

INTERNET OF THINGS: REALIZATION OF AN ANALYSIS OF THE STATE OF TECHNOLOGICAL ART IN ORDER TO IDENTIFY CURRENT AND FUTURE TECHNOLOGIES AND PLATFORMS REGARDING THE IOT SECTOR

Data: 07/23/2019



The ERDF project 2023 Beacon Südtirol (CUP: B31H17000060001) was funded by the European Development Fund/Regional Autonomous Province of Bolzano, Investing for Growth and employment 2014-2020 ERDF.

Project partner



Edited by



Giovanni Giannotta, Gruppo FOS

Gabriele Scarton, Gruppo FOS

Federico Boero, Gruppo FOS

Andrea Sansalone, Gruppo FOS

Giorgio Allasia, Gruppo FOS



Stefano Seppi, NOI S.p.a.

Patrick Ohnewein, NOI S.p.a.

Italian to English translation by Emma Victoria Rawlinson

Index

1	Introduction.....	4
2	The study.....	6
3	A bit of history.....	7
4	<i>Evolutionary trends of the IoT</i>	9
5	IoT Alliances and Consortia.....	12
5.1	Alliances and IoT consortia comparison.....	15
6	IoT technologies/platforms.....	18
6.1	From small to large distances.....	19
6.2	IoT Architecture.....	20
6.2.1	Architettura a 3 e 5 livelli.....	22
6.2.2	Security.....	22
6.2.3	Architectures based on Cloud, FOG and EDGE.....	28
7	Examination Comparison of the technological specifications and protocol in IoT landscape.....	31
7.1	Network Access Layer.....	31
7.2	Communication Models.....	32
7.2.1	Analyzed technologies that define the Medium Access Control level (MAC).....	32
	Ethernet 802.3.....	32
	WLAN – Wifi 802.11 a/b/g/n.....	33
	Ingenu/RPMA.....	34
	Radio Frequency Identification (RFID).....	35
	Near Field Communication (NFC).....	36
	Bluetooth IEEE 802.15.1 e successive versioni.....	36
	Bluetooth Low Energy.....	37
	Z-Wave.....	37
	M-Bus / WM-Bus.....	40
	Weightless W-N-P.....	43
	NB-IoT.....	44
	LTE - Long Term Evolution.....	44
	EC-GSM-IoT.....	45
	LoRa — Long Range Protocol.....	46
	Sigfox.....	46
7.2.2	Analyzed technologies that are based on other standards.....	47
	Dash7.....	47
	Zigbee, Zigbee Pro, Zigbee 3.0.....	48
	DigiMesh®.....	51
	Thread / OpenThread.....	53
	Ant / Ant+.....	54
	Wireless-HART.....	57
7.2.3	Comparative Tables.....	57
7.3	Transport Layer.....	64
7.3.1	IPV4.....	65
7.3.2	IPV6.....	65
	IPV6.....	65
7.3.3	6LoWPAN.....	66
7.3.4	RPL.....	66
7.4	Session/communication.....	67

7.4.1 HTTP.....	68
7.4.2 MQTT.....	68
7.4.3 CoAP.....	72
7.4.4 AMQP.....	72
7.4.5 NATS / NATS 2.0.....	73
7.4.6 DDS.....	74
7.4.7 XMPP.....	76
7.4.8 Comparative tables.....	77
7.5 Data Aggregation / <i>Processing</i> Layer.....	78
7.6 Data <i>Storage</i> Layer.....	80
7.7 Final tables.....	83
8 The security issue.....	88
8.1 IoT Communication Technologies.....	88
8.1.1 ZigBee.....	88
8.1.2 Bluetooth.....	89
8.1.3 WSN in generale.....	89
8.1.4 Wireless Fidelity (Wi-Fi).....	89
8.1.5 LoRaWan.....	90
8.1.6 Sigfox.....	95
8.1.7 5G Networks.....	98
8.2 Cybersecurity Issues.....	98
9 Technological trends in South Tyrol.....	101
10 Conclusions.....	104

Index of figures

Figure 1: Gartner hype cycle of emerging technologies in 2018 (Source Gartner Inc.).....	9
Figure 2: Google Trends from 2011 to 2018 of technologies: IoT, A.I., Blockchain and Big data....	9
Figure 3: Forecast of economic impact in the IoT 2025 ⁷	10
Figure 4: Panorama delle associazioni e consorzi <i>IoT</i> - Technology and Marketing.....	12
Figure 5: Panorama of IoT associations and consortia - Horizontal and Vertical Domains.....	13
Figure 6: Initiatives IoT OSS - Technology and Marketing.....	14
Figure 7: <i>Internet of Things</i> Alliance and Consortia.....	15
Figure 8: Panorama dei protocolli per l' <i>IoT</i> dai dispositivi al mercato.....	19
Figure 9: Confronto tra i modelli di interconnessione <i>IoT</i> e Web con riferimento all'ISO/OSI.....	21
Figure 10: Architecture 3 (A) and 5 (B) layer.....	22
Figure 11: Architecture in 4 levels and related useful security mechanisms.....	26
Figure 12: The Internet of Things Reference Model.....	29
Figure 13: <i>IoT</i> Data <i>Processing</i> Layer <i>Stack</i>	30
Figure 14: Comparison of communication protocols.....	32
Figure 15: Operational Range of the IEEE 802.11 Technologies.....	33

List of Tables

Table 1: Confronto Alleanze/Consorti dell'ecosistema <i>IoT</i> - Core / Communication / <i>Messaging</i> - Multilayer / <i>Stack</i>	16
---	----

Table 2: Confronto Alleanze/Consorzi dell'ecosistema <i>IoT</i> - Connected body / Home - Industrial <i>IoT</i> & Connected Buildings / Lighting - Infrastructure - Industry Marketing / Education Focused..	17
Table 3: Panorama <i>IoT</i> per livelli applicativi - dall'infrastruttura allo Storage.....	31
Table 4: 802.11 technologies comparison table.....	34
Table 5: Comparison between ISO / OSI e WM-Bus Models.....	40
Table 6: WM-Bus Mode.....	41
Table 7: WM-Bus Data Rate.....	42
Table 8: Zigbee Stack Comparison.....	49
Table 9: ZigBee 3.0 Technical Specifications.....	51
Table 10: General comparison of the protocols that also define the physical and MAC level.....	59
Table 11: General comparison of the analysed protocols based on other standards.....	61
Table 12: Technological comparison of the protocols analysed for WLAN and PAN.....	63
Table 13: <i>Technological comparison between protocols for LPWAN/Cellular Like</i>	63
Table 14: Comparison of transport protocols.....	65
Table 15: Comparison between aggregation platforms, management and processing data.....	79
Table 16: <i>Network Access Layer</i> – technology evaluation table.....	86
Table 17: Communication & Session Layer - technology evaluation table.....	87

1 Introduction

The document contains all results obtained in the development of the analysis of the state of technological art, aimed at identifying the current and possibly future technologies and platforms with regard to the Internet of Things (IoT) sector.

The first difficulty encountered in dealing with an analysis such as this is given by the reality that the *Internet of Things* is a concept, a paradigm and not a technology but is embodied in the technology of things, in fact it arises from important intuitions that have seen a maturation which started with the telegraph, perceived by research on Wireless Power Transfer (WPT) by Tesla, inadvertently applied to solve some student problems at Carnegie University and finally defined and summarized with the idiomatic phrase "*Internet of Things*" by Ashton. Today, 20 years after the awareness of the existence of the Internet of things we can affirm that the expansion of this paradigm has meant that the technologies related to it have become so important that they are changing our social and industrial life, both in habits and in the management of business processes.

Developing *IoT* applications does not just mean creating systems to connect devices in a network but it is something much more complex. We are at the peak of development and of relative expectations for the *IoT*. It is therefore necessary to first understand the technological structure involved in an *IoT* application. In fact, to be applied, the *IoT* paradigm must be considered as a set of different systems, such as: objects, communication systems and combinations of various *Software* solutions and the data itself, the related analysis activities and the actions that arise from them.

In the study, the technological world of the *IoT* was analysed considering its fundamental aspects: *Device*, communication and *Application* framework.

Internet of Things (IoT) the description of an idea that can be seen as a single term.

Coined by Kevin Ashton in 1999 to describe the use of RFID technology by Product & Gable and which he himself claims was "a great intuition", in fact after just 10 years it led to the birth of a concept, a protocol, a new vision: the Internet-0, as reported by an article in the Scientific American Journal of 2004. All this clearly presaged that the future of "things" is the *Internet of Things*, which represents the birth of objects that have an intelligent virtual space reflected in objects that they feel and implement in reality. The *IoT* aims to unify everything in our world under a common infrastructure, giving us not only control over the things around us, but also keeping us informed about the state of things.

The historical period in which the *IoT* paradigms have become important, affecting both our daily lives and the management of business processes, is this, the one in which we are all immersed - the beginning of the 21st century.

With this premise, the study reported in this document aims to analyse the state of the art of *IoT*-related technologies after 20 years of growth and expansion. The document is based on the bibliographic study of existing technologies considering both the

market/commercial context and the research/scientific context, through the systematic review of official company reports, comparisons with industry experts, academic research documents and archives available on-line. The main objective of this work is to provide an overview of the state of the technological art of the *Internet of Things*, of the architecture and of the vital technologies and applications relating to everyday life. Moreover, the study also wants to give the sector's players an idea of the IoT technology that it will be, trying to identify those that seem to be the most promising in terms of ease of use, availability and market pervasiveness.

2 The study

The analysis saw a first bibliographic study of existing technologies, considering both the market/commercial context and the research/scientific context, with the relative evaluation of the most promising.

The evaluation was carried out considering both platforms independent of the *Hardware*, therefore disconnected from the type of infrastructure and *Hardware* technology, and platforms operating only with a specific type of *Hardware* and considering off-the-shelf commercial components or made up of chipsets only.

The technologies and platforms have been evaluated based on the following features:

- level of development;
- quality, availability in the market place and relative support;
- development philosophy: *Open*, closed, proprietary or free, both *Hardware* and *Software*, and then its distribution licenses and use;
- quantity and quality of the projects in which they are used;
- prospects for evolution in the following years;

Subsequently the technological world of the *IoT* was analysed considering its fundamental aspects: *Device*, communication and data management, always keeping the inputs coming from the South Tyrol-Alto Adige *Beacon Community* as a reference.

The study is certainly not exhaustive, given the technological vastness that the *IoT* invests, but it is a tool that can give the idea of the technological path that will be configured, with a look at what the situation is in South Tyrol.

The work continued with the identification of exemplary *IoT* platforms that were subsequently tested in the field, exploiting a specially designed test protocol together with the South Tyrol-Alto Adige *Beacon Community*.

3 A bit of history

Remembering where the *IoT* concept comes from and considering the 3 fundamental technological aspects (*Device*, *Communication* and *Software*), we must start from the invention that allowed, for the first time, long distance communication through electrical signals, the telegraph, invented by Shilling in 1834, to continue with the insights of Nikola Tesla, who in an interview in 1929 stated: *"When Wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole.....and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket."*¹, and he continued saying *".....Present Wireless receiving apparatus.....will be scrapped for much simpler machines; innumerable transmitters and receivers may be operated without interference. Domestic management--the problems of heat, light and household mechanics--will be freed from all labor"*¹. In 1937 in Chicago, Guglielmo Marconi defined *Broadcasting* as a "one-way" communication, emphasizing that *"a far greater importance lies, in my opinion, in the possibilities offered by radio to exchange communications wherever correspondents are"*². Alan Turing who in 1950 wrote: *"...It can also be maintained that it is best to provide the machine with the best sense organs that money can buy... "*³, in 1966 Karl Steinbuch stated: *"In a few decades time, computers will be interwoven into almost every industrial product"*⁴, and others, until 1982 when, involuntarily, some students of the Carnegie University of Pennsylvania created the first *IoT* object by connecting a Coca Cola distributor to the ARPANET to check the presence of bottles of Coca Cola and which of them were cold⁵. Kazar himself, now CTO at Avere Systems who was one of the Carnegie University students in 1982, said that when computers cost a million dollars and ARPANET was still the only game in town, having an *IoT* dominated world seemed a distant fantasy⁵. Then in 1990 John RomKey connected the first toaster to the Internet so as to control its switching on and off remotely. Subsequently, the era of the web opens, with the first theories of ubiquitous computing, distributed computing, etc., a time when Mark Weiser stated: *"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it"*⁶, finally arriving at Kevin Ashton who in 1999 coined the name *"Internet of Things"* in a presentation at MIT in Boston⁷, and as he himself stated in an article on the RFID Journal site ten years later, claiming the authorship of the name but not its control, like the internet, the *IoT* will have the potential to change the world, if

1 WHEN WOMAN IS BOSS - An interview with Nikola Tesla by John B. Kennedy. Colliers, January 30, 1926

2 Marconi Day 2017, fari puntati su IoT e 5G. <https://www.corrierecomunicazioni.it/digital-economy/marconi-day-2017-fari-puntati-su-iot-e-5g/> (ultima visita 13/12/2018 alle 15.00)

3 A. M. Turing (1950) Computing Machinery and Intelligence. Mind 49: 433-460

4 Magdalena Gabriel, Ernst Pessl - INDUSTRY 4.0 AND SUSTAINABILITY IMPACTS: CRITICAL DISCUSSION OF SUSTAINABILITY ASPECTS WITH A SPECIAL FOCUS ON FUTURE OF WORK AND ECOLOGICAL CONSEQUENCES

5 <https://www.ibm.com/blogs/industries/little-known-story-first-IoT-Device/> (ultima visita 13/12/2018 alle 15.15)

6 Mark Weiser - The Computer for the 21st Century. 09-91 SCI AMER WEISER *** 1

7 <https://www.rfidjournal.com/articles/view?4986> (ultima visita 13/12/2018 alle 15.45)

not more. This may be increasingly true as computers learn to extract data from and to objects on their own.

In fact, from 1999 to 2009 the phrase *Internet of Things* is fully cleared through various articles, including that of the Scientific American Journal in 2004, and with the publication in 2005 of the report "The *Internet of Things* - Executive summary" by the International Telecommunication Union (ITU). In 2008 there were the first European conferences on the *IoT*¹ and the birth of the IPSO Alliance to promote the use of the IP protocol in "smart objects" and enabling the *IoT*. Furthermore, between 2008 and 2009, there was the first overtaking of things connected to the internet compared to men, this allowed the Cisco Internet Business Solutions Group (IBSG) to state that in that period of time the era of the *Internet of Things* was born².

1 <http://www.internet-of-things-research.eu/documents.htm> (ultima visita 13/12/2018 alle 16.00)

2 The Internet of Things. How the Next Evolution of the Internet Is Changing Everything. Dave Evans, 2011 CISCO White Paper.

4 Evolutionary trends of the IoT

In 2011 the *IoT* joined the emerging technologies in the study of GARTNER³ and in 2014 was already found to be a mature technology "Peak of Inflated Expectation", in 2018 the

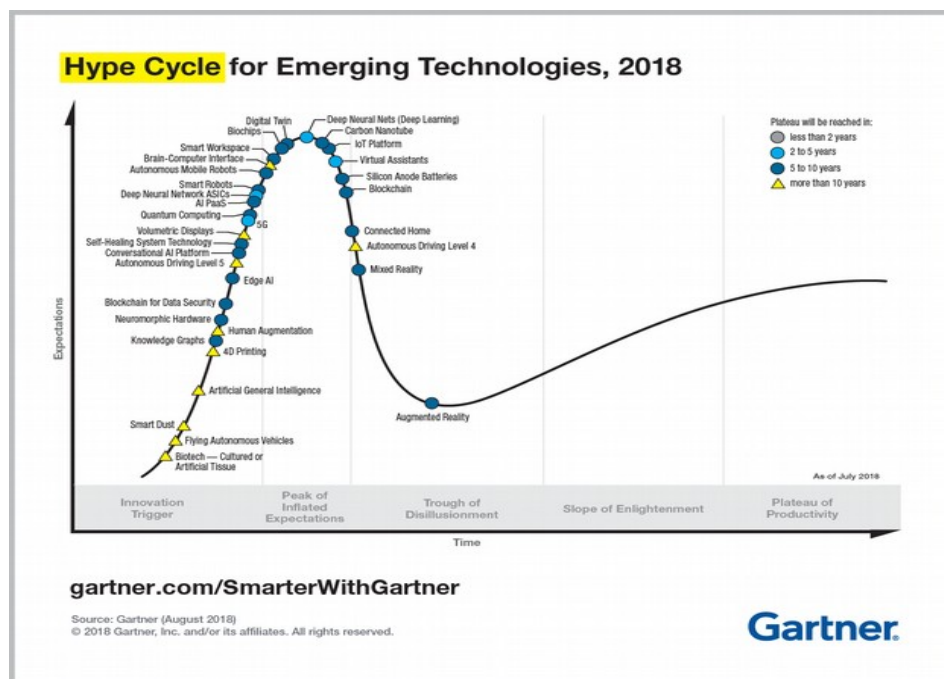


Figure 1: Gartner hype cycle of emerging technologies in 2018 (Source Gartner Inc.)

next stage begins (1), proving the facts that it is a technology that is about to invade society.

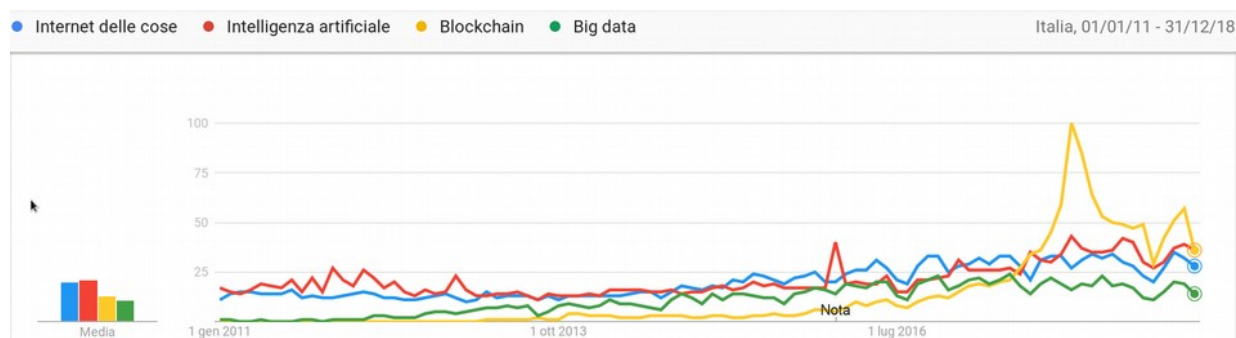


Figure 2: Google Trends from 2011 to 2018 of technologies: IoT, A.I., Blockchain and Big data

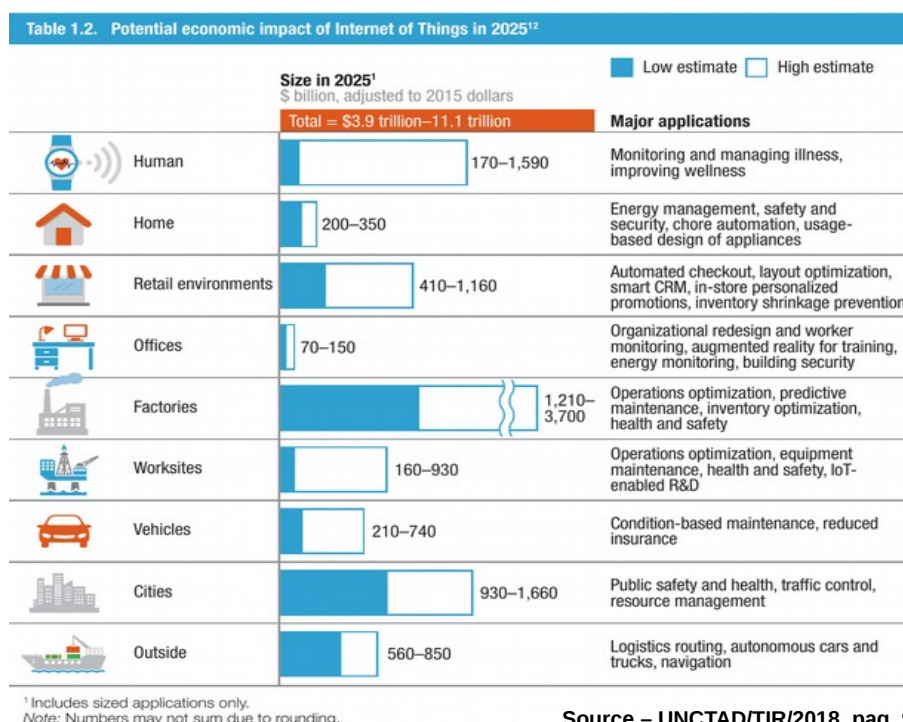
In the analysis reported in the Accenture report 2018 on the technological future of 25 world nations, the technologies of the *Internet of Things* is one of the main trend technologies together with the *Cloud*, artificial intelligence, *Blockchain*, augmented reality, robotics, and quantum computing⁴⁵. Also demonstrated by the interest of users of the Google

3 <https://www.postscapes.com/internet-of-things-added-to-the-2011-hype-cycle/> (ultima visita 13/12/2018 alle 16.30)

4 Accenture Technology vision 2018 https://www.accenture.com/t20180227T215953Z__w_/us-en/_acn-media/Accenture/next-gen-7/tech-vision-2018/pdf/Accenture-TechVision-2018-Tech-Trends-Report.pdf

5 Sharma, N., Shamkuwar, M., & Singh, I. (2018). *The History, Present and Future with IoT. Internet of Things and Big Data Analytics for Smart Generation*, 27–51.

search engine (2). In fact, through the Google trends tools we compared the research related to the *IoT* (Internet of things) topic with three other topics that intersect a lot with the intrinsic needs of the *Internet of Things*: artificial intelligence (A.I. that on the hip cycle of Gartner appears only with the deep learning part), the *Blockchain* and Big data. As you can see the *IoT* declared as such in 2011 has always maintained a certain interest that in recent years has been growing to then to remain at current levels since mid-2017. Considering that in 2016 Google modified and improved its analysis tools, it must be said that in 2017 the fever of virtual coins exploded and this explains the greater interest of the *Blockchain* technology that today is beginning to be seen as a possible tool for *Data Security* (as also reported by Gartner's Hype Cycle), and once the coin boom is underway, it is very quickly reaching very low interest levels. Unlike A.I. that from that date begins to feel a comparable and slightly higher interest than the *IoT*, also because the *IoT* itself begins to be seen as a useful tool for artificial intelligence, thanks to the possibility of collect-



Source – UNCTAD/TIR/2018, pag. 9

Figure 3: Forecast of economic impact in the IoT 2025⁷

ing heterogeneous data from all the things that surround us and that interact directly with man - allowing the simplification of human-machine interaction ⁶. For Big data, the story is slightly different given that compared to the *IoT* and other technologies it is considered support and therefore little known to the general public, determining a level of interest that shows a parallelism with *IoT*. Figure 3 ⁷ shows the table taken from the United Nations In-

6 EY report 2016 - *Internet of Things* Human-machine interactions that unlock possibilities - EY Global Media & Entertainment -. [https://www.ey.com/Publication/vwLUAssets/ey-m-e-internet-of-things/\\$FILE/ey-m-e-internet-of-things.pdf](https://www.ey.com/Publication/vwLUAssets/ey-m-e-internet-of-things/$FILE/ey-m-e-internet-of-things.pdf).

7 UNCTAD - INNOVATION TECHNOLOGY AND REPORT 2018 - Harnessing Frontier Technologies for Sustainable Development. UNITED NATIONS Publication, UNCTAD/TIR/2018, e-ISBN 978-92-1-363310-6

novation Technology and Report 2018, which highlights the forecast of the economic impact of *IoT* technologies to 2025.

5 IoT Alliances and Consortia

Before going on to evaluate the communication models/protocols it is interesting to have an overview of the most important discussion, analysis, study and influence groups, born and present today in the world scene, and to have a character and vision comparison. In fact, if they have not generated one or more protocols or standards, they have put in place a series of models and guidelines, technologies and more, that in some way try to solve all those problems that afflict the now established and consolidated models and protocols, such as TCP/IP.

The following images show different ways of seeing and understanding the combination of alliances and consortia, the data refer to the 2017-2018 period and some of them could have been merged, integrated into others or dissolved.



Figure 4: Panorama delle associazioni e consorzi IoT - Technology and Marketing

In 4 the horizontal axis represents the type of market and the vertical axis represents the technology/solution/knowledge area on which these initiatives focus. It should be understood that the leftmost part of the horizontal axis represents the Customer's market (i.e. Business to Customer: B2C), while the rightmost part of the same axis represents the industrial Internet market (i.e. Business to Business: B2B). The upper part of the vertical axis represents the technological areas related to services and applications, while the lower part of the same axis represents the technological areas related to connectivity ⁸

8 *IoT LSP Standard Framework Concepts Release 2.8 AIoTI WG03 – IoT Standardisation 2017*

In 5⁸ the panorama of initiatives is represented according to their main activities. On the vertical axis the applications relating to the IoT domains are represented, while on the horizontal axis the technological areas (communication infrastructures) are visible.

Another very important classification is that linked to *Open Source*, in Figure 6¹⁵ they are represented based on the technological typology and the application target.

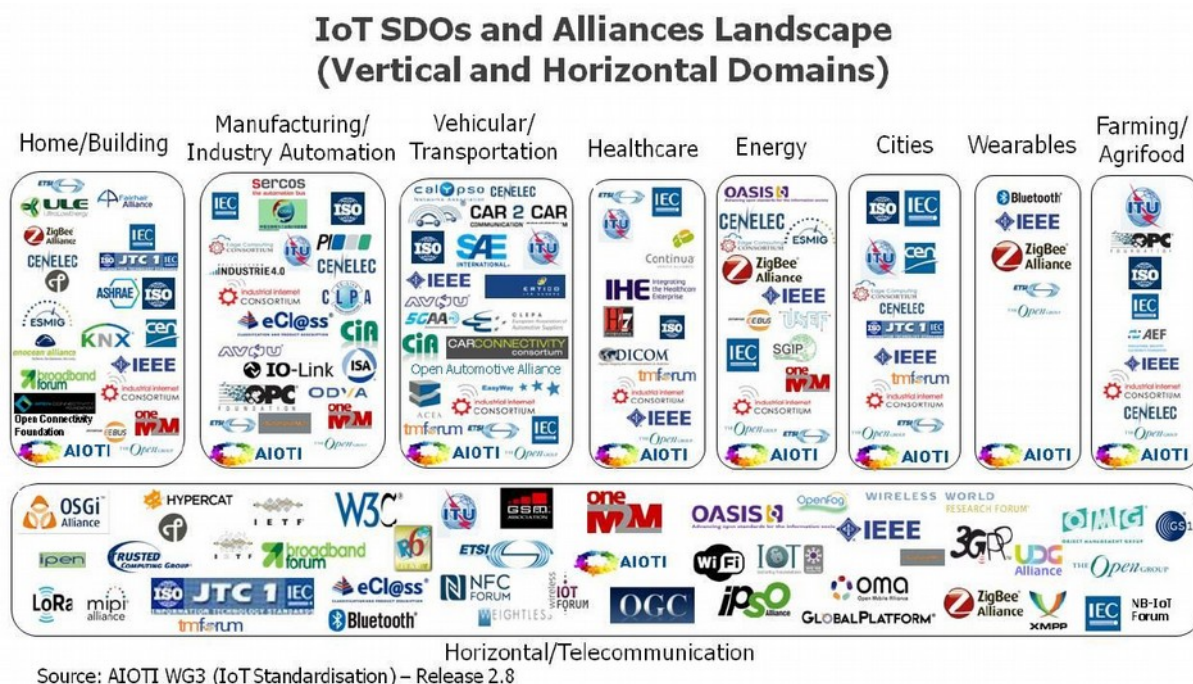


Figure 5: Panorama of IoT associations and consortia - Horizontal and Vertical Domains

In Figure 7⁹ we try to give an overall idea considering the technological typology and the set of *Hardware* technological architectures, transmission and communication protocols.

9 Postscope.com. Marzo 2015

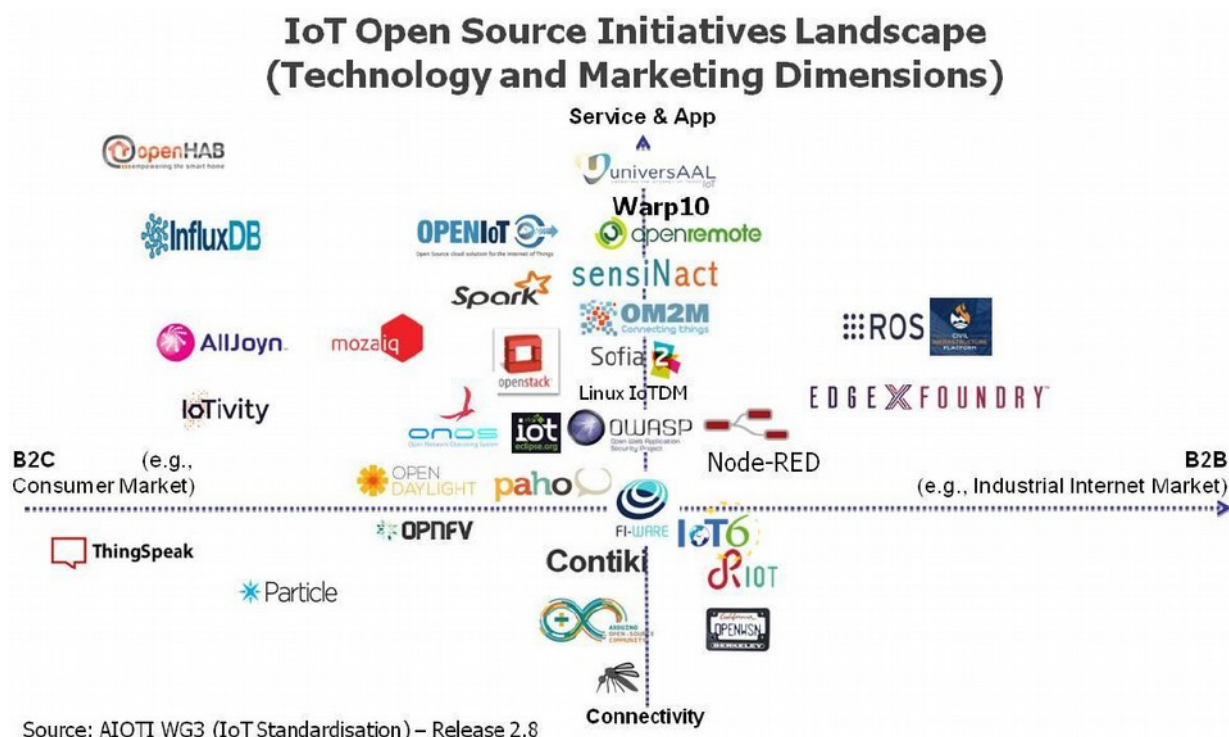


Figure 6: Initiatives IoT OSS - Technology and Marketing

As an application target, specific applications are considered for specific needs: vertical

Handbook: Internet of Things Alliances and Consortia



CC Attribution: Postscapes.com - Version 1.0 Updated March 2015

Figure 7: Internet of Things Alliance and Consortia

and industry-focused, more open and generalized, focused on marketing and education

5.1 Alliances and IoT consortia comparison

Below is a comparison table of the major alliances and consortia currently present in the IoT scenario.













