Spectrum Management in the smart home

Pagomenos Apostolos

SID: 3301140009

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Information and Communication Systems

DECEMBER 2015

THESSALONIKI – GREECE

Spectrum Management in the smart home

Pagomenos Apostolos

SID: 3301140009

Supervisor: Dr Andreas Pitsillides

Supervising Committee Members:

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Information and Communication Systems

DECEMBER 2015

THESSALONIKI – GREECE

Abstract

This dissertation was written as a part of the MSc in ICT Systems at the International Hellenic University.

It is generally accepted that the wireless communication has become very popular and its everyday use has increased. Many devices have been developed that provide users a large number of services, aiming to make their lives easier. Their increase rate has a direct result at their domination on the market replacing the wired communication. We live in the era of “smart”. Smart phones, smart televisions, smart cars, and of course smart homes, i.e., they can take decisions and acting alone without the need of human presence.

The home networking market is growing rapidly and wireless technologies play an important role in the smart home networks. Using service-oriented approaches, we determine one of the main challenges of the home networking, the spectrum management. Several wireless technologies of varying bandwidth, operating range, and form factor currently exist or are emerging for the home networking (e.g. Wi-Fi, Bluetooth, ZigBee, WiMAX etc.) and thus may interfere with each other, if some strategy for the management of the spectrum is not provided.

Recent analysis shows that this spectrum is not being utilized efficiently. So, this thesis will involve a literature search of the topic and then the proposal of a strategy for spectrum management. The main scope of this dissertation is to search and create a strategy on how to avoid different wireless systems sharing the same frequency band and operating in the same environment, to interfere with each other and experience a severe decrease in throughput. In the conclusion, we analyze the future of smart home as well as the possible spectrum management strategies should be followed.

Pagomenos Apostolos

11/12/2015

Contents

1 Introduction

Home networking plays undoubtedly a critical role in our everyday life. The main usage of home networking was till now, only how to provide PCs with shared access to the Internet.

However, home networks also provide a wide variety of applications running on different devices such as personal computers, laptops, tablets, smart phones, printers, scanners etc.

Home networking can be easily divided into two categories, *wired* and *wireless*. The competition of technologies in the first category is quite weak. Only a slow replacing of 100 Mbit/s Ethernet technology with its 1 Gbit/s successor can be mentioned. Simultaneously, in the wireless market there is a crowd of competitors. People who choose to install a home network prefer not to tear up walls, but to use the wireless solution. Additionally, home networks usually are connected to other networks and they have subnetworks.

The present thesis is divided as follows: we first analyze the smart home, the main networking areas and current applications of the home networking. Then we focus on the current wireless technologies which can be used for the home networking.

Then, there are comparisons between their technical characteristics and analyze advantages and disadvantages proposing strategies to avoid interference. Finally, we conclude with the possible smart home network of the future as well as mentioning other aspects need to be addressed in future research.

"Gartner is predicting a typical family home could contain more than 500 smart devices by 2022, but right now, most consumers see smart home as a nebulous term without a clear value proposition."

2 SMART HOME

Nowadays everything tends to be automated. In this automative framework the main part of our everyday life, our own house, could not be absent.

2.1 Defining the "Smart Home"

Officially the word "smart" first used during the 70s as identification of technological achievements. Specifically, referring to military products, such as bombs or missiles guided themselves to the goal ("smart bombs").

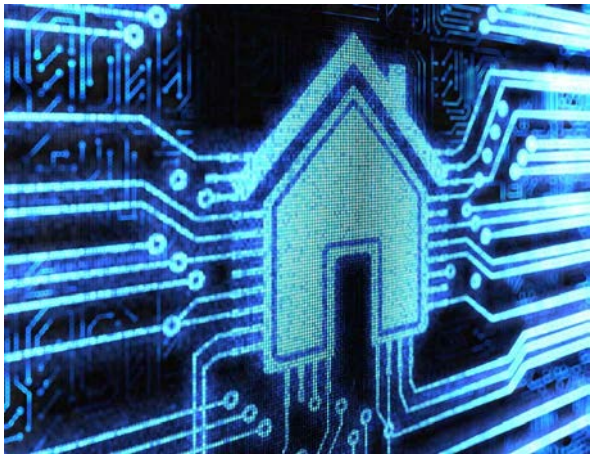
In the technological boom of the 80s the word "smart" acquired other extensions: referring to devices that entailed complete circuits (chips), such as computers and advanced home appliances. Of course, this changed with the lapse of time and no longer is a modern PC called "smart", although the current computers are exponentially stronger than those of the 80s. The term "smart home" was established by the American federation homebuilding in 1984.

A simple definition for the meaning of smart home is:

"Smart home is a house that incorporates a communications network, connecting electrical appliances and services, and allows remote control, monitoring and access to information." [1]

When we talk about remote control we mean that the devices and services can be checked in or out of residence. This definition agrees with most of the cases of smart homes, since almost everything deal with networking and interaction devices. Therefore, the term "smart" does not indicate the actual infrastructure system (networking, sensors, switches, etc.), but refers to the combination of human environment and infrastructure which drive the final user to "smart" results.

2.2 Networking technology in “Smart Home”



The basic technology used in smart home is with no doubt the wireless such as Bluetooth, ZigBee and Wi-Fi. Although many of the technologies they need batteries to power and sometimes are considered inefficient, the advantage of lack of wiring is too “long” for the end user. Indeed, there are researchers who mention that future wireless technologies will be strict prerequisite for any smart home. When dealing with networking on pre-existing houses rather than new, wireless options even look better.

A clear strong point is that the cabling installation can mean quite expensive, especially in a house that is under construction needed interventions. It is estimated that the cost of installing a sensor varies from 50% to 90% of its value. A further advantage of wireless technology is the mobility of devices and users. More specifically, the user can carry easily a device without worrying about cables. Also, it is easy to install and operate a new device to an existing wireless network. Instead, this is not true to a wired network. Despite the many advantages of wireless solutions traditional wiring remains a good choice. It may cost more, it is difficult to be replaced or amended in the future, but wired networking offers distinct advantages such as safety and stability. In those fields the wireless technology lags.

3 WLAN Channels, Frequencies, Bands & Bandwidths

The IEEE 802.11 Wi-Fi / WLAN standards set the attributes for the different channels that may be used. These attributes enable different Wi-Fi modules to talk to each other and effectively set up a WLAN. To ensure that WLAN solutions operate satisfactorily, parameters such as the RF signal centre frequencies, channel numbers and the bandwidths must all be set.

3.1 ISM bands

Wi-Fi is used in unlicensed spectrum (Table 1). This enables users to have access to the radio spectrum without any need for the regulations and restrictions that might be applicable elsewhere. The disadvantage is that the unlicensed spectrum is also shared by many other users and as a result the system has to be resilient to interference.

There are a number of unlicensed spectrum bands in a variety of areas of the radio spectrum. Often these are referred to as ISM bands - Industrial, Scientific and Medical, and they carry everything from microwave ovens to radio communications [19].

Table 1: The main bands used for carrying Wi-Fi

LOWER FREQUENCY MHZ	UPPER FREQUENCY MHZ	COMMENTS
2400	2500	Often referred to as the 2.4 GHz band, this spectrum is the most widely used of the bands available for Wi-Fi. Used by 802.11b, g, & n. It can carry a maximum of three non-overlapping channels.
5725	5875	This 5 GHz band or 5.8 GHz band provides additional bandwidth, and being at a higher frequency, equipment costs are slightly higher, although usage, and hence interference is less. It can be used by 802.11a & n. It can carry up to 23 non-overlapping channels, but gives a shorter range than 2.4 GHz.

3.1.1 802.11 Systems & Bands

There are several different 802.11 variants in use (Table 2). Different 802.11 variants use different bands.

Table 2: Summary of the bands used by the 802.11 systems

IEEE 802.11 VARIANT	FREQUENCY BANDS USED
802.11a	5GHz
802.11b	2.4GHz
802.11g	2.4GHz
802.11n	2.4 & 5 GHz
802.11ac	Below 6GHz
802.11ad	Up to 60 GHz
802.11af	TV white space (below 1 GHz)
802.11ah	700 MHz, 860MHz, 902 MHz, etc. ISM bands dependent upon country and allocations

3.2 2.4 GHz 802.11 CHANNELS & FREQUENCIES

There are 14 channels defined for use by Wi-Fi 802.11 for the 2.4 GHz ISM band. Not all of the channels are allowed in all countries: 11 are allowed by the FCC and used in what is often termed the North American domain, and 13 are allowed in Europe where channels have been defined by ETSI. The WLAN / Wi-Fi channels are spaced 5 MHz apart (with the exception of a 12 MHz spacing between the last two channels).

The 802.11 WLAN standards specify a bandwidth of 22 MHz and a 25 MHz channel separation, although nominal figures for the bandwidth of 20 MHz are often given. The 20 / 22 MHz bandwidth and channel separation of 5 MHz means that adjacent channels overlap and signals on adjacent channels will interfere with each other.

The 22 MHz channel bandwidth holds for all standards even though 802.11b WLAN standard can run at variety of speeds: 1, 2, 5.5, or 11 Mbps and the newer 802.11g standard can run at speeds up to 54 Mbps. The differences occur in the RF modulation scheme used, but the WLAN channels are identical across all of the applicable 802.11 standards [17].

When using 802.11 Wi-Fi to provide WLAN solutions for any WLAN applications, it is necessary to ensure that parameters such as the channels (Table 3) are correctly set to ensure the required performance is achieved [19].

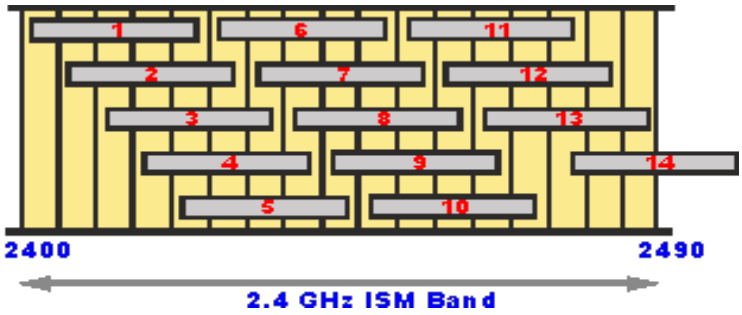
Table 3: Frequencies of the 802.11 Wi-Fi channels that are available around the globe

CHANNEL NUMBER	LOWER FREQUENCY MHZ	CENTER FREQUENCY MHZ	UPPER FREQUENCY MHZ
1	2401	2412	2423
2	2404	2417	2428
3	2411	2422	2433
4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2451	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483
14	2473	2484	2495

3.2.1 2.4 GHz 802.11 Overlap & Selection

The channels used for Wi-Fi are separated by 5 MHz in most cases but have a bandwidth of 22 MHz as a result channels overlap and it can be seen that it is possible to find a maximum of three non-overlapping channels. Therefore if there are adjacent pieces of WLAN equipment that need to work on non-interfering channels, there is only a possibility of three.

The 5 combinations of available non overlapping channels are given below: (Picture 1)



Picture 1: Wi-Fi Channel overlap and which ones can be used as sets.

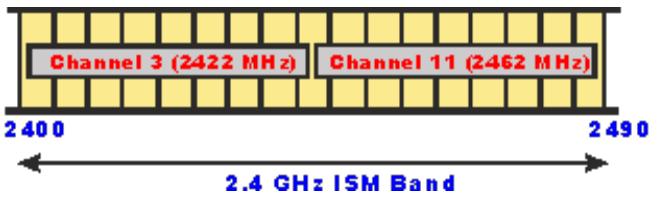
From (Picture 1), Wi-Fi channels 1, 6, 11, or 2, 7, 12, or 3, 8, 13 or 4, 9, 14 (if allowed) or 5, 10 (and possibly 14 if allowed) can be used together as sets. Usually, Wi-Fi routers are set to channel 6 as the default, and therefore the set of channels 1, 6 and 11 is possibly the most widely used.

As some energy spreads out further outside the nominal bandwidth, if only two channels are used, then the further away from each other the better the performance.

It is found that when interference exists, the throughput of the system is reduced. It therefore pays to reduce the levels of interference to improve the overall performance of the WLAN equipment [19].

With the use of IEEE 802.11n, there is the possibility of using signal bandwidths of either 20 MHz or 40 MHz. When 40 MHz bandwidth is used to gain the higher data throughput, this obviously reduces the number of channels that can be used.

The (Picture 2) shows the 802.11n 40 MHz signals.



Picture 2: 802.11n 40 MHz channel capacity

3.2.2 2.4 GHz 802.11 Channel Availability

If we observe carefully the differences in spectrum allocations and different requirements for the regulatory authorities globally, we can assume that not all the WLAN channels are available in every country (Table 4).

Table 4: The availability of the different Wi-Fi channels in different parts of the world

CHANNEL NUMBER	EUROPE (ETSI)	NORTH AMERICA (FCC)	JAPAN
1	✔	✔	✔
2	✔	✔	✔
3	✔	✔	✔
4	✔	✔	✔
5	✔	✔	✔
6	✔	✔	✔
7	✔	✔	✔
8	✔	✔	✔
9	✔	✔	✔
10	✔	✔	✔
11	✔	✔	✔
12	✔	No	✔
13	✔	No	✔
14	No	No	802.11b only

This table provides a general view, and there may be variations between different countries. For example some countries within the European zone Spain have restrictions on the channels that may be used (France: channels 10 - 13 and Spain channels 10 and 11) use of Wi-Fi and do not allow many of the channels that might be thought to be available, although the position is likely to change.

3.3 3.6 GHz Wi-Fi Band

The following band of frequencies (Table 5) are only allowed for use in USA known as 802.11y. In this band high powered stations can be used as backhaul for networks, etc.

