European Commission
Information Society and Media

SEVENTH FRAMEWORK PROGRAMME

Large Scale Integrating Project

EXALTED

Expanding LTE for Devices

FP7 Contract Number: 258512

WP7 – Integration & Proof of Concepts

D7.3

Final Proof of Concept Validation Results and Analysis

Contractual Date of Delivery to the CEC:	28 February 2013
Actual Date of Delivery to the CEC:	28 February 2013
Responsible Beneficiary:	VIDAVO
Contributing Beneficiaries:	ALUD, TST, CTTC, GTO, SIERRA WIRELESS, TUD, CEA,UNIS
Estimated Person Months:	40
Security:	Public
Nature	Report
Version:	1.0

Document Information

Document ID: EXALTED WP7 D7_3 FINAL2.doc
Version Date: 28 February 2013
Total Number of Pages: 89

Abstract This report provides a detailed description of the methods and metrics used in order to validate the performance of EXALTED testbeds. The results achieved for each and every one of the sub-testbeds are also listed and commented upon. This deliverable is the direct continuation of D7.2 where the aforementioned components of the overall EXALTED solution were explicitly described. Moreover a new sub–testbed proving the continuum of our work, is presented in the appendix for reasons of coherence with the previous deliverables

Keywords EXALTED, LTE-M, capillary networks. E2E connectivity, IPv6, security, device management

Authors

Name	Organisation	Email
Eleftheria Vellidou	Vidavo S.A.	projects@vidavo.eu
Sofiane Imadali	CEA-Paris	sofiane.imadali@cea.fr
Nhon Chu	Sierra Wireless	nchu@sierrawireless.com
Javier Matamoros	CTTC	javier.matamoros@cttc.es
Pol Henarejos	CTTC	pol.henarejos@cttc.es
Carles Antón	CTTC	carles.anton@cttc.es
Walter Nitzold	TUD	walter.nitzold@ifn.et.tu-dresden.de
Stephan Saur	ALUD	Stephan.Saur@alcatel-lucent.com
Jerome d'Annoville	GTO	Jerome.d-annoville@gemalto.com
Djelal Raouf	Sierra Wireless	draouf@sierrawireless.com
Javier Valiño	TST	jvalino@tst-sistemas.es
Juan Rico	TST	jrico@tst-sistemas.es
David Garcés	TST	dgarces@tst-sistemas.es
Daniel Getino	TST	dgetino@tst-sistemas.es
Hongfei Du	UNIS	hongfei.du@surrey.ac.uk

Approvals

	Name	Organisation	Date	Visa
Internal Reviewer 1	Stephan Saur	ALUD	15/02 - 17/2/2013	OK
Internal Reviewer 2	Dejan Drajic	EYU	15/02 - 17/2/2013	OK
Technical Manager	Pirabakaran Navaratnam	UNIS	28/02/2013	OK
Project Manager	Djelal Raouf	SC	28/02/2013	OK

Executive Summary

This document is the final report of the EXALTED WP7 dedicated to Integration and Proof of Concepts. It summarises the work carried out throughout the project's life cycle by assessing and consequently validating each and every testbed that was implemented in the framework of the project.

The document was preceded by two deliverables D7.1 (Selection of scenarios for proof of concept testbeds and specifications for key building blocks functionalities and interfaces) and D7.2 [1] (Integration of selected algorithms into platforms & interfaces finalization) where the basis for the validation mechanisms were discussed in the form of performance measures and verification procedures. The document follows closely the organization of D7.2 i.e. all testbeds and their related subtests are thoroughly assessed.

In the chapter 1 brief introduction of the concept of validation implemented in in the EXALTED project is given. The second chapter is dedicated to Testbed 1, entitled LTE-M with main objective the efficient validation of the LTE-M PHY layer algorithms Generalized Frequency Division Multiplexing (GFDM) and Code Division Multiple Access (CDMA)-overlay.

The third chapter is dedicated to Testbed 2, entitled End to End Communication.The testbed itself is analysed in 4 subtestbeds covering different aspects of the broader chapter's theme. These are:

a) Connectivity for a combined Intelligent Transport Systems (ITS) and eHealth scenario (corresponding to 2.1 subtestbed)
b) Heterogeneity and Interoperability (corresponding to 2.2 subtestbed)
c) Connectivity for low power devices (corresponding to 2.3 subtestbed) and
d) End to End Security (corresponding to 2.4 subtestbed)

Chapter 4 follows with the Device Management Testbed. Again, there are three distinct subtestbeds each own assessing and validating different aspects on Device Management. In detail these are:

e) Lightweight device management (corresponding to 3.1 subtestbed)
f) Self-Diagnostics (corresponding to 3.2 subtestbed) and finally
g) Security Element Device Management (corresponding to 3.3 subtestbed)

The structure of each chapter is identical for reasons of content coherence hence facilitating the reader into navigating through EXALTED development effort as this is expressed in the form of all subtestbeds. The starting point is a thorough description of the evaluation scenario followed by the definition of key objectives and performance indicators. The results are listed in the performance measures sub-section while they are analysed in the verification procedures sub-section. Each subtestbed closes with a wrap up paragraph summarizing the work carried out in a tabulated format.

The document closes with the conclusions section (chapter 5) where practically the overall EXALTED performance is scrutinized. The section is a summary of the considerable results achieved per each subestbed along with their qualitative characteristics as the quantifiable parameters were stated in the relevant subsections. It is worth to be noted that the results achieved regardless of the application domain followed closely the assumptions primarily made during the proposal preparation phase. There was a certain escalation from the work

carried out in WP2 on requirements of applications all the way to the implementation of hypotheses and their testing according to plan.

Apart from the typical sections of acronyms and references there is also an Annex in the document, where a relatively new subtestbed (2.5) on end to end communications (Testbed 2) has been added describing the work carried out on compressed sensing for capillary networks. The reason why an annex was introduced was that subtestbed 2.5 appears for the first time in the EXALTED literature and for reasons of continuum and coherence with D7.1 and D7.2 it was omitted in the main body of the document. However, the important fact is that EXALTED even beyond what was stated in the accepted DoW continues to produce results in M2M related techniques.

Table of Contents

Table of Contents v

1. Introduction 1

1.1 Overview of Key Performance Indicators 1
1.2 Methodology 2

2. Validation of Testbed 1: LTE-M 3

2.1 Evaluation Scenario 4
2.2 Key Objectives and Performance Indicators 5
2.3 Verification Procedures 6
2.4 Performance Measures 7
2.5 Wrap up 14

3. Validation of Testbed 2: End to End (E2E) Communication 16

3.1 Evaluation Scenario 16
3.2 Key Objectives and Performance Indicators 17
3.3 Sub-testbed 2.1: Connectivity for a combined ITS and eHealth scenario 18
3.3.1 Verification Procedures 21
3.3.2 Performance Measures 23
3.3.3 Wrap Up 29
3.4 Sub-testbed 2.2: Heterogeneity and Interoperability 31
3.4.2 Performance Measures 36
3.4.3 Verification Procedures 40
3.4.4 Wrap Up 40
3.5 Sub-testbed 2.3: Connectivity for low power devices 41
3.5.1 Performance Measures 45
3.5.2 Verification Procedures 46
3.5.3 Wrap Up 47
3.6 Sub-testbed 2.4: End to End security 48
3.6.1 Performance Measures 50
3.6.2 Verification Procedures 51
3.6.3 Wrap Up 52

4. Validation of Testbed3: Device Management (DM) 53

4.1 Evaluation Scenario 53
4.2 Key Objectives and Performance Indicators 53
4.3 Sub-testbed 3.1: Lightweight Device Management 54
4.3.1 Performance Measures 57
4.3.2 Verification Procedures 63
4.3.3 Wrap Up 64
4.4 Sub-testbed 3.2: Self Diagnostics 65
4.4.1 Performance Measures 65
4.4.2 Verification Procedures 65
4.4.3 Wrap Up 71
4.5 Sub-testbed 3.3: Secure Element Device Management 71
4.5.1 Performance Measures 72
4.5.2 Evaluation scenario 73
4.5.3 Wrap Up 73

5. Conclusions 74

A. Annex 76

A.1. Subtestbed 2.5: Compressed sensing for capillary networks 76

A.1.1. Performance measures 77

A.1.2. Verification Procedures 77

A.1.3. Wrap up 80

List of Acronyms 82

References 83

1. Introduction

The purpose of this report is to validate the overall proof of concept for the EXALTED project. Validation is done based on the results achieved through vigorous testing of each and every subtestbed and their analysis.

The three original testbeds described in the DoW were further analysed into various autonomous subtestbeds each one exploring the potential of a different scenario however. However they were all under the thematic umbrella of their parent testbed. LTE-M, End to end communications and Device Management were the three thematic areas. The scenarios of validation are a direct derivative of work carried out in other WPs and more specifically WP2.

The concept of validation or evaluation at the time was first addressed during the preparation of D2.1, Description of baseline reference systems, scenarios, technical requirements & evaluation methodology. As this document was delivered quite early in the project's life cycle it was obvious that alterations, improvements and updates were going to take place not only in the course of WP2 but also in other relevant WPs such as WP4 on the overall EXALTED Architecture. The concept of validation per se is pertinent to the quality of any service provided over M2M networks hence it is a horizontal aspect for nearly all WPs and their respective effort.

Useful tools for the validation effort were also the previous deliverables of WP7 where the scenarios and use cases per subtestbed were combined with the Key Performance Indicators and the overall technical requirements as these were explicitly described in the Appendix of D2.3 [2]. Each subsection, corresponding to a subtestbed, concludes with a wrap up in the form of a table with the following parameters:

- Scenario of evaluation
- Technical requirement addressed
- Qualitative Assessment
- Quantitative Assessment
- Measurable KPIs
- KPIs Assessment and contribution to Key Objective

This was selected as the most profound way of proving coherence between all EXALTED project's deliverables elaborating on the project's overall architecture and performance.

1.1 Overview of Key Performance Indicators

LTE and LTE-M based solutions are characterised by complexity of attributes and a plethora of parameters influencing the quality of the offered solution per case. The EXALTED Consortium in an effort to be as effective as possible in showcasing achievements and innovative aspects of the work undertaken has made a careful selection of Key Performance Indicators suitable for each scenario but not limited to it. This selection was a collective procedure taking into consideration contributions from all aspects of the project's components as these were expressed in the relevant WPs. A detailed list of KPIs can be found in D7.2

1.2 Methodology

As basis for validation we have considered the scenario (a more elaborated version of the use cases as defined in WP2) along with the relevant assumptions for testing specific parameters. EXALTED has focused upon scenarios addressing complex problems and proposed various innovative solutions.
The following Figure 1-1 provides an overview of the scenarios that ended up in testing during the validation phase. It has to be noted that non all scenarios in the figure were actually implemented as testbeds mostly due to time and resources constraints.

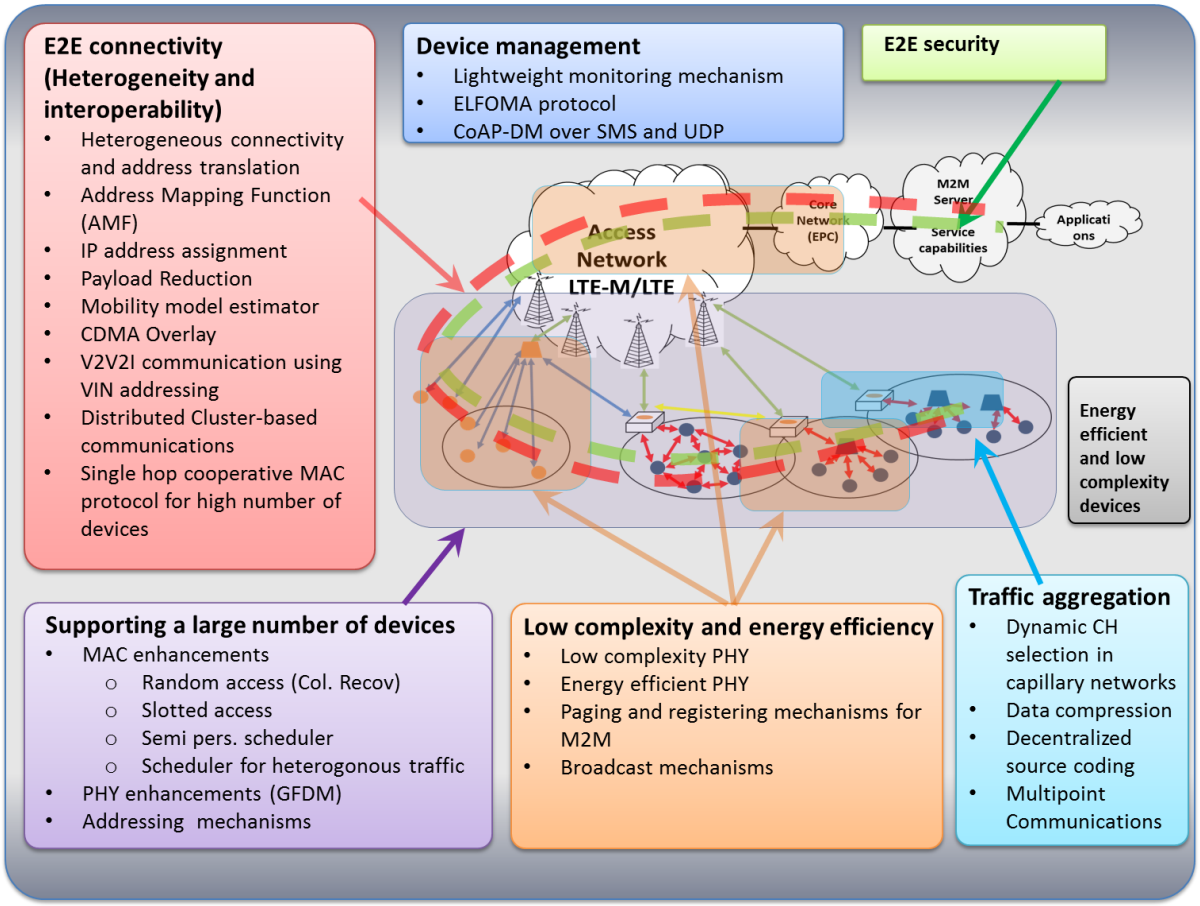


Figure 1-1: EXALTED evaluation scenarios

2. Validation of Testbed 1: LTE-M

The main objective of this testbed is the efficient validation of the LTE-M Physical (PHY) layer algorithms Generalized Frequency Division Multiplexing (GFDM) and Code Division Multiple Access (CDMA)-overlay. Algorithms and protocols that belong to other layers are not realized. Also, it is not the intention to demonstrate the applicability of the algorithms for one specific use case, but to show their generally valid functionality.

Commonly used tools for PHY layer algorithms are link level simulation chains. They usually consist of three components, the transmitter, the radio channel and the receiver. All transmitter and receiver baseband algorithms are firstly tested with software tools, e.g. MATLAB. While the MATLAB versions of these algorithms never differ from their behaviour in the actual LTE-M device and the evolved NodeB (eNodeB) hardware, this is not the case for the radio channel. Therefore, several software models for the radio channel have been proposed, e.g. the Spatial Channel Model Extended (SCME) [3]. Typical parameters of channel models are the number of propagation paths, their delays, their mean attenuation, their angles of departure and arrival, and of course the statistical metrics describing how all these parameters change over time.

An analysis of the MATLAB link level simulation tool has shown that the channel model consumes nearly 80% of the overall computation time. This fact excludes a broad evaluation, i.e. the simulation with different channel models, different system parameters, different signal-to-noise-power ratio (SNR) values and different modulation and coding schemes is not possible in a reasonable time. A solution for this problem is the so-called Hardware-in-the-Loop (HaLo) principle. In a simplified view, HaLo replaces the computationally intensive MATLAB equivalent lowpass radio channel model, just by the real radio channel. The difference between a pure software simulation chain and the HaLo is shown in Figure 2-1. In both cases the transmitter algorithms are executed in the MATLAB simulation chain. Instead of feeding the time samples in the software channel model, the HaLo transmitter constructs a physical transmit signal including up conversion to the carrier frequency and radiation from an antenna. After the propagation over the air, the signal is received, filtered and down-converted by the respective inverse entity labelled with Sorbas in Figure 2-1. The result is a set of time samples in exactly the same format than the output of the software channel model would be. They are further processed in the MATLAB chain with the receiver algorithms. A more detailed description of Testbed 1 is available in the project deliverable D7.2 [1]

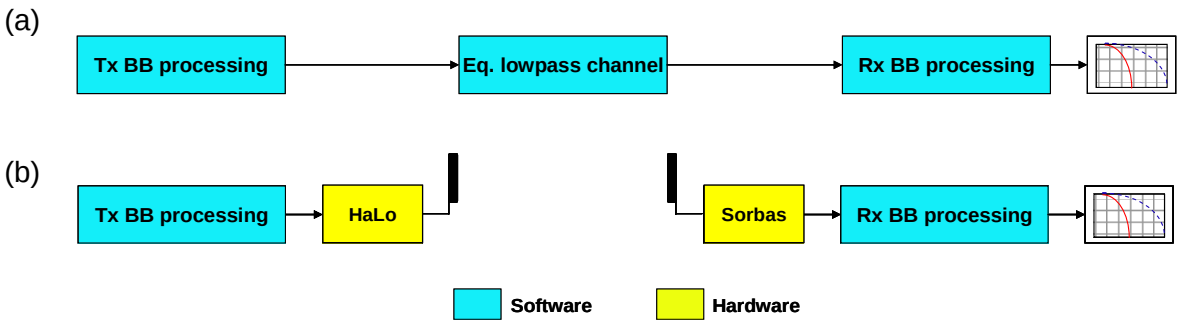


Figure 2-1: Performance evaluation with (a) link level simulation chain and (b) HaLo over the air replacing the software channel model

In this section firstly two different evaluation scenarios are introduced, one for a joint LTE and LTE-M transmission, and the second for pure LTE-M transmission. Afterwards the key objectives and performance metrics for the evaluation are described. Then the verification procedures are explained, and finally, the measurement results for both scenarios are presented.

2.1 Evaluation Scenario

The evaluation of algorithms in Testbed 1 was carried out in two different scenarios. While one is representing the interaction of LTE-M algorithms with the primary LTE system, the second focuses on the specific properties of the LTE-M algorithms and therefore doesn't incorporate the primary LTE system.

Scenario 1 (Joint LTE and LTE-M transmission):

In this scenario a single cell setup in a noise-limited regime is considered. Inter-cell interference is not present. The communication system is based on an uplink transmission of one M2M message as this is the typical use case for example in smart meter reading or other monitoring applications. The setup consists of three devices:

- **LTE-M device**: The LTE-M device is configured with either GFDM or CDMA in the base band processing. The specification of both solutions can be found in the project deliverable D3.3 [4]. A transmit frame is generated, based on the respective algorithm chosen for evaluation which is then sent over the air in a time-continuous manner (greedy source traffic model). The LTE-M device typically occupies the same amount of resources as compared to 6 physical resource blocks in frequency (72 subcarriers) if not otherwise stated. The LTE-M device uses one single transmit antenna and a carrier frequency of 2.53GHz. As adaptive modulation and coding is not envisaged for single-shot message transmission, no control channels are used and the evaluation is carried out only for Physical Machine Type Communications (MTC) Uplink Shared CHannel (PMUSCH) (see project deliverable D3.4 [5])
- **LTE User Equipment (UE)**: Two LTE UEs are part of the Joint Transmission scenario. These do represent the typical LTE users of the primary LTE system. The LTE UEs are constantly communicating on the adjacent frequency bands to the LTE-M transmission (within the bandwidth of LTE), i.e. resources for LTE-M and LTE do not overlap **LTE eNodeB**: The LTE eNodeB is used to receive the joint transmissions of the LTE UEs together with the transmissions from the LTE-M device. The extraction of the different transmissions can then be done via individual base band processing incorporating the complex base band samples from the eNodeB. Performance evaluation for the LTE system and the LTE-M algorithms is carried out.

Scenario 2 (Single LTE-M transmission):

To further study the real-world performance of proposed algorithms from LTE-M, Scenario 2 is used. It focuses on the pure evaluation of characteristics of GFDM and CDMA algorithms with different parameterization. Therefore the testbed setup consists of two devices:

- LTE-M device: The LTE-M device is configured with either GFDM or CDMA in the base band processing. A transmit frame is generated, based on the respective algorithm chosen for evaluation which is then sent over the air in a time-continuous manner (greedy source traffic model). The parameterization is done with respect to specific evaluation criteria. The LTE-M device uses one single transmit antenna and a carrier frequency of 2.53GHz.
- Link Level Simulator: The link-level simulator serves as the counterpart to the LTE-M device and is needed for reception and evaluation of the uplink transmissions.

With these two scenarios the evaluation of key objectives for Testbed 1 can be covered.

2.2 Key Objectives and Performance Indicators

The key objective of Testbed 1 is the evaluation and the proof-of-concept for two key algorithms within the LTE-M system design. While the EXALTED project aimed at the investigation and specification of specific solutions for a coherent LTE-M system design, the objective of Testbed 1 is to choose exemplary solutions/algorithms from the respective work package (WP3) and evaluate the performance of these solutions within a real world setting. The two algorithms selected for evaluation are

- Generalized Frequency Division Multiplexing (GFDM): A novel filtered multi-carrier approach for radio access
- CDMA overlay: An additional code spread overlay for increased coverage

For technical details on the algorithms, please refer to project deliverables D3.3 [4] and D3.4 [5].

To assess the performance of the solutions from the LTE-M design and especially to compare them against the theoretical results found in other work packages, the evaluation is based on predefined key performance indicators.

- Bit Error Rate (BER) and Transport Block Error Rate (BLER) as proof for successful separation of the three devices and decoding of the signals at the receiver (associated metric to BER for coexistence requirement is “Achievable Rate”)
- Peak-to-Average Power Ratio (PAPR)
- Out-Of-Band (OOB) radiation as proof for the claimed beneficial spectral properties of GFDM

While BER (Achievable Rate), BLER and PAPR can be assessed quantitatively, OOB will be shown qualitatively via spectral masks.

To assess whether the key objective has been achieved, technical requirements have been defined in the project deliverable D2.1 [6] and shall be applied to the verification of the algorithms in Testbed 1 as described in D7.2 [1]. While some requirements are directly connected to the assessment via a specific Key Performance Indicator (KPI), others can only be evaluated qualitatively and via deduction.

To summarize the evaluation of Testbed 1, the considered scenarios together with the addressed technical requirements and KPIs used are summarized in Table 2-1.

Table 2-1: Technical requirements for LTE-M and mapping to evaluation scenarios.

Scenario	ID	Title	Comments
Scenario 1 (Joint LTE and LTE-M transmission):	NT.2	LTE-M backward compatibility	Testbed 1 shows two indications: • Only negligible performance degradation for LTE users with respect to the achievable rate (indirect assessment of BER) At least with respect to uplink PHY, the inclusion of LTE-M does not require additional hardware in the eNodeB
	SV.1	Overall Quality-of-Service (QoS) concept	As Testbed 1 is restricted to the uplink PHY layer of LTE-M, the tracing of this requirement is limited to a qualitative assessment based on (K1) – BER observations.
Scenario 2 (Single LTE-M transmission):	SV.1	Overall QoS concept	As Testbed 1 is restricted to the uplink PHY layer of LTE-M, the tracing of this requirement is limited to a qualitative assessment based on (K1) – BER observations.
	FU.2	Efficient spectrum management	The aim is to show that LTE-M GFDM signals can fit in very small spectrum gaps not occupied by LTE users (specification of joint LTE/LTE-M uplink frame see report D3.3 [4]). The used KPIs are (K1) BER, (K6) Peak-to-Average Power Ratio (PAPR), and (K7) OOB
	NF.1, FU.1	Scalability, Support of large number of devices	The fact shown by experiment with Testbed 1 that GFDM can occupy very small, but scalable frequency resources indicates that at least LTE-M PHY uplink supports a big number of short messages transmitted simultaneously..
Misc	NT.3	Minimum number of modifications in network infrastructure	In can be shown qualitatively that the operation of LTE-M PHY uplink in Testbed 1 does not require any changes in the network infrastructure.
	NT.5	Half duplex transmission mode	It can be shown qualitatively that LTE-M PHY functionality supports the application of half-duplex operation.
	NF.2	Energy efficiency	The tracing of this requirement with Testbed 1 is limited to a qualitative assessment. The capabilities of GFDM enable efficient duty cycles in the sense of sporadic wake-up of devices and one shot transmissions in small spectrum chunks.

Note that some technical requirements are covered in both scenarios!

2.3 Verification Procedures

The verification of results in Testbed 1 is done by comparison of theoretical and simulative results carried out in WP3. In WP3, the specific solutions of LTE-M were investigated and results from this WP are the baseline for comparison. The proof-of-concept incorporates, that measured results should somehow be related to the theoretical investigations done in WP3. If this is not the case, a reasonable explanation for this is given, pointing out the limitations of Testbed 1 or subjects to further study and implementation.

The comparisons outperformed for the measured results of Testbed 1 are covered in Section 2.4 to ensure and simplify a coherent comparison of theoretical/simulative and measured results.

2.4 Performance Measures

The performance measurements are carried out within the two specified scenarios to obtain statements for proof of concept regarding the technical requirements aimed.

Scenario 1:

To assess the technical requirement of LTE backward compatibility (NT.2) measurements for the achievable rates of the LTE were performed when GFDM is used in the LTE-M uplink. The goal of the LTE-M system is to work properly without harming the performance of the primary LTE system. LTE users should not suffer from the additionally served M2M devices in the cell and therefore performance should not be degraded for LTE. Figure 2-2 shows the performance of LTE in terms of the achievable rate for the LTE users with two settings.

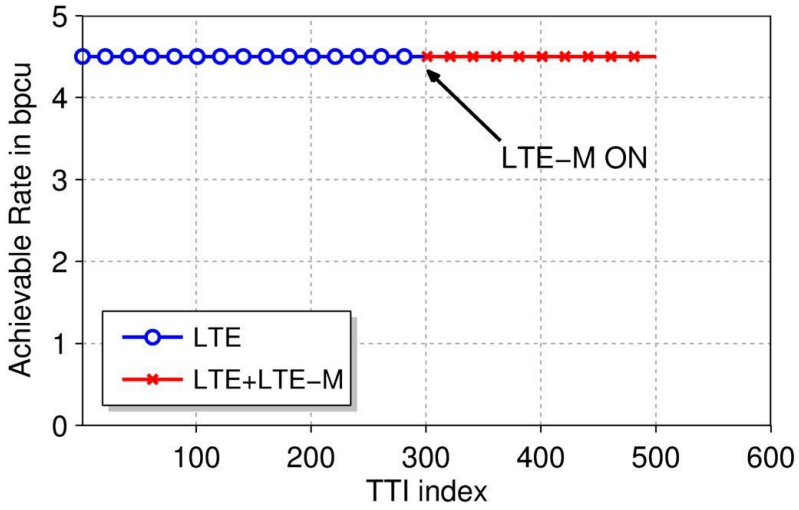


Figure 2-2: Achievable rate for LTE-when only LTE is running (blue) and after switching on LTE-M transmission (Transmission Time Interval (TTI) index = 300, red)

In setting one, the achievable rate of the LTE primary system on the PHY layer is provided when LTE-M transmission is not incorporated within the bandwidth of the LTE. An achievable rate of 4.5bpcu (bits per channel use) can be shown stable over time. This setting serves as the case for comparison. When LTE-M transmission is switched on (LTE-M ON), the achievable rate should not or only to a minor extend be degraded. Setting two shows exactly this behaviour. The use of GFDM in the uplink of LTE-M interferes negligibly with the primary LTE system which yields a similar achievable rate (4.5bpcu) as in the setting without LTE-M. Backward compatibility regarding the performance degradation of primary users is achieved. Additionally, to the performance in terms of achievable rate, backward compatibility must be ensured by keeping the hardware that is used in the eNodeB unchanged. A massive hardware change at every site that should support LTE-M is simply not feasible. The implementation of GFDM receiver algorithms for reception of LTE-M uplink in the base station did not need any changes in hardware. The base station used for evaluation was a reference implementation of the LTE-Advanced PHY layer and the incorporation of GFDM receiver algorithms did not need any change in hardware. Therefore, LTE backward compatibility (NT.2) with respect to hardware changes was also achieved.

To further underlay the coexistence of LTE and LTE-M a spectrum plot (Figure 2-3) shows the resource sharing of LTE-M and LTE in the uplink (PMUSCH).

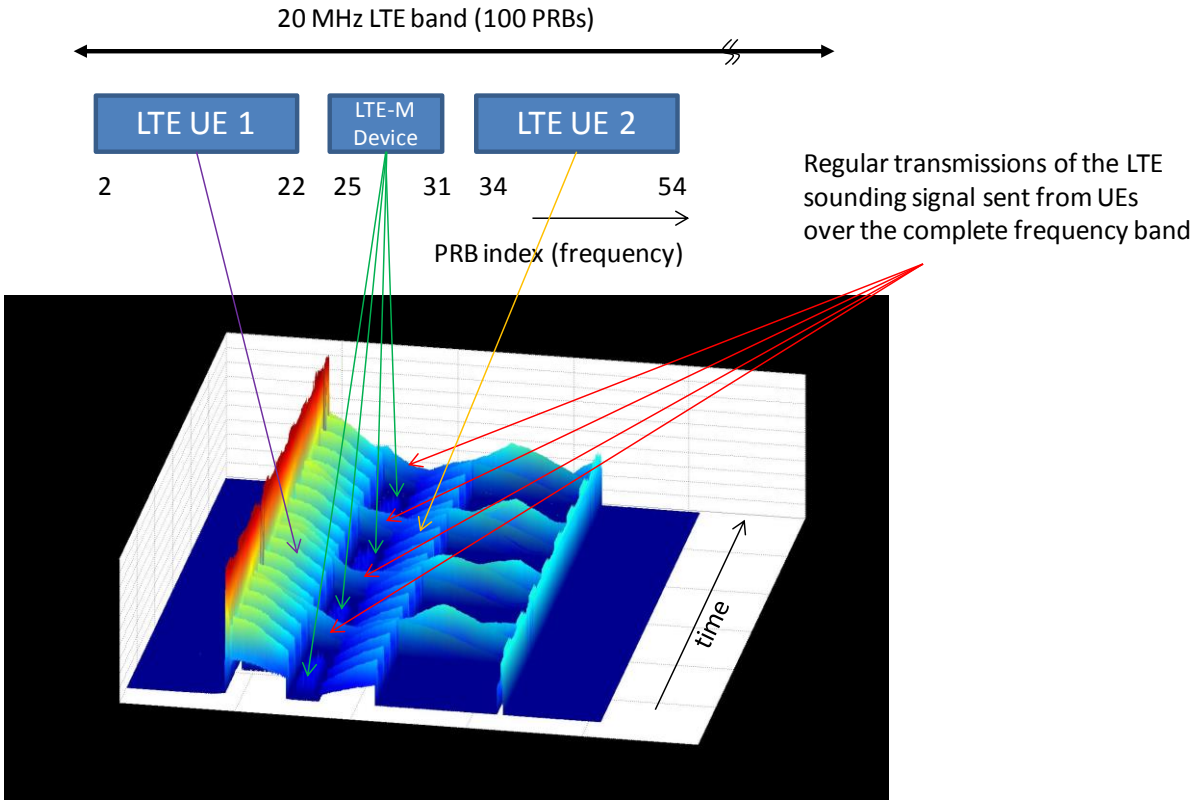


Figure 2-3: Received signal strength of LTE and LTE-M waveforms over time and frequency.

Figure 2-3 illustrates the cumulative receive signal at the eNodeB over time and frequency. The colour code refers to the detected signal strength. The two LTE UEs and the LTE-M device each occupy a dedicated part of the frequency band. Moreover, it is evident that both LTE UEs transmit their sounding signal over the complete frequency band. The LTE-M signal appears in the gaps between the LTE signals (in frequency direction) and between the sounding signals (in time direction), visible as the bright blue regions.

As in D3.4 described, the resources in the uplink are freely shared between Physical Uplink Shared CHannel (PUSCH) (LTE) and PMUSCH (LTE-M). While in the evaluation scenario PUSCH and PMUSCH are separated in frequency, any arbitrarily resource use pattern based on the resource grid defined in D3.4 [5] can be used. Measurements were carried out with GFDM in the LTE-M uplink. While the inter-system orthogonality (between PUSCH and PMUSCH) ensures that the systems do not interfere, the intra-system non-orthogonality of GFDM in the PMUSCH ensures that transmissions can exhibit larger time- and frequency offsets.

Similar measurements were carried out applying the CDMA-overlay in LTE-M. In contrast to the previous results, Single Carrier Frequency Division Multiple Access (SC-FDMA) was used instead of GFDM. However, this fact does not restrict the general validity of the following evaluation.

