सत्यमेव जयते

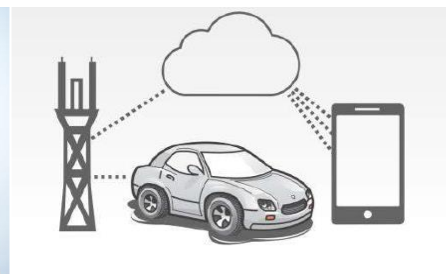
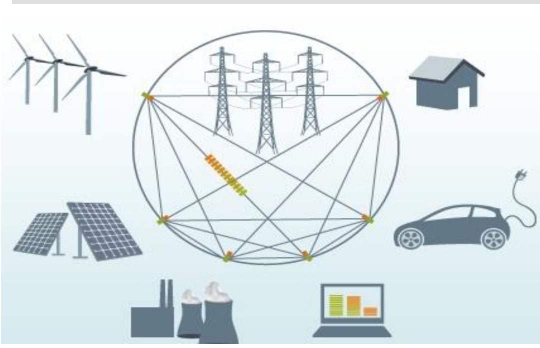
TECHNICAL REPORT

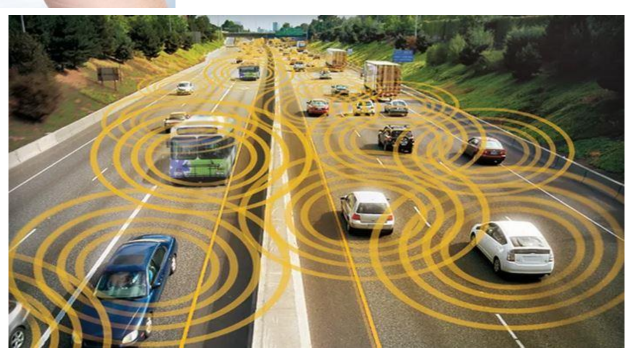
COMMUNICATION TECHNOLOGIES in M2M/IoT Domain

TEC-TR-IoT-M2M-008-01

COMMUNICATION TECHNOLOGIES WORKING GROUP





TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS
MINISTRY OF COMMUNICATIONS
GOVERNMENT OF INDIA

RELEASE 1.0

JULY 2017

Revision History

Date	Release	Document No.	Description
05/07/2017	R1.0	TEC-TR-IoT-M2M-008-01	Technical Report on Communication Technologies in M2M/ IoT domain

Important Notice

Individual copies of the present document can be downloaded from **http://www.tec.gov.in/technical-reports/**.
Users of the present document should be aware that the document may be subject to revision or change of status.
Any comments / suggestions may please be sent to **m2mreports.tec@gov.in**

Disclaimer

TABLE OF CONTENTS

Contents

Page no.

List of Contributors viii

Executive Summary xii

1 Introduction 1

1.1 M2M Communication 1

1.2 Internet of Things 2

2 Projections on Connected Devices 3

3 Terms and Abbreviations 5

4 Various Communication Technologies for M2M / IoT 10

5 Cellular Technologies 12

5.1 Deployment scenarios of cellular M2M 12

5.2 Combining strengths of Cellular & Unlicensed networks 13

5.3 Key performance requirements for the cellular M2M 13

5.3.1 Long battery life 13

5.3.2 Low device cost 14

5.3.3 Low deployment cost 14

5.3.4 Extended coverage 14

5.3.5 Support for a massive number of devices 14

5.4 IoT as a heterogeneously connected system 14

5.5 Cellular Technologies for the Internet of Things 15

5.6 3GPP based LTE IoT narrowband technologies – eMTC and NB-IoT 16

5.7 IoT Optimized Solutions 19
5.8 Battery Performance optimizations 20
5.9 Coverage enhancements 21
5.10 Core network optimizations 22
5.11 Low device cost 23
5.12 LTE-M Rel.12 UE optimizations 24
5.13 Low deployment cost 24
5.14 Summary of 3GPP Solutions 25
5.15 Benefits of 3GPP IoT solutions 29
5.16 Global Roadmap of Next Generation Cellular Technologies for M2M 31
6 Non-Cellular Wireless Technologies 32
6.1 Technologies in Sub-GHz bands 34
6.1.1 Characteristics of Sub-GHz 34
6.1.2 Applications in Smart Grid 35
6.1.3 Low power consumption 37
6.1.4 Wireless range 37
6.1.5 IEEE Standards for Sub GHz 37
6.2 Wi-SUN (Wi-SUN Alliance) 41
6.2.1 Wi-SUN HAN Profile 41
6.2.2 Wi-SUN FAN Profile 43
6.3 NFC 44
6.3.1 How NFC works 46
6.3.2 NFC Eco-system 46
6.3.3 Use-cases of NFC technologies 46

6.4 RFID ... 46
6.5 LPWAN Technologies ... 47
6.5.1 LoRa ... 47
6.5.2 SIGFOX ... 52
6.6 Bluetooth ... 54
6.6.1 Bluetooth Low Energy ... 56
6.7 Wi-Fi ... 57
6.8 IEEE 802.11p ... 58
6.9 Wireless USB ... 59
6.9.1 Protocol architecture ... 59
6.9.2 Functioning ... 60
6.9.3 Radio Requirements ... 60
6.9.4 Power Management ... 60
6.9.5 Security ... 60
6.9.6 Performance ... 61
6.10 ZigBee ... 62
6.11 Visible Light Communications ... 63
6.12 Z-wave ... 65
6.13 Thread ... 65
6.14 Dash7 ... 66
6.15 Ingenu ... 66
6.16 ANT/ANT+ ... 67
6.17 6LoWPAN ... 67
7 Wireline Technologies ... 70

7.1 Power Line Communication 70

7.1.1 Narrow Band Power Line Communication 71

7.1.2 Broadband PLCs 75

7.2 Digital Subscriber Line (DSL) 77

7.2.1 G.fast broadband standard (ITU-T G.9701) 77

7.2.2 FTTH standards for 10 Gbit/s fibre to the home 78

7.3 Coexistence of PLC and DSL technologies 78

8 Comparison Table for Wired and Wireless Technologies 80

9 Broad requirements for a Gateway / Platform 85

9.1 Gateway 85

9.2 Platform 85

10 Testing and certifications 86

11 Recommendations / Way Forward 87

12 Bibliography 89

ANNEXURE 1 : Architecture and Protocols for a Gateway 92

ANNEXURE 2 : NB-IoT Based Use Case 98

ANNEXURE 3 : Flood Alert System using LoRa network 101

ANNEXURE 4 : Smart Street Lights Solution using LoRa Network 104

ANNEXURE 5 : Smart Street Lighting solution based on 6LowPAN 106

ANNEXURE 6 : Smart metering in advanced metering infrastructure (AMI). 109

ANNEXURE 7 : Advanced Metering Infrastructure (AMI) pilots using 6LoWPAN 114

ANNEXURE 8 : Street Light Automation and Smart Living (using C-DOT CCSP) 118

ANNEXURE 9 : Communication Technologies – related SDOs and certification details 123

LIST OF TABLES

Table 1 : Terms and Abbreviations..5

Table 2 : Reducing complexity for LTE IoT devices, [7] 19

Table 3 : Complexity / cost reductions for LTE-M and NB-IoT evolution, [8] 24

Table 4 : 3GPP Optimizations and Applications 26

Table 5 : 3GPP Optimizations and KPI values..28

Table 6 : Snapshot of de-licensed spectrum in Sub-GHz in various countries......................................32

Table 7 : Snapshot of specifications of the De-Licensed bands in India 33

Table 8 : Bluetooth Operating Frequency Bands 55

Table 9 : Bluetooth Power Classes 55

Table 10 : Various 802.11 Standards...57

Table 11 : Properties of VLC 64

Table 12 : Global PLC Standards, Narrowband, [18] 70

Table 13 : Global PLC standards,Broadband, [18]..71

Table 14 : Comparison of Communication Technologies, [9] 80

LIST OF FIGURES

Figure 1 : M2M Concept, [1] 1

Figure 2 : Connecting Things in M2M / IoT, [1]...3

Figure 3 : Key Enabling Wireless Technologies for IoT, [1] 10

Figure 4 : Communication Technology Usage Scenarios, [3] 12

Figure 5 : Examples of wireless connectivity technologies for IoT, [6] 15

Figure 6 : LTE platform and Connectivity requirements, [7]..15

Figure 7 : 3GPP evolution steps for massive IoT, [3]...17

Figure 8 : LTE IoT - Cat-M1 and Cat-NB1 devices, [7] 18
Figure 9 : Cat-NB1 (NB-IoT) deployment options, [7] 19
Figure 10 : Techniques to increase coverage, [7] 21
Figure 11 : eMTC sharing carrier capacity in legacy LTE configuration, [8] 25
Figure 12 : Advantages of Cellular IoT, [3] 30
Figure 13 : Automated Metering System for a Smart Grid Application 36
Figure 14 : 802.11ah Bandwidth Modes [11] 39
Figure 15: Wi-SUN Home Area Network 42
Figure 16: Wi-SUN FAN System Architecture 44
Figure 17 : LoRAWAN Protocol 49
Figure 18 : Sigfox Architecture 53
Figure 19 : Wireless USB Protocol Stack 59
Figure 20 : Wireless USB Supporting Cluster Connectivity, [13] 62
Figure 21 : Z Wave Architecture 65
Figure 22 : IP Stack Architecture in Contiki Based 6LoWPAN Systems 69
Figure 23 : Meters and More Architecture, [19] 72
Figure 24 : DLMS and COSEM 74

List of Contributors

A. Joint Working Group (JWG) Chairman

Name	Designation	Organization	e-mail address
D.P. De	Sr DDG	Telecommunication Engineering Centre (TEC)	srddg.tec@gov.in

B. Joint Working Group (JWG) Vice Chairman

Name	Designation	Organization	e-mail address
Sushil Kumar	DDG (IoT)	TEC	ddgsd.tec@gov.in

C. Working Group Chairs (Sub WG1 : Non-Cellular Technologies)

Designation	Name	Organization	e-mail address
Chairman	Dr. Manoj Kumar	STMicroelectronics	manoj.kumar@st.com
Vice Chairman	Dr. (Ms) Subashini	VIT	subashini.s@vit.ac.in
Rapporteur	Hem Thukral	ISGF / Ernst & Young	hem.thukral@in.ey.com
Co- Rapporteur	Rajeev Tyagi	TEC	dirsd1.tec@gov.in

D. Working Group Chairs (Sub WG2 : Cellular Technologies)

Designation	Name	Organization	e-mail address
Chairman	Dr. Sendil Kumar	Ericsson	sendil.devar@ericsson.com
Vice Chairman	Dr. Punit Rathod	Intel	punit.rathod@intel.com
Rapporteur	Nirant Amogh	Huawei	namogh@huawei.com
Rapporteur	Dr. Vinosh Babu James	Qualcomm	vinosh@qti.qualcomm.com

Co- Rapporteur	Rajeev Tyagi	TEC	dirsd1.tec@gov.in

E. Primary Authors / Drafting Committee

Name	**Organization**	**e-mail address**
Dr. Manoj Kumar	STMicroelectronics	manoj.kumar@st.com
Dr. Vinosh Babu James	Qualcomm	vinosh@qti.qualcomm.com
Nirant Amogh	Huawei	namogh@huawei.com
Dinesh Chand Sharma	EU Project SESEI	dinesh.chand.sharma@eustandards.in
Sushil Kumar	TEC	ddgsd.tec@gov.in

F. Contributors

Name	**Organization**	**Mail ID**
Sushil Kumar	TEC	ddgsd.tec@gov.in
Dr Manoj Kumar	STMicroelectronics	manoj.kumar@st.com
Dr. Sendil Kumar	Ericsson	sendil.devar@ericsson.com
Dr. Punit Rathod	Intel	punit.rathod@intel.com
Nirant Amogh	Huawei	namogh@huawei.com
Dr. Vinosh Babu James	Qualcomm	vinosh@qti.qualcomm.com
Nagendra Bykampadi	Nokia	nagendra.bykampadi@nokia.com
Anand Nadar	Tata Communications	anand.nadar@tatacommunications.com
Ajay Kumar Mittal	Retired Sr. DDG TEC	akmittal77@gmail.com
Vijay Madan	Ex-TTSL	madan70vijay@yahoo.in
Dinesh Sharma	ETSI	dinesh.chand.sharma@eustandards.in

Roger Samy	SAGEMCOM	roger.samy@sagemcom.com
Benoit PONSARD	SIGFOX	benoit.abeloos@ec.europa.eu
Sumit Monga	Reliance ADAG	sumit.monga@relianceada.com
Hem Thukral	ISGF / Ernst & Young	hem.thukral@in.ey.com
Indar-prakash Singhal	STMicroelectronics	indar.singhal@st.com
Raunaque Quaiser	STMicroelectronics	raunaque.quaiser@st.com
Vinay Thapliyal	STMicroelectronics	vinay.kumar@st.com
Alok Mittal	STMicroelectronics	alok.mittal@st.com
Sharadha Kariyawasam	HW Communications Ltd	sharadha@hwcomms.com
RK Soni	BSNL	rksoni96@gmail.com
Sharad Arora	Sensorise Digital Services Private Limited	sharad.arora@sensorise.net
(Ms) Ranjana Sivaram	TEC	adetm.tec@gov.in
Dr. (Ms) Subashini	VIT	subashini.s@vit.ac.in
Dr. Vetrivelan	VIT	vetrivelan.p@vit.ac.in
Prof. Balamurugan MS	VIT	balamurugan.ms@vit.ac.in
Narang N Kishore	Narnix Techno Labs	kishor@narnix.com
Vishal Kumar	Landis & Gyr	vishal.kumar1@landisgyr.com
Anuj Ashokan	TTSL	anuj.ashokan@tatatel.co.in
Amarjeet Kumar	Procubed	kumar@procubedinc.com
A S Meena	TEC	dirsmc.tec@gov.in
Saurabh Singhal	Tech Mahindra	SS00346355@techmahindra.com
Aurindam Bhattacharya	C-DOT	aurindam@cdot.in

Anupama Chopra	C-DOT	anupama@cdot.in
Ajoy Rajani	Reliance Infrastructure Ltd	ajoy.rajani@relianceada.com
Om Gangwar	Reliance Infrastructure Ltd	om.gangwar@relianceada.com
Rajeev Tyagi	TEC	dirsd1.tec@gov.in

G. Joint Editorial Team

Name	Organization
D.P. De	TEC
Dr. Manoj Kumar	STMicroelectronics
Dr. Vinosh Babu James	Qualcomm
Nirant Amogh	Huawei
Dr. Sendil Kumar	Ericsson
Anand Nadar	Tata Communications
Dr. Punit Rathod	Intel
Ajay Kumar Mittal	Retired Sr. DDG TEC
Sharad Arora	Sensorise Digital Services Private Limited
(Ms) Ranjana Sivaram	TEC
Dinesh Chand Sharma	EU Project SESEI
Amarjeet Kumar	Procubed Inc
Raunaque Quaiser	STMicroelectronics
Ms Namrata Singh	TEC
Sushil Kumar	TEC

Executive Summary

The adoption of M2M / IoT devices and technologies has been increasing at a tremendous rate worldwide. There have been different estimates by different organizations regarding the possible number of connected devices, varying from 24 billion to 50 billion by year 2020. One can safely imagine that there are going to be billions of connected devices in the near term and trillions of devices in the long term. Multiple and different kinds of sensors and communication technologies have helped to create applications and use cases that were beyond imagination some years ago.

With the advent of many technologies, it becomes imperative to have a common mechanism to provide a level playing field and create a guiding mechanism in a country like India. It is further necessary that standards be proposed / adopted fast in order that there are not too many diverse networks that work only within themselves.

Interoperability is of paramount importance at all levels: devices, networks and applications. To integrate all the ideas and to present a complete view of all the requirements and driving forces, TEC has formed several multi stakeholder working groups in the last three years. The areas addressed by these work groups are: Power, Health, Safety & Surveillance, Automotive, Smart Homes, Smart Cities, M2M Gateway & Architecture, Security, Communication technologies etc. Ten technical reports have been released until now and are available on www.tec.gov.in/technical-reports. Actionable points emerging from these technical reports have been used to develop the eco system and are a reference for gap analysis in the areas addressed.

The working Group on “Communication Technologies in M2M / IoT Domain” was created in the year 2016, with the objective to study available wireless / wireline communication technologies in the area of M2M / IoT. Recommendations for Indian implementation was one of the deliverables while considering and building upon the work carried out by earlier working groups in this domain.

Vision and the driving force has been to provide a unified view of all kinds of technologies. The focus is to provide a connected view while individual and independent / Standalone implementations are very much part of it. The idea is to provide a framework where network can work independently as also in an interconnected manner if so desired or required.

Communication gateways play a vital role in connecting devices based on one communication technology to the ones that are based on another technology. This is the ultimate vision that whatever is legally permissible in terms of frequency bands, we should be able to make those devices to communicate with each other by means of the gateways that can be specifically designed for the purpose.

This report brings out comprehensively at one place, details of the range of communication technologies available for connecting sensors to gateways or networks as well as for backbone networks. These inter alia consist of cellular, low power wide area networks (LPWAN), short range wireless and wireline technologies. Comparison of technologies w. r. t their possible use cases has been tabulated. De licensed spectrum is going to play a big role in serving communication network for M2M / IoT. It has been emphasized that there will be need for additional de-licensed spectrum as already brought out in an earlier report of TEC.

This report will help in deciding the appropriate communication technologies while being able to take care of interoperability requirements. Key recommendations in the “Recommendations / Way Forward” section may be used to develop the eco system and for gap analysis.

1 Introduction

1.1 M2M Communication

M2M refers to the technologies that allow wired / wireless system to communicate with devices of same ability. M2M uses a device (sensor, meter etc.) to capture an 'event' (motion, meter reading, temperature etc.), which is relayed through a network (wireless, wired or hybrid) to an application (software program), that translates the captured event into meaningful information. A conceptual picture is shown in Figure 1.

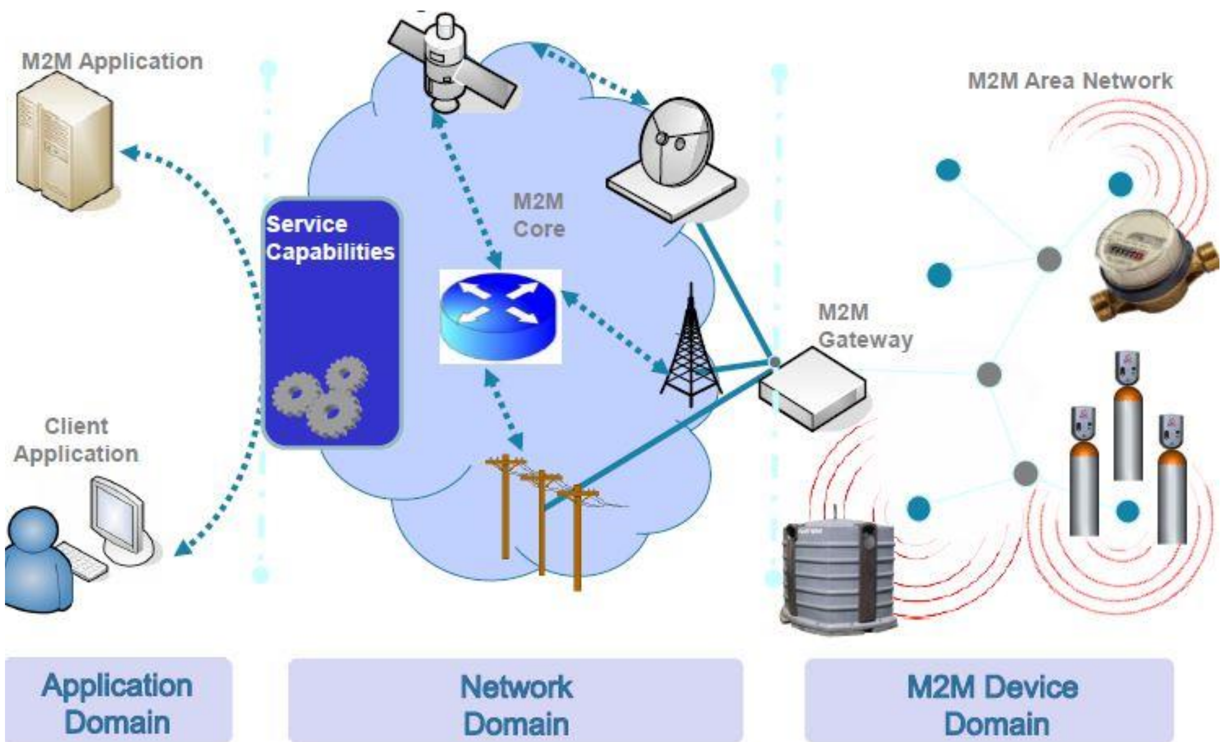


Figure 1 : M2M Concept, [1]

The enabling technologies for M2M communication are sensor networks, RFID, mobile Internet, wired & wireless communication network, IPv4 / IPv6, etc. In Personal area network (PAN)/ Home area network (HAN) / Local area network (LAN)/ Field area network (FAN), low power wireless communication technologies such as Wi-Fi, ZigBee, 6LoWPAN, Bluetooth Low Energy (BLE), Z-wave etc. may be used to connect the devices with the M2M gateway. GSM 3G/ 4G or fixed line broadband / FTTH may be used for connecting M2M gateway to the server. Low Power wide area network (LPWAN) technologies such as LoRa and Sigfox may be used for transmitting very small data over a long range. Based on 3GPP release

13 and onwards specifications, cellular operator can develop LPWAN in three variants namely EC-GSM-IoT, LTE-M and NBIoT.

IPv4 addresses are going to exhaust. Adoption of IPv6 addressing scheme in telecom and ICT organizations provides an opportunity of having billions of devices which can be IP enabled and seamlessly addressable through mobile or wired broadband connections.

1.2 Internet of Things

ITU-T in its Recommendation ITU-T Y.2060 (06/2012) has defined Internet of Things (IoT), as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

ITU-T has also created a Study Group (SG-20) in 2015 to study IoT and its applications in Smart cities and communities.

The Internet of Things (IoT) will revolutionize and change the way all businesses, governments, and consumers interact with the physical world. This level of disruption will have a significant impact on the world in improving the quality of life. The IoT ecosystem may have M2M devices, Gateways, M2M Communication technologies, big data and process management, IoT platform, User interface (web, Mobile, HMI) and end to end security.

IoT will be having a heterogeneous network, having IP and non IP devices connected through IP Gateways. Gateways will be connected to IoT Platform. A huge amount of data will be generated by the sensors. Big data analytics may be used to create intelligence, which may be further used for various operational and planning activities. A typical network having various communication technologies and Gateways has been shown in Figure 2.

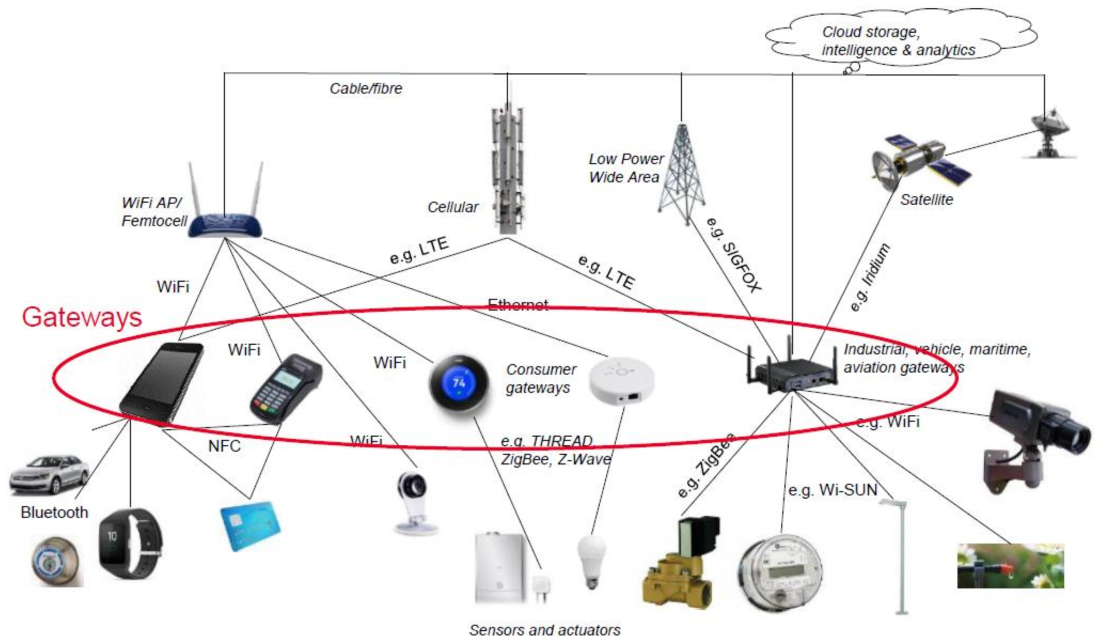


Figure 2 : Connecting Things in M2M / IoT, [1]

Various verticals such as Power sector, Intelligent Transport system, Remote Health management, Safety & Surveillance systems, Village &Agriculture, Homes, and Industries etc. will be transformed to become smart by using M2M / IoT technologies. This will improve the efficiency and in turn the quality of life.

2 Projections on Connected Devices

Chapter 4 of TEC Technical Report on **M2M Numbering Resource requirement and options** [2] has described the detailed study of Global and Indian projections of connected devices. Some important points are as given below:

1. GSMA (GSM Association) and Machina Research estimated that there may be 24 billion connected devices globally by 2020.

2. CISCO/ Ericsson / ITU estimated that there may be around 50 billion connected devices globally by 2020.

3. As per the CISCO study 2015, share of computers (including PCs, tablets, and smart phones) will be just 17 percent of all Internet connections; the other 83 percent will result from IoT including wearable and smart home devices.

4. GSMA study on IoT, 2014 projected that there may be around 25.6 Billion connected devices globally by 2020 and approx. 40% of the total devices may be connected using SIM and a connection to mobile network.

5. Share of wire line technologies for M2M is likely to be very less as the devices / Gateways needing higher bandwidth may be connected directly on fiber. For example camera will require higher bandwidth (2MBps or more) for transmitting real time video.

6. In Mobile World Congress (MWC) 2016, Ericsson announced a drop in the share of SIM connected devices from 40% to just 2% by 2020. It means out of 50B devices, only 1B devices may be connected on SIM by 2020, remaining 49B will be connected on other technologies such as low power wireless / wireline.

7. Global projections vary from 24 Billion to 50 Billion IoT devices by 2020.

8. In India, there may be around 2.6 billion connected devices by 2020.

3 Terms and Abbreviations

Table 1 : Terms and Abbreviations

Abbreviation	Description
3GPP	3rd Generation Partnership Project
3G/4G	3rd Generation/4th Generation (of mobile technology)
AES	Advance Encryption Standard
ARAI	Automotive Research Association of India
ARPV	Advanced Remotely Piloted Vehicle
BLE	Bluetooth Low Energy
BSNL	Bharat Sanchar Nigam Limited
CAB	Conformity Assessment Body
CAGR	Compounded Annual Growth Rate
CAPEX	Capital Expenditure
CCTV	Closed Circuit Television
CDMA	Code Division Multiple Access
CE	Conformité Européene
CE Mode (FeMTC)	Coverage Enhancement Mode
CMS	Central Monitoring System
CSMA / CA	Carrier Sense Multiple Access / Collision Avoidance
DCI	Downlink Control Information
DES	Data Encryption Standard
DIMTS	Delhi Integrated Multi-Modal Transport System
DL	Downlink
DoT	Department of Telecommunications
DSL	Digital Subscriber Line
EC-GSM-IoT	Extended coverage GSM for IoT
eDRX	Enhanced Discontinuous Reception
EPDCCH	Enhanced physical downlink control channel

Abbreviation	Description
ETSI	European Telecommunications Standards Institute
eUICC	Embedded UICC
FAN	Field Area Network
FCC	Federal Communications Commission
FD-FDD	Full Duplex – Frequency Division Duplex
FFS-TBS	For Further Study / To Be Specified
FTTH	Fiber to the Home
G3-PLC	G3-Power Line Communication
GFSK	Gaussian Frequency Shift Keying
GPS	Global Positioning System
GSA	Global mobile suppliers association
GSM	Global System for Mobile (communications)
HAN	Home Area Network
HD	High Definition
HD-FDD	Half Duplex – Frequency Division Duplex
HLAP	High Level Application Requirements
IEC	International Electro Technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoE	Internet of Every thing
IoT	Internet of Things
IPv4/v6	Internet Protocol Version 4/ Version 6
ISM	Industrial Scientific and Medical (Band)
IT	Information Technology
ITS	Intelligent Transport System
ITU-T G.hnem	International Telecommunication Union-Telecommunication G. Home Network Energy Management
iUCC	Integrated UICC
LAN	Local Area Network

Abbreviation	Description
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution
LTE-M	LTE for M2M
M2M	Machine to Machine
MAC	Media Access Controller
Mbps	Mega Bits Per Second
MCL	Minimum Coupling Loss
MCU	Microcontroller / Microcontroller Unit
MDS	Minimum Data Set
MIMO	Multiple Input Multiple Output
MPDCCH	MTC physical downlink control channel
MRA	Mutual Recognition Arrangement / Mutual Recognition Agreement
MTC	Machine Type Communication
NAN	Neighborhood Area Network
NB-IOT	Narrow Band LTE for Internet of Things
NPDCH	Narrowband physical downlink control channel
NPDSCH	Narrowband physical downlink shared channel
NPSS	Narrowband Primary Synchronization Signal
NPRACH	Narrowband physical random access channel
NPUSCH	Narrowband physical uplink shared channel
NSSS	Narrowband Secondary Synchronization Signal
OBD	On-Board Diagnostics
OFC	Optical Fiber cable
OFDM	Orthogonal Frequency Division Multiplexing
OPEX	Operating Expenditure
OSGP	Open Smart Grid Protocol
OTA	Over the Air
PAN	Personal Area Network

Abbreviation	Description
PDSCH	Physical downlink shared channel
PLC	Power Line Communication
PLMN	Public Land Mobile Network
PLT	PoweRline Technologies
POS	Point of Sale
PPDR	Public Protection and Disaster Relief
PRB	Physical Resource Block
PRIME	PoweRline Intelligent Metering Evolution (Alliance)
PSM	Power save Mode
PSTN	Public Switched Telephone Network
PUSCH	Physical uplink shared channel
QoS	Quality of Service
RF	Radio Frequency
RFID	Radio Frequency Identification
RRC	Radio Resource Control
SC-PTM	Single Cell – Point to Multipoint
SIAM	Society of Indian Automobile Manufacturers
SIM	Subscriber Identification Module
TAN	Touch Area Network
TCO	Total Cost of Ownership
TCXO	Temperature-compensated crystal oscillator
TDD	Time division duplex
TEC	Telecommunication Engineering Centre
TTI	Transmission Time Interval
TWACS	Two-Way Automatic Communication System
UICC	Universal Integrated Circuit Card
UL	Uplink
USB	Universal Serial Bus

Abbreviation	Description
UTDOA	Uplink time difference of arrival
V2I	Vehicle to Infrastructure
V2N	Vehicle to Network
V2V	Vehicle to Vehicle
V2X	Vehicle to (X) where X could be I,N,V,etc.
VMS	Variable Message Sign
VoLTE	Voice over LTE
VTS	Vehicle Tracking System
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity (IEEE 802.11x)

4 Various Communication Technologies for M2M / IoT

Cellular technologies have played an instrumental role in connecting the people to one another via voice, and also extended connectivity to the mobile Internet by delivering fast and mobile broadband services.

In the area of M2M / IoT, data from the devices varies from few kilobits (water/ electricity meters, environmental sensors) to several megabytes (Security camera) depending upon the use case. Data may be in the form of bursts and may also be non-critical / critical in nature.

In M2M/ IoT domain, there are various types of communication technologies depending upon the coverage, power, QoS etc. Communication technologies may be categorized to work in TAN / PAN/ NAN/ LAN / WAN depending upon coverage distance. These have been shown in Figure 3 below:

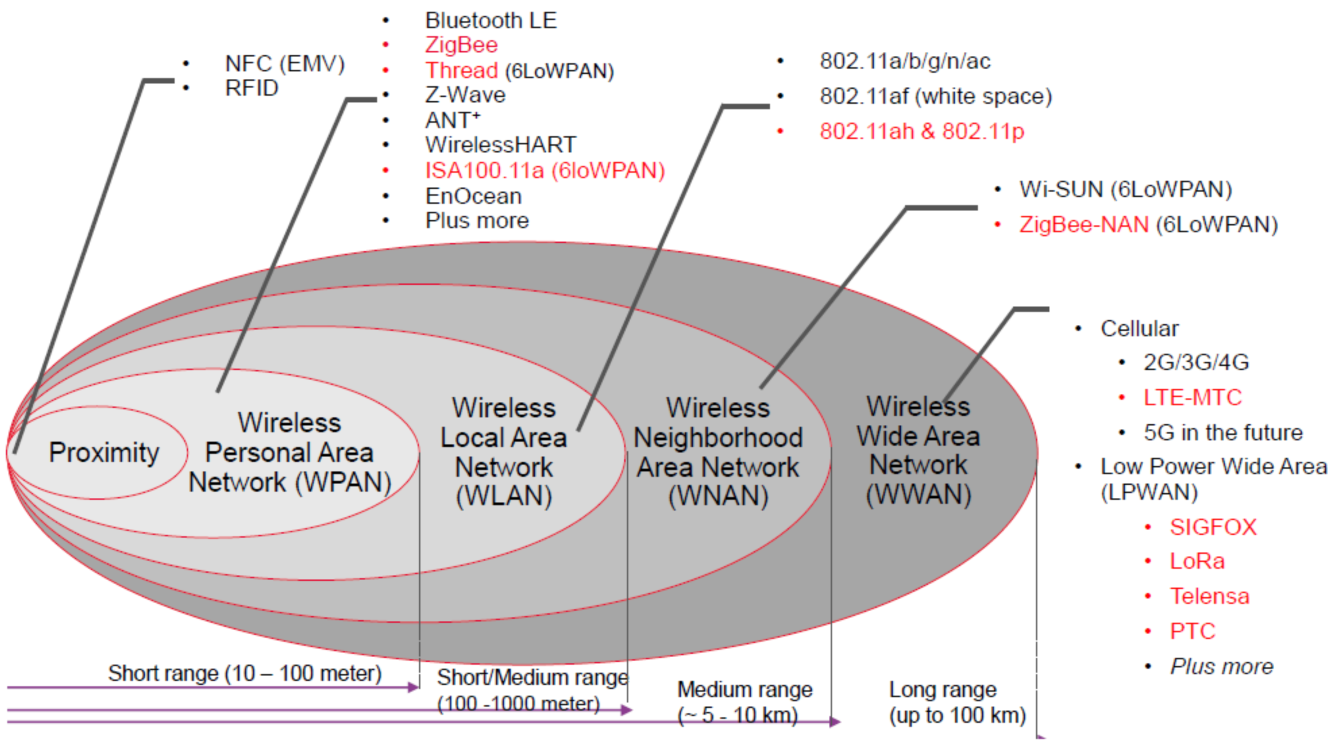


Figure 3 : Key Enabling Wireless Technologies for IoT, [1]

Wide area network may also have wired technologies such as fixed line broadband, Fiber to the home (FTTH) and Power line communication (PLC). These technologies have been described in detail in this report.

