormhole, Acknowledgement Spoofing, Hello Flood, Routing Information Manipulation and Impersonation [15]. Although, several techniques such as channel hopping and blacklisting, key manipulation, cyclic redundancy check (CRC) and time diversity etc. are in place to tackle these threats, the computational, communication and storage requirements of these techniques still remain a challenge [13]. Hence the need to develop new and better solutions to guarantee the security of WSNs.

5. 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 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 (Bluetooth^{TM}, 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 [5]. Bluetooth only supports star topology, uses master-slave based MAC protocol and full duplex transmission through the use of time-division duplexing.

The simplified version of Bluetooth was released to the public in 2006 and is called Bluetooth Low Energy Technology. Designed to be more efficient (about 15 times than existing Bluetooth), however, it interoperate with existing Bluetooth. This efficiency is achieved by improvement on number of packets transmitted during connection, node discovery and the size of each individual packet [8].

In WSNs, applications of Bluetooth technology are increasing drastically. Bluetooth technology finds application in smart home, automation, health and fitness, mobile telephony, PC and peripherals etc. "*Bluetooth Low Energy will be a significant contributor to the overall Wireless Sensor Network market, representing nearly half of all shipments in 2015*" [23].

ii. WiFi

Based on IEEE 802.11 standards, WiFi 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. WiFi is robust, easily expandable and cost effective. WiFi data transfer rate is up to 300Mbps depending on the standard and has about 100 to 150Mbps through-put. It also has a broad coverage area, some non-line-of-sight (NLOS) transmission capacity, small disturbance of links, and supports mesh networking.

A WiFi-based WSN is a combination of traditional WiFi mesh network and WSN and hence possesses both the features of WiFi mesh network and WSN. Therefore, it is both network-centred and data-centred.

WiFi-based WSNs are used in smart grid, smart agriculture and intelligent environment protection. Also because of WiFi's high bandwidth, fast transmission rate, long transmission distance and NLOS, WiFi-based WSN is being deployed in video monitoring which requires data transition and good-real time.

iii. Z-Wave

Z-Wave is a proprietary low-power and low data wireless communication technology specifically designed for home automation and control. Initially developed by a Danish company, Zen-Sys, it was later acquired by Sigma Designs in 2008 and is now been standardized by Z-Wave Alliance. It uses the 868MHz ISM band and hence unsusceptible to interference due to 802.11 and 802.15.1 devices. Z-Wave uses 9.6kbps and 40kbps with 1% duty cycle limitation and allows up to 100 meters outdoor range. It also supports source-routed mesh networking and allows 232 maximum nodes.

Comparing ZigBee and Z-Wave, they are similar in many respects including areas of application. They are both designed for low power and low through-put. They also both support mesh topology. However, ZigBee is more robust and provides a higher data rate [16].

Z-Wave chips are embedded in consumer electronic products such as TV, remote controls and lighting and thus they can easily form a WSN to enhance home automation, for monitoring and controlling residential, and to light commercial environments.

iv. *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. 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 [3].

One feature of ANT that must be emphasized is its extremely low power consumption compared to other wireless technologies and standards. This is achieved by allowing a system to spend most of its time in an ultra-low sleep mode, wake up quickly, transmit for the shortest possible time and then quickly return back to an ultra-low power sleep mode. Bluetooth power consumption is 10 times higher with 90% higher hardware cost. When compared to ZigBee, ANT is relatively less complex and presents a larger data rate of 1 Mbps [8]. However, ANT lacks interoperability because it is a proprietary technology.

Applications of ANT technology are found in various aspects of WSNs including sport, fitness and wellness applications, home health monitoring and industrial automation.

v. *WirelessHART*

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 [11]. Other key features of WirelessHART includes network wide time synchronization, channel hopping, channel blacklisting, and industry standard AES-128 ciphers and keys.

WirelessHART provides a centralized WSN. The eight types of network devices defined by WirelessHART are network manager, network security, gateway, access point, field device, adapter, router and handheld device. These devices are connected to support network formation, maintenance, reliability, routing and security. The network manager is centralized and maintains up-to-date routes and communication schedules for the network, thereby guaranteeing the network performance. Features common to WirelessHART, Bluetooth, WiFi and ZigBee include the sharing of the unrestricted 2.4 GHz ISM band. But then, they are different from each other in some other aspects. Both WirelessHART and ZigBee are based on IEEE 802.15.4 standard. WirelessHART additionally uses channel hopping and channel blacklisting (useful to minimise persistence noise which is common in industrial set up) while ZigBee only utilizes Direct Sequence Spread Spectrum (DSSS) provided by IEEE 802.15.4. Like ZigBee, WiFi too does not support channel hopping. Like WirelessHART, Bluetooth supports time slots and channel hopping. But while Bluetooth is targeted at Personal Area Network (PAN) with a limited range of 10 metres and only supports star topology, WirelessHART network supports all types of network topology to enhance network scalability. These features make WirelessHART more suitable for industrial applications.

vi. *6LoWPAN*

IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) is another open wireless communication protocol that is targeted on low-power applications that requires wireless internet connectivity at lower data rate and limited form factor. It was released by the IETF in 2007. It allows IPv6packets to be sent to and received from low rate WPAN (IEEE 802.15.4) based networks, thus bringing IP to small devices such as sensor and controllers [18].