The fact that both LTE and LTE-M utilize the same waveform (SC-FDMA) and separated resources implies that LTE-M does not impact the performance of LTE. Although not explicitly measured, it is clear that the same behaviour as shown in Figure 2.3 is observed. This important aspect of backward compatibility is fulfilled. For the same reason, the requirement that the LTE-M transceiver must not require additional hardware is achieved as well. All in all it is claimed that the requirement NT.2 is completely fulfilled.

The second requirement, SV.1 – Overall QoS concept, using CDMA-overlay was validated qualitatively. For this purpose different pre-processed LTE-M transmit signals were sent with CDMA-overlay from the HaLo box and received with the Sorbas. Afterwards, the received signals were fed in the MATLAB link level chain as shown in Figure 2-1. Two different cases with Quadrature Phase Shift Keying (QPSK) and spreading factor 4 were investigated. The first case applies spreading of a small transport block (150 bits) within one single subframe. In the second case, the transport block is big (600) and the spreading ranges over four subframes. The four subframes were sent and received independently from each other in separate consecutive experiments and reworked afterwards. The decoding results for the different cases are summarized in Table 2-2.

Table 2-2: Summary of CDMA Transmit (Tx) vectors and decoding results.

Tx vector parameters	Decoding result
QPSK, spreading factor 4, transport block size 150 (spreading within one single subframe)	Successful
QPSK, spreading factor 4, transport block size 600 (spreading over four subframes)	Successful

For practical reasons the variety of parameter settings in Scenario 1 is small. However, the successful decoding implies that the principle of CDMA-overlay is applicable as LTE-M PHY layer solution. These results cannot be compared directly with the findings in WP3. The evaluation in WP3 is based on system level simulation in a multi-cell environment including inter-cell interference, whereas the experiments described above were carried out in an isolated indoor lab. However, the outcomes in both work packages complement each other, and both of them underline the potential for coverage extension in noise-limited environments.

Scenario 2

To quality of service for M2M devices is of major interest as energy constraint nodes often only want to transmit one single message (e.g. a measurement) in the uplink and then go to sleep mode again for preserving energy. Therefore it is very important to show that the PHY layer algorithms of LTE-M exhibit almost optimal performance compared to the simulated ones shown in D3.3 and D3.4.

The assessment of the technical requirement of overall QoS (SV.1) in Testbed 1 is carried out with bit error rate as the KPI that shows if the theoretical and simulative results can be obtained within a real world setting for proof of concept.

Figure 2-4 shows the BER in a typical M2M devices setting as e.g. for the metering use case. The M2M device is located at a fixed position and also the surrounding is not changing rapidly. This results in a frequency-selective but time-flat multipath channel.

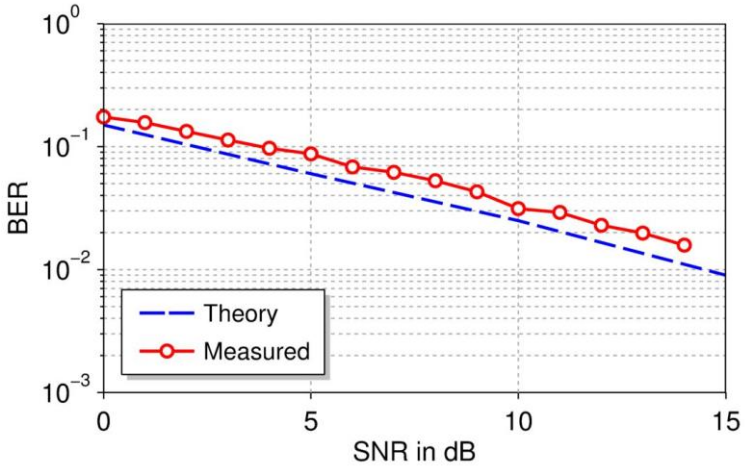


Figure 2-4: BER of GFDM in the LTE-M uplink (comparison of theoretical result in blue with measured result in red)

For comparison, the theoretical curve (from D3.3) is given as reference. The results for K=128, M=5 and QPSK show similar performance for the proof-of-concept system as compared to the simulated system. The BER follows the typical fading characteristic of a Rayleigh channel model. A slight gap and therefore performance decrease can be measured. This degradation is due to the incorporated synchronization algorithm which was not simulated in the theoretical work of D3.3.

The above shown results mimic the behaviour of GFDM in real fading channel environments with a specific parameter set exemplarily. Table 2-3 summarizes the BER performance of GFDM for other parameters (common: QPSK, a=.01).

Table 2-3: BER measurement results for GFDM

K	M	Subcarriers used for data	Result
128	5	128	Theoretical BER achieved
2048	15	200	Theoretical BER achieved
2048	15	72	Theoretical BER achieved

The uplink of LTE-M is specifically designed for efficient spectrum access. The spectral properties of GFDM together with the variable resource use methods of the PMUSCH form an elegant and spectrum efficient way of radio access. While GFDM itself is already a pulse-shaped waveform that exhibits good spectral properties its behaviour with a real power amplifier is very important. Cheap power amplifiers (as used in M2M devices) can produce significant out-of-band radiation when a waveform is used for transmission that has a high peak-to-average power ratio (PAPR). Figure 2-5 shows measurements that compare the PAPR of GFDM (2048 point Fast Fourier Transform (FFT) and M=15) in the LTE-M uplink to the typical waveforms of SC-FDMA and OFDM.

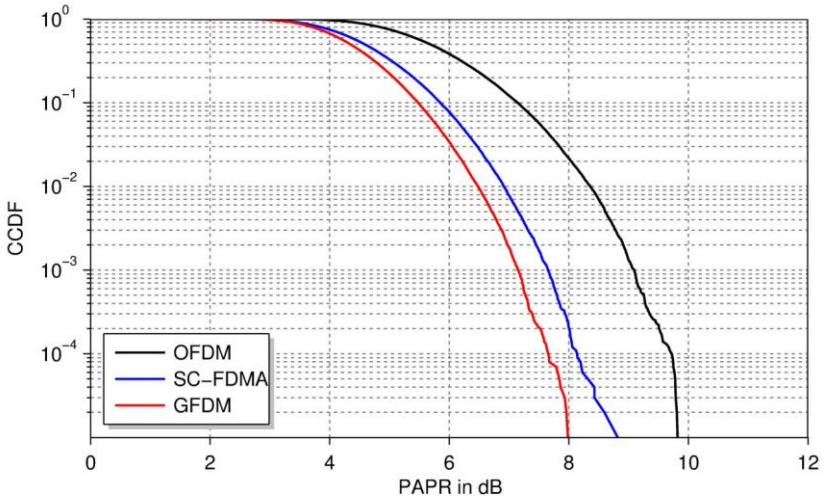


Figure 2-5: PAPR of LTE-M uplink compared to typical solutions of LTE (SC-FDMA and OFDM)

It can be seen easily, that in the setting of transmission with one resource block (as it can be done in PMUSCH for one-shot transmission of a meter reading message) the PAPR of the proposed uplink waveform in LTE-M reduces the PAPR compared to the traditional ones of LTE. This outcome is even underlined when observing the spectral properties of the LTE-M uplink waveform. Figure 2-6 shows the measurements of spectra of the primary LTE uplink system in comparison with the proposed GFDM waveform for LTE-M.

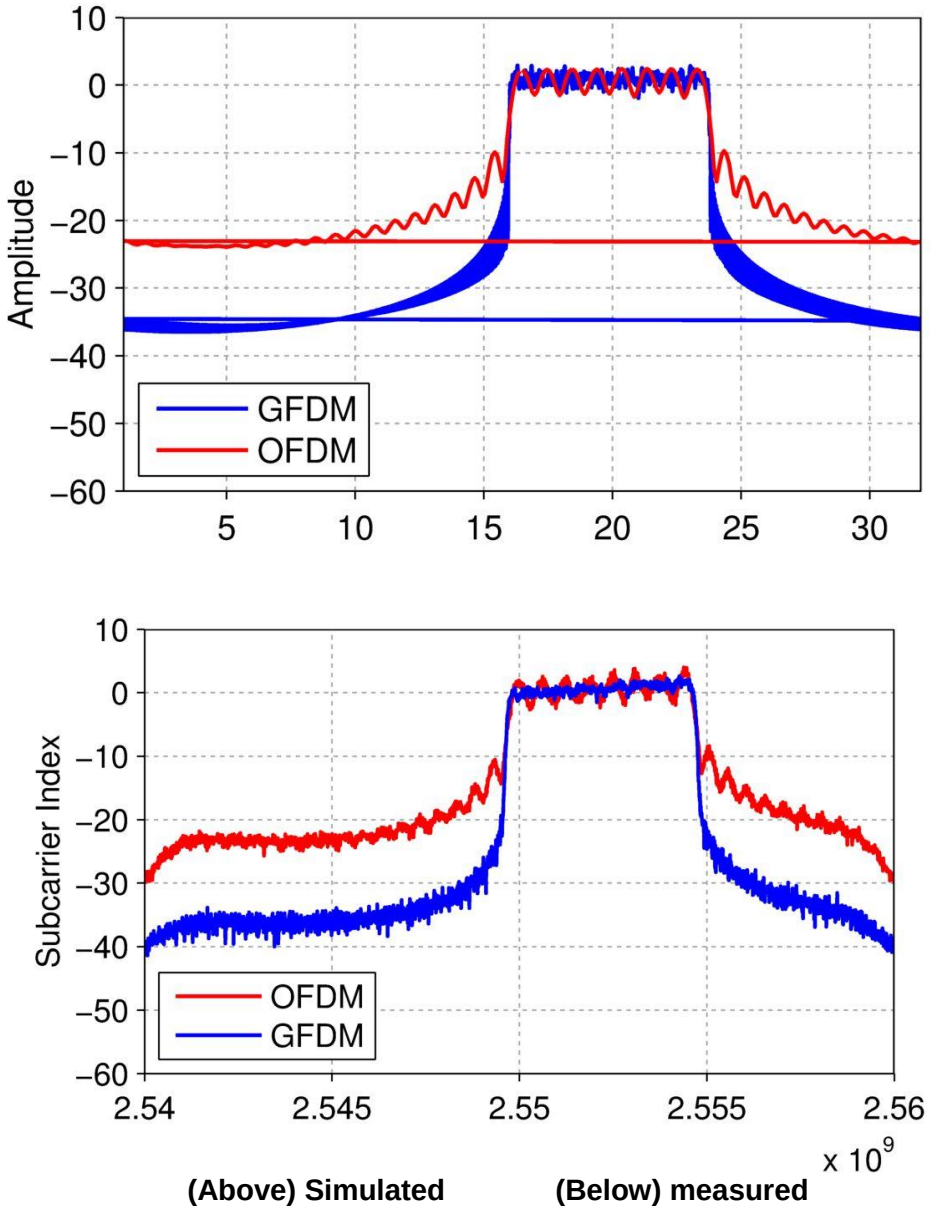


Figure 2-6: OOB radiation comparison between LTE-M uplink waveform (blue) and exemplary LTE waveform (red)

A clear reduction in OOB can be observed compared to OFDM. Similar reduction can be deduced from the PAPR behaviour also compared to SC-FDMA. The advantage of such an OOB reduction is the flexible support of efficient spectrum use. Even when the LTE-M uplink signal is slightly shifted in time and frequency due to cheap hardware used in the M2M device, the spectral properties and low OOB ensure for successful decoding of LTE-M and LTE signals as they do not interfere. Technical requirement NT.2 (backward compatibility) is therefore supported again.

Additionally, the specific resource structure of GFDM (see D3.4) together with its spectral properties enables the LTE-M uplink to serve more users as compared to the LTE uplink structure. The gain in terms of additional frequency resources (as shown in D3.4) can be seen in Figure 2-6. The additional gain in time cannot be shown within Testbed 1 but as the resource structure of LTE-M uplink is used in Testbed 1, this gain is still applicable. The

technical requirements NF.1 and FU.1 are therefore shown to be met reasonably in a qualitative way.

The requirement SV.1 (Overall QoS-Concept) was evaluated in Scenario 2 with CDMA-overlay as well. Whereas in Scenario 1 only the two cases with QPSK and spreading factor 4 in Figure 2-6 were investigated, the variety of parameter settings in Scenario 2 was significantly increased because the measurements can be carried out much easier and faster without the presence of the two LTE UEs. The combinations of Tx vector parameters that were tested and the respective decoding results are summarized in Table 2-4.

Table 2-4: CDMA-overlay parameter settings

Modulation scheme	Spreading factor	Transport block size	Decoding result
QPSK	4	150	Successful
QPSK	16	150	Successful
QPSK	32	150	Successful
QPSK	64	150	Successful
QPSK	128	150	Successful
QPSK	1 (LTE uplink)	600	Successful
QPSK	4	600	Successful
QPSK	8	600	Successful
QPSK	16	600	Successful
QPSK	32	600	Successful
16-QAM*)	4	650	Successful
16-QAM	16	650	Successful
16-QAM	32	650	Successful
16-QAM	64	650	Successful
16-QAM	128	650	Successful
16-QAM	1 (LTE uplink)	2600	Successful
16-QAM	4	2600	Successful
16-QAM	8	2600	Successful
16-QAM	16	2600	Successful
16-QAM	32	2600	Successful

*) QAM = Quadrature Amplitude Modulation

In all cases the received vector could be decoded successfully. The applicability of CDMA-overlay to serve as solution facilitating an overall QoS-concept is therefore claimed. These results cannot be compared directly with the findings in WP3. The evaluation in WP3 is based on system level simulation in a multi-cell environment including inter-cell interference, whereas the experiments described above were carried out in an isolated indoor lab as an experimental proof-of-concept.

The technical requirements that do not relate directly to one of the above used measurement scenarios are discussed in the following:

- NT.3 (Minimum number of modifications in network infrastructure): This technical requirement is related to the one of backward compatibility. When introducing a new PHY layer for LTE-M, the goal is to minimize the number of modifications that shall be done within the current infrastructure. The implementation of LTE-M uplink solutions for the evaluation and proof-of-concept in Testbed 1 didn't incorporate any changes to the infrastructure of the LTE Advanced testbed. The testbed was used in the same setting as it would be used for LTE. The technical requirement NT.3 therefore was met completely.
- NT.5 (Half-duplex transmission): Half duplex transmission is an important solution for M2M communications as it supports the use of only one RF-chain in the M2M transceiver. A cost reduction is the result. Within the scope of evaluations and

measurements in Testbed 1, a transmission protocol based on the idea of single message transmission was used and was implemented in half-duplex. All performance evaluations and measurements of Testbed 1 where carried out with this simple greedy transmission protocol and successful operation was shown. Therefore, half-duplex transmission is supported and the technical requirement was achieved.

- NF.2 (Energy efficiency): The technical requirement of energy efficiency is probably the most important one when considering energy constraint M2M devices such as sensor nodes in rural areas. The evaluation of this requirement nevertheless is only indirect in Testbed 1. The applied one-shot transmission of short messages that can be successfully decoded was shown in previous evaluations in the two above mentioned scenarios. Assume a long-term measure and transmit protocol that works as follows: With a specific duty cycle, an M2M node takes measurements (e.g. temperature) and has to deliver these measurements to the application server. The most energy efficient way to serve this application is to let the M2M device sleep completely within the time where no measurement takes place and only wake up to measure and deliver the short message. Exactly this kind of transmission is inherently modelled within Testbed 1 and successful transmission was shown. Therefore the requirement of energy efficiency was shown to be met.

2.5 Wrap up

The objective of Testbed 1 is to demonstrate the generally valid applicability of LTE-M PHY layer solutions GFDM and CDMA-overlay with lab experiments. These complement simulation studies carried out in work package WP3. The focus of the measurements was to verify the coexistence of LTE-M and LTE in the same frequency band. For this, a transmission scenario consisting of two LTE UEs and one LTE-M device was defined. The results show firstly that the performance of the LTE UEs is not affected at all and secondly that the LTE-M signal can be decoded successfully. These findings confirm the theoretical results from WP3.

A second measurement scenario without the two LTE UEs primarily aimed at the verification of the spectral properties of GFDM. This was shown by a comparison of the measured spectral power density with a respective simulation. Moreover, the required overall QoS concept was evaluated. The BER depending on the SNR was determined using GFDM and compared against simulation results. It was further shown that CDMA-overlay Tx vectors representing different settings of modulation scheme, spreading factor, and transport block size can be successfully decoded. Again, a reasonable match between results from WP3 and the measurement campaign is claimed.

Table 2-5 summarizes the achievements of technical requirements in Testbed 1.

Table 2-5: Summary of achieved technical requirements

Scenario	ID	Title	Result/Achievement
Scenario 1 (Joint LTE and LTE-M transmission):	NT.2	LTE-M backward compatibility	• Stable rates (4.5bpcu) for LTE when LTE-M transmission is running • No additional hardware in eNodeB (PHY layer)
	SV.1	Overall QoS concept	Successful decoding of CDMA overlay
Scenario 2 (Single LTE-M transmission):	SV.1	Overall QoS concept	Theoretical BER performance was met with measurements.
	FU.2	Efficient spectrum management	Reduced PAPR and reduced OOB in conjunction with adaptive resource usage makes LTE-M uplink flexible and spectrum efficient

	NF.1, FU.1	Scalability, Support of large number of devices	Successful decoding (BER) of GFDM together with spectral properties as well as reduced CP ensure for increased number of users.
Misc	NT.3	Minimum number of modifications in network infrastructure	No modifications in infrastructure applied.
	NT.5	Half duplex transmission mode	Is supported.
	NF.2	Energy efficiency	GFDM enables for efficient duty cycles in the sense of sporadic wake-up of devices and one shot transmissions in small spectrum chunks.

3. Validation of Testbed 2: End to End (E2E) Communication

One of the major objectives in the EXALTED project is the support of a very large number of LTE-M devices consequently the testbed addressing end to end communication (E2E) is expected to focus on scalability issues pertinent per case and scenario of validation.

Practically what we will try to achieve is to transmit the same amount of information but using as few resources as possible due to fact that the radio resources available for LTE-M are fixed (LTE frame structure and LTE-M super frame principle).

There are two ways in order to achieve minimisation of transmitted information:

- Minimising size and control of feedback messages
- Use of traffic aggregation or novel signal formats against inefficient resource utilisation

The aforementioned techniques vary according to the capabilities of devices as well as the application specific requirements. The following analysis per testbed provides analytic information on the devices used as well as the evaluation scenario implemented hence defining the requirements pertinent to it.

For an extensive analysis on the LTE-M performance evaluation as addressed by EXALTED please refer to D3.4 [5].

3.1 Evaluation Scenario

This scenario will focus on demonstrating the novelties developed in three main fields [1]:

- Concepts developed within capillary networks
- Providing end-to-end connectivity between M2M devices, not only belonging to the same capillary network, but also from different ones connected to the LTE/LTE-M network.
- Providing end-to-end security between M2M devices and M2M server

For this purpose and in order to address every use case, this testbed can be seen as a composition of four subtestbeds (five taking into consideration testbed 2.5 described in the Annex) each one based on its capillary network. This represents the real-life sub-networks each one addressing a set of requirements for the end user.

Figure 3-1 shows the different pieces of hardware and their relationship with the proposed algorithms, as well as the way connectivity is shown:

- **Subtestbed 2.1** is ITS and eHealth oriented. The objective is to prove connectivity when energy efficiency and high compression is not critical, but mobility, reliability and delay are crucial aspects to take into account. eHealth use case is intended to be built on top of a vehicular use case, using different elements in the architecture combining cellular radio communications technologies and capillary vehicles, with an E2E IPv6 framework that assures scalability, efficient and fast routing and reliable mobility management.
- **Subtestbed 2.2** aims at demonstrating connectivity for a Smart Metering and Monitoring (SMM) scenario using different technologies and heterogeneous devices. Several radio interfaces will be used, integrating low cost and low power devices controlled by enhanced M2M gateways implementing software capabilities developed within EXALTED. The result is a common testbed using multi-vendor devices interacting together and managed via a purpose specific protocol derived from the work in the project.
- **Subtestbed 2.3** tackles the problem of maintaining connectivity when the network is composed of very constrained low power devices, again using the example of SMM. Due to the simplicity of end nodes, they cannot implement a traditional communication protocol

stack as it is, so there is a need for defining a lightweight address translation mechanism able to provide seamless communication between M2M servers in the IP world and these low power devices. With that implementation, E2E connectivity and scalability are achieved while maintaining the efficiency required in the capillary network.

- The purpose of **Subtestbed 2.4** is to protect application payloads from security attacks. This E2E security is performed in the context of a SMM application deployment where some meter index values are sent by devices to the M2M server to be analyzed. Business case is to control on a server the energy produced by photovoltaic panels. Service provider wants to protect the collected values against malicious tampering. Two different Secure Element form factors are used with this subtestbed: either a SIM card or the Secure Element developed for the purpose of the project. In the former case the SIM of the device used to manage the communication with the network is also used to protect messages while the EXALTED Secure Element is embedded on a non LTE-M device in the latter case.

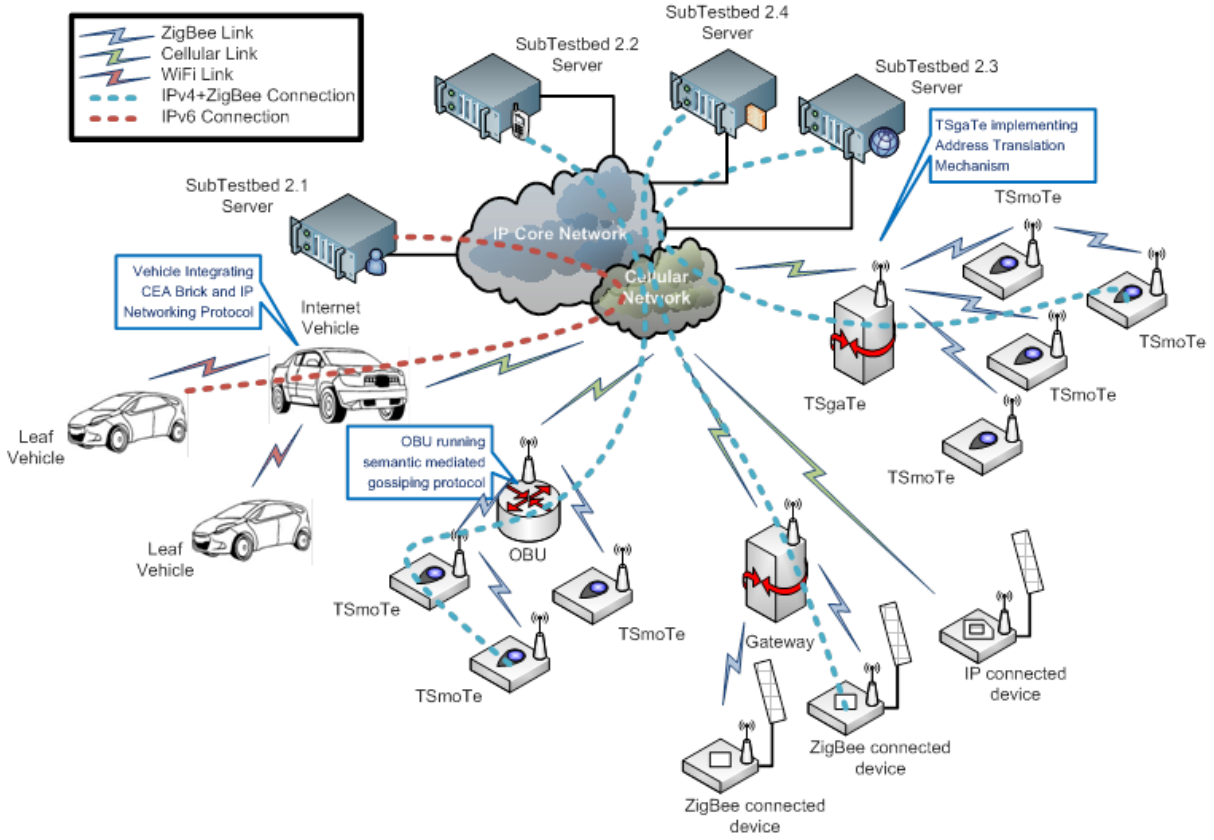


Figure 3-1: Hardware, algorithms and connectivity mapped for Testbed 2

The combination of the four subtestbeds makes this proof of concept applicable to all key use cases assumed by the project. Moreover, all of them can coexist and share the same location sharing the same physical resources, so it enables demonstrating the scalability, interoperability and heterogeneity of the applications.

3.2 Key Objectives and Performance Indicators

Table 3-1 summarizes the Key Objectives and Performance Indicators per Use Case as these were first defined in deliverable D2.4 [7].

Table 3-1: Summary of Connectivity oriented Testbed per use case

Solution/innovation	Main KPI	Use cases that the solution is applicable to	Comments/remarks
Device addressing and address translation	**K20** Number of addresses mapped	ITS, SMM, e-Health	Up to 65536 devices can be successfully configured in each capillary network.
Payload reduction	**K30** Transmission Payload Size	ITS, SMM, e-Health	Reduction policies may lower transmission packet sizes by a factor of 4.
Device association	**K5** Outage probability	SMM	Reliability in device connectivity of a CH-based network significantly increases if the devices are able to choose between CHs.
Mobility estimation	**K29** Mobility management efficiency	ITS	An accurate estimator is provided which will help the network allocate its resource better, based on device mobility patterns
Coverage extension	**K26** Coverage	ITS, SMM, e-Health	By extending the transmission time of a transport block over multiple sub-frames, an eNodeB is able to extend its coverage area.

3.3 Sub-testbed 2.1: Connectivity for a combined ITS and eHealth scenario

Connectivity oriented subtestbed 2.1 demonstrates the feasibility of capillary-to-capillary-to-Infrastructure IP communications. In the particular paradigm of vehicular communications, Vehicle-to-Vehicle-to-Infrastructure (V2V2I) is the equivalent. In particular, an eHealth setting is deployed on two parts of the architecture and connected through an IPv6 networking setting involving two neighbouring M2M gateways where only one is connected to the infrastructure. The M2M Electronic Health Record (EHR) server is deployed in the application domain, while the M2M eHealth devices are connected to the infrastructure through the leaf M2M Gateway; that is, the M2M GW is not provided with access to the LTE-M infrastructure. This leaf M2M Gateway relies on its neighbour in order to access the M2M services provided by the M2M server. The second M2M Gateway is connected to the infrastructure and

provides the requesting M2M gateway with the IPv6 network settings (prefix and default route) that allow it to reach the Infrastructure (Figure 3-2).

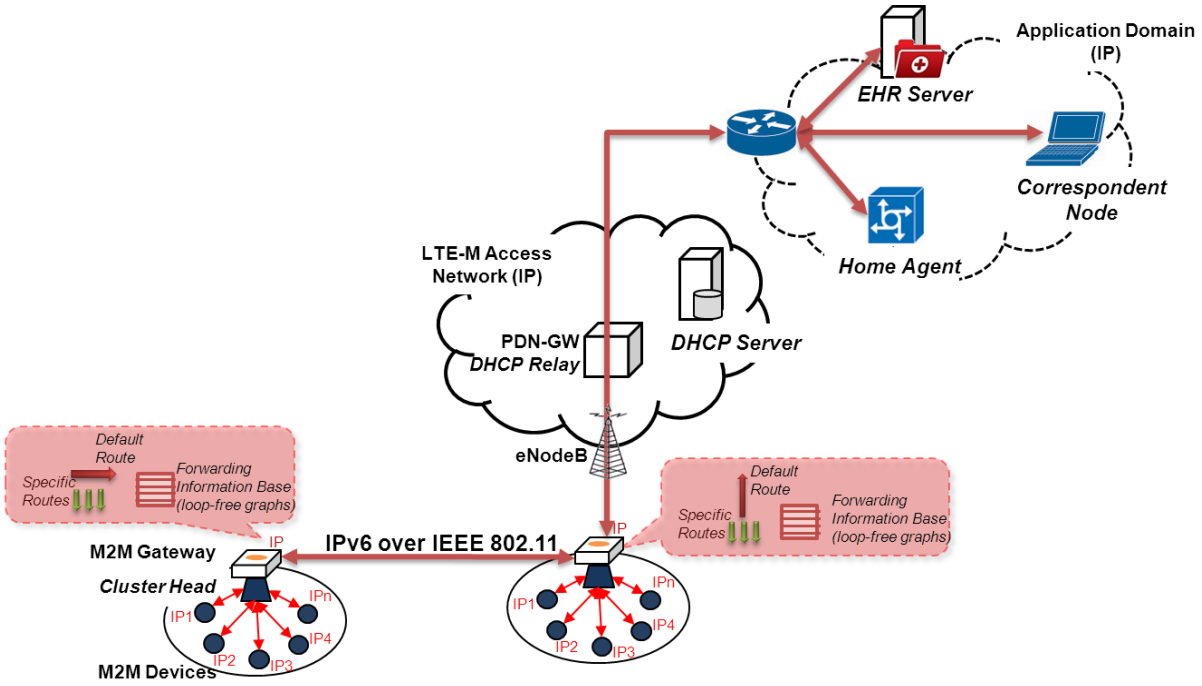


Figure 3-2: Overall architecture of subtestbed 2.1

By enabling an extended capillary setting, subtestbed 2.1 reflects early stages of EXALTED solutions deployment. Basically, the deployment of LTE-M base-stations, relays and radio chipsets for M2M Gateways will not be immediate. During this deployment phase, unstable by definition, an M2M gateway may be disconnected from the infrastructure, may not be LTE-M enabled, or experience better QoS through neighbouring M2M gateway. On the other hand, a long-term picture for subtestbed 2.1 represents the gradual integration of other sorts of networks that are non-capillary wishing to access LTE-M services through a heterogeneous setting using a cheap unlicensed radio technology (typical ad-hoc IEEE 802.11 settings). The validation of the concept is done by assuming an Intelligent Transportation System context. The capillaries attached to a gateway represent a vehicular network attached to its Mobile Router, and the overall instance is illustrated in Figure 3-3.

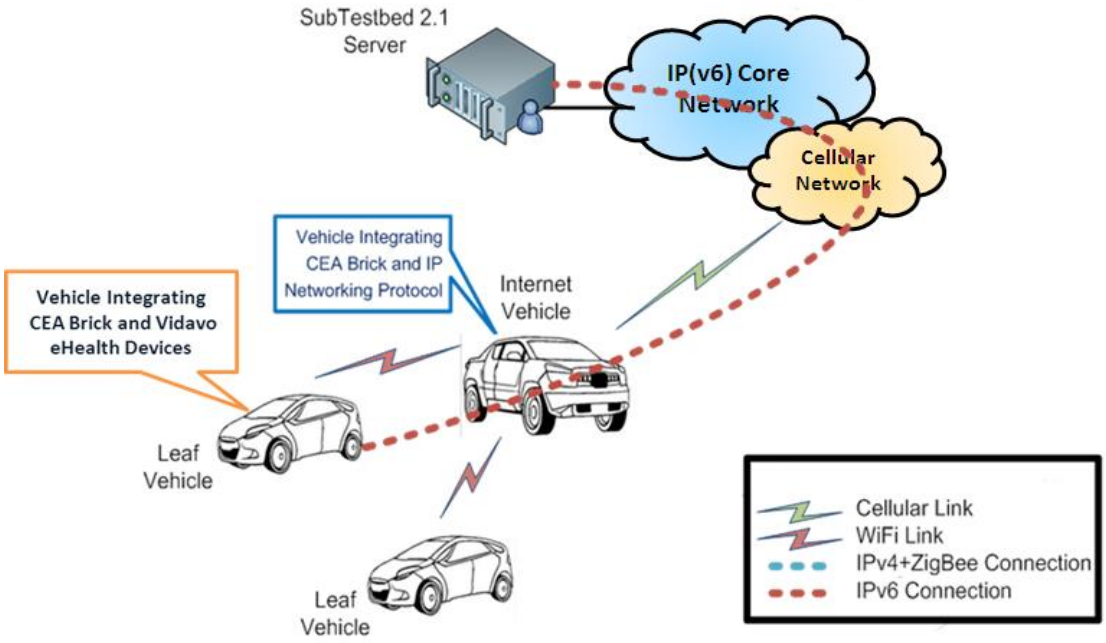


Figure 3-3: High level view of ITS and eHealth scenario

In summary, key features of this testbed are:

- **Scalability**, by addressing up to 65536 devices behind the M2M GW and on the other side by supporting the requests of neighbouring M2M gateways. Machines can be the in-vehicle embedded devices, or user-devices (eHealth). These addresses are bound to the GW and do not leak to the infrastructure, which enhances the scalability of the testbed.
- **Heterogeneity**, by supporting at least two types of wireless technologies. In particular, Cellular and IEEE 802.11.
- **E2E IPv6 Connectivity**, by supporting bi-directional communications. Server initiated communications must be possible.
- **Mobility**, vehicular networks being mobile, sessions continuity is an interesting feature to enable.

In order to demonstrate these features and to measure the efficiency of the proposed solutions, the following techniques are highlighted:

- **Vehicle Identification Number (VIN) based IPv6 addressing**
- **IPv6 prefix delegation over Neighbor Discovery Protocol (NDP)**
- **Network mobility support using MIPv6/NEMO**
- **Extended E2E connectivity scenario**
- **ITS and eHealth testbeds integration**

These techniques are in-line with the EXALTED objectives highlighted in Table 3-2 and bring the innovations summarized in Table 3-3.