Connectivity is the foundation for IoT, and the type of access required will depend on the nature of the application. Many IoT devices will be served by radio technologies that operate on unlicensed spectrum and that are designed for short-range connectivity with limited Quality of Service (QoS) and security requirements typically applicable for a home or indoor environment. Currently, there are two alternative connectivity tracks for the many IoT applications that depend on wide-area coverage:

1. Cellular technologies: 3GPP technologies like GSM, WCDMA, LTE and future 5G. These technologies operate on licensed spectrum and historically have primarily targeted high-quality mobile voice and data services. Now, however, they are being rapidly evolved with new functionality and the new radio access technology Narrowband IoT (NB-IoT) specifically tailored to form an attractive solution for emerging low power wide area network (LPWAN) applications. LTE is established globally and is the fastest growing wireless standard, already delivering over one billion connections worldwide. LTE has delivered on the promise of faster, better mobile broadband, and it is now scaling down for the IoT to bring multi-year battery life and lower cost devices. It is backed by a common global standard (3GPP) with support of a strong, interoperable, end-to-end ecosystem.

2. Non-Cellular Wireless Technologies: Low power and short range wireless technologies such as Bluetooth, ZigBee, have been developed as last mile connectivity to connect End Devices to Gateways. On the other hand, radio technologies, provided by SIGFOX and LoRa, have been developed and designed solely for machine-type communication (MTC) applications with relatively limited demands on throughput, reliability or QoS.

Besides this there are a number of other technologies for short range like Wi-Fi, NFC, RFID, etc. as shown in Figure 3 and described in later sections.

5 Cellular Technologies

5.1 Deployment scenarios of cellular M2M

The coverage needs of a particular use case may be highly localized (such as a stationary installation within a building), while other use cases require global service coverage (such as container tracking). 3GPP technologies already dominate use cases with large geographic coverage needs and medium- to high-performance requirements. With new feature sets specifically tailored for LPWAN IoT applications, 3GPP technologies are taking a large leap forward to cover segments with low-cost, low-performance requirements too. Cellular and non-cellular (wireless technologies excluding cellular) technologies complement each other in terms of range and cloud connectivity as shown in Figure 4.

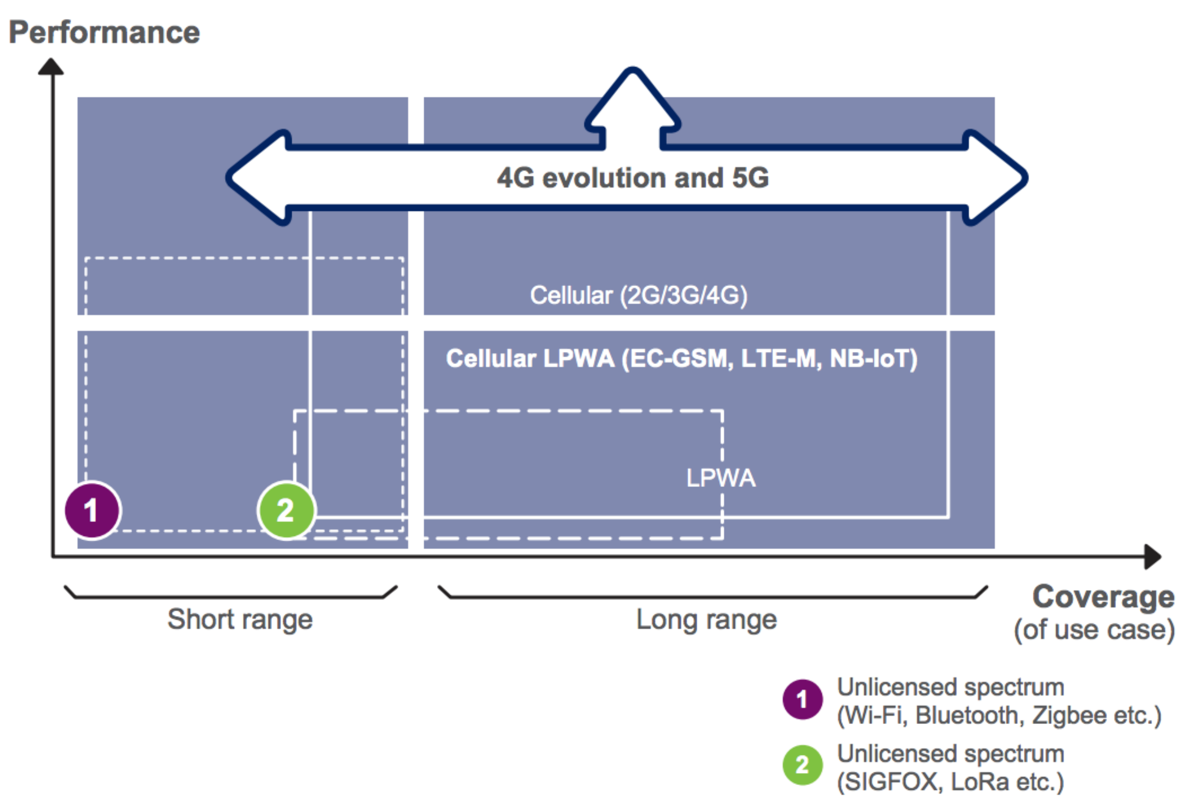


Figure 4 : Communication Technology Usage Scenarios, [3]

5.2 Combining strengths of Cellular & Unlicensed networks

Even when existing 3GPP end-to-end connectivity is not feasible, cellular technology can still provide key benefits when used as a bridging option, i.e. as an aggregation and routing solution. This approach allows end devices to utilize varying access solutions from either the short range or LPWAN domain and access the cellular networks via a gateway device. Such networks enable the reuse of cellular functions and assets such as security, device management, billing and QoS without requiring each end device to be cellular-enabled.

The 3GPP Technologies have also been optimized to support such aggregated traffic from IoT devices through networks using unlicensed spectrum [4]. Due to diverse use cases of IoT deployment, it is important to know their characteristics in terms of energy consumption, massive numbers, reliability, latency & availability.

5.3 Key performance requirements for the cellular M2M

The key requirements for cellular M2M networks to successfully support massive IoT deployment are:

1. Long battery life
2. Low device cost
3. Low deployment cost
4. Extended coverage
5. Support for a massive number of devices.
6. Acceptable latency

These are described in detail as below:

5.3.1 Long battery life

Mobile phone and especially smartphone users are accustomed to charging their device batteries frequently. However, many IoT devices must operate for very long times, often years, without human intervention. A good example is a fire alarm device sending data directly to a fire department. The time interval between battery replacements in such a device is a very important cost factor.

Majority of the devices in M2M/ IoT domain will be battery operated and will also be unmanned. Long battery life is required to keep the device in the network for a long time. Devices may remain in sleep mode while not communicating, to reduce the power consumption.

The industry aims to achieve a minimum of 10 years of battery life for M2M/ IoT devices.

5.3.2 Low device cost

IoT connectivity will generate low ARPU and will give a much less revenue compared to mobile or broadband subscriptions. This in turn requires the device costs to be low. The current industry target is for a module cost of less than 5 USD. To enable a positive business case for cellular IoT, the total cost of ownership including the device must be extremely low or the total number of deployed devices have to be large.

5.3.3 Low deployment cost

The network cost of IoT connectivity, including initial CAPEX and annual OPEX, must also be kept to a minimum. A simple, centrally pushed software upgrade may deploy LPWAN IoT connectivity over existing cellular networks to avoid any new hardware and site visits and keep CAPEX and OPEX to a minimum.

5.3.4 Extended coverage

Extended coverage is important in many IoT applications. Simple examples are smart meters, which are often in the basements of buildings behind concrete walls. Industrial applications such as elevators or conveyor belts can also be located deep indoors. This has driven the M2M community to look for methods to increase coverage by tolerating lower signal strength than is required for other devices. The target for the IoT connectivity link budget is an enhancement of 15-20dB. This coverage enhancement would typically be equivalent to the signal penetrating a wall or floor, enabling deeper indoor coverage.

5.3.5 Support for a massive number of devices

IoT connectivity is growing significantly faster than normal mobile broadband connections and by 2025 there will be seven billion connected devices over cellular IoT networks [5]. This is equivalent to the current number of global cellular subscriptions. The density of connected devices may not be uniform, leading to some cells having very high numbers of connected devices. This means that LPWAN IoT connectivity needs to handle many simultaneous connected devices

5.4 IoT as a heterogeneously connected system

The Internet of Things encompasses a wide variety of applications across many different industries, with devices that can drive very diverse computing and connectivity requirements. In some use cases, devices may only require short-range communication to the network access point, such as ones deployed in connected homes, while many other applications need wider-area, ubiquitous coverage. Connecting the Internet of Things will require heterogeneous connectivity technologies that offer different levels of optimization to address the varying needs. Figure 5 provides a simplified illustration of the different wireless technologies often used to connect the IoT based on how far they can reach. For example, smart lighting in an office building may be best served with a short-range wireless technology, such as Wi-Fi, as light fixtures are usually deployed in areas with reasonable Wi-Fi coverage (i.e. indoors). In contrast, parking meters deployed across a smart city will most likely leverage a wide-area network. Such deployments will require a technology that can provide ubiquitous coverage in both outdoor (e.g. street parking) and indoor (e.g. parking structure) locations.

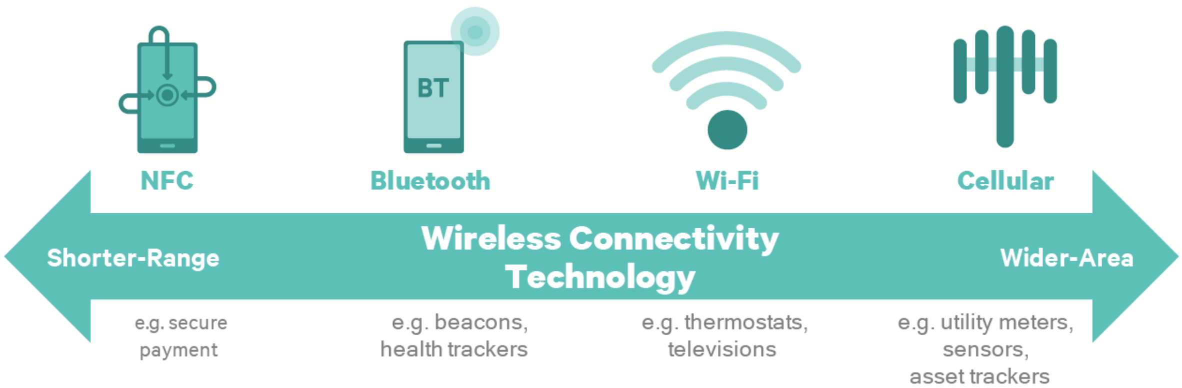


Figure 5 : Examples of wireless connectivity technologies for IoT, [6]

5.5 Cellular Technologies for the Internet of Things

For the wide-area Internet of Things, cellular is evolving to become an attractive platform to address the growing connectivity needs. Not only do cellular-based solutions offer ubiquitous reach into both outdoor and indoor locations, they also bring many additional benefits to the table. The highly-available network design allows IoT devices to reliably access application services around the clock; moreover, the tried-and-true cellular deployments already deliver end-to-end security required by the most demanding users such as governments and financial institutions. And most importantly, the mature ecosystem is backed by global standards that ensure seamless interoperability across regions and devices.

LTE is globally established and the fastest growing wireless standard. LTE, originally introduced in Release 8 of the 3GPP standard, was developed to provide faster mobile broadband access, offering a generational performance leap over 3G. The core LTE technology has evolved over time to adapt to the ever-changing market requirements, ensuring network longevity. LTE Advanced (3GPP release 10, 11, 12) evolved to optimize for better mobile broadband experience, enabling gigabit-class throughput with the introduction of advanced techniques, such as carrier aggregation and higher-order MIMO. While some IoT applications can benefit from the improvements introduced in LTE Advanced (e.g. HD security cameras), many IoT devices require optimizations for a much reduced set of functionalities.

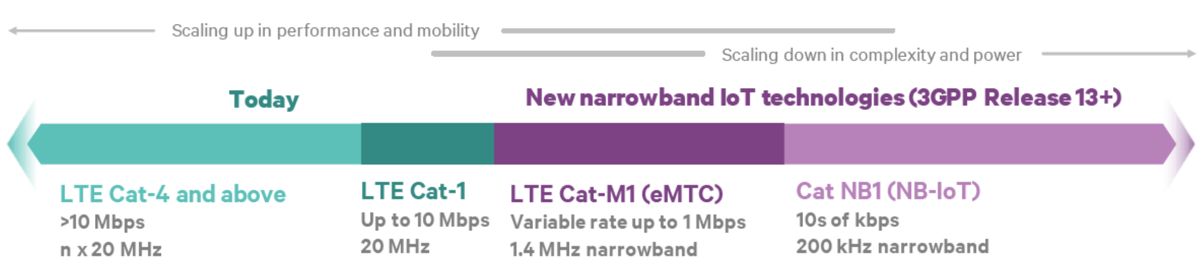


Figure 6 : LTE platform and Connectivity requirements, [7]

Release 13 of the 3GPP standard introduces a suite of new narrowband technologies optimizing for the IoT. Collectively referred to as LTE IoT, it includes two new User Equipment (UE) categories that can more efficiently support lower data-rate applications. LTE IoT is part of the unified LTE roadmap, providing a seamless path to deliver IoT service in existing network deployments; LTE can scale up to offer gigabit class data rates for high performance applications, or to scale down for applications requiring high power efficiency. LTE Cat-M1 (eMTC) enables the broadest range of IoT capabilities, and LTE Cat-NB1 (NB-IoT) scales down further in cost and power for low-end IoT use cases. Both device categories are part of the single, scalable LTE roadmap, and designed to coexist with existing LTE Advanced infrastructure, spectrum, and devices as shown in Figure 6. LTE IoT brings many improvements, including complexity reduction to enable lower cost devices, more efficient low-power modes to deliver multi-year battery life, and new advanced transmission techniques to deepen coverage. Beyond air interface improvements, LTE IoT also enhances the core network to more efficiently handle IoT-centric traffic and to support large number of devices.

NB-IoT also establishes the foundation for Narrowband 5G, which will bring even more opportunities for the Internet of Things. 5G will enhance massive IoT with new capabilities such as Resource Spread Multiple Access (RSMA) for grant-free transmissions, and multi-hop mesh to further extend coverage. 5G will also enable new services, such as mission-critical control, with many innovative use cases in robotics, aviation, healthcare, industrial control, and vehicles, where enhancement dimensions such as sub-1ms latency, ultra-high reliability, and availability are required (but not simultaneously needed for all services). All in all, connecting the Internet of Things will be an integral part of 5G – a unified, more capable connectivity platform for the next decade and beyond.

5.6 3GPP based LTE IoT narrowband technologies – eMTC and NB-IoT

To meet the new connectivity requirements of the emerging Massive IoT segment, 3GPP has taken evolutionary steps on both the network side and the device side. Some of the key improvement areas addressed in 3GPP up to Release 13 are:

1. Lower device cost - cutting module cost for LTE devices by reducing peak rate, memory requirement and device complexity. The LTE module cost-reduction evolution started in Release 8 with the introduction of LTE for machine-type communication (LTE-M) Cat 1 devices with reduced peak rate to a maximum of 10Mbps, and continued in Releases 12 and 13 with reduced device complexity for lower performance and using less bandwidth or a narrowband IoT carrier to cut costs further.
2. Improved battery life – more than 10 years of battery life can be achieved by introducing Power Saving Mode and/or extended discontinuous reception functionality. These features allow the device to contact the network – or to be contacted – on a per-need basis, meaning that it can stay in sleep mode for minutes, hours or even days.
3. Improved Coverage – an improvement of 15dB on LTE-M and of 20dB on NB-IoT and GSM, which translates into a seven-fold increase in the outdoor coverage area and significantly improved indoor signal penetration to reach deep indoors. This supports many IoT devices like smart meters, which are often placed in a basement.

4. Support for massive numbers of IoT connections – specifically, one LTE cell site can support millions of IoT devices, depending on the use case. Core network enhancements include software upgrades for service differentiation handling, signaling optimization and high-capacity platforms.

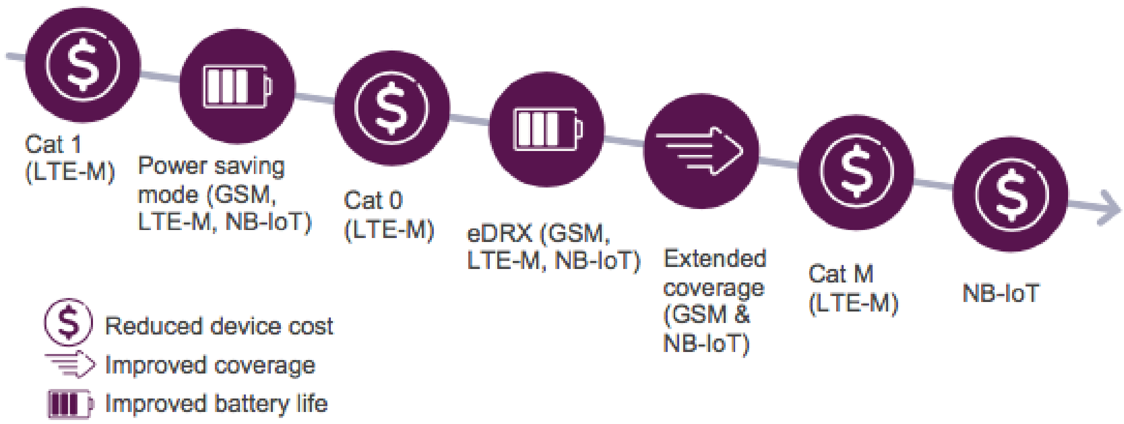


Figure 7 : 3GPP evolution steps for massive IoT, [3]

3GPP Release 13 introduces two new User Equipment (UE) categories that scale down in functionalities to bring more efficiencies for connecting the Internet of Things:

LTE Cat-M1, defined by the eMTC (enhanced machine-type communications) standard, provides the broadest range of IoT capabilities, delivering data rates up to 1 Mbps, while utilizing only 1.4 MHz device bandwidth (1.08 MHz in-band transmissions of 6 resource blocks) in existing LTE FDD/TDD spectrum. It is designed to fully coexist with regular LTE traffic (Cat-0 and above). Cat-M1 can also support voice (VoLTE) and full-to-limited mobility. In enhanced coverage mode, it can deliver 15 dB of increased link budget, allowing LTE signals to penetrate more walls and floors to reach devices deployed deep indoors or in remote locations.

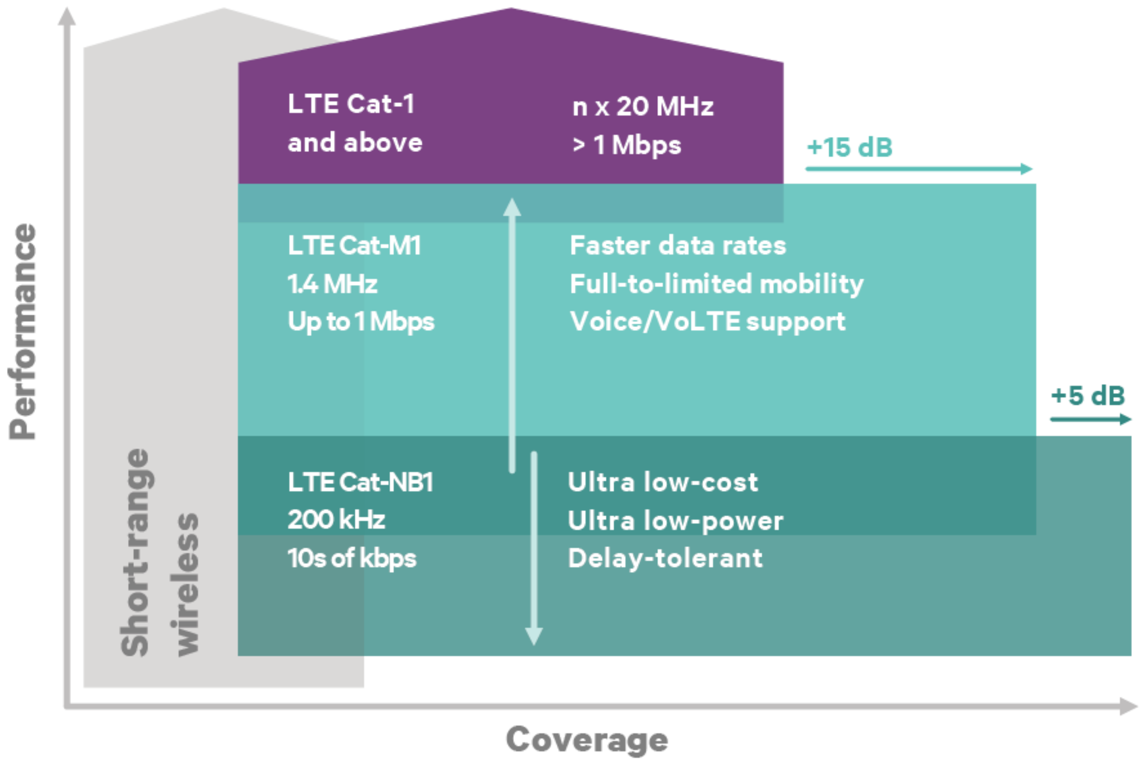


Figure 8 : LTE IoT - Cat-M1 and Cat-NB1 devices, [7]

LTE Cat-NB1, or NB-IoT (narrow band IoT), further reduces device complexity and extends coverage to address the needs of low-end IoT use cases. Cat-NB1 leverages narrowband operations, using 200 kHz device bandwidth (180 kHz in-band transmissions of 1 resource block) in LTE FDD, to deliver throughputs of 10's of kbps. NB-IoT supports more flexible deployment options: LTE in-band, LTE guard-band, and standalone. To further enhance coverage, it trades off spectral efficiency (e.g. data rate), and capabilities (e.g. no mobility or voice support) to achieve >5 dB of extra gain over Cat-M1.

Cat-NB1 devices can be deployed in LTE guard-bands or as a standalone carrier in addition to LTE in-band. Nevertheless, the new 200 kHz device numerology (utilizing a single LTE resource block, or RB of 180 kHz) requires a new set of narrowband control and data channels. Unlike Cat-M1 in-band, Cat-NB1 does not allow for frequency retuning or hopping and occupies a fixed spectrum location. For guard-band deployment, NB-IoT leverages unused resource blocks without interfering with neighboring carriers. In standalone mode, Cat-NB1 devices can be deployed in re-farmed 2G/3G bands.

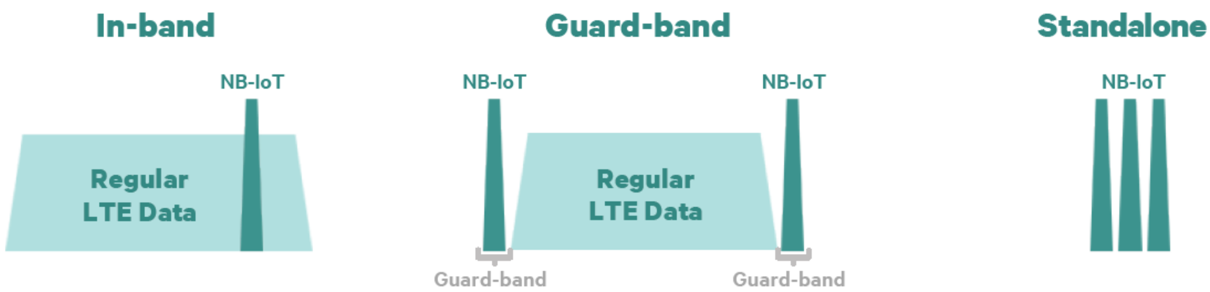


Figure 9 : Cat-NB1 (NB-IoT) deployment options, [7]

5.7 IoT Optimized Solutions

The new LTE IoT narrowband technologies are paving the path to Narrowband 5G, bringing four main areas of improvements to better support the Internet of Things: reducing complexity, improving battery life, enhancing coverage, and enabling higher node density deployments. The proliferation of IoT will bring significant benefits to a diverse set of industries and applications. While there are many IoT use cases that have the potential to drive higher ARPC (average revenue per connection) that is comparable to today's mobile broadband services (e.g. smartphones, tablets), most use cases will require much lower-cost devices and subscriptions to justify massive deployments. For example, the hardware and service cost of a smartphone is very different from a simple remote sensor that provides temperature measurements a few times a day. For this reason, both Cat-M1 and Cat-NB1 devices will scale down in levels of complexity to enable lower cost, while still meeting the IoT application requirements. Table 2 summarizes the high-level complexity differences of the two new LTE IoT UE categories.

Table 2 : Reducing complexity for LTE IoT devices, [7]

	LTE Cat-1 (Today)	LTE Cat-M1 (Rel-13)	LTE Cat-NB1 (Rel-13)
Peak data rate	DL: 10 Mbps UL: 5 Mbps	DL: 1 Mbps UL: 1 Mbps	DL: ~20 kbps UL: ~60 kbps
Bandwidth	20 MHz	1.4 MHz	200 kHz
Rx Antenna	MIMO	Single Rx	Single Rx
Duplex mode	Fill duplex FDD/TDD	Support half duplex FDD/TDD	Half duplex FDD only
Transmit power	23 dBm	20 dBm	20 dBm

Higher throughput, lower latency, full mobility

Peak data rate: Both Cat-M1 and Cat-NB1 devices will have reduced peak data rates compared to regular LTE devices (e.g. Cat-1). Cat-M1 has limited throughput of up to 1 MBps in both downlink and uplink directions, while Cat-NB1 further reduces peak data rate down to 10's of kbps. The reduced peak data rates allow for both processing and memory savings in the device hardware.

Bandwidth: LTE supports scalable carrier bandwidths from 1.4 MHz to 20 MHz, utilizing 6 to 100 resource blocks. For LTE Cat-M1, the device bandwidth is limited to 1.4 MHz only (1.08 MHz plus guard-band for 6 RBs in-band), to support the lower data rate. On the other hand, Cat-NB1 further reduces device bandwidth to 200 kHz (180 kHz plus guard-band for a single RB). The bandwidth reduction for Cat-M1 requires a new control channel to replace the legacy control channels, which can no longer fit within the narrower bandwidth. While for Cat-NB1, a new set of NB-IoT synch, control, and data channels are introduced to accommodate the narrower bandwidth.

Rx Antenna: Multiple antennas for MIMO (multiple-input, multiple-output) and receive diversity was introduced in LTE to improve spectral efficiency. For LTE IoT applications, there is little need to push for higher data rates, but important to reduce complexity. For both Cat-M1 and Cat-NB1, the receive RF is managed with a single antenna, which simplifies the RF frontend. Though there is some RF degradation due to the lack of receive diversity, the lost signal sensitivity can be compensated by other advanced coverage enhancing techniques.

Duplex Modes: Due to the less frequent and latency-tolerant nature of IoT data transmissions, LTE IoT devices can reduce complexity by only supporting half-duplex communications, where only the transmit or receive path is active at a given time. Cat-M1 devices can support half-duplex FDD in addition to TDD, while Cat-NB1 devices only support half-duplex FDD. This allows the device to implement a simpler RF switch instead of a full duplexer that is more complex and costly.

Transmit Power: For both new LTE IoT UE categories, the maximum uplink transmission power is reduced to 20 dBm (100mW) from LTE's 23 dBm (200mW), allowing the power amplifier (PA) to be integrated for lower device cost.

Other simplifications: Other complexity reduction techniques include Cat-NB1's limited support for voice (VoLTE or circuit switched services), and mobility (no link measurement or reporting).

5.8 Battery Performance optimizations

Many IoT devices are battery-operated, and it is highly desirable for them to last for as long as possible on a single charge. The associated cost for field maintenance can be quite daunting, especially in massive deployments. Not only would the planning of scheduled maintenance be an operational overhead, but physically locating these mobile devices (e.g. asset trackers sprinkled all over the world) can also become a nightmare. Thus, maximizing battery life has become one of the most important improvement vectors in LTE IoT. In addition to the power savings realized through reduced device complexity, two new low-power enhancements have been introduced: power save mode (PSM) and extended discontinuous receive (eDRx) – both are applicable to Cat-M1 and Cat-NB1 devices.

Power Save Mode (PSM): PSM is a new low-power mode that allows the device to skip the periodic page monitoring cycles between active data transmissions, allowing the device to sleep for longer. However, the device becomes unreachable when PSM is active; therefore, it is best utilized by device-originated or scheduled applications, where the device initiates communication with the network. Moreover, it enables more efficient low-power mode entry/exit, as the device remains registered with the network during PSM, without having the need to spend additional cycles to setup registration/connection after each PSM exit event. Example applications that can take advantage of PSM include smart meters, sensors, and any IoT devices that periodically push data up to the network.

Extended Discontinuous Reception (eDRx): eDRx optimizes battery life by extending the maximum time between data reception from the network in connected mode to 10.24s, and time between page monitoring and tracking area update in idle mode to 40+ minutes [6]. It allows the network and device to synchronize sleep periods, so that the device can check for network messages less frequently. This however increases latency, so eDRx is optimized for device-terminated applications. Use cases such as asset tracking and smart grid can benefit from the lower power consumption realized through the longer eDRx cycles.

5.9 Coverage enhancements

There are many IoT use cases that can benefit from deeper network coverage, especially for devices deployed in challenging locations such as utility meters. In many use cases, trading off uplink spectral efficiency and latency can effectively increase coverage without increasing output power that will negatively impact the device battery life. A few techniques to enhance the coverage are described below:

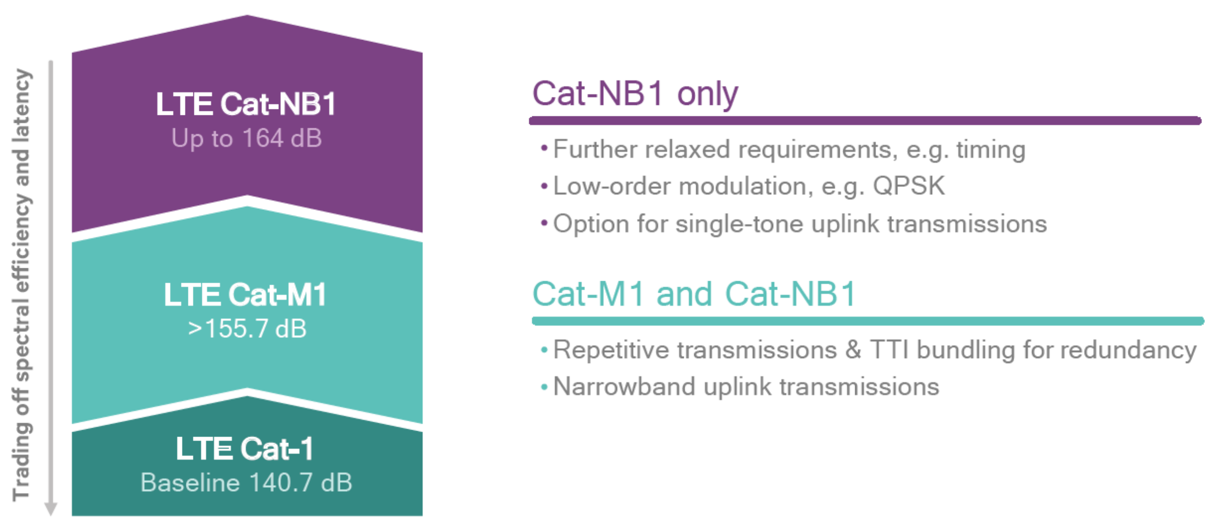


Figure 10 : Techniques to increase coverage, [7]

Redundant transmissions: Transmitting the same transport block multiple times in consecutive sub-frames (TTI bundling) or repeatedly sending the same data over a period of time (repetitive transmission) can significantly increase the probability for the receiver (cell or device) to correctly decode the transmitted messages.

Power Spectral Density (PSD) boosting: While the serving cell can simply increase transmit power in the downlink to extend coverage, it is also possible for the device to put all the power together on some decreased bandwidth (e.g. Cat-NB1 can transmit on 3.75 kHz sub-carrier spacing in a new numerology, vs. 15 kHz in Cat-M1 and LTE) to effectively increase the transmit power density.

Single-tone uplink: Similarly, Cat-NB1 device can utilize single-tone uplink (3.75 kHz or 15 kHz sub-carrier spacing) to further extend coverage, trading off peak data rate (limiting to 10's of kbps).

Lower-order modulation: By utilizing QPSK instead of 16-QAM, the SINR (Signal to Interference plus Noise Ratio) threshold reduces significantly thereby trading off modulation efficiency (fewer bits per symbol).

With these new coverage enhancements, the link budget of a Cat-M1 device is increased to 155.7dB, a +15dB improvement over regular LTE. For Cat-NB1, it is further increased to 164dB.

To provide ubiquitous network coverage for IoT services, 3GPP introduces a coverage enhancement feature in Rel.13:

- eMTC provides 15dB additional link budget, enabling about seven times better area coverage.
- NB-IoT provides 20dB additional link budget, enabling about ten times better area coverage.

An important feature of NB-IoT and LTE-M is that they share the same numerology as LTE. This allows spectrum to be shared between the two systems without causing mutual interference.

5.10 Core network optimizations

IoT is bringing a huge amount of connected devices that will push the capability boundary of existing LTE networks. Most IoT devices transmit small amount of data sporadically, rather than in large data packets; therefore, the LTE core network also needs to evolve to better support IoT traffic profiles by providing more efficient signaling and resource management. Some of the core network optimization techniques are described below:

More efficient signaling: New access control mechanisms such as Extended Access Barring (EAB) prevents devices from generating access requests when the network is congested, thus eliminating unnecessary signaling. The network can also utilize group-based paging and messaging to more efficiently communicate with multiple downlink devices.

Enhanced resource management: The network can allow a large set of devices to share the same subscription, such that resources and device management can be consolidated. For example, a group of water meters in a smart city can be collectively provisioned, controlled, and billed.