Tipologia	Core / Communication / Messaging				Multilayer / Stack							
Consorzio / Alleanza												
Nazionalità	IEEE (Institute of Electrical and Electronics Engineers)	Internet Engineering Task Force (IETF)	ISO (International Organization for Standardization)	The LoRa™ Alliance Wide Area networks for Internet of Things	The Weightless SIG	OASIS	Object Management Group® (OMG®)	HyperCat/BSI community	Open Connectivity Foundation & AllSeen Alliance	OMA SpecWorks	Eclipse IoT	oneM2M
Descrizione	IEEE è la più importante organizzazione al mondo nell'ambito dell'ingegneria elettrica ed elettronica e delle tecnologie dell'informazione. Scopo dell'IEEE è promuovere l'innovazione e l'eccellenza tecnologica a beneficio dell'umanità favorendo la comunicazione e la collaborazione tra le menti più brillanti del mondo.	IETF (Internet Engineering Task Force) è un organismo internazionale, libero, composto da tecnici, specialisti e ricercatori interessati all'evoluzione tecnica e tecnologica di Internet. Il lavoro in IETF viene svolto da working groups (WG) che si occupano ciascuno di uno specifico argomento e sono organizzati in aree (protocolli applicativi, sicurezza, ecc.), in modo da coprire tutte le aree scientifiche e tecnologiche della rete. Il frutto del lavoro di ogni WG si traduce in documenti denominati RFC (Request For Comments) che vengono sottoposti ad un comitato per il loro avanzamento a standard ufficiale.	L'Organizzazione internazionale per la normalizzazione è la più importante organizzazione a livello mondiale per la definizione di norme tecniche.	LoRa Alliance ha l'obiettivo di definire tutte le specifiche necessarie per le applicazioni Long Range wide area a lunga distanza, basso baud rate e ridotto consumo nel settore dell'IoT e del M2M nelle bande 868 MHz e 915 MHz. LoRa Alliance	Il Weightless rappresenta sia il nome dello Special Interest Group (SIG) sia la tecnologia connessa. La tecnologia Weightless è una LPWAN che può operare sia otticamente a lunga distanza, basso baud rate e ridotto consumo nel settore dell'IoT e del M2M nelle bande 868 MHz e 915 MHz. LoRa Alliance	OASIS è un consorzio senza scopo di lucro che promuove lo sviluppo, la convergenza e l'adozione di standard aperti per la società dell'informazione globale.	Object Management Group® (OMG®) è un consorzio di standard tecnologici a livello internazionale, aperto e senza scopo di lucro.	HyperCat è nato come consorzio inglese per creare uno standard interoperabile IoT per industrie e città. Il consorzio non è più operativo e ogni riferimento rimanda ad uno dei partner leader dei progetti del consorzio, la British Standard Institution. BSI è un'azienda che fornisce supporto, certificazioni e il proprio standard IoT, oltre ad una community IoT interna.	All Seen Alliance era una iniziativa nonprofit della Linux Foundation e mirava allo sviluppo di un framework open source che permettesse alle device e alle app di trovarsi e comunicare tra di loro in modo semplice. Il framework si chiamava AllJoyn. La Open Connectivity Foundation (OCF) è il nome che l'Open Interconnect Consortium (OIC) ha assunto dopo che Microsoft e Qualcomm si unirono al gruppo di progetto. Si trattava di un progetto sponsorizzato dalla AllSeen Alliance e che lavorava al progetto IoTivity. Nel 2016 le due entità si sono fuse come OCF. La fusione mirava all'aumento dell'interoperabilità tra i dispositivi connessi di entrambi i gruppi, consentendo il pieno potenziale operativo dell'IoT e rappresentare così un passo significativo verso un ecosistema connesso. I nuovi gruppi uniti collaborano alle specifiche OCF, nonché ai progetti open source IoTivity e AllJoyn.	OMA SpecWorks è il nuovo nome della Open Mobile Alliance (ex-OMA). OMA SpecWorks semplifica la missione e l'operatività di OMA assorbendo anche il lavoro della IPSO Alliance. Il re-branding permette la convergenza identitaria della OMA e della IPSO in un'unica organizzazione globale che pone l'enfasi sulle procedure che aiutano le aziende a sviluppare in modo rapido, efficiente e professionale le specifiche tecniche nei mercati mobili e IoT.	Eclipse IoT è la divisione IoT della Eclipse Foundation, un'organizzazione non-profit il cui fulcro è una comunità globale di persone e aziende concentrata sullo sviluppo di progetti open source.	oneM2M è un consorzio formato principalmente da 8 organizzazioni mondiali di telecomunicazioni, Orea specifiche, standard e certificazioni riguardo le comunicazioni macchina-macchina (M2M).
Partner fondatori	423,000 members in over 160 countries	There is no formal membership, no membership fee, and nothing to sign. By participating, you do automatically accept the IETF's rules, including the rules about intellectual property (patents, copyrights and trademarks).	L'ISO è un'organizzazione indipendente non governativa composta da membri degli organismi nazionali di normalizzazione di 163 paesi.	Cisco, IBM, Kerlink, Semtech, Microchip Technology, Bouygues Telecom, SingTel, Swisscom, FastNet, ed altre ancora.	Neul, Landis+Gyr, Cable & Wireless, and ARM	AIS, ArborText, Avalanche, Computer Task Group, Database Publishing Systems, EBT, Fulcrum, InfoDesign, Information Dimensions, Intergraph, Interact, Open Text, Object Design, Office@ninth, OMS, Oracle, SoftQuad, Xsoft	Hewlett-Packard, IBM, Sun Microsystems, Apple Computer, American Airlines and Data General	Fondatori di HyperCat: DISTANCE, EyeHub, IoTBay, iMOVE, OpenIoT Smart Streets, Stride, col supporto finanziario del governo britannico.	Electrolux, Arepik, Aris International, Cablelabs, Canon, Cisco Systems, GE Digital, Haier, Intel, LG Electronics, Microsoft, Qualcomm, Samsung Electronics and Technicolor	OMA members + IPSO Members	Borland, IBM, MERANT, QNX Software Systems, Rational Software, Red Hat, SUSE, TogetherSoft, Webgain	Formato da associazioni quali ARIB (Giappone), ATIS (USA), CCSA (Cina), ETSI (Europa), TTA (U.S.), TTA (Korea), TTC (Giappone), BBF (Broadband Forum), Continua, H3I (Home Gateway Initiative), the New Generation M2M Consortium - Japan e OMA (Open Mobile Alliance)
Memberships	In funzione del paese, del settore e della tipologia varia tra i 56/anno e i 1806/anno, circa	N.A.	ISO ha un membro per paese. Membri effettivi, membri corrispondenti, membri dell'ufficio: le tasse sono calcolate utilizzando un valore unitario e assegnando un'unità a ciascun membro. Le unità a variano in base alla loro importanza economica (reddito nazionale lordo, esportazioni e importazioni).	Tariffe per anno Istituzioni: gratis Adopter: 3000,005 Contributor: 20.000,005 Sponsor: 50.000,005	Tariffe per anno Foundational: \$44.000 - \$50.000 Supporting: \$11.025 - \$17.650 Contributing: \$1.210 - \$8.825	Costi annuali: \$550-\$75.000	L'accesso alla community è gratuito, previa registrazione. C'è la possibilità di diventare Consulenti. Associato in caso di utilizzo dei sistemi gestionali certificati dall'azienda.	Tariffe per anno: Diamond Member Benefits: \$350.000 Platinum Member Benefits: da \$5.000 a \$50.000 USD, dipende dal numero di dipendenti. Gold Member Benefits: \$2.000 Nonprofit Educational Gold Member Benefits: \$1.000 (si paga solo l'accesso, una tantum) Basic Member Benefits: \$0	Sponsor: \$35,000 Full: \$10,000 Associate: \$5,000 Supporter: \$1,000	Diventare membro della community è gratuito. Le aziende possono aumentare il loro status di membro della comunità pagando delle rate annuali dai \$5000 ai \$250.000 dollari in base al tipo di azienda e allo status richiesto	Per diventare membri è necessario essere membri di una delle organizzazioni partner di tipo 1: ARIB, ATIS, CCSA, ETSI, TTA, TSDSI, TTA, TTC.	
Licenze	The terms and conditions of IEEE	IP Rights	Copyright Watermark Single User Licence Electronic copies Paper copies Codes and Graphical Symbols (and their Collections) Termination Limitations Governing Law	Eclipse Public License per il protocollo. Vedi tabella annessa.	License: For terminals and related products a royalty-free regime is used. For base stations a 'Free, Reasonable and Non-Discriminatory' (FRAND) regime is in place.	Vedi: Oasis IPR details	BYLAWS P&P OMC IPR POLICY ANTITRUST POLICY OMC TRADEMARKS, LOGOS, AND COPYRIGHTED MATERIAL. REQUESTS FOR USE COPYRIGHT OMC'S PRIVACY POLICY LINKS TO THIRD PARTY SITES CONTENT DISCLAIMER AND LIMITATION OF LIABILITY	Le aziende che aderiscono a OCF come membro possono certificare i dispositivi UPnP senza costi aggiuntivi, ma devono firmare il Contratto di certificazione e certificazione UPnP (CTLA).	Le aziende che non aderiscono a OCF possono diventare un Licenziatario non membro ai sensi del Contratto di certificazione e certificazione UPnP (CTLA). Le aziende devono completare il Contratto di certificazione UPnP e il Contratto di licenza (CTLA). Il Modulo di richiesta e pagare la tassa annuale di licenza (\$ 5.000 USD).	Prevalentemente Open-Source	I oneM2M Partners Type 1 (ARIB, ATIS, CCSA, ETSI, TTA, TSDSI, TTA, TTC) possiedono congiuntamente i copyright sulle specifiche tecniche e i report tecnici sviluppati e approvati all'interno di oneM2M.	
Attività inerenti IoT	IEEE 802.3 Ethernet IEEE 1901 - Broadband over Power Line Networks IEEE 802.15.4e - IEEE Standard for Local and metropolitan area networks IEEE 802.15.4g - Physical Layer (PHY) IEEE 802.11 - WiFi	DTLS - Datagram Transport Layer Security UDP - User Datagram Protocol IPv6 - Internet Protocol, Version 6 CORE is providing a framework for resource-oriented applications intended to run on constrained IP networks. ROLL - Routing Over Low power and Lossy Networks CoAP - Constrained Application Protocol 6LoWPAN - IPv6 over Low power Wireless Personal Area Networks XMPP - Extensible Messaging and Presence Protocol - XMPP IoT HTTP - Hypertext Transfer Protocol	ISO/IEC 30141:2018 Preview: Internet of Things (IoT) - Reference Architecture ISO/IEC JTC 1/ISWG 5 ISO/IEC TR 22417:2017 Preview: Information technology - Internet of things (IoT) use cases	Protocol: LoRaWAN network protocol	Protocol: Weightless-N	OASIS Advanced Message Queuing Protocol (AMQP) Bindings and Mappings (AMQP-BINDMAP) TC - Defining bindings and mappings of AMQP wire-level messaging protocol for real-time data passing and business transactions. OASIS Advanced Message Queuing Protocol (AMQP) TC - Defining a ubiquitous, secure, reliable and open internet protocol for handling business messaging. OASIS Classification of Everyday Living (COEL) TC - Providing a privacy-by-design framework for behavioral data collection and processing. OASIS Message Queuing Telemetry Transport (MQTT) TC - Providing a lightweight publish/subscribe reliable messaging transport protocol suitable for communication in M2M/IoT contexts where a small code footprint is required and/or network bandwidth is at a premium. OASIS Open Building Information Exchange (OBIX) TC - Enabling mechanical and electrical control systems in buildings to communicate with enterprise applications	Incantata sugli standard per l'Industrial Internet of Things (IIoT). In particolare evidenzia il Data-Distribution Service for Real-Time Systems (DDS) che rappresenta il primo standard internazionale middleware aperto che affronta direttamente il publish-subscribe comunicazioni per il real-time ed embedded systems. OASIS è anche il direttivo dell'Industrial Internet Consortium (IIC)	BSI propone uno standard IoT basato sulla loro community interna. A chi adotta questo standard BSI fornisce servizi di testing e certificazione. Vengono forniti inoltre corsi introduttivi per chi si avvicina al loro standard IoT	- Forniscono specifiche, codice e un programma di certificazione per consentire ai produttori di portare sul mercato prodotti certificati OCF che possano integrare con gli attuali dispositivi IoT e sistemi legacy. - Un framework per l'interoperabilità sicura per più SO, piattaforme, modalità di comunicazione, trasporti e casi d'uso. - Specifiche di bridging OCF per scoperta e connettività in altri ecosistemi. - OCF Security Framework e meccanismi di identificazione. - Le piattaforme di punta sono due prodotti Open Source indipendenti ospitati presso la Linux Foundation: IoTivity e AllJoyn. Consentono ai produttori di progettare prodotti e innovare nuove applicazioni utilizzando il codice e le specifiche OCF, astrandosi dal tipo di trasporto fisico o sistema operativo al fine di massimizzare interoperabilità e dimensione del mercato.	Key OMA SpecWorks enablers for IoT devices and services include OMA Device Management (DM), and its Management Objects OMA DM Gateway Management Object OMA DM Firmware Update Management Object OMA M2M Device Classification OMA LightweightM2M (LwM2M) protocol OMA Converged Personal Network service OMA Open Connection Manager API OMA Generic Open Terminal API Framework (GoAP)	- Eclipse Edge, API di alto livello per la gestione di microcontroller. - Eclipse Paho, un'implementazione del protocollo MQTT. - Eclipse Wakama ed Eclipse Leshan, basati sul protocollo OMA LWM2M. - Eclipse Cura, un middleware IoT. - Eclipse SmartHome, un gateway orientato alla domotica. - Eclipse adiac, un'infrastruttura basata sullo standard IEC 61499 pensata per le aziende. - Eclipse Kapua, piattaforma modulare per la gestione di apparecchi IoT. - Eclipse OM2M, piattaforma IoT per aziende basata sulla specifica oneM2M. - Eclipse Hono, delle API per la comunicazione di dispositivi IoT con altri protocolli, con possibilità di estenderlo con altri protocolli. - Eclipse Mosquitto, un'implementazione di un broker MQTT. - Eclipse hawkbit, sistema di gestione per gli aggiornamenti dei dispositivi IoT.	Creazione di specifiche riguardo protocolli di comunicazione (MQTT, CoAP, HTTP, OIC, LWM2M Interworking, oneM2M - AllJoyn Interworking, etc)
Note	Il consorzio HyperCat è scomparso a favore dell'azienda BSI											
Riferimenti	https://www.ieee.org/membership/ordues.html	https://www6.ietf.org/newcomers.html	https://www.iso.org/	https://www.oasis-open.org/commit	https://www.omg.org/	https://www.bsigroup.com/en-GB/	https://www.omaspecworks.org	http://www.oneM2M.org/	http://www.oneM2M.org/about-oneM2M/intellectual-property-rights			

Table 1: Confronto Alleanze/Consorzi dell'ecosistema IoT - Core / Communication / Messaging - Multilayer / Stack

Tipologia	Connected body / Home - Industrial IoT & Connected Buildings / Lighting				Infrastructure		Industry Marketing / Education Focused		Project/Ideas/Studies Aggregators		
Consorzio / Alleanza											
	Continua & PCH Alliance	Thread Group	Industrial Internet Consortium	EnOcean Alliance	GSMA - Global System Mobile Association	IoT World Alliance	The Internet of Things Consortium	International m2m council	IoT European Research Cluster	IOT-Council	AIOTI
Nazionalità	Internazionale / USA	Internazionale / USA	Internazionale / USA	Internazionale / USA		Internazionale	Internazionale / USA	Internazionale / EU / GB	Europa	Internazionale / Europa	EU
Descrizione	Continua è nato come un consorzio indipendente, ora è un insieme di linee guida della Personal Connected Health Alliance finalizzato alla creazione di un framework standard dove creare uno scambio sicuro di dati medici.	Thread è un protocollo di comunicazione wireless per i prodotti IoT orientato alla sicurezza e al basso consumo energetico basato sullo standard IEEE 802.15.4. Ha certificato vari prodotti di vari venditori che implementano il protocollo Thread.	L'Industrial Internet Consortium* (IIC™) è un consorzio del Object Management Group formatosi per creare un efficiente IoT attraverso l'analisi di casi d'uso di problemi concreti e progetti di test per tecnologie con applicazioni nel mondo reale. Da gennaio 2019 ingloba anche il consorzio OpenFog per il fog computing.	EnOcean è un'alleanza che fornisce standard per la creazione di reti wireless con device a bassa manutenzione. Gli standard coprono i livelli OSI 1-2-3 (fisico, data link e networking).	La GSMA è un'associazione mondiale che rappresenta gli interessi degli operatori mobili di tutto il mondo ed è il più ampio ecosistema globale tra aziende di telecomunicazioni per fornire ai propri clienti una connessione per dispositivi IoT unica globale.	IoT World Alliance è una partnership globale tra aziende di telecomunicazioni per fornire ai propri clienti una connessione per dispositivi IoT unica globale.	IoT World Alliance è il nuovo nome della M2M World Alliance. Ora conta varie aziende di telecomunicazioni da tutto il mondo.	IoT World Alliance è un consorzio che fornisce un insieme di best practices e un ambiente collaborativo a tutti i suoi membri. Rispetto alle altre organizzazioni, ha un programma di affiliazione più snello ed economico e quindi un più alto numero di utenti.	Imc è un consorzio che fornisce un insieme di best practices e un ambiente collaborativo a tutti i suoi membri. Rispetto alle altre organizzazioni, ha un programma di affiliazione più snello ed economico e quindi un più alto numero di utenti.	IERC si propone come punto d'incontro tra i vari progetti di ricerca europei sull'IoT, per rendere possibile la comunicazione tra loro e quindi l'ottimizzazione delle risorse.	IOT-Council è un thinktank in cui scambiarsi informazioni sull'IoT e sui cambiamenti in corso nel mercato e promuovendo standard interoperabili.
Partner fondatori	BodyMedia, Cisco Systems, GE Healthcare, IBM, Intel, Kaiser Permanente, Medtronic, Motorola, Nonin Medical, Omron Healthcare, Panasonic, Partners HealthCare, Polar Electro, Royal Philips Electronics, RMD Networks, Samsung Electronics, Sharp, The Tensil Group, Welch Allyn, Zensys	Arm, Nest, Somfy, Big Ass Fans, Samsung, Tyco, Freescale, Silicon Labs, Yale	AT&T, Cisco, GE, Intel, IBM	General Electric, Lutron, Osram, Panasonic, Philips, and Toshiba	Più di 750 operatori con oltre 400 aziende		Attualmente 50+ membri				
Memberships	Continua non prevede una propria comunità, ma è possibile diventare membri della PCH Alliance con un costo annuale dal \$1,500 ai \$50,000 in base al tipo di benefit richiesti	\$0 per i membri accademici \$750 Affiliate \$5,000 Implementer \$15,000 Contributor \$65,000 (+\$35,000 all'iscrizione) Sponsor	Founder \$150K, Contributing \$150K, Industry (>\$50M) \$50K, Small industry \$5K, Academic or non-profit \$2.5K, Government \$12.5K	Associate: \$500 ogni due anni Participant: \$6,000 Promoter: \$35,000	*Reported Annual Turnover Figure in USD 0 - 50 million 50 - 100 million 100 - 250 million 250 - 500 million 500 - 700 million >700 million	Annual Contribution in USD 13000,00 18000,00 31000,00 62000,00 93000,00 124000,00	Nessuna informazione al riguardo, ma nel corso del tempo si sono uniti nuovi membri, possibili che accettino candidature	Per le aziende che vogliono aderire come General Member la quota annuale dipende dal fatturato, per la startup dagli investimenti ottenuti. Per i singoli o per le aziende che vogliono aderire come Participant, la quota è gratuita	Adopter Members: Grati Sustaining Members: dai €5,000 ai €15,000 in base ai dipendenti Affiliate Members: pensato per giornalisti e analisti, è gratuito ma richiede promozione via social network e email.	Non viene indicato come far parte dei progetti del cluster	Per diventare membri bisogna contattare la mail indicata nel sito e chiedere di essere inseriti
Licenze		Le tecnologie sono disponibili su licenza RAND-RF (reasonable and non-discriminatory, royalty-free) tra i vari membri. L'utilizzo gratuito delle tecnologie protette da copyright è subordinato all'essere almeno Contributor e aver ottenuto la certificazione per la tecnologia richiesta	Non presenti								
Attività inerenti IoT	Creazione di una serie di linee guida per lo scambio sicuro di dati medici tra i vari apparecchi utilizzando un'interfaccia di trasmissione unificata che sfrutta protocolli SOAP e REST e tecnologie per il trasporto dei dati quali NFC, Bluetooth, ZigBee e USB. Vengono inoltre messe a disposizione certificazioni che attestano il rispetto degli standard delle linee guida	Certificazione di apparecchi di trasmissione a basso consumo energetico orientati alla sicurezza. Creazione di reti wireless da 250/300 dispositivi	IIC non rilascia certificati ma analizza use case e crea banchi di prova per progetti concreti proposti dai suoi membri, rilasciando raccomandazioni al termine dei progetti. Collabora inoltre con vari consorzi e associazioni, alcuni presenti in questo documento	EnOcean fornisce standard (ISO/IEC 14543-3-1X) per reti wireless ottimizzate per gli edifici (raggio 30m). L'alimentazione dei dispositivi viene data dallo sfruttamento dell'energia generata da cambiamenti di luce, temperatura e movimento, rendendo i dispositivi a lunga durata senza bisogno di un potente sistema di batterie o di una continua manutenzione.	Il programma Internet of Things di GSMA è un'iniziativa del settore progettata per aiutare gli operatori di telefonia mobile ad accelerare l'erogazione di soluzioni IoT convincenti e sicure che sfruttano i Big Data per creare valore. Tra le iniziative vi sono quelle legate al: Mobile IoT - mira ad aumentare la conoscenza e la conoscenza sulle L'WPA IoT Security - linee guida sulla sicurezza IoT IoT Big Data - armonizzazione dei dati attraverso le comuni API (Application Program Interface) Politica e regolamento IoT - politica sostenibile e un ambiente normativo per supportare la scalabilità dell'IoT Smart Cities - sostegno agli operatori di telefonia mobile e alle città per collaborare. Veicoli connessi - regolamentazione per accelerare la crescita del mercato dei veicoli connessi concordando un approccio comune alle soluzioni di sicurezza, di regolamentazione e di connettività di rete Droni - Le reti mobili possono essere utilizzate per identificare in modo sicuro un drone e la sua posizione, al fine di garantire la sicurezza dei droni commerciali e contribuire a mitigare i rischi di privacy, sicurezza e sicurezza.	IoT World Alliance si propone di fornire un servizio di comunicazione globale (piani tariffari che coprono più possibile il globo e che rispettino le regolamentazioni globali, con una piattaforma unificata per la gestione dei dispositivi IoT)	IoT World Alliance offre una rete di comunicazione tra partner interessati al mondo IoT. La comunicazione viene promossa attraverso meeting, comitati con tutti i membri e report mensili incentrati su analisi di mercato, analisi delle tecnologie e analisi dei clienti	Fornisce un ambiente di cooperazione tra varie realtà differenti nel mondo dell'IoT: i membri fondatori più grossi forniscono le proprie tecnologie e sistemi, i membri più piccoli possono utilizzarle per creare progetti su larga scala, che da soli sarebbero ingestibili		Accesso alla "Council List" dove è possibile scambiare informazioni riguardo all'IoT. Promozione di eventi IoT nel mondo, tra cui il proprio "today".	Coordinatione e mappatura dei membri, promozione di standard interoperabili, valutazioni del mercato IoT. Progetto finanziato dalla Commissione Europea
Note									I progetti del cluster sono attuali ma il sito sembra non aggiornato dal 2016		
Riferimenti	https://www.pchalliance.org/about-continua	https://www.threadgroup.org/	https://www.iiconsortium.org/faq.htm	https://www.enocean-alliance.org/		http://www.iotworldalliance.org	https://iothings.org/	https://www.idm2mcouncil.org/	http://www.internet-of-things-research.eu/index	https://www.theinternetofthings.eu/	https://aioti.eu/

Table 2: Confronto Alleanze/Consorzi dell'ecosistema IoT - Connected body / Home - Industrial IoT & Connected Buildings / Lighting - Infrastructure - Industry Marketing / Education Focused

6 IoT technologies/platforms

For *IoT* technologies there is a heterogeneity of platforms and consequently many different standards and approaches, in fact often the technologies as a whole are seen indiscriminately and altogether as platforms. As can be seen today the *IoT* landscape is chaotic and until there is an internationally accepted standardization this is not destined to change. In fact, there are many protocols, many standards and too many revolutions.¹⁷

In Figure 8, inspired by the article “The *Internet of Things* Protocol Stack – from sensors to business value” by Antony Passernard in 2014¹⁷, they tried to give an order and a structure to the *IoT* world, but it turns out to be one of the many non-exhaustive photographs of the situation, however, it manages to show the complexity and extension that underlies the *IoT*. Obviously today it is to be updated, but it represents well the idea of the complexity of the protocol landscape of the *Internet of Things* world.

Resuming the definition given by Gartner “the *IoT* is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment”, which, condensing it with the other definitions given the *IoT* is a set of physical devices interconnected through the Internet and other types of networks through a unique identifying IP address, (whose data is collected and communicated through a set of sensors, electronics and dedicated Software)¹⁸. The *IoT* covers an ensemble of components and is applicable to a huge sphere of applications both of common and industrial life. In fact, under the term of *IoT* we include what can be defined as the *Consumer Internet of Things (CIoT)* and the *Industrial Internet of Things (IIoT)*¹⁶. In this analysis we are not going to distinguish the two categories as both the *CIoT* and the *IIoT* represent sets of applications and use cases that overlap in any case with difficult distinctions, and the technologies and paradigms used are often the same, if not in very specific or critical areas.

In this we identify 7 common elements¹⁹:

Connectivity. Devices and sensors need to be connected to each other, with actuators, processes through the internet or other networks.

Objects (Things). They represent everything that can be identified, connected or thought to be connected, sensors, appliances, animals, industrial equipment. Devices may contain sensors or detection materials that can be connected to devices and items.

The data. They represent the fundamental element and they unite the whole world of the *Internet of Things*, they represent the first step towards actions and intelligence.

1 ¹⁷ <https://entrepreneurshiptalk.wordpress.com/2014/01/29/the-internet-of-thing-protocol-Stack-from-sensors-to-business-value/> (last visit 30/4/2019 at 13.00)

1 ¹⁸ <https://www.i-scoop.eu/internet-of-things/> (last visit 7/1/2019 at 11.00)

1 ¹⁹ https://www.i-scoop.eu/internet-of-things-guide/#The_origins_of_the_Internet_of_Things_how_it_all_started (last visit 7/1/2019 at 11.00)

Communication channels. All the devices (*Device*) must be connected and must exchange data which could then be further analysed.

The intelligence. Understood as the sensorial and deriving capacity of the analysis of the data, to also consider aspects of Artificial Intelligence.

The implementation. The result of intelligence. It can be derived from manual commands, from a sequence of predefined actions according to the phenomenon identified or be completely automated. It is the final result of the activity of an *IoT* platform.

The ecosystem. Everything about the *IoT*.

	Device Management				Business Processes				Analytics			Security and Privacy	
Business Apps	Asset Mgt.		Firmware Mgt.		Efficiency gain		Marketing / Sales		Machine Learning				
	Device Provisioning		Device Registration		Support				AI	DataMining			
	Remote Control								Data Analysis				
									Visualizzation Eng.				
Business Model	Open		Indirect	Integrate	Cloud	On demar	On Premise	Platform	Direct	Closed			
Data Storage / Retrieval					Hadoop	HBase	Cassandra	MongoDB	Postgress				
Data Aggregation / Processing	Scribe				RapidQM	Flume	Kafka	Storm	Luxun	Fluentd			
Session /Communication	Coap	DDS	XMPP	HTTP	Telnet	MQTT	DDS	AMQP	FTP	SSH	NATS		
Transport					IPv4	6LoWPAN		IPv6	RPL				
Link Protocol Layer	BLE	Bluetooth		RFID	Wifi	802.11	Zigbee	CDMA	GSM	Ethernet	802.14.4e	DASH7	LoRa/LoRaWan
	Sigfox	INGENU	LTE	NB-IoT									
Connectivity	ODB2		PLC	RS-232	RS-485	Modbus	Wireless	USB	SPI	RJ45			
	Device						Smart Gateways						
	Sensors												

Figure 8: Panorama dei protocolli per l'IoT dai dispositivi al mercato.

6.1 From small to large distances

For WANs (Wide Area Networks) in recent years we have seen the attempt by mobile cellular systems to develop protocol standards that allow low consumption of devices and long-life batteries (at least 10 years). Given the delays in issuing standards (by 3GPP), new proprietary protocols and Lpwa (Low Power Wide Area) applications have been

created that operate on unlicensed spectral bands: LoRa, Sigfox, Weightless, etc. The Lpwa protocols (identified as "*Cellular Like radio*") guarantee the low consumption of the devices, operation at low capacity (up to some tens of kbit/s), and allow low cost solutions, great coverage and prompt availability.

For the applications on the MAN (Metropolitan Area Network), in competition with the Lpwa protocols, there are first two standards derived from successful LAN protocols: the Wireless MBus (at 169 MHz) and WiFi: the latter was developed for the *IoT* and is called WiFi HaLow.

To counter the success of the Lpwa protocols, 3GPP recently announced two new cellular standards for the *IoT*: the most awaited is based on the Lte and is called Nb-*IoT* (narrowband *IoT*) with 180 KHz channels and up to 250 kbit/s capacities, while the other is based on the GSM and is called Ec-gsm (Extended Coverage GSM).

For slightly wider band *IoT* applications, both the Lte-M protocol (renamed: eMtc, enhanced Machine Type Communication) with 1.4 MHz channels and 1 Mbit/s band, both the Lte-Cat1 protocol and the up to 10Mbit/s capabilities are confirmed.

The application sectors of the *IoT* are innumerable and can be classified into two large application clusters.

Massive *IoT*: applications are characterized by low cost, low consumption, and low communication capacity, as well as by a large number of devices connected and focused in the sectors:

transport and logistics, environment, smart home, smart city, agriculture, etc.

Mission Critical *IoT*: applications are characterized by high reliability, low latency and high capacity, focused on applications in sectors such as:

automotive, energy (smart grid), medicine, security, augmented reality, factory automation, etc.²⁰

6.2 IoT Architecture

By now it has been established that even for architecture there is no single line and there are different ideas and proposals both from the world of research and from that of industry.

The *Internet of Things* has the potential to network a huge number of devices with limited resources and today's *IoT* systems are largely based on the use of TCP/IP protocols, in particular IPv6. However, the TCP/IP protocol *stack* was not originally designed for *IoT* environments.²¹

The many associations and consortia established in recent years (see paragraph 5.1), in addition to the existing ones that also operate in other sectors, aim to modify or replace the TCP/IP protocol *stack* in order to adapt to the scenarios of *IoT* distribution. These efforts have led to the extension of existing protocols in the TCP/IP protocol suite and to the

²⁰ A. Capone, G. Verticale, Politecnico di Milano, 2016

development of new protocols. However, the problems do not end here, indeed new ones are born. The most common architectures are shown below.

Figure 9 shows a comparison between a classic IoT *Stack* and the ordinary IP network protocol *stack* with direct reference to the ISO/OSI model. Some of the main application interfaces that are used in the field of typical technologies of the *Internet of Things* can be seen.

All the structures/infrastructures and protocols represented in Figure 9 for data management are obviously not exhaustive.

As mentioned, there is no single general agreement on the architecture of the *Internet of Things* that is shared by the whole world and by researchers. Researchers have proposed many different architectures. According to some researchers, the *IoT* architecture has three levels, other researchers support the four-level architecture. The latter believe that, due to the improvement of the *IoT*, the three-tier architecture cannot meet the requirements of the applications. To address the issue of security and privacy, the five-level architecture has also been proposed, which is considered satisfactory in terms of *Internet of Things* requirements with regard to security and privacy²⁴

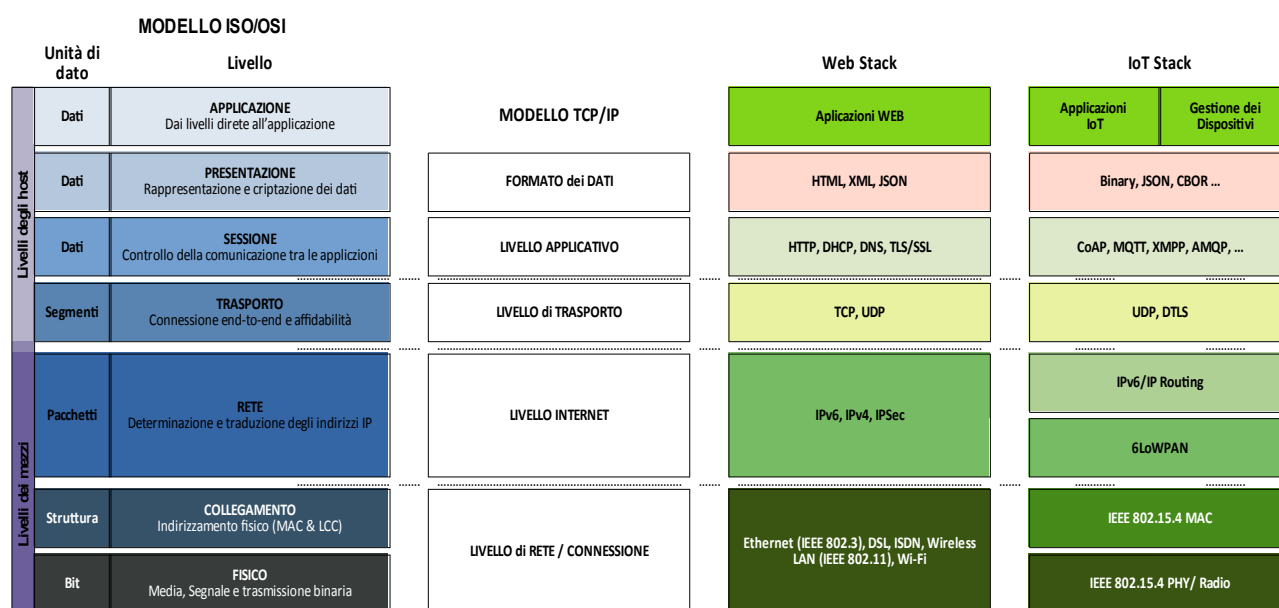


Figure 9: Confronto tra i modelli di interconnessione IoT e Web con riferimento all'ISO/OSI

- 2²¹ Wentao Shang (UCLA), Yingdi Yu (UCLA), Ralph Droms (Cisco Systems Cambridge), Lixia Zhang (UCLA). Challenges in *IoT Networking* via TCP/IP Architecture. NDN Technical Report NDN-0038, 2016. Revision 1: February 10, 2016.
- 2²⁴ Muhammad Burhan, Rana Asif Rehman, Bilal Khan, and Byung-Seo Kim. *IoT Elements, Layered Architectures and Secyurity Issues: A Comprehensive Survey*

6.2.1 Architettura a 3 e 5 livelli

In the previous section, in Figure 9 what is shown is the *IoT Stack*, 1:1 compared with the ISO/OSI model, the levels were considered with the same method. The levels are seen with greater abstraction below.

The simplest and most basic architecture is the 3-layer architecture ^{22 23}:

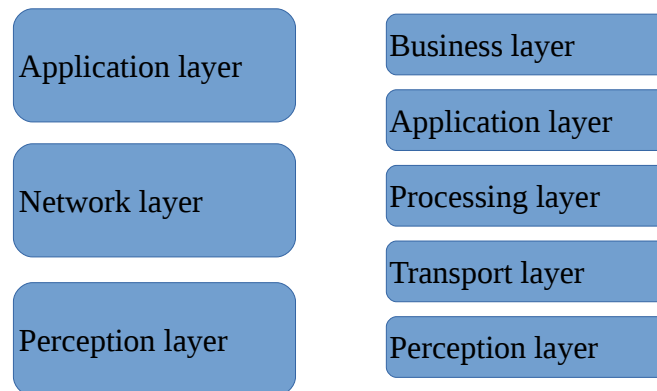


Figure 10: Architecture 3 (A) and 5 (B) layer

- Physical layer: also called perception layer. This is the sensory layer and presents sensors for the detection of information and data from the environment.
- Network layer: the layer that contains the communication and intercommunication between the various intelligent objects (smart things/*Device*), network devices and *Servers*. It also includes data transmission and analysis.
- Application layer: the layer that defines the applicability of the *IoT* and provides the specific services for applications to users.

With the 5-layer architecture, the functionality of the 3-layer architecture is explained further, this is the fundamental representation of the *IoT*. The physical and application layers remain unchanged, while the network layer is expressed in the transport layer, which provides for the connection and management of the communication between the devices and the data, and in the Processing Layer, which processes and analyses the large amount of data received.

6.2.2 Security

As seen the three-layer architecture is a basic architecture and meets the fundamental idea of the *IoT*. It is an architecture developed in the early stages of development of the *IoT* paradigm. Unfortunately, security systems are not always implemented in the various layers to protect against possible attacks. This section contains brief descriptions of the

²² Spyros G. Tzafestas (2018). *The Internet of Things: A Conceptual Guided Tour*. European Journal of Advances in Engineering and Technology, 2018, 5(10): 745-767.

²³ Pallavi Sethi and Smruti R. Sarangi (2016). *Internet of Things: Architectures, Protocols, and Applications*. Journal of Electrical and Computer Engineering - Volume 2017, Article ID 9324035, 25 pages

most frequent attacks possible in the various levels/layers, distinguishing them and integrating them according to the type of architecture (3, 4 or 5 layers).

In a **3-level architecture**, the sensory layer represents the level with the greatest amount of data, data coming from the environment, from things. There are many types of sensors attached to objects to collect information like RFID, 2D barcodes and sensors. The sensors are chosen based on the needs of the applications. The information collected by these sensors may relate to location, changes in the air, the environment, movement, vibrations, health status, etc. Data that in itself can be difficult to analyse and discern, however, they are the main goal of attackers who want to use them to replace the sensor with their own. Therefore, most threats are related to sensors that are part of the **Perception Layer**.²⁴

The common security threats of the level of perception are^{25 26 27}:

Malicious interception: Eavesdropping, often translated as interception but which in the event of a cyber-attack is closer to eavesdropping. This is an unauthorized *real-time* interception in which private communications are intercepted by an attacker. The goal is to steal information that is transmitted over the network. It takes advantage of unsafe transmission to access sent and received information.

Capture of the nodes: a targeted attack to take complete control of a key node in the network is one of the most dangerous attacks on the physical level. The target nodes are usually *gateways* or coordinator nodes, in a *FOG/EDGE* structure they could be the *EDGE* level nodes. It manages to steal all the information, including the communication keys between the sender and recipient and the stored data. Often this attack is associated with the replacement of the node with a fake Node²⁸.

Fake Node and Malicious: This is an attack in which an attacker adds a node to the system and inserts false data. The purpose of this attack is to block the network, overloading data and therefore the overall consumption of the nodes.

Play Back: Also known as *Replay Attack*. In this case the objective is to recover an exchange of data between the sender and receiver and retransmit it so that the attacked device interprets the correct and trusted data chain, guaranteeing access

-
- 2 ²⁴ Muhammad Burhan, Rana Asif Rehman, Bilal Khan, and Byung-Seo Kim. *IoT Elements, Layered Architectures and Secyurity Issues: A Comprehensive Survey*
 - 2 ²⁵ Suo H., Wan J., Zou C., Liu J. *Secyurity in the Internet of Things: A review*; Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE); Hangzhou, China. 23–25 March 2012; pp. 648–651
 - 2 ²⁶ Xiaohui X. *Study on Secyurity problems and Key technologies of the Internet of Things*; Proceedings of the 5th International Conference on Computational and Information Sciences (ICCIS); Shiyang, China. 21–23 June 2013; pp. 407–410
 - 2 ²⁷ Kozlov D., Veijalainen J., Ali Y. *Secyurity and privacy threats in IoT architectures*; Proceedings of the 7th International Conference on Body Area Networks; Oslo, Norway. 24–26 February 2012; Brussels, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering); 2012. pp. 256–262
 - 2 ²⁸ Bharathi M.V., Tanguturi R.C., Jayakumar C., Selvamani K. *Node capture Attack in Wireless Sensor Network: A survey*; Proceedings of the 2012 IEEE International Conference on Computational Intelligence & Computing Research (ICCIC); Coimbatore, India. 18–20 December 2012; pp. 1–3

to the data required by the malicious connection. In addition to the recovery of any credentials, the need to decrypt the data is a characteristic of this attack²⁹.

Time Attack: a cryptographic method defined as a time attack. It is a side channel attack in which the attacker attempts to compromise a cryptographic system by analysing the time taken to execute cryptographic algorithms. It is usually used in devices that have weak computational capabilities. It allows the attacker to discover vulnerabilities and extract access data maintained in the security of a system, observing how long the system takes to respond to different requests, inputs or cryptographic algorithms³⁰.

The network layer connects and manages the data flow between the physical level and the application level. Given its characteristics it is highly sensitive to attacks. Being responsible for the data entrusted to it, security becomes fundamental as regards the integrity and authentication of information carried on the network.

The threats and common safety problems to the network layers are:³²

Denial-of-Service (DoS) attack: aims to obtain a service interruption that usually occurs when an IT infrastructure component is overloaded. The operation takes place by intentionally sending more requests to a target system than it can answer. A DoS attack is an attack that prevents authentic users from accessing devices or other network resources

Man-in-The-Middle attack (MitM): abbreviated also in literary form as MIM, MiM, MitM, MitM or MITMA, it is a sort of attack in which a malicious third party secretly takes control of the communication channel between two or more *End-points*. The MITM aggressor can intercept, modify, change or replace the communication traffic of the victims (this distinguishes an MiTM from a simple interception). Furthermore, the victims are unaware of the intruder, believing that the communication channel is protected. The MiTM attack can be performed on different communication channels such as GSM, UMTS, Long Term Evolution (LTE), Bluetooth, Near Field Communication (NFC), Wi-Fi, etc. The objectives of the attack are not only the actual data flowing between the end points, but also the confidentiality and integrity of the data itself. Since the attacker controls communication, he can change messages according to his needs. This poses a serious threat to online security because it allows the attacker to capture and manipulate information in real-time.³²

- *Storage attack*: user information is stored on storage devices or in the *Cloud*. Both storage devices and the *Cloud* can be attacked by the attacker and user information can be changed to incorrect details. Replication of information associated with

2 ²⁹ <https://www.kaspersky.com/resource-center/definitions/Replay-Attack> (last visit 18/02/2019 at 18.00)

3 ³⁰ Brumley D., Boneh D. Remote timing attacks are practical. *Comput. Netw.* 2005;48:701–716. doi: 10.1016/j.comnet.2005.01.010.