Table 5:3.6 GHz 802.11y channels

CHANNEL NUMBER	FREQUENCY (MHZ)	5 MHZ BANDWIDTH	10 MHZ BANDWIDTH	20 MHZ BANDWIDTH
131	3657.5	✔		
132	36622.5	✔		
132	3660.0		✔	
133	3667.5	✔		
133	3665.0			✔
134	3672.5	✔		
134	3670.0		✔	
135	3677.5	✔		
136	3682.5	✔		
136	3680.0		✔	
137	3687.5	✔		
137	3685.0			✔
138	3689.5	✔		
138	3690.0		✔	

Note: The channel centre frequency depends upon the bandwidth used. This accounts for the fact that the centre frequency for various channels is different if different signal bandwidths are used [19].

3.4 5 GHz Wi-Fi CHANNELS & FREQUENCIES

While the 2.4 GHz band is overcrowded, many users select to use the 5 GHz ISM band (Table 6). This not only provides more spectrum, but it is not as widely used by Wi-Fi as well as many other appliances including items such as microwave ovens. Many of the 5 GHz Wi-Fi channels fall outside the accepted ISM unlicensed band resulting various restrictions which are placed on operation at these frequencies [19].

Table 6: 5GHz Wi-Fi channels

CHANNEL NUMBER	FREQUENCY MHZ	EUROPE (ETSI)	NORTH AMERICA (FCC)	JAPAN
36	5180	Indoors	✔	✔
40	5200	Indoors	✔	✔
44	5220	Indoors	✔	✔
48	5240	Indoors	✔	✔
52	5260	Indoors / DFS / TPC	DFS	DFS / TPC
56	5280	Indoors / DFS / TPC	DFS	DFS / TPC
60	5300	Indoors / DFS / TPC	DFS	DFS / TPC
64	5320	Indoors / DFS / TPC	DFS	DFS / TPC
100	5500	DFS / TPC	DFS	DFS / TPC
104	5520	DFS / TPC	DFS	DFS / TPC
108	5540	DFS / TPC	DFS	DFS / TPC
112	5560	DFS / TPC	DFS	DFS / TPC
116	5580	DFS / TPC	DFS	DFS / TPC
120	5600	DFS / TPC	No Access	DFS / TPC
124	5620	DFS / TPC	No Access	DFS / TPC
128	5640	DFS / TPC	No Access	DFS / TPC
132	5660	DFS / TPC	DFS	DFS / TPC
136	5680	DFS / TPC	DFS	DFS / TPC
140	5700	DFS / TPC	DFS	DFS / TPC
149	5745	SRD	✔	No Access
153	5765	SRD	✔	No Access
157	5785	SRD	✔	No Access
161	5805	SRD	✔	No Access
165	5825	SRD	✔	No Access

3.5 ADDITIONAL BANDS & FREQUENCIES

New formats are being developed which will use new frequencies and bands (Table 7). Technologies employing white space usage and new standards using bands that are located into the microwave region delivering in gigabit transfer speeds are being developed. Such technologies will require the use of new spectrum for Wi-Fi.

Table 7: Wi-Fi new formats

WI-FI TECHNOLOGY	STANDARD	FREQUENCIES BANDS
White-Fi	802.11af	470 - 710MHz
Microwave Wi-Fi	802.11ad	57.0 - 64.0 GHz ISM band (Regional variations apply) Channels: 58,32, 60.48, 62.64, and 64.80 GHz

As WLAN and Wi-Fi technology develops further new bands will be added to enable sufficient interference bandwidth to be available to ensure the ever increasing requirement for the transfer of high speed data [19].

4 COMPETING WIRELESS TECHNOLOGIES

IEEE 802.11, IEEE 802.16 - WiMAX, IEEE 802.15.4 - ZigBee, Bluetooth, IEEE 802.22 – Cognitive Radio, SRD – Short Range Device Applications

4.1 IEEE 802.11 WI-FI STANDARDS

Picture 3: Wi-Fi Logo

From WLAN solutions that are available, the IEEE 802.11 standard, Wi-Fi (Picture 3), has become the known standard. The operating speeds of systems using the IEEE 802.11 standards are up to 54 Mbps. Because of the flexibility and performance of Wi-Fi, Wi-Fi "hotpots" are widespread and in use at a high rate [8].

Table 8: IEEE 802.11 standards

802.11a	5 GHz ISM band with data rate up to 54 Mbps
802.11b	2.4 GHz ISM band with data rates up to 11 Mbps
802.11e	Quality of service and prioritization
802.11f	Handover
802.11g	2.4 GHz ISM band with data rates up to 54 Mbps.
802.11h	Power control
802.11i	Authentication and encryption
802.11j	Interworking
802.11k	Measurement reporting
802.11n	2.4 and 5 GHz ISM bands with data rates up to 600 Mbps
802.11s	Mesh networking
802.11ac	Below 6GHz with data rates of at least 1Gbps per second for multi-station operation and 500 Mbps on a single link
802.11ad	Very high throughput at frequencies up to 60GHz
802.11af	Wi-Fi in TV spectrum white spaces (often called White-Fi)
802.11ah	Wi-Fi using unlicensed spectrum below 1 GHz for long range communications and support for the Internet of Everything

From the above standards (Table 8) the most widely known are the most network bearer standards, 802.11a, 802.11b, 802.11g and 802.11n.

All the 802.11 Wi-Fi standards operate within the ISM (Industrial, Scientific and Medical) frequency bands. These are shared by a variety of other users, but no license is required for operation within these frequencies. This makes them ideal for a general system for widespread use.

The 802.11n standard is the latest providing raw data rates of up to 600 Mbps. Each of the different standards has different features and they were launched at different times. The first accepted 802.11 WLAN standard was 802.11b. This used frequencies in the 2.4 GHz Industrial Scientific and Medial (ISM) frequency band, this offered raw, over the air data rates of 11 Mbps using a modulation scheme known as Complementary Code Keying (CCK) as well as supporting Direct-Sequence Spread Spectrum, or DSSS, from the original 802.11 specification.

802.11a was defined at the same time which used a different modulation technique, Orthogonal Frequency Division Multiplexing (OFDM) and used the 5 GHz ISM band. Of the two standards it was the 802.11b variant that caught on. This was primarily because the chips for the lower 2.4 GHz band were easier and cheaper to manufacture.

The 802.11b standard became the main Wi-Fi standard. Looking to increase the speeds, another standard, 802.11g was introduced and ratified in June 2003. Using the more popular 2.4 GHz band and OFDM, it offered raw data rates of 54 Mbps, the same as 802.11b. In addition to this, it offered backward compatibility to 802.11b. Even before the standard was ratified, many vendors were offering chipsets for the new standard, and today the vast majority of computer networking that is shipped uses 802.11g [8].

4.2 IEEE 802.16 - WiMAX

IEEE 802.16, WiMAX or Wireless Microwave Access technology provides 4G levels of Broadband Wireless Access for both mobile and fixed applications. WiMAX is a broadband wireless data communications technology based on IEEE 802.16 standard providing high speed data over wide areas.

WiMAX technology meet the needs of a large variety of users from those in developed nations wanting to install a new high speed data network very cheaply without the cost and time required to install a wired network, to those in rural areas needing fast access where wired solutions may not be viable because of the distances and costs involved. Additionally it is being used for mobile applications, providing high speed data to users on the move [20]. The standard for WiMAX technology specializes in point-to-multipoint broadband wireless access. WiMAX technology uses some key technologies to enable it to provide the high speed data rates:

OFDM (Orthogonal Frequency Division Multiplex): OFDM has been incorporated into WiMAX technology to enable it to provide high speed data without the selective fading and other issues of other forms of signal format.

MIMO (Multiple Input Multiple Output): WiMAX technology makes use of multipath propagation using MIMO.

4.2.1 WiMAX Versions

There are two "flavors" of WiMAX technology that are available:

802.16d (802.16-2004)

802.16e (802.16-2005)

The two flavors of WiMAX technology are based on the same standard but they are used for different applications [20].

The 802.16d version is closer to what may be termed the original version of WiMAX defined under 802.16a. It is aimed at fixed applications and providing a wireless equivalent of DSL broadband data. In fact the WiMAX Forum describes the technology as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL." It is able to provide data rates of up to 75 Mbps and as a result it is ideal for fixed, DSL replacement applications. It may also be used for backhaul where the final data may be distributed further to individual users. Its cell radius is 75 km.

The 802.16e currently provides the ability for users to connect to a WiMAX cell from a variety of locations, and there are future enhancements to provide cell handover. 802.16e is able to provide data rates up to 15 Mbps and the cell radius distances are typically between 2 and 4 km. Although initially it was thought that there could be significant competition with Wi-Fi, there are other areas to which WiMAX is posing a threat. Cell phone operators saw the mobile version of WiMAX as a significant threat. It is offering data download speeds in excess of those that can be offered even using the cellular UMTS HSPA (High Speed Packet Access). However LTE has gained acceptance as the global cellular telecommunications system. WiMAX technology is now being deployed in many areas and while it was initially seen as yet another wireless standard that might fall into the background, it is now emerging as a major front runner and posing threats to other areas of the industry.

4.2.2 WiMAX Frequencies and Spectrum Allocations

The IEEE 802.16 WiMAX standard enables data transmission using multiple broadband frequency ranges. The 802.16a standard specified transmissions in the range 10 - 66 GHz, but 802.16d allowed lower frequencies in the range 2 to 11 GHz. The lower frequencies used in the later specifications means that the signals suffer less from attenuation and therefore they provide improved range and better coverage within buildings. This brings many advantages to those using these data links within buildings and means that external antennas are not required.

Different bands are available for WiMAX applications in different countries of the world (Table 9). The frequencies used are 3.5 and 5.8 GHz for 802.16d and 2.3, 2.5 and 3.5 GHz for 802.16e but the use depends on the countries' authorities [20]:

Table 9: Current major spectrum allocations for WiMAX worldwide

REGION	FREQUENCY BANDS (GHZ)	COMMENTS
Canada	2.3, 2.5, 3.5, 5.8	
USA	2.3, 2.5, 5.8	
Central and South America	2.5, 3.5, 5.8	The spectrum is very fragmented and allocations vary from country to country
Europe	2.5, 3.5, 5.8	The spectrum is very fragmented and varies from country to country. The 2.5 GHz allocation is currently allocated to IMT 2000. 5.8 GHz is also not available in most European countries.
Middle East and Africa	2.5, 5.8	The spectrum is very fragmented.
Russia	2.5, 3.5, 5.8	The 2.5 GHz allocation is currently allocated to IMT 2000.
Asia Pacific (incl. China, India, Australia, etc.)	2.3, 2.5, 3.3 3.5, 5.8	The spectrum is very fragmented and varies between countries.

4.3 IEEE 802.15.4 - ZigBee

ZigBee is a wireless networking standard that aims at remote control and sensor applications which are suitable for harsh radio environments and isolated locations. ZigBee technology builds on 802.15.4 IEEE standard which defines the physical and MAC layers. Above the 802.15.4, ZigBee defines the application and security layer specifications enabling interoperability between products from different manufacturers. ZigBee can be defined as a superset of the 802.15.4 specification. (Table 10)

The ZigBee standard is organized under the auspices of the ZigBee Alliance [21].

Table 10: ZigBee Versions

ZIGBEE VERSIONS	COMMENTS AND DETAILS
ZigBee 2004	This was the original release of ZigBee - defined as ZigBee 1.0 which was publicly released in June 2005.
ZigBee 2006	This release of the ZigBee standard introduced the concept of a cluster library and was released in September 2006.
ZigBee 2007	The next version of the ZigBee standard was released publicly in October 2008 and contained two different profile classes
ZigBee PRO	ZigBee PRO was a profile class that was released in the ZigBee 2007 release. ZigBee PRO provides additional features required for robust deployments including enhanced security.
RF4CE	RF4CE - Radio Frequency for (4) Consumer Electronics was a standard that was aimed at audio visual applications. It was taken on board by the ZigBee Alliance and the Version 1.0 of the standard was released in 2009.

4.3.1 ZigBee Basics

The maximum distance of ZigBee is 70 meters, and larger distances can be achieved by relaying data from one node to another. In 802.15.4 control and monitoring applications are the most usual in which low amounts of data throughput needed, and with the possibility of remote, autonomous powered sensors; low power consumption is a key factor.

The system operates at 2.4 GHz or 915 MHz in North America and 868 MHz in Europe. The standard can operate globally, despite a few specifications for each of the bands are different. At 2.4 GHz there are 16 available channels with maximum data rate of 250 kbps. At 915 MHz there are 10 channels with maximum data rate of 40 kbps, and finally, at 868 MHz there is 1 channel with maximum data rate up to 20 kbps. Modulation techniques differ depending on the in-use band. DSSS (Direct sequence spread spectrum) is used in all bands. Because of the usual presence of congested environments, or generally areas with high levels of extraneous interference, the 802.15.4 has features to ensure the trustworthiness of the operation. A few of them are receiver energy detection, clear channel and quality assessment. CSMA (Carrier Sense Multiple Access) techniques are used to select when a transmission should be done, and in order to avoid connectivity problems [22].

The data is transferred in maximum 128 bytes packets allowing for a maximum payload of 104 bytes. This is not low because the applications in which 802.15.4 and ZigBee are used do not require higher level data rates. 802.15.4 supports both 64 bit and 16 bit IEEE addresses. The 64 bit addresses identify every device like IP addresses. When a network is established, 16 bit addresses are used and enable more than 65,000 supported nodes. Alternatively, there is a superframe structure which imports time synchronization. Additionally, some messages have higher priority than others. To achieve this discrimination, a time slot mechanism is attached to the specification. [16].