Simplified core network (EPC-lite): The LTE core network can be optimized for IoT traffic, allowing more efficient use of resources and consolidation of the MME, S-GW, and P-GW into a single EPC-lite. With this, the operators have the option to optimize for lower OPEX, or to minimize CAPEX spend by leveraging existing LTE core network to support LTE IoT.

5.11 Low device cost

LTE was designed in 3GPP Rel.8 to provide affordable mobile broadband and has been developed by subsequent 3GPP releases. Yet the focus has always been on optimizing performance, a factor that has created increasing complexity. Rel.12 looks at how to reduce the complexity of LTE with lower performance Key Performance Indicators (KPIs) while still complying with the LTE system. This reduced complexity helps cut costs significantly.

Further cost reductions are needed to make LTE a competitive M2M solution and these have been addressed in Rel.13 and beyond.

Table 3 below summarizes the complexity/cost reductions as we move from Rel.8 Cat-4 devices towards potential Rel.13 low cost LTE-M devices.

Table 3 : Complexity / cost reductions for LTE-M and NB-IoT evolution, [8]

	Release 8	Release 8	Release 13	Release 13
Modem/device chip category	Category 4	Category 1	Category M1 (eMTC)	Category NB1 (NB-IoT)
Downlink peak rate	150Mbps	10Mbps	1Mbps	170kbps
Uplink peak rate	50Mbps	5Mbps	1Mbps	250kbps
Number of antennas	2	2	1	1
Duplex mode	Full duplex	Full duplex	Full/Half duplex	Half duplex
UE receive bandwidth	1.08-18MHz	1.08-18MHz	1.08MHz	180kHz
UE transmit power	23dBm	23dBm	20/23dBm	20/23dBm
Multiplexed within LTE	Yes	Yes	Yes	Yes/No
Modem complexity	**100%**	**80%**	**20%**	**15%**

5.12 LTE-M Rel.12 UE optimizations

Rel.12 introduces a new low complexity device category (Cat-0). This low cost category defines a set of reduced requirements, enabling less complex, lower cost devices. The key reductions agreed in Rel.12 are:

- Half duplex FDD operation allowed. This makes it possible to operate LTE FDD time multiplexed, avoiding the duplex filter
- Single receive chain. This removes the dual receiver chain for MIMO
- Lower data rates. With a lower data rate requirement, the complexity and cost for both processing power and memory will be reduced significantly.

5.13 Low deployment cost

Enabling low cost deployment of IoT networks is a key challenge for mobile operators providing IoT connectivity. Figure 11below shows how eMTC shares capacity with legacy LTE networks.

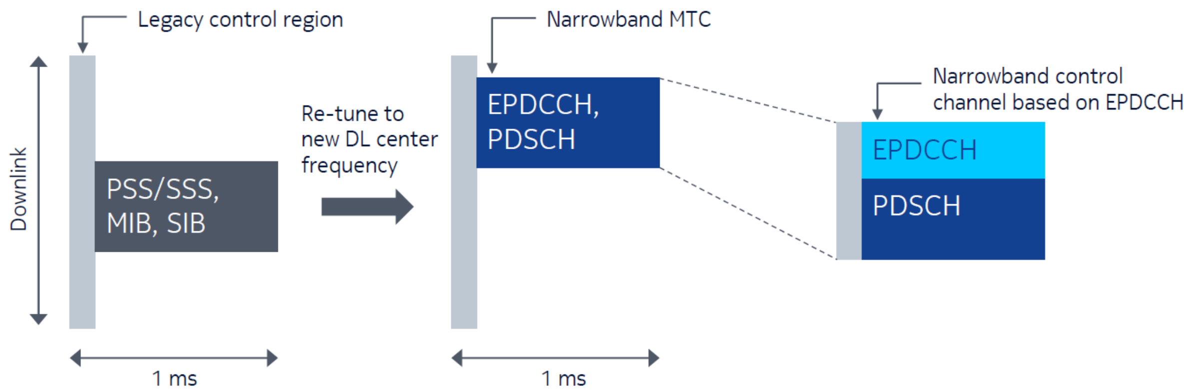


Figure 11 : eMTC sharing carrier capacity in legacy LTE configuration, [8]

eMTC operates on a 1.4MHz carrier or 6 PRB. The IoT device will always listen to the center 6 PRB for control information, just like any normal device. When the device is scheduled for IoT traffic, it will be allocated several PRBs (up to 6) at any consecutive location within the spectrum of operation. This means that the device will be allocated a 1.4MHz carrier within, for example, a 20MHz carrier. The dedicated control and data is multiplexed in the frequency domain ignoring the legacy control information. This enables LTE IoT devices to be scheduled within any legacy LTE system and share the carrier capacity, antenna, radio and hardware at the site.

Reusing LTE for narrowband IoT systems (eMTC and NB-IoT) takes advantage of existing technology as well as the installed system base. It is possible to reuse the same hardware and share spectrum by making LTE-M and NB-IoT compatible with LTE, without running into coexistence.

By 2020, the average mobile subscriber will use several GB of mobile broadband data per day. By contrast, a connected ‘thing’ may use hundreds of kB per day on average. The IoT traffic will in this example only consume about 0.01 percent of the mobile broadband data. Furthermore, most of the IoT traffic will not follow the same peak data consumption as mobile broadband and most IoT traffic can be scheduled overnight.

Therefore, deploying LTE-M and NB-IoT is as simple as a software upgrade to enable a full IoT network with significantly better coverage than the legacy LTE network.

5.14 Summary of 3GPP Solutions

As discussed in the previous sections, there are several optimizations possible to the 3GPP IoT technologies.

The Table 4 provides a view of the optimizations against a variety of applications.

Table 4 : 3GPP Optimizations and Applications

Applications	**Description**	**Battery Life** **<2yrs/ Mid/ >10 (Long)**	**Coverage** **Normal/Extended/Extreme**	**Latency** **Low (LTE like: few ms)/ Mid (ms to sec)/ High (sec to hrs)**	**Mobility** **Mobile/Nomadic/Stationary**	**Data rate**
Utility meters	Smart meters, they require un-frequent exchange of small data.	Long	Deep indoor coverage (Extreme coverage)	High	Stationary	Low ~ 100bps to some kpbs
Payment transactions (POS terminals at retail establishments and kiosks)	Case 1. Entry Level Vending – Case 2.High level vending management, dynamic control.	Wall powered.	Outdoor/indoor, deep coverage	Mid to high	Stationary	Low - some kbps for Case 1. Potentially higher for case 2
Tracking of people, pets, vehicles and assets	In general communication can be periodic or event triggered.	Long	Outdoors / indoors (extreme coverage)	Low/Mid	Mobile/Nomadic	Low ~ up to 100kbps
Wearable	Smart watch which can be used as a normal phone (calls/data	Same as smart phone	Normal coverage	Low	As LTE	High

	download and upload even when the phone is left home).					
Home alarm panels with and without voice	Device sends the information about alarm state to a security company.	High/Mid	Normal to extended	Mid	Stationary	Low/high depending on voice/video
Automotive	Communication with Road Side Unit (V2I) or communicationV2N or V2V	On car battery	Normal to extended coverage	Mid to low or very low	Mobility	From low to high
Industrial control	Communication between machine in a factory	Wall powered	Normal	Low to extremely low	Stationary	Might be large

In addition to this, specific comparison of KPI values of 3GPP technologies for the optimizations is depicted in Table 5.

Table 5 : 3GPP Optimizations and KPI values

3GPP Rel / Criteria	Cat. 1 (Rel. 8+)	Cat. M1 (Rel. 13)	Cat. NB1 (Rel. 13)	FeMTC (Rel. 14)	eNB-IOT (Rel. 14)
Bandwidth	20 MHz	1.4 MHz	180 kHz	Up to 5 MHz (CE Mode A and B for PDSCH and A only for PUSCH)	180 kHz
Deployments/ HD-FDD	LTE channel / No HD-FDD	Standalone, in LTE channel/ HD-FDD preferred	Standalone, in LTE channel, LTE guard bands, HD-FDD	Standalone, in LTE channel / HD-FDD, FD-FDD, TDD	Standalone, in LTE channel, LTE guard bands, HD-FDD preferred
Max. Output Power	23dBm	23dBm/ 20dBm	23dBm/ 20dBm	23dBm/ 20dBm	23dBm/ 20dBm/ 14dBm
Rx antennas/ layers	2/1	1/1	1/1	1/1	1/1
Coverage, MCL	145.4dB DL,140.7dB UL (20 Kbps, FDD)	155.7dB	Deep coverage: 164dB +3	155.7dB (at 23dBm)	Deep coverage: 164dB
Data rates (peak)	DL: 10 Mbps, UL: 5 Mbps	~800kbps (FD-FDD) 300kbps / 375kbps DL/UL (HD-FDD)	30kbps (HD-FDD)	DL/UL: 4 Mbps FD-FDD@5MHz	TBS in 80kbps/ 105kbps/ 1352kbps/ 1800kbps peak rates
Latency	Legacy LTE: < 1s	~ 5s at 155dB	<10s at 164dB	At least the same as Cat. M1 Legacy LTE (normal MCL)	At least the same as Cat. NB1, some improvements are FFS
Mobility	Legacy support	Legacy support	Cell selection, re-selection only	Legacy support	More mobility compared to Cat. NB1
Positioning	Legacy support	Partial support	Partial support	OTDA with legacy PRS and Frequency hopping	50m H target, new PRS introduced. Details FSS. UTDOA under study
Voice	Yes (possible)	No	No	Yes	No

Optimizations	n/a	MPDCCH structure, Frequency hopping, repetitions	NPDCCH, NPSS/NSSS, NPDSCH, NPUSCH, NPRACH, frequency hopping, repetitions, MCO	Higher bandwidth will be DCI or RRC configured, Multi-cast e.g. SC-PTM	Multi-cast e.g. SC-PTM
Power saving	DRX	eDRX, PSM	eDRX, PSM	eDRX, PSM	eDRX, PSM

5.15 Benefits of 3GPP IoT solutions

As the number of IoT applications continues to grow, it is expected that many new IoT-enabling connectivity technologies will emerge. Each of the technologies available for IoT connectivity has its own advantages and disadvantages. However, the range of IoT connectivity requirements – both technical and commercial – means cellular technologies can provide clear benefits across a wide variety of applications, as summarized below:

Figure 12 : Advantages of Cellular IoT, [3]

While some of these new technologies can potentially address the wide-area coverage requirement, they are likely to fall short in other aspects compared to 3GPP standardized technologies such as eMTC and NB-IoT.

Ubiquitous coverage: LTE IoT leverages existing LTE networks without requiring a core network overlay. To date, there are already more than 500 LTE networks deployed in over 160 countries, with many more future deployments in planning.

Scalability: LTE IoT is a part of a unified platform that can adapt to application's performance needs. LTE can easily scale up to support IoT use cases that require high bandwidth and low latency, and scale down to optimize for low-performance applications – all using the same network infrastructure.

Coexistence: LTE IoT is compatible with existing and planned LTE networks and spectrum, coexisting with regular LTE traffic without interfering with other devices or services.

Mature ecosystem: LTE IoT is backed by global 3GPP standards with a rich roadmap to 5G. Devices and networks are designed to interoperate across different vendors and regions.

Diversity: Cellular connectivity offers the diversity to serve a wide range of applications with varying requirements within one secure network. LTE IoT networks have the capability to address everything from Massive to Critical IoT use cases.

Managed quality of service (QoS): One of the most important benefits of LTE is its ability to utilize licensed spectrum, as it allows network operators to guarantee QoS by effectively allocating network resources as well as managing and mitigating interferences and congestions. A redundant network design also helps to ensure service availability with minimal downtime. QoS, along with licensed spectrum, provides a foundation for long-term Service Level Agreements with a specific grade of service.

End-to-end security: LTE IoT will inherit the established/trusted security and authentication features delivered by LTE, meeting the most stringent requirements of many high-security applications. The SIM will also be essential in future IoT applications, with SIM functionality embedded in the chipset (eUICC) or handled as a soft-SIM solution running in a trusted runtime environment of the module. More details about embedded SIM are available in the TEC Technical Report on “V2V / V2I Radio communication and Embedded SIM” [9]. GSMA is currently considering a system-on-chip solution called integrated UICC (iUICC), in which the UICC is integrated as a separate secure processor core alongside other cores.

Most importantly, the cellular mobile industry represents a huge and mature ecosystem, incorporating chipset, device and network equipment vendors, operators, application providers and many others. The global cellular ecosystem is governed by the 3GPP standardization forum, which guarantees broad industry support for future development

5.16 Global Roadmap of Next Generation Cellular Technologies for M2M

5G will be a unified, more capable connectivity platform that will connect new industries, enable new services, and empower new user experiences. And the Internet of Things will be an integral part of 5G, delivering new classes of IoT services and efficiencies not possible with 4G LTE. The vision of 5G is now well defined, slated for commercialization by 2020, and it will further enhance mobile broadband, more efficiently support massive IoT, and enable new mission-critical services. The new 5G platform will be defined in release 15 of the 3GPP standard and beyond, but many of the foundational technologies are already introduced as part of LTE Advanced Pro. NB-IoT will continue to evolve beyond 3GPP Release 13, taking another step closer to Narrowband 5G to enable massive IoT. Some of the proposed enhancements for Release 14 will include, but not limited to, voice/mobility, location services, and broadcast support for more efficient over-the-air (OTA) firmware updates.

6 Non-Cellular Wireless Technologies

Most of the devices in M2M/ IoT domain will be unmanned/ scattered and operate on battery. To have a long battery life, devices should consume less power. As a thumb rule, the network should be designed in such a way that if the device is not transmitting data, it should be in sleep mode.

Some countries have de-licensed spectrum in various slots in Sub-GHz band which can enable the M2M / IoT services. Table 6 gives an overview of the spectrum band country wise

Table 6 : Snapshot of de-licensed spectrum in Sub-GHz in various countries

Country / Region	Frequency Band
North America, Mexico and South America	433.075-434.775 MHz and 902-928 MHz
Africa and Middle-Eastern countries	433.05-434.79 MHz and 863-870 MHz
Europe	433.05-434.79 MHz, 863-870 MHz, 870 – 876 MHz, 915-921MHz
Japan	426-430 MHz and 920-928 MHz
Australia/New Zealand	915-928 MHz
India	433-434 MHz and 865-867 MHz
China	470-510 MHz and 920.5 – 924.5 MHz
Singapore	866 – 869 MHz and 920 – 925 MHz
Hong Kong/Thailand/Vietnam	920 – 925 MHz
Brazil	902-907.5 and 915-928
Philippines	915 – 918 MHz
Malaysia	919 – 923 MHz

Globally, various countries have allocated un-licensed frequency bands in excess of 7 MHz. North America and South America have allocated the most (26 MHz) in the Sub-GHz band. Australia has allocated 13 MHz band in the Sub-GHz band. Europe, Africa and most middle-eastern countries have access to 7 MHz of un-licensed spectrum. Japan has de-licensed 8 MHz for M2M/IoT/IoE/Smart Cities initiatives.

Most of the countries today have an un-licensed band also in 902-928 MHz frequency range. Recently few of the countries who had different un-licensed frequency band have also delicensed a band in 902-928MHz. This is to get the benefit of the eco system which is already available for other countries.

A previous report released in TEC (Release 2 of 'M2M Enablement in Power Sector') mentioned the specifications of the de-licensed bands in India. A snapshot of this is depicted in Table 7, [10].

Table 7 : Snapshot of specifications of the De-Licensed bands in India

Frequency Band	Power Requirements	Antenna	Use of this frequency band
433-434 MHz	Maximum Effective Radiated Power: 10mW Maximum Channel Bandwidth: 10KHz	In-built.	Indoor applications.
865-867 MHz	Maximum Transmitted power: 1W Maximum Effective Radiated Power: 4W Maximum Channel Bandwidth: 200KHz	Nothing specified.	Any low power device or equipment.
2.4-2.4835 MHz	Maximum Transmitted Power: 1W (in a spread of 10 MHz or higher) Maximum effective radiated power: 4W Maximum antenna height: 5 metres above the roof-top of an existing authorised building	Nothing specified.	Any low power device or equipment.
5.150-5.350 GHz and 5.725-5.875 GHz	Maximum Mean Effective Isotropic Radiated Power: 200mW Maximum Mean Effective Isotropic Radiated Power Density: 10mW/MHz in any 1MHz band	In-built or indoor.	Indoor applications which include single contiguous campus of an individual, duly recognised organisation or institution.
5.825-5.875 GHz	Maximum Transmitted Power: 1W in a spread of 10 MHz	Nothing specified.	Any low power device or equipment installed at outdoor locations.

	Maximum Effective Isotropic Radiated Power: 4W		

As only 2MHz (865-867 MHz) spectrum is available in India, there may be a need of spectrum when billions of devices are deployed in future in M2M/ IoT domain especially in view of Smart cities. Detailed study was done by M2M working group in TEC resulting in Technical report on “Spectrum requirement for PLC and Low power RF communication” [10]. One key recommendation in this report is to allocate a band close to existing 865-867 MHz band. This will be extremely useful for utilizing the full potential in this band and also help in international harmonization.

6.1 Technologies in Sub-GHz bands

6.1.1 Characteristics of Sub-GHz

Sub-GHz communication enables the IoT devices to communicate with each other for low-data-rate applications, such as home security/automation and smart metering etc. It has several advantages including longer range, reduced power consumption and lower deployment and operating costs.

Sub-GHz wireless networks can provide an extremely cost-effective solution in any low-data-rate system, from simple point-to-point connections to much larger mesh networks, where long range, robust radio links and extended battery life are leading priorities. In many of the deployment environments and scenarios for IoT devices, the frequencies below 1 GHz provide superior propagation characteristics compared to higher frequencies. For example, using simple modulation, signals at 865MHz will tend to penetrate foliage (trees, shrubs, other plants) more readily than 2.4GHz, which is attenuated more by the water contained in plants and animals. Propagation through some building materials too may be improved at lower frequencies. The effective antenna aperture will be improved at lower frequencies as well.

Devices having communication technology in Sub-GHz band can operate for a much longer period (around 10 years) as compared to the technologies in 2.4 GHz band. The Sub-GHz radio devices can transmit signals over a kilometer due to its narrowband operation. Devices operating in 2.4 GHz band use hop to hop communication because of their short ranges. The primary reasons for the same is that 2.4 GHz spectrum signal weakens more as it passes through walls and other obstacles as compared to sub-GHz signals.

Even though radio waves travel in a straight line, they do bend when they hit a solid edge (like the corner of a building). As frequencies decrease the angle of diffraction increases, allowing sub-GHz signals to bend further around an obstacle, reducing the blocking effect.

The Friis Equation demonstrates the superior propagation characteristics of a sub-GHz radio, showing that path loss at 2.4GHz is 8.5dB higher than that at 900MHz.

$$Path\ Loss = 20\log_{10}\left[\frac{4*\pi*d}{\lambda}\right]$$ dB, where d = distance, λ = wavelength

Equation 1 : Friis Transmission Formula

This results in 2.67 times longer range for a 900 MHz radio since for every 6dB increase in power the range doubles. 2.4 GHz spectrum needs an additional power of 8.5dB to match the range of 900MHz radio.

2.4 GHz spectrum creates lots of interference due to the fact that WiFi, Bluetooth, and microwave oven work in the same band.

6.1.2 Applications in Smart Grid

Sub-GHz communication offers distinct advantages in a number of smart grid applications. For instance, its longer range allows more homes and businesses to communicate with fewer hubs, which saves deployment and maintenance costs for the utilities provider. In addition, battery-powered gas and water meters can operate for years without changing batteries. There are major standardization efforts underway for smart energy applications around the world (802.15.4G, Wireless MBUS, etc.) with sub-GHz being the dominant frequency band for long range communications links from the meter to the utility.

Automated metering system— automated electronic meters offer utilities providers the benefits of improved reliability and accuracy, ease of calibration, improved security and advanced billing features. The full system can take advantage of long-range, low-cost wireless communication for the effective data exchange the smart grid requires.

Sub GHz plays a significant role in enabling two way communication between homes and business offering significant applications like battery powered gas and water meters that can work for years without changing batteries. Using the automated metering system in the smart grid can improve the accuracy and reliability of the meters in the grid. Also the devices offer ease of calibration, improved security and advanced billing features in the grid.

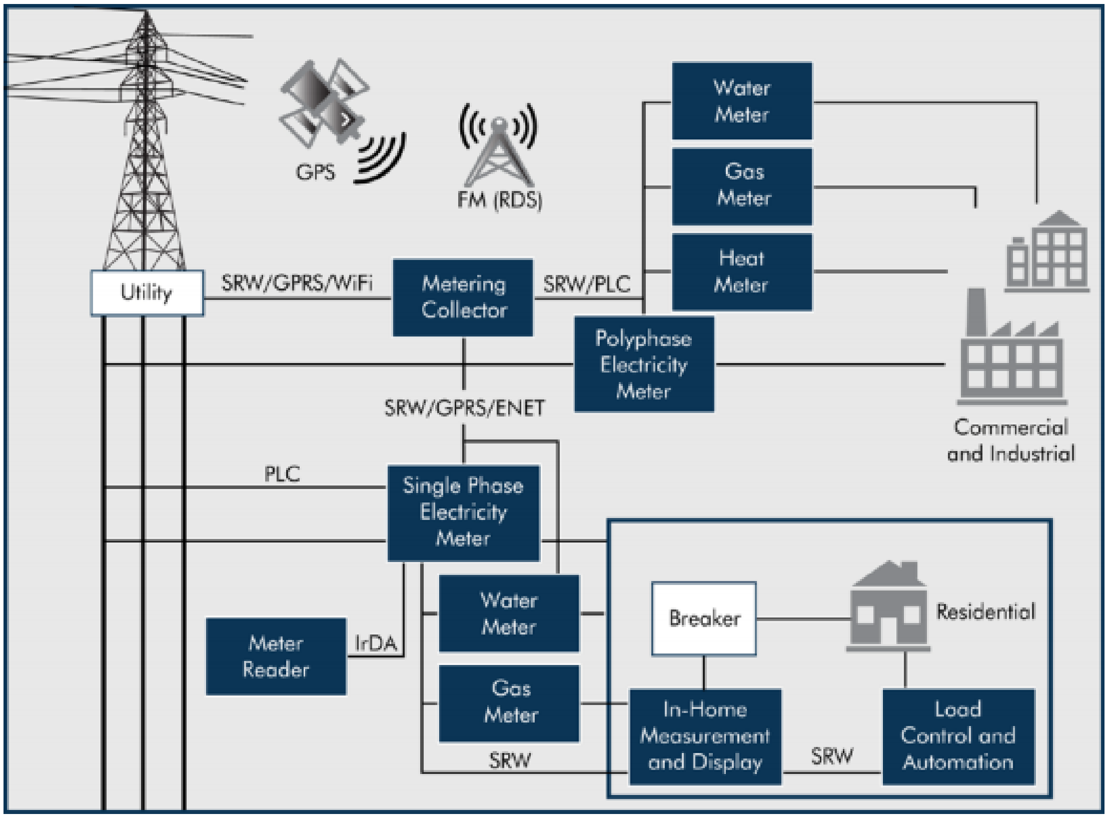


Figure 13 : Automated Metering System for a Smart Grid Application

As shown in Figure 13, there are four different kinds of automated metering systems in this smart grid application

- The electricity meter supports multi-rate metering by measuring the kilowatt hours consumed and the power factor of the load and by recording the time the electricity was used.
- The gas and water meters use positive displacement flow meters that measure the number of times a unit volume of fluid or gas moves through the meter. Low operating power is critical as these meters are usually battery powered.
- Heat meters enable utilities to bill customers by the kilowatts used, which are calculated by measuring the flow of hot water through the system and recording its input and exit temperatures. These meters are primarily used by industrial customers.

All of these metering systems employs a sub GHz radio which offers quick and inexpensive data transmission (hub) to the gateway of the utility. In return the utility can communicate back to the individual nodes through the same sub GHz network.

6.1.3 Low power consumption

In today's scenario the MCU's (Microcontrollers) have built in capabilities like sleep mode, deep sleep mode of operation where in the MCU's can be operated in different power consumption modes which saves is battery life of the system designed. The MCU is designed in such a way that only if there is data the host MCU wakes up the system. The decision is typically made based on preamble detection or receive signal strength indicator. If the system finds no data to then MCU goes to deep sleep mode until further interruption.

The factors that determine the current consumption of a duty cycling application. They are

- The energy required to transition from sleep to receive mode, the time required to evaluate the channel for a valid packet, and the sleep mode current.
- The power amplifier (PA) consumes the highest current in these sub-GHz transceivers, so an efficient PA design is also critical to achieve long battery life. Power amplifies enhances the range but is not required to be used in all scenarios.

6.1.4 Wireless range

The sub GHz is likely to be the adopted frequency band for long range wireless communication due to the factors like fewer base stations requirement in providing the solutions to the applications even in obstructed conditions. In deciding the wireless communication system, factors such as frequency, transmit power, antenna design, bandwidth, BER, should be taken to consideration. The narrower the bandwidth, the higher will be the sensitivity since channel bandwidth is inversely proportional to sensitivity.

Recovery of the desired data from the spread signal typically requires a longer preamble for synchronization, which increases the transmission time of the packet and further reduces battery life. Narrowband systems provide excellent adjacent channel rejection in the range of 60 dB to 70 dB depending on the frequency band. Spread spectrum signals are less susceptible to interference. However, several narrowband signals in or around the same frequency as the wideband spread spectrum signal will reduce the range of the coded system significantly.

One benefit of spreading systems is the ability to use a lower-cost crystal instead of a higher-priced temperature-compensated crystal oscillator (TCXO). GFSK-based narrowband systems typically require a TCXO to ensure frequency accuracy and extend range.

6.1.5 IEEE Standards for Sub GHz

6.1.5.1 802.15.4u

IEEE 802.15.4u is a PHY amendment, published in March 2017 has been built on the success of the 802.15.4 standard for application to IoT Networks including field (also known as neighborhood) and home area networking. IEEE 802.15.4u provides data rates from 6.25 kbps to 300 kbps. This amendment complements the short-range PHYs of IEEE 802.15.4-2015 with the capability to support large, geographically diverse networks with minimal infrastructure and with a large number of participating devices.

The amendment includes three different PHY options:

- FSK PHY based on legacy systems (also used in part by Wi-SUN Alliance)
- Extension of the legacy 802.15.4 DSSS PHY
- OFDM

Implementations conforming to 802.15.4u standard are available from a large number of vendors, and have proven to be an effective basis for constructing large scale outdoor wireless mesh networks. The proven technology standard enables interoperable products and addresses global market and has been adopted in many regions and markets.

6.1.5.2 802.11ah

IEEE 802.11ah is a MAC/PHY amendment of the 802.11 standard and intended to support low energy for IoT applications. It has a range of up to 1 Km (outdoor).

This amendment defines an Orthogonal Frequency Division Multiplexing (OFDM) Physical layer (PHY) operating in the license-exempt bands below 1 GHz, excluding the TV white spaces. 802.11ah is having channel width as 1/2/4/8/16 MHz.

The data rates defined in this amendment optimize the rate vs range performance of the specific channelization in each of the bands as shown in Figure 14.

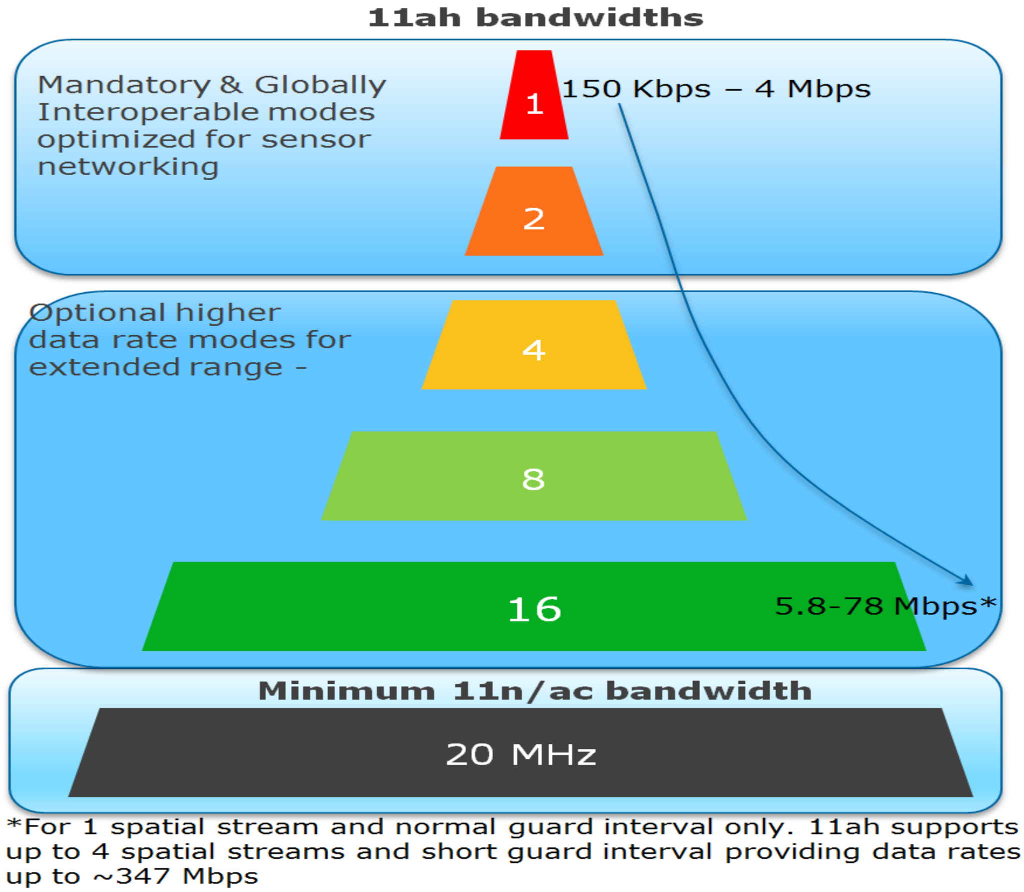


Figure 14 : 802.11ah Bandwidth Modes [11]

6.1.5.3 TV White Space

Although TVWS standards have been available for several years, there has not been widespread commercialization and deployment. The reduction of available channels will significantly curtail availability of vacant TV channels in metropolitan areas. Another aspect is the lack of maturity of database services that these IEEE 802 TVWS standards depend on for operation.

6.1.5.3.1 802.15.4m (TVWS)

802.15.4m amendment specifies a physical layer definitions and MAC layer extensions for 802.15.4 enabling operation according to TV white space regulatory requirements in various regulatory domains. The standard enables operation in the VHF/UHF TV broadcast bands between 54 MHz and 862 MHz, supporting typical data rates in the 40 Kbits per second to 2000 Kbits per second range, to realize optimal and power efficient device command and control applications.

6.1.5.3.2 802.11af (TVHT)

The 802.11af amendment defines enhancements to the 802.11 WLAN physical layer (PHY) and medium access control (MAC) specifications to support operation in the TV white space (TVWS) spectrum in the VHF and UHF bands between 54 and 790 MHz. 802.11af introduces a new Television Very High Throughput (TVHT) PHY to accommodate the narrow TV channels that are available in the TVWS spectrum. The TVHT PHY is based on the Very High Throughput (VHT) PHY defined in the IEEE 802.11ac-2013 amendment, but it is modified to support basic channel units (BCU) of 6, 7, or 8 MHz. 802.11af also supports aggregation of these BCUs.

6.1.5.3.3 IEEE 802.22 (Wi-FAR™)

The IEEE 802.22 (Wi-FAR™) Standard on Cognitive Radio based Wireless Regional Area Networks (WRAN) takes advantage of the favorable transmission characteristics of the VHF and UHF TV bands to provide broadband wireless access over a large area with a range of 10 - 30 km from the transmitter. Hence each IEEE 802.22 Base Station can potentially provide a typical coverage over 300 sq km and in some cases, up to 900 sq. km.

IEEE 802.22-based wireless regional area networks take advantage of the favorable propagation characteristics in the VHF and low UHF TV bands, to provide broadband wireless access under both line-of-sight (LoS) and non-line-of-sight (NLoS) conditions. This occurs while operating on a strict non-interference basis in “TV white space” (TVWS)—spectrum that is assigned to, but unused by, incumbent licensed services. As a result, some industry trade associations, such as the White Space Alliance, have started referring to IEEE 802.22 standard as “Wi-FAR™.” Each IEEE 802.22 network proposes to deliver up to 22 Mbps per 6 MHz channel and 28 Mbps per 8 MHz Channel. This technology is especially useful for serving rural areas, and developing countries where most vacant TV channels can be found.

Use cases for IEEE 802.22-based devices include broadband access over large distances and NLoS conditions, broadband Internet access for remote and rural areas, Internet of Things (IoT) applications, cellular offload, monitoring of the rain forests, long-range backhaul, smart grid, critical infrastructure monitoring, defense, Internal security, healthcare, small office/home office (SoHo) and campus-wide broadband wireless access. IEEE 802.22 incorporates advanced cognitive radio capabilities including dynamic spectrum access, incumbent database access, accurate geolocation techniques, spectrum sensing, regulatory domain dependent policies, spectrum etiquette, and coexistence for optimal use of the available spectrum. In addition, IEEE 802.22 systems have been incorporated with enhanced security features for both, traditional and cognitive functions.

IEEE 802.22b is an amendment to IEEE 802.22™-2011. IEEE 802.22b-2015 is designed to double the throughput of devices based on the original IEEE 802.22 standard. The new amendment is intended also to serve more users per base station and enable relay capability for machine-to-machine (M2M) and Internet of Things (IoT) use cases.

6.2 Wi-SUN (Wi-SUN Alliance)

Wi-SUN Alliance provides wireless mesh solutions for Field Area Networks for applications such as Advanced Metering Infrastructure and Distribution Automation, and for Home Energy Management

Key features of Wi-SUN technology:

- Long range: Around 0.7 km in city areas and 2-3 km in rural areas.
- Low-power: 10+ year expected battery lifetime
- Secure: Enterprise level security using 802.1x, 802.11i, EAP-TLS

6.2.1 Wi-SUN HAN Profile

The Wi-SUN Alliance HAN covers primarily indoor or short range networks and its specification is oriented towards meeting the challenges of these environments. Examples include Home Automation, Building Automation, and other sensor networks.

The Wi-SUN Alliance HAN profile specifies an 802.15.4g/u physical layer, IEEE 802.15.4/4e as MAC Layer, including 6LoWPAN, address management, unicast and multicast forwarding, standards-based multi-layer security specification encompassing authentication, and encryption.

The Layer 2 routing is supported to extend the range using IE elements of IEEE 802.15.4e MAC Layer.