Comparing with ZigBee, they are both based on IEEE 802.15.4 standard. However, while 6LowPAN devices can interoperate with other IP-enabled devices, ZigBee node needs an 802.15.4 IP gateway to communicate with an IP network [8]. This IP interoperability makes 6LoWPAN a better option when considering applications that requires interfacing with IP devices or small packet sizes.

Popular wireless network standards such as WirelessHART utilize 6LowPAN to achieve fragmentation and reassembly. Applications of 6LoWPAN inWSNs are found in automation and entertainment applications in home, office and factory environments, security and safety, asset management, heath care and wellbeing etc.

6. CONCLUSION

ZigBee technology 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. It is built on existing IEEE 802.15.4 protocol and therefore combines the IEEE 802.15.4 features and newly added features to meet required functionalities thereby finding applications in wide variety of wireless personal area networked systems. This paper has provided a general overview of the ZigBee sensor networking technology in which its definition, topology, applications and challenges have been presented.

Furthermore, the ZigBee stack protocol and other wireless sensor networking technologies were also discussed; this together with the general overview of the technology is to assist the users in considering the necessary factors when adopting the technology while allowing the vendors and the manufacturer of various ZigBee devices to work out the necessary improvements in the areas with deficiencies.

7. REFERENCES

[1] ZigBee Alliance.: Low-Power, IPv6 Networking for Home Energy Management. (2014). (Online). ZigBee Press, California. Available at: http://www.zigbee.org/920ip-low-power-ipv6-networking-for-home-energy-management-by-zigbee-alliance/ (Accessed 20 September, 2015).

[2] 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)

[3] ANT.: Multi-Channel Design Considerations. (2012). (online). Dynastream Innovations Inc., Alberta. Available at: file:///C:/Users/Owner/Downloads/ANT_AN15_Multi_Channel_Design_Considerations%20(1).pdf (Accessed 23 July, 2015).

[4] Bell, B. S, Kanar, A. M, Kozlowski, S. W.: Current issues and future directions in simulation-based training in North America. The International Journal of Human Resource Management, Vol. 19, 1416–1436. (2008)

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

[6] Blum, B. M.: ZigBee and ZigBee PRO: Which feature set is right for you? EE Times. (2008). [online]. Available at: http://www.eetimes.com/design/microwave-rf-design/4019000/ZigBee-and-ZigBee-PRO-Which-feature-set-is-right-for-you- (Accessed 8 June, 2015)

[7] Bowers, B.: ZigBee Wireless Security: A New Age Penetration Tester's Toolkit. Cisco Press, (2012). (Online): Cisco Press. [Online]. Available at: http://www.ciscopress.com/articles/article.asp?p=1823368&seqNum=4 (Accessed 2 July, 2015).

[8] Buratti, C, Conti, A, Dardari, D.: 2009. An overview on wireless sensor networks technology and evolution. (Online). (2009). Sensors 2009.9. 6869-6896. (2009)

[9] Cache, J, Wright, J, Liu, V.: Hacking Exposed Wireless: Wireless Security Secrets and Solutions. (2nd ed). McGraw Hill, London. (2010)

[10] Chandane, M, Bhirud, S, Bonde, S.: Performance Analysis of IEEE 802.15.4. International Journal of Computer Applications, (e-journal). Vol.40, No.5. (2012)

[11] Dargie, W, Poellabauer, C.: Fundamentals of wireless sensor networks: theory and practice. (e-book). John Wiley & Sons Inc., New Jersey. (2010)

[12] Johnstone, M. N, Jarvis, J. A.: Penetration of ZigBee-based Wireless Sensor Networks. A Proceeding of *Australian information Warfare and Security Conferenece*. (Online). (2011). Available at: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1044&context=isw (Accessed 25 August, 2015).

[13] Kalita, H.K, Kar, A.: 2009. Wireless Sensor Network Security Analysis. International Journal of Next-Generation Networks (IJNGN). (e-journal), (2009). Vol.1, No 1. 1-10.

[14] Karl, H, Willing, A.: 2007. Protocols And Architectures For Wireless Sensor Networks. John Wiley & Sons, New Jersey. (2007).

[15] 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).

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

[17] 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)

[18] Shelby, Z, Bormann, C.: 6LoWPAN: The Wireless Embedded Internet. John Wiley & Sons, New Jersey. (2009)

[19] Silva, I, Guedes, L, Portugal, P, Vasques, F.: Reliability and Availability Evaluation of Wireless Sensor Networks for Industrial Applications. *Sensors, Vol*. 12, No. 1. 806-838. (2012)

[20] IEEE 802.15.4 Standard. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs) IEEE; Piscataway, New Jersey. (2006)

[21] Loukas, G., Oke, G, Gelenbe, E.: Defending against Denial of Service in a Self-Aware Network: A Practical Approach. NATO Symposium on Information Assurance for Emerging and Future Military Systems. Ljubljana, Slovenia.(2008)

[22] Radmand, P.: ZigBee/ZigBee PRO security assessment based on compromised cryptographic keys. Proceeding of International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. (2010). 465-470

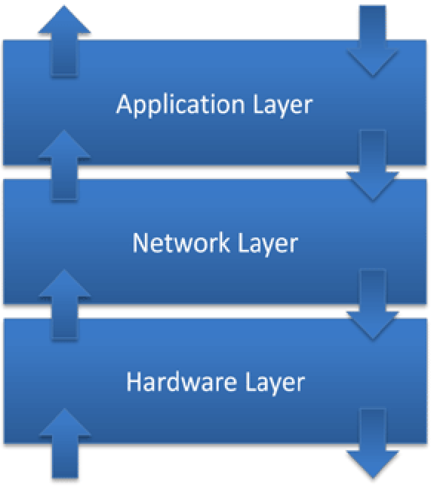
[23] SNRG.: Smart Network Research Group. (Online), (2012). Available at: http://www.pafkiet.edu.pk/Default.aspx?tabid=696 (Accessed 24 August 2015].

