

Zigbee Technology Overview.

Within a healthcare context

eklektek Ltd.



Convergent Thinking

www.eklektek.com

Disclaimer : The information contained in this Report is intended solely to provide general guidance on matters of interest for the personal use of the reader, who accepts full responsibility for its use. The information on this Report is provided with the understanding that the authors and publishers are not herein engaged in rendering professional advice or services. As such, it should not be used as a substitute for consultation with professional or other competent advisers. While we have made every attempt to ensure that the information contained in this Report has been obtained from reliable sources, eklektek ltd is not responsible for any errors or omissions, or for the results obtained from the use of this information. All information in this Report is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. Nothing herein shall to any extent substitute for the independent investigations and the sound technical and business judgment of the reader. In no event will eklektek Ltd or its employees or agents, be liable to you or anyone else for any decision made or action taken in reliance on the information in this Report or for any consequential, special or similar damages, even if advised of the possibility of such damages. Certain links in this Report connect to other Web Reports maintained by third parties over whom eklektek Ltd has no control. eklektek Ltd makes no representations as to the accuracy or any other aspect of information contained in other Web Reports.

Contents

1	Technology Overview	3
1.1	Channel Access.....	5
1.2	Routing.....	6
1.3	Network Association.....	6
2	Applications	7
2.1	End Points	7
2.2	Application Profile.....	7
2.3	Endpoint Binding	8
2.3.1	Binding Process	9
3	Comparison	10
3.1	Bluetooth.....	11
4	Market Evolution.....	13
4.1	Self Adopters	13
4.1.1	Engagement.....	13
4.2	Directed Adopters	14
4.3	Outsourcing.....	14
4.4	Virtual Doctor	14
5	Spectrum.....	15
5.1	Spectrum Allocation	15
5.2	Spectrum Congestion	15
6	Security	17
6.1	Unsecured Mode	17
6.2	Secure Mode	17
6.2.1	Access Control List Mode	17
6.2.2	Data Encryption	17
6.2.3	Frame Integrity.....	17
6.2.4	Sequential Freshness.....	18
7	Conclusion	19
8	References.....	20

1 Technology Overview

The Zigbee stack depicted below is the culmination of several years of development work by the [IEEE 802.15 WPAN Task Group 4](#) and the [Zigbee Alliance](#). The IEEE defined the Physical and Medium Access Control layer the Zigbee Alliance specified the higher layers of the stack. The Alliance defines the application aspects of the standard, driven by commercial and technological pragmatism combined with the need to maintain low power consumption.

A detailed description of each of the stack layers can be found in the specifications. This paper aims to give a functional view, providing the reader with a scenario within which to apply the information provided. In many cases a care home for the elderly is the chosen application environment.

This section gives an overview of the first three layers while section 2 looks at the remaining layers dealing with the application aspects of the stack.

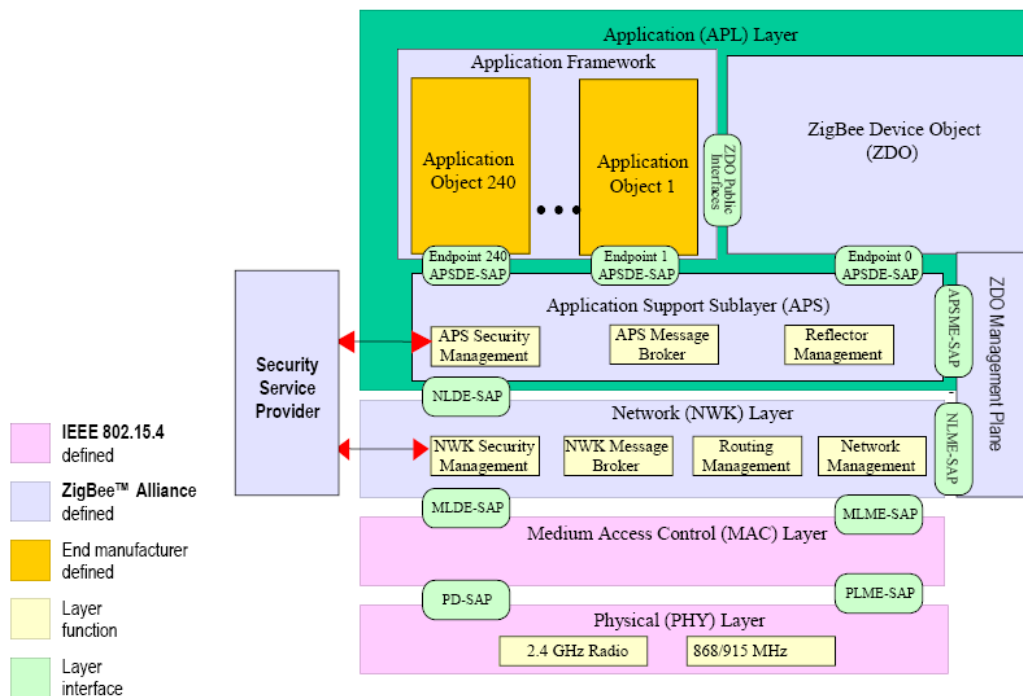


Figure 1 Zigbee stack architecture

Diagram from the Zigbee Specification [1]