ZigBee defines the upper layers of the physical and MAC layers. These include services such as messaging, configurations which can be used, and of course security issues as well as application profile layers. There are 3 ZigBee network topologies a) star, b) mesh and c) cluster tree or hybrid networks. Each of them has its own pros and cons. The star network is widely used, because it is very simple to be created. Mesh or peer-to-peer networks are very reliable. There are nodes placed as needed within the appro-

priate range in such a way that can easily communicate with each other. Messages are sent over the network using the nodes as relays. If interference exists on one part of a network, then the other can be used without any problems. A combination of star and mesh topologies creates essentially a cluster tree network. 802.15.4 and ZigBee have been designed to assure low power consumption. Although nodes with sensors of control mechanisms towards the centre of a network are more likely to have mains power, many towards the extreme may not. The low power design has enabled battery life to be typically measured in years, enabling the network not to require constant maintenance [22].

One of the key elements of the ZigBee system is the way in which the ZigBee network operates. A ZigBee network is set up to enable data messages to be sent efficiently across the ZigBee network that may extend over considerable distances. With applications including lighting and heating control, the ZigBee network must be able to communicate over distances that may be well in excess of the single hop distance achievable by each individual node. To achieve the full ZigBee network coverage messages must be able to be relayed.

4.3.2 ZigBee IP

ZigBee IP has been developed to enable full Internet connectivity of ZigBee devices using IPv6 protocol. ZigBee IP is a version of the ZigBee standard for mesh networking for remote control and sensing. This standard enables operation of devices as part of the Internet of Things concepts. ZigBee IP offers several key features such as *IEEE 802.15.4 base* to provide the low layer functionality, *Frequency compatibility* for use in license free bands: 2.4 GHz (global); 868 MHz (Europe); 915 MHz (USA); 920 MHz (Japan), *Link layer security* using AES-128-CCM to provide security using known and proven technology, *Header compression* to reduce the transmission overhead and increase efficiency *IPv6* so each node on a network can be individually addressed using IPv6 routing and addressing protocol, *Multicast capability* to enable service discovery using mDNS and DNS-SD protocols, *Inter-networking* by using the IPv6 protocol in order to communicate end to end with devices in its own network or other networks with an ultimate connection.

One of the main advantages of ZigBee IP using 802.15.4 is that it provides a scalable architecture with end-to-end IPv6 networking. In this way it provides an ideal basis for many applications that are considered as part of the Internet of Things. In this way ZigBee IP enables low-power devices to connect with other IPv6-enabled Ethernet, Wi-Fi, and, Home Plug devices [21].

Signal interference: Although ZigBee can move channels in the presence of interference, this is relatively slow - it is not a frequency hopping ability.

4.4 Bluetooth

The Bluetooth Special Interest Group (SIG) was founded in 1998 by Ericsson, Nokia, IBM, Toshiba, and Intel "to establish a de facto standard for the air interface and the software that controls it."

Bluetooth is a wireless technology which was created for short-range communication. Security, robustness, low power, and low cost method for exchanging information between devices are its main benefits. It is a global standard; so any Bluetooth-enabled device can communicate with any other. Bluetooth devices can also connect with up to 7 other devices in an ad-hoc personal-area network (piconet), and be a member of several piconets simultaneously. Bluetooth uses a property named “frequency-hopping” in order to ensure that it is resilient to interference [12].

4.4.1 Bluetooth Radio interface

Running in the 2.4 GHz ISM band, Bluetooth employs frequency hopping techniques with the carrier modulated using Gaussian Frequency Shift Keying (GFSK).
With many other users on the ISM band from microwave ovens to Wi-Fi, the hopping carrier enables interference to be avoided by Bluetooth devices. A Bluetooth transmission only remains on a given frequency for a short time, and if any interference is present the data will be re-sent later when the signal has changed to a different channel which is likely to be clear of other interfering signals. The standard uses a hopping rate of 1600 hops per second, and the system hops over all the available frequencies using a pre-determined pseudo-random hop sequence based upon the Bluetooth address of the master node in the network.

While developing the Bluetooth standard it was decided to adopt the use of frequency hopping system because it is able to operate over a greater dynamic range than a direct sequence spread spectrum approach. If direct sequence spread spectrum techniques

were preferred to be used the transmitters nearer to the receiver would block the required transmission if it is weaker and further away.

Bluetooth frequencies are located within the 2.4GHz ISM band. The ISM band extends from 2,400MHz to 2,483.5MHz. The Bluetooth channels are spaced 1MHz apart, starting at 2,402MHz and finishing at 2,480MHz. This can be formulated as 2,401 + n, where n varies from 1 to 79.

This arrangement of Bluetooth channels gives a guard band of 2MHz at the bottom end of the band and 3.5MHz at the top. In some countries the ISM band allocation does not allow the full range of frequencies to be used. In France, Japan and Spain, the hop sequence has to be restricted to only 23 frequencies because the ISM band allocation is smaller [12].

There are also some Bluetooth frequency accuracy requirements for Bluetooth transmissions. The transmitted initial centre frequency must be within ±75kHz from the receiver centre frequency. The initial frequency accuracy is defined as being the frequency accuracy before any information is transmitted and as such any frequency drift requirement is not included. In order to enable effective communications to take place in an environment where a number of devices may receive the signal, each device has its own identifier. This is provided by having a 48 bit hard wired address identity giving a total of 2,815 x 10^14 unique identifiers.

4.4.2 Bluetooth modulation

Gaussian frequency shift keying, GFSK, was the first format for Bluetooth 1 but the requirement for higher data rates introduced two forms of phase shift keying for Bluetooth 2 to provide the Enhanced Data Rate, EDR capability.

Gaussian frequency shift keying: In this case, the frequency of the carrier is shifted to carry the modulation. A positive frequency deviation is represented by a binary one and a negative by a binary zero. A filter with a Gaussian response curve filters the modulated signal to ensure the sidebands do not extend too far either side of the main carrier. A bandwidth of 1 MHz is achieved by the Bluetooth modulation with stringent filter requirements to prevent interference on other channels. In order to have correct operation the level of Bluetooth is set to 0.5 and the modulation index should be between 0.28 and 0.35.

Phase shift keying is the form of Bluetooth modulation used to enable the higher data rates with Bluetooth 2 EDR (Enhanced Data Rate). Two forms of PSK are used:

- *π/4 DQPSK:* Form of phase shift keying known as π/4 differential phase shift keying. Raw data rates of 2 Mbps can be achieved.
- *8DPSK:* It is known as 8-ary phase shift keying. It is used when link conditions are quite good. Raw data rates of up to 3 Mbps can be achieved.

The enhanced data rate capability for Bluetooth modulation is implemented as an additional capability so that the system remains backwards compatible. The Bluetooth modulation schemes and the general format do not lend themselves to carrying higher data rates. For Bluetooth 3, the higher data rates are not achieved by changing the format of the Bluetooth modulation, but by working cooperatively with an IEEE 802.11g physical layer. In this way data rates of up to around 25 Mbps can be achieved [12].

4.5 IEEE 802.22 - COGNITIVE RADIO TECHNOLOGY

Wireless Regional Area Network, WRAN are unused or white spaces within the television bands between 54 and 862 MHz, especially within rural areas where usage may be lower are spectrum regions for which the IEEE 802.22 standard defines a system to incorporate the concept of cognitive radio. To achieve this, the 802.22 utilizes cognitive radio technology to ensure that no interference is caused to television services using the television bands. [24].

The 802.22 is aimed at supporting license-exempt devices on a non-interfering basis in spectrum that is allocated to the TV Broadcast Service. With operating data rates comparable to those offered by many DSL / ADSL services it can provide broadband connectivity using spectrum that is nominally allocated to other services without causing any undue interference. In this way IEEE 802.22 makes effective use of the available spectrum without the need for new allocations.

The 802.22 standard for a WRAN system was created because of a number of requirements and as a result of a development in many areas of technology. Recently, there has been an important increase in the number of wireless applications that have been deployed, and along with the more traditional services it has placed a critical amount of pressure on sharing the available spectrum. Apart from this, there is always a delay in re-allocating any spectrum that may become available. In addition to this the occupancy levels of much of the spectrum that has already been allocated is relatively low. For instance, in USA, TV channels are not all used as it is necessary to allow guard bands between active high power transmitters to prevent mutual interference. Furthermore, all stations are not active continuously. Also, organizing other services around these constraints can drive us to gain greater spectrum utilization without causing interference to others.

One technology which is significant to the deployment of new services and may bring better spectrum utilization is with no doubt cognitive radio technology. With this technology the radios can sense their environment and adapt accordingly. The use of cognitive radio plays significant role to the 802.22 standard.

4.5.1 Standard History & Basics

J Mitola in 2000 about Cognitive Radio: “A form of radio that would change its performance by detecting its environment and changing accordingly”.

A notice of proposed rulemaking was issued by FCC in 2004 regarding the television spectrum. Then the IEEE 802.22 working group developed a WRAN system aiming to deliver broadband connectivity to rural areas by sharing the television spectrum and by May 2006 draft v0.1 was reality [24].

The basis of the 802.22 standard was contributed by features like the system capacity, the projected coverage and the system topology.

System topology: It is a point to multipoint system consisting of a base station with a number of users or Customer Premises Equipments (CPEs), located in a cell. The base station sends through the network the data on the downlink to the various users and receivers’ data from the CPEs on the uplink. It controls the medium access and addition to the classic roles for a base station; it manages the "cognitive radio" issues of the system too. CPEs are used to perform a distributed measurement of the signal levels of possible TV signals on the various channels at their locations. These measurements are collected and the base station decides whether any actions need to be taken.

Coverage area: It is larger than other IEEE 802 standards – for a CPE is 33 km and in some cases base station’s coverage extends to 100 km.

System capacity: The system aims to achieve DSL services performance levels. This means downlink speed of 1.5 Mbps and uplink speed of 384 kbps. These can serve 12 users simultaneously. To achieve that, the capacity should have downlink speed of 18 Mbps [23].

4.5.2 Standard Specification Parameters.

"The IEEE 802.22 standard aims to provide additional usage of the enormous amounts of broadcast spectrum which is available in lots of countries".

Due to the fact that 802.22 uses cognitive radio technology, it will be necessary to ensure that no interference is caused to any existing services and users should not be affected in performance of their terrestrial television reception. Therefore, the use of 802.22 WRAN technologies should drive to a more efficient use of the spectrum as well as offering new services for users, mainly in rural areas.

In IEEE 802.22, the physical layers create a sufficient level of performance along with the requirement to assure that the system has the ability to maintain its white space in the TV spectrum. To succeed in this, the system requires flexibility and also cognitive radio techniques to be implemented (Table 11).

In order to meet the requirements of 802.22, the physical layer should be flexible. The modulation scheme is one main characteristic. An OFDM scheme has been invented with 802.22 WRAN in order to provide resilience to selective fading and multipath propagation as well as a high degree of sufficient data throughput and spectrum efficiency. In order to give access to many users, OFDM is used both for uplink and downlink data streams.

IEEE 802.22 allows a variety of modulation schemes to be used within the OFDM signal: QPSK, 16-QAM and 64-QAM can all be selected with convolutional coding rates of 1/2, 3/4, and 2/3. The required modulation and error correction rates are chosen according to the prevailing conditions. In order to meet the requirements for the individual users that may be experiencing very different signal conditions, it is necessary to dynamically adapt the modulation, bandwidth and coding on a per CPE basis [23].

In order to achieve the desired level of performance, it is necessary to the 802.22 to affiliate a system of what named "Channel Bonding". This is a scheme which gives the ability to 802.22 to use more than one channel simultaneously to provide the desired throughput. It is usual to use adjacent channels as frequency planners allow 2 or more, empty channels between stations transmitting signals in order to prevent interference on TV signals. These free channels allow the use of contiguous channel bonding. In reality,

the number of channels which are bonded is limited to 3 resulting in front-end bandwidth limitations. A duplex scheme named TDD is used to give access for upstream and downstream data. The advantages are many. Firstly, it requires only 1 channel to be used rather than FDD. Secondly, TDD enables change of the downstream and upstream capacity dynamically [23].

Table 11: Specification parameters of the IEEE 802.22

PARAMETER	SPECIFICATION
Typical cell radius (km)	30 - 100 km
Methodology	Spectrum sensing to identify free channels
Channel bandwidth (MHz)	6, (7, 8)
Modulation	OFDM
Channel capacity	18 Mbps
User capacity	Downlink: 1.5Mbps Uplink: 384 kbps

4.5.3 802.22 MAC Medium Access Control

The IEEE 802.22 standard flexibility brings new challenges to the practical implementation of the system. Consequently, the MAC has been designed to give the flexibility to incorporate in these new ideas.

In the first instance the initialization and network entry needs to accommodate the elements of the spectrum usage flexibility. As there is not fixed channel for the system, and no pilot channel can be broadcast, any CPE when turning on and initializing needs to be able to find the signals. Accordingly, when initializing, any CPE first scans the available spectrum to look at channel occupancy. It will detect those channels free of television transmissions. In the remaining empty channels it will then scan for base station pilot signals and acquire any network information. Once it has acquired the correct network it can then proceed to connect to the network. It is also necessary to have a defined format for the data. To enable the data to be suitably structured, the transmission is formatted into frames and superframes.

1. *Superframes:* are created by the smaller frames. A superframe's usage is to provide synchronization for the system, and accordingly to provide the initial network access / entry initialization. Each superframe starts with a preamble called as the Superframe Control Header, SCH. The SCH has the needed information for any new CPEs want to have access to the base station,
2. *Frames:* They are the ingredients of superframes. They consist of 2 elements: the downstream subframe (DS) and the upstream subframe (US). The boundary between the subframes is variable and it can be adapted to accommodate changes on the levels of upstream and downstream capacity if required.