6.2.1.1 System Architecture

A typical Wi-SUN HAN Profile deployment would offer a single Home Gateway (HEMS) and multiple sensor nodes. In some cases we may also use Router node to extend the range. Wi-SUN Enhanced HAN also supports the sleeping end node to make sure that the battery operated End nodes are used effectively.

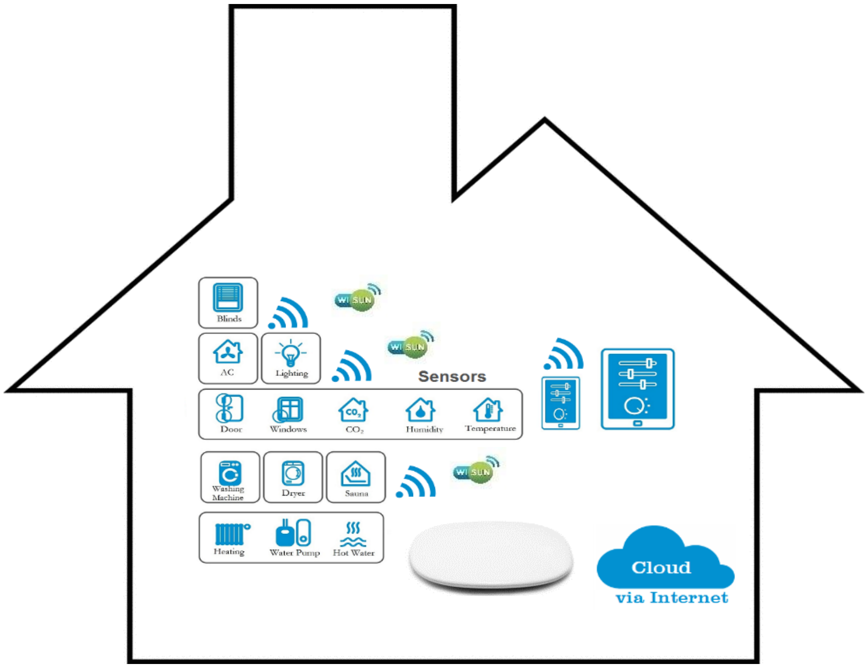


Figure 15: Wi-SUN Home Area Network

6.2.1.2 Security

Wi-SUN HAN Profile provides WPA-PSK security over PANA Framework for security credential exchange. Since application Layer is out of scope of Wi-SUN Alliance, service providers can implement any application layer security for further increasing the security level.

There are interference avoidance mechanisms built into Wi-SUN HAN and IEEE 802.15.4u. The IEEE 802.15.4u standard supports Clear Channel Assessment (CCA) with options for (a) Energy above threshold (b) Carrier Sense only (c) Carrier sense with energy above threshold and (d) ALOHA. Finally, IEEE 802.15.4u also provides for Carrier Sense/Multiple Access (CSMA) to support transmission/reception in unlicensed operation.

6.2.1.3 RF Characteristics

Sl. No.	PHY Band	Data Rate	Modulation	Tx Power	Hop Limit
1		50	2FSK	Max 1W[1]	10

2	865-867 MHz	100			
3		150			

[1] As per the local regulatory restriction.

6.2.2 Wi-SUN FAN Profile

The Wi-SUN Alliance FAN covers primarily outdoor networks and its specification is oriented towards meeting the rigorous challenges of these environments. Examples include Advanced Metering Infrastructure, Distribution Automation and Distributed Energy Resources, Street Light Monitoring and Control, Traffic Management and other Smart City and Building Applications.

The Wi-SUN Alliance FAN profile specifies an 802.15.4g/u physical layer, frequency hopping, network discovery/join and protocol dispatch, IPv6 protocol suite including 6LoWPAN, address management, routing using RPL, unicast and multicast forwarding, standards-based multi-layer enterprise grade security specification encompassing authentication, authorization, encryption.

6.2.2.1 System Architecture

A typical Wi-SUN FAN Profile deployment would offer multiple Access Points (each advertising the same Network Name if they are all participating in the same network, much like commercial Wi-Fi equipment). Each Access Point advertises a Personal Area Network (PAN) supported by the Access Point. Devices use information propagated from the Access Points to select a PAN (and Access Point) with optimal routing cost.

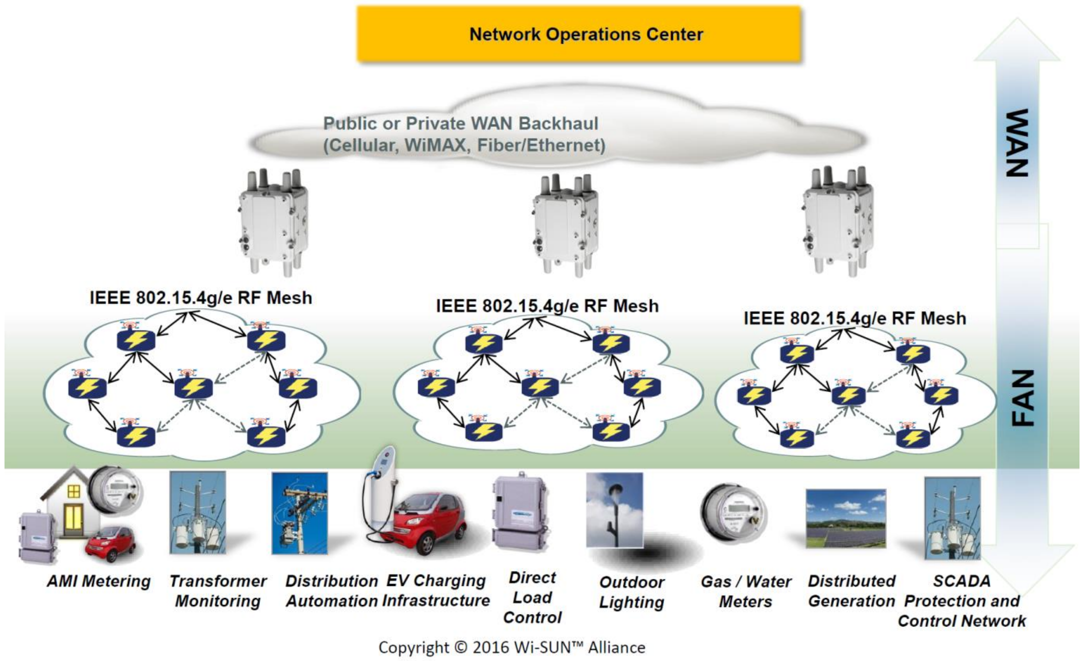


Figure 16: Wi-SUN FAN System Architecture

6.2.2.2 Security

Wi-SUN FAN Profile provides enterprise level security with 802.1x, 802.11i and EAP-TLS. There are interference avoidance mechanisms built into Wi-SUN FAN and IEEE 802.15.4u. Wi-SUN FAN Profile uses frequency hopping over all channels in the regional band. Additionally, Wi-SUN FAN offers the ability to exclude channels that are observed to regularly contain interfering signals. The IEEE 802.15.4u standard supports Clear Channel Assessment (CCA) with options for (a) Energy above threshold (b) Carrier Sense only (c) Carrier sense with energy above threshold and (d) ALOHA. Finally, IEEE 802.15.4u also provides for Carrier Sense/Multiple Access (CSMA) to support transmission/reception in unlicensed operation.

6.3 NFC

NFC stands for Near Field Communication. NFC works at 13.56 MHz and the data rate is 106 Kbit/s to 424 Kbit/s. NFC devices share the similar technology as the RFID tags and contactless Smartcards. NFC is acknowledged by ISO/IEC (International Organization for Standardization / International Electro technical Commission), ETSI (European Telecommunications Standards Institute), and ECMA (European association for standardizing information and communication systems). NFC is an offshoot of radio-frequency identification (RFID) with the exception that NFC is designed for use by devices within close proximity to each other. NFC requires 4 cm or less to initiate the connection with the tag. There are two variants of NFC. One is the Transceiver and the other is Tag.

Transceivers are active devices which need power to operate. An active NFC device, such as a smartphone, would not only be able to collect information from NFC tags, but it would also be able to exchange information with other compatible phones or devices and could even alter the information on the NFC tag if authorized to make such changes

Tags are the passive devices and work on the principle of inductive coupling when the tag is brought near a transceiver.

NFC allows to transfer small amount of data between transceiver and tags. There are three mode of data transfer in NFC

- Peer to Peer communication: Peer-to-peer mode enables two NFC-enabled devices to communicate with each other to exchange information and share files. NFC-enabled devices are used to quickly share contact information and other files with a touch. For example, users can share Bluetooth or WiFi link set-up parameters or exchange data such as virtual business cards or digital photos. Peer-to-peer mode is standardized on the ISO/IEC 18092 standard and based on NFC Forum's Logical Link Control Protocol Specification.

- Card Emulation: Card emulation mode enables NFC-enabled devices to act like smart cards, allowing users to perform transactions such as purchases, ticketing, and transit access control with just a touch. In Card Emulation mode, the NFC-enabled device communicates with an external reader much like a traditional contactless smart card. This enables contactless payments and ticketing by NFC-enabled devices without changing existing infrastructure. Adding NFC to a contactless infrastructure enables two-way communications. For the air transport industry, this could mean updating seat information while boarding, or adding frequent flyer points when making a payment.

- Reader / Writer: Reader/writer mode enables NFC-enabled devices to read information stored on inexpensive NFC tags embedded in smart posters and displays, providing a great marketing tool for companies. In reader/writer mode, the NFC-enabled device is capable of reading NFC Forum-mandated tag types, such as a tag embedded in an NFC smart poster. The reader/writer mode on the RF interface is compliant with the NFC-A, NFC-B and NFC-F schemes. Examples include reading timetables, tapping for special offers, and updating frequent flyer points.

There are different variants for NFC. Some of them are :

- ISO14443 Type A /Type B
- ISO15693
- Felicia.

6.3.1 How NFC works

NFC works using magnetic induction where a reader emits a small electric current that creates a magnetic field that bridges the physical space between the devices. The generated field is received by a similar coil in the client device where it is turned back into electrical impulses to communicate data such as identification number status information or any other information. So-called ‘passive’ NFC tags use the energy from the reader to encode their response while ‘active’ or ‘peer-to-peer’ tags have their own power source and respond to the reader using their own electromagnetic fields. The passive tag should be held close to the active one in order to produce sufficient energy for its operation.

6.3.2 NFC Eco-system

The real value of NFC however comes not from its technical workings but from the protocols that have been built around it. By setting standards and building layers of abstraction on top of core NFC functionality smartphone platform vendors can give developers a rich set of interfaces for interacting with the NFC ecosystem. NFC’s rapid and promiscuous communication has made it well-suited for public transport where the ability to quickly read ticket information has made it widespread in countries like Singapore, Japan and the UK. Point-of-sale transactions are also possible through NFC with card-based services such as MasterCard Pay Pass eventually likely to allow NFC-equipped mobiles to act as virtual ‘wallets’ holding banking loyalty program, personal preferences and other details.

6.3.3 Use-cases of NFC technologies

- Automated fare collection system
- ID Cards
- Access Management
- Road tolling
- Transport ticketing
- Event ticketing
- Mobile ticketing
- Citizen card
- Membership cards
- Parking
- Smart advertising
- Social welfare
- Waste management

6.4 RFID

A radio-frequency identification (RFID) system uses tags, or labels attached to the objects to be identified. Two-way radio transmitter-receivers called interrogators or readers send a signal to the tag and read its response. The readers generally transmit their observations to a computer system running RFID software or RFID middleware.

RFID tags can be either passive, active or battery assisted passive. An active tag has an on-board battery and periodically transmits its ID signal. A battery assisted passive (BAP) has a small battery on board and is activated when in the presence of a RFID reader. The salient characteristics of this technology are:

1. Standard: ISO/IEC 14543-3-10
2. Frequency: 120–150 kHz (LF), 13.56 MHz (HF), 433 MHz (UHF), 865-868 MHz (Europe) 902-928 MHz (North America) UHF, 2450-5800 MHz (microwave), 3.1–10 GHz (microwave)
3. Range: 10cm to 200m

6.5 LPWAN Technologies

LPWAN technologies have been designed to transmit very low amount of data (such as meter readings, sensor data from pollution devices etc.) to large distances. LoRa and SIGFOX technologies have been developed and are being deployed globally. Their range can go beyond 10 kms in open air and devices can have a battery life of up to 10 years.

LoRa and SIGFOX use unlicensed frequency bands worldwide in Sub-GHz.

3GPP in its Release 13 has come out with the specifications for LPWAN technologies on cellular network. These technologies have been described in details in section 5.

6.5.1 LoRa

6.5.1.1 Introduction

LoRa® is the physical layer or the wireless modulation utilized to create the long range communication link. LoRa® is based on chirp spread spectrum modulation, which maintains the same low power characteristics as FSK modulation but significantly increases the communication range enabling a low cost commercial deployment. Chirp spread spectrum has been used in military and space communication for decades due to the long communication distances that can be achieved and robustness to interference and Doppler.

The advantage of LoRa® is in the technology’s long range capability. LoRa® and LoRaWAN™ have a very good sensitivity of about -141dBm. LoRaWAN™ defines the communication protocol and system architecture for the network while the LoRa® physical layer enables the long-range communication link. The protocol and network architecture have the most influence in determining the battery lifetime of a node, the network capacity, the quality of service, and the security

Key features of LoRa technology:

- Long range: 2 km – 4 km in city / congested areas and 12-15 km in rural or open areas.
- Low-power: 5-10 year expected battery lifetime, depending upon the applications.
- Low-cost: Network deployment cost is very low.
- Secure: with embedded end-to-end AES-128 encryption of data
- Geolocation: enables indoor/outdoor tracking without GPS, with an accuracy of around 100 meters.

6.5.1.2 Network Architecture

Many existing deployed networks utilize a mesh network architecture. In a mesh network, the individual end-nodes forward the information of other nodes to increase the communication range and cell size of the network. While this increases the range, it reduces network capacity, and reduces battery lifetime as nodes receive and forward information from other nodes that may be irrelevant for them. Long range star architecture is more useful for preserving battery lifetime.

The LoRa® system consists of three main components: –

LoRa® End-devices

LoRa® Gateways: concentrators connecting end-devices to the LoRa® Network Server,

LoRa® Network Server: the network server that controls the whole network.

The network is laid out in a star- topology, where the end-devices are connected via single-hop LoRa® communication to one or many gateways. The gateways relay messages between end devices and Network Server, All the gateways that successfully decode the message sent by an end-device will forward the packet to the Network Server. The Network Server will hence reply to the end-device by choosing one such gateway, according to pre-defined criteria. The gateways are totally transparent to the end-devices, which are logically connected directly to the Network Server.

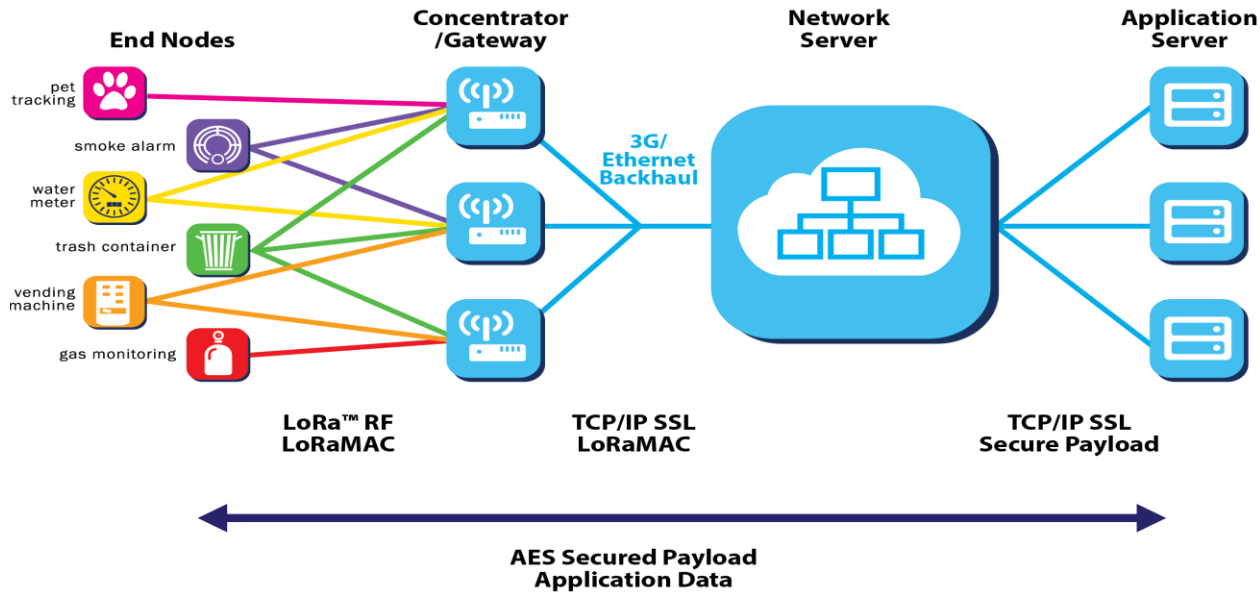


Figure 17 : LoRAWAN Protocol

In a LoRaWAN™ network nodes are not associated with a specific gateway. Data from a node is received by multiple gateways. Each gateway will forward the received packet from the end-node to the cloud-based network server via cellular/ Ethernet backhaul. The network server, which manages the network will filter redundant received packets, perform security checks, schedule acknowledgments through the optimal gateway, and perform adaptive data rate, etc. If a node is mobile or moving there is no handover between gateways.

6.5.1.3 Class of Device and Battery life

The nodes in a LoRaWAN™ network are asynchronous and communicate when they have data to be sent, based on an event or pre-scheduled, typically referred to as the Aloha.

LoRaWAN™ utilizes different device classes. The device classes trade off network downlink communication latency versus battery lifetime.

1. Bi-directional end-devices (Class A): End-devices of Class A allow for bi-directional communications whereby each end-device's uplink transmission is followed by two short downlink receive windows. The transmission slot from the end-device is based on its own communication needs with a small variation based on a random time basis (ALOHA-type of protocol). This Class A operation is the lowest power end-device system for applications that only require downlink communication from the server

shortly after the end-device has sent an uplink transmission. Downlink communications from the server at any other time will have to wait until the next scheduled uplink.

2. Bi-directional end-devices with scheduled receive slots (Class B): In addition to the Class A random receive windows, Class B devices open extra receive windows at scheduled times. In order for the end-device to open a receive window at the scheduled time, it receives a time-synchronized beacon from the gateway. This allows the server to know when the end-device is listening.
3. Bi-directional end-devices with maximal receive slots (Class C): End-devices of Class C have almost continuously open receive windows, only closed when transmitting

6.5.1.4 Capacity and Network Densification

With different spreading factor the data rate supported ranges from 0.3-50Kbps. High network capacity in a LoRaWAN™ network is achieved by adaptive data rate (ADR) and by using a multichannel transceiver in the gateway so that simultaneous messages on multiple channels can be received. LoRa® being a spread spectrum based modulation, the signals are practically orthogonal to each other when different spreading factors are utilized. Due to the spread spectrum technology, communications with different data rates do not interfere with each other and create a set of "virtual" channels increasing the capacity of the gateway. As the spreading factor changes, the effective data rate also changes. This enables GW to receive messages on same channel with different spreading factor.

If a node has a good link and is close to a gateway the data rate of device is shifted higher, the time on air is shortened providing potential space for other nodes to transmit. Adaptive data rate also optimizes the battery lifetime of a node. In order to make adaptive data rate work, symmetrical up link and down link is required with sufficient downlink capacity. These features enable a LoRaWAN™ network to have a very high capacity and make the network scalable.

6.5.1.5 Security

LoRaWAN™ utilizes two layers of security: one for the network and one for the application. The network security ensures authenticity of the node in the network while the application layer of security ensures the network operator does not have access to the end user’s application data. AES encryption is used with the key exchange utilizing an IEEE EUI64 identifier.

Key Enabler for security are

- Unique Network key (EUI64) and ensure security on network level
- Unique Application key (EUI64) ensure end to end security on application level
- Device specific key (EUI128)

6.5.1.5.1 Activation

LoRa® enabled end-devices must follow a joining procedure prior to participating in any data exchange with the network server. The LoRaWAN core network server supports two authentication and activation methods:

- Over-The-Air Activation (OTAA)
- Activation by Personalization (ABP)

In case of OTAA, devices are not initially personalized for any particular network. An end-device has to also go through a new join procedure every time it has lost the session context information. They send a JOIN request to a given LoRa® Network to receive a device address and an authorization token from which it derives session keys. A root AppKey is pre-provisioned in the device as part of manufacturing or commissioning. The Application and Network session keys are derived from this AppKey. The network server will respond to the join-request message with a join-accept message if the end-device is permitted to join a network. OTA Activation provides a high level of security.

In case of ABP, devices are personalized to work with a given LoRaWAN™ network defined by its Network ID. Devices are pre-provisioned with the Network and Application session keys and device network address.

6.5.1.5.2 Data Protection over Network

After a node joins the LoRa® network, all future messages are encrypted and signed using a combination of Network and Application session keys. Since the keys are known by the Network Server and specific Node, there should be no way for another node, or a man in the middle attack to recover the clear-text data. The message is encrypted using AES128 in Counter mode (CTR). The MAC Payload section of message is signed to prevent manipulation of the cipher-text, or of other values.

6.5.1.6 LoRa technology applications

LoRa technology is ideally suited for the applications:

- Smart street light solutions
- Smart Environment for sending environment sensor data
- Smart Metering in Utilities (Gas, water, electricity metering)
- Smart Agriculture applications such as transmission of soil parameters from the field.
- Industrial applications such as assets monitoring (monitoring of emergency services like fire, environmental hazardous conditions)

- Retail and Logistics: Assets tracking.

6.5.2 SIGFOX

6.5.2.1 Introduction

In Sigfox system, low throughput transmissions combined with advanced signal processing techniques provide high link budget and highly effective protection against interference. Because of these characteristics, Sigfox system is particularly well adapted for low throughput IoT traffic. Sigfox LPWAN autonomous battery-operated devices send only a few bytes per day, week or month in an asynchronous manner and without the needed for central coordination, which allows them to remain on a single battery for up to 10-15 years.

6.5.2.2 Terminology

The following terms below are used for describing the Sigfox solution and have been defined by ETSI/ERM/TG28/LTN group working for the standardization of Low Power Wide Area Networks:

Base Station (BS) - A Base Station is a radio hub of an LTN system

Device Application (DA) - An application running on the End Point or device

End Point (EP) - A leaf node (also known as device) of an LTN system that communicates application data between the local device application (DA) and the network application (NA)

Low Throughput Networks (LTN) - Terminology used in ETSI to define Low Power Wide Area (LPWA) networks. The Sigfox solution is aligned with LTN standards under work in ETSI/ERM/TG28/LTN.

Network Application (NA) - An application running in the network at the opposite extreme of the device

Registration Authority (RA) - The Registration Authority is a central entity that contains all allocated and authorized End Point identifiers.

Service Center (SC) - Each LTN system has a single service center. The SC performs the following functions:

* EPs and BSs management

* EP authentication

* Application data packets forwarding

* Cooperative reception support

6.5.2.3 System Architecture

The Sigfox solution architecture, Figure 18, consists of a single core network, which allows global connectivity with minimal impact on the end device and radio access network. The core network elements are the Service Center (SC) and the Registration Authority (RA). The SC is in charge of the data connectivity between the Base Station (BS) and the global Internet, as well as the control and management of the BSs and End Points. The RA is in charge of the End Point network access authorization. The radio access network is comprised of several BSs connected directly to the SC. Each BS performs L1/L2 functions, leaving some L2 and L3 functionalities to the SC. The devices or End Points (EPs) are the objects that communicate application data between local device applications (DAs) and network applications (NAs). EPs can be static or nomadic, as they associate with the SC and they do not attach to a specific BS. Hence, they can communicate with the SC through one or many BSs. Due to constraints in the complexity of the EP, it is assumed that EPs host only one or very few device applications, which communicate to one single network application (NA) at a time.

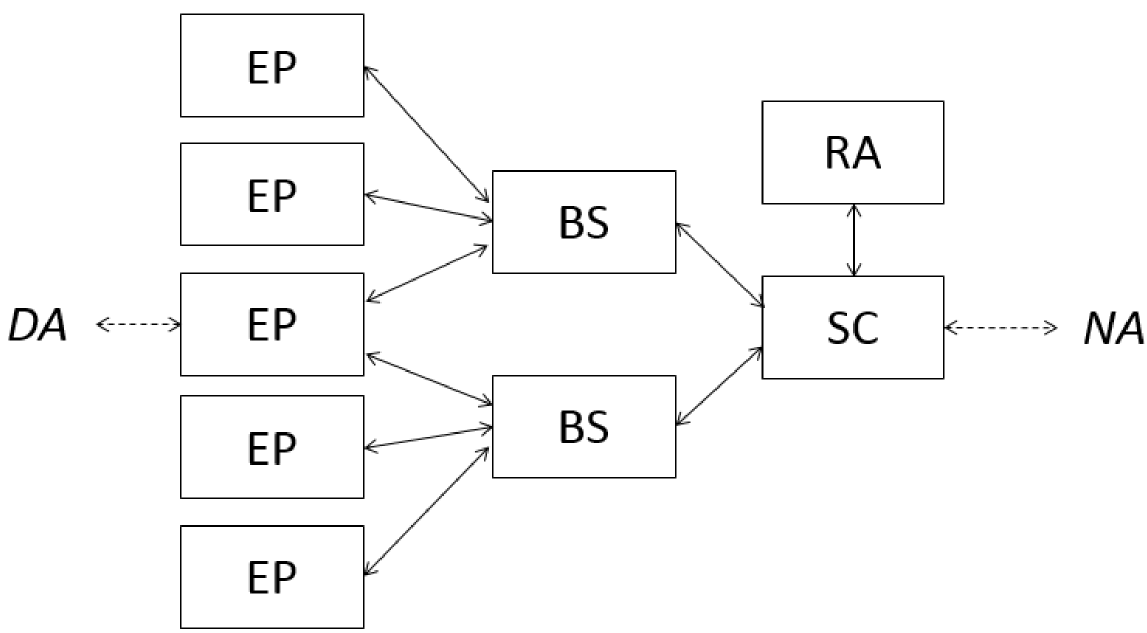


Figure 18 : Sigfox Architecture

6.5.2.4 Sigfox Coverage

At present, the SIGFOX LTN radio interface is operating in the following countries / regions:

- USA, Europe, Japan, Australia, Brazil, Canada, Kenya, Lebanon, Mauritius, Mexico, New Zealand, Oman, Peru, Singapore, South Africa, South Korea, and Thailand.

6.5.2.5 Synchronization between Uplink and Downlink

The radio interface is optimized for uplink transmissions, which are asynchronous. Downlink communications are achieved by querying the network for existing data from the device. A device willing to receive downlink messages opens a fixed window for reception after sending an uplink transmission. The delay and duration of this window have fixed values. The Sigfox network transmits the downlink message for a given device during the reception window. The Sigfox service center selects the BS for transmitting the corresponding downlink message. Uplink and downlink transmissions are unbalanced due to the regulatory constraints on the ISM bands. Under the strictest regulations, the system can allow a maximum of 140 uplink messages and 4 downlink messages per device, per day. These restrictions can be slightly relaxed depending on system conditions and the specific regulatory domain of operation.

6.5.2.6 Radio Protocol

The radio interface of the Sigfox solution is based on Ultra Narrow Band (UNB) communications, which allow an increased transmission range while spending a limited amount of energy at the device. Moreover, UNB allows a large number of devices to coexist in a given cell without significantly increasing the spectrum interference. Both uplink and downlink communications are possible in the Sigfox solution. Due to spectrum optimizations, different uplink and downlink frames and timing are implemented.

6.5.2.7 Internet interfaces

The Sigfox solution connects the network applications (NA) in a RESTfull architecture. The Internet interface uses with state-of-the-art web services and APIs. Each device or End-Point is owned by a Network Application. Endpoint provisioning and commissioning are made by the corresponding Network Application server, using control APIs of the Sigfox Service Center.

.

6.6 Bluetooth

Bluetooth devices operate in the unlicensed 2.4 GHz ISM (Industrial Scientific Medical) band. A frequency hop transceiver is applied to combat interference and fading.

Two modulation modes are defined. A mandatory mode, called Basic Rate, uses a shaped, binary FM modulation to minimize transceiver complexity. An optional mode, called Enhanced Data Rate, uses PSK modulation and has two variants: π/4-DQPSK and 8DPSK. The symbol rate for all modulation modes is 1 Msym/s. The gross air data rate is 1 Mb/s for Basic Rate, 2 Mb/s for Enhanced Data Rate using π/4-DQPSK and 3 Mb/s for Enhanced Data Rate using 8DPSK, [12].

A Time Division Duplex (TDD) scheme is used in both modes. This specification defines the requirements for a Bluetooth radio for the Basic Rate and Enhanced Data Rate modes.

The Bluetooth system operates in the 2.4 GHz ISM band. This frequency band is 2400 - 2483.5 MHz.

Table 8 : Bluetooth Operating Frequency Bands

Frequency Range	**RF Channels**
2.400-2.4835 GHz	f=2402+k MHz, k=0,…,78

The requirements stated in this section are given as power levels at the antenna connector of the Bluetooth device. If the device does not have a connector, a reference antenna with 0 dBi gain is assumed. Bluetooth devices are classified as Class1, 2 or 3 as in Table 9

Table 9 : Bluetooth Power Classes

Power Class	**Maximum Output Power**	**Minimum Output Power**
1	100 mW (20 dBm)	1 mW (0 dBm)
2	2.5 mW (4 dBm)	0.26 mW (-6 dBm)
3	1 mW (0 dBm)	N / A

Bluetooth has Basic and Enhanced Data rates.

For the Basic Data rate case, the Modulation is GFSK (Gaussian Frequency Shift Keying) with a bandwidth-bit period product BT=0.5. The Modulation index shall be between 0.28 and 0.35. A binary one shall be represented by a positive frequency deviation, and a binary zero shall be represented by a negative frequency deviation. The symbol timing shall be less than ±20 ppm.

A key characteristic of the Enhanced Data Rate mode is that the modulation mode is changed within the packet. The access code and packet header are transmitted with the Basic Rate 1 Mb/s GFSK modulation mode, whereas the subsequent synchronization sequence, payload, and trailer sequence are transmitted using the Enhanced Data Rate PSK modulation mode.

During access code and packet header transmission the Basic Rate GFSK modulation mode is used. During the transmission of the synchronization sequence, payload, and trailer sequence a PSK type of modulation with a data rate of 2 Mb/s or optionally 3 Mb/s is used.

Bluetooth Core Specifications v5.0 was released in December 2016, [12].

6.6.1 Bluetooth Low Energy

Bluetooth Low Energy (LE) devices operate in the unlicensed 2.4 GHz ISM (Industrial Scientific Medical) band. A frequency hopping transceiver is used to combat interference and fading, [12].

Two modulation schemes are defined. The mandatory modulation scheme (“1 Msym/s modulation”) uses a shaped, binary FM to minimize transceiver complexity. The symbol rate is 1 Msym/s. An optional modulation scheme (“2 Msym/s modulation”) is similar but uses a symbol rate of 2 Msym/s.

- The 1 Msym/s modulation supports two PHYs:
    - LE 1M, with uncoded data at 1 Mb/s;
    - LE Coded, with the Access Address, Coding Indicator, and the packet coded at 125 kb/s and the payload coded at either 125 kb/s or 500 kb/s.
- All devices support the LE 1M PHY. Support for the LE Coded PHY is optional.
    - The 2 Msym/s modulation supports a single PHY:
    - LE 2M, with uncoded data at 2 Mb/s

A Time Division Duplex (TDD) scheme is used in both modes. This specification defines the requirements for a Bluetooth radio for the Low Energy radio.

Requirements are defined for two reasons:

- Provide compatibility between radios used in the system
- Define the quality of the system

An LE radio shall have a transmitter or a receiver, or both.

Like IEEE 802.15.4, BLE operates in the 2.4 GHz ISM band. In order to reduce the transceivers’ costs and the amount of energy consumed, BLE prescribes binary frequency modulation with a 1 Mbit/s over-the-air data rate. Unlike the classical Bluetooth, which uses 79: 1-MHz-wide channels, BLE uses 40: 2-MHz wide channels. Three of these channels, which are located between commonly used wireless local area network channels, are used for advertising and service discovery and are called advertising channels. The remaining 37 data channels are used to transfer the data. The transmission of data between BLE devices is bound to time units known as advertising and connection events.

6.7 Wi-Fi

Wi-Fi is based on the IEEE 802.11 standards and is a trademark of the Wi-Fi Alliance. Wi-Fi operates at 2.4 GHz (12 cm) UHF and 5 GHz (6 cm) SHF ISM radio bands. A Wi-Fi signal occupies five channels in the 2.4 GHz band. Any two channel numbers that differ by five or more, such as 2 and 7, do not overlap. Channels 1, 6, and 11 are the only group of three non-overlapping channels in North America and the United Kingdom. In Europe and Japan Channels 1, 5, 9, and 13 for 802.11g and 802.11n are used. 802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 23 non-overlapping channels rather than the 2.4 GHz ISM frequency band, where adjacent channels overlap. The 802.11a, 802.11b and 802.11g standards, called "physical standards" are amendments to the 802.11 standard and offer different modes of operation, which lets them reach different data transfer speeds depending on their range.

Wi-Fi compatible devices can connect to the Internet via a WLAN network and a wireless access point. Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometers achieved by using multiple overlapping access points. Since there is no physical connections, Wi-Fi is more vulnerable to attack than wired connections.

Table 10 : Various 802.11 Standards

Standard	Frequency Bands	Speed	Range
Wi-Fi a (802.11a)	5 GHz	54 Mbit/s	10 m
Wi-Fi b (802.11b)	2.4 GHz	11 Mbit/s	100 m
Wi-Fi b (802.11b)	2.4 GHz	54 Mbit/s	100 m
Wi-Fi g (802.11g)	2.4 GHz	54 Mbit/s	150 m
Wi-Fi n (802.11n)	2.4 GHz and 5 GHz	72 Mbit/s	250 m
Wi-Fi ac (802.11 ac)	5 GHz	180 Mbit/s	115 m

It may be mentioned here that Wi-Fi is an important communication protocol pertaining to M2M communication as in several scenarios Wi-Fi hotspots are potentially the gateways for most sensor nodes. A case study with Wi-Fi as a gateway is presented in ANNEXURE 1 : Architecture and Protocols for a Gateway.