ZigBee has been specifically designed to permit many devices, in close proximity, to cooperate. This is the typical arrangement found within hospitals and care homes where many sensors are worn by many patients. Network topologies are chosen to suite the particular target application. Home networking was the main motivation for Star configuration where the network traffic relies on one Coordinator (expanded upon later). Larger networks of devices as found in care homes and hospitals will drive the

deployment of Peer-to-Peer configurations that permit the creation of more exotic structures such as Clustered tree and Mesh configurations.

ZigBee devices are broken into two basic types, Full Functioned Devices (FFD) and Reduced Function Devices (RFD). The latter are typically sensors whose only function is to record and transmit data to the nearest FFD. A RFD is only capable of communication with one other FFD device. FFD's have additional computing resources and are able to communicate with more than one device. A subset of FFD's can perform a co-ordinating function (a coordinator), providing signals (beacons, described later) that make more efficient use of the network bandwidth for a given level of traffic. They may also act as access points to other networks wired or wireless and due to this additional functionality may have power requirements not practically served by batteries.

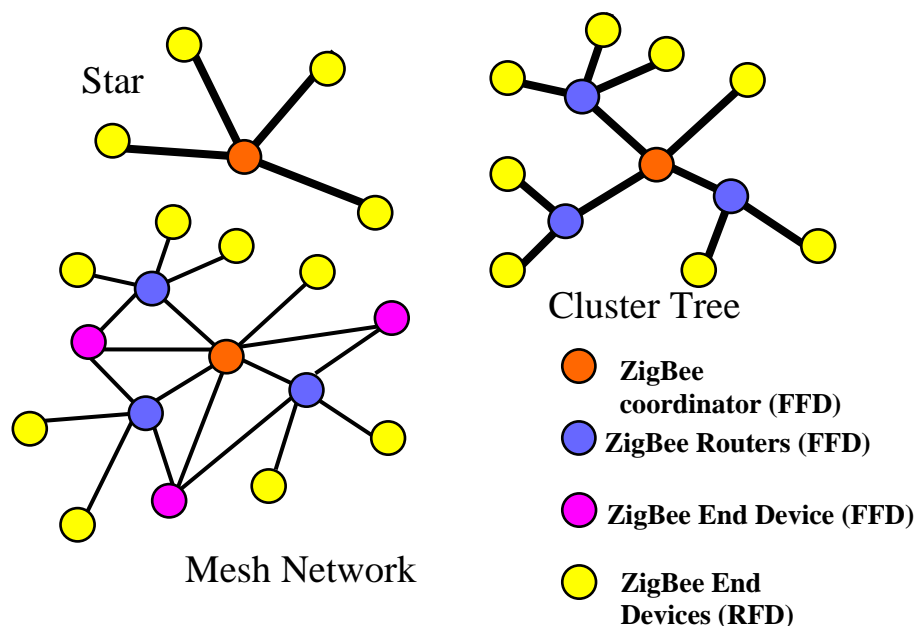


Figure 2 Topologies

In the case of the Cluster tree and Mesh Network another set of FFD's can provide routing capabilities. Routers extend the physical range of the network, permitting end devices to be beyond the radio range of a coordinator. Mesh topology makes further use of FFD's permitting them to perform the function of End Devices. FFD's are not restricted to communication with one other FFD, as in the case of RFD's. This allows data from a FFD to travel multiple paths, this has the result of reducing latency and increasing reliability. If one path fails the alternative path can be used.

A Mesh or Clustered tree will be more suitable for the arrangement found within a care home. In such a situation a patient wearing a Zigbee enabled sensor may move through several tens of meters and in the process disconnect and connect from several routers. In Figure 2 we see some typical network arrangements dependent on the capability of the devices deployed which will impact the price and performance.

All devices possess a unique 64-bit value used for identification. In most circumstances this value can be reduced to 16-bits limiting the number of devices in a network to 65536 adequate for most applications.

1.1 Channel Access

Zigbee is a global technology and as shown in section 5 uses different frequency allocations depending on world location. It is spread over 27 channels some of which are useable everywhere.

Devices share channels, consequently there will be a collision when two or more devices transmit at the same time. To manage this situation devices monitor their chosen channel before transmission and only transmit when the channel is free. If a collision is detected the transmission will be retried some time later. This protocol is called Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA). As the population of devices increases so will the potential for collisions. An increase in device population will cause collisions to increase which will result in a decrease in free channel access and maximum data rate.

