**DICOMA: DI**saster **CO**ntrol **MA**nagement


# Deliverable D5.1

# Design Document Identification of communication requirements and functionalities

| | |
|---|---|
| ***Project Identifier*** | DICOMA |
| ***Project Title*** | **DIsaster COntrol MAnagement** |
| ***Document Version*** | 0.1 |
| ***Planned Delivery Date*** | |
| ***Actual Delivery Date*** | 30th September 2013 |
| ***Document Title*** | Design Document Identification of communication requirements and functionalities |
| ***Work Package*** | WP5 |
| ***Document Type*** | Deliverable |

***Abstract*** This document provides an analysis of the state of the art of the existing and emerging fixed and mobile communications systems and networks regarding co-existence issues operating on site and identifies the communication requirements, functionalities, performances and types of the applications required for the gathering of information, routing and coordination among the decision-making bodies in the different DiCoMa Scenarios.

***Keywords*** State-of-the-art, communication requirements, co-existence, decision-making

| Function | Name | Entity |
|---|---|---|
| **Editor** | Clara Luján | Universidad de Sevilla |
| **Author/s** | Juan Pablo García | Universidad de Sevilla |
| | | |
| | | |

**List of DiCoMa participants in the deliverable:**

| Partner | Country | Type |
|---|---|---|
| Deusto Tech | Spain | RES |
| Finnish Meteorological Institute/Arctic Research and Meteorological Research Group | Finland | RES |
| Infotripla | Finland | SME |
| Mattersoft | Finland | SME |
| Mobisoft | Finland | SME |
| Savox | Finland | SME |
| University of Seville | Spain | UNI |
| VTT | Finland | RES |

# Table of Contents

# List of Figures

# List of Tables

# List of abbreviations

| | |
|---|---|
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **ISM band** | Industrial, Scientific and Medical band |
| **FCC** | Federal Communications Commission |
| **ECC** | Electronic Communications Committee |
| **CEPT** | European Conference of Postal and Telecommunications Administration |
| **SRRC** | State Radio Regulatory Commission |
| **ITU** | International Telecommunications Union |
| **ISA** | International Society of Automation |
| **SRD** | Short Range Device |
| **MAN** | Metropolitan Area Network |
| **LAN** | Local Area Network |
| **WLAN** | Wireless Local Area Networks |
| **WiFi** | Wireless-Fidelity |
| **DSSS** | Direct Sequence Spread Spectrum |
| **FHSS** | Frequency Hoping Spread Spectrum |
| **TDM** | Time Division Multiplexing |
| **FDM** | Frequency Division Multiplexing |
| **OFDM** | Orthogonal Frequency Division Multiplexing |
| **SOFDMA** | Scalable Orthogonal Frequency Division Multiplexing Access |
| **WEP** | Wired Equivalent Privacy |
| **WPA** | Wi-Fi Protected Access |
| **CCK** | Complementary Code Keying |
| **DRS** | Dynamic Rate Switching |
| **MIMO** | Multiple Input/Multiple Output |

| | |
|---|---|
| **WMM** | WiFi Multimedia |
| **NIC** | Network Interface Card |
| **AP** | Access Point |
| **VPN** | Virtual Private Network |
| **AAA server** | Authentication, Authorization and Accounting server |
| **BSS** | Basic Service Group |
| **IBSS** | Independent BSS |
| **ESS** | Extended BSS |
| **WDS** | Wireless Distribution System |
| **ADSL** | Asymmetric Digital Subscriber Line |
| **ISDN** | Integrated Services Digital Network |
| **SSID** | Service Set IDentifier |
| **EAP** | Extensible Authentication Protocol |
| **RSN** | Robust Security Network |
| **WiMAX** | Worldwide Interoperability for Microwave Access |
| **LMDS** | Local Multipoint Distribution Service |
| **QoS** | Quality of Service |
| **LOS** | Line Of Sight |
| **NLOS** | Non Line Of Sight |
| **MAC** | Medium Access Control |
| **BWA** | Broadband Wireless Access |
| **PKM** | Privacy Key Management |
| **CSMA/CA** | Carrier Sense Multiple Access with Collision Avoidance |
| **PER** | Probability of Error Rate |
| **PN** | Pseudo Number |
| **HART** | Highway Addressable Remote Transducer |

# 1 Introduction

## 1.1 Document Objectives and Scope

The main objective of this document is to define the communication requirements, functionalities, performances and types of applications required for the gathering of information, routing and coordination among decision-making bodies in the different DiCoMa scenarios. For this, an analysis on the "state of the art" of existing and emerging fixed and mobile communication protocols has been performed regarding co-existence issues and a description of the communication protocols, routing and security issues has been provided as the result of a comprehensive study of the different use cases.

In disaster management communication between all units and stakeholders is essential. The main possible channels are:

- Wireless RF communication.
- Satellite communication.
- Mobile communication.
- Wired communication.

Naturally in crisis situations the wired networks may be partially ruined and not available. The same may go with the cellular networks, if the base stations overcome out of order or destroyed. In these situations wireless meshed networks allow the deployment of a temporary broadband and narrow-band network in the affected areas reinforcing the means of communication. Therefore, in the case of natural disaster or crisis situation, it is necessary to cover all the existing means of communication.

Communications cause often most of the challenges and drawbacks during disaster situations. The involved stakeholders should be efficiently coordinated and provided with the information of the disaster location, scale and available resources to manage the situation. In the chaotic environment of disasters or crisis, new technologies in communications and advanced "smart devices" have the potential to vastly improve the management of them.

## 1.2 Document Structure

Chapter 2 is dedicated to the state of the art of the communication protocols and the co-existences issues applicable to each use case. Chapter 3 analyzes the communication requirements and coordination among the different decision-making bodies and finally, chapter 4 lists the main references (i.e. standards, scientific contributions, etc.) that have been used to prepare this document.

# 2 State of the art and coexistence of communications

## 2.1 Fixed technologies

### 2.1.1 Global perspective

As reported in the Deliverable D4.10 Middleware architecture definition, the evolution that Switched Ethernet technology has suffered in recent years, in addition to the emergence of new standards [1] that allow the prioritization of network traffic, and the low cost of their implementation, have led to a great interest in the industry for its application in the development of applications with temporary requirements. The use of switches instead of hubs has allowed achieving a more predictable traffic in terms of behaviour by introducing a single collision domain per port and the use of full-duplex communications to suppress collisions. Moreover, the volume of information that the switch can receive simultaneously has increased and consequently, the existence of extremely long messages or an excess of multicast or broadcast package may result in an overflow in the queues of each port [2]. This effect can be controlled by traffic control techniques [3] or in the future specification of IEEE 802.1Qbb [4].

The IEEE 802.1p standard aims to distinguish different types of transmitted traffic through the switch. For this, the Ethernet frame is extended with four bytes, from which only three bits are used to specify the priority of the message, providing eight different levels of priority.

Another important aspect to consider in the use of commercial equipment in real-time systems is the internally generated traffic by switches themselves. This traffic from other protocols such as Spanning Tree [5] must be disabled and if this is not possible, the traffic influence must be modeled on the temporal response of the network.

The increasing use of Switched Ethernet in real-time systems has spread across even in fields that were unthinkable in the last years. In avionics, for example, networks used until now were based on serial lines or commercial standards ARINC-429 and ARINC-629. The new specification ARINC-664 integrates the Switched Ethernet technology into data networks for aircraft, specifically in its Chapter 7 called Avionics Full-Duplex Switched Ethernet (AFDX). Nevertheless, this specification imposes set of restrictions to solve the temporal unresolved indeterminism in Switched Ethernet in general: resizing of input/output queues, static forwarding of messages, minimum performance in package processing, resource reservation for each connection, etc. The required high-integrity features to these networks and the low number of units in comparison with the general-purpose Ethernet mean that, for the moment, the cost of such networks is very high.

Therefore, Switched Ethernet technology is presented as a valid alternative to the traditional real-time networks, but this is only when it is running under certain specific conditions (eg with controlled traffic loads).

The Ethernet standard, included in the IEEE 802.3 standard, was initially designed for equipment interconnections at office level. However, the debate about its application in Automated control systems and real-time has been the source of a major research field over the last decade due to its low cost and high speed transmission (up to 10Gbps today). In its original conception, Ethernet technology did not meet some basic requirements for its use in real-time systems. The main reason of discussion resides in the medium access algorithm known as CSMA / CD (Collision

Sensing Multiple Access with Carrier Detection): according to this algorithm, those nodes that want to initiate communication must wait until the communication bus is free, instant in which the transmission can be started. Similarly, other network nodes can in a similar situation and will initiate the transmission producing collision between messages. This collision is detected by every station that will stop the transmission and, according to the algorithm CSMA / CD, will wait a random time to resume communication. This time will be increased exponentially in other attempts up to a maximum of 16. To overcome the lack of temporal determinism of CSMA / CD various solutions have been proposed.

### 2.1.2 References

[1] IEEE Std 802.1Q. "Virtual Bridged Local Area Networks" Annex G. IEEE Document, May 2006

[2] Pedreiras P., Almeida L., y Gai P. "Characterizing the Real-Time Behavior of Prioritized Switched-Ethernet" Proc. of the 2nd Intl Workshop on Real-Time LANs in the Internet Age, Porto Portugal, July 2003

[3] Vila-Carbó J., Tur-Masanet X., y Hernández-Orallo E. "An evaluation of switched ethernet and linux traffic control for real-time transmission". Proc. of the IEEE International Conference on Emerging Technologies and Factory Automation, Hamburg Germany, September 2008

[4] IEEE 802.1Qbb "Priority based flow-control", Draft v1.3, Febrero 2010

[5] IEEE Std 802.1D-2004. "Media Access Control (MAC) Bridges". IEEE Document, June 2004

## 2.2 Mobile technologies

### 2.2.1 Global perspective

Broadband communications between moving units such as emergency vehicles, fire fighters, police, etc. are essential in disaster situations. In mobile communications the possible technologies are:

- Cellular telephony systems (2G, GPRS, 3G, LTE and 4G)
- Terrestrial Trunked Radio (TETRA)
- Satellite communications systems
- Millimetre wave systems (medium and long range, high speed, air interface parameters and protocols for broadcast, point-point communications)
- WLAN
- WiFi

Section 2.2 concentrates on 2G, 3G, LTE and 4G. WLAN and WiFi are discussed in section 2.3. Mobile or cellular networks are radio networks distributed over land areas called cells, each served by at least one fixed-location transceiver, base station. In a cellular network, each cell uses a different set of frequencies from neighboring cells to avoid interference and provide

guaranteed bandwidth within each cell. When joined together these cells provide radio coverage over a wide geographic area. This enables a large number of portable transceivers (e.g., mobile phones) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission. The most common example of a cellular network is a mobile phone (cell phone) network. As long as the cellular network exists and is up and running it can be used in the disaster and crisis situations.

Cellular networks offer a number of advantages over alternative solutions:

- flexible enough to use the features and functions of almost all public and private networks [http://scis.nova.edu/~raciti/cellular.html]
- increased capacity
- reduced power use
- larger coverage area
- reduced interference from other signals

Mobile technology is the technology used for cellular communication. Mobile code division multiple access (CDMA) technology has evolved rapidly over the past few years. Since the start of this millennium, a standard mobile device can in addition to a simple mobile phone also include a GPS navigation device, an embedded web browser and instant messaging client, and a handheld game console.

### 2.2.2 2G

2G is short for the second-generation wireless telephone technology. Second generation 2G cellular telecom networks were commercially launched on the GSM standard in Finland by company Radiolinja in 1991.[1] The three primary benefits of 2G networks over their predecessors were that the phone conversations were digitally encrypted, 2G systems were significantly more efficient on the spectrum allowing for far greater mobile phone penetration levels and 2G introduced data services for mobile, starting with SMS text messages. Especially the data services can be seen as huge step further in professional usage.

While radio signals on old 1G networks were analog, radio signals on 2G networks were digital. Both systems used digital signaling to connect the radio towers (which listen to the handsets) to the rest of the telephone system. 2G has been superseded by newer technologies such as 2.5G, 2.75G, 3G, and 4G; however, 2G networks are still used in many parts of the world.

### 2.2.3 GPRS

2.5G ("second and a half generation") is used to describe 2G-systems that have implemented a packet-switched domain in addition to the circuit-switched domain. The first major step in the evolution of GSM networks to 3G occurred with the introduction of General Packet Radio Service (GPRS). CDMA2000 networks similarly evolved through the introduction of 1xRTT. The combination of these capabilities came to be known as 2.5G. GPRS could provide data rates from 56 kbit/s up to 115 kbit/s. It can be used for services such as Wireless Application Protocol

(WAP) access, Multimedia Messaging Service (MMS), and for Internet communication services such as email and WWW access. GPRS data transfer is typically charged per megabyte of traffic transferred, while data communication via traditional circuit switching is billed per minute of connection time, independent of whether the user actually is utilizing the capacity or is in an idle state. 1xRTT supports bi-directional (up and downlink) peak data rates up to 153.6 kbit/s, delivering an average user data throughput of 80-100 kbit/s in commercial networks. [2] It can also be used for WAP, SMS & MMS services, as well as Internet access.

GPRS1 networks evolved to 2,75G (EDGE) networks with the introduction of 8PSK encoding. Enhanced Data rates for GSM Evolution (EDGE), Enhanced GPRS (EGPRS), or IMT Single Carrier (IMT-SC) is a backward-compatible digital mobile phone technology that allows improved data transmission rates, as an extension on top of standard GSM. EDGE was deployed on GSM networks beginning in 2003—initially by Cingular (now AT&T) in the United States. EDGE is standardized by 3GPP as part of the GSM family and it is an upgrade that provides a potential three-fold increase in capacity of GSM/GPRS networks.

### 2.2.4 3G

3G is the third generation of mobile telecommunications technology. 3G telecommunication networks support services that provide an information transfer rate of at least 200 kbit/s. However, many services advertised as 3G provide higher speed than the minimum technical requirements for a 3G service. Recent 3G releases often denoted 3.5G and 3.75G, also provide mobile broadband access of several Mbit/s to smartphones and mobile modems in laptop computers.

3G finds application in wireless voice telephony, mobile Internet access, fixed wireless Internet access, video calls and mobile TV. 3G has been relatively slow to be adopted globally. In some instances, 3G networks do not use the same radio frequencies as 2G so mobile operators must build entirely new networks and license entirely new frequencies, especially to achieve high data transmission rates. Other delays were due to the expenses of upgrading transmission hardware, especially for UMTS, whose deployment required the replacement of most broadcast towers. Due to these issues and difficulties with deployment, many carriers were not able to provide these updated capabilities or delayed in their acquisition.

In December 2007, 190 3G networks were operating in 40 countries and 154 HSDPA networks were operating in 71 countries, according to the Global Mobile Suppliers Association (GSA). In Asia, Europe, Canada and the USA, telecommunication companies use W-CDMA technology with the support of around 100 terminal designs to operate 3G mobile networks.

Roll-out of 3G networks was delayed in some countries by the enormous costs of additional spectrum licensing fees. The license fees in some European countries were particularly high, bolstered by government auctions of a limited number of licenses and sealed bid auctions, and initial excitement over 3G's potential.

