FP7-SMARTCITIES-2013
Project number: 609132
http://www.e-balance-project.eu/

e-balance

Deliverable D4.1

Detailed Network Stack Specification and Implementation

Editor:	António Grilo (INOV)
Dissemination level: (Confidentiality)	PU
Suggested readers:	Consortium/Experts/other reader groups
Version:	1.0
Total number of pages:	75
Keywords:	Network Architecture, Communication Technologies, Protocol Stack

Abstract

This deliverable presents the specification and implementation of the e-balance communication network. The latter are based on the specification of networking requirements and analysis of candidate communication technologies. A networking architecture is then defined, in which the selected technologies are combined in order to support the higher level e-balance services. Finally, the communication technologies and equipment used in the demonstrator scenarios is presented.

Disclaimer

The information, documentation and figures available in this deliverable are written by the e-balance partners under EC co-financing (project number: 609132) and does not necessarily reflect the view of the European Commission.

Impressum

[Full project title] Balancing energy production and consumption in energy efficient smart neighbourhoods

[Short project title] e-balance

[Number and title of work-package] WP4 Communication Platform
[Document title] Deliverable 4.1: Detailed Network Stack Specification and Implementation
[Editor: Name, company] António Grilo, INOV

[Work-package leader: Name, company] Daniel Garrido, Universidad de Málaga

Copyright notice

Executive Summary

This deliverable presents the specification and implementation of the e-balance communication network. The structure of this deliverable follows closely the methodology that was adopted to reach the e-balance network implementation.

The definition of the e-balance networking mechanisms started from the overall e-balance system architecture, from which the e-balance network architecture was derived. The networking mechanisms were then extracted for significant use cases of e-balance. Preliminary studies were then carried out in order to identify the communication technologies, protocol stacks and standards that are applicable in each part of the e-balance network architecture, constituting potential candidates for inclusion in the network specification. A limited set of candidate communication technologies was selected for detailed performance analysis. For the Field Area Networks, IEEE 802.15.4, PLC PRIME and 3G/4G were selected, while Z-Wave, Bluetooth and IEEE 802.15.4 were selected for the HAN. Technologies like WiFi are widely available, but their energy consumption of the currently available standards is too large to be acceptable for a large number of small intelligent devices distributed in the home area. The results of this detailed analysis were compared with the requirements specification in order to validate the selection of communication technologies. The specification of the networking mechanisms includes the selection of communication technologies and protocol stacks, which is based on the results of the performance analysis. This specification represents an abstract e-balance networking solution, which is partially instantiated in the project demonstrators defined in WP6. The actual network equipment and interfaces used in the network implementation is also described.

List of authors

Company	Author
CEMOSA	Juan Jacobo Peralta Escalante
EDP	Francisco melo, João Pinto de Almeida
EFACEC	Alberto Jorge Bernardo, Paulo Delfim Rodrigues, Nuno Silva, António Carrapatoso, Alberto Rodrigues
IHP	Krzysztof Piotrowski
INOV	António Grilo, Mário Nunes, Augusto Casaca
UTWE	Marijn Jongerden, Marco Gerards, Boudewijn Haverkort
UMA	Eduardo Cañete, Jaime Chen, Daniel Garrido, Manuel Díaz

Table of Contents

List of Tables

List of Figures

Abbreviations

6LoWPAN	Pv6 over Low power Wireless Personal Area Networks
AC	Alternating Current
AES	Advanced Encryption Standard
AFH	Adaptive Frequency Hopping
ALM	Airline Link Metric
AMR	Automatic Meter Reading
AODV	Ad-hoc On-Demand Distance Vector
ARQ	Automatic Repeat Request
ASK	Amplitude Shift Keying
BB-PLC	Broadband PLC
BPSK	Binary PSK
CAPEX	Capital Expenditure
CDMA	Code Division Multiple Access
CFP	Contention-Free Period
CL	Convergence Layer
CMS	Central Management Systems
CoAP	Constrained Application Protocol
COSEM	Companion Specification for Energy Metering
CP	Cyclic Prefix
CPCS	Common Part Convergence Sublayer
CSMA	Carrier Sense Multiple Access
CSMA/CA	CSMA with Collision Avoidance
CSMA/CD	CSMA with Collision Detection
D8PSK	Differential 8-PSK
DBPSK	Differential BPSK
DC	Direct Current
DCSK	Differential Chaos Shift Keying
DER	Distributed Energy Resource
DLMS	Device Language Message Specification
DMS	Distribution Management System
DOCSIS	Data Over Cable Service Interface Specification
DQPSK	Differential QPSK
DSL	Digital Subscriber Line
DSLAM	DSL Access Multiplexer
DSO	Distribution System Operator
DSSS	Direct-Sequence Spread Spectrum
DTC	Distribution Transformer Controller

DTLS	Datagram Transport Layer Security
EDGM	Electrical Distribution Grid Monitoring
ERP	Effective Radiated Power
E-UTRAN	Evolved UTRAN
FAN	Field Area Network
FCS	Frame Check Sequence
FDD	Frequency Division Duplexing
FDLIR	Fault Detection, Location, Isolation and Restoration
FDM	Frequency-Division Multiplexing
FDMA	Frequency-Division Multiple Access
FFD	Full-Function Device
FHSS	Frequency-Hopping Spread Spectrum
FSK	Frequency Shift Keying
GMU	Grid Management Unit
GPDU	Generic MAC PDU
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GTS	Guaranteed Time Slot
HAN	Home Area Network
HARQ	Hybrid ARQ
HCI	Host Controller Interface
HF	High Frequency
HFC	Hybrid Fiber Coax
HSDPA	High-Speed Downlink Packet Access
HSUPA	High-Speed Uplink Packet Access
HTTP	Hypertext Transfer Protocol
HWMP	Hybrid Wireless Mesh Protocol
IED	Intelligent Electronic Devices
IFS	Inter-Frame Space
IoT	Internet of Things
IP	Internet Protocol
IPHC	IP Header Compression
IPv4	IP version 4
IPv6	IP version 6
ISM	Industrial, Scientific and Medical
LEO	Low Earth Orbit
LE	Low Energy
LF	Low Frequency

LIFS	Long IFS
LLN	Low Power and Lossy Network
LTE	Long-Term Evolution
LV	Low Voltage
LV-FAN	Low Voltage FAN
LV-GMU	Low Voltage GMU
MAC	Medium Access Control
MCU	Microcontroller Unit
MDM	Meter Data Management
MFR	MAC Footer
MHR	MAC Header
MIB	Management Information Base
MSDU	MAC SDU
MU	Management Unit
MV	Medium Voltage
MV-FAN	Medium Voltage FAN
MV-GMU	Medium Voltage GMU
NAN	Neighborhood Area Network
NB-PLC	Narrowband PLC
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OLSR	Optimized Link State Routing Protocol
OPEX	Operational Expenditure
O-QPSK	Offset QPSK
PAN	Personal Area Network
PDCP	Packet Data Convergence Protocol
PDU	Protocol Data Unit
PFR	Power Flow Recognition
PHR	PHY Header
PHY	Physical
PL	Public Lighting
PLC	Power Line Communications
PON	Passive Optical Network
PRIME	PoweRline Intelligent Metering Evolution
PS	Primary Substation
PSDU	PHY SDU
PSK	Phase Shift Keying
PV	Photovoltaic

QPSK	Quadrature PSK
RB	Resource Block
RE	Resource Element
RF	Radiofrequency
RFD	Reduced-Function Device
RF-Mesh	Radiofrequency Mesh
RLC	Radio Link Control
RPL	Routing Protocol for Low Power and Lossy Networks
RRC	Radio Resource Control
RTU	Remote Terminal Unit
SAR	Segmentation and Reassembly
SCADA	Supervisory Control and Data Acquisition
SC-FDMA	Single Carrier FDMA
SCP	Shared-Contention Period
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
S-FSK	Spread FSK
SHA	Secure Hash Algorithm
SHR	Synchronization Header
SIFS	Short IFS
SIG	Special Interest Group
SM	Smart Meter
SONET	Synchronous Optical Networking
SS	Secondary Substation
SSCS	Service Specific Convergence Sublayer
SUN	Smart Utility Networks
TCP	Transmission Control Protocol
TDM	Time-Division Multiplexing
TDMA	Time-Division Multiple Access
TDD	Time Division Duplexing
TETRA	Terrestrial Trunked Radio
UDP	User Datagram Protocol
UHF	Ultra-High Frequency
UMTS	Universal Mobile Telecommunications System
UNB-PLC	Ultra Narrowband PLC
UTRAN	UMTS Terrestrial Radio Access Network
VHF	Very-High Frequency
VLF	Very-Low Frequency

VSAT	Very-Small Aperture Terminal
WAN	Wide Area Network
WDM	Wavelength-Division Multiplexing
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WSN	Wireless Sensor Network
ZigBee SE	ZigBee Smart Energy

1 Introduction

The networking mechanisms provide the low level communication support to the e-balance system, interconnecting both physically and logically the relevant system entities, such as Management Units (MUs), sensors, actuators and Smart Meters (SM). They support the transmission of e-balance information flows between those entities, granting the performance required by the respective services, while minimizing the costs associated with network deployment and operation. This deliverable presents the work done in the context of task T4.1, whose objective is to specify and to implement the networking mechanisms of e-balance. The structure of this deliverable follows closely the methodology that was adopted to reach the e-balance network implementation.

The definition of the e-balance networking mechanisms started from the overall e-balance system architecture, from which the e-balance network architecture was derived. The network architecture was first presented in D3.1 [1] and is recalled in Chapter 2.

The networking mechanisms must be specified taking the e-balance service requirements into account. Networking requirements were extracted for significant use cases of e-balance, which are presented in Chapter 3. These networking requirements will be the basis of technology validation in Chapter 3.3.

Preliminary studies were carried out in order to identify the communication technologies, protocol stacks and standards that are applicable in each part of the e-balance network architecture, constituting potential candidates for inclusion in the network specification (see Appendix I). From the preliminary studies, a limited set of candidate communication technologies was selected for detailed performance analysis. The chapter also includes the specification of algorithms and mechanisms that were developed within the project in order to improve networking performance. The results of this detailed analysis were compared with the requirements specification in order to validate the selection of communication technologies. This analysis and discussion are presented in Chapter 3.3.

The specification of the networking mechanisms includes the selection of communication technologies and protocol stacks, which is based on the results of the detailed performance analysis and technology validation. This specification represents an abstract e-balance networking solution, which will be partially instantiated in the project demonstrators defined in WP6. The specification of the networking mechanisms is presented in Chapter 5.

The design and implementation of the networking modules that will be integrated in the demonstrators are presented in Chapter 6.

2 e-balance Network Architecture

The e-balance communications network architecture was defined in D3.1 [1] and is depicted in Figure 1. The architecture is hierarchical and fractal-like with management units (MUs) at each level, managing the MUs at the levels below. The MUs that govern the grid infrastructure are explicitly designated grid management units (GMUs).

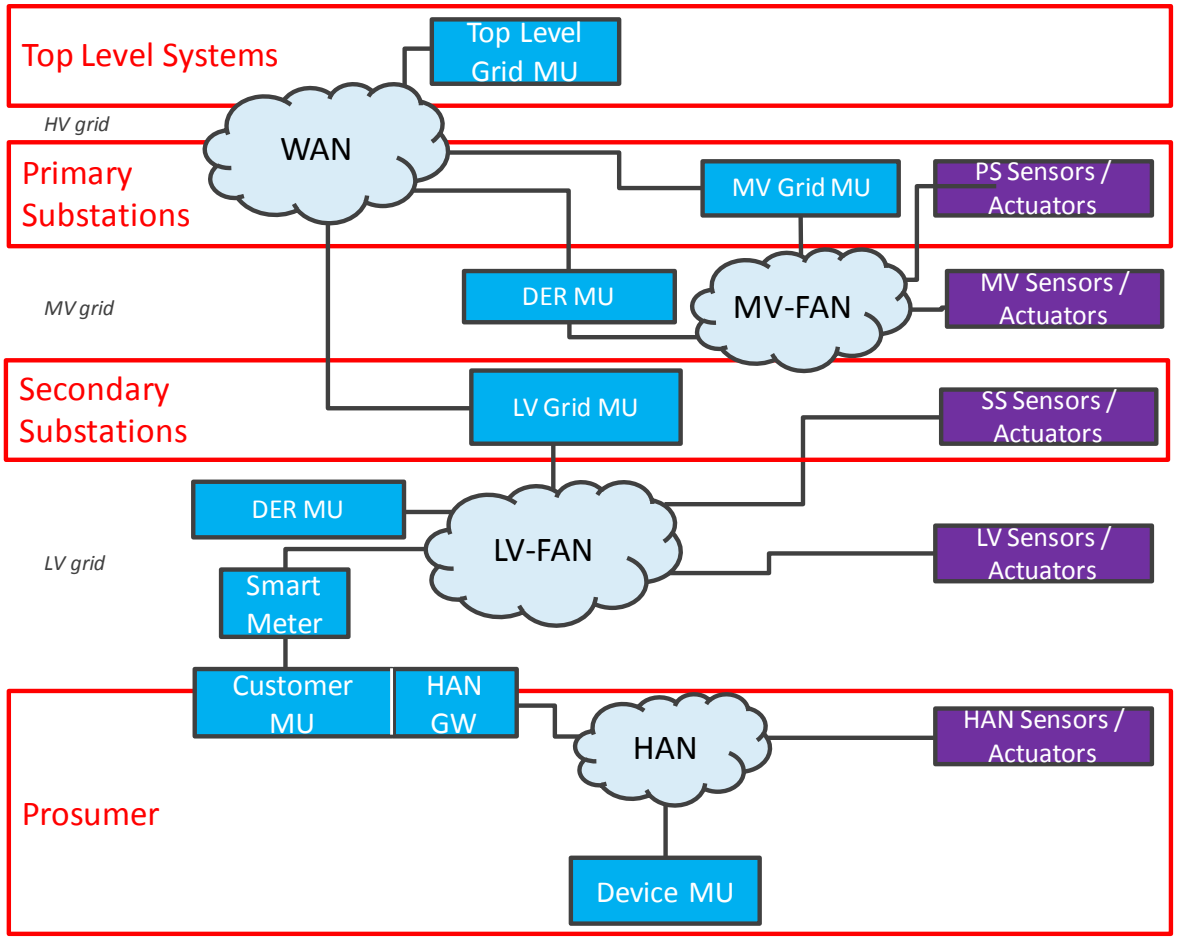


Figure 1: e-balance communication network architecture.

The communication architecture is structured in four levels. The top level corresponds to the Central Management Systems (CMSs), where the Top-Level GMU (TL-GMU) resides. This forms the core of the Smart Grid distribution intelligence and must be fed by data coming from the systems and devices that lie below in the network architecture, while issuing management and control commands downstream.

The next level is constituted by the Primary Substations (PS), each comprising an MV-GMU. The latter gathers data from sensors located within the PS, as well as from MV field sensors, issuing management and control commands to MV grid actuators. It also interacts with DER MUs as well as with LV-GMUs (LV-GMU) located at the Secondary Substations (SS). Communication between the TL-GMU, the MV-GMUs and LV-GMUs is accomplished through a Wide Area Network (WAN) technology due to the large geographical scale associated with the regional character of distribution at the top levels of the grid architecture. Communication between the MV-GMU, MV field sensors/actuators and DER MUs is accomplished through the MV Field Area Network (MV-FAN). The character of the MV-FAN is more local since the sensor/actuator nodes are located in devices and/or power lines that constitute a grid subset that is directly connected to the Primary Substation.

The level below is constituted by the SSs, which are responsible for Low Voltage (LV) energy distribution at a neighbourhood scale. Each SS comprises an LV-GMU, which receives data from LV sensors as well as from the SMs and DERs located in the LV, issuing management and control commands downstream (e.g.,

control of LV actuators, load management and control of DERs located in the LV). Connectivity between the LV-GMU, SMs, LV field sensors/actuators and DER MUs is accomplished through the LV-FAN.

Finally, we reach the bottom level constituted by the prosumer premises. The SM is able to control advanced power consumptions functionalities and it also manages the power outputs of energy generating devices based on the set points issued by the LV-GMU. The SM is directly connected to the Customer MU (CMU). Connectivity between the CMU, appliance sensors, actuators and device MUs (DMU) is accomplished through the Home Area Network (HAN). At device level, the DMU interacts locally with smart device sensors and actuators.

In summary, the e-balance communication network architecture comprises four network areas: WAN, MV-FAN, LV-FAN and HAN. These network areas will instantiate the communication needs of the information flows between the different entities represented in the system architecture.

3 Information Flow Requirements

This chapter presents provisional information flow requirements, taking into account the main use cases considered in D2.1 [2]. These requirements will constitute the basis for the validation of the technologies selected in Chapter 4. A more detailed specification of the information flows is provided in D3.2 [3].

Information flows belonging to specific types of use cases will be presented, followed by the definition of two validation scenario based on more realistic Bronsbergen and Batalha settings (i.e., they will be supersets of the demo scenarios), which will be used to assess the suitability of the selected FAN and HAN communication technologies in Chapter 3.3.

3.1 Energy Balancing

The information flows required for Energy Balancing are listed in Table 1. As can be concluded from the involved devices, these information flows occur either over the LV-FAN or over the HAN. The capacity that is actually needed in the LV-FAN and HAN to transport these flows depends on three variables:

- M: Interval between profile exchanges (in minutes).
- I: Number of iterations within M.
- N: Number of CMUs below the LV-GMU.
- P: Number of smart appliances below the CMU.

This allows some flexibility and adaptation of the service to different technologies. However, it should be noted that the frequency and accuracy of the information has an impact of the performance of the energy balancing algorithms that should not be neglected.

Table 1: Energy Balancing information flows

Name	Short description	Source	Destination	Data size	Data frequency	Network Area
Energy forecast profile	forecast of energy consumption/production of customer	CMU	LV-GMU	Array of 1440/M doubles	once per *M* min	LV-FAN
Request delta profile	difference sum forecast with desired power profile, some potential earnings may be added here	LV-GMU	CMU	Array of 1440/M doubles (broadcast, one to N)	once per iteration several iterations (max 2*N*) per *M* min	LV-FAN
Deliverable delta customer	customer provides the changes it can make, summarized in one single value	CMU	LV-GMU	Double	once per iteration several iterations (max 2*N*) per *M* min	LV-FAN
Assign customer	LV-GMU notifies the customer that it must change its profile.	LV-GMU	CMU	Command code	once per iteration several iterations (max 2*N*) per M min	LV-FAN
Updated profile customer	customer provides its changed profile	CMU	LV-GMU	Array of doubles	At most once per iteration	LV-FAN

					several iterations (max 2*N*) per M min	
SM measurement	Power measurement from the SM	SM	CMU	Number	Every 10 seconds	Direct interface
Aappliance event	Update of the status of a smart appliance	Smart appliance	CMU	Variable	When an event occurs	HAN
Appliance control	Control of the appliance by the CMU	CMU	Smart appliance	Variable	When an action is required	HAN

3.2 Neighborhood Monitoring

Neighborhood monitoring takes place mainly through the FAN and encompasses the following groups of use cases:

- Power Flow Recognition (PFR)
- Electrical Distribution Grid Monitoring (EDGM)
- Fault Detection, Location, Isolation and Restoration (FDLIR)

PFR and EDGM achieve their results based on the same data, which consist of periodic measurements of voltage and current, which are performed by FAN sensors and SMs. On the other hand, FDLIR is mainly based on the transmission of alarm events, issued by the nodes where the alarm situations were detected. Consequently, periodic quantity measurements and alarms constitute the main traffic flows related to neighborhood monitoring and will be quantified in the following sections.

3.2.1 Periodic voltage, current and energy measurements

The period (T) and length ($l_{periodic}$) of the measurement messages, as well as the number of measurement points (S) determine the net throughput required by the application layer. Parameter $l_{periodic}$ is related with the accuracy of the quantity measurements. Since this parameter is usually fixed, a resulting message rate ($\lambda_{NH\_measure}$) can be found, which is simply calculated as the ratio between S and T.

$$\lambda_{NH\_measure} = \frac{S}{T} \quad (1)$$

For message length, latency and reliability requirements, [4] is adopted as a reference. The following figures are relative to on-demand meter readings, but may apply to FAN sensor readings as well. That document considers the typical value of $l_{periodic}$ for an isolated meter reading to be around 100 octets. Regarding the maximum latency, the same document specifies 15s for on-demand samples. Delivery reliability should be greater than 98%.

3.2.2 Alarm event notifications

Since the alarm messages are supposed to be transmitted only once by the application layer upon occurrence of the respective event, the length (l_{alarm}) of the measurement messages, the number of measurement points (S) and the maximum latency (d_{max}) determine the net throughput required by the application layer. If l_{alarm} is fixed, a resulting message rate (λ_{NH_alarm}) can be found, which is simply calculated as follows:

$$\lambda_{NH\_alarm} = \frac{S}{d_{max}} \quad (2)$$

For message length, latency and reliability requirements, [4] is again adopted as a reference. The following figures are relative to fault detection in distribution automation. That document considers the typical value of

l_{alarm} for an alarm notification to be 25 octets. Regarding the maximum latency, it specifies 20s for messages coming from the meters. Delivery reliability should be greater than 98%.

3.3 Technology Validation Scenarios

In this section, two technology validation scenarios will be defined, based on the Bronsbergen and Batalha demo scenarios, which are described in more detail in D6.1 [5]. The validation scenarios are extended versions of the latter to encompass a more realistic number of nodes and amount of network traffic. Possible aggregate traffic patterns will be defined taking into account Energy Balancing and Neighborhood Monitoring information flows. Only the LV grid will be considered.

3.3.1 Bronsbergen Scenario

In the holiday park Bronsbergen scenario, 208 cottages are connected with SS Roelofs (where the LV-GMU is located) through the respective LV-FAN. From these, 92 cottages are or will be equipped with solar panels. An area of 500×200 m^2 is assumed. In order to compute a realistic aggregate traffic pattern, values will be assigned to the parameters identified in 3.1 and 3.2. The alarm event notifications constitute exceptional traffic and thus will not be considered as part of the steady-state aggregate. The considered parameter configuration is listed in Table 2.

Table 2: Parameters of the Bronsbergen LV-FAN validation scenario

Variable	Value	Comments
M	15 min	Standard metering period
N	208	
P	4	
I	416	$2\times N$
S	248	208 SMs and 20 field area sensors
T	15 min	Standard metering period
$l_{periodic}$	100	

The scenario's traffic characterization and technology assessment will be made separately for the LV-FAN and HAN.

The LV-FAN will support all communications between the LV-GMU and SMs, as well as between the LV-GMU and the CMUs. Table 3 lists the messages that must be transmitted within an interval of 15 min.

Table 3: Bronsbergen LV-FAN messages characterization

Message	Message Length (bytes)	Message Rate (per 15 minutes)	Message Rate (per second)	Comment
Energy forecast profile	768	208	0.23	
Request delta profile	768	416	0.46	2*N* iterations
Deliverable delta customer	8	416	0.46	2*N* iterations
Assign customer	1	416	0.46	2*N* iterations
Updated profile customer	768	416	0.46	2*N* iterations
Periodic measurements	100	228	0.25	

The HAN supports communication between the CMU and the smart appliances. As can be seen from Table 1 and Table 2, this traffic is event-oriented and very sporadic, since the expected number of smart appliances is also small ($P = 4$ in the considered scenario). The chosen technologies and protocols for the HAN (ZigBee and Z-Wave) are designed for much more dense networks. In the runtime of the demonstrators we will monitor the traffic in the network in order to estimate the actual use of the available channel capacity.

3.3.2 Batalha Scenario

In the Batalha LV grid, 9000 clients are distributed by 133 SSs, which results into an average of 68 clients per SS. As for the Bronsbergen scenario, in order to compute a realistic aggregate traffic pattern, values will be assigned to the parameters identified in 3.1 and 3.2. Again, the alarm event notifications constitute exceptional traffic and thus will not be considered as part of the steady-state aggregate. The considered parameter configuration is listed in Table 4.

Table 4: Parameters of the Batalha LV-FAN validation scenario

Variable	Value	Comments
M	15 min	Standard metering period
N	68	
P	4	
I	136	$2\times N$
S	74	68 SMs and 6 field area sensors
T	15 min	Standard metering period
$l_{periodic}$	100	

The LV-FAN will support all communications between the LV-GMU and SMs, as well as between the LV-GMU and the CMUs. Table 5 lists the messages that must be transmitted within an interval of 15 min.

Table 5: Batalha LV-FAN messages characterization

Message	Message Length (bytes)	Message Rate (per 15 minutes)	Message Rate (per second)	Comment
Energy forecast profile	768	68	0.08	
Request delta profile	768	136	0.15	2*N* iterations
Deliverable delta customer	8	136	0.15	2*N* iterations
Assign customer	1	136	0.15	2*N* iterations
Updated profile customer	768	136	0.15	2*N* iterations
Periodic measurements	100	72	0.08	

The HAN supports communication between the CMU and the smart appliances. As can be seen from Table 1 and Table 4, this traffic is event-oriented and very sporadic The chosen technologies are defined to support dense HAN networks. We will monitor the network traffic to identify the actual use of the channel capacity.

4 Analysis of Communication Technologies and Protocol Stack

Preliminary studies were conducted in order to identify the main communication technologies that are applicable in the Smart Grid. The resultant technology survey is presented in Appendix I. A summary of these results is presented in Table 6, which provides a comparison encompassing transmission speeds, communications range and their suitability to be employed at different areas of the Smart Grid.