All networks have a Pan (Personnel Area Network)-Coordinator that can impose structure on the utilisation of the channels, if the application can tolerate the increased expense. This is achieved through the use of Super Frames which are bounded by Beacons (Figure 3) defining a period of channel access. A Super Frame is divided into 16 slots which may all be accessed using CSMA-CA. In an alternative configuration, the slots between beacons can be divided into two groups. Use of the first group is negotiated at transmission time using CSMA-CA and the latter group are only accessible after prior arrangement between a device and Pan-Coordinator. Once negotiated, use of this second group is contention free with one device having been allocated its own slot. These are called guaranteed time slots (GTS), being used in situations that require minimal network latency, probably in a Telemedicine application when a patient is being closely monitored and real time data is required.

The frequency of Beacons can be varied to manage the traffic load and affect latency. The frequency of Beacons has a direct effect on battery life, as we will see in the comparison section 3. Beacons contain control information including, the Beacon frequency, the Network identifier and the Super Frame structure. However under conditions of very light infrequent traffic the overhead of Super Frames can be high, making their use inefficient. In such situations, beacons will not be used and a network device must use a polling protocol with its Pan-Coordinator. Polling requires the Zigbee devices ask the Pan – Coordinator if there is any data for it. Alternatively it must ask the Pan – Coordinator for permission to transmit if it has data to send.

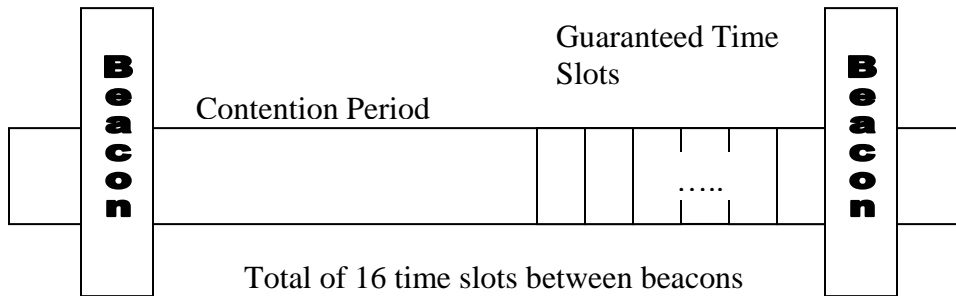


Figure 3 Beacon delimited Super Frame.

Transactions over the physical part of the network make use of Acknowledgements and associated time-outs, when the timeout expires. This protocol is used within both Beacons and non-Beacons networks.

Within a healthcare environment, a Telecare system in sheltered accommodation, is an example of a scenario that might use a non-Beacons network. Such systems monitor infrequent events, such as falls and intruder alerts. These situations are irregular and rare not requiring the overhead of a Beacons network. More data intensive applications requiring frequent data transmission such as Telemedicine will only achieve efficient operation by employing Beacons networks with GTS enabled. Such systems monitor; heart rate, breathing rate, temperature and other vital signs data.

1.2 Routing

Depending upon the chosen topology routing of data can be either trivial or complex and consequently effect the price and performance of the network. In the case of the Star topology, the PAN coordinator can hear all the devices. Each end device will communicate with the coordinator. There is therefore no need for complex routing algorithms. The path from device A to device B remains constant via the coordinator.

Peer to peer networks such as the Cluster Tree and Mesh are more complex requiring sophisticated routing algorithms. They must self heal, providing an alternative when a route is lost due to node failure. The ability to handle devices joining and leaving the network must also be managed.

1.3 Network Association

Network association is the term used to describe the process a device goes through when it joins and leaves a network. The joining process involves determining what devices are in the neighbourhood and adding entries to memory tables. Leaving the net requires that the entries are modified to represent the new state. There are security considerations involved in the association process, as it offers a potential intruder a way into the network.

Network association is a task performed by the Network Layer of the Zigbee stack and should not be confused with Endpoint Binding which relates to connection of Application End points, explained in the following section 2.3.

2 Applications

The applications running on Zigbee devices are intended to conform to an industry wide Profile, this combined with the [Certification process](#) is intended to guarantee interoperability between devices and applications from multiple vendors. Interest groups within the Zigbee Alliance perform the task specifying the base set of requirements for a particular profile. Each application object depicted in the application Layer of the Zigbee stack (Figure 1) must comply with mandatory parts of a profile. Differentiation is enabled by permitting the definition of optional elements of the profile which can extend and enhance the base set of profile requirements.

2.1 End Points

End Points are central to Zigbee applications. An End Point represents either the start (source) or finish (sink) points for data within a Zigbee network. A source of data would typically represent a sensor (transducer) converting one form of energy into electrical energy. A sink, is a destination End Point where data will be processed or moved to another network. In the “Pulse Rate” application depicted in the following sections the destination End Point could be USB connection to a local PC where data is analyzed and stored. Alternatively it may represent access to the internet or GSM network sending the data to analysis services outsourced to India.

The Zigbee Specification permits each device the ability to support up to 240 user definable End Points, each of which maybe involved in a different profile. Other end points exist, but they have predefined functions. For example every Zigbee Compliant device has an End Point 0 (ZD0). Within the Zigbee Specification ZD0 is allocated to perform device management.