Table 3-2: Requirements addressed

#	Functional requirement	Testbed 2.1
FU.1 **NF.1**	Support for large Number of devices Scalability.	Up to 2^{16} = 65536 devices theoretically

FU.3	Support for diverse M2M services.	Support for multiple applications.
NT.1	Heterogeneous networks	Multiple capillary interfaces
NT.2	LTE-M backward compatibility	Technologies compatible with early LTE releases
NT.4	Support of multi-hop communication	Multi-hop communications for M2M services
NT.6	End-to-end device to device communication	Two-way E2E communications
NT.8	Mobility management	Support session continuity

Table 3-3: Novelties and objectives

Algorithm	Novelties	EXALTED Objectives	KPIs
Address Translation	Generate Unique Local IPv6 Prefixes and Addresses out of a Vehicle Identification Number enhancing inter-capillaries communications	O4.5 Design an IP based E2E networking system for M2M communications.	K12. Throughput K20. Addresses mapped. K30. Payload size. K35. Energy per message.
Extended capillary-to-capillary-to-Infrastructure use case	Connecting a CAPILLARY network (instead of single terminals) with numerous attached devices (based on IPv6 and Heterogeneous radio technologies) to the Infrastructure more than one hop away	O4.2 V2V2I communications using VIN addressing, and Prefix delegation over Neighbor Discovery Protocol	
Integrated Vehicular-eHealth testbed	Integrated Vehicular-eHealth setting with Vidavo's eHealth technology	O4.2 V2V2I communications using Prefix delegation over NDP O4.5 Design an IP based E2E networking system for M2M communications.	

3.3.1 Verification Procedures

Figure 3-1 illustrates the overall picture of the evaluation testbed. In order to measure the actual performance parameters expected when using this setting, and understand the communication capabilities enabled by this testbed (especially in an ITS context), we propose to measure the following performance parameters.

- **K12. Throughput**. LTE-M specification is compatible with LTE release 8. In particular, standard 3GPP theoretical throughput is reduced to be relevant and cost-effective for M2M applications (about 1Kbits/s per device). This KPI determines the limits of the V2V2I system in terms of technical bottlenecks. In particular, we show that Capillary-to-Infrastructure model can be extended (with limited additional effort) to the pattern Capillary-to-Capillary-to-Infrastructure. This extension (hybridation) allows supporting an additional M2M capillary network through one LTE-M infrastructure connection, which tackles the issue of scalability, addressing and routing.

For this particular KPI, we propose to measure *separately* the case of inter-capillary communications (E2E communications from devices located *inside* neighbouring vehicles) which is mainly dependent on the IEEE 802.11 technology used, and the case of capillary-infrastructure communications (E2E communications from a device inside a vehicle to a server in the infrastructure) mainly dependent on the cellular technology used. In the remainder of this section, we refer to tests relative to inter-capillary communications by V2V communications. The experiments involving a single vehicle and infrastructure access is a V2I setting, whereas tests involving infrastructure access from a vehicle not directly connected is the V2V2I use case.

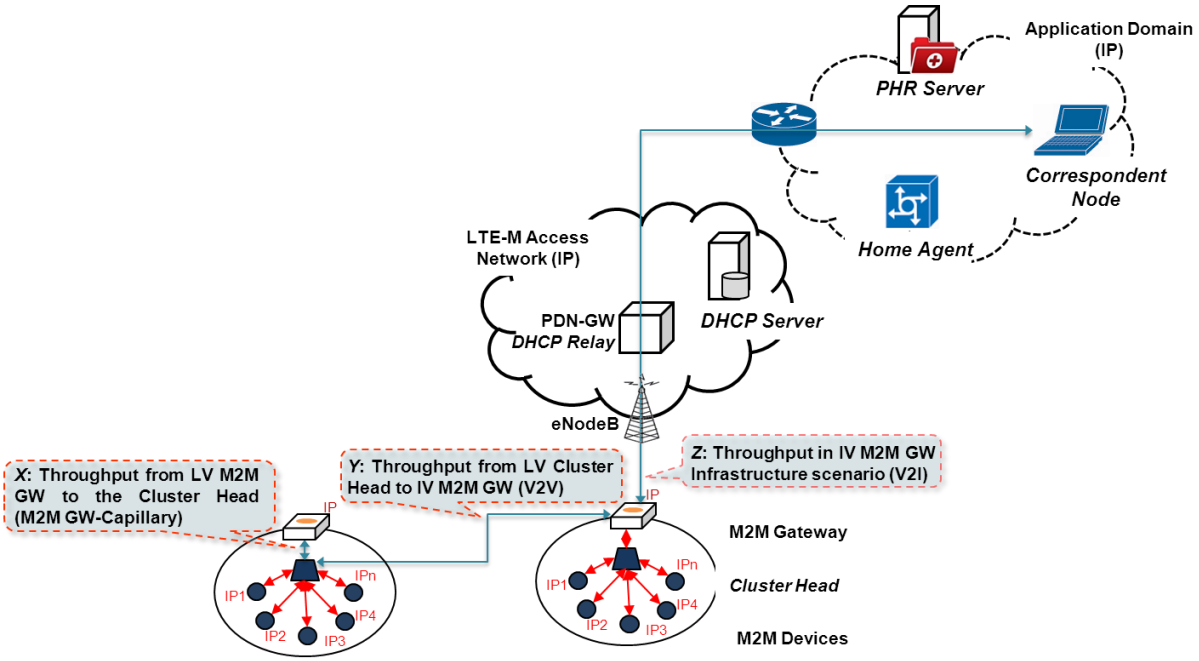


Figure 3-4: Determining the throughput of the extended capillary to infrastructure system and measuring the outcome for the direct capillary to infrastructure scenario

The evaluation of the throughput parameter not only gives a quantitative value of how the system should behave under experimental conditions, but also determines under which conditions the extended capillary-infrastructure (V2V2I) setting can be considered as equivalent to a single capillary-infrastructure (V2I) regarding this parameter. Basically, the choice of radio technologies and their respective bandwidth capabilities are discussed in order to conclude with an ideal setting for V2V2I that approaches V2I. Of course, IP version is irrelevant for K12 throughput measures.

Figure 3-4 shows how the K12 parameter for V2V2I breaks up the setting into three parameters to measure:

- ***X*** is the throughput measured between the LV M2M GW and the Cluster head of the same capillary network.
- ***Y*** is the throughput measured between the LV Cluster Head to the IV M2M GW.
- ***Z*** is the throughput measured between the IV M2M GW and the M2M Server in the Application Domain.

In a V2I setting the E2E throughput from the Cluster Head to the M2M Server is equivalent to (X+Z), and the same E2E throughput in a V2V2I setting is equivalent to (Y+Z). The two

previous assumptions are true **IFF** (X > Z) and (Y > Z) in the case of network heterogeneity involving cellular link. The K12 for this testbed is expected to demonstrate when this condition is true and under which circumstances the two previous assumptions are then true. If not, K12 will help determining the bottleneck that prevents V2V2I from achieving V2I throughput performances and how the overall system behaves in this case.

A second variable that has a great influence on the throughput and perceived QoS is the mobility. The case of vehicles encounter and departure, where a *short IPv6 communication opportunity* is created between two M2M GWs, is *not* considered for these evaluations as it is typical of the vehicular use cases (highly mobile) and not relevant for the mobility models considered for the capillary networks paradigm.

- **K20. Addresses mapped**. M2M Gateway and Devices addressing is a major issue of the M2M paradigm. This testbed sets IPv6 addresses and prefixes (and infer appropriate routing) by derivation of the Vehicle Identification Number, considered as an identifier for the capillary network embedded in the vehicle. VIN-based generated addresses should support the addressing of a total 2^16 (65536) distinct devices in the capillary network.

Using the IETF document Request for Comments (RFC) 4193 which defines the Unique IPv6 Local Unicast Addresses (ULA) enables each M2M GW to generate a set of global addresses and to use them for mapping up to 65536 capillary M2M devices inside a vehicle. Due to its infrastructure-less generation mode, the capillary is set with a stable networking configuration based on the unique identity of the vehicle.

This addresses generation mode involves a compressing mechanism based on numbering systems. The VIN-based numbering system approach is compared to other numbering and conversion techniques.

- **K30. Payload size**. The efficiency of the control plane, and the overall overhead generated using the subtestbed 2.1 proposals is evaluated. In particular, the NDP extension Prefix Delegation (ND-PD) [8] is compared to the Dynamic Host Configuration Protocol for IPv6 – Prefix Delegation (DHCPv6-PD) extension, which is specified as the next IPv6 prefix delegation standard for LTE-R8.

In particular, the number of messages generated through both control planes is compared and a summary table compares the advantages and the limits of using each approach.

- **K35. Energy per message**. This measure is relevant for the eHealth scenario extension of our V2V2I setting. A rough estimate of the energy spent on sending a message from an eHealth end device through the Android Cluster Head is measured.

3.3.2 Performance Measures

This section encloses the results of the performance indicators described in section 1.1 and identifies the communication capabilities enabled by this setting.

- **K12. Throughput**. LTE-R8 specification provides a theoretical throughput of up to 100Mb/s in the Downlink and 50Mb/s in the Uplink. The throughput is a minor requirement for M2M applications though (which consumes a limited size of data). LTE-M architecture is built to monitor a high number of devices (up to 65536 devices in theory). Subtestbed 2.1 provides an additional milestone towards extending this limit by enabling a V2V2I architecture that doubles the number of supported devices with one M2M GW connected to the infrastructure without increasing the data throughput.

For K12 experiments**,** E2E throughput is measured through 3 parameters described in section 1.1: X, Y, and Z. The experiments performed for this KPI determine the highest limit that can reach subtestbed 2.1 with respect to throughput. The settings considered are thus not those of an LTE-M network. We show that using our system in an LTE-M setting is possible and could benefit the architecture by supporting a larger number of devices, using cheap AdHoc setting and demonstrate the scalability feature by supporting 2 capillary networks through one LTE-M connection.

Parameter X is measured from the CH to LV M2M GW using ***iperf*** [9]. Figure 3-5 summarizes the results of this measure and shows stable overall throughput (around 2 Mbytes/s = 16 Mbits/s) when the CH is connected to the M2M GW using 802.11bg AP. From the LV M2M GW perspective, M2M GW received for X a total of 123 MBytes over a period of 60.3 seconds which sets the throughput to 17.1 Mbits/sec (that is an average of 2.125Mbytes/s).

Figure 3-5: Throughput X: Throughput measured between the Cluster Head and the LV M2M GW using IEEE 802.11 WiFi Link

Parameter Y is measured between the CH and the IV M2M GW and summarized in Figure 3-6. Figure (A) pictures the throughput of a fast Ethernet link used between gateways and between LV M2M GW and the CH. This is to approach the theoretical conditions of LTE-R8 using MIMO regarding CH access to the Application Domain. The overall stable throughput (around 11 Mbytes/s = 88 Mbits/s) pictured in (A) represents actually the throughput of a V2I setting; that is if the LV CH is actually in the IV. From the IV M2M GW perspective, for parameter Y a total of 664 MBytes is received over 60.1 seconds, which sets the throughput to 92.6 Mbits/s (that is an average of 11.575Mbytes/s).

Figure (B) represents the measures of Y using ad-hoc WiFi link between the M2M GWs. This is a more realistic scenario of deployment and shows (with no surprise) that throughput limit is far from the LTE-R8 standards (an average of 2 Mbytes/s = 16 Mbits/s). From The MR-IV perspective, for parameter Y a total of 122 MBytes is received over 60.7 seconds, which sets the throughput to 16.8 Mbits/sec (that is an average of 2.1 Mbytes/s). Please note that these

measurements demonstrate the limits of V2V2I settings and shows that these limits are irrelevant using LTE-M.

This difference between both technologies sets the limit of the V2V2I setting regarding the throughput parameter; that is the ad-hoc link between vehicles represents a bottleneck for the throughput. Formally, the assumption (X+Z ≈ Y+Z) is no longer valid *if LTE-R8 is used for X*, as the condition of fair heterogeneity ((X > Z) and (Y > Z)) is no longer verified when Z approaches 100Mbits/s. Nonetheless, this limit regarding throughput is a performance bottleneck only if the application running on the CH requests a throughput greater than Y (around 16 Mbits/s). That is, for capillary networks considered in EXALTED, and which run applications requiring an estimated throughput of 10Kbits/s (sensors and actuators) *there is no performance bottleneck perceived at the lower level*.

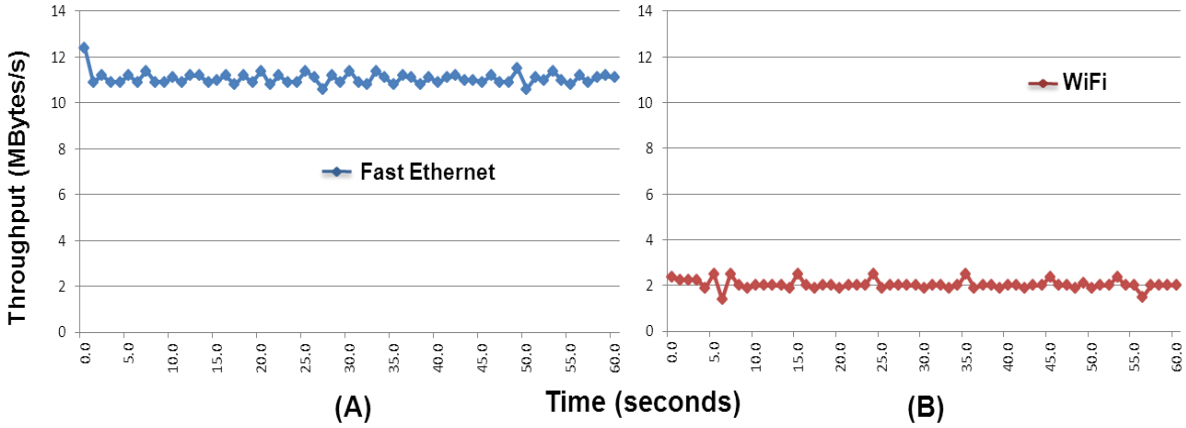


Figure 3-6: Throughput Y: Throughput measured between the Cluster Head and the IV M2M GW. (A) Fully Fast-Ethernet (100MB/s) wired setting to approach the theoritical limit of LTE-R8 with MIMO. (B) Ad-Hoc link between IV and LV M2M GWs to demonstrate the experimen

For the vehicular specific use case the 802.11p specification helps overcoming this 16 Mbits/s barrier on the ad-hoc link as it specializes in the vehicular-only settings. This standard will help integrating a larger set of applications for the V2V2I settings in the future.

Parameter Z measures the throughput for the 3G High Speed Uplink Packet Access (HSUPA) (LTE-R6) Infrastructure link in two conditions: Enterprise public IPv4 Access Point Name (APN) connection and an Experimental IPv6 APN. Of course, IP version does not determine the obtained throughput but the quality of the cellular link does. Parameter Z also verifies that for an LTE-R6 deployment, the V2V2I and the V2I are regarded as the same from the K12 perspective by verifying the conditions previously stated.

Figure 3-7 (A) shows a variable throughput measure using a public Enterprise IPv4 APN. From the server perspective, the throughput measure for Z generated a total of 15.6 MBytes received over a period of 64.1 seconds which sets the throughput to 2.04 Mbits/sec (that is an average of 0.255 Mbytes/s).

Figure 3-7 (B) shows the same KPI measured over an experimental IPv6 APN specially deployed for V2V2I experiments. From the server perspective, a total amount of 17.4 MBytes data over 60.6 seconds is received, which sets the throughput to 2.40 Mbits/sec (that is an average of 0.3 Mbytes/s). This highlights the performances of this experimental APN which are equivalent to those of a public IPv4 APN regarding throughput. Of course, this experiment is not affected by the IP version running on top of the cellular link.

The experimental IPv6 APN on the other hand, allows demonstrating the V2V2I concept of the subtestbed 2.1 that uses IPv6 for Addresses Mapping without using an IP version agnostic protocol on the IV M2M GW or another IPv4-IPv6 translation box.

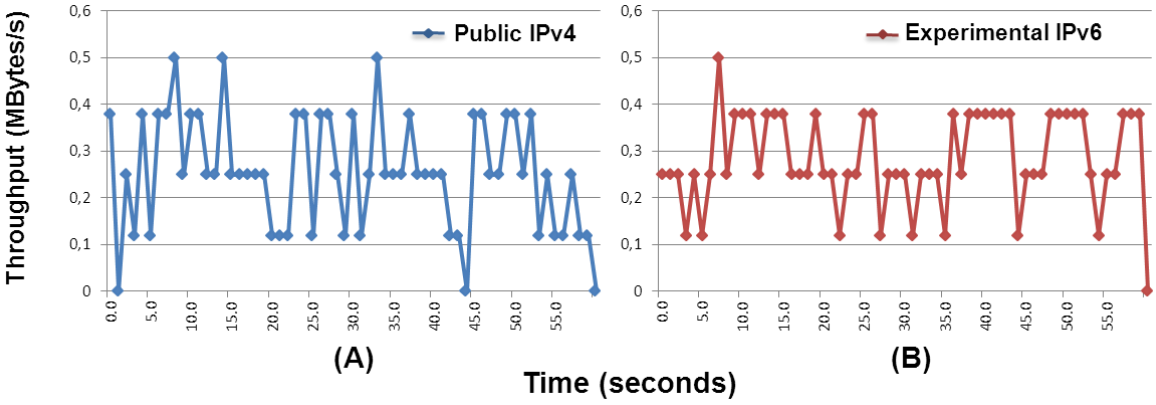


Figure 3-7: Delay Z: Throughput measured between the IV M2M GW connected to the 3G+ Link (HSDPA, LTE-R6) and a Server in the Application Domain. (A) Entreprise IPv4 3G APN. (B) Experimental IPv6 3G APN

The K12 for subtestbed 2.1 demonstrates the limitations of V2V2I settings; that is, when extending the capillary network by cheap IEEE 802.11 connectivity between M2M GWs, what could be a bottleneck in LTE-R8, is no longer the case in LTE-M. This architecture that combines two capillary networks to the infrastructure through one LTE-M enable GW allows easier deployment scenarios, and greater scalability.

- **K20. Addresses mapped**. Figure 3-8 summarizes the algorithm of VIN conversion into VIN-based ULA prefix (VULA), IPv6 interface identifier (VIID), and Mobile node identifier (MNID). In particular, the resulting VULA prefix is 59 bits long and the VIID is 53 bits long. Taking into account the 128 bits of the IPv6 address divided into two 64 bits parts, the VULA gives up to 2^5 (32) different sub-prefixes and the VIID may be used by up to 2^11 (2048) devices per sub-prefix. This is if both components are combined. The use of VULA with Extended Unique Identifier 64 (EUI64) (up to 32 devices addressed), or the use of another type of prefixes with VIID (up to 2048 devices addressed) is possible.

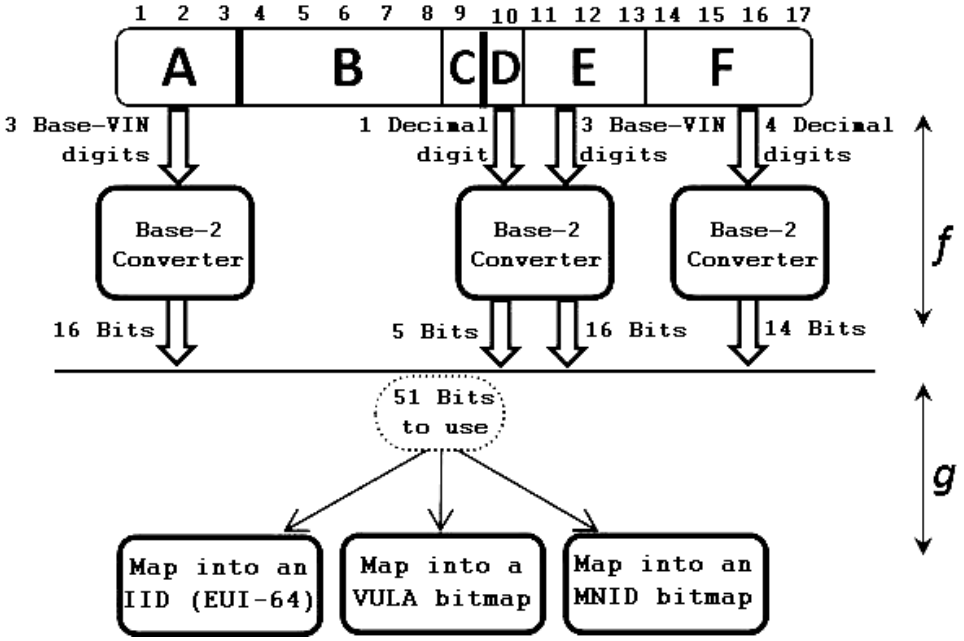
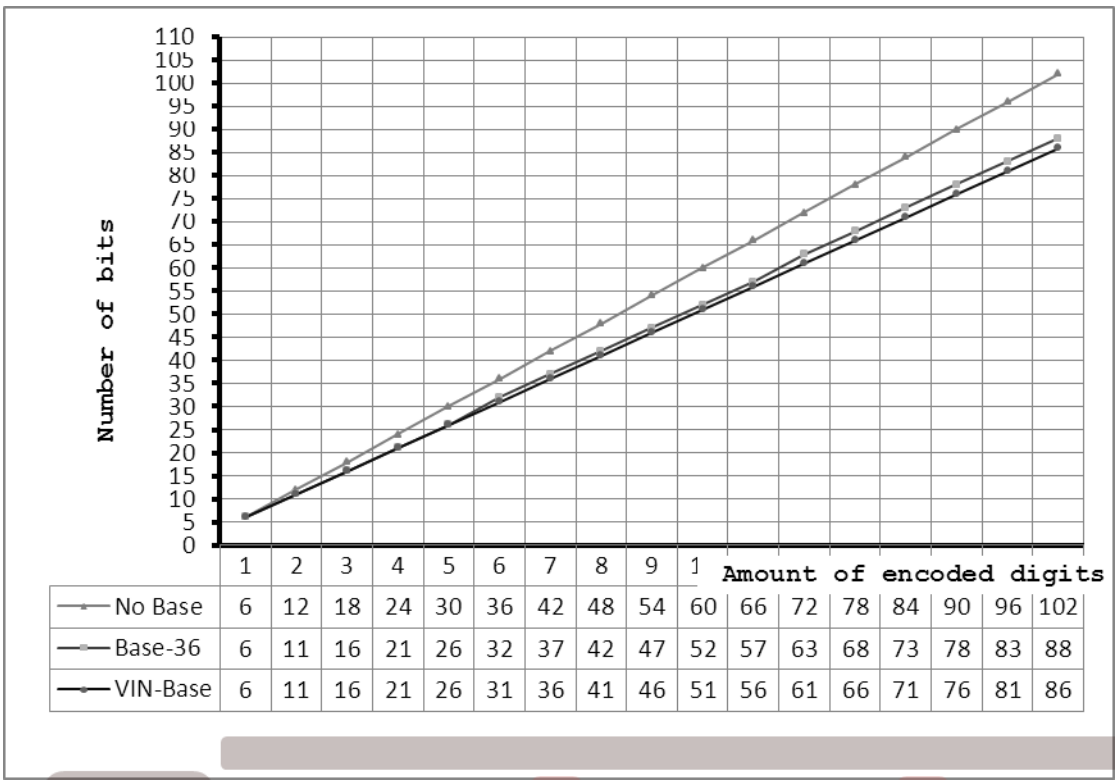


Figure 3-8: VIN to IPv6 networking objects conversion method summary

The number of addresses mapped out of a VIN number is not the only evaluation criteria for the proposed algorithm. VIN uniqueness property conservation is another important characteristic obtained from proposed derivation method, and essential for the IPv6 generated prefixes and addresses to be unique and routable with no ambiguity. Figure 3-9 shows the bit compression gain when using the proposed conversion method. This compression gain (16 bits) allows enclosing (map) up to 65536 devices behind one GW.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
No Base	6	12	18	24	30	36	42	48	54	60	66	72	78	84	90	96	102
Base-36	6	11	16	21	26	32	37	42	47	52	57	63	68	73	78	83	88
VIN-Base	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86

Figure 3-9: Compression bit gain. The use of no particular base system, the use of base 36 and base VIN is compared when converting a VIN into a prefix or interface ID

- **K30. Payload size**. One major motivation for ND-PD extension over DHCPv6-PD is ETSI TS 102 636-6-1 recommendation for not using stateful address configuration mechanisms (namely DHCPv6) in a vehicular scenario (due to important latency) and also not to use manual address configuration [10]. As a reminder, prefix delegation is essential for the deployment of IPv6 protocol which relies on globally-scoped prefixes for routing and addressing, and prevents the use of Network Address Translation boxes [11].

ND-PD proposal runs on the ad-hoc link between two M2M GWs. For the LTE-M enabled M2M GW (IV), it is then possible to hold a pool of IPv6 global prefixes to delegate in case a moving M2M GW (not LTE-M enabled, LV) requests it for IPv6 configuration in order to access the service/application domain, and this upon ideal encounter conditions (stable ad-hoc radio link). To stick with DHCPv6-PD RFC 3633 notations, the IV is the delegating router and the LV is the requesting router.

Table 3-4 summarizes the pros and cons of using ND-PD over the LTE-R8's DHCPv6-PD for IPv6 prefix delegation. The comparison focuses on important and time-consuming features.

Table 3-4: Features comparison of DHCPv6-PD and ND-PD

#	DHCPv6-PD	ND-PD
Min Nb of messages	2 messages when using DHCPv6 rapid commit (subject to unused assigned IPv6 addresses problem)	2 messages (options included in regular RS/RA NDP messages)
Max Nb of messages	4 messages when using "regular" DHCPv6 exchange (Discovery phase and delegation part)	2 messages (options in regular RS/RA NDP messages)
Latency	Higher due to number of messages and execution time	Slower due to local prefixes pool and short advertisements delays
Availability	Not default in IPv6 stack, additional program should be installed	NDP is default in any IPv6 stack implementation. Must be augmented with ND-PD extension
State maintenance	Stateful. Delegating and Requesting routers must keep track of configuration state.	Stateful in the current state of specification (work in progress). Requesting router must conserve a state of the prefix that it has been delegated.
Standardization point	RFC 3633 (regular), RFC 6276 (with MIPv6/NEMO)	Work in progress (Draft) at initial state

- **K35. Energy per message**. For the extended vehicular use case, involving the eHealth scenario, the energy spent on sending a message from an eHealth end device through the Android Cluster Head is measured. K35 within EXALTED is a strong requirement for M2M Devices, as M2M GW is in many cases (including ITS scenario) considered to have unlimited energy resources. For instance, some vehicular scenarios consider that GWs are plugged into a secondary battery (not the main that serves the engine) that is recharged when the vehicle's engine is running.

Using the Vida24 application on the Android phone (cluster head) results on average smartphone energy consumption at minimum usage of 5% phone battery energy consumed per hour. The eHealth end device (Oxymeter for subtestbed 2.1) on the other hand, will consume 60mW in a typical operating mode (off the shelf, manufacturer default configuration).

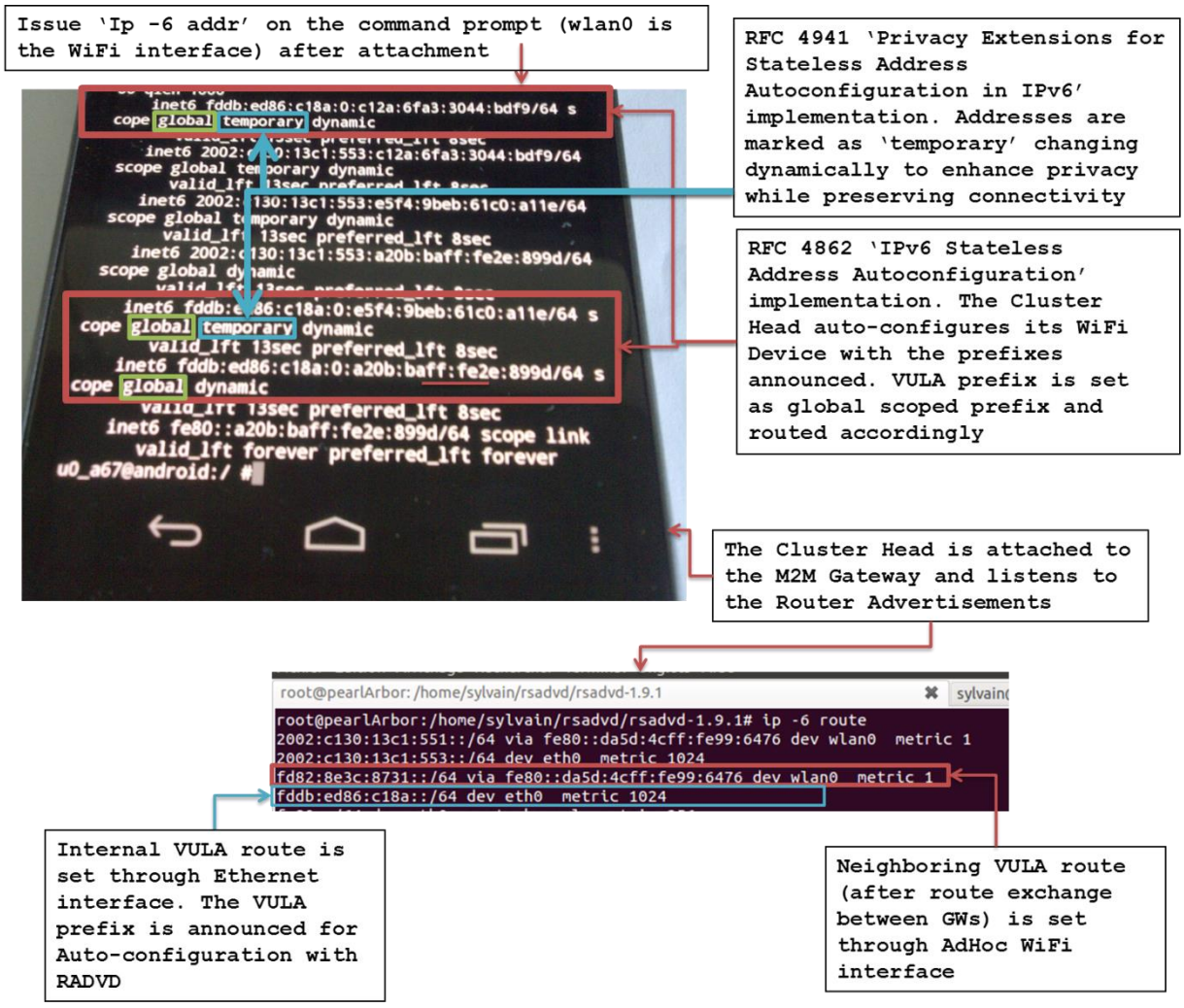


Figure 3-10: Details of K35 ITS-eHealth setting. Cluster Head (off-the-shelf Android phone) with standard IPv6 protocol stack auto-configures global routable addresses behind its gateway. Temporary addresses RFC 4941-compliant (privacy concerns)

3.3.3 Wrap Up

Subtestbed 2.1 demonstrates the feasibility of capillary-to-capillary-to-Infrastructure IP communications and uses an eHealth application as a proof of concept. The architecture is connected through an IPv6 networking technology involving two neighbouring M2M gateways where only one is connected to the infrastructure. The leaf M2M Gateway relies on its neighbour for accessing the M2M services provided by the M2M application domain.

The extended capillary setting reflects early stages of EXALTED solutions deployment during which an M2M gateway may be disconnected from the infrastructure, may not be LTE-M enabled, or experience better QoS through neighbouring M2M gateway. On the long-term, this setting should enable gradual integration of other sorts of machine-type networks and allow them accessing LTE-M services through a heterogeneous ad-hoc radio access.

In summary, key features of this testbed are:

• **Scalability**, by addressing up to 65536 devices and on the other side by supporting the requests of neighbouring M2M gateways. This is achieved using VIN-based IPv6 addressing and IPv6 prefix delegation over Neighbor Discovery Protocol, which allows us to double the number of supported devices.
• **Heterogeneity**, by supporting at least two types of wireless technologies. This is achieved by setting an Extended E2E connectivity scenario which *behaves similarly* to a single Capillary-Infrastructure setting *regarding the throughput aspect*
• **E2E IPv6 Connectivity**, by supporting bi-directional communications. Server initiated communications are also possible by using Mobile Network Prefix (MNP) through MIPv6/NEMO and Prefix Delegation to obtain globally-scoped communications. The PoC is done through ITS and eHealth testbeds integration
• **Mobility**, vehicular networks being mobile, sessions continuity is an interesting feature to enable performed with the use Network mobility support using MIPv6/NEMO that *accepts* to anchor the neighbouring LV prefix after its delegation by the IV.