IEEE 802.22 equipment is designed to ensure that no undue interference is caused to existing television services. As a result the whole system has to be adaptive to ensure that the system avoids channels that are in use while still maintaining the required throughput. It even has to adapt to changes in radio propagation that may occur from time to time. As a result the cognitive radio and cognitive network technology has been incorporated to ensure this requirement is met.

One of the main characteristics of 802.22 is that it is able to coexist with other users of the radio spectrum, without causing any interference. It is generally accepted that as any 802.22 system is likely to be given access to any spectrum as a secondary user where no interference is caused to the primary user, the system is logically able to adapt itself around the primary users. To meet this expectation, cognitive radio networking is necessary to provide the spectrum adaptation and sensing.

4.5.4 802.22 Spectrum Management

The 802.22 network has the responsibility for ensuring that it does not create any interference to other users of the spectrum. The network consists of the base station (BS), and a number of user equipments called customer premises equipments (CPEs). In order to provide the level of interference avoidance that is desired, 802.22 spectrum sensing is delivered across the network of users. Proportionally, the 802.22 spectrum sensing is taken over in the CPEs. CPEs scan the channels that are open for use and send back info about signals and strengths on the channels to the BS equipment.

The decisions about which channels are occupied and whether they can be used for the 802.22 transmissions are taken by the BS. In order to decide, the BS uses the spectrum sensing results and also geo-location information and any other information provided by an entity named network manager. The 802.22 takes into account that there will be 3 types of users of the used frequencies:

- Analogue television: In North America (NTSC), and in Europe (PAL). The level of an analogue signal above which the 802.22 system will vacate the channel is -94 dBm measured at the peak of the sync pulse.
- Digital television: In North America (DTV), and in Europe (DVB-T). The level of a DTV signal above which the 802.22 system will vacate the channel is -116 dBm.
- Wireless microphones: There are many formats as they are not standardized, but in general they use FM and the bandwidth is about 200 kHz. The level of a wireless microphone signal above which the 802.22 system will vacate the channel is -107 dBm.

In this way the IEEE 802.22 WRAN performs spectrum sensing across the whole network and adjusts itself accordingly. This means that the 802.22 WRAN system is a true cognitive radio network, rather than an individual cognitive radio operating in isolation.

The channel management and spectrum sensing or signal measurements form an important part of the overall 802.22 scheme. The MAC layer within the CPEs carries out many important tasks that enable this to work efficiently and smoothly.

BS instructs CPEs to take periodic measurements in one of 2 existing formats;

- *In band spectrum sensing:* Applies to the channels that are being used by the BS to communicate with CPEs. It is necessary in order to be undertaken this type of sensing for the BS to quieten all the transmissions on the channel. Having a short break of the transmissions, the CPEs can listen for transmissions. When inspecting the presence of other signals on the channel, the CPE need to look for very low level. The levels required and the accuracy, are controlled by the BS. The duration for the measurement, which channels, the time of measurement, and probability of false alarm are controlled by the BS. To gain the best measurement, the BS instructs different CPEs to take different measurements. BS makes the selection of how this is done and calculates with the algorithms it contains. From the instructing of different CPEs in order to make different measurements and over different lengths of time, the BS makes an occupancy map for the whole cell.
- *Out of band spectrum sensing:* refers to channels which are not used by the BS to contact with the CPEs. These measurements are used to locate possible empty channels. By this way it is created an adequate guard band between the in-use channels by the BS and any TVs stations that may use adjacent channels.

The in band spectrum sensing is used on a regular basis. During the transmission timings the quiet periods for sensing are built. There are 2 types of sensing:

- *Fast sensing:* which is accomplished quickly. It uses a typical energy detection algorithm and lasts in 1ms. The results are returned to the BS which analyzes them and determines if any fine sensing measurement is needed.

- *Fine sensing:* is undertaken if there is need for a more accurate measurement. Fine sensing lasts 25ms. During the procedure, CPE checks the signatures of signals that may be the primary user, for example TV.

It is also possible that adjacent 802.22 networks may cause interference to one another, and the adjacent networks may sense each other. To overcome the possibility of confusion caused by adjacent networks detecting each other algorithms are built into the system to synchronize overlapping cells. This also includes the synchronization of the quiet periods when the spectrum sensing occurs.

4.6 SRD - Short Range Device Applications

SRD, Short Range Device is a term that is applied to a radio or wireless device that is designed to operate over a short range. This also implies that the power levels are low and hence the likelihood of interference to other devices is low. This enables SRDs, Short range Devices to be operated under relaxed regimes of regulation, which are often termed "license free."

In general, the term SRD or Short range device refers to a variety of short range transmitter receiver systems that have power output levels of less than a watt, with most falling below 10mW. As a result their range is limited, most operating at ranges well below 1 km. Data rates can vary considerably, ranging from a rates in the region of 100 bps to as high as 1 Mbps and more. These levels of functionality are ideal for many applications where short ranges are needed along with proprietary radio technology [25].

Short Range Devices may be used in a large variety of applications where low power transmission of data is needed over short distances. In many instances the use of an existing standard such as Wi-Fi or ZigBee may not be appropriate as it may require a large overhead in terms of formatting the data for the particular standard. In these cases a standard alone solution may be more appropriate. Accordingly specialized SRD, Short Range Devices may be more appropriate. There are many applications for which short range devices are used. (Table 12)

Table 12: List of Applications for SRDs

Garage door and gate controls
Alarms and movement detectors
Industrial control
Industrial monitoring
Low rate data transmission
RF identification (RFID)
Anti- Theft devices

The regulations for SRDs vary according to the country in question. One of the main areas where care has to be taken when using SRDs is to ensure that the frequencies used match those of the particular region in question. A wide variety of frequencies and bands are available (Table 13), although some are only available in particular countries as shown below:

Table 13: Examples of license free bands that can be used by SRDs

BAND (MHZ)	REGION AND COMMENTS
433	Europe
458	UK
868	Europe
915	USA
2400	Worldwide

In these bands the regulatory authorities allow suitably approved and tested radios to be used without the need for individual user licenses [25].

4.6.1 International SRD Standards

As it is inevitable that SRDs will be used in many countries around the world, it is essential that international standards are adopted for these devices. (Table 14)

Table 14: Standards developed for SRDs

STANDARD NUMBER	ORGANISATION	DETAILS
EN 300 220	ETSI	This standard covers SRD equipment operating in the frequency range 25 MHz to 1000 MHz.
EN 300 330	ETSI[]	This ETSI standard covers SRD radio equipment operating in the frequency range 9 kHz to 25 MHz (and inductive loop systems operating up to 30 MHz).
EN 300 440	ETSI	This covers SRD radio equipment operating in the frequency range 1 GHz to 40 GHz.
Part 15.247	FCC	This SRD definition is primarily used for devices for North America.

Although there have been many attempts to harmonize standards across the globe there are still many variations. Most of Europe, Africa and Australia use systems based on the ETSI standards, whereas USA and Canada have those based on the FCC standards.

One area that is particularly important where unlicensed transmitting devices are concerned is that of EMC. It is necessary to ensure that these SRDs do not radiate unwanted transmissions that may cause interference to other users.

As a result of this requirement, ETSI has produced standards that specify the Electromagnetic Compatibility or EMC requirements. For SRDs, the ETSI EMC standards are:

- EN 301 489-1 (General technical requirements for radio)
- EN 301 489-3 (Special conditions for SRDs)

SRDs are used for many wireless or radio applications where only limited ranges are needed. Often small data transmission devices conforming to the relevant specification provide low cost but effective solutions enabling data to be transferred over a radio link. While standards such as 802.11, 802.15 and other specifications are ideal for many applications, SRD short range devices may be used for many other specific applications where data needs to be transported over short distances. The short range devices, SRDs using proprietary radio designs do not have the overheads of the protocol stack and high degrees of conformance testing required for standards such as ZigBee, Bluetooth, etc. Accordingly SRD developments may be the ideal path for many applications [25].

5 Interference in the 2.4 GHz ISM Band

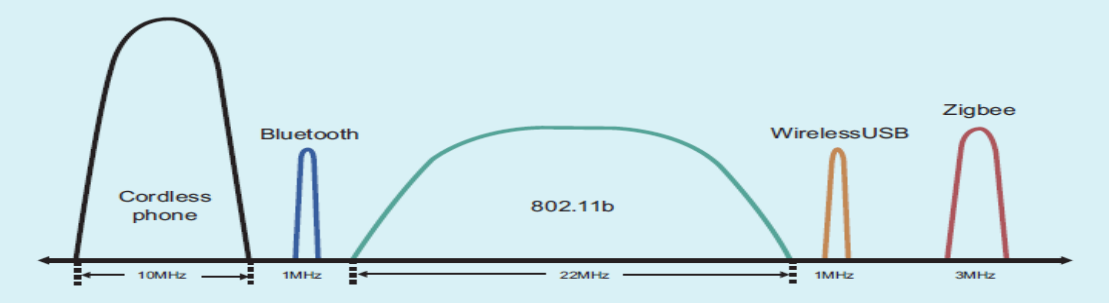
The number of companies which produces products located in the 2.4-GHz portion of the radio spectrum is increasing dramatically. Designers have to deal with the increased interference signals from other sources.

5.1 Various Interference Management Techniques

How can designers get the best performance out of their 2.4-GHz solution under these hostile conditions? Often the product works in a controlled lab environment but then suffers performance degradation from the storm of interference from other 2.4GHz solutions in the field. With existing standards like Wi-Fi, Bluetooth, and ZigBee there is little that can be done beyond what the architects of the standard provide. But when the designer controls the protocol there are procedures that will minimize the interference from other sources [26].

Wi-Fi

There are 2 methods for radio frequency modulation in the 2.4 GHz band. These are FHSS (Frequency-Hopping Spread Spectrum) and DSSS (Direct-Sequence Spread Spectrum). FHSS is used by Bluetooth and DSSS is used by WirelessUSB, 802.11b/g/a (Wi-Fi), and 802.15.4 (ZigBee) (Picture 4). All of them operate in 2.400 - 2.483 GHz, which is available globally.



Picture 4: 2.4 GHz Channels Width

DSSS is used by Wi-Fi. Each channel has 22 MHz width, allowing up to 3 channels to be used at the same time without overlapping. Each Wi-Fi access point should configure the used channel; Wi-Fi clients investigate all channels for available-free access points. 802.11 uses a Barker code (11-bit pseudorandom noise code, PN) to encode each information bit for the original 1 and 2 Mbit/s data rates. In order to have higher data rates 802.11b encodes 6 information bits into an 8-chip symbol using CCK (Complementary Code Keying.

In CCK algorithm there are 64 possible symbols, requiring each 802.11b radio to have 64 different correlators (transforming symbols into information bits), which may increase the complexity and the cost, but also increase the data rate (11 Mbps) [26].

Bluetooth

The main characteristic of Bluetooth is the ad-hoc interoperability between mobile phones, headsets, and other mobile devices. Bluetooth devices need recharging regularly. FHSS is used by Bluetooth and the 2.4 GHz band is divided into 79 1 MHz channels. Bluetooth devices change 1600 times per second channel in a pseudo-random pattern. Bluetooth devices connected each other, are grouped into networks named piconets; each piconet consists of one master and up to 7 active slaves. The master's clock derives the channel-hopping sequence of the piconet. The slave devices are synchronized with master’s clock.

FEC (Forward error correction) is used on packet headers, by transmitting every bit in the header 3 times. Hamming code is used for FEC of the data payload of several packet types. The Hamming code imports a 50% overhead on every data packet, but can correct all single errors and detect all double errors in each 15-bit code word.

ZigBee

ZigBee is a standardized solution for sensor networks. ZigBee devices are power-sensitive (thermostats, alarm-security sensors, etc.) with their battery life measured in years. DSSS is used by ZigBee in the 868 MHz band (Europe), 915 MHz band (North America), and the 2.4 GHz band (worldwide). 16 channels are defined in the 2.4-GHz band; 3 MHz are occupied by each channel and they are centered 5 MHz from each other, having a 2-MHz gap between pairs of channels. An 11-chip PN code is used, with 4 information bits encoded into each symbol giving it a maximum data rate (128 Kbps). IEEE 802.15.4 Working Group defines the physical and MAC layers and shares many of the same design characteristics like the IEEE 802.11b standard [16].

2.4-GHz Cordless Phones

They are increasingly popular in North America and they do not use a standard net-networking technology. Cordless phones use DSSS and FHSS. Phones using DSSS have a button on the phone allowing users to change the channel manually. FHSS phones do not have this button, because they are changing channels continuously. The majority of 2.4 GHz cordless phones use 5 to 10 MHz channel width.

Collision Avoidance

Collision-avoidance algorithm of Wi-Fi listens for a quiet channel before transmitting (Table 15). This gives the ability to multiple Wi-Fi clients to communicate with a single Wi-Fi access point. If the channel is noisy the device does a random back off and listens to the channel again. If the channel is still noisy the procedure is repeated respectively; when the channel is quiet the device begins its transmission. If the channel is always noisy the device searches for other access points on another channel.

When Wi-Fi networks use overlapping or the same channels will co-exist because of the collision avoidance algorithm, but the throughput of the network will be decreased. If several networks are used in the same area the best solution is to use non-overlapping channels such as 1, 6, and 11. This maximizes each network's throughput since it will not be obliged to share the bandwidth with another network.