Standard Z-wave

Z-Wave è un protocollo wireless progettato **appositamente per la domotica**, il cui ambito di utilizzo comprende l'automazione negli ambienti residenziali, commerciali, ricettivi e assistenziali e le cui applicazioni spaziano dalla domotica alla telesorveglianza e alla telemedicina, per continuare con l'intrattenimento domestico, il controllo accessi, i sistemi di efficientamento e di risparmio energetico. In tutta Europa le unità Z-Wave possono operare alla stessa frequenza di 868.4MHz, nel resto del mondo le frequenze impiegate sono leggermente diverse anche se sempre attorno ai 900 MHz. L'utilizzo di tale banda di frequenze permette di evitare le interferenze con sistemi Wi-Fi, Bluetooth e con gli altri sistemi che operano nella banda dei 2.4 GHz ed inoltre fa sì che il segnale Z-Wave attraversi le pareti degli edifici con maggiore facilità rispetto al segnale Wi-Fi. I livelli MAC e fisico del protocollo, sono stati adottati dall'ITU (International Telecomunicational Unit) e costituiscono in larga parte lo standard T G.99593 la cui evoluzione è affidata a un'organizzazione composta da più di 250 membri denominata Z-Wave Alliance.

Z-Wave home automation technology comprises of three layers. The radio layer, network layer and application layer work together to create a robust and reliable network that enables numerous nodes and devices to communicate with each other simultaneously.

- **Radio Layer**: Defines the way a signal is exchanged between network and the physical radio hardware. This includes frequency, encoding, hardware access, etc.
- **Network Layer**: Defines how control data is exchanged between two devices or nodes. This includes addressing, network organisation, routing, etc.
- **Application Layer**: Defines which messages need to be handled by specific applications in order to accomplish particular tasks such as switching a light or changing the temperature of a heating device.



The Network Layer

The Z-Wave network layer controls how data is exchanged between different devices (nodes) on the network, it consists of three sub-layers.

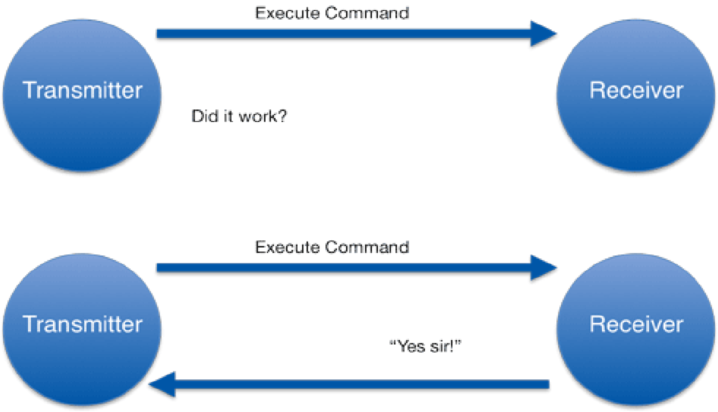
- **Media Access Layer (MAC)**: Controls the basic usage of the wireless hardware (CSMA/CA) - these functions are invisible to the end user.
- **Transport Layer**: Controls message transfer, ensuring error-free communication between two wireless nodes. The end user cannot influence this layer’s functions but the results of this layer are visible.
- **Routing Layer**: Manages Z-Wave’s “Mesh” capabilities to maximise network range and ensure messages get to their destination node. This layer will use additional nodes to re-send the message if the destination is outside of the “direct” range of the transmitting node.

The Media Access (MAC) and Transport Layers Explained

Rather like sending a text message, you can’t see how the information transfers from your phone to theirs. You assume that it’s sent and will be received and read by the recipient. Similarly, wireless home automation technologies use the same principles to enable communication between sender and receiver nodes. Occasionally, a message may get lost.

In a mobile phone's case, it could be due to poor reception. In the case of a home automation network it could be due to interference or positioning the receiver too far away from the sender. In a simple network, the sender gets no feedback on whether the message has been received and if the command has been executed correctly. This can cause stability problems, unless the installation was planned and tested correctly.

Z-Wave is the one of the most reliable wireless technologies, every command sent is acknowledged by the receiver which sends a return receipt to the sender. This doesn't guarantee that the message was delivered correctly, however, the sender will get an indication that a situation has changed, or an error has occurred.



communication with and without acknowledgment

The return receipt is called **Acknowledge (ACK)**. A Z-Wave transceiver will try up to three-times to send a message while waiting for an ACK. After three unsuccessful attempts the Z-Wave transceiver will give up and report a failure message to the user. The number of unsuccessful attempts is also a good indicator of the network's wireless connection quality.

Using Nodes for Successful Communication

A network consists of at least two nodes. To be able to communicate with each other, the nodes need to have access to a common media or need to have "something in common".