The 3G standard is perhaps well known because of a massive expansion of the mobile communications market post-2G and advances of the consumer mophone. An especially notable development during this time is the smartphone (for example, the iPhone, and the Android family), combining the abilities of a PDA with a mobile phone, leading to widespread demand for mobile internet connectivity. 3G has also introduced the term "mobile broadband" because its speed and capability make it a viable alternative for internet browsing, and USB Modems connecting to 3G networks are becoming increasingly common.

*From DiCoMa point of view 3G can perhaps be seen as the main mobile communication channel.*

### 2.2.5 LTE

LTE, an initialism of Long Term Evolution, marketed as 4G LTE, is a standard for wireless communication of high-speed data for mobile phones and data terminals. It is based on the GSM/EDGE and UMTS/HSPA network technologies, increasing the capacity and speed using a different radio interface together with core network improvements [3]. The standard has been developed by the 3GPP (3rd Generation Partnership Project) and is specified in its Release 8 document series, with minor enhancements described in Release 9.

The world's first publicly available LTE service was launched by TeliaSonera in Oslo and Stockholm on December 14, 2009. LTE is the natural upgrade path for carriers with both GSM/UMTS networks and CDMA networks such as Verizon Wireless, who launched the first large-scale LTE network in North America in 2010 and au by KDDI in Japan have announced they will migrate to LTE. Airtel launched the LTE service in India in April 2012. LTE is, therefore, anticipated to become the first truly global mobile phone standard, although the different LTE frequencies and bands used in different countries will mean that only multi-band phones will be able to use LTE in all countries where it is supported.

Although marketed as a 4G wireless service, LTE (as specified in the 3GPP Release 8 and 9 document series) does not satisfy the technical requirements the 3GPP consortium has adopted for its new standard generation, and which were originally set forth by the ITU-R organization in its IMT-Advanced specification. However, due to marketing pressures and the significant advancements that WIMAX, HSPA+ and LTE bring to the original 3G technologies, ITU later decided that LTE together with the aforementioned technologies can be called 4G technologies[4] The LTE Advanced standard formally satisfies the ITU-R requirements to be considered IMT-Advanced [5]. And to differentiate LTE Advanced and WiMAX-Advanced from current 4G technologies, ITU has defined them as "True 4G". [4].

**¡Error! No se encuentra el origen de la referencia.***When it comes to the DiCoMa countries Finland and Spain have commercial LTE service, in Israel LTE network deployment is on-going/planned and in Turkey LTE is in trial phase.*

### 2.2.6 4G

4G is the fourth generation of mobile phone mobile communication technology standards. It is a successor of the third generation (3G) standards. As mentioned above LTE does not satisfy the technical requirements for 4G. 4G system provides mobile ultra-broadband Internet access, for example to laptops with USB wireless modems, to smartphones, and to other mobile devices. Conceivable applications include amended mobile web access, IP telephony, gaming services, high-definition mobile TV, video conferencing, 3D television, and cloud computing.

One of the most important features in the 4G mobile networks is the domination of high-speed packet transmissions or burst traffic in the channels. The same codes used in the 2G-3G networks is applied to 4G mobile or wireless networks, the detection of very short bursts will be a serious problem due to their very poor partial correlation properties. Recent study has indicated that traditional multi-layer network architecture based on the Open Systems Interconnection (OSI) model may not be well suited for 4G mobile network, where transactions of short packets will be the major part of the traffic in the channels. As the packets from different mobiles carry

completely different channel characteristics, the receiver should execute all necessary algorithms, such as channel estimation, interactions with all upper layers and so on, within a very short time to make the detections of each packet flawless and even to reduce the clutter of traffic.

### 2.2.7 TETRA

TETRA is a professional mobile radio [TETRA Association. 2012-03-22] and two-way transceiver (colloquially known as a walkie talkie) specification. TETRA was specifically designed for use by government agencies, emergency services, (police forces, fire departments, ambulance) for public safety networks, rail transportation staff for train radios, transport services and the military.

TETRA uses Time Division Multiple Access (TDMA) with four user channels on one radio carrier and 25 kHz spacing between carriers. Both point-to-point and point-to-multipoint transfer can be used. Digital data transmission is also included in the standard though at a low data rate. [http://en.wikipedia.org/wiki/Terrestrial_Trunked_Radio].

TETRA Mobile Stations (MS) can communicate direct-mode operation (DMO) or using trunked-mode operation (TMO) using switching and management infrastructure (SwMI) made of TETRA base stations (TBS). As well as allowing direct communications in situations where network coverage is not available, DMO also includes the possibility of using a sequence of one or more TETRA terminals as relays. This functionality is called DMO gateway (from DMO to TMO) or DMO repeater (from DMO to DMO). In emergency situations this feature allows direct communications underground or in areas of bad coverage.

In addition to voice and dispatch services, the TETRA system supports several types of data communication. Status messages and short data services (SDS) are provided over the system's main control channel, while packet-switched data or circuit-switched data communication uses specifically assigned channels.

TETRA provides for authentication of terminals towards infrastructure and vice versa. For protection against eavesdropping; air interface encryption and end-to-end encryption is available.

The common mode of operation is in a group calling mode in which a single button push will connect the user to the users in a selected call group and/or a dispatcher. It is also possible for the terminal to act as a one-to-one walkie talkie but without the normal range limitation since the call still uses the network. TETRA terminals can act as mobile phones (cell phones), with a full-duplex direct connection to other TETRA Users or the PSTN. Emergency buttons, provided on the terminals, enable the users to transmit emergency signals, to the dispatcher, overriding any other activity taking place at the same time.

The main advantages of TETRA over other technologies (such as GSM) are:

- The lower frequency used gives longer range, which in turn permits very high levels of geographic coverage with a smaller number of transmitters, thus cutting infrastructure costs.
- During a voice call, the communications are not interrupted when moving to another network site. This is a unique feature which dPMR anetworks typically provide a number of fall-back modes such as the ability for a base station to process local calls. So called 'mission critical' networks can be built with TETRA where all aspects are fail-safe/multiple-redundant.

- In the absence of a network mobiles/portables can use 'direct mode' whereby they share channels directly (walkie-talkie mode).
- Gateway mode - where a single mobile with connection to the network can act as a relay for other nearby mobiles that are out of range of the infrastructure.
- TETRA also provides a point-to-point function that traditional analogue emergency services radio systems did not provide. This enables users to have a one-to-one trunked 'radio' link between sets without the need for the direct involvement of a control room operator/dispatcher.
- Unlike cellular technologies, which connect one subscriber to one other subscriber (one-to-one), TETRA is built to do one-to-one, one-to-many and many-to-many. These operational modes are directly relevant to the public safety and professional users.
- TETRA supports both air-interface encryption and end-to-end encryption
- Rapid deployment (transportable) network solutions are available for disaster relief and temporary capacity provision.
- Equipment is available from many suppliers around the world, thus providing the benefits of interoperable competition.
- Network solutions are available in both the older circuit-switched (telephone like) architectures and flat, IP architectures with soft (software) switches.

The main disadvantages of TETRA are:

- Requires a linear amplifier to meet the stringent RF specifications that allow it to exist alongside other radio services.
- Data transfer is efficient and long range (many km), but slow by modern standards at 7.2 kbit/s per timeslot (3.5 kbit/slot net packet data throughput, noting that this rate is ostensibly faster than what DMR, DpMR, P25 are capable of), although the Tetra standard states that up to 4 timeslots can be combined into a single data channel to achieve higher rates whilst still fitting into a single 25 kHz bandwidth channel. Albeit there are no deployed networks where this data rate has reportedly been achieved from mobile users (hand portables or vehicle mobiles). Latest version of the standard supports 115.2 kbit/s in a 25kHz-channel or up to 691.2kbit/s in an expanded 150kHz-channel. But again, no deployed networks supporting such data rates are currently in operation. To overcome the limitations many software vendors have begun to consider hybrid solutions where TETRA is used for critical signaling while large data synchronization and transfer of images and video is done over 3G / LTE.

### 2.2.8 VIRVE

In Finland “Viranomaisverkko” (VIRVE) the governmental official radio network is based on the TETRA standard and is one of the few nation-wide networks in the world. The VIRVE network was created for the Finnish authorities to have their own nation-wide and secure radio network. The planning of the network began in the early 1990s, when analog authority networks were deemed to be expensive to keep up and the demands for authority communications had grown. In 1995 the Finnish government decided to invest €134 million for a new shared authority

network. Construction of the network began in 1998 and the network became nation-wide in 2002. Today there are over 60,000 users and about 1,300 base stations in the whole country.

The VIRVE technology has been developed by Nokia and the construction was overseen by the Ministry of Internal Affairs. The system uses the frequency band of 380-400 megahertz, which is lower than GSM. Due to the lower frequency band fewer base stations are needed. Digital VIRVE is encrypted, unlike its analog counterparts, and it has unified all previous authority networks into one network. The network makes it possible to transfer pictures and the same digital services as the GSM network. In addition, the network has a group call service that enables fast and efficient communication in a group of users. The expected number of clients in the network is 50,000. The power of the base stations is set to 25 watts, in vehicular devices it is 10 watts and in portable devices 0.5—3 watts.

The network is separated into groups that can be modified in according to the needs of the operation at hand. The network is used by security officials: the police, rescue services, customs, border guard, social- and health department and the Finnish Defense Forces. Authorities can also allow access to the network for other personnel separately for a limited amount of time, under contract or limited to certain events.

### 2.2.9 Summary on mobile networks

Large scale disasters cripple mobile networks by taking out individual base stations, power outages and breaking backbone communications between network building blocks. Older technology ( 2G, GPRS, TETRA ) are commonly the last to fail since base stations are scattered away. Damaged area can be covered by neighboring base stations since range is far greater than later technology. The TDMA modulation limits the GSM network maximum distance to 35 km and TETRA systems 58 km from base station to mobile. Such a high range is practically achievable with good RF and antenna design and finding optical locations. 3G and other later technologies have practical limits less than 10 km radius from base station since complex modulation is not optimized for far reaching solutions.

Base station power requirements rise as the data throughput and general capacity rises. During large scale power outage, the base stations are running on backup power. The backup capacity is ranging from few hours ( 3G, 4G, LTE ) to several days ( GSM, TETRA ). The local authorities may regulate the minimum uptime during power outages which help emergency communications, but these applications are primarily voice only. TETRA network operators normally have fast response support organizations who keep base stations running using all means of backup power.

Data communications during incidents are first to suffer. The last standing 3G, 4G, LTE networks are fully occupied by people trying to access network and probably only emergency calls can be relayed. Faster data streams could be utilized but it would require privileged access in subscription to allocate data bandwidth for rescue teams. Theoretically much slower data rate in 2G, GPRS and TETRA systems is far more reliable in practice and can be easily utilized by turning off 3G options in mobile devices.

Network operators like Rivada Networks (http://rivada.com/) can substitute whole fixed 2G, 3G and 4G networks with their portable systems. They have packed all necessary network components to a portable system, which can be rapidly deployed in emergency area to create Access to their subscribers.

### 2.2.10 References

[1] “Radiolinja's History". April 20th, 2004. Retrieved December 23rd 2009

[2] CDMA2000 1X". CDG.org. CDMA Development Group. Archived from the original on 25 July 2011. Retrieved July 31, 2011.

[3] “An Introduction to LTE". 3GPP LTE Encyclopedia. Retrieved December 3, 2010.

[4] "Newsroom Press Release". Itu.int. Retrieved 2012-10-28.

[5] http://www.3gpp.org/ITU-R-Confers-IMT-Advanced-4G

## 2.3 Other wireless technologies

### 2.3.1 Global perspective

Other wireless technologies are used in applications where sensors and actuators are required. The market is dominated by some solutions with several common features and differences.

Among their similarities, the most remarkable one is on the network layer which establishes the capacity of making a meshed network. It provides some properties such as path redundancy, error recovery capability, scalability and ease of installation. Given the importance of this characteristic, IEEE has set the standard 802.15.5 (Mesh Topology Capability in Wireless Personal Area Networks) but there are not available commercial implementations yet. However, this not a limitation as there are many scenarios in which it is not needed or even desirable to have a mesh network. In these cases using 802.11 (WiFi) or the new amendment 802.15.4e is recommended, both with a star topology.

The most commonly used range of frequencies for sensor and actuator networks is the 2.4GHz ISM band, but there are other variety of bands on which to transmit with certain limitations of transmission power and working cycles. For instance, for the IEEE 802.15.4g there are 14 different bands available:

| Parameter | Description |
|---|---|
| 169.400-169.475 | Europe |
| 450-470 | USA |

| Parameter | Description |
|---|---|
| 470-510 | China |
| 779-787 | China |
| 863-870 | Europe |
| 896-901 | USA |
| 901-902 | USA |
| 902-928 | USA |
| 917-923.5 | South Korea |
| 920-928 | Japan |
| 928-960 | USA |
| 950-958 | Japan |
| 1427-1518 | USA/Canada |
| 2400-2483.5 | Worldwide |

**Table 1: 802.15.4g-2012 possible frequency bands**

Each band also imposes restrictions such as maximum power that can be issued. The set of constraints is managed by different agencies such as the FCC, in the United States; the ECC of the CEPT in Europe; the SRRC in China There is also an international organization, the ITU, which provides a common framework that encourages to follow their recommendations.

There are three well-defined regions ITU. The first one corresponds to Europe, Middle East and Africa. Region 2 affects the entire American continent and Greenland. The third region applies to Asia (excluding Russia) and Australia. For example, in the region 1 the use of the 433MHz band as an ISM band is allowed and regulated by the ITU 5.150 and that defines part of spectrum as available for unlicensed citizens if the constraints (power, duty cycle ...) are satisfied. The greatest example of a global ISM band is located at a frequency between 2.4GHz and 2.5GHz (where great commercial technologies such as Wi-Fi or Bluetooth are located). The advantage of these bands is also its main drawback, as no license is required anyone can make use of it. In Europe, these bands are known as SRD.

Besides legal issues, it is need to consider the objectives of the application when selecting a technology. It should be noted that several technologies can be used for different layers of the protocol stack. Below wireless technologies with great potential for wireless instrumentation on the DiCoMa scenarios are presented.

### 2.3.2 Wi-Fi

#### Introduction

Wi-Fi is used as a generic term for products that incorporate any kind of the 802.11 wireless technologies, enabling wireless networking known as Wireless Local Area Networks. At the beginning, the term Wi-Fi was used only for devices with IEEE 802.11b technology, the dominant standard in the development of wireless networks. In order to avoid confusion in the compatibility of equipment and interoperability of networks, the term was extended to all appliances equipped with 802.11: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.