2.2 Application Profile

A Zigbee Profile is meta data (data that describes data). It defines enumerations mapping to human readable names used (in application code) to define data flowing between End Points using the same profile. Attributes define values like variables in application source code. Each Attribute has an ID and associated data type. Attributes are grouped into Clusters and Clusters are further grouped to form and define Profiles.

The figure below depicts the components of a Profile, in this case a fictional Pulse Rate Profile consisting of two clusters. In this application the patient wears the monitor. A Mandatory Cluster reports the Beats Per Minute (BPM) of the patient to which it is attached, the source End Point. Within the Mandatory definition this value would be supplied when requested by the Pulse Rate Monitor, the sink End Point.

In this fictional example the Extension Cluster permits the definition of a Period attribute. This value defines the time between updates about which the Monitor wants the Sensor to inform it about the patient’s heart rate. It then becomes the responsibility of the sensor to initiate the transmission of data every “period” seconds.

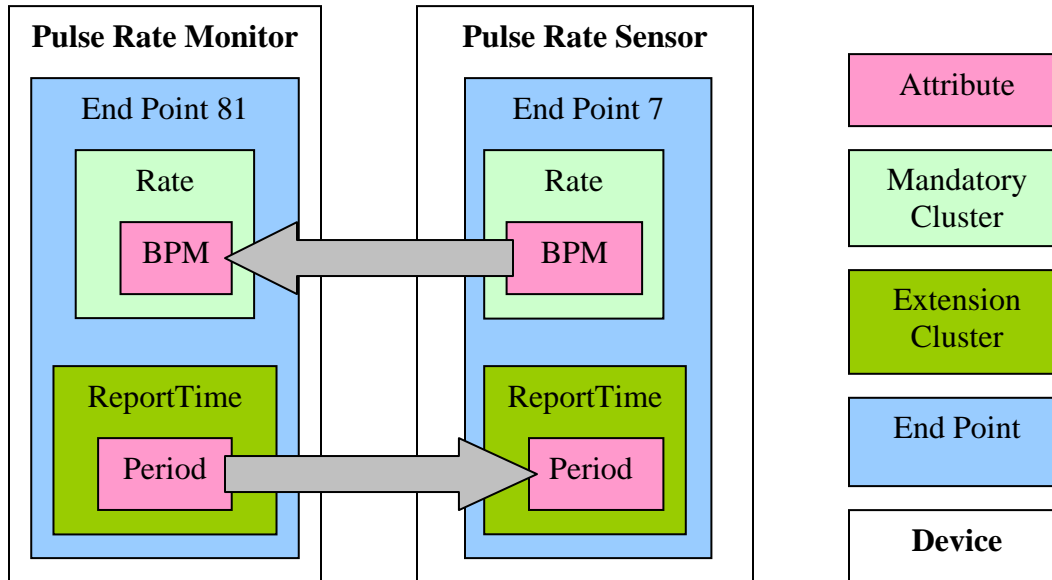


Figure 4 Example Profile with Extension

2.3 Endpoint Binding

End Points represent the interface through which, device resident, applications exchange data with other devices. End Points communicated with other End Points on other Zigbee devices or on the same Zigbee device. The connectivity of End Points is maintained via a binding table.

A Zigbee End Point can consist of one or more Clusters. For example in Figure 4 two Clusters are depicted within the same End Point within one device. Many other arrangements are also valid. Although unlikely multiple, “Rate output Clusters” (Sensors) could exist on a single device each in a different End Point.

The more likely scenario, in the case of the fictional Pulse Rate Profile, would consist of a many to one mapping of a Rate output Cluster (one End Point) on one device, as shown below. This arrangement is duplicated over multiple devices, one per patient. Each Rate output Cluster on each Sensor would map to the same Rate input Cluster on one Pulse Rate Monitor.

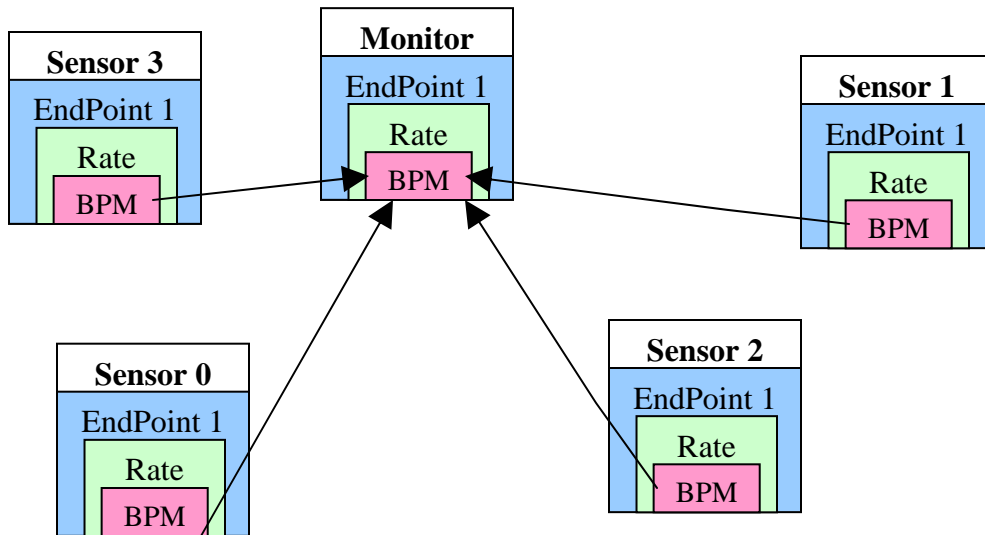


Figure 5 Many to One Binding Example.