In most cases this is a physical communication media like a cable. The communication media for radio (wireless) is the air, which is also used by all sorts of different technologies - TV, Wi-Fi, mobile phones etc. Therefore, each type of "network" needs to have a defined protocol that allows the different nodes of one network to identify each other and to exclude messages from other radio sources.

Each node in the network also needs to have a unique identification to distinguish it from other nodes in the same network.

The Z-Wave protocol defines two identifications for the organisation of the network.

- The **Home ID** is the common identification of all nodes belonging to one logical Z-Wave network. It has a length of 4 bytes = 32 bits.
- The **Node ID** is the address of a single node in the network. The Node ID has a length of 1 byte = 8 bits.

Nodes with different Home IDs cannot communicate with each other, but they may have a similar Node ID. This is because the two networks are isolated from each other. On a single network (one

Home ID) two nodes cannot have identical Node IDs. This means each node can be individually addressed giving you complete control of your own home automation system.

Devices

Z-Wave has two basic types of device:

- **Controllers** - devices that control other Z-Wave devices
- **Slaves** - devices that are controlled by other Z-Wave devices.

Controllers are factory programmed with a Home ID, this cannot be changed by the user. Slaves do not have a pre-programmed Home ID as they take the Home ID assigned to them by the network.

The primary controller includes other nodes into the network by assigning them its own Home ID. If a node accepts the Home ID of the primary controller this node becomes part of the network. The primary controller also assigns an individual Node ID to each new device that is added to the network. This process is known as **Inclusion**.

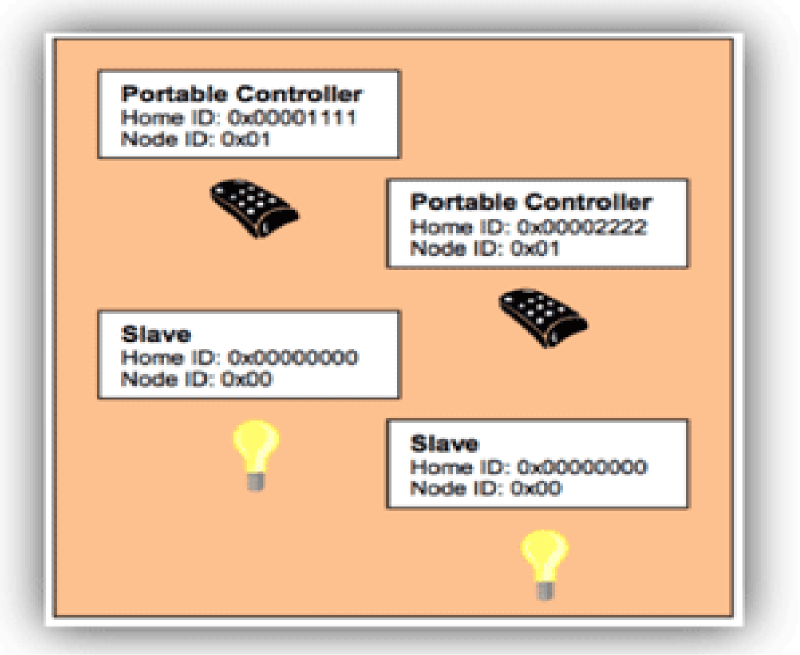
	Definition	In the Controller	In the Slave
Home ID	The Home ID is the common identification of a Z-Wave network	The Home ID is already set as factory default	No Home ID at factory default
Node ID	The Node ID is the individual identification (address) of a node within a common network	Controller has its won Node ID predefined (typically 0x01)	Assigned by the primary controller

Table 1 - Home ID and Node ID comparison

Example

This network has two Controllers with a factory default Home ID and two other Slave devices which do not have any assigned Home ID.

Before Inclusion



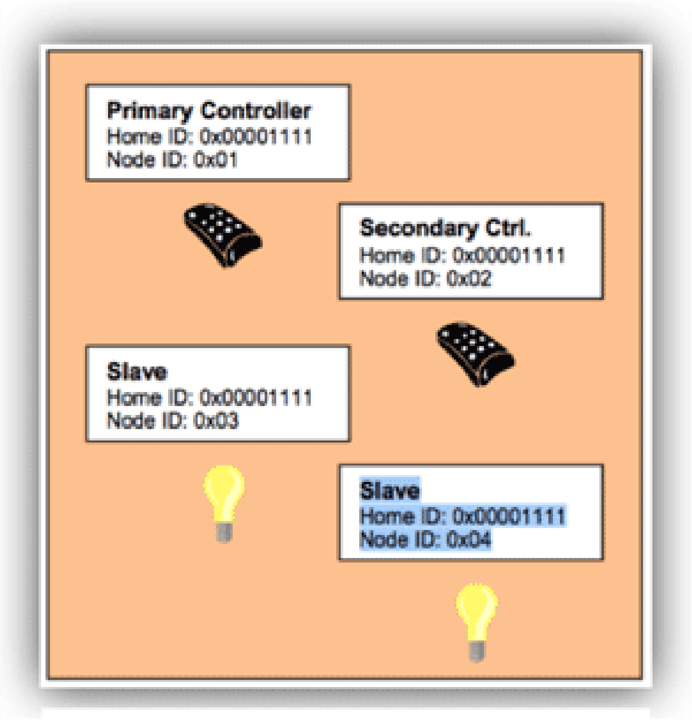
Depending on which of the controllers is used to configure the Z-Wave network, the network Home ID in this example will be either #0x00001111 or #0x00002222.