The following table shows the most important characteristics of the 802.11 standards.

| Parameter | Description |
|---|---|
| Frequency Band | IEEE 802.11b/g 2.4 GHz<br>IEEE 802.11a/h 5GHz |
| Maximum Rate | IEEE 802.11b 11 Mbps<br>IEEE 802.11a/h 54 Mbps<br>IEEE 802.11g 11/54 Mbps |
| Throughput | IEEE 802.11b 5.5 Mbps<br>IEEE 802.11a 30 Mbps |
| Number of Channels | IEEE 802.11b/g 3 non overlapped channels<br>IEEE 802.11a 12 non overlapped channels<br>IEEE 802.11h 19 non overlapped channels |

| Parameter | Description |
|---|---|
| Modulation | IEEE 802.11 DSSS, FHSS<br>IEEE 802.11b DSSS with CCK<br>IEEE 802.11a/h OFDM<br>IEEE 802.11g DSSS, OFDM |
| Topology | Point to point (PTP)<br>Point to Multipoint (PMP)<br>Mesh |
| Security | WEP/WPA<br>802.1x Protocols |
| Range | IEEE 802.11b 30-460 m<br>IEEE 802.11a 12-300 m |

**Table 2: Wi-Fi main characteristics**

- **802.11**. First of the standards defined by the IEEE for WLAN applications. It works on the 2.4 GHz ISM band and uses two types of modulation: DSSS and FHSS. Available transmission rate is assumed to be between 1 to 2 Mbps, depending on the manufacturer. This standard is virtually obsolete, due to the appearance of a series of variants that enhance not only the transfer rate, but also cover special security features and integration with wired networks.
- **802.11b**. This standard represents the evolution of the previous one. Basically, it differs in the exclusive use of the DSSS modulation with CCK coding system that runs only on this modulation. This allows you to offer up to 11 Mbps and transmission rates ranging of 1, 2, 5.5,and 11 Mbps, depending on different factors. This feature, called DRS, allows wireless network adapters to reduce speeds to compensate for possible reception problems that can appeared due to distance or obstacles found in the path. Other important features of this standard include support for three non-overlapping channels and perform low-power consumption, which makes it perfectly valid for the use in notebook PCs or PDAs.
- **802.11a**. Also named as "Wi-Fi5". It presents a fundamental difference which is theoperation over the 5 GHz frequency band using the OFDM radio modulation techniques. This modulation enables splitting a data high speed carrier into 52 low speed subcarriers which are transmitted in parallel. These subcarriers can be grouped in a much more integrated way with the same spectrum technique that is used by the 802.11b standard. 802.11a also allows up to eight channels in operation with no overlap, thereby increasing the capacity for simultaneous communications. The immediate consequence of this is a considerable increase in the transmission rate, reaching up to 54 Mbps to make it especially useful in environments with high bandwidth requirements. However,

this standard also has some disadvantages compared to 802.11b. Concretely, higher power consumption (which makes it less suitable for installation on laptops or PDAs) and the lack of compatibility with the 802.11b standard due to the frequency band change. Nevertheless, the latter problem has been resolved through access points that support both standards.

- **802.11g**. It is based on the 802.11b standard. More advanced than its predecessor, 802.11g works on the same frequency (2.4 GHz) and it is capable of using two modulation methods (DSSS and OFDM). By supporting both encodings, this new standard is able to significantly increase the transmission rate reaching up to 54 Mbps as 802.11a offers, while maintaining the characteristics of 802.11b in distance, power consumption and frequency. Thus, the major advantage of this new standard is the increased rate while maintaining full compatibility with the 802.11b standard. It allows the coexistence of both standards in the same installation.
- **802.11h**. An evolution of the IEEE 802.11a standard that allows dynamic channel allocation and automatic power control to minimize the effects of interference.
- **802.11n.** This new standard improves the previous one by adding MIMO antennas. Both the upstream and downstream operating in the 2.4GHz band, using the 5GHz band as downlink only. This standard is also known by the acronym WMM.
- **802.11ac**. It aims to be the next Wi-Fi standard. There is not much information about technical specifications. It will operate in the radio band below 6GHz and its design allows to reach transmission rates on wireless networks of about 1000 Mbps (1 Gigabit per second), which is an interesting increase from the current 802.11n rate of 600Mbps.

It is expected that future 802.11ac Wi-Fi standard will hit the market late next year, however it will be necessary to renew devices such as network cards, routers, laptops, mobile devices, internet connections. Thus, it will not be possible to take advantage of the standard until 2015.

## Architecture

Main components which require to be configured in a WLAN are detailed in the following list:

- User Terminals or Clients incorporating a Network Interface Card that includes a radio transceiver and an antenna.
- Access Points, which can send the information of the wired network, such as Ethernet, to users.
- APs Controllers. They become necessary for multiple APs deployments, either for reasons of coverage or traffic. This controller usually includes AP functionality, VPN client and RADIUS client for authentication and authorization tasks with appropriate AAA server, routing and firewall.

The core element of the 802.11 architecture is the cell. A cell can be defined as the geographic area in which a number of devices are interconnected wirelessly. In general, this cell consists on stations and a single access point. The stations are adapters that allow conversion of existing information at terminals or client equipment, and send/receive required data within the cell. This

information is generally encapsulated using the Ethernet protocol (IEEE 802.3). APs are network components that have the ability to control and manage all communication that occurs within a wireless LAN cell, between wireless LAN cells and finally between wireless LAN cells and other LAN technologies. The access points ensure optimum utilization of available transmission time on the wireless network. For all purposes, this is a link level bridge between devices. This configuration is called a Basic Service Group.

BSS is, therefore, an independent entity that can be linked with other BSS through an AP. This connection takes place via a Distribution System. The DS may be '*questioned'* (BSS communicates with an external network), 'wired' (with other BSS via cable, such as a conventional fixed Ethernet) or 'wireless'. In the latter case, the system is called Wireless Distribution System.

On this basic concept raises a number of alternative use and configuration ways:

- **Independent BSS**. A wireless cell without any distribution system and, therefore, unable to connect with other networks.
- **Ad-Hoc mode**. It is built like an IBSS variant where there is not any access point. The configuration can be seen in Figure 1. Coordination functions are randomly taken by one of the present stations. The data traffic takes place directly between the two involved devices, without having to resort to a higher-level of centralization. As a result maximum utilization of the communications channel is achieved. The coverage is determined by the maximum distance between two stations, which is significantly lower than the cases in which there is an access point. This is an unusual configuration because of the connotations of isolation that it entails. But it can be very useful when the existing traffic is distributed among all existing stations.

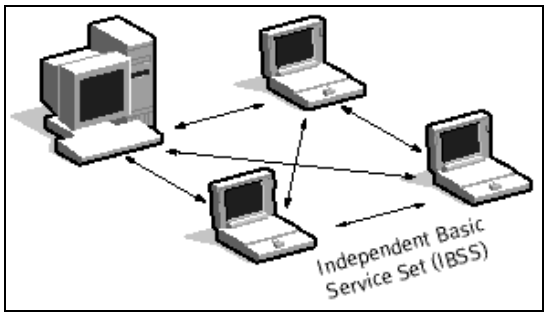


**Figure 1: Ad-Hoc mode configuration**

- **Infrastructure Mode**. The AP performs coordination function. All the traffic has to pass through it, so there is a clear loss of efficiency in the event that two stations within a BSS wish to communicate with each other (data packets are sent once to the access point and another time to the destination). This is an appropriate architecture when most of the traffic is originated or terminated in the external networks which the access point is connected to. The coverage is close to a distance twice of the maximum distance between the access point and station. This mode is the one that is commonly used to

connect a wireless network with Internet access networks (ADSL, ISDN, …) and local business networks. See Figure 2.

- **Extended BSS** (ESS). This is a specific case of infrastructure mode, represented by a set of associated BSS through a distribution system. This enables a number of advanced options such as roaming between cells.

To unambiguously identify each wireless cell, a unique network name is assigned. This name is a string of 32 characters maximum length, called SSID. One station could only be added to a cell if it has the same SSID into its internal configuration. If the station can connect to any wireless cell present, the parameter "ANY" must be used. Immediately, the equipment analyzes all cells that are present and it is connected to one of them taking their SSID. Generally, the selected cell is the one who has a higher signal level.

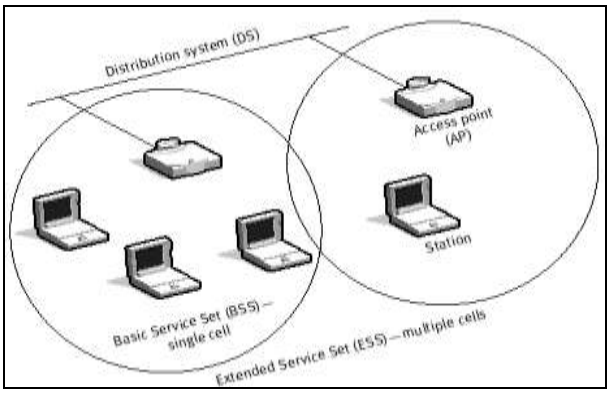


**Figure 2: Infrastructure mode configuration**

## Topology

IEEE 802.11 standard supports multiple topologies for networking. The resulting topology will be based on the design requirements and on the application that the network was oriented to.

A. Point to Point (PTP). On this configuration the communication is established between two devices only. These devices can be end WiFi or WAPs nodes. When long range is required, point to point networks utilize directional antennas.

B. Point to multipoint (PMP). This configuration is characterized by the existence of a device that provides multiple services to others who are around. Indoor wireless networks are usually PMP. The high-range wireless networks that serve multiple clients typically employ a single omnidirectional antenna or multiple antennas industry.

C. Mesh. With this configuration, each device can communicate with any other affordable node, i.e. any other device separate less than the maximum transmission range.

## Range

Distances to be covered by the IEEE 802.11 standards depend on applied rates, the number of connected users and the type of antennas and amplifiers that can be used. The following table shows some coverage data and maximum speed for 802.11b and 802.11a.

| Standard | 802.11b | | 802.11a | |
|---|---|---|---|---|
| Environment | Indoor | Outdoor | Indoor | Outdoor |
| Coverage | 30-90 m | 120-460 m | 12-90 m | 30-300 m |
| Rate | 11-1 Mbps | 11-1 Mbps | 54-6 Mbps | 54-6 Mbps |

**Table 3: WiFi coverage and transmission rate**

## Consumption

In general, WiFi power consumption is rather high when compared to other standards. This causes reduced battery life. Thus, it is not suitable for applications in which not frequent battery replacement can be performed.

## Security

Wireless access creates security issues. A misconfigured AP opens a backdoor that undermines the security of a network. It is very common to find networks in which Internet access is protected with a properly configured firewall, but into the network completely unprotected APs appear and they radiate outward from the building. As a consequence, anyone who picks up the AP signal can:

- Surf freely
- Use the network as an attack point against other networks.
- Steal information and software.
- Introduce malware and viruses.

In terms of security is required to: Confine radio waves as much as possible. This in a difficult task but a good job can be done using directional antennas and a proper setting of the transmitted power.

- Implement mechanisms for two-way authentication, which, on the one hand, allows the customer to verify that you are connecting to the right network and, on the other hand, allowing the network to see that the client is authorized to access it.
- Prevent computer from outside of the network to intercept data through passive listening by encryption.

Compliance with these requirements needs from the use of security methods. Most important 802.11 security methods are:

A. **SSID**. Also known as ESSID. It is not considered as a security method itself. One or more points are connected to a single wireless network constituting an ESS. The ESSID, which is nothing more than a string of 32 ASCII characters, identifies the AP and network clients.

B. **MAC addressing filtering**. It is an authentication process controlled by MAC. At each AP there is a table with the MAC addresses of clients that can connect to the AP. There is a unique MAC for each client. This mechanism is simple for small and home networks. but it has a problem of scalability; in addition, the format of the MAC is not very manageable. Another problem is that sniffers may intercept unencrypted MAC traveling by air.**WEP**. This mechanism was designed to protect the data that are transmitted over the air using encryption. 40-bit keys (128 optional) are accomplished. The client and the AP shared static keys. It is based on RC4 encryption algorithm. The 802.11 standard provides two schemes to define WEP keys:

   1. Four default keys shared by all users.
   2. Each customer establishes a mapping of keys to another station, which is safer but more complex.

   The features that infringe the WEP security protections are:

   - Use of static encryption keys, allowing an attacker to accumulate large amounts of text with the same key.
   - Manually keys changing.
   - Lack of mutual authentication service. Simply the client and the AP must share the key so that the communication can take place. Authentication is based on devices, instead of users.

To increase the reliability of the standard, there are other security mechanisms to implement out of the 802.11 standard:

A. **IEEE 802.1x protocol**. This standard offers:

   - Authentication and access control based on client/server architecture.
   - RADIUS. Mutual Authentication Server recommended as centralized management system for applications with a large number of users.
   - Dynamic WEP keys.
   - Port-based EAP authentication. Several types of EAP TLS, TTLS, PEAP, MD5, SPEKE and LEAP.

   This protocol involves three devices:

   1. The Supplicant or client computer, which wants to connect to the network.
   2. Authentication/authorization server, which contains all the needed information to know which computers or users are authorized to access to the network.
   3. Authenticator, which is the network equipment that receives the Supplicant connection. The authenticator acts as an intermediary between the supplicant and the authentication server and only allows access to the network when Supplicant Authentication Server authorizes.

   Client authentication is performed by EAP and RADIUS service. There are different variants of EAP as the authentication mode being used. You can talk about two variants: those that employ security certificates and those which use passwords.

B. **WPA.** This is the first part of the 802.11i standard. It was performed as a WEP substitute, improving data encryption and providing an authentication mechanism. It is being call for all products by Wi-Fi Certification Alliance. Gives user authentication via 802.1x and EAP. To solve the problem of data encryption, WPA proposes a new protocol encryption, TKIP. This protocol takes care of changing the shared key between the AP and the client from time to time to prevent attacks. The advantage is that you can activate with a simple software update.

C. **RSN**. (Robust Security Network). It represents the second part of the 802.11i standard. Also called WPA2, it is fully compatible with WPA adding more security to wireless networks. It uses a robust encryption algorithm: AES. The major disadvantage is the need to upgrade hardware equipment.

D. **VPN.** Virtual Private Networks employ encryption technologies to create a private virtual channel on a public scope network. The part of the network that handles wireless access must be isolated from the rest. For this, an access list on a router can be properly recorded, or group all wireless access ports in a VLAN (if switching is used). VPN servers are responsible for authenticate and authorize wireless clients and they encrypt all traffic from these customers.

### 2.3.3 WiMAX

#### Introduction

WiMAX (Worldwide Interoperability for Microwave Access) integrates the IEEE 802.16 family of standards and the Hyperman standard from the ETSI. WiMAX is a standard for wireless data transmission (802.MAN) that provides concurrent access in areas up to 50 kilometers in radius and speeds up to 70 Mbps using LMDS portable technology.

The main idea of WiMAX technology is as "last mile" and can be used to access links, MAN or WAN. The WiMAX standard has full capability as a technology carrier, on which you can carry IP, TDM, T1/E1, ATM, Frame Relay, and voice; making it perfectly suited for environments of large voice and data corporate networks, as well as for telecommunications operators forced to use wireless links as part of its backbone network. To meet this latter requirement is essential to have different levels of quality of service (QoS) as well as the use of different communication channels on the same physical radio link.