3 ³² Burhan M., Rehman R., Khan B., Kim B.S. *IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey*. *Sensors*. 2018;18:2796. doi: 10.3390/s18092796. [[PMC free article](#)] [[PubMed](#)] [[CrossRef](#)] [[Google Scholar](#)]

access to other information by different types of people offers more possibilities for attack.³²

Exploit based Attack: An *Exploit* is any immoral or illegal attack in the form of *Software*, data blocks or a sequence of commands. It exploits the security vulnerabilities of an application, system or *hardware*. It usually aims to gain control of the system and steal information stored in a network.³³

As seen **the application layer** defines all the applications they use and which are used for the *IoT*. It is responsible for providing services to the applications. Data can be disparate and usually comes from sensors that have low computing capacity and *Storage*, so they cannot afford high levels of security.

The most common security problems are due to:

- *Cross Site Scripting:* is an *Injection Attack*. It allows an attacker to insert a *Client-side script*, such as *JavaScript* into a trusted site visited by different users. In doing so, an attacker can completely change the content of the application according to his needs and use the original information illegally, for example by retrieving the access data, downloading the user's navigation data, etc.³⁴
- *Malicious Code Attack:* is a code in any part of the *Software* intended to cause unwanted effects and damage to the system. This is a type of threat that cannot be blocked or controlled by the use of antivirus tools. It can be activated or be like a program that requires the user's attention to perform an action.³²
- *The ability to manage the massive data:* due to a large number of devices and an enormous amount of data transmission between users, the victim is not able to manage the processing of data according to needs. This leads to network disturbances and data loss³². In this case it is not stated that there is an attack but it could simply be an operational problem. Obviously if conditions were imposed through the inclusion of fraudulent nodes in the network then it would certainly be an attack.

Due to the ongoing development of the *IoT*, the 3-layer architecture has shown significant limitations. Therefore, the ITU-T (*International Telecommunications Union-Telecommunication Standardization Sector*) proposed an **architecture** composed of **four layers**; the first top layer or first layer is the *IoT* application layer that contains the application user interface, the second layer is the services and application support level, the third layer is the network layer that contains the capabilities of network and transport, the lower level is the device level, which contains the *Gateways*, the *Hardware* and the sensors, and the RFID tags and others. The security and management capabilities and functions are distributed along the four levels.

3 ³³ *Exploit Attack in Network Layer*. <http://searchsecurity.techtarget.com/definition/Exploit> (ultima visita 22 gennaio 2019)

3 ³⁴ Gupta S., Gupta B.B. Cross-Site Scripting (XSS) attacks and defence mechanisms: Classification and state-of-the-art. *Int. J. Syst. Assur. Eng. Manag.* 2017;8:512–530. doi: 10.1007/s13198-015-0376-0.

Compared to the previous architecture, it also has the support level, located between the application level and the network level. Figure 11 shows the levels with the possible countermeasures for security. As you can see, the level of support acts as a buffer, avoiding passing threats through the network to the sensory layer, in fact it has two responsibilities:

confirmation that the information is sent by authentic users and protected from threats, for example through authentication.

sending information to the network level. The means to transmit information from the support level to the network level can be *Wireless* and wire-based. As with the 3-layer structure, there are various attacks that can affect this level, such as DoS attacks, malicious *insiders*, unauthorized accesses, etc...

Application Layer	Authentication/Key Agreements	Privacy Protection
↓		
Support Layer	Secure Cloud Computing / Computing	Antivirus
↓		
Network Layer	Identity Authentication	Encryption Mechanism
↓		
Perception Layer	Encryption and Key Agreement	Sensor Data Protection

Figure 11: Architecture in 4 levels and related useful security mechanisms

Common threats and problems of the level of support are:

the DoS attack: is carried out in the same manner already described;

The Malicious Insider Attack: occurs from within an *Internet of Things* environment to access users' personal information. It is run by an authorized user to access information from other users. This is a very different and complex attack that requires different mechanisms to prevent the threat ^{35 36 32}

To overcome security issues regarding data storage, the researchers proposed a **five-layer architecture** so as to further secure the *Internet of Things* ^{37 38 39}. In this architecture (figure 10), compared to the 3-layer one, the network layer has been completely replaced with the support level and the new processing level (the *Processing layer*). The *Business*

- 3 ³⁵ Sanzgiri A., Dasgupta D. Classification of insider threat detection techniques; Proceedings of the 11th Annual Cyber and Information Security Research Conference; Oak Ridge, TN, USA. 5–7 April 2016; New York, NY, USA: ACM; 2016. p. 25
- 3 ³⁶ Nurse J.R., Erola A., Agraftis I., Goldsmith M., Creese S. Smart insiders: Exploring the threat from insiders using the Internet-of-things; Proceedings of the 2015 International Workshop on Secure Internet of Things (SIoT); Vienna, Austria. 21–25 September 2015; pp. 5–14
- 3 ³⁷ Madakam S., Ramaswamy R., Tripathi S. Internet of Things (IoT): A literature review. J. Comput. Commun. 2015;3:164. doi: 10.4236/jcc.2015.35021
- 3 ³⁸ Khan R., Khan S.U., Zaheer R., Khan S. Future Internet: The *Internet of Things* architecture, possible Applications and Key challenges; Proceedings of the 2012 10th International Conference on Frontiers of Information Technology (FIT); Islamabad, India. 17–19 December 2012; pp. 257–260.
- 3 ³⁹ Sethi P., Sarangi S.R. Internet of Things: Architectures, Protocols, and Applications. J. Electr. Comput. Eng. 2017;2017:9324035. doi: 10.1155/2017/9324035

layer has been added to the Application level. In this architecture, all the requirements of the *IoT* have been closely approached, including safety.

The Processing Layer is a *Middleware* level. It collects information sent from a transport layer and processes the information collected. It has the responsibility of eliminating the extra information that has no meaning and extracts useful information. Moreover, it also eliminates the problem of the large mass of data generated by *IoT* structures, improving their performance.³²

This level is subject to various types of attacks that can affect the functioning and the level of processing.

The common attacks are:³²

Exhaustion: an attacker uses exhaustion to disturb the processing of the Internet of Things structure. the attack is executed like the DoS attack, in which an attacker sends the victim many requests so as to make the network unavailable to users. It could be the result of other attacks that aim to exhaust system resources, such as battery and memory resources. The *IoT* having a distributed nature can, if well configured not to be seriously damaged by this type of attack, so it turns out to be low risk.⁴⁰

Malware: is an attack on the confidentiality of user information. It refers to the application of viruses, *Spyware*, *Adware*, Trojan horses and *Worms* to interact with the system. It takes the form of executable codes, *scripts* and content. It acts against the requirements of the system to steal confidential information⁴¹.

The level of business refers to the intended behaviour of an application and acts as a manager of an entire system. It has the responsibility of managing and controlling the applications, the business, and the profit models of the *Internet of Things*. User privacy is also managed by this level. It also has the ability to determine how information can be created, stored and modified. The vulnerability of this level allows attackers to abuse an application by avoiding the business logic. Most of the safety issues are weaknesses in an application resulting from a deficient safety check.

Common problems with regard to the Business Layer Security are:³²

Logic attack: exploits a programming flaw. Controls and manages the exchange of information between a user and an application support database. There are several common defects in the business layer, such as improper coding by a programmer, validation of password recovery, input validation and encryption techniques⁴².

⁴⁰ Ashraf Q.M., Habaebi M.H. Autonomic schemes for threat mitigation in *Internet of Things*. J. Netw. Comput. Appl. 2015;49:112–127. doi: 10.1016/j.jnca.2014.11.011

⁴¹ Andrei Costin, Jonas Zaddach. *IoT Malware: Comprehensive Survey, AnalysisFramework and Case Studies*

⁴² <https://whatistechtarget.com/definition/business-logic-Attack> (last visit 15/01/2019 at 16.00)

Zero-Day Attack: refers to a security gap or a problem in an application that is unknown to the vendor. This security flaw is exploited by the attacker to take control without the user's consent and without his knowledge.

In addition to these architectures there are also 7 levels, the *Cloud*, *FOG* and *EDGE*, in general the most common types of attacks remain those described.

6.2.3 Architectures based on Cloud, FOG and EDGE

By "*Cloud Computing*" (computational cloud) in simple words we mean the distribution of calculation services, such as *Server*, storage resources, *Database*, network, *Software*, analysis, "*Business Intelligence*" and others, via the Internet ("the *Cloud* ")⁴³. This structure allows rapid updates and flexibility even in scalability. As usual there are also different definitions for "*FOG Computing*" and in some of these "*EDGE Computing*" is confused or integrated. However, the term "*FOG Computing*" was coined by CISCO Systems to define a new model to facilitate *Wireless* data transfer to distributed devices in the *Internet of Things (IoT)* paradigm. Cisco defines *FOG Computing* as a paradigm that extends *Cloud Computing* and services related to peripheral devices on the network. As in the case of the *Cloud*, the *FOG* provides data, processing, archiving and services to the end user. The distinctive features of the *FOG* are its proximity to end users, its dense geographical distribution and its support for mobility. In this way, fog reduces service latency and improves QoS (*Quality of Service*), resulting in superior user experience. *FOG Computing* supports the emerging applications of the *Internet of Everything (IoE)* that require near-zero and/or predictable latency (industrial automation, transport, sensor networks and actuators). Thanks to its wide geographical distribution, the *FOG* paradigm is ideal for managing *real-time big data* and *real-time* analysis. The fog supports densely distributed data collection points, so it adds a fourth axis to the size of *Big Data*⁴⁴. In 2015 ARM, Cisco, Dell, Intel, Microsoft and Princeton University founded the "*OpenFog Consortium*" to promote and accelerate the adoption of *Open FOG computing*. The *OpenFog Consortium* defines *FOG computing* as: "*FOG computing is a horizontal architecture at system level that distributes computing, archiving, control and networking resources and services anywhere along the Cloud of Things continuum*".

Yi et al.⁴⁵ have defined *FOG computing* as: "*FOG computing is a geographically distributed computing architecture with a resource pool consisting of one or more ubiquitously connected heterogeneous Devices (including EDGE Devices) at the EDGE of network and not exclusively seamlessly backed by Cloud services, to collaboratively provide elastic computation, Storage and communication (and many other new services and tasks) in isolated environments to a large scale, collaboratively provide elastic computation, Storage and communication (and many other new services and tasks) in isolated environments to a large scale of Clients in proximity*". Aazam et al. ⁴⁶ gave the following

⁴³ <https://azure.microsoft.com/it-it/overview/what-is-Cloud-computing/> (last visit 15/01/2019 at 14.10)

⁴⁴ <https://blogs.cisco.com/perspectives/IoT-from-Cloud-to-FOG-computing>

⁴⁵ Yi, Z. Hao, Z. Qin, and Q. Li, "FOG computing: Platform and Applications," in IEEE WorksHop on Hot Topics in Web Systems and Technologies (HotWeb) , Washington, DC, USA, November 2015, pp. 73–78

definition: "FOG computing refers to bringing Networking resources near the underlying networks. It is a network between the underlying network(s) and the Cloud(s). FOG computing extends the traditional Cloud computing paradigm to the *EDGE* of the network, enabling the creation of refined and better Applications or services. FOG is an *EDGE* computing and micro data center (MDC) paradigm for IoTs and Wireless sensor networks (WSNs)"⁴⁷.

The latter definition is the classic example where *FOG* computing and *EDGE* computing mingle. To this the same CISCO systems has given a clarification^{48 49}, in fact with *EDGE Computing*, often simply "*EDGE*", specific reference is made to bringing *Processing* as close as possible to the data sources, without the need to transfer them to the *Cloud* or to other remote systems for processing tasks.

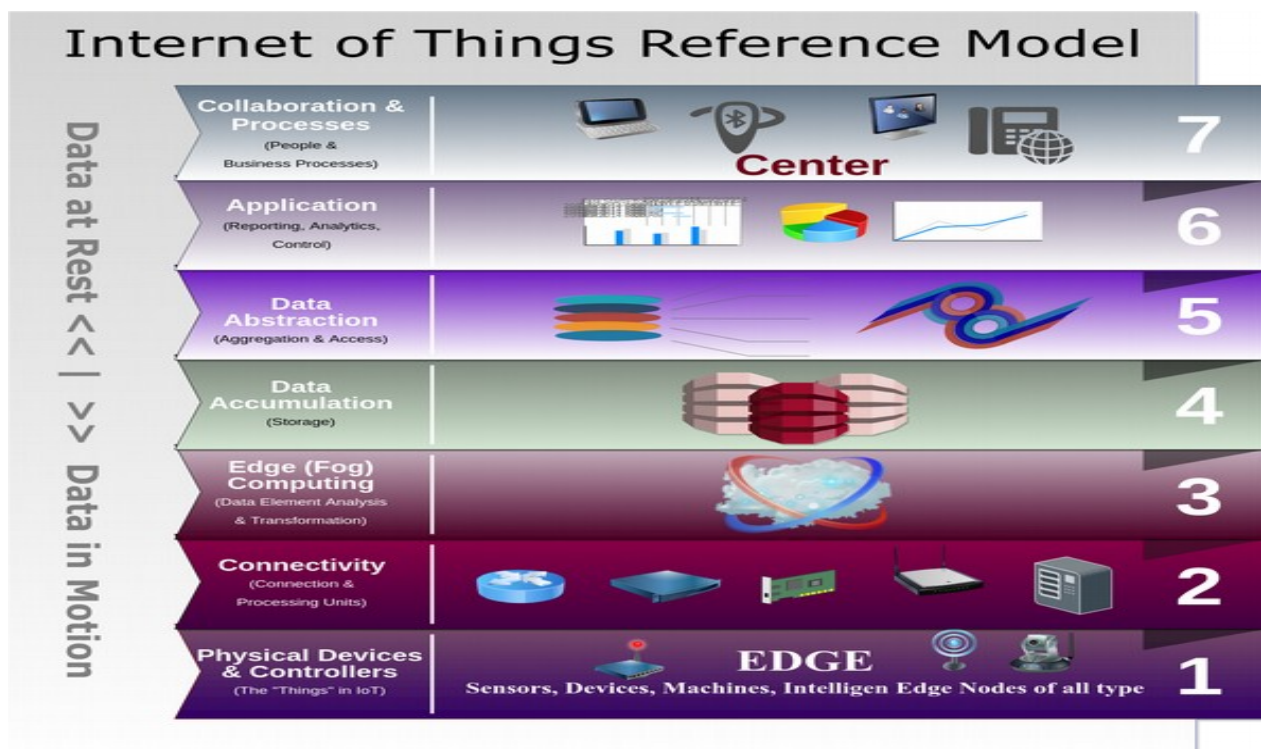


Figure 12: The Internet of Things Reference Model

This eliminates the distances and the time required for data transfer to centralized sources, improving speed and performance. With *FOG Computing*, a definition coined in 2014 by Cisco itself, it indicates the standard that defines the functioning of *EDGE computing*, thus facilitating the operation of processing, storage and network services between devices, objects and the *Cloud*. How the three technologies are intertwined and

⁴⁶ M. Aazam and E.-N. Huh, "FOG computing: The Cloud-IoT/edge middleware paradigm," IEEE Potentials, vol. 35, no. 3, pp. 40–44, May 2016

⁴⁷ Arslan Munir, Prasanna Kansakar and Samee U. Khan. IFCIoT: Integrated FOG Cloud IoT Architectural

Paradigm for Future Internet of Things

⁴⁸ <https://www.cisco.com/c/en/us/solutions/enterprise-networks/EDGE-computing.html> (last access 18/01/2019 at 17.00)

⁴⁹ CISCO, The Internet of Things Reference Model, p.3

interconnected is well specified in Figure 13 inspired by CISCO's ⁵⁰*The Internet of Things Reference Model* where one can sense the complexity of an IoT ecosystem and how, as one moves towards a more abstract level of analysis, regarding the physical level the speed of the process is reduced.

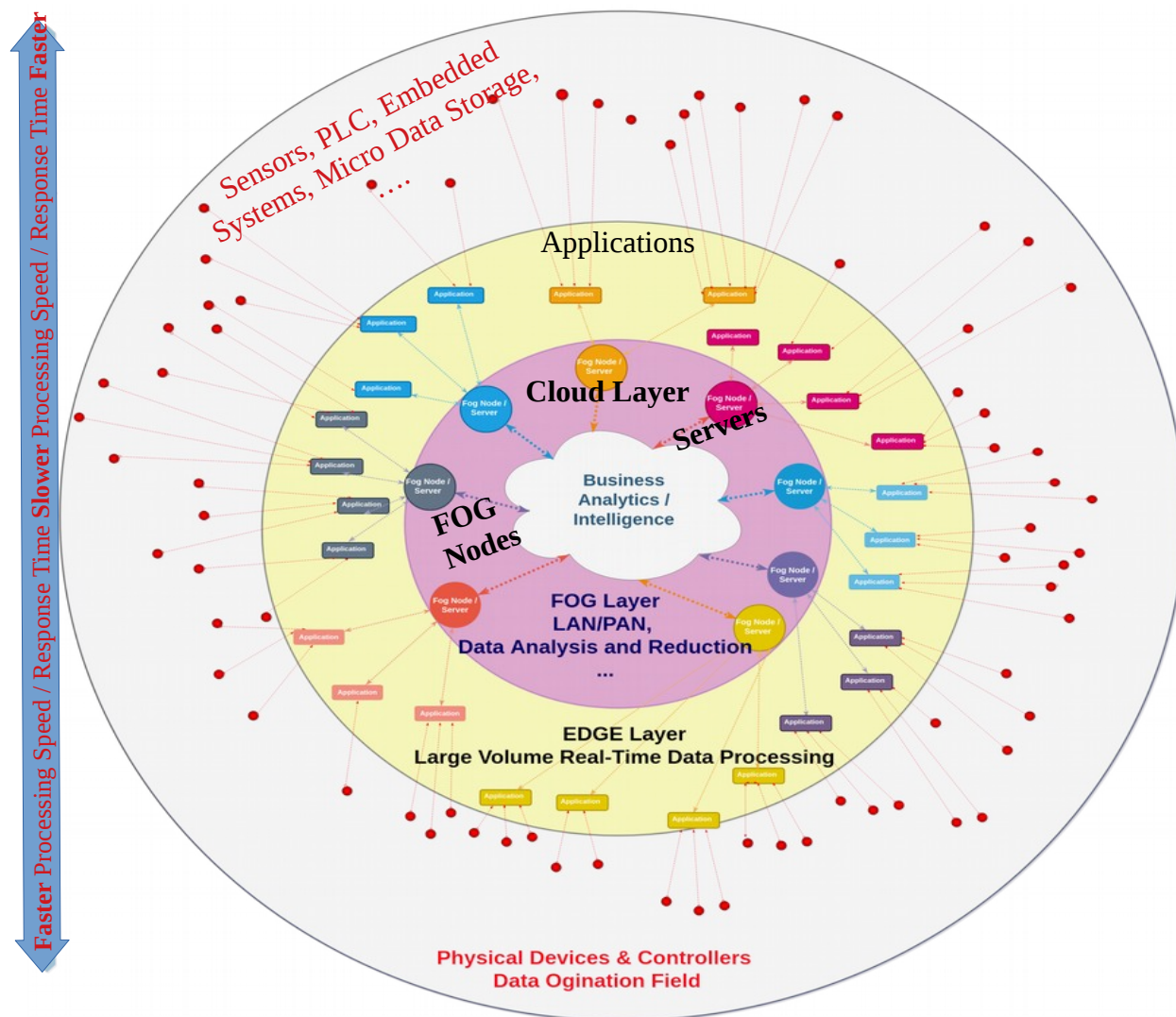


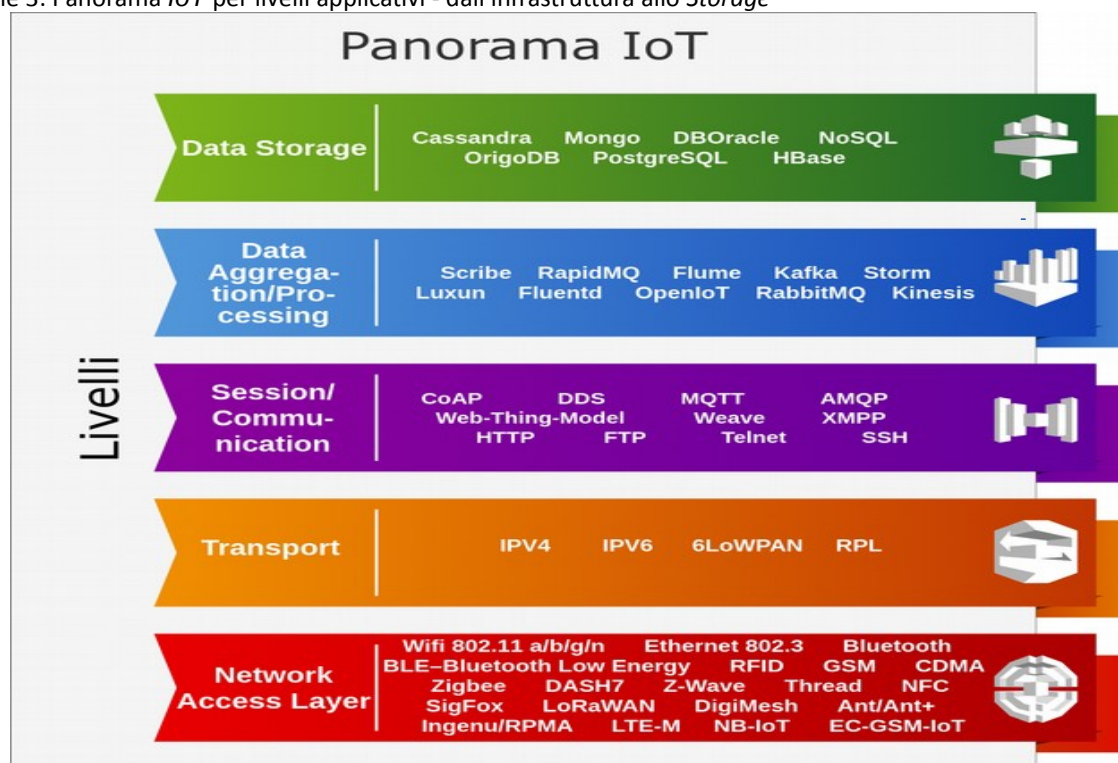
Figure 13: IoT Data Processing Layer Stack

⁵⁰ <https://www.winsystems.com/Cloud-FOG-and-EDGE-computing-whats-the-difference/> (last access 19/1/2019 at 10.00)

7 Examination Comparison of the technological specifications and protocol in IoT landscape

In this chapter a discussion of the comparison of the specific release of technology associations, consortia and companies of reference is presented. Certainly it is not exhaustive nor definitive given the great variety of technologies and paradigms present at all levels are taken into consideration.³

Table 3: Panorama IoT per livelli applicativi - dall'infrastruttura allo Storage



7.1 Network Access Layer

The technologies considered to belong to this layer are divided into two broad categories:

- technologies that define *Medium Access Control* (MAC);
- technologies that rely on standards/protocols that define the MAC layer.

Of these, there are technologies/protocols that cover all ISO/OSI levels (in the scientific bibliography, comparisons to identify *Stack* correspondence are easily found for each of them) and technologies/protocols that define only some of the levels. For example, the IEEE 802.15.4 defines only the physical and MAC levels of the ISO/OSI *Stack*, while the Zigbee technology replaces all the other levels and relies on it. Bluetooth, on the other hand, reinterprets the ISO/OSI standard at all levels, also identifying others.

7.2 Communication Models

The architectures can be distinguished as radio and wireless, the latter are normally used in industrial areas. From the point of view of network architectures, "short range" radio applications (which include Pan, Personal Area Network, up to 10m, and Lan, Local, up to 100 meters) must be distinguished from those "long range" (MAN, Metro, up to 1km, and WAN, Wide, over 1km). In the case of short-range applications there is a device called *Gateway* (local platform) that coordinates the cluster of intelligent objects and provides for communication with the *IoT* platform placed in the *Cloud*. In long range applications the objects are directly in communication with the *Cloud-IoT* platform through an infrastructure of radio stations placed on the territory (as in the case of cellular networks).

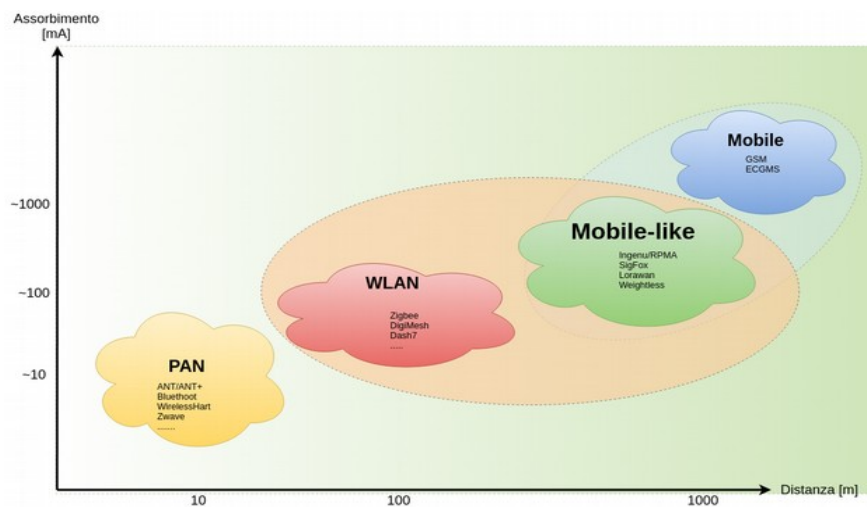


Figure 14: Comparison of communication protocols

Figure 14⁵¹ shows the communication protocols scenario for the *IoT*. In short range applications various competing standards are emerging, such as: Bluetooth Low Energy (BLE), ZigBee, Z-Wave, *WirelessMbus*. BLE is very [promising for interaction with users because it is supported by all *Smart Phones*, in particular for home and car automation, while ZigBee was one of the first standards with ranges of up to 250 meters.

7.2.1 Analyzed technologies that define the Medium Access Control level (MAC)

Ethernet 802.3

The 802.3 Ethernet standard defines local, access and metropolitan cable networks. It works at fixed operational speed and is based on MAC (*Media Access Control*) and MIB (*Management Information Base*). It uses the CSMA/CD MAC protocol (*Carrier Sense Multiple Access with Collision Detection*) for *Half Duplex* and *Full Duplex* operations. Thanks to the MII interfaces (*Media Independent Interfaces*) it provides an architecture independent of the type of physical layer, in which various PHYs (*Physical Layer entities*) can be interfaced to the same MAC. Each PHY is responsible for encoding the packets to be sent and decoded with a modulation based on the speed of the operation, the

⁵¹ A. Capone, G. Verticale, Politecnico di Milano, 2016

transmission medium and the supported cable length. Its other features include the control and management of protocols, and the supply of current through selected twisted pairs. Current projects point to Ethernet protocols on optical cables, fibre and copper at hundreds of *Gigabits* per second. The 802.3 Ethernet standard according to IEEE will have a fundamental role in the creation of the fixed infrastructure for 5G networks, both as a network and current provider to the *Access points* as well as a *Back-Haul* network for *Wireless* networks, and as a connection to *Data-centres* in the industrial field.⁵²

WLAN – Wifi 802.11 a/b/g/n

IEEE 802.11 (also known as Wifi⁵³) is the *Wireless* technology that represents the reference standard for all worldwide networks. Used almost everywhere for internet access in both public and private networks, institutions or personal networks. *Wireless* LAN technology makes it possible to extend the availability of services on mobile networks and wired networks. It is believed that it currently covers 80% of mobile traffic⁵⁴ and that there will be around 32 billion 802.11 (Wi-Fi) devices by 2021⁵⁵.

IEEE 802.11 operates on free frequencies and is evolving for next generation networks, such as

IEEE 802.11ac™-2013 (> 7 Gbps to 5 GHz) and IEEE 802.11ad™-2012 (7 Gbps at 60

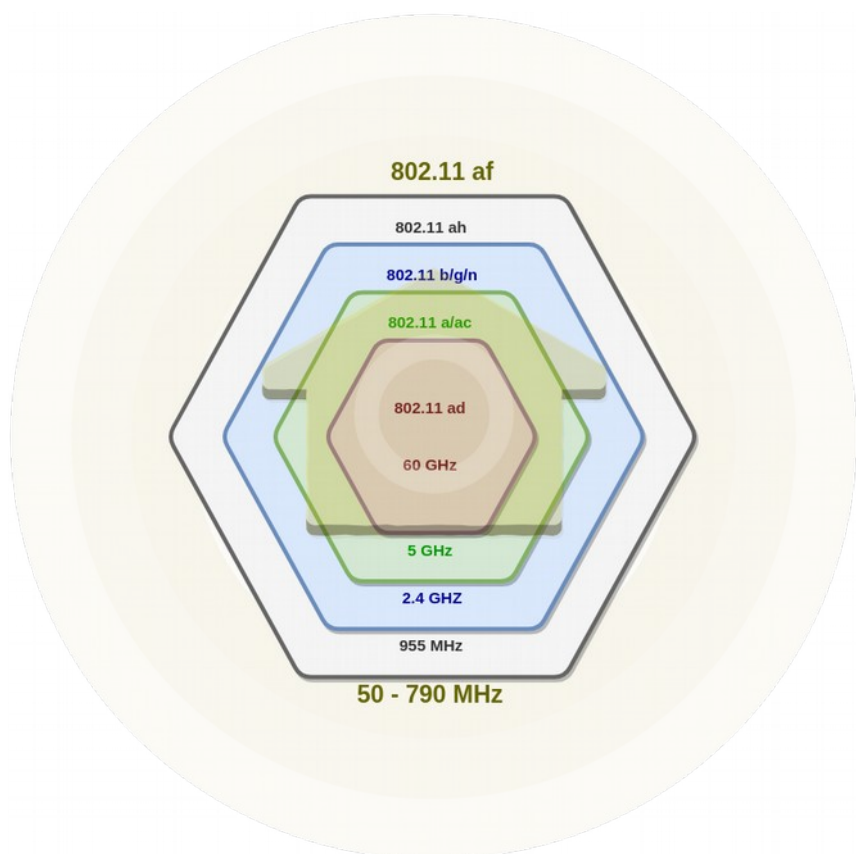


Figure 15: Operational Range of the IEEE 802.11 Technologies

⁵² <https://futurenetworks.ieee.org/standards>

⁵³ Wi-Fi is a trademark of the Wi-Fi Alliance, the trade organization that certifies products that incorporate IEEE 802.11 standards.

⁵⁴ Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020, *White Paper*, CISCO, February 3, 2016

⁵⁵ Wi-Fi Market Data – ABI Research, June 2016

GHz). IEEE 802.11 will continue the support of *Enhanced Mobile Broadband* supporting them with an integration with 3GPP networks such as LWA⁵⁶, LWIP⁵⁷, e-LWA⁵⁸, NBIFOM⁵⁹.

IEEE 802.11 supports *Massive Machine Type Communications* through IEEE 802.11ahTM-2016 technology, called "*HaLow*" by the Wi-Fi Alliance. IEEE Std 802.11ah-2016 devices operate at sub-gigahertz frequencies and cover large distances with low connectivity power. This technology enables energy-efficient connection devices, necessary in *IoT* applications. In addition, the IEEE Std 802.11-2016 in the 2.4 and 5 GHz bands maintains backward compatibility with existing IEEE 802.11 based networks. IEEE 802.11 supports battery-powered devices and the "wake up radio" optimization mechanism is being developed.^{60 61}

Table 4: 802.11 technologies comparison table

Standard	Frequenza	Larghezza di banda	Schema di modulazione	Tipo di trasmissione	Data Rate massimo	Intervallo	Potenza TX massima
802.11	2,4 GHz	20 MHz	BPSK – 256-QAM	DSSS, FHSS	2 Mbps	20 m	100 mW
b	2,4 GHz	21 MHz	BPSK – 256-QAM	CCK, FHSS	11 Mbps	35 m	100 mW
a	5 GHz	22 MHz	BPSK – 256-QAM	OFDM	54 Mbps	35 m,	100 mW
g	2,4 GHz	23 MHz	BPSK – 256-QAM	DSSS,OFDM	54 Mbps	70 m	100 mW
n	2,4 / 5 GHz	24 e 40 MHz	BPSK – 256-QAM	OFDM	600 Mbps	70 m	100 mW
ac	5 GHz	20, 40, 80 80+80=160 MHz	BPSK – 256-QAM	OFDM	6+,93 Gbps	35 m	100 mW
ad	60 GHz	2,16 GHz	BPSK – 256-QAM	SC, OFDM	6,76 Gbps	10 m	100 mW
af	54-790 MHz	6,7 e 8 MHz	BPSK – 256-QAM	SC, OFDM	26,7 Mbps	> 1 km ??	100 mW
ah	900 MHz	1, 2, 4, 8, 16 MHz	BPSK – 256-QAM	SC, OFDM	40 Mbps	1 km	100 mW

Ingenu/RPMA

The RPMA protocol (*Random Phase Multiple Access*) by Ingenu⁶² is a broad-spectrum solution that operates on the 2.4 GHz ISM band. The 2.5 GHz ISM band was chosen with respect to the sub-GHz bands because it is the freest ISM band worldwide. RPMA coverage is mainly due to the transmission power available in this band: thanks to the maximum transmission power it is possible to reach a range of 16 km. Furthermore, in Europe, there are no regulations on duty cycle to be followed in the 2.4 GHz band. An RPMA distribution uses 1 MHz of the 80 MHz band, allowing multiple simultaneous installations or alternatively the use of multiple channels to support a network. RPMA uses an adaptive data rate technique, in which it is possible to select the optimal spread factor based on the resistance of the *Down-link* signal. The base station is able to receive all the diffusion factors and the delay times. Furthermore, the devices retransmit the conditions within *Up-link* messages, allowing the base to optimize the speed of *Down-link* data, optimizing the capacity and use of energy. All messages are encrypted and based on the

⁵⁶ LWA (LTE-WLAN Aggregation)

⁵⁷ LWIP (LTE-WLAN Radio Level Integration with IPsec Tunnel)

⁵⁸ eLWA (enhanced LWA)

⁵⁹ NBIFOM (IP Flow Mobility support for S2a and S2b Interfaces) – EPS (Enhanced Packet System)

⁶⁰ <https://futurenetworks.ieee.org/standards>

⁶¹ <https://www.mwrf.com/active-components/what-s-difference-between-ieee-80211af-and-80211ah>

⁶² Ingenu. An Educational Guide: How RPMA Works.2016

Viterbi algorithm, which allows the recovery of the message even with a package error percentage (PER) of 50%.⁶³

Ingenu's technology is licensed to local operators, who create geographical networks. To access the network you need to connect to these operators.

In Italy, the licensee is Materliq srl, which uses Ingenu RPMA for its gas meters. At the moment the website www.Materliq.com is not functional [last visit 19 June 2019, 17.50], but from the documentation found on the net it seems that it uses RPMA technology only for its own products.

On the Ingenu website you can buy a development and test kit at:

<https://www.ingenu.com/get-started/Hardware/rpma-devkit/>

The protocol is closed.

Radio Frequency Identification (RFID)

Set of technologies formed by two classes of devices: devices to be identified (commonly called *tags*) and the devices that try and identify the leaders. These readers scan the surrounding area with predefined radio frequencies that activate the tag devices, which respond by sending their own identification. There are various registered RFID systems that differ in the frequency used, the radio interface, the communication range, and the autonomy of the tag with respect to the pulses (passive, semi-passive, active). The best known are ISO 14443 (for *smart cards*) and EPC (*Electronic Product Code*, a 96-bit string that defines the 8-bit standard of the protocol, 28-bit manufacturer, 24-bit of class and 36-bit identifier). In general, they differ in three areas:

PRAT (*Passive Reader Active Tag*): the reader is passive and only receives data from autonomously active battery-supplied tags.

ARPT (*Active Reader Passive Tag*): the reader is active and sends impulses. The tags are passive and respond to impulses by feeding on the electromagnetic waves in the air.

ARAT (*Active Reader Active Tag*): both are battery powered, the tag sends data at the request of the reader.