Table 6: Comparison between communication technologies and their applicability in the Smart Grid

Type	Subtype	CAPEX	OPEX	Maximum Bit rate	Range[1]	Network Area Suitability
Broadband Technologies	Optical fiber SONET/SDH	Low (hired service)	High (hired service)	160 Gbit/s	2-80 km	WAN (core)
	Optical fiber WDM					
	Optical fiber PON					
	DSL	Low (hired service	Medium (hired service	100Mbits/s	5km	WAN (access)
	DOCSIS	Low (hired service)	Medium (hired service)	172Mbit/s	28km	WAN (access)
	Satellite	Low (hired service)	High (hired service)	50Mbit/s	100-6000Km	WAN (access)
	Ethernet (1000BASE-LX)	Medium	Negligible	40 Gbit/s	5 km	LAN
PLC	UNB	Low	Negligible	100 bit/s	150 km	FAN
	NB	Low	Negligible	128 kbit/s (CENELEC-A)	Several km	FAN, NAN
	BB	Low	Negligible	500 Mbit/s	Tens of meters	HAN
Infra-structure-based Wireless Networks	2.5G (GPRS)	Low (hired service)	High (hired service)	85.6 kbit/s	Coverage dependent	WAN, FAN, NAN
	3G (HSDPA, HSUPA)	Low (hired service)	High (hired service)	42 Mbit/s downlink 5.76 Mbit/s uplink	Coverage dependent	WAN, FAN, NAN
	4G (WiMAX, LTE)	Low (hired service)	High (hired service)	299.6 Mbit/s downlink 75.4 Mbit/s uplink	Coverage dependent	WAN, FAN, NAN
RF Mesh	Broadband (IEEE 802.11n/s)	High	Negligible	6-600 Mbit/s	50-400m	FAN, NAN, LAN
	Narrowband (Silver Spring Networks)	Low	Negligible	100 kbit/s	Several km	FAN, NAN, HAN
	Narrowband (IEEE 802.15.4g)	Low	Negligible	1094 kbit/s	Several km (e.g., XbeePro 868 @ 24 kbit/s)	FAN, NAN, HAN

This chapter provides an analysis on the expected performance bounds of selected communication technologies in order to support the e-balance information flows through higher layer Smart Grid protocols within each network area. This analysis assumes an Internet of Things (IoT) protocol stack (see I.2.5), as defined in D3.2 [3]. The analysis is performed separately for each network area: WAN, FAN and HAN.

4.1 WAN

According to the e-balance network architecture (see Chapter 1), the WAN interconnects the CMSs to the Primary Substations and Secondary Substations due to the large geographical scale associated with the regional character of distribution at the top levels of the grid architecture. Due to the large scale and diversity of scenarios encompassing the WAN, the latter will most probably integrate more than one communication technology and protocol stack. Also due to the high investment necessary to install this kind of networks, preexisting networks are typically reused as the WAN network of the smart grid. For example, the standard internet IP network under which many different broadband technologies are used (such as optic fiber, DSL, Ethernet, etc.) is one of the most common choices in current smart grid projects. In this case, security is an

[1] Maximum ranges are usually achieved with the lowest bitrates only.

essential feature due to the fact that not dedicated communication networks are used and therefore they are more prone to attacks.

In [4], authors analyze the communication networks requirements for major smart grid applications in WAN (also in HAN and FAN). In this work they present an interesting table where the WAN communication requirements in terms of data size, data sampling, latency and reliability are presented. It is highlighted that the values used to fill in the mentioned table are based on official standards, such as MIRRORED BITS, IEC 61850 Generic Object-Oriented Substation Event (GOOSE), IEEE Standard for Synchrophasors for Power Systems, etc. Table 7 shows the results extracted from table above mentioned.

Table 7: Network requirements for wide-area protection, control and monitoring applications

Application	**Typical data size (bytes)**	**Typical data sampling requirement**	**Latency**	**Reliability (%)**
Wide- area protection	4-157			
Adaptive islanding		Once every 0.1 s	<0.1s	>99.9
Predictive under frequency load shedding		Once every 0.1 s	<0.1s	>99.9
Wide-are control	4-157			
Wide-area voltage stability control		Once every 0.5-5s	<5 s	>99.9
FACTS and HVDC control		Once every 30 s-2min	<2 min	>99.9
Cascading failure control			<5 s	>99.9
Precalculation transient stability control		Once every 0.5-5s	<2 min	>99.9
Close-loop transient stability control		Once every 30s - 2min	<0.1s	>99.9
Wide-area power oscillation damping control		Once every 0.02-0.1s	<0.1s	>99.9
		Once every 0.1s		
Wide-area monitoring	>52			
Local power oscillation monitoring		Once every 0.1s	<30 s	>99.9
Wide-area power oscillation monitoring		Once every 0.1s	<0.1 s	>99.9
Local voltage stability monitoring		Once every 0.5-5s	<30 s	>99.9
Wide-area voltage stability monitoring		Once every 0.5-5s	<5 s	>99.9
PMU-based state estimation		Once every 0.1s	<0.1 s	>99.9
Dynamic state estimation		Once every 0.02-0.1s	<0.1 s	>99.9
PMU-assited state estimation		Once every 30 s-2min	<2 min	>99.9

The technologies that can be used in the WAN can be grouped into three main types:

1. Broadband Access Technologies: Some of these technologies briefly presented in Section I.1.1 such as Digital Subscriber Line (DSL), Hybrid Fiber Coax (HFC) and Passive Optical Network (PON) are only employed in the last mile segment of the WAN, which implies that the traffic will have to cross a broadband core network (see below).
2. Infrastructure-based Wireless Networks: Examples of these technologies are WiMAX, the General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS), Terrestrial Trunked Radio (TETRA) and Long-Term Evolution (LTE) and satellite systems. These technologies are typically used at the edge of the WAN to provide a broad coverage in areas that cannot be reached through broadband access.
3. Core Network Technologies: SONET/SDH, Optical Transport Network (OTN) and multi-gigabit Ethernet are examples of technologies that can be used in the core network. In a Smart Grid context,

a part of the core network may belong to the DSO, or the service can be hired from an Internet Service Provider (ISP) or telecom operator.

Table 8 presents the main features or each of the technologies identified as promising for the WAN part of the smart grid. As can be seen, the WAN networking interfaces have typically a huge capacity and do not constitute the bottleneck of the system. Core network technologies typically use optic fiber which provides the highest transmission speed of all technologies in the communication network. The last mile segment provides transmission speeds lower than the core network technologies but still enough for the smart grid requirements, especially modern technologies that can, for example, even provide optic fiber to the end users. Also, modern mobile telecommunication networks provide high speed data transfer with the advantage of not requiring wiring. In this communication technology, most of the time routing is not an issue since the data can be transmitted in one hop to the destination (e.g., WiMAX, 4G, GPRS).

A WAN network is usually not limited to a single of these technologies, but rather a combination of several of them based on different factors such as:

- Existing deployments (usually by a utility): wiring, equipment, etc.
- Limitation in the use of some technologies due to technical factors, for example due to interferences
- Location of the network that may make it impossible to deploy certain technologies (e.g. inaccessible places)
- Economical and strategic reasons: utilities may not choose a technology based on technical features but rather on economic and strategic reasons such as return of investment, reusing existing equipment such as coaxial cable, etc.

Table 8: Communication technologies for the WAN

	Type	**Maximum Bit Rate**	**Coverage Range**
DSL	Wired	1-100Mbps	Up to 28 Km
SONET/SDH	Optic fiber	10-1000 Mbps	Up to 100 Km
HFC	Coaxial/ Optic fiber	-	Depending on coaxial/ optic fiber configuration
WDM	Optic fiber	40Gbps	Up to 100Km
DOCSIS	Coaxial	172 Mbps	Up to 28 Km
PON	Optic fiber	155 Mbps - 2.5 Gbps	Up to 60 Km
Satellite	Satellite	50Mbps	100-6000 Km
WiMAX	Wireless	Up to 75 Mbps	10-50 Km (LOS), 1-5 Km (NLOS)
GSM	Wireless (cellular)	Up to 14.4 Kbps	35 Km
GPRS	Wireless (cellular)	Up to 170 Kbps	35Km
3G	Wireless (cellular)	384 Kbps - 2Mbps	1-10 Km
TETRA	Wireless	2400 bps	Up to 50 Km
LTE	Wireless	75 Mbps - 300 Mbps	Up to 50 Km
LTE-A	Wireless	100 Mbps - 1 Gbps	Up to 50 Km

The authors of the work [4] carry out a deeper study on many smart grid projects deployed in US, European countries and Chine. From the whole set of projects, nine were selected and analysed from the communication point of view. It is worth highlighting to mention in some of these projects around 80000 SMs are used. The communication of technologies and the main features of these projects are summarized in the Table 9.

Table 9: WAN technology selection in different international projects

Organization	Technology	Features
Austin Energy	Optical fiber, RF mesh network	410000 SMs, 86000 smart thermostats, 2500 sensors, 3000 computers
City of Glendale Water and Power	Ethernet/Internet, wireless mesh network	85526 SMs, 80000 HAN, 30000 in-home displays
Baltimore Gas and Electric Company	Optical fiber, RF mesh network	1272911 SMs, 400000 direct load control devices
AC Propulsion, Inc.	CDPD	V2G demonstration project with VW Beetle EV
Duke Energy Carolinas, LLC	Optical fiber	102 PMUs, 2 phasor data concentrators
Eandis and Infrax	PLC, DSL, GPRS	36000 smart communication gateways
Acea Distribuzione	PLC, GPRS	One of Europe's largest smart metering projects, gas and water meters, serving 1.5 million households.
Public Power Corporation	Wi-Fi, BPL	remote monitoring and control of irrigation pumps during peak hours
China Southern Power Grid	2G, 3G	monitor end-users' electricity usage in real-time

The selection of the WAN technology will be based on different factors that may not always be limited to technical reasons. The cost of deployment of a WAN network is most of the times usually prohibitive for a single company. Therefore, it is difficult to assess or propose a protocol stack for the WAN that works for all deployments. Since this network segment do not constitute the bottleneck of the system, as previously stated, the WAN technology selection in e-balance will be made per demonstrator. More details about the WAN technology selection will be given in deliverables of WP6 where specific demonstrators are specified and presented. Consequently, no further analysis on the communication technology performance will be presented in this section.

4.2 LV-FAN and MV-FAN

This section presents an analysis of performance of selected FAN technologies, followed by a proposal of an alarm aggregation mechanism for use with multihop FAN technologies such as PLC PRIME and RF-Mesh.

According to the e-balance network architecture (see Chapter 1), the MV-FAN and LV-FAN perform the interconnection between field sensors and actuators, DER management units, grid management units and SMs at the respective voltage levels. As in Table 6, it is assumed that the same communication technologies are applicable in both the LV-FAN and the MV-FAN, allowing a common capacity analysis.The groups of communication technologies that are applicable to the FAN are the following:

- NB-PLC Power Line Communications.
- Radio frequency Mesh (RF-Mesh) networks.
- Infrastructure-based Wireless Networks.

Three particular technologies were selected to illustrate each of the above groups, which will be separately analyzed in the following sections:

- PLC PRIME
- IEEE 802.15.4 at 868 MHz
- LTE

In order to estimate the performance achieved by the application layer protocols, we have considered the four types of application layer interaction defined for the Data Interface [3]:

- Read: This is the typical monitoring scenario in state-of-the-art solutions. The reading is performed on-demand. The client sends a query packet and the server responds with the requested data.
- Write: This is a typical control operation, whereby the client requests that the value of a control variable is changed.
- Event: The sensor/meter device is pre-configured to send an asynchronous notification when a specified event occurs. The notifications are sent to interested clients that have previously subscribed to them.
- Periodic: The server periodically sends variable update notifications. The notifications are sent to interested clients that have previously subscribed to them.

These message exchange patterns are governed by the middleware protocol. In this study, the CoAP protocol will be assumed. Although the middleware protocols actually used in e-balance may be different, the considered payload size range is thought to encompass the typical patterns observed in other middleware protocol suites as well.

The Read exchange is considered to follow a CoAP piggy-backed response pattern. The Read request message is assumed to consist of a CoAP GET method with 12 octets in length.

The Write exchange is almost symmetrical to the Read exchange. It consists of a CoAP POST method with a variable payload size, while the response will be significantly shorter. In this way, results are expected to be similar to the Read exchange and will not be analyzed separately.

The Event and Periodic exchanges are considered to follow a CoAP separate non-confirmable response pattern. In the context of a performance limits analysis, they can be treated as the same exchange pattern, which will henceforth be designated by Event. Since in both exchange patterns the subscription happens only once, its impact on performance can be considered negligible.

The detailed performance analysis carried out for PLC PRIME and IEEE 802.15.4 assumes an IPv6 stack for LLNs. As the application data messages go down the IPv6 protocol stack, overhead is added at each layer. The message sizes and the respective protocol overhead estimates are listed in Table 10, taking as a reference the Read and Event exchanges. The routing overhead (e.g., RPL) is considered negligible in steady-state, since the nodes are static. Below the header compression layer, the overhead is technology dependent.

Table 10: Message sizes considered in the FAN analysis for the Read and Event exchanges over LLN technologies

Layer	Request Length (octets)	Typical Response Length (octets)	Comment
Application	0	30-500	
CoAP	12	8	Response message with 4-byte token and no options
6LoWPAN	6	6	Compressed UDP/IPv6 in a link-local exchange using IPHC
Total	18	44-514	

The communication technology poses potential constraints on data transfer performance in the FAN, which must be analyzed in order to assure that the FAN design conforms to the requirements imposed by the information flows (see Chapter 3). The selected technologies are analyzed in greater detail in the following sections.

4.2.1 PLC PRIME

The PLC PRIME technology is defined in recommendation ITU-T G.9904 [6]. PLC PRIME uses Orthogonal Frequency Division Multiplexing (OFDM) technology and operates in the CENELEC-A frequency range (3-95 kHz).

PRIME defines a tree topology with root at a Base Node. The other nodes are designated Service Nodes. In order to extent the communication range, PRIME supports multihop communication, allowing Service Nodes to be promoted to switch traffic from other nodes.

The PRIME protocol architecture is depicted in Figure 2.

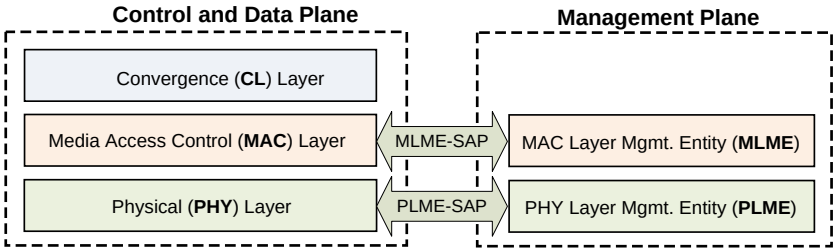


Figure 2: PRIME protocol architecture [6]

The PHY layer transmits and receives MPDUs between neighbor nodes.

The MAC layer provides core MAC functionalities of system access, bandwidth allocation, connection establishment/maintenance and topology resolution.

The Convergence Layer (CL) classifies traffic associating it with its proper MAC connection. This layer performs the mapping of any kind of traffic to be properly included in MAC packets. It may also include header compression functions. It comprises a Common Part Convergence Sublayer (CPCS) and one or more Service Specific Convergence Sublayers (SSCS) to accommodate different kinds of traffic into MAC packets, namely 6LoWPAN traffic.

At the PHY layer, the modulation and coding can be adapted based on channel conditions. Supported modulations for the frame data payload are DBPSK, DQPSK and D8PSK, and optional ½ convolutional coding can be used for increased robustness. The physical frame header always uses the most robust transmission mode, which is DBPSK with ½ convolutional coding. The supported transmission mode performances for the payload and header parts are listed in Table 11 and Table 12, respectively. The transmission mode should be dynamically selected based on channel conditions.

Table 11: Transmission modes for the PRIME packet payload

	DBPSK		DQPSK		D8PSK	
½ Convolutional Coding	On	Off	On	Off	On	Off
Information bits per carrier	0.5	1	1	2	1.5	3
Information bits per OFDM symbol	48	96	96	192	144	288
Raw data rate (kbit/s)	21.4	42.9	42.9	85.7	64.3	128.6
Maximum payload size for a 63-symbol payload (bits)	3016	6048	6040	12096	9064	18144

Table 12: Transmission modes for the PRIME packet header

	DBPSK
½ Convolutional Coding	On
Information bits per carrier	0.5
Information bits per OFDM symbol	48

The structure of the PHY frame is shown in Figure 3. Each PHY frame starts with a preamble lasting 2.048 ms, followed by a number of OFDM symbols, each lasting 2.24 ms. The first two OFDM symbols carry the frame's PHY header. The remaining *M* OFDM symbols carry payload. The value of *M* is signaled in the header, and is at most equal to 63. For longer payloads, PRIME supports segmentation and reassembly (SAR) at the Common Part Convergence Sublayer (CPCS). The PHY header also includes the first 52 bits of the MAC header.

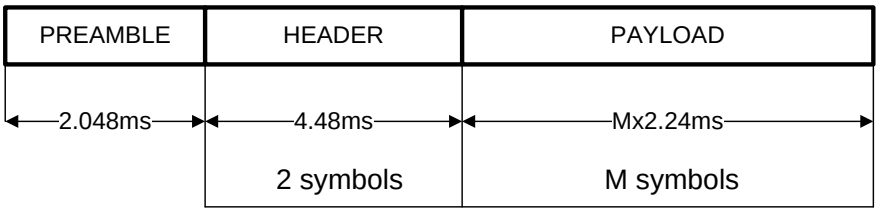


Figure 3: PRIME PHY frame format [6]

A MAC superframe comprises one or more Beacons, one Shared-Contention Period (SCP) and zero or one Contention-Free Period (CFP) (see Figure 4). When present, the length of the CFP is indicated in the beacons.

Figure 4: PRIME MAC superframe structure [6]

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with priorities is used to control medium access. Implementations start with a random backoff time (*macSCPRBO* symbols) based on the priority of data queued for transmission. Levels of priority (parameter *MACPriorityLevels*) need to be defined in each implementation, with a lower value indicating higher priority. A binary exponential backoff scheme is used to adapt to the local contention level.

Most Subnetwork traffic comprises Generic MAC PDUs (GPDU). GPDUs are used for all data traffic and most control traffic. All MAC control packets are transmitted as GPDUs. GPDU composition is shown in Figure 5. It is composed of a Generic MAC Header of 3 octets, followed by one or more MAC packets and 32 bit CRC appended at the end.

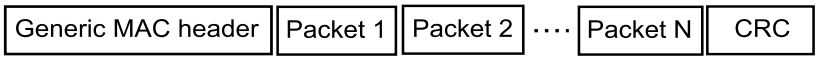


Figure 5: Generic MAC PDU [6]

A packet is comprised of a packet header (PH) of 6 octets and a packet payload, as depicted in Figure 6.

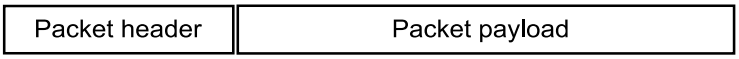


Figure 6: PRIME packet structure [6]

An Automatic Repeat Request (ARQ) mechanism at the MAC layer may be activated in order to counter transmission errors. The ARQ mechanism works between directly connected peers (original source and final destination), as long as both of them support ARQ implementation, even in multihop configurations. If the ARQ is enabled, an ARQ subheader (ARQH) of at least one octet is placed inside the data packets, after the packet header and before the original packet payload.

The following analysis provides an estimate of the maximum performance that can be achieved with PLC PRIME in ideal conditions (i.e., no errors). Still, a stop-and-wait ARQ mechanism (the default in PRIME) is considered, with the length of the ARQH being equal to 1. The *macSCPRBO* is made equal to 1. It is assumed that the communication takes place during the SCP and that the time reserved for Beacon transmission and for the CFP is negligible.

It is considered that the sink node interface (the Base Node in the case of PRIME) constitutes the bottleneck. Consequently, the exchange rate results are only meant to estimate single hop performance around the sink node. Multihop performance depends highly on the topology and would better be obtained through computer simulation, though we present figures for minimum delay.

The time required to perform a Read exchange in milliseconds can be calculated as follows:

$$T_{read} \sim T_{req} + T_{resp} + T_{ack} \tag{3}$$

$$T_{req} = t_s + 2.048 + 4.48 + ceil\left(\frac{(l_{GPDU}+l_{PH}+l_{ARQH}+l_{req})\cdot 8-52}{N_{bit\_s}}\right)\cdot t_s \tag{4}$$

$$T_{resp} = t_s + 2.048 + 4.48 + ceil\left(\frac{(l_{GPDU}+l_{PH}+l_{ARQH}+l_{resp})\cdot 8-52}{N_{bit\_s}}\right)\cdot t_s \tag{5}$$

$$T_{ack} = t_s + 2.048 + 4.48 + ceil\left(\frac{(l_{GPDU}+l_{PH}+l_{ARQH}+0)\cdot 8-52}{N_{bit\_s}}\right)\cdot t_s \tag{6}$$

Where t_s is the symbol time, N_{bit_s} is the number of bits transmitted in one symbol (depends on the selected transmission mode), l_{GPDU}, l_{PH}, l_{ARQH}, l_{req} and l_{resp} are the lengths of the GPDU header and CRC, packet header, ARQ subheader, request message and response message, respectively. It is assumed that the acknowledgements to the request are piggybacked in the response frame. The Read exchange frequency can be easily obtained as:

$$f_{read} = \frac{1}{T_{read}} \tag{7}$$

For the Event exchange, the time and frequency are given by the following equations:

$$T_{event} \sim T_{resp} + T_{ack} \tag{8}$$

$$f_{event} = \frac{1}{T_{event}} \tag{9}$$

The maximum exchange rates that can be obtained for the Read and Event patterns as a function of the data message size and transmission mode are depicted in Figure 7 and Figure 8.

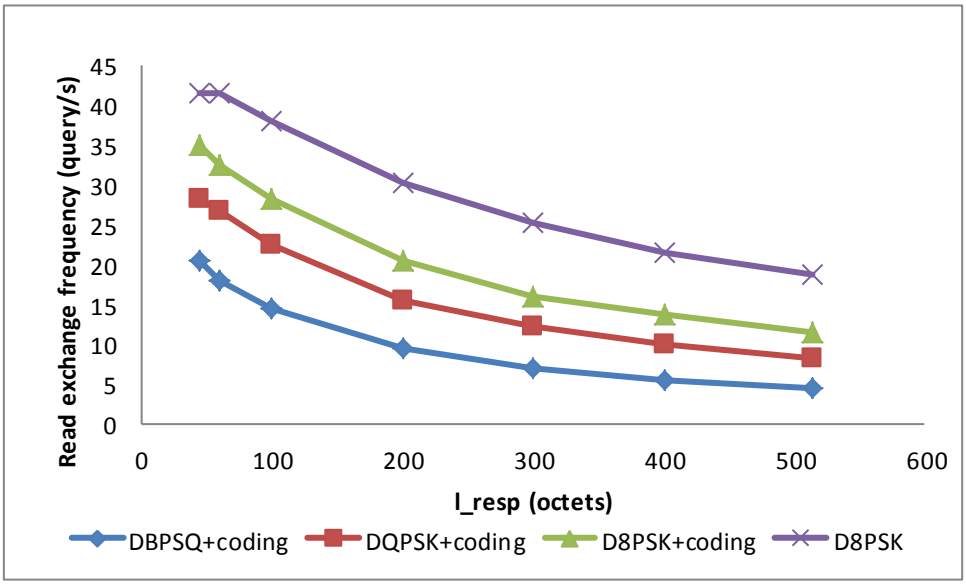


Figure 7: Read exchange rate in PLC PRIME, as a function of message size and transmission mode

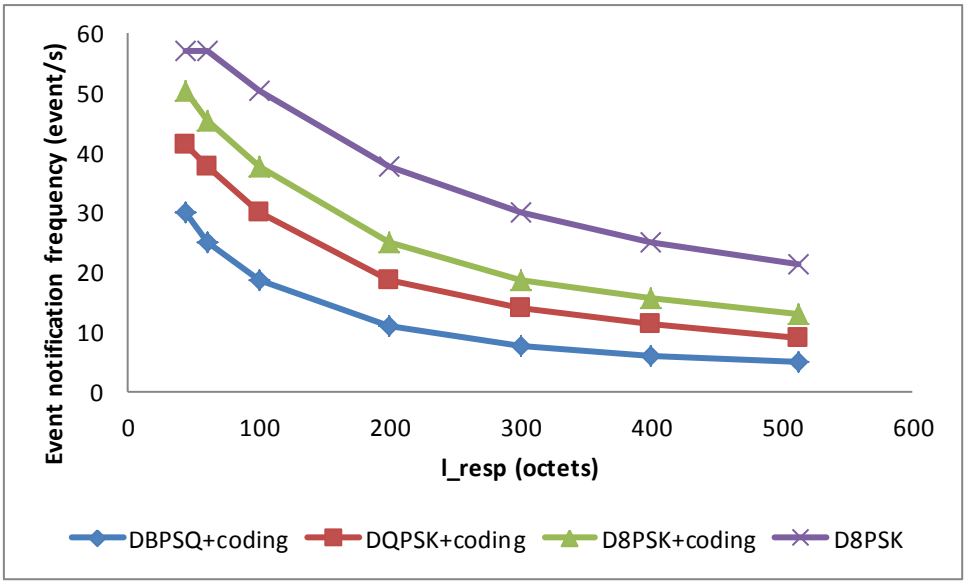


Figure 8: Event notification rate in PLC PRIME, as a function of message size and transmission mode

The end-to-end delay is another important performance quantity, since some traffic types establish delay bound requirements. The minimum end-to-end delays for the Read and Event message exchanges are given by the following equations:

$$\Theta_{read} = N_{hops} \cdot T_{query} \quad (10)$$

$$\Theta_{read} = N_{hops} \cdot T_{event} \quad (11)$$

N_{hops} is the number of hops between the source and the destination. Those delays are depicted in Figure 9 and Figure 10, respectively.