The main features of WiMAX are included in the following table.

| Parameter | Description |
|---|---|
| Frequency Band | IEEE 802.16a between 2-11 GHz (LOS)<br>IEEE 802.16b between 5-6 GHz<br>IEEE 802.16c between 10-66 GHz<br>IEEE 802.16e between 2-6 GHz (NLOS) |

| Parameter | Description |
|---|---|
| Maximum Rate | 75 Mbps |
| Channels Size | 5 and 10 MHz |
| Modulation | OFDM |
| Multiplex | FDM<br>TDM |
| Topology | Point to point (PTP)<br>Point to Multipoint (PMP) |
| Security | x.509 certificates<br>DES in CBC mode |
| Range | 50 Km (NLOS)<br>8-10 Km in high demographic density areas |

**Table 4: WiMAX main characteristics**

Listed below are the various standards that cause the creation of the WiMAX standard.

A. **802.16**. This is the initial standard. It applies to point-to-multipoint connections with directional antennas and without mobility. It is defined in the frequency band from 10 to 66 GHz and required LOS towers.

B. **802.16a**. This new version uses a narrower and lower spectrum band, 2-11 GHz. In this band there are frequencies that does not require operating license, the so-called "unlicensed frequency bands." Furthermore, as an added benefit, in this case it does not need LOS towers but only the deployment of base stations (BS) formed by antennas transmissor/receiver capable of serving about 200 subscriber stations (SS), which in turn can provide coverage and complete building service.

C. **802.16-2004**. Previous standards were unified in this new standard. Access technology converts voice signals and data to radio waves within said frequency band. It is based on OFDM and with 256 subcarriers it can cover an area of 50 kilometers allowing connection without line of sight, i.e., with obstacles placed. Furthermore, it has the capacity to transmit data at a rate up to 70 Mbps with a spectral efficiency of 5.0 bps/Hz and can support thousands of users and a channel scalability from 1.5 MHz to 20 MHz. This standard supports service levels (SLAs) and quality of service (QoS).

D. **802.16e**. Although official publication 802.16-2004 settled the basis for the initial deployment of the new technology access wireless broadband, WiMAX expectations go beyond being a wireless ADSL type system for urban and rural environments. Actually, the promoters of this project pursue the ambitious goal of WiMAX being the wireless technology that unifies the world of mobile telephony and data networks. With this aim was created IEEE 802.16e Working Group to improve and optimize the combination of support capabilities, both fixed and mobile communications, at frequencies below 6 GHz The new standard version introduces support for the technology SOFDMA (a variation of the OFDMA modulation technique), provides improved support for MIMO and AAS technology including improvements to optimize the power consumption for mobile devices.

802.16 x standards define a MAC layer specification supporting different physical layers (PHY). This feature is essential when devices can differentiate offers, while being interoperable, so they can adapt the system in a particular frequency band.

## Architecture

BWA systems typically include base stations (BS), subscriber stations (SS), terminal equipment (TE), relay stations (RS), links between cells and other equipment. A BWA system contains at least one BS and a number of SS units.

A WiMAX system normally has two parts:

A. On the one side the WiMAX towers are found, which provide coverage of up to 8,000 $km^2$ depending on the type of transmitted signal.

B. On the other side the receivers are found, i.e., electronic cards that connect to any PC, laptop or PDA in order to network accessing.

The next figure shows an example of WiMAX network.

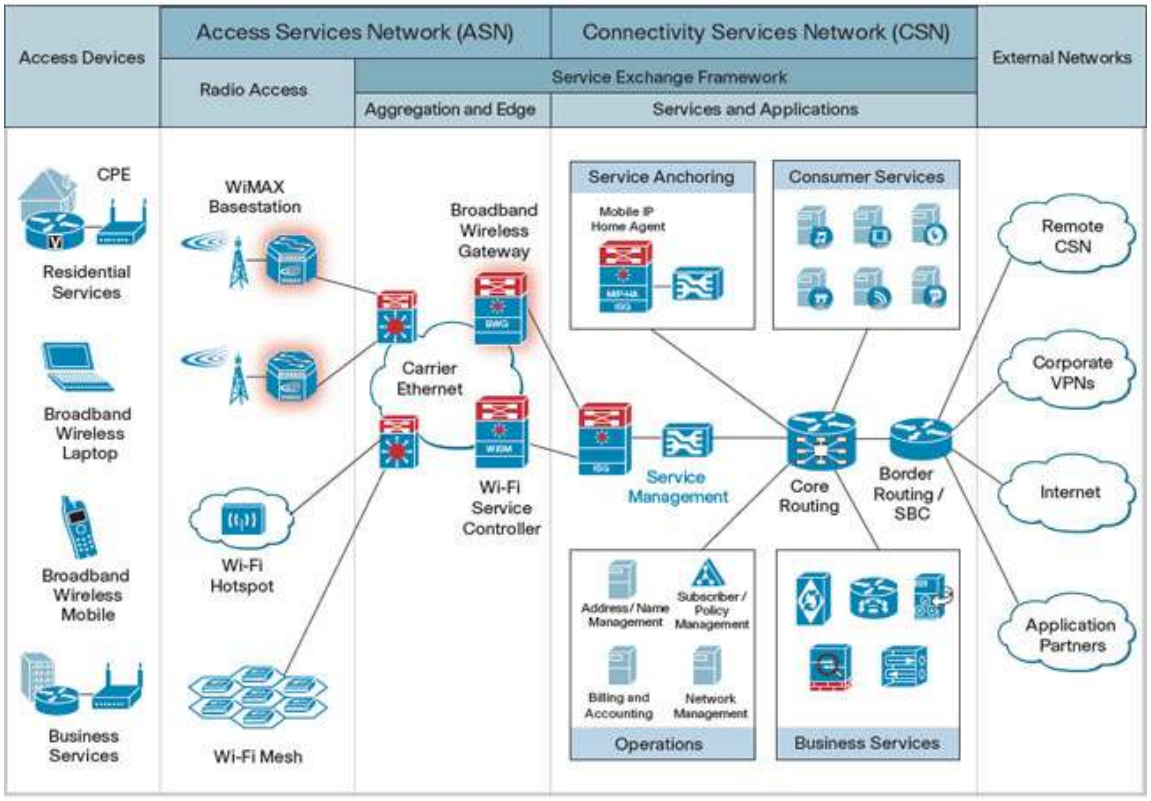


**Figure 3: WiMAX deployment example**

WiMAX Metropolitan Area Networks (MAN) are configured into cellular mode and generally they consist on a cell or group of cells, each of which contains multiple handsets (also called subscriber units or CPE). In turn, each cell comprises one or more unit access devices (base stations) that are normally connected to the network backbone with the purpose of managing all traffic within the area covered and the backbone. The terminals within the coverage area of an access unit are connected to the backbone network via the access unit. All terminals that are associated with a base station are synchronized, both in frequency and time and they use a rigorous protocol to communicate with the access unit. The same rule applies for an interception device. For data to be intercepted, wireless equipment should be employed and synchronized within the area covered by the access unit.

## Topology

There are two key WiMAX topologies:

A. Point to point for backhaul.

B. Point-to-multipoint, between the base station and clients.

In any of these situations MIMO antennas may be used. The image shows a point to point link between two base stations and point-to-multipoint link between the base station and many subscriber stations.

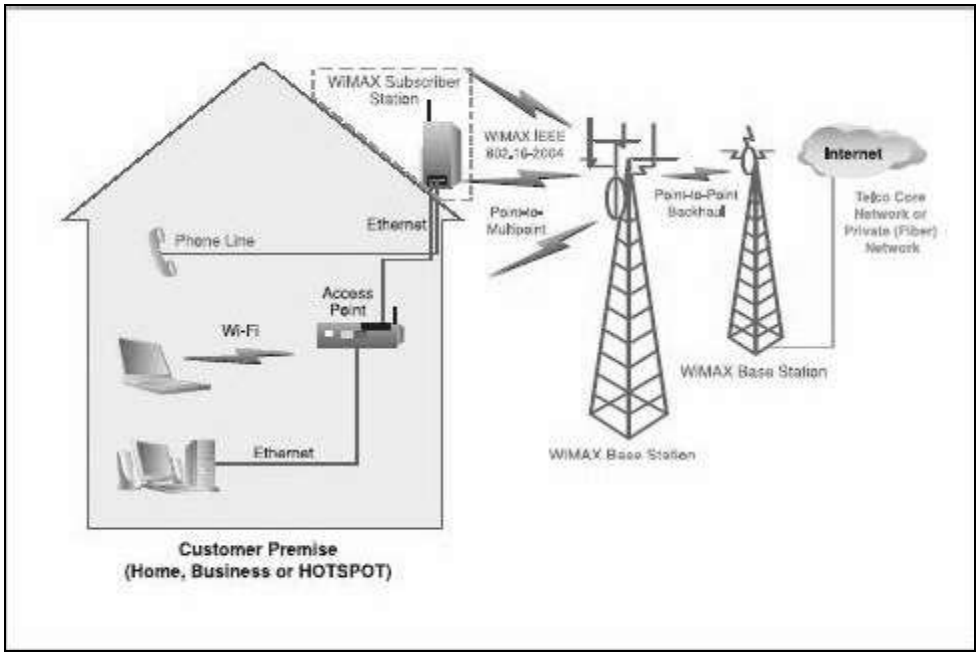


**Figure 4: WiMAX network topology**

## Range

Table 4 shows typical cell sizes and the performance at the frequency of 3.5 GHz in different environments and configurations.

| Environment | Cell size | Performance |
|---|---|---|
| Urban indoor (NLOS) | 1 km | 21 Mbps with channels of 10 MHz |
| Suburban indoor (NLOS) | 2.5 km | 22 Mbps with channels of 10 MHz |
| Suburban outdoor (NLOS) | 7 km | 22 Mbps with channels of 10 MHz |
| Rural indoor (NLOS) | 5 km | 4.5 Mbps with channels of 3.5 MHz |
| Rural outdoor (NLOS) | 15 km | 4.5 Mbps with channels of 3.5 MHz |

**Table 5: Performance and cell size for a WiMAX network**

### Consumption

One of the main disadvantages of WIMAX technology is energy consumption, which is so high that his receivers cannot be used in consumer products such as laptops or mobile phones.

### Security

WiMAX offers strong security with certificate-based encryption. Safety features are independent of the type of operator (ILEC or CLEC) and the topology of the access network. In this sense, the standard addresses the four main areas to be considered regarding safety:

A. Prevention of illegal use of the wireless connection.

B. Denial of services to stolen or fraudulently used units.

C. Provision of services only to specific end users.

D. Secure Access Management Compliance.

Regarding how to prevent illegal use of the wireless connection, the key is encryption. WiMAX security supports two encryption standards for quality, DES3 and AES. Basically, all traffic in WiMAX networks must be encrypted using the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) which uses AES for secure transmission and authentication of data integration. End-to-end authentication methodology PKM-EAP (Extensible Authentication Protocol) is used in accordance with the TLS public key encryption standard.

The standard defines a dedicated security process for beginners at the base station. Similarly, there are some minimum requirements for traffic encryption and for end-to-end authentication (the latter which is adapted from the interface specification data service over cable, DOCSIS BPI, and security protocol).

Relating to service provision to end users only specific authentication (based on X.509 digital certificates) is included in the access to the media control layer. The authentication system gives each user its own 802.16 certificate, plus one for the manufacturer, allowing the base station to authorize the end user. The privacy of the connection is implemented as part of another MAC sub-layer, the privacy layer. This protocol is based on Privacy Key Management, which is part of the DOCSIS BPI specification.

## 2.3.4 IEEE 802.15.4

### Introduction

IEEE 802.15.4 protocol corresponds to the bottom two layers of a variety of protocols that are mentioned in the document. The main features are described in the following table.

| Parameter | Description |
|---|---|
| Frequency Band and Maximum Rates | 868 MHz: 20Kb/s<br>915 MHz: 40 Kb/s |

| Parameter | Description |
|---|---|
| | 2.4 GHz: 250 Kb/s |
| Range | 10-1000 m |
| Number of Channels | 868/915 MHz: 11 channels<br>2.4 GHz: 16 channels |
| Latency | Less than 15 ms |
| Addressing Mode | 64 bits IEEE addressing |
| Security | 128 AES |
| Access Channel | CSMA-CA |
| Network Size | Up to $2^{64}$ devices |
| Temperature | -40º a -85º C |

**Table 6: IEEE 802.15.4 main characteristics**

In 2000 two groups specialize in standards (Zigbee and IEEE 802 working group) came together to raise awareness of the need for a new standard for low-power wireless networks and low cost home automation and industrial applications, resulting in a new standard for personal area (LR-WPAN) which is now known as 802.15.4. As happened with IEEE 802.11, which inherited the generic name of WiFi, 802.15.4 is sometimes confused with ZigBee although the latter defines the application stack that works on the physical layer and data link that really is IEEE 802.15 .4.

The 802.15.4 physical layer at 2.4 GHz employs a semi-orthogonal modulation technique, where each symbol is represented by one of the 16 PN code semi-orthogonal transmission sequences. This modulation method is very efficient providing low SNR and SIR (signal/interference ratio) in cases where the bandwidth of the signal is significantly higher than the rate. With a low cost receiver can get a PER of 1%, with values of PN code about 5-6 dB.

The 802.15.4 standard has been expanded with corrections such as 802.15.4g, initially oriented to the expansion of smart meters in Smart Grid. To do this, it uses the typical frequencies below 2.4GHz. This opens the possibilities for a lot of scenarios and regulatory standards in different countries and regions.

## Protocols based on 802.15.4

### 1. Wireless HART

Wireless-HART is an open standard for wireless networks developed by the HART Communication Foundation. It is based on 802.15.4 but adds a new data, network, transport and application layers. Moreover, it operates in the ISM band (Industrial, Scientific and Medic) 2.4GHz using a synchronous clock, auto-organization and self-regeneration of the mesh architecture. Another important feature is the use of a spread spectrum modulation (DSSS) and frequency jumps based on packet by packet sending.

As specific features include:

- Reliability: even in the presence of interference thanks to the performance of a mesh network and channel hopping synchronization messages.
- Security and privacy: in terms of network communications through encryption, verification, authentication and key management; and other open standards of the industrial field.
- Energy management: effectively by Smart Data Publishing (Intelligent Data Transmission) and other techniques that make batteries, solar and other low-power options being practical for wireless devices.

W-HART is mainly used in industrial automation and it is compatible with the rest of the current HART technology.

### 2. ISA 100.11A

The International Society of Automation approved in 2009 a new communication standard called ISA-100.11a - Wireless Systems for Industrial Automation: Control Process and Related Applications. ISA-100.11a is intended to provide a reliable and secure wireless operation for non-critical monitoring; alerting; supervision, open-loop or closed-loop control applications.

According to ISA, the standard defines the specifications of the protocol suite, system management, the gateway and security specifications for wireless communication with low data rate. Communications should be fixed, portable or mobile supporting different requirements consumption.

ISA-100.11a supports monitoring and control of processes where latencies in the order of 100 ms can be tolerated, with normal behavior of lower latency.

To meet the needs of industrial users and wireless carriers, the ISA-100.11a standard provides robustness in the presence of interference in industrial environments and with legacy devices are not compatible with the standard.