The transmission distance varies from LF (*Low Frequencies*) to, more recently, UHF (*Ultra High Frequencies*). The evolution of tags in UHF and the use of integrated sensors favour use in an *IoT* ecosystem.^{64 65 66}

⁶³ Joseph Finnegan, Stephen Brown. A Comparative Survey of LPWA *Networking*. arXiv:1802.04222v1 [cs.NI] . 12 Feb 2018

⁶⁴ Oliveira, L .; Rodrigues, JJPC; Kozlov, SA; Rabelo, RAL; Albuquerque, VHC MAC Layer Protocols for Internet of Things: A Survey. Future Internet 2019, 11, 16. <https://www.mdpi.com/1999-5903/11/1/16>

⁶⁵ Chen Jiming & Hu, & Kang Wang, Qi & Sun, Yuyi & Shi, & He Zhiguo, Shibo. (2017). Narrow-Band Internet of Things: Implementations and applications. IEEE Internet of Things Journal. 1-1. 10.1109 / JIoT.2017.2764475

⁶⁶ Hossein Motlagh, Naser. (2012). Near Field Communication (NFC) - A technical Overview. 10.13140 / RG.2.1.1232.0720.

Due to its widespread use, various development kits are available, even on Amazon for less than € 10: <https://www.amazon.it/IZOKEE-Lettore-MFRC-522-Raspberry-Portachiavi/dp/B076HTH56Q/>

Near Field Communication (NFC)

NFC is a very short-range technology that uses a low-power connection and does not require *pairing*, the only requirement is that the devices are close enough. The very small range (maximum 20cm) makes communication safer due to the fact that communication occurs only on user input. The technology is similar to RFID because each NFC tag can be seen as both a reader and an RFID tag. NFC operates in the 13.56 MHz band.

NFC tags can operate in different ways:

in "card emulation" mode, the active device reads the passive data

in the "reader/writer" mode, a tag is responsible for reading data from a tag writer

in the "peer-to-peer" mode, the tags are connected together by an ad hoc network.

Depending on the modulation of the frequencies and the coding used, the speed varies from 106, 212, 424 and 848 Kbps. The modulation schemes used are ASK (*Amplitude Shift Keying*) and *Binary Phase Shift Keying* (BPSK), while the encodings are *Non-Return-to-Zero Level* (NRZ-L), *Manchester* or *Miller* modified. The transmission power varies from 20 to 23 dBm depending on the region.^{66 68}

Given its widespread use, various development kits are available, the most basic less than 10 €: <https://it.rs-online.com/web/p/products/9064621/>.

Bluetooth IEEE 802.15.1 e successive versioni

The IEEE 802.15.1 WPAN or *Bluetooth Basic Rate* (BR) is a global 2.4 GHz specification covering the first versions of the technology that provide the basic telephone communication services (v1.0), the AFH (*adaptive frequency Hopping*, v1.2) and finally a resistance to radio interference and a visible range of 100m (v2.0), in addition to a more secure and efficient pairing system (v2.1). Later versions improve reliability, speed and energy consumption. In particular, version 4.2 is designed for *IoT* devices by introducing the IPv6 support profile and a secure connection with low power consumption. All versions are managed by the Bluetooth Special Interest Group (SIG), which has more than 30,000 member companies in the areas of telecommunications, computing, networks and consumer electronics. At the band and radio level, Bluetooth operates in 79 1 MHz radio channels in the ISM band, using an FHSS (*frequency Hopping spread spectrum*) technique. At transmission level, it uses a TDD (*Time Division Duplex*) scheme dividing the channel into time slots from μ s. At network level it operates on a *pico-net* in which one *Master* device and seven *Slaves* can be connected. Given that networks can overlap or that more complex networks are needed, a *Slave* can use *multiplexing* to communicate with different networks in different

⁶⁶ ⁶⁸ Bluetooth® low energy Protocol Stack Introduction, Rev 1.00 Jan. 12, 2018 R01QS0014EJ0100, Renesas Electronics Corporation. <https://www.renesas.com/eu/en/img/solutions/Key-technology/connectivity/bluetooth-smart/r01qs0014ej0100-bleintro.pdf>

time *slots*. It is not possible to communicate to different networks on the same slot due to the need to configure the synchronization parameters. Bluetooth is proposed as an alternative to Wi-Fi for LAN networks, offering a lower cost at the expense of *range* and connection speed.^{66 67}

Due to its widespread use, various development kits are available.

To be able to market your own Bluetooth device, you need to obtain a license:
<https://www.bluetooth.com/develop-with-bluetooth/qualification-listing/>

Bluetooth Low Energy

BLE is part of the Bluetooth v4.0 standard of 2010. Also known as Smart Bluetooth, it is oriented to low energy consumption applications. It has a similar

Stack but is incompatible with Bluetooth Basic Rate and only accepts star network topologies, since two *Slave* devices cannot communicate with each other directly but must pass through a *Master*. The substantial differences are at L2CAP level (*Logical Link Control and Adaptation Protocol*), to which BLE adds functionality through the GAP (*Generic Access Profile*), formed by the ATT (*Attribute Protocol*) to manage connection attributes, the GATT (*Generic Attribute Profile*) to define the functionalities and the SMP (*Security Manager Protocol*) for security. Compared to normal Bluetooth, a *Slave* node belongs to a single *pico-net* during its operation and is therefore synchronized with a single *Master*.^{66 68 69}

Given its widespread use, various development kits are available.

In order to market your own Bluetooth device, you must obtain a license:
<https://www.bluetooth.com/develop-with-bluetooth/qualification-listing/>

Z-Wave

Z-Wave is a proprietary protocol of Silicon Labs, whose diffusion is managed by the Z-Wave Alliance, a consortium of companies in the field of technology and communication. Based on ITU G.9959, it operates on the ISM sub-1GHz band with region-based frequencies modulated with FSK and GFSK (*Gaussian Phase Shift Keying*). The transmission has a speed of the order of tens of Kbps and is protected by AES-128 encryption. The MAC level uses CSMA-CA and guarantees 232 identifiers for the *Mesh Network* and reliability given by the use of ACK (*Acknowledge*) and *Frame* validation. Some Z-Wave devices have the capability of *Routing* and *Packet Forwarding* acting as a repeater. To obtain an efficient system, the protocol has its own *Routing* table update system which is very fast but subject to potential unauthorized changes by malicious nodes.

Each network has its own Controller and is usually the only device on the network connected to the Internet.

⁶⁷ Notes from the BME 362 Biomedical Instrumentation Design course Rhode Island University.
<https://www.ele.uri.edu/courses/bme362/handouts/Bluetooth.pdf>

⁶⁹ Adafruit learning system, Introduction to Bluetooth Low Energy by Kevin Townsend. <https://cdn-learn.adafruit.com/Downloads/pdf/introduction-to-bluetooth-low-energy.pdf>

Z-Wave can be positioned halfway between WiFi LAN and Bluetooth: it has a lower consumption than the first and a greater range than the second.⁶⁶

The Silicon Labs website offers the kits: <https://www.silabs.com/products/development-tools/Wireless/mesh-Networking/z-wave>

Among the various proposals, to start you must consider:

- **SLWSTK6050A, Z-Wave 700 Development Kit, The Z-Wave 700 Zen Gecko *Wireless* Starter Kit** includes the *Z-Wave Software Stack*, sample code and integrated debug adapter. A single worldwide development kit for both terminal devices and *gateways* with multiple radio cards allows developers to create a mesh network and evaluate the Z-Wave 700 module.
 - **Includes:**
 - 2 x BRD4001A - *Wireless* Starter Kit Mainboard
 - 2 x BRD4202A - ZGM130S Radio Board
 - 2 x BRD8029A - Buttons and LEDs Expansion Board
 - 1 x SLUSB7000A - UZB-7 USB stick
 - 1 x UZB-S - (ACC-UZB3-S) UZB-S USB stick network sniffer
 - 2 x SMAMFL - Flexi Antenna, male with skirt
 - 2 x ENRM002 - 1m USB A <-> Mini-B USB cable
 - It guarantees the following features:
 - Wave 700 SiP module Radio Boards to start your development
 - *Z-Wave Application Framework* and pre-certified common *End-Device Application code*
 - Expansion header allows easy expansion and direct integration with *Z-Wave Application Framework*
 - Z-Wave UZB-7 stick to get started with your *Gateway* development on a Linux machine
 - Pre-built Z / IP and Z-Wave binaries allow for easy *Gateway* development at your preferred API level
- **RBK-ZW500-E2, Z-Wave 500 Series Regional Development Kits.** The kit, which has taken into account in the sub-giga frequencies allowed in Europe, is part of the Z-Wave Regional Kits, so it also includes the kit for the USA and Asia.
 - **Includes:**
 - 2 x ZDB5101
 - 2 x ZDB5202
 - 1 x ZDB5304
 - 1 x UZB - USB stick static controller
 - 4 x ZM5202
 - 4 x ZM5304
 - It guarantees the following features:

- **Z-Wave technology world-wide application license**
- **Access to SDK protocol**
- **All *Hardware* required to develop a Z-Wave embedded *Application***
- **Ideally suited for applications:**
 - **testing of Z-Wave end *Devices***
 - **Door locks**
 - **Lights**
 - **Sensors**
 - **Thermostats**

Obviously both kits come with development software and access to the Z-Wave *Framework*.

In terms of test and development software, the Simplicity Studio 4 suite is worth mentioning.

It is an IDE based on Eclipse 4.5 for simplified *IoT* development and includes everything the developers need to complete projects. Simplicity Studio includes a suite of tools for *energy profiling*, configuration and analysis of the *wireless* network, as well as demos, *software* examples, complete documentation, technical support and forums.

Furthermore, it provides tools capable of automatically detecting the 8-bit or 32-bit MCU or the *Wireless* SoC, graphically configuring the device and showing the supported configuration options.⁷⁰

Simplicity Studio is provided free of charge, and for the development of MCUs EFM32, Silicon Labs provides the GNU ARM toolchain which is *Open Source* (Simplicity Studio also supports the GNU ARM toolchain for EFR32 *Wireless* parts). For EFM8 devices Silicon Labs provides a version of the Keil C8051 compiler toolchain and it is possible to obtain a free license from Keil for its use with Simplicity Studio. Basic *Software Stacks* (SDKs) provided by Silicon Labs to support these products are also provided free of charge and without license fees. Therefore, the development for Silicon Labs products can be done for free. If some optional Micrium OS components are used, they require a license, but these components will not be installed by default and at the time of installation it is clear that they require a license.^{66 71}

In general, to develop a Z-Wave product you need to buy a development kit and follow the guidelines to get the certification: <https://z-wavealliance.org/z-wave-oems-developers/>

The SiliconLabs kits can be purchased directly from: <https://www.silabs.com/products/development-tools/Wireless/mesh-Networking/z-wave>.

⁷⁰ <https://www.silabs.com/products/development-tools/Software/simplicity-studio>

⁷¹ https://www.silabs.com/Community/Software/simplicity-studio/forum.Topic.html/i_going_to_develop-DoFI. [last vist 30/05/2019]

M-Bus / WM-Bus

The M-Bus (*Meter Bus*) was developed to satisfy the need for a system for the networking and remote reading of meters, for example to measure the consumption of gas or water in the home. This bus meets the special requirements of remote powered or battery powered systems, including utility meters. When interrogated, the meters supply the data collected to a common *Master*, such as a laptop, connected at periodic intervals to read all the meters in a building. An alternative method for centralized data collection is to transmit meter readings via modem. M-Bus is regulated both at a physical and a connection level, with the EN 13757-2 standard, and at the application level, EN 13757-3 standard. The M-Bus interface is designed for two-wire communication. A radio variant of the M-Bus (*Wireless M-Bus*) is also specified in the EN 13757-4 standard. For each *Layer* an EN standard is present, in table 5 the comparison between the ISO/OSI *Stack* and the WM-BUS *Stack* is shown.

Table 5: Comparison between ISO / OSI e WM-Bus Models

Modello ISO / OSI	Wireless M-Bus stack	Standard	Descrizione
Application Layer	Application Layer	PrEN 13757-3	M-Bus Dedicated Application Layer (DAL)
Presentation Layer			
Session Layer			
Transport Layer	Optionally used for advanced security	EN 13757-5	Wireless relaying (optional for meters supporting the router approach)
Network Layer			
Data Link Layer	Data Link Layer	PrEN 13757-4	Wireless meter readout (Radio meter reading for operation in SRD bands) whereat the data link layer is related to EN 60870-5-1 [69] and EN 60870-5-2 [70]
Physical Layer	Physical Layer	PrEN 13757-4	Wireless meter readout (Radio meter reading for operation in SRD bands). The standard proposes Manchester [60], "3 out of 6" and no- return-to-zero (NRZ [71]) for bit-coding, a cyclic redundancy check (CRC) for error detection.

The *Wireless M-Bus* - or *Wireless Meter Bus* - is an open standard developed for high energy efficiency *Smart Metering* and *Advanced Metering Infrastructure* (AMI) applications and is spreading rapidly in Europe for measuring electricity, gas, water and heat.

A *Wireless M-Bus* network (wM-Bus) is based on a star network with *Master* and *Slave* devices described in the EN 13757 standard which includes different operating modes, of which the most used are: S, T, R and C (868 MHz), F (433 MHz) and N (169 MHz). The EN 13757 standard also defines the modes R, Q, Q, P and F, but they are rarely or never used, so they do not fall within the scope of this summary. The defined frequencies are 868MHz and 169MHz, as well as 433MHz which is intended for markets where 868MHz is not allowed. Table 6 shows the frequencies and operating modes provided for by the EN 13757 standard.

Table 6: WM-Bus Mode

Mode	Frequency	Uni-/bidirectional	Description of Use
S1, Stationary	868.3 MHz 433 MHz	Uni	Send data a few times per day. Optimized for battery operation and stationary operation. 32.7 kbps
S1-m, Stationary?	868.3 MHz 433 MHz	Uni	Same as S1, but optimized for mobile receiver
S2, Stationary	868.3 MHz 433 MHz	Bi	Same as S1, but bidirectional communication
T1, Frequent transmit	868.95 MHz 433 MHz	Uni	Send data every few seconds. Configurable interval. 100 kbps
T2, Frequent transmit	868.95 MHz 868.3 MHz 433 MHz	Bi	Same as T2 (T1?), but bidirectional operation
C1, Compact	868.95 MHz 433 MHz	Uni	Unidirectional communication using NRZ coding. Similar to T1 but higher data-rate, 50 kbps. Stationary operation
C2, Compact	868.95 MHz 433 MHz 869.525 MHz	Bi	Same as C1, but bidirectional operation
N1a-f, Narrowband	169 MHz @12.5 kHz	Uni	Unidirectional, 4.8 kbps, stationary operation
N2a-f, Narrowband	169 MHz @12.5 kHz	Bi	Same as N1a-f, but bidirectional operation
N1g, Narrowband	169 MHz @50 kHz	Uni	Unidirectional, 19.2 kbps, stationary operation
N2g, Narrowband	169 MHz @50 kHz	Bi	Same as N1g, but bidirectional operation

The *Wireless* WM-Bus version (EN 13757-4) at 868MHz allows transmissions up to a few hundred meters, or 169MHz, up to 1-2 km, with reduced consumption (battery life declared up to 20 years). As stated, M-Bus represents one of the main connections with gas meters and other energy sources. WM-Bus in turn allows communication with meters that otherwise would not have simple access to the apartment or to the other meters.

Like all the standards that work in ISM 868-870, they must have the devices conforming to the directives contained in the ETSI standard EN300220 and CEPT / ERC / REC 70-03.⁷²

73 74 75 76

⁷² <http://www.ti.com/tool/WMBUS#descriptionArea> [last visit 30/05/2019]

⁷³ <https://www.st.com/en/Applications/connectivity/wm-bus.html> [last visit 30/05/2019]

⁷⁴ *Open Metering* System Specification – General Part Issue 2.0.1 / 2014-10 (RELEASE). OMS GROUP

⁷⁵ Cyrill Brunswiler, Compass Secyry AG. *Wireless M-Bus Secyry* Whitepaper Black Hat USA 2013. June 30th 2013

⁷⁶ Vivek Mohan. *An Introduction to Wireless M-Bus*. SiliconLabs

Table 7: WM-Bus Data Rate

Configuration	Frequency	Device (meter) node Tx	Collector node Tx	Uplink	Downlink
Device S1, S2 / Collector S1,S2	868/433	32.7 kbps Manch code	32.7 kbps Manch code	32.7 kbps	32.7 kbps
Device T1, T2 / Collector T1,T2	868/433	100 kbps, 3 out of 6	32.7 kbps Manch code	67 kbps	32.7 kbps
Device T1, T2 / Collector C1, C2	868/433	100 kbps, 3 out of 6	32.7 kbps Manch code	67 kbps	32.7 kbps
Device C1, C2 / Collector C1, C2	868/433	100 kbps, NRZ	50 kbps NRZ	100 kbps	50 kbps
Nc mode (Collector and device)	169	2.4 kbps, NRZ	2.4 kbps, NRZ	2.4 kbps	2.4 kbps
Na mode (Collector and device)	169	4.8 kbps, NRZ	4.8 kbps, NRZ	4.8 kbps	4.8 kbps
Ng mode (Collector and device)	169	19.2 kbps, NRZ	19.2 kbps, NRZ	19.2 kbps	19.2 kbps

As far as security is concerned, it is mainly based on AES in the *Dedicate Application Layer*, then on the *Extended Link Layer* additional security levels can be implemented.

It is an open standard based on EU standards; the documentation can be found at: https://ec.europa.eu/eip/ageing/standards/ict-and-communication/data/en-13757_en

This is one of the most widely used standards for *Metering* and many manufacturers provide development and test kits. Available kits include:

- **SiliconLabs:**
 - **SLWSTK6220A - EZR32 Wonder Gecko 868 MHz Wireless Starter Kit, featuring:**
 - **Device: EZR32WG330FG60G**
 - **Frequency: 868 MHz**
 - **Core CPU: ARM® Cortex®-M4**
 - **Flash memory: 256 kB**
 - **RAM: 32 kB**
 - **Crystals for LFXO and HFXO: 32.768 kHz and 48 MHz**
 - **Crystal for RF: 26 MHz**
 - **USB 2.0 Full Speed (12 Mbps)**
 - **Output Power: +13 dBm**
- **The kit consists of:**
 - **(2) BRD4502C EZR32WG 868 MHz 13 dBm Radio Boards**
 - **(2) 868 MHz antennas with SMA connector**
 - **(2) USB Type A to Mini-B USB cables**
 - **(2) USB Type A to Micro-B USB cables**

- **EMB-WMB868-EVK - EMBIT 868MHz Wireless M-Bus Evaluation Kit, characterized as follows:**

EMB-WMBx-EVK Evaluation Kit Content		LIGHT Kit	FULL Kit
EMB-WMBx-EVB	Evaluation Board carrying EMB-WMBx module	2	4
USB CABLE	USB supply / connection with a PC	2	4
EMB-ANx ANTENNA	Compact Antenna (169 MHz or 868 MHz)	2	4
EMB-AN169-001	Ground Plane antenna (only for 169 MHz kit)	1	1
MSP-FET430UIF	USB debugger interface	0	1
EMB-MULTIPROG	Programmer adapter	0	1
U.FL TO SMA PIGTAIL	RF cable	2	4
CD DOCS	CD-ROM with documentation and binaries	1	1

Weightless W-N-P

Weightless identifies a group of LP-WAN protocols with low transmission speed: Weightless-P, Weightless-N and Weightless-W, standardized by the Weightless Special Interest Group (Weightless SIG). They are star networks composed of basic devices (BS, stations) and end devices (ED, sensors). These form the BSN (Base Station network), which manages authentication, *Scheduling* and band allocation.

The physical layer has two variants with different speeds: a 125 Kbps configuration with BPSK and FEC (*Forward Error Correction*) and a 16 Mbps configuration with only 16-QAM (*Quadrature Amplitude Modulation*). Communication takes place in three channels: The *Down-link* (information from the base to the nodes), the *Up-link* (communications from the node to the base) the disputed-access *Up-link* (data from the nodes to the base. Access is contended because a small number of nodes can use it simultaneously).

The contention and the sending of the data are managed by a BB (*Base-Band*) sub-layer at the top of the physical layer. The link layer above deals with the reliability of the connection, the division of data into packets and their reconstruction.

Weightless-W is a two-way communication that operates on television frequencies (TVWS) between 470 and 490 MHz via FHMA (*Frequency Hopping Multiple Access*) and TDD. This technology supports a star topology with connections from 1 Kbps to 10 Mbps encrypted with 128-bit AES with a maximum battery life of the devices from 3 to 5 years.

Weightless-N is based on Weightless-W and is optimized for short distances and reduced consumption, at the cost of a maximum transmission speed reduced to 100 Kbps and providing only *Up-link* communications. It operates at 800-900 MHz, on the UNB (*Ultra Narrow Band*) frequencies of the ISM band modulated with UNB DBPSK (*Differential Phase Shift Keying*), which extends the maximum battery life of the devices to 10 years.

Weightless-P is a standard whose main difference with the previous ones is the modulation through GMSK (*Gaussian Minimum Shift Keying*), which does not require the use of a TCXO (*Temperature Compensated Crystal Oscillator*), which makes the system less expensive and less vulnerable to loss of synchronism due to ambient temperature.⁶⁶

77

⁷⁷ Usman Raza, Parag Kulkarni, and Mahesh Sooriyabandara, "Low Power Wide Area Networks: An

Regarding the kits, the only official recognised retailer is Ubiik:
<https://www.ubiik.com/starterkit>.

Il kit è composto da:

- **1 x Base Station (Starter Kit)**
- **1 x Base Station Antenna (868 MHz o 915 MHz)**
- **2 x End-Device Module EVB**
- **2 x End-Device Module EVB Antennas (868 MHz o 915 MHz)**
- **1 x Micro USB to USB cable**

The Ubiik Cloud also provides a development and test software, which is not free. A 60-day trial license is granted with the kit.

To become a Weightless developer you need to become a member by paying the appropriate fee: <http://www.weightless.org/about/weightless-terminal-licence>

NB-IoT

NB-IoT is a communication system managed by 3GPP that can be implemented as an autonomous system in the GSM band.

It offers Down-link and Up-link at 250 Kbps in Half-duplex within a 15km radius.

Its strengths are its ease of use and the large coverage provided by GSM, making it suitable for sensor applications that require reduced communications and is not affected by possible connection delays.

It is seen as the future of IoT communications on cellular networks, as it also operates on LTE and is adaptable to future technologies.^{66 78}

Various kits are available, some indicated directly on the GSMA website, where you can request to add your own marketed product: <https://www.gsma.com/IoT/mobile-IoT-development-kits/>

LTE - Long Term Evolution

The *IoT* standards based on LTE (LTE and TMC, *enhanced Machine-Type Communication*) support the CAT-0 and CAT-M categories, whose standards are regulated by 3GPP. These differ from the CAT-1 standard for H2H (*Human-to-Human*) use, as the use of data changes drastically: in H2H use there are peaks of heavy usage in *Downloads* corresponding to the use of the device by man interspersed with inactivity. While in M2M use the use of data is a less intensive *upload* but constant over time. In CAT-0, the transmission speed is reduced to the advantage of a less complex and therefore cheaper hardware. In CAT-M, the substantial difference lies in using only 1.4 MHz of the 20

Overview". arXiv:1606.07360v2 [cs.NI] 11 Jan 2017. <https://arxiv.org/pdf/1606.07360.pdf>

⁷⁸ Chen, Jiming & Hu, Kang & Wang, Qi & Sun, Yuyi & Shi, Zhiguo & He, Shibo. (2017). Narrow-Band *Internet of Things*: Implementations and Applications. *IEEE Internet of Things Journal*. 1-1. 10.1109/JIoT.2017.2764475. https://www.researchgate.net/Publication/320544536_Narrow-Band_Internet_of_Things_Implementations_and_Applications

available. Both of these LTE and TMC standards have a range of about 11 km and adopt the same *Stack* of the CAT-1 protocol. An LTE eMTC *Device* has a *Buffer* to save the received data, in order to analyse the network synchronization signals and adapt to its current conditions. When not transmitting, an LTE eMTC device has the same power consumption as an NB-*IoT* device, however, when transmitting, the first one has a consumption of 50% less than the second, thanks to a better *Throughput*.⁷⁹

Various kits are available, some indicated directly on the GSMA website, where you can request to add your own marketed product: <https://www.gsma.com/loT/mobile-loT-development-kits/>

EC-GSM-IoT

The *Extended Coverage Global System for Mobile Communications Internet of Things* (EC-GSM-IoT) is a standard designed for regions where LTE is not present, it adds functionality to EGPRS (*Enhanced GPRS*) which, together with *Power Saving Mode* (PSM), transforms a GSM/EDGE network into a network that can provide *IoT* services. With regard to EC-GSM, the specifications are defined by the 3GPP in Release 13 of the standard. This technology uses the existing GSM/GPRS network infrastructure, for which only a *software* update is required. EC-GSM achieves an improvement in coverage without the need for additional carriers: the data and control channels are mapped in traditional GSM channels; EC-GSM device traffic is multiplexed with GPRS traffic. Up to 50,000 devices per cell are supported, per single transmitter. The use of the aforementioned eDRX technique allows the improvement of power efficiency and battery life.⁸⁰

The total band occupation is 2.8MHz, given by 200 kHz data from the *legacy GSM* channels, considering a minimum useful bandwidth of 2.4 MHz to allow *frequency Hopping*, for *IoT* applications, and 2 guard channels of 200 kHz each at the ends of the band. In the absence of GSM service, 600 kHz is sufficient, attributable to 1 MHz of bandwidth required with the aforementioned guard channels. The transmission power of the terminals is the same as for GSM terminals, i.e. 33 dBm in order to reach an extension of the radio coverage corresponding to an MCL (*Maximum Coupling Loss*) of 164 dB. Bringing the power level to those expected in the LTE and the NB-*IoT*, i.e. 23 dB has a 10 dB reduction on the coverage and an MCL of 154 dB. The peak data rate that can be reached both in DL and in UL is 491 kbps, while the nominal average value is 98 kbps in both DL and UL. In order to satisfy the capacity requirements (more than 50,000 terminals in each sector of a three-sector cell), it is necessary to use an overlay technique based on CDMA, both on traffic channels and on signalling channels.^{81 82}

7 ⁷⁹ Halberd Bastion Pty Ltd. eMTC (LTE Cat-M1). <https://halberdbastion.com/technology/loT/IoT-protocols/emtc-lte-cat-m1>

8 ⁸⁰ Results of the work of the Working Group For the analysis of the communication technologies of the smart Metering systems. AGCOM. 06-12-2016.

8 ⁸¹ Practical Guide to LTE-A, VoLTE and *IoT*: Paving the way towards 5G. Ayman Elnashar, Mohamed A. El-saidny. 2018 John Wiley & Sons Ltd

8 ⁸² Roberto Fantini, Francesca Mondello, Alessandro Rigallo, Davide Sorbara. LE TECNOLOGIE ABILITANTI PER L' *IoT*. No-tiziario Tecnico Tim. Anno 25, 3/2016

Development kits are not available as the standard is release 13 but has not yet been released. Therefore the specifications are not yet final.

LoRa — Long Range Protocol

LoRa is a broad-spectrum modulation for low-power and long-range *wireless* networks (<https://www.semtech.com/lora/what-is-lora>), using chirp spread spectrum technology (CSS). An advantage of CSS is the little influence the Doppler effect has on it, making it ideal for moving sensors. It operates in Europe at 863-870 MHz on the ISM band.

LoRa was developed by Cycleo, a French company later acquired by Semtech. Based on LoRa, the LoRaWAN specification was created, managed by the LoRa Alliance, a consortium of companies where Semtech is a founding member. LoRa technology is adaptable based on the type of use, by changing speed, packet size and the spread spectrum. These parameters form what in LoRaWAN is called Adaptive Data Rate, which defines three classes of devices⁸³:

Class A, in which the node transmits only when necessary. To receive messages from the Gateway, it opens a reception window after it has transmitted

Class B, where the node synchronizes with a Beacon and opens reception windows at regular intervals

Class C, in which the node is constantly receiving when it does not send data (at the cost of a considerably greater consumption).^{66 84 85}

LoRa devices are available in various markets, including Amazon Italy. An online reference market for kits is not reported, only for LoRaWAN certified devices: <https://lora-alliance.org/LoRaWAN-certified-products>

LoRa is a proprietary protocol. In order to use the LoRaWAN logo on your devices, you need to become a member of the alliance: <https://lora-alliance.org/become-a-member>

Sigfox

Sigfox, is an LTN (*Low Throughput Network*) defined by the ETSI ERM TG28 standard and based on the *Ultra Narrow Band*. It uses an ISM sub-GHz band of 100 Hz in Europe and Japan and 600 Hz in America, Asia and Oceania.

Diversification has been used to solve problems related to interference: the devices must not synchronize but transmit their data in multiple replicas in time intervals and random frequencies. For modulation it uses DBPSK in *Up-link* and GFSK in *Down-link*, which is only available at the end of the *Up-link*, when the *Device* opens a window of reception. For the use of the channel it uses RFTDMA of the Aloha protocol: there is no bandwidth control, saving consumption but increasing the risk of packet collision. The network

⁸³ <https://lora-alliance.org/sites/default/files/2018-07/LoRaWAN1.0.3.pdf>

⁸⁴ Pratap Singh, Bhupendra. (2019). A survey on LPWAN technologies in content to *IoT Applications*. https://www.researchgate.net/Publication/330840657_A_survey_on_LPWAN_technologies_in_content_to_IoT_Applications

⁸⁵ Guillaume Ferré, Eric Simon. An introduction to Sigfox and LoRa PHY and MAC layers. 2018. fhal-01774080f. <https://hal.archives-ouvertes.fr/hal-01774080/document>

topology is a global star: each *Device* sends its data to a Sigfox station, which saves the data on its own Server and makes it available to users via API. By regulation, it is not possible to send more than 140 messages per device per day.^{66 84 83}

The Sigfox kits are grouped in a special page of the company:

<https://partners.Sigfox.com/products/kit>. Some kits, in addition to the device, they offer a 1-year registration included in the Sigfox network. As of June 2019, a subscription in Italy is not available directly from <https://buy.Sigfox.com/buy>, but requires direct contact with the Nettrotter supplier (<https://nettrotter.io/index.php/en/>).

Creating your own kit does not require a license, however as written above the use of the Sigfox network is subject to registration.

7.2.2 Analyzed technologies that are based on other standards

Dash7

The DASH7 Alliance protocol (D7AP) is based on ISO 18000-7, a standard that defines active RFID technology. D7AP extends the standard by adding a more general asynchronous MAC, enabling greater flexibility in communication than standard RFID. D7AP-based networks differ from typical networks, both wired and not, because they use a session. It is a technology characterized by:

Bursty: abrupt data transfer and does not include content such as video, audio or other isochronous data.

Light: the packet size is almost always limited to 256 bytes and multiple transactions with consecutive packets are generally avoided.

Asynchronous: The main communication method of D7AP is the response to the command, which by its nature does not require periodic "hand-shaking" or synchronization between the devices.

Sthealt: D7AP devices do not require periodic *beaconing* to respond in a communication.

Transitive: A D7AP device system is inherently mobile or transient. Unlike other *wireless* technologies, D7AP is centred on the *upload*, not on the *download*, so the devices do not need to be managed extensively by a fixed infrastructure (i.e. the base stations)

D7AP communicates on sub-GHz bands (433, 868 and 915 MHz) to have the possibility to operate in all states. D7AP in many cases provides for star or tree network topologies (only 1 jump is required), this allows it to be more economical in terms of energy.

D7AP defines all levels of the ISO/OSI model, so as to allow a very wide implementation flexibility at all levels of the *Stack*, for example connecting it to a modem module and exploiting a file interface.

The *Stack* has been released as *Open Source* and granted under the Apache license, version 2.0 (the "License").

The sources are available at: [https://github.com/MOSAIC-LoPoW/dash7-ap-Open Source-Stack](https://github.com/MOSAIC-LoPoW/dash7-ap-Open-Source-Stack)

The documentation is available at: [http://mosaic-lopow.github.io/dash7-ap-Open Source-Stack / docs / home /](http://mosaic-lopow.github.io/dash7-ap-Open-Source-Stack/docs/home/)

Submit a *Community* to the address: dash7-ap-oss Google Group (<https://groups.google.com/forum/#!forum/dash7-ap-oss>).

Test kits based on D7AP and LoRaWAN can be purchased at <http://wizzilab.com/sHop>. The kit is:

WizziKit D7A 1.2 - LoRaWAN: The WizziKit is a *Wireless Sensor-Actuator Network* prototyping framework based on WizziLab *Hardware* and *Open Source* collaborative platforms, completely dual-band "DASH7 v1.2" and LoRaWAN. Operates in the ISM bands at 863-870 MHz (EU) or 902-928 (USA).⁸⁶

Zigbee, Zigbee Pro, Zigbee 3.0

ZigBee is a *wireless* network standard that is aimed at remote control and sensor applications, suitable for operation in difficult radio environments and in isolated places. It is a set of specifications established for the *wireless* personal area network (WPAN). ZigBee is one of the global standards of the communication protocol formulated by the relevant task force within the IEEE 802.15 working group which defines the physical and MAC levels. The main applications for 802.15.4 are specifically designed for monitoring and control applications, where relatively low levels of effective data transmission capacity are required with a large range of 10-100 meters, and with the possibility of remote sensors, battery-powered, where low energy consumption is a fundamental requirement. This technology includes: sensors, lighting controls, safety controls and many other applications.

The system has been designed to operate in one of the three license free bands at 2.4 GHz, 915 MHz and 868 MHz. At 2.4 GHz the maximum data rate is 250 kbps. For 915 MHz the standard supports a maximum data rate of 40 kbps, while at 868 MHz it can support data transfer up to 20 kbps. There are three different network topologies supported by ZigBee, namely star, mesh and cluster tree or hybrid networks. There are numerous advantages to the Zigbee protocol, including its reliability, scalability and the ability to self-repair its Mesh Network.

ZigBee PRO is a version of ZigBee that involves more features, such as routing techniques, network jumps, maximum number of devices, and network protection. By adopting ZigBee PRO as an advanced version, it is possible to provide the additional

8 ⁸⁶ <http://wizzilab.com/product/wizzikit-dash7-1-x>

features of some applications, while maintaining a simpler, lower-cost *stack*, and lower power consumption for applications that do not require additional features.⁸⁷

Table 8: Zigbee Stack Comparison

Standard Feature	ZigBee Feature Set	ZigBee PRO Feature Set	EmberZNet PRO Stack
Indirizzamento	Tree	Stochastic	Stochastic
Routing	Tree and Mesh	Mesh	Mesh
Aggregazione	No	Required	Yes
Link asimmetrici	No	Required	Yes
Frequency Agility	Optional	Required	Yes
APS Multicast	Required	Supported	Yes
Network Multicast	No	Required	Supported
Fragmentation	Optional	Optional	Yes
Base Security	Residential	Standard	Standard
APS Encryption	Optional	Optional	Yes
High Security	No	Optional	No
Enhanced Sleepy & Mobile ZEDs	No	No	Yes
Dense Networks	No	No	Yes

Zigbee 3.0 was developed from Zigbee PRO and was specifically designed for the *IoT*. The introduction is recent and aims precisely to better integrate ZigBee WPAN into the *IoT* and strengthen the network-level security options for ZigBee nodes. Traditionally, the ZigBee standard provides a number of market-specific "application profiles", such as ZigBee Home Automation and ZigBee Light Link. A ZigBee WPAN adopts a particular profile and all devices within the network come from the same profile. In the spirit of the *IoT*, where devices/things with completely different functionalities are networked, there are no application profiles in ZigBee 3.0 and devices from different market sectors can communicate with each other. In practice, the devices may not be able to communicate in a functional sense by exchanging useful data, but they are able to provide services at network level to each other, for example the union of the network and the *routing* of messages, in other words, regardless of their functional roles, devices can participate in the same network infrastructure.

The ZigBee standard has always included security measures to protect communications between nodes, but has never insisted on their use for ZigBee certification: the security choices for a product are left to the manufacturer. Security at the ZigBee network level is provided by a randomly generated encryption key called a "network key".

ZigBee 3.0 offers advanced protection for the network key allowing you to derive the pre-configured key from an "installation code". An individual installation code is randomly

⁸⁷ <https://it.farnell.com/Wireless-zigbee-technology>

generated for a node and programmed into the node during production. The ZigBee protocol *stack* in the node derives an encryption key from this code. Therefore, the network key is protected with a different pre-configured key for each connection node and this key is never exposed outside the participating nodes. The code is communicated to the installer in a non-specified manner, to comply with the activities of securing the network. Besides the encryption key mechanism, it also provides a milder mechanism called "distributed *Security*". Thanks to the *Over-The-Air* (OTA) update function of ZigBee it is possible to upgrade the nodes already in the field to the Zigbee 3.0 version. The OTA update is an optional feature that manufacturers are encouraged to support in their ZigBee products.