Table 3-5: Summary of subtesbed 2.1

Scenarios	Technical Requirements addressed	Qualitative Assessment	Quantitative Assessment	Measurable KPIs	KPIs assessment & Contribution to key objective
Connectivity	**FU.1 and NF.1**	Support for large Number of devices Scalability	Up to 2^16 = 65536 devices	K12. Throughput K20. Addresses mapped. K30. Payload size. K35. Energy per message.	Achieved through VIN-based mapping
	FU.3, NT.4 and NT.6	Support for diverse M2M services, Support of multi-hop communication, and End-to-end device to device communication	Support for multiple applications, Multi-hop communications for M2M services, and Two-way E2E communications		Achieved by enabling globally and site-scoped communications, enabling IPv6 addresses and routes generation with VIN, routing setting by routes exchange through NDP extension and Prefix Delegation
	NT.1	Heterogeneous networks	Multiple capillary interfaces		Support of devices connected to the M2M GW and capable of setting an IPv6 address
	NT.8	Mobility management	Support session continuity		Network mobility support using MIPv6/NEMO that *accepts* to anchor the neighbouring LV prefix after its delegation by the IV.

3.4 Sub-testbed 2.2: Heterogeneity and Interoperability

An intelligent M2M gateway component for LTE-M networks to support communications amongst M2M devices, high-level application and service layers is developed. The M2M gateway design and architecture in particular focus on three main aspects: connectivity of heterogeneous resources, data processing and optimization of access and resource usage for resource/power constrained devices, provisioning and interaction with network and service layers.

The planned architecture for the M2M gateway is in line with the testbed design and scenarios that were selected for the testbeds. The communication between the M2M gateway and capillary networks and intelligent decision making within the components will enable the EXALTED components to provide connectivity and interoperability for the underlying heterogeneous networks and at the same time optimize and manage resource access for constraint devices using context-aware and intelligent machine learning mechanisms.

The current M2M gateway software supports the integration of 802.15.4 enabled devices in the capillary network. The M2M gateway groups the nodes in the capillary network according to semantic context information, which corresponds to different QoS requirements, to reduce the communication overhead. Two main features are introduced, namely data dissemination and data aggregation. The data dissemination feature utilizes the semantic context information to distribute messages in the capillary network to the suited sensor nodes. The data aggregation feature aggregates data of nodes within a group for message-reduced data provision. The software runs on Advanced RISC Machine (ARM) and x86 devices and is ported for the Sagemcom On-Board Unit (OBU). The current data aggregation and approximation framework supports both TSTmotes as well as Sun SPOT units accessing the gateway.

The intelligent M2M gateway features the following features:

- **Adaptive Data Scaling**: is performed for different measurements via normalization amongst all streams before aggregation, as it is meaningless to compare time series with different offset and amplitudes as measured from real sensors.
- **Dimensionality Reduction:** this feature is carried over from the nature of conventional piecewise aggregate approximation (PAA), which represents data series in a greatly reduced representations
- **Numerousity Reduction:** by including only the anomaly data from the original time series, the computational complexity is significantly reduced, therefore fast aggregation is achievable.
- **Fast Aggregation:** as sensor node may capture data periodically, rather than wait for hundreds of data buffered before generating the first representation, the algorithm generates a pre-representation for the first few samples and revises where applicable.
- **Accuracy Preservation:** by taken into account key representative data from the original data series, the key information can be maximum preserved after the approximation process.
- **Faulty Detection & Recovery:** by monitoring the data from each sensor compared with historical statistics, the algorithm is able to detect faulty device reporting useless wrong data and remove those data from aggregation.

The main idea behind this work is the parallel development on data mining techniques and machine-to-machine communications, yet surprisingly lack of interactions in between. This work is to bridge the advanced machine learning technique to the machine-to-machine communications. As a matter of fact, the past decades have been witnessed hundreds of papers in representing time series data to discrete representation in a compact yet effective

manner, thus reduce the information to describe the real world tracking/monitoring events. This concept is more than favourite if can be applied to communication domain as the main benefits induced herein are not only less memory/computation cost but also significantly reduced transmission payload size and bandwidth in air interface required for communication hardware implementation.

As shown in Figure 3-11, the intelligent M2M gateway applies the newly proposed adaptive data aggregate algorithm for approximating M2M data, namely, Forecheck Aggregation Approximation (FAX), which includes the following main procedures:

- Weighted Fair Aggregation (WFA)
- Faulty Detection & Recovery (FDR)
- Similarity Avoidance approXimation (SAX)

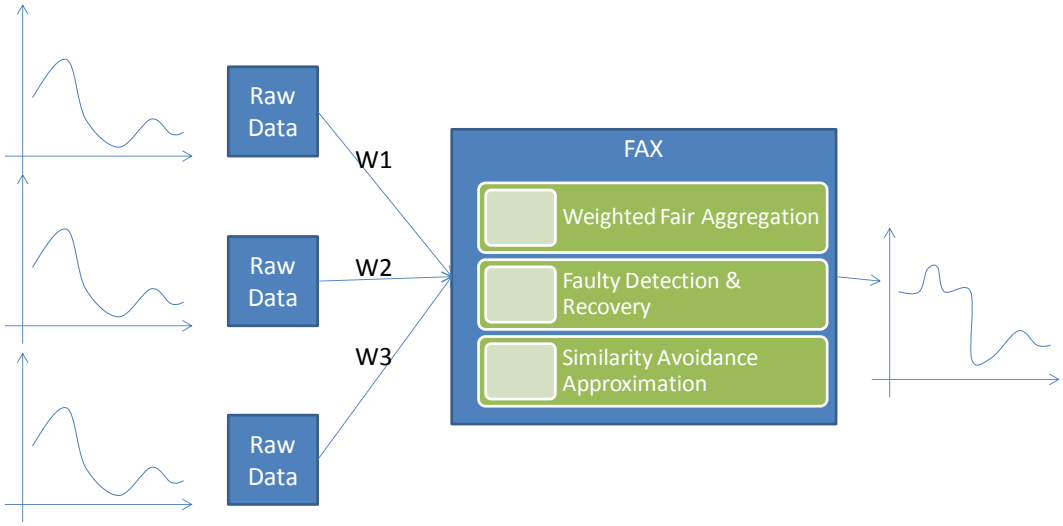


Figure 3-11: Forecheck Aggregation Approximation algorithm for approximating M2M data

In order to achieve these objectives, the following solutions developed in WP4 are demonstrated as listed in Table 3-6 and Table 3-7, namely Heterogeneous Connectivity, Weighted Fair Aggregation, Faulty Device Detection and Similarity Avoidance.

Table 3-6: Requirements addressed

#	Functional requirement	Testbed 2.2
FU.3	Support for diverse M2M services.	Support for multiple applications.
NT.1	Heterogeneous networks	Multiple capillary interfaces
NT.11	Traffic Aggregation	Support of data aggregation from multiple sensors
DV.6	M2M Gateway detection and registration	Self-configuration of capillary networks
NF.3	Extensibility and adaptability	Procedures exportable regardless underlying technologies
SV.3	Efficient provisioning of a set of M2M equipment	Procedures exportable regardless underlying technologies
NT.9	Reliable delivery of a message	Faulty Device detection

Table 3-7: Novelties and objectives

Algorithm	Novelties	EXALTED Objectives	KPIs
Weighted Fair Aggregation	Prioritized treatment on upstream data	**O4.4.** Traffic aggregation point architectures to support reduced traffic	**K30. Transmission**

		load	**Payload Size K32:Actual Payload Size**
Heterogeneous connectivity	Support for multiple access technologies.	O4.1 Maintaining connection/transmission through heterogeneous connections.	
Similarity Avoidance	Reduce the uplink data	O4.4. Traffic aggregation point architectures to support reduced traffic load	
Faulty Device Detection	Reliability	O4.6 Device/node monitoring mechanism to ensure authentic, reliable and secure response-to-demand datum.	

3.4.1.1 Weighted Fair Aggregation (WFA)

The first part of the work is data aggregation, which aggregates all upcoming data streams in to a single stream for future processing. To allow different streams to contribute in a fair share manner while maintaining the balance amongst competing interests. Streams are given proportional weight based on the predefined priority as well as traffic dynamics. Let's define Aggregated Data $\alpha(n)$ in the n^{th} time slot:

$$\alpha(n) = \sum_{m=1}^{M} \omega_m * \alpha_m(n)$$

where ω_m is set based on the predefined specific criteria for each sensor, reflecting the relative importance of the data reported from each sensor node, $\alpha_m(n)$ is the data reported from the m^{th} sensor node at the n^{th} time slot. M represents the total number of sensor nodes.

3.4.1.2 Faulty Device Detection (FDD)

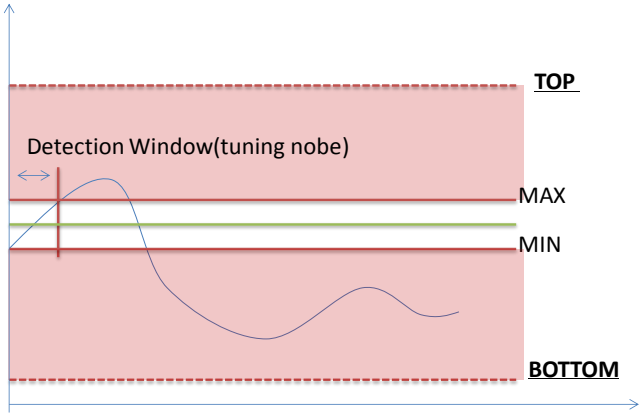


Figure 3-12: Faulty Device Detection for M2M data

Device fault is common and unexpected in sensor networks considering huge number of sensor nodes, therefore, data reported from all upcoming streams are not always correct data that to be aggregated and approximated. If the node becomes faulty in the middle of a transmission, the corresponding weight of the node will be automatically set to zero. This is implemented based on historical assessment of a measuring factor by defining a max and min reasonable value for the normal data range. For instance, if the reported data is out of the normal data range, the data reported from the sensor will be removed from the following aggregation algorithm and therefore improves the accuracy and removes the redundant data from the final approximation. In another case, once a sensor device is recovered from faulty

status and starts sending correct data again, the system is able to recover the status of this sensor after a very short detection time and automatically includes the subsequent reporting data from this sensor into the aggregation algorithm.

```
--------------------------------------------------------------------------------
|                        Data Extraction: # 19                                 |
--------------------------------------------------------------------------------
Data: 22.90
Faulty data detected!
Data:  22.90  is removed faulty sensor: 0013a200406ee064
Data from node 2:  0013a200406ee06408F2100702fdff -> 0013a200406ee064 22.90 41.03 2 253 255
None
Data buffered at OBU(e.g., Temperature):
-->Aggregating data from node 2: 22.9
tmpB_n1: [26.03, 25.06, 25.28, 25.25, 24.75, 26.05]
tmpB_n2: [23.07, 24.53, 24.6, 24.24, 23.16, 23.2, 22.9]
tmpB_n3: [25.52, 26.3, 25.5, 25.74, 24.87, 25.29]
tmpB: [23.07, 26.03, 25.52, 24.53, 25.06, 26.3, 24.6, 25.28, 25.5, 24.24, 25.25, 25.74, 23.16, 24.75, 24.87, 23.2, 26.05
, 25.29]

length: 18
--------------------------------------------------------------------------------
```

Figure 3-13: Faulty Device Detection for M2M data

Figure 3-13 shows an example of faulty data detection, for instance in this scenario, the 19th data in this buffering cycle is 22.90 degree which is reported from node 2 tmpB_n2, yet is detected as faulty data, as it is out of the normal range of 23.00-27.00, therefore the faulty data 22.90 is excluded from the aggregated data tmpB.

3.4.1.3 Faulty Auto-Recovery (FAR)

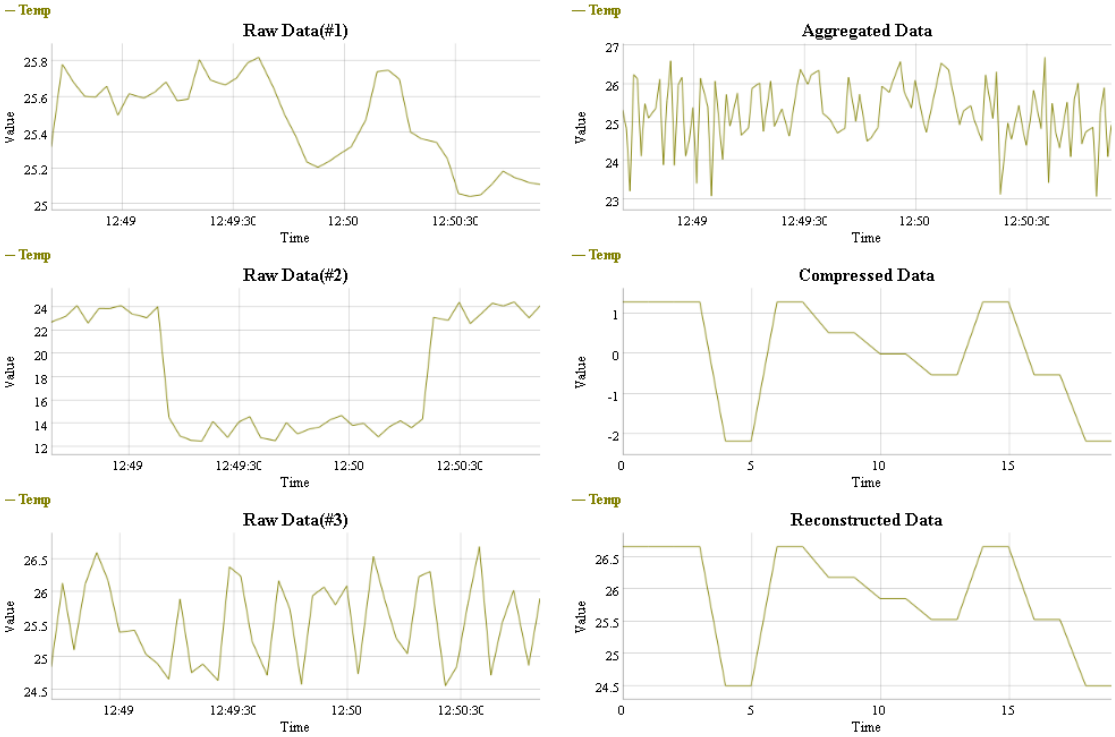


Figure 3-14: Example of M2M data faulty auto-recovery

As shown in Figure 3-14, by monitoring the data from the faulty sensors, the gateway is able to recover the data from faulty sensor as long as the data reporting is back to normal range. For instance in this scenario, based on the historical assessment, the normal data range for detecting temperature is in the range of 20-30 degree, once a faulty event has been detected from sensor #2, where its reported data is out of the normal range between 12:49:10-

12:50:20, during this period, the wrong data is therefore excluded from the aggregated data and compressed data as shown in the figure. Besides, it is also shown that once the sensor #2 is recovered back to normal working status after 12:50:20, the data reported from sensor #2 will be included in to the subsequent calculations of the aggregation algorithm.

3.4.1.4 Similarity Avoidance approximation (SAX)

In real M2M applications, data collected by M2M network is often presented as time-series continuous data with real float representation, where data mining technique can be utilized in this typical data streaming scenario. However, there are respective issues to be taken into account for this utilization. One of the key feature for data stream in M2M network is the value captured from sensors, e.g., temperature, humidity, illumination, etc, does not vary much for a relatively long period of time. For instance the room temperature in an hour can be with 1000 monitoring samples in a narrow data range of 22.00-22.50 degree. Therefore, most of the data can be with very similar value and therefore optimization is needed to remove the redundancy involved in the data similarity.

Piecewise aggregate approximation (PAA) is the classical scheme that is used for transforming the continuous time series value to discrete representations. It is one of the simplest approaches for time series data mining by the means of equal sized segments, thereby representing the series of data in reduced format. It is simple yet missing most of the important information regarding to the variance/dynamics in each segment and inefficient when applied to M2M applications where data value in a window can keep unchanged for a long period of time. Thus, it is reasonable to identify data which is least similar to the majority of other data in the window before the calculation.

To optimize this issue and save computational power for unnecessary similar data, UniS proposes a novel data aggregate algorithm, namely, Similarity Avoidance approXimation (SAX), which performs a fast check for the first few data of each window and thereafter discard the similar data in the remaining data series of the window, thereby the aggregation is only performed for key representative data in the window rather than all data. The algorithm keeps adjusting the sampling rate based on the data dynamics of the samples in each sub-window, i.e. the more similarity of the data the less sampling rate. As the sensor is hard coded with the sampling rate which may not be necessary for the application usage, the adaptive sampling rate adjustment at the gateway can reduce the unnecessary computational complexity. We evaluate the performance of the algorithm in extensive scenarios to show the performance trade-offs in between computational saving and imposed inaccuracy.

The SAX applies a small adjustable window, namely F (forecheck)-window (e.g. 5%-10% of the original data) to estimate the average and deviation of each sub-window, the algorithm features the following main benefits:

- Only key data outside the max-min is included in the aggregated data to preserve the most effective data whilst removing repeating similar data.
- Adaptively cope with data dynamics, more dynamics->more aggregated data
- Detection window can be adjusted based on the scenario, larger F-window ->less aggregated data
- The price is reduced accuracy, performance becomes worse in window with large deviation F-window
- Repetition can increase the accuracy of the algorithm
- Voluminous reduction, memory, energy efficiency, computational cost, fast regression
- The F-window can be adjusted as the following settings:
    - Predefined fixed value: e.g. 10 samples, or 10% of the Window

- Dynamic: derived for each window based on the previous statistics, e.g. bigger deviation or more outliers will give larger window.

- Higher F-window indicates less key data to be extracted.

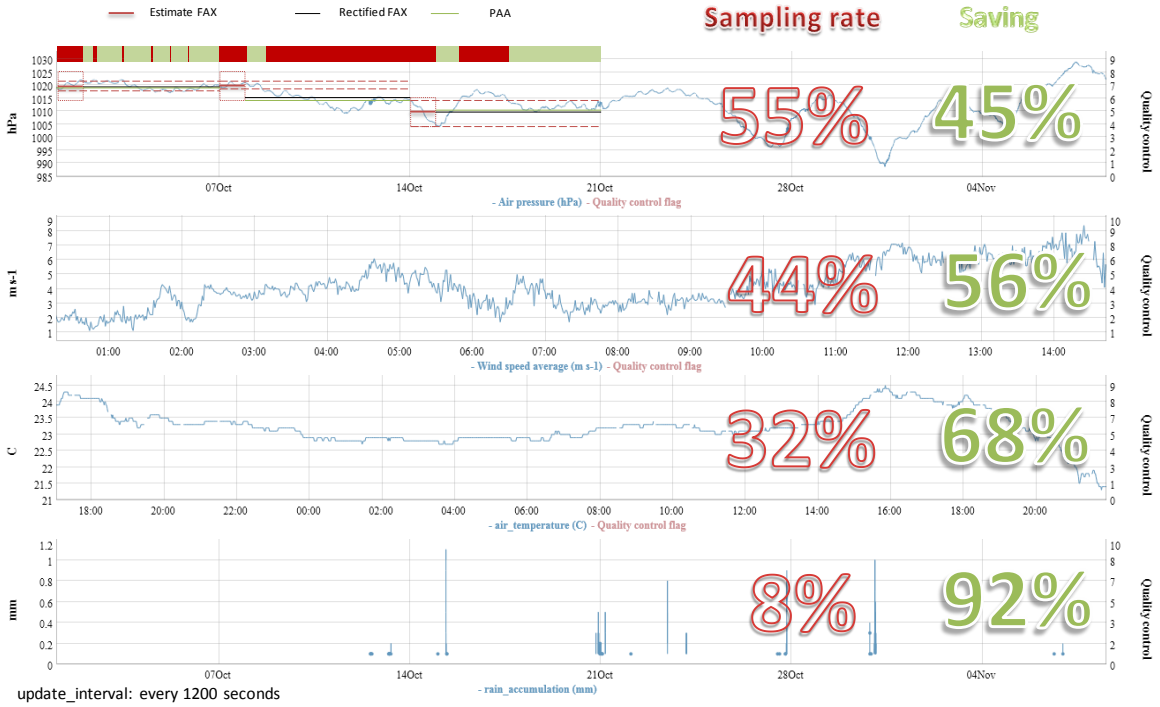


Figure 3-15: Redundancy saving by SAX in different MTC data patterns

Figure 3-15 addresses the performance in redundancy saving by SAX in different M2M data patterns. By using a small detection window to detect the potential similarity of the reporting data curve, the SAX is effectively adjusting the sampling rate of the aggregation algorithm, and is capable of reducing the redundancy in aggregation algorithm for a variation of MTC application scenarios. Numerically, it achieves the effective sampling rate of 55% and redundancy saving of 45% for the scenario of air pressure reporting, whilst achieves the effective sampling rate of 8% and redundancy saving as high as 92% for the scenario of rain accumulation data.

3.4.2 Performance Measures

Figure 3-16 captures the Web interface for UniS intelligent gateway: Scenario – Environment Monitoring. Multiple performance metrics are captured from the real sensors, e.g., temperature, humidity, accelerator-X/Y/Z. By using the weighted fair aggregation, the aggregated data keep tracking the effective data from the 3 real sensors based on the relative priority of data reported from each sensor. By adopting the SAX data approximation algorithm the real aggregated data are further approximated to a reduced format whilst preserves the required accuracy. By searching the look-up table, the server is capable of reconstructs data from the compressed form and therefore outcomes a series of representative data with great reduction on the transmission payload size.

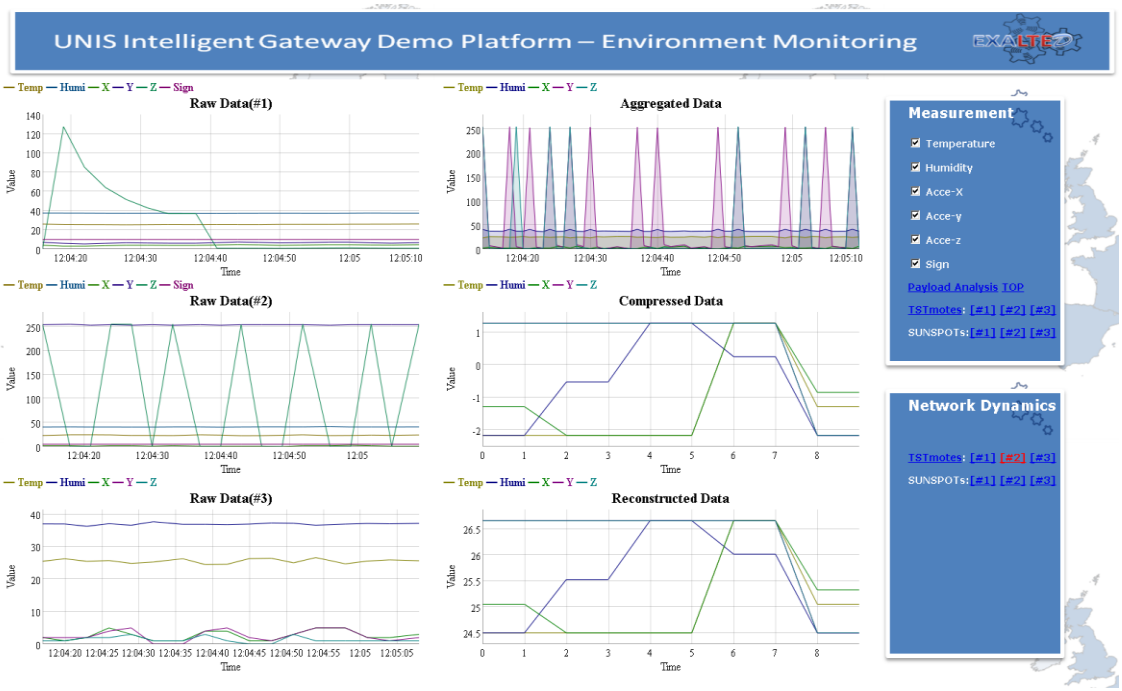


Figure 3-16: Demo Web Interface of the Intelligent Gateway – Environment Monitoring

```
Request Headers:
  REFERER: http://localhost:8080/sensorPage
  HOST: localhost:8080
  CONNECTION: keep-alive
  Remote-Addr: 127.0.0.1
  ACCEPT: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
  USER-AGENT: Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0
  ACCEPT-LANGUAGE: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
  ACCEPT-ENCODING: gzip, deflate
 1[27.0.0.1 - - [19/Feb/2013:12:08:31] "GET /data/sunsensor/7F2A HTTP/1.1" 500 1502 "http://localhost:8080/sensorPage" "
Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
19/Feb/2013:12:08:31] HTTP
Request Headers:
  REFERER: http://localhost:8080/sensorPage
  HOST: localhost:8080
  CONNECTION: keep-alive
  Remote-Addr: 127.0.0.1
  ACCEPT: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
  USER-AGENT: Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0
  ACCEPT-LANGUAGE: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
  ACCEPT-ENCODING: gzip, deflate
2013-02-19 12:08:31,24.24,40.99,2,254,255

->Raw_TST_n2>>>>>>>127.0.0.1 - - [19/Feb/2013:12:08:31] "GET /data/sunsensorsax/7F2A HTTP/1.1" 500 1508 "http://localhos
t:8080/sensorPage" "Mozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
 127.0.0.1 - - [19/Feb/2013:12:08:31] "GET /data/sunsensor/7F3A HTTP/1.1" 500 1502 "http://localhost:8080/sensorPage" "M
ozilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
2013-02-19 12:08:31,24.24,40.99,2,254,255,5

127.0.0.1 - - [19/Feb/2013:12:08:31] "GET /data/sunsensor/4706 HTTP/1.1" 500 1502 "http://localhost:8080/sensorPage" "Mo
zilla/5.0 (Windows NT 6.1; rv:18.0) Gecko/20100101 Firefox/18.0"
->Raw_TST>>>>>>> 2013-02-19 12:08:31,25.25,36.86,5,8,1

->Raw_TST_n1>>>>>>> 2013-02-19 12:08:31,25.25,36.86,5,8,1,10

->Raw_TST>>>>>>> 2013-02-19 12:08:31,25.74,37.11,5,4,2

->Raw_TST_n3>>>>>>> 2013-02-19 12:08:31,25.74,37.11,5,4,2

->Raw_TST>>>>>>> 2013-02-19 12:08:31,23.16,40.77,2,253,255

->Raw_TST_n2>>>>>>> 2013-02-19 12:08:31,23.16,40.77,2,253,255,5

->Raw_TST>>>>>>> 2013-02-19 12:08:31,24.75,37.09,6,9,1

->Raw_TST_n1>>>>>>> 2013-02-19 12:08:31,24.75,37.09,6,9,1,10
```

Figure 3-17 (a) Simulation instance of 1 buffering cycle for 50 sensor data from 3 sensor nodes at the server side

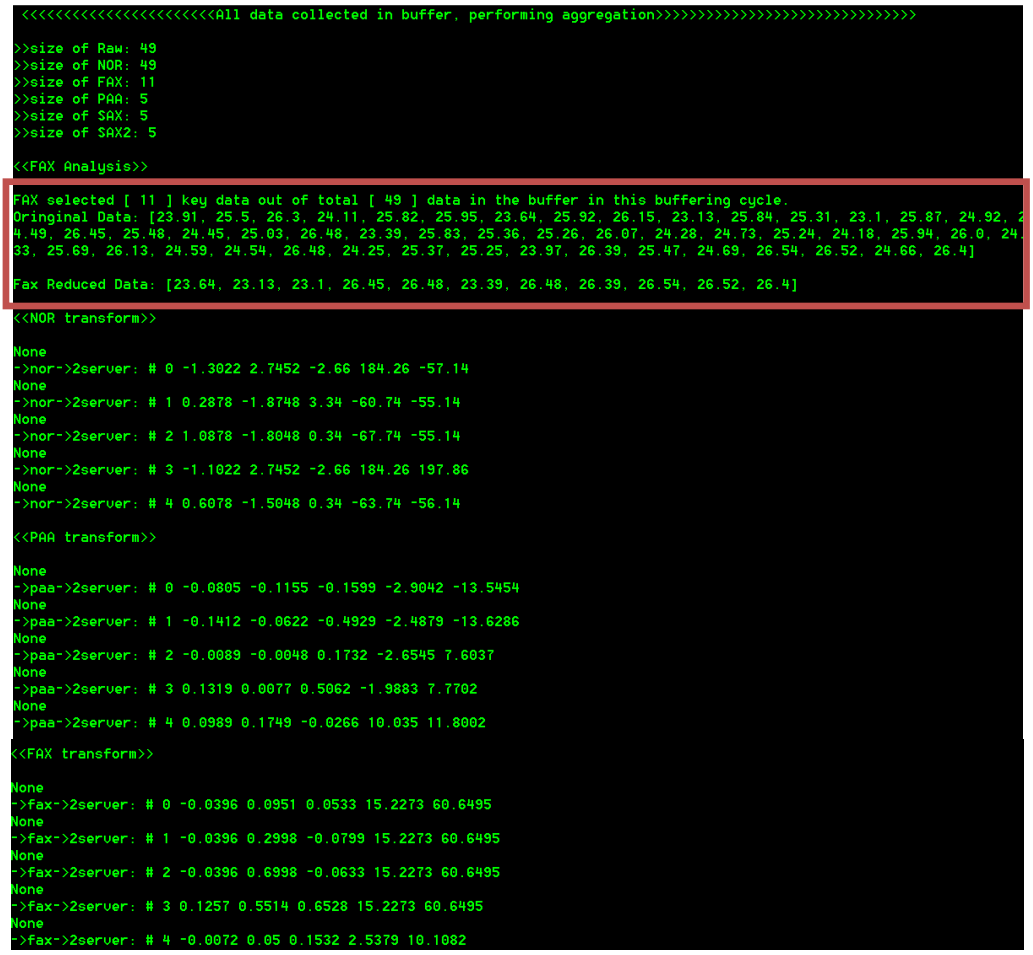


Figure 3-17: (b) Simulation instance of 1 buffering cycle for 50 sensor data from 3 sensor nodes at the client side

An example simulation instance is shown in Figure 3-17(a)-(b) capturing the simulation data for a representative scenario with a buffer cycle of 50 sensor data at the gateway from 3 sensor nodes. The effectiveness of similarity avoidance can be seen from the data as shown in Figure 3-17 (b), in this specific buffering cycle, the algorithm will only extract 11 key data from the original 50 data, whilst removing all similarly repeating data, increasing the efficiency and reducing the computational complexity of the aggregation and approximation algorithm. Figure 3-18 shows the performance of emulated environment monitoring scenario of 2000 samples in a period of around 5 minutes in a room. To test the faulty detection and recovery mechanism, we set one of the sensor, i.e., sensor 2, besides window, therefore its reported data is slightly lower than senor 1 and 3, at the range of 22-24 degree. It is viewable from the results in the aggregated and compressed data that, the final extracted data is slightly higher at the range of 24-26 degree during the period of 12:37:30-12:38:15, as we put the sensor outside the window in an environment of approximately 12-14 degree. After12:38:15, the sensor is collected back to the room, the aggregated data becomes lower as it automatically recovered the data in the range of 22-24 degree reported from the sensor 2.

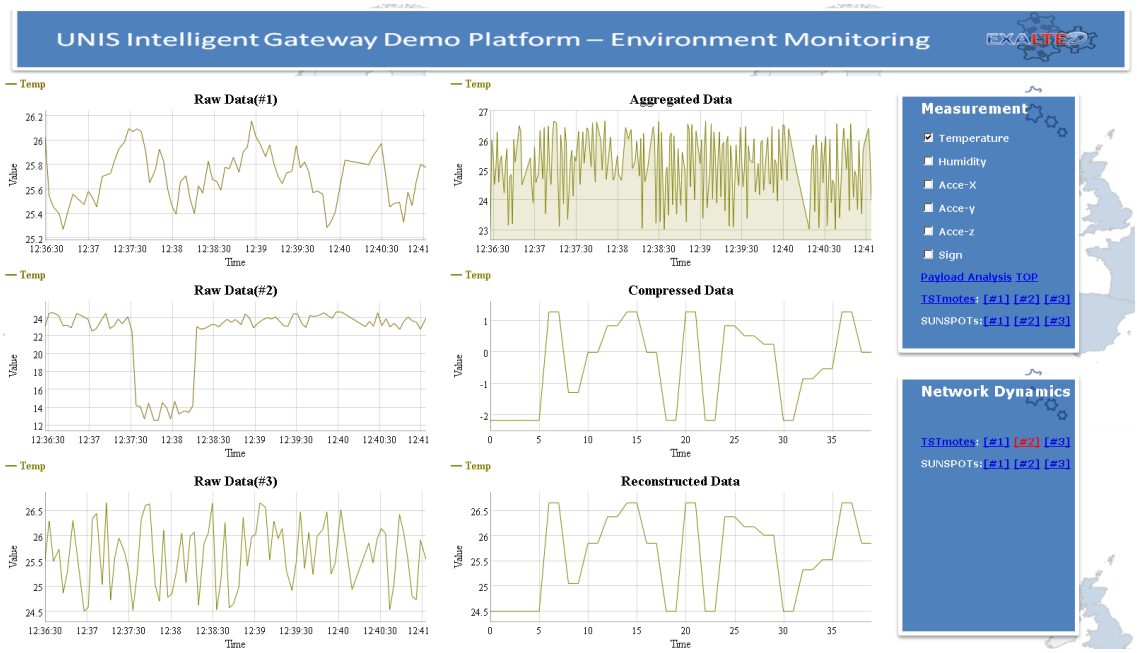


Figure 3-18: Performance for environment monitoring on temperature reporting

In order to evaluate the performance, the following measures have been also examined:

- **K30.Transmission Payload Size.** This is defined as the amount of data transmitted from the gateway to the LTE air interface.
- **K32: Actual Payload Size.** This is defined as the amount of data reported from the sensor to gateway.