Interference from Bluetooth is minimal due to the hopping nature of the Bluetooth transmission. If a Bluetooth device transmits on a frequency that overlaps the Wi-Fi channel while a Wi-Fi device is doing a "listen before transmit", the Wi-Fi device will do a random back off during which time the Bluetooth device will hop to a non-overlapping channel allowing the Wi-Fi device to begin its transmission.

2.4 GHz cordless phones can stop a Wi-Fi network with interference, even if the cordless phones use FHSS as opposed to DSSS. This is because of the wider channel compared to Bluetooth and also because of the high power of the cordless phone signal [18].

How to handle interference in Bluetooth

Interference from Bluetooth piconets is minimal. Every piconet has its own pseudo-random frequency-hopping pattern (Table 15). If 2 co-located piconets are active the probability of collision is 1/79. The probability of collision increases linearly with the number of co-located active piconets.

Bluetooth relies on the frequency-hopping algorithm to handle interference. It is realized that a single active Wi-Fi network can cause interference on 25% of the Bluetooth channels. Lost packets because of overlap have to be retransmitted on quiet channels, as a result to reduce the throughput of Bluetooth devices.

Bluetooth specification version 1.2 addresses this issue by defining an adaptive frequency hopping (AFH) algorithm. This algorithm allows Bluetooth devices to mark channels as good, bad, or unknown. Bad channels in the frequency-hopping pattern are then replaced with good channels via a look-up table. The Bluetooth master may periodically listen on bad channels to determine if the interference has disappeared; if so, the channel is then marked as a good channel and removed from the look-up table. Bluetooth slaves, when requested by the master, can also send a report to the master informing the master of the slave's assessment of channel quality. For instance, the slave may be able to hear a Wi-Fi network the master cannot. The Federal Communications Commission (FCC) requires at least fifteen different channels be used.

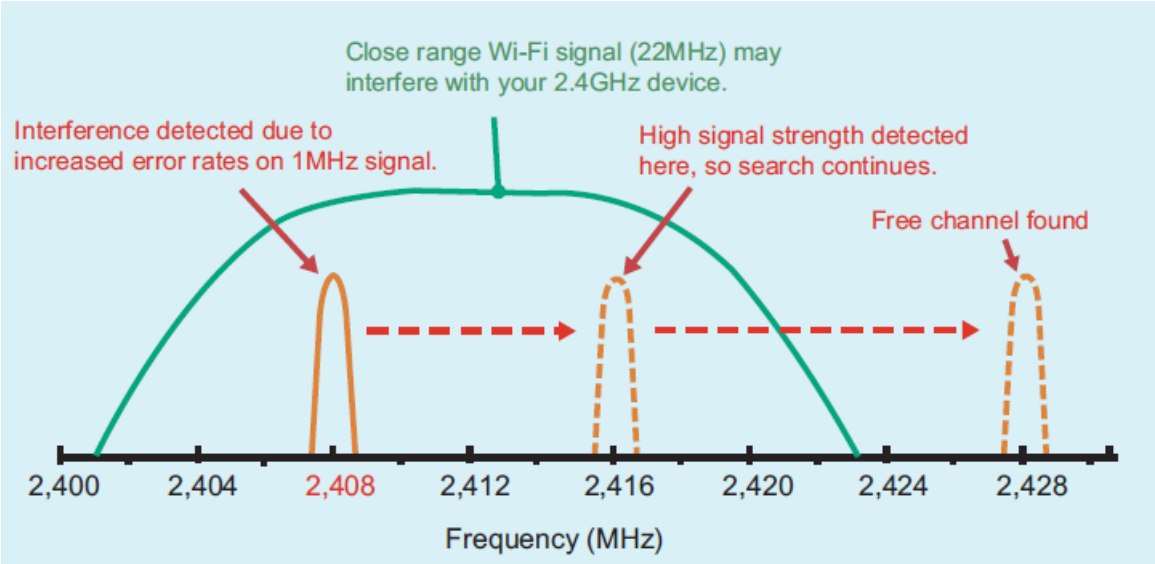
AFH allows Bluetooth to avoid channels occupied by DSSS systems. FHSS cordless phones may cause interference with Bluetooth since both systems are hopping over the band, but since the Bluetooth signal width is 1 MHz, the frequency of collisions between Bluetooth and the FHSS cordless phone is importantly less than the frequency of collisions between FHSS cordless phones and Wi-Fi.

Bluetooth packets can have 3 different lengths that translate into different dwell times on a channel. Bluetooth has the option to decrease the packet length in order to increase the data throughput. Generally, it is more preferable to get small packets through at a slower data rate than losing large packets at a faster data rate.

How to handle interference in WirelessUSB, ZigBee

WirelessUSB: Each network checks if there are other WirelessUSB networks before selecting a channel (Picture 5). Regarding the interference, it is minimal if the source is another WirelessUSB network. WirelessUSB checks the noise level of the channel frequently (once every 50ms). On the contrary, interference caused by Wi-Fi devices pro-

duces consecutive high noise readings making the WirelessUSB master to choose a new channel. WirelessUSB can co-exist with Wi-Fi networks, because WirelessUSB can find quiet channels between the Wi-Fi networks.



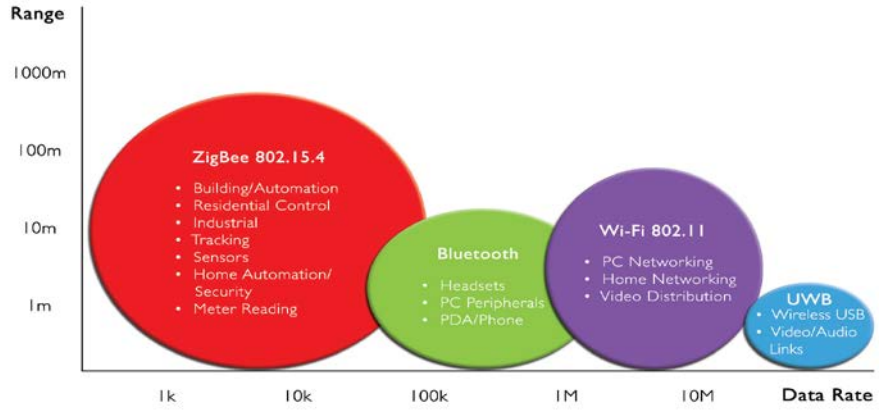
Picture 5: WirelessUSB peacefully coexists with multiple Wi-Fi networks because WirelessUSB is able to find the quiet channels between them.

Interference derived from Bluetooth may enforce WirelessUSB packets to be resent. Because of the hopping algorithm of Bluetooth, WirelessUSB retransmissions will not have collisions with the next Bluetooth transmission because the Bluetooth device will already have moved to a different channel (Table 15). ZigBee uses a collision-avoidance algorithm in the same way as 802.11b. Each device listens to the channel before transmission in order to reduce the collisions-frequency between the ZigBee devices. ZigBee relies on collision-avoidance algorithms and its low duty cycle to minimize data loss produced by collisions and it does not change channels if heavy interference exists; (Table 15).

Table 15: 2.4GHz networking technologies design trade-offs to reduce interference

	Data rate	Number of channels	Interference avoidance method	Minimum quiet bandwidth required
Wi-Fi (802.11b)	11Mbps	13	Fixed channel collision avoidance	22MHz (static)
Bluetooth	723Kbps	79	Avoidance frequency hopping	15MHz (dynamic)
WirelessUSB	62.5Kbps	79	Frequency agility	1MHz (dynamic)
ZigBee	128Kbps	16	Fixed channel collision avoidance	3MHz (static)

5.2 Why ZigBee in a Smart Home?



Picture 6: Various signals overlapping

- ✓ ZigBee is based on the IEEE 802.15.4 standard
- ✓ ZigBee products have been designed to be immune to RF interference; the standard consists of 16 channels in the worldwide 2.4 GHz band, giving it plenty of space to interoperate with other systems operating in the same range.
- ✓ ZigBee units have considerably longer battery life than competing communication protocols (e.g. Infrared, Bluetooth, etc.) and are designed with omnidirectional radiation patterns, which allow frequencies used by
- ✓ ZigBee devices to penetrate the materials used by standard room construction, including furniture and cabinets.
- ✓ ZigBee establishes a two-way communication path, greatly increasing the possibilities for new functionality. Actions can be acknowledged locally; an advantage if you are not in the same room as the device. The capability can even be used for upgrades and bug fixes. For example, ZigBee devices like thermostats and controllers use flash memory-based processors and can have firmware reflashed over the air, without having to visit the device in the field. This feature greatly enhances the product and makes it future-proof as it can be remotely configured and/or upgraded [14].

5.3 Wi-Fi and ZigBee in Smart Home – Example

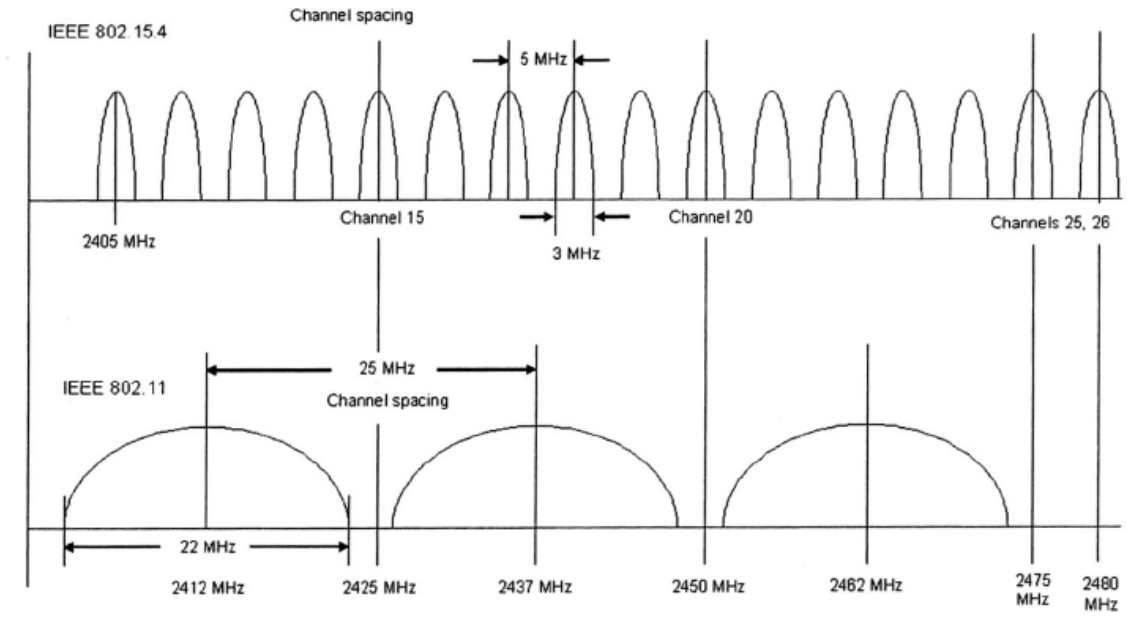
Picture 7: ZigBee Vs Wi-Fi

This example discusses how to avoid RF interference when deploying Wi-Fi and IEEE 802.15.4 / ZigBee radios simultaneously or in close proximity. The testing and deployments conducted for this application note used Crossbow's MICAz ZigBee-ready wireless Smart-Dust sensors and a Crossbow Stargate Gateway running both high-power and low-power Wi-Fi cards. When properly configured, the issue of RF interference and lost data can be avoided. However, without proper care and software configuration serious interference issues can occur [11].

USA/FCC & Canada regions have 11 total channels allocated. All frequencies are in GHz.

Channel	Lower Frequency	Central Frequency	Upper Frequency
1	2.401	2.412	2.423
2	2.404	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
11	2.451	2.462	2.473

Picture 8: 802.11b Channel-to-Frequency Mappings



Picture 9: RF channel spectrum of IEEE801.15.4 / ZigBee against IEEE802.11b / WiFi

A combination of a MICAz (ZigBee-ready radio) based sensor network and a Wi-Fi network using Stargate is rather than common deployment. (Picture 9). In order to examine the RF interference patterns a number of field trials were conducted while running both of them. The example here is based on a Stargate and a 6 node MICAz network. The first test was without the existence of Wi-Fi card attached to the Stargate. Then with a standard power 802.11b Wi-Fi card–Netgear MA701 (Picture 10) and finally with a high power Wi-Fi card (SMC Networks SMC2532W-B) (Picture 12). While the tests were taking place with Wi-Fi enabled, it was observed a continuous traffic on the Wi-Fi channel including a circular retransmission of an 8 MByte file across the Wi-Fi network. The Wi-Fi channel 3 was used for connection to the access point (Picture 8). It is noteworthy to be mentioned that the output power of the MICAz was at maximum RF power [11].

Results:

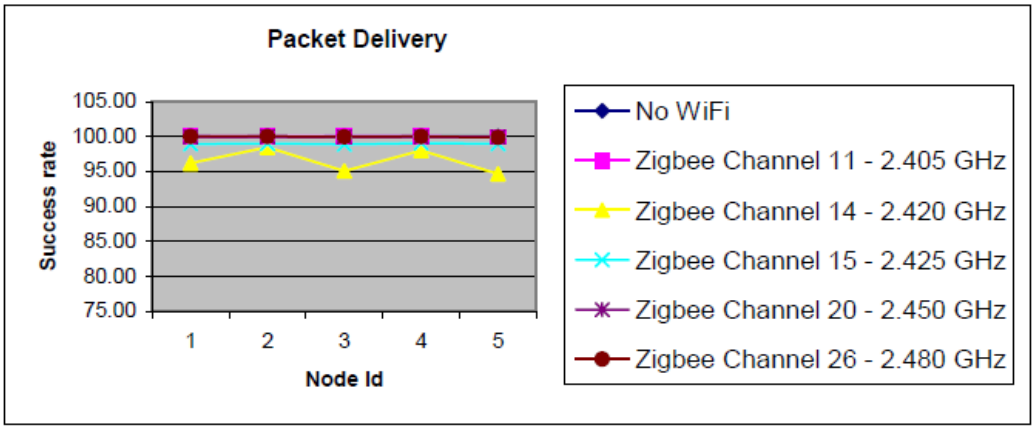
When the MICAz's ZigBee and the Stargate's Wi-Fi channel overlap each other the packet delivery rate is reduced by 100%. When the channels are not overlapped then the packet rate is at the normal rate (Picture 11). As it was expected, the degradation is more notable in the presence of high-power Wi-Fi card (Picture 13). It should be mentioned that interference was noticed on some adjacent channels, because intermodulation frequencies cause interference. These frequencies were created by interaction of the 2 signals in close proximity [11].