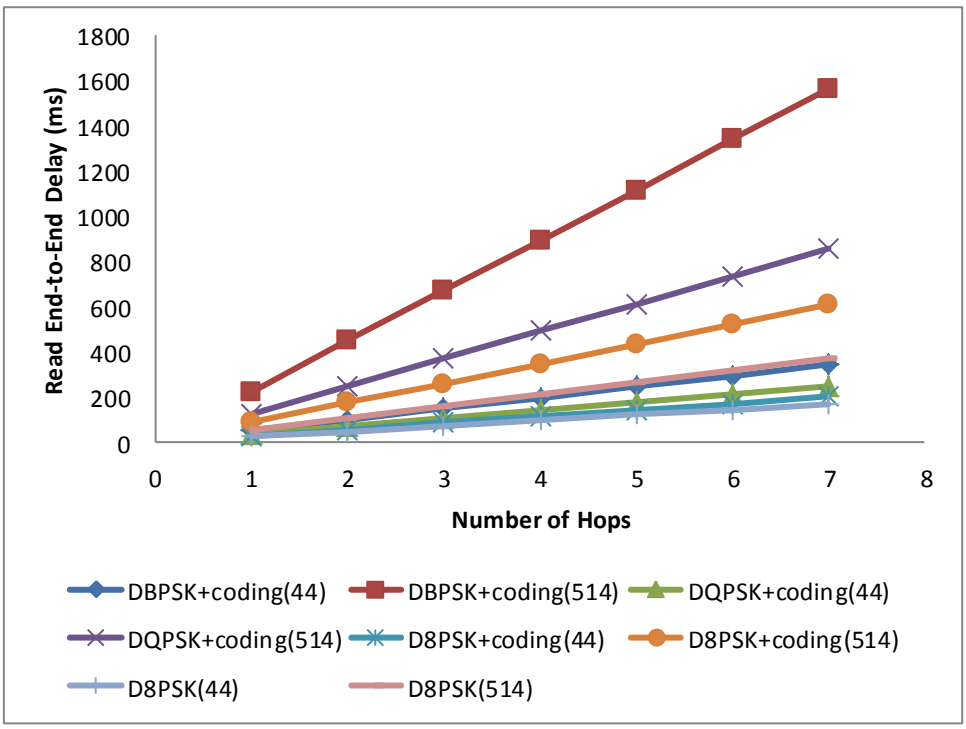


Figure 9: Minimum end-to-end delay for the Read exchange as a function of the transmission mode and hop distance in PLC PRIME, for $l_{resp} = 44$ and $l_{resp} = 514$

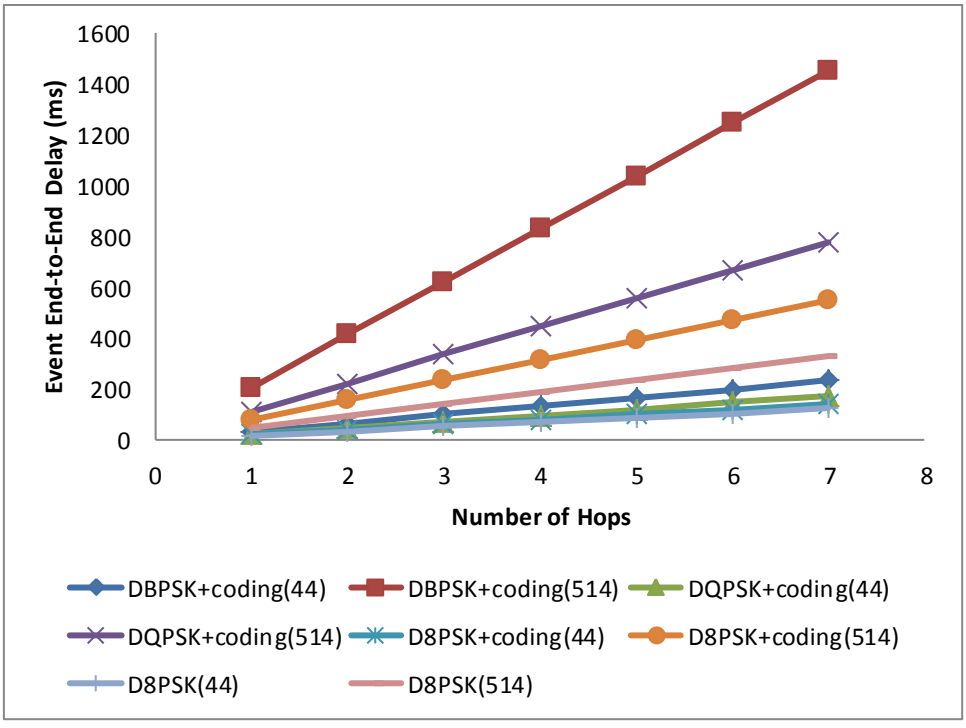


Figure 10: Minimum end-to-end delay for the Event exchange as a function of the transmission mode and hop distance in PLC PRIME, for $l_{resp} = 44$ and $l_{resp} = 514$

In order to assess the suitability of the PLC PRIME technology for e-balance, we will now verify whether the bottleneck interface at the Base Node is able to support the traffic patterns estimated for the Bronsbergen (Section 3.3.1) and Batalha (3.3.2) validation scenarios. Since the Energy Balancing request and response

messages are individually provided in Table 3 and the Neighborhood Monitoring messages are periodic, the Event exchange pattern will be used to approximate both. For each message type *i*, the fraction of required capacity (φ_i) will be calculated as follows:

$$\varphi_i = \frac{\lambda_i}{f_{event}(i)} \quad (12)$$

Where λ_i is the message rate required for message type *i* and $f_{event}(i)$ is the maximum rate for messages of type *i* supported by the communications technology (the length of messages of type *I* is taken from Table 3 or Table 5). In order to guarantee that the capacity of the technology is enough to support the estimated traffic the following condition must be respected regarding the total capacity consumed by the aggregate traffic pattern (Φ):

$$\Phi = \sum_i \varphi_i \leq 1.0 \quad (13)$$

Considering the worst case PLC PRIME transmission mode (DBPSK+coding), $\Phi \approx 0.43$ for the Bronsbergen scenario, which means that 57% of the capacity is still available to support additional services. Foe the Batalha scenario, $\Phi \approx 0.14$ leaving 86% of spare capacity.

4.2.2 IEEE 802.15.4

This analysis will use [7] as the IEEE 802.15.4 reference specification. In Europe, this technology can operate in the 868 MHz (1 channels) and 2450 MHz (16 channels) frequency bands. The protocol architecture only addresses the PHY and MAC layers. This means that if multihop communication is required, routing will be managed by the higher layers.

Two different device types can participate in an IEEE 802.15.4 network: a full-function device (FFD) and a reduced-function device (RFD). The FFD has typically more processing, storage and energy resources and can operate in three modes: serving as a personal area network (PAN) coordinator, a coordinator, or a device. An FFD can talk to RFDs or other FFDs, while an RFD can talk only to an FFD. When multihop routing functions are available, these are supported by FFDs only. An RFD is intended for applications that are extremely simple, such as a light switch or a passive infrared sensor; they do not have the need to send large amounts of data and may only associate with a single FFD at a time.

The PHY layer supports different operating modes, with different data rates, corresponding to different combinations of frequency band and modulation (see Table 13). The PAN is configured to operate in a single operating mode, with no rate adaptation mechanisms being supported.

Table 13: IEEE 802.15.4 operating modes

PHY (MHz)	Frequency Band (MHz)	Modulation	Symbol Rate (kbaud)	Data Rate (kbit/s)
868 MHz	868–868.6	BPSK	20	20
		ASK	12.5	250
		O-QPSK	25	100
2450	2400–2483.5	O-QPSK	62.5	250

The PHY frame structure is depicted in Figure 11 and is common to all MAC frame types. The PHY payload is prefixed with a synchronization header (SHR), containing the preamble sequence and Start-of-Frame Delimiter (SFD) fields, and a PHY header (PHR) containing the length of the PHY payload in octets. Together, the PHY preamble, SFD and PHR total 6 octets, except for 868 MHz with ASK (8.5 octets). The PHY payload can have at most 127 octets in length. However, fragmentation support in 6LoWPAN allows the transmission of larger messages.

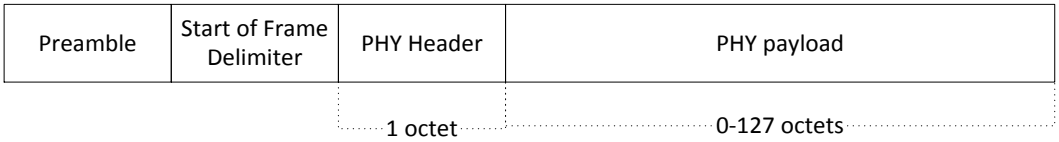


Figure 11: IEEE 802.15.4 PHY frame [7]

The MAC protocol defines two modes of operation: beaconed and non-beaconed mode. In beaconed mode, the standard allows the optional use of a superframe structure. The format of the superframe is defined by the coordinator. It is bounded by network beacons sent by the coordinator and is divided into 16 equally sized contention access slots. Optionally, the superframe can have an active and an inactive portion. During the inactive portion, the coordinator may enter a low-power mode. In beaconed mode, contention is solved using slotted CSMA/CA. The beacon frame is transmitted in the first slot of each superframe. The beacons are used to synchronize the attached devices, to identify the PAN, and to describe the structure of the superframes. In case of delay sensitive applications, a contention-free portion can be defined in the superframe structure, where reserved time slots, called Guaranteed Time Slots (GTS) – seven at most – can be assigned to specific modes and used according to the schedule defined in the beacon. Note that each GTS may occupy more than one timeslot. The superframe structure is in this case as depicted in Figure 12, where two GTSs are depicted as an example.

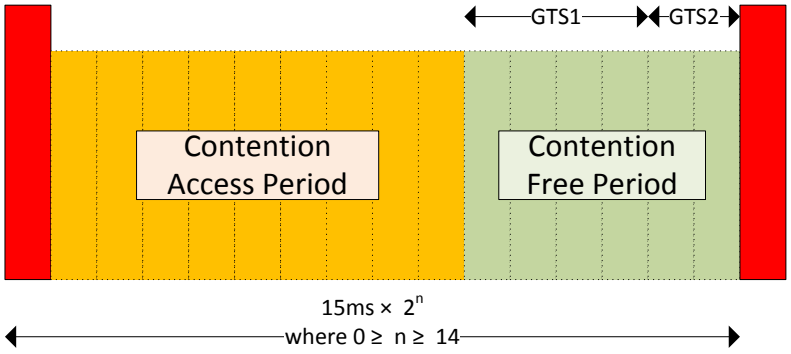


Figure 12: IEEE 802.15.4 superframe structure, based on [7]. The red stripes represent beacon frames

The coordinator may also employ non-beaconed mode, turning off the beacon transmissions. In this case, the superframe is not used. There is also the possibility of configuring the network to operate in peer-to-peer mode, without coordinators. In both cases contention is resolved based on unslotted CSMA/CA.

MAC addressing is designed in order to attain scalability and efficiency at the same time. Nodes are identified by a 64-bit IEEE address. However, there is the possibility of assigning shorter 16-bit addresses, thus significantly reducing MAC header overhead. A PAN identifier of 2 octets can also be omitted from the address in frame headers.

The MAC layer defines four frame types: Beacon, Data, Acknowledgement and Command. These are depicted in Figure 13, Figure 14, Figure 15, Figure 16, respectively. All frame types start with the Frame Control field (see Figure 17) and end with a 16-bit Frame Check Sequence (FCS). The Frame Control field latter controls whether security is enabled or not, bears data pending information, allows acknowledgement frames to be requested and defined the addressing mode of the frame. The Beacon frame identifies the coordinator and PAN, defines the structure of the superframe – including the assignment of GTSs. It also notifies the devices about pending data in the coordinator queues, providing support to the implementation of power saving mechanisms. The Data frame is self-explanatory. The optional Acknowledgement frame is employed when reliable data transmission is required. The Command frame is used for handling all MAC peer entity control transfers, e.g., association and disassociation to a coordinator.

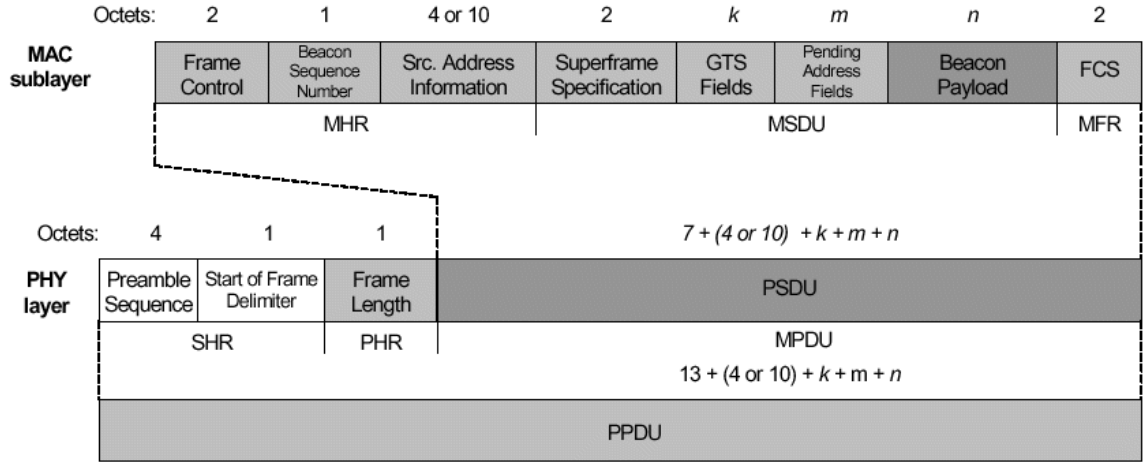


Figure 13: IEEE 802.15.4 MAC Beacon frame format [7]

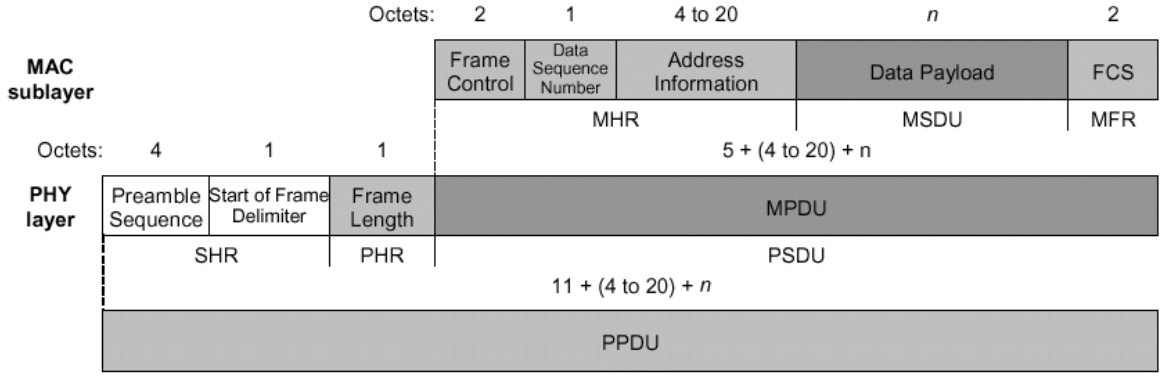


Figure 14: IEEE 802.15.4 MAC Data frame format [7]

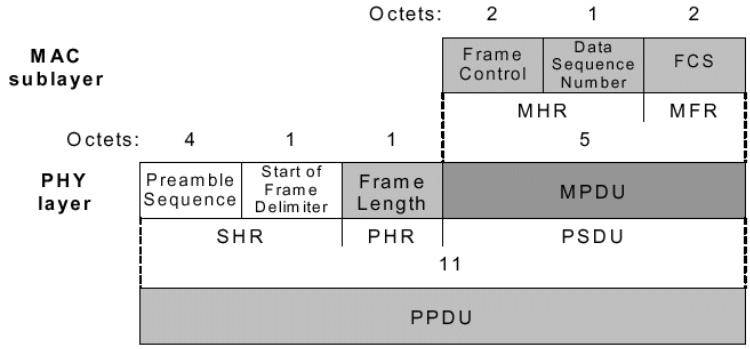


Figure 15: IEEE 802.15.4 MAC Acknowledgement frame format [7]

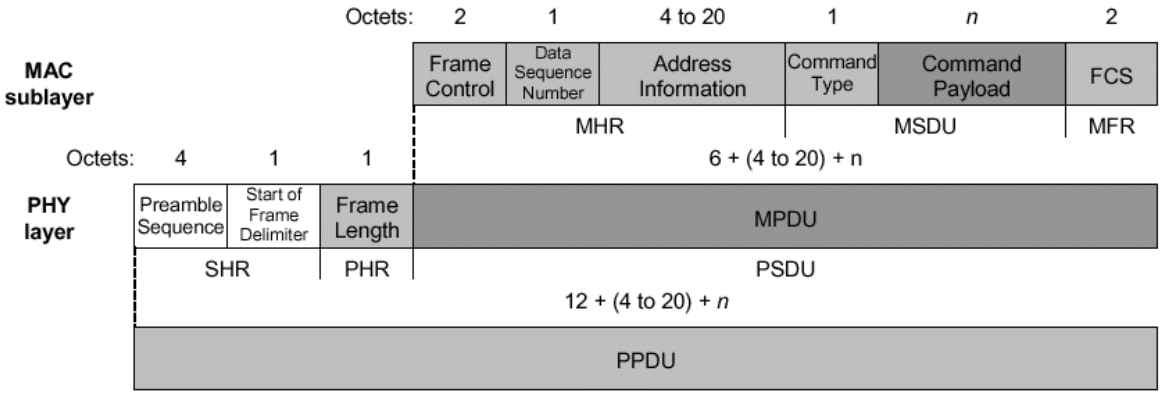


Figure 16: IEEE 802.15.4 MAC Command frame format [7]

Bits: 0–2	3	4	5	6	7–9	10–11	12–13	14–15
Frame Type	Security Enabled	Frame Pending	Ack. Request	PAN ID Compression	Reserved	Dest. Addressing Mode	Frame Version	Source Addressing Mode

Figure 17: IEEE 802.15.4 MAC Frame Control header field [7]

During continuous transmission, there is a minimum gap or inter-frame space (IFS) between two consecutive frames. The length of the IFS period is dependent on the size of the frame that has just been transmitted. Frames of up to *aMaxSIFSFrameSize* octets in length are followed by a short IFS (SIFS) period of duration at least equal to *macMinSIFSPeriod* symbols. Frames with lengths greater than *aMaxSIFSFrameSize* octets shall be followed by a long IFS (LIFS) period with duration of at least *macMinLIFSPeriod* symbols. Between a Data or Command frame and its Acknowledgement, there is a special IFS (t_{ack}). These parameters are configured in the Management Information Base (MIB) of the device.

Binary exponential backoff mechanism is used to ensure collision avoidance. Before each access attempts, the node waits for a random number of slots between 0 and 2^{BE}, where BE is the binary exponent. The length of a backoff slot is given by *aUnitBackoffPeriod*. For each new frame, the binary exponent starts at *macMinBE* and is incremented each time that the node loses contention, up to *macMaxBE*.

The analysis that follows, considers peer-to-peer operation with CSMA/CA and the use of 16-bit short addresses. Data frame transmissions are assumed to be confirmed by Acknowledgement frames. Once again, we take the simplified assumption that there are no collisions or other sources of frame loss. The main PHY and MAC layer parameters used in the analysis are listed in Table 14 for the considered transmission modes. The assigned values correspond to the default ones defined in the IEEE 802.15.4 standard document.

Table 14: IEEE 802.15.4 PHY and MAC parameters

Parameter	868 MHz BPSK	868 MHz ASK	868 MHz O-QPSK	2450 MHz O-QPSK
$macMinSIFSPeriod$ (symbols)	12	12	12	12
$macMinLIFSPeriod$ (symbols)	12	12	12	12
$aUnitBackoffPeriod$ (symbols)	20	20	20	20
t_{ack} (symbols) [2]	12	12	12	12

[2] The minimum value of t_{ack} was used, corresponding to the default value of the TX/RX turnaround time ($aTurnaroundTime$).

$macMinBE$	3	3	3	3
$macMaxBE$	3	3	3	3
Maximum PHY payload length (octets)	127	127	127	127

It is considered that the sink node of the PAN constitutes the bottleneck. Consequently, the exchange rate results are only meant to estimate single hop performance around the sink node. Multihop performance depends highly on the topology and would better be obtained through computer simulation, though we present figures for minimum delay. It is assumed that 6LoWPAN fragmentation is supported.

The time required to perform a Read exchange in milliseconds can be calculated as follows:

$$T_{read} \sim T_{req} + T_{resp} \tag{14}$$

$$T_{req} = \frac{l_{IFS}+minBO}{R_s} + \frac{(l_{SHR}+l_{PHR}+l_{hData}+l_{req})\cdot 8}{R_b} + \frac{t_{ack}}{R_s} + \frac{(l_{SHR}+l_{PHR}+l_{Ack})\cdot 8}{R_b} \tag{15}$$

$$T_{resp} = N_{frag} \cdot \left[\frac{l_{IFS}+minBO}{R_s} + \frac{(l_{SHR}+l_{PHR}+l_{hData}+l_{hFrag}+l_{resp})\cdot 8}{R_b} + \frac{t_{ack}}{R_s} + \frac{(l_{SHR}+l_{PHR}+l_{Ack})\cdot 8}{R_b}\right] \tag{16}$$

Where N_{frag} is the number of fragments, l_{IFS} is the SIFS/LIFS length in symbols, $minBO$ is the minimum backoff interval in symbols, l_{SHR} is the SHR length in octets, l_{PHR} is the PHR length in octets, l_{hData} is the length of the MAC Data header and tail, l_{hFrag} is the length of the 6LoWPAN fragmentation header, l_{Ack} is the length of the MAC Acknowledgement frame, R_s is the symbol rate, R_b is the bit rate, l_{req} and l_{resp} are the lengths of the request and response messages, respectively. The Read exchange frequency can be easily obtained as:

$$f_{read} = \frac{1}{T_{read}} \tag{17}$$

For the Event exchange, the time and frequency are given by the following equations:

$$T_{event} \sim T_{resp} \tag{18}$$

$$f_{event} = \frac{1}{T_{event}} \tag{19}$$

The maximum exchange rates that can be obtained for the Read and Event scenarios as a function of the data message size and transmission mode are depicted in Figure 18 and Figure 19.

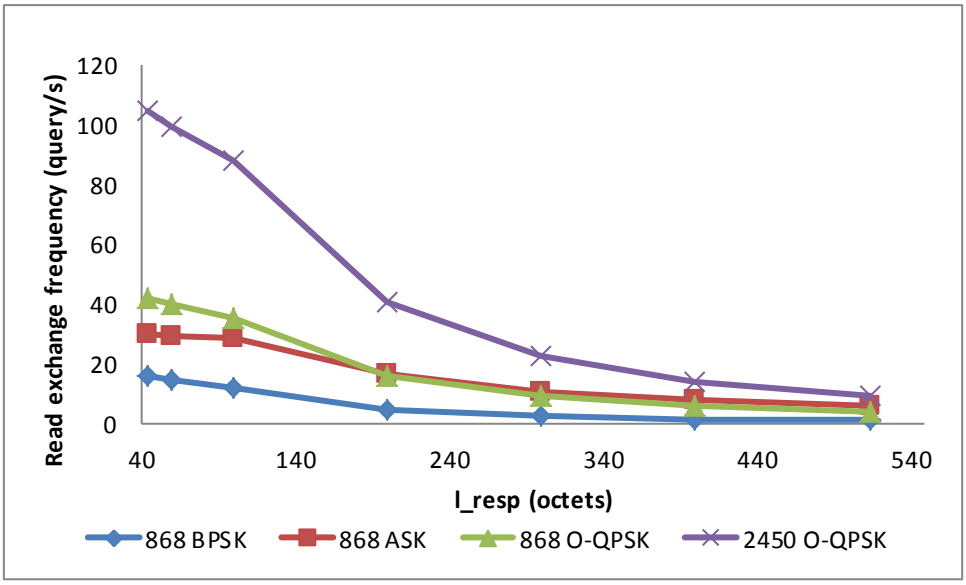


Figure 18: Read exchange rate in IEEE 802.15.4, as a function of message size and transmission mode

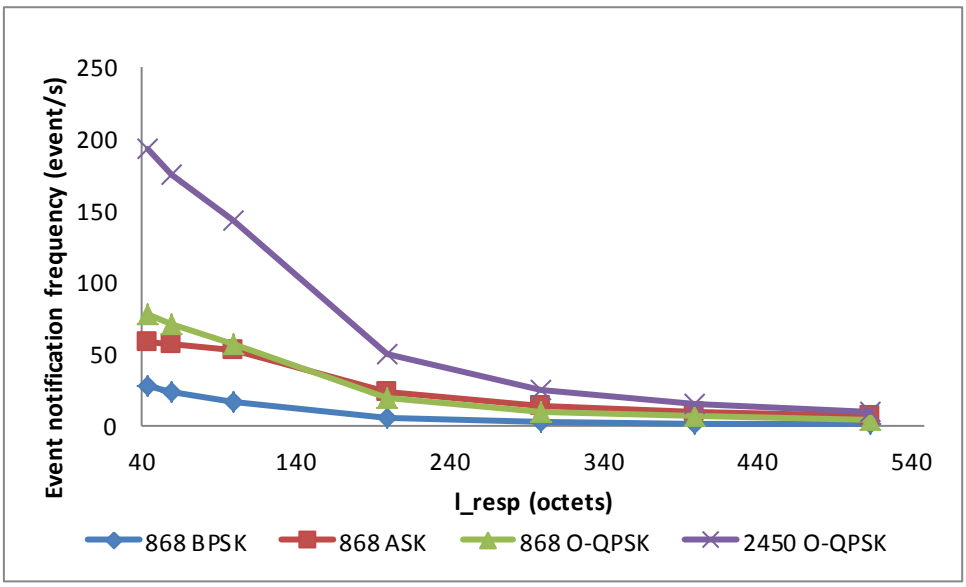


Figure 19: Event notification rate in IEEE 802.15.4, as a function of message size and transmission mode

The minimum end-to-end delay estimates can be calculated in a similar way to PLC PRIME (see equations (10) and (11)). Those delays are depicted in Figure 20 and Figure 21, respectively.