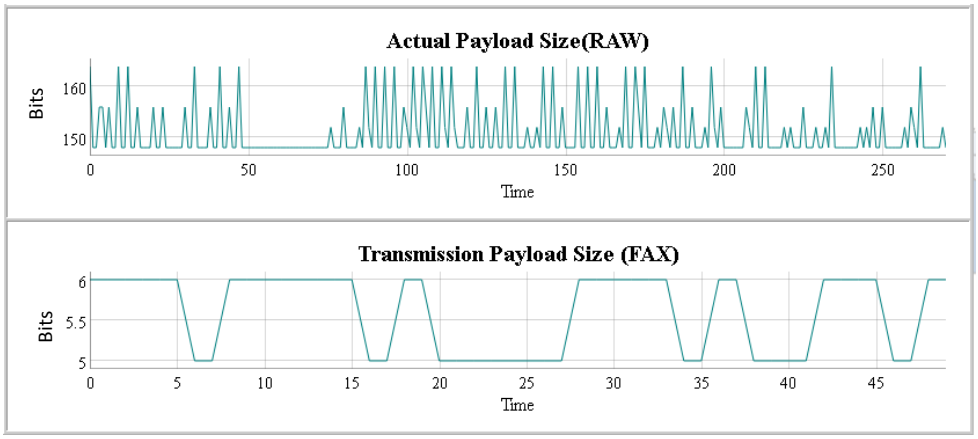


Figure 3-19: Performance evaluation on actual payload size and transmission payload size

Figure 3-19 shows the payload size comparison between the raw sensor data (actual payload size) and the aggregated data (transmission payload size), it is shown that for each 50 raw data in this example scenario, only 5 representative data are needed for transmission over the air interface, whilst the size of each representative symbol is greatly reduced due to the simplicity of the represented data. In this scenario, great reduction can be achievable in that, transmission payload size is around 3.75% of the original actual payload size. In summary, the gateway is able to achieve payload size reduction in the dimension of both time and amplitude.

3.4.3 Verification Procedures

In order to validate the performance of Transmission Payload Size and Actual Payload Size, the verification for the above measurements has been carried out by monitoring the data stream via specifically designed verification module. In the real scenarios, the data reported from each of the sensor nodes is consistently monitored and recorded for the data received by the M2M server and transmitted from the M2M server, therefore the verification procedure for transmission payload size is straightforward.

3.4.4 Wrap Up

New modules with novel features have been introduced in the intelligent gateway covering the following aspects: 1) data scaling, 2) data aggregation, 3) reliability, 4) transmission payload reduction. The whole framework has been revised and reconstructed, several new key algorithms have been proposed and implemented in the testbed, including adaptive data scaling, weighted fair aggregation, similarity avoidance approximation, and faulty detection and recovery. The revised framework is capable of handling the following typical treatment in M2M data aggregations:

- Adaptively adjusts different offset and amplitudes as measured from real sensors and scales them into a unified scale via performing normalization amongst all streams before data aggregation.
- Reduce the complexity in both dimensionality and numerosity, in that only key data are selected for data aggregation
- Provide reliability by intelligently detecting wrong data reported from faulty device and prevent those data from being considered in the aggregation algorithm.
- Preserves good accuracy level with significant complexity reduction and processing speed improvement.

Table 3-8: Summary of subtestbed 2.2

Scenarios	Technical Requirements addressed	Qualitative Assessment	Quantitative Assessment	Measurable KPIs	KPIs assessment & Contribution to key objective
	FU.3	Support for diverse M2M services.	Number of supported applications.	**K30. Transmission Payload Size** **K32: Actual Payload Size**	Enable diverse M2M services.
Heterogeneity and Interoperability	NT.1	Support different radio interfaces.	3 radio interfaces (NFC, ZigBee and GPRS) enabled.		Enable heterogeneity
	NT.11	Traffic Aggregation	Number of data streams		Enable the data aggregation
	DV.6	M2M Gateway detection and registration	Self-configuration of capillary networks		Support device detection and registration
	NF.3	Extensibility and	Procedures exportable		Extensible to other underlying technology

		adaptability	regardless underlying technologies		
	SV.3	Efficient provisioning of a set of M2M equipment	Procedures exportable regardless underlying technologies		Support multiple types of M2M devices
	NT.9	Reliable delivery of a message	Faulty Device detection		Faulty Device detection

3.5 Sub-testbed 2.3: Connectivity for low power devices

This subtestbed is called “Connectivity for low power devices”, and it is included into “E2E connectivity” testbed. It is oriented to SMM, but it could be applied to any M2M use case. The scenario covered is handling large number of constrained devices behind a gateway, so payload reduction and energy efficiency are critical parameters.

The main goal of this demo is to showcase the following items, so as to be compliant with the requirements presented on Table 3-9:

- **Scalability**, by being able to address up to 60.000 devices with just one Gateway.
- **Heterogeneity**, by using devices able to communicate using different radio technologies, as well as supporting several applications with the same hardware.
- **E2E IP Connectivity**, by establishing trusted end-to-end sessions from devices to M2M application servers.

In order to achieve these objectives, three solutions developed in WP4 are demonstrated, namely Address translation mechanism, Heterogeneous E2E connectivity and Lightweight monitoring, further explained in Table 3-9 and Table 3-10.

Table 3-9: Requirements addressed

#	Functional requirement	Testbed 2.3
FU.1 **NF.1**	Support for large Number of devices Scalability.	Up to 2^{16} devices theoretically
FU.3	Support for diverse M2M services.	Support for multiple applications.
NT.1	Heterogeneous networks	Multiple capillary interfaces

Table 3-10: Novelties and objectives

Algorithm	Novelties	EXALTED Objectives	KPIs
Address Translation	Support M2M non-IP devices as if they were IP enabled with the lowest overhead.	O4.1 Maintaining connection/transmission through heterogeneous connections. O4.5 Design an IP based E2E networking system for M2M communications.	K20. Addresses mapped. K30. Payload size. K35. Energy per message.
Heterogeneous	Support for multiple	O4.1 Maintaining	

E2E connectivity	access technologies.	connection/transmission through heterogeneous connections.	
Lightweight monitoring	Payload formats to enable energy efficient transmissions.	O4.6 Device/node monitoring mechanism to ensure authentic, reliable and secure response-to-demand datum.	

Main EXALTED objectives are showcased, and they have been all included into a real and commercial use case developed within the project. This demo is oriented to monitor hospital logistics, a real problem hospitals are facing. By taking advantage of EXALTED mechanisms, a ready to use technology is being implemented and tested right now on several hospitals in Spain. The problem addressed is that the stock of medicines is currently monitored manually, by dedicated personnel in charge of controlling huge panels of drawers containing medicines in each hospital department. There are as well some automatic approaches, but using non-scalable, fixed and big devices with high insulation costs. With the proposed system, medicines can be automatically monitored, saving costs and enabling just-in-time methodology when placing orders.

The principle consists of attaching an NFC tag to medicines. Whenever the medicine package is empty, it is put into a box containing an NFC reader. This box detects the medicine and transmits to a central server the information about that particular medicine becoming empty. This is emulated here by approaching the NFC tag to the boxes containing the M2M devices.

As it is very expensive to embed cellular modems at each place inside the same hospital where medicines must be monitored, it is needed as well to implement a way to grow the network using unlicensed capillary interfaces. This is achieved using ZigBee interfaces for those nodes connecting to a remote gateway with cellular capabilities. But the problem here is that these nodes are not natively IP enabled, and, in order to establish and E2E secure connection with the M2M server it is needed to talk IP. For that reason an address translation mechanism is developed and integrated on devices enabling up to 60.000 devices handles with the same gateway theoretically (the real implementation is limited by the cellular modem used). The principle for addressing them (selected after studying different approaches) consists on opening a socket for each device handled. The Gateway is in charge of monitoring and maintaining this link but without looking into the data sent, what enables security. The overall architecture of the proposed system can be seen in Figure 3-20.

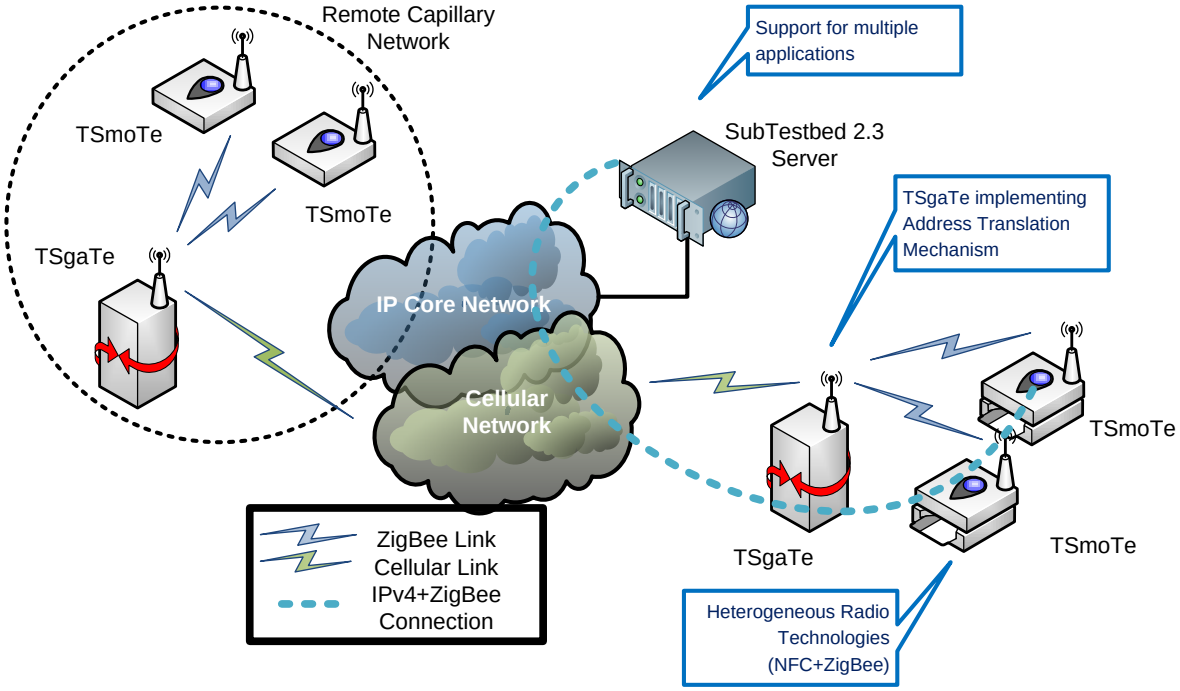


Figure 3-20: Subtestbed 2.3 architecture

Once the Gateway is authenticated at M2M server, it is possible to start the application. The gateway label will turn green detecting it is ready to be used, and it is possible to connect end devices and see them being attached at the server. Now we can test the logistics use case and communicate with nodes (see message chart in Figure 3-21)

- It is possible to approach NFC tags to nodes and see that the action is stored in the application and the node receives the confirmation that makes it flash the led.
- It is possible to send remote commands to nodes acting over the led colour and even kicking it out of the network if we detect malicious behaviours.

Other applications can also be run over the very same devices. For instance, some hospital departments need ambient parameter monitoring, such as temperature or humidity. A second remote network is set in this demo showcasing this feature. It is possible to act over these devices the same way as with the ones present here, and, in addition, it is possible to consult the data monitored and even see graphs of last data (as shown in Figure 3-22)

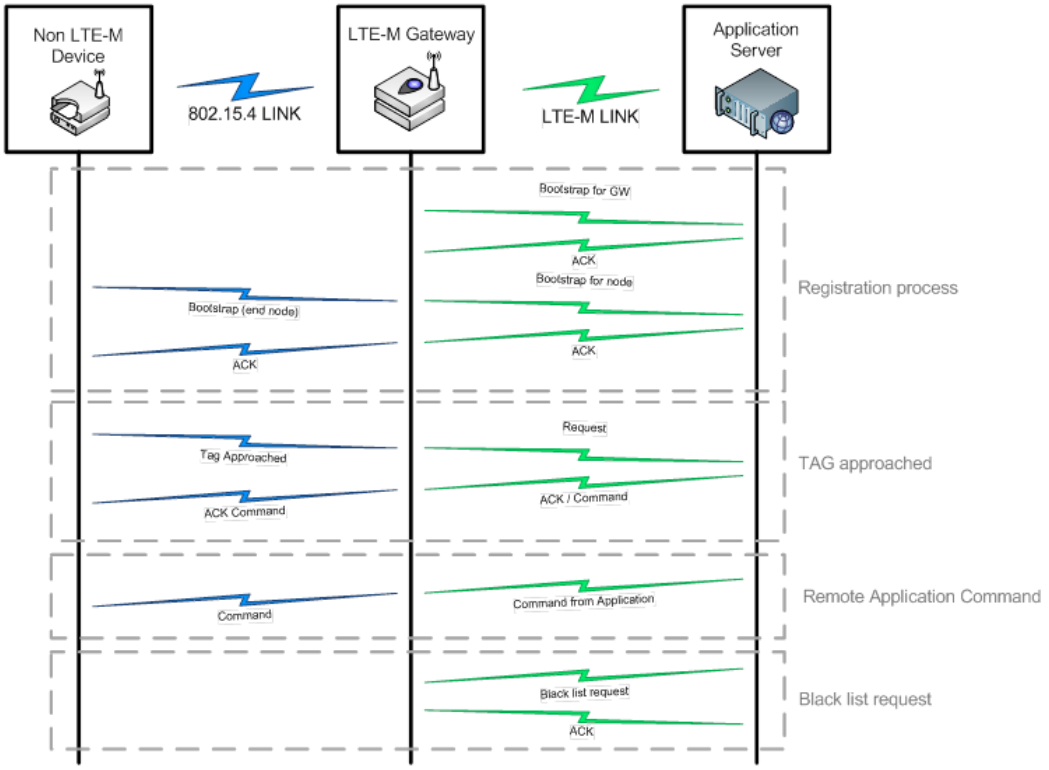


Figure 3-21: Message Sequence Chart

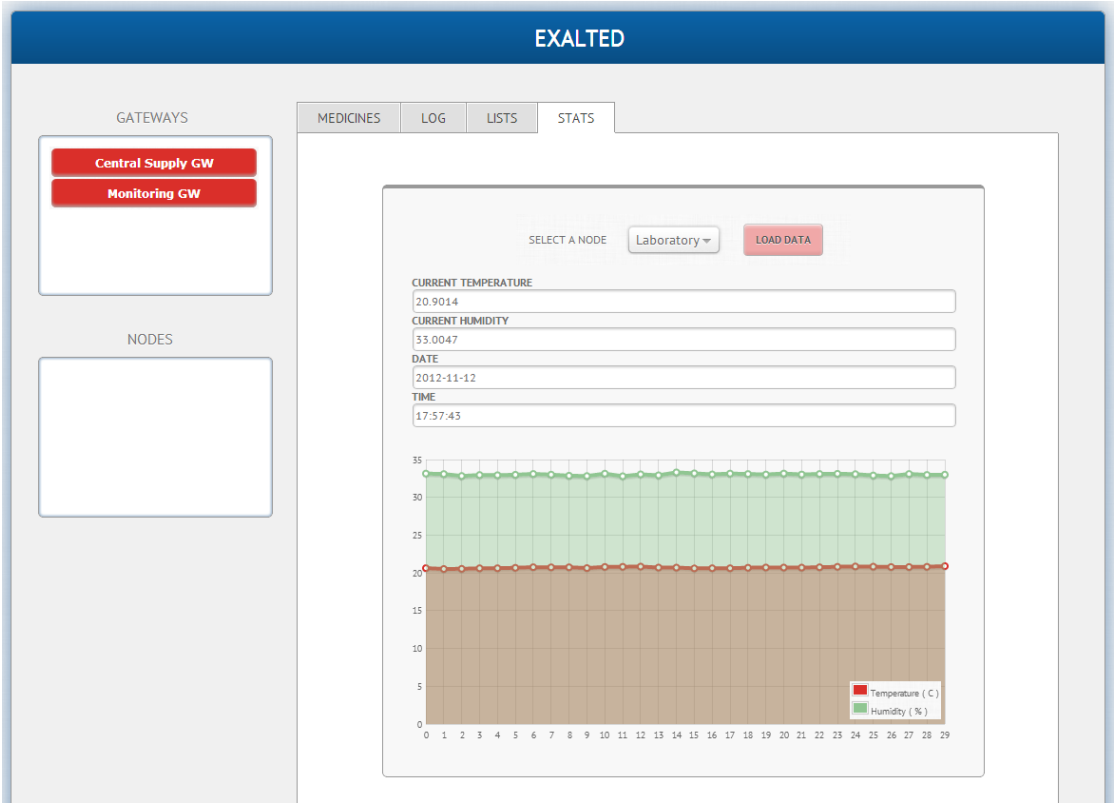


Figure 3-22: Capture of the web interface showing monitoring parameters

3.5.1 Performance Measures

In order to evaluate this testbed, as described in Figure 3-20, three main KPIs have been selected:

- **K20. Number of addresses mapped.** Theoretically, the mechanism is able to support up to 2^{16} nodes (65536) behind A SINGLE GATEWAY, as this is the number of different TCP ports. Please note the number of nodes in a capillary network is not limited by this, as there can be multiple Gateways or CHs.
  Anyway this number of supported nodes is limited by the chosen hardware. The module in charge of establishing the socket connections is the GPRS module. Due to its Internal IP stack limitations, just 8 sockets can be opened at the same time (or about 200 if they are not concurrent). So the practical implementation using this hardware is limited to that number.

- **K30.Transmission Payload Size.** The payload sent depends on the strategy used.
  - Using Strategy 1 [12][13] (all info included on Gateway memory and nothing in tha message payload) it is possible to send very efficient payloads (up to 80% efficiency)
  - On the other hand, if the goal is to avoid wasting memory resources, strategy 2 (storing IP address in memory but sending ZigBee addresses in the payload) or strategy 3 [12][13] (sending and IP packet capsule into the ZigBee packet, so no memory is used) can be used, resulting in less efficient transmissions (between 50 and 30%).

- **K35. Consumed energy per message.** Considering the average radio and microcontroller usage for typical transmission operations (250Kbps bitrate), and 85 bytes as payload for the messages it is needed to use the radio during 2,72 ms, which translates into
  - 0.753W per message using level 0 profile (or 3.012 µJoules per bit transmitted).
  - 0.975W per message using level 3 profile (or 3.9 µJoules per bit transmitted).

  Accurate measurements have been performed using professional power meters attached to the zigbee modules of M2M devices. This measurement has been done varying the data sent from 10 to 10.000 bytes, and setting the output power profiles from 10 dBm (level 0) to 18 dBm (level 4).

Table 3-11: Power profiles of ZigBee radio

Level	Power
0	10 dBm
1	12 dBm
2	14 dBm
3	16 dBm
4	18 dBm

Measures beyond 102 byte sent (the maximum payload size allowed by the capillary protocol) suppose transmissions of more than one packet, and that is why the curves decrease their power in Figure 3-23.

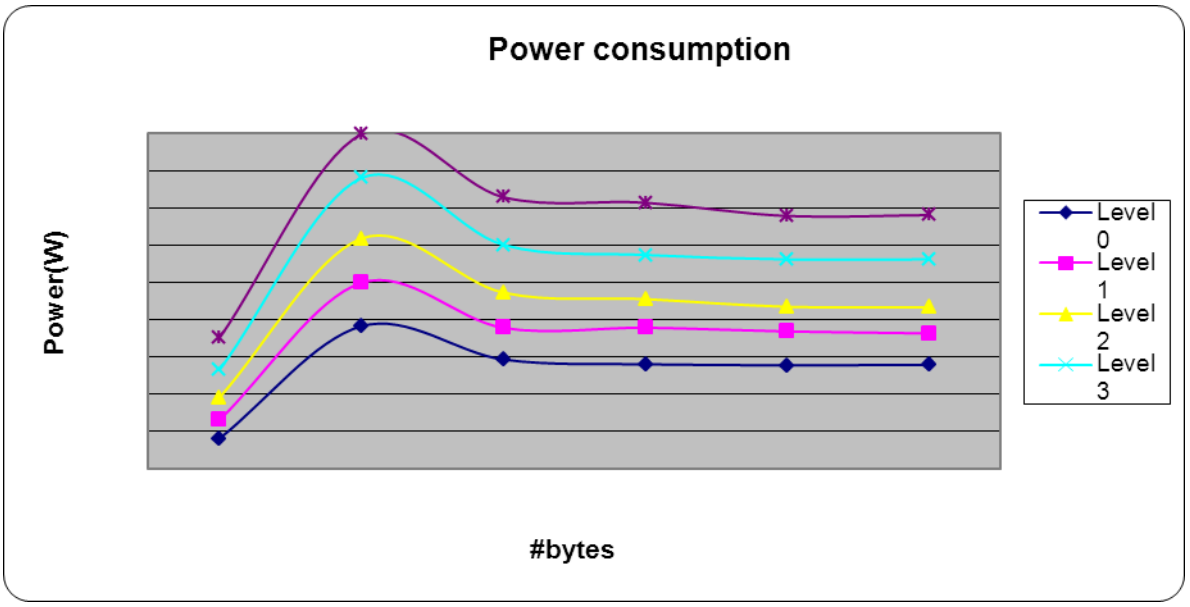


Figure 3-23: Power consumption for TSmarT devices varying data sent and output power profile

3.5.2 Verification Procedures

In order to validate the theoretical assumptions gathered from technical studies, several tools have been used. The aim is, in all cases, to provide real measurements to compare and backup the theoretical results.

In the following paragraphs, what has been used to verify each KPI measurement is explained.

- **K20. Number of addresses mapped.** The theoretical studies provided a limit of 2^{16} (number of available TCP ports) addresses behind a single gateway. In addition, the cellular modem datasheet included the hardware limitation of just 8 active TCP connections, with more than 200 concurrent connections. In order to verify this, a very basic set up was deployed with 9 end nodes transmitting through the gateway. With static resource allocation (establishing fixed connections for each node) the 8 node limit was proven. For more than 8 connections, the cellular modem would refuse any new socket creation request. But with dynamic resource allocation, this can be avoided, maintaining active (understanding as active a connection that is open and transmitting data, while an inactive connection can be opened but silent) just 8 links. This way, it was possible to maintain up to 10 socket connections (no more could be proven due to no more hardware (end nodes) available)

- **K30.Transmission Payload Size.** The verification of this KPI is very evident, as the application protocol is customized, as it was programmed as part of the project. Anyway, for validation purposes a network traffic sniffer (WireShark [20]) was used to capture the data transmitted by the M2M server and received at the M2M server (where the sniffer was working).

- **K35. Consumed energy per message.** Finally, the energy consumption has been measured using two approaches, a first one based on datasheets and a real one:
  - For the first one, both the cellular modem and the Zigbee module user guides provide the energy consumed per second. Knowing the length of the payload

sent and the throughput used, it is possible to obtain the energy consumed per message.

- In addition, real measurements were done using professional power meters attached to real devices transmitting different amounts of data, using the setup shown in Figure 3-24. This measurements where, in addition, repeated for different output power profiles (level 0, the lowest, to level 4, the highest):

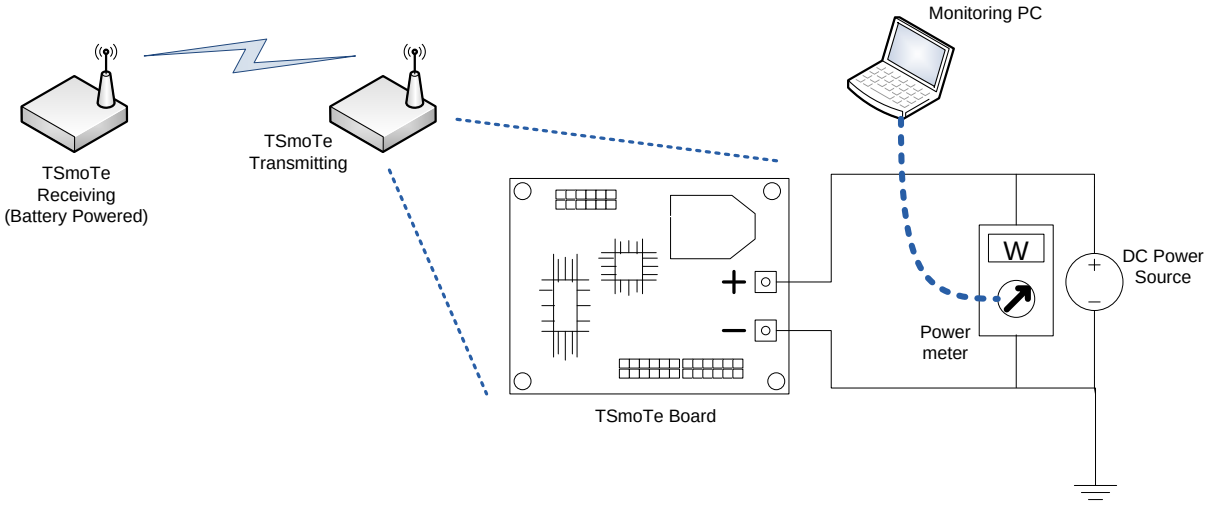


Figure 3-24: Setup configured to measure the power consumption

3.5.3 Wrap Up

The contribution of this testbed to the project objectives is manifold. Seamless connectivity is demonstrated explicitly for constrained low power devices, which is considered as one of the key challenges in EXALTED. The proposed solution is a lightweight address translation at the M2M gateway, which connects the IP world with the low power devices.

Table 3-12 summarizes the content depicted along section 3.5, from scenarios addressed to KPI assessment (quantitative and qualitative) going through technical requirements.

Table 3-12: Summary of subtestbed 2.3

Scenarios	Testbed & Solutions	Technical Requirements addressed	Qualitative Assessment	Quantitative Assessment	Measurable KPIs	KPIs assessment & Contribution to key objective
E2E connectivity	**Heterogeneous E2E connectivity Address translation mechanism**	FU.1	Addressing the maximum number of devices behind a M2M Gateway with the lightest overhead possible.	Maximum number of TCP connection allowed or maximum port numbers	**K20. Number of addresses mapped: 8 concurrent nodes or 200 non-concurrent nodes able to be addressed**	Overhead reduction versus IP. Number of supported nodes.
		FU.3	Implement	Web		Nodes able

			several applications on the same devices.	interface provided for two applications	**with the current GPRS modem. K30. Transmission Payload Size: 85 bytes reduced payload (80% reduction) using strategy 1** **K35. Consumed energy per message: depends on power profile used**	to understand remote commands. Over The Air Programming enabled nodes.
		NT.1	Support different radio interfaces.	3 radio interfaces (NFC, ZigBee and GPRS) enabled.		Enable heterogeneity
		NF.1	Scalability	Support for large number of devices.		Enable Gateways to handle high number of end nodes.
		NT.9	Deliver the message without compromising raw data at any point.	Unreachable data if trying to read it in intermediate points.		Security

3.6 Sub-testbed 2.4: End to End security

The context of this sub-testbed is the Energy Smart Metering and Monitoring business domain. As shown in the Figure 3-25 smart metering devices organized in a capillary network control photovoltaic panels. In this architecture each device controls a single photovoltaic panel. As announced in the title of this section the goal of this sub-tested is to showcase the End-to-End security. The security is brought by the Secure Element (SE) associated to each device.

There are 2 different uses-cases: one is based on messages send from the devices to the M2M server direction while the other one makes use of messages from the server to devices direction.

- The first use-case is an Energy Service Provider that needs to read remotely the electricity produced by various panels. From this collected data the Service Provider is able to pay the energy producers thanks to its back-office.
- In the second use-case the server is able to monitor the devices by sending commands to the devices (e.g.: start / stop production).

For various reasons the server may ask some devices to stop generating electricity, either because the electric network is near overloading or because of security reasons like a fire alarm in the installation and so no more electricity must be produced. After the alert the server can ask devices to restart production again.

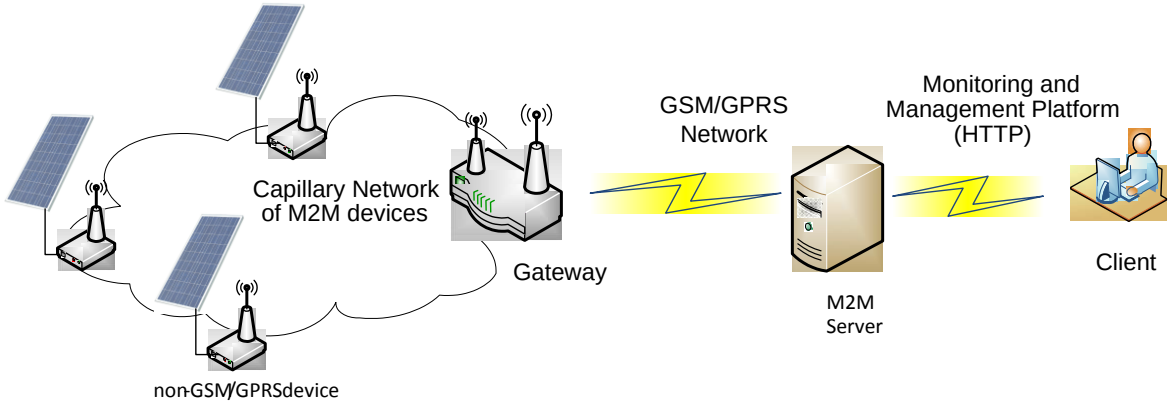


Figure 3-25: End to End Security Sub-testbed architecture

The security requirement for these use-cases is the data integrity.

- In the first use-case both ends have interest to tamper the metering data: on the energy producing end it would be nice to artificially increase the amount of electricity produced while the electricity operator could be tempted by under evaluating the amount of produced electricity.
- In the second use-case a malicious attacker could confuse the service by sending wrong commands to devices.

As illustrated on the figure above a gateway provides the connection between non IP device to the M2M server and enables data exchange between both ends. For the purpose of the demonstrator the module is not able to connect on 3G but uses GPRS. The Non-GSM/GPRS Devices connect through the capillary network to the M2M Gateway which provides connectivity to the M2M server.

In the implementation, the capillary network is a ZigBee network, and then the gateway is a bridge between the ZigBee network and the GSM/GPRS. The device sends data production to the ZigBee coordinator. The coordinator is part of the gateway and sends the data to the Cinterion GSM module through a serial port. Data are then sent by the Cinterion module trough HTTP over GPRS to the M2M server. In the other direction, the server sent commands by SMS to the Cinterion module, which sends them by the serial port to the ZigBee coordinator, and it delivers the command to a device according to the ID specified on the message.

The server sends a command to be executed by the End-Device. This command is sent over SMS to the gateway. The gateway has two parts: one responsible for the connection GPRS/GSM and the other one responsible for the communication with a ZigBee network. These two parts communicate between them over Universal Asynchronous Receiver Transmitter (UART) on port RS232. When the end-device receives the command to be executed, it sends the message received to the reader that forwards it to the SE which computes a new signature to be compared with the one contained in the message. If both signatures are the same, then the end-device will perform the command contained in the message. After that it will generate a response (Ack) to the server to notify that the command has been executed. This response is sent first to the SE to generate the signature before being sent to the M2M server.

An address translation mechanism is implemented on the gateway to enable the End-to-End communication. The feature is equivalent to what is implemented in other sub-testbeds

except this is done only to showcase the security provided by the SE. This is far to be exploited as a product.

An HTTP client can connect to the M2M server to check the production. The Graphical User Interface shown below enables to track the status, the energy produced and some static data like the location.