WiFi at 2.4220 GHz (Channel 3 802.11b band)
Netgear MA701 CF

Percent Packets Received

	Node 1	Node 2	Node 3	Node 4	Node 5
No WiFi	100.00	99.95	100.00	100.00	100.00
Zigbee Channel 11 - 2.405 GHz	100.00	100.00	100.00	100.00	99.95
Zigbee Channel 14 - 2.420 GHz	96.19	98.45	95.05	98.02	94.67
Zigbee Channel 15 - 2.425 GHz	98.93	98.99	98.89	99.05	98.96
Zigbee Channel 20 - 2.450 GHz	99.95	100.00	99.95	99.95	99.95
Zigbee Channel 26 - 2.480 GHz	100.00	100.00	99.95	100.00	99.89

Picture 10: Normal (Low) Power WiFi Card and ZigBee radio using MICAz Nodes 1-5



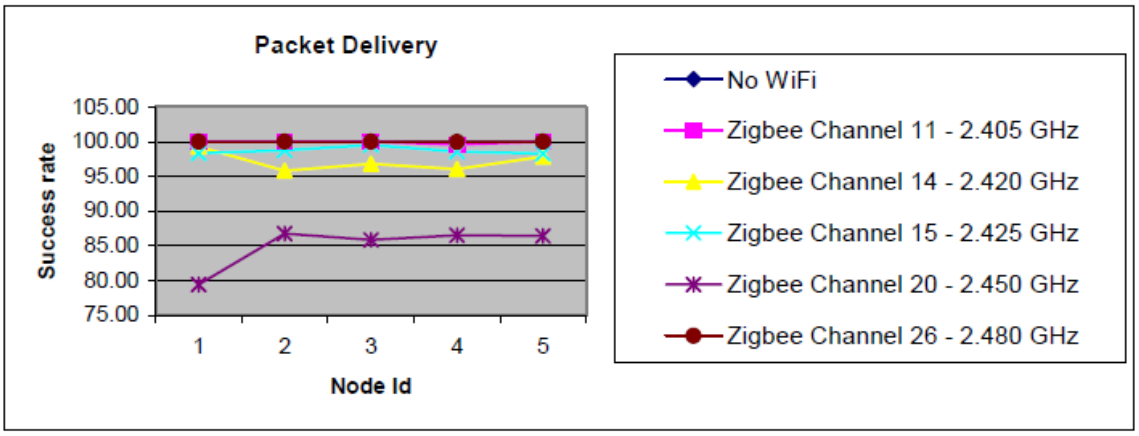
Picture 11: Normal (Low) Power WiFi Card and ZigBee radio using MICAz Nodes 1-5

WiFi at 2.422 GHz (Channel 3 802.11b band)
Hi Power SMC2532-W-B Card

Percent Packets Received

	Node 1	Node 2	Node 3	Node 4	Node 5
No WiFi	100.00	99.95	100.00	100.00	100.00
Zigbee Channel 11 - 2.405 GHz	100.00	100.00	100.00	99.55	100.00
Zigbee Channel 14 - 2.420 GHz	99.30	95.79	96.79	96.06	97.85
Zigbee Channel 15 - 2.425 GHz	98.31	98.75	99.51	98.55	98.30
Zigbee Channel 20 - 2.450 GHz	79.45	86.76	85.86	86.54	86.42
Zigbee Channel 26 - 2.480 GHz	100.00	100.00	100.00	99.96	100.00

Picture 12: High-Power WiFi Card and ZigBee radio using MICAz Nodes 1-5



Picture 13: High-Power WiFi Card and ZigBee radio using MICAz Nodes 1-5

To Sum up: The rapid growth in wireless sensing and control networks as well as the continuing adoption of Wi-Fi-based computer networks drive developers of such networks to take into account the interference avoidance and RF congestion. Examples like this can describe the issue and find solutions with correct channel choice and assignment [11].

5.4 15 Myths about Wi-Fi Interference

1. *802.11 networks only create interference problems .*

The number of 802.11 devices is enormous. It is known and generally accepted that 802.11 networks can affect with interference our network. (co-channel and adjacent channel interference). Due to the fact that 802.11 devices follow the same protocol, they cooperatively share the channel.

In fact, devices such as microwave ovens, cordless phones, Bluetooth devices, etc emitting in the unlicensed band scrimp the number of 802.11 devices. Furthermore, RF emissions are created by electrical connections. Non-802.11 devices do not work cooperatively with 802.11 devices, and can cause important loss of data. In addition, they can cause retransmissions which trick the 802.11 devices into working on lower data rates than appropriate.

2. *If my network seems to be working, interference should not be a problem.*

The 802.11 protocol is designed to be resilient to interference. When an 802.11 device senses an interference burst occurring before it has started its own transmission, it will hold off transmission until the interference burst is finished. If the interference burst starts in the middle of an ongoing 802.11 transmission (and results in the packet not being received properly), the lack of an acknowledgement packet will cause the transmitter to resend the packet. In the end, the packets generally get through. The result of all these, is that the throughput and capacity of your wireless network are impacted.

For example, microwave ovens emit interference on a 50 percent duty cycle. This means that a microwave oven operating at the same frequency as one of your 802.11 access points can reduce the effective throughput and capacity of your access by 50 percent. So, if your access point was designed to achieve 24 Mbps, it may now be reduced to 12 Mbps in the vicinity of the microwave when it operates.

3. *RF sweep before deployment cannot find interference sources.*

Interference is often intermittent in nature. Interference may occur when someone is operating a device a few times in a day, such as a phone call through a cordless phone. So, unless RF sweep is done, it's very easy to miss sources of interference.

4. *Interference cannot be detected by your infrastructure equipment automatically.*

Switch-based WLAN products provide some features of RF interference management. These features detect non-802.11 signals and they change the 802.11 channel of the APs in the area of the interference. Unfortunately, Bluetooth devices, 2.4 GHz cordless phones and other 802.11 devices are broadband and they are everywhere across the band. It is critical to search for the source and location of interference, in order to solve the problem. Removing the device is usually the best action.

5. *A high density of access points can overcome interference.*

By spreading around many APs, it is obvious that a client will be able to operate successfully no matter if interference exists. However, the reality is different!

When you have a network of many access points, you should decrease the signal power of each AP. Otherwise, access points will interfere with each other. So, many access points have even worse results.

6. *A packet sniffer can analyze interference problems.*

802.11 packet sniffer products can analyze only what 802.11 chips tell them. They cannot i) analyze interference problems, ii) find the cause of the interference, iii) find where the location of the interfering device is.

7. *Wireless policy protects me from interfering devices.*

A wireless policy is not enough without enforcement in tackling the interference problem. Unlicensed band wireless devices are widely available and in most cases we are not aware even if a device may interfere our wireless network.

8. *In 5 GHz, interference does not exist.*

It is accepted that a smaller number of devices operate at 5 GHz than at 2.4-GHz. But unfortunately, this will change in the near future. In the same way as we moved from 900 MHz to 2.4 GHz, we are going to “jump” to another band. Some devices already exist at 5 GHz and their number is increasing rapidly.

9. *Wi-Fi interference does not usually happen.*

Wi-Fi interference is a common and unstoppable issue.

Jupiter Research reports “67 percent of all residential Wi-Fi problems are linked to interfering devices”. Wi-Fi interference happens and we should live with that.

10. I cannot do anything about interference even if I find it.

The solution for interference is to replace the interfering device in most cases. For example, you can replace the cordless phone headset with a non-Wi-Fi frequency band device. Another solution is to move the affected AP, or "jump" to a frequency which is not overlapped by other interfering device.

11. There are a few devices that interfere with Wi-Fi.

It is not obvious which device might be a source of interference. Wireless links can be found in mobile phones, tablets and many other personal devices.

12. The impact on data when interference exists is typically minor.

False. The impact on data throughput of Wi-Fi network can be critical. There are 3 factors that describe the impact of an interference device:

Output power: The higher the power is, the larger the "zone of interference".

Signal behavior with respect to time: Analog devices have constant always-on signal in comparison to digital devices which tend to "burst" on and off. The higher the percentage of time that the signal is "on", the greater the impact it will have on throughput.

Signal behavior with respect to frequency: Some devices operate on a single frequency, and impact specific Wi-Fi channels and some others hop among frequencies.

13. Interference on voice over Wi-Fi should be low because voice data rates are also low.

The data rate of a voice call is no more than eight Kbps. Comparing to the maximum throughput of a Wi-Fi network it seems too little, and it seems reasonable to believe that a Wi-Fi access point can handle many concurrent voice-over-IP calls. However, several factors decrease the number of calls which an access point can handle. First of all, there is important VoIP protocol-level overhead, which increases the stream to 100 Kbps. Then there is additional protocol overhead imposed by Wi-Fi. Secondly, voice traffic is very sensitive to jitter and delay, requiring extra capacity in the network to minimize possible congestions. The typical number of voice calls a Wi-Fi access point can handle is approximately 15. When interference is introduced, the number of calls drops.

14. 802.11n and antenna systems will not be affected by the interference problems.

Systems which use smart antennas can increase their immunity to interference by increasing the signal seen at a receiver. While the signal is stronger, the ratio of signal to interference is also improved. This decreases the interference, but the gain achieved by a smart antenna is only 10 dB of enhanced signal power. This means that the range might be reduced by a factor of 2 in comparison to a traditional antenna system, but the interference problem is not solved.

15. Site survey tools are the solution. They can find interference problems.

Wi-Fi site survey tools are designed to measure Wi-Fi coverage. Wi-Fi chips can detect only Wi-Fi signals, and cannot find any interference produced by non-Wi-Fi devices. [13].

5.5 Smart Tips for your smart home

Public Enemy Number One: Your Neighbors' Wi-Fi Networks

The problem is that most existing Wi-Fi equipment operates on the crowded 2.4GHz band. There are basically three non-overlapping channels. It can be described as a busy three-lane road. If you use a 2.4GHz router and live in a densely populated area, your neighbors' Wi-Fi networks could interfere with yours, hindering the performance and range of your wireless network.

Picture 14: Dual Band Router

The solution: A Dual Band Router can operate at 2.4GHz and 5GHz at the same time (Picture 14). 2.4GHz band is necessary for supporting older Wi-Fi devices but 5GHz is like a new road that nobody's know its existence yet. Newer Wi-Fi devices are all dual-band. They can operate in the 5GHz band.

It is necessary to get a router that supports both 2.4GHz and 5GHz at the same time in order to serve your old and possibly our new 5 GHz devices.

Household Electronics

Picture 15: Microwave oven

Microwave ovens (Picture 15), cordless phones and baby monitors are many times the reasons why your video stream sticks. Most cordless phones and microwave ovens use the 2.4GHz band. Many baby monitors operate at 900MHz and won't interfere with Wi-Fi but some of them are 2.4GHz, which interfere with 802.11 routers.

The solution: Select a wireless baby monitor, (Picture 16) which operates at 900MHz. Alternatively, get a Wi-Fi-friendly system that connects to the existing wireless network. Also, new cordless phone systems using DECT 6.0 technology and operate at the 1.9GHz band is a very good choice.

Picture 16: Wireless baby monitor

Bluetooth Devices

Older Bluetooth devices interfere with Wi-Fi networks--but those days have passed. Over the past several years, Bluetooth and Wi-Fi manufacturers have implemented specific techniques to minimize interference.

Picture 17: Bluetooth Headset

The solution: Most people replace their phones every couple of years, so unless you have a really old phone or Bluetooth device, it's unlikely that your Bluetooth headset (Picture 17) will interfere with Wi-Fi.

6 SOLUTIONS TO INTERFERENCE

6.1 IAMA

Interference-aware multiple access (IAMA) scheme for medium access control (MAC) in ad hoc networks and multihop wireless LANs.

IAMA is the first distributed MAC scheme that can support interference-aware and collision-free transmissions without relying on busy tone or dual transceivers per mobile device. Enabled by its interference awareness, IAMA can naturally support efficient power-controlled variable-radius multiple access, power engineering, and directional antennas [3].

In single-hop WLANs, MAC protocols of IEEE 802.11 work well, but when they are applied to ad hoc networks several problems arise. Particularly, interference problem is a significant issue which is inevitable in ad hoc networks and degrades the throughput and QoS capability if they are not handled carefully. One interference problem occurs when the range of interference is bigger than the coverage range, and when the RTS/CTS messages are only sent in the coverage range of the associated data packet. When there is an irrelevant transmitter in the interference range of an ongoing receiver but outside its own coverage range, then the receiver will be collided by the transmitter if it wants to send a data packet or a control message (Hidden terminal part of the interference-range problem). Additive interference problem is also another interference problem which is difficult to solve. Problems like the above appear when there are multiple interference sources, a reception may be collided even though the receiver is outside of the interference ranges of any other transmitters. This happens because of the additive effect of the interfering signals. The IAMA (Interference-Aware Multiple Access) scheme is based on RTS/Object-to-sending (OTS)/triggered-CTS dialogues. IAMA can solve at the same time the hidden and exposed terminal problem, the additive interference problem, the interference-range problem as well as the heterogeneous

terminal problem concerning power-controlled ad hoc MAC protocols, and the alternate blocking problem concerning QoS provisioning.