The ISA-100 is a steering committee making wireless devices and control systems in areas including:

- Environments where wireless technology is implemented.

- Technology and life cycle for wireless equipment and systems.
- The application of the wireless technology itself.

### 3. 6LowPAN

6LoWPAN is the name of a working group of the Internet Engineering Task Force (IETF), which defines the necessary mechanisms to networking IPv6 over IEEE 802.15.4 networks. Three main features of 6LowPAN are:

- Header compression.
- Fragmentation.
- Forwarding of Layer 2 IPv6 datagrams.

Defined methods are used for compression and encapsulation mechanisms that enable sending and receiving header IPv6 packets through these networks.

6LoWPAN defines HC1, a compression scheme optimized for IPv6 communication. Compressing the maximum, with HC1 the IPv6 header can be reduced of 40 bytes to 2 bytes. Regarding the transport layer, there is a bit in HC1 to indicate compression is applied on this layer. As it can be seen, 6LoWPAN removes many "overhead" aspects of IPv6.

Finally, we must mention that IP routing is traditionally carried out in the network layer, regardless of the lower layers. 6LoWPAN, for his role of adaptation layer, can support routing at the link layer and at the network layer. 6LoWPAN play an important role for the future of sensor networks, because of its high compatibility with current Internet infrastructure, allowing the connection of these networks with other IP networks. Connectivity to other IP networks can be provided by any arbitrary link (e.g. Wi-Fi, Ethernet, GPRS, etc.)

## 2.3.5 Bluetooth

### Introduction

Bluetooth wireless technology is a short-range communication system, which aims to eliminate the connections between electronic devices, both portable and fixed, while maintaining high levels of security. The main features of this technology are reliability, low power consumption and low cost. Bluetooth specification sets a standard organization to allow a wide range of devices to connect and communicate between them. One of the main advantages of Bluetooth wireless technology is its ability to simultaneously manage both voice transmissions and data. This allows users to enjoy a variety of innovative solutions such as the use of hands free to handle calls, printing features and face, or synchronization between PDA applications, computers and phones, among many others. Unlike other wireless standards, the Bluetooth specification gives definitions development companies for the link and application layers, allowing that voice and data support solutions.

Bluetooth technology includes hardware, software and interoperability requirements, so that their development has required the participation of the leading manufacturers in the sectors of telecommunications and computing, such as Ericsson, Nokia, Motorola, Toshiba, IBM and Intel.

This group of companies founded in 1999 the Bluetooth SIG. Subsequently there have been incorporating many more companies, and is expected to do so soon also companies in sectors as diverse as industrial automation, machinery, leisure and entertainment, toy manufacturers and appliances. Bluetooth operates in an ISM unlicensed frequency band and specifically falls between 2.4 and 2.485 GHz. It also uses a spread spectrum frequency hopping to a rated speed of 1600 hops/second. The 2.4 GHz ISM band is available in almost all countries, usually requiring no license.

The SIG has developed all Bluetooth standards from the initial version 1.0 to the latest version 2.0. Today GIS is composed around 6000 companies worldwide.

| Parameter | Description |
|---|---|
| Frequency Band | 2.4 GHz |
| Maximum Rate | Version 1.1: 723.1 Kbps (up to 57.6 Kbps downward)<br>433.9 Kbps symmetric<br>Versión 1.2: 1 Mbps<br>Versión 2.0 + EDR: 2.1 – 3 Mbps |
| Network Size | 8 devices by piconets and up to 10 piconets |
| Number of Channels | 3 channels by piconet for voice<br>7 channels by piconet for data |
| Modulation | GFSK |
| Topology | Point to point (PTP)<br>Point to Multipoint (PMP)<br>Scatternet |
| Security | Base band: Salto de frecuencia (FHSS)<br>Link layer: 128 bits authentication, authorization<br>Data encryption between 8 and 128 bits (SAFER+) |
| Range | Class 1: 100m<br>Class 2: 10m<br>Class 3: 1- 3m |

**Table 7: Bluetooth main characteristics**

## Topology

Bluetooth wireless links are formed in the context of a piconet. A piconet comprises two or more devices that take the same physical channel, so that they are synchronized with the same clock and hopping sequence. The clock used in the piconet is set on one of the devices that comprise the so-called master device. Regarding the hopping sequence, it is derived from the clock and the address of the device is the master's one. All other paired devices are called slaves.

Bluetooth provides point-to-point and point-to-multipoint, so that two or more devices share the same physical channel form a piconet. Slave devices can only communicate with the master and cannot talk to the other slaves belonging to the piconet. The maximum number of units that can actively participate in a simple piconet is eight, one master and seven slaves. Many more devices can remain connected to the parked state. These devices are not active in the channel (no MAC address assigned) but remain synchronized to the master and can become active without making the connection establishment procedure.

Teams that share the same channel can only use a portion of its capacity. Although channels have a bandwidth of 1MHz, the more users join the piconet, the less capacity, reaching about 10 kbit/s. A solution was adopted to solve this problem, borning the concept of scatternet. In Figure 3 possible network topologies are found.

In one area may be several piconets, each of which has a different physical channel, that is, independent master device, clock and hopping sequence.

A Bluetooth device can be simultaneously used in two or more piconets by time division multiplexing. However, this device does not ever act as a master in more than one piconet. This is because the piconet is synchronized with the master clock. Instead, the device itself can act as a slave in several piconets. When a Bluetooth device is participating in two or more piconets, it becomes part of what is known as a scatternet. This does not necessarily mean that the device has network routing functions. The basic protocols of Bluetooth have not been developed to provide such functions, since they depend on higher layer protocols and are not reflected in the Bluetooth specifications.

Performance, collectively and individually, to the users of a scatternet is greater than each user when participating in a channel of 1 MHz. In addition, statistically multiplexing gains are obtained and rejection of hopping channels. Because each piconet has individually a different frequency hopping, different piconets may use different hopping channels simultaneously.

It should be borne in mind that the more piconets are added to the scatternet, the higher probability of collision and the lower FHSS system performance are gathered. However, on the multiple piconets configuration the performance is higher than on a simple piconet design.

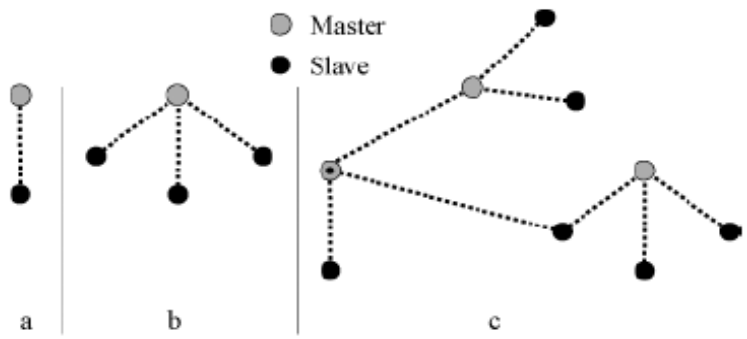


**Figure 5: Bluetooth topologies a) PTP. b) PMP. c) Scatternet**

## Range

In Bluetooth technology there are three types of devices depending on the involved transmission power level. The following table shows the maximum, rated and minimum value for each defined class.

| Class | Maximum output power ($P_{max}$) | Rated output power | Minimum output power ($P_{min}$) |
|---|---|---|---|
| 1 | 100 mW (20dBm) | N/A | 1mW (0 dBm) |
| 2 | 2.5 mW (4 dBm) | 1mW (0dBm) | 0.25 mW (-6dBm) |
| 3 | 1 mW (0 dBm) | N/A | N/A |

**Table 8: Classes of Bluetooth devices regarding the transmission power level**

The range depends on the device class. Class 1 devices are mainly used in the industry and achieve a range of 100 meters, Class 2 devices are common in portable devices and have a range of 10 meters and Class 3 devices usually have a range between 1 and 3 meters.

## Consumption

Bluetooth provides different ways in which the devices remain "asleep" to reduce consumption (extend battery life) and to release the piconet allowing other devices to access it. These modes include the hold mode, sniff mode and park mode.

*Hold mode* is a temporary mode which devices come when there is no need to send information over a relatively long time. In this mode, the transceiver is turned off to reduce power consumption. This mode is used to free the devices in their communication with the master. This allows devices to "sleep" for short periods of time, releasing the piconet to do other functions, e.g., discover new devices.

*Sniff mode* is a mode in which the devices listen to specific commands occurring periodically. This mode is used by devices that must remain continuously in contact with the master. This mode is used to reduce the consumption of the transceiver devices putting them in standby mode between periods of listening.

*Park mode* is a process in which a device is deactivated temporarily releasing direction (probably it will be reassigned to another device). When the teacher puts a slave in park mode, it wakes up periodically and looks for a sync signal from the master. If the sync signal contains the address of the device in park mode, the device wakes up and returns to join the piconet.

## Data rate

In the Bluetooth specification two kinds of links with different supported rates are defined, even allowing multimedia applications:

**Synchronous connection oriented (SCO)** link for voice and audio. Data rate defined in the Bluetooth specification is 1 Mbps, however, in an SCO link supports up to three 64Kbps channels per device.

**Asynchronous connectionless link (ACL)**. ACL links support symmetric or asymmetric point to point, used in data transmissions. The maximum speed for transmissions in asymmetric ACL link is 721 Kbps in one direction and 57.6 Kbps in the other. In a symmetrical communication is 433.9 Kbps.

### Frequency hopping

Bluetooth operates in the unlicensed 2.4 GHz ISM band. In order to avoid interference with other technologies operating in the same frequency band, Bluetooth uses the technique of frequency hopping (FHSS) which involves splitting the band into 79 channels (23 in Spain, France and Japan) with a length of 1 MHz and making 1600 hops per second. During the process of establishing the connection in a piconet, the master device generates a table with the pseudorandom frequency hopping sequence or pattern to be used during communications by the devices belonging to the piconet. The exchange of the jump table from the master to the slave (or slaves) is performed on a given channel from the frequency spectrum.

## 2.3.6 References

The main references are the standardization documents generated by the IEEE organism. WiFi has been defined by the "IEEE 802.11: Wireless Local Area Networks Working Group". It has made the following publications:

[1] IEEE 802.11, 1999 Edition (ISO/IEC 8802-11: 1999) IEEE Standards for Information Technology -- Telecommunications and Information Exchange between Systems -- Local and Metropolitan Area Network -- Specific Requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[2] IEEE 802.11**a**-1999 (8802-11:1999/Amd 1:2000(E)), IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Amendment 1: High-speed Physical Layer in the 5 GHz band.

[3] IEEE 802.11b-1999 Supplement to 802.11-1999, Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band.

[4] IEEE 802.11b-1999/Cor1-2001, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Amendment 2: Higher-speed Physical Layer (PHY) extension in the 2.4 GHz band—Corrigendum.

[5] IEEE 802.11d-2001, Amendment to IEEE 802.11-1999, (ISO/IEC 8802-11) Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Operation in Additional Regulartory Domains.

[6] IEEE 802.11f-2003 IEEE Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation.

[7] IEEE 802.11g-2003 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band.

[8] IEEE 802.11h-2003 IEEE Standard for Information technology—Telecommunications and Information Exchange Between Systems—LAN/MAN Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Spectrum and Transmit Power Management Extensions in the 5GHz band in Europe.

The “IEEE 802.15: Wireless Personal Area Networks Working Group” has standardized Bluetooth and 802.15.4 with these publications:

[9] IEEE 802.15.1(tm)-2002,IEEE Standard for Information technology--Telecommunications and information exchange between systems-- Local and metropolitan area networks--Specific requirements Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs(tm))

[10] IEEE 802.15.2-2003 IEEE Recommended Practice for Telecommunications and Information exchange between systems – Local and metropolitan area networks Specific Requirements - Part 15.2: Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Band

[11] IEEE 802.15.3-2003 IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPAN)

[12] IEEE 802.15.4-2003 IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks-- Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs).

Finally, WiMAX protocol has been presented by the “IEEE 802.16: Broadband Wireless Metropolitan Area Networks Working Group”:

[13] IEEE 802.16-2001 IEEE Standard for Local and Metropolitan Area Networks--Part 16 -- Air Interface for Fixed Broadband Wireless Access Systems

[14] IEEE 802.16a-2003 IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems--Amendment 2: Medium Access Control Modifications and Additional Physical Layer Specifications for 2-11 GHz

[15] IEEE 802.16c-2002 IEEE Standard for Local and metropolitan area networks--Part 16: Air Interface for Fixed Broadband Wireless Access Systems--Amendment 1: Detailed System Profiles for 10-66 GHz

[16] IEEE 802.16Conformance01-2003 IEEE Standard for Conformance to IEEE 802.16 Part 1: Protocol Implementation Conformance Statement (PICS) Proforma for 10-66 GHz WirelessMAN-SC Air Interface

[17] IEEE Std 802.16.2(tm)-2001 IEEE Recommended Practice for Local and metropolitan area networks Coexistence of Fixed Broadband Wireless Access Systems.

# 2.4 Coexistence

## 2.4.1 802.15.4 coexistence

The IEEE 802.15.4 standard provides several mechanisms to improve coexistence with other wireless devices operating in the 2.4 GHz ISM band. Firstly, the 802.15.4 specification augments the opportunities for smooth coexistence by dividing the band into 16 non-overlapping channels, which are 2-MHz wide and 5-MHz apart. As shown in Figure 3, four of these channels (15, 16, 21, 22) fall between the often-used and non-overlapping 802.11b/g channels (1, 7, 13).

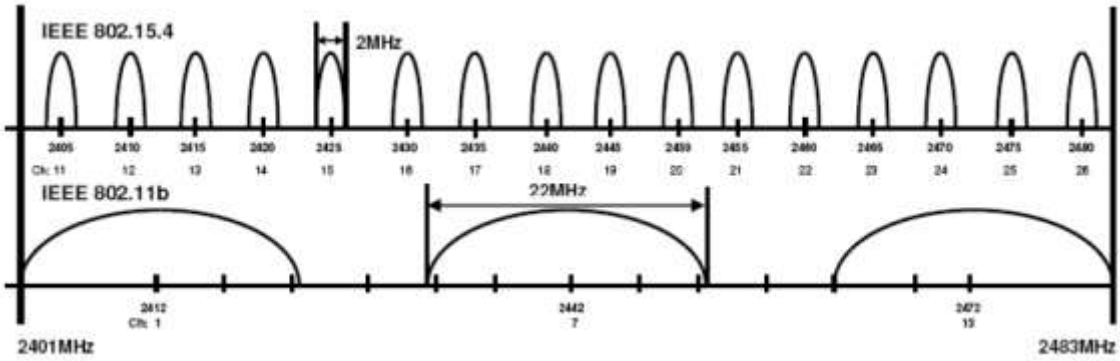


**Figure 6: IEEE 802.15.4 and IEEE 802.11b/g 2.4 GHz interference**

Another way to minimize the risk of interference is to reduce channel occupancy and the IEEE 802.15.4 PHY layer provides the ability to sample a channel, measure the energy and report whether the channel is free from interference and thus clear to transmit. Even with the techniques described above, a 802.15.4 device may find itself sharing a channel with interferers. The IEEE 802.15.4 standard makes use of a simple “listen before talk” strategy, also known as CSMA, and implemented in other wireless technologies such as WiFi. In this approach, a device that discovers that the channel is busy will wait a while before checking the channel again and transmitting its data. If the channel remains busy for a long while the device will change dynamically to another channel. It is called clear channel assessment (CCA).