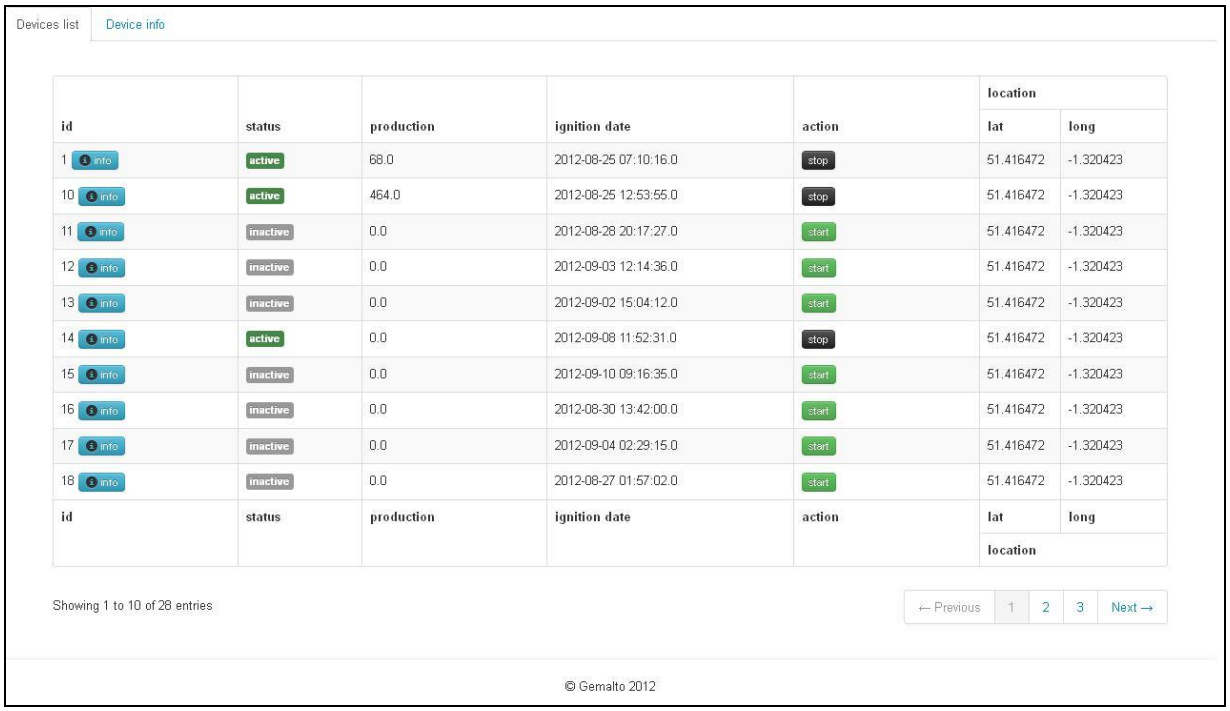


Figure 3-26: HTTP client interface

3.6.1 Performance Measures

A single KPI has been considered for this sub-testbed: K46-Computational energy consumption.

The device doesn't enable to take an actual measure of the specific SE extra electrical consumption. Statically values have been taken that can be put together to feature how would evolve the **K46 KPI** in an exploitation context. There are 2 cases according the SE usage frequency

- The SE is switched off between two successive cryptography operations
- The SE is in stand-by between two successive cryptography operations

According to the frequency required to send messages to the M2M server an application has the choice to apply the best SE activity management to optimize the energy consumed.

About duration, the SE bootstrap takes 67 ms while an Advanced Encryption Standard AES cryptographic operation takes 1.6 ms. The bootstrap time looks very long but during this bootstrap a communication channel has to be set up, the GEM02 component of the SE has to load its code and it needs to be run.

Mean power consumption is given in the following table

Table 3-13: SE consumption per activity

SE activity	Duration (ms)	Consumption (mA)
SE bootstrap	67	6,444
Cryptographic operation (AES)	1.596	6.606
Stand-by		0.2

The Cipher/Decipher uses a symmetrical AES key of 128 bits length.

An average measure for a smartcard commonly deployed on the field today is 5 ms duration for a consumption of 10 mA. A reason of the lower consumption of the SE compared to a classical smart card is that a coprocessor is invoked with the smartcard that boosts the ciphering/deciphering operation, but it comes along with a high electrical consumption.

The AES ciphering in the SE is implemented in software which explains the long duration. Still, it is quicker than for a classical smartcard, which is a surprise because the coprocessor should be much more efficient. But this comparison is not fair because operating systems are different.

The operating system of the SE has been reduced to the minimum while a smartcard manages a Java Card virtual machine with applet firewalling and supports the Open Platform standard that enables to have various secure channels. A precise snapshot of the actual ciphering operation only on a classical smart card would probably leads to a few micro-seconds. But many layers are invoked for this processing and the actual timing at the terminal application level incorporates all layers processing.

For a 24 hour activity and with the assumption that there are 100 cipher/decipher per hour the duration and power consumption are the following according to the SE management policy:

Table 3-14: Duration and Power according to SE management policy

Policy	Activity	Duration	Power (mAh)
SE switched-off between each operation	SE bootstrap	160.8	0.288
	Cipher/Decipher	3.830	0.007
	Stand-By	0.0	0.0
	Total:	164.63	0.295
SE in stand-by between each operation	SE bootstrap	0.067	0.0
	Cipher/Decipher	3.830	0.007
	Stand-By	86396.1	4.8
	Total:	86400	4.8

There is a bit of irony to measure the electrical consumption of a device that is dedicated to track the energy produced by a panel where there is plenty of energy. The photovoltaic panel is just a case study for the SE that could be integrated in any end-device where indeed the consumption does matter.

3.6.2 Verification Procedures

K46-Computational energy consumption: As there were no theoretical figures for the consumption of the SE, then actual measures cannot really compared to any initial expectation.

The architecture of the SE has changed during the course of the project to minimize this KPI. With the initial design, a full Java Card virtual machine enabled to process commands sent by the end-device. Considering the very limited requirements on the SE (i.e. to sign a hash value) this initial design has been reviewed to optimize the electrical consumption. It is up to the marketing to decide in the future what the favourite design for a product is. The final SE produced in the project minimises the energy required but has limited features.

3.6.3 Wrap Up

The following table summarizes the achievements and performance results of the End-to-End security sub-testbed

Table 3-15: Summary of sub-testbed 2.4

Scenarios	Technical Requirements	Achievements	Performance Results
End-to-End security	SV.6 Security	Data exchanged between both ends are protected	K46 – Computational energy consumption: • SE designed to be produced at low cost and with low-energy consumption. • 2 SE management policy considered: either stand-by or switch off between 2 processing to minimize the electric consumption

4. Validation of Testbed3: Device Management (DM)

Testbed 3 validates novelties in the field of device management. Considered aspects in the three subtestbeds are the lightweight device management message encoding, a novel self-diagnostic for reliability and monitoring, as well as security with respect to provisioning of group keys in self-organized capillary networks. Device diagnostic and monitoring mechanism is needed to manage devices in order to prevent failure and to maintain continuity of operations. Provisioning of group keys is an important step towards managing a group of devices securely while using the network bandwidth efficiently.
In EXALTED, the design scope of LTE-M is restricted to the PHY layer, therefore LTE-M is not available to be used in this testbed. Although LTE-M is not needed to showcase the novelties, LTE-M is required in real world deployments in order to further scale up the number of M2M devices supported in the system.

4.1 Evaluation Scenario

The validation of Testbed 3 will be done for smart metering and monitoring use cases. More specifically, a scenario to control energy consumption peak is envisaged to assess the performance of the lightweight DM solution. Provisioning of group keys is assessed using the same monitoring scenario, solar farm, as in subtestbed 2.4. Self-diagnostic and monitoring algorithms are generic; no particular scenario has been applied for the validation.

4.2 Key Objectives and Performance Indicators

The validation is composed of 2 steps: functional validation and performance assessment.
The functional validation makes sure that technical requirements pertaining to each subtestbed are fulfilled. Technical requirements have been defined in the report D2.1 [6]. The report D7.2 [1] provides a mapping of technical requirements for subtestbeds.
Performance indicators are then evaluated to assess the values of the novelties brought to the system in order to achieve EXALTED high-level objectives, such as scalability and energy efficiency.

Table 4-1: Summary of solutions and KPIs

Solution/innovation	Main KPI	Use cases that the solution is applicable to	Comments/remarks
ELFOMA DM Payload reduction	**K30** Transmission Payload Size	ITS, SMM, e-Health	Reduce size of messages being sent over LTE-M. Enhance scalability
ELFOMA DM Energy efficiency	**K32** Actual Payload Size **K45** Resources consumption	ITS, SMM, e-Health	Low complexity coding scheme and low resource demanding. Reduce cost of devices.
Self-Diagnostic Distributed and aggregated device diagnostic model	**K54** Frequency of queries	ITS, SMM, e-Health	Reduce the number of connections to M2M server. Enhance scalability
Secure provisioning	**K49** Flexibility of the security enrolment	ITS, SMM, e-Health	Number of messages required

Group keys provisioning efficiency			to provision device. Reactivity of provisioning operations.

4.3 Sub-testbed 3.1: Lightweight Device Management

EXALTED enables the anticipated massive number of low cost M2M devices to connect to the internet over LTE-M radio access network. As LTE-M is a system co-existing with LTE in the same spectrum, the amount of available radio resources for M2M is limited. Therefore device management (DM) control and data flows exchanged over LTE-M must not be verbose. Two Lightweight DM solutions have been proposed in WP4-D4.3 [14]. The first DM solution, namely ELFOMA (Exalted Lightweight DM For OMA-DM v1.x), enables operators to save cost by reusing existing OMA-DM v1.x servers to incrementally manage new constrained M2M devices. Operators not relying on existing OMA-DM server can use the second DM solution which is based on CoAP.

This subtestbed aims evaluate performances of ELFOMA against OMA-DM. The envisaged scenario for the evaluation and key objectives are described below. Measured performances are then unveiled and compared to the simulated results in the next sections.
DM solutions developed in WP4-D4.3 [14] can support any device management needs in all EXALTED use cases, namely ITS, eHealth and SMM. A SMM scenario has been selected to evaluate performances of ELFOMA.
The selected SMM use case emphasises “Green” values by providing a novel procedure to electricity supplier to avoid importing electricity from abroad or starting a fossil fuelled thermal power plant, in case of energy consumption peaks. These temporary electricity consumption peaks could occur in cold winter, particularly between 6PM to 10PM timeframe, as millions of heaters, ovens and other energy demanding household appliances are likely to operate at once. Importing energy from abroad or starting an additional power plant to satisfy this instant high energy demand has negative impacts on supplier’s operational cost and environment. To avoid this case, the proposed scenario consists in monitoring the global energy consumption. When it exceeds a predefined threshold, the system will be sending “power cut” orders to selected heaters. Cutting heaters for 10 or 15 minutes does not affect households comfort level. Heaters could be powered off based on a round robin basis so that households are evenly affected in order to prevent the consumption peak to happen. The scenario is depicted in Figure 4-1. An alternative option is to lower the heating temperature instead of turning the heaters off.

The energy consumption peak controller is composed of the following components:

1. Energy monitoring application server is connected to the internet. Operational users interact with this server through a user interface, in order to view device data and trigger power cut action, to remotely turn on/off heater.
2. M2M Server interfaces with M2M gateways (indicated as energy gateway in Figure 4-1) over the ELFOMA protocol, using cellular network. On the backend, M2M server interconnects with the application using REST interface.
3. Energy Gateways are connected to the capillary network that cover actuators and smart meters
4. Each actuator is linked to a heater. The actuator can turn the heater on or off. This on/off order is sent by the energy gateway (on behalf of the M2M server)

The proposed use case supports the workflow as depicted in Figure 4-1:

1. The gateway collects smart meter indexes on periodical basis. The retrieved meter index is posted to M2M server over the ELFOMA protocol.

2. M2M server gathers metering indexes from all gateways and made data available to the energy monitoring application server. This latter keeps track of the global power consumption. The power cut logic continuously monitors the global power consumption. This automatic power cut logic is not implemented in the testbed, manual operation, in step 4, is used instead to showcase this remote control feature.
3. If the global power consumption exceeds the defined threshold, then the application server sends power cut order to actuators to power off heaters. If the global power consumption drops below the threshold, then the application server sends power on orders to actuators to resume heaters.
4. Supplier operational staff members can access the control panel of the application server, using a computer connected to the internet. The user can view the current global power consumption, view/edit the threshold, and trigger manually a power cut on a selected actuator (heater).

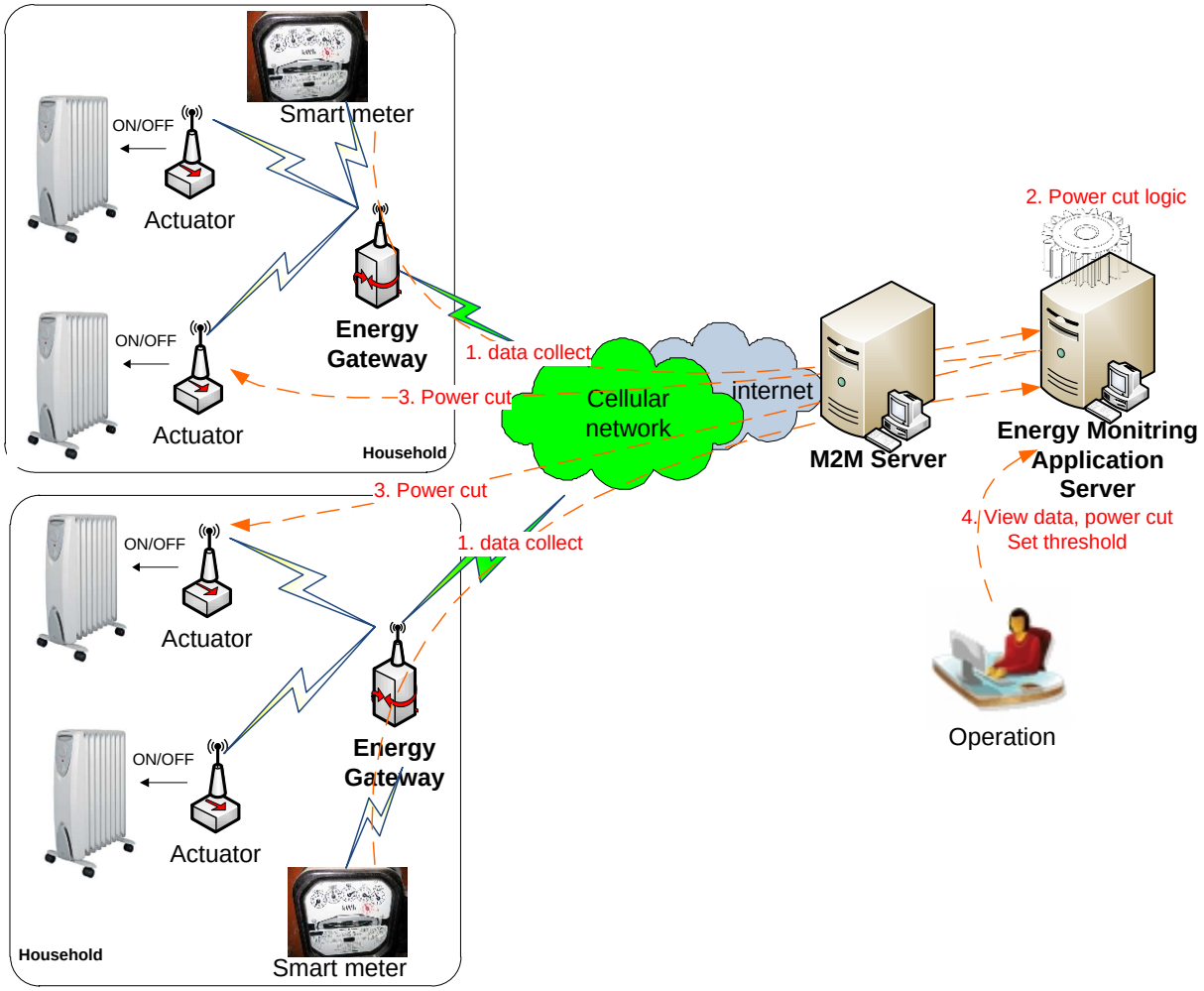


Figure 4-1: SMM, energy consumption peak scenario

This energy consumption peak controller scenario is emulated by the subtestbed with the following assumptions:

1. Energy gateways are emulated by smartphone running Android application
2. Physical smart meters and heaters are emulated by mobile phones, this latter send text message to the smartphone (acting as gateway). The SMS is emulating device-gateway communication within the capillary network.

3. The Android application communicates with the M2M Server over the ELFOMA protocol.

The user interface of smartphone application yields several advantages, such as variable customization without recompiling the application, visualization of ELFOMA payload, clear indication of functional behaviour.
The key objectives of this subtestbed are to validate the following aspects:

1. Make sure that ELFOMA can be used to functionally manage devices for the selected scenario. This can be performed by fulfilling all technical requirements as listed in Table 4-2.

Table 4-2: Technical requirements

ID	Technical Requirements	Comments
FU.5	Local and remote device management	Manage devices deployed over a wide area, either locally or remotely
FU.6	Unique identity for devices	Due to the huge number of devices, this latter must be uniquely identified (sensors, actuators, cluster heads or gateways)
NT.6	End to end device to device communication	Device communication must be possible between different types of capillary network (heterogeneity)
NT.13	Multicast & Broadcast	To be bandwidth efficient, a single message can be sent to all devices or to selected devices within a group
NF.1	Scalability	Compared to OMA-DM baseline, the proposed DM solution must be able to manage a high number of devices
NF.2	Energy efficiency	ELFOMA is expected to consume less energy than the referenced OMA-DM protocol
DV.7	Protocol translation at the gateway	To increase the interoperability, protocol translation must be implemented by the gateway
DV.10	Remote configuration	To extend the life cycle of devices, this latter must be remotely configurable by M2M Applications, e.g. update settings

2. Assess that ELFOMA contributes to the following operational objectives:
   (i) Scalability in terms of spectrum usage, more concurrent communication, thus a higher number of devices, can be supported using the same bandwidth
   (ii) Cost efficiency, telecommunication cost could be lower as the transmission time is reduced. The unit cost of the device is also reduced due to the low complexity of the proposed payload encoding (e.g. CSV) and the number of protocols to be embedded in the device is reduced to one.
   (iii) Energy efficiency, shortened transmission time and low complexity message encoding help to increase the energy efficiency.
   (iv) Reliability, the proposed protocols are reliable, none confirmed messages are retransmitted.

The achievement of the aforementioned operational objectives is validated by the following performance indicators:

- **K30 - Transmission Payload Size.** The size of DM payloads being transmitted over the cellular network (emulating LTE-M). Small transmission payload size obviously enhances the scalability, cost efficiency and energy efficiency of the system.
- **K45 – System resource consumption.** Upon receiving the transmitted payload (K30), the M2M device consumes resources to: (i) decompress/decode it to recover the actual payload, (ii) parse the latter payload to execute DM commands,. Memory usage and CPU usage are measured for the above 2 operations. These resource usages are used to assess the energy efficiency of algorithms being benchmarked. In addition, memory usage indicator affects the cost of the device.
- **K32 – Actual Payload Size.** The size of the actual payload being used by the DM server and client. Upon receiving the transmitted payload (K30), the device decompresses/decodes it in order to retrieve the actual payload (K32). A small K32 number will lower the cost of device, as it is less memory capacity demanding.

Figure 4-2 depicts where these performance indicators are measured within the system.

4.3.1 Performance Measures

This section unveils performances that have been measured with the subtestbed implementing the selected energy consumption peak controller scenario described earlier.

Figure 4-2 depicts the components residing in the energy gateway and in the M2M server.
The measurements are performed on the triangle spots. The logic is described hereafter:

1. OMA-DM v1.x server is not implemented in this subtestbed (out of the measurement scope)
2. OMA-DM v1.x payload is therefore created manually based on the messages required in the selected scenario to be implemented.
3. ELFOMA Server is implemented in the M2M Server. Other payload conversion methods, such as, EXI and WBXML, are also implemented for benchmarking purposes.
4. OMA-DM v1.x payload created in step 2, is converted for transmission over the cellular network (emulating LTE-M). Different conversion methods implemented in step 3 yield different payload packages whose sizes are to be evaluated to obtain K30.
5. Upon receiving the above converted payload, the gateway decodes it. The decoding consumes resources that should be measured to obtain K45.
6. The actual payload is recovered after performing the decoding in the previous step. This payload is the same as the one in step 2, therefore they have the same size, measured as K32.
7. The actual payload in step 6 has to be parsed by the device to extract the DM commands. This parsing consumes resources that should be measured to obtain K45

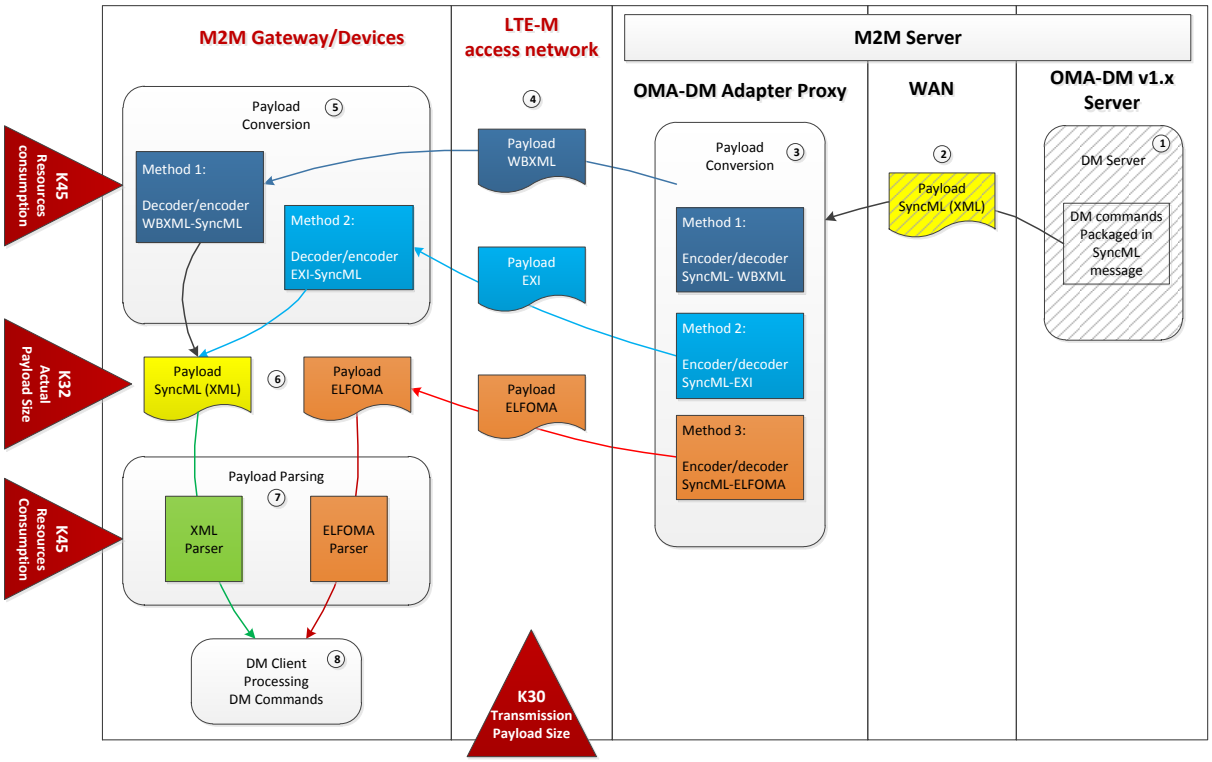


Figure 4-2: Performance measurement points

It should be noted that ELFOMA does not require steps 5 and 7.

Measurements are performed using the message flows as shown in Figure 4-3 implementing the selected scenario.

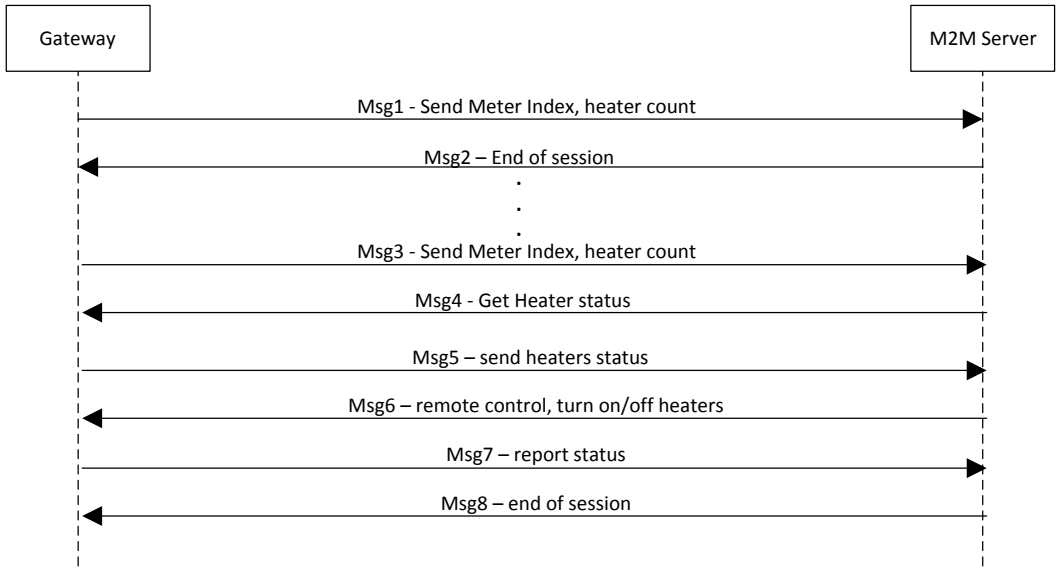


Figure 4-3: Energy consumption peak controller message flows

4.3.1.1 K30 – Transmission Payload Size

Messages depicted in Figure 4-3 have been encoded to the following message package types:

- OMA-DM SyncML

- WBXML
- GZIP
- EXI
- EXI with Schema
- ELFOMA

The corresponding sizes are depicted in Figure 4-4 and K30 performances are presented in Figure 4-5

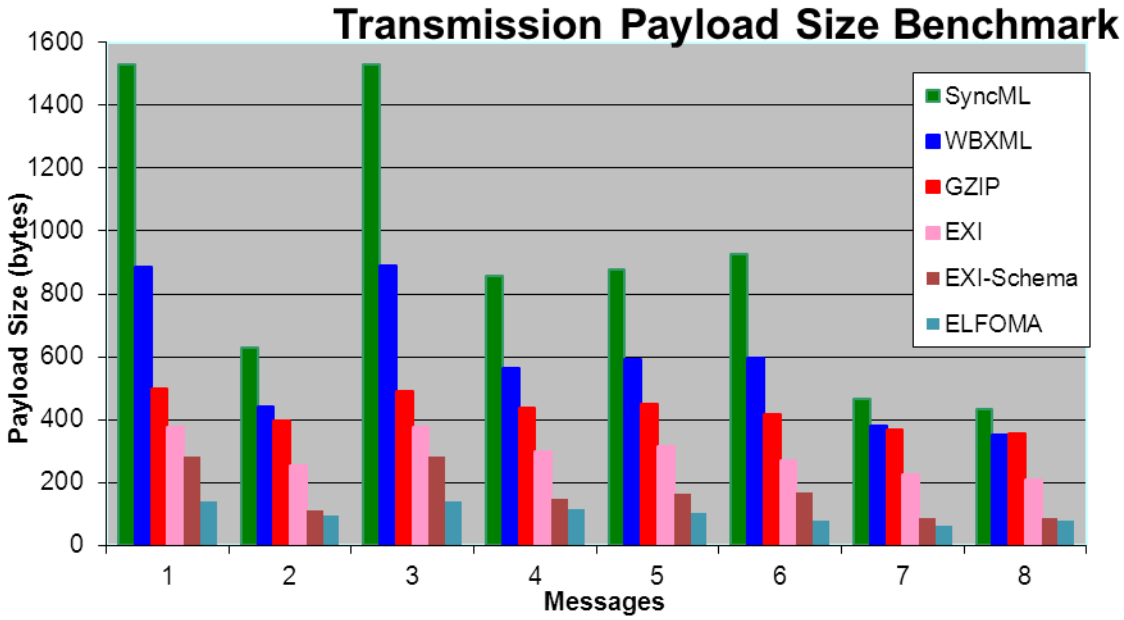


Figure 4-4: Measured Transmission Payload Sizes

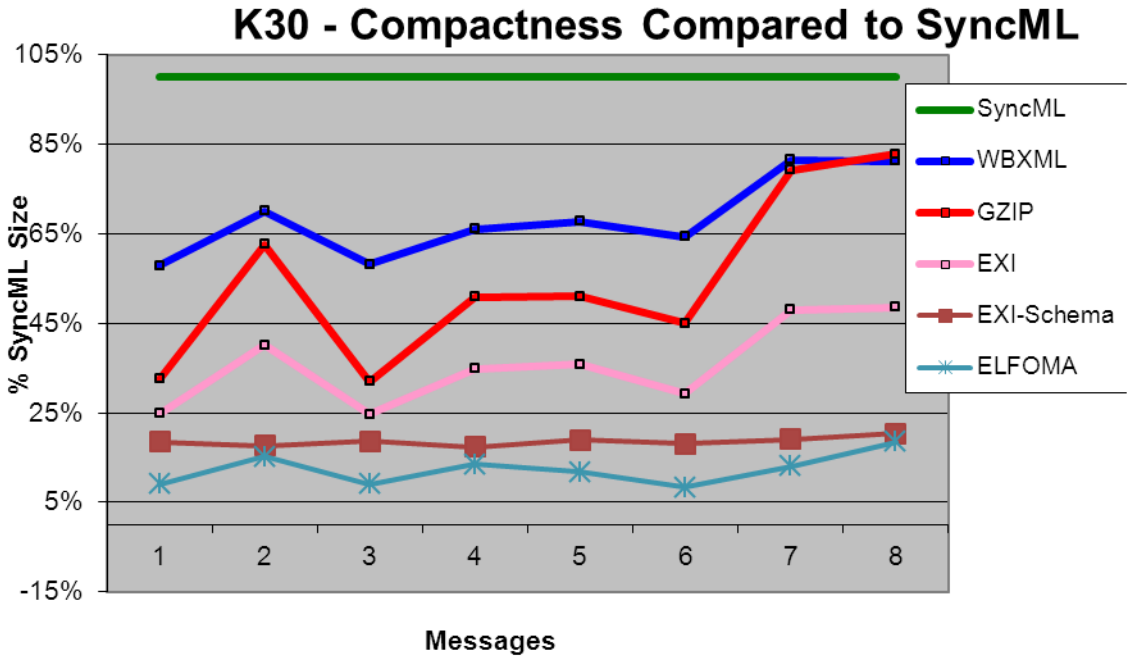


Figure 4-5: Compactness of algorithms compared to OMA-DM v1.x messages

As shown in Figure 4-5, ELFOMA yields the most compact DM messages. This compactness reduces the transmission time of DM data over the LTE-M link (refer to step 4 in Figure 4-2). The average transmission payload sizes as measured for the implemented scenario are:

- OMA-DM : 906 bytes
- WBXML : 588 bytes
- GZIP : 427 bytes
- EXI schemaless : 291 bytes
- EXI schema : 167 bytes
- ELFOMA : 102 bytes

The average performance indicators K30 are:

- WBXML: 68,4%
- GZIP: 54,5%
- EXI schemaless: 35,8%
- EXI schema: 18,5%
- ELFOMA: 12,3%

ELFOMA transmission payload size is 8.95 times smaller than OMA-DM payload size. In other words, for a given bandwidth the number of devices communicating simultaneously over the radio access network can be increased by a factor of 9. This up-scaling factor is comparable in magnitude with the air interface performance obtained by LTE-M. [5]

4.3.1.2 Payload Decoding Efficiency

Upon receiving the payload as transmitted in step 4, the device decodes it in order to recover the native DM message format. This step is not required in ELFOMA, however this decoding is required for WBXML and EXI encoding methods, refer to step 5 in Figure 4-2.
The WBXML and EXI payload decoding aim to convert the received payload back to OMA DM SyncML payload format. This process consumes resources. CPU and memory resource consumption figures are depicted below for WBXML and EXI (schema and schemaless) encoding methods.
EXI with schema is far more CPU and memory demanding than EXI schemaless and WBXML schemes. WBXML is the less resource demanding, however it does not yield acceptable payload compactness, as shown in the previous section.

Based on Figure 4-6, the average CPU times required for this decoding are the following:

- EXI schemaless: 150,25ms
- EXI with schema: 552,37ms
- WBXML: 31,12ms
- ELFOMA: 0ms (no decoding for ELFOMA)

Based on Figure 4-7, the average required memory capacity:

- EXI schemaless: 741KB
- EXI with schema: 2018KB
- WBXML: 46KB
- ELFOMA: 0KB (no decoding for ELFOMA)

KXML2 [19] library has been used to perform WBXML encoding and decoding.
EXI encoding and decoding are performed using an open source implementation of the W3C Efficient XML Interchange (EXI) format, EXIfficient [15].