Both controllers have the same Node ID #0x01 and at this stage the slave devices do not have any Node ID assigned. In theory this picture shows two networks with one node in each of them.

Because none of the nodes has a common Home ID, no communication can take place.

One of the two controllers is now selected as being the primary controller of the network. This controller assigns its Home ID to all the other devices (Includes them) and also assigns them individual Node ID numbers.

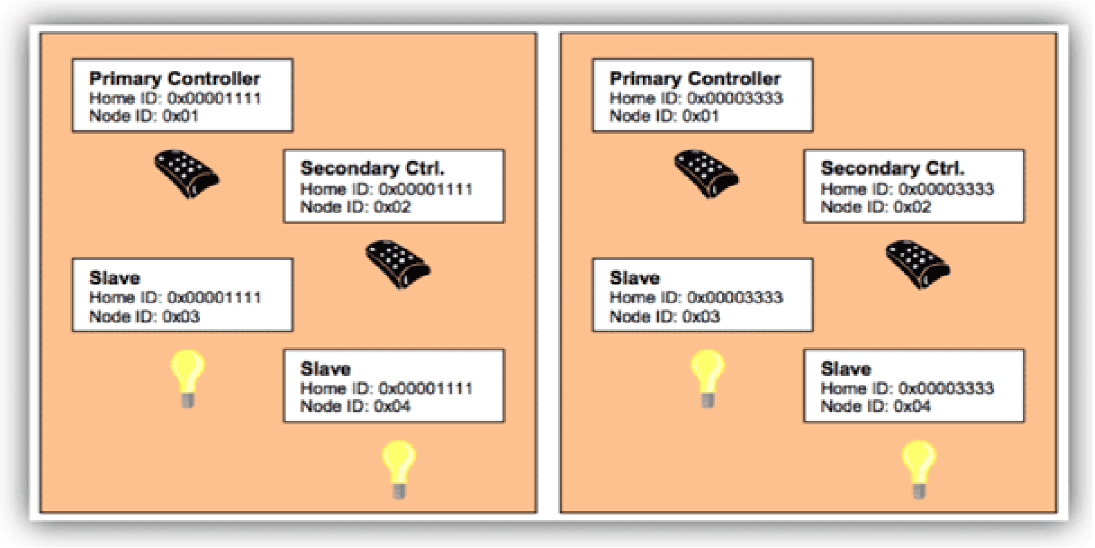
After Inclusion



After successful Inclusion, all nodes have the same Home ID - they are connected to the same network. They also each have a unique Node ID, allowing them to be individually identified and communicate with each other.

In this example there are two controllers. The controller whose Home ID, became the Home ID for all devices, is called the ‘primary controller.’ All other controllers become ‘secondary controllers.’

The primary controller can include further devices, whereas the secondary controller cannot. However, the primary and secondary controllers operate the same in all other respects.



Two Z-Wave networks with different Home IDs co-exist

Because the nodes of different networks cannot communicate with each other due to the different Home ID, they can coexist and do not even “see” each other.

The 32-bit Home ID allows up to 4 billion (2^32) different Z-Wave to networks to be defined, each having a maximum of 256 (2^8) different nodes. However, some of these nodes are allocated by the network for internal communication and special functions, therefore, the Z-Wave network can have a maximum of 232 devices.

Nodes can be removed from a Z-Wave network, this is called Exclusion. During the Exclusion process the Home ID and the Node ID are deleted from the device. The device is reset to the factory default state (controllers have their own Home ID and slaves have no Home ID).

Meshing and Routing

In a typical wireless network the central controller has a direct wireless connection to all of the other network nodes. This requires a direct radio link. However, if there is a disturbance the controller does not have any backup route to reach the nodes and communication will break.

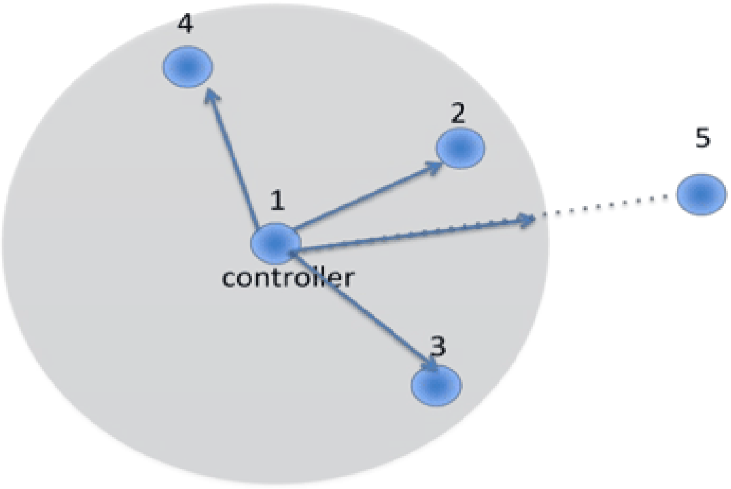


Figure 6 - Network without routing

The radio network in *figure 6* is a non-routed network. Nodes two, three and four are within the radio range of the controller. Node 5 is outside the radio range and cannot be reached by the controller.