Binding of Zigbee devices is performed at the Cluster level by matching an Input Cluster on one device with an Output Cluster on another. The Rate Cluster (input) on a Pulse Rate Monitor must be bound with a Rate Cluster (output) in Pulse Rate Sensor. Figure 5 depicts Many to One binding.

Typically the Monitor device maybe connected to a computer performing analysis and or acting as a gateway permitting remote network access.

2.3.1 Binding Process

In its simplest form the binding process can be initiated by button presses on the devices containing the binding End Points. Typically the process will involve bringing the two devices into close proximity and reducing the transmit energy for the duration of the binding process. This then reduces the opportunity for an eavesdropper.

In large extensive networks it may not be physically possible to bring devices within close proximity. This scenario requires more sophisticate intervention where the new device is added to the network by a human administrator modifying the binding table via programmatic methods.

3 Comparison

Zigbee has a well defined market position in terms of its application space with little overlap with other wireless technologies such as Bluetooth and WiFi.

Zigbee can be characterized by its relative simplicity when compared with the other wireless technologies. This simplicity is possible due to the market segment that it is addressing; multiple, simple devices within a short range of their PAN Coordinator. Typically such devices transmit small amounts of data infrequently at low power. Keeping the power low, keeps the silicon cheap.

	Wi-Fi	Bluetooth	Zigbee
Battery Life	Hours	Days	Months-Years
Network type	WLAN	WPAN	WPAN
IEEE	802.11x	802.15.1	802.15.4
Standards	Wi-Fi Alliance	Bluetooth SIG	Zigbee Alliance
URL	wi-fi.org	Bluetooth.org	Zigbee.org
Range(m)	100	10	30
Max Data Rates	11-54Mbps	1Mbps	20-250Kbps
Main use	Laptop networking	Cable replacement	Sensor networks
BOM (US\$)	9	6	3

Table 1 Wireless Technology Comparison.

Table 1 compares Zigbee (802.15.4) against Bluetooth (802.15.1) and Wi-Fi (802.11x).

Of the three technologies Zigbee offer the best match for patient mounted healthcare applications. From the comparison we see that Zigbee offers greater battery life at lower cost. It does this partly at the expense of maximum data rate which we see varies from 20-250Kbps (maximum) dependent on world location (See section 5). The human body is a slow changing system hence the relatively lower data rate is not a disadvantage for the majority of healthcare applications.

Bluetooth is Zigbee's nearest neighbour the following section 3.1 looks in more detail at the differences between Bluetooth and Zigbee.

3.1 Bluetooth

The Bluetooth SIG (special interest group) in 2004, proposed enhancements (EDR enhanced data rate) to the Bluetooth specification. These modifications increased the data rate to 3Mbps while at the same time reducing the power. The higher data rate means that a Bluetooth device can spend less time transmitting data and more time in a quiescent low power state.

The EDR changes also increased the maximum the number of devices that can form a Bluetooth pico network. This figure has been increased from 8 to 256.

The additional stack complexity of Bluetooth is reflected in the implementation size. At around 250KB the Bluetooth stack requires almost ten times as much memory as Zigbee at around 28KB. Zigbee's modest requirements permits its stack to reside in the Flash memory of many of the Microcontroller devices on the market. Hence we see many Microcontroller manufacturers participating in the activities of the Zigbee Alliance.

Table 2 shows the important quantitative differences between Zigbee and Bluetooth.

Characteristic	ZigBee	Bluetooth
Power profile	Years Optimizes slave power requirements	Days Maximises adhoc functionality
Data Rate	20 - 250 Kbps	1 Mbps
Range	10 - 100 metres Special kit or outdoors up to 400 metres	10 metres 100+ metres dep. on radio
Network Latency (typical) Sleeping slave changing to active	15ms	3s
Operating Frequency	868 MHz, 902 - 928 MHz, 2.4 GHz ISM	2.4 GHz ISM
Complexity	Low	High
Topologies	Ad hoc, star, mesh, hybrid	Ad hoc piconets
Devices per network	2 to 65,000	8
Scalability / Extendability	Very High / Yes	Low / No
Security	128 bit AES and application layer user definable	64 bit, 128 bit

Table 2 Comparison with Bluetooth

Many of these difference we are already aware of, such as the data rate and power profile. However less obvious are the latency times which are important in achieving low power operation. This value places a limit on the time a device can stay in the low power sleeping state and so has a direct effect on battery life. This value is much higher in the Bluetooth case and reasons for this can be gained by considering the way in which Bluetooth makes use of its physical layer, its RF interface.