Regarding coexistence issues between IEEE 802.15.4 and WiFi, the following conclusions can be considered:

- In presence of today’s real WiFi applications (web surfing, file transfer, audio and video streaming), 802.15.4 operates satisfactorily, even in the most adverse interference conditions. Although 802.15.4 packets are delivered successfully, they can experience an increased latency due to a higher number of retransmissions. In real environments, WiFi interference is not an issue for 802.15.4 applications.
- When increasing WiFi’s duty cycle and power level above what is achievable or available today (by arbitrarily increasing the channel occupancy), coexistence properties of ZigBee can be affected and packets can be lost. This is true in particular in IEEE 802.11b mode since interfering packets spend more time on air.

- These results confirm that although ZigBee/WiFi coexistence has theoretical limits that have been highlighted in many laboratory experiments, those limits are not reached today given real traffic conditions, hardware limitations or nominal power levels of commercial WiFi equipments.

Same results arise when using simultaneously IEEE 802.15.4 and WiMAX technologies.

Regarding coexistence issues between IEEE 802.15.4 and Bluetooth, the following conclusions can be considered:

- Bluetooth interference is less of an issue. The packet retry mechanism employed by IEEE 802.15.4 ensures re-transmission of packets corrupted by Bluetooth interference. Bluetooth may interfere with a first transmission attempt, but will usually have hopped to a different part of the spectrum for the retry.
- To achieve satisfactory IEEE 802.15.4 performance in the presence of Bluetooth interference, a separation distance of 2 m is recommended.

Further details on the Co-existence of 802.15.4 with other IEEE standards can be found in Annex E of the IEEE 802.15.4-2003 standard.

# 3 Communication requirements

## 3.1 Introduction

As stated in previous deliverables of the project. The DiCoMa system must support multiple alternative communications methods which can be changed and configured during run time. The basis for this requirement is that in disaster situations, some communication networks might not work. Additionally, information and communication must be secured and information security and identity security standards must be followed. On the other hand, all units must be able to communicate with each other. Thus, management centers must be able to establish voice connection to mobile units.

## 3.2 Chemical disaster

### 3.2.1 Chemical disaster communication requirements

Communication requirements in the chemical disaster are addressed towards WSANs (Wireless Sensor Actuator Networks) that are collecting the required information to be sent to DiCoMa Decision Support System (DDSS). The access network technologies to be utilized rely on the interfaces that are available on the crisis area. Possible technologies are listed in sections 2.2 and 2.3.

**Interoperable communication in WSANs**

Chemical disasters are time critical situations where decisions are made ad hoc. Once sensors are deployed and data is gathered, they have to be made available in real-time to the Dicoma system in section 3.1.

Today, there is a large variety of different sensor types and sensor manufacturers accompanying their equipment with different protocols. Hence, the biggest problems arise when the sensors have to be integrated and made as an interoperable sensor infrastructure. Many companies have their own proprietary solutions but nowadays also several open platforms are being developed in a standardized way, and widely used especially in research projects:

- Sensor Web Enablement (SWE) has resulted in a mature and robust suite of OGC (Open Geospatial Consortium) standards related to describing, tasking, and accessing network accessible sensors in a standardized way [1].
- ITA sensor fabric (IBM) is a middleware infrastructure developed as a part of International Technology Alliance in Network and Information Science that provides unified access and management of sensor networks [2]. SIXTH is a open source Java-based solution for the Sensor Web that promotes modularity, extensibility, scalability, reusability, and heterogeneity. The goal of SIXTH is to support the rapid development of a diverse range of Sensor Web applications. The framework itself is built on the Open Service Gateway

initiative (OSGi) component framework that has been developed by IBM in conjunction with numerous industry and academic partners [3].

- Open SensorWeb Architecture (OSWA) implements standards compliant platform and middleware (SWE in the core middleware) for integration of sensor networks with emerging distributed computing platforms such as Grids. It confirms to Web Services standard defined by the World-Wide Web and SensorML (Sensor Model Language) standard defined by the OGC [4].
- LinkSmart (HYDRA) is a middleware for heterogeneous physical devices in a distributed architecture. LinkSmart enables diversity of devices to be detectable and usable from a LinkSmart application. This overcomes the common problem of incompatibility between proprietary protocols and devices [5].

The management of a chemical disaster requires many authority groups to communicate and work together and making decisions coherently. Effective response, decision making and relief to large-scale disasters requires that a common operational picture (COP) is formed and managed so that all participants can rapidly assess the available information.

To achieve these goals, different emergency authorities use different types of sensors suitable for monitoring and collecting information about people, objects and the environment. They can react to the sensor information automatically utilizing the actuators that act on devices – to turn them off, adjust them or maneuver them.

### 3.2.2 Chemical disaster management protocols

Amount of required sensors in WSAN(s) is determined through intensive installation and validation process. Environmental/Thermal/Chemical models have to be done by the means of sensor characteristics, data gathering methods and the communication structure. Per each sensor the main accuracy values, range and measurement intervals have to be listed and validated. Some of the sensor devices can be very constrained utilizing WSN radio technologies whereas other equipment might also have cellular networking capabilities and more CPU and memory. The devices are assumed to have an IP connectivity provided by 6LoWPAN or Zigbee.

All measurements are collected to a Central Command, Control and Communications gateway (C4) which can be situated in a Leading Emergency Vehicle with the on-board unit that will act as an incident commander. The sensors and actuators can be linked to the gateway utilizing e.g. CoAP (Constrained Application Protocol) via LAN or local wireless connection. CoAP meets the specialized requirements of constrained environments such as low overhead, simplicity, and ability to deal with sleeping nodes.

Part of the sensors, such as weather related information, can be observed and gathered in a weather station installed also in the Leading Emergency Vehicle. On-board unit can communicate with the units that emergency personnel have, and communicate with the main DiCoMa Decision Support System (DDSS) in the Reception Center.

## 3.3 Storm disaster

### 3.3.1 Storm disaster communication requirements

Storm disaster scenario focuses on a storm disaster occurring in Northern Finland, where the road and telecommunications network is not very dense, and thus posing stringent requirements for the communications. Traffic and transportation are many times one of the parties that suffer the most of bad weather conditions. Therefore, monitoring the road and weather conditions and managing the incident warnings is a critical part of the disaster management related to stormy weather. Communication entities consist of Road Side Unit(s) (RSU), Linking Point(s) and Service Core(s). Vehicles receive real-time service data from the vehicle sensors and systems, and also by exchanging observation data with other vehicles. Roadside units deliver this data to the linking point using alternative available connections (IEEE 802.11p, GPRS, 2G, 3G, LTE) to update the service core's data bases and disseminate the critical data among authorities. By combining different information sources e.g. geo-sensors and RSUs information, it is expected to reach the most effective response for decision makers of severe incidents.

The architectural model of the storm disaster communications shall achieve an automated on-the-fly integration of different kind of sensors as presented in Dicoma system in section 3.1.

### 3.3.2 Storm disaster management protocols

Management protocols in a storm disaster are solving the problems related to organization of the sensor nodes, collecting information about the phenomenon and routing via neighboring nodes to the sink. The gateway node can be mobile such as the leading emergency vehicle or static with an ability to connect sensor networks to the outer existing communication infrastructure. Also security management issues are really important in the data transferring chain from the sensors all the way to DDSS.

Resource management and routing in sensor networks is closely related to architectural model issues [6]:

1.) Updating routing tables in a common fashion in a dynamic environment leads to heavy overhead in terms of time, memory and energy.

2.) Sensor nodes in WSANs send data to the sink based on a multiple hop routing composed by distributed networking and control functions compared to the traditional communications in cellular networks.

3.) Need to design proper routing protocols to improve energy efficiency and bandwidth utilization e.g. to eliminate data redundancy.

4.) Resource management protocols have to consider constraints of sensor nodes in terms of their transmission power, residual energy, processing and storage capacity.

### 3.3.3 References

[1] A. Bröring, E. H. Jürrens, S. Jirka, and C. Stasch. Development of Sensor Web Applications with Open Source Software. In First Open Source GIS UK Conference (OSGIS 2009), 22 June 2009,Nottingham, UK, 2009.

[2] Bergamaschi, F.; Conway-Jones, D.; Gibson, C.; Stanford-Clark, A. Policy enabled ITA sensor fabric a distributed framework for the validation of experimental algorithms using real and simulated sensors. In *Proceedings of IEEE Workshop on Policies for Distributed Systems and Networks*, Palisades, NY, USA, 2–4 June 2008.

[3] O'Hare, G. M. P. (Greg M. P.); Muldoon, Conor; O'Grady,Michael J.; Collier, Rem; Murdoch, Olga; Carr, Dominic. Sensor Web Interaction, International Journal on Artificial Intelligence Tools, 21 (2).

[4] Chu X, Kobialka T, Durnota B, Buyya R (2006) Open sensor web architecture: core services. In: Proc of the 4th Int. Conf. on Intelligent Sensing and Information Processing (ICISIP). IEEE Press, Piscataway, New Jersey, USA, pp 98-103.

[5] M. Eisenhauer, P. Rosengren, and P. Antolin. A Development Platform for Integrating Wireless Devices and Sensors into Ambient Intelligence Systems. 2009 6th IEEE Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops, 00(c):1–3, Juni 2009.

[6] K. Akkaya, M. Younis, A survey on routing protocols for wireless sensor networks, Ad Hoc Networks 3 (3) (2005), 325–349.

## 3.4 Forest Fire scenario

### 3.4.1 Forest Fire communication requirements

This section contains a review of communication requirements between the different systems which are responsible for the gathering of the needed information into the DiCoMa Forest Fire scenario and the DiCoMa platform. As explained on the deliverable "D1.4 DiCoMa Architecture" a service-oriented development is done to satisfy this communication.

The service-oriented development provides a common programming to access any possible application. Services defined in this way became the basic unit of a more complex structure of services. This paradigm lets the creation of a variety of new strategic solutions, including: rapid application integration, automated business processes and multi-channel access to applications.

The major advantages of Service Oriented Architecture (SOA) that makes use the Web Services (WS) paradigm are that WSs are pervasive, simple, and platform-neutral. The basic Web services architecture consists of specifications (SOAP, WSDL, and UDDI) that support the interaction of a client with a Web service provider and the potential discovery of the Web service description. The provider typically publishes a WSDL description (in case of SOAP) of its offered services, and the requester accesses the description using a UDDI or other type of registry, and requests the execution of the provider's service by sending a SOAP message to it.

Web services roles include requester and provider, the service *requester* initiates the execution of a service by sending a message to a service provider. The service *provider* executes the service upon receipt of a message and returns the results, if any are specified, to the requester. A requester can be a provider, and vice versa, meaning an execution agent can play either or both roles.

Requirements for a service oriented design:

- A service provider must be implemented into the DiCoMa platform. Using the appropriate service description document, WSDL, any client may connect and execute all the specified utilities.
- At least one client device must be present: it is any software with the ability of generating requests to the service provider.

Within the DiCoMa Forest Fire environment, there are two possible service oriented designs: firstly, each of the sensor HW boards could act as a client using the Constrained Application Protocol (CoAP); otherwise, a gateway (GW) could be included as the traditional SOAP WS client.

CoAP is a software protocol intended to be used in very simple electronics devices that allows them to communicate interactively over the Internet. It is particularly targeted for small low power sensors, switches, valves and similar components that need to be controlled or supervised remotely, through standard Internet networks. It is designed to easily translate to HTTP for simplified integration with the web, while also meeting specialized requirements such as multicast support, very low overhead, and simplicity. The standardization group (CoRE) has proposed the following features for CoAP:

- RESTful protocol design minimizing the complexity of mapping with HTTP.
- Low header overhead and parsing complexity.
- URI and content-type support.
- Support for the discovery of resources provided by known CoAP services.
- Simple subscription for resources, and resulting push notifications.
- Simple caching based on max-age.


Figure 7: CoAP layers in the protocol stack

### 3.4.2 Forest fire management protocols

The wireless acquisition network must satisfy the mesh topology, instead of the traditional tree structure. A mesh seamlessly extends the device's reach and the need for simple deployment and configuration providing multiple paths between nodes, so all that should be necessary is for the node to be able to communicate with just one other node, any node, in the mesh. Additionally

a mesh provides improved reliability though path diversity. If one link fails because of signal fade or multi-path interference another path can be used instead.

An extremely interesting alternative to the current mesh routing approaches appears when building the mesh network above IP using standard or new routing protocols designed to be more efficient for low power and limited bandwidth scopes. These protocols would manage the IP routing tables to let IP "route" packets between the various nodes. IP routing works by separating the routing engine and forwarding engine into separate distinct functions. The routing function is responsible for maintaining the routing tables and the forwarding function (IP) examines the routing table for a "path" to forward the packet. Sometimes the routing table is as simple as a single "default route" entry. This would be completely sufficient for an 802.15.4 Reduced Function Device (RFD) or edge node with a single parent. More recent versions of IP allow for multiple default routes, which would provide the path diversity previously mentioned.

By the way of the security issues, the IEEE 802.15.4 standard provides link layer security services. It has three modes of operation: 1) unsecured; 2) an Access Control List (ACL) mode; and 3) secured mode.

In the unsecured mode, as the name implies, no security services are provided. In the ACL mode the device maintains a list of devices with which it can communicate. Any communication from devices not on the list is ignored. However, it must be noted that this mode offers no cryptographic security so it is trivial for the message source address to be spoofed. Finally, the secured mode offers seven security suites and depending on which is used any of four security services are offered these being:

- access control;
- data encryption;
- frame integrity; and
- sequential freshness.

One cryptographic algorithm, AES-128, is employed for all security suites, which allows for a very efficient implementation. For high security, the full 128-bit message integrity code (MIC) can be added to each transmitted message. The MIC, however, can be truncated to 64 or 32 bits to trade security for shorter message length.

Otherwise, there have been some problems found with some of the optional security modes and with the feasibility of supporting different keying models but these limitations can be overcome by higher level protocols. Higher level protocols have thus to guarantee keying models without use much extra energy. Another issue is that no explicit key management scheme has been proposed. Finally, as identified in a 6LoWPAN draft [69], a major vulnerability is the unsecured ACK packet which renders most security measures at MAC useless. Notably, as the ACK frame integrity is not protected, it opens the door for a malicious node to prevent a legitimate device from receiving a particular frame, which is possible by forging an ACK using the unencrypted sequence number from the data frame and sending it to the source while creating enough interference, in order to prevent the legitimate receiver from receiving the frame. It hence allows for DoS in form of Acknowledgement Spoofing, which can be prevented by securing the ACK.

## 3.5 Coordination among decision-making bodies

This kind of systems needs the integration of the data received from different systems in order to homogenize the information for further processing. This kind of activities is called *Data Fusion*. In

the recent years, multi-sensor data fusion has received significant attention for several applications. As we can consider, the DiCoMa system needs to gather information from several network sensors. Therefore, data fusion techniques combine data from multiple sensors, and related information from associated databases to achieve improved accuracies and more specific inferences than could be achieves by the use of a single sensor alone [1-4].