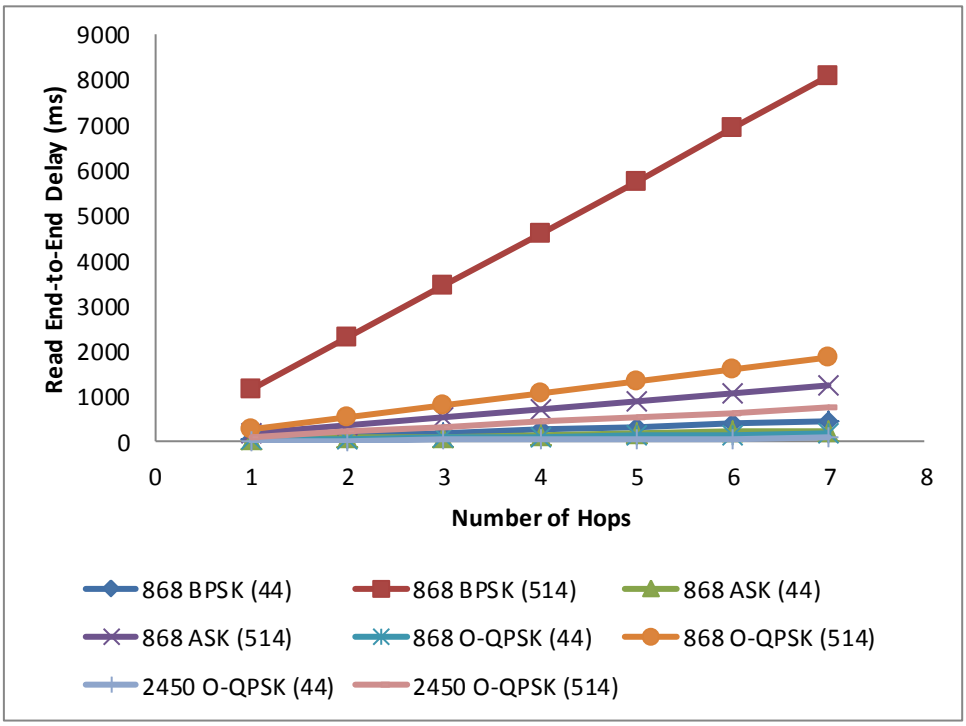


Figure 20: Minimum end-to-end delay for the Read exchange as a function of the transmission mode and hop distance in IEEE 802.15.4, for $l_{resp} = 44$ and $l_{resp} = 118$

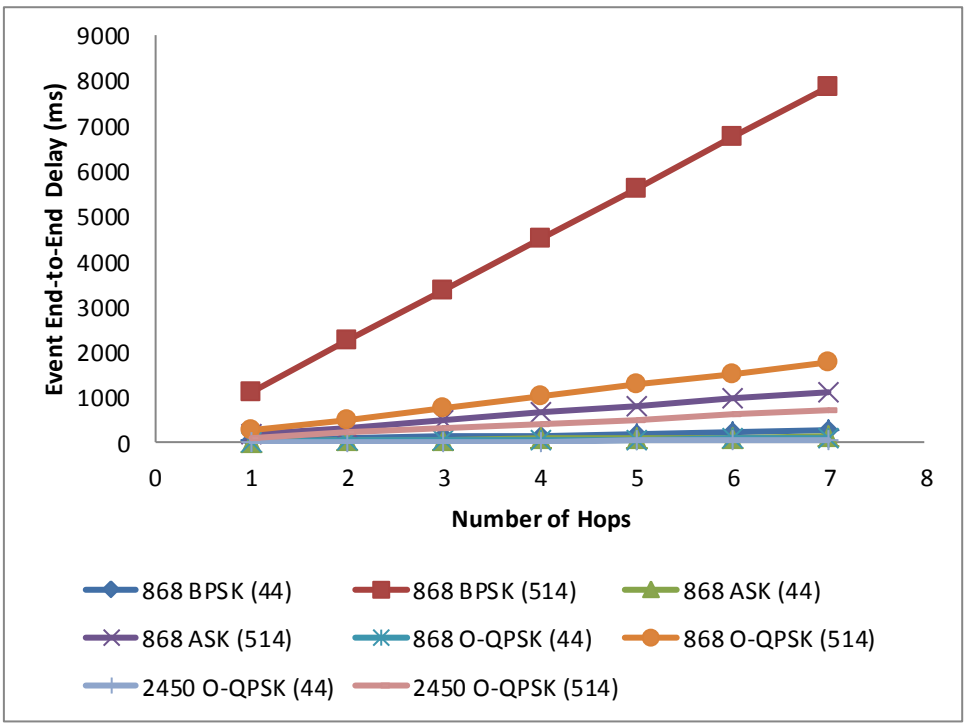


Figure 21: Minimum end-to-end delay for the Event exchange as a function of the transmission mode and hop distance in IEEE 802.15.4, for $l_{resp} = 44$ and $l_{resp} = 118$

Based on these results, the IEEE 802.15.4 technology was validated in a similar way as for PLC PRIME, using Table 3 and Table 5 for traffic characterization. It was concluded that the 868 MHz BPSK transmission mode is not able to support the Bronsbergen scenario, though it can support the Batalha scenario. In this case, $\Phi \approx 0.78$, leaving 22% of spare capacity. Regarding 868 MHz ASK and O-QPSK, they are both able to support both traffic scenarios. For the Bronsbergen scenario, $\Phi \approx 0.31$ and $\Phi \approx 0.40$, respectively. For the Batalha scenario, $\Phi \approx 0.10$ and $\Phi \approx 0.13$, respectively. For 2.4 GHz O-QPSK, $\Phi \approx 0.13$ and $\Phi \approx 0.04$, respectively for the Bronsbergen and Batalha scenarios.

4.2.3 LTE

LTE was specified by 3GPP and forms the last step in the evolution of 3G technologies rooted in UMTS, aiming to deploy an IP-only infrastructure and supporting data rates up to 150 Mbit/s the downlink and up to 50 Mbit/s uplink. This section presents a short description of LTE's radio access network, the Evolved UMTS Terrestrial Radio Access Network (E-UTRAN).

The protocol stack in the E-UTRAN consists of layers 1-3, where layer 1 corresponds to the Physical layer, layer 2 comprises the MAC, Radio Link Control (RLC), Packet Data Convergence Protocol (PDCP), and layer 3 corresponds to the Radio Resource Control (RRC). This section focuses layers 1 and 2, whose inter-layer relationships are depicted in Figure 22.

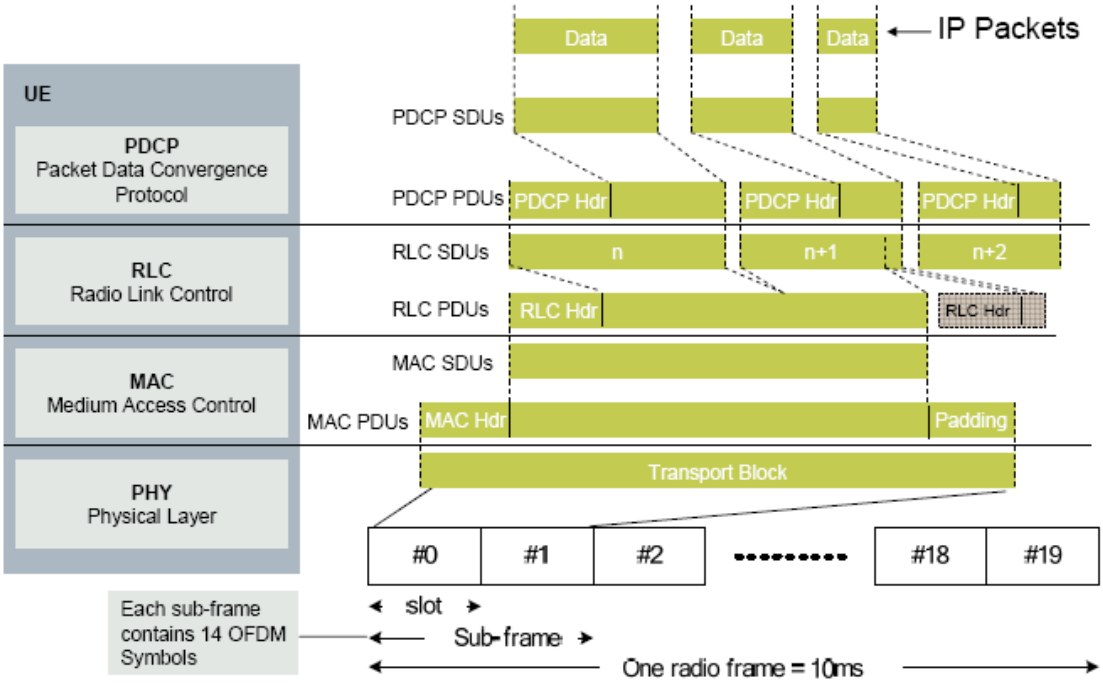


Figure 22: E-UTRAN inter-layer relationships. [8]

The Physical layer employs OFDMA for downlink and SC-FDMA for uplink and can operate in either FDD or TDD mode. Resources are divided in time, frequency and space. In the time domain, resources are structured in frames of 10 ms, which are further subdivided into ten 1ms subframes, each of which is split into two 0.5-ms slots. Each slot contains seven OFDM symbols in case of the normal cyclic prefix (CP) length, or six if the extended CP is configured in the cell. In the frequency domain, resources are grouped in units of 12 subcarriers. A resource block (RB) consists of one unit of 12 subcarriers for the duration of one slot. The smallest unit of resource is the Resource Element (RE) which consists of one subcarrier for a duration of one OFDM symbol. Consequently, a RB comprises 84 (normal CP) or 74 (extended CP) REs. A transport block is a group of resource blocks with a common modulation/coding. Each radio subframe is 1 ms long; each frame is 10 milliseconds. Multiple UEs can be serviced on the downlink at any particular time in one transport block. The Physical layer is also responsible for mapping the transport channels (the services offered to the MAC) into physical channels.

The MAC layer implements medium access, maps the logical channels into the transport channels, implements the Hybrid Automatic Repeat-reQuest (HARQ) error recovery process and performs coding and modulation selection for the next transport block. The MAC header is formed by multiple sub-headers, one for each Control Element (special information elements transmitted by the MAC: e.g., uplink buffer status report, power headroom supported by the user equipment, etc.), MAC PDU or padding.

The RLC layer can operate in one of three modes: transparent, acknowledged and unacknowledged. In transparent mode, it adds no headers and simply forwards the SDUs down to the MAC or up to the PDCP layer. The acknowledgement mode activates the ARQ mechanism. This ARQ applies is performed ta RLC SDU level, while MAC HARQ applies to a transport block. The RLC also performs segmentation and reassembly of Service Data Units (SDUs), in order to fit in the transport block. The segmentation and reassembly mechanism completely decouples the size and boundaries of the higher layer messages from MAC payload size limits and boundaries: each RLC PDU may include chunks from more than one RLC SDU and each RLC SDU may correspond to chunks in more than one RLC PDU (see Figure 22). The RLC also assures in-order delivery of SDUs.

The PDCP includes security functions and also adapts the higher layer messages to the characteristics of the underlying technology. PDCP functions in the user plane include ciphering, ROHC header decompression, sequence numbering and duplicate removal. PDCP functions in the control plane include ciphering, integrity protection, sequence numbering and duplicate removal. There is one PDCP instance per radio bearer.

The characteristics of LTE are very different from those of PRIME and IEEE 802.15.4 technologies. For example, LTE transmits downlink and uplink traffic in different channels. The expected throughput is also considerably different, with LTE being a broadband technology. The diversity of possible configurations and the fact that LTE will most likely be hired by the utility from telecom companies (which also serve other subscribers) also contributes to make a detailed performance analysis pointless to our purposes. However it is useful to look at existing works in which the LTE performance was measured. In [9], a testbed was deployed in order to evaluate the performance of both LTE TDD and LTE FDD. The measured latencies did not go beyond 23 ms for UDP (100-byte packets, including the UDP and IP headers) and beyond 25 ms for TCP (1500-byte segments, including TCP and IP headers). Regarding the throughput performance, downlink/uplink data rates fell in the intervals 20-35/3-8 Mbit/s for three UEs sharing the cell.

4.2.4 Alarm Aggregation Scheme for the LV-FAN

Automatic fault detection and location constitutes a very important improvement in LV grid management, which will be enabled by Smart Grid technologies. The most frequent faults expected to occur in the LV grid are related with outage, the violation of the operating voltage limits, or overcurrent due to short circuit. These faulty situations are detected by FAN sensors and/or SMs and reported to the LV-GMU in the form of alarm notifications. The notifications may then climb further for processing by higher level MUs. Once the fault is located, the fault is isolated or corrective action is started, which may be done automatically through the grid's self-healing mechanisms, or by deploying repair teams to the spot or to the device where the fault originated.

For all the types of anomalies mentioned above, a high degree of correlation is expected between sensors in the same feeder: an outage, if originated at the secondary substation, will probably affect all the nodes in the feeder, or, if it is due to a broken cable or malfunctioning distribution cabinet, it will affect at least all nodes located downstream from the fault; similarly, overvoltage and undervoltage situations may likely be detected by several sensor nodes simultaneously; a short-circuit situation will also be likely to cause an overcurrent in the upstream portion of the feeder. Since all nodes detecting the fault event will report upstream to the LV-GMU, high detection correlation may cause an alarm implosion, leading to congestion in the LV-FAN, with consequent loss of alarm messages. The loss of alarm messages also means that the fault location algorithms may get their accuracy reduced. It should be noted that the LV-FAN constitutes the edge of the distribution grid, being significantly braided and thus comprising many nodes including distribution cabinets, SMs, field sensors and actuators. On the other hand, the technology is likely to support only low data rates (e.g., NB-PLC or RF-Mesh). All these factors concur to make it more prone to congestion. A solution to the alarm implosion is to aggregate the alarm messages taking advantage of the correlation of alarms, as well as the correlation between the positions of nodes along the feeder.

The alarm aggregation scheme that we propose for e-balance, exploits the fact that the LV grid topology is radial, i.e., tree-like. The feeder's MV/LV transformer is located within the secondary substation, which forms its root. The starting segment begins to branch and each new branch leads to more branches as we approach the edges of the feeder. The important characteristic to retain is that we can establish an ordered relationship between the positions of nodes along the feeder, with each node being either upstream or downstream from each of its neighbors. If this topology is well known, it can be used to represent groups of cascading nodes as ranges, from the downmost to the uppermost node. In this case, the latter's identifiers are enough to represent all the range, since the ordered relationship is well known. This avoids including the identifiers of all the nodes in the range. In practice, the alarm notification will be compressed. The proposed scheme provides better results if the alarm data follows multihop convergecast paths, which are usually featured by NB-PLC and RF-Mesh. Even so, this advantage comes out when these paths obey to the ordered relationship between nodes (i.e., nodes in the routing paths occupy succeeding positions on the ordered grid topology). This is not always possible, since succeeding nodes may not be able to communicate due to the propagation characteristics of the environment, or the respective links may be subject to too much interference. Consequently, we propose a routing metric that tries to build routing paths that obey to the ordered relationship between nodes whenever possible, while retaining some flexibility to find alternative paths whenever required by the propagation characteristics of the environment.

4.2.4.1 Alarm Aggregation Scheme

In order to implement the aggregation scheme, a special alarm information item was defined, as depicted in Figure 23. This information item has a header with two fields of 2 octets each, followed by a body with a variable number of node ranges (see Figure 24):

- Type: Alarm type identifier. The alarm aggregation is done separately for each type of alarm. As such, the information item must identify the type of alarm for which it applies.
- Length: Number of node rage items in the body.

Each node range item represents a range of succeeding nodes in the ordered grid topology. It is included in the body has the following fields:

- Up Node: This is the identification of the node that is located uppermost in a range of contiguous nodes where the alarm identified in the first field is raised.
- Down Node: This is the identification of the node that is located downmost in a range of contiguous nodes where the alarm identified in the first field is raised.

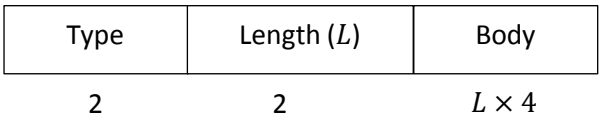


Figure 23: Alarm information item

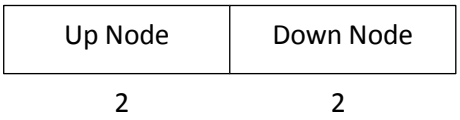


Figure 24: Node Range

The pseudocode of the algorithm is listed in Figure 25. Given a radial grid topology, the proposed alarm aggregation scheme aims to represent the nodes where the alarm condition is detected, using the minimum number of transmitted octets. In order accomplish this goal, the reporting nodes are represented with the minimum number or alarm information items. This is illustrated by the example in Figure 26. Node number 0 corresponds to the LV-FAN gateway and thus is the sink node for the reception of LV-FAN alarms. Assuming that an outage alarm (e.g., type 20) is active is all the other nodes, using a similar information item format, 30 octets would be needed without aggregation (except that single node identifiers of 2 bytes would be used instead of node ranges): $2 + 2 + 13 \times 2$. With aggregation, three node range items are enough to represent the overall alarm detection situation: [1, 9], [4, 6] and [10, 13]. This corresponds to a total of 16 octets ($2 + 2 + 3 \times (2 + 2)$).

Notice that this is the amount of data that reaches the LV-FAN gateway. The alarm information items are gradually built along the convergecast tree, as the data climbs from the leaf nodes to the gateway. In order to avoid redundant transmission of the same data, the nodes that stay upwards in the tree should wait from the data coming from their siblings for a predefined amount of time, the aggregation timer. A good heuristic is to have this amount of time to vary proportionally with the number of siblings. Each node aggregates its own alarm data with the data arriving from its siblings (`alarmItemSet2`) according to the function **MergeAggItems**, which assumes that the alarm types of the aggregated items are the same. The result is kept in `alarmItem1`. Each time the aggregation timer expires, the contents of `alarmItem1` are sent to next node in case there are changes since the last transmission. In the pseudocode, function **IsParent(X, Y)** returns true if **X** is the parent node of **Y**, and false otherwise. Function **IsBetween(X, Y Z)** returns true if **X** is located between **Y** and **Z** in the node hierarchy and false otherwise. In Figure 26, the contents of the messages issued by each node are represented, assuming the ideal situation where each node is able to gather the data from all its siblings before sending its aggregated result upwards.

```
MergeAggItems(alarmItem1, alarmItem2)
foreach (item2 in alarmItem2) {
      node = item2.downNode
      alarmItem1 = AddNodeToAggSet(alarmItem1, node);
      while (node != item2.upNode) {
            node = GetParent(node);
            alarmItem1 = AddNodeToAggSet(alarmItem1, node);
      }
}
return alarmItem1;


AddNodeToAggSet(alarmItem, node)
inserted = false;
foreach (range in alarmItem) {
      if (node != range.downNode && node != range.upNode) {
            if (IsParent(range.upNode, node)) {
                  range.upNode = node;
                  inserted = true;
                  break;
            }
            else if (IsParent(node, range.downNode)) {
                  range.downNode = node;
                  inserted = true;
                  break;
            }
            else if (IsBetween(node, range.upNode, range.downNode)) {
                  inserted = true;
                  break;
            }
      }
}
if ( !inserted ) {
      newRange.upNode = node;
      newRange.downNode = node;
      alarmItem.insert(newRange);
}
return alarmItem;
```

Figure 25: Pseudocode of functions MergeAggItems and AddNodeToAggSet

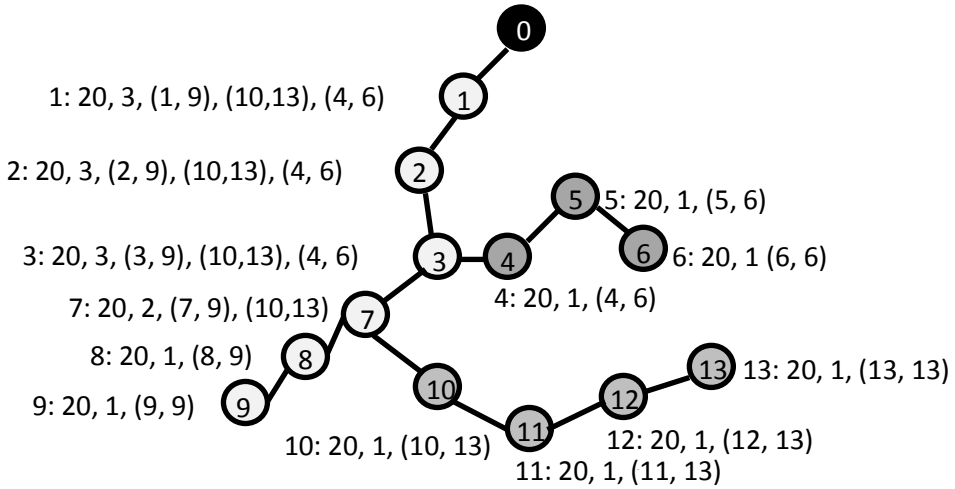


Figure 26: Alarm aggregation example, including the contents of the aggregated alarm item issued by each node

4.2.4.2 Hop-by-Hop Reliable Delivery

A significant number of alarm situations (e.g., short-circuit) may lead to outage within a short time interval (e.g., a few seconds). During normal operation, network nodes are fed from the LV grid. When an outage occurs, affected nodes must resort to their batteries or super-capacitors, which give them a limited lifetime to transmit the alarm notifications. Since the packet error probability is very high in NB-PLC and low power RF-Mesh, mechanisms must be in place to increase the transmission reliability with minimum overhead and energy consumption. In our proposal, a hop-by-hop reliable transmission scheme is proposed. The message formats are depicted in Figure 27 and comprise the following fields:

- Code (1 octet): This indicates the type of message, which can be Data (0) or Acknowledgement (1).
- Last Aggregator Node (2 octets): This is the identifier of the node that has most recently processed and issued the Data message.
- Sequence Number (1 octet): This is the sequence number of the message. The meaning of this sequence number is local to the node that issued the message (the Last Aggregator Node) and serves the purpose of matching the Data with the respective Acknowledgement.
- Aggregate Items (n): These are the alarm information items (see Figure 23) carried by the message.

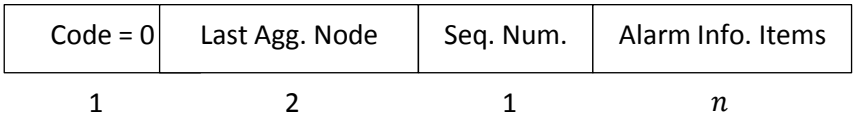


Figure 27: Reliable delivery Data message

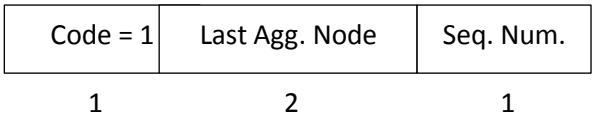


Figure 28: Reliable delivery Acknowledgement message

Each node in the path, upon reception of a Data packet, issues the respective acknowledgement to the Last Aggregator Node. The latter can then mark the acknowledged items as confirmed. In case the acknowledgement is not received within a predefined time interval, the Data message is retransmitted.

It should be noted that reliable delivery would be required even if alarm aggregation is not used, so it forms an independent mechanism.

4.2.4.3 Multihop Routing Metric

In order to maximize the chances of reducing the message size, the alarm data should follow as much as possible the hierarchy of nodes defined by the grid topology. A possible way to enforce this would be to establish the routes as static and according to this grid topology. However, it is not guaranteed that these static links would be always available for transmission, since they may be subject to shadowing, interference and other propagation phenomena, besides node failure. In fact, node failure may even be caused by the very grid malfunction that led to the alarm situation. On the other hand, we must bear in mind the initial motivation for alarm aggregation: to reduce the amount of transmitted data, as well as the energy consumption, such that the node and network lifetime available for alarm transmission during an outage is maximized – this will in turn maximize the fraction of alarm reports that are able to reach the sink node. It may thus be advantageous to follow alternative paths with less chance for aggregation, if the overall result is an increase of alarm delivery ratio. The multihop routing metric should be able to enforce compliance with the default routing path (i.e., the routing path that follows the LV grid topology), while shifting to alternative paths if the default one becomes too costly. The proposed routing metrics is based on the Airtime Link Metric (ALM) defined for mesh networking in the IEEE 802.11 standard, which is expressed in the following equation:

$$c_a = \left[O + \frac{B_t}{r}\right] \cdot \frac{1}{1-e_f} \tag{20}$$

Where O is the channel access overhead (frame headers, training sequences, access protocol frames, etc.), B_t is the number of data bits in the test or reference frame, r is the data rate and e_f is the frame error probability for a frame of size B_t transmitted at rate r.

The proposed aggregation routing metric (c_{agg}) consists of imposing a penalty on the ALM whenever the next hop of an upstream data message does not correspond to the parent node in the LV grid topology. This is expressed by the following equation:

$$\begin{cases} c_{agg} = c_a, \ \ if\ Parent(nextHop, sender) \\ c_{agg} = \alpha \cdot c_a, \ \ otherwise \end{cases} \tag{21}$$

Where $\alpha \geq 1$ is the penalty factor.

4.2.4.4 Simulation Results

The proposed alarm aggregation scheme was evaluated using the ns-3 simulator. Since ns-3 does not support PLC PRIME or routing in IEEE 802.15.4 networks, the IEEE 802.11s extension for mesh networking was used, in which the HWMP protocol employs the ALM metric to select routes. The simulated deployment topologies consist of square matrices of different sizes: 5×5, 7×7, 11×11 and 13×13. The nodes in a matrix are only able to communicate with their vertical and horizontal immediate neighbors. For each of these matrix sizes, random radial grid topologies were built, where the central node corresponds to the root node, i.e., the LV-GMU. This is also the sink node for the alarms. The remaining nodes consist of grid sensor nodes that are capable of issuing alarms upon anomaly detection. In the considered scenario, it is assumed that an alarm situation will be detected by all nodes in the grid topology at $t = 1000s$. From then on, all nodes will try to transmit an alarm notification to the sink. The time interval between $t = 0s$ and $t = 1000s$ is used as a setup phase, where HWMP routes are established and stabilized.

Three configurations were compared:

- No aggregation.
- Aggregation with HWMP routing (standard ALM metric).

- Aggregation with modified HWMP routing (modified ALM metric).
- Optimal aggregation (see below).