ZigBee 3.0 supports ZigBee Green Power (GP). The *Green Power* specification provides a simplified protocol to minimize the energy consumption of self-powered devices through *Energy Harvesting*. GP devices can only transmit and use a specific set of commands that allow short packets of data and minimum transmission times.

In ZigBee version 3.0 the *ZigBee Control Bridge* was also introduced. It is a device that manages the ZigBee side of an *IoT Gateway*. In fact, the integration of a WPAN ZigBee in the *Internet of Things* requires an *IoT Gateway*. Data messages exist as IEEE802.15.4 *Over-The-Air* packages within the WPAN but as IP packets external to the WPAN. The *IoT Gateway* is needed to transform messages between the two types of packets, in both directions. The *ZigBee Control Bridge* can also act as ZigBee coordinator and/or WPAN trust centre. A device with an IP connection, such as a tablet, can run an application that provides a graphical user interface that interacts with the *ZigBee Control Bridge* to allow monitoring and control of the nodes in the WPAN.^{88 89 90}

8 ⁸⁸ <https://www.nxp.com/docs/en/white-paper/JN-WP-7005.pdf?fsrch=1&sr=7&pageNum=1&ICID=I-CT-TP-re-sources-161>

8 ⁸⁹ <https://www.zigbee.org/zigbee-for-developers/zigbee-3-0/>

Table 9: ZigBee 3.0 Technical Specifications

Protocollo di rete	Zigbee PRO 2015 (or newer)
Topologia di rete	Self-Forming, Self-Healing MESH
Configurazione dei dispositivi di rete	Coordinator (routing capable), Router, End Device, Zigbee Green Power Device
Dimensione, in numero di nodi, della rete	Up to 65,000
Tecnologia radio di rete	IEEE 802.15.4-2011
Frequenze di lavoro / canali	2.4 GHz (ISM band) ÷ 16-channels (2 MHz wide)
Data Rate	250 Kbits/sec
Modello di sicurezza	Centralized (with Install Codes support) Distributed
Supporto di Criptazione	AES-128 at Network Layer AES-128 available at Application Layer
Distanza operativa media	Up to 300+ meters (line of sight) Up to 75-100 meters indoor
Low Power Support	Sleeping End Devices Zigbee Green Power Devices (energy harvesting)
Legacy profile support	Zigbee 3 devices can join legacy Zigbee profile networks. Legacy devices may join Zigbee 3 networks (based on network's security policy)
Logical device support	Each physical device may support up to 240 end-points (logical devices)

For non-commercial purposes, the ZigBee specification is available free of charge⁹¹. An entry level membership in the ZigBee Alliance, called Adopter, provides access to unpublished specifications and permission to create products for the market using the specifications.

The "*click through*" license on the ZigBee specification requires a commercial developer to join the ZigBee Alliance. "No part of this specification can be used in the development of a product for sale without becoming a member of the ZigBee Alliance". The annual fee is in conflict with the GNU General Public License. From the GPL v2, "b) You must ensure that any work you distribute or publish, which in whole or in part contains or derives from the Program or any part of it, is licensed free of charge to all third parties under the terms of this License ". Since the GPL makes no distinction between commercial and non-commercial use, it is impossible to implement a ZigBee battery with a GPL license or to combine a ZigBee implementation with the GPL-licensed code. The developer's requirement to join the ZigBee Alliance conflicts with most other Free Software licenses.⁹²

In the latest versions of the specifications the *Open Source* part is no longer shown, in fact you must always be licensees.⁹³

DigiMesh®

DigiMesh® is a proprietary *Peer-to-Peer Wireless* network protocol developed by Digi International Inc. DigiMesh forms a *Mesh Network*. The protocol allows synchronized

⁹¹ ZigBee Cluster Library ZigBee - Document 075123r04ZB. May 29, 2012 10:50 am

⁹² <https://archive.freaklabs.org/index.php/blog/zigbee/zigbee-linux-and-the-gpl.html>

⁹³ Base Device Behavior Specification, ZigBee Document 13-0402-13. February 24th, 2016

operation of the nodes/routers and low battery power. The protocol is currently supported by several Digi 900 MHz, 868 MHz, 865 MHz and 2.4 GHz radio modules.

DigiMesh® 2.4 offers connectivity for end-point devices with a globally distributable 2.4 GHz transceiver. It supports advanced *Networking* features including dormant routers and tight mesh networks. DigiMesh supports multiple network topologies such as *point-to-point*, *point-to-multipoint* and *Meshnetworks*. With support for dormant routers, DigiMesh is ideal for low-power applications, in particular, battery-powered or with energy harvesting technology. The features of DigiMesh are:

- Self-healing: any node can enter or exit the network at any time without the network falling as a whole.
- Easy to use: the *Mesh Network* is simplified as it does not require hierarchy or parent-child relationships.
- Silent: *Routing overhead* is reduced by using reactive protocols similar to *Routing ADV (Vector On Distance Distance) Ad-hoc (AODV)*

Digi International Inc. also produces the XBEE Hardware, and the only DigiMesh protocol radios on the market are from Digi Xbee. In addition to the standard modules, there are the Digi XBee-PRO modules which are amplified power versions of the Digi XBee modules for wide-range applications. Part of the Digi XBee RF product family, these modules are easy to use, have a common socket and are completely interoperable with other XBee products using the same technology.

The updated Digi XBee S2C DigiMesh® 2.4 module is built with the SiliconLabs EM357 SoC and has better energy management, support for *Over-The-Air firmware* updates, and provides an upgrade path to IEEE 802.15.4 *mesh* or ZigBee® protocol if desired.

All the necessary documentation is available on the DIGI website: <https://www.digi.com/>

You can buy DigiMesh-based test kits at:

- <https://www.digi.com/products> (tutti i prodotti Xbee)
- <https://www.digi.com/products/models/xk-wdm> (il kit specifico a 2.4GHz)

Il kit individuato è:

XK-WDM - DIGI XBEE® S2CDIGIMESH® 2.4 KIT: Digi XBee S2C DigiMesh Development Kit has 2 XB24CDMPIT-001 modules and 1 XB24DMPIS-001 module. Overall it consists of:

- **3 Digi XBee Grove Development Boards**
- **3 Digi XBee DigiMesh Modules (TH and SMT)**
- **3 Micro-USB Cables**
- **2 Digi XBee Stickers**
- **Access to Web and video instructions**

Thread / OpenThread

Thread is a network standard recently implemented by Google Nest and is intended for *IoT* devices, in particular for home automation. The official specification of the Thread was published by *Thread Group* on 13 July 2015 and also features an *Open Source* version. The main objective is to have a low power, high resilience D2D (*Device to Device*) communication, with safe operations based on IP. It aims to interconnect devices that communicate with different protocols through its *Stack*. *Thread* brings IPv6 functionality to *IoT* devices through the 6LoWPAN standard and is based on existing *hardware* that supports the IEEE 802.15.4 standard that defines the operation of personal *wireless* networks at low speed. In particular, it allows IPv6 addressing, which allows all devices in a Thread network to have an IPv6 address so that they can be accessed directly from local devices on a home network (HAN) or off-network using *Thread-capable* IP routers called *border routers*. The nodes on the network form the global IPv6 addresses from the prefixes assigned by the *border routers* or locally by a self-assigned prefix to form a ULA (*Unique Local Address*). The *routing* IDs used in the network are assigned by the leader. Thread exploits UDP (*User Datagram Protocol*) so as to further lighten the connection, even at the expense of functionality on the certainty of transmission and error control.⁹⁴

Ultimately Thread is a Mesh Network technology designed for high levels of security and based on low power *IoT* protocols. It uses IPv6 (6LoWPAN), works on 802.15.4 protocol, and is legacy-free designed with architecture update.

It supports over 250 nodes. In a Thread network, the maximum number of active routers is 32. Routing information can be efficiently distributed across the network and all routers maintain visibility of all routes within the network. When nodes are added to the network and the topology changes, the network adapts by exchanging MES messages (Mesh Link Establishment)⁵³. Energy optimization is provided by keeping devices in dormant state most of the time. Thanks to the features given by the concept of Mesh networks it has a high resilience to failures.

It is also defined as an interoperable protocol; in fact, The Thread Group has defined a standard test harness to be used for the certification of all Thread *Stacks* and final Thread products. This test harness is provided to companies that are members of the Thread group for the development and testing of the *Software* prior to certification.

All Thread components (IC, *Software Stack* or modules) must be certified as thread-compliant before being used in the final products. All final products intended to carry the Thread logo must be presented for laboratory certification at an authorized test laboratory.

9 ⁹⁴ SKIP ASHTON, Vice Presidente di *IoT Software*, Silicon Labs. <https://it.electronics-council.com/seven-Keys-understanding-thread-protocol-39972>

Recently, the ZigBee Alliance and Thread Group announced a collaboration to allow the ZigBee Cluster Library to run on Thread networks. This interoperability will help simplify product development and improve the consumer experience in the connected home.^{72 95 96}

Thread "being a protocol based on open standards has also enabled *Open Source* implementation, such as OpenThread *Stack Nest*, allowing developers to evaluate technology using example code"⁹⁷. **Openthread** is licensed under the BSD 3-Clause "New" or "Revised" License. This is a similar license to the BSD 2-Clause License, but with the addition of the third clause prohibiting the use of the project name and its contributors to promote products developed without explicit consent.⁹⁸

All the necessary Nest Thread documentation is available on the site:

<https://www.threadgroup.org/Support>

The OpenThread documentation can be found at: <https://openthread.io/>

The sources of OpenThread can be found at: <https://github.com/openthread/>

As a test and development kit, OpenThread recommends:⁹⁹

Hardware:

- 3 Nordic Semiconductor nRF52840 dev boards
- 3 USB to Micro-USB cables to connect the boards
- A Linux machine with at least 3 USB ports

Software:

- GNU Toolchain
- Nordic nRF5x command line tools
- Segger J-Link *Software*
- OpenThread and wpantund
- Git

La board nRF52840DK è una singolboard Development kit che supporta Bluetooth5/Bluetooth mesh/Thread/Zigbee/802.15.4/ANT/2.4 GHz. Il datasheet è all'indirizzo:

<https://www.nordicsemi.com/-/media/Software-and-other-Downloads/Product-Briefs/nRF52840-DK-product-brief.pdf?la=en&hash=5D78D8104D4FC04D539BDBACFBB5150F34487447> .

Ant / Ant+

ANTTM is a proprietary Ultra Low Power *Wireless* (ULP) protocol developed and sold by the Canadian company Dynastream Innovations Inc., a subsidiary of Garmin Ltd.

⁹⁵ Thread *Stack Fundamentals*. Thread Group Luglio 2015.

⁹⁶ https://www.threadgroup.org/Portals/0/documents/support/ThreadWebinarJun18final_2596_1.pdf

⁹⁷ SKIP ASHTON, Vice Presidente di *IoT Software*, Silicon Labs. <https://it.electronics-council.com/seven-Keys-understanding-thread-protocol-39972>

⁹⁸ <https://github.com/openthread/openthread/blob/master/LICENSE>

⁹⁹ <https://codelabs.developers.google.com>

Currently, ANT™ can manage all the topologies of low-speed data sensor networks from *Peer-to-Peer* or *Star*, to *Mesh*, as personal networks (PAN) on a 2.4 GHz *Wireless* network, the major applications have been in sport, fitness, wellness and home health applications. It is also a practical solution for local area networks (LANs) in domestic applications and low-rate industrial automation.

The ANT protocol is set to use a single 1-MHz channel for multiple nodes thanks to the *time-division-multiplex* technique. Each node transmits in its own time interval. The transmission time of the basic message is 150 µs, while the speed of the message, the time between transmissions, goes from 0.5 Hz to 200 Hz with 8 bytes per message. Error detection occurs by applying the 16-bit CRC sumchek. 65,536 time slots per channel are possible. To avoid interference, the nodes change channels. The modulation is GFSK.

The ANT devices work on RF frequencies from 2400 MHz to 2524 MHz and can use safety devices based on public network keys, a private network key or a privately-run network key.

The 2457 MHz frequency is excluded from the above range because it is reserved for ANT+ devices, like the ANT+ key.^{100 101}

Ant+ are a set of profiles defined by the Ant+ Alliance to manage shared interoperability between the various ANT devices. The Ant+ profiles operate on the ANT protocol, for the various applications, so as to encourage interoperability and open access to data between the various device manufacturers.

The profiles currently most used are the Heart rate monitor, Bike speed and cadence sensors, Bike power sensors, Weight scales, Fitness equipment data sensors, and Temperature sensors. All ANT+ devices have their own profile. Each profile determines the functions of the device to which it refers and is pre-configured in the various display terminals, such as PC, Smartphone and tablet, together with the type of device and the sensors with which it is equipped.

Various user license profiles are provided, the highlights of each of these profiles are shown below.

The ANT+ license is applied when creating a product that must interact in the ANT+ world. In this case, you can access the Download section of the site where pre-configured profiles of ANT+ devices and a series of design tools are available. The elements marked with the ANT+ logo are accessible only to ANT+ Adopters, and to access them you must register as ANT+ Adopters, registration is free. Registration entitles you to access the forum and ANT+ network keys. Furthermore, in order to participate in the development of new ANT+ device profiles, obtain direct technical support and participate in B2B opportunities such as the ANT+ Symposium; you must be part of the ANT+ Alliance.

1 ¹⁰⁰ What's The Difference Between Bluetooth Low Energy And ANT? Lou Frenzel | Nov 30, 2012. <https://www.electronicdesign.com>

1 ¹⁰¹ https://web.archive.org/web/20160304125934/http://cwi.unik.no/images/8/84/Wireless_technologies.pdf

All the *Software* that can be downloaded from the *Download* page of the site is under the Apache 2.0 license or with the license of the FIT protocol. The *Software* marked with an ANT+ icon, is only accessible to ANT+ Adopters and is covered by the ANT+ shared license.

The *Hardware license* for cards that already include the ANT protocol, such as those produced by Nordic Semiconductor (for example nRF24AP2 and TI CC257x), and the related modules within a project, does not require a license.

If you work to implement a product that does not implement an ANT+ device profile, therefore a non-ANT+ product, the use of the ANT+ network button or the ANT+ frequency (2457MHz) is prohibited, but it is possible to use any other frequency and the public network key or a private network key. This rule is part of network key licenses.

The ANT protocol *stack* is not always present in the device, in particular for System in Chip (SoC) devices, in which case it is possible to download and install it as a separate component.

Equally, Garmin Ltd, on its website www.Thisisant.com, highlights that the Nordic Semiconductor series nRF51 SoCs are not equipped with ANT *stacks* and are accessible via a click-through agreement from the Nordic website.

In this case the ANT *Wireless* license is issued in two forms, either evaluative or for commercial purposes that generates revenue. In the first case it is free, in the second a royalty is paid for each instance associated with the use of ANT *stacks* that generate revenue.

All required ANT™/ANT+™ documentation is available on the manufacturer's and ANT+ Alliance websites.

The FIT SDK for development falls under the aforementioned licenses and can be downloaded from the developer section of the site www.thisisant.com, on the *Download* page.

As a test and development kit we recommend the purchase of **2 ANT USB2 Sticks, which have the following features:**

- **2403 to 2480MHz world-wide ISM band**
- **78 selectable RF channel**
- **ANT channel combined Message rate up to 190Hz (8byte data Payload)**
- **Minimum Message rate per ANT channel 0.5Hz**
- **Burst transfer rate up to 20Kbps (true data Throughput)**
- **Up to 8 ANT channels** — Up to 3 public, managed and/or private network Keys
- **1 Mbps RF data rate, GFSK modulation**
- **2 nd generation ANT feature enhancements**
- **15°C to +70°C operating temperature**

- **Type A USB connector**
- **WHQL certified Windows driver**
- **No driver installation is required on Mac OS X machines**
- **ANT library files for *Applications* development**
- **Radio regulatory approval for major markets**

They can be purchased in Europe on the website: <https://www.digiKey.it/products/it?Keywords=ant%2B&pKeyword=ant%2B&Keywords=ANTUSB2+Stick&v=>

There are also *Open Source* implementations of the ANT protocol, they are the **ANT+minus**, developed by the user GitHub *ralovich* implemented in C++, and the **python-ant** created by the user GitHub *mvillalba*.

The ANT+minus project is located at <https://github.com/ralovich/antpm>.

The python-ant project is located at <https://github.com/mvillalba/python-ant>.

Wireless-HART

Wireless-HART (*Highway Addressable Remote Transducer Protocol*) is a variant based on the DSSS (*Direct Sequence Spread Spectrum*) of IEEE 802.15.4 based on centralized *wireless* networks. It was created by the HART *Communications* Foundation (HCF) consortium of companies and is now owned by the FielComm Foundation, born of the union of HCF and Fieldbus Foundation. It shares the PHY level with the IEEE standard (and therefore operates in the ISM band) but has its own MAC level based on TDMA (*Time-division multiple access*). The network layer supports mesh network technology. Creating a mesh network that self-organizes and self-repairs, using a network manager even if the network is centralized, it meets the performance and security requirements for industrial applications. By prioritizing packages, *WirelessHART* ensures the operation of a network and assigns sufficient bandwidth to monitoring and control applications. *WirelessHART* uses standard AES-128 ciphers and keys at both the MAC and network levels. With the introduction of channel hopping on IEEE 802.15.4 PHY, *WirelessHART* can support a very high reliability and coexist with other IEEE 802.15.4.80 based protocols.⁸⁰

The development of HART devices requires the purchase of protocol documents: <https://fieldcommgroup.org/hart-specifications>

The proprietary foundation provides a list of kits: <https://www.fieldcommgroup.org/zh-hans/Node/153>

7.2.3 Comparative Tables

The following tables show comparisons of the major protocols used for *IoT* at network level. The comparison arises from the study of the documentation made available by the association/consortium of reference or by the internationally accepted standard, which is

usually issued by the IEEE or ISO/IEC. Some of them, such as the standards that do not include the physical and MAC levels, developing the ISO/OSI model levels (not covered by the standard), fall into the IEEE 802.15.4 standard, among which Zigbee, *Wireless* Hart, Thread and other protocols are to be considered. In the following tables they are not always explicitly mentioned. The tables show the characteristics on the rows and the protocol on the columns. The colouring of the characters shows the type of protocol (Cable, WLAN, BAN, PAN, ULPW, LWPA, Cellular Like, Cellular) and reflects the colours of Figure 14 on page 30.

Table 10: General comparison of the protocols that also define the physical and MAC level

Protocollo di connessione	Tipo	Standard	Descrizione	Capacità	Ideale per	Frequenza	Hardware aggiuntivo al dispositivo IoT
Wifi 802.11 a/b/g/n	WLAN	Disponibile nell'apposito sito IEEE: https://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=68	Standard di trasmissione per le reti WLAN	Centinaia di Mbps	Reti con un gran numero di utenti e con un grosso carico di dati	2,4 o 5 GHz.	Non ha bisogno, gratuito dove disponibile, si paga il traffico
Ethernet 802.3	Cavo	Specifiche nel sito del gruppo IEEE dedicato: http://www.ieee802.org/3/	Tecnologia di trasmissione via cavo	Cavo a 10, 100 e 1000 Mbit/s	Dispositivi fissi che richiedono un grosso flusso di dati e/o una connessione estremamente stabile	-	Non ha bisogno, gratuito dove disponibile, si paga il traffico
M-Bus	Cavo	Standard EN 1434-3 (1997), M-Bus rivisto e aggiornato dallo standard EN 13757	M-Bus(Meter Bus) è un protocollo definito a livello applicativo del modello ISO/OSI, pensato e sviluppato per la lettura di contatori di energia (elettricità, acqua, gas, calore)	Comunicazione seriale tipicamente a 300, 2400 e 9600 bps	Lettura di contatori di energia (elettricità, acqua, gas, calore)	-	Non ha bisogno, rete locale
RFID	BAN / Basso consumo / contactless	Vari standard ISO dipendenti dal tipo di tag utilizzato	Tecnologia per memorizzazione di dati in appositi tag elettromagnetici e la loro lettura/scrittura tramite radiofrequenze	Wireless, con raggio molto ridotto. Frequenza e bitrate variano molto in base al tipo di tag	Apparecchi con poche informazioni che devono durare nel tempo (chip delle tessere, sistemi antitaccheggio, etc)	Low frequency LF: 125-134 kHz High frequency HF: 13.56 MHz Ultra-high frequency UHF: 433-860-960 MHz	Non ha bisogno, rete locale
NFC	Contactless / Basso consumo	Standard: ISO/IEC 18000-3	Protocollo wireless tramite NFC tag e appositi lettori. Caso particolare di RFID	Range: 10cm, Bitrate 100-420kbps	Oggetti che interagiscono tra di loro a distanza molto ravvicinata (es pagamenti contactless)	13.56MHz (ISM)	Non ha bisogno, rete locale
WM-Bus	PAN	EN 13757-3/5 PrEN 1357-4	M-Bus(Meter Bus) è un protocollo definito a livello applicativo del modello ISO/OSI, pensato e sviluppato per la lettura di contatori di energia (elettricità, acqua, gas, calore)	Wireless con range variabile dai pochi centinaia di metri a 868MHz a circa 1,5Km a 169MHz.	Lettura di contatori di energia (elettricità, acqua, gas, calore)	868MHz, 433MHz, 169MHz	non ha bisogno, rete locale
Bluetooth	PAN	Specifiche nel sito della Bluetooth SIG (Basic Core Specification): https://www.bluetooth.com/specifications	Tecnologia wireless master-slave per comunicazioni a corto raggio	raggio circa 100m, bitrate circa 1Mbps	Reti locali, wearable.	2.4GHz (ISM)	Non ha bisogno, rete locale
BLE – Bluetooth Low Energy	PAN / Basso consumo	Sito della Bluetooth SIG (Low Energy Specification): https://www.bluetooth.com/specifications	Tecnologia wireless master-slave per comunicazioni a corto raggio e con un modesto flusso di dati, a bassissimo consumo energetico	Uso simile al Bluetooth, ma per trasmissioni corte	Dispositivi sempre connessi che scambiano pochi dati (es. apparecchi medici)	2.4GHz (ISM)	Non ha bisogno, rete locale
Ingenu / RPMA	LPWAN	Standard spiegato nel sito Ingenu: https://www.ingenu.com/technology/rpma/lpwa/	LPWAN ottimizzata per essere affidabile a lunghe distanze e grandi numeri di dispositivi utilizzando RPMA (Random Phase Multiple Access)	Range di decine di km,	IoT in generale	2.4GHz (ISM)	RPMA attualmente è disponibile in alcune zone degli USA, in espansione
SigFox	LPWAN / Cellular-like	Protocollo proprietario SigFox: https://www.sigfox.com/en , i propri dispositivi sono certificati e pronti all'uso	Rete globale pensata per l'IoT e la trasmissione di brevi messaggi	200 kHz, bitrate 100-600Kbps	IoT in generale	868 Mhz	Rete di propri operatori (NetTrotter in Italia)

Weightless	LPWAN	Fare riferimento alle specifiche presenti sul sito: www.weightless.org/keyfeatures/capacity	licenze proprietarie e royalty-free per la comunicazione M2M wireless. Primo e unico standard M2M al mondo progettato per funzionare anche nello spazio bianco dello spettro TV. Presenta tre diverse specifiche tutte e tre sub-giga, utili a seconda	Weightless W	Si appoggia sullo spettro non utilizzato dalle TV (non utilizzabile ovunque). La copertura media è di 5 km in ambienti urbani e 10 km in ambiente rurale.	Reti basate su sensori, letture della temperatura, monitoraggio del livello del serbatoio, misurazione intelligente e altre applicazioni simili.	470-790 MHz in TDM	Non ha bisogno, rete locale
				Weightless N/Nwave	Nwave. Il data-rate si aggira fra 30-100 kbps ed è pensato per gli end-device che necessitano di comunicazioni unidirezionali a basso costo. Utilizza frequenze sub-GHz e fornisce una copertura di 5 km anche in ambienti urbani.	Reti basate su sensori, letture della temperatura, monitoraggio del livello del serbatoio, misurazione intelligente e altre applicazioni simili.	Tutte le Sub-1GHz permesse: 169, 433, 479, 780, 868, 915, 923 MHz	Non ha bisogno, rete locale
				Weightless P	Estensione dello standard Nwave permettendo la comunicazione bidirezionale in uplink e downlink. La copertura è di circa 2 km in ambiente urbano.	Private networks, casi d'uso complessi e casi in cui è necessario la certezza della trasmissione e necessità di comunicazione bidirezionale.	FDMA+TDMA modulation in 12.5 kHz narrowband	Non ha bisogno, rete locale
LoRaWAN	LPWAN / Cellular-like	Definito dalla LoRa alliance: https://loralliance.org/resource-hub Corrente: https://loralliance.org/resource-hub/lorawantm-specification-v11	Architettura di rete star-of-star, dove i gateway gestiscono i messaggi tra i dispositivi e il server centrale.	0.3-50 kbps			Dipende dai vari stati	Connettività basata sugli operatori membri della LoRa Alliance
LTE-M	LPWAN / Cellular	Standard 3gpp: https://www.3gpp.org/news-events/3gpp-news/1805-iot_r14	LTE-M (o LTE-MTC, Machine Type Communication), è un tipo di LTE LPWAN pensata per il m2m e l'IoT ma con caratteristiche di rete cellulare.	Bitrate 1Mbps		IoT in generale	Si basa su LTE e utilizza le sue frequenze	Non ha bisogno, gratuito dove disponibile, si paga il traffico
NB-IoT	LPWAN / Cellular	Standard 3gpp: https://www.3gpp.org/news-events/3gpp-news/1805-iot_r14	Standard simile a LTE-M ma non necessariamente legato a LTE. In Italia implementato dalle compagnie telefoniche nelle proprie reti	Bitrate 250Kbps		IoT in generale	800Mhz	Non ha bisogno, gratuito dove disponibile, si paga il traffico
EC-GSM-IoT	LPWAN / Cellular	Standard 3gpp: https://www.3gpp.org/news-events/3gpp-news/1805-iot_r14	Tecnologia 2G per sopperire alle zone dove non è possibile utilizzare LTE	474 kbit/s (EDGE) 2 Mbit/s (EGPRS2B) Alta latenza		IoT in generale		Non ha bisogno, gratuito dove disponibile, si paga il traffico
GSM	Cellular	https://www.3gpp.org/specifications	Standard di seconda generazione di telefonia mobile sviluppato dall'ETSI	Sistema best-effort, la qualità del servizio dipende dall'utilizzo della rete da parte di tutti i dispositivi. Range 35km		Data la capillarità della rete nel mondo, è adatta ad apparecchi che devono comunicare a lunghissime distanze	850, 900, 1800, 1900 MHz	Non ha bisogno, gratuito dove disponibile, si paga il traffico
CDMA	Cellular	W-CDMA: https://www.3gpp.org/technologies/keywords-acronyms/104-w-cdma	Protocollo di accesso multiplo ad un canale. Nato per le reti 2G, le versioni successive (W-CDMA) sono parte delle tecnologie 3G	Dato che tutti i dispositivi trasmettono sullo stesso canale, il servizio dipende da come e quanto il canale è utilizzato		Data la capillarità della rete nel mondo, è adatta ad apparecchi che devono comunicare a lunghissime distanze	Come GSM	Non ha bisogno, gratuito dove disponibile

Table 11: General comparison of the analysed protocols based on other standards

Protocollo di connessione	Tipo	Standard	Descrizione	Capacità	Ideale per	Frequenza	Hardware aggiuntivo al dispositivo IoT
DigiMesh	PAN / WLAN	Non chiaramente specificato, in quanto proprietario e associato ai moduli dell'azienda	Protocollo mesh proprietario simile a ZigBee ma con un'architettura con un unico tipo di nodo e funzioni di sleep		Reti che richiedono un setup semplice, reti che richiedono funzioni di sleep	900-868-865MHz, 2.4 GHz	Non ha bisogno, rete locale
Zigbee	PAN / WLAN	ZigBee Alliance Network specification: https://www.zigbee.org/zigbee-for-developers/network-specifications/	Lan mesh basata su IEEE802.15.4	Range fino a 100m, bitrate circa 250kbps	Domotica e controllori	2.4GHz (ISM)	Non ha bisogno, rete mesh locale
DASH7	PAN / WLAN	DASH7 Alliance Protocol: http://www.dash7-alliance-protocol/	Nato da uno standard ISO come protocollo RFID per usi militari, una sua evoluzione viene rilasciata nel 2011 per applicazioni commerciali	Range di 2km, bitrate di circa 160kbps	Applicazioni su larga scala per evitare l'uso di cavi (es: sistema di conteggio dei parcheggi liberi)	433 MHz, 868 MHz e 915 MHz (ISM)	Non ha bisogno, rete locale
Z-Wave	PAN	Raccomandazioni date dalla Z-Wave alliance: https://z-wavealliance.org/ https://z-wavealliance.org/wp-content/uploads/2018/03/ZAD12837-10.pdf	Protocollo wireless progettato appositamente per la domotica. I nodi possono essere controllori (almeno uno richiesto, ospitano le tabelle di indirizzamento) o slave	Range 30-40 metri tra 2 nodi	Domotica	868.42 MHz (Europa), 908.42 MHz (Nord America), altre frequenze ISM in altre regioni in base alle regolamentazioni locali	Almeno uno dei dispositivi deve fare da controllore della rete mesh
Thread	PAN	Basato su IEEE 802.15.4 e 6LoWPAN	Protocollo wireless per reti mesh a basso consumo		IoT in generale	2.4GHz (ISM)	Non ha bisogno, sfrutta il protocollo IP implementato nei dispositivi
Ant/Ant+	ULPW LAN / BAN / PAN	Proprietario: https://www.thisisant.com/developer/ant/licensing/	Ultra Low Powered network punto a punto, stella, albero o mesh per PAN o LAN. ANT+ è un protocollo di comunicazione per reti ANT	Range 30m, bitrate 12.8-60 kbps	Embedded devices, usato principalmente per registrare dati fitness	2.4GHz, 2457MHz riservata a ANT+	Non ha bisogno, rete locale. Richiede antenne esterne per connessione con iOS e Android
Wireless HART	PAN	Basata sullo standard HART ("Highway Addressable Remote Transducer"). International standard IEC62591- IEEE 802.15.4 standard radios	Tecnologia wireless pensata per l'automazione di processo. Si aggiunge funzionalità wireless al protocollo HART mantenendo la compatibilità con dispositivi esistenti HART.	WirelessHART può essere utilizzato su strumenti cablati esistenti per raccogliere la grande quantità di informazioni precedentemente bloccate nello strumento e offre inoltre un modo economico, semplice e affidabile per implementare nuovi punti di misurazione e controllo senza i costi di cablaggio.	Automazione di processo. Ambiti Industriali	2.4 GHz ISM band	La componentistica dipende dall'applicazione.

Table 12: Technological comparison of the protocols analysed for WLAN and PAN

	RFID	NFC	Bluetooth Low Energy	IEEE 802.15.4	Z-Wave	Wireless HART	WM-BUS	Weightless W	Weightless N	Weightless P	IEEE 802.11ah
Standard	ISO/IEC 18000, 29167, 20248, JTC 1/SC 31. Global: 6 MHz	ISO/IEC 14443, 18092 JIS X6319-4	IEEE 802.15.1	IEEE 802.15.4	ITU G.9959 Based	HART MAC IEEE 802.15.4 PHY	EN 13757-3/5 PrEN 1357-4	Weightless SIG	Weightless SIG	Weightless SIG	IEEE 802.11ah
Frequency band	Global: 6 MHz ISM: 13.5 MHz ISM: 433 MHz ISM ELI: 863-870 MHz ISM NA: 902-928 MHz ISM: 2.4 GHz I-JWB: 5-27 GHz	13.56 MHz	2.4 GHz	EU: 868 MHz NA: 915 MHz Global: 2.4 GHz	EU: 868 MHz NA: 915 MHz	Global: 2.4 GHz 250 kb/s	868 MHz, 869 MHz, 433 MHz, 169 MHz	TV White spaces 470-790MHz	ISM Sub-GHz, EIJ (868MHz), US(915MHz)	ISM Sub-GHz, EIJ (433/470/868 MHz), US (915 MHz), Asia (430 MHz)	Sub-iGHz
Data rate	500 Kb/s @ Payload of 16 32 bits	106 kb/s or 212 kb/s or 424 kb/s 848 Kbps	1 Mbps	20 kb/s @ 868 MHz 40 kb/s @ 915 MHz 250 kb/s @ 2.4 GHz	9.6, 40 and 100 kb/s		Da 2,4 kbps a 100 kbps	1 kb/s - 10 Mb/s	30 kb/s-100 kb/s	200 b/s - 100 kb/s	0.15-4 Mb/s @ BW=1MHz 0.65-7.8 Mb/s @ BW=2MHz
Typical range	0.1 - 5 m	0.1 m	70m	10-100 m @ 2.4 GHz	100 m	10-600 m	Da ~100m con 868 a oltre 1,5km a 169MHz	5 km	2 km	2 km	100-1000m
TX power	1,5 mw	20 or 23 dBm	0 – 10dBm	0 – 20 dBm	1mW 0dBm	10 dBm		17 dBm	17 dBm	17 dBm	>0 – 1 W (@ local regulations)
Bandwidth per channel	10 MHz @ 6 MHz 14 MHz @ 13.5 MHz 1.74 MHz @ 433 MHz 7 MHz @ 800 MHz 8 MHz @ 2.4 GHz 5-27 GHz segmented	Variable	40 channels of 2 MHz width	868 MHz band: 0.3 MHz 915 MHz band: 0.6 MHz 2.4 GHz band: 2 MHz	300, 400 kHz	2 MHz	169MHz: 12,5 kHz	5 MHz	200 Hz	12.5 kHz	1, 2, MHz or 16 MHz for GFSK
Modulation	Proximity	ASK,	GFSK	O-QPSK	GFSK	O-QPSK	GFSK	BPSK	D3PSK	GMSK	

Table 12: Technological comparison of the protocols analysed for WLAN and PAN

	RFID	NFC	Bluetooth Low Energy	IEEE 802.15.4	Z-Wave	Wireless HART	WM-BUS	Weightless W	Weightless N	Weightless P	IEEE 802.11ah
Transmission / Technique	Field Modulation Induced Pulse	BPSK	FHSS Star	BPSK ASK DSSS	CSMA-CA	BPSK ASK	4GFSK	QPSK 16-QAM DB-PSK	slotted ALOHA	offset-QPSK FDMA+TDMA	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM OFDM
Topology	Point to Point Point to Multipoint	Peer-to-peer	Single-Hop	Mesh	Mesh	Star Cluster Mesh	Star Tree Linear	Star	Star	Star	Star
Power saving mechanisms		N/A	Standby mode	only in ZigBee RF4C	Sleep / Wakeup Modes	On / Off Radio	Sleep / Wakeup Modes	N/A	N/A	N/A	Native
Packet length	16—64 Kbps	Segments	8 to 47 bytes	100 bytes	255 bits	250 bits	Max 256 bits	> 10 bytes	< 20 bytes	> 10 bytes	100 bytes
Security	Clandestine Tracking and Inventorying EPC Discovery Service	Encryption Cryptographic, Secure Channel, Key Agreements.	Advanced Encryption Standard (AES) a—12 bits	AES-128	AES-128	Cipher Block Chaining Message Authentication Code (CCM) AES-128	AES-128	AES-128	AES-128	AES-128	WPA
Licensing	Free	Free	Free	Free	Free	Free	Free	Free	Free	Free	Free
Scalability	Limited	Peer to Peer	5917	Upper layers	232	N/A	256	High	High	High	8191
Typical scenarios	Human Implantation Tracking Identification	Healthcare, Smart Environment, Mobile Payment, Ticketing & Loyalty	Multimedia data exchange between nearby Nodes	Multi-Hop networks with few Nodes	Automation in residential and light commercial	Industrial	Smart Metering	M2M Applications	M2M Applications	M2M Applications	One-Hop networks with many Nodes

Table 13: Technological comparison between protocols for LPWAN/Cellular Like

	NB-IOT	Cat-M	Cat-0	LoRaWAN	Sigfox
Standard	3Gpp	3Gpp	3Gpp	LoRaWAN	Sigfox
Frequency band	Licensed	Licensed	Licensed	EU: 868MHz US: 433/915MHz AS: 430MHz	ELI: 868MHz US: 902MHz
Data rate	DL: 234.7 kb/s UL: 204.8 kb/s	UL/ DL: 1 Mb/s	UL/ DL: 1 Mb/s	22 b/s @BW=7,8kHz / SF=12 27 kb/s @BW=500kHz / SF=7 100kbps @ GFSK for Europe	100 bps (UL) 600 bps (DL)
Typical range	Deployment Driven	20Deployment Driven	Deployment Driven	5 km (urban) 15 km	15 Km LOS

