European Commission
Information Society and Media

SEVENTH FRAMEWORK PROGRAMME

Large Scale Integrating Project

EXALTED

Expanding LTE for Devices

FP7 Contract Number: 258512

WP4 – End-to-End (E2E) M2M System

D 4.1
M2M Packet Data Protocols between LTE-M and Capillary Networks

Contractual Date of Delivery:	30 June 2012
Actual Date of Delivery:	30 June 2012
Responsible Beneficiary:	TST
Contributing Beneficiaries:	TST, CTTC, UPRC, CEA, EYU, UNIS
Estimated Person Months:	45
Security:	Public
Nature	Deliverable
Version:	1.00

Document Information

Document ID: EXALTED_WP4_D4.1
Version Date: 29 June 2012
Total Number of Pages: 110

Authors

Name	Organisation	Email
Javier Valiño	Tecnologías, Servicios Telemáticos y Sistemas, S.A (TST)	jvalino@tst-sistemas.es
Juan Rico	Tecnologías, Servicios Telemáticos y Sistemas, S.A (TST)	jrico@tst-sistemas.es
David Garcés	Tecnologías, Servicios Telemáticos y Sistemas, S.A (TST)	dgarces@tst-sistemas.es
Petros Bithas	University of Piraeus (UPRC)	pbithas@unipi.gr
Athanasios Lioumpas	University of Piraeus (UPRC)	lioumpas@unipi.gr
Jesús Alonso-Zárate	Centre Tecnològic de Telecomunicacions de Catalunya (CTTC)	jesus.alonso@cttc.es
Tatjana Predojev	Centre Tecnològic de Telecomunicacions de Catalunya (CTTC)	tatjana.predojev@cttc.es
Cédric Abgrall	Commissariat à l'Energie Atomique et aux Energies Alternatives (CEA)	cedric.abgrall@cea.fr
Emilio Calvanese Strinati	Commissariat à l'Energie Atomique et aux Energies Alternatives (CEA)	emilio.calvanese-strinati@cea.fr
Nenad Gligorić	Ericsson (EYU)	nenad.gligoric@ericsson.com
Dejan Drajić	Ericsson (EYU)	dejan.drajic@ericsson.com
Bernard Hunt	University of Surrey (UNIS)	bernard.hunt@surrey.ac.uk

Approvals

	Name	Organisation	Date	Visa
Internal Reviewer 1	Nemanja Ognjanovic	TKS	26/06/2012	OK
Internal Reviewer 2	Jesús Alonso-Zárate	CTTC	26/06/2012	OK
Technical Manager	Pirabakaran Navaratnam	UNIS	28/06/2012	OK
Project Manager	Djelal Raouf	SCET	29/06/2012	OK

Executive Summary

This deliverable covers protocol design considerations and proposes protocol stack(s) for ensuring efficient packet data context management for E2E M2M (Machine-to-Machine) communications between heterogeneous networks consisting of capillary (for example Zigbee) and LTE-M networks foreseen in the EXALTED system architecture.

The structure of the document is organized as follows:

Section 1 provides introduction positioning general aspects and considerations regarding “M2M Packet Data Protocols between LTE-M and Capillary Networks”. The main study items are analyzed and a common goal is presented: the definition of a complete protocol stack consisting of novel protocols proposed by EXALTED addressing specific technical issues, as well as suitable existing protocols after a deep study considering all possible options and technical requirements.

Section 2 outlines the previous work related to the definition of M2M packet data protocols between LTE-M and capillary networks. Technical assumptions and requirements identified at the project level, performance evaluation metrics for M2M packet data protocols and how M2M packet data protocols fit onto the EXALTED system architecture are also described under this section.

Section 3 describes in detail the proposed MAC (Medium Access Control) protocols envisaged to deal with efficient packet data management. Maintaining a continuous packet flow in an E2E (end-to-end) M2M scenario requires that the existing MAC protocols for the capillary networks need to be modified in order to support various requirements of M2M applications. Consequently, design of new M2M MAC protocols for capillary networks needs to be based on three important characteristics of M2M systems, namely, high number of devices, energy constraint of devices, and packet congestion that appears near to the sink (i.e. CH or M2M Gateway: nodes receiving data from end devices and in charge of processing/aggregating/retransmitting). Three different but complementary approaches (they exploit different aspects) are proposed, namely Cooperative MAC protocol, Cooperative ARQ and Congestion aware MAC protocol.

Section 4 gathers the research studies carried out in the context of maintaining packet continuity between capillary and LTE-M networks. Device reachability and addressability are addressed by this work for continuous packet data connectivity. In particular, the studies performed are:

- Heterogeneous connectivity aiming to study the impact of using different access technologies and different radio interfaces and also identifying an efficient way of communicating across capillary networks formed by different types of sensors. The key objective of this work is to assure the packet data continuity across heterogeneous networks. In other words, enabling efficient communications across different types of networks foreseen in the EXALTED architecture.
- Mobility management aiming to handle jointly MAC and mobility by designing a cross-layer approach which is aware of the current mobility scenario and adapt the MAC parameters accordingly in order to efficiently handle device mobility.
- Auto IP configuration aiming to assign IP addresses for LTE-M devices and also to M2M devices behind the M2M Gateway.

Section 5 describes payload reduction mechanisms for improving the overall efficiency of the protocol stack. One of the goals of the EXALTED project is to leverage PHY and MAC layer

mechanisms for M2M communications over LTE networks. Efficient PHY/MAC protocols/procedures for M2M capillary networks will provide more efficient handling of a large number of M2M devices. Integration of such a large number of devices with varying characteristics and capabilities is a complex task that requires cross-layer optimization. Thus, the PHY/MAC layer optimizations for M2M networks need to be accompanied by higher layer optimizations such as application protocols oriented on available resources and payload reduction mechanisms in order to achieve overall efficiency. This has been studied in detail in this section.

Finally section 6 concludes the protocol solutions identified in this document, followed by an ANNEX including a complete list of Key Performance Indicators (KPIs) identified at the project level, as some of them are referenced across the document.

Table of Contents

1. Introduction

The design of M2M data exchange protocols between LTE-M and capillary networks is a complex task that involves several topics and is related to several EXALTED objectives. Two most relevant ones are:

1. To maintain connection/transmission integrity across aggregation points through heterogeneous connections,
2. To ensure efficient and consistent IPv6 packet mapping throughout and across the connections in order to obtain the lowest possible IP overhead.

These objectives have a common goal of maintaining packet continuity between capillary and LTE-M networks. To achieve this goal, three major tasks must be performed:

1. Defining new MAC-level protocols for M2M capillary networks,
2. Handling heterogeneous radio access technologies,
3. Managing node mobility.

MAC protocol design is the principal task addressed in this deliverable. Therefore, an entire section (Section 3) is dedicated to the definition of EXALTED MAC protocols, with detailed descriptions of novel MAC protocols that are specifically designed for M2M capillary networks. The central idea is to consider the requirements/constraints and the prospective benefits of the LTE-M system. Existing MAC protocols are not suitable to handle the specific characteristics of M2M traffic, i.e. low data rate and infrequent user traffic, yet high aggregate traffic load on the LTE-M core network, which requires handling a large number of devices and avoiding bursty network congestion.

The protocols proposed in EXALTED address three issues: energy-efficiency, handling a large number of devices, and network congestion. Different use cases of EXALTED have varying properties, which calls for specialised mechanisms for each. Hence, the defined protocols are designed for relevant use cases, and are optimized to work under the corresponding set of assumptions for each use case. With this perspective, three novel and complementary protocols are defined in this document, considering different characteristics of the M2M world: The first one exploits the broadcast nature of the channel to efficiently handle a large number of devices. The second focuses on cooperative ARQ schemes to improve energy-efficiency. The third protocol aims to avoid packet congestions near the gateway.

The second task is related with maintaining E2E (End-to-End) connectivity at the transport level, while using heterogeneous radio access technologies. The goal is to minimize the required overhead and satisfy connectivity, reliability, energy consumption, throughput, and delay requirements. The description of EXALTED's proposal for providing packet data continuity at the transport level is provided in Section 4.1. First, a state-of-the-art study is presented and an overview of different mechanisms that maintain packet continuity at transport level is provided. Then, in an attempt to understand prior studies and test their performance, some proof-of-concept experiments that are conducted in real heterogeneous capillary networks are explained. These experiments focus on specific E2E packet continuity and heterogeneous access issues and provide supporting evidence to the assumptions in studying heterogeneity.

The studies on packet continuity deal with very different aspects, but they pursue a common goal. This goal is translated into the definition, study, and proposal beyond the state of the art of mechanisms defining a complete stack regarding capillary networks. Here, a capillary network is defined as a network that is formed of a large number of devices that

communicate using low-power transmission technologies in order to deliver the information that must be forwarded to the application server they are linked to. Figure 1.1 displays the basic communication stack that comprises the heterogeneity in capillary networks. One of the main objectives of this deliverable is to provide an E2E seamless communication link between both LTE-M devices and non-LTE-M devices and application server located in a public IP address.

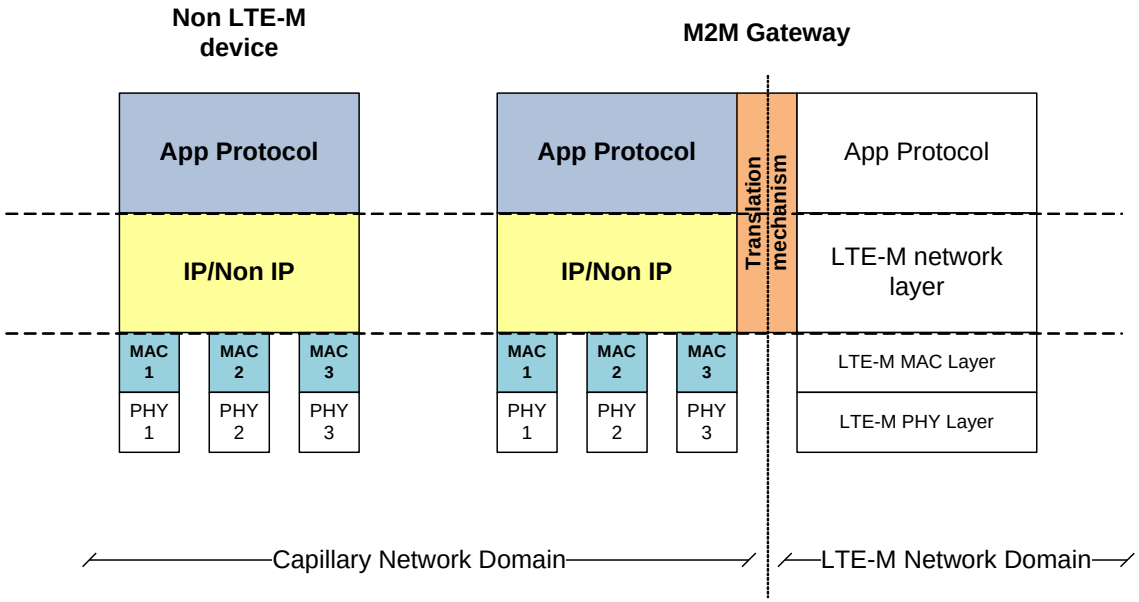

Figure 1.1 Communication stack in capillary networks

In the framework of EXALTED, several solutions have been designed for addressing different requirements imposed by the project's use cases. Their different characteristics have led to the development of specific solutions for each use case. The presented use cases are considered in EXALTED are:

- Intelligent Transport System (ITS): Focuses on mobile vehicles that interact with each other. The critical features are mobility management and delay minimization.
- Smart Metering and Monitoring (SMM): Covers scenarios considering a large number of constrained devices (low power and low-cost) sending low amounts of data. The focus is on optimizing the introduced overhead and assuring energy efficiency.
- E-Health: Considers personal devices communicating sensitive data through a secure channel towards the qualified personnel on hospitals. The important aspects are assuring low failure communications and personal data protection.

As the project aims at developing solutions for low cost and low power devices, it is mandatory to optimize each component of M2M communication for very low rate applications. Based on Figure 1.1 and assuming that each solution focuses on a single use case, the final picture of the communication stack can be presented as shown in Figure 1.2. The figure gathers all possibilities of connectivity, but in real optimized deployments, the devices in capillary networks are supposed to implement only one of the MAC protocols presented, the one that better fits the envisioned application. Coloured blocks represent the components studied in this deliverable. For the MAC level protocols and address translation mechanisms, contributions beyond the state of the art are presented by providing novel algorithms.

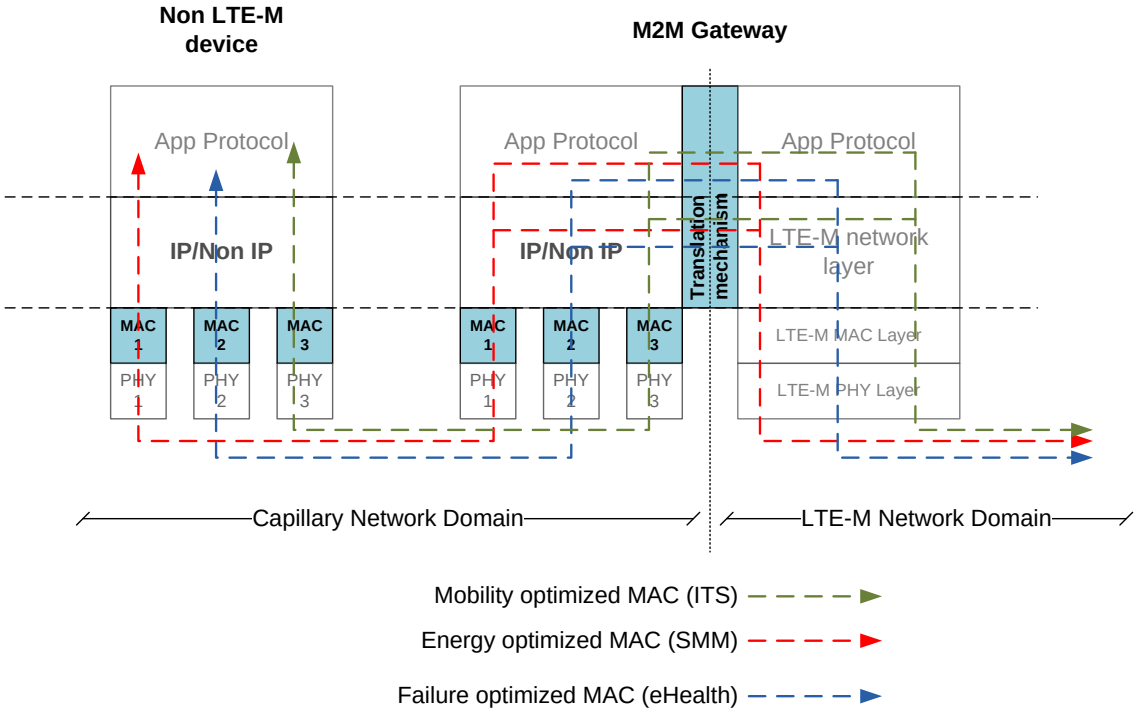

Figure 1.2 Communication stack for E2E connectivity

For network and application level protocols, several studies have been carried out so as to determine which one is the best option to be implemented on M2M devices given the constraints imposed by M2M networks and by the project.

Finally, the third task is related to the mobility of both nodes and sinks. Section 4.2 contains the studied scenarios and the achievements regarding the selection of the most suitable mobility models for M2M constraints. Furthermore, the section aims at positioning the work into the general context of EXALTED:

- Assumptions and requirements have been identified on early stages of the project, trying to set a common background for investigations.
- The defined KPIs and system architecture have been used as a reference for the design of EXALTED's innovations.

Mobility of a single node or a group of nodes is considered in the following mobility scenarios:

- Nodes are static and sinks are mobile.
- Nodes are mobile and sinks are static.
- Both nodes and sinks are mobile.

2. General considerations

On this section, general considerations taken into account for the definition of mechanisms to assure packet continuity between capillary and LTE-M networks are introduced. The goal is to present the basis from which the work described on this deliverable started.

The definition of all techniques presented on next chapters rely on the following critical concepts:

- Assumptions from which the current work started. It was needed to set up a common basis, agreed not only between the partners involved, but from the whole project. They comprise definitions about nodes, applications, management issues and standards.
- Requirements derived from the need of defining the M2M packet data protocols, oriented to influence the common architecture. They focus on which specific features are needed in each part of the system so as to handle the expectations.
- EXALTED high level architecture, and how the envisaged protocols fit into the overall picture agreed at the project level.

2.1 Assumptions

As a starting point, a set of assumptions has been agreed to act as basis for the work that is going to be shown in the next technical sections (Sections 3, 4 and 5). These assumptions are aimed to configure the basic initial common scenario from which all the requirements and system design concepts are referred. They are based on the project objectives and general information about capillary and cellular networks (typical architecture, common protocols, device considerations, etc.).

- There are three different types of entities in LTE-M scenarios:
  - End devices (sensors and actuators); sensor nodes are low-power, low-cost, with limited transmission power and limited computation capabilities; however actuators are resource richer, with higher radio transmission range, better processing capability.
  - Gateway nodes, in charge of managing capillary networks, populated by end devices, providing connectivity between nodes within capillary and LTE/LTE-A/LTE-M networks.
  - LTE/LTE-A/LTE-M core network elements.
- The number of sensor nodes is higher than the number of actuators.
- All nodes are reachable through their identifier (IP address, MAC address, IMSI, etc.).

For specific assumptions about elements in the project's architecture, some grouping has been done in order to make a more comprehensive document: they have been merged regarding areas of application:

- **End Devices**, Listed in section 2.1.1.
- **Non-device related issues**. Gathered in section 2.1.2
- **Application-specific.** Proposed in section 2.1.3

2.1.1 End devices

The behaviour of end devices (sensors and actuators) in the EXALTED project will be fully depicted by a set of requirements (these requirements are listed in section 2.2). The following assumptions are made prior to the definition of the requirements:

- Nodes (sensors and actuators) can be uniquely identified by a unique address. The addressing scheme will be dependent on the device itself, the application and the IP capability. All of them execute a very basic MAC centric protocol.
- All devices included in a capillary network can keep communication in ad-hoc as well as in infrastructure mode and in both peer-to-peer and multi-hop fashion.
- There are two main groups of devices. On the one hand the ones often called "M2M modules", including at least one SIM (Subscriber Identity Module) based LTE-M interface, together with other computing and communication needs. On the other hand, capillary networks will be populated by devices using other radio access technologies, such as ZigBee or IEEE802.15.4.
- A routing system natively supporting mobility is possible, presumably using a different addressing mechanism than that of Internet (IP). This M2M routing system may be built to satisfy particular requirements of M2M.

2.1.2 Non-device related issues

The assumptions made at network level will cover generic aspects regarding service provisioning and seamless connectivity to all elements which intend to connect to an LTE/LTE-A/LTE-M network. They can be summarised as follows.

- Nodes within LTE network will be mobile and the network is capable of managing that mobility. In order to accomplish it the handover mechanisms are defined, providing intra LTE handover and also between different LTE networks.
- Network operator includes a security layer which defines the set of security functions allowing the Device/Gateway to authenticate and securely access to the network. That process will not be carried out by device management operations.
- IP Mobility (a device changing its address) is accommodated by tunnel-based protocols like Mobile IP and/or by all end-node modifying protocols like Shim.

2.1.3 Specific applications

As an extra categorisation for assumptions, the ones derived from the study of use cases made a specific group. As there are plenty of uses cases involved, the list of general assumptions should be done taking into account all the different cases.

It is needed to reach a compromise between the ones actually critical and the optional ones.

The following assumptions will be categorised following the same notation as in [1] for scenarios (ITS (Intelligent Transport System), SMM (Smart Metering and Monitoring) and e-Health).

- **ITS:**
  - Each vehicle is equipped with GPS (Global Position System) receiver to track its position and speed.
  - Each vehicle can communicate directly with base station (single-hop)
  - Vehicle to vehicle communication is also possible in multi-hop fashion.
  - Vehicles can communicate to the base station through a gateway
  - Regarding the in-vehicular communications, a number of addressable devices are deployed in one vehicle and are reachable for data transmission.
  - When referring to overall vehicular communications, vehicles move independently, over large geographical areas and are equipped with

communication devices to exchange data between themselves and the Internet.

- The number of devices involved is relatively large. As such, the addressability assumption should express the fact that the address space should be large enough to accommodate vehicular communications at a worldwide scale: a very large number of very small devices geographically distributed on continents.

- **SMM**
  - Devices autonomy. The devices will not be handled by humans, so they will be capable of self connecting and autonomous actuations.
  - Mesh networking. This kind of scenarios are characterised by a number of devices in limited areas, so mesh networking solutions should be taken into account.

- **E-Health**
  - Data integrity and security. Due to the kind of information this application will handle, it is assumed that communication must not be corrupted.
  - Real-Time. Due to the need of quick action in case of alarm, it is assumed that communications will be established in real time.
  - High mobility nodes. The devices involved in these networks are not static, so it is necessary to consider mobility in M2M e-health communications.