The considered performance metrics were the following:

- **Transmission cost in terms of number of transmitted bytes.**
- **Transmission cost in terms of total number of transmitted messages.**
- **Delivery Delay from beginning of alarm situation until all alarms are delivered.**

These only take the application layer into account, i.e., the reliable delivery data and acknowledgement packets. I this way, we have kept the results less dependent on the underlying technology and protocol stack. However, the cost in terms of total number of transmitted messages is useful as a coarse evaluation of the underlying protocol overhead, since the headers of underlying protocols will be added to each packet.

Since our model does not consider finite energy storage, all alarm messages are delivered to sink sooner or later. However, energy requirements may be indirectly evaluated based on the considered metrics.

In the non-optimal aggregation configurations, the aggregation timer of each node was set to $0.5s \times N_{desc}$, where N_{desc} is the number of descendants of that node. When there is no aggregation, each node immediately forwards received data packets and no timers are set.

In optimal aggregation, the proposed alarm aggregation mechanism is used without changes. However, the routing paths always follow the grid hierarchy and the aggregation timers at intermediate nodes never expire before the alarms of all siblings are received. In this specific configuration, performance evaluation was analytical and only the cost metrics were considered.

The results for the three metrics are depicted in Figure 29, Figure 30 and Figure 31 as a function of network size. The latter is given in terms of the size of the square matrix side in number of nodes. The cost metrics are normalized to the respective values without aggregation. This facilitates the evaluation of the aggregation mechanisms.

From the cost metrics, it is obvious that the advantage of the proposed aggregation mechanism increases with the size of the network. With the 11x11 matrix topology, it achieves cost reductions of approximately 30% and 20% respectively for the number of transmitted bytes and the number of transmitted messages. It can also be seen that the modified ALM slightly reduces the cost, though less than expected. This may indicate that the amount of traffic exchanged before the alarm situation started was not enough to appropriately set the modified ALM metric values in each node, thus leading to routes that only slightly follow the electrical grid topology. This result points to the need of further tests considering the transmission of traffic streams other than alarms during the normal operation of the grid. It should be noted that the improvements achieved by the aggregation mechanisms are still far from the optimal, which points to improvements between 50% and 80% for the considered network sizes. This constitutes motivation for future work on routing metrics and timer parameterization.

Regarding the delivery delay, the aggregation mechanisms pay a significant price compared with the situation without aggregation. This is due to the aggregation timers, which force each node to wait for the alarms issued by its siblings. Additional tests (not depicted) have shown that the cost metrics of the aggregation mechanisms can be further reduced by increasing the value of the aggregation timer, though this will naturally increase even more the delivery delay.

As a final note, it should be recalled that the present study did not take the energy limitations of sensor nodes into account. In case of an outage situation, the sensor nodes would have to operate from batteries or supercapacitors, possibly complemented with energy harvesting schemes (e.g., small solar panel). Alarm delivery reliability would depend on how long the nodes would remain energized. In this scenario, the cost would directly translate to energy consumption and hence to node and network lifetime. Though alarm aggregation is able to reduce the cost and thus overall energy consumption, load balancing is also important as a means to achieve a more distributed energy consumption pattern, which can ultimately lead to an increase of network lifetime and improved reliability. These aspects will also be exploited in future work.

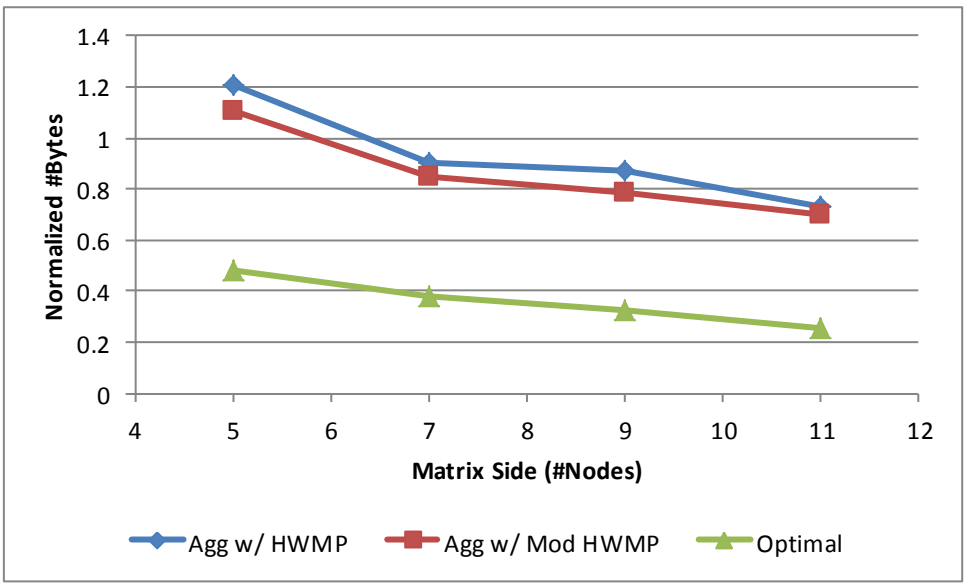


Figure 29: Normalized cost in terms of number of transmitted bytes as a function of network size

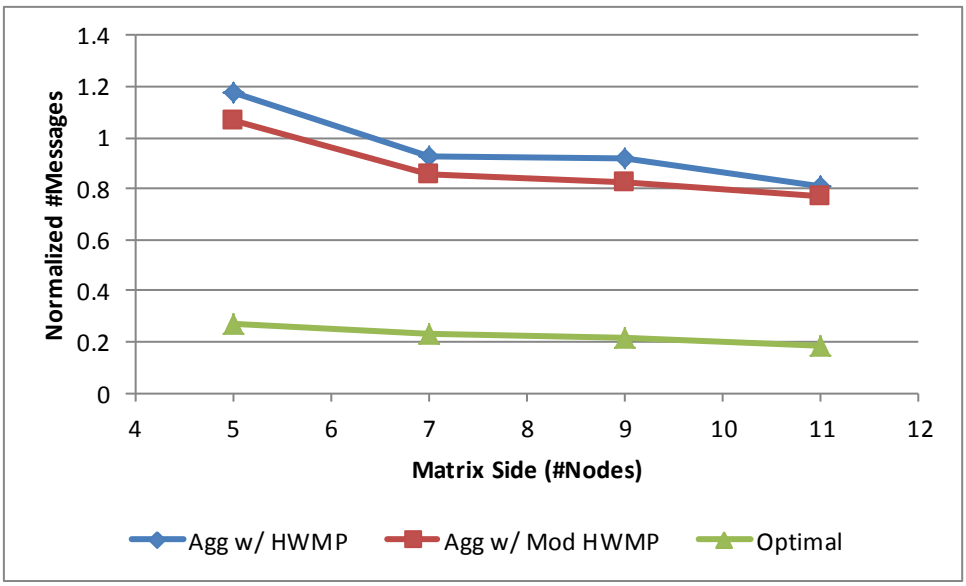


Figure 30: Normalized cost in terms of number of transmitted messages as a function of network size

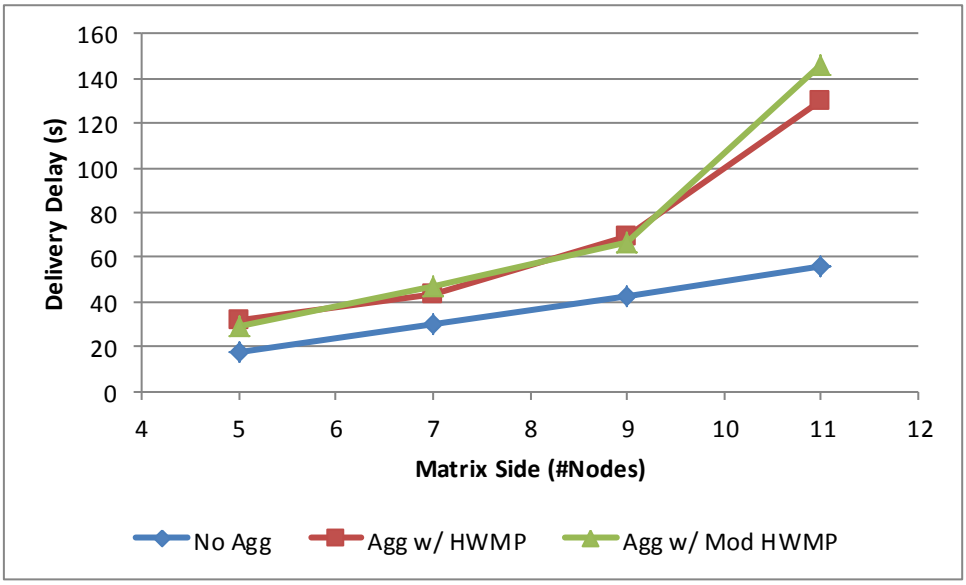


Figure 31: Average alarm delivery delay in seconds as a function of network size

4.2.5 Conclusions

In Section 4.2, a representative technology from each of the three most significant classes of technologies applicable in the FAN was selected: PLC PRIME, IEEE 802.15.4 and LTE.

The performance analysis of PLC PRIME and IEEE 802.15.4 allows a direct comparison between these technologies regarding their capability to support the e-balance middleware services. It can be concluded that IEEE 802.15.4 promises to offer higher message rates than PLC PRIME, while keeping end-to-end delay within the same order of magnitude. This is true even if the operating frequency band is 868 MHz, as long as the modulation is ASK or O-QPSK. When the modulation is BPSK, the performance of IEEE 802.15.4 becomes manifestly worse than PLC PRIME. IEEE 802.15.4 at 2.4 GHz achieves the highest message rates and lowers delays. However, we must not forget that 2.4 GHz is worse than 868 MHz in terms of communication range, making it unsuitable to constitute the basis of a FAN deployment. Even at 868 MHz, radio coverage may be difficult to achieve in some areas, and it must also not be forgotten that the PLC communication channel is often subject to noise, signal reflections and other phenomena that may limit its range and performance.

Validation of the choice of PLC PRIME and IEEE 802.15.4 was conducted based on the estimated traffic pattern for realistic Bronsbergen and Batalha scenarios, as defined in Section 3.3. The results have shown that IEEE 802.15.4 868 MHz BPSK was unable to support the Bronsbergen scenario. All the other transmission modes were able to support both validation scenarios.

RF-Mesh and NB-PLC offer the best compromise between bit rate, range and deployment cost, especially if the selected Smart Grid services require only a low bit rate. Mobile cellular solutions are reliable and easy to deploy, since mobile cellular coverage is extensive. Additionally, the recent developments such as LTE offer high speed data transmission. However, this communication service must be paid to the operator, which may result into significant OPEX when deployed at all FAN nodes. An alternative for the DSO is to invest on its own mobile cellular infrastructure, which allows it to reduce the OPEX, while increasing the CAPEX. Anyway, the use of mobile cellular technologies may be justified in areas where the deployment of RF-Mesh or NB-PLC is technically difficult, or to aggregate traffic coming from the latter.

An alarm aggregation mechanism developed within e-balance was also presented, which aims to improve the performance of alarm delivery over multihop transmission technologies (e.g., PLC and RF-Mesh) during outage situations. Though the simulation results confirm that the proposed mechanism achieves significant improvements that tend to increase with the size of the network, these improvements still stay far from the optimal. The difference seems to be related with the need for better routing metrics, which should be able to result into more aggregation-friendly logical topologies. This issue will be explored in future work.

4.3 HAN

According to the e-balance network architecture (see Chapter 1), the HAN interconnects the Customer MU, appliance sensors, actuators and device MUs. Performance of communication technologies for such networks has to be evaluated referring to the following aspects:

- Costs of integration of a new member into the network,
- Latency and throughput,
- Interoperability,
- Energy consumption,
- Dependability and security capabilities.

The first point influence two phases in network lifecycle. First, the total costs of network setup depend on the cost to integrate a new member into the HAL. Second, the value influences the cost of node replacement.

Latency and Throughput are essential characteristics of a network technology. Due to both being contrary properties it must be clarified how a specific network technology can fit requirements of a HAN.

HANs are installed in flats or houses together with other networks like LANs. The question is how the HAN is disturbed by other networks installed in the environment and how the HAN will influence these networks.

Most of the nodes of a HAN are battery-powered. Hence, a closer examination of energy consumption is necessary.

HANs have clear requirements to dependability and security capabilities of the network services. The design goals associated with dependability and security are given in Figure 32. The given goals must be fulfilled by a network technology in order to be adopted as a HAN technology.

Figure 32: Relationship between Design goals of Dependability and Security

Three network technologies have been evaluated related to their suitability for HAN scenarios: Z-Wave, Bluetooth and IEEE 802.15.4.

4.3.1 Z-Wave

Z-Wave is an interoperable wireless communications technology. It is designed specifically for control, monitoring and status reading applications in residential and light commercial environments.

It operates in Sub-GHz band. 868.42 MHz SRD Band (Europe); the 900 MHz ISM band: 908.42 MHz (United States); 916 MHz (Israel); 919.82 MHz (Hong Kong); 921.42 MHz (Australian/New Zealand),India 865.2 Mhz.

Figure 33 gives an overview about the layered architecture of the Z-Wave network stack. Since 2012 physical layer and MAC sublayer are specified by [10]. Z-Wave specific details are specified in appendix A. Higher layers are defined in proprietary standards like e.g. [11], [12] and [13].

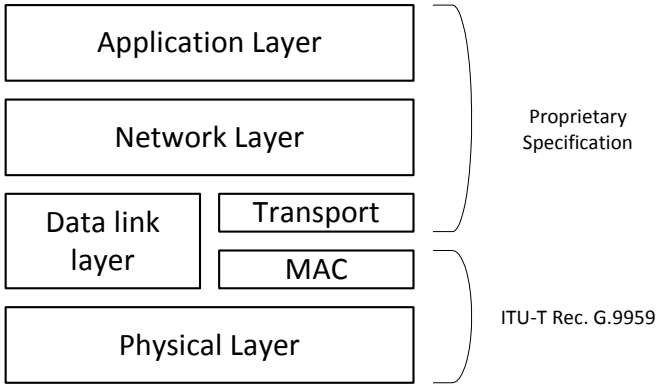


Figure 33: Z-Wave's layered architecture

Data rates provided by Z-Wave are given in Table 15. According to minimum sensitivity values Z-Wave supports ranges up to 40 m in buildings and 150 m outside buildings.

Table 15: Data rates, Modulation schemes and encoding supported by Z-Wave

Bitrate	Symbolrate	Name	Modulation	Encoding	Checksum	Minimum sensitivity
9.6 kbit/s	19.2 kbaud	R1	FSK	Manchester	XOR	-95 dBm
40 kbit/s	40 kbaud	R2	FSK	NRZ	XOR	-92 dBm
100 kbit/s	100 kbaud	R3	GFSK BT=0.6	NRZ	CRC-CCITT	-89 dBm

Z-Wave units can operate in power-save mode and only be active 0.1% of the time, thus reducing power consumption substantially.

Z-Wave supports Multi-Hop networks, but is supports Source Routing only. Nodes are able to exchange information without participation of any master node. Thus even if the master nodes fail communication is not interrupted. Encryption with AES-128 is supported. Z-Wave supports the acknowledge schemes given in Figure 34 and Figure 35 which can be used according to application's reliability requirements.

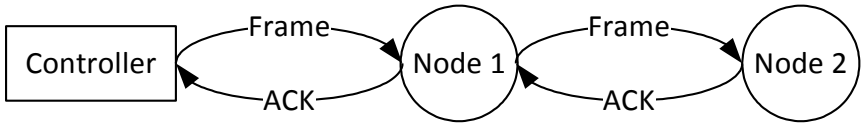


Figure 34: Z-Wave's Peer-to-Peer acknowledgement

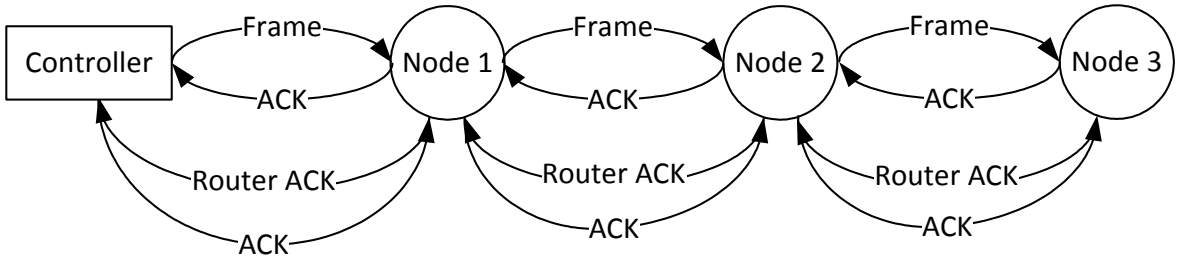


Figure 35: Z-Waves's End-to-End acknowledgement. (Johansen, 2006)

Inclusion means the integration of a node into a Z-Wave network. The counterpart is Exclusion that describes how devices are being removed from network. Only nodes included to the same network can communicate with each other. The inclusion and the exclusion processes are not part of (ITU-T, 2012). Rather each producer is allowed to implement a proprietary method.

No public vulnerability research on Z-Wave could be found prior to [14]. The authors focused on Application layer and demonstrate a successful attack on a Z-Wave enabled door lock.

4.3.2 Bluetooth

Bluetooth® is a wireless technology standardized by IEEE as IEEE 802.15.1 [15]. It utilizes the 2.4 GHz band and thus, it competes against several wireless technologies like ZigBee and IEEE 802.11. However, in contrast to these technologies Bluetooth uses an adaptive frequency hopping (AFH) to utilize the whole 2.4 GHz band. Consequently, it disturbs potentially wireless networks using only one channel.

Range in Bluetooth® is application specific and although a minimum range is mandated by the Core Specification, there is not a limit and manufacturers can tune their implementation to support the use case they are enabling. Range may vary depending on class of radio used in an implementation:

- Class 3 radios – have a range of up to 1 meter or 3 feet
- Class 2 radios – most commonly found in mobile devices – have a range of 10 meters or 33 feet
- Class 1 radios – used primarily in industrial use cases – have a range of 100 meters or 300 feet

The most commonly used radio is Class 2 and uses 2.5 mW of power. Bluetooth technology is designed to have very low power consumption. This is reinforced in the specification by allowing radios to be powered down when inactive.

Bluetooth® has limitation in supported network topologies. As shown in Figure 36 only star and tree topologies are supported. In a Piconet cell a master node coordinates up to seven slave nodes. Each slave node must be within range of the master node.

To overcome the limitations of Piconets in node count and range Bluetooth® provides Scatternets which a formed of a set of Piconets. In a Scatternet several Piconets share nodes e.g. a node is master in one Piconet and slave in another or a node is slave in more Piconets. Due to HAV with typically limited dimensions are investigated in this text Scatternets are out scope.

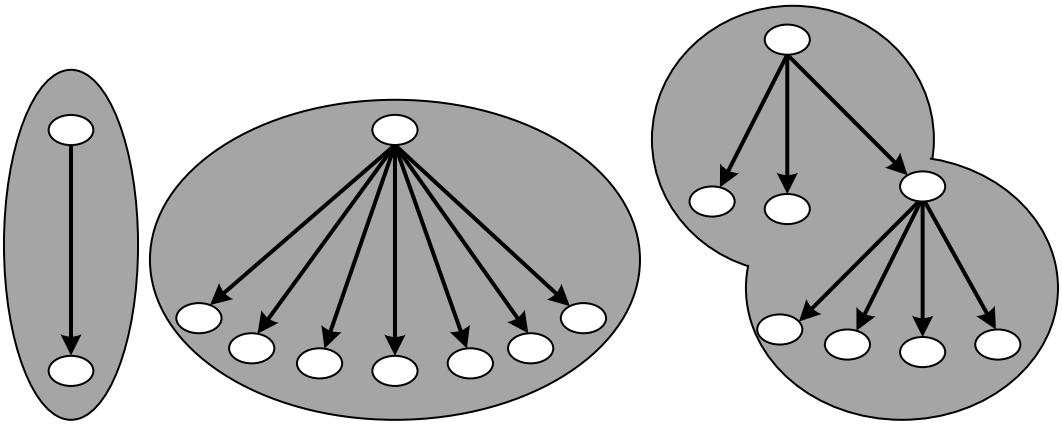


Figure 36: Topologies of Bluetooth networks: (a) Point-toPoint, (b) Piconet and (c) Scatternet

Bluetooth® has been designed as easy-to-use cable replacement. While it supports strong encryption of connection at link layer, two weak key exchange methods are specified. The first method defines derivation of a key for link encryption from an up to 16 characters long shared secret called. For the second method the user has to enter a 16 bit value to each device during connection setup. For both schemes the devices can store the generated encryption keys and stay “paired”. Then the secret exchange is only necessary at the first time the devices are connected.

Bluetooth® supports three modulation schemes each with three different frame sizes. For each frame size error detection respective error correction with a fewer data rate can be activated. Table 16 shows minimum

(error correction with smallest frame size) and maximum (error detection with largest frame size) values of the supported data rates.

Table 16: Bluetooth® Modulations schemes with minimum and maximum data rates

Modulation	Data rate	
	Min	Max
GFSK	108.8 kb/s	723.2 kb/s
PI/4-DQPSK	345.6 kb/s	1448.5 kb/s
8DPSK	531.2 kb/s	2178.1 kb/s

Bluetooth® uses a TDM scheme for the communication between master and slave nodes in a Piconet. The slot length is 625 µs. The association of time slots for a point to point connection is given in Figure 37. In the uneven numbered slots the master sends a data frame to the slave, in the even slots sends its frames to the master.

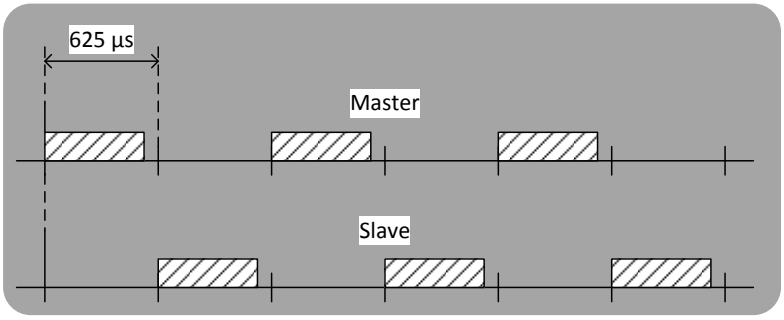


Figure 37: TDM scheme for data transmission between Bluetooth master and one slave

If the master node is connected to two or more slaves the scheme is extended like in Figure 38 illustrated. The slaves are served by the master sequentially.

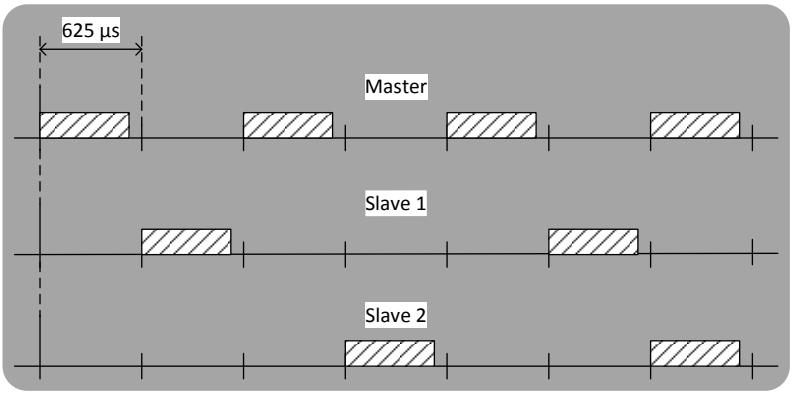


Figure 38: TDM scheme for data transmission between Bluetooth master and two slaves

To increase throughput Bluetooth® supports multi slot frames occupying three or five time slots. The scheme is pictured in Figure 39.

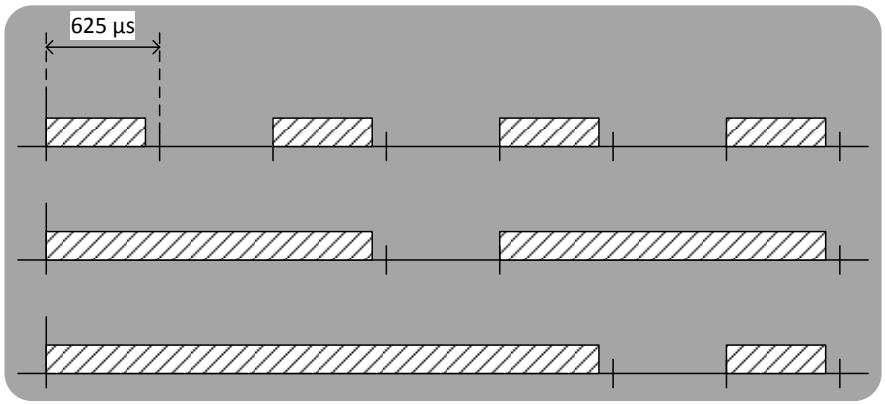


Figure 39: 1-, 3-, and 5-slots packets in Bluetooth

To get realistic we studied the behaviour in case of one point-to-point connection in contrast to a fully connected Piconet. We looked at 1-slot frames and 5-slot frames. Over 5 seconds frame over frame is sent. Each frame transports a random number of bytes (17 for DM1 frames and 339 for DH5 frames). The results are given in Figure 40 to Figure 43. While the red dots show the distribution of latency values the green graph gives the average latency over the last packets transmitted. The blue dots give the data rate for each packet transmitted while the violet graph shows the throughput over the whole time.

In Figure 44 the architecture of a Bluetooth® system is given. Besides the pure Bluetooth® transmission several other components influence throughput and latency. First component is the Host Controller Interface (HCI). The HCI can be implemented as UART, USB or SDIO. Throughput and latency of the HCI influence throughput and latency of the whole system. The second important component is the Bluetooth® Host implementing the Bluetooth® Protocol Stack. Due to Bluetooth® devices supports ranges up to 100 m the signal propagation with $333.6\,ns = \frac{100\,m}{c}$ has no evident effect to the total latency.