	NB-IOT	Cat-M	Cat-0	LoRaWAN	Sigfox
	Km LOS	~5 Km	~5 Km	LOS	
TX power	23 dBm	23 dBm	23 dBm	EU: 13 dBm US: 20 dBm	EU: 14 dBm (ETS 300-220) US: 21.7 dBm
Bandwidth per channel	180 kHz	1.4 - 20 MHz	1.4 - 20 MHz	0.3 MHz: 863-870 MHz 2.16 MHz: 902-928 MHz	100 Hz (600 Hz USA)
Modulation - Transmission Technique	GFSK BPSK – FDD	OFDMA SC-FDMA - FDD/TDD	OFDMA SC-FDMA - FDD/TDD	Proprietary CSS - FHSS (Aloha)	DBPSK (UL) GFSK (DL) – UNB
Topology	Star	Star	Star	Star of stars	Star
Power saving mechanisms	PSM EDRX	PSM EDRX	PSM EDRX	3 Devices classes operation	Deployment Driven
Battery operation	Many Years	Many Years	Many Years	Many Years	Many Years
Packet length	Network Deployment Driven	Network Deployment Driven	Network Deployment Driven	255 Bytes	12 Bytes UL 8 Bytes DL
Secyurity	NSA AES 256	AES 256	AES 256	AES CCM 128	Key Generation, Message Encryption, MAC Verification, Sequence
Licensing	Technology freely available for chip/Device vendors. Network operators owns and manages its networks	Technology freely available for chip/Device vendors. Network operators owns and manages its networks	Technology freely available for chip/Device vendors. Network operators owns and manages its networks	Technology licensed by Device vendors. No royalty to be paid by network operators Network	Technology freely available for chip/Device vendors. Network operators pay royalty to Sigfox (revenue sharing basis)
Scalability	Network Deployment Driven	Transport Layer Il transport layer raccoglie tutte le tecnologie che forniscono una comunicazione logica tra il Network Access Layer e il Session / communication layer. I protocolli presi in considerazione in questo studio sono quelli più usati nell'ambito IoT e sono comparati nella Table14. Network Deployment Driven	Network Deployment Driven	>10000 Network Configuration	>10000 Network Configuration
Typical scenarios	M2M, Tracking, Smart Things, Point Of Sales (POS) terminals, Mobile Applications.	M2M, Tracking, Smart Things, Point Of Sales (POS) terminals, Mobile Applications-	M2M, Tracking, Smart Things, Point Of Sales (POS) terminals, Mobile Applications.	Building Automation and Secyurity, Smart Metering, Land Agriculture, White Goods Household Information Devices, Tracking, Positioning	Building Automation and Secyurity, Smart Metering, Land Agriculture, White Goods Household Information Devices, Tracking, Positioning

7.3 Transport Layer

The transport layer contains all the technologies that provide logical communication between the *Network Access Layer* and the *Session/communication layer*. The protocols

taken into consideration in this study are those most used in the *IoT* context and are compared in table 14

Table 14: Comparison of transport protocols

Trasporto	IPv4	IPv6	6LoWPAN	RPL
Standard	RFC 791: https://tools.ietf.org/html/rfc791	RFC 8200: https://tools.ietf.org/html/rfc8200	RFC 4944: https://tools.ietf.org/html/rfc4944	RFC 6550: https://tools.ietf.org/html/rfc6550
Descrizione	Protocollo internet a pacchetti. Gli indirizzi vengono codificati in 32 bit, più comunemente visti come 4 numeri da 0 a 255 separati da un punto.	Miglioramento di IPv4, in cui gli indirizzi sono codificati a 128 bit (8 word esadecimali di 4 caratteri separate dai due punti)	IPv6 per Personal Area Network deboli. L'header e l'incapsulamento vengono compressi per ridurre i pacchetti	Protocollo IPv6 di routing per reti deboli e/o instabili basato su IEEE 802.15.4
Uso	Creato come protocollo universale, di base non ha un uso specifico	Creato come protocollo universale, di base non ha un uso specifico	Ethernet, Wi-Fi, 802.15.4, sub-1GHz ISM, Bluetooth Smart (2.4GHz), ZigBee	802.15.4
Ideale per	Protocollo general purpose	Protocollo general purpose	Domotica o rete di un edificio	Apparecchi poco potenti

7.3.1 IPV4

IPv4 is the fourth version of the Internet protocol, developed in 1979 and released as IETF RFC 791 in 1981. It uses a 32-bit code for addressing, usually read as 4 numbers from 0 to 255 separated by a dot ".", for a maximum of about 4.3 billion different connected devices. This limit has become important as the years and the technological process progresses. The use of NAT (*Network Address Translation*) has partially reduced the problem, to the detriment of RTC (*Real Time Communication*). It is used globally for LANs and Internet access.¹⁰³

7.3.2 IPV6

IPv4 is the fourth version of the Internet protocol, developed in 1979 and released as IETF RFC 791 in 1981. It uses a 32-bit code for addressing, usually read as 4 numbers from 0 to 255 separated by a dot ".", for a maximum of about 4.3 billion different connected devices. This limit has become important as the years and the technological process progresses. The use of NAT (*Network Address Translation*) has partially reduced the problem, to the detriment of RTC (*Real Time Communication*). It is used globally for LANs and Internet access.¹⁰³

IPV6

IPv6 is the update for IPv4, released as IETF RFC 2460 in 1999, then rendered obsolete by the new release of the IETF RFC 8200 in 2017. Compared to IPv4, the addresses pass to 128 bits, usually read as 4 hexadecimal digits from 0 to FFFF separated by a colon ":", considerably increasing the number of unique addresses available. Some additional features compared to IPv4 are:

- *Auto-configuration*: the devices are able to independently configure their address without user intervention or DHCP.

1 ¹⁰³ Khan, Rafiqul Zaman. (2015). A Comparative Study on IPv4 and IPv6. International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682 Vol.33, No.33, January 2015. 33. 9-16.

1 ¹⁰³ Khan, Rafiqul Zaman. (2015). A Comparative Study on IPv4 and IPv6. International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682 Vol.33, No.33, January 2015. 33. 9-16.

- *No NAT*: given the high number of available addresses, each Device can have its own, without using a NAT.
- *Automatic IP renumbering* in case of changes (extensions, merges) to the network.
- *IP mobility*: a device can move and change networks without getting lost and getting its IP address reassigned.
- *Mandatory IPsec*, increasing connection security.¹⁰³

7.3.3 6LoWPAN

6LoWPAN is a standard based on 802.15.4, developed by IETF to easily adapt to 32K flash memories (much smaller than Zigbee or other protocols) and designed to be used in small sensor networks. It uses IPV6 (although with a *header* compression system) and is currently regulated by RFC 8066. The networks that implement 6LoWPAN are characterized by being simple, cheap and requiring little or no infrastructure and are typically used with limited battery devices operating in the POS (*Personal Operating Space*, about 10 meters).¹⁰⁴

7.3.4 RPL

RPL (*Low-Power and Lossy Networks*) is a *routing* protocol standardized by the IETF in 2011. It brings together the IETF *IoT* protocol *stack* and its *IoT* versatility is certified by the ZigBee Alliance's adoption of the standard. It uses a direct acyclic graph topology (DAG) in which each link is oriented towards the *router* called DODAG, *Destination-Oriented DAG*. The structure is created and maintained through the sending of DIO (*DODAG Information Object*) and DAO (*Destination Advertisement Object*) and through a data analysis function in each node that chooses its own parent node. RPL can work in 2 modes: in the first, "*storing mode*", each node also creates and maintains its own *routing* table; in the second, "*non-storing mode*", only the *router* node keeps the table and the *routing* information is encapsulated in each packet.¹⁰⁵

1 ¹⁰⁴ Omer, Khalid. (2019). Implementation and Analysis of the 6LoWPAN for the *Internet of Things Applications*: Future Networks. International Journal of Computer Science and Information Security, 17. 91

1 ¹⁰⁵ Oana Iova, Gian Pietro Picco, Timofei Istomin, and Csaba Kiraly. RPL, the Routing Standard for the *Internet of Things* ... Or Is It?

7.4 Session/communication

Taking the ISO/OSI model as a reference (see Figure 9) the *Session layer* is used to hide the *Transport Layer* and start active communication sessions between the machines.

The primary objective of this level is to establish, maintain and synchronize the interconnections between communication systems. It then manages and synchronizes the communications between two different applications by sending the data with information for the correct resynchronization, so as to prevent any accidental loss of data and information.

The session/communication level is involved in the following operations:

- sets, lowers and manages the communication between two end-points of the application;
- builds semi-permanent transport bridges for greater efficiency and organization of data flows;
- masks communication errors from higher level services in the OSI model;
- manages the synchronization of data from multiple session flows.

It should be noted that in the TCP/IP model, a model that directly inspires most *IoT Stacks*, the *Session Layer* is identified with the *Application Layer*.

Basically, on this level the protocols that are of interest are short and real time messaging protocols. An *IoT* system can be implemented with existing web technologies, although it will be less efficient than protocols specifically designed or designed for very close applications such as the M2M. Examples of these are, the *Hypertext Transfer Protocol/Secure* (HTTP/S) and *WebSockets* which are common standards, together with the *eXtensible Markup Language* (XML) or *JavaScript Object Notation* (JSON) in the *Payload*. Combining all this with a normal *web browser* you have an *HTTP client*, where with JSON tools you can develop at a comfortable level of abstraction for Web applications. When using a standard *web browser* (*HTTP client*), JSON provides web developers with an abstraction layer with an already established duplex connection to a *Web Server* and an HTTP communication.

As stated, the protocols that have normally been defined on this level are various, this shows how difficult and demanding it is to choose the most effective one, since the choice is strictly linked to the availability of the *IoT* system and its messaging requirements. None of the protocols developed so far can support all messaging requirements of all types of *IoT* systems. The messaging protocol is an ongoing dilemma for the *IoT* industry; consequently, it is important to understand the pros and cons of widely accepted and emerging messaging protocols for *IoT* systems that define their best scenarios.

This chapter includes the result of the analysis of messaging protocols developed for specific IoT/M2M applications (MQTT, CoAP, AMQP, DSS). Also included is the result of

the analysis of protocols used in the IoT sector but not designed specifically for this scope (XMPP). Finally, we will also include the analysis of the classic protocols (HTTP, FTP, Telnet, SSH), also not specifically designed for the IOT application but often used in this sector.

The analysis focuses on the most specific protocols, in some cases there will only be a description and an explanation of why it was included in the comparison. Therefore, the comparison between these messaging protocols is presented to introduce their characteristics in a comparative way. Subsequently, it follows further in-depth and relative analyses based on some interconnected criteria to obtain information on their strengths and limits.

7.4.1 HTTP

Hyper Text Transport Protocol (HTTP) is the predominant system in the *Web Messaging Protocol* scenario, it was developed by *Tim Berners-Lee*. Subsequently the development passed to the IETF in collaboration with the W3C and in 1997 the first standard was released. HTTP supports a RESTful *Web Request/Response* architecture. HTTP uses the *Universal Resource Identifier* (URI) and not the *Topics*. The *Server* sends the data through the URI and the *Client* receives the data through the URI. HTTP is a *Text-based* protocol and does not define the size of the header and the *Message Payload* that depends on the web server or programming technology. HTTP by default uses TCP as transport protocol and TLS/SSL for security. Therefore, the communication between *Client* and *Server* is connection-oriented. A QoS is not explicitly defined and requires additional modules to implement it. HTTP is now accepted globally as *standard Web messaging* and offers many features such as *persistent connections*, *Request pipelining* and *chunked transfer encoding*^{106 107 108}.

7.4.2 MQTT

Message Queuing Telemetry Transport (MQTT) is one of the first M2M communication protocols, developed by IBM and Arcom Control Systems Ltd, standardized, it is a messaging protocol for publishing/subscribing *Server Client*. Characterized as being light, open, simple and designed to be easy to implement. These features make it ideal for use in many situations, including constrained environments such as communication in *Machine to Machine* (M2M) and *Internet of Things* (IoT) contexts where a small code footprint and/or reduced use of band is required. The protocol can be based on TCP/IP or other network protocols that provide ordered two-way connections, without data loss.

Its features include:

-
- 1 ¹⁰⁶ I. Grigorik, "Making the web faster with HTTP 2.0," *Communications of the ACM*, vol. 56, no. 12, pp. 42–49, 2013
 - 1 ¹⁰⁷ N. Naik, P. Jenkins, P. Davies, and D. Newell, "Native web communication protocols and their effects on the performance of web services and systems," in *16th IEEE International Conference on Computer and Information Technology (CIT)*. IEEE, 2016, pp. 219–225
 - 1 ¹⁰⁸ N. Naik and P. Jenkins, "Web protocols and challenges of web latency in the web of things," in *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE, 2016, pp. 845–850

- Use of the publication/subscription message model which provides the distribution and decoupling of one-to-many message applications.
- A transport of messages that is agnostic to the content of the *Payload*.
- Three qualities of service for message delivery:

"At most once", where messages are delivered based on the best efforts of the operating environment. Message loss can occur. This level could be used, for example, with the environmental sensor data in which it does not matter if an individual reading is lost because the next one will be published immediately afterwards.

"At least once", where messages are sure to arrive but duplicates may occur.

"Exactly once", where messages are sure to arrive exactly once. This level could be used, for example, with billing systems where duplicate or lost messages could result in the application of incorrect rates.

A small transport *overhead* and protocol exchange minimized to reduce network traffic.

A mechanism to inform interested parties when an abnormal disconnection occurs.¹⁰⁹

The MQTT *Client* publishes the messages on an MQTT *Broker*, which holds the subscription of other *Clients* or gives the possibility of the *future* subscription. All messages are published on an address are defined as *Topics*.¹¹⁰ Each *client* can subscribe to multiple *topics* and receive messages from any one of them. MQTT is a binary protocol and requires 2 *bytes* for the *header* and incorporates a maximum *Payload* of 256 MB.¹¹¹ As mentioned, it can use TCP as a transport protocol and uses security based on TLS/SSL. The connection is, therefore, a connection-oriented communication of the *client-broker* type. Another important feature is the use of three levels of *Quality of Service* (QoS) to make delivery of the message reliable.¹¹²

MQTT is an excellent choice for extended networks of devices that must be monitored and controlled by a server through the internet. It is a protocol with basic features and offers very few control options.¹¹³

1 ¹⁰⁹ MQTT Version 5.0. Edited by Andrew Banks, Ed Briggs, Ken Borgendale, and Rahul Gupta. 07 March 2019. OASIS Standard. <https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.html>. Latest version: <https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html>

1 ¹¹⁰ T. Jaffey. (2014, February) MQTT and CoAP, *IoT protocols*. <https://eclipse.org/Community/eclipsenewsletter/2014/february/article2.php>

1 ¹¹¹ D. Thangavel, X. Ma, A. Valera, H.-X. Tan, and C. K.-Y. Tan, "Performance evaluation of MQTT and CoAP via a common middleware," in *Intelligent Sensors, Sensor Networks and Information Processing*, 2014 IEEE Ninth International Conference on. IEEE, 2014, pp. 1–6

1 ¹¹² S. Bandyopadhyay and A. Bhattacharyya, "Lightweight internet protocols for web enablement of sensors using constrained *Gateway Devices*," in *Computing, Networking and Communications (ICNC)*, 2013 International Conference on. IEEE, 2013, pp. 334–340

1 ¹¹³ Nitin Naik. Choice of Effective *Messaging* Protocols for *IoT* Systems: MQTT, CoAP, AMQP and HTTP. Defence School of Communications and Information Systems-Ministry of Defence, United Kingdom

Differences between the MQTT specifications of versions 3.1.1 and 5.0:

The specification documents can be found at the addresses:

Specification 3.1.1: <http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html>

Specification 5.0: <http://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html>

Added or updated features:

Session expiration: the *Clean Session flag* is divided into a *Clean Start flag*, which indicates that the session must start without using an existing session, and the session expiration interval, which indicates how long to keep the session after a disconnection. The session expiration interval can be changed upon disconnection. The setting of *Clean Start* at 1 and Interval expiration of the session at 0 is equivalent in MQTT v3.1.1 to the setting of *Clean Start* 1.

Expiration of the message: sets an expiration interval when a message is published.

ACK Identification Code: modifies all response packets to contain an identification code. Includes CONNACK, PUBACK, PUBREC, PUBREL, PUBCOMP, SUBACK, UNSUBACK, DISCONNECT and AUTH. This allows you to determine if the requested function was successful.

Reason string on all ACKs: changes most packages with an identification code to allow an optional explanatory string. Designed to identify problems and is not intended to be analysed by the receiver.

Server Disconnection: allows DISCONNECT to be sent by the *Server* to indicate the reason for the closure of the connection.

Payload format and content type: specifies the *Payload* format (binary, text) and a MIME-style content type when a message is published. These are forwarded to the recipient of the message.

Request/Response: formalizes the request/response model within MQTT and provide the properties of the Response argument and Correlation Data to allow *Routing* of reply messages to the *Publisher* of a request. Furthermore, adds the possibility for the *Client* to obtain configuration information from the *Server* on how to construct the response arguments.

Shared subscriptions: represents support for shared subscriptions and allows you to distribute the messages of a subscription group to members of the subscription group.

Subscription ID: allows you to specify a numeric subscription identifier in *Subscribe* and to return it in the message upon delivery. This allows the client to determine which subscription the message delivery refers to.

Topic aliases: reduces the size of the MQTT packet overhead by allowing you to shorten the topic name to a small integer. *Client* and *Server* independently specify the number of aliases of arguments they allow.

Flow control: allows the *Client* and the *Server* to independently specify the number of reliable messages allowed (QoS > 0). The sender stops sending these messages to stay below this quota. This is used to limit the rate of reliable messages and to limit the number of simultaneous messages.

User property: defines the user property for most packages. User properties on *Publish* are included in the message and defined by *Client* applications. The properties of the user on *Publish* and Will Properties are forwarded by the *Server* to the recipient of the message. The user properties on the CONNECT, *Subscribe* and *UNSubscribe* packages are defined by the *Server* implementation. The user properties on the CONNACK PUBACK, PUBREC, PUBREL, PUBCOMP, SUBACK, UNSUBACK and AUTH packages are defined by the sender and are unique to the sender's implementation. The meaning of the user's properties is not defined by MQTT.

Maximum packet size: allows the *Client* and *Server* to independently specify the maximum packet size they support. Returns error if the session partner sends a larger packet.

Availability of the optional functions of the *Server*: it defines a set of functions that the *Server* does not allow and provides a mechanism to the *Server* to indicate it to the *Client*. The features that can be specified in this way are: Maximum QoS, Keep Available, Available *Wildcard* Subscription, Available Subscription Identification, and Available Shared Subscription. It is a mistake for the *Client* to use the features that the *Server* has declared unavailable. In previous versions of MQTT for a *Server* it is possible not to implement a functionality by declaring that the *Client* is not authorized for that function. This function allows you to declare this optional behaviour and adds specific motivation codes when the *Client* still uses one of these features.

Advanced authentication: provides a mechanism to enable challenge/response style authentication, including mutual authentication. This allows the use of SASL-style authentication if supported by *Client* and *Server* and includes the possibility for a *Client* to re-authenticate within a connection.

Subscription options: provides subscription options primarily defined to allow message bridge applications. These include an option to not send messages originating from a *Client* (noLocal) and options for managing messages stored on *Subscribe*.

Delay: adds the possibility to specify a delay between the end of the connection and the sending of the message. Designed so that if the connection is re-established the

message will not be sent. This allows short breaks in the connection without notifying others.

Keep Alive Server: allows the *Server* to specify the *Keepalive* value that the *Client* must use. The *Client* must respect the *Keepalive* set by the *Server*.

ClientID assigned: in cases where the *ClientID* is assigned by the *Server*, it returns the assigned *Client* ID. In this case, the restriction that the *ClientID* assigned by the *Server* can be used only with *Clean Session* connections = 1 is eliminated.

Server Reference: allows the *Server* to specify an alternative *Server* to use on CONNACK or DISCONNECT. Can be used as redirection or Provisioning.¹¹⁴

7.4.3 CoAP

Constrained Application Protocol (CoAP) is also a very light M2M protocol and was released by IETF CoRE (Constrained RESTful Environments) Working Group. CoAP supports both the *Request/Response* and the *resource/observe* architecture (which represents a variant of *Publish/Subscribe*)¹¹³. CoAP was developed to work with HTTP and RESTful Webs through a *proxy*. Unlike the MQTT, the CoAP uses the *Universal Resource Identifier (URI)* in place of the *Topics*.¹¹¹

The data is published on the URI and the subscriber subscribes to the resources indicated by the URI. CoAP is a binary protocol and requires 4 bytes for the header with a message in the *payload* depending on the size defined in the *web-server* or by programming. Transport-level CoAP is based on UDP and uses the DTLS for security.¹¹⁵ *Clients* and *Servers* communicate through UDP, however, it uses confirmable messages to be acknowledged by the receiver with an ACK packet and non-confirmable messages. CoAP offers more features than MQTT 3.1.1 such as the support for content negotiation that allows the representation of a resource; this allows the *Client* and the *Server* to evolve independently, adding new representations without influencing each other¹¹³. Conversely, compared to the last version of MQTT the difference in functionality has been reduced.

7.4.4 AMQP

Advanced Message Queuing Protocol (AMQP) is an open standard M2M protocol designed to support messaging on middle-ware. AMQP has created a functional interoperability between the *client* and the messaging middle-ware.¹¹⁶ The model consists of a set of components that route messages within the *Broker* service and a *wire live* network protocol that allows the *Client* application to communicate with the *Server* and interact with the AMQ model. The protocol is used in distributed applications and includes *Point-To-Point*, *Publish*, *Subscribe*, *Fan-Out* and *Request-Response Messaging System*. AMQP does not store messages, but queues them on behalf of the recipient.

¹¹⁴ <https://github.com/mqtt/mqtt.github.io/wiki/Differences-between-3.1.1-and-5.0>

¹¹⁵ A.Ludovici, P.Moreno and A.Calveras, "TinyCoAP:a novel con-strained *Application* protocol(CoAP) implementation for embedding RESTful web services in *Wireless* sensor networks based on tinyos" Journal of Sensor and Actuator Networks, vol. 2, no. 2, pp. 288–315,2013

¹¹⁶ <https://www.amqp.org/about/what>. [Last visit 30/05/2019]

It is a corporate messaging protocol designed for reliability, security, *provisioning* and interoperability¹¹⁷. AMQP supports both the *Request/Response* architecture and the *Publish/Subscribe* architecture¹¹⁸. It offers a wide range of messaging features, such as reliable queue, topic-based publishing and subscription, flexible routing and transactions¹¹⁶. The communication system requires the *Publisher* or *Consumer* to create an "exchange" with a given name and then transmit that name. *Publishers* and *Consumers* use the name to identify themselves. Subsequently, *Consumers* create a "queue" and connect it to the exchange at the same time. The messages received from the exchange must be matched to the queue through a process called "binding". AMQP exchanges messages in various ways: directly, in the form of fanout, by topic or based on headers. AMQP is a binary protocol and normally requires a fixed 8-byte header with small *Message Payloads* up to the maximum size depending on the *Broker/Server* or programming technology.^{119 120}

AMQP uses TCP as the default transport protocol and TLS/SSL and SASL for security¹¹⁷. Therefore, the communication between *Client* and *Broker* is connection-oriented. Reliability is one of the fundamental features of AMQP, and offers two preliminary levels of quality of service (QoS) for message delivery: *UnsettleFormat* (not reliable) and *SettleFormat* (reliable)¹¹⁷.

The current reference version is the AMQP 1.0, released in 2012. It is a completely different version from the AMQP 0.xx, resulting incompatible.

7.4.5 NATS / NATS 2.0

NATS stands for Neural Autonomic Transport System. The idea behind the messaging platform is to imitate the functioning of a central nervous system.

NATS is a native *Cloud* and *Open Source* infrastructure messaging system, designed to be light and high performance. It implements a highly scalable and elegant distribution model for the publication of subscriptions (pub/sub). The performing nature of NATS makes it an ideal base for building modern, reliable and scalable native *Cloud* distributed systems.

NATS is offered in two interoperable modules:

- core NATS (simply called "NATS" or "NATS Server"),
- NATS *Streaming*, an event *streaming* service, with delivery guarantees and reproduction of historical data to the NATS.

1 ¹¹⁷ A.Foster, "Messaging technologies for the industrial internet and the internet of things whitepaper," PrismTech, 2015

1 ¹¹⁸ N. S. Han, "Semantic service *Provisioning* for 6LoWPAN: powering internet of things *Applications* on web," Ph.D. dissertation, Institut National des Télécommunications, 2015

1 ¹¹⁹ J. E. Luzuriaga, M. Perez, P. Boronat, J. C. Cano, C. Calafate, and P. Manzoni, "A comparative evaluation of AMQP and MQTT protocol over unstable and mobile networks," in 12th Annual IEEE Consumer Communications and Networking Conference, 2015, pp. 931–936

1 ¹²⁰ G. Marsh, A. P. Sampat, S. Potluri, and D. K. Panda, "Scaling advanced Message queuing protocol (AMQP) architecture with *Broker* federation and infiniband," Ohio State University, Tech. Rep. OSU-CISRC-5/09-TR17, 2008

NATS was created by Derek Collison and is managed through an *Open Source* ecosystem through GitHub.

NATS can run on both large *servers* and *cloud* instances, through *EDGE gateways* and even *IoT* devices.

Use cases for NATS include:

- In-the-Cloud messages
 - Services (microservices, service network)
 - Event / Data Streaming (observability, analytics, ML/AI)
- Command and control
 - *IoT* and edge
 - Telemetry/Sensor data/Command and control
- Increase or replace legacy messaging systems

The NATS *Server* is written in Go, the *Clients* can be written in different languages.

The development of NATS is sponsored and supported by Synadia, a company founded by Derek Collison. The Synadia team is responsible for maintaining and developing the NATS *Server* and its libraries for various languages. The user *community* develops libraries for *clients* in various languages, these can be downloaded at the following address: <https://nats.io/Download>

NATS 2.0 is the most important feature release since the original *Server* base code was released. The development of NATS 2.0 has been developed to allow a new operation of the NATS system as a shared utility, solving problems in scalability through distributed security, *multi-tenancy*, larger networks and secure data sharing.

The main mission of NATS 2.0 is to address the problems of distributed computing on a large scale and increase security by lowering the TCO (*Total Cost of Ownership*). To achieve this goal, a series of new features have been added that are transparent to existing customers, maintaining 100% backward compatibility.

All the documentation is available at: <https://nats-io.github.io/docs/>

7.4.6 DDS

Data Distribution Service (DDS) is designed as a publication and subscription service. The specifications are registered with the OM. The idea is to represent an infrastructure capable of communicating different entities, overcoming the inherent heterogeneities of the membership node.

The main reference features of the DDS are:

Communication based on the *Publish/Subscribe* model, guaranteeing the anonymity of the entities involved;

Wide variety of configuration parameters of QoS (*Quality of Service*) that allow the developer to manage the traffic of messages at will;

Auto-Discovery support which tracks new application *end-points* on the network;

Use of a standard language such as IDL to define message characteristics and object access interfaces;

The data values (*Samples*) are transferred through the system for conceptual "*Data Objects*". The "*Publication*" (the association of a *Publisher* and a *DataWriter*) sends *Samples* to one or more "*Subscriptions*" (the association of a *DataReader* and a *Subscriber*).

The basic components are *Topic*, *Publisher*, *Subscriber*, *DataWriter*, and *DataReader*.

The *Topics* represent information about the individual data types and the distribution of available *Samples*.

The *Publishers* apply controls and data flow restrictions from the *DataWriters*

The *Subscribers* apply data flow controls and restrictions from *DataReaders*.

The *DataWriters* create the *Samples* of the single *Application data type*.

The *DataReaders* receive the *Samples* of the single *Application data type*.

A *Publisher* can have multiple *DataWriters*.

A *Subscriber* can have multiple *DataReaders*.

A *DataWriter* has a single *Topic*.

A *DataReader* has a single *Topic*.

A *Topic* can have multiple *DataReaders* and *DataWriters*.

A "*Publication*" may have multiple "*Subscriptions*" associated with it.

A *subscription* may have multiple "*Publication*" associated with it.¹²¹

The data flow is started by the application through a publication, writing a value on the *DataWriter*. The *DataWriter* publishes the *samples*. The samples are sent to the various associated subscribers, each of which passes them to the *DataReaders* that are associated with the *DataWriters*. The process ends when the subscriber side application returns the data from the *DataReader*.

Topics, *DataReaders*, *DataWriters*, *Publishers* and *Subscribers* all include QoS (*Quality of Services*) policies. The QoS policies of the *Publisher*, the *DataWriter* and the *Topics* control the data on the transmission side. The QoS policies of the *Subscriber*, *DataReader* and *Topics* control the data on the receiving side.¹²¹

1 ¹²¹ http://opendds.org/about/dds_overview.html

7.4.7 XMPP

Extensible *Messaging* and Presence Protocol, originally identified with the name "Jabber" was developed for *Text-based* instant messaging platforms. XMPP is an acronym for Extensible *Messaging* and Presence Protocol. XMPP uses the Extensible Markup Language (XML) *Text* format as a native type, which allows natural communication between people. As for the MQTT at transport level we find TCP, or even HTTP on TCP. Its strength is given by the use of an address such as *name@domain.com* which helps in intricate internet addressing. The XMPP protocol contextualized in the IoT world offers a simple addressing system to the device. The protocol is not meant to be fast but to transmit data between points that are not well defined, so often *Polling* or update control systems are implemented only on demand. However, it is a protocol designed for *Real-Time* applications and therefore efficiently supports small low-latency messages. It does not provide any guarantee of quality of service (QoS) and, therefore, it is not practical for M2M communications. In addition, XML messages create additional overhead due to numerous headers and tag formats that increase power consumption which is critical to the *IoT* application. Consequently, XMPP is rarely used in the *IoT* but having aroused some interest we try to improve its architecture in order to support *IoT* applications.¹²²

1 ¹²² Internet of Things and data analytics handbook / edited by Hwaiyu Geng. ISBN 9781119173632

7.4.8 Comparative tables

Tipologia	Protocollo	Link	Nome completo	Descrizione	Modello	Trasporto	Sicurezza	Comunicazione	Note
Protocolli per IOT/M2M	CoAP	https://tools.ietf.org/html/rfc8323	Constrained Application Protocol	Protocollo per reti a basso consumo e potenziale perdita di dati	Request-Response Publish-Subscribe	Solitamente UDP, può essere usato anche TCP	IPSEC (cifatura IP) o DTLS	Sincrona e asincrona	
	DDS	https://www.dds-foundation.org/	Data Distribution Service	Protocollo m2m	Publish-Subscribe	Indipendente dal tipo di trasporto	https://www.omg.org/spec/DDS-SECURITY/1.1/PDF	Sincrona e asincrona	Protocollo chiuso, versione open source in C++: http://opendds.org/
	MQTT	http://mqtt.org/	Message Queue Telemetry Transport	Protocollo m2m	Publish-Subscribe	Solitamente TCP, può essere usato anche UDP	Non prevista di base	Asincrona	
	AMQP	https://www.amqp.org/	Advanced Message Queuing Protocol	Protocollo a livello applicativo per il MOM (message-oriented middleware)	Message-oriented	TCP	SSL e Kerberos	Sincrona e asincrona	
	Web Thing Model	https://www.w3.org/Submission/wot-model/	Risulta non aggiornato dal 2015						
	Weave	https://nest.com/weave/	Nest ora fa parte di Google e il servizio viene venduto con gli apparecchi Google Home						
	NATS	https://nats.io/	Neural Autonomous Transport System	Protocollo nato il messaging system all'interno di un'infrastruttura cloud nativa.	Subject-based Messaging. Request-Response. Publish-Subscribe	TCP	TLS	Sincrona e asincrona	Protocollo Open Source nato per operare in una famiglia di prodotti open source
Protocollo con altri utilizzi ma con propria documentazione IOT	XMPP	https://xmpp.org/	Extensible Messaging and Presence Protocol	Protocollo a messaggio basato su XML. Completamente aperto e gratuito, ha implementazioni in vari linguaggi	Message-oriented	Dipende dall'implementazione	In https://tools.ietf.org/html/rfc6120 , SASL e TLS	Sincrona e asincrona	https://xmpp.org/uses/internet-of-things.html , http://www.xmpp-iot.org/
Protocolli utilizzati per l'IOT, anche se non è l'utilizzo principale	HTTP	https://tools.ietf.org/html/rfc2616	Hyper-Text Transfer Protocol	Protocollo a livello applicativo, per architetture client-server	Request-Response	TCP	HTTPS	Sincrona	
	FTP	https://tools.ietf.org/html/rfc959	File Transfer Protocol	Protocollo per lo scambio di file tra architetture client-server. Utilizza 2 canali, uno per i comandi e uno per lo scambio dati	Request-Response	TCP	Richiede autenticazione ma il passaggio di dati è in chiaro. FTPS versione con SSL/TLS	Sincrona	
	Telnet	https://tools.ietf.org/html/rfc854	Telnet	Protocollo di rete solitamente utilizzato per il login remoto	Request-Response	TCP	Non c'è autenticazione e non è crittografato	Sincrona	
	SSH	https://tools.ietf.org/html/rfc4253	Secure SHell	Protocollo di rete cifrato utilizzato prevalentemente da riga di comando	Request-Response	In teoria indipendente, nell'uso pratico TCP	Cifrato, con scambio chiavi e autenticazione	Sincrona	

7.5 Data Aggregation / Processing Layer

Data Aggregation can be seen as the collective display of data in a unified platform, or the physical collection of data within a centralized archiving system from separate sources.¹²³

Data processing represents all the methods and operations necessary to transform raw data into structured or integrated data.¹²⁴ In the *IoT* context it represents all those platforms, usually *Software*, which collect the data and process it to enable them to later be used at the application level. This level is in fact already at a very high and transversal level on the *IoT* as they are designed for managing large amounts of data. Therefore, in this case the most common platforms have been compared and linked as much as possible to the *Open Source* concept. The Scribe and Kinesis platforms are only included for completeness.

1 ¹²³ Xiaoming Wang, Lili Liu, James Fackenthal, Shelly Cummings, Oluwatobi I. Olopade, Kisha Hope, Jonathan C. Silverstein, Olufunmilayo I. Olopade -Translational integrity and continuity: Personalized biomedical data integration. *Journal of Biomedical Informatics* 42 (2009) 100–112

1 ¹²⁴ <https://www.britannica.com/technology/data-Processing>

Table 15: Comparison between aggregation platforms, management and processing data

	Link	Descrizione	Linguaggio	Licenza	DB / Filesystem	Note
Scribe	https://www.scribsoft.com/	Paas con interfaccia browser, non sono richieste abilità di programmazione	C++	A partire da 400\$/mese	Connettori per DB (MySQL, PostgreSQL, Amazon S3, etc) e vari servizi (SMTP, REST, Excel, Twitter, etc). Non risultano connettori per DB NoSQL	Acquistata nel 2018 da TIBCO, società che fa Business Process Management in ambito bancario
RapidMQ	https://github.com/sybrexsys/RapidMQ	Libreria per la gestione di una coda locale di messaggi da integrare in un proprio progetto	GO	Apache 2.0	Basata sulla manipolazione di file	Progetto open-source di una singola persona
Flume	https://flume.apache.org/	Sistema per raccogliere stream di log (es Avro, Thrift, Syslog, Netcat, Social Networks, etc) e salvarli in un data store centralizzato Hadoop	Java	Apache 2.0	Hadoop	Serve la Flume Pro licence code
Kafka	https://kafka.apache.org/	Sistema publisher/subscriber per lo stream di dati. Installato su cluster, comunica via TCP. Salva <i>records</i> (chiave, valore, timestamp) in <i>topics</i>	Scala	Apache 2.0	Solitamente integrato con Apache Storm, Apache HBase, Apache Spark	Inizialmente sviluppato da LinkedIn
Storm	https://storm.apache.org/	Sistema per consumare dati, applicarci calcoli in real-time e salvarli in data center come Hadoop oppure inviarli ad altri sistemi di data-aggregation	Java ma con estensioni per vari linguaggi	Apache 2.0		Inizialmente sviluppato da Twitter
Luxun	https://github.com/bulldog2011/luxun	Progetto abbandonato in beta nel 2016				
Fluentd	https://www.fluentd.org/	Open source data collector. Cerca di unificare quello che chiama "logging layer" utilizzando JSON. Costruito per essere piccolo e leggero	C e Ruby	Apache 2.0	Vari: SQL, Hadoop, MongoDB, etc	Member of Cloud Native Computing Foundation: https://www.cncf.io/
OpenIoT	http://www.openiot.eu/	Progetto open source finanziato dall'Unione Europea. Middleware per collegare sensori IoT compatibili alla specifica W3C Semantic Sensor Networks (SSN) ad un sistema cloud	Java	Non specificata ma progetto dichiarato open source	Cloud basato su LSM-Light (Linked Stream Middleware Light)	Codice: https://github.com/C
RabbitMQ	https://www.rabbitmq.com/	Message broker per code asincrone, selettive, a topic. Supporta il cloud e il deploy distribuito	Erlang. Fatto per essere usato con vari linguaggi	Server pubblicato su Github con licenza MOZILLA PUBLIC LICENSE (MPL) Version 1.1	Open Source. Una versione commerciale con più funzionalità e assistenza richiede registrazione	Codice: https://github.com/r
Kinesis	https://aws.amazon.com/it/kinesis/	Sistema di raccolta, elaborazione e analisi di flussi di dati in tempo reale.	AWS SDK fornito in vari linguaggi	Al momento non è compreso nella prova gratuita AWS. Si paga il servizio in base all'uso	Sfrutta gli altri servizi di Amazon	https://github.com/aws-labs/amazon-kinesis-producer
Mosquitto	https://mosquitto.org/	Eclipse Mosquitto è un broker di messaggi open source che implementa le versioni del protocollo MQTT 5.0, 3.1.1 e 3.1. Mosquitto è leggero ed è adatto per l'uso su tutti i dispositivi da computer a scheda singola a basso consumo a server completi.	C, C++	EPL/EDL		https://github.com/eclipse/mosquitto

7.6 Data Storage Layer

This paragraph shows the comparison between various *Databases* that present a NOSQL philosophy, which to date is the most relevant for *Storage* of large amounts of data.