2.2 Requirements

This section proposes a list of requirements related to M2M Packet Data Protocols operating between LTE-M and capillary networks (explained in Table 2-1). Requirements are sorted by categories according to their nature and then the requirement is identified according to the common notation:

- **NEEDED** means that the requirement is unavoidable in order to reach the main goal. On the other hand, if the requirement is not needed, it will be marked as **IRRELEVANT**.
- **POSSIBLE** indicates that it would be interesting having this particular requirement, but it is not mandatory.
- On quantifiable parameters, estimation is given, trying to be as accurate as possible.

Table 2-1. General Requirements

Category	Description	Requirements	
Deployment architecture	This group covers different topologies and how data is exchanged through them, within capillary network and also the relation with the gateway. There are many possibilities, in topologies (mainly ring, mesh, star and combinations of them) as well as in communication mode among nodes that belong to such networks.	Device-to-device communication	NEEDED
		Infrastructure-to-device communication and vice versa	NEEDED
		Hybrid architecture, devices-to-cluster head	POSSIBLE
		Cluster head -to-infrastructure	POSSIBLE
		Multi-hop	NEEDED
		Network type (Mesh, Star, bus…)	IRRELEVANT
		Communications with devices behind a M2M gateway	ADVISED
Transmission mode	Depending on radio channel capabilities used by nodes for establishing communication, three different set of requirements can be set. Each mode supposes different characteristics in terms of available bandwidth, and power consumption.	Simplex	NEEDED
		Half-duplex	NEEDED
		Full-duplex	POSSIBLE
Communication type	The messages sent and communication links could be set in different manners depending on communication infrastructure and network implementation over nodes in capillary network. This group exposes the possibilities that the capillary network should offer to their members.	Peer-to-peer	NEEDED
		Unicast	NEEDED
		Multicast	NEEDED
		End to end communication	NEEDED
		Broadcast	NEEDED
Network partitioning	Depending on network size, in number of nodes and in terms of area covered, the network could be divided into smaller sectors, clusters, which improve the network behaviour	Clustering	POSSIBLE
		Cluster-head selection	POSSIBLE

	in all aspects. This partitioning scheme allows devices to reduce power consumption and increase network efficiency.		
Devices' transmission range	Parameters associated to this group show the needs in terms of proximity of the nodes between themselves and between them and the gateway. The range of communications could be from less than a few meters to more than hundreds, depending on the scenario, output power and physical characteristics of the implemented antennas.	Short Range (<1m)	NEEDED
		Medium Range (<100m)	NEEDED
		Large Range (>100m)	NEEDED
MAC cooperation	This set of requirements express the possibility of sharing MAC interface between different technologies, (6LoWPAN and ZigBee are both based on IEEE 802.15.4) or implement more than one in single devices or in the gateway.	Homogenous MAC cooperation (one distinct MAC)	IRRELEVANT
		Heterogeneous MAC cooperation (from different systems)	IRRELEVANT
Device capabilities	Under this categorisation, the hardware and standard-dependant parameters will be studied, **such as the power consumption,** frequency/bandwidth used or transmission delay.	Power consumption	LOW
		Bandwidth usage	NARROWBAND
		Delay	REAL TIME
Gateway	It is one of the most critical parameters on the network as well as one of the most scenario-dependant devices. This section also takes into account the number and capabilities of the Gateway's MAC interfaces available as well as internal process features.	Address translation (between LTE-M and capillary network)	NEEDED
		Maximum supported devices (Scalability)	HIGH
		Power consumption (Batteries or plugged)	PLUGGED unless all nodes are low powered
		MAC interfaces	POSSIBLE
Mobility	The mobility is studied from the MAC point of view, trying to solve the problem regarding mobile nodes and/or sinks, as well as the single user and group mobility issue.	Self-organised network	NEEDED
		Routing protocols	NEEDED
		Single user mobility	NEEDED
		Model tracking and recognition	NEEDED
		Group mobility	NEEDED
		Nodes are static and sinks are mobile	NEEDED
		Nodes are mobile and sinks are static	NEEDED
		Both nodes and sinks are mobile	NEEDED
		Adaptive mechanisms and parameters for Mobility Management	NEEDED
		Setting of the frequency of location updates performed by the MTC device	NEEDED
		Delay of mobility model recognition and tracking, period of update	Smaller than channel time coherence
Addressing scheme	It differentiates the capillary network regarding the MAC protocol used and the network layer deployed in each device.	IEEE (ZigBee, DASH7,…)	POSSIBLE
		IP	POSSIBLE
		Abstraction of the underlying network	ADVISED

		structure, including any network addressing mechanism used	
		Access to M2M devices and M2M gateways with their respective name	ADVISED
		Support of more than one naming scheme	ADVISED
		Identification of Connected Objects (CO) or groups of CO by their name, temporary ID, pseudonym, location or combination thereof	ADVISED
		Reuse of names for certain classes of devises for devices operating in certain environments	ADVISED
		Flexible addressing schemes, including IP address of CO, IP address of groups of Cos, E.164 addresses of CO	NEEDED
Security	Security aspects are shown, in an effort to gather to other tasks on WP 4. Simple guidelines are given for the security needed at MAC, network and Application level.	MAC level	AES128
		Network level	POSSIBLE
		Application level	POSSIBLE
Subscription, identification	Some requirements to identify Machine-Type Communication (MTC) devices within the network.	Number of identifiers to cater	At least 2 orders of magnitude higher than for human-to-human communications
		Providing of packet switched subscriptions with our without assigning an MSISDN	NEEDED
		Remote MTC Device triggering with or without assigning an MSISDN	NEEDED
		Remote MTC Device configuration without the use of an MSISDN	NEEDED
Reliable mechanisms, applications and services	List of some services that must be adopted to ensure reliable MTC between nodes.	Network mechanism to broadcast to a MTC group	NEEDED
		Reliable delivery of a message	NEEDED
		Notification of any failure to deliver the message	NEEDED
		Seamless mobility and roaming if supported by the underlying network	NEEDED
		Assurance of communications integrity	NEEDED
		Use of QoS capabilities of the underlying network	ADVISED
Heterogeneity	List of some heterogeneous features between nodes that must be considered in the network.	Support of asymmetric flows for M2M devices and M2M gateways	ADVISED
		Static or mobiles nodes and sinks	NEEDED
		Presence of anchor nodes	NEEDED
		Radio link features (TX power, etc.)	NEEDED
		Source and kind of traffics (constant bit rate, burst, etc.)	NEEDED
		Density of nodes in different environments	NEEDED
Miscellaneous	Optional issues.	Cognitive radio	POSSIBLE
		Interference management	POSSIBLE

The previous table depicts the needs and assumptions for the underlying infrastructure needed to basis the technical work. After some refinement, they are translated into technical requirements (stated in [1]).

Table 2-2 relates the technical requirements identified as relevant for assuring packet continuity between capillary and LTE-M networks and the approaches proposed in this document.

Table 2-2: Technical requirements.

ID	Title	Priority	Algorithm dealing with it
FU.1	Support of large number of devices	Mandatory	Heterogeneous connectivity, MAC Protocol for capillary M2M multi-hop networks, DPCF (MAC Protocol for high number of devices), Analysis of IP address assignment, State of the art M2M protocols
FU.3	Support for diverse M2M services	Mandatory	Heterogeneous connectivity
FU.6	Unique identity for devices	Mandatory	Heterogeneous connectivity, Analysis of IP address assignment
NT.1	Heterogeneous networks	Mandatory	Heterogeneous connectivity, State of the art M2M protocols
NT.4	Support of multi-hop communication	Medium	Heterogeneous connectivity, MAC Protocol for capillary M2M multi-hop networks
NT.5	Half duplex operation of terminals	Mandatory	Heterogeneous connectivity
NT.6	End to end device to device communication	Mandatory	Heterogeneous connectivity
NT.7	Flexible addressing scheme	Mandatory	Heterogeneous connectivity
NT.8	Mobility management	Mandatory	Mobility models estimator
NT.9	Reliable delivery of a message	High	Cooperative ARQ schemes for capillary networks, Evaluation of data formats over CoAP
NT.11	Traffic Aggregation	Medium	MAC Protocol for capillary M2M multi-hop networks
NT.15	End-to-end session continuity	Mandatory	Heterogeneous connectivity
NT.16	Support for dual stack IPv4/IPv6	Mandatory	Analysis of IP address assignment
NF.1	Scalability	Mandatory	Heterogeneous connectivity, Mobility models estimator
NF.2	Energy efficiency	Mandatory	Cooperative ARQ scheme for capillary networks, State of the art M2M protocols
NF.6	Address space scalability	High	Heterogeneous connectivity
DV.4	Location information	High	Mobility models estimator
DV.5	Location locked M2M equipment	High	Mobility models estimator
SV.1	Overall QoS	Mandatory	MAC Protocol for capillary M2M multi-hop networks

2.3 System concept and high level architecture

The EXALTED system architecture shows the logical topology of the nodes and high level subsystems within the EXALTED system. This allows the system to be divided into a number of domains, according to the ETSI M2M functional architecture. By mapping required functionalities within the system onto the nodes and the interfaces between them a general description of the system operation can be developed.

In order to achieve the EXALTED system concept, proposed specific technology solutions are mapped onto the elements of the architecture, giving a more detailed system description within which the performance of technologies can be estimated.

The system architecture, concept and performance evaluation are major outputs of the EXALTED project, which follow on from the work done on individual aspects of the system, as well as scenarios and requirements. As such, they will be finalised and presented towards the end of the project. This section presents a subset of the *working status* of these aspects to provide the interested reader with some context for the technical work presented within this deliverable. However, it should be noted that this work is not yet complete, and details may also be subject to change. The actual EXALTED system architecture and concept shall be presented in [2] and [3].

2.3.1 EXALTED system architecture and devices

Figure 2.1 shows the high level architecture of the EXALTED system. A number of application servers and management servers may use a combination of IP based networks and LTE / LTE-M networks to reach individual M2M devices, or capillary networks containing one of more M2M devices.

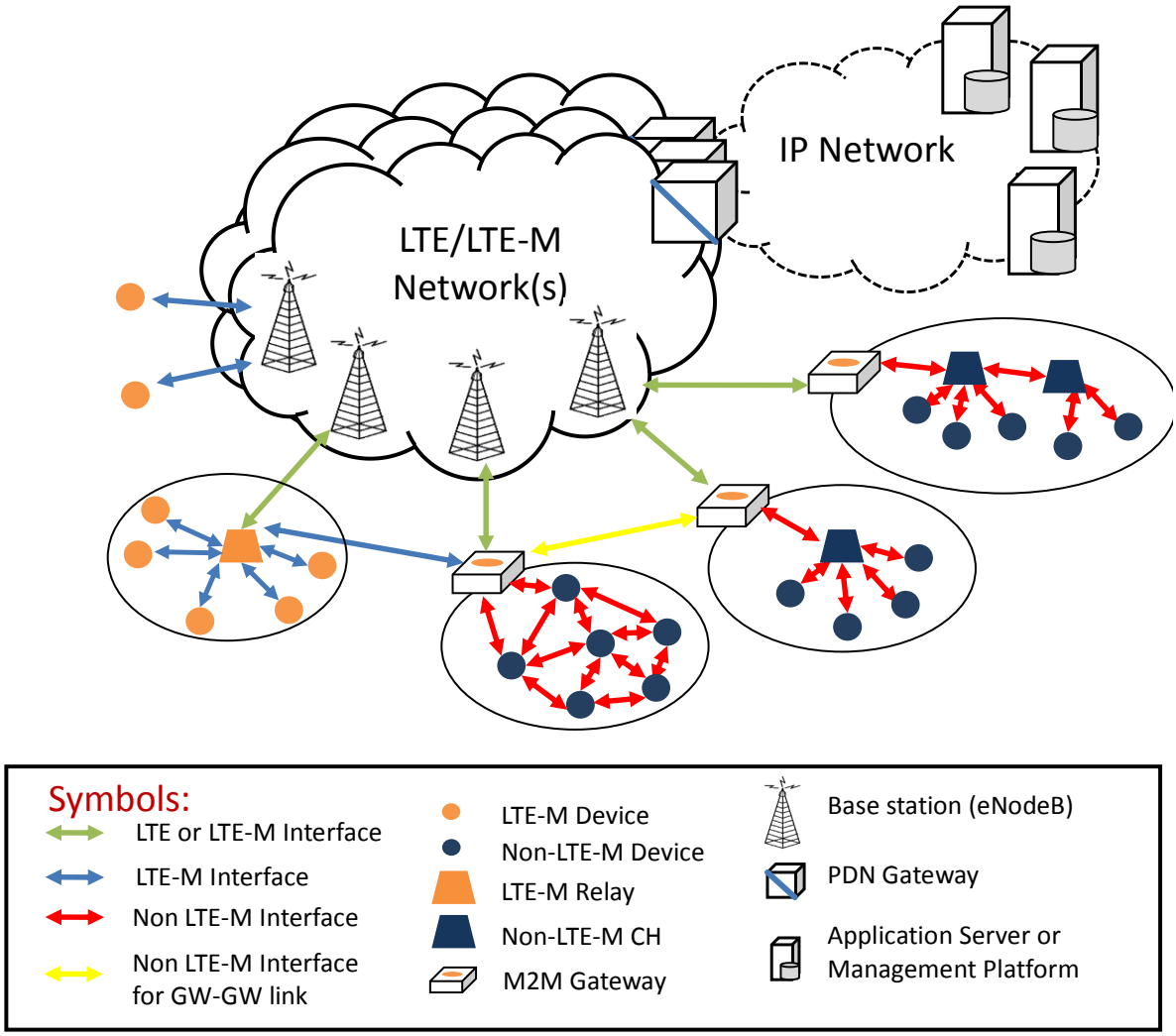

Figure 2.1: EXALTED system architecture.

By adopting the ETSI M2M functional architecture, the EXALTED system architecture consists of the following domains:

- The **M2M Device Domain (DD)** involves those devices that support one or more M2M applications, by connecting them to Application Servers through the Network domain.
- The **M2M Network Domain (ND)** is the access and transport network that provides the interconnection of an M2M device or Gateway to Application Servers.

The ND also includes the Network Management functions and the M2M Device Management functions. The Device and Network domains are shown in Figure 2.2.

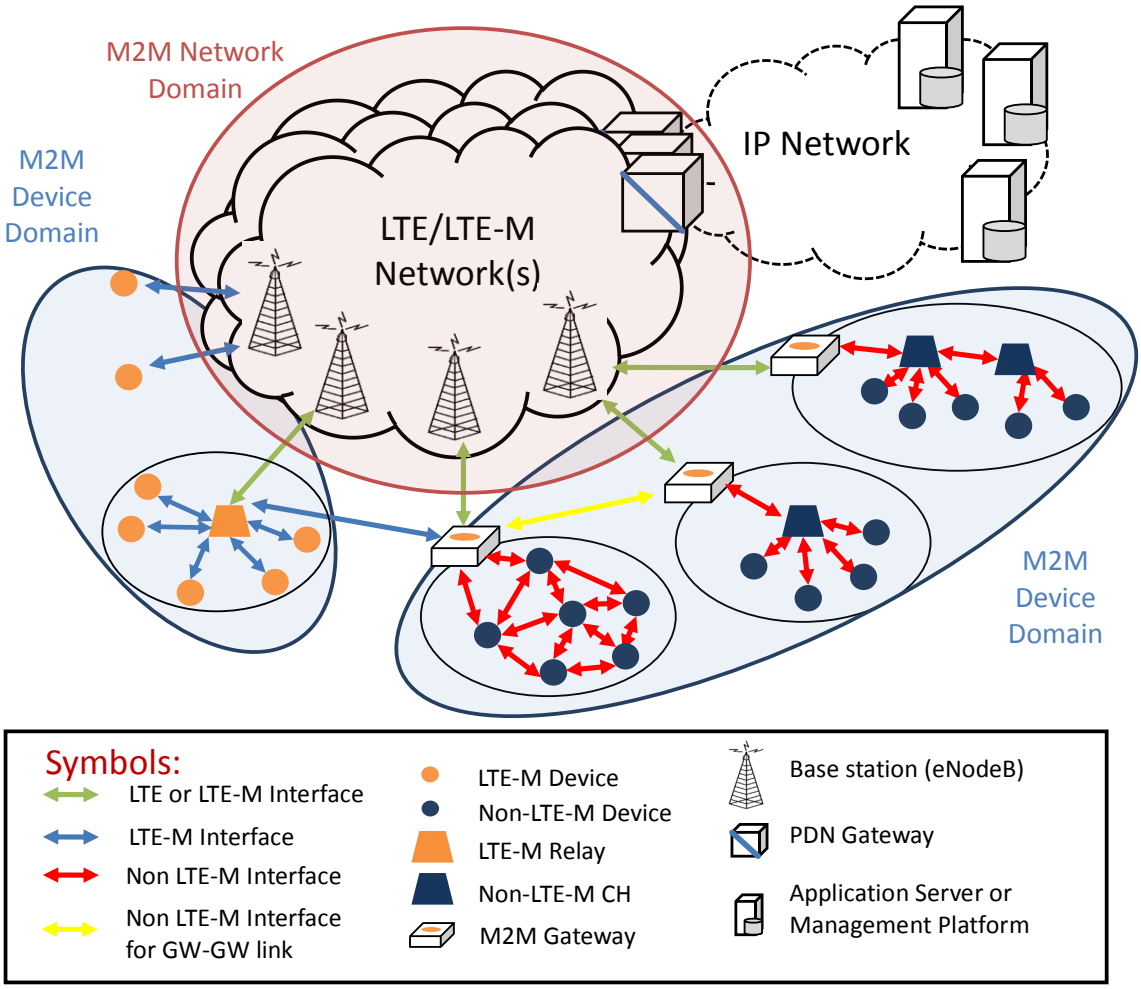

Figure 2.2: M2M Network and Device Domains within the EXALTED architecture.

Within the EXALTED system architecture, the following devices are defined within the **M2M Device Domain**:

A. **M2M Gateway** (GW): provides the interconnection between the LTE-X (i.e. LTE/LTE-A/LTE-M) network and the capillary networks (consisting of one or more non-LTE-M devices). It can provide various functionalities, such as protocol translation, routing, resource management, device management, data aggregation, etc. In some cases, the Gateway may also act as an application server providing M2M services locally in the capillary network. It is expected that the M2M Gateway will normally connect to the LTE-X network with a direct radio link. In the case that an M2M Gateway is unable to establish direct connectivity (for example, due to deployment in a remote area without coverage, or due to localised infrastructure failure) connectivity to the LTE-X network may be achieved by hopping via an LTE-M Relay and/or one or more other M2M Gateways. The availability of direct M2M Gateway to M2M Gateway links will depend on the capillary radio network interfaces supported within the Gateways. LTE-M will not support such links. Direct M2M Gateway to M2M Gateway connectivity for the purpose of E2E device to device connection without any LTE-X involvement (e.g. local breakout) is not the primary focus of EXALTED.

B. **M2M Devices**: devices that can support one or more M2M applications. They are categorised into:

- **LTE-M Devices**: they have LTE-M interface and can connect to the network domain, either by directly accessing the LTE-M network (LTE-M capable eNodeB), or through an LTE-M Relay.
- **Non-LTE-M Devices**: they do not have LTE-M interface, but form capillary network(s) using other network access technologies, such as Zigbee, and IEEE 802.11x. They can connect to the network domain through a M2M Gateway, and run M2M applications locally.

C. **LTE-M Relay**: These elements are similar to 3GPP rel.10 LTE-A Relays. They are used in the LTE-M environment primarily for coverage extension and traffic aggregation. They form a capillary network with LTE-M Devices, which use LTE-M Relays for communication with the rest of the network. Both transparent and non-transparent Relays are supported within 3GPP.

D. **Non-LTE-M Cluster Heads** (CHs): They can be considered as more powerful M2M Devices with some additional capabilities, or as M2M Gateways with reduced functionality. Like regular M2M Devices, they are also part of capillary networks and the communication from a regular M2M Device may be directed through and managed by a CH. The functionalities of a CH may include data aggregation, device management, routing, etc. Unlike an M2M Gateway, a CH will not perform protocol translation.

2.3.2 Communication types within the EXALTED architecture

Figure 2.3 and Figure 2.4 show examples of the different types of E2E communication paths possible between end devices and application servers / management platforms, and between different end devices. When considering the different communication paths available, the key role of the Gateway and the importance of technologies addressing issues such as funneling / traffic aggregation, address translation and mobility management for capillary networks should become clear.