6.8 IEEE 802.11p

This technology has been developed as amendment to IEEE 802.11 standard specifications in order to support ad-hoc communication between vehicles and between vehicle and infrastructure network. There are changes made to PHY (Physical) and MAC layers for the same. IEEE 802.11p is also known by names such as WAVE (Wireless Access for Vehicular Environments) and DSRC (Dedicated Short Range Communication).

It is working in the frequency range 5.850 -5.925 GHz. FCC has allocated 75 MHz spectrum in the 5.9 GHz band and European Telecommunications Standards Institute (ETSI) has identified of 30 MHz spectrum in the 5.9 GHz band for ITS.

The main objective of 802.11p compliant devices is to improve traffic efficiency and have safety in the traffic flow (i.e. to prevent accidents). It also supports low latency, Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication.

Main uses of V2V and V2I communication services are to transmit information for:

- Road side beacons
- Traffic signals
- Toll collections
- Petrol pumps and charging centers (for electric vehicles)
- Digital signage
- Safety applications like red light violation, overloading or crossing speed limit
- eCall (911 in USA and 112 in Europe)
- Maintenance
- Navigation

This technology is being used in USA, Europe, Japan, Korea, China and Singapore etc. A TEC report on V2V / V2I Radio communication and Embedded SIM exists on this subject [9].

6.9 Wireless USB

USB having become the most successful interface in PC history, and wireless communications becoming more widespread, it was certain that the two would be married to fulfill the user's wish of de-

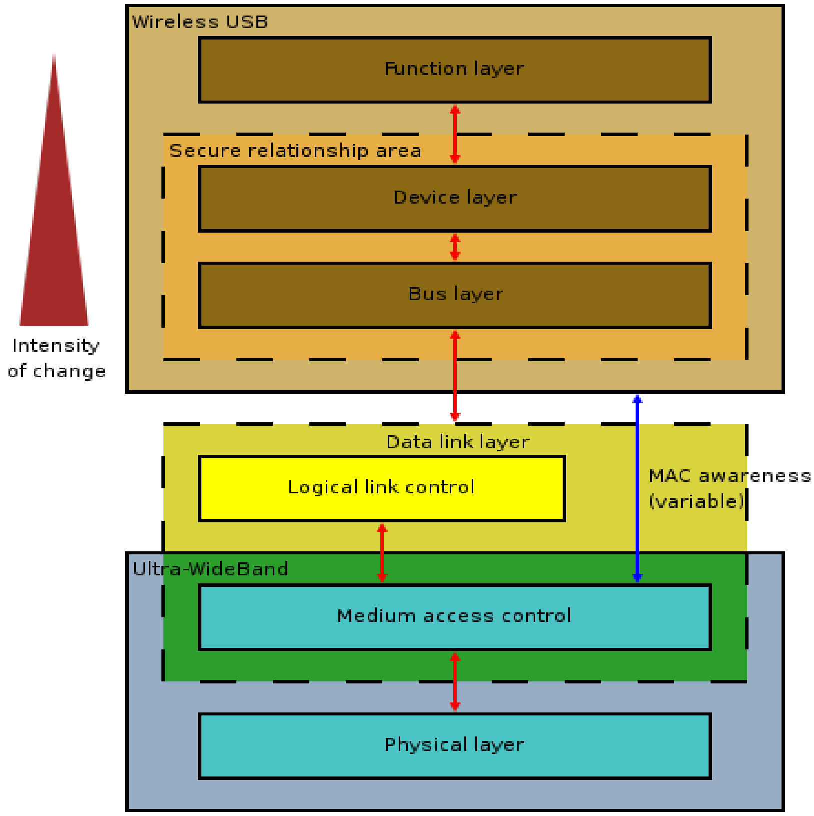


Figure 19 : Wireless USB Protocol Stack

cluttering the web of wires dangling around our PCs. The Wireless USB (WUSB) is the first high speed Personal Wireless Interconnect. It is a form of Universal Serial Bus (USB) technology that uses radio-frequency (RF) links rather than cables to provide the interfaces between a computer and peripherals, such as monitors, printers, external drives, head sets, MP3 players and digital cameras.

6.9.1 Protocol architecture

The wireless USB protocol has more or less preserved the USB model. Minor adjustments have been made to fit the specific needs of a wireless system. The changes are as given below (from top to bottom).

- The function layer has been modified to increase efficiency and support isochronism.

- The device layer includes wireless-oriented security and device management features.
- The bus layer does not change its functionality, but is substantially adapted for efficiency and security on wireless networks. Every W-USB transmission is encrypted by the bus layer without impairing layer-to-layer horizontal communication.

6.9.2 Functioning

To maintain the same usage and architecture as wired USB, the Wireless USB specification has been defined as a high-speed host-to-device connection. The bus follows a TDMA-based polling approach supervised by the host. A transfer is formed by three parts: token, data and handshake. For efficiency reasons, several tokens containing timing information for the devices can be grouped into one, thus forming transaction groups. Flow control and packet sizes are adjusted for power efficiency, while respecting the high-level pipe model of communication between source and destination.

6.9.3 Radio Requirements

The radio connectivity for W-USB is as easy as the wired USB and has been achieved by shifting the complexity upon the host which mitigates the unreliability of wireless medium by maintaining counters and statistics for each device. It can also access and modify the transmit power control functions of each device, as well as change transmission parameters such as data payload size and bandwidth adjustments. Packet loss and corruption are dealt through timeouts as well as hardware buffering, guaranteed retries and other flow control methods.

6.9.4 Power Management

Low power consumption was also one of the major requirements placed upon the chip designers for the radio interface with the target of less than 300 mW and reducing to 100 mW. Use of TDMA aids both host and devices to know exactly when their presence is not required and that they can enter power saving modes. Devices turn off their radios transparently to the host while maintaining their connections and trigger the wakeup procedure to check for pending work. In turn, the host notifies the devices before turning off its radio to either stop the channel temporarily or to enter hibernation or shutdown states.

6.9.5 Security

- **Device Association.** Establishment of secure relationships is necessary for the security of communications. W-USB manages security explicitly by restricting membership to the group, which serves as the base of trust similar to the wired systems and translates into the wireless domain through the concept of ownership: the user grants trust to the devices, which in turn proves this trust to others in order to form the desired associations. The USB address identifier is a token of the owner's trust. After receiving the group key of a cluster, a device must keep the connection alive by at least confirming its presence within each trust timeout boundary, which is usually set to four seconds else re-authentication is demanded.

- **Encryption of Transmission.** Following the natural asymmetry of USB, the host initiates all processes (except signaling). The standard, symmetric encryption method is AES-128 with CCM, though Public key encryption may be used for initial authentication (namely, only the sending of the initial CCM key), provided that the achieved security level is comparable (in practice by using 3072-bit RSA and SHA-256 for hashing).

6.9.6 Performance.

The WUSB architecture allows up to 127 devices to connect directly to a host. Even though the physical layer is based on Ultra-Wide Band, W-USB devices have a fully compliant USB interface. Wireless USB is based on the Ultra-Wideband (UWB) platform, which operates in the 3.1 to 10.6 GHz frequency range, and thus can pass through intervening bodies. WUSB allows for connections over distances up to 10 feet (3 meters) at 480 Mbps (megabits per second), or up to 33 feet (10 meters) at 110 Mbps. The standard has built in future proofing to allow for even high data rates to be achieved using later generations of the specification. It is anticipated that speeds of 1 Gbps or more should be possible.

Though Wireless USB is a viable alternative to its wired counterpart, however one of the major disadvantages of W-USB is that the device has to be self-powered unlike wired USBs where the power to the device (up to 500mW) was supplied by its host.

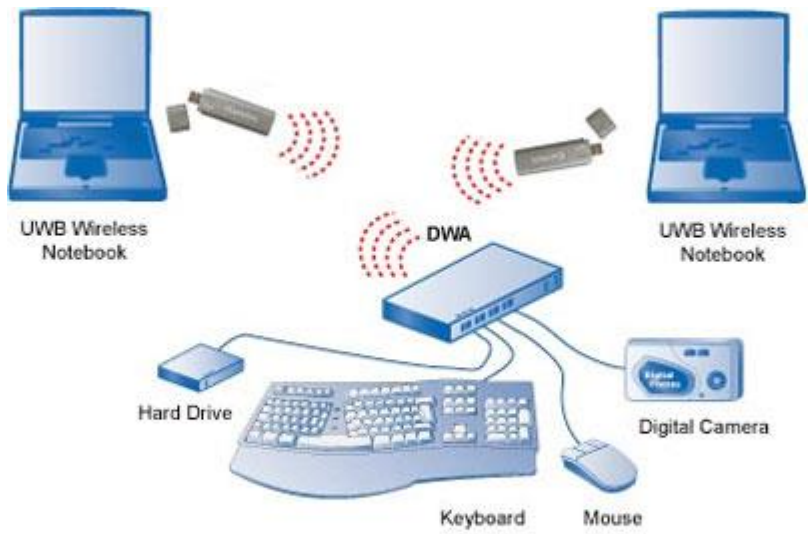


Figure 20 : Wireless USB Supporting Cluster Connectivity, [13]

6.10 ZigBee

ZigBee is a low-cost, low-power, wireless mesh network standard targeted at the wide development of long battery life devices in wireless control and monitoring applications. ZigBee devices have low latency that further reduces average current. ZigBee operates in the industrial, scientific and medical (ISM) radio bands: 2.4 GHz in most jurisdictions worldwide; 784 MHz in China, 868 MHz in Europe and 915 MHz in the USA and Australia. Data rates vary from 20 Kbit/s (868 MHz band) to 250 Kbit/s (2.4 GHz band).

ZigBee is one of the global standards of communication protocol formulated by the significant task force under the IEEE 802.15 working group. ZigBee builds on the physical layer and media access control defined in IEEE standard 802.15.4 for low-rate WPANs.

The specification includes four additional key components:

- network layer
- application layer
- ZigBee device objects (ZDOs)
- Manufacturer defined application objects which allow for customization and favor total integration.

ZDOs are responsible for some tasks, including keeping track of device roles, managing requests to join a network, as well as device discovery and security. The ZigBee network layer natively supports both star and tree networks, and generic mesh networking. Every network must have one coordinator device, tasked with its creation, the control of its parameters and basic maintenance. Within star networks, the coordinator must be the central node. Both trees and meshes allow the use of ZigBee routers to extend communication at the network level.

6.11 Visible Light Communications

In recent years Visible Light Communication (VLC) has matured as an emerging optical wireless technology for high speed data delivery applications. Main attraction of VLC is its dual functionality of providing illumination and data from the same LED light bulb. This technology is capable of supporting both short and long range optical communications. VLC is riding on the back of growing LED lighting market with the potential deployment and commercialization opportunities across diverse business sectors.

Use of visible light spectrum for establishing wireless communication has many benefits due to its unique channel properties. The visible light uses unlicensed and unregulated optical spectrum between 400THz (780nm) and 800THz (375nm), including wavelengths of the primary colors Red, Green and Blue. The bandwidth of VLC is very large when compared to the Radio Frequency (RF) spectrum demonstrating the large capacity available for supporting high speed 5G and beyond 5G applications, [14]. VLC can operate in RF sensitive environments, secure due to beam isolation property and safe for the user community compared to laser and infrared technologies [15]. VLC is considered as an additional complementing wireless technology to work co-operatively with existing RF systems, alleviating the radio spectrum congestion by offloading some of the traffic to the VLC bearer.

At present there is no globally agreed standard available for commercial VLC product development. The IEEE 802.15 WPAN Task Group 7 is working on developing the IEEE 802.15.7 VLC standard, where as Japan has already established three VLC standards. Japan Electronics and Information Technology Industries Association (JEITA) describe these are as CP-1221 (VLC communication system), CP-1222(VLC light ID system) and CP-1223 (VLC Beacon) [16].

Available full duplex VLC systems use white, red, green or blue colors to provide the downlink. For the uplink some systems use color LEDs and others use infrared when there is no benefit of an illuminated uplink. Furthermore, there are hybrid VLC systems where the downlink is VLC and the uplink uses RF. Demonstrable VLC systems are not complying with any specific protocol standards, where these systems have been developed using Commercial off-the-shelf (COTS) hardware based on Ethernet (IEEE802.3), PoE (IEEE802.3af) or HomePlug standards. These systems consist of OFDM PHY integrated with newly developed optical front ends to deliver VLC high speed links. In these systems backbone interface support TCP/IP allowing easy integration to existing communication infrastructure. There are few shortcoming of

VLC compared to RF Communications. Mainly the data rates drop sharply with the increase of the link distance and prone to interference by sun light saturating the receiver photo detectors. Other challenge is that the lights have to be always working to keep the communication link running. It is possible to dim the lights to reduce the level of room illumination. However this would reduce the speed of the link and the coverage area. Table 11 shows the properties of VLC.

Future development areas of VLC are to support indoor high speed content delivery in airports, stations, shopping malls and office environments using LED lighting infrastructure [17].

Table 11 : Properties of VLC

Property	**Comments**
Wavelength	375-780nm (Visible Light Spectrum)
Distance	0.5m - 300m Line-of-Sight
Coverage	Can be narrow or wide (Beam Angle can be 5 - 60 degree based on available systems)
Speeds	20Mbps to 1Gbps today, future beyond 10Gbps.
Service	Data communication and illumination at the same time
Frequency Regulation	No regulation on the visible light spectrum
Safety	Eye and skin safe (Human eyes can see where the light falls)
RF interference	No interference with RF system
Optical Interference	Sun light and other illumination sources can interfere creating saturation
Security	Inherently secure where the light cannot penetrate walls or ceilings. It can also be controlled and isolated easily.
Colours	Can use primary colour LEDs (Red, Blue and Green) or white phosphor LEDs
Power Consumption	Reduced power use as LEDs are low energy bulbs.
Mobility	As the light coverage area is limited to few meters (2-3 meter diameter), mobility within this area is possible.

6.12 Z-wave

An IoT Hub or Gateway is a key component of any Z-Wave based Internet of Things (IoT) deployment. The hub communicates with the smartphone and/or the communication router to allow access to the home automation devices remotely. A typical deployment may consist of scores or even hundreds of sensors, devices and actuators, which need to send data to a server and/or receive commands for configuration changes or action. Some hubs have multiple smart home radios in them (Z-Wave, Bluetooth, etc) so that they can perform different functions and support different products. The Z-Wave IoT Hub provides a bridge between these sensors, devices and the application server.

Main functionalities provided by a Gateway can be classified as follows (a) Protocol translation to connect variety of devices (b) Perform data encryption for security (c) Edge analytics (d) Sensor Supervision (e) provide cloud identity for the deployment and (f) Local data storage in-case of connectivity is lost temporarily

Figure 21 : Z Wave Architecture

The size of the property being managed by a Z-Wave Hub can be quite large because Z-Wave runs on a type of network called a "mesh network." Utility powered Z-Wave products assist the Z-wave Hub, passing the signal along by acting as a signal repeater to another product until the final destination product is reached.

Each Z-Wave network has a unique ID, which is assigned to the Z-Wave Hub and to every device in the network. This ensures that the neighbor's hub cannot control other's devices. When an extra level of security is needed, such as for door locks and other high security devices, Z-Wave has another level of security which uses AES128 encryption at the same level that major banks use to protect financial information. Z-Wave AES encryption is mandatory for hubs with the Z-Wave Plus support.

6.13 Thread

Thread is an IPv6 based networking protocol for Internet of Things (IoT) "smart" home automation devices to communicate on a local wireless mesh network.

Thread uses 6LoWPAN, which in turn uses the IEEE 802.15.4 wireless protocol with mesh communication, as does ZigBee and other systems. Thread however is IP-addressable, with cloud access and AES encryption. It currently supports up to 250 devices in one local network mesh.

6.14 Dash7

DASH7 operates primarily in sub-1GHz frequency bands, usually at 433 MHz, 868 MHz and 915 MHz unlicensed ISM band.

The DASH7 protocol is developed by the DASH7 Alliance which is a non-profit mutual benefit corporation formed to foster the existence and the further development of the DASH7 protocol specification based on ISO/IEC 18000-7. Initially DASH7 protocol were used for Defense logistics in US but later on in 2011, it has been re-purposed and it has been used for commercial applications.

The DASH7 Alliance Protocol covers all Sub-GHz ISM bands making it available globally. The name of the new protocol was derived from the section seven denoted as -7 (dash 7) of the original standard document. The current version of the DASH7 Alliance protocol i.e. Dash7 v1.0 is no more compliant with the ISO/IEC 18000-7 standard.

The DASH7 Alliance, a non-profit industry consortium was announced in March-2009 to promote interoperability among DASH7-compliant devices and in April 2011, the DASH7 Alliance announced adoption of DASH7 Mode 2, a next-generation version of the ISO 18000-7 standard that makes better use of modern silicon to achieve faster throughput, multi-hop, lower latency, better security, sensor support, and a built-in query protocol.

Later on in March 2012, the DASH7 Mode 2 specification has been made available to non-members on an open source basis. The current version of DASH 7 v1.0 was released in May 2015.

DASH7 utilizes the 433 MHz frequencies, which is globally available and license-free. This 433 MHz is not the most widely used frequency for M2M communication, it is a non-harmonized band and it spans from 433.05 to 434.79 MHz. It has better propagation characteristic due to its frequency band as compared to higher frequencies. DASH7 has the ability to transmit/receive over very long ranges without requiring a large power drain on a battery. The low input current of typical tag configurations allows for battery powering on coin cell or thin film batteries.

6.15 Ingenu

IoT connectivity that works like it should, with reliable uplink and downlink, 100% message acknowledgement, and background firmware upgrades is the tagline for Ingenu.

Ingenu's RPMA® (Random Phase Multiple Access) meets or exceeds the data features that the industry has come to expect from cellular providers. LPWAN endpoints may not require voice and video data rates, but they do require certain inalienable rights. The RPMA ensures the following:

- Industry grade security including strong authentication
- Reliable delivery of data
- Full two-way data flow
- Flexible frame sizes
- Reliable, flexible, acknowledged delivery
- Broadcast channel for firmware downloads and other functions

RPMA gives a connectivity experience that allows users to use their devices to fullest potential.

6.16 ANT/ANT+

ANT represents another ultra-low-power, short-range wireless technology designed for sensor networks and similar applications. It, too, uses the 2.4 GHz ISM band. This protocol is developed and sold by Canadian company Dyna stream Innovations Inc., a subsidiary of GPS personal navigation firm Garmin. It defines a wireless communications protocol stack that enables hardware operating in the 2.4 GHz ISM band to communicate by establishing standard rules for co-existence, data representation, signaling, authentication, and error detection. It is conceptually similar to Bluetooth low energy, but is oriented towards usage with sensors.

ANT also uses the very short duty- cycle technique and deep -sleep modes to ensure very low power consumption. The ANT protocol is set up to use a single 1 MHz channel for multiple nodes due to a time -division multiplex technique. Each node transmits in its own time slot. Modulation is GFSK. The salient characteristics of this technology are:

1. Standardization : Proprietary
2. Frequency : 2.4 GHz
3. Range : 30 m at 0dBm

6.17 6LoWPAN

6LoWPAN stands for IPv6 over Low Power Wireless Personal Area Networks. A key IP (Internet Protocol) based technology is 6LowPAN. Rather than being an IoT application protocol technology like Bluetooth or ZigBee, 6LowPAN is a network protocol that defines encapsulation and header compression mechanisms. The standard has the freedom of frequency band and physical layer and can also be used across multiple communications platforms, including Ethernet, Wi-Fi, 802.15.4 and sub-1GHz ISM. A key attribute is the IPv6 (Internet Protocol version 6) stack, which has been a very important introduction in recent years to enable the IoT. IPv6 is the successor to IPv4 and offers approximately 2^{128} addresses (approximately 3.4×10^{38}), enabling any embedded object or device to have its own unique IP address and connect to the Internet. IPv6 provides a basic transport mechanism to produce complex control systems and to communicate with devices in a cost-effective manner via a low-power wireless network.

Designed to send IPv6 packets over IEEE802.15.4-based networks and implementing open IP standards including TCP, UDP, HTTP, COAP, MQTT, and web sockets, the standard offers end-to-end addressable nodes, allowing a router to connect the network to IP. 6LowPAN is a mesh network that is robust, scalable and self-healing. Mesh router devices can route data destined for other devices, while hosts are able to sleep for long periods of time.

Currently Contiki, Thread, WSN etc. are 6LoWPAN supported solutions as shown in Figure 22.

The salient characteristics of this technology are:

a) Small packet size
b) Low bandwidth. (250/40/20 kbps)
c) Topologies include star and mesh
d) Low power, typically battery operated
e) Relatively low cost
f) Networks are ad hoc & devices have limited accessibility and user interfaces

6LoWPAN Supports:

a) Header Compression
b) Fragmentation and Re-assembly
c) Routing
d) Neighbor discovery and Multicast support

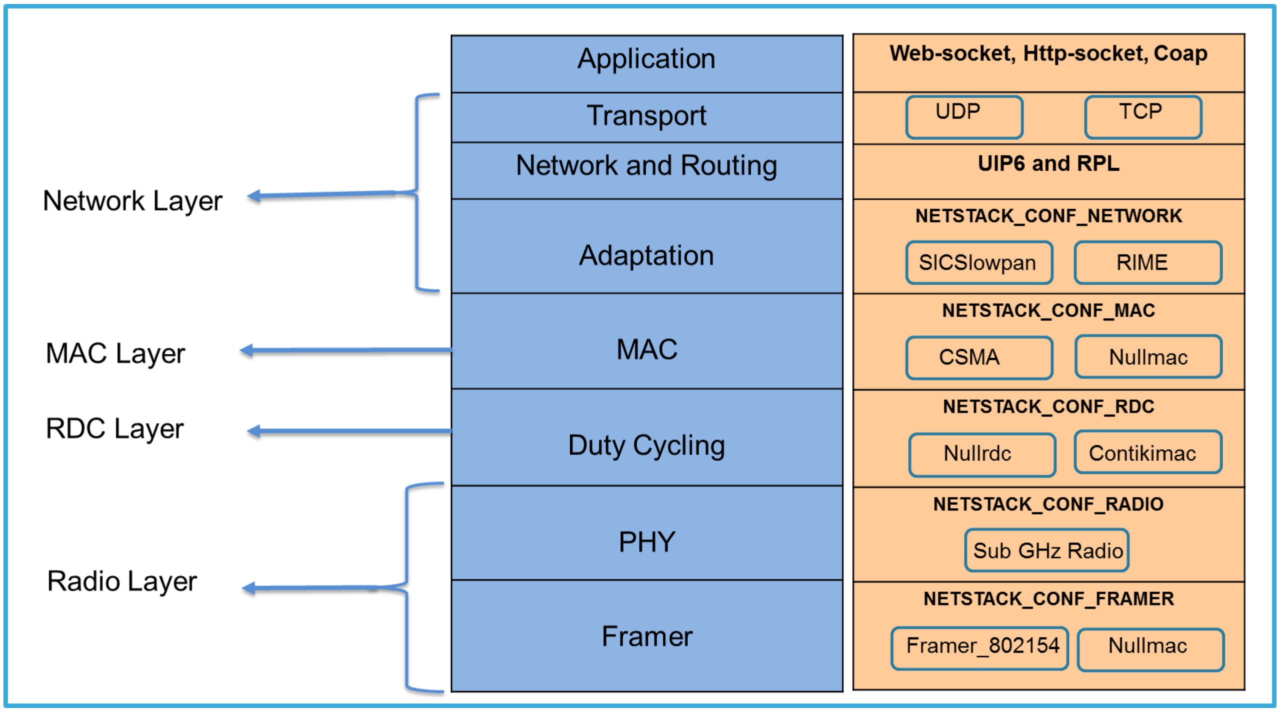


Figure 22 : IP Stack Architecture in Contiki Based 6LoWPAN Systems

7 Wireline Technologies

7.1 Power Line Communication

Power Line Communication is at a nascent stage in India. It can be used for providing last mile connectivity as well as for creating a wide area network. A key requirement of this technology is the existence of a clean network of cables for carrying information. Issues such as noise generated by different loads on the power line, dynamic changes in the line impedance and absence of trained man-power capable of custom engineering in the field are some of the issues that will need to be addressed in order to make this technology ready for use in India. In addition to the above mentioned, there is no frequency band allocated for PLC communications in India.

Power Line Communication is being tested in a few smart grid pilot projects. The following table mentions the popular narrowband PLC standards used globally:

Table 12 : Global PLC Standards, Narrowband, [18]

Standard/Protocol	Frequency band	Maximum data rate
IEEE 1901.2 – 2013	<500 KHz	500 Kbps
PRIME	42-89 KHz	128.6 Kbps
G3-PLC	35-91 KHz	33.4 Kbps
ITU-T G.hnem	10-490 KHz	1 Mbps
IEC 61334	60-76 KHz	Upto 2.4 Kbps
TWACS	200-600 Hz	100 bps
Meters & More	3-148.5 KHz	28.8 Kbps (nominal) and 4.8 Kbps (effective)
HomePlug C&C	10-450 KHz	7.5 Kbps
OSGP	9-95 KHz	3.24 Kbps (raw channel rate) & 2.36Kbps (effective)

The following table mentions the popular broadband PLC standards used globally:

Table 13 : Global PLC standards, Broadband, [18]

Standard/Protocol	Frequency band	Maximum data rate
IEEE 1901-2010	< 100 MHz	500 Mbps
HomePlug Green PHY	2-30 MHz	10 Mbps
ITU-T G.hn (G.9960/G.9961)	2-200 MHz	1Gbps

7.1.1 Narrow Band Power Line Communication

There are several standards for narrowband PLC as summarized in Table 12. Meters & More and G3 PLC are described in this section.

7.1.1.1 Meters & More

METERS AND MORE is an international non-profit association. The association operates and promotes the new generation communication protocol.

The protocol enables bidirectional data transfer between smart meters and central billing systems in an Advanced Smart Metering environment. The METERS AND MORE initiative is aimed at implementing the EU Commission Mandate 441 to provide standard pan-European Smart Metering solutions.

The architecture of Meters & More is shown in Figure 23.

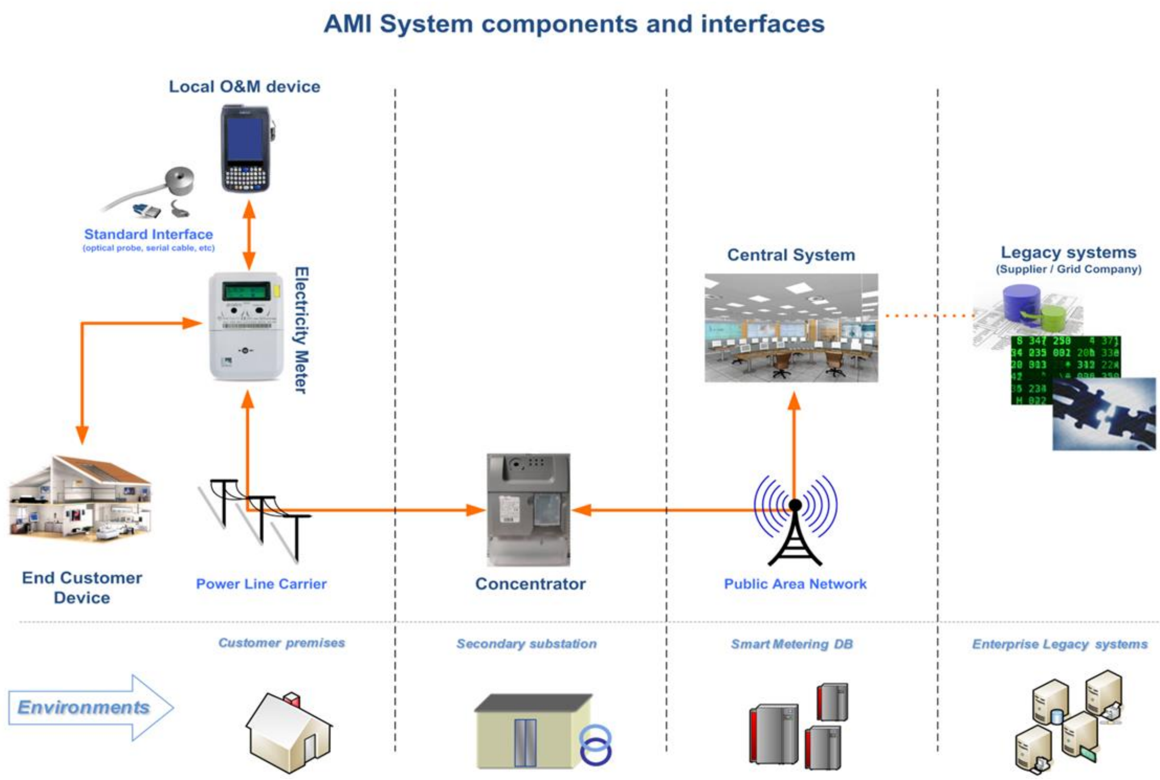


Figure 23 : Meters and More Architecture, [19]

The architecture of METERS AND MORE system consists of the following:

- Central System that manages the whole smart metering network
- Data Concentrator unit (DCU) that collect data provided by Smart Meters
- Smart Meters
- Local O&M devices for local management of Smart Meters

METERS AND MORE architecture, functionalities and requirements fulfil most of the requisites defined by the European OPEN Meter project and Smart Meters Co-ordination Group (SMCG)

The main features of the METERS AND MORE technology are efficiency, robustness and security of communications. These are summarized as given below:

- Very short message exchanges, optimized for narrow-band powerline.
- Use of a BPSK modulation the allows the communication to reach a coded bit-rate of 4800 bps
- Optimization of communication paths

- Support to a high level of encryption and authentication, by the use of symmetric key based 128 bit AES algorithms
- Automatic network configuration and management
- Re-transmission management.

METERS AND MORE system covers the entire protocol stack, from the Physical layer to the Application layer, and is able to work on Powerline networks, Public Communication networks and local optical links. METERS AND MORE specifications protocol, named SMITP (Smart Metering Information and Telecommunication Protocol) is defined in the CLC/prTS 50568-4 and CLC/prTS 50568-8 documents. CLC/prTS 50568-4 specifies the B-PSK Physical and Data Link Layers for communications on LV distribution network between a master node (the Data Concentrator) and one or more slave nodes (Smart Meters and customer devices). The Data Link layer is designed in order to perform key functionalities such as repetition, data protection and optimization of media access.

CLC/prTS 50568-8 specifies following communication profiles:

- the Original-SMITP over B-PSK PLC profile. It refers to smart metering system specifications defined prior to the availability of the DLMS/COSEM over SMITP B-PSK PLC profile.
- the Original-SMITP over IP profile, for the communication on a public network between the Central System and the Concentrator.
- the Original-SMITP over IEC 62056-21 local data exchange profile
- the DLMS/COSEM over SMITP B-PSK PLC profile

The Application layer of Original SMITP profile provides authentication functionality to ensure a high level of security and advanced features of network management, and accesses configuration parameters and measurement data defined in the Original SMITP data model.

METERS AND MORE protocol evolved in order to include a DLMS/COSEM profile over the SMITP B-PSK modulation, in addition (and as a possible alternative) to the Original SMITP profile. It defines the use of the CLC/prTS 50568-4 communication protocol and methods to access and exchange data modelled by the COSEM objects and interfaces of EN/IEC 62056-6-1 and 6-2 via the EN/IEC 62056-5-3 application layer. This section forms part of the DLMS/COSEM suite as described in EN/IEC 62056-1-0 13/1548/CDV and shown in Figure 24.

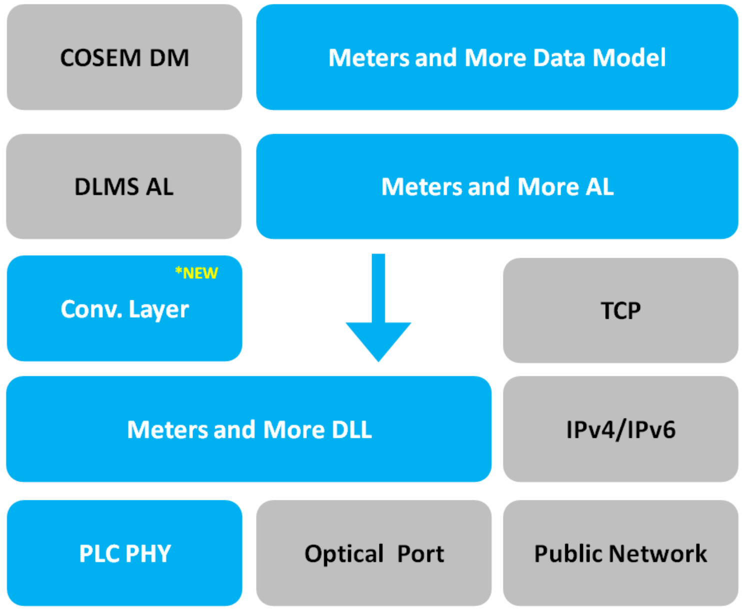


Figure 24 : DLMS and COSEM

7.1.1.2 G3-PLC

G3-PLC facilitates high-speed, reliable, long-range communication over the existing powerline grid. It has the ability to cross transformers and supports IPv6.

G3-PLC Technology and Features:

- G3-PLC supports frequency bands worldwide (10 kHz to 490 kHz). It coexists with IEC 61334, IEEE P1901 and ITU G.hn. It is compliant with world regulatory bodies such as CENELEC, ARIB, and FCC (10 kHz - 490 kHz).
- OFDM-based PHY (BPSK, QPSK, 8PSK) makes efficient use of the spectrum.
- Coexists with other technologies: G3-PLC coexists with S-FSK and BPL
- Standards based — pre-standard in IEEE, ITU, IEC/CENELEC and IEC/SAE.
- Two layers of forward error correction (FEC) for robust data communication in harsh channels.
- Adaptive tone mapping for optimal bandwidth utilization.
- Channel estimation to select the optimal modulation scheme between neighboring nodes.
- "Robust" mode to improve communication under noisy channel conditions.
- IEEE 802.15.4-based MAC layer well suited to low data rates.
- 6LoWPAN adaptation layer to transmit IPv6 packets over powerline channels.
- AES-128 cryptographic engine for optimum data security.
- Coexistence with older S-FSK (IEC 61334), and broadband IEEE P1901 and ITU G.hn standards.
- Supports IPv6 to allow Internet-based energy management systems and applications.
- Mesh routing protocol to determine the best path between remote network nodes.

7.1.2 Broadband PLCs

7.1.2.1 Wireline Home networking

Modern residential homes contain an increasing number of consumer electronic (CE) devices for communications and entertainment, which are increasingly required to be interconnected among themselves and to the outside service providers that deliver entertainment content, telecom services and Internet access.