Bluetooth uses a technique called frequency-hopping spread spectrum (FHSS). It hops 1600 times a second between a maximum of 80 channels following a pseudo random sequence. Using this technique obviously makes eaves dropping difficult, but it also makes the tasks of the receiver synchronising with the transmitter challenging. This fact is reflected in the network latency figures presented in Table 2. Zigbee does not use such an elaborate method of physical layer utilisation (see Section 5.2). The typical time taken

for a Bluetooth device to move from a low power state and to deliver its data is 3 seconds compared to around 15ms for a Zigbee device. Frequency hopping has advantages when interference is present. By moving the channel around the spectrum, the interference is only likely to block the channel for the duration of one or two hops.

The battery life of Zigbee is considerably longer than Bluetooth. This is aided by several of the other characteristics; data rate, complexity and network latency (Sleeping to active). A lower data rate means system clocks are much slower hence less electrical energy has to be dissipated in forcing clocks to change state. Lower stack complexity means there is less code for the processor to execute in order to perform an operation such as sending a packet of data as each processor operation consumes power. Low latency means that a Zigbee device can wake up send its data and then return to the Sleeping state preserving battery life.

In the Bluetooth case a network is referred to as a Piconet and all devices participating in the Piconet must have their hops synchronised and be using the same Pseudo random sequence. This synchronisation typically takes 3s and must occur each time a new device joins the network.

In the Zigbee case the device must wait for Super Frame, a period which can range from 15.36ms to over 4 minutes. This means the network must be configured to meet the requirement of the device requiring the quickest Sleeping to active state. The longer the Super Frame period, the longer devices will stay asleep prolonging battery life. However if the application requires the data to be moved around the network more frequently, then the Super Frame period must be decreased at the expense of battery life.

Zigbee battery life could be dramatically reduced in a non-beaconed network where the population is high, here a device could remain awake for a long time while waiting for a free channel through which to send data.

4 Market Evolution

The impact, of Zigbee, on the healthcare market is likely to be slow initially. The healthcare sector has been quick to see the advantages in wireless deployment. In the Telecare sector wireless is used extensively in the unlicensed 862 to 870Mhz band for short range applications. It greatly reduces installation costs and gives patient freedom and security in the knowledge that they can call for help using a personal alarm. Manufacturers such as [Tunstall](#) make use of wireless in most of their products which include Personal Alarms, Pull Cords, Gas Detectors and Euresis Sensors. Some of these devices may benefit from the extended battery life and additional features that Zigbee could provide, however updating is costly so unlikely to be rapid unless there is competitive pressure.

The Healthcare market is constantly growing and would simply require a forward thinking startup company to produce Zigbee products cheaply in China to force others to follow. There is evidence this trend is starting. [Lusora](#) a London based startup is developing products targeting personal security and home health care.

Incorporating Zigbee into mobile phones is the prerequisite to trigger mass market healthcare applications. Once this occurs two groups of adopters are likely to develop.

4.1 Self Adopters

This early adopting group is computer literate, have knowledge of smart phones and the economic means to own one. They will be familiar with exercise or fitness programs and the technology and devices typically found within a commercial fitness centres.

This group, having an interest in its own health will analyse their own data using software resident in the mobile terminal or PC. Connection to sensors monitoring breathing, temperature and heart rate is likely to be only for the duration of the exercise period and the data recorded is unlikely to be transmitted to a third party for collation and further analysis. However as the market matures and the NHS Information Technology infrastructure develops, so data could be processed by a third party.

Products targeting customers in this market have already come from Garmin who produce a range of [training products](#) monitoring heart rate together with GPS location. Data captured by these devices can either be processed on a local PC or be uploaded to an internet based server for more extensive analysis and archive. Garmin recently acquired [Motion Based](#) who perform this web based function.

4.1.1 Engagement

The Government has identified that the financial burden shouldered by the NHS will only be corrected by changing the behaviour of the public [5]. Engaging the public in its own health will be a slow process, consequently correction in the finances of the NHS will not occur over night. Mobile Phones have become the “must have product” of the young. The

same technology used to verify the taking of exercise can be used to incentivise exercise. Exercise for 30 minutes per day and earn a free ring tone!

4.2 Directed Adopters

Users within this group will be instructed to wear sensors by their care provider. Patients can be monitored and contacted at the first sign of trouble. More engaged patients will be able to monitor their own data.

The network infrastructure already exists to support the transmission of patient data to anywhere in the world. The NHS is currently developing the technology infrastructure to support the collation and processing of huge amounts of vital signs data.