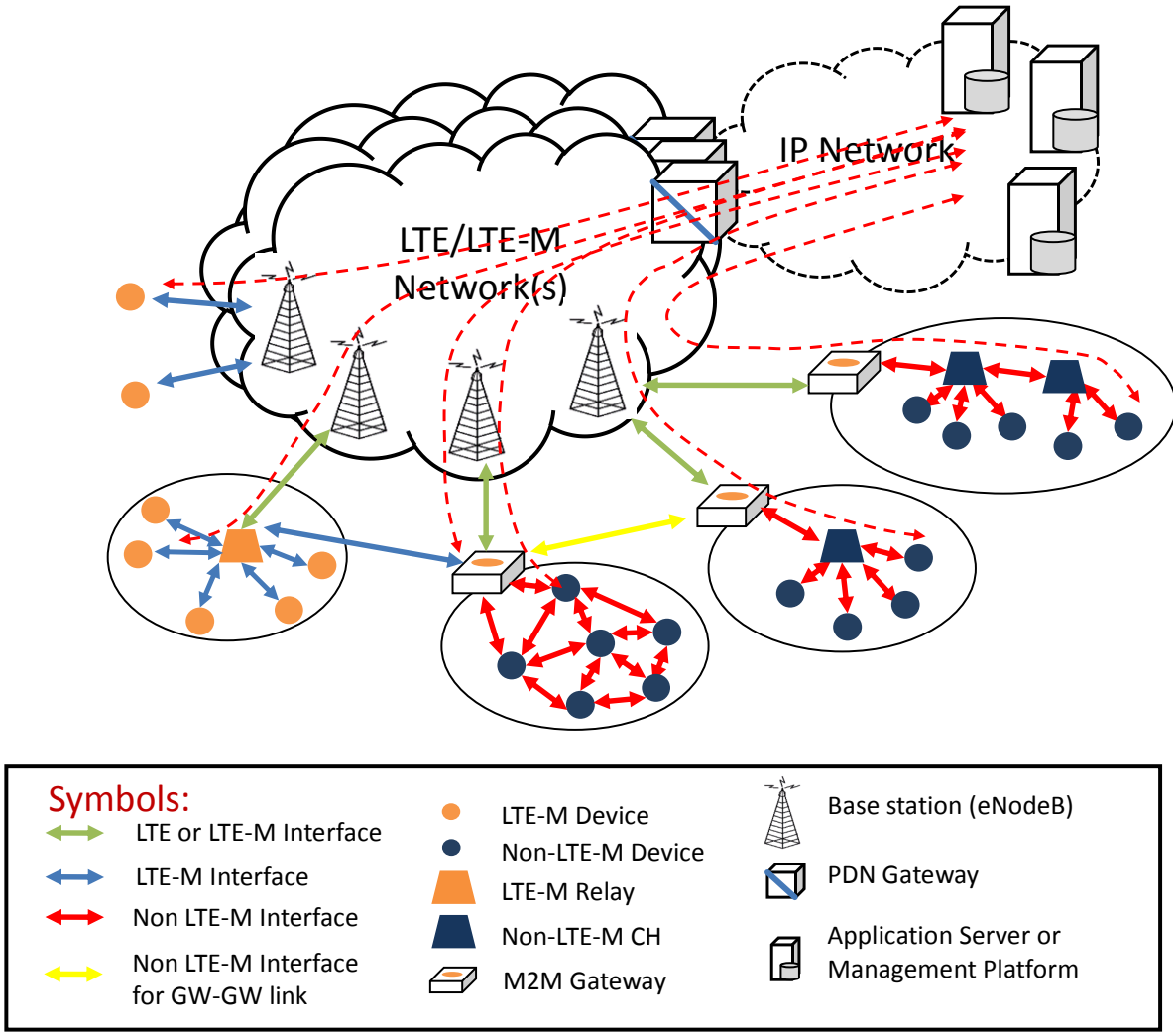

Figure 2.3: Communication paths between End Devices and Application Servers.

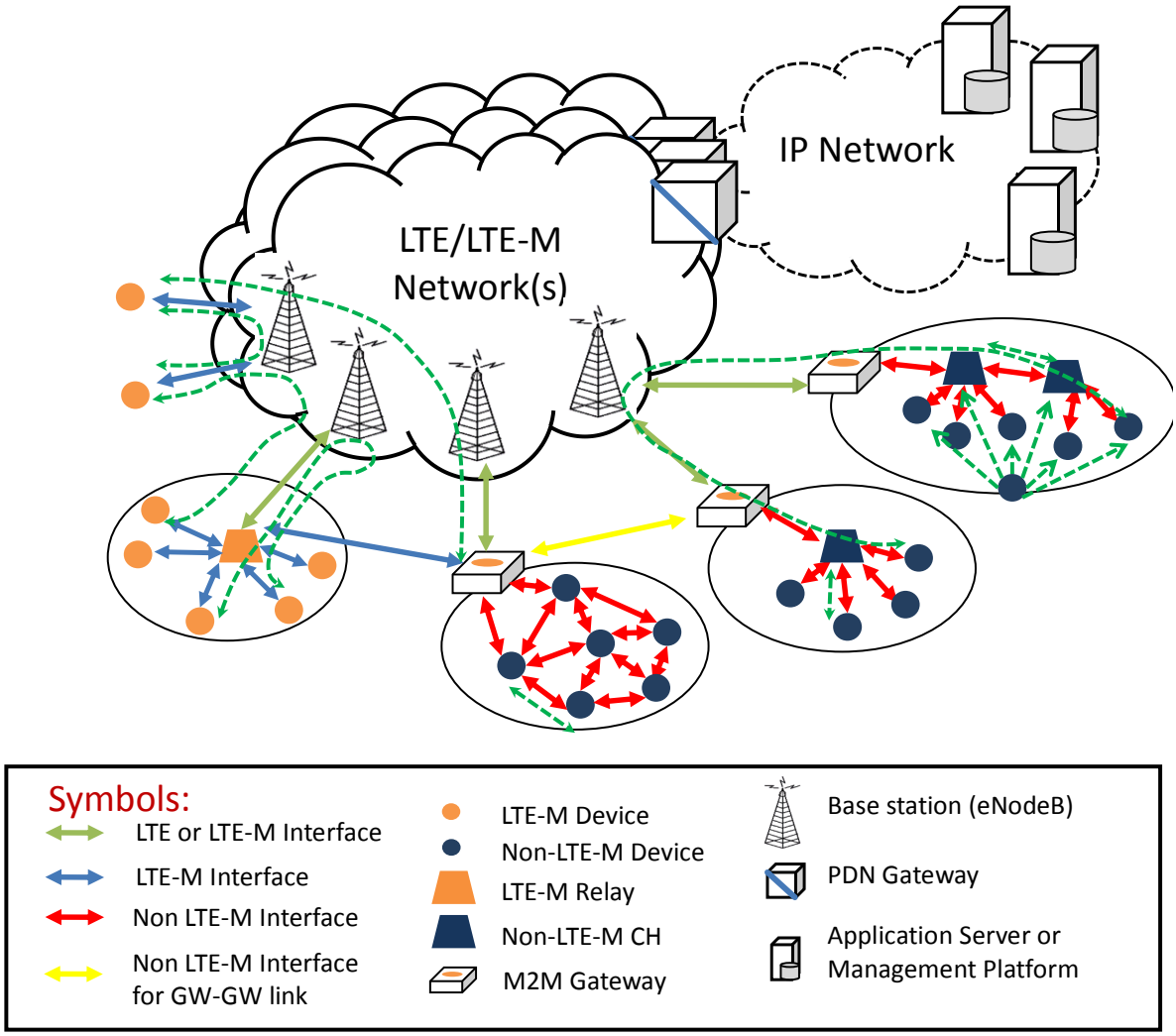

Figure 2.4: Communications paths between different End Devices.

3. EXALTED M2M proposed MAC protocols

Capillary networks play a critical role in the performance of M2M communication systems. The possibility of enabling M2M devices to communicate over short-range distances can be beneficial from different points of view:

- The energy consumption of the devices can be reduced, thus extending their lifetime, by transmitting at lower transmission powers.
- The interference between devices can be reduced, thus enabling the coexistence of a greater number of simultaneous operating networks.
- The traffic of the LTE-M system can be reduced, thus balancing the load of the network between wide-range communication (LTE-M) and short-range links (capillary networks).

Therefore, the design of efficient communication protocols for the capillary M2M segment of the LTE-M solution is one of the objectives of EXALTED. More precisely, one of the objectives of EXALTED is to design efficient solutions for the Medium Access Control (MAC) layer of capillary M2M networks. According to the EXALTED protocol stack represented in Figure 3.1, the focus of this section is on the MAC layer of the non-LTE devices and the M2M Gateway on the capillary network domain.

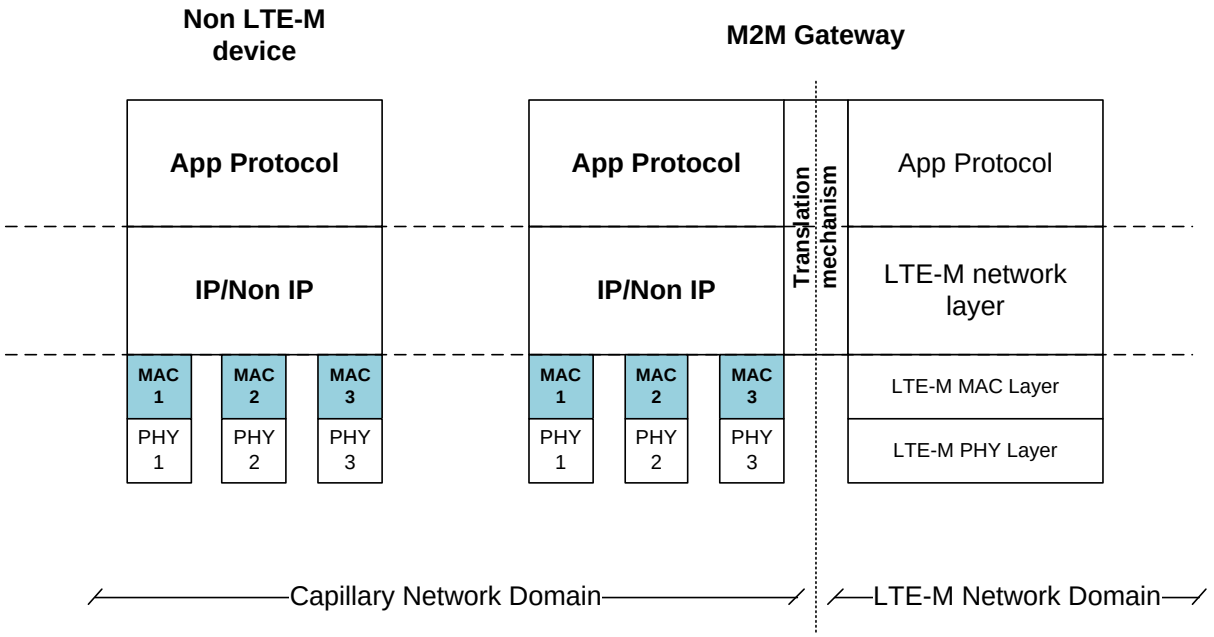

Figure 3.1 EXALTED Protocol Stack

Towards this goal, three complementary communication techniques have been designed and evaluated within EXALTED:

1) The design of a cooperative MAC protocol suitable for handling a huge number of devices, and enabling cooperation among devices. The key idea of the Distributed Point Coordination Function (DPCF) protocol proposed within EXALTED is that LTE-M capable devices can provide LTE-M connectivity to their neighbors, thus avoiding the need for the deployment of a fixed infrastructure. The DPCF protocol is described in Section 3.1.
2) The design of cooperative retransmission schemes that can improve the energy-efficiency of communications. Within the scope of EXALTED, the suitability of using

cooperative retransmission techniques towards improving energy-efficiency has been assessed first. Then, the cooperative approach to the specific scenario composed by M2M capillary devices is applied. This study is shown in Section 3.2.

3) The design of a MAC protocol that can handle the bottle-neck problem that occurs when multi-hop communication within the capillary network converges to a M2M Gateway. This problem can be exacerbated when the number of competing devices is high, as is the case for M2M applications. This protocol is described in Section 3.3.

3.1 Cooperative MAC protocol for high number of devices

3.1.1 Scenario and motivation

Capillary M2M networks may be composed of a number of heterogeneous devices, with and without LTE-M capabilities, which require E2E connectivity from the devices to the M2M servers. In EXALTED, it is considered the scenario where this connectivity can be provided by the LTE-M system. However, due to cost constraints, some devices have no cellular transceiver, but they are just equipped with short-range low-cost radio transceivers compliant with standards such as the IEEE 802.11 for Wireless Local Area Networks (WLANs) [4] or the IEEE 802.15.4 Standard for Low-Range Wireless Personal Networks (LR-WPANs) [5].

Although other technologies are available, in this task of EXALTED, the focus is put on these two technologies because:

1) The infrastructure for the IEEE 802.11 is already deployed, offering almost ubiquitous coverage, and thus becoming an excellent approach for the deployment of capillary M2M networks. In addition, recent studied show that the use of the IEEE 802.11 in a smart manner can improve the energy-efficiency of communications with regard to low-rate standards [6].
2) The IEEE 802.15.4 is the Standard defined to cover the requirements of sensor networks, and thus it is suitable for capillary M2M networks.

In this kind of heterogeneous scenarios, with LTE-M enabled and non-LTE-M enabled devices, cooperation among devices can be exploited to improve the performance of the network. It is proposed in EXALTED to let LTE-M capable devices to cooperate with simpler devices within its capillary network to provide them with LTE-M connectivity (through two-hop communication). This kind of approach can alleviate the need to transmit along multi-hop paths to reach a single-point gateway.

The design of a cooperation scheme for capillary M2M networks has to take into account two unique design requirements posed by M2M capillary networks:

1) The role of cooperating LTE-M device to provide LTE-M connectivity must be shared and rotated among all the available LTE-M devices in order to avoid LTE-M capable devices to drain their batteries.
2) The number of devices of an M2M capillary network can be very high, thus setting the network into heavy load conditions from the Medium Access Control (MAC) layer point of view. Note that for the MAC layer the number of contending devices has more impact on the performance than the actual amount of information to be transmitted by each single device.

Therefore, an efficient MAC layer, capable of handling a great number of devices, is required to manage this kind of capillary networks.

3.1.2 State of the art and contribution

The IEEE 801.11 and the IEEE 802.15.4 standards define the specifications for the PHY and the MAC layers for local area networks and for low-rate short-range networks, being thus suitable technologies for M2M communications. The MAC layer defines the set of rules that devices of a capillary short-range network must obey to get access to the radio channel in an efficient manner.

The MAC protocols of the two standards are very similar to each other and they are based on the Distributed Coordination Function (DCF). This access method is based on Carrier Sensing Multiple Access (CSMA), i.e., "listen before transmit", in combination with a Binary Exponential Backoff (BEB) mechanism as the collision resolution algorithm. An optional Collision Avoidance (CA) mechanism is also defined by which a handshake Request to Send (RTS) – Clear to Send (CTS) can be established between source and destination before the actual transmission of data. This CA mechanism aims at reducing the impact of the collisions of data packets and to combat the hidden terminal problem. The DCF can be executed in either ad hoc or infrastructure-based networks and, indeed, is the only access method implemented in most commercial wireless cards. It offers good performance when the traffic load of the network is relatively low. For greater traffic demands, the Point Coordination Function (PCF) is also defined in the IEEE 802.11 standard as an optional polling-based access method for infrastructure-based networks. In PCF, there is no contention to get access to the channel since the access point (AP) polls the devices of the network to transmit data. Therefore, collisions of data packets can be completely avoided. Despite the fact that this access method may achieve superior performance under heavy traffic loads, is capable of handling a big number of contending devices and can provide some degree of Quality of Service (QoS), it has received less attention in the literature.

The fact that the DCF of the IEEE 802.11 and the IEEE 802.15.4 Standard MAC protocol is based on CSMA/CA and BEB as the collision resolution algorithm leads to some throughput and delay underperformance under high traffic load conditions. Contention based on CSMA suffers from congestion as the number of contending devices or the number of channel access requests increase. This problem has been deeply analyzed in the literature over the last years and has motivated some research works on the topic. Some works propose to improve both fairness and throughput by tuning the backoff algorithm at run-time and adjusting it to the load conditions of the network (i.e., the number of active devices and the amount of offered data traffic) [7]-[9]. These works are inspired by the great impact that the tuning of the size of the contention window has on the performance of the protocol; more precisely, the specific way this size is increased upon collision and decreased upon successful transmission. Other works have focused on adding a power control mechanism to the system, as in [10], where the RTS/CTS handshake is transmitted at maximum power while data and ACK are transmitted at the minimum required power, or [11] where, based on the same idea of [10], data senders transmit power spikes during data transmission in order to reduce the probability of having any potential interfering device. Slotting time [12] or using multiple minislot pairs for RTS/CTS handshake [13] are ideas that have been also proposed to improve the performance of the system, among a vast amount of published proposals.

Since the fundamentals of the MAC layer have survived across new amendments of the standard, still more progress in the incremental evolution of the DCF MAC protocol is expected to come. Unfortunately, the simplicity of a CSMA-based protocol comes at the cost of a "trial-and-error" approach where a transmission attempt can result in a collision if several users contend for the access to a common medium as either the traffic load of the network or the number of competing devices increases. For this reason, it seems reasonable to believe that the ***combination of different access methods***, integrating random access for low traffic loads with reservation mechanisms for higher traffic loads, could improve the overall

performance of capillary M2M networks which may be formed by a high number of simultaneously active devices. In fact, this approach has been already used in the context of infrastructure-based networks [14]-[18] combining static Time Division Multiple Access (TDMA) with dynamic CSMA access. Most of these works deal with different approaches to use empty pre-allocated TDMA slots by other users with data ready to transmit and which contend for the channel using CSMA. However, there are very few works in the literature dealing with this approach in a distributed manner, i.e., for dynamic distributed network, such as those formed by M2M devices. This is the main motivation of the work presented in this task of EXALTED, where it is defined the Distributed Point Coordination Function (DPCF) protocol as a combination of the DCF of the IEEE 802.11 (or the IEEE 802.15.4) and the PCF of the IEEE 802.11 Standard to provide highly dense M2M capillary networks with high throughput despite of the high number of contending devices.

Indeed, there are very few works dealing with the PCF, which can indeed potentially achieve better performance than the DCF under heavy load conditions. Some contributions related to the PCF improve the overall network performance through novel scheduling algorithms [19]-[23] or by designing new polling mechanisms that can reduce the overhead associated to the polling process [24]. However, there have been almost no efforts in extending the operation of the PCF to distributed networks in order to provide them with some degree of QoS. The only exception can be found in [25] where a virtual infrastructure is created into a MAC protocol called Mobile Point Coordinator MAC (MPC-MAC) in order to achieve QoS delivery and priority access for real time traffic in ad hoc networks maintaining both the PCF and the DCF. In summary, a clustering based mechanism is used to achieve the correct operation of the PCF in a distributed environment. The duration of PCF and DCF periods and the criterion upon which a device is chosen to be the MPC (acting as AP) are fixed and they are determined by the MAC protocol configuration. This approach works well in low dynamic environments without energy-constraints where the topology does not vary frequently and the devices can periodically broadcast “hello” messages to announce their availability. However, it may not be convenient for dynamic environments where the clustering overhead could impact negatively on the efficiency of the network and drain the batteries of the devices. In addition, this protocol does not consider that the availability of devices ready to become cluster heads may depend on duty cycling periods, and thus static and permanent decision cannot be made.

Taking this background into account, in EXALTED it is proposed the DPCF protocol as an extension of PCF to operate over infrastructure-less capillary networks where some LTE-M enabled devices can cooperate with non LTE-M devices to provide access to the cellular connectivity. By combining both DCF and PCF using a spontaneous and dynamic clustering mechanism at the MAC layer it is possible to extend the higher performance of PCF to networks without infrastructure.

It is worth mentioning that the design of the DPCF protocol has been inspired by the work presented in [27], where the near-optimum Distributed Queuing Collision Avoidance (DQCA) MAC protocol for WLAN [28] was adapted to be executed in distributed networks without infrastructure. The new resulting protocol was called Distributed Queuing MAC Protocol for Ad hoc Networks (DQMAN). The essential idea of that work is that the DCF protocol is used to create spontaneous clusters. One a node seizes the channel using the rules of the DCF, it becomes master and establishes a temporary cluster where the DQCA protocol can be executed. A similar idea is presented in this deliverable to extend the operation of the PCF to capillary networks where some devices can cooperate with their one-hop neighborhood to provide LTE-M connectivity.

3.1.3 IEEE 802.11 and IEEE 802.15.4 MAC overview

3.1.3.1 Distributed coordination function (DCF)

The DCF is the mandatory coordination function implemented in all IEEE 802.11 standard compliant devices. As for the IEEE 802.15.4, the access method without beacons (the one commonly implemented in commercial devices) is very similar to the operation of the DCF of the IEEE 802.11. Indeed, the only remarkable difference is that devices of an IEEE 802.15.4 do not listen to the channel when they are performing a backoff in order to save energy. Therefore, in order to avoid redundancy in the explanation, the text herein is focused on the DCF of the IEEE 802.11 Standard, bearing in mind that the access method of the IEEE 802.15.4 without beacons has an almost identic operation. The IEEE 802.15.4 MAC protocol with beacons is out of the scope of this deliverable.