However, Z-Wave offers a very powerful mechanism to overcome this limitation. Z-Wave nodes can forward and repeat messages to other nodes that are not in direct range of the controller. This enables Z-Wave to create very flexible and robust networks. Communication can be made to all nodes within the network even if they are outside of direct range or if the direct connection is interrupted.

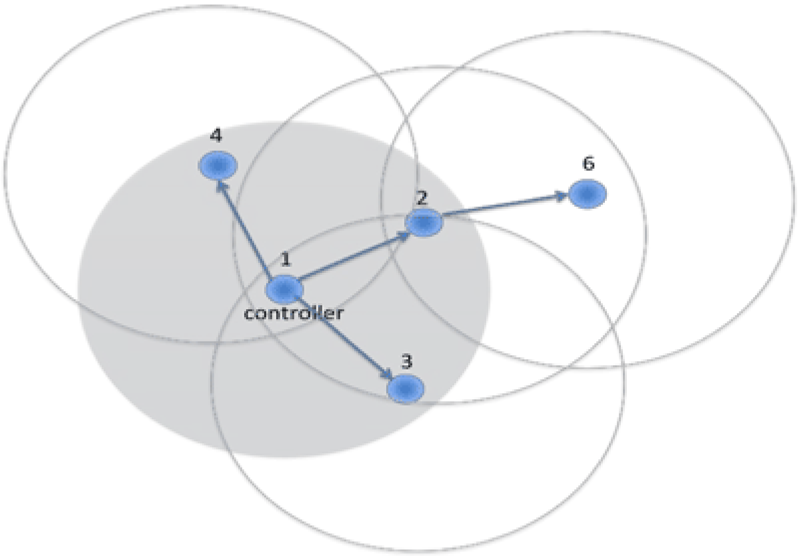


Figure 7 - Z-Wave network with routing

The Z-Wave network with routing (*figure 7*) shows the controller can communicate directly with the Nodes 2, 3 and 4. Node 6 lies outside its radio range, however, it is within the radio range of node 2. Therefore the controller can communicate to node 6 via node 2. This is called a “route”.

Using this routing system, Z-Wave signals can even work around corners! Other technologies work on ‘line of sight’ where every transmitter must have direct sight of the receiver, but Z-Wave simply sends the signal on a small detour around an obstacle using another node.

Z-Wave’s routing can automatically adapt to any changes in the network. For instance *figure 8* shows that direct communication between Node 1 and Node 2 is blocked. But it is still possible for Node 1 to communicate with Node 6 by using Node 3 as an additional repeater.

The more nodes in a network, the more flexible and robust the network becomes.

<u>Z-Wave is able to route messages via up to four repeating nodes</u>. This is a compromise between the network size and stability, and the maximum time a message is allowed to travel in the network.

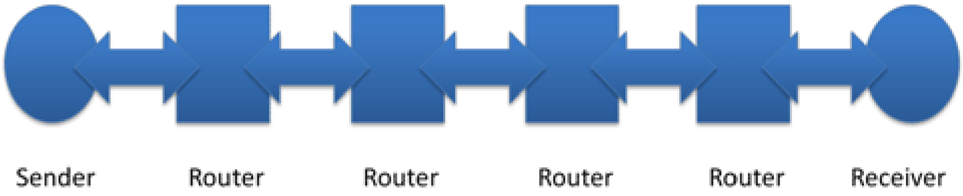


Figure 8 - Maximum distance between two nodes via four repeaters

Building Routes in a Z-Wave Network

Every node is able to determine which nodes are in its direct wireless range. These nodes are called neighbours. During Inclusion and later on Request, the node is able to inform the controller about its list of neighbours. Using this information, the controller is able to build a table that has all information about possible communication routes in a network. This routing table can be accessed by the user and there are several software solutions, typically called installer tools, that visualise the routing table helping you to optimise the network setup.

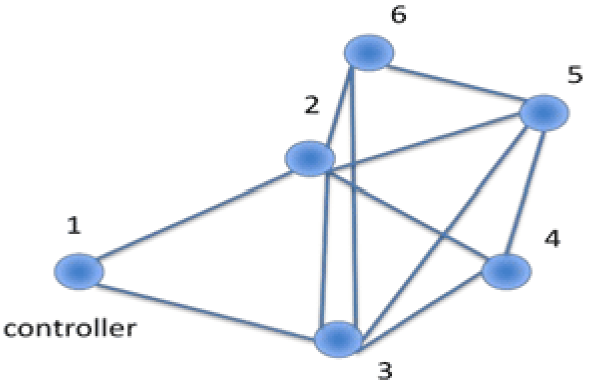
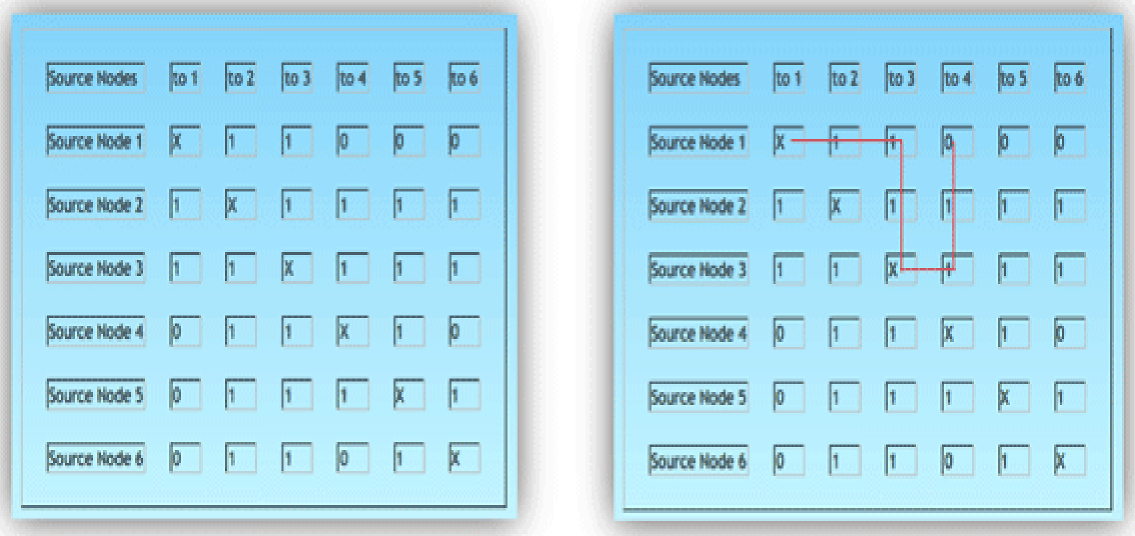