The *databases* are not strictly linked to particular *IoT* technologies but above all to the quantity and type of data, to the processing and to the applications that will exploit such data, therefore the comparison has taken into consideration the operational aspects of the same.

Furthermore, some of the most used in this area were taken into consideration.

	Cassandra	MongoDB	Oracle No-SQL	OrigoDB	PostgreSQL	HBase	InfluxDB	TimescaleDB
Descrizione	Sistema Wide-column store basato sull'idea di BigTable e DynamoDB	Uno dei più popolari DB NOSQL	Key-value store basato su Berkeley DB Java Edition	Basato su ACID in-memory object graph <i>Databases</i>	RDBMS molto diffuso, presenta anche l'uso NOSQL	Sistema Wide-column store basato su Apache Hadoop e sui concetti di BigTable	DBMS per la memorizzazione di serie temporali, eventi e metriche	DBMS basato su serie temporali, ottimizzato per l'inserimento veloce e query complesse, basato su PostgreSQL
Modello primario di database	Wide column store	Document store	Key-value store	Document store Object oriented DBMS	Relational DBMS	Wide column store	Time Series DBMS	Time Series DBMS
Modello secondario di database			Relational DBMS		Document store			Relational DBMS
Sito Web	cassandra.apache.org	www.mongodb.com	www.oracle.com	origodb.com	www.postgresql.org	hbase.apache.org	www.influxdata.com/	www.timescale.com
Documentazione tecnica	cassandra.apache.org/doc/latest	docs.mongodb.com/manual	docs.oracle.com/cd/NO-SQL/index.html	origodb.com/docs	www.postgresql.org/docs/manuals	hbase.apache.org	docs.influxdata.com/influxdb	docs.timescale.com
Titolare del progetto	Apache Software Foundation	MongoDB, Inc	Oracle	Robert Friberg et al	PostgreSQL Global Development Group	Apache Software Foundation	InfluxData Inc.	Timescale
Prima release	2008	2009	2011	2009	1989	2008	2013	2017
Release attuale	3.11.4, 2/2019	4.0.8, 3/2019	18.3, 11/2018		11.3, 5/2019	1.4.8, 10/2018	1.7.6, 4/2019	1.2.29, 1/2019
Tipologia di licenza	Open Source	Open Source	Open Source	Open Source	Open Source	Open Source	Open Source	Open Source
Cloud-based	Non solo	Non solo	Non solo	Non solo	Non solo	Non solo	Non solo	Non solo
Implementato con	Java	C++	Java	C#	C	Java	Go	C
Server operating systems	BSD Linux OS X Windows	Linux OS X Solaris Windows	Linux Solaris SPARC/x86	Linux Windows	FreeBSD HP-UX Linux NetBSD OpenBSD OS X Solaris Unix Windows	Linux Windows Unix	Linux, OS X	Linux Windows Unix
Data scheme	Schem Free	Schem Free	AVRO otable-	Si	Si	Schem Free	Schema Free	Si

	Cassandra	MongoDB	Oracle No-SQL	OrigoDB	PostgreSQL	HBase	InfluxDB	TimescaleDB
			style					
Supporta tipizzazione	Si	Si	Opzionale	Definibili dall'utente in .NET.	Si	No	Dati numerici e stringhe	Numerico, stringa, booleano, array, JSON blob, dimensioni geospaziali, monetario, dati binari, altri tipi di dati complessi
Supporto all'XML	No	Si	No	No	Si	No	No	Si
Secondary indexes	Soggetto a restrizioni	Si	Si	Si	Si	No	No	Si
Supporto l'SQL	SQL-like SELECT, DML e DDL statements (CQL)	Lettura delle query SQL con connector per BI	SQL-like DML e DDL statements	No	Si	No	Numeric data and Strings	Yes – PostgreSQL
Accessibilità con API o altre metodologie	Protocollo proprietario: Thrift	Protocollo proprietario basato su JSON	RESTfull HTTP API	.NET <i>Client</i> API HTTP API LINQ	Native C library <i>Streaming</i> API for large objects ADO.-NET JDBC ODBC	Java API RESTful HTTP API Thrift	HTTP API JSON over UDP	native C library, <i>Streaming</i> API for large objects, ADO.-NET, JDBC, ODBC
Linguaggi di programmazione supportati	C# C++ Clojure Erlang Go Haskell Java JavaScript Perl PHP Python Ruby Scala	Actionscript, C, C#, C++, Clojure, ColdFusion, D, Dart, Delphi, Erlang, Go, Groovy, Haskell, Java, JavaScript, Lisp, Lua, MatLab, Perl, PHP, PowerShell, Prolog, Python, R, Ruby, Scala, Smalltalk	C C# Java JavaScript (Node.js) Python	.NET	.Net C C++ Delphi Java JavaScript (Node.js) Perl PHP Python Tcl	C C# C++ Groovy Java PHP Python Scala	.Net Clojure Erlang Go Haskell Java JavaScript (Node.js) Lisp Perl PHP Python R Ruby Rust Scala	.Net C C++ Delphi Java info JavaScript Perl PHP Python R Ruby Scheme Tcl
Supporto a script lato Server	No	JavaScript	No	Si	Funzioni definite dall'utente	Si	No	Funzioni definite dall'utente, PL/pgSQL, PL/Tcl, PL/Perl, PL/Python, PL/Java, PL/PHP, PL/R, PL/Ruby, PL/Scheme, PL/Unix shell
Triggers	Si	No	No	Si	Si	Si	No	Si

	Cassandra	MongoDB	Oracle No-SQL	OrigoDB	PostgreSQL	HBase	InfluxDB	TimescaleDB
Partitioning methods	Sharding	Sharding	Sharding	horizontal partitioning	Partitioning by range, list and (since PostgreSQL 11) by hash	Sharding	Sharding	Across time and space (hash partitioning) attributes
Replication methods	Selectable replication factor	Master-Slave replication	Selectable Master-Slave per shard	Master-Slave replication	Master-Slave replication	Selectable replication factor	Selectable replication factor	Master-Slave replication with hot standby and reads on Slaves
MapReduce	Si	Si	Con Hadoop integration	No	No	Si	No	No
Consistenza	Immediate Consistency / Eventual Consistency	Immediate Consistency / Eventual Consistency	Immediate Consistency / Eventual Consistency		Immediate Consistency	Immediate Consistency		Immediate Consistency
Foreign Keys	No	No	No	Dipendenti dal modello	Si	No	No	Si
Transaction concepts	No	Multi-documento ACID Transactions con snapshot isolation	Configurabile	ACID	ACID	No	No	ACID
Concurrency	Si	Si	Si	Si	Si	Si	Si	Si
Durability	Si	Si	Si	Si	Si	Si	Si	Si
In-memory capabilities	No	Si	Si	Si	No	No	Si	No
Gestione degli accessi	I diritti di accesso per gli utenti possono essere definiti per oggetto	Diritti di accesso per utenti e ruoli	Diritti di accesso per utenti e ruoli	Autorizzazione basata sul ruolo	Diritti secondo lo standard SQL	Access Control Lists (ACL)	Attraverso la gestione degli utenti	Diritti di accesso granulari in accordo allo standard SQL

7.7 Final tables

Protocollo di connessione	Livello di sviluppo	Sicurezza	Qualità, disponibilità a livello di mercato e relativo supporto	Filosofia di sviluppo	Quantità e qualità dei progetti	Prospettive di evoluzione
RFID	Tecnologia Matura	Alto	Grande disponibilità a livello di mercato e di documentazione e tutti i vendor mettono a disposizione molta documentazione e supporti tecnici.	Lo sviluppo della tecnologia è legata all' <i>Hardware</i> dei tag e dei lettori	Tecnologia già altamente diffusa – Carte di credito, passaporti.	Si tratta di una tecnologia altamente diffusa ed ha una forte presenza in tutte le nostre attività. La definizione di <i>Internet of Things</i> nasce proprio grazie all'uso di questa tecnologia. Si prevede un ulteriore incremento anche in ambito <i>IoT</i> grazie alla evoluzione della tecnologia stessa.
NFC	Tecnologia Matura	Alto	Grande disponibilità a livello di mercato e di documentazione e tutti i vendor mettono a disposizione molta documentazione e supporti tecnici.	Lo sviluppo della tecnologia è legata all' <i>Hardware</i> . L' <i>Hardware</i> deve rispettare le direttive: ISO/IEC 14443A, ISO/IEC 14443B e X6319-4	Tecnologia già altamente diffusa – POS, carte di accesso.	Si tratta di una tecnologia altamente diffusa ed ha una forte presenza in tutte le nostre attività. Si prevede un ulteriore incremento anche in ambito <i>IoT</i> grazie alla evoluzione della tecnologia stessa.
M-BUS / WM-BUS	Tecnologia Matura	Medio: AES	Il protocollo <i>Wireless M-Bus</i> (wM-Bus) è diventato il riferimento per lo smart <i>Metering</i> in Europa. Si tratta, ormai dello standard per la ripartizione del riscaldamento più usato in Germania. Esiste un ottimo supporto e documentazione più che sufficienti.	Si tratta di una tecnologia aperta e basata su standard Europei: EU 13757	Tecnologia installata in una miriade di prodotti commerciali.	Si tratta di una tecnologia altamente diffusa ed ha una forte presenza nelle attività di smart <i>Metering</i> . Attualmente molto usata con concetto M2M ma si prevede un ulteriore incremento anche in ambito <i>IoT</i> grazie alla evoluzione della tecnologia stessa.
DigiMesh	Tecnologia Matura	Alta	Protocollo creato dalla Digi International Inc. da cui sono nati i prodotti Digi XBEE 3 digimesh. Sono acquistabili sui maggiori venditori di elettronica mondiale. Libellium basa molti dei suoi progetti su radio Xbee.	Si tratta di un protocollo proprietario ed è disponibile solo su prodotti Digi Xbee.	Sono utilizzati da Libellium per i suoi prodotti. Spesso nei progetti sono indicati i prodotti Xbee senza precisare quale radio specifica è stata usata.	Tecnologia chiusa, ha delle buone caratteristiche ma risulta legata ad una sola azienda. Non è una tecnologia che verrà adottata al di fuori dei prodotti Digi.
Zigbee	Tecnologia Matura	Dallo Zigbee 2 Alto	Grande disponibilità a livello di mercato e di documentazione e tutti i vendor mettono a disposizione molta documentazione e supporti tecnici.	Lo standard è aperto, ma è necessaria la licenza per rilasciare il dispositivo come zigbee	Tecnologia già altamente diffusa – gestione parcheggi, domotica	Lo standard e la relativa tecnologia sono supportati dalla ZigBee Alliance, composta da importanti player del settore.
DASH7	Tecnologia Matura	Medio: Cifratura AES-128	Documentazione specifica previa registrazione gratuita al sito. Esiste un kit di sviluppo ufficiale (WizziKit2), inoltre l'azienda francese Cortus	Standard aperto ma DASH7 Alliance gestisce programmi di test, plugfest e certificazione necessari per qualsiasi prodotto	N/A	Tecnologia nata nel 2009 ma non si è mai realmente diffusa e l'evoluzione è stata lentissima. Il 2019 ha portato qualche novità, in quanto la DASH7 Alliance ha rilasciato a Gennaio

Protocollo di connessione	Livello di sviluppo	Sicurezza	Qualità, disponibilità a livello di mercato e relativo supporto	Filosofia di sviluppo	Quantità e qualità dei progetti	Prospettive di evoluzione
			ha presentato recentemente (Aprile 2019) il primo system-on-chip in grado di supportare DASH7, ma non si trova altrove. Esiste attualmente una implementazione <i>Open Source</i> dello Stack di protocollo (OSS-7) in grado di supportare alcune piattaforme <i>Hardware</i> e radio.	to che utilizza la tecnologia <i>Wireless</i> DASH7. Il laboratorio di certificazione, in Belgio, convalida il livello fisico RF e la conformità alle specifiche. L'uso dello Stack OSS-7 è autorizzato con licenza Apache, versione 2.0.		2019 la specifica del protocollo V.1.2 e l'azienda francese Cortus ha presentato recentemente (Aprile 2019) il primo system-on-chip in grado di supportare DASH7. Tuttavia non si intravedono le premesse per una sua diffusione senza l'interesse di importanti player del settore.
Z-Wave	Tecnologia Matura	Bassa	Protocollo pensato per la domotica ed è adottato da migliaia di produttori. I prodotti con protocollo Z-Wave sono acquistabili facilmente come prodotti per la domotica.	Protocollo proprietario e brevettato.	Esistono molti prodotti, con svariate tipologie di sensori e attuatori, basati su Z-Wave.	Protocollo già adottato da molte aziende. Quindi si tratta di uno standard affermato e che sicuramente evolverà estendendo il sistema di sicurezza.
Thread	Tecnologia Matura	Buona	Protocollo basato su IP. I prodotti certificati Thread sono rilasciati dai maggiori produttori di chip.	Esistono 2 versioni una <i>Open Source</i> e una chiusa. Comunque la commercializzazione può avvenire solo in presenza di certificazione.	Si tratta di uno standard voluto da Google Nest e sviluppato in collaborazione con Samsung, Freescale e Arm. Google Nest lo ha adottato per i suoi prodotti.	Da maggio 2016 Google Nest ha rilasciato una versione <i>Open Source</i> , comunque non si trovano ancora molti prodotti che l'adottano oltre ai già menzionati google nest. Essendo però un protocollo che è capace di operare su un <i>Hardware</i> già esistente ed utilizzare indirizzamento IPv6 su 6LowPan ha grandi potenzialità di sviluppo.
Bluetooth	Tecnologia Matura	Alta	Presenza ubiqua e pervasiva nella nostra vita. M.Phone, PC, TV,	Gli standard di riferimento sono: » IEEE 802.15.1 » IEEE 802.15.2 » IEEE 802.15.3 » IEEE 802.15.4	Tecnologia già altamente diffusa. Progetti di ricerca e studi ormai non si contano più	Si tratta di un protocollo in continua evoluzione attualmente si è arrivati alla versione 5 e a breve sarà rilasciata la 5.1.
BLE – Bluetooth Low Energy	Tecnologia Matura			Lo standard è basato su Bluetooth 4.0/4.1 ed ha caratteristiche per il basso consumo. Non è compatibile con il Bluetooth. Si paga il diritto a definirlo Compliant.	Tecnologia già altamente diffusa. Progetti di ricerca e studi ormai non si contano più	Si tratta di un protocollo in continua evoluzione attualmente si è arrivati alla versione 5 e a breve sarà rilasciata la 5.1.
Ant/Ant+	Tecnologia matura	Medio: Cifratura AES-128	ANT è una tecnologia proprietaria di progettata e commercializzata da ANT <i>Wireless</i>	ANT+ è un protocollo proprietario. I dispositivi con ANT+ richiedono la certificazione della ANT+ Alliance	Tecnologia già altamente diffusa, usata in milioni di sensori per attività sportive, di fitness e di monitoraggio dello stato di salute.	Tecnologia già altamente diffusa, usata in milioni di sensori per attività sportive, di fitness e di monitoraggio dello stato di salute. Ormai si può definire standard de facto per i dispositivi fitness.

Protocollo di connessione	Livello di sviluppo	Sicurezza	Qualità, disponibilità a livello di mercato e relativo supporto	Filosofia di sviluppo	Quantità e qualità dei progetti	Prospettive di evoluzione
Wireless HART	Tecnologia Matura	Alta	Si tratta di un protocollo di comunicazione <i>Wireless</i> per reti mesh industriale. Oltre 30mil.di dispositivi compatibili installati nel mondo.	Primo <i>Open</i> standard <i>Wireless</i> per i processi industriali.	Più di 30milioni di dispositivi Hart compatibili sono installati nel mondo.	Si tratta di un protocollo industriale ormai standardizzato. L'evoluzione sarà più verso le applicazioni che sul protocollo.

Table 16: Network Access Layer – technology evaluation table

Protocollo di connessione	Livello di sviluppo	Livello di sicurezza intrinseca	Qualità, disponibilità a livello di mercato e relativo supporto	Filosofia di sviluppo	Quantità e qualità dei progetti	Prospettive di evoluzione
Weightless W	Release candidate	Medio: Cifratura AES-128/256	Documentazione previa registrazione gratuita al sito. Un solo venditore autorizzato per kit Weightless	Open standard	N/A	Trattandosi di una tecnologia basata sulle frequenze televisive (regolate diversamente nei vari paesi), si prevede che sarà difficile una sua diffusione globale
Weightless N	Esiste uno starter kit, ma non si trova altro. Tecnologia ancora immatura	Medio: Cifratura AES-128/256	Documentazione previa registrazione gratuita al sito. Un solo venditore autorizzato per kit Weightless	Open standard	N/A	La tecnologia sembra promettente ma ha solo un rivenditore ufficiale e le notizie sul sito si interrompono a luglio 2018
Weightless P	Esiste uno starter kit, ma non si trova altro. Tecnologia ancora immatura	Medio: Cifratura AES-128/256	Documentazione previa registrazione gratuita al sito. Un solo venditore autorizzato per kit Weightless	Open standard	N/A	La tecnologia sembra promettente ma ha solo un rivenditore ufficiale e le notizie sul sito si interrompono a luglio 2018
Ingenu / RPMA	Tecnologia matura	Alta	L'uso della tecnologia con protocollo RPMA è legata alla presenza sul territorio delle rete. Da marzo 2018 il modello di business è passato ad un sistema PaaS, ed presenta una licenza per gli operatori di rete e i produttori di Hardware. Sono presenti unicamente negli USA per accesso ampio. Negli altri paesi ci sono accordi specifici. In Italia la licenziataria è la Materliq srl, che sfrutta Ingenu RPMA per i propri contatori del gas.	Protocollo proprietario, rete proprietaria, sviluppo chiuso.	In Italia la licenziataria è la Materliq srl, che sfrutta Ingenu RPMA per i propri contatori del gas.	Nel 2018 ha cambiato modello di business in quanto è stata sorpassata da Sigfox in termini di tempo. Il nuovo modello fa prevedere una evoluzione tipo quella adottata da Materliq, quindi usata per applicazioni specifiche.
SigFox	Tecnologia matura	Alta	L'uso della tecnologia con protocollo Sigfox è legata alla presenza sul territorio delle rete. La rete è creata secondo il modello dell'operatore mobile, fornendo copertura di rete on-demand per chi voglia realizzare progetti IoT. Vi sono accordi e collaborazioni con società partner per la produzione dei dispositivi (chip e moduli) per realizzare i terminali e le applicazioni.	Protocollo proprietario, rete proprietaria, sviluppo chiuso.		Negli ultimi tre anni, grazie anche ai finanziamenti raccolti, la rete SIGFOX si è diffusa rapidamente in Francia, Spagna, Olanda e Regno Unito – oltre che in alcune grandi città metropolitane – con promettenti prospettive di crescita anche in altre nazioni europee al fianco partner locali. In Italia, SIGFOX ha siglato un accordo con EI Towers, sfociato nella costituzione di Netrotter.
LoRaWAN	Tecnologia matura	Medio: crittografia a due livelli, una chiave device-network server e una chiave end-to-end	Grande disponibilità di dispositivi e specifiche attraverso il sito della Lora Alliance	Certificazione dei dispositivi previa adesione alla Lora Alliance	Tecnologia in diffusione, attualmente 100 operatori in 50 stati implementano reti Lora	Si tratta di una tecnologia in sviluppo che si sta espandendo globalmente. L'alliance fornisce documentazione e dispositivi certificati ed è aperta a nuovi membri.
LTE-M	Tecnologia in fase di testing e implementata come rete in alcune zone	Medio, ereditata dalle reti cellulari su cui si basa (autenticazione, cifratura, etc)	Tecnologia poco diffusa, associata a poche board.	Protocollo definito da 3GPP, testabile dalle compagnie di telecomunicazione e implementabile dai costruttori di board	A marzo 2019, più di 30 operatori in più di 20 paesi hanno implementato la propria rete. Trovato solo un progetto di prototipazione a Cracovia	Si tratta di una tecnologia in fase di testing, poco diffusa e spesso non utilizzata a discapito dell'NB-IoT. Si prevede una migrazione in NB-IoT, in quanto la maggior parte delle board li supportano entrambi.
NB-IoT	Tecnologia in fase di testing avanzato e implementata come rete in alcune zone	Medio, ereditata dalle reti cellulari su cui si basa (autenticazione, cifratura, etc)	Varie aziende (es Accent Systems, Ericsson, Rohde & Schwarz) forniscono supporto e consulenza per i propri progetti IoT utilizzando NB-IoT	Protocollo definito da 3GPP, testabile dalle compagnie di telecomunicazione e implementabile dai costruttori di board	Tecnologia che si sta diffondendo. Varie board vendute da varie aziende. Nel mondo è implementata da varie compagnie telefoniche. In Italia da Vodafone e TIM	Tecnologia in fase di testing avanzato, già implementata in varie zone. Il protocollo è già pronto per supportare reti 5G, si prevede possa diventare uno dei protocolli di riferimento per i servizi IoT forniti dalle compagnie di telecomunicazioni
EC-GSM-IoT	Tecnologia in fase di testing	Medio, ereditata dalle reti cellulari su cui si basa (autenticazione, cifratura, etc)	Disponibile come upgrade software per le reti GSM. Essendo basato su EGPRS, può essere disponibile in moltissime zone, soprattutto nei paesi in via di sviluppo. Questo a discapito della velocità di connessione.	Protocollo definito e gestito da un apposito gruppo di lavoro 3GPP, implementabile dai costruttori di board	Tecnologia che si sta diffondendo, usata da Orange in Africa per monitorare campi coltivati.	Si tratta di una tecnologia in fase di testing. Si distingue da LTE-M e NB-IoT per basarsi solo su EGPRS, rendendola adatta ai paesi in via di sviluppo in cui altre connessioni non sono presenti
GSM	Tecnologia matura	Medio: autenticazione utente, cifratura	Disponibile globalmente. Molti tipi di moduli radio disponibili, di vari prezzi e qualità. Il supporto varia in base al modello di modulo.	Protocolli definiti da ETSI e 3GPP. Lo sviluppo della tecnologia è legato all'uso cellulare	Tecnologia globalmente diffusa, usata per la comunicazione dei cellulari	Tecnologia largamente diffusa. La tecnologia in sé non ha evoluzione in ambito IoT ma questo è dovuto al fatto di essere la base di LTE-M, NB-IoT e EC-GSM-IoT, su cui si concentra lo sviluppo

Table 17: Communication & Sessoin Layer - technology evaluation table

Protocollo di connessione	Livello di sviluppo	Sicurezza	Qualità, disponibilità a livello di mercato e relativo supporto	Licenza	Quantità e qualità dei progetti	Prospettive di evoluzione
CoAP	Protocollo maturo nato nel 2010	IPSEC (cifatura IP) o DTLS (per UDP, https://tools.ietf.org/html/rfc6347)	Protocollo per reti a basso consumo e potenziale perdita di dati	Open Source	Protocollo standardizzato IETF e presenta implementazione per tutti i maggiori linguaggi di programmazione e OS embedded presenti nel panorama dell'IoT.	Il protocollo è maturo ed è stato standardizzato dall'IETF quindi non sono previste nuove versioni.
DDS	Protocollo maturo nato nel 2004	Bassa basato su RTPS	La OMG ha creato al DDS foundation per individuare linee d'uso e nuove possibilità. Attualmente conta 9/10 vendors.	Proprietaria, esiste una versione open, sempre rilasciata dalla OMG: OpenDDS	I vendors sono attivi in modo trasversale su vari argomenti. https://www.dds-foundation.org/who-is-using-dds-2/	La versione è la 1.2 e stata rilasciata nel 2007. La Open Management Group insieme alla DDS Foundation sta lavorando alla versione DDS 1.3. Il progetto è nato da Tales su finanziamento da parte del governo Francese ed è seguito dall'OMG. Le aziende dichiarate "Vendors" non sono molte e sono altamente specializzate, applicano il protocollo per le loro applicazioni.
MQTT	Protocollo maturo, sviluppato dal 1999 per dati di telemetria.	Non prevista di base	MQTT è il protocollo più utilizzato nell'ambito dell'IoT. Supportato da molte piattaforme di sviluppo e fondazioni, risulta anche utilizzato nella messaggistica istantanea, come Facebook Messenger.	Open Source	Tra i protocolli, se non il protocollo, più usati nell'ambito dell'IoT.	Ad aprile 2019 è stata rilasciata la V5.0 dello standard da parte della OASIS. Nell'ultima versione sono state migliorate e aggiunte molte funzionalità: Better Error Reporting, Shared Subscriptions, Message Properties, Message Expiry, Session Expiry, Topic Alias, Allowed Function Discovery. Questo dimostra che è un protocollo molto versatile e che è soggetto ad uno sviluppo continuo quindi ha una evoluzione prevedibilmente elevata.
AMQP	Protocollo maturo, sviluppato dal 2003	Buona si basa su comunicazione SSL e autenticazione Kerberos	Come l'MQTT è un protocollo sviluppato dalla OASIS ed è nato per M2M. Sia Redhat che Microsoft forniscono supporto completo al protocollo, avendolo inserito nelle loro piattaforme WEB per IoT.	Open Source	Esistono implementazioni di broker per tutte le piattaforme e sviluppati da importanti realtà, come Azure di Microsoft, Jboss di Redhat, Apache Inoltre si tratta di un protocollo standardizzato ISO/IEC.	Ad aprile del 2014 è stato standardizzato dalla ISO/IEC, standard n. 19464. Come detto è uno standard appoggiato da grandi player e sviluppato dall'associazione OASIS.
XMPP	XMPP è rilasciato come Jabber, nasce come nel 2000, poi standardizzato nel 2004 dall'IETF (RFC 6120 e RFC 6121). Protocollo nato per altri utilizzi ma presenta caratteristiche di applicabilità all'IoT. Inoltre esiste una documentazione specifica per l'IoT	Non prevista di base.	Protocollo a messaggi basato su XML. Completamente aperto e gratuito, ha implementazioni in vari linguaggi ed è utilizzata dal 1999.	Truly open in all aspects	Essendo un protocollo completamente libero e sviluppato per altre applicazioni è presente in sistemi di messaggistica di ogni tipo. Per questo si adatta facilmente anche al mondo dell'IoT.	Come indicato sul sito xmpp.org, è uno standard aperto e utilizza un approccio di sviluppo aperto. Inoltre è progettato per essere estensibile. In altre parole è stato pensato per crescere e adattarsi ai cambiamenti. Come dimostra il sito http://www.xmpp-iot.org/ è uno standard che già si è adattato al mondo IoT.
NATS / NATS 2.0	NATS è l'acronimo di Neural Autonomic Transport System. Derek Collison ha concepito NATS come una piattaforma di messaggistica che funziona come un sistema nervoso centrale.	Utilizza il TLS. Con NATS 2.0 ha incrementato il livello di sicurezza. Prevede sistemi di sicurezza, autenticazione, autorizzazione e isolamento.	Può contare su una grossa community su Github, dal sito possono essere scaricati diversi documenti e le informazioni sono esaustive. Dal sito si riporta che il sistema di messaggistica NATS è utilizzato da grandi aziende che forniscono servizi di ogni genere.	Open Source	Essendo un protocollo completamente libero e sviluppato anche attraverso una community, esistono diverse implementazioni. A livello modale è utilizzato su piattaforme importanti.	Sembra essere un protocollo molto promettente, ma più che di protocollo parlerei di sistema. Infatti si tratta di un completo sistema di gestione dei dati, che può essere implementati a vari livelli all'interno di una catena IoT. L'idea di vedere il tutto come un sistema nervoso centrale ne implica non solo l'utilizzo come messaging protocol ma anche come sistema di gestione e controllo, oltre che già in idea EDGE e Fog computing.

8 The security issue

Echoing section 6.2.2 and the information related to the respective technologies seen in section 7.2, in this chapter we analyse some additional aspects related to security in *IoT* networks. In particular, a more precise description is given of some of the mechanisms linked to the most common technologies.

Furthermore, vulnerabilities related to the *IoT* will be analysed in a more general way with general indications of possible countermeasures.

8.1 IoT Communication Technologies

All the technologies at the *Network Layer* level define security systems and structures. In the descriptions given in the paragraph dedicated to the technologies of the communication level, the safety conditions associated with them have already been analysed, here they are taken up and extended.

8.1.1 ZigBee

As already illustrated, the ZigBee architecture is composed of 4 levels for application, network, *Media Access Control* (MAC) and physical layer.¹²⁵

The MAC layer is used to provide security in ZigBee technology. There are three types of services to provide security. The first is access control. This is a security technique that can be used to control and manage who or what can view or use resources in a system. The second service is encryption, which is provided by a MAC layer. It provides the ability to change the message to another form, called ciphertext, which cannot be understood by anyone except authorized users. Integrity is also provided by the third level of ZigBee.

The most common attack is the *Man-in-The-Middle* attack. It receives information from a sender and makes changes to it. The MAC level provides an integrity structure as a third service to control a *Man-in-The-Middle* attack. It provides the possibility for the recipient to check the contents of messages that have been changed or modified by the attackers.

ZigBee technology guarantees security by assigning a network key to each device. It is mandatory for each device to have a network key that is assigned at the time of registration. When the device sends a communication request, the network key is requested. Therefore, only authorized and authentic devices can communicate with each other. It also has some drawbacks. The assigned network key can never be changed. It provides no possibility to update or change the key, which is not a good security tactic.³²

1 ¹²⁵ Wang W., He G., Wan J. Research on Zigbee *Wireless* communication technology; Proceedings of the 2011 International Conference on Electrical and Control Engineering (ICECE); Yichang, China. 16–18 September 2011; pp. 1245–1249

8.1.2 Bluetooth

Bluetooth¹²⁶ is used for applications that want to communicate over short distances. It provides many security mechanisms to secure communication between the sender and the recipient. It provides an encryption function for message encryption. On the other hand, the recipient also has the option to change the ciphertext in an original message. Thanks to encryption, a message cannot be understood by anyone, except the user who has the right to see the message. The sender must obtain authorization from the recipient before sending the message. First of all, a request is sent to a recipient who has information that the sender wants to share. The recipient decides whether to accept or reject the sender's request.

There are many threats that can affect Bluetooth performance. The most common threat faced by Bluetooth technology is *Blue Jacking*. It is usually harmless because users generally do not notice it. It sends a text message, but with a Smartphone, you can also send images or sounds. The second threat is *Bluesnarfing*. This is unauthorized access to information. It allows access to calendars, contact lists, e-mails and text messages. It also allows you to copy private user images and videos. The difference between these two threats is that *Blue Jacking* is essentially harmful as it only transmits data to the target device, while *Bluesnarfing* is theft of information from the target device.³²

8.1.3 WSN in generale

Normally the WSNs (*Wireless Sensor Networks*) are the set of technologies that require a *Gateway* for network access. They are composed of a variable number of nodes, from a few nodes to tens of thousands of nodes. Normally each node has four parts: sensors, battery, microcontroller and memory.

The functionality of a WSN can be easily understood by analysing how sensors are used to collect information and how it is stored for re-use. The goal is to send them all to the *Server*. They can also be powered by batteries, which offer the possibility of working continuously. The architecture of a WSN is composed of five levels: physical, connection, network, transport and application level³².

There are several attacks against WSNs, such as service attacks, authentication problems, *Denial-of-Service* (DOS) and *Distributed DOS* (DDOS)^{127 32}.

8.1.4 Wireless Fidelity (Wi-Fi)

Wi-Fi networks are wireless communication networks, the technology does not include intrinsic security systems, such as encryption. This implies the possibility for an attacker to

1 ¹²⁶ Padgett J., Scarfone K., Chen L. Guide to Bluetooth *Secyrity*. National Institute of Standards and Technology; Gaithersburg, MD, USA: 2012

1 ¹²⁷ Drira W., Renault E., Zeghlache D. Towards a secure social sensor network; Proceedings of the 2013 IEEE International Conference on Bioinformatics and Biomedicine (BIBM); Shanghai, China. 18–21 December 2013; pp. 24–29

intercept the message and modify it. Obviously at the application level we can consider using cryptographic systems that at high level make the messages more secure.

8.1.5 LoRaWan

LoRaWAN security is designed to comply with the features of the protocol: low power consumption, low implementation complexity, low cost and high scalability.

A more detailed examination of this technology is presented, given that the *Beacon Südtirol - Alto Adige* project intends to implement *IoT* networks based on LoRaWAN for field tests, also with the provision to users of the relevant Community.

The current version of LoRaWAN is 1.1, which was a major update of the LoRaWAN specification introduced in October 2017¹²⁸. As with earlier versions, the network is composed of end devices that are connected with a single *Hop* to one or more *Gateways* which, in turn, forward the packets to the *Network Server* through a *Backhaul* network using IP protocols. The *Network Server* is a central element of the network architecture that, in addition to maintaining the same tasks and roles as the previous version, in LoRaWAN v1.1, through a *Roaming* system, can have different roles: Home, Forwarding and Serving; depending on the type of *roaming* involved.¹²⁹ The *Join Server* has been revised in its architecture and continues to have the same roles.

As regards the authentication mechanism, there was an important improvement in LoRaWAN v1.1 with the complete separation between the network and security in the applications, using two separate keys. It is important to note that the keys must be specific to each device, that is to say that each device must have its own set of keys and the disclosure of these keys must concern only the final device.¹²⁹

LoRaWAN uses two security levels: one for the network and one for the application level. The Network layer security guarantees the authenticity of the device in the network. The application layer security ensures that the network operator does not have access to the end user's application data. In the LoRaWAN security protocol, mechanisms have been developed that guarantee mutual authentication of devices, protection of data integrity and confidentiality. Mutual authentication is established between a LoRaWAN end device and the LoRaWAN network as part of the network access procedure. This ensures that only authentic and authorized devices are connected to authentic and authorized networks.

MACs (DevEUI) LoRaWAN and application messaging are exchanged in an authenticated way and protected from attacks that undermine the integrity of the data, they are protected by *Replay* attacks as well as being encrypted.

The mechanisms related to the MAC, combined with mutual authentication, ensure that the network traffic has not been altered, comes from a legitimate device, is not

1 ¹²⁸ Lora Alliance. 2017. LoRaWAN 1.1 Specification, Oct. 2017. <http://lora-alliance.org/lorawan-for-developers>. (21/01/2019)

1 ¹²⁹ Butun, Ismail & Pereira, Nuno & Gidlund, Mikael. (2018). Analysis of LoRaWAN v1.1 *Secyrity*: research paper. 1-6. 10.1145/3213299.3213304

understandable to the interceptors and has not been captured and reproduced in a malicious way.

LoRaWAN *Security* also implements *End-to-End* encryption for application *payloads* exchanged between end devices and application *servers*. The security mechanisms mentioned above are based on AES1 cryptographic algorithms, the method applies different operating modes to the primitive AES cryptographic: CMAC2 for integrity protection and CTR3 for encryption. Each LoRaWAN device is customized with a single 128-bit AES key (called *AppKey*) and a unique global identifier (EUI-64 based on DevEUI), both used during the device authentication process. The assignment of EUI-64 identifiers requires that the transferor has an OUI (*Organizationally Unique Identifier*) issued by the IEEE. Similarly, LoRaWAN networks are identified by a globally unique 24-bit identifier assigned by the LoRa Alliance TM.¹³¹

The *Application Payloads* are always *End-to-End* encrypted between the *End-Device* and the *Application Server*. Integrity protection is provided in a *Hop-by-Hop*, *Hop Over-The-Air* nature through the protection of the integrity provided by the LoRaWAN protocol, while for the *hop* between networks the *Application Server* is guaranteed by the classic HTTPS and VPNs. To be able to communicate on the LoRaWAN network it is necessary to activate a final device (Node). In LoRaWAN networks, two activation methods are available: OTAA and ABP.