Two access modes of operation are defined in the DCF:

1) ***Basic access (BASIC) mode;*** the device which seizes the channel transmits its data packets without establishing any previous handshake with the intended destination.

2) ***Collision avoidance access (COLAV) mode;*** a handshake RTS/CTS is established between source and destination before initiating the actual transmission of data. These RTS and CTS get the form of special control packets. The COLAV access mode is aimed at reducing the impact of collisions of data packets and at combating the presence of hidden devices.

Two examples are illustrated in Figure 3.1 and Figure 3.2 representing the operation of the BASIC and the COLAV access modes, respectively. In summary, any device with data to transmit listens to (senses) the channel for a DCF Inter Frame Space (DIFS). If the channel is sensed idle for this DIFS period, the device seizes the channel and initiates the data transmission (or the RTS transmission in the COLAV mode). Otherwise, if the channel is sensed busy, the device backs off and executes a BEB algorithm by which the size of the contention window is doubled up upon any transmission failure and reset to the minimum value upon success. In the case of the IEEE 802.15.4 Standard, during these backoff periods, devices do not listen to the channel in order to save energy. When a data packet is received without errors, the destination sends back an ACK packet after a Short Inter Frame Space (SIFS). This SIFS is necessary to compensate both propagation delays and radio transceivers turn-around times to switch from receiving to transmitting mode. It is worth noting that since a SIFS is shorter than a DIFS, acknowledgments have higher priority than regular data traffic.

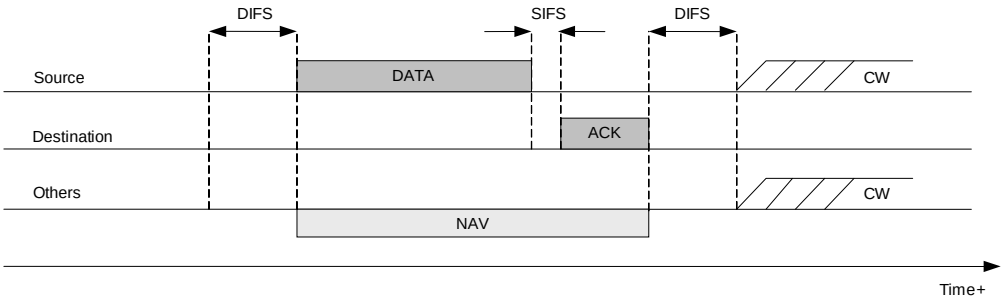

Figure 3.1: Example: DCF Operation (Basic Access mode).

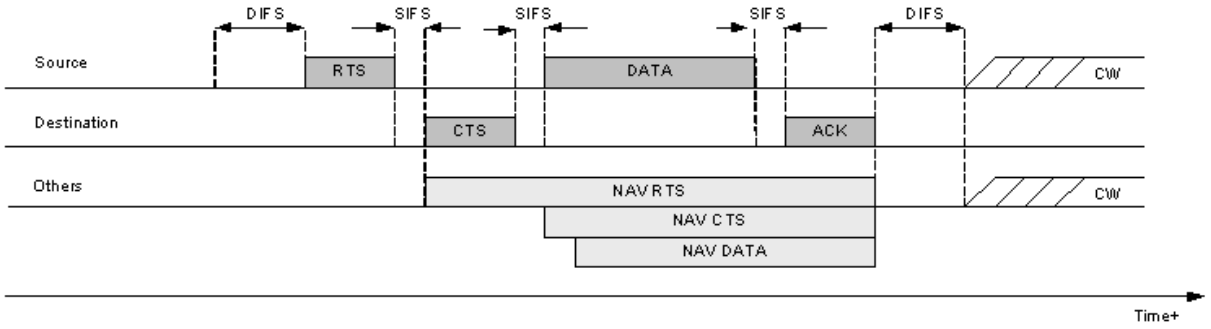

Figure 3.2: Example: DCF Operation (Collision Avoidance mode).

A relevant feature of the DCF is the Virtual Carrier Sensing (VCS) mechanism. Devices not involved in an ongoing transmission defer from attempting to transmit for the time the channel is expected to be used for an effective transmission between any pair of source and destination devices regardless of the actual physical carrier sensing. To do so, devices update the Network Allocation Vector (NAV) which accounts for the time the channel is expected to be occupied. This information is retrieved from the duration field attached to the overheard RTS, CTS, and data packets. This mechanism is mainly aimed at combating the presence of hidden devices.

3.1.3.2 Point coordination function (PCF)

PCF can only be executed in infrastructure-based networks wherein an AP or gateway can sequentially poll devices to transmit data, totally avoiding the presence of collisions. This mechanism was originally aimed at provisioning QoS over WLANs.

When PCF is executed, time is divided into Contention Free Periods (CFP), wherein the gateway sends poll messages to give transmission opportunities to the devices, and Contention Periods (CP), where the regular operation of the DCF is executed. Since the PCF is an optional coordination function and is not implemented in all standard-compliant devices, DCF periods are necessary to ensure access to DCF devices. The interleaving of CFPs and CPs is illustrated in Figure 3.3. As also shown in this figure, a CFP is initiated and maintained by the gateway, which periodically transmits a beacon (B). The first beacon after a CP (DCF access) is transmitted after a PCF Inter Frame Space (PIFS). The duration of a PIFS is shorter than a DIFS but longer than a SIFS, providing thus the initialization of a CFP with less priority than the transmission of control packets, but with higher priority than the transmission of data packets. The periodically transmitted beacons contain information regarding the duration of both the CFP and the CP and allow a new arrived device to associate to the AP during a CFP. The CFP is finished whenever the gateway transmits a CFP End (CE) control packet.

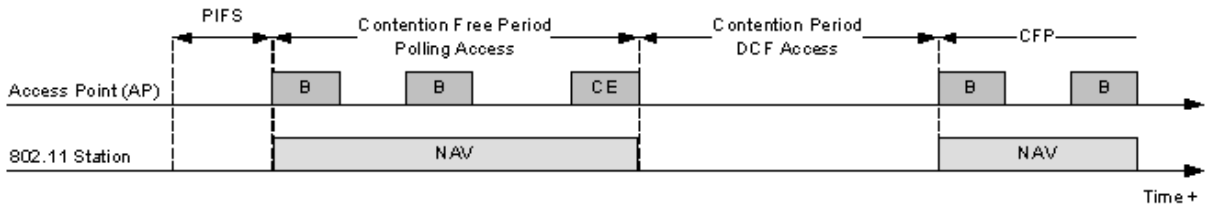

Figure 3.3: IEEE 802.11 PCF Interleaves CFPs with CPs.

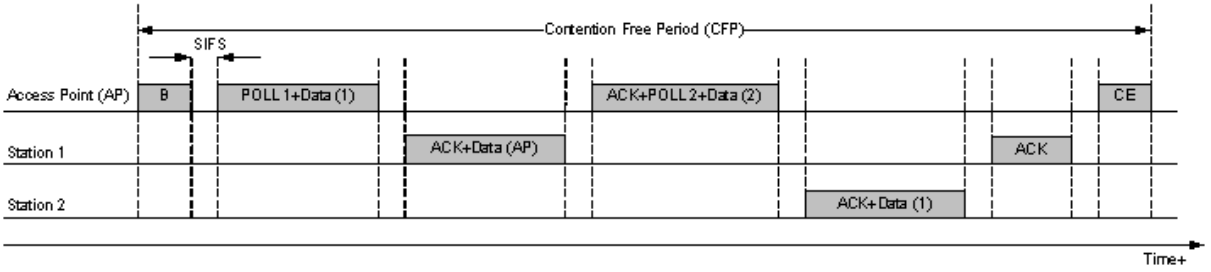

Figure 3.4: Example: PCF Operation.

During a CFP, the only device allowed to transmit data is the one being polled by the gateway or any destination device which receives a data packet and has to acknowledge (ACK) it, if applicable, and can combine the ACK with data in a same packet. In PCF, some packets can be combined together in order to reduce the number of MAC and PHY headers and thus increase the efficiency of the communications. In any case, the access to the channel is granted one SIFS after the reception of either the poll or the data packet, respectively. A polled device can either transmit a data packet to the gateway or to any other device in the network, establishing a peer-to-peer link. If a polled device has no data to transmit, it responds with a special type of control packet, referred to as NULL packet.

An example of PCF operation is illustrated in Figure 3.4. In this example, the gateway initiates a CFP by transmitting a beacon (B). After a SIFS, it combines a poll packet with data to device 1. Upon the reception of this combined packet, device 1 acknowledges the data packet received and responds to the poll by transmitting a data packet to the gateway. Note that this is also a combined packet. Then, the gateway acknowledges the data packet received from device 1 and combines a poll packet with data to device 2. Upon the reception of the packet, device 2 acknowledges the packet to the gateway and transmits data to device 1. Upon the reception of the packet, device 1 acknowledges the received packet. The CFP is finished with the transmission of a CE packet.

3.1.4 Distributed point coordination function for M2M networks (DPCF)

The Distributed PCF (DPCF) protocol is presented in this section as an adaptation and extension of the PCF to operate on distributed M2M capillary networks, without the presence of a fixed LTE-M gateway, but with the presence of a subgroup of devices equipped with both LTE-M capabilities and short-range technologies, such as the IEEE 802.11 or the IEEE 802.15.4 Standard, based on CSMA access.

3.1.4.1 Protocol description

A set of devices equipped with IEEE 802.11 or IEEE 802.15.4 cards forming a spontaneous ad hoc network are considered. A subset of these devices is equipped with LTE-M capabilities. Other devices, non-LTE-M devices are just equipped with short-range Radio Access Technology (RAT). Any device must be able to operate in three different modes of operation: *idle*, *master*, and *slave*. Initially, all the devices operate in idle mode but they must be able to change the mode of operation when necessary.

Idle devices with data to transmit get access to the channel using the rules of the regular DCF. Whenever a device gets access to the channel, it transmits an RTS targeted to the intended next-hop destination of the data packet. If the destination of the packet is the M2M Server, then the next hop destination must be one of the available LTE-M enabled devices. This packet initiates a clustering process. Upon the reception of the RTS, the intended destination of the packet becomes master and responds to the RTS with a beacon (B)

followed by a poll targeted to the device which transmitted the RTS. A cluster is established and a CFP is initiated inside this cluster. From this moment, the master can provide LTE-M connectivity and thus route all the traffic to the M2M server using the LTE-M interface (doing no other function than retransmitting the data packets). All the other idle devices become slaves and get synchronized to the master when they receive the beacon. Cluster membership is spontaneous and soft-binding: there are no explicit association and disassociation processes and a device belongs to a cluster as long as it can receive the beacons broadcast by the master. As in PCF, a cluster is broken when the master transmits a CE packet. Upon the reception of this CE packet, all the slaves revert to idle mode and execute a backoff in order to avoid a certain collision if more than one device has data to transmit. Therefore, according to this operation, the clustering algorithm of DPCF is spontaneous in the sense that the first idle device with data to transmit initiates the clustering algorithm.

An example of operation is represented in Figure 3.5. In this example, device 1 has data to transmit to device 2. Once the device 1 successfully seizes the channel executing the rules of the DCF, it transmits an RTS to device 2. Upon the reception of the packet, device 2 becomes master and transmits a beacon. The first poll is then sent to device 1, which has a data packet ready to transmit. Device 1 transmits the data packet to device 2. Then, device 2 acknowledges the reception of the packet and polls device *N* with a combined packet. Since device *N* has no data packets to transmit, it sends a NULL packet. Finally, device 2 transmits the CE packet to indicate the end of the cluster phase. All the slave devices revert to idle mode and execute a backoff to reduce the probability of collision if more than one device has data to transmit.

Within a cluster, the master can poll the slaves following any arbitrary order. Regardless of the specific polling policy, the master requires some knowledge of the local neighborhood in order to be able to carry out the polling mechanism. This information can be transferred to the devices upon deployment of the network or can be acquired along the lifetime of the networks. In this latter case, all the devices must overhear ongoing packet transmissions in their vicinity in order to create a neighbor table with an entry for each device in the local neighborhood. This table should be updated along time. The specific scheduling of the polling mechanism is out of the scope of the basic definition of DPCF. Only as an example, a round robin polling scheme can be executed following the entries of the neighbor table. In any case, once a device is polled by the master, it may transmit a data packet to any other slave (peer-to-peer communication model) without routing all the data through the master. Therefore, the master only acts as an indirect coordinator of the communications, but not necessarily as a concentrator of traffic (as the AP does in a regular centralized network). This role of concentrator is done only for those packets that need to reach the M2M Server and will be transmitted in the uplink of the LTE-M interface through a different RAT.

The duration of a cluster is variable and depends on the aggregate traffic load of the network. An *inactivity mechanism* is considered in DPCF to avoid the transmission of unnecessary polls when there are no more data packets to be transmitted. This mechanism consists of the following: any master maintains a counter that is incremented by one unit upon each NULL packet received from a polled device with no data to transmit. This counter is reset to zero whenever a device responds to a poll with the transmission of a data packet. If the counter gets to a given tunable value, a CE packet is sent and the cluster is broken.

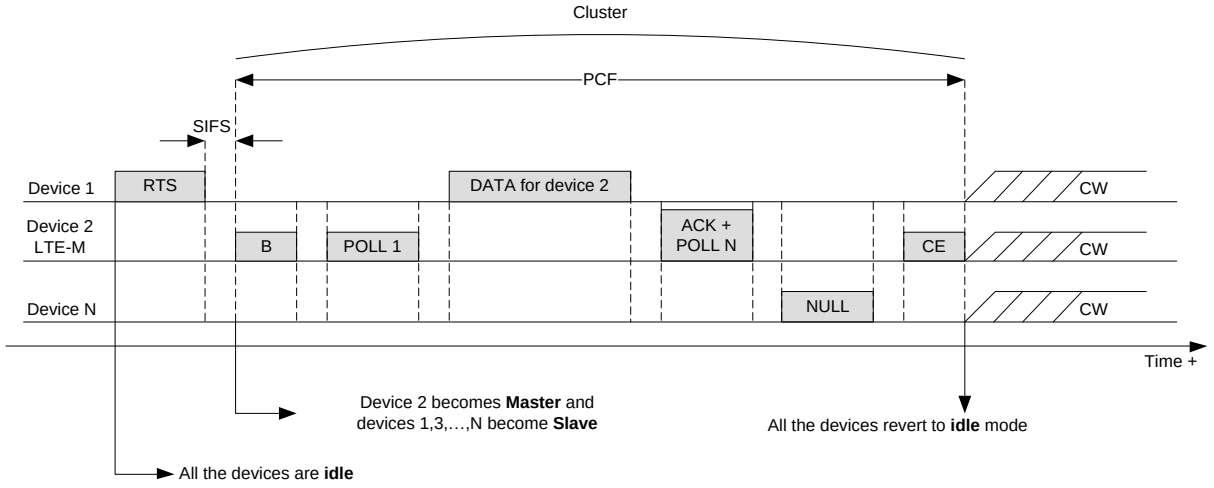

Figure 3.5: Example: DPCF Operation.

On the contrary, it may happen that under heavy traffic conditions once a device becomes master it operates as such for the whole operation of the network due to the absence of idle periods. This would be unfair in terms of sharing the responsibility of being master in the network among all the devices. Therefore, it is necessary to determine an upper-bound for the maximum time that a device can operate as master without interruption. This limit is especially since fair share of the energy consumption is a must in M2M capillary networks.

The approach in DPCF is the following: any master maintains a *Master Time Out* (MTO) counter which determines the maximum duration of a cluster. The value of the MTO corresponds to the maximum number of beacons (MTO=$N_{beacons}$) that a master can transmit without interrupting the operation of its cluster. The MTO counter is decremented by one unit after each beacon is transmitted. Whenever the MTO counter expires, a CE packet is transmitted and the cluster is broken regardless of the traffic load or activity of the devices. Therefore, the maximum time that a device can operate as master is denoted by T_{MAX} and can be computed as

$$T_{MAX} = N_{beacons} \cdot N_{polls} \cdot MIFS = MTO \cdot N_{polls} \cdot MIFS. \quad (1)$$

N_{polls} denotes the number of polls transmitted between beacons, which can also be tuned, and MIFS is defined as the Maximum Inter Frame Space whose duration corresponds to the *maximum possible* time between two consecutive polls. The duration of a MIFS can be computed as the time elapsed when:

1) The master device combines an ACK of a recently received data packet with a poll and a data packet.
2) The device polled acknowledges the reception of the data packet from the master and combines the ACK with data for a third device.
3) The third device transmits the ACK of the data packet received from the second device.

The definition of a MIFS is illustrated in Figure 3.6. Note that it also corresponds to the minimum period of time that a device has to listen to the channel before establishing a new cluster in order to reduce the probability that another master is present.

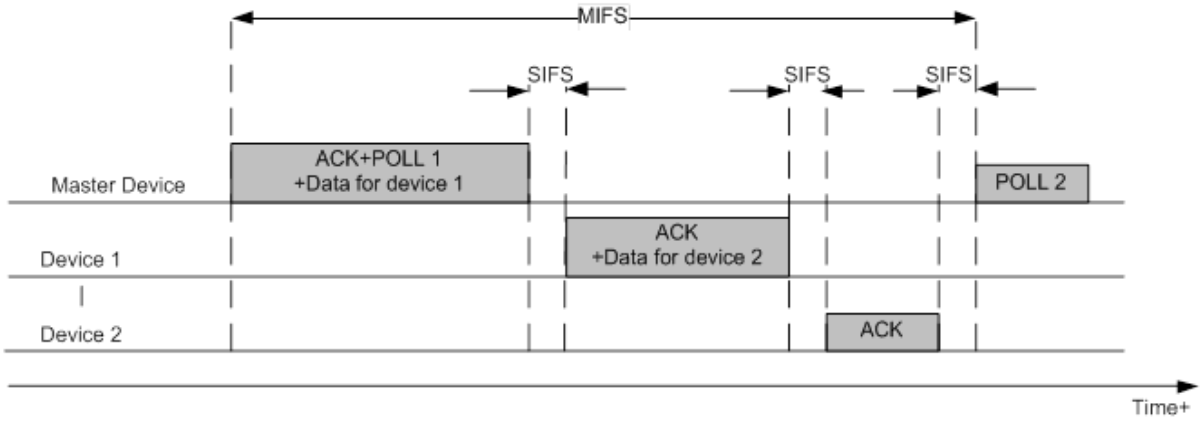

Figure 3.6: Definition of MIFS.

The criteria to set the value of the MTO are highly application-dependent. A greater value of the MTO will lead to greater efficiency in terms of throughput since more time will be used in collision free periods than in contention-based clustering processes. However, longer clusters may lead to unbalanced energy consumption between those users becoming masters, and those users just behaving as slaves. This tradeoff has to be managed depending on higher-level application requirements.

Regarding the channel reservation information (duration fields attached to data and control packets for the execution of the virtual carrier sensing function), the two following simple rules apply to DPCF:

1) The first RTS triggering the clustering mechanism reserves the channel just for the time required to receive the first beacon from the intended destination (the one that will become master).
2) Each transmitted beacon (broadcast by the master) reserves the channel for the maximum interbeacon time, computed as $N_{polls} \cdot MIFS$. Recall that the actual interbeacon time is not deterministic and thus the worst case is considered for channel reservation purposes (conservative approach).

In order to summarize the whole operation of DPCF, a general flowchart is shown in Figure 3.7. The left branch of the chart models the operation of any device becoming master when requested by any other devices and the right branch of the chart represents the operation of the device initiating the clustering algorithm when it has data to transmit.

3.1.4.2 Performance evaluation

In order to evaluate the performance of DPCF, the protocol rules have been implemented in a custom-made C++ link-level simulator [29]. The simulator works in an object-oriented basis and the source code of each device runs in parallel. Each node in the network constitutes a different entity (instance of a class) that executes the code that would be implemented in a real platform. The main motivations for implementing the protocol in a custom-made C++ simulator rather than in any other well-known system simulation platform (such as ns-3, for example) are the possibility of isolating the MAC protocol performance from the rest of the network and the faster execution of the simulations as the simulator can be tailored for the specific protocol that is wanted to be evaluated.