(IAMA/SSS) IAMA with Spread Spectrum Scheduling

In this case is used direct sequence spread spectrum techniques with a bigger spreading factor to send control messages in order to raise the reachable control coverage range and solve possible interference problems. When there is not any transmitting or receiving data packets procedure active, all active nodes synchronize to a common code to receive control messages. There is no need for data packets to be transmitted using any other spread spectrum techniques, unless *spread spectrum data* is employed. Since spread spectrum control messages are not utilized for multiplexing concurrent nearby transmissions to avoid collisions, the approach, motivations, and objectives are very different from CDMA-based ad hoc MAC protocols that intend to channelize an ad hoc network and transform it into a multichannel network to achieve concurrent code division multiple access (CDMA) between nearby transmitters [3].

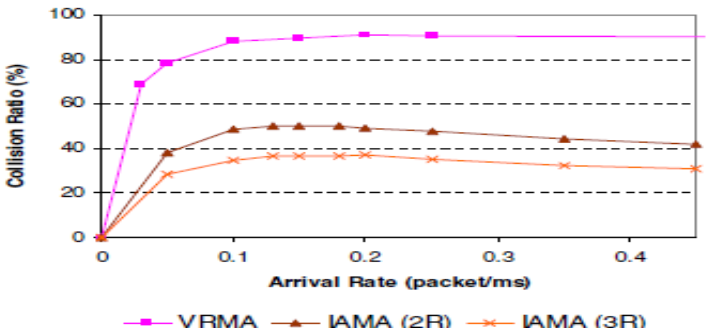
Data-to-control interference ranges are minimized in IAMA/SSS. This scheme has flexibility in modifying the coverage range for control messages. Concluding, IAMA/SSS is more flexible than other protocols using spread spectrum techniques only at the Physical layer and not at the MAC layer. A meaningful application is MAC for ad hoc networks with use of directional antenna. Control messages can be transmitted to big ranges so nodes that are not close to an intended transmitter or receiver can still receive RTS/CTS messages. This results that the IAMA/SSS approach can solve naturally the known as “directional-antenna deafness problem” [3].

(IAMA/SSD) IAMA with Spread Spectrum Data

The scopes for employing spread spectrum techniques comprise, increase the transmission radius for larger connectivity, reduce the data-to-data interference range for *spread spectrum interference control*, and for power control support a differentiated code channel.

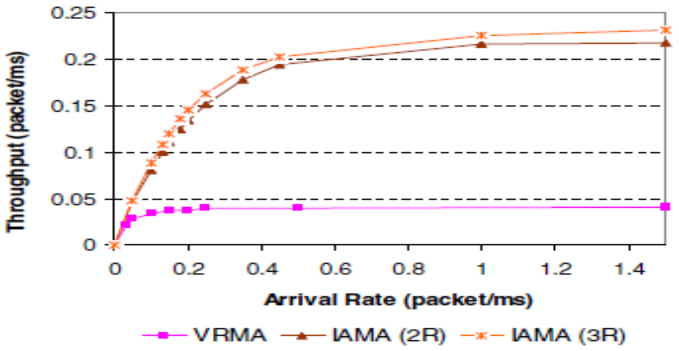
Protocols which support power-controlled VRMA (*Variable-Radius Multiple Access)* like *ROC*, *ROAD*, *ROV*, can reach higher throughput comparing to fixed-radius RTS/CTS protocols and power-controlled MAC protocols with the *heterogeneous terminal problem*. Comparing the performances for IAMA and VRMA with different parameters, IAMA(2R) means IAMA that uses the double data coverage range for RTS and CTS messages. [3]

The same logic is followed for IAMA(3R). IAMA(2R) and IAMA(3R) are *interference-aware VRMA* protocols. It should be mentioned that interference unaware VRMA(R) with the interference-range problem causes collisions (Picture 18).



Picture 17: IAMA(3R) and IAMA(2R) reach lower collision rate comparing with interference-unaware VRMA(R).

From (Picture 19), it can be assumed that IAMA(2R) and IAMA(3R) have higher throughput in comparison with the interference-unaware VRMA(R) because of their fewer collisions (Picture 18). When the path loss exponent stays small for bigger distance, IAMA(2R) performs poorly. In such a case, IAMA(3R) or any dynamic control coverage range/power protocol should be employed in order to have better results [3].



Picture 18: IAMA(3R) and IAMA(2R) reach higher throughput in comparison with interference-unaware VRMA(R) because of smaller collision rates.

SSS (Spread Spectrum Scheduling) can be a solution to the interference-range problem, because combinations of IAMA schemes with detached dialogues, OTS and triggered CTS can overcome the additive interference problem. Furthermore, collision prevention techniques can minimize collisions of control messages driving to a MAC protocol that supports collision-free control-message/data-packet transmissions no matter the presence of any hidden terminals [3].

6.2 SITE SURVEYS - WSN

Site surveys are procedures used to detect interference coming from radio sources in a specific area. The most appropriate time for a site survey is before and after the installation in order to check if the best frequency channel is selected for a given Wireless Sensor Network. Additionally, site surveys can be used to find the appropriate location as well as the number of nodes in a Wireless Sensor Network.

Performance degradation or intermittent broken network connections may result from interference and high bit error rate (BER). This is particularly true in the unregulated Industrial/Scientific/Medical (ISM) 2.4GHz band where IEEE 802.15.4 and 802.11b/g/n (Wi-Fi) devices operate. Additionally, it should be understood that other electronic gear – such as a security camera, cordless phone, microwave oven, amateur radio, wireless USB mouse, video transmitter, RFID reader and others – running in the same band, may add to the interference [10].

Wi-Fi networks and wireless sensors many times share the same frequency bands and overlap of channels and increase of transmission power may produce interference. Interference could raise the BER for both networking technologies forcing them to share the PHY layer. It is obvious that when overlap is lower, the more stable the network will be [7].

After a survey test, a number of indicators are excluded such as:

1. Minimum, Mean, Maximum Signal Strength
2. Ping Success Rate (%)
3. Minimum, Mean, Maximum Link Quality Indicator

Interference derived by wireless devices such as 2.4 GHz cordless phones may not be overcome by a channel change, because such devices run across a very broad spectrum. In such a case turning off or removing the device to another location are the best solutions.

A site survey can be performed using various tools – software and hardware – available in the market. A more complete survey requires a 2.4GHz RF spectrum analyzer to scan and display network activity.

Generally, a site survey is the best insurance policy when operating in the 2.4GHz spectrum. By doing so, users can avoid potential network disruptions or performance degradations caused by signal interference [8], [9].

6.3 NCMAC PROTOCOL

It is globally accepted that IEEE 802.11 is the standard used in the vast majority of Wireless LANs both in infrastructure and ad-hoc mode. The standard specifies a MAC mechanism named DCF (Distributed Coordination Function). However, 802.11 DCF in multi-hop wireless networks has inefficient utilization of energy and bandwidth because of many collisions. The solution to this problem was given by NCMAC (Neighbor-aware Collision avoidance MAC). This protocol specifies algorithms which estimate CWmin and CWmax (Contention Window sizes) depending on the number of nodes-neighbors in the one-hop neighborhood and the energy level of the battery. After a successful or unsuccessful transmission another resetting algorithm has been also designed to be applied [6].

NCMAC results in throughput numbers and also reduces collisions resulting in comparison with IEEE 802.11 DCF.

This MAC protocol with a novel resetting algorithm is based on the number of neighbors in the 1-hop neighborhood, a coefficient of the fast/slow increase/decrease of 1-hop neighbors and the number of retransmission attempts. The minimum and maximum Contention Window sizes are selected taking into account the number of 1-hop neighbors and the energy level of battery. The NCMAC protocol achieves better throughput and noticeably reduces the number of collisions resulting in longer network lifetime and later dead of the first node as compared with the 802.11 DCF [6].

6.4 MULTICHANNEL COGNITIVE MAC PROTOCOL

CR (Cognitive radio) is a relatively new wireless communication concept in which a network or a wireless node can sense spectrum holes, and change its transmission and reception chains to communicate in an opportunistic way, without interfering with other users. CR also aims to change the utilization of the scarce radio spectrum. Nowadays' approach is to divide the spectrum into pieces, each for a special purpose. But due to the fact that applications use their spectrum to a limited extent, this results in under-utilization of the scarce radio resource. Because of the constant radio communications growth, authorities realize that the typical approach is on its limits and they are planning to open bands for cognitive use. Therefore, dynamic spectrum allocation and cognitive

radio are becoming mainstream technologies in the field of wireless communications [4].

Characteristics of cognitive radio

1) Cognitive capability

Because of real-time interaction with the radio environment, portions of spectrum which are unused at a specific location or time can be found. Cognitive Radio enables temporarily unused spectrum, known as spectrum holes or white spaces. This results in the best selection of the spectrum, shared with other users, without interfering with the licensed users.

2) Reconfigurability

A Cognitive Radio can transmit and receive on many frequencies, and use different technologies supported by the hardware. Because of this property, the most appropriate band and the best operating parameters can be chosen and reconfigured.

Also, the channels in the spectrum can be scanned by secondary users learning at the same time which is the behavior of the primary users on every channel. Knowing that learning, secondary users choose the best available channel and start communicating without creating any damage to the primary users' data.

The multichannel cognitive MAC protocol learns the behavior of primary users on each channel and allows the secondary users to occupy the unused spectrum without any harmful interference with the primary user and with other secondary users. By using the probabilistic model, CR estimates each available channel and selects the best one for transmission [4].

The Cognitive MAC protocol is designed for secondary users to identify time varying availability of channels and decide when and which channel should be chosen to communicate among the secondary users without damaging the primary users' data. Although this protocol improves the utilization of the spectrum, it further exploits the available spectrum and reduces the probability of collision [4].

Description of the protocol

Secondary users track the behavior of primary users on each channel and update periodically their Channel Status Table. The protocol deals with multiple channels, secondary users jump among available channels, with handshaking processes between pairs of secondary users. For example, a universal control channel is available and secondary nodes exchange information in this control channel in order to select data channel.

Sender sends Ready to Send (RTS) packet including information about which channels are available and predicted transmission duration (*timeslot*) of each channel to the receiver. This predicted transmission duration is calculated depending on the behavior of primary users in each channel and time to choose. Receiver compares *timeslots* of each free channel and selects the best, sending information about the selected channel in a Clear to Send (CTS) packet to the sender. At the same time, CTS packet informs neighboring secondary users about the coming soon connection to avoid possible collisions. Then, sender and receiver start sending data within the predicted timeslot in the selected channel [4].

This protocol improves the numbers of spectrum utilization and network throughput. Secondary users find free spectrum and capitalize this without causing any interference to primary users [4].

6.5 DISTRIBUTED ADAPTIVE INTERFERENCE-AVOIDANCE PROTOCOL

In order to face interference, ZigBee uses frequency agility, which is more specifically the ability of ZigBee networks to change the used channel when interference is identified. However, large ZigBee networks are too difficult to change their operational channel to an idle one, if there is no any single idle channel available globally. A distributed adaptive multi-channel MAC interference-avoidance protocol, which enables a conventional large-scale single-channel ZigBee network to change the operational channel in order to avoid interference, would be a good solution. According to simulation results, that protocol can improve the ZigBee network robustness as well as the coexistence performance [2].

It consists of two phases:

A. Interference detection

An ACK/NACK interference detection scheme is the whole idea. Interference is detected by each device. There is no need to exchange info among each other. Initially, a device tracks the transmission failures because of the inhibition loss which is produced by channel access failures. While transmission failure ratio, (transmission failures / specified total transmission attempts), is bigger than a threshold, ($TH_{transfailure}$) the device

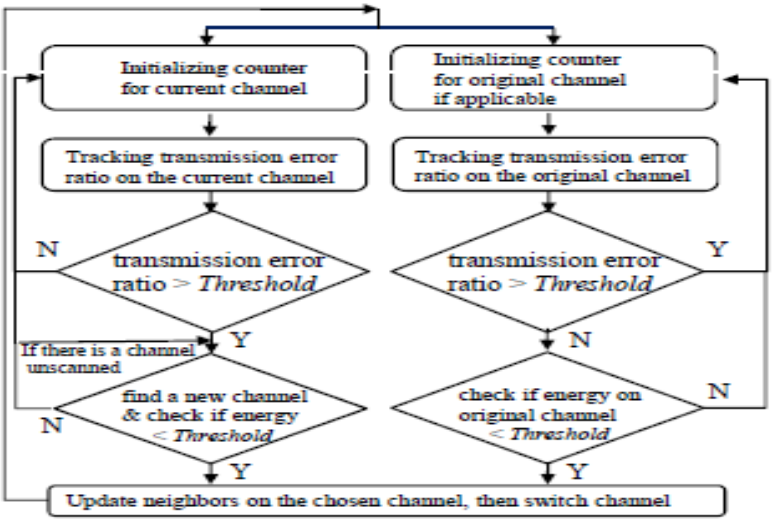
makes an energy scan in the channel. If the energy level of the channel is larger than another threshold, (TH_{energy}) the device defines that interference exists [2].

B. Interference avoidance

When a ZigBee device detects interference, it manages energy scans on channels in a sequence provided by a channel selection algorithm until finding a channel the energy level is less than the threshold. If scanning fails to find such a channel the device remains at the current channel.