The *Over-The-Air Activation* (OTAA) mode requires that the nodes make a connection (*Join*) before starting the data communication with the network *Server*. The *Join* is run in sessions and is repeated every time the session expires. The *Join* cannot occur if the nodes do not have a DevEUI (*End-Device Unique Identifier*) of 64 bits that globally identifies the node, an AppEUI (*Application Device Unique Identifier*) always of 64 bits and that identifies the application, and, finally, an AppKey (*Application Key*) which is an AES-128 key. The latter generates the NwksKey (*Network Session Key*) and the AppSKey (*Application Session Key*), respectively the network session key and the application session key. The DevEUI corresponds to the MAC of a TCP/IP connection and the *Joining* is nothing but the sending of a *Join* request (connection request), by the node, containing the DevEUI and the AppEUI. The network server responds to this request with a DevAddr and an AppNonce (random value) that indicates the acceptance of the connection request. With the AppEUI the node creates the AppSKey and the NwksKey.¹³⁰

The other activation mode is given by *Activation By Personalization* (ABP), in this mode the nodes do not follow the *Join* procedure, as seen in the OTAA method. In fact, the DevAddr, the NwksKey and the AppSKey are already present in the node.¹³⁰

1 ¹³¹ A *White Paper* PREPARED FOR THE LoRa ALLIANCE™ BY GEMALTO, ACTILITY AND SEMTECH February 2017. https://lora-alliance.org/sites/default/files/2019-05/lorawan_Secrity_whitepaper.pdf (last access 20/01/2019)

1 ¹³⁰ LoRaWAN® 1.0.3 Specification. <https://lora-alliance.org/resource-Hub/lorawanr-specification-v103> (last visit 20/01/2019)

To ensure security in this case, each node must have a set of unique network keys and applications, so that network security is maintained even if a node is compromised. The simplicity of implementation linked to the ABP methodology involves less security, because if an attacker came into possession of a node, he could obtain all the security information.

131 130

The attacks that a LoRaWAN network may be subject to are:

RF Jamming Attack, this is an attack aimed at blocking the reception of a *Gateway* signal or a node, which is feasible using low-cost and readily available *hardware*.¹³² This type of attack on the *wireless* network results in a *Denial-of-Service* (DoS), which is generally easy to detect. However, selective RF noise attacks are difficult to detect and very harmful to *Wireless* communications, as they are not easy to avoid.¹²⁹

The *Replay Attack*, as already seen, is an attack in which an attempt is made to replicate a message, in order to make the receiver believe that it is a safe transmission. In LoRaWAN networks this attack is practiced during the *Join* procedure using *Selective RF Jamming* techniques. This attack is particularly effective for LoRaWAN as communication is limited and under quota. For example, each end device can transmit a maximum of 14 packets per day (maximum payload of 12 bytes), including the confirmation confirmations from *Up-links*¹²⁸. At the same time the attack is made substantially more difficult by the existence of different reception paths for the *End-Device* packets (for example when *End-Device* transmissions can be received by multiple *Gateways*), which should be common in a LoRa network.¹²⁹

Beacon (Class B) Synchronization Attack – Class B *Beacons* (they are a new class of device that simply sends a presence message sent from a device) are in no way protected, which means that an attacker can set a *Gateway* to send fake *Beacons*. This could desynchronize the Class B *End-Device* with the *Gateway* and increase the collisions on the transmitted packets. This security flaw could be resolved by inserting a key that *gateways* could use to authenticate *Beacon* transmissions.

Analysis of network traffic - this is a particular type of *Eavesdropping* attack, as it is not intended to understand the message exactly but to infer information from the traffic generated and its type. With this type of attack an attacker can set up a *gateway* to receive packets and deduce some information. Without access to the key, the attacker will not be able to decode the content of the received packets and the object, the usefulness of this traffic analysis will depend largely on the application. For example, a LoRa network distributed in a building to detect employment patterns could leak information on the level of activity in the building through the analysis of transmission speeds.

1 ¹³² Emekcan Aras, Gowri Sankar Ramachandran, Piers Lawrence, and Danny Hughes. 2017. Exploring The Security Vulnerabilities of LoRa. In Cybernetics (CYBCONF), 2017 3rd IEEE International Conference on. IEEE, 1–6

Man-in-The-Middle Attack: in the literature there are many works that have considered this type of attack in LoRaWAN networks, in particular for v1.0. In fact, in the work reported in note 133¹³³, it presents different vulnerabilities of LoRaWAN v1.0. The author refers in particular to a "*Bit-flipping attack*", a particular MITM attack. Yang clearly showed that LoRaWAN v1.0 has a vulnerability to MITM attacks between the *Network Server* and the *Application Server*. An attacker who can intercept communications between these two servers can discover some of the secret keys that are exchanged, as the communication is not encrypted¹²⁹. The work of Donmez et al ¹³⁴ focused on the security of LoRaWAN v1.1 in back-compatibility scenarios and verified that the handover-roaming offers greater possibilities of *Man-in-The-Middle* (MITM) attacks, since *FRMPayload* messages are not protected and are first transported from the *serving-Network Server* to the *homing-Network Server*, from there to its *Application Server*.¹³⁵ Therefore the same vulnerability is still valid for LoRaWAN v1.1, in which the security of communications between the various roles of the *Network Server*, the *Join Server* and the *Application Server* are not specified very well nor in detail. The v1.1 specification suggests using encrypted communications between servers, but implementation errors are always possible¹³⁵. To quote the passage in the article of note 135 "*According to our interview with the real users of LoRaWAN, network administrators are not at all worried about MITM attacks and do not follow recommendations on the use of encryption between servers*". This shows how a LoRaWAN network can be subjected to this type of attack.

In general, therefore, the two types of MITM attacks that are brought to a LoRaWAN network are:

- *Bit-flipping or Message Forgery Attack*: as already mentioned it is an attack in which someone introduces changes the content of messages between the *Network Server* and the *Application Server*, for example using a rogue *Network Server*.
- *Frame Payload Attack*: is a sort of *Frame injection Attack*. As already explained, it is possible thanks to the *handover-roaming* that offers more possibilities for a MITM attack, since the unprotected *FRMPayloads* are first transported from the *serving-Network Server* to the *homing-Network Server*, and from there to the *Application Server*.¹³⁵

1 ¹³³ Xueying Yang. 2017. LoRaWAN: Vulnerability Analysis and Practical Exploitation. (2017)

1 ¹³⁴ Dönmez, T.C. ; Nigussie, E. Security of LoRaWAN v1.1 in Backward Compatibility Scenarios. Procedia Comput Sci. 2018, 134, 51–58

1 ¹³⁵ Butun, Ismail & Pereira, Nuno & Gidlund, Mikael. (2018). Security Risk Analysis of LoRaWAN and Future Directions. Future Internet. 11. 3. 10.3390 / fi11010003

These possible threats then have to be associated with all those related to physical conditions, ie when a Node, *Gateway* or *Network Server* is missing. In these cases, you could run into one:

- *Destruction or removal, even fraudulent, or failure*: the network problem that is created in all three or four cases has a network problem, in particular if there is no *Gateway* or *Network Server*. Worst case if stolen, in this case the roads would be opened to other scenarios, such as the extraction of the security parameters and the cloning of the device or replacement of the firmware.¹³⁵

Ismail Butun et al.¹³⁵ have compiled a list of possible security threats with the methods and tools of analysis devised by ETSI (European Telecommunications Standards Institute). By obtaining the following results:

LoRaWAN v1.1 presents a low risk in case of security attacks of the following types:

Bit-flipping or Message Forgery Attack

Destroy, Remove, or steal an *End-Device*

Fake *Join* Packet

Frame *Payload Attack*

Network Flooding *Attack*

Network Traffic Analysis

RF *Jamming Attack*

Selective Forwarding Attack

Sinkhole or Blackhole Attack

LoRaWAN v1.1 presents a high risk in case of security attacks of the following types:

- *Beacon Synchronization DoS Attack* (high for accessibility and low for the rest)
- *Impersonation Attack* (high for accessibility and low for the rest)
- *Plaintext Key Capture* (low for accessibility and high for the rest)
- *Security Parameter Extraction* (low for data integrity and accessibility, high risk for the rest)

Furthermore, the following attack types are critical:

Device Cloning or Firmware Replacement (critical risk for authentication and access control, high risk for confidentiality and integrity and low risk for data accessibility)

Self-Replay Attack (critical to accessibility and low for the rest)

Rogue End-Device Attack (critical for authentication and access control, low for the rest)

Thus, with the release of LoRaWAN v1.1, security breaches and inconveniences affecting LoRaWAN v1.0 were resolved. Although it has improved the security properties compared to the previous version, LoRaWAN v1.1 still presents some security risks, some introduced by the new security framework, others not being covered by the specification, which guarantees the attention of the developers.

According to the result of the analyses taken into consideration^{129 132 133 134 135}, LoRaWAN v1.1 seems to have a couple of relevant security threats (in particular vulnerabilities due to physical attacks of the final device, rogue *gateways* and *Replay* attacks). However, LoRaWAN v1.1 has proved more secure and reliable than the previous version (v1.0).

8.1.6 Sigfox

There is not much security on the Sigfox networks linked to the bibliographic level, as was found for other *Open* technologies. Many articles simply report what is stated in the officially released documents, or make an examination of the types of security systems present in the specifications. The reason is probably to be found in the fact that access to Sigfox networks is granted for a fee, the technology foresees the presence of *servers* held by technology licensees and that for the end user the only devices available are nodes and *gateways*. In January 2019¹³⁶ during the last Sigfox Connect event in Berlin, the Sigfox *Micro Base-station* was announced, a base station that allows the extension the low-cost Sigfox public network to non-coverage areas and the creation of a local network that connects to it.

Security in Sigfox is addressed through a systematic process, in fact in the *Sigfox White Paper* the security is defined as "*By Design*". This is because Sigfox devices work mainly in *Offline* mode with an integrated behavior. Furthermore, *Sigfox Ready* certified devices cannot connect directly to the internet, when a device has to communicate through the internet, it sends a message to the *Base Station* that forwards it on the network, vice versa a message coming from the internet is received by the *Base Station* and the message is transmitted to the Sigfox central network, which is delivered to the corresponding *IoT* applications in the area. Therefore, all certified devices cannot connect to the internet, they can send data arbitrarily. *Sigfox Ready* devices are separated from the internet through a Firewall.¹³⁷ This Sigfox network architecture offers an *Air Gap* and it is not possible to access an end point through the Internet in a malicious way. In Sigfox¹³⁸, each device is equipped with a unique symmetric authentication key assigned by the manufacturer during production. If one of the devices is compromised, it can have a limited impact on the network. A cryptographic *Token* is calculated using this authentication key for each sending or receiving of a message. This *token* is used for sender authentication and message integrity. Authentication of communications between the *Sigfox Core Network* and application servers is based on classic internet approaches such as VPN or HTTPS.¹³⁷

1 ¹³⁶ <https://www.disk91.com/2019/technology/Sigfox/the-Sigfox-micro-base-station-test/>. (last access 18/02/2019)

1 ¹³⁷ Make things come alive in a secure way. https://www.Sigfox.com/sites/default/files/1701-Sigfox-White_Paper_Secyurity.pdf (last visit 19/february 2019)

1 ¹³⁸ LPWA Technology Security Comparison, A *White Paper* from Franklin Heath Ltd, 02 May 2017. Available: <http://www.huawei.com/en/events/mwc/2016/summit/global-nb-IoT/nb-IoT-enabling-new-business-opportunities>

To detect *Replay* attempts, the Sigfox core network uses a sequence counter contained in each Sigfox message. Since Sigfox devices are not IP-addressable there is no *over-the-air* (OTA) activation mechanism and the possibility of *Jamming* attacks is reduced. In Sigfox the user can choose whether or not to encrypt the message using the encryption solutions provided by Sigfox. Users can also use their own encryption methods, if necessary^{137 138 139 140}.

As mentioned, the *Sigfox Ready* devices memorize the authentication key. Since the key is unique per device, compromising a device has a very limited impact. The Base Stations store the credentials to communicate with the *Sigfox Core Network*. State-of-the-art protection approaches are based on TPM.

Finally, the *Sigfox Core Network*, stated in *White Paper*¹³⁷, “stores the authentication keys of *Sigfox Ready* devices and the traffic meta-data. To ensure the integrity, availability and confidentiality of these data, state-of-the-art solutions have been implemented - without specifying which ones. “A continuous improvement process has been defined to ensure that *Sigfox Core Network* complies with local regulations” - without saying how.

Sigfox contains a sequence counter that is verified by the *Sigfox Core Network* to detect *Replay* attempts.

Finally, cryptography. Rather than trying to develop a single solution for all applications, for Sigfox, security is relative and should therefore be adaptable to the risk requirements of any application. For many applications, encryption is an unnecessary expense; for others it is essential, for this reason the user is left with the decision to use it or not.

At this point it is reported by Fujdiak et al.¹⁴¹, Sigfox is a proprietary solution with a greater potential risk.¹⁴² Furthermore, Centenaro et. Al¹⁴³ comes to a very similar conclusion adding that Sigfox is leaving the final security to the user.

From the point of view of the safety assessment, the Sigfox security solution is based on the following key components:^{144 145 146}

- 1 ¹³⁹ Laurentiu Coman, Florian & Malarski, Krzysztof & Petersen, Martin & Ruepp, Sarah. (2019). *Secyrity Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox and NB-IoT*. 1-6. 10.1109/GIoT.2019.8766430
- 1 ¹⁴⁰ Chacko, Smilty & Deepu Job, Mr. (2018). *Secyrity mechanisms and Vulnerabilities in LPWAN*. IOP Conference Series: Materials Science and Engineering. 396. 012027. 10.1088/1757-899X/396/1/012027
- 1 ¹⁴¹ Fujdiak, Radek & Blažek, Petr & Mikhaylov, Konstantin & Malina, Lukas & Mlynek, Petr & Misurec, Jiri & Blazek, Vojtech. (2018). *On Track of Sigfox Confidentiality with End-to-End Encryption*. 1-6. 10.1145/3230833.3232805
- 1 ¹⁴² Noushin Poursafar, Md Eshrat E Alahi, and Subhas MukHopadhyay. 2017. Long-range *Wireless* technologies for *IoT Applications*: A review. In *Sensing Technology (ICST)*, 2017 Eleventh International Conference on. IEEE, 1–6. DOI:<http://dx.doi.org/10.1109/ICSensT.2017.8304507>
- 1 ¹⁴³ Marco Centenaro, Lorenzo Vangelista, Andrea Zanella, and Michele Zorzi. 2016. Long-range communications in unlicensed bands: The rising stars in the *IoT* and *Smart City* scenarios. *IEEE Wireless Communications* 23, 5 (11 2016), 60–67. DOI: <http://dx.doi.org/10.1109/MWC.2016.7721743>
- 1 ¹⁴⁴ Sigfox 2017. *Secure Sigfox Ready Devices: Recommendation guide*. Sigfox. (Technical documentation, rev. 34)
- 1 ¹⁴⁵ Sigfox 2017. *Sigfox Technical Overview*. Sigfox. (Technical documentation).
- 1 ¹⁴⁶ Oriol Solà Campillo. 2017. *Secyrity issues in Internet of Things*. (2017). <http://hdl.handle.net/2117/109290>

Manufacturer's Static key, the so-called *Porting Authorization Code* (PAC), which is used for registering devices to the network (regenerated after use).

Unique identifier of the device (ID), which is used together with the *Unique Network Authentication Key* (NAK) generated by the Server in a *Cipher-based Message Authentication Code* (CMAC) function for device authentication.

Message Integrity Code (MIC) with a size of 2-5 bytes, which is calculated by the *Payload* of a message and guarantees the integrity of the message together with a progressive number provided by the base counter to determine the precedence of the message.

Each message is sent three times to guarantee the availability of the service, but there is no recognition.

In addition, the Sigfox documentation discusses cryptography using symmetrical AES-128 encryption in flow meter (CTR) mode¹⁴⁴. However, this encryption is not yet implemented and does not provide the *End-to-End* encryption application level from the sensor to the end user. This imperfection could hinder the use of Sigfox in the context of more critical applications, where private and sensitive data is transferred¹⁴¹. In fact, as stated by Alessandro Bassi, President of *IoTItaly* in the article *Sigfox and the Crittografia*¹⁴⁷ "The biggest problem is due to the implementations of this system. Many Sigfox Modems either do not implement or specify how to enable encryption. This can be done using the Sigfox library directly, which requires an AES implementation and uses a Secure Element to store secret keys."

Other security flaws have been identified in the work of Florian Laurentiu Coman et al¹³⁹. The article reports a series of attacks with PoC (*proof of concept*), in particular for Sigfox they tested a *Replay* attack with DoS. From which they verified that *Replay* attacks are very likely. In fact, the algorithm that calculates the MAC is not, at the moment, public, and uses an AES in CMAC mode similar to LoRaWAN, with the secret NAK (*Network Access Key*) and the 12-bit SN (*Serial Number*) (for *Up-link* messages). For *Down-link* messages, there is no public information about the size of the SN, so it is impossible to tell if they are more or less secure than the *Up-link* messages.¹³⁹ From this the number of different *Up-link* messages is 4096 before resetting the SN, this is joined by the fact that the key to calculating the MAC does not change for the life of the device. So with 140 messages per day the SN resets in a month. Given the characteristics of the protocol that are far more efficient than the limitations imposed, the reset could be even faster.¹³⁹ After the reset, the attacker can play any of the previous 4096 open-ended packages, since the NAK security key used to calculate the MAC never changes, which means that the MACs will always be valid for the life of the victim's device.¹³⁹ Obviously even if there is a maximum distance allowed between the SNs between consecutive *Sigfox frames* before the packets are deleted, the problem does not change. In fact, this parameter depends on the subscription and the attacker can calibrate his algorithm so as to replicate it at the correct time.¹³⁹

1 ¹⁴⁷ <http://www.IoTItaly.net/Sigfox-e-la-crittografia-IoTItaly-associazione-italiana-internet-of-things/>

Another consequence of the Sigfox SN gap limit is that the *End-Nodes* can naturally be DoS-ed, without the attacker intervening, if they remain without coverage for a prolonged period of time. The attacker can however make sure that the device is DoS-ed by blocking a number of packets equal to the maximum distance.¹³⁹

Obviously, these are the risk situations detected with the current infrastructure, with the introduction of the Sigfox *Micro Base-station* it is easy to imagine that security problems will be accentuated, in particular for the type of attack presented. Hitting a *Micro Base station* means blocking a whole network of nodes and *Gateways* by cutting them off from the Sigfox public network.

8.1.7 5G Networks

5G networks, as mentioned above, are the latest generation of cellular networks, the fifth to be precise. The objective of 5G technologies is to speed up communication, improve coverage and make *Wireless* networks more responsive. The current situation does not allow us to understand the actual risk linked to technology. Even in light of the various prohibitions that have been imposed by some world countries on the products of some companies, they do not go so far as to clarify how safe 5G technology is, simply stating that devices capable of sniffing and modifying information passing through them can be installed at the infrastructure level. However as reported by Sole 24 ore¹⁴⁸, which incorporates the "*position paper*" published by the *Cesintes-economic intelligence study centre* and Security management of the University of Tor Vergata, entitled: "5G: between economic *intelligence* and *Security*"; the biggest threat that 5G can bring is the amplification of the existing threat space. This happens because the speed of data circulation is much greater and consequently there is an increase in the volume of data that can be maliciously used. Reporting the sentence as inserted in the article "What is increasing in the canonical formula for the determination of the magnitude of the risks is first of all the" impact ", the economic dimension of the exposure, of the trillions of sensitive data moved or kept. Obviously, at this point the potential risks and threats to which we may be subject are many, practically all those highlighted in paragraph 6.2.2.

The prevention and intervention measures are innumerable. Among others, there is one "more effective", recalls Tor Vergata: "Making data unusable or unchangeable". It is encryption, the great new bet now is to examine *Intelligence* and all public and private managers for large amounts of data or sensitive data¹⁴⁸.

8.2 Cybersecurity Issues

Cybersecurity is the term that implies what we call computer security, specifically linked to technology. The concept itself aims to summarize the qualities necessary to reduce vulnerabilities and to tackle the risks that can lead to attacks, ensuring technological functionality under attack.

1 ¹⁴⁸ 5G, security alarm: the risk map. Il Sole 24 ore 28/06/2019. Accessible via web at: <https://www.ilsole24ore.com/art/5g-allarme-sicurezza-mappa-rischi-ACL8ONV> (last access 06/28/2019, 11.00 pm)

Compared to previous years, the problem of cyber-attacks related to internet connectivity is experiencing an exponential increase. Before, they were limited to *Personal Computers* (PCs), laptops and servers, which were already common but not so pervasively integrated into everyone's life. Today, on the other hand, the presence of smartphones and the proliferation of media is leading to a massive and practically continuous use of the connection. This is only the beginning, as pervasive and *Real-Time* communication is being transferred to both domestic and industrial devices and, as can be seen from this document, everything is closely linked to the *Internet of Things*. Unfortunately, this ease of communication has had a price. The risk of data and identification theft has also increased.

As also reported in the "Report 2019 on ICT Security" of CLUSIT¹⁴⁹, due to the *IoT Device* and the current ease of communication, in Italy, on 28 February 2018, the largest DDoS attack (with the aim of striking) ever recorded hit an Akamai¹⁵⁰ customer, who registered a 1.3 Tbps¹⁵² Memcached¹⁵¹ DDoS traffic, a quantity of traffic never before recorded. Furthermore it is stated that the attack had a double dimension compared to the peak generated by Mirai in 2016, *IoT Botnet*, the title of ITespresso¹⁵³ of October 23, 2016 reported: "A gigantic *Distributed Denial-of-Service* (Ddos) which has hit Twitter, Spotify, Reddit and CNN, on the east coast of the United States, originated from the *Smart Home* devices".

In general, from the Akamai site it can be noted that in July 2019 in 7 days, between the 24th and the 31st, the total frequency of attacks observed on all the chains was 81,439,275, the country most under attack was the United States of America with 11.777.443 and the most commonly used attacks were the *SQL Injections* 72.032.394.

This makes us understand the dimension of the problem related to computer security, in particular we must consider that the pool of *IoT* devices exploitable for cyber-attacks is enormous, they are able to create ever more powerful *Botnets* so as to launch attacks of vast scope and with a serious difficulty in identifying the origin. For example, Flashpoint¹⁵⁴ assumes that the attack carried out on Akamai customers was mainly carried out by digital video recorders and IP cameras by XiongMai Technologies.

Therefore, it is easy to imagine coffee machines connected to cloned networks and used to install a *Ransomware*¹⁵⁵ on the control systems of a factory or to block the network creating excessive traffic. Or if we consider the aquarium which is connected to the network and controlled remotely, which acts as a bridge for data theft from the *PC* or

1 ¹⁴⁹ Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia. 2019

1 ¹⁵⁰ <https://www.akamai.com>

1 ¹⁵² <https://www.dynstatus.com/incidents/nlr4yrr162t8>

1 ¹⁵¹ MEMECACHED - <http://memcached.org>. It is a Free & Open Source Cache system, with high performance, specifically it is a Caching system of objects on distributed memory. It does not have a specific application, but is designed to speed up dynamic WEB services based on Database

1 ¹⁵³ <https://www.itespresso.it/cyber-attacco-ddos-negli-usa-via-dispositivi-IoT-122901.html>

1 ¹⁵⁴ <https://www.flashpoint-intel.com/mirai-Botnet-linked-dyn-dns-ddos-attacks/>

1 ¹⁵⁵ class of malware that makes the data of infected computers inaccessible and requests the payment of a ransom to restore them

security cameras placed in the living room or bedroom that start sending data to external Servers.

There are so many scenarios that can be thought of, as can be seen from the previous paragraphs. The important thing is that those who develop technology do not stand and look at the problems to identify the solution. Do not forget, however, that in addition to the problems directly related to the specifications of the technology, the attacks often succeed due to bad habits of the installers and users of the technologies themselves.

Normally, with basic actions, networks can be made more secure, in particular in the case of "things" of an *IoT* network:

- **Set up an authentication process**, this prevents unauthorized users from accessing the network. By carefully setting the authentication rules you can also create customized and profiled accesses, so as to also improve the experience of use. You can start with a Username and Password based authentication, to continue with increasingly complex systems depending on what you want, for example authentication in two steps, or using biometrics.
- As explained, a point of great discussion is the readability of the data that is transferred and that could be stolen by some malicious users who intercept them. In this regard, one of the most powerful systems is **cryptography**. Using an upstream data encryption system, it is possible to create an important and powerful barrier to those who try to steal sensitive information and data from connected devices.
- The *Cloud* is one of the main sources of potential cyber threats hanging over the *Internet of Things* network. The *Cloud* often refers to the *Software* environment of the *IoT* configuration that connects the smart devices and a central *Hub* where the data is analysed and stored. In this case it is the data coming from the *IoT* network that is in danger. Therefore, it is important to choose **a reliable and secure provider** that has security components to check the integrity of the stored data, the platform and the applications.
- It is good to think about **updating all the devices and components present in the network**. This makes it possible to resolve any bugs connected to errors or oversights in the production phase, which over time become known and exploited by the bad guys.
- Also **keeping the APIs** (*Application Programming Interface*), which are used to access the devices connected to the *IoT* network configuration, **secure**. In this case the security must be understood in the management of the authorization to the intercommunication of the devices, the developers and the applications, so as to maintain the integrity of the data. Therefore, it is important to use an API environment that integrates tools and methods for maintaining data integrity.

9 Technological trends in South Tyrol

In this chapter we took a look at the technological trends of the *IoT* world on the Italian territory and in particular from South Tyrol.

In Italy the evolution towards the *Internet of Things* for the corporate fabric has been imprinted by the Italian Government through the incentives provided for by the National Industry 4.0 Plan (today, Company 4.0), which provides tax breaks in various forms for industrial machines equipped with remote maintenance and/or remote diagnosis and/or control systems, continuous monitoring of working conditions and process parameters and other monitoring systems of the production process.

Therefore, it can be said that on a national level the *Internet of Things* is moving on the definition of technological developments, to push the industrial digitalization process towards *IIoT* and consequently the birth of *IoT* services for the people.

Obviously individual companies can move freely in the intricate world of *Hardware*, *Software* and available protocols, but at the national level it is necessary to have a reference infrastructure, in particular with regard to *Networking* and access technologies (see Network Access Layer pag. 29).

The technologies that in this case are taken into consideration, of course, are the technologies that allow the coverage of large areas, so, if we are talking about *Wireless*, we go from the *Cellular-like* to the cellular technologies.

In fact, as can be seen from the document issued by the Chamber of Deputies' research department (XVIII legislature) of 5 April 2019¹⁵⁶, there is a reorganization of the electric radio spectrum following the new National Frequency Distribution Plan (PNRF 2018 - MISE decree of 5/10/2018).

The Plan divides the spectrum by providing for the reassignment of frequencies according to international and European agreements in recent years, to allow the development of new technologies, which provide, for the reduction of the band for television broadcasts in favour of new developments in 5G¹²² communication networks. For the concrete allocation of frequencies, the new National Frequency Allocation Plan (FIP 2018) was approved by the Communications Regulatory Authority (with resolution no. 290/18/CONS of June 27, 2018), then updated February 7, 2019 with Resolution No. 39/19/EC, as required by the budget law for 2019¹²². Moreover, with the decree law n. 135 of 2018, the definitions of *Blockchain* and *Smart Contract* were introduced into Italian law and the 2019 budget law established a Fund for the development of *artificial intelligence* technologies and applications, *Blockchain* and *Internet of Things*¹²². It is also clear from the analysis document of the Chamber of Deputies that the requirements for its implementation were scheduled within the four-year period 2018-2022 to arrive at the definitive passage of the

1 ¹⁵⁶ <http://www.camera.it/temiap/documentazione/temi/pdf/1105154.pdf>

frequencies of the 700MHz band, from digital terrestrial TV Broadcasting to that of 5G wireless broadband communication.

Currently in Italy 5G is being tested in 120 small municipalities, as well as some "Smart Cities": Milan, Prato, L'Aquila, Matera and Bari, Rome and Turin, among which there are no municipalities in South Tyrol.

In addition to the mobile operators with cellular technologies, such as 5G, on the national territory other realities are moving, mostly related to *Cellular-like* technologies such as Sigfox, Ingenu / RPMA and LoRaWAN.

Nettrotter, a subsidiary of EI Towers, is the only licensee for the distribution of the Sigfox network for the *Internet of Things (IoT)* in Italy. The website reads, "*The Sigfox project is already underway: Nettrotter, using the existing TLC and television towers, plans to reach national coverage, with almost **1,000 Sigfox Base Stations installed**.*"

Over 40 of the main Italian cities, including Rome, Milan, Turin, Bologna, Florence, Naples, Bari, Reggio Calabria, Palermo, etc. are already covered",¹⁵⁷ and they declare that 80% of the population is already served by the Sigfox network .

Materlink spa is the licensee for Italy of Ingenu/RPMA technology, but is only available for its own *Metering* products. There is no coverage from the site outside the United States of America.

For LoRaWAN, the discussion changes, as a Dutch company THE THINGS NETWORK has identified a different business model and proposes the installation of a global LoRaWAN network with free access. As also stated in the Community Manifesto, The Things Network "The mission is to build a completely open, decentralized, user-owned and managed *Internet of Things* network". **Currently in Italy there are 31 registered communities and about 211 gateways installed¹⁵⁸.**

In general, Trentino Alto Adige at the level of the AGCOM decree is affected by the 5G experimentation in some Trentino municipalities. Nettrotter, which holds licenses for the development of the Sigfox network in Italy, from its website <https://www.nettrotter.io/index.php/it/our-network-it/italy-it> points out through the coverage map that Trentino Alto Adige has a coverage of between 20% and 49% of the population. In addition, Autobrennero Spa, together with the Bruno Kesler Foundation and other international partners, will also test its 5G motorway network¹⁵⁹ with the "5G-Carmen" project. The LoRaWAN discourse in Trentino Alto Adige is different, to date, there are 3 Gateways registered in THE THINGS NETWORK network in the Province of Trento and around 15 communities present.¹⁶⁰

1 ¹⁵⁷ <https://www.nettrotter.io/index.php/it/our-network-it/italy-it>

1 ¹⁵⁸ <https://www.thethingsnetwork.org/country/italy/>

1 ¹⁵⁹ http://www.ansa.it/sito/notizie/tecnologia/hitech/2019/03/27/fbk-tecnologia-5g-lungo-lautobrennero_26c282c8-3b44-4e33-a96c-f6d26f4b482b.html, https://create-net.fbk.eu/wp-content/Uploads/2019/03/Gds.it_27-03-19.pdf

1 ¹⁶⁰ <https://www.thethingsnetwork.org/Community> [last visit 10/07/2019]

Since 2018 in South Tyrol there has been a particular excitement regarding the infrastructure for *IoT* technologies and applications. In fact, in addition to the "**5g-Carmen**" project, Fastweb has also announced an investment of 3 billion over 5 years for the expansion of the broadband infrastructure¹⁶¹, so it is very likely to create a **26GHz Backbone** for **5G** (of which it is the licensee).

To these important initiatives, aimed at creating a complete infrastructure, in this sense there are both *Wireless* and *Wired* initiatives, such as the project carried out by Alperia Fiber in collaboration with Saidea and Huawei,¹⁶² whose goal is to make the most advanced digital services accessible to the citizens and businesses of Alto Adige¹⁶³; the "**Open IoT for Smart Cities**" project, carried out by Fraunhofer and a local company, whose experimentation takes place through a comparison with a medium-sized municipality of Alto-Adige identified in the Municipality of Merano¹⁶³, where one of the technologies considered is LoRaWan. Still on the subject of LoRa, there is an important initiative by the business incubator Noi Spa with the **Beacon Südtirol-Alto Adige** project, which provided the technology park with a free access LoRa network for study and test purposes. In addition, there are many initiatives that involve the use of technologies that require gateways to access the Internet and implement concepts of *EDGE* and *FOG* internet. Ultimately, in the territory of South Tyrol, we can envisage an evolution of the 5G/5G Fixed *Wireless Access*/Fiber as a *Backbone* and the growth of LoRaWAN Gateways and technologies that require particular Gateways both for routing on LoRaWan and directly on the 5G network. It is understood that the current LTE networks will also still be widely used in the *IoT* area.

1 ¹⁶¹ <http://www.altoadige.it/cronaca/bolzano/la-rete-fissa-5g-di-fastweb-parte-da-bolzano-1.1992703>

1 ¹⁶² https://e.huawei.com/it/videos/it/Huawei-Alperia_Video_CaseStudy

1 ¹⁶³ <https://www.fraunhofer.it/it/i-nostri-servizi/process-engineering-in-construction/openIoTforsmartcities.html>

10 Conclusions

The *Internet of Things* represents one of the components necessary for the new industrial revolution. The fact that every "thing" will be connected to a network, univocally reachable, and can be integrated in a context of centralized or distributed information systems, will allow a technological and shared and pervasive service development. However, in the technological study, the concept of *IoT* and *IIoT* (*Industrial Internet of Things*) is not clearly distinguished. Therefore, the vision of the *IoT* can be consumer or industry oriented. In the consumer-oriented concept the focal points are people, domestic applications, consumer electronic devices, cars, computers and many other commonly used objects. Industry 4.0 (*IIoT*) instead creates opportunities for companies, production plants or entire sensor networks.

The examination of the various protocols and technologies, which often merge to give rise to a set of specifications and technical characteristics, present at the *Network Access Layer* level in the *IoT* panorama, has highlighted a first adjustment for the *LWPAN/Cellular Like*. In fact, 3GPP has already released all the LTE and NB-*IoT* specifications, the EC-GSM-*IoT* remains, which is at version 13, and the national authorities have already made frequencies and test sites available. On the other hand, companies and research centres do not wait for GSM operators and thanks to the various associations and consortia they have given rise to various valid alternatives, first of all noting Sigfox and LoRaWAN.

In the world of WLAN, PAN, ULPW LAN, very targeted and application-related technologies are emerging such as ANT/ANT+, now present on the market for personal fitness and *health care* gadgets, technologies such as BLE and ZigBee that instead are linked to more broad-spectrum activities are also emerging. ZigBee is more on the industrial and home automation side, where even in these cases there are convergences, as for example is happening between the ZigBee Alliance and the Thread group. The latter products are now becoming part of our homes, in fact many Google NEST Thread products already exist.

In the *Session Communication Layer*, the situation is in the process of stabilization, the most used protocol is the MQTT that is seeing an evolution from a protocol designed for telemetry to the *IoT*-oriented protocol. Not to forget the classic protocols of the WEB, among which the adaptation of the XMPP, born for the exchange of messages, but which is also proving to be an excellent protocol for the *IoT*, and the protocols created to give the entire infrastructure to *Messaging* systems and designed also in an AI perspective, such as NATS.

Finally, the way of managing and analysing data can boast the presence of a myriad of different systems and platforms. In this analysis, only a few that are not always the most used in the *IoT* world have been considered, but they are very interesting from a technological point of view. The results have been released in tabular form in the respective chapters.

Another topic addressed was that of the theme of cybersecurity which, with the spread of the *IoT*, is an increasingly central topic. In this sense, a look was given to the intrinsic safety of devices and technologies, trying to grasp the problems. Finally, it is natural to wonder how much the *IoT* expands the possibilities and methods of intrusion and attack thinking of the spread that the *IoT* paradigm is having. Think about connecting myriads of devices around the world, extending technology and information systems to physical objects that are different in nature and application. All this has led to a small examination of the fundamental actions to be taken to resolve those that, regardless of the technology itself, may be weak points.

Finally, the situation in South Tyrol shows a diversity of applications linked both to technologies and that require a *Gateway* to have access to the Internet and technologies directly connected to the Internet. Considering only the latter, we notice an important start on 5G-related technologies, but at the moment we note only either specific projects or the creation of connection *backbones*. Moreover, as it is also being structured at national level, 5G will complete the areas of greater voracity of data, large cities or large industrial areas. The peripheral areas and, in particular, the rural ones, which are important for South Tyrol, will not be the centre of attention and here, obviously, the company ecosystem, not to mention that of research centres like EURAC, UNIBZ, Fraunhofer Italia, linked to the South Tyrolean *IoT*, is organizing itself with both PAN, LP-WAN and data infrastructures. These allow, through *Gateway*, access to Internet networks maintaining transparency with very high connectivity (indifferent to the use of *Wireless* and *Wired*, cellular or *Cellular-like* technologies) and being able to take advantage of the technological evolution of connectivity that will arrive on the territory.