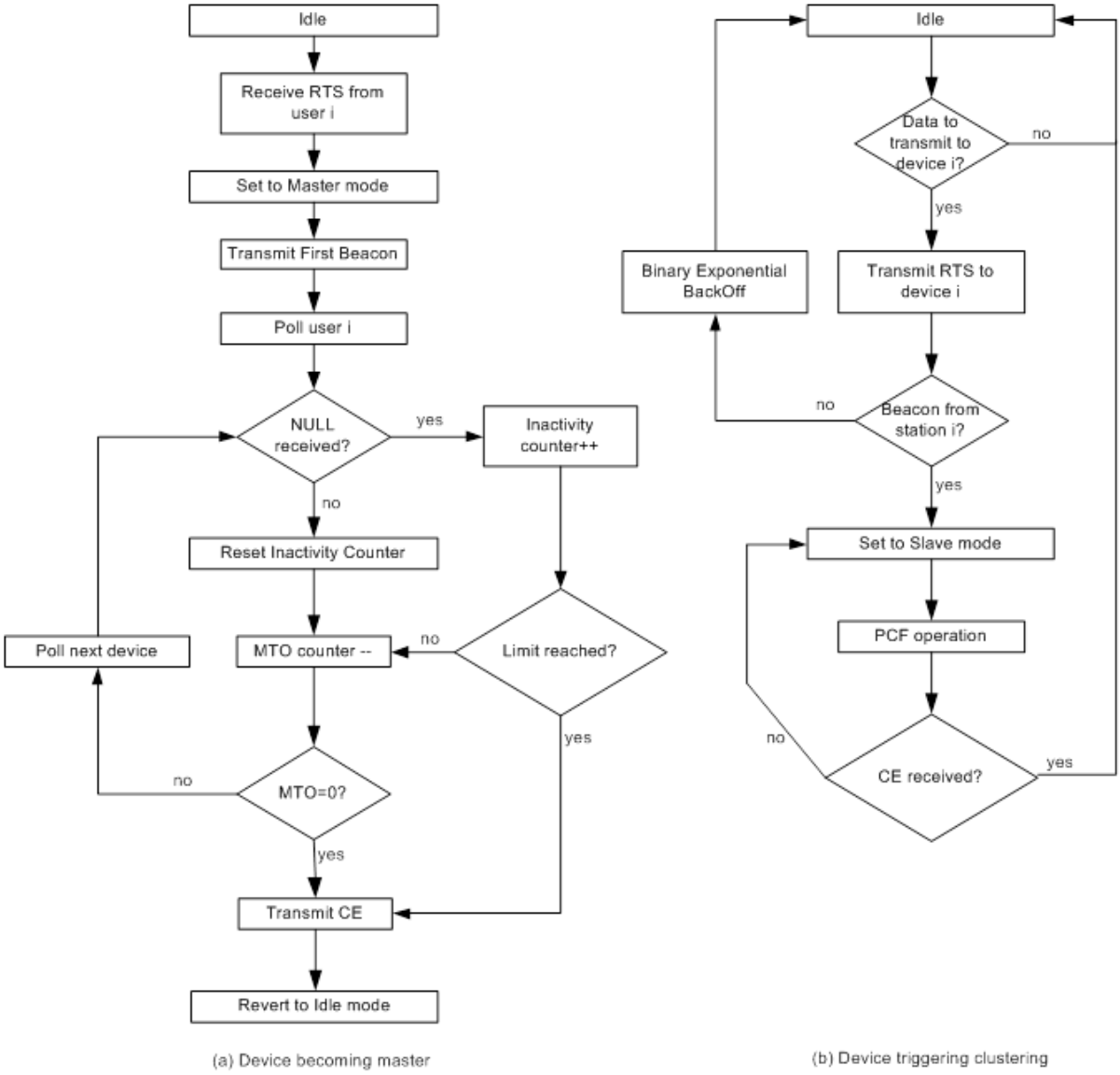

Figure 3.7: DPCF Clustering Flowchart.

The system parameters have been set according to the one of the modes defined in the PHY layer of the IEEE 802.11g Standard [4] and they are summarized in Table 3-1. It is considered a single-hop network, wherein all the devices can sense the same state for the channel (no hidden and exposed terminals).

It is first considered a hop network composed of 100 M2M devices, all of them within the transmission range of each other and all of them LTE-M enabled. All the devices generate data packets of fixed-length following a Poisson arrival distribution and they contribute equally (homogeneously) to the total aggregate data traffic of the network. The destination of each packet is randomly selected among all the devices of the network with equal probability. In order to focus on the MAC layer, all the packets are assumed to be received without errors and thus the results herein presented correspond to an upper-bound of the performance of the protocol (from the wireless channel effects point of view). It is also assumed that an ideal round robin scheduling is performed to poll all the devices once a cluster is established. Three different networks have been studied (they all have been implemented in the simulator):

1) **DCF:** a network wherein all the devices only execute the DCF with the collision avoidance access method.
2) **PCF:** a network wherein a fixed gateway manages the access to the channel. In this network, it is considered that the gateway also has data to transmit to the devices in the downlink as any other regular device.
3) **DPCF:** a network wherein all the devices execute the proposed DPCF protocol.

According to the parameters presented in Table 3-1, the number of polls between beacons has been set to 99 and it indicates that all the slaves within a cluster are polled exactly once by the master between the transmission of two consecutive beacons. In addition, the setting MTO=3 indicates that all the slaves are polled at most three times when a cluster is established unless the inactivity mechanism is triggered by the master.

Table 3-1: System Parameters for Evaluation of DPCF.

Parameter	Value	Parameter	Value
Data Packet Length (MPDU)	1500 bytes	Constant Message Length	1500 bytes
Data Tx. Rate	54 Mbps	Control Tx. Rate	6 Mbps
MAC header	34 bytes	PHY preamble	96 μs
SIFS, PIFS, DIFS	10, 30, 50 μs	SlotTime (σ),	10 μs
RTS, BEACON, CF_END and POLL packets	20 bytes	CTS and ACK packets	14 bytes
CW_{min}	128	CW_{max}	512
MTO	3	Polls per beacon	99

The throughput of the three different networks is plotted in Figure 3.8 as a function of the total aggregate offered load to the network. As expected, the three curves grow linearly until they reach the saturation throughput. The three protocols are stable for heavy traffic conditions without entering in congestion and thus they can operate under sporadic situations of high peak traffic loads without collapsing the network. The saturation throughput of DPCF is remarkably higher than that of DCF, achieving an improvement of approximately 250%. Collisions and backoff periods are reduced in the DPCF network compared to the DCF network, thus yielding higher performance. In addition, the performance of DPCF is even superior to the regular PCF, attaining 25% higher saturation throughput.

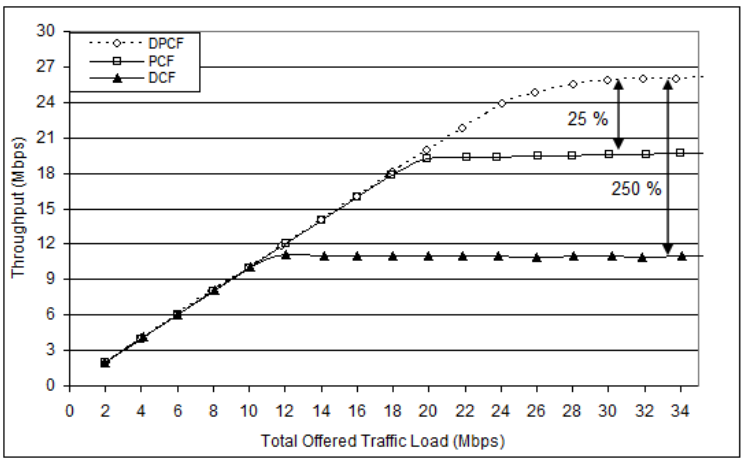

Figure 3.8: Throughput Comparison DPCF, PCF, and DCF.

In order to further analyze this apparently counter-intuitive result, Figure 3.9 shows the probability that a device transmits a data packet when it is polled. It has been considered for this calculation that the gateway (in the PCF network) and the masters (in the DPCF network) are *virtually* polled every time they poll a device as they have the possibility to combine the polls with data and ACK packets. The probability of transmitting data when being polled is quite similar in the two networks for low traffic loads. However, this probability is much higher in the DPCF network than in the PCF network for high traffic loads. While the efficiency of the polling in DPCF gets close to 98% for high traffic loads, it remains close to 55% in the PCF network.

This efficiency translates directly into a higher efficiency of DPCF, since the ratio of data packets transmitted per control overhead is higher. The reason for these figures is that there is a severe unbalance between the channel access opportunities between the gateway and the regular devices in the PCF network. This can be seen in Figure 3.10, where the probability of actually transmitting when being polled is plotted again. Now, two different curves for the PCF network are represented corresponding to the average probability among of all the regular devices and to the probability for the gateway alone, separately. The gateway has a channel access opportunity every time it polls another device, but most of these transmission opportunities are not used for the actual transmission of data (note that the probability of transmitting when being polled is below 10% in all cases for the AP), decreasing the overall efficiency of the polling mechanism.

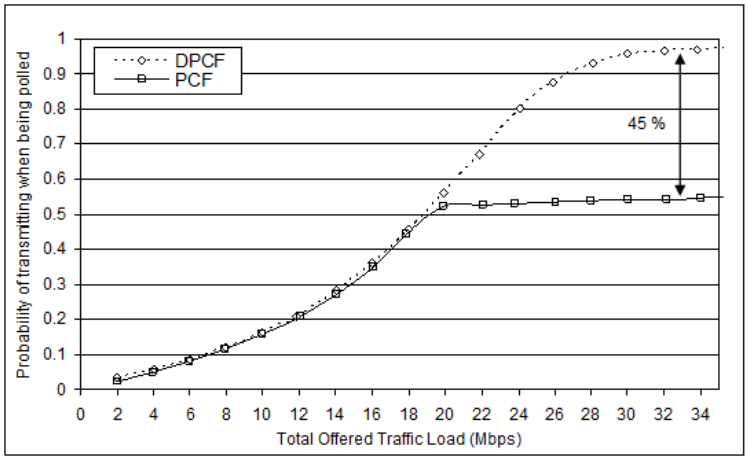

Figure 3.9: Probability of Transmitting when Being Polled.

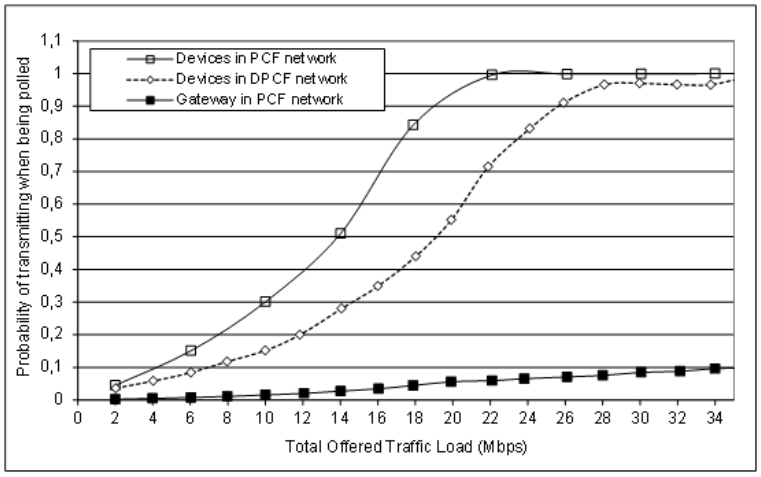

Figure 3.10: Probability of Transmitting when Being Polled.

This unbalance between master and slave devices is avoided in DPCF by sharing dynamically and spontaneously in time the responsibility of being master among all the devices of the network. It is well known that the DCF is fair in the long-term, and so is the clustering algorithm of DPCF. Since all the devices of the network get the role of master periodically, the unbalanced access of the gateway in the PCF network is shared in the DPCF network. Every time a device is set to master it can transmit all its backlogged data packets and thus take advantage of the prioritized access to empty its data buffers while operating as master. Indeed, the fact that a device operating in master mode has more channel access opportunities than a slave device can be seen as an implicit mechanism to provide devices with some incentive to become master despite the extra functionality and its corresponding increase in energy consumption.

3.1.4.3 Coexistence with legacy networks

A simple modification to the protocol operation can facilitate the coexistence of DPCF with legacy DCF networks. Let us consider a mixed network formed by two different kinds of devices, namely, DPCF and DCF devices. It is assumed that DPCF devices can execute the rules of DPCF as well as the rules of the DCF. In fact, the rules of the DCF are included in DPCF. For this reason, this kind of devices will be hereafter referred to as either DPCF or *dual* devices. On the other hand, DCF devices can only execute the rules of the DCF and are not aware of the presence of DPCF devices and, indeed, they do not know the rules of DPCF. This latter group represents already deployed equipment which has been shipped without knowledge of the existence of DPCF.

By default, all the devices execute the Standard DCF to get access to the channel. However, a DPCF device which gets the channel can either *i)* transmit data following the rules of the DCF or *ii)* initiate a cluster following the rules of DPCF. Therefore, it is necessary to include a stamp in the RTS packets to indicate whether the transmitting device wills to initiate a cluster or not. To do so, it is possible to use either bit B8 or B9 of the Frame Control (FC) field of RTS packets, which are only used in infrastructure-based communications [4]. One of these bits will be used as a flag to distinguish between regular RTS packets and what will be called *dual*-RTS packets, which are associated to the initialization of a DPCF clustering phase. A key advantage of this approach is that DCF devices will ignore this field and will thus decode a *dual*-RTS packet as a regular RTS packet.

If a cluster is established, all the DCF devices must update their NAV with the value of the duration field attached to the beacons transmitted by the master and wait for the transmission of the CE packet indicating the end of the cluster. However, neither beacons nor CE packets can be decoded by DCF devices. In order to overcome this problem, both beacons and CE packets can be substituted by what will be called *dual*-CTS packets, defined as regular CTS packets with the following two modifications:

1) The duration field of the CTS has the value of the inter-beacon interval if it is used as a beacon and the value zero if it is used as a CE packet.
2) As in the case of *dual*-RTS packets, a flag bit is included to distinguish CTS packets acting as beacons from regular CTS packets.

In addition, it is necessary to ensure that DPCF devices do not capture the channel. Note that DCF devices will be unable to get access to the channel if DPCF devices establish a cluster every time they seize it. Therefore, DPCF devices must not be allowed to initiate a cluster before a certain time has elapsed from the transmission of the last CE packet, i.e., the end of the last cluster. To this end, it is defineed the Equivalent Cluster Time (ECT) as the minimum DCF operation time between two consecutive clusters. For the sake of simplicity, this time is measured in MTO units and can be easily translated into time duration using (1).

It is worth mentioning that these forced DCF periods can be also used by DPCF devices to overhear ongoing transmissions and learn the composition of the network in order to optimize the polling mechanism whenever a cluster is established. The interleaving of clustering and DCF periods is illustrated in Figure 3.11.

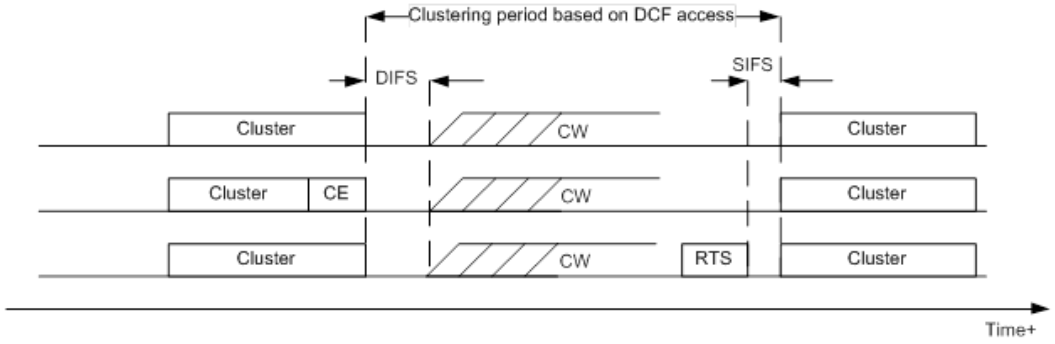

Figure 3.11: Alternating DCF and DPCF periods for backwards compatibility.

The performance of a mixed scenario composed by DPCF and legacy DCF devices has been evaluated by means of computer simulations to show that the mechanism works and DPCF can coexist with already deployed WLANs. More precisely, the aforementioned C++ computer-based simulator has been used to evaluate the performance of a network formed by a total of 20 devices in a single-hop layout, all of them in the transmission range of each other. 5 out of these 20 devices are DPCF devices while the other 15 devices are legacy DCF devices. The rest of the configuration parameters have been set as for the single-hop performance evaluation of DPCF presented before but with the following modifications: DPCF devices transmit 16 poll packets in between two consecutive beacons and the MTO has been set to 4.

In order to obtain the results presented in this section, the mixed scenario as well as two benchmark networks where the 20 devices execute only the DPCF or the DCF, respectively, have been simulated.

The throughput as a function of the total offered traffic load is illustrated in Figure 3.12 for the three considered networks. The ECT has been set to 1, i.e., the duration of the forced DCF operation period after a DPCF cluster is equal to the maximum duration of the cluster time. As shown in the figure, the performance of the mixed network lies in between the performance of the DCF and the DPCF networks. Since both protocols are alternately executed in a mixed network, it seems reasonable that the results show an intermediate performance. Therefore, the main conclusion is that the mixed network works properly and, as a consequence, the coexistence and a smooth migration to the new protocol are actually feasible.

It is interesting to analyze the throughput performance perceived separately by the group of DPCF and DCF devices. To do so, the throughput of the group of 15 DCF devices is illustrated in Figure 3.13, while the performance of the group of 5 DPCF devices is illustrated in Figure 3.14. As a benchmark performance, the curve labeled *DCF operation* corresponds to the situation where only the DCF is executed. Note that the values of the x-axis in these curves correspond to the *total offered traffic load* considering the contribution of all the devices regardless of whether they are DCF or DPCF devices.

It is worth seeing that the performances perceived by each group of devices are complementary. As the value of the ECT increases, i.e., longer DCF periods are allowed, the performance of the DCF devices increases, as expected. In the limit, where the DCF tends to

be the only access method used by all the devices (including the dual DPCF devices), the performance of the DCF group of devices is exactly ¾ of the total throughput of the network (which corresponds to 15 out of 20 devices). This is due to the well-known long-term fairness of the DCF.

On the other hand, the throughput perceived by the group of DPCF devices is higher as the value of the ECT becomes smaller. A smaller value of the ECT allows the occurrence of more frequent DPCF periods where the performance is higher than the one within DCF periods. It is worth noting that the performance of the DPCF devices can increase up to 400% when the ECT=1 with respect to the case of only executing the DCF.

According to these results, the value of the ECT plays a key role in the performance perceived by each of the group of devices, and thus the fairness between the DCF and the DPCF devices. The higher the ECT, the fairer the network is. However, the lower the overall network performance. This tradeoff should be handled differently depending on the application or the priority that DPCF users should have. In some applications it might be interesting to give higher priority to the DPCF devices, while in other situations it will be more convenient to ensure fairness, letting the DPCF operation to run only when there are no legacy devices.

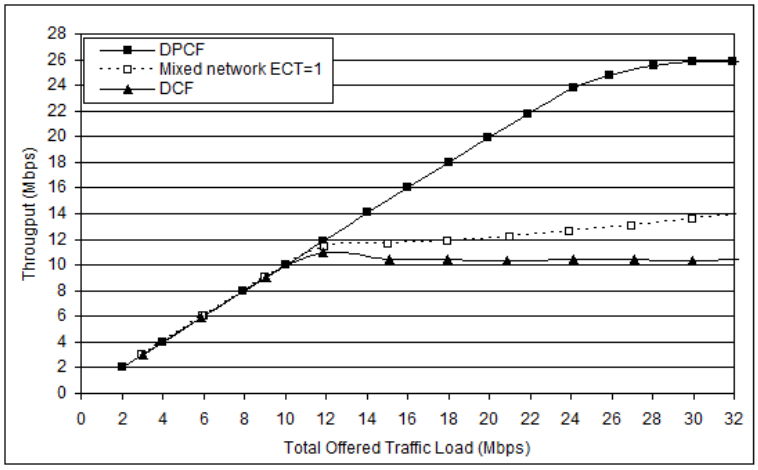

Figure 3.12: Throughput in a Mixed Scenario DPCF-DCF.

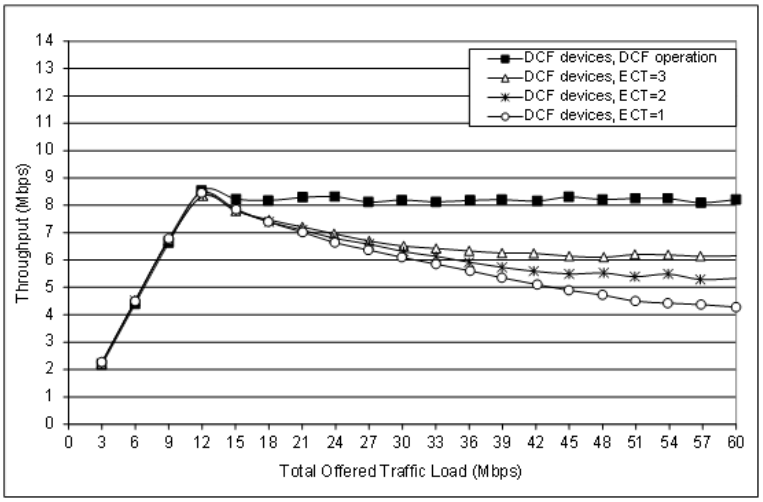

Figure 3.13: Throughput of DCF Devices in a Mixed Scenario.