While the concept of data fusion is not new, the emergence of new sensors, advanced processing techniques and improved processing hardware make real-time fusion of data increasingly possible [5, 6].

In principle, fusion of multi-sensor data provides significant advantages over single source data. In addition to the statistical advantage gained by combining same-source data (e.g., obtaining an improved estimate of a physical phenomenon via redundant observations), the use of multiple types of sensors may increase the accuracy with which a quantity can be observed and characterized.

### 3.5.1 Types of evidences

There are two critical and related issues concerning the combination of evidence obtained from multiple sources: one is the type of evidence involved and the other is how to handle conflicting evidence. It can be considered four types of evidence from multiple sources that impact the choice of how information is to be combined [7]:

- **Consonant evidence** can be represented as a nested structure of subsets where the elements of the smallest set are included in the next larger set… all of whose elements are included in the next larger set and so on. This can correspond to the situation where information is obtained over time that increasingly narrows or refines the size of the evidentiary set.

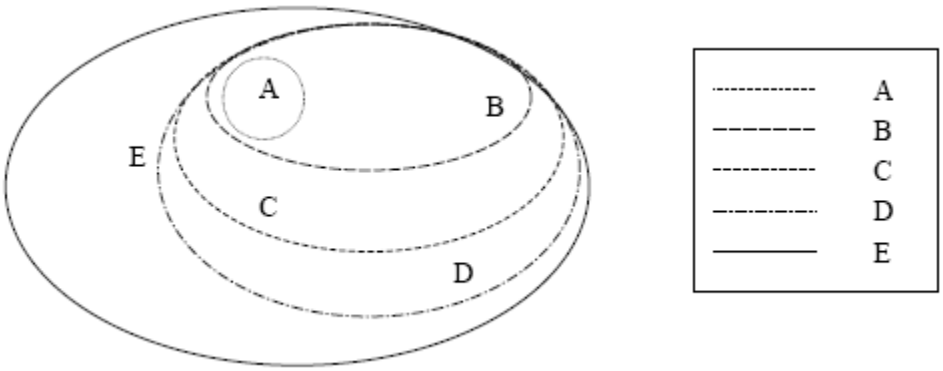


**Figure 8. Consonant evidences from multiple sources.**

- **Consistent evidence** means that there is at least one element that is common to all subsets.

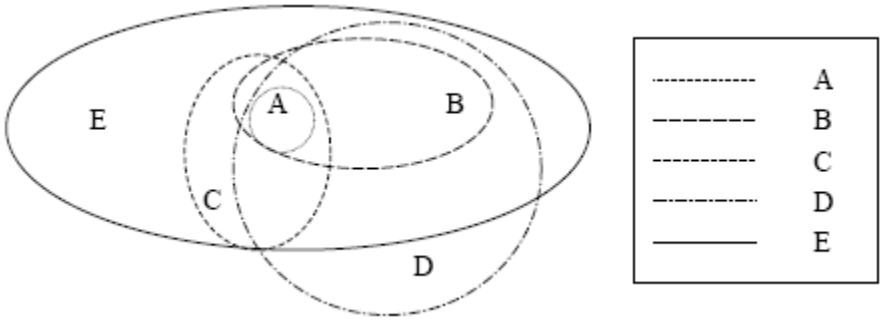


**Figure 9. Consistent evidences from multiple sources**

- **Arbitrary evidence** corresponds to the situation where there is no element common to all subsets, though some subsets may have elements in common.

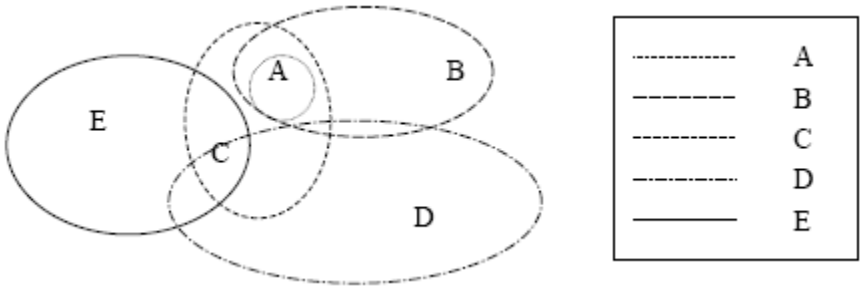


**Figure 10. Arbitrary evidences from multiple sources**

- **Disjoint evidence** implies that any two subsets have no elements in common with any other subset.

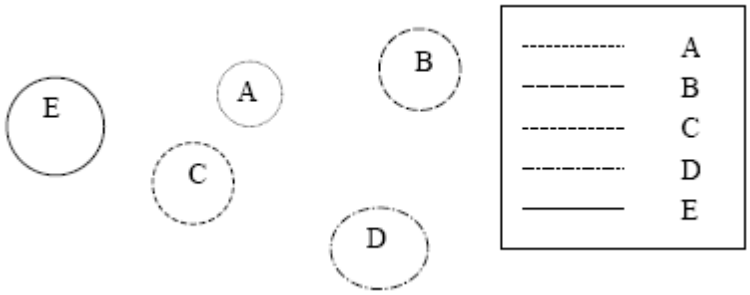


**Figure 11. Disjoint evidences from multiple sources.**

Each of these possible configurations has different implications on the level of conflict associated with the situation. Clearly in the case of disjoint evidence, all of the sources supply conflicting evidence. With arbitrary evidence, there is some agreement between some sources but there is no consensus among sources on any one element. Consistent evidence implies an agreement on at least one evidential set or element. Consonant evidence represents the situation where each set is supported by the next larger set and implies an agreement on the smallest evidential set; however, there is conflict between the additional evidence that the larger set represents in relation to the smaller set. Thereby, the data fusion process is really difficult as we can see. All used methods should be able to manage all these different scenarios.

### 3.5.2 Data Fusion Process Model

One of the historical barriers to technology transfer in data fusion has been the lack of a unifying terminology, which crosses application-specific boundaries. In order to improve communications among researchers and system developers, the Joint Directors of Laboratories (JDL) Data Fusion Working Group, established in 1986, began an effort to codify the terminology related to data fusion. The result of that effort was the creation of a process model for data fusion, and a Data Fusion Lexicon [8, 9].

The JDL process model is a functionally-oriented model of data fusion and is intended to be very general and useful across multiple application areas. While the boundaries of the data fusion process are fuzzy and case-by-case dependent, generally speaking the input boundary is usually at the post-detection, extracted parameter level of signal processing. The output of the data fusion process is (ideally) a minimally ambiguous identification and characterization of individual entities, as well as a higher level interpretation of those entities in the context of the application environment.

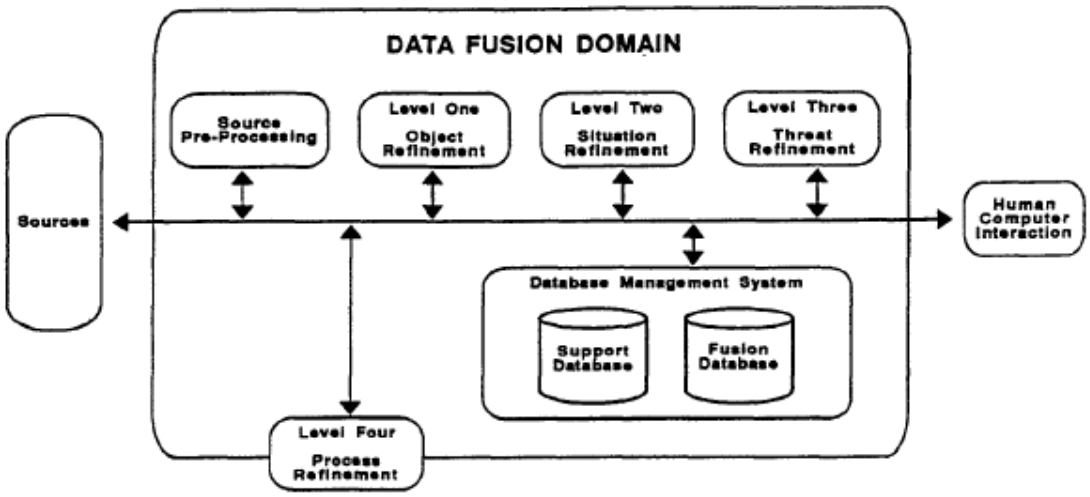


**Figure 12. JDL Data fusion model.**

The JDL Data Fusion Process model identifies the processes, functions, categories of techniques, and specific techniques applicable to data fusion. It is divided in the following levels:

- **Sources of Information.** The left side of Figure 6 indicates that a number of sources of information may be available as input including local sensors associated with a data fusion system.
- **Human Computer Interaction (HCI).** The right side of Figure 6 shows the human computer interaction function for fusion systems. HCI allows human input such as commands, information requests, human assessments of inferences, reports from human operators, etc.
- **Source Preprocessing (Process Assignment).** An initial process allocates data to appropriate processes and performs data prescreening.
- **Level 1 Processing (Object Refinement).** This process combines locational, parametric and identity information to achieve refined representations of individual objects.
- **Level 2 Processing (Situation Refinement).** Level 2 processing develops a description of current relationships among objects and events in the context of their environment.

- **Level 3 Processing (Threat Refinement).** This level projects the current situation into the future to draw inferences about enemy threats, friendly and enemy vulnerabilities, and opportunities for operations.
- **Level 4 Processing (Process Refinement).** Level 4 processing may be considered a meta-process. This level carries out functions as monitoring the whole process to provide information about real-time control and determining the source specific data requirements to collect required information among others.
- **Data Management.** The most extensive support function required to support data fusion processing is database management. This collection of functions provides access to, and management of data fusion databases, including data retrieval, storage, archiving, compression, relational queries, and data protection.

### 3.5.3 Methods

There are several methods to achieve the data fusion. In the following we will discuss the most popular methods:

- ***Linear Evidence Combination***

The first method of evidence combination is the linear combination. A simple linear combination is a weighted sum of normalized individual features. Either the feature values (similarities) themselves or the ranks can be combined [10]:

$$Rank_{final} = \omega_1 * Rank_{FR} + \omega_2 * Rank_{TA} + ...$$

where $\omega_1$ and $\omega_2$ are weights, $Rank_{FR}$ and $Rank_{AT}$ are the rank of a evidence as determined by some selected feature by an analysis module. It is also used a feature-value combination scheme:

$$Score_{combined} = \omega_1 * Score_{FR} + \omega_2 * Score_{TA} + ..$$

where $Score_{FR}$ *and* $Score_{TA}$ *are* the numeric "degree of association" scores assigned to each pair of features selected previously. The simplest approach to assigning weights to classifier inputs is to use constant weights. A more sophisticated approach might improve these weights by several learning algorithms.

- ***Classical Inference and Bayesian Inference Method***

The classical inference method and Bayesian inference network method are often referred as the "classical" or "canonical" sensor fusion methods because not only are they the most widely used, but also they are the bases of, or the starting points for, many new methods.

Classical inference methods seek to judge the validity of a proposed hypothesis based on empirical probabilities. Given an assumed hypothesis $H_i$ (a contextual fact is true or an event has happened), the joint probability $P$ that an observation $E_k$ would be reported by the sensors is:

$$P(E_k would\_be\_observed \mid H_k is\_true$$

Many decision rules can be used to form the judgment in the classical inference method. Another example of the decision rules is to use statistical significant test techniques. In the case where there are several alternative hypotheses, then the joint probability for each hypothesis needs to be computed and the results compared.

The classical inference method quantitatively compares the probability that an observation can be attributed to a given assumed hypothesis. But it has the following major disadvantages [11]:

- Difficulty in obtaining the density functions that describe the observables used to classify the object.
- Complexities that arise when multivariate data are encountered.
- Its capability to assess only two hypotheses at a time.
- Its inability to take direct advantage of a priori likelihood probabilities.

Bayesian inference overcomes some of these limitations by updating the likelihood of a hypothesis given a previous likelihood estimate and additional new observations. It is applicable when two or more hypotheses are to be assessed.

Given the observed phenomena or evidence $E$, Bayesian inference calculates the likelihood $P(H_i|E)$ that the contextual fact or event $H_i$ should be true or should have occurred in the form of [11]:

$$P(H_i \mid E) = \frac{P(E \mid H_i)P(H_i)}{\sum_j P(E \mid H_j)P(H_j)}$$

where, $P(H_i)$ is the a priori probability that the contextual fact or event $H_i$ has occurred; $P(E|H_i)$ is the likelihood that the phenomenon or evidence $E$ can be observed given the contextual fact or event $H_i$ has occurred.

Compared with the classical inference method, the Bayesian inference network method provides the following advantages:

- Given new observations, it incrementally estimates the probability of the hypothesis being true.
- The inference process can incorporate the a priori knowledge about the likelihood of a hypothesis being true.
- When empirical data are not available, it permits the use of subjective probability estimates for the a priori of hypotheses.

Despite these advantages, Bayesian inference method also has some disadvantages that prevent it from being used in many situations. The key limits are [11]: difficulty in defining a priori probabilities, complexities when there are multiple potential hypotheses and multiple conditionally dependent events, mutual exclusivity required for competing hypotheses, and inability to account for general uncertainty.

- ***Dempster-Shafer Theory***

The Dempster-Shafer method generalizes Bayesian theory to allow for distributing support not only to single hypothesis but also to the union of hypotheses. This way, it easily includes uncertainty in the likelihood function and acknowledgement and even quantification of ignorance [12]. The Dempster-Shafer and Bayesian methods produce identical results when all the hypotheses are singletons (not nested) and mutually exclusive [13].

In a Dempster-Shafer reasoning system, all the hypothesis elements that are not further dividable, mutually exclusive, and exhaustive are collectively called “the frame of discernment” ($T$). The system inference space is the power set ($\Theta$) of $T$, which includes all the possible combinations of the elements of $T$.

With the frame of discernment $T$ defined, the system’s possible hypotheses $\Theta$ defined, “belief” can be assigned over $\Theta$. Analogous to probability, the total belief equals to value 1, and each

sensor $S_i$ reports its observation by assigning beliefs. This assignment function is called the "probability mass function" of $S_i$, denoted as $m_i$. The belief assignment is based on the observed "evidence" ($E$) that supports the belief.