For reasons of cost, this group will use application specific, cost reduced hardware and software. For liability insurance reasons these devices are likely to require safety accreditation not something supported by the manufacturers of mobile phones. Encrypted patient data is more likely to find a cheaper route to the care provider, via the internet rather than one of the wireless networks.

4.3 Outsourcing

Telemedicine was originally seen as a method of delivering healthcare to developing countries lacking in healthcare infrastructure and clinicians. However in recent years, with the dramatic reduction in the price of technology and the increased burden placed upon developed world's healthcare services, the flow has reversed.

Within a Telemedicine scenario where the healthcare provider is remote to the patient the location of the provider is irrelevant. From the perspective of a patient the point of delivery remains unchanged. Hence the provider could be in the next town or on another continent.

The patient however is likely to experience higher levels of service as monitoring can be switched between time zones.

4.4 Virtual Doctor

Algorithms already exist to process vital signs data and identify symptoms of disease. Such algorithms can run over the data faster than real time and alert a real physician if signs of disease are detected. This capability could open a market in the development of new algorithms that sift through gigabytes of patient's data.

5 Spectrum

Zigbee is limited in the Spectrum it can use and in all cases it must co-exist with other wireless standards. The following section looks at spectrum allocation and how Zigbee manages the problems associated with congestion.

5.1 Spectrum Allocation

ZigBee is divided into 27 channels spread over three bands of spectrum dependent on location in the world, with different regulations applying to each of these bands. In Europe, for example, the band 868-868.6 is restricted 20kb/s with a 1% duty cycle. Dependent upon location, two different modulation techniques are employed, which impact the maximum data rate. The channel bandwidth varies depending on the Band, hence the maximum bit rate varies. This information is summarised in Table 3

Band	Max Bit Rate (kb/s)	Channel	Centre Frequencies	Area
868	20	0	868.3	Europe
915	40	1-10	906-924	The America's
2.4	250	11-26	2405-2480	The World

Table 3 Zigbee Spectrum

In the Europe channel 0 resides in the licence exempt band ranging from 862 to 870 MHz allocated to General purpose telemetry and RF door bells. Already used by many Telecare applications. The lower frequencies provide better penetration within buildings.

The Band 2405-2480 is known as the Industrial, Scientific and Medical band (ISM) and is available world wide. Many applications use this range including micro wave ovens and Bluetooth which is likely to result in congestion and a degraded service. Zigbee employs several strategies to cope with congestion and ensure its resilience.

5.2 Spectrum Congestion

Congestion in the 2.4 Ghz band is a potential problem for ZigBee which may ultimately limit its usability and sales. This band is shared by a number of other applications including Microwave ovens, Bluetooth and Wi-Fi. ZigBee provides three mechanisms to manage its operation in a congested region of spectra. ZigBee must also ensure that it minimizes the interference that it generates. The techniques that Zigbee employs are described in the following sections.

Transmitter power is limited by the 802.15.4 standard and indirectly through its market profile and economics. To achieve high transmitter power on a system-on-chip, although possible, would move ZigBee out side of the cost sensitive applications that it is trying to address. Limiting transmitter power limits the interference it can cause.

Channel alignment permits ZigBee to utilize a channel outside the bands of other applications. For example in some configurations of Wi-Fi three consecutive bands (channels) of 22Mhz are used. This forces ZigBee to operate in the guard bands of these channels. The guard band is free area of spectra, between Wi-Fi channels, specified to prevent Wi-Fi channels from interfering with each other. In the Wi-Fi case the guard bands are large enough to accommodate a ZigBee channel. However to detect the existence of the guard bands, ZigBee must perform a channel selection sequence.

Prior to any transmission a **Clear Channel Assessment (CCA)** is performed in accordance with the CSMA-CA channel access protocol. This behaviour reduces the chance of collision with other ZigBee devices and other protocols operating in the same frequency band. Three techniques beyond the scope of this discussion are used to perform a CCA [2].

Channel Selection is only performed after a Clear Channel Assessment. The CCA permits a PAN coordinator to form its Channel List. Each channel is then monitored for the presence of an existing PAN, which might be used by the coordinator in preference to starting a new PAN. The intention being to minimize the number of PANs co-existing in band. The coordinator will start a PAN if no appropriate pre-existing ones can be found.

Use of **Spread Spectrum Modulation** makes ZigBee reasonably immune to narrow band interference. In the 2.4GHz band a 250kb/s transmission is spread over a bandwidth greater than 2MHz. This characteristic protects against interference of bandwidths less than 200khz.

Link Quality Indication (LQI) is provided for each packet of data. It gives the receiving device warning if the data is corrupt, permitting the decision to choose a alternative channel if necessary. The basis of the LQI can be Signal - Strength, Signal to Noise ratio the same techniques used by Clear Channel Assessment.

6 Security

ZigBee uses a combination of techniques to ensure that its data is secure. Typically the ZigBee application space requires minimal implementation to ensure that the required level of service can be achieved with the limited processing resources available. Hence there is always the trade-off between the required level of security and the complexity of the implementation.