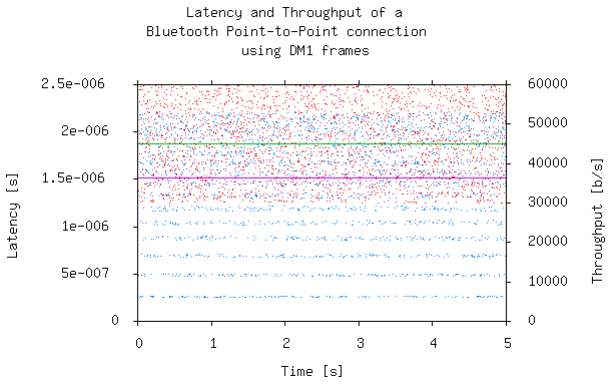


Figure 40: Results 1-slot Point-to-Point

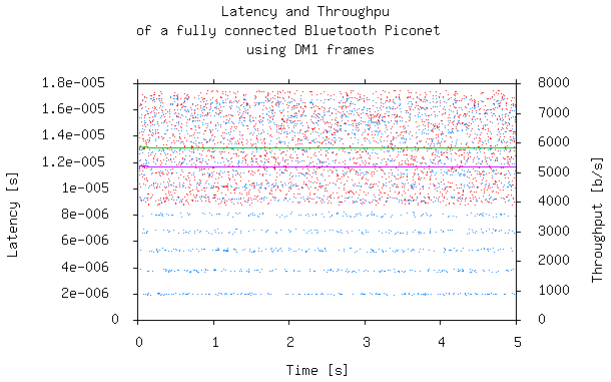


Figure 41: Results 1-slot fully connected Piconet

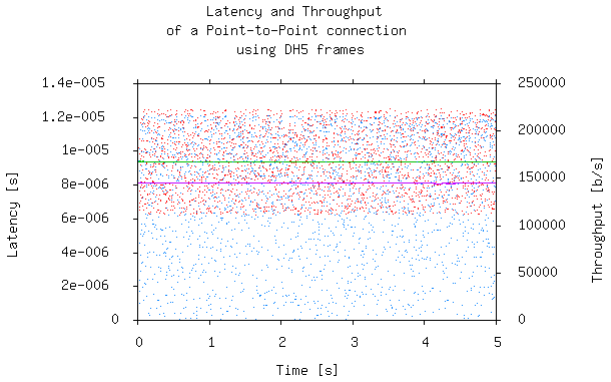


Figure 42: Results 5-slot Point-to-Point

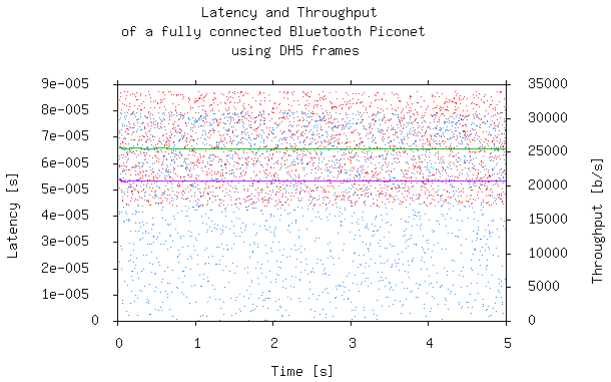


Figure 43: Results 5-slot fully connected Piconet

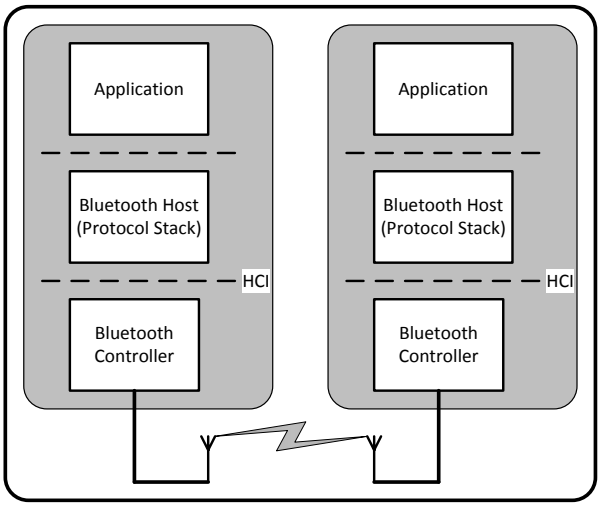


Figure 44: Architecture of a Bluetooth® system

4.3.3 IEEE 802.15.4

IEEE 802.15.4 specifies the PHY and MAC layers of ZigBee. On top of IEEE 802.15.4, a ZigBee SE 1.0 protocol stack or an IP-based ZigBee SE 2.0 protocol stack is supported. The performance of the IP protocol stack over IEEE 802.15.4 was already evaluated within the context of the FAN and thus it will not be repeated here. The shorter ranges needed in the HAN allow the higher frequency band of 2.4 GHz to be used, resulting in a maximum bitrate of 250 kbit/s. However, interference with Bluetooth and Wi-Fi in the home may provide motivation for the use of the 868 MHz frequency band, significantly lowering the bitrate. Still, since the traffic to/from smart appliances is expected to be sporadic, the bitrate will likely not constitute an obstacle for the use of IEEE 802.15.4. As already mentioned, security is an important issue to be taken into account. IEEE 802.15.4 provides support for AES encryption. The use of pre-installed keys can be considered in the home environment to the stability and reduced number of nodes in the HAN, though more sophisticated key distribution methods may be considered and implemented at the higher layers of the protocol stack.

4.3.4 Conclusion

We investigated the wireless technologies Bluetooth®, Z-Wave and IEEE 802.15.4 according to their suitability for HAN networks. We compared network setup, latency and throughput, interoperability, and security and reliability properties.

Those technologies do not support an automatic integration, but except for integration they work without maintenance. Those technologies support security. In throughput and latency Bluetooth® has clear advantages over Z-Wave and IEEE 802.15.4 868 MHz. On the other hand Z-Wave works in the Sub-Ghz band near 900 MHz while Bluetooth® occupies the full 2.4 GHz ISM-Band disturbing other wireless technologies e.g. Wi-Fi and IEEE 802.15.4 2.4 GHz. All of these technologies provide reliability.

In conclusion all of these technologies are suitable for HAN scenarios. We excluded technologies like WiFi, since their energy consumption fingerprint is too expensive to be applied at all smart appliances in the currently available version. All the above mentioned technologies support ultra-low power modes saving energy.

5 Network Specification

This chapter presents the e-balance network specification, including the selected technologies, network topology and protocol stacks. The WAN specification is demonstrator specific and will be provided in D6.1 [16].

5.1 LV-FAN and MV-FAN

This section presents the LV-FAN and MV-FAN architecture specification. The LV-FAN and MV-FAN present many similarities, allowing them to be treated as the same from the point of view of network architecture and protocol stack. Following the conclusions in 4.2.4, the LV-FAN and MV-FAN may present different configurations, depending if the DSO deploys its own 3G/4G infrastructure. The two envisaged scenarios are depicted in Figure 45a) and b), which represent the respective physical network topologies.

Figure 45a) represents the situation where the DSO decided to hire 3G/4G services from a telecom operator. In this case, in order to minimize its OPEX, 3G/4G is used sparingly at aggregator nodes, which concentrate the traffic from NB-PLC or RF-Mesh islands. The latter technologies provide the bulk of network interfaces, equipping most of the network nodes, since they represent a low OPEX (see Table 6).

Figure 45b) represents the situation where the DSO owns the 3G/4G infrastructure. In this case, it is advantageous for the DSO to employ 3G/4G whenever possible, in order to get its return on infrastructure investment. The terminal equipment itself is not expected to be significantly more expensive than for NB-PLC or RF-Mesh (see Table 6) and thus most network nodes will be directly connected to 3G/4G. In areas where 3G/4G coverage is bad (e.g., indoors, basements, underground equipment, etc.), NB-PLC and/or RF-Mesh can be used, forming small islands that are then connected with 3G/4G at aggregator nodes.

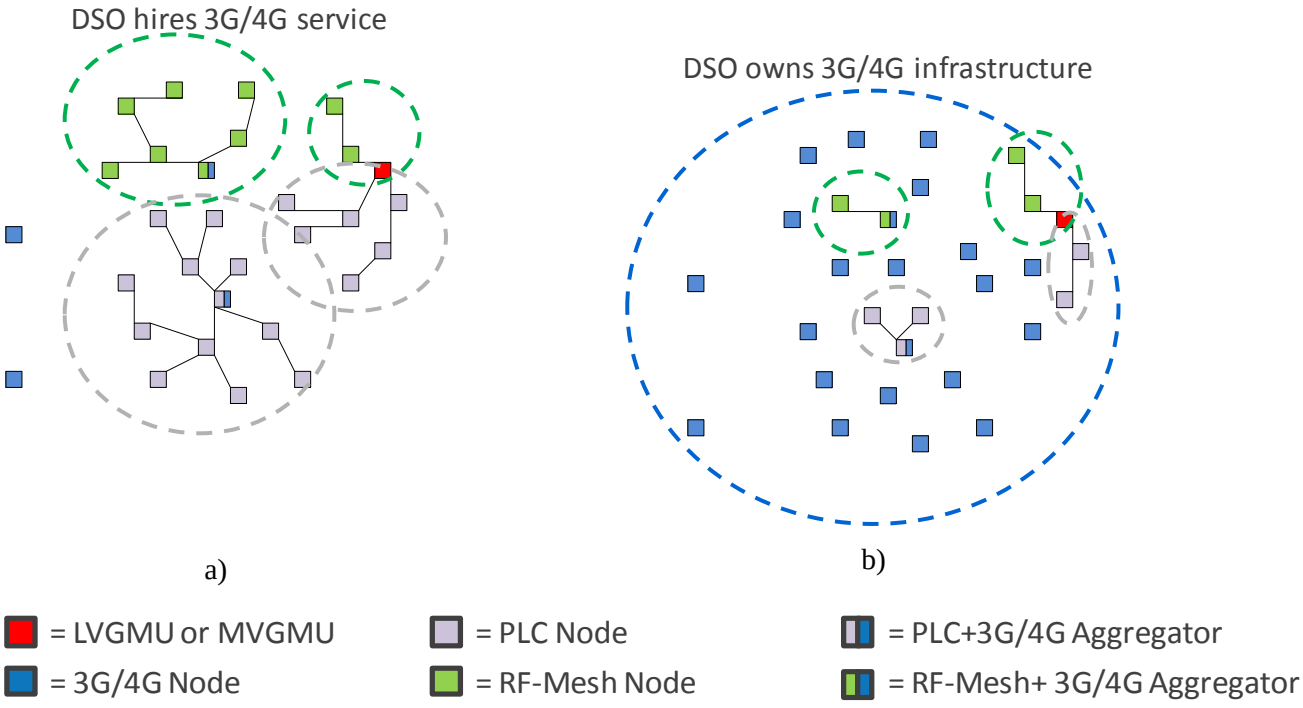


Figure 45: Two-tier physical network topology integrating PLC and RF-Mesh with 3G/4G

An IoT protocol stack based on IPv6 was selected for the FAN. The 6LoWPAN adaptation layer will be employed over PLC PRIME and IEEE 802.15.4, as depicted in Figure 54b). A standard IPv6 protocol stack will be employed over LTE, as depicted in Figure 54a).

It is considered that the MV-FAN and LV-FAN are hierarchical and rooted at the MV-GMU and LV-GMU, respectively. For each FAN, a gateway performs the interface with the communication FAN technology. This gateway is located nearby and attached to the respective MV-GMU or LV-GMU through a cabled

technology such as Ethernet. The gateway should support all communication technologies in use at the FAN sector under control of its attached LV-GMU or MV-GMU. The network architecture and protocol stack is depicted in Figure 46.

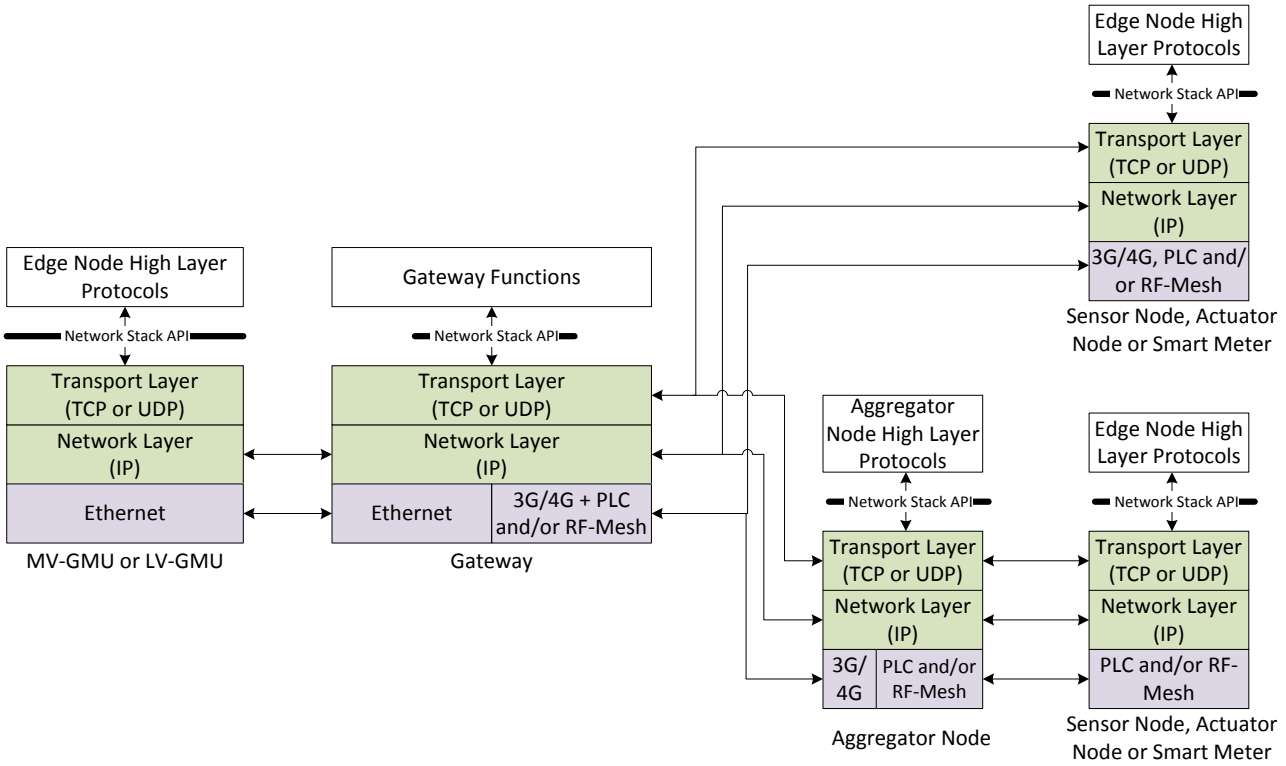


Figure 46: LV-FAN and MV-FAN network architecture and protocol stack

5.2 HAN

This section presents the HAN architecture specification. In order to provide interoperability with smart devices currently available on the market we decided to use the standard protocols that the majority of the devices support. The modular approach allows future extensions to support additional protocols (and devices).

Depending on the protocol, there may be different topologies in the HAN. In fact the proposed HAN is a combination of several subnetworks, each supporting a given communication protocol. The HAN is thus a structure with the CMU as a central station that also interconnects all the supported protocols.

Figure 47 presents the sketch of the HAN network architecture. It consists of the CMU that is equipped with a set of gateways to support the chosen network protocols. These are connected to the CMU using a serial interface and translate the commands to the proper network packets. The gateways connect smart devices to the CMU. The figure shows only a single Bluetooth Low Energy – BLE device connected to the respective gateway. The exact topology of the network of smart devices is controlled by the gateway.

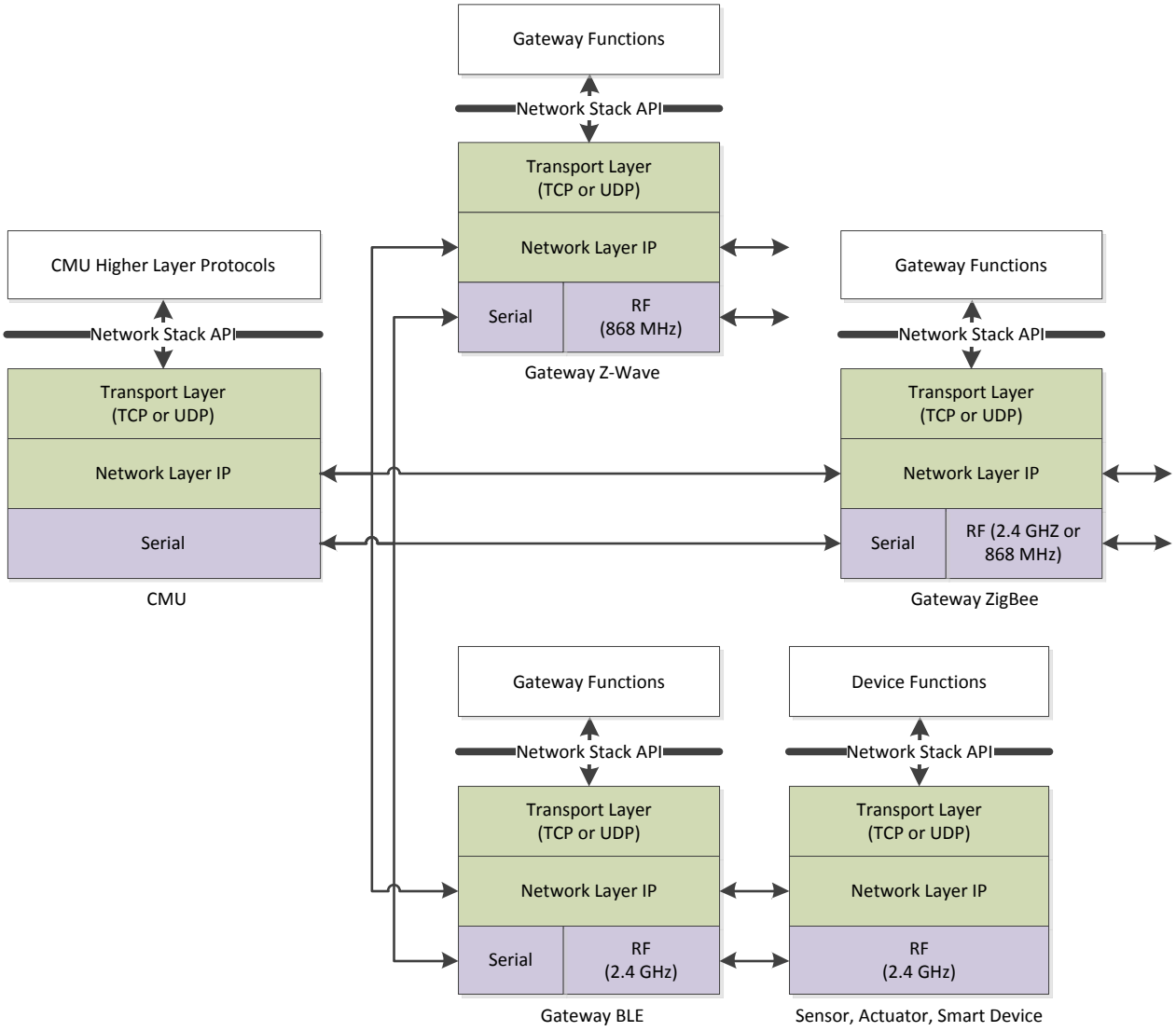


Figure 47: The architecture of the HAN network

6 Network Implementation

This chapter presents a description of the network adaptors that will actually implement the selected communication technologies for each network area of the e-balance network architecture in each demonstrator.

6.1 Batalha

In terms of the communications network, the Batalha demonstrator, in Portugal, will focus mainly on the LV-FAN and MV-FAN network areas. Two main technologies will support the networking services underlying the implemented use cases: RF-Mesh and PLC PRIME. Some of the networking infrastructures are already deployed or are under deployment, which relate to the InovGrid architecture – another demonstration project, by EDP Distribuição, an e-balance consortium member –, and thus outside the scope of e-balance (see D6.1 [16]). That external project comprises smart metering, employing already PLC PRIME and RF Mesh. The e-balance Consortium decided to use pertinent data from this external smart metering infrastructure, so that useful data arising from already deployed SMs could be used towards feeding the neighborhood power flow algorithms, as well as to improve the selectivity of LV fault location. Moreover, smart metering data will be useful to feed the fraud detection algorithms. Besides the SMs, the Distribution Transformer Controller (DTC) is another InovGrid component that was integrated in e-balance. The DTC is a node located at the SS, which performs control and management of an MV/LV power transformer and of the LV grid located downstream. In the context of e-balance, it will be used to implement part of the LV-GMU functionality in the Batalha demonstrator. The implemented LV-FAN is an instantiation of the architecture specified in Section 5.1 and is depicted in Figure 48.

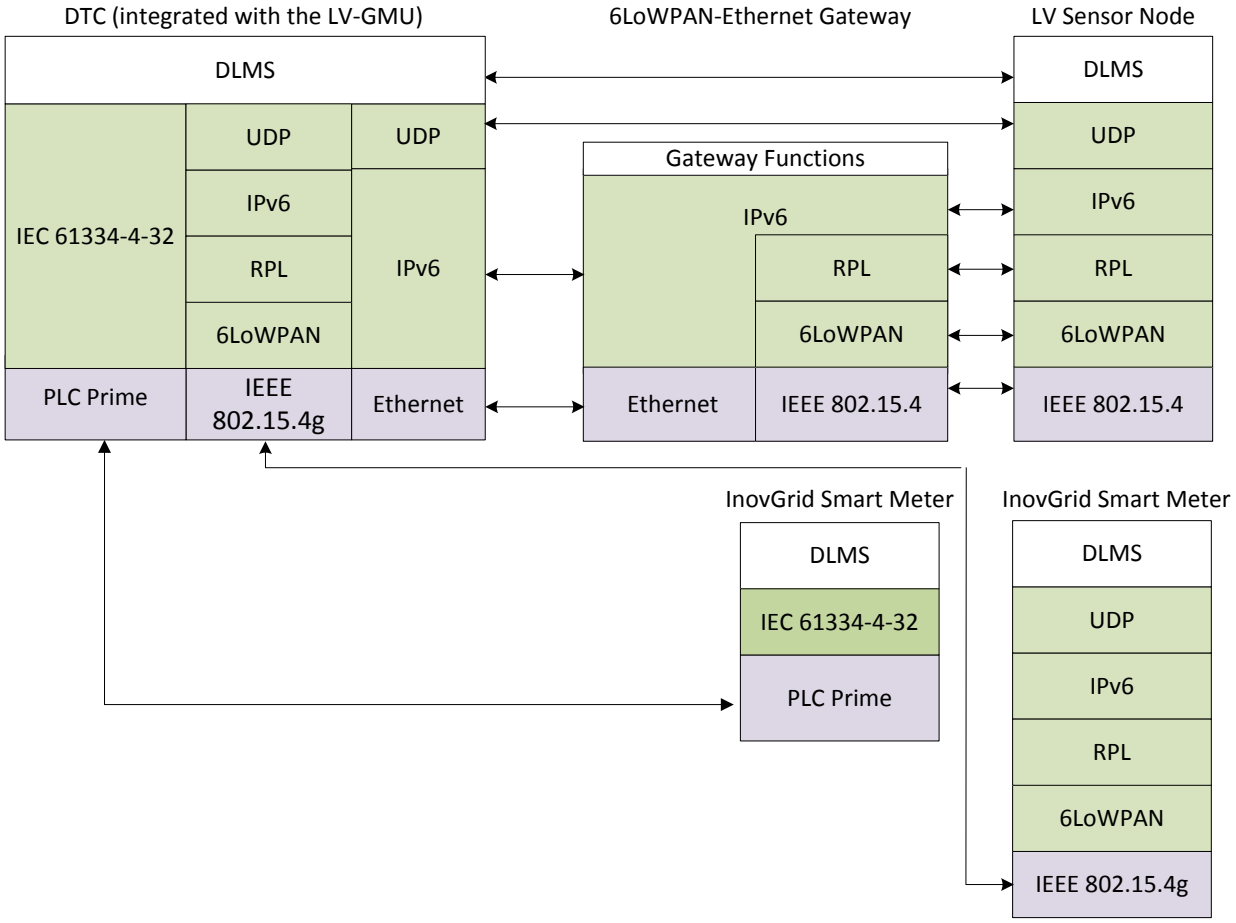


Figure 48: LV-FAN implementation in Batalha

Two main technologies will support the networking services underlying the implemented use cases: RF-Mesh and PLC PRIME. The following sections present the main characteristics of the respective adaptors used in the Batalha demonstrator, comprising a slight mention to the current projects run by EDP.

6.1.1 RF-Mesh (XBee)

The LV sensors deployed in distribution cabinets and public lighting will form a 6LoWPAN based RF-Mesh (according to the IEEE 802.15.4 standard) network, whose root node will be the LV-FAN Gateway. The RF-Mesh modules consist of iBee boards developed by INOV (see Figure 49). This board includes the ATmega1284P microcontroller unit (MCU) from ATMEL [17]. A super-capacitor of 2.5 F assures temporary operation during outage situations, when the iBee AC/DC converter cannot be powered from the LV grid. The radio module consists of a XBee-Pro®868 adaptor module [18]. The latter operates in the Short Range Device (SRD) 868 MHz frequency band, more specifically using 869.525 MHz as its center frequency. The maximum transmit power is 315 mW (25dBm) and the receiver sensitivity is -112 dBm. It supports a raw RF data rate of 24 kbit/s. This results into 2.4 kbit/s of usable data rate due to the mandatory duty cycle of 10%. The MCU runs the Contiki v3.0 operating system [19]. Multihop mesh routing is assured by the RPL routing protocol.