Today, broadband residential services are delivered to homes by coaxial cable, twisted pair, or optical fiber. Regardless of the access transmission media, the signal is terminated in the modem (DSL, cable, or Optical Networking Unit), and the signal can be distributed inside the home to connect various CE devices.

The known in-home networking (IHN) solutions include wired Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11 b/g/n), Powerline Communications (IEEE 1901, ITU G.hn), and Multi-media over Coax Alliance (MOCA), and Home Phone-line Network Alliance (Home PNA).

In consumer homes today, several types of physically separate networks may be available such as:

- Networks that distribute digital signals (usually connected to access networks),
- Analog TV signals (typically coax cable),
- And a large number of device-to-device links that operate at speeds up to 10 Gb/s.

In-home PLC is a technology that delivers telecom services to every corner of a household through already existing electrical wiring. In recent years, PLC has emerged as a potential candidate for domestic high bit rate services.

The current in-home PLC technology, based on Single-Input Single-Output (SISO) configuration, does not fully achieve the capacity offered by the physical PLC channel. The in home PLC channel offers multiple signal feed ports as, usually, it comprises of three wires: Phase, Neutral and Protective Earth.

7.1.2.2 Powerline Technologies (PLT)

Traditionally, a single input single output (SISO) channel is used for in-home communication by PLT technologies. It is typically based upon the differential use of the L-N (Line or Phase to Neutral) wire pair.

In powerline communications, the use of MIMO (multiple inputs multiple outputs) -PLT offers several improvements over legacy SISO powerline transceivers:

a) Increasing the coverage in a home or building.

b) The ability of MIMO signals to cross over to other phases in the electrical wiring increases coverage and performance for many areas of the building.

c) Improving the throughput as MIMO is based on a highly optimized signal processing spatially multiplexed signals over each port.

MIMO-PLT transceivers are able to transmit and/or receive over three powerline conductors (e.g. Phase, neutral, and ground) using more than one TX and/or Rx port, thus providing a significant increase of data rate, noise immunity improvements, and enhancing the connectivity of the home network in increased coverage.

The MIMO-PLT specifications describe the required modifications to define MIMO home networking transceivers for operation over powerline wiring.

7.1.2.3 Transportation of HD and UHD video over Powerline.

The contemporary in home single phase electrical power delivery network consists of three wires. Therefore, multiple signal feeding ports are available in most in-home PLC channels.

Multiple-input multiple-output (MIMO) technology has already been used in power-line communication (PLC). An accurate description of MIMO channels for PLC network topologies is of great interest and importance in the development and testing of digital communication algorithm.

However, the considerable variability of PLC networks makes this task quite difficult. In this regard, a random channel generator for a single-input single-output (SISO) configuration has been presented in the literature. The procedure was applied to a set of measured channels that were interestingly divided into nine classes.

A MIMO channel is considered as the superposition of correlated SISO channels so we attempt to describe an MIMO channel using the nine classes obtained with the SISO configuration. An additional parameter, related to the correlation factor, had to be taken into account.

The phase 1 of STF468 had shown the benefit of PLT networks coverage when the video is encoded with HEVC/H265 compared to the same video encoded with H264/AVC.

Transcoding is one of the most promising technologies, which provides video adaptation in terms of bit-rate reduction, resolution reduction and format conversion to meet various requirements. The wide use of the AVC standard today and the expected adoption of HEVC raises a new demand for AVC to HEVC transcoding.

In practice, a video transcoder should make tradeoff between complexity and coding performance while making full use of the input bit-stream to generate a new one.

According to ITU/SG15 standard, the current HEVC model still belongs to block-based hybrid video coding framework, except that the block size is extended to up to 64x64 compared with that of AVC (16x16). Basically, AVC and HEVC share a similar prediction, transform, quantization, and entropy coding architecture.

However, since rate-distortion cost of multiple modes still needs to be evaluated, a mass of sum of absolute difference/sum of square difference (SAD/SSD) computation as well as fractional pixel interpolation has to be involved in the motion re-estimation or motion refinement process. Thus, the computation complexity of these techniques cannot be ignored.

7.2 Digital Subscriber Line (DSL)

DSL over PSTN network is a well-established technology. Broadband services are being provided using DSL technology for more than two decades. A number of ITU standards exist on this technology.

Broadly speaking, DSL is a family of technologies that are used to transmit digital data over telephone lines. In telecommunications marketing, the term DSL is widely understood to mean asymmetric digital subscriber line (ADSL), the most commonly installed DSL technology, for Internet access. DSL service can be delivered simultaneously with wired telephone service on the same telephone line. This is possible because DSL uses higher frequency bands for data. On the customer premises, a DSL filter on each non-DSL outlet blocks any high-frequency interference to enable simultaneous use of the voice and DSL services.

Asymmetric DSL (ADSL), is a form of DSL where more bandwidth is allocated to download than to upload. This makes it ideal for web browsing and typical Internet usage, where downloading of large files is more important than uploading, because it enables maximum speeds of 8-10 Mbit/s downstream and a maximum of 1 Mbit/s upstream. ADSL is available at a maximum distance of 3 km from the local exchange. It is well suited to residential use because it shares a single twisted copper pair with voice, allowing users to use the telephone and surf the Internet simultaneously on the same line. ADSL is the most popular form of DSL offered around the world and the transceivers falling in this category are described in the ITU-T Recommendations of the G.99x-series. Further variant in ADSL technology are ADSL2, ADSL2plus and VDSL. These technologies have revolutionized the internet services across the globe.

7.2.1 G.fast broadband standard (ITU-T G.9701)

G.fast refers to “fast access to subscriber terminals”. It is the broadband standard designed to provide access speed of 1Gbps over existing telephone lines. Physical layer specification G.9701 has been approved by ITU-T in December 2014.

G.fast, within the fibre to the distribution point (FTTdp) architecture, combines the best aspects of fibre and DSL. Within 400 metres of a distribution point, G.fast provides fibre-like speeds matched with the customer self-installation of DSL, resulting in cost-savings for service providers and improved customer experience.

G.fast will increase the feasibility of implementing bandwidth-intensive services such as Ultra-HD '4K' or '8K' streaming and next-generation IPTV, advanced cloud-based storage, and communication via HD video. The standard will comfortably serve the broadband access needs of small-to-medium enterprises, with other envisioned applications including backhaul for small wireless cell sites and WiFi hotspots.

G.fast's spectrum compatibility with VDSL2 enables service providers to play to the strengths of each standard in different environments.

As optical fiber cable (OFC) is much cheaper than the copper cable, Telecom service providers will opt the FTTH in the green field scenarios. But in the brown field scenarios – for example, an urban environment with an abundance of copper telephone cables – G.fast will be more cost-efficient than FTTH [20].

7.2.2 FTTH standards for 10 Gbit/s fibre to the home

The ITU-T family of 10 Gbit/s PON standards now offers both asymmetric and symmetric transmission for broadband services, with XG-PON enabling downstream service at 10 Gbit/s and upstream service at 2.5 Gbit/s, and XGS-PON enabling 10 Gbit/s bi-directional service.

The ITU-T standards underlying optical systems for fibre access networks are developed in ITU-T Study Group 15. Experts continue to work in the interests of enhancing the data rates achieved by fibre access networks. A study of 25 Gbit/s per wavelength over PON has been initiated with the aim of enhancing the capacity of PON systems to beyond 100 Gbit/s [21].

Optical Fiber Cable (OFC) is being used in the core network as well as in the access network (FTTH). High bandwidth is available through various SDH switches (MADM16/64 etc) in the core network. DWDM technology has made it possible to create multiple virtual fibres. This further adds huge capacity in the network. In the fibre to home network, speeds up to and beyond 100 Mbps are already available. ITU standards are available to define the interconnections for the above technologies.

7.3 Coexistence of PLC and DSL technologies

The demand for higher bit rate data services from customer side is promoted by high-speed Internet access and many forthcoming innovative services .This demand can be met with the deployment of VDSL2 technology as well as the extension to VDSL2 vectoring and bonding. With the progress of VDSL2 technologies such as Vectoring and Bonding, where self-crosstalk of VDSL users is actively removed through coordinated signal processing, the impact of PLT interference on this VDSL2 technology is expected to increase.

The interactions between a Digital Subscriber Line (DSL) access network and Home Networks based on Powerline Telecommunication (PLT) have been reported during past years as PLT modems are widely used for IPTV distribution in a home.

PLC (Power Line Communication) networks and VDSL networks (limited to 30MHz) use common frequencies in the unlicensed band from 2-88MHz. PLC devices and VDSL devices may often be placed in relative proximity to each other and there are concerns that this could create interference

Recently, the interactions at the physical layer between VDSL2 access technologies and various powerline telecommunications technologies have been studied by ETSI STF 384 and analyzed through ETSI PLUGTEST. VDSL2 deployments are regaining interest for very high speed access Internet services. In the meantime distributing these services in a home through electrical networks using PLT modems is also gaining momentum. DSL, FTTH and Broadband PLCs will be used to connect the Gateway routers to the headend systems for sending the data for sensors and to provide high speed internet services. In the homes and offices these will be able to provide high speed internet access through Wi-Fi hotspots etc. In IoT domain, high speed and stable Internet services are required to connect millions of sensors to the cloud. This can be provided by the fixed line technologies.

8 Comparison Table for Wired and Wireless Technologies

A technological description in brief has been given in the following table. However a detailed description has been taken up in the following chapters:

Table 14 : Comparison of Communication Technologies, [9]

Technology/Protocol	Frequency band (s)	Advantages	Limitations	Suitable for
Wireless				
Bluetooth Low Energy	2.4 GHz	• Mature technology • Easy to implement • Low Power • Powered by coin cell • Longer battery life	• Small data packets	• Healthcare devices • Fitness devices • Smart Metering
NFC	13.56 MHz	• Consumes less power • Almost instantaneous connectivity between devices • No power is required in-case of passive Tags	• Extremely short range • Expensive • Low information security • Low market penetration	• Healthcare devices • Fitness devices • Smart Metering
Wi-Fi	2.4 GHz	• Mature technology • High home/office penetration • High data rates achievable • Easy to implement	• Limited range • Poor building penetration • High interference from other sources • Power consumption higher than those technologies that operate in the sub-GHz band	• Base station in Health Clinics • Smart Metering • Home Automation

ZigBee	2.4 GHz, 920 MHz, 915 MHz, 868 MHz, 780 MHz	• Full support of IEEE 11073 device specialization profile • Longer battery life from low cost coin cells for wearable devices (source: ZigBee alliance) • Wireless range up to 70 meters indoor and 400 meters outdoor (source: ZigBee alliance)	• Not widely adopted • BLE is the direct competition for ZigBee providing different modes/profiles of operation. BLE is getting adopted faster than ZigBee within short span of time	• Health Monitoring and Safety • Client Activity Monitoring • Health and Wellness monitoring
Z-Wave	Sub 1GHz for India (865-867 MHz)	• Standardised by CSR 564 (E) • very successful due to its ease of use and interoperability • Majority share of the Home Automation market	• Proprietary radio systems available • Limited Range drives up costs	• Security systems. • Home automation. • Lighting controls
Wi-SUN	Sub 1GHz for India (865-867 MHz)	• Open standards based • Interoperable • High data rate • Long Range • Widely adopted in Japan, Singapore and USA. Currently being adopted in Asia, Australia South America and parts of Europe and other regions • Low power consumption • Operates as RF mesh network delivering higher reliability.	• Based on latest IEEE standard which is not yet adopted widely	• Smart metering • Distribution Automation • Smart Home • Smart City • Industrial automation
ANT	2.4GHz	• Low power mode supporting longer battery life	• BLE is giving direct competition to ANT as it is already supported by all the mobile manufacturer	• Fitness device • Healthcare device

		• Adopted by major mobile manufacturer • Supports mesh capability which is an edge over BTLE	• Not all mobile Manufacturer are supporting ANT hardware	
Cellular (2G-GSM/EDGE, 3G-UMTS, 4G-LTE)	For India, 900 MHz, 1800 MHz, 2100 MHz and 2300 MHz is allocated .	• Mature technology • Developed by global community of 400+ companies from 39 countries • Rapid deployment • Communication modules are low cost and standardised. • Roaming • Wide availability of Network Infrastructure	• Coverage not 100% • Reliability not the best • Short technology life-cycle (2G, EDGE, 3G, LTE etc.)	• Tele-Health • Remote Health Monitoring • Smart Metering
Cellular: EC GSM IoT	2G Bands	• Network infrastructure is backwards-compatible to previous releases to allow the technology to be introduced into existing GSM networks	• Eco system is yet to be developed	• Smart cities & homes • Smart utilities • Industrial automation • Wearables • Smart energy • Intelligent transport systems
Cellular: NB-IoT	Conventional LTE cellular bands like 700 MHz, 800 MHz and 900 MHz, and re-farmed 2G bands	• Standards based defined by 3gpp, the global standardization organizations supported by a mature global ecosystem • wide area ubiquitous coverage • deployed through upgrade of existing network (reuses existing network infrastructure) • Ultra-low-power consumption in devices • Enhanced for 20+dB additional coupling gain. (reaches deeper in-building & underground) • low cost terminal • plug and play	• Limited Mobility is not yet supported (limited support based on cell reselection) • Voice is not supported • Low Data rate applications with link peak DL = 60~100kbps & UL=~50kbps	• Sensor based applications, with low data rate requirement. • Applications not requiring high speed mobility handovers. • Systems where devices/sensor measurements are expected to be for long ~10years

		• high reliability and high carrier-class e2e network security (based on LTE)		
Cellular: eMTC	Conventional LTE cellular bands like 700 MHz, 800 MHz and 900 MHz	• Developed by 3GPP a mature global ecosystem • Low power consumption • Works over existing LTE networks • Easily configurable on demand scaling possible • Supports full mobility • Supports voice through VoLTE • high reliability and high carrier-class e2e network security (based on LTE)	• Support of higher bandwidth limits the other optimizations possible, compared to NB-IoT and EC-GSM-IoT	• Wearables, • Asset Tracking, • Pet Trackers • Telematics, • KIOSK, • Parking, • Industry environment monitoring, • Connected Healthcare personal & Enterprise equipment • Industrial IoT with Emergency Voice call support
LoRa	Sub GHz	• Network can be defined by the individuals / owners. • Support long range and high battery life • High security using AES 128 encryption	• Own deployment with no subscription fees • Works in unlicensed band.	• Smart Metering, • Smart street Lighting solutions • Asset monitoring
SIGFOX	Sub GHz	• Infrastructure being deployed. Several countries SIGFX ready	• Deployment by Network Operator • Subscription fee	• Smart Metering, Lighting
Wireline				
DSL	0-2.208 MHz	• Inexpensive (installation and use) • High SLA • Less installation time • Bonded DSL provides inherent redundancy	• Low data security • Lower throughput • Higher latency	• Gateway for Remote Health Monitoring • Concentrator for Tele-Health • Home Automation

Ethernet	16,100,250 ,500, 600 MHz 1 GHz, 1.6-2.0 GHz	• Inexpensive (installation and use) • Excellent throughput • Low installation time • Easily scalable	• Lowest data security • Lowest SLA • Highest latency • Bursts of additional bandwidth not possible	• Gateway for Remote Health Monitoring • Concentrator for Tele-Health • Smart Metering • Home Automation
PLC	No defined frequency band in India	• Ready infrastructure • Communication possible in challenging environments such as underground installations, metal-shielded cases etc. • Long technology life-cycle • Many standards and protocols available	• Point-to-point communication • Can cause disturbances on the lines • Not suitable where power cables are not in a good condition; initial and ongoing line conditioning and maintenance can add significant O&M costs • Highly trained manpower required for O&M • Communication not possible in case of an outage • Absence of regulations on use of frequency bands	• Smart metering • Home automation

9 Broad requirements for a Gateway / Platform

In M2M / IoT communication, Gateway and the platform play an important role. For M2M Communication, devices should be able to communicate with the headend servers (application server) either through the Gateways and platform or directly through a platform. Brief description about the features/ requirement is given below.

9.1 Gateway

Gateway has been described in detail in Chapter 8 of TEC Technical Report on Smart Homes [9]. Gateway design has also been described in brief in Annexure 1 of this technical report. It may be noted that the Gateway provides connectivity to the devices on wired / wireless communication technologies for onward connectivity to the network and platform. It is not necessary that all the devices will communicate via gateway, as an example devices connected on short range communication technologies will communicate with the platform via gateways however the devices connected on WAN / LPWAN technologies may communicate directly to the platform without using gateways. Gateways may have more than one communication technologies supported in the LAN as well as WAN areas.

9.2 Platform

IoT platforms provides connectivity to take device data and translate it into meaningful information. Facilities like device management, data management, connection management, security, maintaining unique identity of devices and applications shall be the integral part of platform. Platform can be deployed in the cloud / data centres as per the need and it should be scalable.

At present most of the Industries are working in silos and on vertical centric approach where interoperability of the devices and data sharing among the verticals is difficult and will require complex integration of isolated data. Deployment of devices in this manner will be costlier and may have proprietary APIs.

Comprehensive study of various vertical use cases make it clear that sharing of data among divergent verticals is a practical reality. The Smart health vertical may require some data from the Smart Automotive vertical (for example the location of the vehicle). Smart Automotive vertical will require the data to be shared with smart parking vertical. Therefore real smartness can be achieved only when the data is shared among various verticals. Sharing of data can be best achieved using horizontal / common service layer approach. It has been described in Chapter 10.2 of TEC Technical Report on Smart Homes [9].

The concept of common M2M service layer was described by ITU in 2012. In this concept, devices are proposed to communicate with the Head end servers with or without Gateways and via a common service layer platform. This will enable interoperability and seamless data sharing among stakeholders. A number of standard developing organizations (SDOs) have been working together to finalize the standards for the common service layer. OneM2M has published the Release 2 specifications for M2M and Internet of Things in 2016. OneM2M standards are being used by a number of independent open source foundations and projects such as OCEAN, IOTDM, OM2M, CDOT, HP etc.

OneM2M specifications are being studied in M2M Gateway & Architecture working group in TEC. Use case with common service layer based on OneM2M specifications has been described in Annexure 8.

10 Testing and certifications

Testing and certifications of various technologies and devices is required to ensure the reliability and the quality of service across large number of devices and networks. There is an unstated expectation from the customers that wireless devices with them should function flawlessly at all times in different networks and for different applications. Ensuring it all works reliably and consistently is challenging but can be managed. Communication technologies for M2M/ IoT domain may be of different types as described in chapter 4. SDOs/ Alliances have come up with the specifications related to respective technologies. There are test labs accredited by the concerned SDOs. A table has been prepared having details of various communication technologies, respective SDOs and the links related to test labs. This is available in ANNEXURE 9 : Communication Technologies – related SDOs and certification details.

Work is already going on in TEC related to device certification and responsibility centers for the M2M/ IoT domain.

11 Recommendations / Way Forward

1. In view of expected deployment of billions of IoT / M2M devices in India, it is apparent that 2 MHz spectrum (865-867) MHz available in ISM band may not be sufficient. TEC has already conducted a study and released “Technical Report on spectrum requirement for PLC and Low power RF radio”. It is having recommendation for release of additional delicensed spectrum in Sub GHz band [10], preferably adjacent to the existing one.

2. Indian spectrum bands should be harmonized with the international bands in various technologies. This will create the possibility of releasing additional spectrum in Sub GHz and other bands.

3. With billions of devices, the Identification / addressability/ traceability of all the devices is required to ensure uniqueness and security. There may be IP and non IP devices in the eco system. It is therefore necessary that all the devices / Gateways, which are to be connected directly to PSTN/ PLMN, should have IPv6 ready or with dual stack (IPv6 and IPv4) capability.

4. ISM band based networks when used to provide public services may be subject to licensing requirements. Further, many LPWAN technologies may have proprietary wide area network of their own without requiring to connect with existing / standard PSTN / PLMN networks. Consideration is required for some form of licensing of such types of standalone network technologies also if such independent networks using these LPWAN technologies are being deployed for commercial use while at the same time keeping in view standards based implementation requirement at service layer. These types of networks may also be required to be connected to central monitoring system(CMS) from the point of view of National security.

5. It is necessary to develop telecom interface specifications for devices, Gateways etc so that standard based devices prevail in the market. This needs to be followed up with development of eco system for testing and certification of M2M devices. Once such standards are adopted, TEC can certify the devices based on its own testing or testing by designated CABs as per interface standards. This step will also promote the use of open standard based technologies more and more instead of proprietary technologies. The development of standards would not only assure interoperability but also bring down the cost of interconnections and perhaps the devices as well.

6. Due to the use of variety of RF interfaces in the devices / gateways in M2M/ IoT, it is imperative that the test instruments required for development / certification of devices will have RF interfaces. For giving a push to development of indigenous products, there is a need to simplify the import license process for such instruments, including their replacement by certain declaration at the time of import. Industry / TEC can provide details of such interfaces / instruments to DoT / WPC and the matter can be decided in consultation with stakeholders.

7. Telecom service providers may be encouraged to study the expected impact of large scale M2M/ IoT deployment on the current network so that they should not suddenly find the network service quality getting adversely affected.

8. To achieve Interoperability and sharing of data among the servers / platforms of various verticals, standards for common service layer as detailed in Chapter 9 are required to be finalized in Indian context, in sync with global standards.

12 Bibliography

[1] M. Wang, "Explosion of the Internet of Things: What does it mean for wireless devices?," Keysight Technologies, 2015. [Online]. Available: http://www.keysight.com/upload/cmc_upload/All/Slide_IOT_Part_1.pdf?&cc=GB&lc=eng. [Accessed March 2017].

[2] TEC, "Technical Report on M2M Gateway and Architecture (M2M Number Resource Requirements and Options)," TEC, New Delhi, 2015.

[3] Ericsson, "Cellular Networks for massive IoT," 2016.

[4] Ericsson, "Cellular networks for Massive IoT – enabling low power wide area applications," 6 Jan 2016. [Online]. Available: https://www.ericsson.com/publications/white-papers/cellular-networks-for-massive-iot--enabling-low-power-wide-area-applications. [Accessed 2017].

[5] Nokia Networks, "LTE-M – Optimizing LTE for the Internet of Things," 2015. [Online]. Available: https://iotfuse.com/wp-content/uploads/2016/02/nokia_lte-m_-_optimizing_lte_for_the_internet_of_things_white_paper.pdf. [Accessed 13 May 2017].

[6] Qualcomm, "Paving the path to Narrowband 5G with LTE Internet of Things," 2016.

[7] Qualcomm Technologies, Inc., "Paving the path to Narrowband 5G with LTE Internet of Things (IoT)," July 2016. [Online]. Available: https://www.qualcomm.com/documents/paving-path-narrowband-5g-lte-iot. [Accessed 2017].

[8] NOKIA, "LTE evolution for IoT connectivity," [Online]. Available: http://resources.alcatel-lucent.com/asset/200178. [Accessed 2017].

[9] TEC, "TEC M2M / IoT Technical Reports," [Online]. Available: http://www.tec.gov.in/technical-reports/. [Accessed 2017].

[10] TEC, "Technical Report : M2M Enablement in Power Sector (Spectrum Requirements for PLC and Low Power RF Communications)," TEC, New Delhi, 2015.

[11] IEEE, "IEEE 802.11ah (Wi-Fi in 900 MHz License-exempt Band) for IoT Application," 2016. [Online]. Available: https://www.standardsuniversity.org/e-magazine/august-2016-volume-6/ieee-802-11ah-wi-fi-900-mhz-license-exempt-band-iot-application/.

[12] B. SIG, *Bluetooth Core Specifications, v5.0,* SIG, 2016.

[13] Everything USB, "Cables Unlimited Wireless USB Adapter Kit Review," [Online]. Available: https://www.everythingusb.com/cables-unlimited-wireless-usb-adapter-kit-15823.html. [Accessed 2017].

[14] "European Technology Platform for Communications Networks and Services, Expert Working Group on 5G: Challenges, Research Priorities, and Recommendations,," in *NETWORLD 2020*, August 2014.

[15] T. K. a. M. Nakagawa, "Fundamental Analysis for Visible Light Communications System using LED lights," *IEEE Transaction of Consumer Electronics,* p. 100, 2004.

[16] "Visible Light Communication Association (Japan)," December 2016. [Online]. Available: http://vlca.net/standard/. [Accessed 2017].

[17] B. H. S. K. a. B. H. S. Ayub, "A Practical Approach of VLC Architecture for Smart City," in *Antennas & Propagation*, Loughborough, 2013.

[18] ISGF, "Need for Allocating a Frequency Band for Power Line Carrier Communications," 2014.

[19] "Meters and More Open Technologies," Meters and More, [Online]. Available: http://www.metersandmore.com/technology/. [Accessed June 2017].

[20] ZDNet, "ITU approves G.fast DSL high-speed broadband standard," 2014. [Online]. Available: http://www.zdnet.com/article/itu-approves-g-fast-mixed-technology-broadband-standard/. [Accessed May 2017].

[21] FSAN, "New ITU-T standard for 10 Gbit/s symmetric fibre to the home," 2016. [Online]. Available: https://www.fsan.org/new-itu-t-standard-for-10-gbits-symmetric-fibre-to-the-home/. [Accessed May 2017].

[22] N. Jones, "Top 10 IoT Technologies for 2017 and 2018," Gartner, [Online]. Available: https://www.gartner.com/webinar/3435117?srcId=1-4554397745. [Accessed March 2017].

[23] L. Alliance, "A technical overview of LoRa® and LoRaWAN™," [Online]. Available: https://www.lora-alliance.org/portals/0/documents/whitepapers/LoRaWAN101.pdf <https://www.lora-alliance.org/portals/0/documents/whitepapers/LoRaWAN101.pdf> .

[24] 3GPP, "Cellular system support for ultra-low complexity and low throughput Internet of Things (CIoT)," 2015.

ANNEXURE 1 : Architecture and Protocols for a Gateway

Source: STMicroelectronics India.

The promise of efficient and intelligent use of resources enabled by IoT has raised the expectations of the technical as well as the consumer community. However it's not always possible to connect the IoT nodes directly to the public internet due to power or computational limitations.

IoT Gateway help connect Things to broader internet by using connectivity technologies suitable for resource limited Things. There are a myriad of technologies and protocols available to communicate between Things, Gateway and Cloud Application. Devices for different vendors are based on the chosen technology and often require independent gateways. Wireless bridge is an attempt to integrate multiple protocols in a manner that a sensor devices based on different communication technologies are integrated on to a single platform. The diagram below, represents a flexible architecture for Internet of Things Gateway Platform known as "Wireless Bridge" which supports different wireless technologies.

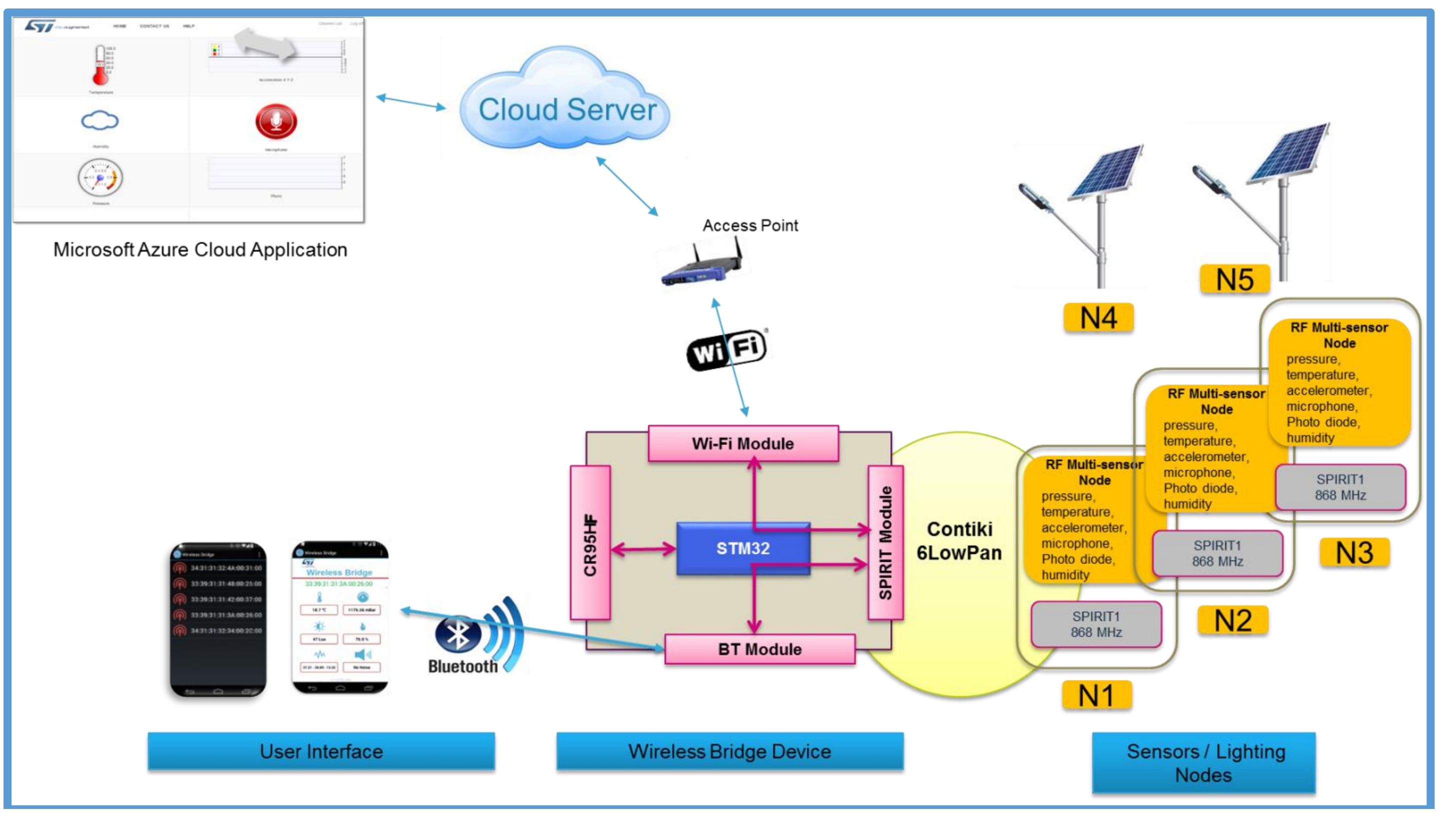


Fig ANNEX1.1: IoT Home Gateway System Architecture

IoT Gateway Architecture:

Gateway device is MCU based IoT Platform as shown in above Figure, having different connectivity technologies. The system comprises of Bluetooth, Wi-Fi, Sub-GHz and Near Field Communication. Wi-Fi is used for exchanging Things or Node data with the Cloud Platform through IoT Gateway Platform. Bluetooth is used for communicating the Things or Node data with the Android App through Gateway Platform and Sub-GHz is used for exchanging data between Gateway Platform and Things. An Application layer is added on the Gateway solution that acts as bridge between the Cloud Application and Things.

Key Communication Elements:

a) Sub-GHz Module: The communication between Home Gateway and Things is based on 6LoWPAN using Sub-GHz module. Sub-GHz module is ultra-low power & fully integrated RF module operating in the 865 MHz. Optionally modules with same footprint and working at 915 MHz ISM band can be used for other markets.

b) Wi-Fi Module: The Wi-Fi module connects the Home Gateway device to Microsoft Azure based cloud application. Wi-Fi module works as STA mode and connect to AP and upload the sensors / lighting data on cloud server.

c) Near Field Communication: The Gateway has NFC transceiver used as NFC reader/writer device to communicate with the NFC Passive Tag on the Things for configuration purpose.

d) Bluetooth Module: Bluetooth module is used in home automation applications for communicating with Bluetooth devices and smart phones.

e) BLE module: Possibilities exist to replace any of the modules with some changes in layout as long as the modules are designed in a manner that communication with host microcontroller is supported. As an example, BLE module has been integrated and tested in the Wireless Bridge successfully.

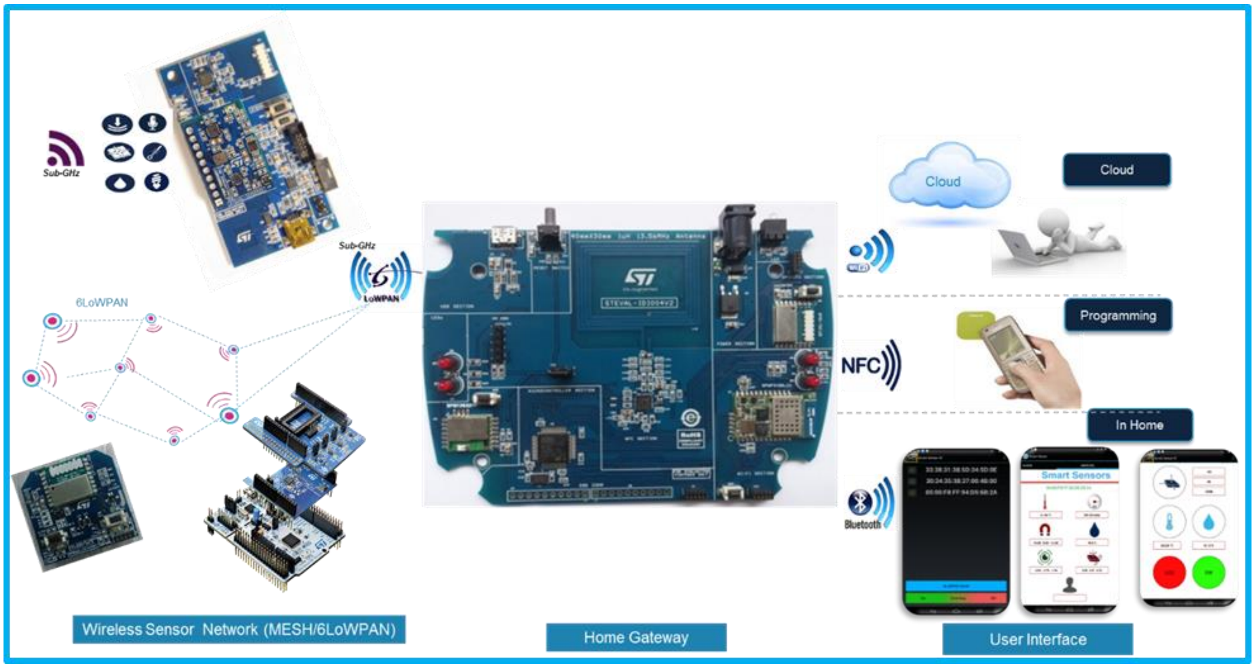


Fig ANNEX1.2: IoT Home Gateway Solution

Things Architecture

'Things' in this solution are based on Multi Sensors-RF platform which has 2 parts (Sensor Board and RF board). RF board is the master board consisting of a low power MCU device, Dynamic NFC Tag (M24LR) and Sub-GHz. MCU runs Contiki3x based 6LoWPAN for connectivity with Gateway.