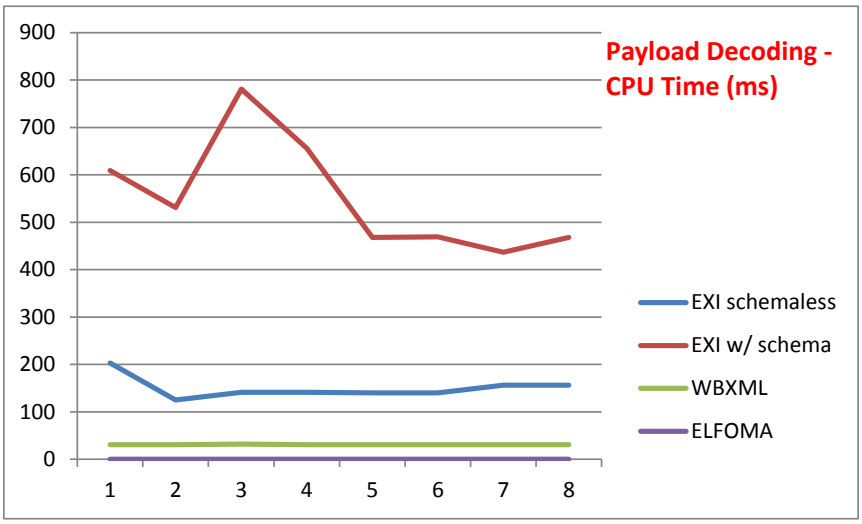


Figure 4-6: Payload decoding time (ms)

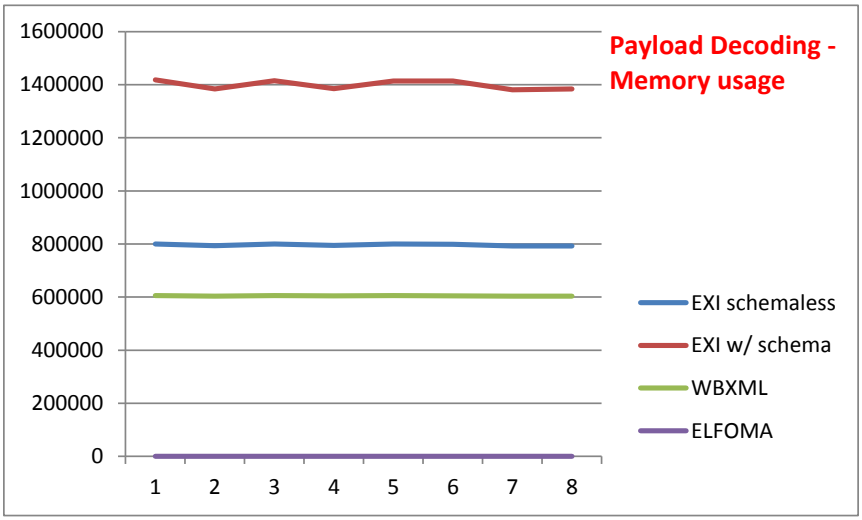


Figure 4-7: Memory usage for payload decoding

ELFOMA does not consume any resources at this stage, as ELFOMA decoding is not required.

4.3.1.3 K32 – Actual Payload Size

The actual payload size can be measured in step 6 of Figure 4-2.
ELFOMA transmission payload size and Actual Payload size are equal. While the actual payload for WBXML and EXI schemes are inflated upon decoding.

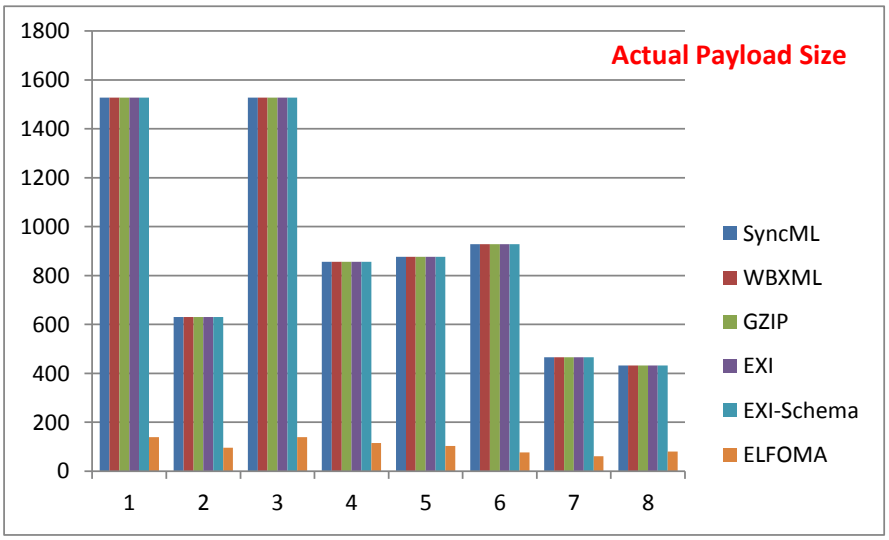


Figure 4-8: Actual Payload size

ELFOMA has the smallest actual payload size. DM Client on the device processes the actual payload to execute DM commands. Therefore ELFOMA is less memory demanding.

Encoding schemes WBXML, GZIP, EXI and EXI with schema yield the same actual payload which is equal to OMA-DM message payload size.
The average ELFOMA actual payload size is 101 bytes, versus 905 bytes for other encoding schemes. Therefore, ELFOMA actual payload size is almost 9 times smaller than the compared encoding schemes.

4.3.1.4 Payload Parsing Efficiency

As shown in step 7 of Figure 4-2, the device parses the actual payload in order to execute DM commands being conveyed. CPU and memory usages are measured to assess the efficiency of algorithms.

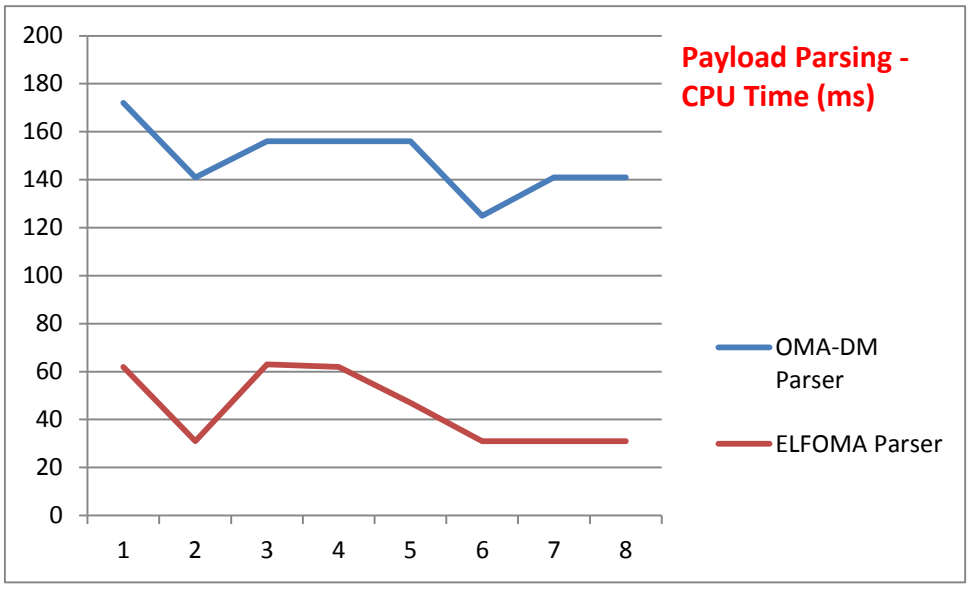


Figure 4-9: OMA-DM vs ELFOMA Parser – CPU processing time

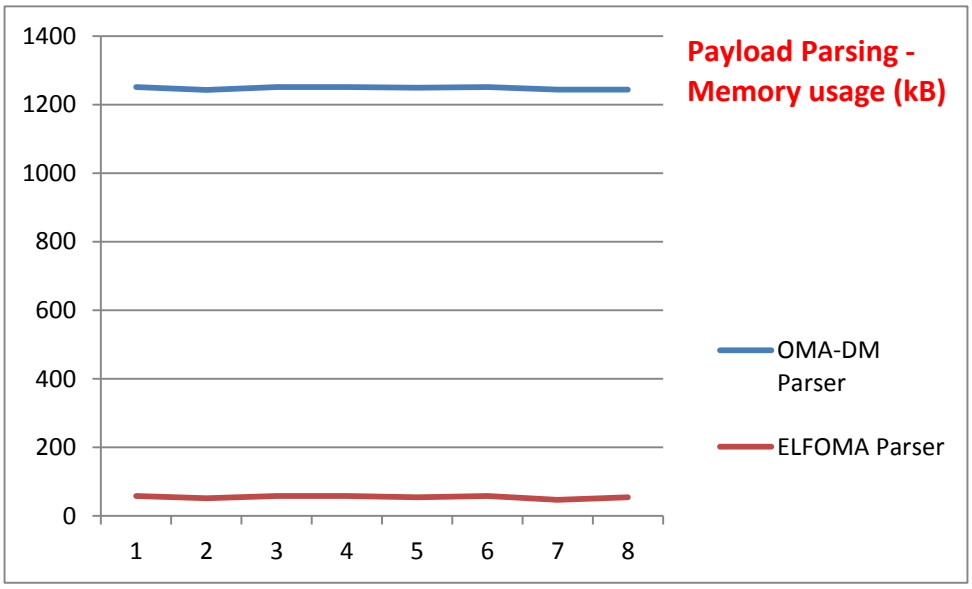


Figure 4-10: OMA-DM vs ELFOMA Parser – Memory usage

Parsing ELFOMA messages is less resource demanding then parsing OMA-DM messages.

Based on Figure 4-9, the average CPU times required for parsing are the following:

- OMA-DM: 148,5ms
- ELFOMA: 44,75ms

Parsing ELFOMA payloads is 3.3 times less CPU demanding than parsing OMA-DM payloads.

Based on Figure 4-10, the average memory usages for the parsing are the following;

- OMA-DM: 1247KB
- ELFOMA: 55KB

Parsing ELFOMA payloads is 22.7 times less memory demanding than parsing OMA-DM payloads.

4.3.2 Verification Procedures

This section compares the theoretical performance results obtained in WP4 to the counterpart experimental results measured in this subtestbed.

- **K30 - Transmission Payload Size.** This KPI has been measured using Wireshark and unveiled in Figure 4-4. Although these experimental values slightly differ from the theoretical numbers obtained in WP4-D4.3 [14], the results are consistent with respect to the range of compactness (ELFOMA compactness is 12,3% experimentally vs 15,4% analytically). It should be noted that results are also consistent across different scenarios: firmware update over the air scenario and controlling energy consumption peak scenario.
- **K32 – Actual Payload Size.** The results measured in Figure 4-8 are consistent with those obtained in WP4-D4.3 [14]. Namely, the content of decoded payloads (not applicable to ELFOMA) is the same as of the original OMA-DM messages, even though linefeed and carriage return characters are removed in XML-based

messages. The formatting deviation is acceptable as it does not affect the content of messages.

- **K45 – System resource consumption.** Due to the complexity, resource consumption figures with respect to payload decoding and payload parsing cannot be analyzed in WP4-D4.3 [14]. However, experimental results obtained in Figure 4-7 and in Figure 4-10 confirm the expected low energy and resource demanding characteristics of ELFOMA.
  The required amount of memory for decoding the incoming payload (Figure 4-6) and for parsing the payload (Figure 4-9) may appear to be very high. VisualVM tool (part of Java Development Kit) has been used to measure memory usage of the testbed java application within the Java Virtual Machine. The amount of memory being measured actually includes java instances (code footprint) and memory allocation to process the said operations.

4.3.3 Wrap Up

Technical requirements as listed in Table 4-3 can be addressed by the device management sub-testbed implementing ELFOMA DM solution. Functional achievements can be demonstrated by the testbed covering an energy consumption peak controlling function.

Furthermore, 3 KPIs have been measured, K30, K32 and K45. Performance results as summarized in Paragraph 4.3.1 yield the following outcomes:

1. With the proposed ELFOMA DM solution, stakeholders can reuse their existing OMA-DM v1.x servers to manage constrained M2M devices. Compared to the standard OMA-DM protocol and for a given bandwidth, the number of devices communicating simultaneously over the radio access network can be scaled up by a factor of 9.
2. The average size of an ELFOMA message is 100 bytes. Thus messages can be exchanged over a low latency radio access network within a reasonable timeframe.
3. ELFOMA is 3.3 times less CPU demanding to parse than OMA-DM. We could assume that devices implementing ELFOMA are consuming 3 times less energy to parse DM payloads. The CPU processing capability of devices can be downsized to save device cost.
4. ELFOMA is 22.7 times less memory demanding to parse than OMA-DM. The device cost could thus be further lowered.

Table 4-3: Summary of sub-testbed 3.1 achievements

Scenarios	Technical Requirements	Achievements	Performance Results
Device Management **Smart Metering and Monitoring** **Energy Consumption Peak**	FU.5 Local and remote device management	DM objects are accessible remotely from M2M Application. DM functions can be performed over the ELFOMA protocol	**K30 – Transmission Payload Size**: The average size of ELFOMA message is 100 bytes. ELFOMA reduces OMA-DM payload size by 87.7%.
	FU.6 Unique identity for devices	ELFOMA is using Unique Device ID to address devices. Can be verified with Wireshark	
	NT.6 End to end device to device communication	An end Device or M2M application can send message to another device located in a different capillary network. Temperature can be sent from a sensor to an actuator.	
	NT.8	Message is routed to the gateway	

	Mobility management	to which the recipient device is attached to.	**K32 – Actual Payload Size**: EMFOMA payload size is 9 times smaller than OMA-DM. **K45 – System Resource Consumption**: ELFOMA is 3.3 times less CPU demanding and 22.7 times less memory demanding to parse than OMA-DM.
	NT.13 Multicast & Broadcast	A message can be sent to selected devices within a group. Can turn on/off several appliances (e.g. lamps, heaters) at once.	
	NF.1 Scalability	ELFOMA payload size is smaller than OMA-DM payload. Can be verified with Wireshark. This enables a high number of simultaneous device communications for a given bandwidth.	
	NF.2 Energy efficiency	Compared to OMA-DM, ELFOMA is less CPU demanding. Can be verified with VisualVM or JProfiler.	
	DV.7 Protocol translation at the gateway	DM commands within ELFOMA protocol are translated onto device specific commands. E.g. to a cell phone using SMS	
	DV.10 Remote Configuration	Device settings can be updated remotely by M2M applications.	

4.4 Sub-testbed 3.2: Self Diagnostics

This sub-testbed is called “Self-Diagnostics” and is included in “Device Management” Testbed 3. It is oriented toward use cases, such as ITS and SMM, that require as much autonomy from human intervention as possible. The covered scenarios are root failure cause detection and assisted self-healing.

4.4.1 Performance Measures

Besides enhancing the reliability of the M2M devices *per se*, the purpose of the self-diagnostic feature is to enable the device to collect autonomously as much relevant data as possible on its operational status before reporting these data to a management module. In order to minimize the number of transactions that would occur on a wireless link, the device ought to process these data first to extract the most meaningful information. This is the purpose of the self-diagnostic rule engine running in the device.
Therefore, an appropriate performance measure is given by **(K54) – Frequency of queries** from the Device Management server to the M2M device.

4.4.2 Verification Procedures

The testbed relies on a Self-diagnostic Module (SDM) package that is composed of two parts:

1. The embedded part (SdmManager) is designed to be executed on the embedded board (an OBU).
2. The Master (Master Sdm) module, playing the role of a Device Management server enabling device self-diagnostic, runs on a PC and is designed to display the diagnostic results.

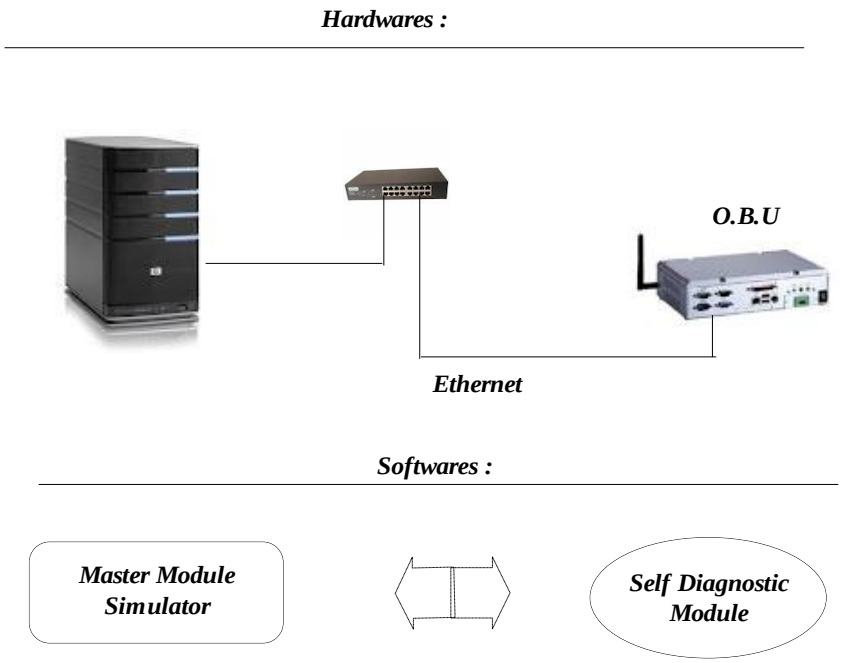


Figure 4-11: Self-diagnostic Testbed

The following figure summarizes for each part, the internal function blocks:

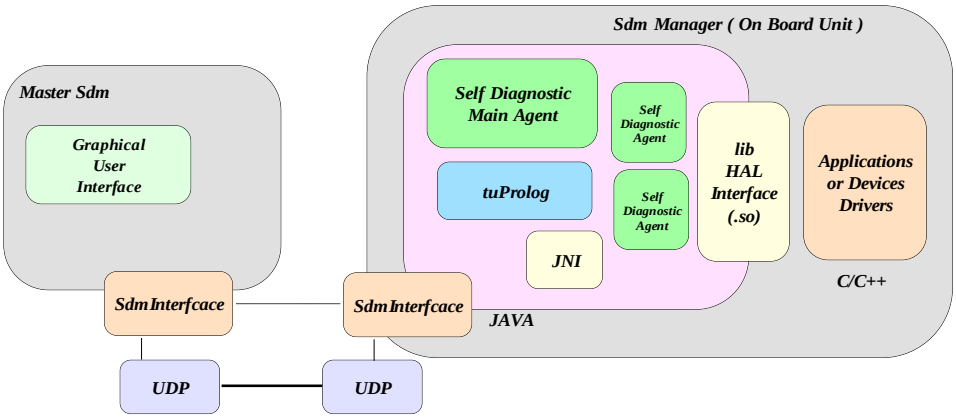


Figure 4-12: Internal Function Blocs

The “Sdm Manager” bloc and the “SdmInterface” module compose the main part of the Self Diagnostic Solution. These elements are designed to be installed in the M2M devices.

The “Master Sdm Manager” module plays the role of a simulator of “Device Manager Module” or a high priority Sdm. It is used here to interact with the remote “Sdm Managers” using a graphical user interface and via the symmetric “SdmInterface” module.

“Master Sdm” and “Sdm Manager” are developed in Java. Each peer uses the “SdmInterface” module for its “diagnostic exchanges”. The “SdmInterface” is also a java module that uses the User Datagram Protocol (UDP) protocol.

The MasterSdmManager module is a graphical based application. This program is used to facilitate the execution of the exchange sequences with the SdmManager and to display the diagnostic action results.

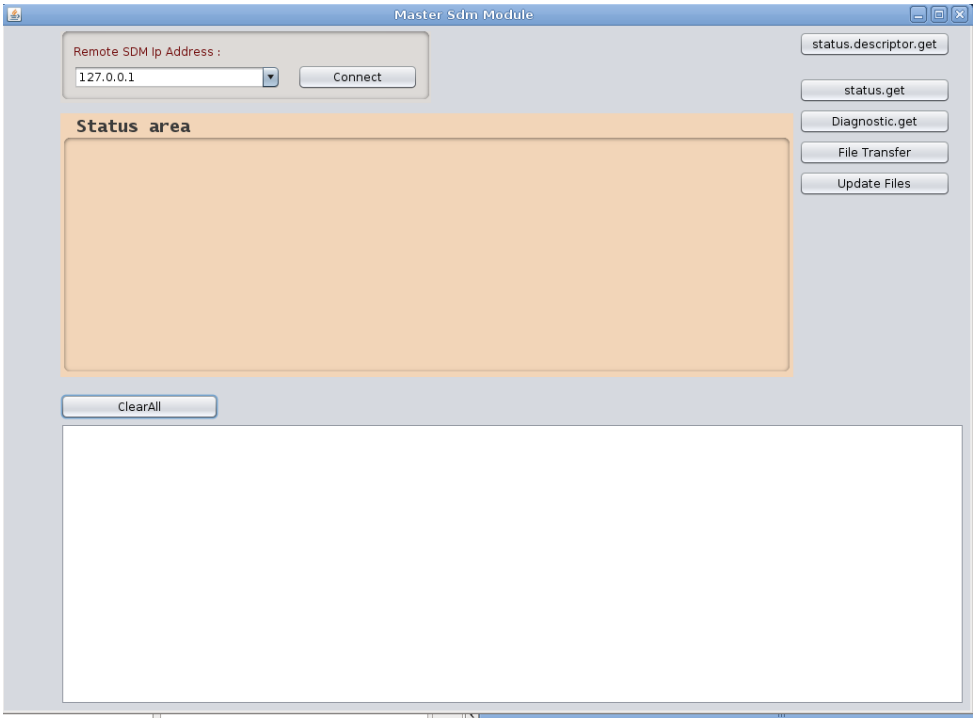


Figure 4-13: Master Sdm Graphical Interface

The typical diagnostic sequence requires the following preliminary actions:

1. Choose the IP address of the (remote) SdmManager.
2. Click on the “Connect” button to activate the connection.
3. Click on “status.descriptor.get” button to retrieve the description of the device status.
4. Click on “status.get” button to read the current status or force the execution of a new diagnostic sequence by “diagnostic.get”.

The following images show this sequence:

a) Connect

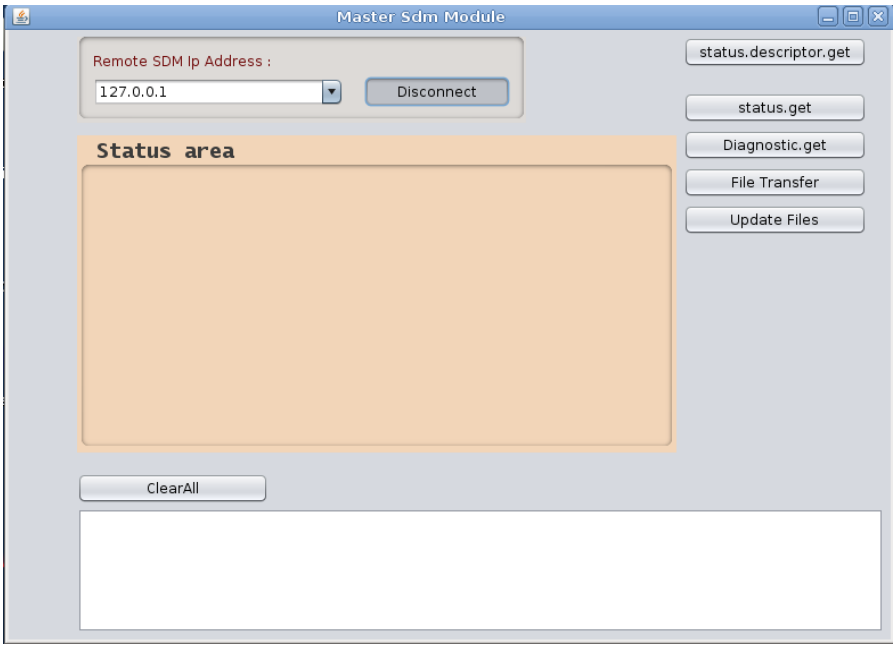


Figure 4-14: Connect to M2M Device

b) Get status descriptor, listing the M2M device components to be diagnosed.

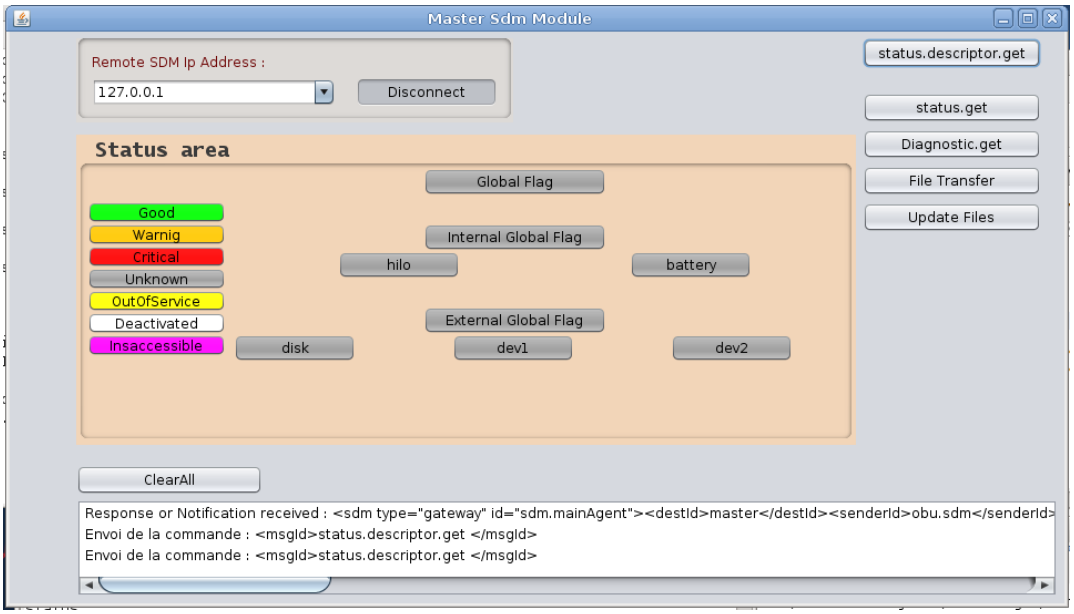


Figure 4-15: Get Status Descriptor

c) Get status with or without forcing a new diagnostic sequence

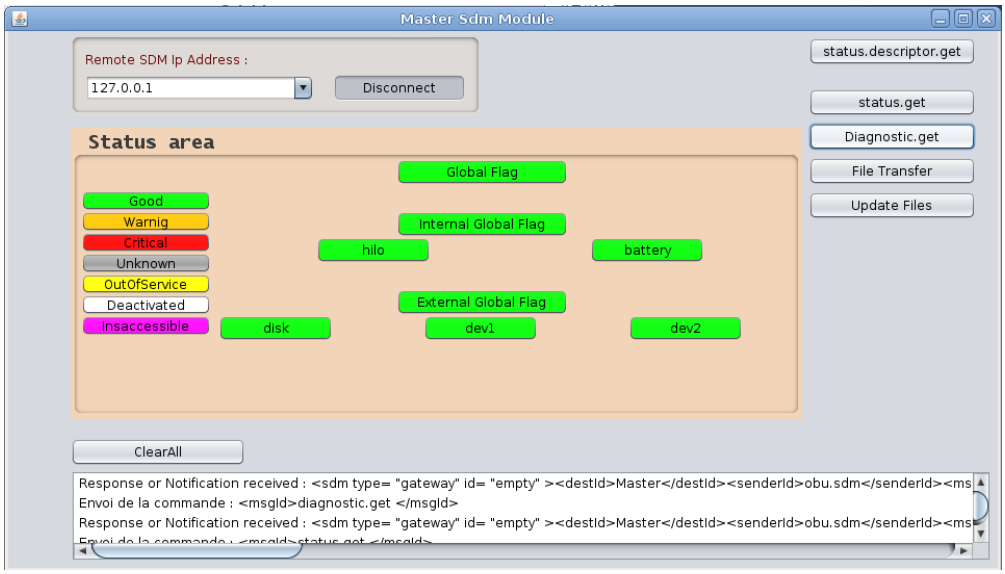


Figure 4-16: Get Self-Diagnostic Status

For each action, the content of the exchanged messages (based on XML format) are shown in the log list element. The diagnostic sequences are based on Prolog rule files. These files must be present in the SdmManager file system.

In the MasterSdmManager side, a repository folder is provided to save and manage these files. The “Update File” button can be used to select them. This button activates the following sequence:

1. Open a file dialog control for searching and displaying a rule file. This file can be modified and saved in repository.
2. Transmit the new file to the SdmManager for being copied to its file system. The file transfer is provided by SdmInterface Library.

The screenshots hereafter show this sequence:

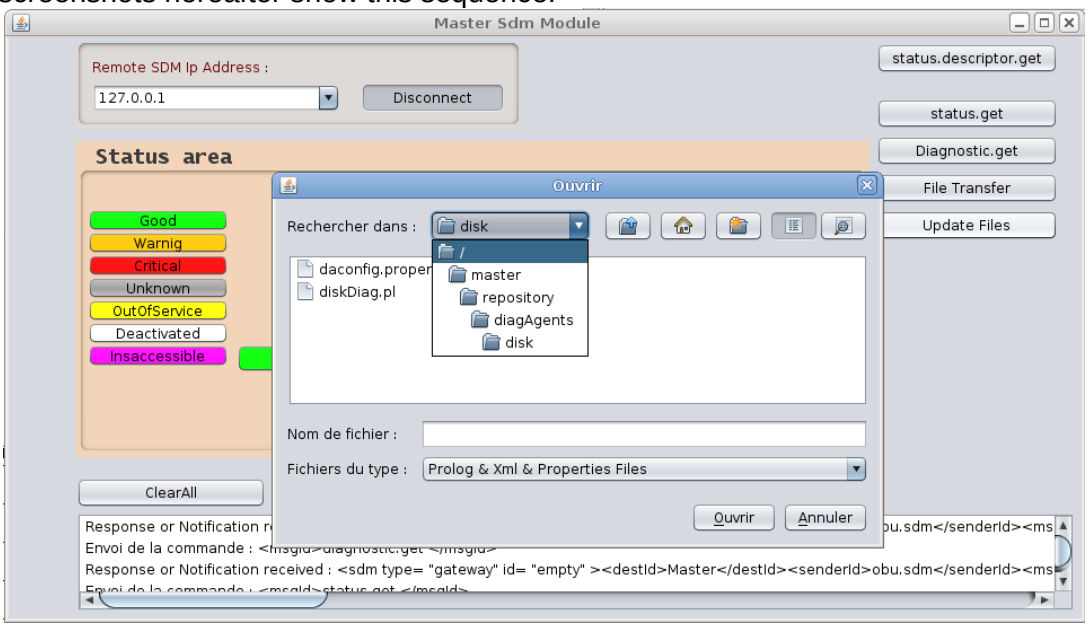


Figure 4-17: Upload New Self-Diagnostic Rules

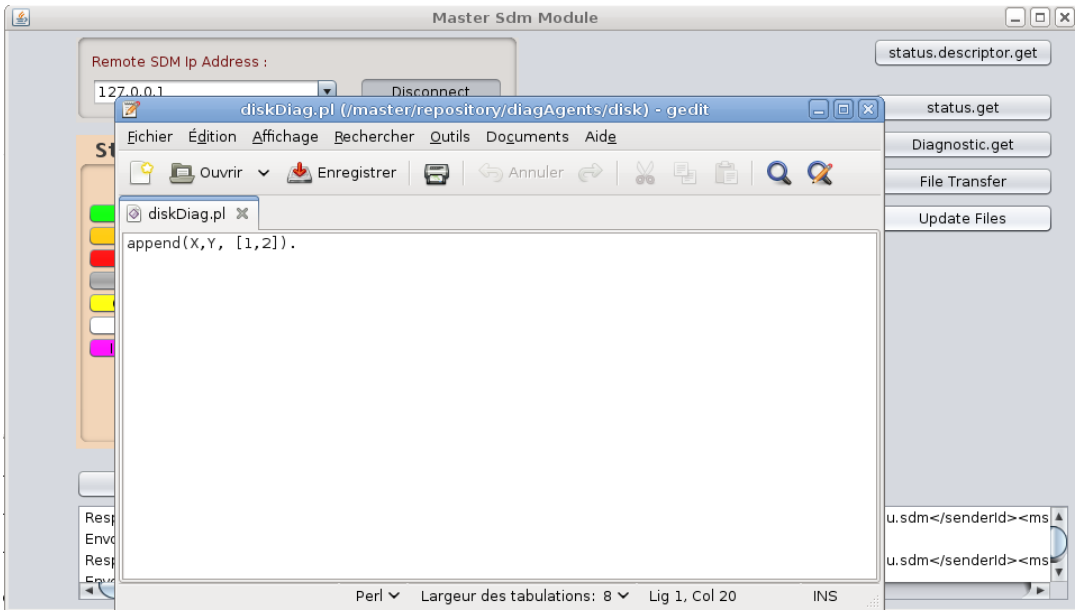


Figure 4-18: Modify Rules

When the user closes the rule file, a new dialog box is displayed before sending the new file to Sdm:

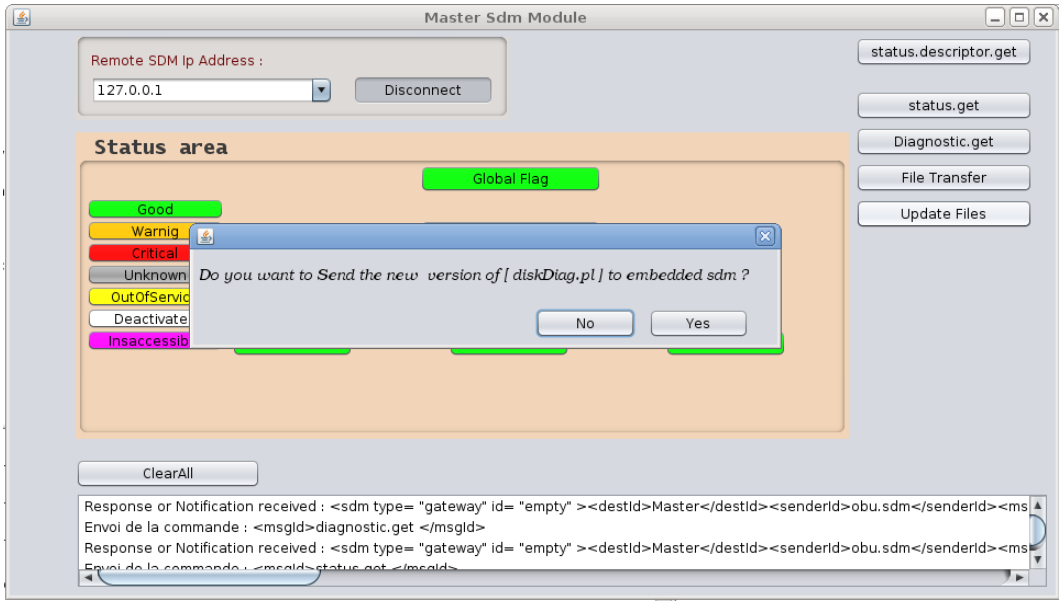


Figure 4-19: Send New Self-Diagnostic Rules to M2M Device

4.4.3 Wrap Up

The following table summarizes the achievements and performance results of the self-diagnostic sub-testbed.