If a new channel is chosen, the device broadcasts to notify its 1-hop neighbors about the new operational channel. Broadcast does not stop until at least one notification is transmitted successfully. Then, the device "jumps" from the current channel to the new one.

After that, the device broadcast every *nwkLinkStatusPeriod* seconds a link status command including its new operational channel number on its neighbors' operational channels, in order to keep the neighbors updated. When the broadcast is received, the neighbors update the device info. When the transmission failure ratio gets less than the threshold, the device will scan again on the original channel. If the energy level is less than TH_{energy}, the device will change the operational channel back to the original one and update the neighbors. In general, the network can operate on the same channel again if interference is gone (Picture 20).

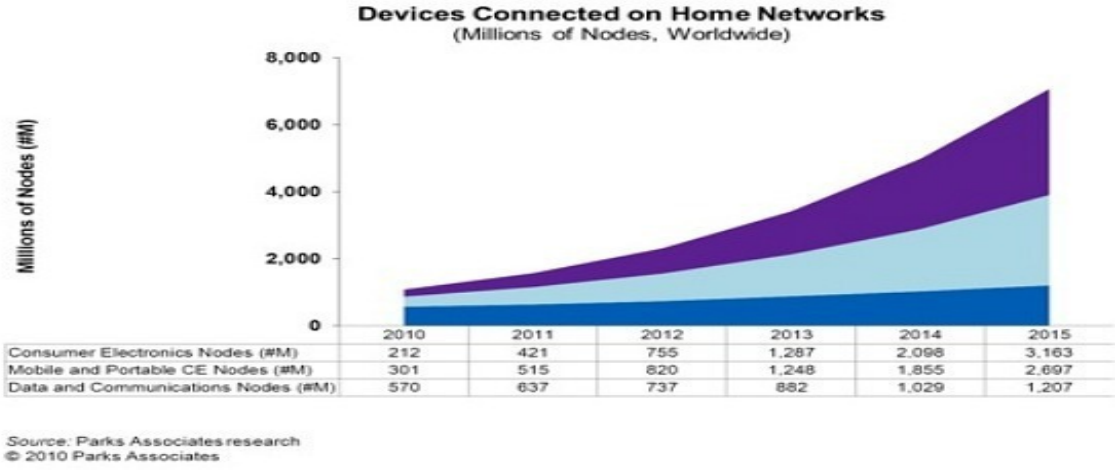


Picture 19: Distributed adaptive multi-channel MAC protocol

Distributed adaptive multi-channel MAC protocol in large-scale ZigBee networks mitigate the local interference and also improve the ZigBee performance. When ZigBee networks are small-scale the protocol may not have better results than the way of changing the channel for the entire network [2].

7 CONCLUSION

7.1 A Look into the Future



Picture 20: Devices Connected on Home Networks

Initially, it was just a film scenario, then just a dream, but now the automated "smart" home is reality and knocks the door of our house (Picture 21). Many years ago, we achieved to remotely lock or unlock our car doors, raise or lower the car windows, change the temperatures for the car seats, and to clean the front and back windows. The question is why cannot we do that with our homes? The smart home with devices communicating each other, with central home systems and appliances that can be controlled from a central home dashboard or over a network will become reality and that is inevitable. Apart from a few innovators, the majority of homes are still stupid nowadays. However, that situation is changing rapidly. Most homes already have more than 2 wireless networks. Wi-Fi for data and cordless phones for communication calls are the most usual. Both are very effective for high bandwidth, power gulping applications like watching videos through the internet or talking on the phone but for many not such intensive data communications, the new low power networks, based on the IEEE 802.15.4 and ZigBee, promise to not only make homes smart, but to do it in a way that is both maintenance-free and friendly for the environment. Electronics manufacturers and service providers already start rolling out systems for homes that finally will make homes as smart as cars. In the near future, new capabilities will be added to that remote. RF powered remote control will give the ability to the user to monitor and control all the

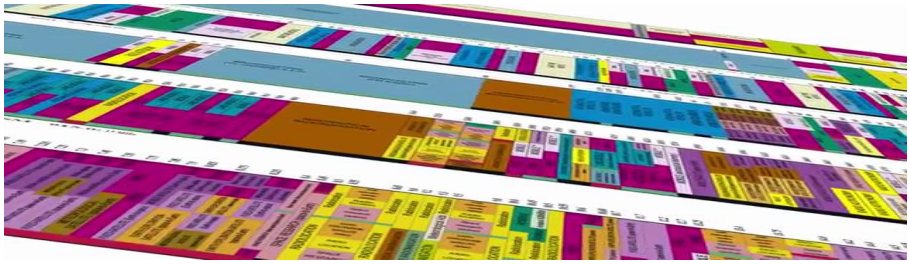
house systems from a central remote control device. By using RF instead of the old fashioned IR (infrared), this central mobile dashboard can be used in any room to control systems based in other parts of the home. RF transits through walls, through doors, and through furniture. Because RF supports interactivity, not only can the home owner control other systems, but he can monitor the systems as well by using the display on the remote. While sitting in the home office, he can monitor and control the temperature in different rooms, set up recording on the DVD in the living room, turn off the lights in the kids' rooms after they go out and play. He can even capture a digital image from the front door camera to see who is ringing the doorbell.

The combination of these technologies of course can be done now, but they are not cheap enough and technical expertise is necessary to make them easy to use. With ZigBee vendors create systems and devices that will be cheaper and able to interact with each other. Additionally, the low power capabilities of ZigBee devices make them maintenance free and friendly for the environment by dramatically decreasing the number of batteries needed to operate the sensors in the home. It is known that batteries because of the toxic chemicals which contain are dangerous polluters of the Earth. Using low-power wireless technology disappears the need to usually change or charge the batteries. Furthermore, ZigBee networks are ecological as well as making our lives more convenient.

Today, connectivity is generally regarded as a high-end novelty in home devices, such as utility meters, thermostats, security cameras, TVs and Blu-ray players, rather than a feature for the mass-market. This view will become outdated as we move to the future where connectivity is pervasive and embedded in virtually all household devices. Many analysts believe that the smart home of the future is likely to contain 15 to 30 connected devices and sensors, all linked via a home area network and connected to service providers' back-end systems and the Internet. [28].

7.2 What about the Spectrum?

The increasing sophistication and growth of new technologies is increasing the demand for spectrum while increasing the opportunity for more productive use of spectrum (Picture 22).



Picture 21: RF Spectrum

It is clear that the strict command-and-control management of the spectrum is on its limits. The regulation authorities as usual do not have adequate understanding of the spectrum requirements of new technologies. Instead, they will fight to create new efficient spectrum allocation strategies. They have realized that the involvement of market makers in the wireless technology space, as well as service providers, equipment manufacturers, network operators and researchers is vital for the development of desired strategies, giving support for innovation and of course to the global economic growth. It is obvious, that spectrum licensing and technology-specific spectrum allocation have been very significant for the development of wireless technologies.

On the whole, the balance of supply and demand for spectrum designates the need for spectrum trading. Devices in the near future will be able to access licensed spectrum on an opportunistic basis. Being aware of the spectral occupancy in their radio environment will be required. With taking statistics of spectrum usage, (from direct measurements or other sources), the devices will have the ability to apply algorithms and evolve strategies for optimum spectrum access. Co-operation among devices may be required, not only for providing info about the spectrum occupancy, but also relating to spectrum access [29].

Concluding, no matter which paths wireless spectrum technologies will take in the future, spectrum usage rights should be defined as a framework for user behavior. Spectrum usage rights are the recognition of the growing trend towards considering spectrum licenses as property rights that can be owned, traded or even shared.

Bibliography

[1] King, Nicola (2003) Smart Home – A Definition, Intertek Research and Testing Centre

[2] Wei Yuan, et al, "Distributed Adaptive Interference-Avoidance Multi-channel MAC Protocol for Zigbee Networks", Proc. Of IEEE international Conference on Computer and Information Technology, June, 2010.

[3] Yeh, C.-H., "High-throughput interference-aware MAC protocols for heterogenous ad hoc networks and multihop wireless LANs", 2003.

[4] Khan, S. ; Dept. of Electr. Eng., COMSAT S Inst. of Inf. Technol., Lahore, Pakistan ; Khan, A.N. ; Akhtar, S., "Multichannel Cognitive MAC Protocol for Efficient Utilization of Wireless Spectrum", Pages: 286 – 289, Third International Conference on Communications and Mobile Computing, 2011.

[5] C.-H. Yeh "Interference-aware Energy-efficient MAC Protocols for Sensor and Wireless Pervasive Networks", Proc. IEEE Int'l Conf. Systems, Man, and Cybernetics, 2006

[6] Sylwia Romaszko, Chris Blondia, "Neighbour-Aware, Collision Avoidance MAC Protocol (NCMac) for Mobile Ad Hoc Networks", IEEE 2006.

[7] ArchRock,

[8] IEEE 802.11

[9] IEEE 802.15.4

[10] Metageek

[11] Moog Crossbow , "Avoiding RF Interference Between WiFi and ZigBee"

[12] Graham Roth, "Bluetooth Wireless Technology", Stanford University, 2012.

[13] Cisco Spectrum Expert White Papers.

[14] Telkonet ECOsmart Product Suite.

[15] GSMA, "Vision of Smart Home, The Role of Mobile in the Home of Future".

[16] David Egan, "Designing a ZigBee network", Ember Corporation, 2006.

[17] Cisco, Radio Channel Frequencies.

[18] Cisco, WLAN Radio Frequency Design Considerations

[19] Radio-Electronics.com.

[20] Jeffrey G. Andrews, Arunabha Ghosh, Rias Muhamed, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking", Pearson Education, 2007

[21] ZigBee Alliance

[22] C. Ramya, M. Shanmugaraj, and R. Prabakaran, "Study on ZigBee technology," in Electronics Computer Technology (ICECT), 2011 3rd International Conference on, 2011, pp. 297-301.

[23] IEEE802.org.

[24] O. B. Akan, O. Karli and O. Ergul, "Cognitive radio sensor networks", IEEE Netw, pp.34 -40, 2009.

[25] ETSI.org, "Short Range Devices".

[26] N. Golmie, National Institute of Standards and Technology, “Interference in the 2.4 GHz ISM Band: Challenges and Solutions”, Gaithersburg, Maryland.

[27] Turning Technologies “RF Interoperability”.

[28] Sergey Gerasimenko, “The evolution of wireless home networking”, Helsinki University of Technology

[29] S Olafsson, B Glover and M Nekovee, “Future management of spectrum”, 2007.

GLOSSARY

ACRONYM	DEFINITION
ACK	Acknowledgement
AFH	Adaptive Frequency Hopping
BER	Bit Error Rate
BS	Base Station
CCK	Complementary Code Keying
CDMA	Code Division Multiple Access
CPE	Customer Premises Equipment
CR	Cognitive Radio
CSMA	Carrier Sense Multiple Access
CTS	Clear to Send
CW	Contention Window
DCF	Distributed Coordination Function
DECT	Digital Enhanced Cordless Telecommunications is a standard primarily used for creating cordless telephone systems
DFS	Dynamic Frequency Selection
DNS-SD	DNS Service Discovery
DPSK	Differential Phase-Shift Keying
DQPSK	Differential Quadrature Phase Shift Keying
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
DTV	Digital Television
DVB-T	Digital Video Broadcasting - Terrestrial
EDR	Enhanced Data Rate
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
FEC	Forward Error Correction
FHSS	Frequency Hopping Spread Spectrum
FM	Frequency Modulation
GFSK	Gaussian Frequency Shift Keying
HSPA	High Speed Packet Access
IAMA/SSD	Spread Spectrum Data
IAMA/SSS	Spread Spectrum Scheduling
IAMA	Interference-Aware Multiple Access protocol
IEEE	Institute of Electrical and Electronics Engineers
IMT 2000	International Mobile Telecommunications for the year 2000
ISM	Industrial Scientific and Medical Radio Bands
LQI	Link Quality Indicator

LTE	Long Term Evolution
MAC	Media Access Control
mDNS	Multicast DNS
MIMO	Multiple-Input Multiple-Output[i]
NACK	Negative Acknowledgement
NCMAC	Neighbor-aware Collision-avoidance MAC protocol
PAL	Phase Alternate Line
OFDM	Orthogonal Frequency Division Multiplex[ii]
PHY layer	Physical layer
PN Codes	Pseudonoise codes
PSK	Phase Shift Keying
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
RFID	Radio Frequency Identification
ROC	Report on Compliance
ROV	Report on Validation
RSSI	Receive Strength Signal Indicator
RTS	Ready to Send
SCH	Superframe Control Header
SIG	Special Interest Group
SRD	Short Range Devices 25 mW max power.
TDD	Time Division Duplex
TH	Threshold
TPC	Transmit Power Control
TS	Time Slot
UMTS	Universal Mobile Telecommunications System
VRMA	Variable-Radius Multiple Access
WRAN	Wireless Regional Area Network
WSN	Wireless Sensor Network

[i] Two major limitations in communications channels can be multipath interference, and the data throughput limitations as a result of Shannon's Law. MIMO provides a way of utilizing the multiple signal paths that exist between a transmitter and receiver to significantly improve the data throughput available on a given channel with its defined bandwidth. By using multiple antennas at the transmitter and receiver along with some complex digital signal processing, MIMO technology enables the system to set up multiple data streams on the same channel, thereby increasing the data capacity of a channel.

[ii] It is a form of transmission that uses a large number of close spaced carriers that are modulated with low rate data. Normally these signals would be expected to interfere with each other, but by making the signals orthogonal to each other there is no mutual interference. The data to be transmitted is split across all the carriers to give resilience against selective fading from multi-path effects.