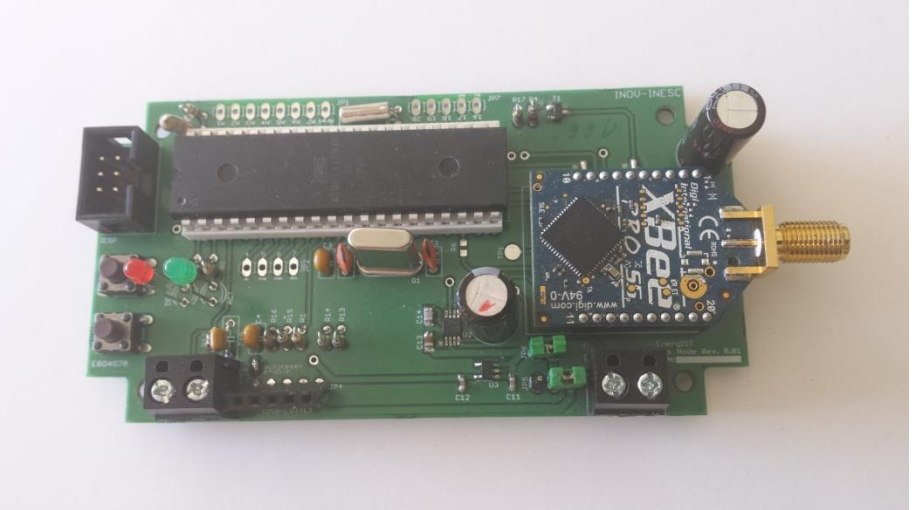


Figure 49: iBee board developed by INOV.

6.1.2 RF-Mesh (deployment of Silver Spring Networks technology by Efacec)

As already mentioned, the is currently a deployment of a smart metering infrastructure being carried out by EDP Distribuição – an e-balance Consortium member. The deployment comprises the installation of a set of single-phase M Box I100 SMs by Efacec – another e-balance Consortium member – enabled by RF Mesh modems by Silver Spring Networks.

This communication infrastructure bridges all SMs with the corresponding concentrator. The SMs dialogue with each concentrator via the DLMS/COSEM standard, coping with a data set specified in 2012 by EDP Distribuição.

The RF Mesh modems, by Silver Spring Networks, also implement a proprietary protocol suitable for spontaneous last gasp messaging, towards informing which SMs have detected a power outage. All other data transfer performed by each SM occurs only when the concentrator polls such SM, through the DLMS/COSEM protocol.

The Silver Spring Networks' modem supports the following communication features [20]:

- Data rates: 50 kbps to 300 kbps
- Frequency Hop Spread spectrum (FHSS)
- Transmitter output: 27 to 30 dBm (500 mW to 1 W)
- Receive sensitivity:
    - Data Rate (kbps) Receive Sensitivity (dBm for 10% PER)

Data Rate (kbps)	Receive Sensitivity (dBm for 10% PER)
50	-101
100	-98
150	-96

200	-95
300	-93

- PHY/MAC protocols: IEEE 802.15.4g

The modem also supports the following protocols and security features:

- Addressing: IPv6
- Encryption: Advanced Encryption Standard (AES-128 or AES-256)
- Security: Secure Hash Algorithm 256-bit (SHA-256) and RSA-1024 or ECC-256
- Key storage: Secure NVRAM with tamper detection and key erasure

The modem follows a System-on-Chip (SoC) architecture. It uses a SoC-based ARM7 processor with adjustable frequencies. It provides 4 MB of RAM and 8 MB of Flash memory.

6.1.3 PLC PRIME (deployment of PLC PRIME technology by Janz)

In the scope of the same deployment of a smart metering infrastructure mentioned in the previous section, it is in progress the installation of a set of single-phase SMs by Janz, enabled by a PLC PRIME modem by ATMEL.

Similarly to the description on the previous section, this communication infrastructure bridges all SMs with the corresponding concentrator. The SMs dialogue with each concentrator via the DLMS/COSEM standard, coping with the same data set specified in 2012 by EDP Distribuição.

Any data transfer performed by each SM occurs only when the concentrator polls such SM, through the DLMS/COSEM protocol.

The Janz modem supports the following communication features:

- Data rates: 5.4 kbps to 128.6 kbps
- Physical layer: OFDM
- Sampling: 250 kHz, with 512 differential phase shift keying channels from 42–89 kHz

It uses a convolutional code for error detection and correction. The upper layer is usually IPv4.

6.2 Bronsbergen

The communication in the Bronsbergen demonstrator, in the Netherlands, will test the entire e-balance architecture (except the TLGMU) spanning from CMU to MVGMU. In this demonstrator, there are two different communication architectures that correspond to the use of two different secondary substations named Roelofs and Bronsbergenmeer. The two communication architectures are the same except for the communication between the LVGMU and the storage RTU and sensors. The two communication architectures will be referred to as Roelofs and Bronsbergenmeer and are depicted in Figure 50 and Figure 51 respectively.

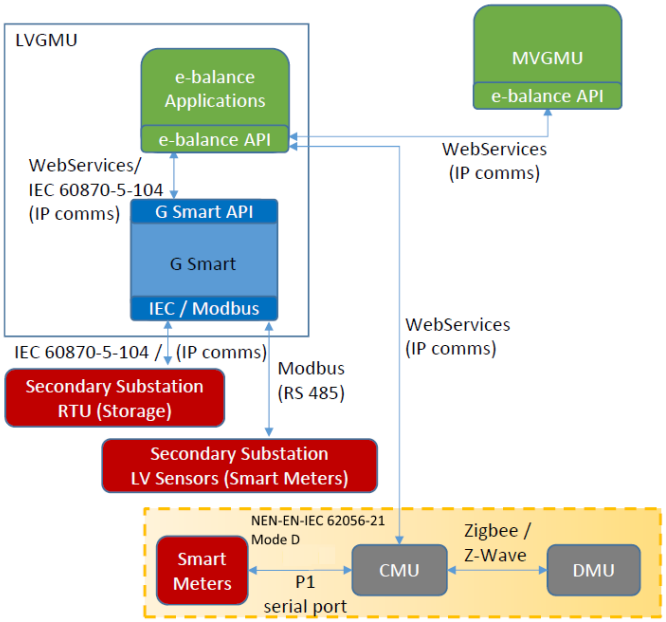


Figure 50: Communication architecture in Bronsgergen (Roelofs)

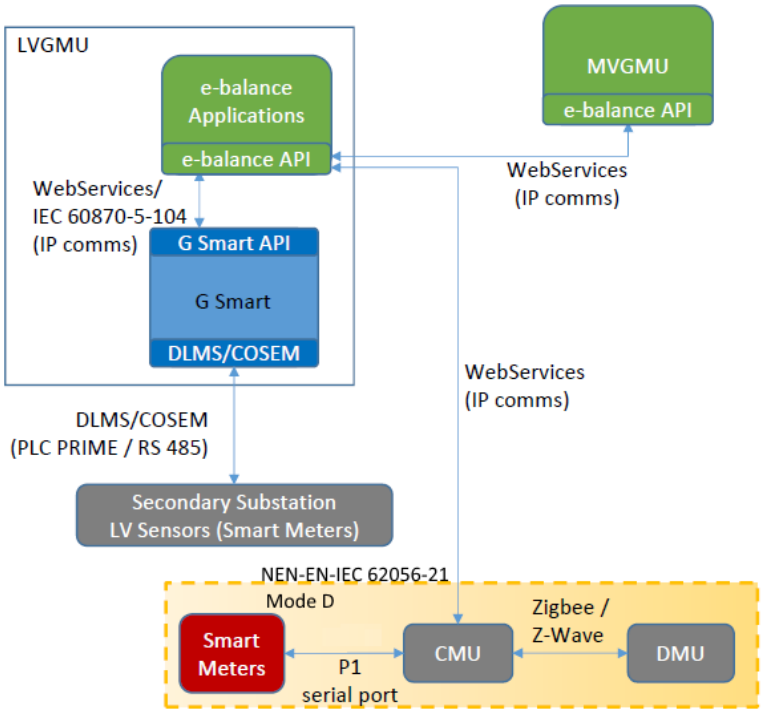


Figure 51: Communication architecture in Bronsbergen (Bronsbergenmeer)

6.2.1 Communication between MUs

The two architectures rely on communication based on web services to exchange information between the different MUs: CMU, LVGMU and MVGMU. The communication between these MUs will be based on simple REST web services that exchange JSON data. These web services will be used on top of HTTP and TCP/IP network. This means that the communication architecture will be platform-independent and will be able to run over different physical layers as long as TCP/IP is available. Table 17 shows the different OSI layers in the communication between MUs. The physical and data link layer choice will depend on the

existing infrastructure in the demonstrator but both Ethernet and Wi-Fi option are possible. The web services infrastructure will be provided by the ServiceStack framework [21].

Table 17: Communication

Layer	Technology / Protocol
Physical	Ethernet/Wi-Fi
Data	
Network	IP
4	TCP
Upper Layers	Web Services over HTTP (ServiceStack)

The LVGMU is composed of two different components as shown in Figure 50 and Figure 51. A piece of hardware that executes the e-balance application and a device called G-Smart that talks to the secondary substation and sensors. The communication between these two components of the LVGMU will communicate using the IEC 60870-5-104 standard over web services.

6.2.2 HAN Communication

The HAN network is coordinated by the CMU. On the one hand, the CMU talks to different appliances devices in the customer premises controlled by a DMU. The communication between the DMU in these appliances and the CMU will be based on the ZigBee standard and optionally on Z-Wave. The hardware used to provide this communication is to be determined based on the existing appliances in the demonstrator. On the other hand the CMU communicates with a smart meter in order to get electric usage related data. The communication between these two devices will be carried out using a protocol based on NEN-EN-IEC 62056-21 Mode D provided by the smart meter via a physical port. This port is accessed using a cable connection.

6.2.3 LVGMU – Secondary substation/LV sensors (Roelofs)

The communication between the LVGMU and the Roelofs storage RTU will be carried out using the IEC 60870-5-104 standard. The LV sensors are accessed directly from the LVGMU using Modbus over RS485. As highlighted before the communication scheme presented in this section is the only difference in communication between the Roelofs and Bronsbergenmeer communication architectures.

6.2.4 LVGMU – Secondary substation (Bronsbergenmeer)

The communication between the LVGMU and the LV sensors in the Bronsbergenmeer secondary substation will be carried out using DLMS/COSEM protocol. This protocol will be used both over PLC PRIME and RS485.

References

[1] e-balance, Deliverable D3.1, “High level system architecture specification”, 2014.

[2] e-balance, Deliverable D2.1, “Selection of representative use cases”, 2014.

[3] e-balance, Deliverable D3.2, "Detailed system architecture specification", 2015.

[4] M. Kuzlu, M. Pipattanasomporn, S. Rahman, “Communication network requirements for major smart grid applications in HAN, NAN and WAN”, Computer Networks, Elsevier, Volume 67, 4 July 2014, Pages 74-88, ISSN 1389-1286, http://dx.doi.org/10.1016/j.comnet.2014.03.029.

[5] e-balance, Deliverable D6.1, “Definition of the demonstrators”, 2015.

[6] ITU-T G.9904, “Narrowband orthogonal frequency division multiplexing power line communication transceivers for PRIME networks”, October 2012.

[7] IEEE 802.15.4, “IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)”, September 2006.

[8] Freescale™, “Long Term Evolution Protocol Overview”, white paper, October 2008.

[9] P.-J. Lin ; N. Tung, “An IP-based packet test environment for TD-LTE and LTE FDD”, IEEE Communications Magazine, IEEE, ISSN: 0163-6804, vol. 52, nr. 3, March 2014.

[10] Standard. Recommendation ITU-T G.9959 Short range narrow-band digital radiocommunication transceivers – PHY and MAC layer specifications, 2012.

[11] SDS10243. Software Design Specification Z-Wave Protocol Overview, 2006.

[12] SDS10242. Software Design Specification Z-Wave Device Class Specification, 2009.

[13] SDS11060. Software Design Specification Z-Wave Command Class Specification, 2009.

[14] Fouladi, B., & Ghanoun, S.: Security Evaluation of the Z-Wave Wireless Protocol. Black hat USA, 2013.

[15] IEEE 802.15.1, “IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 15.1a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPAN)”, 2005.

[16] e-balance, Deliverable D6.1, “High level system architecture specification”, 2015.

[17] ATMEL, “8-bit Microcontroller with 128K Bytes In-System Programmable Flash - ATmega1284P”, http://www.sl.com.cn/down/handbook/datasheet/ATMEGA1284P.pdf, last access: 14th April 2015.

[18] Digi International Inc., “XBee-PRO®868 Long-Range Embedded RF Modules for OEMs”, http://www.digi.com/pdf/ds_xbeepro868.pdf, last access: 14th April 2015.

[19] Contiki OS, “Contiki: The Open Source OS for the Internet of Things”, http://www.contiki-os.org/, last access: 14th April 2015.

[20] Silver Spring Networks, “Communications Module for Electricity Meters – product data sheet”, 2013, available at http://www.silverspringnet.com/pdfs/SilverSpring-Datasheet-Communications-Modules.pdf, last access: 21st April 2015.

[21] ServiceStack framework. https://servicestack.net

[22] CEN-CENELEC-ETSI Smart Grid Coordination Group, "Smart Grid Reference Architecture," November 2012.

[23] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, et al., "Smart grid communications: Overview of research challenges, solutions, and standardization activities," IEEE Communications Surveys & Tutorials, vol. 15(1), pp. 21-38, 2013.

[24] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—the new and improved power grid: a survey," IEEE Communications Surveys & Tutorials, vol. 14(4), pp. 944-980, 2012.

[25] N. Saputro, K. Akkaya, and S. Uludag, "A survey of routing protocols for smart grid communications," Computer Networks, vol. 56(11), pp. 2742-2771, 2012.

[26] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," Computer Networks, vol. 55(15), pp. 3604-3629, 2011.

[27] D. Minoli, "Telecommunications Technology Handbook", 2nd Edition, Artech House Inc., 2003.

[28] A. Saha, N. Manna, "Optoelectronics and Optical Communications", Kindle Edition, University Science Press, 2011.

[29] Wikipedia, "Last mile", http://en.wikipedia.org/wiki/Last_mile, last access: 21st April 2015.

[30] M. Erbes, "Smart Home and Health Telematics: Standards for and with Users", in S. Helal, M. Mokhtari, B. Abdulrazak (eds.), "The Engineering Handbook of Smart Technology for Aging, Disability and Independence", John Wiley & Sons, 2008.

[31] I. H. Cavdar, "A solution to remote detection of illegal electricity usage via power line communications," IEEE Transactions on Power Delivery, vol. 19(4), pp. 1663-1667, 2004.

[32] H. Ferreira, L. Lampe, J. Newbury, and T. Swart, Power line communications: Theory and applications for narrowband and broadband communications over power lines, John Wiley and Sons, 2010.

[33] M. Nassar, J. Lin, Y. Mortazavi, A. Dabak, I. H. Kim, and B. L. Evans, "Local utility power line communications in the 3–500 kHz band: channel impairments, noise, and standards," IEEE Signal Processing Magazine, vol. 29(5), pp. 116-127, 2012.

[34] G3-PLC physical layer specification and G3-PLC MAC Layer specification, G3-PLC Alliance, Aug. 2012.

[35] ITU-T G.9955, "Narrowband orthogonal frequency division multiplexing power line communication transceivers - Physical layer specification," December 2011.

[36] ITU_T G.9956, "Narrowband orthogonal frequency division multiplexing power line communication transceivers - Data link layer specification," ITU-T, November 2011.

[37] IEEE P1901.2, "IEEE Draft Standard for Low Frequency (less than 500 kHz) Narrow Band Power Line Communications for Smart Grid Applications," IEEE, approved Project Authorization Request, March 2010.

[38] ITU-T G.9963, "Unified high-speed wireline-based home networking transceivers - Multiple input/multiple output specification," ITU-T, December 2011.

[39] IEEE 802.16-2009, "IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems," IEEE, May 2009.

[40] B. Akyol, H. Kirkham, S. Clements, and M. Hadley, "A survey of wireless communications for the electric power system," Prepared for the US Department of Energy, 2010.

[41] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," IEEE Transactions on Industrial Electronics, vol. 57(10), pp. 3557-3564, 2010.

[42] B. Lichtensteiger, B. Bjelajac, C. Muller, and C. Wietfeld, "RF mesh systems for smart metering: system architecture and performance," in Proceedings of the First IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010, pp. 379-384.

[43] IEEE 802.11-2012, "IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE, March 2012.

[44] IEEE 802.16j, "IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11:

Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE, June 2009.

[45] S. R. Das, E. M. Belding-Royer, and C. E. Perkins, "Ad hoc on-demand distance vector (AODV) routing," RFC 3561, IETF, July 2003.

[46] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, et al., "Optimized link state routing protocol (OLSR)," RFC 3626, IETF, October 2003.

[47] T. Winter, "RPL: IPv6 routing protocol for low-power and lossy networks," RFC 6550, IETF, March 2012.

[48] Silver Spring Networks, "Smart Grid Standards," whitepaper, 9 April 2012.

[49] P. Kulkarni, S. Gormus, Z. Fan, and B. Motz, "A mesh-radio-based solution for smart metering networks," IEEE Communications Magazine, vol. 50(7), pp. 86-95, 2012.

[50] EUTC, "Spectrum needs for Utilities," EUTC position paper, http://eutc.org/system/files/UTC_private_file/EUTC%20Spectrum%20Position%20Paper-9April2013.pdf, last access 8 April 2014.

[51] NIST, "NIST Framework and roadmap for smart grid interoperability standards, release 1.0," http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf, January 2010.

[52] H. Farhangi, "The path of the smart grid," IEEE Power and Energy Magazine, vol. 8(1), pp. 18-28, 2010.

[53] P. Yi, A. Iwayemi, and C. Zhou, "Developing ZigBee deployment guideline under WiFi interference for smart grid applications," IEEE Transactions on Smart Grid, vol. 2(1), pp. 110-120, 2011.

[54] IEC 62591, "Industrial communication networks – Wireless communication network and communication profiles – WirelessHART™," IEC, Edition 1.0, April 2010.

[55] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, IETF, 1998.

[56] Z. Shelby, "6LoWPAN: The Wireless Embedded Internet", Wiley, ISBN: 978-0-470-74799-5, 2009.

[57] Z. Shelby, K. Hartke, and C. Bormann, "Constrained Application Protocol (CoAP)," IETF Internet Draft, draft-ietf-core-coap-18, URL: https://datatracker.ietf.org/doc/draft-ietf-core-coap/, , last access 8 April 2014.

Appendix I Communication Technologies and Protocols

This chapter presents an analysis of the main communication technologies and networking protocol stacks that are candidates to support Smart Grid applications. A short survey on energy management communication technology standards is also presented.

I.1 Smart Grid Communication Technologies

It is hard to find a communication technology that cannot be used in a Smart Grid, given the latter's dimension, complexity and scenario diversity. In fact, the literature often considers the possibility of integrating several technologies, from low-rate short-range wireless communications on the Field Area Network (FAN), to optical fiber segments capable of aggregating data rates in the order of Mbit/s or Gbit/s in the core network that supports the central management systems. This section presents the communication technologies that are considered more relevant in the literature. The contents of this section are based on [22][23][24][25][26]. The communication technologies are classified into the following groups:

- Broadband technologies;
- Power Line Communications (PLC);
- Infrastructure-based Wireless Networks;
- Radio frequency Mesh (RF-Mesh) networks.

These technologies will be separately described, which will be followed by an overall comparison in terms of their application areas.

I.1.1 Broadband Technologies

Broadband wired technologies, such as SONET/SDH, Wavelength-division multiplexing (WDM), Ethernet, Digital Subscriber Line (DSL), Hybrid Fiber Coax (HFC), Passive Optical Network (PON), Data Over Cable Service Interface Specification (DOCSIS) etc, or broadband wireless technologies such as satellite communication are used/deployed by the utility or hired from telecom operators whenever a high communication capacity and reduced delay are required. Most of these broadband technologies form the backbone of the internet network and are typically used when a high amount of data needs to be transmitted at a high speed between distant users. For example, optic fiber technologies transmit high-speed data packets with supported data rate between 155 Mbps and 40 Gbps. Ethernet can nowadays provide data rates between 10 Mbps and 10 Gbps.
In the current internet network infrastructure a set of different broadband technologies is used to form a world scale communication network. For example, optical fiber technology is the main choice in high speed high length communications links such as transatlantic communications cables, while as DSL, HFC, DOCSIS PON are used in the "last mile" segment, typically reusing existing networks such as coaxial cable or deploying new optical fiber ones. Finally, Ethernet is the preferred choice for local area networks. Due to the required investment and transmitted volume of data of these technologies, they have more use in the WAN part of the Smart Grid.
All these protocols have been classified into three main groups depending on their location in the global communication architecture.

I.1.1.1 Core network technologies

These technologies are used in what is called the core network. This term refers to the central part of the communication network, usually referring to a high capacity high speed portion of the network that serves as path to connect different sub-networks where end users are connected. Due to the high speed and latency requirements the most widely used technologies in this part of the network are the ones based on optical fiber. This technology permit transmission over long distances at a high bandwidth than wire cables.

SONET/SDH refers to two standardized protocols that specify how to transfer multiple digital bit streams synchronously over optical fiber [27]. The SONET/SDH frame structure allows the multiplexing of multiple streams, interleaving the header between the data in a complex way. The hierarchical SDH/SONET structure makes it easy to aggregate lower rate streams into higher rate streams, which is a typical function in a core network. In association with this, the interleaved frame structure avoids burstyness, keeping a low average delay.

Wavelength-division multiplexing, also known as WDM, is used to multiplex a number of optical carrier signals onto a single optical fiber by using different wavelenghts of laser light [28]. It is thus the counterpart of FDM in the optical spectral range. WDM is similar to frequency-division multiplexing (FDM) but instead of taking place at radio frequencies (RF), WDM is done in the IR portion of the electromagnetic spectrum. Each IR channel carries several RF signals combined by means of FDM or time-division multiplexing (TDM). Each multiplexed IR channel is separated, or demultiplexed, into the original signals at the destination. Using FDM or TDM in each IR channel in combination with WDM or several IR channels, data in different formats and at different speeds can be transmitted simultaneously on a single fiber.

I.1.1.2 Technologies for the “Last mile” segment

"Last mile" [29] is a term that refers to the final leg of the telecommunications networks delivering communications connectivity to retail customers. These technologies provide the connection between high speed over high length links (typically optic fiber) and end users at their homes. These are the main technologies used in this communication network segment.

DSL is a hybrid high-speed digital data transmission technology that uses the wires of the voice telephone network, concentrating the traffic in optical fiber segments at special nodes called Digital Subscriber Line Access Multiplexer (DSLAM). The already existing infrastructure of DSL lines reduces installation cost. Hence, many companies chose DSL technology for their smart grid projects.

Hybrid Fibre Coaxial (HFC) is another family of hybrid technologies, at this time combining optical fiber and coaxial cable. Optical fiber is used to reach neighborhood’s hubsites and coaxial cable is used for the rest of the segment towards the homes.

Data over cable service interface specification (DOCSIS) is an international standard that is used to add high-speed and telephony data to existing cable TV systems [30]. It is usually used in combination with HFC to reuse existing networks to provide Internet access to the users.

Passive optical network (PON) is a telecommunication technology that uses optical fiber all or most of the way to the end user. It can be regarded as a development of HFC where the coaxial cable segments were significantly shortened or eliminated. In order to support many users in an efficient way, it uses point-to-multipoint fiber, which becomes a shared transmission medium in contrast with point-to-point optical fiber technologies.

I.1.1.3 LAN protocols

Ethernet is without any doubt the most widely used networking protocol for local area networks (LANs) although it can be used in larger networks, specially the latests versions of it, which can attain speeds up to 10 Gbit/s. Legacy Ethernet assumes a shared medium to exchange information between connected nodes. The Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol is used to arbitrate medium access. More recent Ethernet variants supporting gigabit data rates are switched, avoiding medium access conflicts by design.

I.1.1.4 Satellite

Satellite technology is able to provide high data rates to Internet users through geostationary satellites. Due to the power required to transmit to a satellite, the user is usually only able to directly receive the downstream data using a VSAT (very-small-aperture terminal) dish antenna with a transceiver. The upstream data is sent through an alternative last mile technology to an Internet Service Provider, which forwards it to the satellite service provider. Powerful ground stations are then able to transmit the upstream data to the satellite. Frequency bands in the microwave spectrum are used to communicate with the satellites. The Ka band (26.5–40 GHz) and Ku band (12–18 GHz) are common for broadband satellite services. The main advantage of satellite technology is its ubiquity and little infrastructure required to work since almost no wiring is necessary. On the other hand, satellite deployment is a very expensive task, therefore the use of satellite technology is must be hired by utility companies.

I.1.2 Power Line Communication (PLC)

Power Line Communication (PLC) is used since the 1950s by the electricity distribution companies in order to remotely perform some control functions on electric network equipment [31]. Recently, this technology has earned more relevance because the technology evolution has led to an increase of the achieved data rates, both in medium and low voltage. The advantage of PLC comes from the fact that it uses the same infrastructure for both energy distribution and communications, which greatly reduces the deployment costs.

The PLC systems are usually classified according to three different bandwidth classes: Ultra Narrowband (UNB), Narrowband (NB) and Broadband (BB) [32][33]. Although the attained data rates and ranges are highly dependent on the specific characteristics and transient conditions of the network (e.g., the impedance is highly dependent on the number and characteristics of attached electrical devices), some approximate figures shall be provided as a reference to allow a better comparison between the different classes.

The UNB-PLC systems operate in the Very Low Frequency (VLF) band, which corresponds to 0.3-3.0 kHz. The attained bit rates are usually in the order of 100 bit/s, with ranges of up to 150 km. The relevant UNB-PLC applications comprise Automatic Meter Reading (AMR), fault detection in the distribution grid, and voltage monitoring.