Table 4-4: Summary of testbed 3.2

Scenarios	Technical Requirements	Achievements	Performance Results
Root failure cause detection	DV.2 Reliable M2M equipment	Based on a pre-defined set of rules, the M2M device is able to locate the root failure cause of one of its components.	K54 – Frequency of queries: One query per diagnosed component. When the component under diagnosis is the M2M Device itself, then one single query is to necessary.
Assisted self-healing	NT.12 Self-diagnostic and self-healing operation	It is possible to inject new self-healing rules inside the M2M device from the Master Sdm interface.	

4.5 Sub-testbed 3.3: Secure Element Device Management

The aim of the sub-testbed is to provision an end device by setting a Group key into the Secure Element (SE) associated to a new non LTE-M device deployed in an existing capillary network. The infrastructure of the sub-testbed 2.4 is also used here but this sub-testbed showcases how a device protected by a SE can actually bootstrap its security. After this Group Key setting operation this new device can be started and secure messages are sent to the M2M server as it is described in the sub-testbed 2.4.

A Group Key enables a group of devices to share the same key to enable secure communication. This Group Key can be used either to communicate between devices or between a device and the M2M server to provide End-to-End security. In the use-case described in the sub-testbed 2.4 this Group Key is used to protect the integrity of application payloads send by devices to the M2M server by adding a Crypto Message Authentication Code (crypto-MAC).

Pairing has been done offline which means that each new device has already been associated to its SE: the database of the server already contains the association between the device ID and the SE ID and the SE itself contains the device ID. The way to replace the Factory key by the Group key has been specified in the section 8.8.2 of the D4.3-Device Management document [16]. This SE Management sub-testbed implements the specified handshake. Taking into account the fact that the Factory Key is prepared offline (i.e. before the deployment of the device) the Group key setting algorithm is protected against the Man-In-The-Middle (MITM) attack because there is already a shared secret between the device and the server.

The principle of the protocol is first to set a shared session key and then to send the Group Key to the device protected by this session key. The session key setting is protected by the Factory key.

The first iteration of the communication protocol implemented in summer 2012 between server and devices was very verbose and provided only integrity of the messages as protection. In the second iteration of the protocol these issues have been addressed by introducing a protocol version to manage the various releases, the message size has been optimized with the use of a long to encode the device ID, and the security specification of the message has been standardized with the ability to support 4 types of message:

- Clear message: no cryptography used
- Crypto-MAC only
- Encrypted only
- Encrypted and Crypto-MAC

The important data to be transmitted is the reference of the used key. This data is encoded using a single byte. A circular buffer is used for replacing the reference of the oldest key by the newest one. The key reference is still transported over SMS and HTTP, so it is required to encode the message using base64 encoding rules.

A message is transported by a protocol that contains the following fields:

- Device ID
- Protocol Version
- Type of message
- Key reference
- Data length
- Encrypted/clear data
- MAC (optional)

The reasons of using symmetric keys rather than asymmetric key are to reduce both the energy consumption on the device and to optimize the volume of credentials managed by the database on the server side. Asymmetric cryptography is much slower than symmetric cryptography and then consumes more energy which is a limited resource on a device.

4.5.1 Performance Measures

This sub-testbed has been implemented with the first release of the SE. Support of the final release of the SE by the end device is not finished yet. This final SE release optimizes the energy consumption. Full evaluation of the sub-testbed cannot be done at the present time. The late availability of the final SE and the effort put in the scaffolding to validate the sub-testbed 2.4 has prevented to finish the work before the delivery of this document. Remaining work on the device application to adapt to the final SE will be done before the final review of the project.

Although this sub-testbed is different from the sub-testbed 2.4 the same SE is used in the same way with the same type of key even if the purpose is different. The figures given in the section 0 are also applicable for this sub-testbed regarding the K46 KPI that deals with the computational energy consumption. Main difference is on the frequency: Group keys are distributed and updated from time to time while application payloads are continuously sent to the M2M server.

Still, the main criterion to evaluate the work done in this sub-testbed is the K49 – Flexibility of the security enrolment process for capillary devices. It is not necessary to have the final implementation of the sub-testbed to evaluate the performance of the implementation. This KPI is a combination of both numerical and non-numerical measures.

Two variables have been identified to measure the performance of the sub-testbed:

- The number of the messages required to set the Group key reflects the verbosity of the protocol handshake used. Six messages and responses are required to set the Group key. To be fair, it must be explained again that an initial secret is already shared at the beginning of the handshake, which minimizes this total number of messages.

  For some deployment where it is sure that no eavesdropping attack is possible then the Factory key could be used as a session key to optimize the number of messages which drops to 4 but one must realize that this Factory key could be disclosed and then the overall all security of this group of devices is at risk.

- The processing time and complexity required to deploy a new device is another evaluation criterion. Time processing is tightly related to the size of the capillary network and available bandwidth to communicate with the server. With the early implementation of the sub-testbed using a smart card instead of a SE, the Group key was set in less than a minute.

4.5.2 Evaluation scenario

Accurate measurement of the Group key setting will be made when the device application is fully updated to support the final release of the SE. The ambition is that checking that a new device has been successfully added could be done in less than a minute. It means that the non LTE-M device is integrated in the system and able to be started sending application payloads. This is just an example because most of the time is spend on the end-device which processing capability could change according to the application board select for a business case.

4.5.3 Wrap Up

Achievements and of the sub-testbed are summarized in the following table.

Table 4-5: Summary of sub-testbed 3.3

Scenarios	Technical Requirements	Achievements	Performance Results
Group key setting	NF.1 Scalability and SV.6 Security	Session key securely set through a handshake protocol to enable server to deploy the Group key to a new device in a secure way Ability to process a large number of end-devices with an optimized protocol.	K49 – Flexibility of the security enrolment process for capillary devices : • 6 messages required to set the Group key. • Less than a minute is required for a device to start sending protected application payloads

5. Conclusions

This document concludes the work carried out in WP7, and provides insight in the overall EXALTED contributions to the LTE community. Each testbed was thoroughly tested taking into considerations explicit assumptions and produced separate results. Testbed 1's objective is to demonstrate the generally valid applicability of LTE-M PHY layer solutions GFDM and CDMA-overlay with lab experiments. One focus of the measurements was to verify the coexistence of LTE-M and LTE in the same frequency band. The results show firstly that the performance of the LTE UEs is not affected at all and secondly that the LTE-M signal can be decoded successfully. These findings confirm the theoretical results from WP3 where the original simulations took place. The spectral properties of GFDM were also verified following a second measurement scenario without LTE UEs. Again the theoretical results from WP3 confirmed the original hypothesis.

Testbed 2 is divided into 4 autonomous subtestbeds and their results are discussed below:

Subtestbed 2.1 demonstrates the feasibility of capillary-to-capillary-to-infrastructure IP communications and uses an eHealth application over ITS as a proof of concept. The architecture is connected through an IPv6 networking technology involving two neighbouring M2M gateways where only one is connected to the infrastructure. The leaf M2M Gateway relies on its neighbour for accessing the M2M services provided by the M2M application domain. The key features tested and found to perform according to the original hypotheses were: Scalability, by addressing as many devices as possible and on the other side by supporting the requests of neighbouring M2M gateways, heterogeneity, by supporting at least two types of wireless technologies, E2E IPv6 connectivity by supporting bi-directional communications and finally mobility as part of an ITS scenario.

Subtestbed 2.2 covers the following aspects: data scaling, data aggregation, reliability, and transmission payload reduction. New algorithms have been implemented covering adaptive data scaling, weighted fair aggregation, and forecheck aggregate approximation. The new intelligent gateway proposed tested in a heterogeneity and interoperability scenario it is found to adaptively adjust different offset and amplitudes as measured from real sensors, to reduce complexity in both dimensionality and numerosity. Additionally it provides reliability by intelligently detecting wrong data reported from faulty device and prevents those data from being considered in the aggregation algorithm while preserving good accuracy level with significant complexity reduction and processing speed improvement.

Subtestbed 2.3 demonstrated end to end connectivity in a heterogeneity and interoperability scenario while addressing in parallel the address translation mechanisms developed. The results showed that it addressed the maximum number of devices behind a M2M Gateway with the lightest overhead possible while it was possible to implement several applications on the same devices. It supports different radio interfaces and multi-hop transmissions, in terms of energy consumption this can be limited by using half duplex schemes. Finally it can deliver the message without compromising raw data at any point.

Subtestbed 2.4 demonstrated end to end security with a special Security Element (SE) designed in order to be produced and operated at low cost and with low-energy consumption. The evaluation assumption used was to consider both SE management policies, either stand-by or switched between 2 processing cycles for testing in order to verify the low computational energy consumption.

Testbed 3 albeit the fact that it consists of 3 autonomous subtestbeds only the two of them have produced at the time being concrete results while the third (Security element device management) is still under evaluation.

Subtestbed 3.1 demonstrates that the technical requirements set can be addressed by the ELFOMA DM solution. Functional achievements can be demonstrated by covering an energy consumption peak controlling function.

Subtestbed 3.2 covers self-diagnostics and self-healing operations under the scenarios of route failure cause detection and assisted self-healing. It was found that based on a pre-defined set of rules, the M2M device is able to locate the root failure cause of one of its components. It is also possible to inject new self-healing rules inside the M2M device from the Master Sdm interface.

Overall the testbeds and their respective subtestbeds, covering the majority of technical requirements and objectives of the EXALTED project showed more than adequate performance when compared against the theoretical expectations as these were formed in the previous deliverables of WP7.

A. Annex

A.1. Subtestbed 2.5: Compressed sensing for capillary networks

In this section, we will provide the description and evaluation of a new subtestbed in the EXALTED project. This new subtestbed was not planned and therefore has not been included in previous deliverables. The rationale behind this is that this subtestbed stands on a recent breakthrough on data acquisition [17], and the idea of applying these new results to reduce traffic load at capillary networks arose during the last phase of the project.

Typically, in the SMM and e-Health use cases the signals being monitored at the non-LTE-M devices (sensors) are highly compressible. Consider that a sensor collects $\mathbf{x}$ of length N, thus, the vector $\mathbf{x}$ is said to be compressible if can be projected into L suitable basis with $L << N$ and, still, most of the information is retained.

Therefore, in order to compress the signal $\mathbf{x}$, one first needs to identify the appropriate basis which exclusively depend on the signal structure [17]. Given the basis, the compression methods can be categorized in two main groups: adaptive and non-adaptive. In adaptive methods, the sensor exploits the signal structure and selects the best L orthogonal projections of $\mathbf{x}$, in the sequel denoted by $\mathbf{y}$. Then, in order to reconstruct the original signal $\mathbf{x}$, the sensor not only must inform the GW about $\mathbf{y}$ but also about what projections have been used during compression. On the contrary, in non-adaptive compression, the sensor does not leverage the signal structure to compress $\mathbf{x}$. Recent results on compressed sensing (CS) theory have shown that by merely projecting the signal $\mathbf{x}$ into a sufficiently large number of incoherent (random) projections L but still with $L << N$, there exist feasible algorithms that can recover $\mathbf{x}$ accurately [17].

Bearing all the above in mind, Sub-testbed 2.5 implements a non-adaptive CS algorithm aimed at reducing traffic congestion at the capillary network.

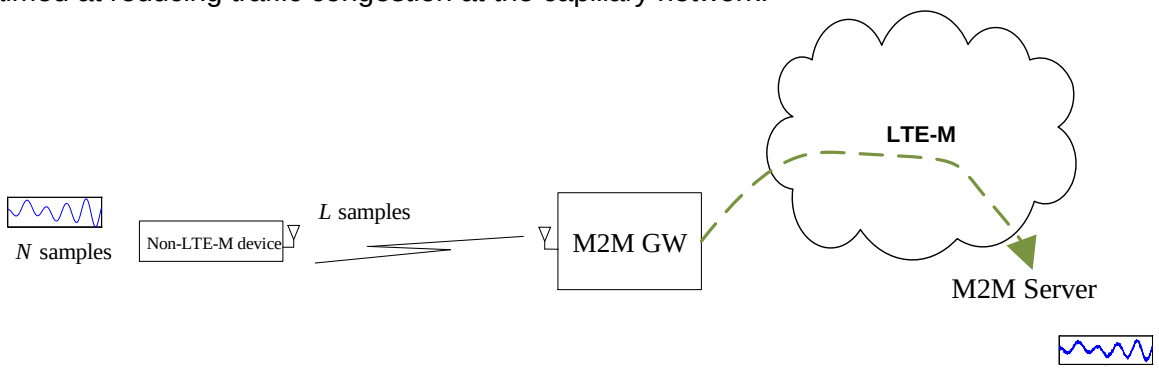


Figure A-1. Sub-testbed 2.4 description

As shown in Figure A-1, Sub-testbed 2.5 is composed of three elements: A sensor node (TSmoTe), an M2M GW (TSgaTe) and the M2M server. The sensor node takes samples of a phenomenon of interest that are stored in memory. Next, each block of N samples, denoted by the length-N vector $\mathbf{x}$, is projected on L Rademacher vectors, that is, $\mathbf{y} = \mathbf{A}\mathbf{x}$, where $\mathbf{A}$ is a $L \times N$ matrix whose entries $[\mathbf{A}]_{i,j} = \pm 1/2$ with probability ½. It is worth noting that this method is appealing in terms of complexity and memory requirements, since sensor nodes merely implement a linear transformation of the data. Next, the compressed signal $\mathbf{y}$ is transmitted to the M2M GW.

Depending on the use case, either the M2M GW sends the information to the application server for decompression or recovers $\mathbf{x}$ by itself. To decompress the information, the destination needs to know the basis in which the signal is compressible. To that end, it has been observed empirically that Haar basis are good candidates for the type of signals that have been measured. Regarding the algorithm to decompress the $\mathbf{x}$, we resort to the so-called orthogonal matching pursuit (OMP) (for further information the interested reader is referred to [18]). To ease the integration on the TST platform, the OMP algorithm has been efficiently implemented in standard C code.

A.1.1. Performance measures

Sub-testbed 2.5 has been evaluated according to the following KPIs:

- **K32** Actual Payload size: The algorithm is able to take as input N samples (where N must be a power of 2) and reduce it to L samples, being $L \approx K \cdot \log\left(\frac{N}{K}\right)$, and K stands for the approximate number of Haar coefficients that carry most of the information about the data. The tested setup corresponds with up to 64 samples, what implies L=42 coefficients on the compressed signal. This way, the payload reduction is 34.37%.

- **K41** Distortion: This indicator varies highly depending on the use case selected. There are signals that are more suitable to be compressed than others. Slow varying signals present less distortion when decompressed than other 'bursty' ones. For this reason, it has been obtained Mean Square Error (MSE) values around 10^{-2} when compressing solar panel samples during several days or MSE values around 10^{-6} if temperature is measured every minute.

- **K47** Radio energy consumption: Considering the average radio and microcontroller usage for typical transmission operations (250Kbps bitrate), and level 0 power profile
  - With N=64 original samples it is needed to use the radio during 2,05 ms, which translates into 0.725W per message (or 2.9 µJoules per bit transmitted).
  - With L=42 compressed samples it is needed to use the radio during 1.34 ms, which translates into 0.677W per message (or 2.6 µJoules per bit transmitted).

A.1.2. Verification Procedures

The verification procedure has followed these steps:

The first goal was to determine whether the algorithm is suitable to be tested with real data. In order to prove this assumption, real data coming from a solar panel measurement over several days was introduced in the C code. Figure A-2. shows the original signal and its reconstruction from a compressed version with a payload reduction of the order of 35 %. The average distortion in the reconstruction (MSE) is depicted in Figure A-3. Clearly, the lower the level of compression (which corresponds to large values of L) the better the accuracy.

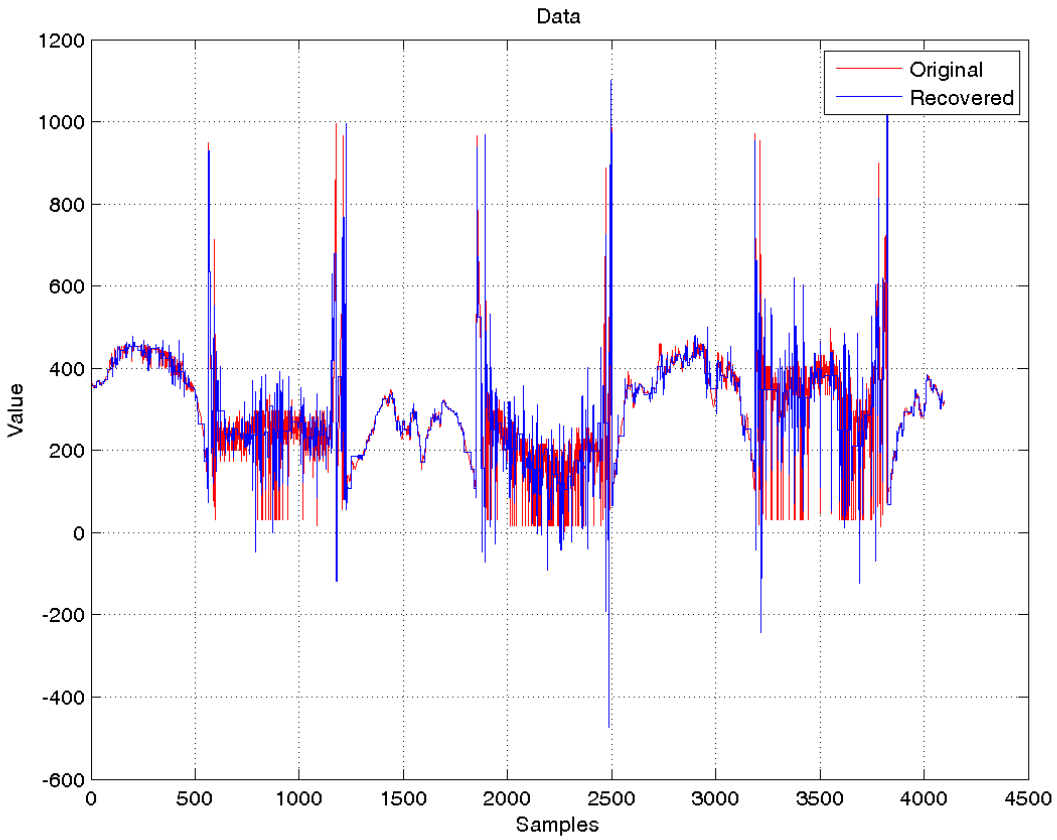


Figure A-2.. Solar panel samples (L=40)

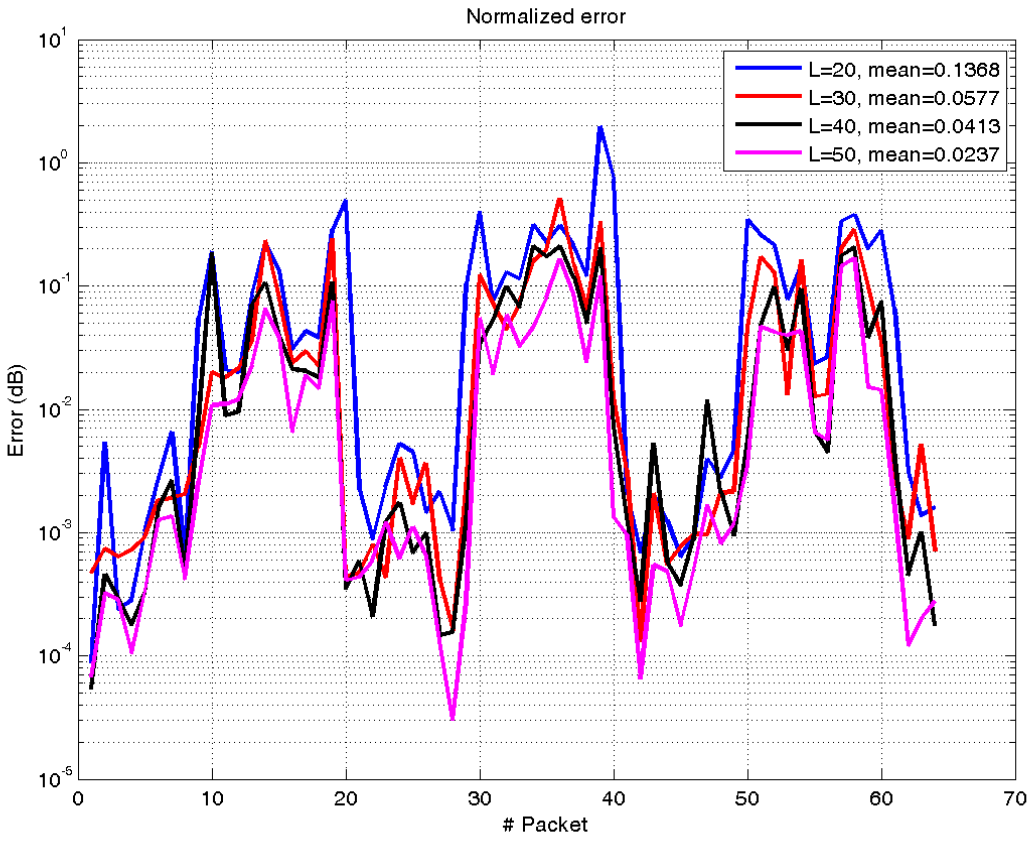


Figure A-3. Average Distortion (Normalized MSE per packet)

- Once determined the suitability of real data, the verification was continued programming the code into real M2M devices. The base signal to be measured is, in this case, the one extracted from a thermometer sampling with different periodicities. Due to restrictions in terms of available memory derived from the use of this kind of hardware, in a first approach, nodes are able to compress up to 64 samples, but gateways are only allowed to decompress up to 16, so two alternatives where studied:

    - **M2M Server reconstructs the signal:** In this case the sensor sends the compressed data to the M2M GW which is in charge of relaying this data to the M2M application where it is finally reconstructed. The compression rate obtained here is 34.37%, as 64 samples are taken and compressed into a 42 coefficient message.
    - **An M2M GW reconstructs the signal:** This is the most challenging case since the M2M GW is typically a device with more limited processing capabilities than the application server. This way the compression is 37,5%.

In all cases the distortion is (in mean) $8*10^{-7}$ when sampling each minute (as you can see in the results box in **Figure A-4**), and a little higher when sampling with less periodicity.

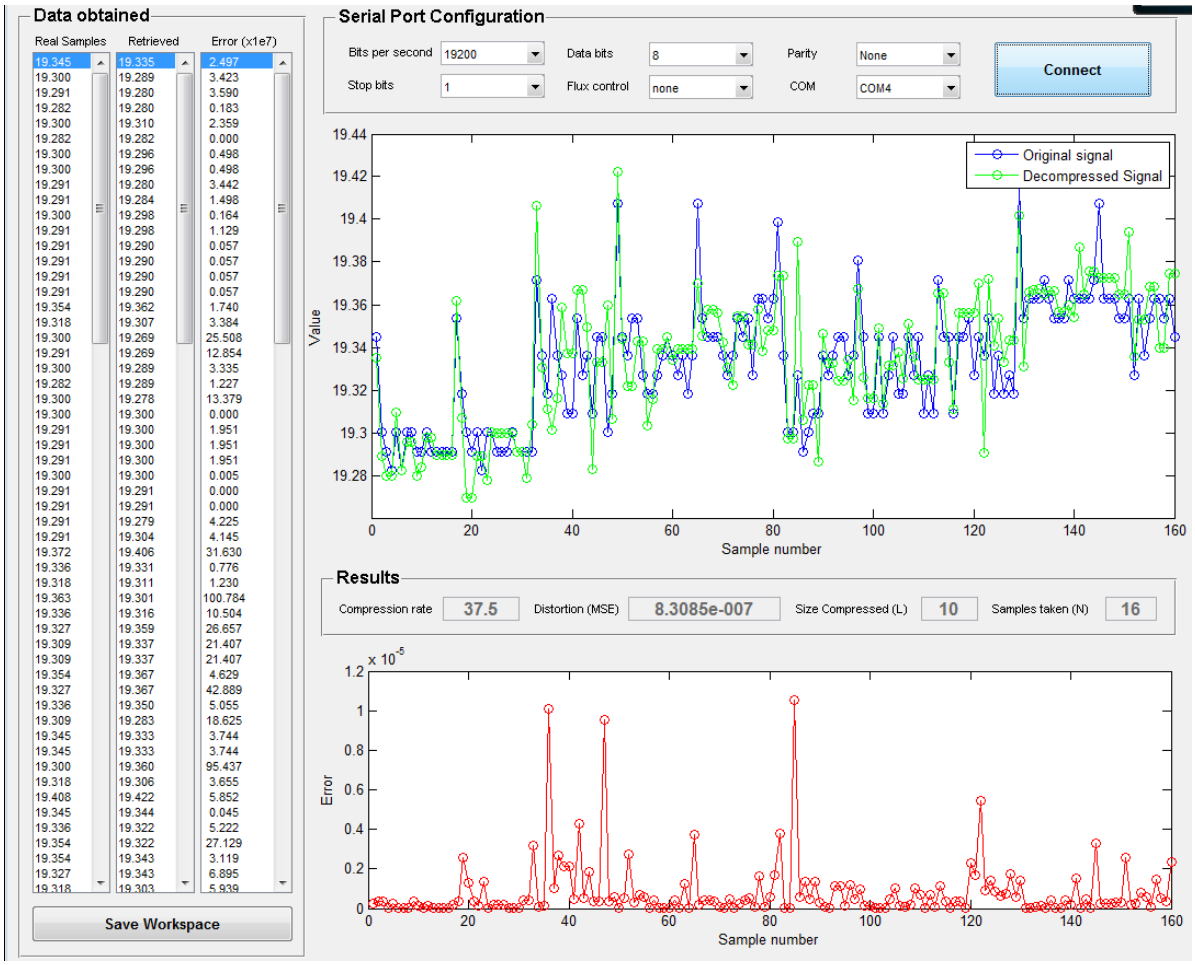


Figure A-4. Results obtained using 10 compressed samples out of 16.

For the final demo, some enhancements are envisaged. Code refinement is a task under development in order to be able to decompress a higher number of samples at the Gateway side. In order to do so, the memory usage has to be optimized to the most.

In addition, other variables will be tested on real devices, aiming to prove the compression on signals presenting more variations than a thermometer. For that purpose, adding a solar panel or an accelerometer to the boards is being evaluated.

A.1.3. Wrap up

The following table summarizes the performance evaluation of this subtestbed. To remark, the payload reduction achieved by Subtestbed 2.5 which entails a reduced traffic load at the capillary network and at the LTE-M network.

Table A.1 Wrap up

Scenario	Objectives	Solutions	KPIs	Evaluation Assumptions
SMM	Traffic aggregation point architectures to support reduced traffic load Energy efficiency	Sub-testbed 2.5 provides means to reduce traffic load at the capillary network. Sub-testbed 2.5 reduces energy consumption at the sensor nodes since no redundant data is sent to the M2M Gateway.	- **K32** Actual Payload size: Payload reduction of 34.37 % - **K41** Distortion 1e-6 for temperature data - **K47** Radio energy consumption: Energy consumption has been reduced around 7%.	- Point-to-point communication between a non-LTE-M device and the M2M Gateway

List of Acronyms

Acronym	Meaning
BB	Baseband
BER	Bit Error Rate
BLER	Block Error Rate
CDMA	Code Division Multiple Access
CoAP	Constrained Application Protocol
Crypto-MAC	Crypto Message Authentication Code
CSV	Comma Separated Values
DM	Device Management
ELFOMA	EXALTED Lightweight DM For OMA-DM v1.x
eNodeB	evolved NodeB
EXI	Efficient XML Interchange
FFT	Fast Fourier Transform
GFDM	Generalized Frequency Division Multiplexing
HaLo	Hardware in the Loop
ITS	Intelligence Transport System
KPI	Key Performance Indicator
LTE	Long Term Evolution
LTE-M	LTE for Machines
M2M	Machine-to-Machine
MSE	Mean Square Error
MTC	Machine Type Communications
OMA-DM	Open Mobile Alliance Device Management
OMP	Orthogonal Matching Pursuit
OOB	Out Of Band
PAPR	Peak-to-Average Power Ratio
PHY	Physical (layer)
PMUSCH	Physical MTC Uplink Shared CHannel
PUSCH	Physical Uplink Shared CHannel
QAM	Quadrature Amplitude Modulation
QoS	Quality-of-Service
QPSK	Quadrature Phase Shift Keying
REST	REpresentational State Transfer
Rx	Receiver
SC-FDMA	Single Carrier Frequency Division Multiple Access
SCME	Spatial Channel Model Extended
SE	Secure Element
SMM	Smart Metering and Monitoring
SNR	Signal-to-Noise power Ratio
TTI	Transmit Time Interval
Tx	Transmit
UART	Universal Asynchronous Receiver Transmitter
UE	User Equipment
WBXML	Wap Binary XML

References

[1] FP7 EXALTED consortium, “D7.2 - Integration of selected algorithms into platforms & interfaces finalization,” project report, Aug. 2012.
[2] FP7 EXALTED consortium “D2.3 – The EXALTED System Architecture”, project report, August 2012
[3] D. S. Baum, J. Salo, G. Del Galdo, M. Milojevic, P. Kyösti, and J. Hansen, “An interim channel model for beyond-3G systems,” in Proc. IEEE VTC’05, Stockholm, Sweden, May 2005.
[4] FP7 EXALTED consortium, “D3.3 – Final report on LTE-M algorithms and procedures,” project report, Jul. 2012.
[5] FP7 EXALTED consortium, “D3.4 – Final LTE-M performance evaluation,” project report, Jan. 2013.
[6] FP7 EXALTED consortium, “D2.1 - Description of baseline reference systems, scenarios, technical requirements & evaluation methodology,” project report, v2.0, Jan. 2012.
[7] FP7 EXALTED consortium “D2.4 – The EXALTED System concept and its performance”, project report, February 2013
[8] A. Kaiser, S. Descremps, and A. Petrescu, “Prefix Delegation extension to Neighbor Discovery protocol”, IETF draft (work in progress), 2012.
[9] iPerf, TCP and UDP bandwidth performance, http://iperf.sourceforge.net/
[10] ETSI TS 102 636-6-1, v1.1.1 (2011-03), “ITS, Vehicular communications, GeoNetworking, Part6: Internet Integration”, 2011.
[11] IETF RFC 3633, “IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6”, 2003.
[12] FP7 EXALTED consortium, “D4.1- M2M Packet Data Protocols between LTE-M and Capillary Networks”, project report, July 2012.
[13] FP7 EXALTED consortium, “D4.2 - IP Networking System for M2M communications for EXALTED use cases”, project report, July 2012 and “D4.2 version 2”, October 2012.
[14] FP7 EXALTED: “D4.3 – Device Management”, project report, October 2012.
[15] EXIfficient, http://exificient.sourceforge.net/
[16] 3GPP TS 23.203 v. 8.8.0, “Policy and charging control architecture,” Dec. 2009.
[17] D. L. Donoho, “Compressed sensing,” IEEE Trans. Inf. Theory, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.
[18] J.A. Tropp, A.C. Gilbert, “Signal recovery from random measurements via orthogonal matching pursuit”, IEEE Trans. Inform. Theory, 53 (12) (2007), pp. 4655–4666
[19] KXML2, http://kxml.sourceforge.net/kxml2/
[20] Wireshark protocol analyzer, http://www.wireshark.org/about.html