Figure 9 - Routing in a Z-Wave Network

The above diagram (*figure 9*) shows a Z-Wave meshed network, with one controller and five nodes. The controller can communicate directly with node 2 and 3. There is no direct connection to node 4, 5 and 6. Communication to node 4 works either via node 2 or via node 3.

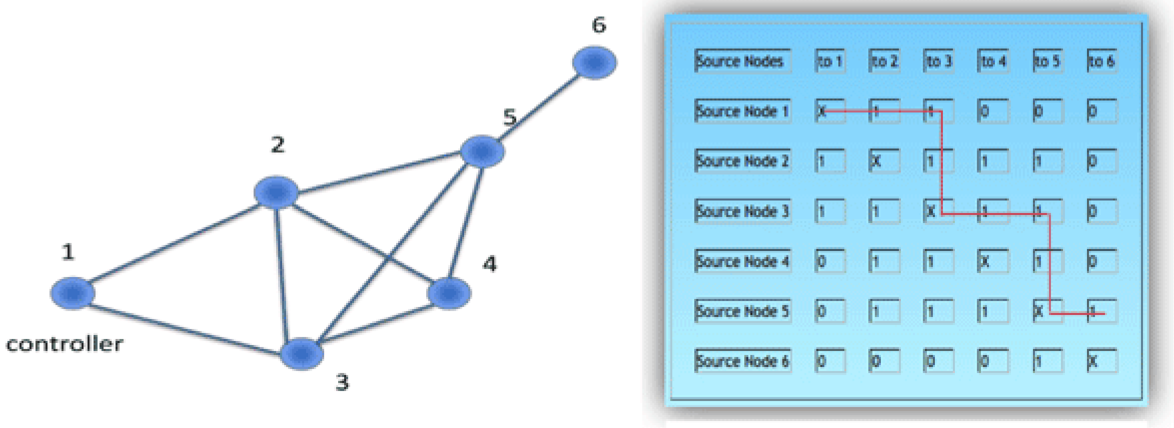


Source Nodes	to 1	to 2	to 3	to 4	to 5	to 6
Source Node 1	X	1	1	0	0	0
Source Node 2	1	X	1	1	1	1
Source Node 3	1	1	X	1	1	1
Source Node 4	0	1	1	X	1	0
Source Node 5	0	1	1	1	X	1
Source Node 6	0	1	1	0	1	X

Source Nodes	to 1	to 2	to 3	to 4	to 5	to 6
Source Node 1	X	1	1	0	0	0
Source Node 2	1	X	1	1	1	1
Source Node 3	1	1	X	1	1	1
Source Node 4	0	1	1	X	1	0
Source Node 5	0	1	1	1	X	1
Source Node 6	0	1	1	0	1	X

Table 2 - Routing table for the Z-Wave Network

The routing for this network is shown in *table 2* - the rows contain the source nodes and the columns contain the destination nodes. A cell with "1" indicates that the nodes are neighbours and a "0" shows there is no direct communication path. The table also shows the connection between Source Node 1 and destination Node 4. The cell between Node 1 and 4 is marked "0". Therefore the network routes the signal via Node 3 which is in direct range of both Node 1 and Node 4.



Source Nodes	to 1	to 2	to 3	to 4	to 5	to 6
Source Node 1	X	1	1	0	0	0
Source Node 2	1	X	1	1	1	0
Source Node 3	1	1	X	1	1	0
Source Node 4	0	1	1	X	1	0
Source Node 5	0	1	1	1	X	1
Source Node 6	0	0	0	0	1	X

Figure 10 - Alternative Z-Wave Netwo Rrouting

Another example (f*igure 10*) shows that Node 6 can only communicate with the rest of the network using Node 5 as a repeater. Since the controller does not have a direct connection to Node 5, the controller needs to use one of the following routes: "**1 -> 3 -> 4 -> 5 -> 6**" or "**1 -> 2 -> 5 ->6**".