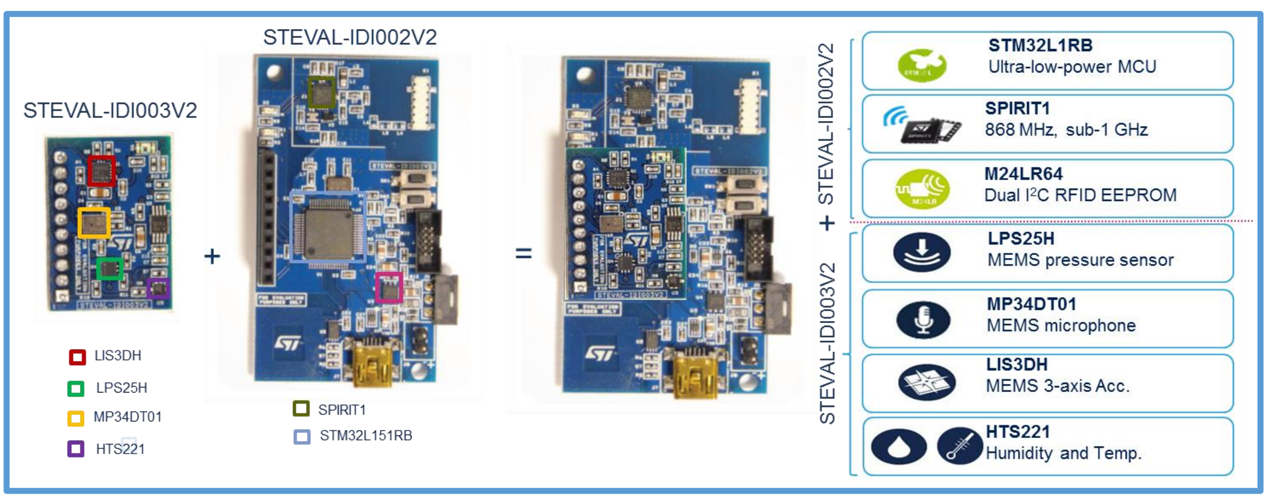


Fig ANNEX1.3: RF Sensor Node (Thing)

"Sensors Board" consists of a multiple sensors such as accelerometer, pressure, humidity, microphone and light sensor.

Gateway has local and remote connectivity options to access sensor data and actuator on the nodes.

Android Application: A local user can access the nodes using the Bluetooth connectivity on smart phones by pairing with the Gateway device.

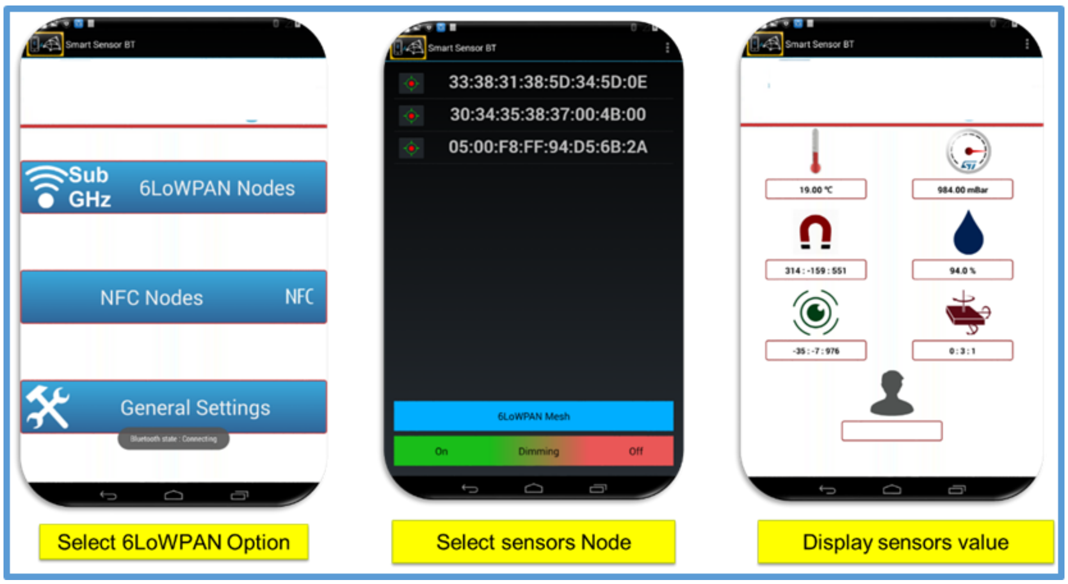


Fig ANNEX1.4: Android APP

The android application provides the facilities to set alias name for each of the sensor node. The user needs to long press over the IP address which pops up a dialog box to set alias name.

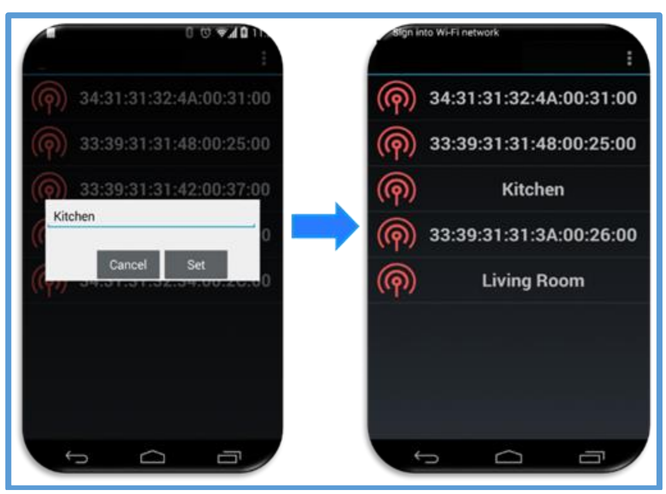


Fig ANNEX1.5: SET Alias name

NFC Application: The Sensor nodes also have the NFC Passive Tags. The passive tag stores the sensor values for each node. If the 6LoWPAN network is not available, the user can put sensor node's NFC antenna on top of Home Gateway NFC antenna and read the sensors values through NFC interface. The communication between Android App and Home gateway is on Bluetooth communication.

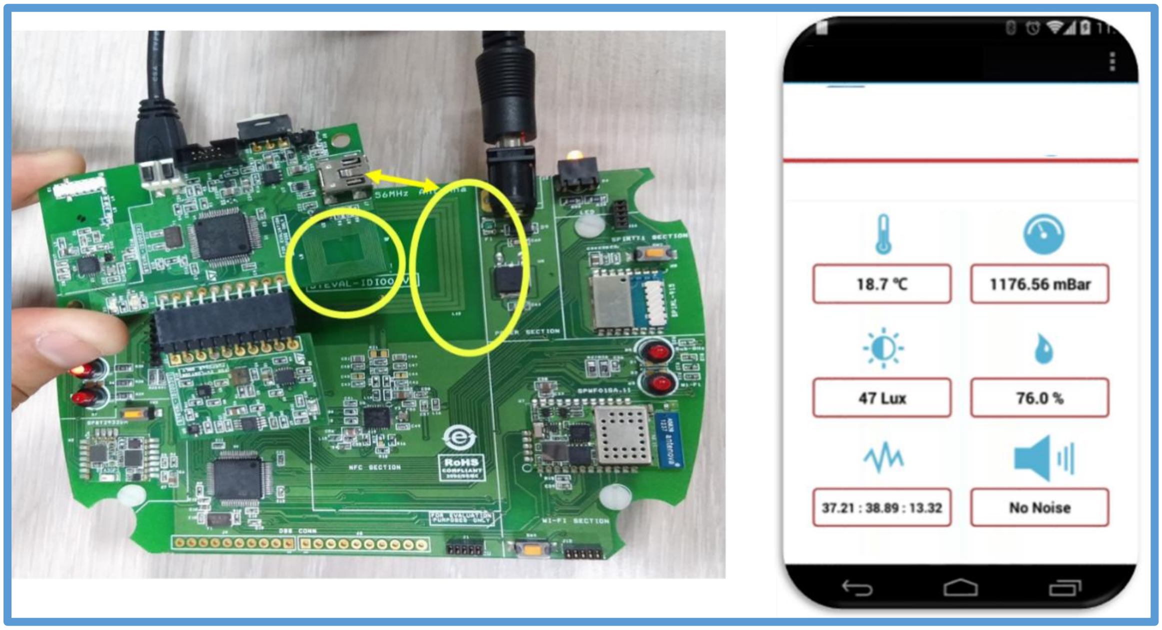
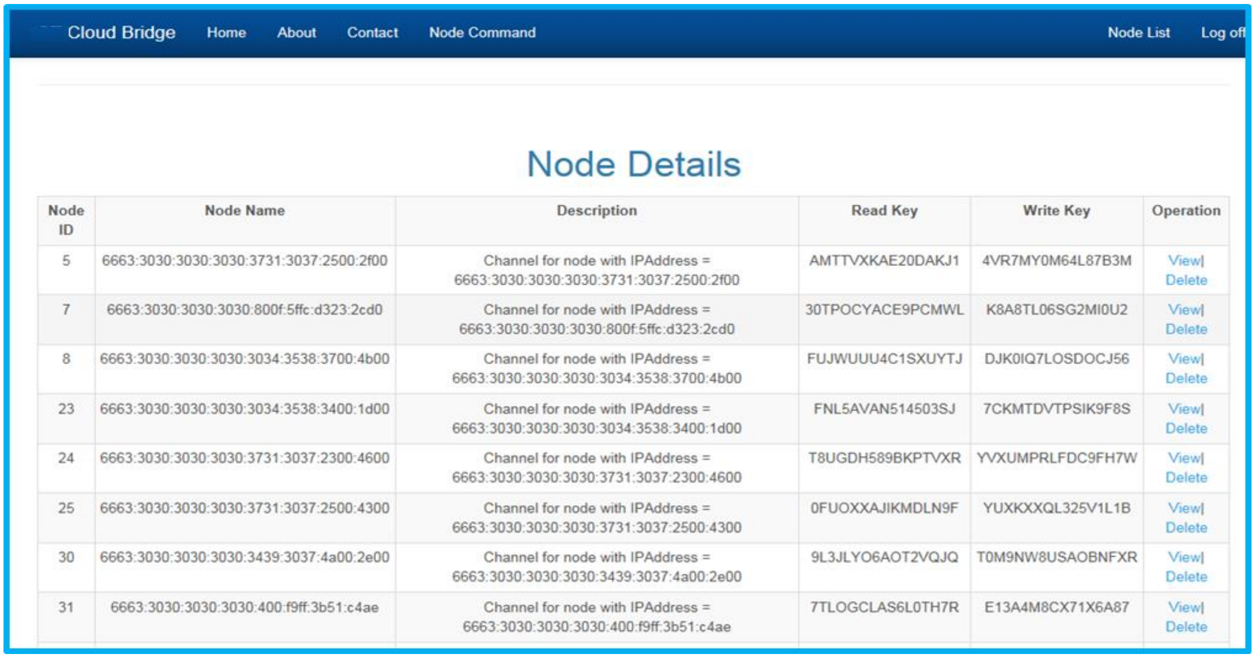


Fig ANNEX1.6: NFC Communication

Cloud Application: User can register sensors node on cloud server and can view the sensor data and control actuators using the cloud application.



Cloud Bridge | Home | About | Contact | Node Command | Node List | Log off

Node Details

Node ID	Node Name	Description	Read Key	Write Key	Operation
5	6663:3030:3030:3030:3731:3037:2500:2f00	Channel for node with IPAddress = 6663:3030:3030:3030:3731:3037:2500:2f00	AMTTVXKAE20DAKJ1	4VR7MY0M64L87B3M	View| Delete
7	6663:3030:3030:3030:800f:5ffc:d323:2cd0	Channel for node with IPAddress = 6663:3030:3030:3030:800f:5ffc:d323:2cd0	30TPOCYACE9PCMWL	K8A8TL06SG2MI0U2	View| Delete
8	6663:3030:3030:3030:3034:3538:3700:4b00	Channel for node with IPAddress = 6663:3030:3030:3030:3034:3538:3700:4b00	FUJWUUU4C1SXUYTJ	DJK0IQ7LOSDOCJ56	View| Delete
23	6663:3030:3030:3030:3034:3538:3400:1d00	Channel for node with IPAddress = 6663:3030:3030:3030:3034:3538:3400:1d00	FNL5AVAN514503SJ	7CKMTDVTPSIK9F8S	View| Delete
24	6663:3030:3030:3030:3731:3037:2300:4600	Channel for node with IPAddress = 6663:3030:3030:3030:3731:3037:2300:4600	T8UGDH589BKPTVXR	YVXUMPRLFDC9FH7W	View| Delete
25	6663:3030:3030:3030:3731:3037:2500:4300	Channel for node with IPAddress = 6663:3030:3030:3030:3731:3037:2500:4300	0FUOXXAJIKMDLN9F	YUXKXXQL325V1L1B	View| Delete
30	6663:3030:3030:3030:3439:3037:4a00:2e00	Channel for node with IPAddress = 6663:3030:3030:3030:3439:3037:4a00:2e00	9L3JLYO6AOT2VQJQ	T0M9NW8USAOBNFXR	View| Delete
31	6663:3030:3030:3030:400:f9ff:3b51:c4ae	Channel for node with IPAddress = 6663:3030:3030:3030:400:f9ff:3b51:c4ae	7TLOGCLAS6L0TH7R	E13A4M8CX71X6A87	View| Delete

Fig ANNEX1.7: Node details on cloud

Conclusion and extending the concept to include more communication technologies

In this gateway it is possible to have sensors connected to the cloud that can communicate using Bluetooth, Wi-Fi, Sub-GHz and NFC etc.. This concept is generic and can be extended to any of different wireless and wireline standards. The architecture is based on a Microcontroller Platform. Likewise an MPU based platform can be designed with operating system ported as well using the same approach.

High quality open source mesh networking stacks such as Contiki has helped the proliferation of IoT. Security still remains a challenging subject to be explored. The existing security techniques are holding well, but as IoT networks become more prevalent we would unearth more challenges. Advances in the semiconductor manufacturing process, decreasing cost and better power management along with energy harvesting would be another gate opener in IoT space.

Wireless bridge with multiple sensing nodes and lighting control for Home Automation Scenario is in continuous operation at STMicroelectronics India at its “Da Vinci” Gallery, a dedicated IoT Experience Centre for Smart Homes and Smart Cities. In conjunction with 6LoWPAN implementation of Wireless Bridge an integration between PLC and RF is also in permanent operation at this place where Lighting, Metering and Monitoring are in operation using wireless or wireline or a combination of the two. In this last scenario one of the PLC nodes acts as the router for the wireless nodes.

ANNEXURE 2 : NB-IoT Based Use Case

Source: Huawei, India

ANN2.1: Smart Parking

The live trial of NB-IoT is composed of the end-to-end infrastructure based on Etisalat live network as well as smart parking sensors deployment at Abu Dhabi as well Dubai, UAE. Smart Parking is one of the most important part of smart City verticals and will bring triple benefits for consumers, service providers and mobile operators, through efficient business and personal life management. In the coming years, Etisalat will explore more LPWAN verticals powered by NB-IoT – from Smart Water Meters to Smart Parking to Smart Tracking to more vertical industries, and thus bringing Etisalat more capabilities to fulfill the requirements of Smart City. The new technology, called Narrow Band Internet of Things (NB-IoT) is the proposed 4.5G standard technology that brings considerable advantages to mobile operators building their LPWAN networks when it comes to deployment, operation and re-usability of existing processes, IT and infrastructure assets. [A2.1]

Vodafone in collaboration with Fangle and Ublox, conducted trial in Vodafone Plaza in Madrid and covered various indoor parking spots. Smart Parking will allow users to access parking data remotely, from mobile application, including checking parking spot availability, navigating to the available spots, etc. In addition, the solution will create new revenue streams for municipal management, lower public parking running costs, as well as helping to alleviate traffic congestion. Having jointly developed the NB-IoT technology and driven the ecosystem establishment, Huawei and Vodafone are working closely to achieve the standardization in June as well as the pre-commercial phrase by the end of the year. Another smart parking live trail is scheduled to take place in Turkey in early June. NB-IoT Smart Parking may be commercially launched in 2017. [A2.3]

ANN2.2: Standardized NB-IoT on a live commercial network

Vodafone and Huawei have completed the first over-the-air connection on a live network using standardized NB-IoT. The commercial trial took place in Madrid, Spain. The engineers used a live 4G base station that supports NB-IoT technology. The connection was made using the 800 MHz licensed spectrum frequency band. The test is the last important milestone before the commercial launch of NB-IoT in 2017. [A2.2]

ANN2.3: NB-IoT smart water metering solution

MTN and Huawei jointly launched the Smart Water Metering solution, the first Narrowband Internet of Things (NB-IoT) solution in Africa. The solution is designed to help MTN develop their NB-IoT services to explore new markets. The Smart Water metering solution enables the automated collection of utility meter data, while manual meter reading leads to high labor costs and missing or inaccurate data. Through sensors installed in water meters, customers can identify water pipeline leakage earlier. Household water meters will automatically report data on a regular basis, reducing fault probabilities and the operating expense. Powered by the NB-IoT technology by Huawei, the sensor array is designed to serve as a diagnostic spine that underpins network management. The data gathered can be used to control waste water flows from each property, identify faults across the network and improve health and safety outcomes. The Smart Water Metering service from MTN will be commercially deployed in 2017. [A2.4]

ANN2.4: Smart Electrical Energy Meter Based on NB-IOT

Huawei and Janz CE have designed and manufactured the new meter, using modules from u-blox, and EDP Distribuição and NOS. To this end, NOS deployed the entire 4.5G NB-loT network based on Huawei infrastructure that supports the project, making it the first operator in Portugal and one of the first in the world to use the standardized version of this technology. This solution implements new market focused Smart Grid services using the latest generation (4.5G) communications networks, answering Horizon 2020 programme challenges set by the European Union through the UPGRID project. NB-IoT has emerged as the Low Power Wide Area (LPWA) wireless access technology, standardized by the 3GPP, which offers a wide range of advantages, among which are the support of more than 100,000 connections per cell, a battery life of up to 10 years and a gain of 20dB over conventional GSM networks. Additionally, NB-IoT provides reliable and secure connectivity by the use of licensed spectrum and 4G ciphering. NB-IoT technology thus has the potential to improve the automation of processes, reduce costs, increase security and provide a better service to final consumers by introducing innovative services that add value. The Parque das Nações area in Lisbon was chosen by EDP Distribuição to pilot the project among 100 customers, beginning this year and continuing until the end of 2017. This area of the city is already served by two NOS base stations which provide 3GPP standardised NB-IoT coverage. Intelligent energy management in the homes of these customers, will also play an active role in helping to improve their energy cost efficiency, and is just the first example of the use of this technology. [A2.5]

Fig ANNEX2.1: Energy Meter [A2.5]

ANN2.5 : Business commitments for NB-IoT

Around 20 operators have committed NB-IoT deployments in 2017. Wide range of use cases have been selected for trials. [A2.6]

As per GSA [A2.6], “2017 will be the year in which LTE-IoT will be deployed, at scale, around the world and where the might of the 3GPP ecosystem will drive commercialization, with mobile operators, infrastructure suppliers, chipsets and module manufacturers, device companies and, development & testing house supporting new services. This hastening activity will support an active and competing ecosystem to realize the vast potential of the LTE-IoT market”.

Operators such as Verizon, AT&T, Vodafone, T-Mobile, Telstra, Softbank, Korea Telecom, LG Uplus, China Telecom, China Unicom and Telia are rolling out commercial deployments in the US, Europe and Asia in 2017.

Infrastructure, chipsets, modules and devices will be available from a range of companies, large and small, well established and start-ups, who are all active in the LTE-IoT market. These companies include stalwarts of the wireless infrastructure industry such as Ericsson, Huawei, and Nokia as well as established silicon companies Intel and Qualcomm. In Europe and Asia, NB-IoT deployment for IoT are in progress.

References:

[A2.1] Etisalat & Huawei Launches the First NB-IoT trial of Smart Parking in the Middle East, http://www.huawei.com/en/news/2016/3/the-First-NB-IoT-trial-of-Smart-Parking

[A2.2] Vodafone completes the world’s first trial of standardised NB-IoT on a live commercial network, http://www.vodafone.com/content/index/what/technology-blog/nbiot-commercial.html

[A2.3] Huawei and Vodafone collaborate with NB-IoT industry partners for Smart Parking pilots in Spain and Turkey, http://www.huawei.com/en/news/2016/6/NB-IoT-industry-partners-for-Smart-Parking-pilots

[A2.4] MTN and Huawei Launched the first NB-IoT solution in Africa, http://www.huawei.com/en/news/2016/11/Huawei-MTN-first-NB-IoT-solution-Africa

[A2.5] Huawei and Janz CE Announce the First Smart Electrical Energy Meter Based on NB-IOT, http://www.huawei.com/en/news/2016/11/First-Smart-Electrical-Energy-Meter-NB-IOT

[A2.6] The Evolution to Narrow Band Internet of Things, GSA Paper dated Feb 2017

ANNEXURE 3 : Flood Alert System using LoRa network

Source: VIT Chennai, India

The proposed system is to alert the people who are staying nearby water bodies before getting affected by flood by measuring the rise and fall of water level in the water bodies by communicating data to the server. LoRa WAN technology has been proposed to communicate to other nodes. The model was demonstrated by taking in factors like weather forecasting.

Introduction

Flood happens less often but when they do occur they tend to be hazardous. Predicting the weather has always been a challenging field of research with a very slow progress rate over years. Advancement in the field of technology providing a platform for weather prediction research. Various weather forecasting techniques are developed recently all the approaches will be based on the mathematical model, statistical analysis to provide proper data to predict the weather conditions. Earlier proposed methods were highly dependent on the training data and some rules used for modelling the system. The performance, efficiency, power consumption are the parameters which are generic to all the methods, care should be taken to achieve optimization. Statistical methods are generic nature makes them efficient in terms of deployment, complexity and performance. Flood control systems are implemented for the water bodies to provide caution. The causes for flooding are deforestation, steep slopes, hard dry soil, heavy rainfall, marshy areas wet soil. Heavy rain fall is the main cause for dynamic rise of water in water bodies. Developing a flood warning system demands attention to three essential factors: Data gathering, data processing, and the hardware and software required, and to propagate flood warning information.

THE PROPOSED WORK

The proposed model is especially meant to measure dynamic rise in the water level in water bodies. Water level sensors are deployed in an artificial prepared water body to measure dynamic flow of water. Velocities, depth, width of the water body are predetermined to understand complete analysis of real system model. Stream flow measurement will play an important role when we come to the dam where water is deposited by rivers. Data sensed by the sensors passed to node deployed using a NUCLEO- L152RE which is attached to LoRa SX1276 shield Structure of the IoT is fully pledged to have better working of the model and make the data transmission to the server with added security.

The entire model is interfaced to a LabVIEW based setup which acts on a data flow model. The VI (Virtual Information system) will read the data from the nodes and the information is plotted in an GUI based Interface. Using inbuilt sound systems of LabVIEW alert may be provided to the control station which will be located near water bodies few hours/days before by doing all the analysis of the present and previous data.

IMPLEMENTATION

The following figure depicts the entire setup of the proposed work which includes LabVIEW, LoRaWAN, NUCLEO-L152RE and sensors. The sensor is dipped in artificial tank to show the demo, sensed data from sensors given to Nucleo-L-152RE microcontroller. NUCLEO-L152RE microcontroller attached to LoRa SX1276 mbed shield using base shield to provide connectivity. The encrypted data from the LoRa is stored in the cloud. The data may be taken from the cloud for further study. The decryption is applied on the encrypted data in order to make it understandable to the user. In the figure we can see that LabVIEW platform to show the height of the water in the tank and decision will be made depending on the level of water, it will show a pop up message to indicate the safe zone and danger zones of the levels. This model depicts the working of a flood alert system.

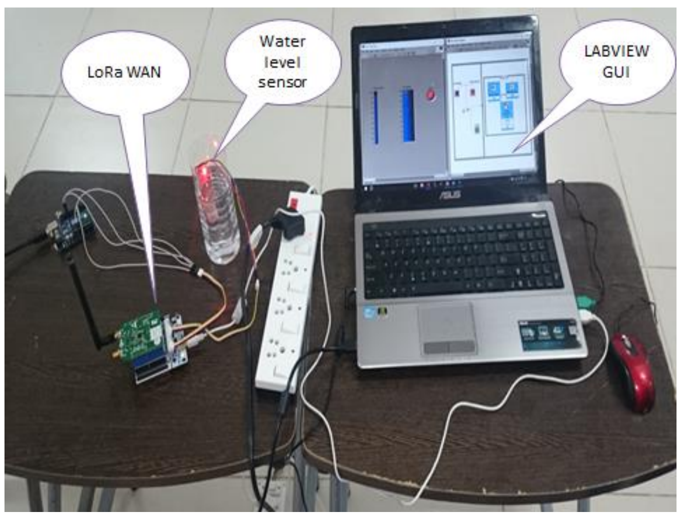


Fig ANNEX3.1: Setup of the proposed model

Model will measure dynamic rise of water level in rainy time if it is brought to real environment.

RESULTS AND DISCUSSION

Data obtained from the LoRa radio model is transmitted to the server which is stored in the encrypted form. The setup is able to provide an automated alert system and also predicts the future course of action in case of flood. The data is updated to the cloud using TATA communication server and retrieved for the analysis and research purpose.

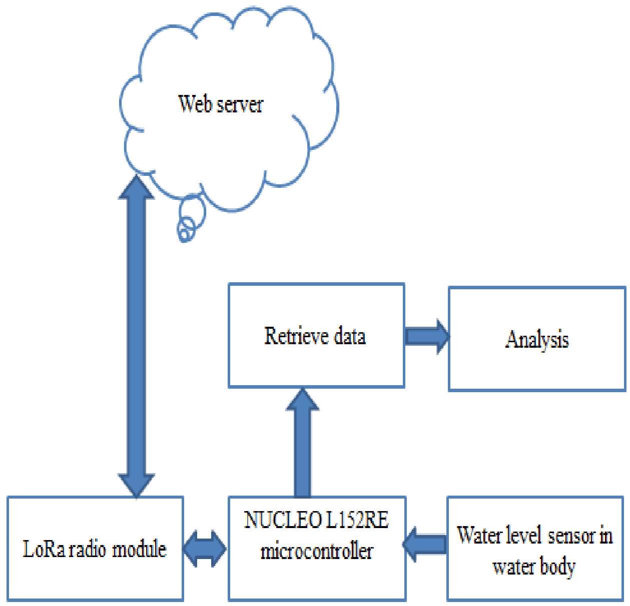


Fig ANNEX3.2: Block diagram of the proposed model

Conclusion and future work

The purpose of this project is to design and test the flood alert system in the lab scenario using a table top model. In the real world scenario there may be more factors that have to be taken into account like flood stream. LoRa has been used as a communication technology to transmit the alert. Range of LoRa has been taken as 10-12 Km (in open areas) for this project. The output obtained in phase 1 is as expected. The system can be made more accurate by adding Artificial Intelligence.

Future work: The proposed entire system can be brought to real environment using some sophisticated tools, which makes more efficient real time module for the marketing purpose. Some more key features of LoRaWAN should be deployed in the work to overcome loss of information during transmission.

References

N. M. Z. Hashim, N. B. Hamdan, Z. Zakaria, R. A. Hamzah, A. Salleh5, “Flood Detector Emergency Warning System”, International Journal Of Engineering And Computer Science ISSN:2319-7242, Melaka Malaysia.

ANNEXURE 4 : Smart Street Lights Solution using LoRa Network

Source: TechMahindra, India

Smart Street Lights targets the public illumination system to allow a better and efficient way to handle complex and vital elements of every area by providing:

- Optimizing the electricity usage
- Ensuring the uptime of the lights in the city
- Easy and speedy rectification of faulty light points
- Real time inventory management & prediction

A smart street light solution involves following components

- LoRa® enabled Luminaire controller with LED lights
- LoRa® Gateway
- Network Management Servers and Platforms
- Smart Street Light Application

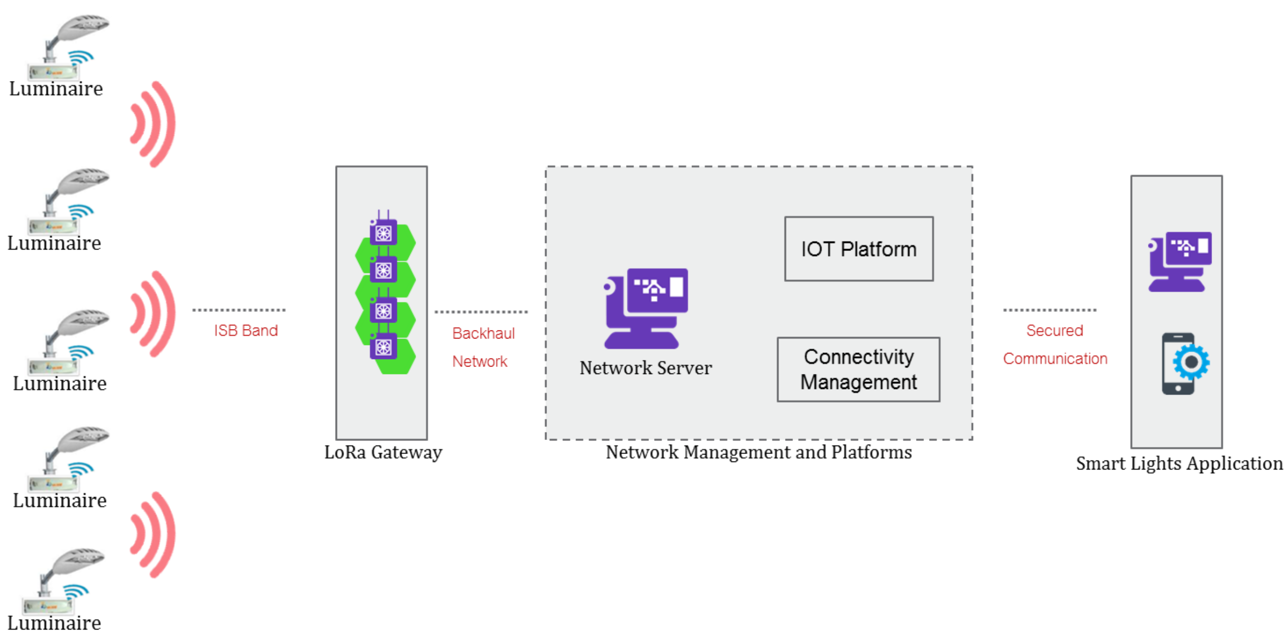


Fig ANNEX4.1: High Level architecture of Smart Street Lights Solution

A luminaire controller is individually registered as described in the above sections of the document. The controller sends data payload such as energy parameters at scheduled frequency to the LoRa gateway. The LoRa® gateway communicates to the Network management servers via backhaul network (3G, Ethernet etc.). The network server pushes the data to registered Smart Lights application and IoT platforms. The information about Street Lights performance is recorded in the Smart Street Lights application which can be reviewed by authorized users.

Smart Street Light Application helps to receive various inputs from Luminaires such as energy parameters, environmental conditions. The application can also send commands from remote location to switch on/off and dim the luminaire. Tech Mahindra’s application runs various analytical algorithms and reports to save energy and help in easy and speedy rectification of lights in case of failure.

The STM32 NUCLEO pack for LoRa™ technology and high-performance FSK/OOK RF transceiver modem (P-NUCLEO-LRWAN1) combined with the LoRaWAN software expansion package for STM32Cube (I-CUBE-LRWAN) is the quickest way to build a LoRaWAN end-node device.

ANNEXURE 5 : Smart Street Lighting solution based on 6LowPAN

Source: STMicroelectronics, India

Solar Smart Street Lighting Solution: This use case describes the Solar Smart Street Light solution proof of concept installed in the premise of STMicroelectronics. There are more than 35 light nodes installed in the parking area controlled by a Data Concentrator Unit that further talks to Cloud Platform. The wireless communication between the lights nodes and DCU is based on 6LoWPAN mesh technology that works at 868 MHz frequency. The communication network is mesh so that any node can talk to DCU through another node. The below diagram shows the pictorial representation.

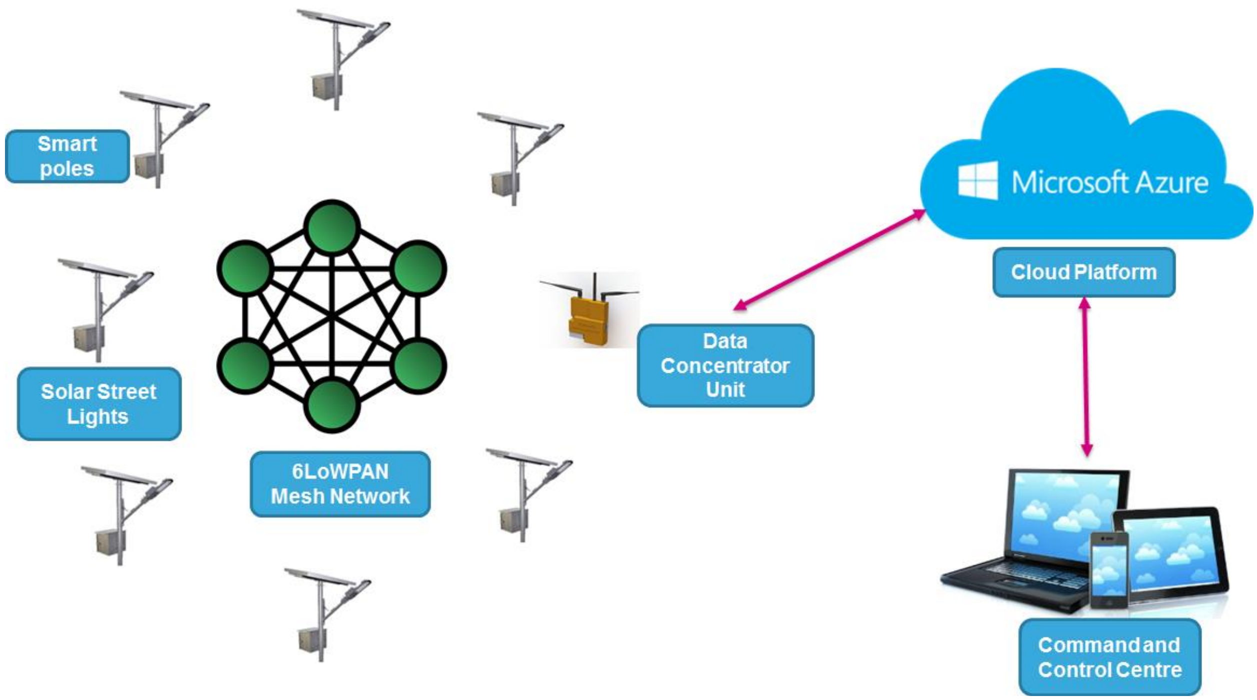


Fig ANNEX5.1: Smart Hybrid Solar Street Lighting System Architecture

The communication between DCU and Cloud Platform is on 3G. The Cloud Platform allows the user to switch on / off and dim individual lights or group of lights on the click of the button. The user can also issue time based commands through the Cloud Platform. The figure above shows the basic architecture of the use case. The Cloud platform also stores the different electrical parameters for each light nodes which can be used for data analysis.