For any given hypothesis $H$, the system's belief in $H$ is the sum of all the evidence $E_k$ objects that support $H$ and the sub-hypotheses nested in $H$:

$$Belief_i(H) = \sum_{E_k \subseteq H} m_i(E_k)$$

On the other hand, the evidence objects that support $H$'s exclusive hypotheses (i.e., the hypotheses that do not include any sub-hypotheses nested in $H$) are then actually the evidences that are against $H$. Therefore, the "plausibility" of hypothesis $H$ should include all the observed evidence objects that do not argue against $H$:

$$Plausibility_i(H) = \sum_{E_k \cap H \neq \phi} E_k = 1 - Belief_i(\overline{H}) = \sum_{E_k \cap H \neq \phi} m_i(E_k)$$

Thus in the Dempster-Shafer reasoning system, according to a sensor $S_i$ 's observation, the belief regarding a hypothesis is measured by a "confidence interval" bounded by its basic belief and plausibility values (as shown in Figure 13):

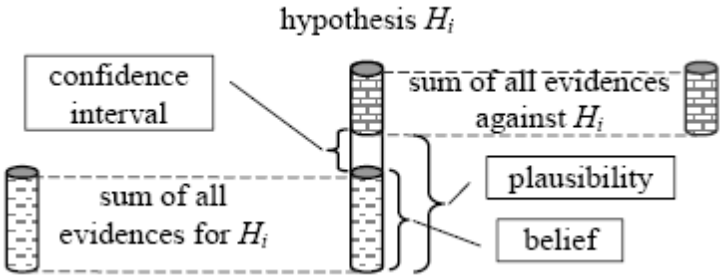


**Figure 13. Confidence interval is between "belief" and "pausibility**

Of course, there can be more than one sensor in a system. When there are multiple sensors in a system and the sensors' observations are assumed independent of each other, the Dempster-Shafer Evidence combination rule provides a means to combine these observations. For each hypothesis in $\Theta$ the rule combines sensor $S_i$'s observation $m_i$ and sensor $S_j$ 's observation $m_j$ as:

$$Belief\ (A) = m_i \oplus m_j(A) = \frac{\sum_{A_k \cap A_{k'} = A} m_i(A_k) m_j(A_{k'})}{1 - \sum_{A_l \cap A_{l'} = \phi} m_i(A_l) m_j(A_{l'})}$$

In last equation, the combined proposition *A* stands for the intersection of the sensor Si observed hypothesis $A_k$ and sensor $S_j$ observed hypothesis $A_{k'}$, whose associated probability mass functions are represented as $m_i(A_k)$ and $m_j(A_{k'})$ respectively. More accurately, the numerator calculates the probability mass function value of the products of two sensors' observed evidence objects that generate proposition A, and sums them up. To properly normalize the result, this sum of the products is divided by the denominator, which accounts for all the impossible proposition {Ø} combinations that have been assigned with non-zero probability mass functions.

Notice that this evidence combination rule is both associative and commutative [13]. This means that the probability mass functions $m_i(A_k)$ can be the results of previously combined evidence, so

the process of combining evidence from multiple sources can be chained, and the order in which the sources are combined does not affect the final results.

Bayesian methods and Dempster-Shafer methods are the most commonly used formalisms in MSDF (Multi-Sensor Data Fusion). The main reason that these two formalisms in particular have received so much attention is that both are associative and commutative, so the results are independent of the order in which the data are received and incorporated [14].

While both the Bayesian inference method and the Dempster-Shafer method can update a priori probability estimation with new observations to obtain a posteriori estimations, the Dempster-Shafer method relaxes the Bayesian method's restriction on mutually exclusive hypotheses, so that it is able to assign evidence to "propositions", i.e. unions of hypotheses.

The underlying concept is that Dempster-Shafer uses a general level of uncertainty [15-18]. Thus, as an extension of the Bayesian inference method, the Dempster-Shafer method largely overcomes the Bayesian's limitations listed in the previous subsection.

- ***Voting Fusion Method***

Voting sensor fusion imitates voting as a means for human decision-making. It combines detection and classification declarations from multiple sensors by treating each sensors declaration as a vote, and the voting process may use majority, plurality, or decision-tree rules. The most commonly used voting architecture is a Boolean combination of outputs from multiple sensors, where additional discrimination can be introduced via weighting each sensors specific declaration [11, 16].

The principle of the underlying mechanism of voting fusion is estimation of the joint detection probability based on the participating sensors' detection confidence levels, which are in turn based on predetermined detection probabilities for an object or an event.

The voting method greatly simplifies the sensor fusion process, and it can provide a prediction of object detection probability as well as false alarm probability. However, voting fusion is more suitable with yes/no problems like the classical inference method. This granularity of reasoning, generally speaking, is not good enough for multiple status context discrimination, which is often required in context-aware computing applications. For a multiple status problem to be solved using the voting method, it has to be converted into multiple yes/no problems first. Further, the more serious disadvantage inherent in the voting fusion method is that it treats each yes/no problem separately rather than taking them as a whole package, as the Dempster-Shafer method does (thus, the available information can be better utilized in the Dempster-Shafer sensor fusion framework).

- ***Fuzzy Logic Method***

The fuzzy logic method accommodates imprecise states or variables. It provides tools to deal with context information that is not easily separated into discrete segments and is difficult to model with conventional mathematical or rule-based schemes. There are three primary elements in a fuzzy logic system, namely, fuzzy sets, membership functions, and production rules. Fuzzy sets consist of the imprecisely labelled groups of the input and output variables that characterize the fuzzy system.

Each fuzzy set has an associated membership function to provide a representation of its scope and boundaries. A variable of a fuzzy set takes on a membership value between the limits of 0 and 1, with 0 indicating the variable is not in that state and 1 indicating it is completely in that state. An intermediate membership value means a "fuzzy" state, somewhat between the "crisp" limits. A variable may belong to more than one fuzzy set.

Production rules specify logic inference in the form of IF-THEN statements, which are also often referred to as fuzzy associative memory. The basic algorithm is that the "AND" operation returns the minimum value of its two arguments, and the "OR" operation returns the maximum value of its two arguments. The output fuzzy set is defuzzified to convert the fuzzy values, represented by the logical products and consequent membership functions, into a fixed and discrete output that can be used by target applications.

Regarding human-users' contextual information, there is a broad range of "fuzzy" situations, where the boundaries between sets of values are not sharply defined, events occur only partially, or the specific mathematical equations that govern a process are not known. With its capability of dealing with this kind of information, and with its cheap computation to solve very complicated problems, the fuzzy logic method is expected to develop extensively in some context-aware computing applications.

The fuzzy logic sensor fusion method provides an effective tool to handle requirements of human daily-life, where imprecision is an inherent property in nature. However, the fuzzy logic sensor fusion method cannot be the main sensor fusion method in a generalizable architectural solution in building a context-aware computing system for two reasons. First, it is not applicable to situations where the objects inherently have clear-cut boundaries. Second, the fuzzy set, membership function assignment, and production rules are usually extremely domain and problem specific, making it difficult to implement the method as a general approach.

- ***Neural Network Method***

Neural networks open a new door for fusing outputs from multiple sensors. A neural network can be thought of as a trainable non-linear black box suitable for solving problems that are generally ill defined and that otherwise require large amounts of computation power to solve.

A neural network consists of an array of input nodes to accept sensors' output data, one or a few output nodes to show sensor fusion results, and sandwiched in between the input and output nodes is a network of interconnecting data paths. The weights along these data paths decide the input-output mapping behaviour, and they can be adjusted to achieve desired behaviour. This weight-adjusting process is called training, which is realized by using a large number of input-output pairs as examples.

The neural network training process can be simplified as follows. From the input nodes to output nodes, the data-path network provides many ways to combine inputs: those that lead to the desired output nodes are strengthened, whereas those that lead to undesired output nodes are weakened. Thus, after using the large number of input-output pair as training examples to adjust weights, the input data are more easily transferred to desired output nodes through the strengthened paths.

The neural networks can work in a high-dimensional problem space and generate high-order nonlinear mapping. Many successful applications have been reported. However, it has some well-known drawbacks too. The three major problems are:

- It is difficult to select a network architecture that reflects the underlying physical nature of the particular applications.
- Training a network is typically tedious and slow
- Training can easily end up with local minima, as there is no indication whether the global minimum has been found.

The neural network method is not suitable for the main sensor fusion method mainly because of the drawbacks. First, the mapping mechanism is not well understood even if the network can provide the desired behaviour; only in the simplest toy-like problems does examination of the

weights in the trained network give any clue as to the underlying analytical connection between the inputs and outputs. Thus, such a solution cannot be easily generalized. Second, the neural network method is, generally speaking, not suitable to work in a dynamic sensor configuration environment, because each sensor needs a unique input node and each possible sensor-set configuration needs to be specifically trained. Third, the neural network sensor fusion method has the "local minimum problem" during its training process, which cannot be easily overcome.

### 3.5.4 Data Fusion in the DiCoMa Platform

The DiCoMa communication platform is shown in the Figure 14. This system, will garther the information form the sensors employing the observer/observable pattern. Hence, using the Enterprise Service Bus (ESB) and the eXtreme Transaction Processing Platform (XTPP) all the collected data will be processed to be stored in the repositories. Therefore, this platform will apply the data fusion techniques.

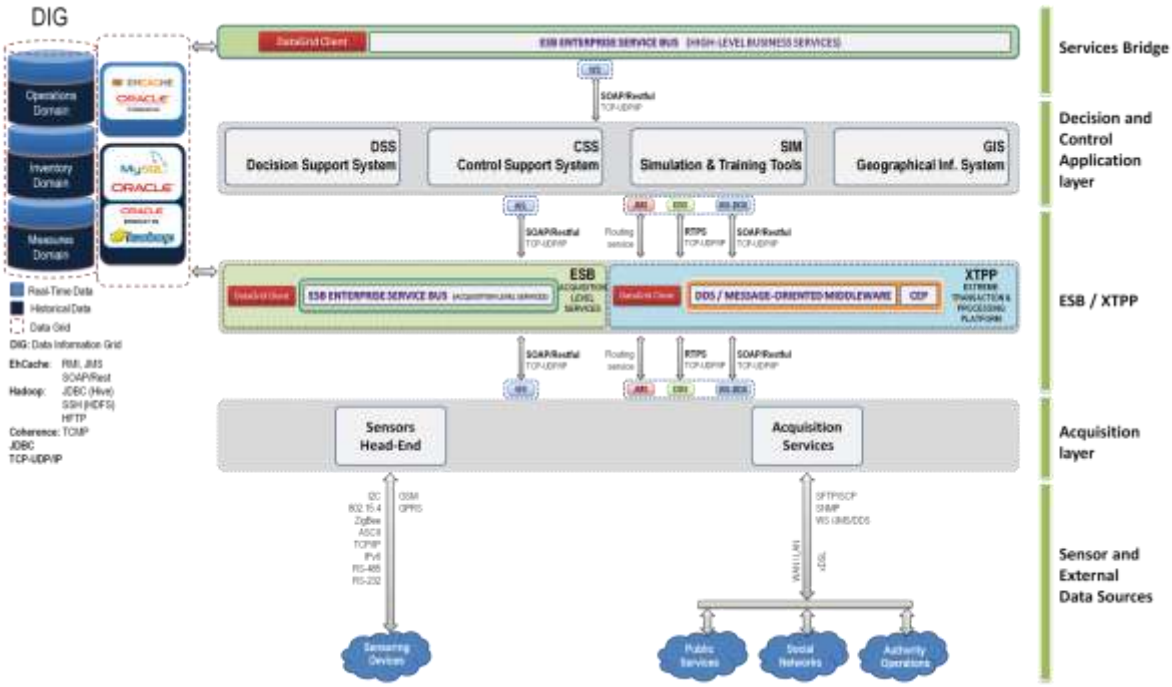


**Figure 14. DiCoMa architecture, physical and fucntional overview.**

After the processing, some modules such as the Decision Support System (DSS) or the Control Support System (CSS) will get the merged data from the Enterprise Service Bus and the repositories for their work. Moreover, other systems, such as the post-mortem analysis system, will recover the merged data only from the repositories.

Although the platform makes the final aggregation, the wireless sensor network, which works under the proposed trust model (see the section 3.4.1), will produce a previous data fusion process to combine the information of the grid before the manager node sends the information to the DiCoMa platform.

## 3.6 References

[1] E. Waltz, "Data Fusion for C31: A Tutorial" Command, Control, Communications Intelligence (C31) Handbook, EW Communications, Inc., Palo Alto, CA, pp. 217-226, 1986.

[2] J. Llinas, E. Waltz, Multisensory Data Fusion, Artech House, Inc., 1990.

[3] D. Hall, Mathematical Techniques in Multisensory Data Fusion, Artech House, Inc., 1992.

[4] L.A. Klein, Sensor and Data Fusion Concepts and Applications, SPIE Optical Engineering Press, Tutorial Texts, Vol. 14, 1993.

[5] D.L, Hall, J. Llinas, "A Challenge for the Data Fusion Community I: Research Imperatives for Improved Processing," Proceedings of the Seventh National Symposium on Sensor Fusion, Albuquerque, NM, March 1994.

[6] J. Llinas, D. L. Hall, "A Challenge for the Data Fusion Community II: Infrastructure Imperatives," Proceedings of the Seventh National Symposium on Sensor Fusion, Albuquerque, NM, March 1994.

[7] Kari Sentz and Scott Ferson, "Combination of evidence in Dempster-Shafer theory", Sandia Report, 2002

[8] Kessler et al., "Functional Description of the Data Fusion Process", report prepared for the Office of Naval Technology, published by the Naval Air Development Center, Warminster, PA, January 1992.

[9] Data Fusion Lexicon, published by the Data Fusion Subpanel of the Joint Directors of Laboratories Technical Panel for C3 (F. E. White, Code 4202, NOSC, San Diego, CA), 1991.

[10] H.L. Van Trees, "Detection, Estimation, and Modulation Theo", Part II: Radar-Sonar Signal Processing and Gaussian Signals in Noise, Krieger, 1992.

[11] Lawrence A. Klein, "Sensor and Data Fusion Concepts and Applications" (Second edition), SPIE Optical Engineering Press, 1999, ISBN 0-8194-3231-8

[12] Huadong Wu, Mel Siegel, Rainer Stiefelhagen, and Jie Yang, "Sensor Fusion Using Dempster-Shafer Theory," presented at IEEE International Measurement Technology Conference (IMTC) 2002, Anchorage AK USA, 2002

[13] Glenn Shafer and Judea Pearl (editors), "Readings in Uncertainty Reasoning" Morgan Kaufmann Publihser Inc., 1990, ISBN 1-55860-125-2

[14] Kari Sentz and Scott Ferson, "Combination of Evidence in Dempster-Shafer Theory", Technical Report, April 2002 Los Alamos National Laboratory, Los Alamos, NMR.S. Doyle and C.J. Harris, "Multi-Sensor Data Fusion for Obstacle Tracking Using Neuro-Fuzzy Estimation Algorithms", SPIE (The International Society for Optical Engineering) Proceedings Vol.2233, Sensor Fusion and Aerospace Applications II, 6-7 April 1994, Orlando, Florida, Page 112-123

[15] George J. Klir, "Uncertainty and Information Measures for Imprecise Probability: An Overview", the Proceedings of the first International Probabilities and Their Applications., Ghent, Belgium, June 29 . July 2, 1999

[16] David Lee Hall, "Mathematical Techniques in Multisensor Data Fusion", Artech House Inc., 1992 ISBN 0-89006-558-6

[17] Luis Mateus Rocha, “Relative Uncertainty and Evidence Sets: A Constructivist Framework”, International Journal of General Systems, Vol. 26 (1-2), pp. 35-61

[18] Egan, J.P., 1975. Signal detection theory and ROC analysis, Series in Cognition and Perception. Academic Press, New York.