The NB-PLC systems operate in the Low Frequency (LF) band, which corresponds to 3-500 kHz. In Europe, the European Committee for Electrotechnical Standardization (CENELEC) has defined four frequency bands for PLC use: CENELEC-A (3-95 kHz), CENELEC-B (95-125 kHz), CENELEC-C (125-140 kHz) and CENELEC-D (140-148.5 kHz). CENELEC-A is reserved for exclusive use by energy providers, while CENELEC-B, CENELEC-C and CENELEC-D are open for end user applications. In NB-PLC, the attained data rates span from a few kbit/s to around 800 kbit/s – depending on the technology, bandwidth and channel conditions –, while the range is in the order of some kilometers. Some standards for Building Automation Applications (BAA), such as BacNet (ISO 16484-5) and LonTalk (ISO/IEC 14908-3), employ NB-PLC with a single carrier. The IEC 61334 standard for low-speed reliable power line communications by electricity meters, water meters and SCADA, uses the 60-76 kHz frequency band, being able to achieve 1.2-2.4 kbit/s with Spread Frequency Shift Keying (S-FSK) modulation. Yitran Communications Ltd. and Renesas Technology provide solutions based on Differential Chaos Shift Keying (DCSK) – a form of Direct-Sequence Spread Spectrum (DSSS) –, which are able to achieve bitrates as high as 60 kbit/s in the CENELEC-A band. On the other hand, PoweRline Intelligent Metering Evolution (PRIME) [6] and G3-PLC [34] are multi-carrier systems based on Orthogonal Frequency Division Multiplexing (OFDM), which allows them to support higher data rates. PRIME operates within the CENELEC-A frequency band, more specifically in the 42–89 kHz range, and is able to achieve 21-128 kbit/s. G3 may operate in the CENELEC-A and CENELEC-B bands, being able to achieve 2.4-46 kbit/s. The G3-PLC MAC layer is based on the IEEE 802.15.4 MAC. In order to unify the OFDM-based NB-PLC systems, ITU has approved recommendations G.9955 (G.hnem physical layer) [35] and G.9956 (G.hnem data link layer) [36], while IEEE has approved recommendation P1901.2 [37].

BB-PLC systems operate in the High Frequency (HF) and Very High Frequency (VHF) bands, which corresponds to 1.8-250 MHz. The achievable data rates may be as high as 500 Mbit/s, but the range is significantly shorter than for NB-PLC. Consequently, BB-PLC is normally used for local connectivity in the HAN or as a broadband access technology. The most recent BB-PLC standards are IEEE P1901 (also designated Broadband Over Power Line – BPL) and ITU G.996x (G.hn), which are based on OFDM. The ITU G.9963 recommendation [38] also incorporates some Multiple-Input Multiple-Output (MIMO) concepts through the use of multiple cables.

Despite the advantages of PLC for Smart Grid applications, namely the reduced costs and easier management of a single infrastructure (i.e. energy distribution plus communications in a single network), PLC faces some obstacles and challenges, which are often similar to the ones faced by RF-Mesh (see below):

- The shared medium is subject to significant attenuation and noise, which limit the data rates and ranges that can be effectively achieved.
- A failure in the energy distribution infrastructure usually means that the communications cannot take place while the malfunction rests unresolved, which may negatively affect some applications.
- Another consequence is that a communications failure may be wrongly interpreted as a malfunction in the energy distribution infrastructure.

I.1.3 Infrastructure-based Wireless Networks

The technologies that fall within the Infrastructure-based Wireless Networks category rely on a fixed infrastructure of base stations, together with switching equipment and management systems, in order to provide wide coverage communication service to the end user. Fixed wireless access and mobile cellular networks, both fit into this category.

The WiMAX technology is defined in the IEEE 802.16 standard for fixed and mobile broadband wireless access [39], being able to achieve a coverage range in the order of 50 km and data rates in the order of tens or even hundreds of Mbit/s. Despite its advantages, the widespread adoption of Long-Term Evolution (LTE) by mobile operators has brought down the initial popularity that WiMax was, for some time, able to enjoy. Moreover, the lack of WiMax networks and operators in Portugal constitute significant obstacles to the adoption of this technology to support Smart Grid functionalities in this country, since the energy provider would have to deploy its own WiMax infrastructure. IEEE 802.16 shall be addressed again in this report, but in the context of RF-Mesh technologies.

The mobile cellular communications technologies divide the covered territory into smaller areas designated cells, each served by a base station. If the base station is equipped with directional antennas, the cell may be further sectorized, which increases the frequency reuse and hence its capacity to support more users. Before communication is established, the mobile user terminal is tracked as it moves between different sectors or cells, allowing the mobile terminal to be paged at any time. Moreover, handover signaling procedures allow the user to move even while a communication is taking place. Mobile cellular technologies have already spanned two digital generations starting on the 2nd Generation (2G) and are already in their fourth generation.

Examples of 2G technologies available in Europe (and Portugal in particular) are Global System for Mobile Communications / General Packet Radio Service (GSM/GPRS) and Terrestrial Trunked Radio (TETRA). GPRS is the packet switched complement of GSM and supports data rates between 9.05 and 85.6 kbit/s per user. The effective data rate depends on the required error protection, class of terminal and sharing with other users using the same frequency channel. The TETRA technology is primarily used by security and civilian protection entities, as well as transportation services, due to the support of specific functionalities like direct mode operation and group calls. The supported data rates span from 2.4 kbit/s to 28 kbit/s, depending on the required error protection and channel allocation.

The 3rd Generation (3G) arrived in the beginning of this century with the Universal Mobile Telecommunications System (UMTS), which offered 2 Mbit/s (shared) in urban areas. UMTS suffered a number of upgrades to increase the supported data rates, namely the High-Speed Downlink Packet Access+ (HSDPA) and HSDPA+ for the downlink, and High-Speed Uplink Packet Access (HSUPA) for the uplink. HSDPA can support data rates up to 42 Mbit/s, though later releases specify data rates up to 337 Mbit/s with HSDPA+. In the opposite direction, HSUPA may support data rates up to 23 Mbit/s, though existing mobile operators might offer a lower value..

CDMA450 is also a 3G technology, based on the adaptation of the American standard CDMA2000 to operate in the 450-470 MHz frequency band. The supported total bitrates depend on the specific mode of operation. For Multicarrier EV-DO, overall bitrates may be as high as 9.3 Mbit/s for downlink and 5.4 Mbit/s for uplink, with average rates per user in the order of 1.8-4.2 Mbit/s for downlink and 1.5-2.4 Mbit/s for uplink. This technology was offered in Portugal by the Zapp operator until 2011, being abandoned afterwards. This means that in order to use CDMA450 as a Smart Grid infrastructure, the utility will have to deploy its own network infrastructure, like for WiMax.

Currently, most European mobile operators already offer LTE. Although marketed as 4G, LTE does not satisfy yet all the 4G requirements defined by 3GPP. LTE employs Orthogonal Frequency Division Multiple Access (OFDMA) in the downlink and Single-Carrier Frequency Division Multiple Access (SC-FDMA). Supported peak data rates are 299.6 Mbit/s for the downlink and 75.4 Mbit/s for the uplink.

A special case of infrastructure wireless communications is satellite communications, which, besides the ground infrastructure, require a satellite constellation to be deployed. Low Earth Orbit (LEO) systems (500 - 1500 km) are especially interesting, since they allow communication with small devices, without the need of big size antennas.

Given their proven reliability, technology maturity and extensive coverage, mobile cellular networks constitute important candidates to support the Smart Grid communications infrastructure, being used already in applications such as Automatic Meter Reading (AMR). However, these technologies face the following challenges:

- The difficulties related with radiofrequency (RF) penetration inside buildings constitute sometimes an obstacle for its use in some Smart Grid applications, namely AMR.
- The fact that the mobile cellular network is most of the time managed by an external operator, means that the utility will have to pay the latter for the provisioning of communications services. Alternatively, the utility might deploy its own communications infrastructure (e.g., WiMax or CDMA450), though that would certainly constitute a substantial investment on communication systems.

I.1.4 Radiofrequency Mesh (RF-Mesh)

An RF-Mesh is a network formed by RF capable nodes, which are self-organized in a mesh topology [40][41][42]. This self-organization capability brings several advantages in the context of Smart Grid communications, namely deployment flexibility and automatic connection re-establishment and topology reconfiguration in the presence of link or node failure. This explains why this family of technologies is so popular in the USA, where it is used to support Smart Metering applications. Within the RF-Mesh family, we can distinguish between broadband and narrowband technologies.

The most representative broadband technologies are currently WiFi [43] and IEEE 802.16j [44]. Even if the IEEE 802.11s mesh extension is not used, IEEE 802.11 can be configured to operate as a mesh by performing ad-hoc routing at the network layer (e.g., IP layer). These technologies support communication ranges in the order of hundreds (IEEE 802.11) or thousands (IEEE 802.16) of meters, as well as high data rates in the order of Mbit/s, which makes them multimedia capable. Besides physical and Medium Access Control (MAC) aspects, IEEE 802.11s specifies the routing protocol, which is the Hybrid Wireless Mesh Protocol (HWMP). The latter is a hybrid between a tree routing protocol and the Ad-hoc On-Demand Distance Vector (AODV) protocol [45]. In case IEEE 802.11 is used without the mesh extension, a myriad of routing protocols such as AODV, Optimized Link State Routing Protocol (OLSR) [46], or Routing Protocol for Low-Power and Lossy Networks (RPL) [47] can be used at the network layer. As to IEEE 802.16j, it does not specify how the path evaluation and selection is done, there being freedom for manufacturer specific implementations. However, it constrains the topology to be tree based. Although the high bitrates supported by broadband RF-Mesh allow the support of virtually any Smart Grid applications, both real-time and non-real-time, these technologies also have some disadvantages that can hinder their global applicability:

- Broadband communications means operating at higher frequencies, which are more vulnerable to path loss and other causes of signal attenuation.
- Broadband RF-Mesh transceivers often present higher energy consumption in comparison with narrowband RF-Mesh. This is made even worse by the need to increase the transmit power in order to compensate for path loss and attenuation. The deployment of a huge number of nodes means that the energy overhead introduced by the Smart Grid communications may start to be non-negligible.
- High bitrates demand a corresponding processing and storage capacity to be available on the network nodes, which will likely be translated into an increase of the unit cost.
- The deployment of these technologies by the utility requires the choice of the operating frequency. IEEE 802.11 operates mainly on the unlicensed bands of 2.4 GHz or 5 GHz. The 2.4 GHz band is cluttered, since it is subject to the interference of both private and public WLANs. On the other hand, the 5 GHz band has a reduced range for the same transmit power. IEEE 802.16 supports frequency bands between 2 GHz and 66 GHz, both licensed and unlicensed. Besides the problems related with spectrum occupancy, the use of unlicensed bands also raises the problem of communications security. On the other hand, the use of licensed bands usually represents additional costs for the utility.

The narrowband RF Mesh technologies correspond to those that belong to the Wireless Sensor Network (WSN) and Internet-of-Things (IoT) domains. These are usually characterized by simpler hardware and

operating systems, leading to a lower unit cost [41]. The lower power consumption that characterizes these technologies allows greater autonomy and effectiveness of energy harvesting techniques, which can feed the network nodes in case they cannot be directly fed by the LV network.

In the context of WSNs, the IEEE 802.15.4 standard [7] is nowadays prominent, constituting the basis (PHY and MAC layers) of several RF-Mesh protocol stacks such as ZigBee, WirelessHART, ISA100.11a and IoT, which are recommended for industrial and Smart Utility Networks (SUN) applications [41] (see Section I.2). The IEEE 802.15.4 MAC protocol is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), but also includes an optional Time Division Multiple Access (TDMA) operational mode. The latter is reserved for traffic that requires stringent access delay guarantees. While the original IEEE 802.15.4 standard restricted operation to the unlicensed frequency bands of 868-870 MHz (Europe), 902-928 MHz (USA) and 2.4 GHz, the IEEE 802.15.4g standard for SUN extends the set of supported Ultra-High Frequency (UHF) bands, adds new transmission modes (e.g., OFDM) and extends the MAC layer functionalities to allow the efficient and fair coexistence of networks using different transmission modes within the same frequency range. IEEE 802.15.14g can achieve a maximum bitrate of 1094 kbit/s and maximum ranges in the order of tens of kilometers. Products supporting IEEE 802.15.4g are manufactured, for example, by Silver Spring Networks [48]

Bluetooth® was created by Ericsson in 1994 and was originally conceived as a wireless alternative to RS-232 data cables. After that, more companies joined the Bluetooth consortium, which is designated the Bluetooth Special Interest Group (SIG). It was later standardized as IEEE 802.15.4 [15]. Bluetooth® technology exchanges data over short distances using radio transmissions. Bluetooth® technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHz, using a spread spectrum, frequency hopping, full-duplex signal at a nominal rate of 1600 hops/sec. The 2.4 GHz ISM band is available and unlicensed in most countries. Bluetooth® uses adaptive frequency hopping (AFH) to reduce interference between wireless technologies sharing the 2.4 GHz spectrum. AFH works within the spectrum to take advantage of the available frequency. This is done by the technology detecting other devices in the spectrum and avoiding the frequencies they are using. This adaptive hopping among 79 frequencies at 1 MHz intervals gives a high degree of interference immunity and also allows for more efficient transmission within the spectrum. For users of Bluetooth® technology this hopping provides greater performance even when other technologies are being used along with Bluetooth® technology. Until recently, Bluetooth® presented the shortcoming of higher power consumption compared with IEEE 802.15.4. In order to make Bluetooth more adapted to application requiring low energy consumption, the Bluetooth® SIG has specified a new version designated Bluetooth Low Energy (LE). This makes part of the Bluetooth Core Specification Version 4.0 since 2010. Bluetooth LE is especially suited to the transaction of short message chunks.

Besides the standard RF Mesh solutions described above, there are a number of proprietary RF Mesh solutions that were developed in the USA and have been enjoying significant popularity among energy operators. These products usually operate within the ISM frequency band of 902-928 MHz and employ Frequency Hop Spread Spectrum (FHSS) to increase the robustness and security of the links, namely to prevent jamming attacks and interference from other equipment operating in the same ISM band. Offered bitrates range between 9.6 kbit/s and 300 kbit/s, with ranges in the order of 2 km with 1 W of transmit power. An example is the Landis+Gyr's Gridstream, which employs a proprietary geographical based routing protocol in order to minimize the routing overhead [49].

The advantages of narrowband RF Mesh solutions are mostly related with deployment flexibility, increased range and use of less cluttered ISM frequency bands such as the 900 MHz in the USA and 868 MHz in Europe. The main disadvantage is, of course, the reduced bitrates as compared with broadband RF Mesh solutions.

Some additional disadvantages can be identified for RF Mesh solutions in general, which are the following:

- Performance is highly dependent on the propagation and interference environment.
- Depending on the scenario and inter-node distances, the deployment of additional relay nodes may be needed, which adds to the deployment costs.
- Wireless communications propagate through a shared medium, which poses some threats in terms of security. The protocol stack must implement security mechanisms that are able to meet the

requirements of the Smart Grid applications. These requirements are often different from application to application.

It should be noted that the European Utilities Telecom Council (EUTC) is seeking to reserve 6 MHz in the 450-470 MHz frequency band for use by grid utility operators, together with a frequency band above 1 GHz (e.g., 1.5 GHz band spanning 10 MHz) [50]. In this way, both low rate and high rate applications would be supported.

I.2 Networking Protocol Stacks

This section presents the most relevant networking protocol stacks in the context of Smart Grid development.

I.2.1 ZigBee

ZigBee is a standard protocol stack brought forth by the ZigBee Alliance consortium, which includes IEEE 802.15.4 at the lower layers, but defining its own network and application support layers. ZigBee, together with its ZigBee Smart Energy application profile (see below), were defined by the National Institute of Standards and Technology (NIST) in USA as standards for communications within the Home Area Network (HAN) domain of the Smart Grid [51]. ZigBee was also selected by many energy companies as the communication technology for smart meters, since it provides a standard platform for data exchange between the meter and HAN devices [52]. The functionalities supported by the Smart Energy profile include load management, AMR, real-time billing and text messaging [53]. The ZigBee Alliance also developed an IP networking specification called ZigBee IP which is based on existing IETF protocols defined for IoT (see below). The ZigBee Smart Energy version 2.0 specifications (see below) already make use of ZigBee IP.

I.2.2 WirelessHART and ISA100.11a

WirelessHART is another protocol stack, based on a TDMA MAC protocol, which uses the IEEE 802.15.4 frame format. It was developed as an adaptation of the HART protocol defined for wired industrial networks. While it was initially developed by a private consortium, the stack was standardized by the International Electrotechnical Commission (IEC) as IEC 62591. ISA100.11a is a standard protocol stack developed by the International Society for Automation (ISA), which is functionally very similar to WirelessHART [54]. The network layer of ISA100.11a is fully compatible with IPv6 (see below).

I.2.3 KNX

KNX is a OSI-based network communication protocol standard (EN 50090, ISO/IEC 14543) used for home and building control. KNX is the convergence of three previous standards called EHS (European Home Systems Protocol), BatiBUS and EIB (European Installation Bus). The standard is based on the communication stack of EIB but enlarged with the physical layers, configuration modes and application experience of BatiBUS and EHS.

Via the KNX medium to which all bus devices are connected (twisted pair, radio frequency, power line or IP/Ethernet), devices are able to exchange information. Bus devices can either be sensors or actuators needed for the control of building management equipment such as: lighting, blinds / shutters, security systems, energy management, heating, ventilation and air-conditioning systems, signaling and monitoring systems, interfaces to service and building control systems, remote control, metering, audio / video control, white goods, etc. All these functions can be controlled, monitored and signaled via a uniform system without the need for extra control centers. Figure 52 depicts a general overview of the KNX Model.

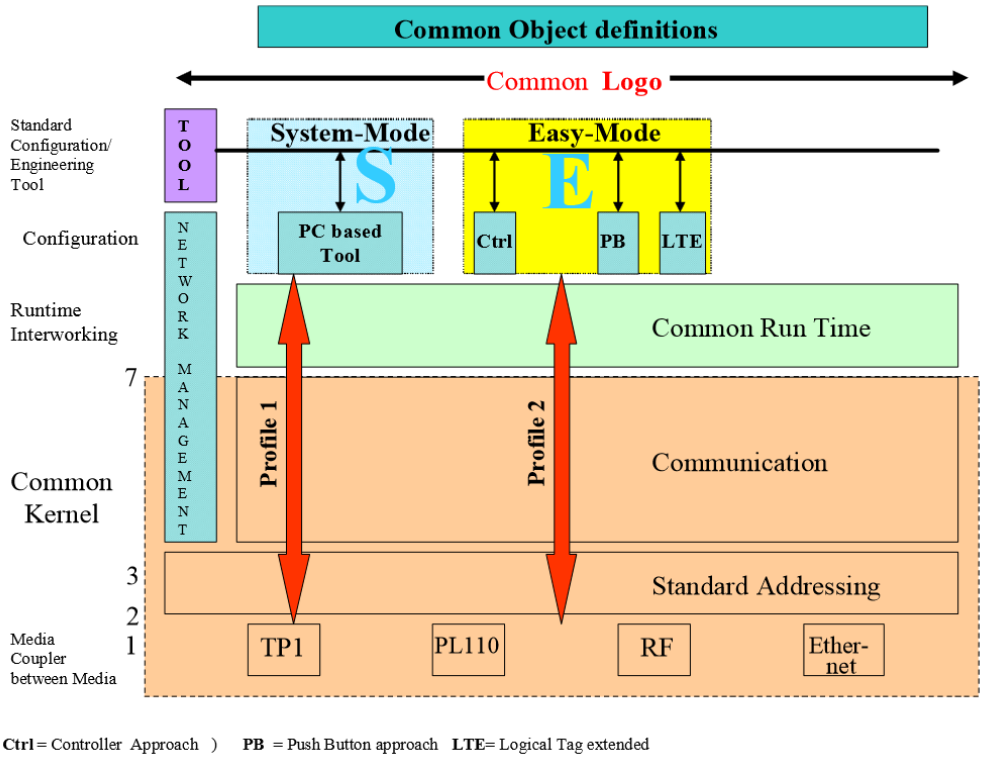


Figure 52 KNX model

Central to KNX's application concepts is the idea of Datapoints: they represent the process and control variables in the system, as explained in the section Application Models. These datapoints may be inputs, outputs, parameters, diagnostic data, etc. The standardized containers for these Datapoints are Group Objects and Interface Object Properties. Information transmitted or received by KNX is sent using a structure called Telegram (shown in FigureFigure 53). Each communication layer in the KNX protocol will contribute to a part of the telegram when a device generates a telegram and will decode part of the telegram when receiving.

octet 0	1	2	3	4	5	6		7	8	..	N - 1	N ≤ 22
Control Field	Source Address		Destination Address		Address Type; NPCI; length	TPCI	APCI	data/ APCI	data			FrameCheck

Figure 53 KNX Telegram structure

I.2.4 LonWorks

LonWorks networking platform is a powerful, pervasive solution for today's advanced control-networking systems. It's the foundation for an open, interoperable system in which products and solutions from the world's leading companies are brought together in a simple, straightforward implementation that integrates many system components into one complete solution.

LonWorks, developed by Echelon, consists of both software (the open protocol) called LonTalk and hardware. The main hardware item is Neuron microchip that includes three 8-bit inline processors, two of which execute the protocol. The third is used for the node's application. A LonWorks network uses the LonWorks protocol, also known as the ANSI/EIA 709.1 Control Networking Standard. The LonTalk protocol implements all seven layers of the International Standards Organization's Reference Model for Open Systems Interconnection (ISO OSI), which defines the structure for open communications protocols.

The product developers consider the technology a local operating network (LON), which allows all types of control devices, such as sensors and actuators, to communicate with one another through a common communications protocol. Communications transceivers are standardized, as are object models and

programming/troubleshooting tools that make it easy to design and set up interoperable LonWorks-based devices.

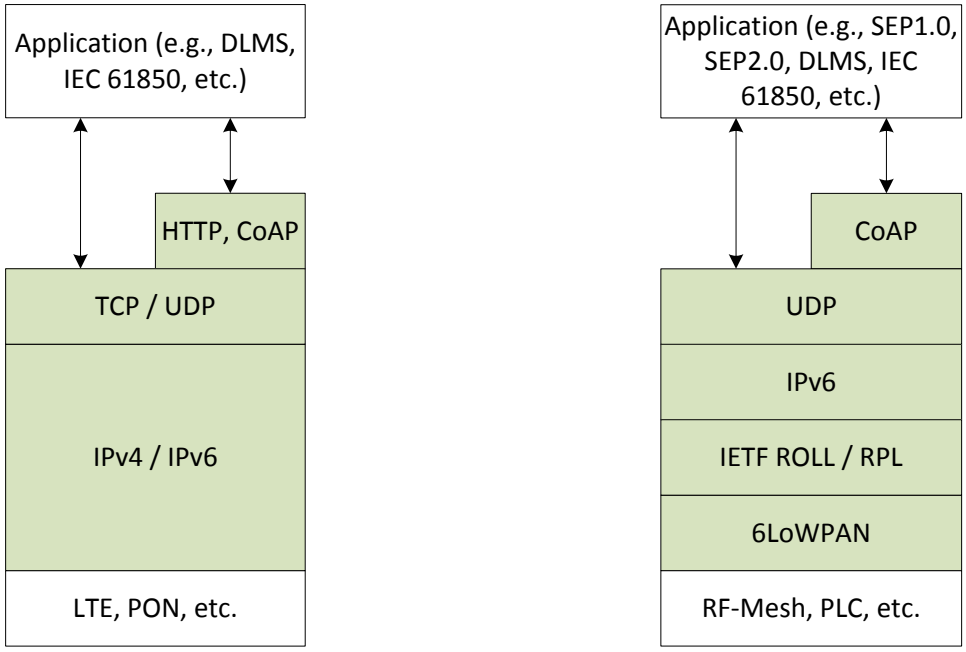
1. In summary, the four major elements of LonWorks are the LonTalk protocol, the Neuron chips, the LonWork transceivers, and network management and applications software. In more detail, we have that:
2. LondTalk protocol supports the following communications media: Twisted-pair, power line, radio frequency, coaxial cabling and fiber optics.
3. Neuron chip. Whenever a node program writes a new value into one of its output variables, the new value is propagated across the network to all nodes with input network variables connected to that output network variable.
4. LonWorks transceivers include the following:
    a. 78-kbps twisted-pair transceiver
    b. 1.25-Mbps twisted-pair transceiver.
    c. power line transceivers
    d. 78-kbps twisted-pair
    e. free topology transceiver
    f. Radio frequency transceiver. Licensed and non-licensed versions are available in the 400-MHz to 470-MHz and 900-MHz bands.
5. The software program for designing, installing, operating, and maintaining a LonWorks network, the LonMaker Integration Tool, uses the Microsoft Visio graphic interface.

I.2.5 IP Protocol Stack

The IP protocol comes in two versions: IPv4 and IPv6. The exhaustion of the IPv4 address space has, so far, been successfully mitigated with solutions based on solutions based on dynamic assignment and private addressing. Nevertheless, the huge number of devices expected to integrate the IoT in the future will likely require a more enduring and scalable solution, which means the general adoption of the IPv6 protocol together with its 128-bit address space [55]. IPv6 is expected to constitute the networking basis of the future Smart Grid.

The 128-bit IPv6 addresses eliminate the problem of address exhaustion and increase Internet scalability, but they also mean larger network layer headers and thus constitute additional protocol overhead. While this does not pose a problem for broadband technologies, it is prohibitive for low bit rate and Low-power and Lossy Networks (LLNs), requiring adaptation mechanisms such as header compression as defined for IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) [56]. In case of multihop LLN networks, The routing layer corresponds to the one defined by the IETF Routing Over Low power and Lossy networks (ROLL) group, which is instantiated by RPL [47].

The IP protocol stack is depicted in Figure 54 in two flavors, where the IP dependent elements are represented as green rectangles. Figure 54a) depicts the generic IP protocol stack, which is used when operating on top of medium and high capacity technologies. Both IPv4 and IPv6 can be used at the network layer. The transport layer consists of the ever present TCP and UDP protocols. The application support is offered by either the Hypertext Transfer Protocol (HTTP) or the more efficient Constrained Application Protocol (CoAP) [57]. The latter is especially suited to interact with edge devices, such as sensor and actuator nodes. Figure 54b) depicts a typical IoT stack for edge devices operating in a multihop LLN. IPv6 constitutes the network layer, but must be adapted for higher efficiency by means of 6LoWPAN. Due to the fact that TCP is too inefficient in LLNs, only the UDP protocol is supported. CoAP is here used as the application support protocol, providing guaranteed data delivery over UDP when required by the higher layers



a) b)

Figure 54: Generic IP protocol stack for the Smart Grid, on top of medium and high capacity technologies (a) and LLN multihop technologies (b)