The system is designed such that the battery gets charged with the help of the solar panel in the day time and during the night time, the light nodes consumes power from the battery. In case the battery is not able to support the power supply to the light nodes, the light nodes fall back on the main supply.

The other features of the system are:

- Monitoring, status and health check reporting/Diagnostics
- Intensity control to reduce power consumption
- Solar Battery Charger with MPPT
- Quasi-resonant driver for mains operation
- Interleaved boost based LED driver
- PIR and other sensors for added smartness
- All protections like Panel Reverse/LED Open-Short

life.augmented

6LoWPAN based Street Light Solution

Node Name	IPv6 Address	Batt Volt (V)	Panel Volt (V)	RSSI (dB)	Switching Request	Node Status
P06	aaaa::3338:3138:7b34:780c	11.8	11.2	-87	Turn Off Light	On Battery
Unknown	aaaa::3338:3138:7e34:790c	11.9	11.4	-87	Turn Off Light	On Battery
Unknown	aaaa::3338:3138:7834:820c	11.9	11.3	-87	Turn Off Light	On Battery
P15	aaaa::3b37:3138:5634:8715	11.7	11.2	-86	Turn Off Light	On Battery
P18	aaaa::3338:3138:7734:830c	12	11.4	-77	Turn Off Light	On Battery
Unknown	aaaa::3338:3138:7b34:6f0c	11.8	11.2	-74	Turn Off Light	On Battery
P24	aaaa::3730:3137:6c33:8719					Node Missing
P14	aaaa::3b37:3138:5534:7015	12	11.4	-91	Turn Off Light	On Battery
P25	aaaa::3b37:3138:5534:7c15					Node Missing
P17	aaaa::3338:3138:7734:850c	12	11.4	-91	Turn Off Light	On Battery
Unknown	aaaa::3338:3138:7634:770c	11.9	11.4	-85	Turn Off Light	On Battery
P26	aaaa::3b37:3138:5234:7715					Node Missing
P10	aaaa::3b37:3138:5434:6715	12.1	11.5	-77	Turn Off Light	On Battery
P20	aaaa::3b37:3138:5134:6815	12.1	11.5	-90	Turn Off Light	On Battery
P08	aaaa::3b37:3138:5534:7e15	11.7	11.2	-74	Turn Off Light	On Battery
Unknown	aaaa::3338:3138:7734:730c	11.9	11.3	-77	Turn Off Light	On Battery

Fig ANNEX5.2: Data on Cloud, Metering and Control Possibilities

Fig ANNEX5.3: Implementation in the field, STMicroelectronics Parking at Greater Noida, INDIA

ANNEXURE 6 : Smart metering in advanced metering infrastructure (AMI).

Source: Landis & Gyr, India

Objective

The document explains the typical use case of how smart meters establish a two-way communication with their Head End Systems in Advance Metering Infrastructure (AMI). It primarily focuses on RF communication part of smart meters rather than electricity measuring part.

Disclaimer

The document contains the conceptual software architecture of a smart meter in the AMI network. It is not intended to give any specific detail whatsoever about the products of Landis+Gyr being delivered to its customers.

Acronyms

AMI: Advanced Metering Infrastructure

HES: Head End System

TSCH: Time Slotted Channel Hopping

DODAG: Destination Oriented Directed Acyclic Graph

DLMS: Device Language Message Specification

PANA: Protocol for Carrying Authentication for Network Access

AES: Advanced Encryption Standards

RF: Radio Frequency

Standards Applicable for the Use Case

- IEEE 802.15.4 TSCH MAC
- IEEE 802.15.4 SUN FSK PHY
- RFC 6550 (IPv6 Routing Protocol for Low-Power and Lossy Networks)
- IEC 62056 (DLMS/COSEM Standard)
- RFC 768 (User Datagram Protocol)
- RFC 2460 (Internet Protocol IPv6)

- RFC 5191 (PANA - Protocol for Carrying Authentication for Network Access)

Smart Meter Architecture

The smart meter performs primarily two functions. One is measurement of electricity that is consumed by the load (appliances) connected to the meter and other function is establishing the real-time communication with its controlling systems called HES (Head End System) for receiving various commands and sending response for them. These two logical functions are shown in *Fig ANNEX6.1* below. The figure assumes these two functions run on two separate hardware, but based on the product design they may run on the same hardware as well. From technical representation standpoint, measurement and communication are two different functions performed by the smart meter.

The communication module reads the measurement data from the measurement unit connected via Serial link and transmits it to the central server called HES (Head End System). The communication module hardware comprises of components like RF chipset which transmits/receives data to/from network, a flash memory which may contain the device configuration information, a microcontroller to execute the programming instructions and other necessary components for hardware circuitry to function correctly. Real Time Operating System (RTOS) is the operating system software, which allows various tasks running on the device to perform actions based on priority and in real-time. The RF Communication stack is explained in the separate section in the document. DLMS Client is the software that establishes the secure communication with the measuring device i.e. the meter. DLMS client communicates with corresponding counterpart that runs in the meter i.e. DLMS server to read the data like billing, load profile, meter tamper events etc. from the meter.

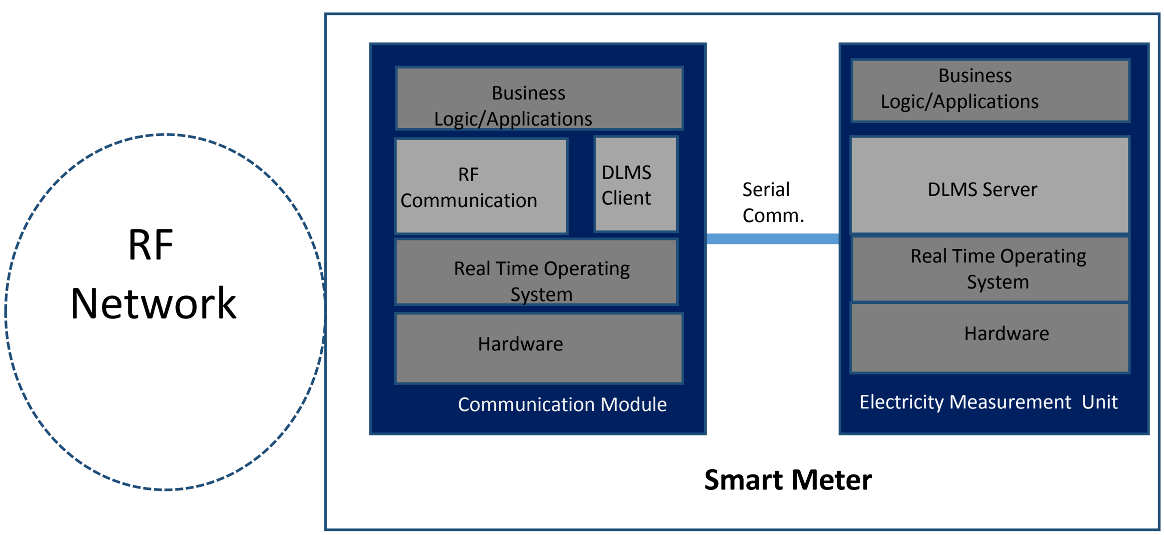


Fig ANNEX6.1: Smart Meter Logical Representation

The measurement unit has hardware components like LCD display to show the required information to the user, a microcontroller, flash memory to store the events and profiling information. It may also have operating system depending on the software architecture in the metering device. DLMS server software establishes communication with the DLMS client as explained above. It does not have any RF communication hardware.

The combined circuitry of measurement unit and communication module is referred as "Smart Meter".

AMI Network Architecture

The smart meters communicate with each other over RF link as shown in *Fig ANNEX6.2*. All packets generated by the smart meters are destined to the collector, which collects the packets from various nodes and send it to the Head End System (HES). HES presents a GUI interface to the Utility user and shows all the nodes connected to the network and information like what data has come from which smart meter deployed in the field network and others. The RF communication stack running on the communication module forms the mesh network by establishing the communication with its neighboring nodes in the network. The details of RF Communication Stack are given in the next section.

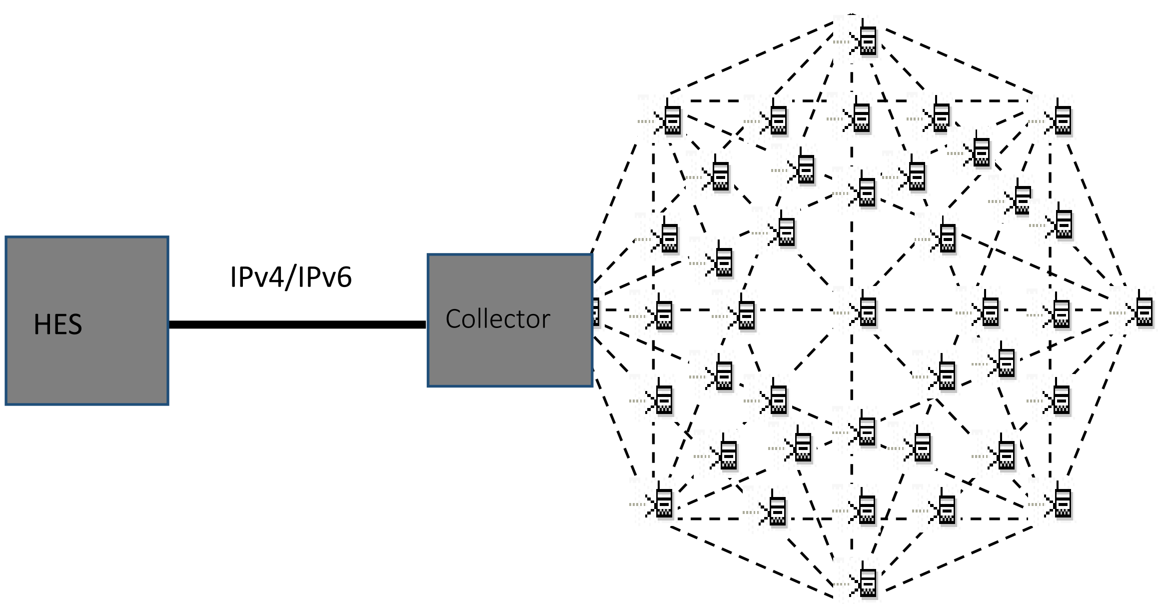


Fig ANNEX6.2: RF Mesh Network of Smart Meters

The connectivity between Collector and HES system may be based on wired/wireless network like fixed line broad band / optical fiber communication /cellular network with static IP (IPv6 or dual stack) depending on actual deployment considerations.

RF Communication Stack

The RF Communication stack is a software that runs on communication modules and consists of implementation as per the various IETF and IEEE Standards. As shown in *Fig ANNEX6.3* below, the layers have been mapped with corresponding layers of OSI reference model.

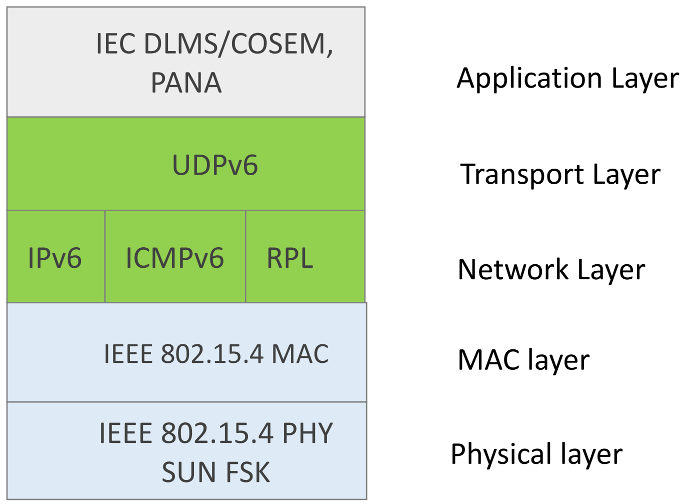


Fig ANNEX6.3: RF Communication Stack

The PHY and MAC layers are based on IEEE Standard 802.15.4. It uses FSK (Frequency Shit Keying) modulation scheme and allows to send the data at different data rates that are 50 kbps, 100 kbps, 150 kbps and 200 kbps. It uses the country specific spectrum i.e. 865-867 MHz for India and 902-928 MHz for US. The MAC layer forms a mesh network where nodes are reachable by multiple neighboring nodes and uses TSCH (Time Slotted Channel Hopping) mechanism to transmit data to its neighboring nodes.

Each node in the network is assigned an IPv6 address and implements the RPL (Routing over low power lossy networks) protocol for forming the DODAG (Destination Oriented Directed Acyclic Graph) network over the RF link. In the DODAG network, each node sends the data to the same destination that is Collector unit as shown in the *Fig ANNEX6.1*. The Collector acts as a PAN (Personal Area Network) coordinator and manage the entire network of nodes under its purview. UDP (User Datagram Protocol) allows application layer to use the network stack services for transmission and reception of packets using sockets and port numbers.

The Application layer provides services like sending the registration information to the HES, which authenticates the meter registration request and if authenticated successfully, confirms its registration to the meter, it then becomes a legitimate component of the network, and various functional scenarios can then be realized.

For security measures, PANA/EAP-PSK protocols are used to ensure the authentication of devices that are willing joining the network. PANA (Protocol for Carrying Authentication for Network Access) is an IP-based protocol that allows a device to authenticate itself with a network before it is granted access. EAP-PSK (A Pre-Shared Key Extensible Authentication Protocol) uses a pre-shared key mechanism using which both HES and device (smart meter or network router) mutually authenticate to each other before becoming part of network. The devices also implement AES cryptography algorithms to encrypt the packets before transmission and receiving device decrypt them upon reception using appropriate security keys. In case, any device fails to authenticate itself to the network, corresponding alarm event is sent to the HES for appropriate actions.

The IEC DLMS protocol is used for communication between RF communication module and electricity meter. Using this protocol, the communication module establishes the secure connection with the meters and reads the required information.

Some of application scenarios are sending of different smart meter events (like alarm, tamper events), timing synchronization of meter with network time, power outage and restoration, remote connect and disconnect, Over-The-Air (OTA) firmware download and others. OTA functionality allows the HES to upgrade the firmware of any node using RF interface.

ANNEXURE 7 : Advanced Metering Infrastructure (AMI) pilots using 6LoWPAN

Source: Reliance Infrastructure Ltd, India

Advanced metering infrastructure (AMI) refers to a system of technologies that measure, collect, communicate, aggregate, and analyze energy usage data from metering devices. AMI system is used for remote smart meter data collection, dynamic tariff, interval metering for energy audit, theft detection, outage detection, remote connect/disconnect, web portal for residential and industrial consumers, prepaid metering, meter-to-home for In-home display.

Smart Meter measurements and other data are transmitted by wireless radio from the meter to a collection point. The data is then delivered by various methods to the utility data systems for processing at a central location. The utility billing, outage management, and other systems use the data for operational purposes. The smart meters talk to each other (hop) to form a LAN cloud to a gateway. The gateway transmits the data using various WAN methods to the utility central location. Key benefits in implementing 6LoWPAN IPv6 are

- Open standards
- Light weight
- Versatile
- Scalable
- Manageability
- Security
- Interoperable

The system is based on the 6LoWPAN initiative founded by an IETF working group dedicated to pushing IPv6 over Low power Wireless Personal Area Networks under the idea that “the Internet Protocol could and should be applied even to the smallest devices.”

Architecture

The *Fig ANNEX7.1* illustrates the solutions architecture. The architecture follows a 3-tier model with one Server application, some Gateway Terminals and many Mesh Terminals.

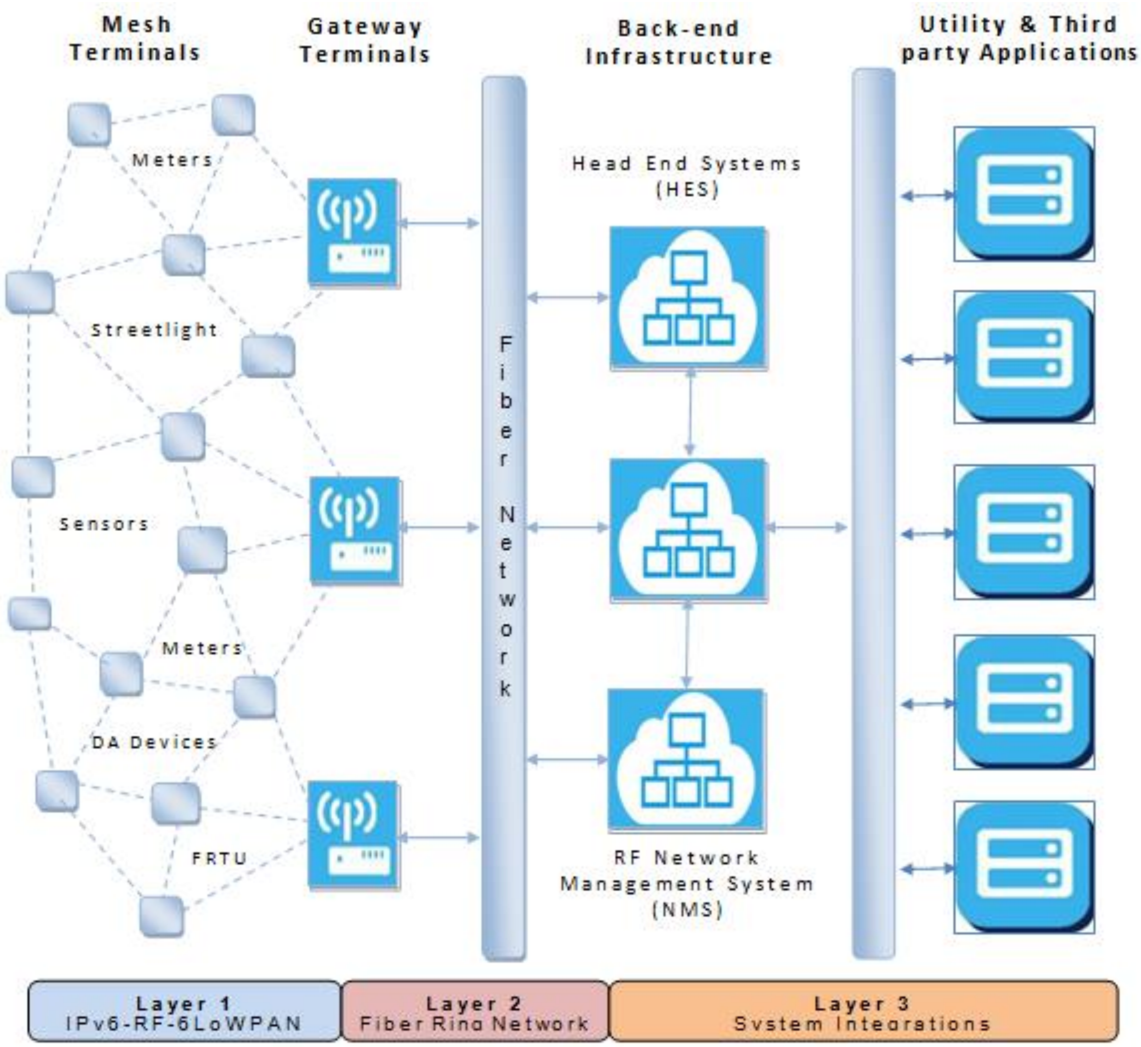


Fig ANNEX7.1: AMI Architecture with 6LoWPAN

Back-end Infrastructure: The Server is an open modular platform which provides Device Management, Topology management, Firmware Management, SLAs monitoring, security management and DNS support. Topology management includes the maintenance of the topology map across all mesh networks, the ability for devices to switch to another mesh network, the IP routing to all devices or the transport of IPv6 traffic directly over an IPv6 backbone or over an IPv4 tunnel.

Gateway Terminal: A radio mesh network contains only one Gateway Terminal, although the individual mesh terminals may migrate between networks as conditions change. A Gateway Terminal identifies the embedded firmware running in devices with the ability to forward traffic from a radio mesh network to the Internet and from the Internet to a radio mesh network. A Gateway Terminal acts as a gateway between a radio mesh network and the Internet enabled backhaul connection (cellular link, Ethernet to fiber connection, etc.). An IPv6 prefix is assigned to each Gateway Terminal which manages its own radio mesh network or 6LoWPAN over RPL.

Mesh Terminal: A Mesh Terminal identifies the embedded firmware running in all devices only equipped to join a radio mesh network. A set of radio Mesh Terminals dynamically maintains the mesh topology using RPL to provide connectivity to the Gateway Terminal and the Internet for all devices in this radio mesh network.

Services offered

Management service: The Management Service regroups all features within the scope of device management, topology management, Over-The-Air-Provisioning, SLAs monitoring etc. The Security Service regroups all features within the scope of mutual authentication between the Smart Meters and the Server, the encryption of any sensitive over-the-air transaction (Meter readings, firmware update, etc.) as well as the initial provisioning of the necessary security credentials, the revocation of certificates, cipher suite upgrades, key store management, secure boot, code signing, etc.

Communication service: The Communication Service regroups all features within the scope of communication over a radio mesh network as well as the communication over a cellular or other network. Each Terminal runs a standard IPv6/6LoWPAN stack and all applications within a Terminal are built on top of COAP and EXI.

Application Service (HES): Applications service such as Smart Metering Service regroups all features specific to a Smart Metering deployment such as the collection of meter readings pushed from Terminals to the Server at periodic intervals, or the on-demand request from the Server for on-demand readings, etc.

AMI Pilots of near about 2500 units has been deployed in Mumbai and Delhi with 99.5% success rate. These are first successfully demonstrated pilots deployed in India on Low Power RF viz. 6LoWPAN technology based on IPv6 to deliver data collection, transactions execution and connectivity success rate. WAN radio has been used to connect the AMI network with back-end servers including cellular 3G and fiber connectivity.

Head-end System is deployed in cloud which could handle millions of transaction with AMI network on real time basis with lowest latency and highest reliability.

The Low Power RF communications chip and firmware are built on

- Open standards like 802.15.4.g
- 6LoWPAN (IPv6 connectivity)
- CoAP
- DTLS
- RPL
- Auto Registration
- Device Management like provisioning, monitoring, events, ping and trace.
- Remote firmware upgrade & configuration, time sync

This RF communications technology operates in the free unlicensed band 865-867MHz. RF network is self-healing; self-configuring and does real-time management of Smart devices like smart meters, smart sensors and smart network equipment.

RF 6LoWPAN based on IPv6 network can be deployed across distribution area to enable one network multiple applications deployment.

Power Sector:

1. Smart Metering & AMI
   a. Single & Three Phase customer meters (Existing and Smart)
   b. Network meters
   c. Pre-paid & Net meters
2. Distribution Automation –
   a. 11KV RMU monitoring & control
   b. DT health monitoring, SS status monitoring, APFC monitoring
   c. LT Panel monitoring & control, Distribution LT Pillar monitoring & control
   d. FRTUs, FPIs,
3. Demand side management & Demand Response
4. Asset monitoring
5. Street Light management

Non-Power Sector:

1. Parking solutions
2. Sensors – Temperature, Humidity, Air quality (Pollution)
3. Home Automation

ANNEXURE 8 : Street Light Automation and Smart Living (using C-DOT CCSP)

Source: C-DOT, India.

Description

A street light automation service provider, provides services to control the luminosity of each street light dependent upon

Local (street level)
1. Light sensors
2. Power quality sensors
3. Proximity sensors (civilian or emergency vehicles, pedestrians)

Street light automation service provider operation center
4. Policies (regulatory & contractual)
5. Ambient light analytics (sunrise/sunset, weather, moonlight, etc.)
6. Predictive analytics (lights parts of streets predicted to be used, etc.)

Communications received from other service providers
7. Traffic light service (emergency vehicle priority)
8. Emergency services (vehicle routing, police action, etc.)
9. Road maintenance service (closures and/or diversions)
10. Electricity service (power overload)

A smart Living Service Provider provides services to control the Air conditioners or Heaters based on the temperature and humidity readings of the surrounding inside a building along with the presence or absence of persons in the respective areas. The electricity consumption is also measures in the same area and accordingly the supply to the lights and other electrical items are cut-off.

Source

oneM2M TR TR-0001-V3.0.0 Use Cases Collection

Actors

- Street light automation application service provider, has the aim is to adjust street light luminosity.
- Street light devices have the aim is to sense, report, execute local and remote policies, illuminate street.
- Traffic light application service provider, has the aim is to enhance their emergency vehicle service using street lighting.
- Emergency services application services provider, have the aim is to brightly illuminate police action areas and brightly illuminate planned path of emergency vehicles.
- Road maintenance application service provider, has the aim is to obtain extra street light signaling near closed roads.

- Electricity application service provider, has the aim is to have electricity consumers reduce their load when an overload is declared.
- Smart Living Service provider provides the automation of the A.C./Heater and power supply control

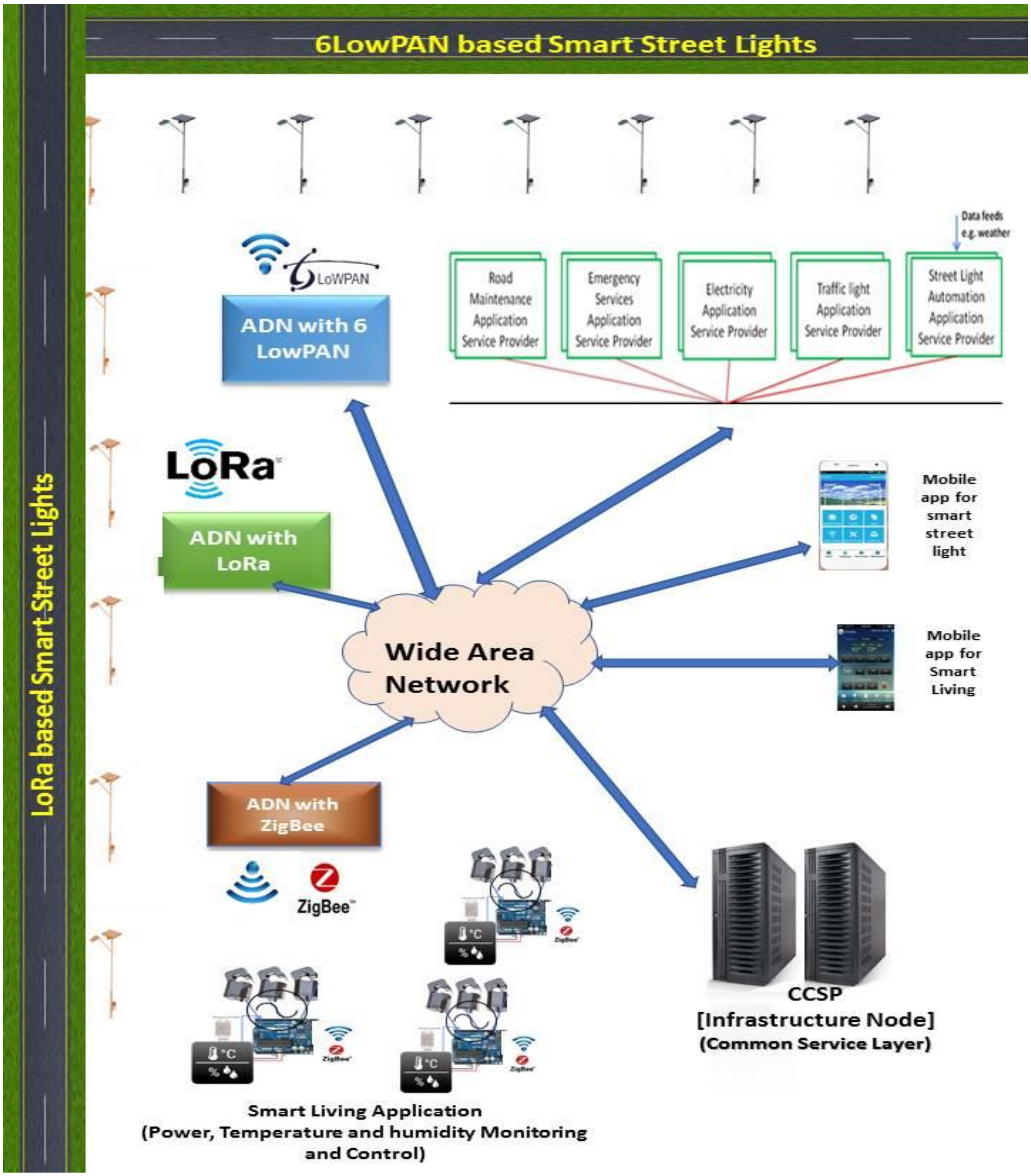


Fig ANNEX8.1: Smart Street Light and Smart Living Automation High Level Illustration

Communication Technologies

Between the Street light controller and the Common Service Gateway

- LoRa
- 6LowPAN

Between the Temperature and Humidity sensors and the current sensors to the Common Service Gateway

- ZigBee

Between the Street light automation service provider or the Smart Living operation center and the Infrastructure Node -

- GPRS
- 3G/4G
- GPON
- Wi-Fi etc.

Platform: C-DOT common service platform based on OneM2M specifications

Normal Flow

For Smart Street Light

1. **Sub use case 1** - Local: Light sensors

   Trigger: Local light sensors detect light levels when they move below/above threshold

   Action taken is to Increase/decrease luminosity in a set of street lights

2. **Sub use case 2** - Local: Light sensors

   Local: Power quality sensors detects input voltage level when it moves above/below threshold

   Action taken is to send alert message to electricity service provider and to decrease/increase energy applied to a set of street lights

3. **Sub use case 3** - Local: proximity sensors (Civilian or emergency vehicle or pedestrian detected entering/leaving street section)

   Action is to increase/decrease luminosity in a set of street lights

4. **Sub use case 4** - Operation center: Ambient light analytics (sunrise/sunset, weather, moonlight)

   A band of rain moves across an area of street lights

   Action is to increase/decrease luminosity in a rolling set of street lights

   Or Sunrise/sunset is predicted to occur area in 30 minutes

   Action is to decrease/increase luminosity in a rolling set of street lights

5. **Sub use case 5** - From other service providers: Traffic light service input (emergency vehicle priority like an emergency vehicle is approaching a junction)

   Action is to increase luminosity in street lights along streets leading away from junction

6. **Sub use case 6** - From other service providers: Road maintenance service input (closures and/or diversions)

   A road is closed **- Action is to** Program a changing luminosity pattern in street lights near to closed road

   Or A route diversion is activated - **Action is to** program a changing luminosity pattern in street lights along the streets of the diversion

7. **Sub use case 7** - From other service providers: Electricity service input (power overload)

   A power overload situation is declared

   Action is to decrease luminosity in a set of street lights

FOR SMART LIVING AND POWER CONTROL

1. The temperature and humidity sensors (DHT22) and the CTs send their respective readings periodically to the ADNs over ZigBee which in turn sends the aggregated Content Instances (readings) in the oneM2M compliant data model to the Infrastructure Node (CCSP) which sends the notifications to the respective command centre applications which have subscribed to the notifications on specific containers having the CIs. Subsequent actions are sent from the respective control/monitoring application either from the desktops or Mobile Apps to the IN which in-turn would notify the ADNs interfacing with the actuators controlling the power to the Air conditioners / Heaters/ Electricity Supply Switch

ANNEXURE 9 : Communication Technologies – related SDOs and certification details

Technology / Protocol	**Frequency band (s)**	**SDO / Forum / Alliances**	**Certification by**	**Related links**
Wireless				
Bluetooth / Bluetooth Low Energy	2.4 GHz	IEEE 15.1, Bluetooth Special Interest Group (SIG)	Bluetooth SIG	https://www.bluetooth.com/membership-working-groups/membership-types-levels https://www.bluetooth.org/apps/qualification/bqtf.aspx https://www.bluetooth.org/apps/qualification/bqe.aspx
NFC	13.56 MHz	ISO/IEC 14443 & ISO/IEC 18000-3	NFC Forum	http://nfc-forum.org/our-work/compliance/certification-program/labs-test-tools/authorized-test-labs/
Wi-Fi	2.4 GHz	IEEE 802.11	Wi-Fi Alliance	http://www.wi-fi.org/certification/authorized-test-laboratories
ZigBee	2.4 GHz, 920 MHz, 915 MHz, 868 MHz, 780 MHz	ZigBee Alliance	ZigBee Alliance	http://www.zigbee.org/zigbee-for-developers/zigbeecertified/

Z-Wave	Sub 1GHz for India (865-867 MHz)	Z-Wave Alliance	Z-wave Alliance	http://z-wavealliance.org/z-wave_plus_certification/
Wi-SUN	Sub 1GHz for India (865-867 MHz)	Wi-SUN Alliance	Wi-SUN Alliance	https://www.wi-sun.org/index.php/en/products/certification-program
ANT	2.4GHz	ANT Wireless (a division of Dynastream Innovations, in turn a wholly owned subsidiary of Garmin	ANT+ Product Certification	https://www.thisisant.com/developer/ant-plus/certification
Cellular (2G,3G,LTE,NB-IoT and 5G)	For India, 900 MHz, 1800 MHz, 2100 MHz and 2300 MHz is allocated.	3GPP	3GPP, GSMA, ITU	http://www.globalcertificationforum.org/certification/rto.html http://www.itu.int/net/ITU-T/conformity/Labs.aspx

LoRa	Sub GHz	LoRa Alliance	LoRa Alliance™ Certification	https://www.lora-alliance.org/Products/Certification-Overview
SIGFOX	Sub GHz	SIGFOX	Sigfox Ready Certification	https://partners.sigfox.com/companies/test-house?or[categories][0]=test-house&q=singapore&limit=12&page=0
Wireline				
DSL	0-2.208 MHz	ITU-T	Broadband Forum	https://www.broadband-forum.org/
Ethernet	16,100,250 ,500, 600 MHz 1 GHz, 1.6- 2.0 GHz	IEEE 802.3	MEF Certification Registry for CE 2.0 FCC Certification ERAC Certification	https://www.mef.net/certification/technology-certification-registry
PLC	No defined frequency band in India	ITU-T/ETSI/IEEE	G3-PLC Alliance	http://www.g3-plc.com/certified-products-platforms/

TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS
MINISTRY OF COMMUNICATIONS
GOVERNMENT OF INDIA