To this end ZigBee provides three security modes; Unsecured, Access Control List and Secured Mode. Access Control List can be used on its own or can contribute to Secure Mode.

For patient confidentiality reasons encryption will be required for most medical applications.

6.1 Unsecured Mode

As the name suggest this mode provides no security services. It might be used by applications where security can be ensured through environment. For example the communication maybe taking place within a large area the perimeter of which forces other devices to be out of range. Alternatively, the value of data maybe low and the implementation budget or available processing power unable to support the security overhead. Toys and games fall into this category.

6.2 Secure Mode

In secure mode the implementer is able to mix four security services; Access Control, Encryption, Frame Integrity and Sequential Freshens. These are combined to form seven security suites. For more detail see [1][2]

The four security services are described in the following sections.

6.2.1 Access Control List Mode

In ACL mode a list of devices is maintained with which communication is permitted. The originator of a received message is compared against the list and ignored if their entry is not found. As this mode provides no cryptographic security a spoofing attack is possible where another device mimics the address of a device on the ACL. If spoofing is considered possible then cryptographic security should be employed.

6.2.2 Data Encryption

This service is used to encrypt both control and data messages, however acknowledgments and addresses remain unencrypted.

6.2.3 Frame Integrity

In may Zigbee applications are unlikely to transmit much secret information making encryption less important. Detecting if data has been tampered with and ensuring that the

source is known and trusted is more important. For example controlling a heating system is not a secret activity but ensuring that the source of the controlling data is authorized to perform this operation is important. Zigbee enables these capabilities through the use of Frame Integrity which appends a message integrity code (MIC) to data and control messages. Frame Integrity carries an implementation, memory and bandwidth cost.

6.2.4 Sequential Freshness

Frame Freshness is employed when replay attacks are anticipated. In this attack the attacker does not have access to the cryptographic key instead he records messages with a view to retransmitting them later. To combat this form of attack a freshness value is assigned to each transmission and stored by the receiver. A frame is accepted if its freshness value is more recent than the stored value. The most recent freshness value must be maintained and frames must contain this additional value. For these reasons this additional security method is optional.

7 Conclusion

This paper considers the features of the emerging LR-WPAN (low-rate wireless personal area network) referred to as Zigbee based on IEEE standard 802.15.4 applied to the health care sector. Compared to other short-range wireless technologies such as Bluetooth, Zigbee offers several advantages. Being a simpler standard it requires a less complex, thus smaller software stack and consequently less processor power yielding greater battery life. Typically two AAA batteries should last 2 years. It is specifically targeted at user scenarios requiring a low duty cycle, sending small amounts of data (small packet) infrequently. In the home this encompasses most of the commonly found monitoring and control scenarios including temperature monitoring and control of heating and lighting systems. Zigbee has a free space range of around 200m which reduces to 30m in a typical working environment.

This paper considers the part that Zigbee, coupled with existing mobile network infrastructure can play in enabling the Wireless Healthcare market. The proposition is that mobile phone technology coupled with wireless sensors will have a key role in the future health care of an increasingly aging and obese population.

The majority of the components required to form this system are already in place, these are:

- Global wireless and data networks.
- Powerful backend servers supporting advanced database technology.
- Mobile wireless computers, supporting data collation and packaging.
- *Short range wireless sensor technology.*

Zigbee fulfils the final requirement. Initially adoption will be slow but will rapidly increase when mobile phone vendors incorporate the technology. Analysis yields two likely groups of users; the **Self Adopters** offer a greater market opportunity to the smart phone market. This group is likely to be the first to commercially test the scenarios presented in this paper. They initiate the monitoring of their own health and purchase their own equipment. The second group, the **Directed Adopters** are instructed in the use of monitoring equipment which is supplied to them by their care provider. For reasons of cost, the latter group will use cost reduced hardware and for liability insurance reasons the software is likely to require safety accreditation.

These latter requirements deviate from Mobile Phone manufactures core business, thus it is unlikely they will wish to address the needs of the **Directed Adopters**. Lessons learned from the **Self Adopters** can be applied by health providers. In Public and Private sectors, the business case, for efficiency gains are compelling. Providers can perform around the clock monitoring of patients in their own homes, greatly reducing the problem of bed blocking. Analysis of patient data can be outsourced to anywhere in the world using the most cost effective processing and input from physicians. Around the clock monitoring will lead to higher levels of customer satisfaction.

8 References

[1] **Zigbee Specification.** By Zigbee Alliance

[2] **Low-Rate Wireless Personal Area Networks. Enabling Wireless Sensors with IEEE 802.15.4.** by Gutierrez, Callaway, Barrett IEEE Press

[3] **Microchip Stack for the ZigBee™ Protocol.** by *Nilesh Rajbharti Microchip Technology Inc.*

[4] **802.15.4 Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY)**

Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs) by IEEE Computer Society

[5] **[Wanless Report](#): Resource Requirement chapter 5** by Derek Wanless. HM Treasury