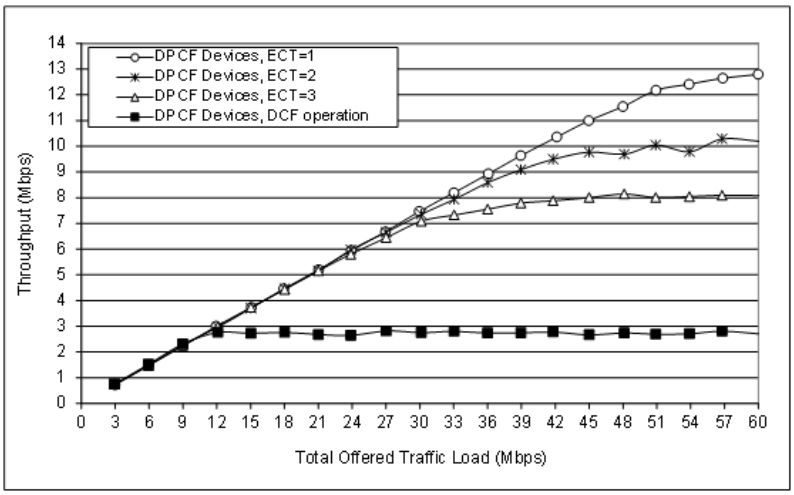

Figure 3.14: Throughput of DPCF Devices in a Mixed Scenario.

3.1.5 Conclusions

DPCF is proposed in EXALTED as a combination of the DCF (of either the IEEE 802.11 or the IEEE 802.15.4) and the PCF of the IEEE 802.11 Standard to operate in distributed M2M capillary networks without a fixed M2M gateway in order to:

1) Enable cooperation among devices and let LTE-M devices provide non-LTE-M devices with LTE-M connectivity.
2) Attain high efficiency in the presence of a high number of devices.

The main idea of DPCF is that the devices of the network get access to the channel by executing the rules of the Standard MAC protocol of either the IEEE 802.11 or the IEEE 802.15.4. Any device which seizes the channel invites the intended destination of its data to become master and establish a temporary dynamic cluster. Within this cluster, the master provides LTE-M connectivity and manages the transmissions of all the neighbors with data ready to be transmitted. The key of this mechanism is that there is no cluster head selection, but clusters are created in a spontaneous manner. This reduces the control overhead to establish a fixed clustering architecture and increases the capability of the network to dynamically adapt to the unpredictable nature of ad hoc networks. Comprehensive performance evaluation of the protocol through link-level computer simulation shows that the new proposal improves the performance of capillary M2M networks when compared to current standards.

In addition, the backwards compatibility of DPCF with legacy IEEE 802.11 or IEEE 802.15.4 networks has been evaluated. It has been presented a simple methodology that facilitates the coexistence of DPCF with legacy IEEE 802.11 or IEEE 802.15.4 networks. A performance evaluation of a mixed network wherein DPCF devices coexist with legacy DCF devices shows that the two protocols can feasibly coexist. By ensuring minimum periods of time wherein all the devices only execute the DCF access, fairness can be attained. Indeed, the results show that by properly balancing the maximum time allowed for clusters and the minimum time reserved for forced DCF access, the performance of the overall network can be tuned at will. Actually, there is a tradeoff between fairness among the different types of devices (DCF and DPCF) and the overall network performance. This trade off might be driven by the specific requirement of each network. Just as a simple example, some preselected devices could execute DPCF only for the transmission of critical control information, while the DCF can be used for the regular transmission of data packets without specific requirements of QoS.

3.2 Cooperative ARQ

3.2.1 Introduction: motivation and objectives

Within the scope of EXALTED, Cooperative Automatic Repeat Request (C-ARQ) has been studied to assess its suitability for use within M2M capillary networks. In the past, the use of C-ARQ schemes has been used to boost throughput and reduce delay in WLANs. EXALTED aims assessing the suitability of exploiting C-ARQ to improve energy-efficiency and thus extend the lifetime of capillary networks based on low-power standards, the most popular being IEEE 802.11 and IEEE 802.15.4.

A C-ARQ scheme consists in the following: due to broadcast nature of the wireless channel, in case of erroneous packet reception, a retransmission may be requested not only from the source, but also from neighboring Non-LTE_M devices acting as helpers, which overheard the original transmission and may experience better channel conditions to the destination than the source. The C-ARQ concept was presented in [29] for the single-helper case, where the effects of the wireless fading channel were modeled as a two-state Markovian process which allowed to determine under what conditions cooperation can be beneficial. In order to extend the scheme to networks with more than one helper, two MAC protocols denoted CoopMAC and rDCF were proposed in [30] and [31], respectively, both inspired in WLANs. In these works, the benefits of cooperation come from the adaptive data rates in the helper-to-destination channel. Namely, the spatial proximity of the helpers to the destination and the related more favorable channel is used to transmit at higher data rates than the one applied in the original source-to-destination channel. Both protocols rely extensively on the IEEE 802.11 Standard [4] in particular, the adaptive transmission rates are based on the PHY layer specification of the standard and the access to a shared broadcast medium is regulated by the MAC layer specification of the standard denoted DCF. Both CoopMAC and rDCF are proactive protocols and always exploit cooperation as a means of communications. A reactive cooperative protocol was proposed in [32], where the C-ARQ scheme that regulates channel access of the helpers is proposed only when a transmission fails. This protocol is named Persistent Relay Carrier Sensing Multiple Access (PRCSMA) and extends the operation of the DCF to include C-ARQ techniques by defining how the retransmissions from the helpers are coordinated.

The main design goal of DCF (within the context of the standard) was throughput maximization, without much emphasis on the energy consumption. Indeed, although the IEEE 802.11 standard does define a power management mechanism, it is usually not commercially implemented. However, as mobility and the capability of autonomous operation (especially required in M2M networks) become more relevant, energy efficiency becomes a primary design goal. Unfortunately, the default operation of DCF leads to a solution whose power management mode is *active* mode. In this mode of operation, a device keeps its transceiver in idle listening also during intervals of inactivity, thus leading to a waste of the energy resources of the battery. For this reason, the design and analysis of energy efficient solutions needs to be addressed and has started to receive some attention from the research community. The throughput and delay of the DCF (and its fine-tuning variants) have been extensively analyzed in the literature using the seminal work of Bianchi [33], based on the idea of modeling the backoff operation of devices with a Markov chain. Recently, the arising need for energy efficiency has triggered many research activities devoted to the energy analysis of DCF. An example can be found in [34] [35], where the authors develop an energy model of DCF and suggest a suitable approximation in order to find the optimal size of the contention window, from the energy point of view, in idealistic channel conditions. To overcome this simplistic channel assumption, in [35], the energy efficiency with regard to the number of nodes has been evaluated by considering a Markov chain to model the channel errors. Another energy model concerning the number of devices in an IEEE 802.11 network

is presented in [36]. In this work, the authors focus on the evaluation of different energy components and their ratio to the total energy consumption. A relevant observation for the analysis of the energy consumption of wireless communication devices was found in [36], stating that overhearing, i.e., listening to packets not intended to a device listening to the channel, takes a significant proportion of the total consumed energy. This is a consequence of the active power management mode of the device that receives all incoming packets and only filters them on the MAC layer to decide whether to process them further or to drop them. To amend the high energy consumption in the active mode, a power safe mode is considered in the IEEE 802.11 Standard. In this mode of operation, the radio of the devices is switched off most of the time and devices only wake up to receive beacons from the Access Point (AP). The AP buffers all the data for the device and notifies it of the pending data in the beacon. Although significant energy savings have been reported for power save mode, most of the devices present on the market still operate in the active mode, although this is changing today due to the emerging M2M applications [6].

The high energy cost of the active mode is wasted when the packets not addressed to the device are dropped after spending energy to decode them. However, active mode can be exploited to improve the energy efficiency of the communications. Indeed, this is what C-ARQ schemes do by letting overhearing devices act as spontaneous helpers upon transmission error. It has been shown in [32] that this protocol can boost the performance of wireless communications in terms of delay and throughput. As far as energy efficiency is concerned, only preliminary computer based performance evaluation has been presented in [37]. However, in order to be able to optimize the system parameters and find optimal operating points, it is necessary to formulate a theoretical model that allows evaluating the energy performance of the protocol. ***This is the first step taken in this task of EXALTED, i.e., validating whether C-ARQ schemes, applied to the IEEE 802.11 Standard can improve energy-efficiency of wireless communications and thus extend life time of M2M devices within the capillary network.***

After studying the behavior of C-ARQ when applied to the IEEE 802.11 standard, ***the second step is the adaptation of C-ARQ techniques to the IEEE 802.15.4*** [5]. It is necessary to evaluate whether C-ARQ techniques can still improve the energy efficiency under the three specific constraints imposed by the low power operation:

1. The absence of data rate adaptation. Recall that C-ARQ strategies known in the literature base their performance benefits on the adaptive data rate capabilities of wireless transceivers. Using the IEEE 802.15.4, all devices transmit at a constant data rate significantly lower than in the IEEE 802.11 standard.
2. Data payloads typical for capillary M2M networks are significantly smaller from the payloads applied in the evaluation of C-ARQ in the literature, which use big data payloads associated to WLAN traffic. Therefore, this analysis is suitable for the Internet data traffic or multimedia streaming, but inappropriate for capillary M2M networks mainly designed for uplink traffic and small data payloads.
3. The absence of overhearing because the devices duty cycle, i.e. switch off the radio transceiver when not active in order to save energy. Therefore, a mechanism needs to be proposed to wake up the helper in order to obtain a packet generated by the other device.

Some works are already available related to duty-cycling and cooperation, such as the work in [38], which is based on the concept of preamble sampling algorithms used in low traffic networks. The key idea of preamble sampling algorithms is that every packet is preceded with a long enough preamble to be detected by all the devices in the communication range during a complete duty-cycle. The cooperative protocol presented in [38] uses the preamble sampling concept to wake up the potential helpers. The performance was evaluated by

computer simulation in Rayleigh fading channels. The performance metrics used were the consumed energy per packet and the data delivery ratio. Although results show that cooperation improves the reliability significantly, the consumed energy of the proposed algorithm is either close to the reference non-cooperative protocol, or even higher.

The suitability of executing C-ARQ schemes in capillary M2M networks without data rate adaptation remains an open issue that has recently started to receive attention. The conditions under which a C-ARQ scheme proves beneficial in the context of low power networks without data rate adaptation under realistic wireless channel conditions need to be studied. To this aim, in EXALTED it is analyzed the energy-efficiency and reliability of a C-ARQ scheme suitable for capillary M2M networks. It is worth emphasizing that while the energy efficiency was not the major concern when C-ARQ schemes were first proposed, it becomes the essential performance metric in capillary M2M networks and, therefore, the benefits of C-ARQ schemes need to be re-examined. For example, considering the energy consumption associated to overhearing presents an additional cost that was irrelevant before, but has a key role in low power networks. Next it is shown that C-ARQ schemes can improve the energy efficiency in harsh shadowing environments even when a constant rate transmission is applied. It is considered the widely spread IEEE 802.15.4 Standard for low-power low-rate networks as a study case. This standard does not include data rate adaptation, but it defines a constant data rate of 250 Kbps for the 2.4 GHz band. In addition, the maximum size of data packets is defined to be of 127 bytes, i.e., significantly smaller than in Wireless Local Area Networks (WLANs) where C-ARQ have been typically studied and whose maximum data packet size is 2312 bytes, and the typical value is 1500, equivalent to the average data size of internet packets.

Therefore, in this report two main contributions of EXALTED within this topic are presented. They have been split in two separate parts:

1. In the first part, the energy model for PRCSMA (cooperative protocol for WLANs) is formulated. The model is next used to compare the energy efficiency of PRCSMA with that of a traditional non-cooperative ARQ scheme where retransmissions are only performed by the source. The model is validated through computer simulations for a wide range of system parameters. The conditions under which PRCSMA outperforms non-cooperative ARQ are identified and discussed.
2. In the second part, the C-ARQ scheme is examined under the specific constraints of low power networks including sleep mode of the device, constant transmission rate, and small data payloads. The performance metrics examined are the energy efficiency (measured in energy consumed per useful transmitted bit) and reliability of the cooperative protocol (number of retransmissions). Again, the conditions under which cooperation proves beneficial are identified and the grounds for further research established.

3.2.2 Achieving energy-efficiency through cooperative retransmissions

The first part is organized as follows. The PRCSMA protocol is first briefly described. Next, the considered scenario is defined as well as the energy model used for both the energy efficiency analysis of a non-cooperative ARQ scheme and PRCSMA. The proposed theoretical model is validated through computer simulations and the energy efficiency of the two schemes is compared.

3.2.2.1 PRCSMA overview

Although PRCSMA has not been designed within EXALTED, a brief summary of it is presented in this section to make the report self-contained, as some of the contributions

presented in this task of EXALTED are based on the operation of PRCSMA. The interested reader is referred to [32] for a complete description of the protocol.

PRCSMA is an innovative MAC protocol that was specifically designed to coordinate the retransmissions from the helpers of a Cooperative-ARQ scheme in short-range WLANs. The rules of PRCSMA are based on the DCF of the IEEE 802.11 Standard, thus enabling backwards compatibility. The protocol works as follows. Consider a scenario formed by a source, a destination, and a group of devices within the transmission range of both the source and the destination. The source transmits packets to the destination following any MAC protocol rules, and it is assumed that the group of surrounding devices can overhear all ongoing transmissions. These are the devices in active mode running an application that requires constant monitoring of the channel. If a device receives and decodes without errors a data packet not addressed to its address, it does not discard it, but it buffers the packet for a certain time interval in a special queue denoted cooperative queue. When the destination receives a data packet with unrecoverable errors, instead of requesting a retransmission from the source, it broadcasts a Call for Cooperation (CFC) control packet and initiates a **cooperation phase**. Those devices that buffered the original packet from the source and receive this CFC packet become active helpers and attempt to retransmit the original packet. In order to avoid a certain collision, the helpers execute a backoff before the first transmission attempt. To do so, each helper selects at random a value for the contention window within the range *CW=[0,W]*. For the randomly selected number of time slots with a constant duration of σ seconds, each helper senses the activity in the channel. If the channel is idle within a slot, the counter is decreased by one unit. If a transmission in the channel is detected, the counter is frozen until the ongoing transmission ends. The countdown is resumed when the channel becomes idle again. When the backoff counter value reaches zero, the helper attempts to transmit. There are three possible outcomes of this transmission attempt:

1. **More than one helper transmits:** there is a collision at the intended receiver and the packet cannot be decoded at the destination. Consequently, the destination takes no further action. Silence from the destination indicates to the helpers that the cooperation phase continues.
2. **Only one helper transmits but the packet is received in error by the destination:** the destination receives and decodes the packet but takes no action since the packet was received erroneously. The cooperation phase continues.
3. **Only one helper transmits and the packet is successfully received by the destination:** the destination transmits an Acknowledgement (ACK) packet to notify the end of the cooperation phase.

Note that an ACK is transmitted only when the destination device is able to decode the original packet. If a helper transmits but does not receive the ACK packet, it resets the backoff counter and attempts a new transmission (it has to compete for the channel again). From the perspective of each individual helper, cooperation might end because of own, but also other helper's successful retransmission.

According to this operation, the benefits of C-ARQ are drawn from the adaptive rate scheme that exploits favorable channel conditions between the helpers and the destination. This allows helpers to transmit at a higher rate than the one used in the main source-to-destination channel. When the channel conditions between the source and all the receiving devices are unfavorable, it might happen that none of the potential helpers has an errorless copy of the original packet. In this case, the cooperation phase ends after the expiration of a predefined timeout period, after which retransmission is requested from the source.

3.2.2.2 Scenario and energy model of PRCSMA

Consider a scenario that corresponds to a gateway communicating with a group of devices in the **downlink**, where the devices help each other to decode packet transmissions, or to a device communicating in the **uplink** with the M2M gateway and having a number of devices helping to reach the gateway with a given reliability condition.

More specifically, it is considered the scenario shown in Figure 3.15. It represents a data source and a number of devices in its communication range. It is assumed that the subset of all the devices runs in active power management mode and thus monitors the channel continuously. Once a destination device is selected for transmission from the source, the number of potential helpers, i.e., active devices in the transmission range of both the source and the destination, is denoted by *n*. The scenario is thus formed by a number of *n+2* devices, i.e., source, destination device, and *n* potential helpers.

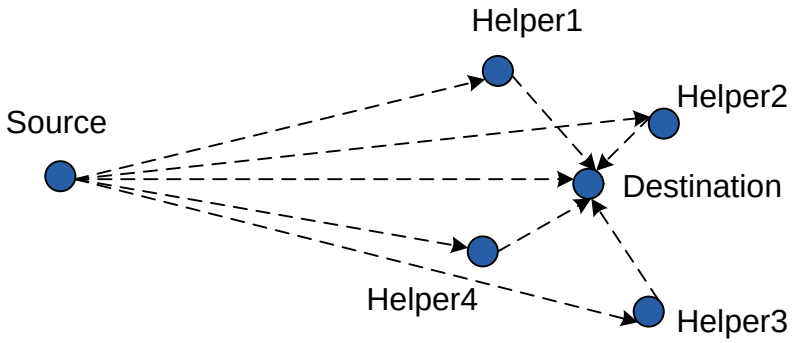

Figure 3.15: M2M capillary network formed by a number of Non-LTE-M devices.

The average packet error rate from the source to the destination is denoted p_{SD}. The packet error rate from source to helper *i*, *i={1,...,n}*, is $p_{SR1} \approx p_{SR2} \approx p_{SRi} \approx p_{SRn} = p_{SR}$ and it is assumed that $p_{SD} = p_{SR}$. It is also assumed that the packet error rate from helper *i* to destination is $p_{R1D} \approx p_{R2D} \approx p_{RiD} \approx p_{RnD} = p_{RD}$ because the channel conditions between any helper and the destination are i.i.d. (independent and identically distributed). Upon a transmission from the source, out of the *n* potential helpers, only *k* will receive the packet from the source without errors and thus become actual active helpers. Indeed, the average number of active helpers can be calculated as

$$E[k]=\lceil n(1-p_{SD}) \rceil, \quad (2)$$

where $\lceil x \rceil$ indicates the closest greatest integer number to *x*, and it is taken to account for the worst-case collision probability.

Here the focus is put on the basic channel access of PRCSMA, i.e., without Request-to-Send and Clear-to-Send handshake between the helpers and the destination, to reduce control signaling.

Three transceiver states can be differentiated:

1. ***transmit***, with respective consumption power P_T.
2. ***receive***, with respective consumption power P_R.
3. ***idle***, with respective consumption power P_{IDLE}.

Therefore, the energy consumed during a period of T_x seconds in each of these modes can be expressed as E_x^T, E_x^R, E_x^I, respectively:

$$E_x^T = P_T \cdot T_x,\ E_x^R = P_R \cdot T_x,\ E_x^I = P_{idle} \cdot T_x. \tag{3}$$

The different values that T_x can take are T_{SIFS} and T_{DIFS} for the duration of a SIFS a DIFS, respectively, and T_{ACK} and T_{CFC} for the duration of the transmission of an ACK and CFC packets, respectively.

As far as data packet transmission is concerned, it is necessary to differentiate between the transmissions from the source and from a helper. The packets are considered to be of constant bit-length and it is assume that, although the data transmission rates are adaptive, once they are established, they remain constant for the duration of the communication session. The bit length of a data packet is denoted by L and R_{SD} and R_{RD} are defined as the transmission rates from source to destination and from helpers to destination, respectively. It is possible to express

$$\begin{aligned} E_{SD}^T &= P_T \cdot \frac{L}{R_{SD}}, E_{SD}^R = P_R \cdot \frac{L}{R_{SD}} \\ E_{RD}^T &= P_T \cdot \frac{L}{R_{RD}}, E_{RD}^R = P_R \cdot \frac{L}{R_{RD}}, \end{aligned} \tag{4}$$

where E_{SD}^T / E_{SD}^R correspond to the energy consumption in a transmission/reception between source and destination, and E_{RD}^T / E_{RD}^R to the energy consumption in a transmission/reception between a helper and the destination.

According to [39], the energy efficiency of the protocol can be defined as

$$\lambda = \frac{total\ amount\ of\ delivered\ data\ (bits)}{total\ energy\ consumed\ (Joule)}. \tag{5}$$

In the next subsections, it is analyzed the energy expenditure and energy efficiency of a traditional non-cooperative ARQ scheme, and that of a C-ARQ with PRCSMA.