A controller will always try first to transmit its message directly to the destination. If this is not possible it will use its routing table to find the next best way to the destination. The controller can select up to three alternative routes and will try to send the message via these routes. Only if all three routes fail (the controller does not receive an acknowledgement from the destination) the controller will report a failure.

Types of Network Nodes

Slaves are categorised as "standard" or "routing" slaves. A **routing slave** includes advanced routing capabilities.

The difference between the three different node types is their knowledge of the network routing table and their ability to send messages to the network.

	Neighbours	**Route**	**Possible functions**
Controller	Knows all neighbours	Has access to complete routing table	Can communicate with every device in the network, if route exists
Slave	Knows all neighbours	Has no information about routing table	Can only reply to the node which it has received the message from. Hence, can not send unsolicited messages
Routing Slave	Knows all neighbours	Has partial knowledge of routing table	Can reply to the node which he has received the message from and can send unsolicited messages to a number of predefined nodes

			he has a route too

Properties of the Z-Wave Device models

Slave	Fixed installed mains powered devices like wall switches, wall dimmers or Venetian blind controllers
Routing Slave	Battery-operated devices and mobile applicable devices as for example sensors with battery operation, wall plugs for Schuko and plug types, thermostats and heaters with battery operation and all other slave applications

Typical Applications for Slaves

Challenges in Typical Network Configurations

Z-Wave network typically starts as a small network that is extended as and when you need. A small network may consist of a remote control and a couple of switches or dimmers. The remote control acts as primary controller and includes and controls the switches and dimmers.

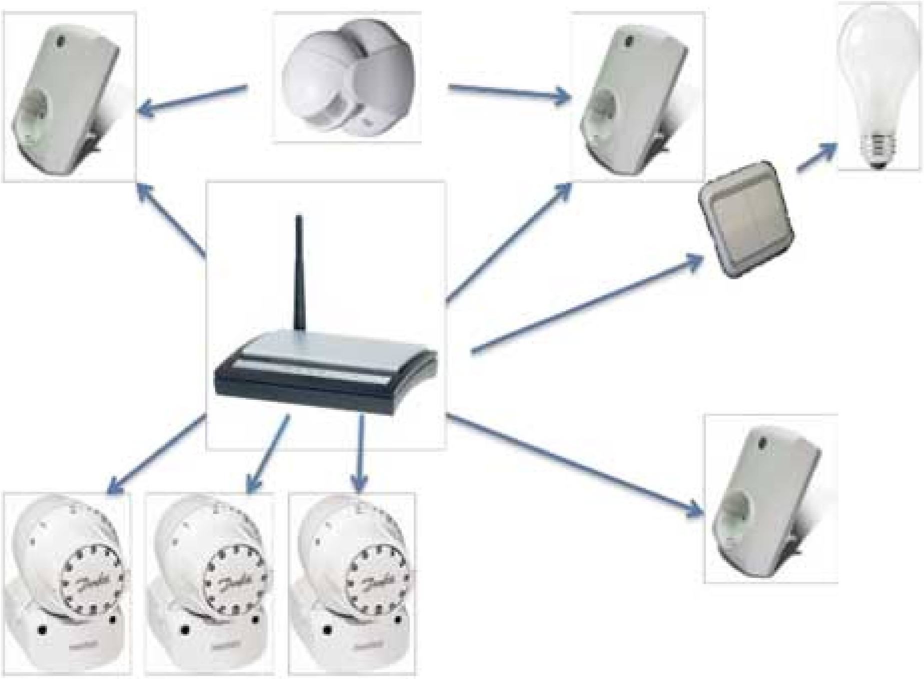
During inclusion the dimmers and switches should be installed at their final location, to ensure that a correct list of neighbours will be recognised and reported.

This type of network configuration works well as long as the remote control can reach all switches and dimmers directly (the node to be controlled is “in range”). If the controlled node is not in range, the user may experience delays, because the remote control needs to detect the network structure first before controlling the device.

In case a device was included and moved afterwards to a new position, this particular device can only be controlled by the remote control if it is in direct range. Otherwise the communication will fail, because the routing table entry for this particular device is wrong and the remote control is not able to do a network scan at the moment of operation.

Z-Wave Network with One Static Controller

Another typical network consists of a static controller - mostly PC software plus Z-Wave USB dongle or an IP gateway together with a number of switches and dimmers.



Z-Wave Network with single static controller

The static controller is the primary controller and includes all other devices.

Because a static controller is bound to a certain location, the other Z-Wave devices must be included while being in direct range with the static controller. They will typically be installed at their final location after inclusion.

Networks with Multiple Controllers

In a larger network several controllers will work together. A static controller is used for the configuration and management of the system and one or several remote controls carry out certain functions in different places.

work with muliple controllers

If a network has multiple controllers, the user needs to determine which of the controllers will be the primary controller.

Inclusion of a static controller is a challenge, if the devices need to be moved to their final location afterwards. A network re-organisation needs to be performed.

Static controllers are usually more reliable and aren’t easily lost. They typically offer backup functions to replace the hardware in case of severe damage.

Network with Portable controller as the Primary Controller

Remote controls are more vulnerable to damage and loss. Usually remote controls do not offer a backup function. If the primary controller was damaged or lost, a complete re-inclusion of the whole network would need to be performed. However, devices can be included after they were installed, which results in a much more stable network, and no need for network re-organisation.

The choice of the primary controller - static or portable - depends more on your personal preference rather than a technical necessity.