3.2.2.3 Energy analysis for non-cooperative ARQ

Recall the scenario in Figure 3.15. Every transmission from the source is received by the destination and by all the potential helpers. A non-cooperative ARQ is considered. This means that, in the case of erroneous reception of a packet, it will not be acknowledged, thus triggering a retransmission from the source along the same transmission path.

The total energy spent in the network for a transmission from the source can be computed as

$$E_S = (n+2)E_{DIFS}^I + E_{SD}^T + (n+1)E_{SD}^R + (n+2)E_{SIFS}^I. \tag{6}$$

Note that this expression does not account for the energy spent in the acknowledgement process. Indeed, if the packet is received and acknowledged successfully by the destination, the energy consumption associated to a successful transmission from the source can be defined as

$$E_{SS} = E_S + E_{ACK}^T + (n+1)E_{ACK}^R. \tag{7}$$

Similarly, if the packet is received with errors, all the nodes of the scenario will listen to the channel for the duration of ACK timeout, here assumed to be equivalent to the duration of an

ACK packet. The energy spent when a transmission from the source results in error can be computed as

$$E_{SE} = E_S + (n+2)E^I_{ACK}. \tag{8}$$

Finally, the energy efficiency of a Non-cooperative ARQ scheme can be calculated as

$$\lambda_{NC} = \frac{L}{(1-p_{SD})E_{SS} + p_{SD}\left(E_{SS} + \frac{1}{1-p_{SD}}E_{SE}\right)} = \frac{L}{E_{SS} + \frac{p_{SD}}{1-p_{SD}}E_{SE}}, \tag{9}$$

where the first component of the sum in the denominator stands for successful receptions and the second component accounts for the average number of retransmissions from the source.

3.2.2.4 Energy analysis for PRCSMA

The embedded Markov chain proposed in [32] describes the counter state of a helper executing the PRCSMA protocol ***when a cooperation phase is running***. This model is based on the work presented in [7] for the modeling of the DCF, and is used to model the sub-network formed by the active helpers once a cooperation phase has been initiated. The probability that the counter of a helper reaches zero and, consequently, attempts to transmit a packet, is denoted by P_0. This parameter can be used to calculate the probabilities of different sub-network states that depend on the counter states of *all* the active helpers for a given time slot. P_I is the probability that the whole sub-network formed by the active helpers is idle. P_S is the probability that only one helper is transmitting and the transmission was successful and P_E is the probability that only one helper transmits and the transmission is received with errors. Finally, P_C is the probability that more than one helper transmit and thus collide. These probabilities depend on the number of active helpers *k*. However, all the *n* potential helpers monitor the activity on the channel and account for the total energy expenditure.

The following energy consumption states can be differentiated in the sub-network formed by the active helpers (without accounting for the source and the intended destination) when a cooperation phase is running:

1. **Idle.** All the helpers remain in the idle state because none of the backoff counters have expired. The total energy spent in the network in this case is
$$E_I = (n+2)E^I_\sigma, \tag{10}$$
where σ is the duration of the slot time.

2. **One transmission.** The counter of only one helper reaches zero. The total energy spent in the network in this case is
$$E_R = (n+2)E^I_{DIFS} + E^T_{RD} + (n+1)E^R_{RD}. \tag{11}$$
With probability 1-p_{RD} this transmission will be successful and will result in the end of the cooperation phase. With probability p_{RD}, it will be received with errors and the cooperation phase will continue.
3. **Collision.** The total energy consumption involved in a collision depends on the number of colliding helpers. The energy spent when *m* helpers collide can be computed as
$$E_C(m) = (n+2)E^I_{DIFS} + mE^T_{RD} + (n+2-m)E^R_{RD}. \tag{12}$$

Next step is now the computation of the expected energy spent during the contention phase defined as the cooperation phase subtracting the actual time devoted to successful transmissions. Towards this end, the probability of successful transmission from a helper is denoted by P_S, and thus the expected number of slots in the contention phase is

$$E[X]=\frac{1}{P_S}-1 \tag{13}$$

where the final successful slot has been subtracted. Consequently, the expected energy spent in the contention phase accounts for the energy spent in *i)* the idle state, *ii)* erroneous transmissions, and *iii)* collisions.
The probabilities of being in each of these states are conditioned on the probability of not being successful 1-P_S. Therefore, the expected energy in the contention phase is obtained as

$$E_{cont}=E[X]\left(\frac{P_I}{1-P_S}E_I+\frac{P_E}{1-P_S}E_R+\frac{P_C}{1-P_S}E_C(m)\right), \tag{14}$$

where P_C is the probability of collision and can be computed as

$$P_C=\sum_{m=2}^{k}P_C(m) \tag{15}$$

$P_C(m)$ is the probability of having *m* helpers colliding when there is a collision in the sub-network formed by the active helpers and can be expressed as

$$P_C(m)=\binom{k}{m}P_0^m(1-P_0)^{k-m},\ 2\le m\le k. \tag{16}$$

Therefore, the total average energy spent in collisions can be computed as

$$\sum_{m=2}^{k}P_C(m)E_C(m)=(n+2)(E_{DIFS}^I+E_{RD}^R)\cdot\left[1-(1-P_0)^k\left(1+\frac{kP_0}{1-P_0}\right)\right]+kP_0(1-(1-P_0)^{k-1})(E_{RD}^T-E_{RD}^R). \tag{17}$$

To complete the energy model, it is necessary to consider the case when no potential helper has received the original packet without error (i.e., *k=0*), and thus the cooperation fails, since there is no helper able to retransmit the original packet. In this case, all the nodes of the network remain idle until a cooperation timeout expires. The destination then sends a negative ACK packet in order to inform the source that a new retransmission is required. In terms of energy consumption, this packet is equivalent to an ACK packet. The duration of the timeout is arbitrary, but it is considered for this analysis that it can be computed as the duration of the maximum contention window, i.e., of duration W·σ. Therefore, the energy spent during a cooperation timeout can be computed as

$$E_{to}=(n+2)WE_\sigma^I. \tag{18}$$

Finally, the total energy spent in a cooperation phase can be written as

$$\begin{aligned}E_{coop}&=E_{CFC}^T+(n+1)E_{CFC}^R+(n+2)E_{SIFS}^I+p_{SD}^nE_{to}+\\&+(1-p_{SD}^n)\left[E_{cont}+E_R+(n+2)E_{SIFS}^I\right]E_{ACK}^T+(n+1)E_{ACK}^R.\end{aligned} \tag{19}$$

If the cooperation fails, the source will retransmit the original packet. The average number of retransmissions is computed as

$$N=\frac{1}{1-p_{SD}^{n+1}}, \tag{20}$$

because it is sufficient that either the destination or any of the helpers receives the packet correctly.

All the components can be summed up to compute the energy efficiency of PRCSMA as

$$\lambda_C = \frac{L}{\frac{1}{1-p_{SD}^{n+1}}\left[(1-p_{SD})E_{SS} + p_{SD}(E_S + E_{coop})\right]}. \quad (21)$$

The first component in brackets in the denominator stands for successful receptions from the source and the second is attributed to the entire cooperation process starting with the erroneous reception from the source and including all the different energy modes involved in the cooperation phase.

3.2.2.5 PRCSMA energy efficiency evaluation

The validation of the analysis presented in the previous section has been done through computer simulations executed in a custom MATLAB simulator. The system parameters are given in Table 3-2 and they have been set according to the recommended values in the IEEE 802.11 Standard. It has been shown in the literature that the energy spent for receiving a packet is approximately the same as the energy spent for listening to the channel [40] and therefore $P_R=P_{idle}$ is adopted.

In the simulation, devices execute the protocol rules and the energy expenditure is recorded for each of the system states. The network state depends on whether a packet from the source was received erroneously by the destination, thus inducing the cooperation phase regulated by randomly set backoff counters. To calculate the energy efficiency, the total data delivered to destination is divided by the total energy spent as defined in (1.4). None of the probabilities developed in the energy model to yield the expected energy spent in the different system states were used in the simulations.

Table 3-2: Simulation Parameters.

Parameter	Value	Parameter	Value
DIFS	50 μs	R_{SD}	24 Mbps
SIFS, σ	10 μs	R_{RD}	54 Mbps
ACK, CFC	14 Bytes	R_C	6 Mbps
DATA	512 Bytes	P_{tx}	1900 mW
W	16	P_{rx}, P_{idle}	1340 mW

Figure 3.16 shows a comparison between the energy efficiency of non-cooperative ARQ scheme and PRCSMA for varying values of p_{SD} and p_{RD}. The markers in the figure stand for simulation results and were omitted in the legend to avoid its overloading.

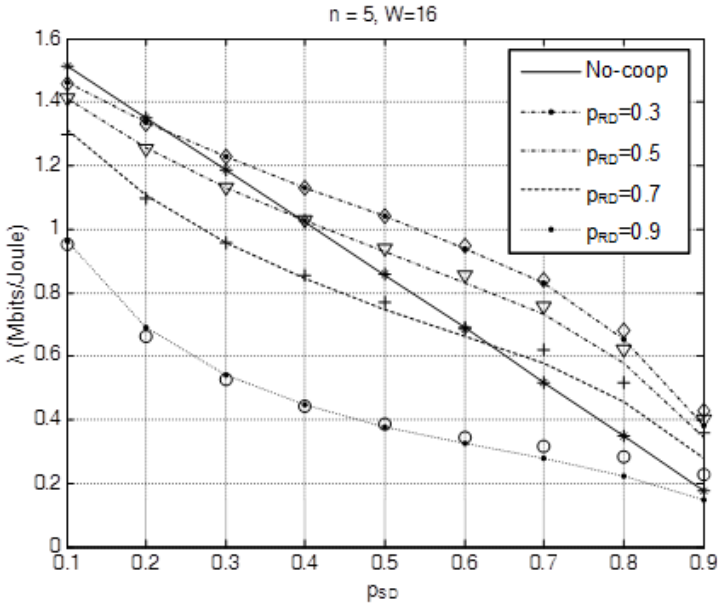

Figure 3.16: Energy efficiency of Non-cooperative and Cooperative-ARQ scheme for varying channel quality from source- and helper-to-destination. Markers correspond to simulated values and lines represent the values obtained with the theoretical model.

One may first observe the good agreement between the theoretical model and the simulation which confirms the validity of the analysis done in section 3.2.2.4.

Regarding performance, it is worth seeing that PRCSMA performs best for the intermediate values of source-to-destination quality. When p_{SD} is small, the cooperation gain does not compensate the protocol overhead cost in terms of energy consumption. As p_{SD} increases, the benefits of PRCSMA are clearly visible due to the increased number of successful cooperation phases whose energy cost is smaller than performing retransmissions from the source at a lower transmission rate. However, it may be observed that the energy-efficiency of PRCSMA drops after p_{SD} becomes greater than a certain value (p_{SD}>0.7 in Figure 3.16). This happens because the channel quality from the source is so low that often there are no active helpers capable of retransmitting and so the packet will be, eventually, retransmitted from the source. The goal will be finding this turning point.

Because of the relative long duration of data packet transmissions, the energy spent for transmissions and overhearing is greater than energy spent on the transmission of control packets or idling until the timeout expires. Therefore, the most significant terms in (1.20) are E_{cont} and E_R. Looking at the energy-efficiency expression (1.20), it is possible to see that the influence of channel on the contribution of these components is $p_{SD}(1-p_{SD}^n)$. Calculating $\frac{\partial p_{SD}(1-p_{SD}^n)}{\partial p_{SD}} = 0$ the turning point obtained from the above approximation is

$$p_{SD}^* = \left(\frac{1}{n+1}\right)^{\frac{1}{n}}. \quad (22)$$

For *n=5*, p_{SD}^*=0.7 as Figure 3.16 confirms. Therefore, it is possible to state that for p_{SD}>p_{SD}^*, cooperation gains are reduced.

Figure 3.16 also shows the energy efficiency for different values of p_{RD}. As expected, when the helper-to-destination packet error rate is high, cooperation does not produce any benefit. However, the proximity of helpers implicates small values of p_{RD} in practical scenarios. This enables using the higher transmission rate than in the original channel. Therefore, in many scenarios with adaptive-rate, C-ARQ is the most energy-efficient ARQ approach.

Since PRCSMA is based on CSMA, its performance depends on the good tuning of the contention parameters. To evaluate this, the dependence of energy efficiency on the contention window size is estudied. The main results are shown in Figure 3.17. An immediate conclusion can be attained: collisions have a great cost in terms of energy. Note that when *W=4*, the energy-efficiency is greatly reduced compared to other configurations, and performance of the cooperative retransmission scheme is only efficient when the channel quality between source and destination is really poor. On the other hand, an increased probability of the idle state during the cooperation phase, caused by a large value of *W*, does not have a major impact on the overall energy efficiency (recall that in this study devices do not sleep as this study is based on the IEEE 802.11 Standard).

According to these results, the most energy efficient approach is to keep the collision probability very low, to avoid the waste of energy in useless transmissions, by setting high values of the contention window (*W*), even at the cost of longer idle periods.

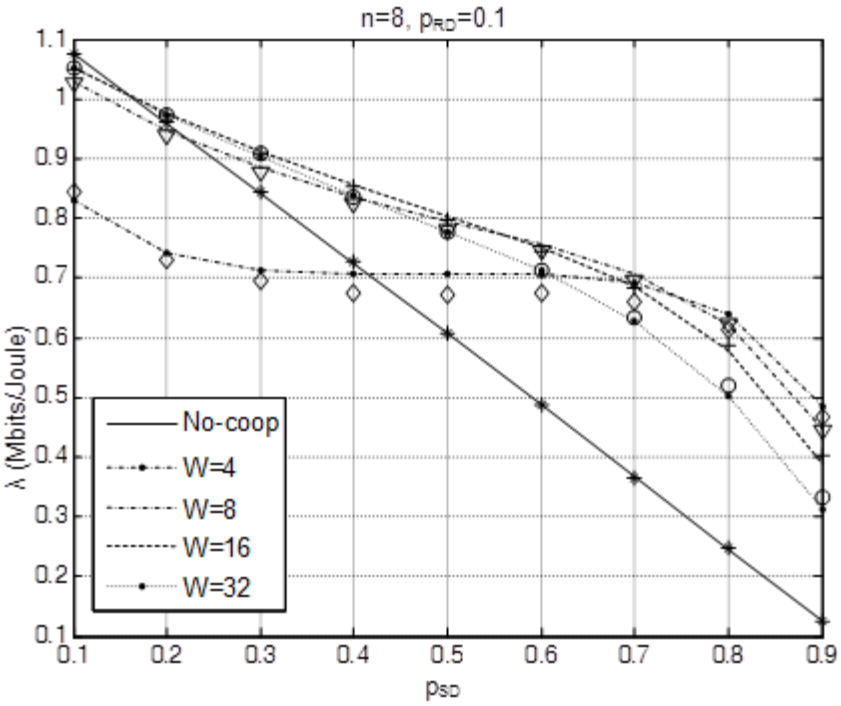

Figure 3.17: Energy efficiency of non-cooperative and cooperative ARQ scheme for varying contention window size. Markers correspond to simulation and lines represent the values obtained with the theoretical model.

3.2.2.6 Conclusions

Within this task of EXALTED, it has been evaluated the energy-efficiency of a cooperative retransmission scheme within the context of a capillary network based on the IEEE 802.11. Results suggest that the gains of cooperation stem from the adaptive data rate that allows some devices to retransmit faster than the source and thus reduce the retransmission time. However, typical M2M deployments will be based on technologies specially designed for low-

power low-range networks, such as the IEEE 802.15.4 Standard. For this reason, once acknowledged that cooperation at the MAC layer can be an energy-efficient solution for wireless short-range network, next section analyzes whether these gains can be attained in the context of low-power low-rate networks based on the IEEE 802.15.4 Standard.

3.2.3 C-ARQ in energy-constrained M2M capillary networks

In the second part of the section, it is assessed whether the energy-efficient cooperative retransmission approach studied and validated for short-range networks based on the IEEE 802.11 can be transposed to the limitations posed by energy-constrained networks based on simpler technologies such as the IEEE 802.15.4. This technology does not provide data rate adaptation, uses shorter data payloads, and enables duty-cycle operation where some devices can alternate between on and off periods to save energy. Therefore, the aim of this section is to evaluate whether cooperation can yield energy-saving gains into M2M capillary networks based on low-power technologies.

Since low-power technologies such as the IEEE 802.15.4 Standard rely on constant transmission rates without data rate adaptation, it is expected that the benefits of cooperation, if any, will come from overcoming bad channel conditions, e.g. substituting a blocked path by an obstacle by a two-hop Line-of-Sight communication path, and thus reduce the number of required retransmissions. In the non-cooperative scheme when plain ARQ is applied, all the retransmissions during the unfavorable shadowing state will fail until the outage limit is reached and the packet is discarded. In a cooperative scheme, the retransmissions may come from a neighboring helper with better chances of success due to the independent channel conditions. Recall that the helper is an ordinary Non-LTE-M device with enabled cooperative capabilities at the MAC layer.

This section is organized as follows. The considered system model for low-power short-range capillary M2M networks is first introduced including the scenario and the adopted channel model. Then, the analysis of the energy efficiency is given, including the analysis of the parameters needed to calculate the energy efficiency. Finally, the results are given and discussed.

3.2.3.1 Scenario for capillary M2M networks

The focus is put on the uplink transmission from a group of n M2M devices to a single common coordinator, e.g. an M2M capillary gateway. The scenario is shown in Figure 3.18. A sub-group of the n devices is shadowed by a large obstacle, while the rest of devices have a line-of-sight (LOS) path with the M2M gateway. Due to the blocking obstacle, the probability that all the transmissions from the shadowed devices to the gateway fail is very high. It is assumed that an alternative two-hop path exists through a device acting as a helper, which experiences more favorable channel conditions. This is a two-hop path expanding from the source to the helper and from the helper to the gateway, which enables the execution of cooperative strategies.

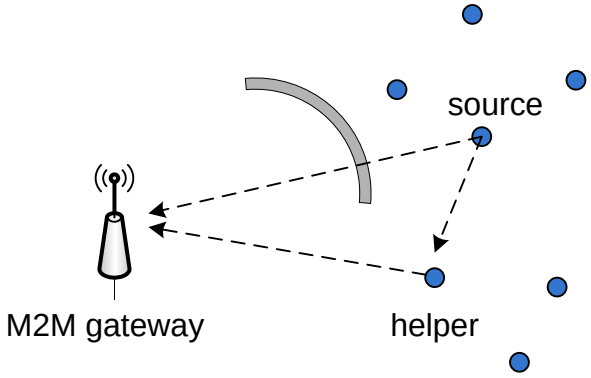

Figure 3.18: The studied scenario consisting of M2M gateway, Non-LTE-M devices and obstacles.

At the MAC layer, it is considered the beacon-enabled access mode described in the IEEE 802.15.4 standard for short-range low-power networks [5]. The gateway is not energy-constrained and thus can listen to the channel constantly and periodically transmits a beacon. The devices are energy-constrained and remain in the sleep state unless they have data to transmit to the gateway. Whenever a device has data to transmit, it executes a random backoff before waking up and switching the radio on to perform a Clear Channel Assessment (CCA), i.e., to assess whether the channel is idle or busy. A transmission is started if the channel is found idle. Otherwise, a new backoff is executed. In addition, all the devices need to periodically wake up in order to synchronize to the beacons. Therefore, it is essential that all the devices listen to the beacons even under unfavorable channel conditions with the gateway. It is worth observing that the devices typically set the transmission power to P_t*=0 dBm* for data transmissions in order to save energy. However, the maximum allowed transmit power depends on the local regulation but it is generally limited to 10 dBm. Since the gateway is not battery powered it is assumed that the beacon is always transmitted at the maximum allowed power. The obstacle between the devices and the gateway introduces additional partition loss. The loss varies depending on the type of material, e.g. a large obstacle like a concrete wall attenuates the signal by 13 dB [41]. Taking into account the additional power budget of the beacon and the fact that its length is smaller than the data packet length, it can be assumed that the beacon is always received by all the devices without errors and can thus be used to coordinate the cooperation process, as described in the next subsection.

3.2.3.2 Retransmission strategies for capillary M2M

Whenever the gateway receives a data packet from a device and cannot decode it without errors, it can decide whether to adopt a non-cooperative retransmission and request a retransmission from the same device, or initiate a cooperation phase, requesting neighboring devices to assist the transmission.

In the case of executing a non-cooperative retransmission scheme, the gateway can request retransmission from the source using the same transmission path. In order to save energy, the maximum number of transmission attempts, denoted by N_{max}, is set to a low value. For example, the IEEE 802.15.4 Standard recommends a maximum of 4 transmission attempts per data packet.

In the case that the gateway opts for a cooperative retransmission scheme, then, the cooperative approach proposed within EXALTED works as follows. The cooperative process is depicted in Figure 3.19.

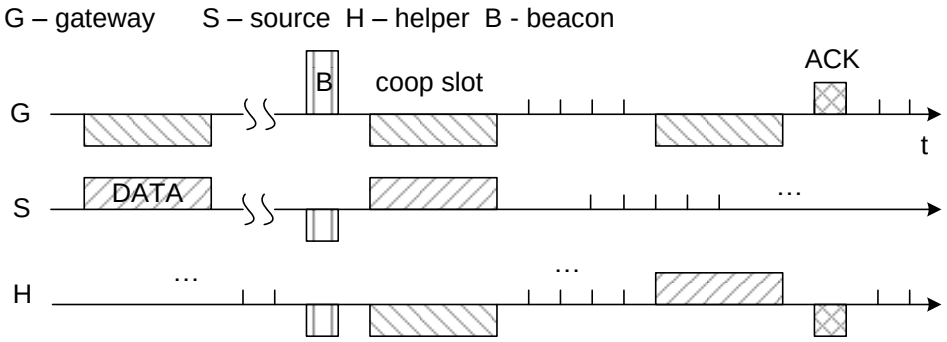

Figure 3.19: Cooperation diagram; packet is placed above the time line when it is being transmitted, below the time line when being received.

A source device transmits a data packet that is received by the gateway with unrecoverable errors. Therefore, the gateway then reserves a ***cooperation slot*** and announces it in the next beacon, thus initiating a cooperation phase. The cooperation slot is similar to the Guaranteed Time Slot (GTS) considered in the IEEE 802.15.4 Standard. Since all the devices listen to the beacon, the device acting as helper knows when it needs to wake up in order to receive the retransmitted packet from the source. The packet is then retransmitted in the cooperation slot by the source. The subsequent retransmissions continue from the helper up to the maximum number of allowed transmission attempts N_{max}. The system is considered to be in outage if the packet is still not successfully delivered after N_{max} number of attempts, in which case it will be discarded.

Two different cooperative strategies are considered in this study:

1. **Cooperation with helper selection**, where the gateway indicates in the beacon the selected helper candidate. This decision can be based on locally available Channel State Information (CSI) regarding all or some of the devices. The specific helper selection algorithm is out of the scope of EXALTED.
2. **Cooperation without helper selection**, where a helper with unknown shadowing state is chosen randomly within the list of devices associated to the gateway.

3.2.3.3 Channel model for capillary M2M

A realistic wireless channel model is considered, where a signal from the transmitter to the receiver experiences three effects: pathloss, shadowing, and multipath fading. Considering the effects of pathloss, the average received power is

$$P_r(dBm) = P_t - PL(d_0) - 10\alpha \log_{10} d, \quad (23)$$

where P_t is the transmission power, $PL(d_0)$ is the pathloss at a reference distance d_0, α is the pathloss exponent, and d is the distance from the transmitter.

μ is defined as the average Signal-to-Noise Ratio (SNR) at the receiver without considering shadowing or multipath fading effects, and it can be expressed as

$$\mu(dB) = P_r - P_n. \quad (24)$$

P_n is the average receiver thermal noise and it can be computed as [42]

$$P_n = (F+1)\,k\,T\,B, \quad (25)$$

where F is the noise figure, k is Boltzmann constant, T is the temperature in Kelvin, and B is the signal bandwidth.

Apart from pathloss, the signal at the receiver experiences the effects of shadowing and multipath fading. The instantaneous value of the SNR is denoted by γ. Multipath effects of the wireless channel are modeled as a Rayleigh block fading process that remains constant for the duration of the transmission of a single packet but changes for each retransmission.

In addition, the average value of γ, denoted $\bar{\gamma}$, represents the average SNR considering the effects of shadowing. The instantaneous value of $\bar{\gamma}$ depends on the shadowing conditions, but it is considered that it remains constant for at least the period of time between two consecutive beacons and, therefore, all the packet retransmissions from the same source or helpers experience the same shadowing state in average. Therefore, the probability density function (pdf) of γ has an exponential distribution (derived from the Rayleigh distribution of the amplitude) conditioned on $\bar{\gamma}$, i.e.,

$$p_{\gamma}(\gamma \mid \bar{\gamma}) = \frac{1}{\bar{\gamma}} e^{-\frac{\gamma}{\bar{\gamma}}}. \tag{26}$$

In its turn, the pdf of $\bar{\gamma}$ is lognormally distributed conditioned on μ and with standard deviation σ, both expressed in dBs, and can thus be expressed as

$$p_{\bar{\gamma}}(\bar{\gamma} \mid \mu) = \frac{10}{\ln 10 \sqrt{2\pi}\sigma\bar{\gamma}} \exp\left[-\frac{(10\log_{10}\bar{\gamma} - \mu)^2}{2\sigma^2}\right]. \tag{27}$$

According to this model, the bit and packet error rates at the receiver can be computed as follows. It is considered the O-QPSK modulation specified in the IEEE 802.15.4 at the 2.4GHz frequency band. If assumed perfect demodulation with coherent detection in the presence of Additive White Gaussian Noise (AWGN), O-QPSK has the same bit error rate as QPSK, and it is possible to express the bit error probability as in [5].

$$P_b = Q\left(\sqrt{2\frac{E_b}{N_0}}\right). \tag{28}$$

The packet error rate assuming independent bit errors (which holds true for block fading channels and AWGN) is

$$P_p = 1-(1-P_b)^L, \tag{29}$$

where *L* is the packet length in bits. In the IEEE 802.15.4, Direct Sequence Spread Spectrum (DSSS) is used to combat interference in the license-free band. Each data symbol consisting of four bits is mapped into a 32-chip sequence and then sent over the wireless channel. To relate μ and E_b/N_0 it is used the expression

$$\frac{E_b}{N_0} = \mu \frac{B_N}{R_b}, \tag{30}$$

where B_N is the noise bandwidth and R_b is the data bit rate, therefore B_N/R_b characterizes the DSSS gain.

3.2.3.4 Energy model for capillary M2M

To evaluate the energy consumption, it is assumed that each device has three operating modes:

1. **Transmitting**, with associated power consumption P_{tx}.
2. **Receiving**, with associated power consumption P_{rx}.
3. **Idle or sleep**, i.e., with the radio switched-off and associated power consumption $P_s \approx 0$.

According to the operation of state of the art sensor devices, it is assumed that $P_{tx} \approx P_{rx}$. This means that the energy spent for packet transmission is approximately the same as the energy spent for the reception, which includes the actual reception of a transmission or the execution of the CCA function, i.e., listen to the channel.

The focus is on the energy spent by the devices, because of the assumption that the gateway is mains powered, and the emphasis is on evaluating whether the use of cooperation within the capillary network can extend the lifetime of the simple devices.

Finally, the two following assumptions are adopted for the energy consumption evaluation:

1) In the non-cooperative scheme, all the other devices of the network are in sleep mode when a device is transmitting to the gateway.
2) In the cooperative schemes, just one helper is woken up for the cooperation phase, while the others are in sleep state.

3.2.3.5 Energy efficiency analysis

The energy efficiency is calculated as defined in (1.4). Recall that the energy efficiency of the scheme has been defined as the ratio of the total number of successfully received bits to the total energy spent by all the devices (excluding the gateway) in delivering them. The gateway is excluded of this metric because it is not battery powered and, therefore, its energy consumption is irrelevant for the lifetime of the system.

In the non-cooperative case, the energy efficiency can be expressed as

$$\lambda_{NC} = \frac{(1-P_{out})L}{\bar{\bar{N}}_{tx} P_{tx} \frac{L}{R_b}}, \tag{31}$$

where:

1) P_{out} is the outage probability, defined as the probability that a packet cannot be successfully recovered without errors upon reaching the maximum number of transmission attempts N_{max},
2) $\bar{\bar{N}}_{tx}$ is the average number of transmission attempts to successfully deliver a data packet, averaged over the effects of the multipath fading and shadowing, and
3) R_b is the data transmission bit rate.

Note that the energy is spent only by the source device to transmit the packet because the other devices are sleeping. Since the energy spent at the gateway is not considered, this expression does not include the energy spent for the packet reception.

The expression for the energy efficiency of the cooperative scheme incorporates the energy cost associated to the active helper to receive the retransmitted packet from the source device. Therefore, the energy efficiency can be defined as

$$\lambda_{C} = \frac{(1-P_{out}^{c})L}{\bar{\bar{N}}_{tx}^{c} P_{tx} \frac{L}{R_b} + P_p P_{rx} \frac{L}{R_b}}, \tag{32}$$

where:

1) P^c_{out} is the outage probability of the cooperative scheme, defined as the event that a packet cannot be successfully recovered without errors upon reaching the maximum number of transmission attempts from source and helper, and
2) $\bar{\bar{N}}^c_{tx}$ is the average number of transmissions in the cooperation process including the original transmission, first retransmission from the source in case of error, and subsequent retransmissions from the helper.

Since cooperation is initiated only when the original packet transmission results in error, the energy cost of packet reception by the helper is proportional to the packet error probability P_p. Effectively, the cost is scaled down by the average number of cooperation slots relative to the total number of packets.

Recall that since the consideration of a constant transmission rate without data rate adaptation, it is expected that the benefits of cooperation come from overcoming bad channel conditions, i.e. substituting a blocked path by a two-hop LOS communication path, and thus reducing the number of required retransmissions. In the non-cooperative scheme when plain ARQ is applied, all the retransmissions during the unfavorable shadowing state will fail until the outage limit is reached and the packet is discarded. In the cooperative scheme, the retransmissions from helper have better chances of success due to the independent channel conditions and the data reliability of the system can be improved. Therefore $P_{out} > P^c_{out}$ is expected, and $\bar{\bar{N}}_{tx} > \bar{\bar{N}}^c_{tx}$. These are the cooperation benefits. However, the cooperation cost represented by the energy consumed by the helper when receiving the packet requires the careful evaluation and comparison of λ_{NC} and λ_C.

From the parameters in (1.31), the average number of transmissions per packet $\bar{\bar{N}}_{tx}$ and the outage probability P_{out} are the only parameters that depend on the wireless channel. In the next subsections, the values of $\bar{\bar{N}}_{tx}$ and P_{out} are computed, in order to obtain the value of the energy efficiency. For the cooperative case, the values of $\bar{\bar{N}}^c_{tx}$ and P^c_{out} have been evaluated by means of computer simulation since its theoretical evaluation becomes hardly tractable.

3.2.3.6 Average number of transmissions per packet in shadowing environments

Assuming that the value of $\bar{\gamma}$ remains constant for all the retransmissions of a given packet (i.e., shadowing state remains static), the average number of transmission attempts to successfully deliver a data packet for a given fixed shadowing state can be expressed as

$$\bar{N}^{inf}_{tx}(\bar{\gamma}) = \sum_{n=1}^{\infty} n \cdot P_p(\bar{\gamma})^{n-1} \cdot (1 - P_p(\bar{\gamma})) = \frac{1}{1 - P_p(\bar{\gamma})}. \quad (33)$$

This expression is valid for an infinite number of retransmissions until success, as denoted by the “inf” subscript. Therefore, when applied to the context of the considered scenario where an upper limit to the number of transmission attempts per packet is imposed, (33) represents an approximation. However, as it will be shown later, the results obtained by using the approximation agree well with the simulation results.

In order to compute the packet error probability in block fading environment taking the packet error probability for QPSK modulation expressed in (29) needs to be averaged over the fading distribution given in (26), and thus

$$P_p(\bar{\gamma}) = 1 - \int_0^{\infty} (1 - Q(\sqrt{2\gamma}))^L \, p_{\gamma}(\gamma \mid \bar{\gamma}) d\gamma. \quad (34)$$

The closed form solution of (34) can be deduced using the binomial formula and the integration of powers of the Q function given in [44]. However, the final result includes the series of Lauricella hypergeometric function, which becomes hardly tractable analytically. For this reason, it has been finally decided to solve (34) numerically.

3.2.3.7 Outage probability and number of retransmissions

Recall that the outage event is defined as the event when the maximum number of attempts N_{max} is reached and a given packet still has unrecoverable errors and therefore needs to be discarded. The average number of transmissions given in (33) can be also expressed as $\bar{N}_{tx} = 1 + \bar{N}_{err}$, where $\bar{N}_{err}$ is the average number of errors, followed by the last successful transmission. Therefore, it is possible to rewrite (33) as

$$\bar{N}_{tx} = 1 + \bar{N}_{err} = 1 + \frac{P_p(\bar{\gamma})}{1 - P_p(\bar{\gamma})}. \tag{35}$$

The average number of errors is a function of the value of $\bar{\gamma}$ and, in the outage event, it is greater than or equal to the maximum number of transmission attempts $\bar{N}_{err} = f(\bar{\gamma}) \geq N_{max}$. Therefore, in order to find the threshold of the SNR, denoted by $\bar{\gamma}_{th}$, for which an outage event occurs in average, it is necessary to find the inverse function of the average number of errors at $\bar{N}_{err} = N_{max}$, i.e., $\bar{\gamma}_{th} = f^{-1}(N_{max})$. Any value of $\bar{\gamma}$ that satisfies $\bar{\gamma} \leq \bar{\gamma}_{th}$ causes the outage event to happen in average. The value of the inverse function is obtained numerically given that (34) is found numerically. Then the outage probability can be computed as [45]

$$P_{out} = \int_0^{\bar{\gamma}_{th}} p_{\bar{\gamma}}(\bar{\gamma} \mid \mu) d\bar{\gamma} = Q\left(\frac{\mu - 10 log_{10}(\bar{\gamma}_{th}(N_{max}))}{\sigma} \right), \tag{36}$$

where $p_{\bar{\gamma}}(\bar{\gamma} \mid \mu)$ is the lognormal distribution as given in (27).

Taking into account the upper limit to the number of transmission attempts, the average number of transmissions per packet for a fixed shadowing state can be expressed as

$$\bar{N}_{tx}(\bar{\gamma}) = \begin{cases} \dfrac{1}{\int_0^{\infty} (1 - Q(\sqrt{2\gamma}))^L \, p_{\gamma}(\gamma \mid \bar{\gamma}) d\gamma}, \bar{\gamma} > \bar{\gamma}_{th} \\ N_{max}, 0 < \bar{\gamma} \leq \bar{\gamma}_{th}. \end{cases} \tag{37}$$

Finally, the average number of transmissions over all shadowing states, which is needed to calculate the energy efficiency of the non-cooperative scheme, is obtained by averaging (37) over the lognormal distribution, i.e.,

$$\bar{\bar{N}}_{tx}(\mu) = \int_0^{\infty} \bar{N}_{tx}(\bar{\gamma}) \, p_{\bar{\gamma}}(\bar{\gamma} \mid \mu) d\bar{\gamma}. \tag{38}$$

This integral can be solved numerically.

3.2.3.8 Results

The energy-efficiency analysis presented in the previous section for the values of the number of retransmissions $\bar{\bar{N}}_{tx}$ and P_{out} has been validated by means of computer simulations in MATLAB. Once their accuracy has been checked, the energy efficiency of both the non-cooperative and the cooperative ARQ schemes have been calculated and compared.

The values of the simulation parameters have been taken from the IEEE 802.15.4 Standard and Section 3.2.3.1. The transmission power was set to P_t=0 dBm and the distance from the

devices to the gateway was varied from 10 to 18 m in the steps of 2 m to get the different values of P_r at the receiver. The pathloss at reference distance is $PL(d_0)$=55 dB and the pathloss exponent is set to α=4 as proposed in [42]. As per (25), at room temperature of T=300 K, adopting the noise figure F=7.3 dB as measured in [46], and with a signal bandwidth of B=2 MHz, it is obtained a noise floor of P_n=-103 dBm. The DSSS gain is calculated by knowing that B_N = B and taking the data bit rate of R_b=250 kbps, leading to the relation E_b/N_0=8μ. The maximum number of transmissions was set to N_{max}=4 and a strong shadowing standard deviation of σ=8 dB. The power levels for different operating modes P_{tx} and P_{rx} have been taken from the CC2430 transceiver data sheet [47], and they are P_{tx}=80.7 mW and P_{rx}=80.1 mW, respectively. The packet length has been set to L=127 Bytes.

For the non-cooperative case, a new realization of a log-normally distributed shadowed mean is generated for each new packet, while it remains constant for all the packet retransmissions. The signal amplitude of the packet was multiplied by the Rayleigh distributed variable and the AWGN was added. Finally, the errors at reception were counted as well as the number of discarded packets when the number of errors reaches N_{max} in order to estimate the value of the outage probability.

Let us recall how the cooperative algorithm operates. Since it is possible to calculate the value of the threshold $\overline{\gamma}_{th}$, the gateway requests cooperation after the first failed transmission if the channel to the source is estimated to be in outage. In the next transmission attempt, the packet is retransmitted by the source to be obtained by the helper, while the gateway again tries to decode the packet. The repeated failure at the gateway reinforces the assumption of the severely shadowed source-destination channel meaning that the failure is not due to the temporary multipath fading effect. The following retransmissions proceed from the helper. The helper is located at the same distance from the gateway than the source, resulting in the same value of μ (average pathloss), but with different shadowing state realization $\overline{\gamma}$.
In the case that helper selection is applied, the favorable helper candidate is indicated whose shadowing state satisfies $\overline{\gamma} > \mu$ and therefore has greater chances of success. To ensure fairness when comparing the cooperative and non-cooperative scheme, the total number of attempts from the source and the helper together is limited to a maximum of N_{max} transmissions, which is the same as in the non-cooperative case. Finally, $\overline{\overline{N}}_{tx}^{c}$ is estimated, as well as the outage probability, considering the number of discarded packets.

The resulting outage probability is shown in Figure 3.20. It is possible to see that the reliability in the communications is significantly improved when using the cooperative scheme, especially with the helper selection. For the lower values of E_b/N_0 the outage probability of the non-cooperative scheme is not acceptable, while the cooperative scheme provides quite reliable data transmissions. Based on our evaluation, even if cooperation has an additional energy cost consumed at the helper when receiving the packet, the benefits outweigh the cost and the energy efficiency results to be better for all the tested values of E_b/N_0 as shown in Figure 3.21.

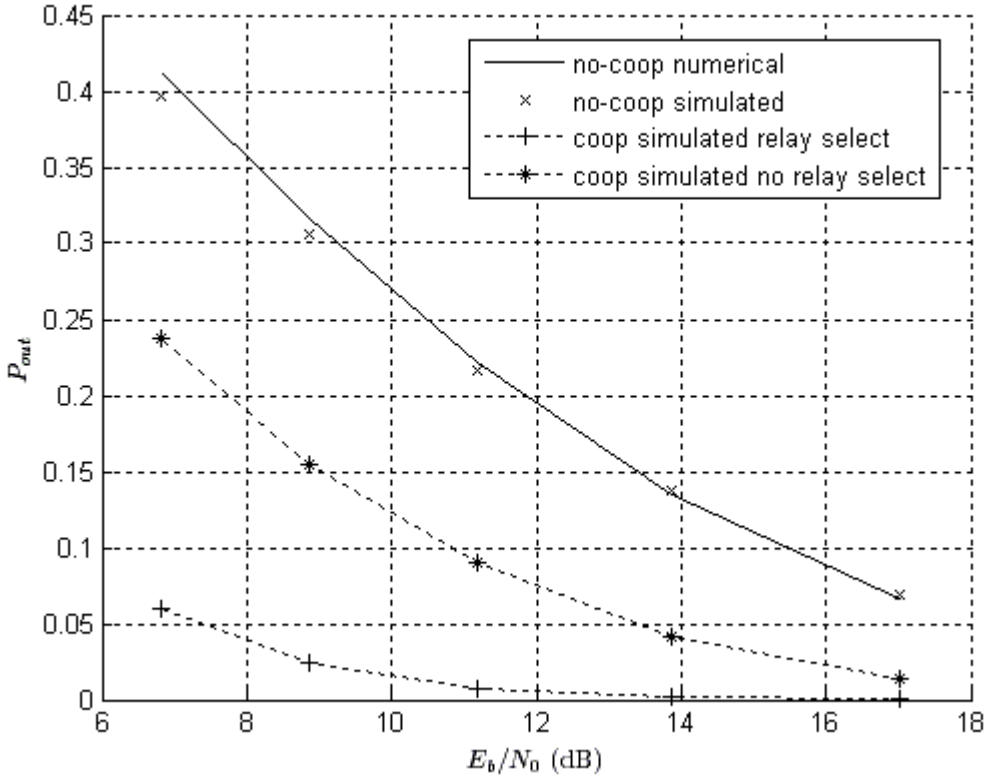

Figure 3.20: Outage probability of cooperative and non-cooperative scheme.

This is due to the fact that the cooperation is initiated only in unfavorable channel conditions. However, one may note that as the E_b/N_0 improves, the energy efficiency of the cooperative scheme approaches that of the non-cooperative. This means that cooperation should be used only when needed, i.e., when the probability of channel source-destination being in outage is high. Finally, recall that the total energy of the whole cooperative protocol was not estimated here, but the focus was on the reliable data transmission and the justification of cooperation in capillary M2M networks.

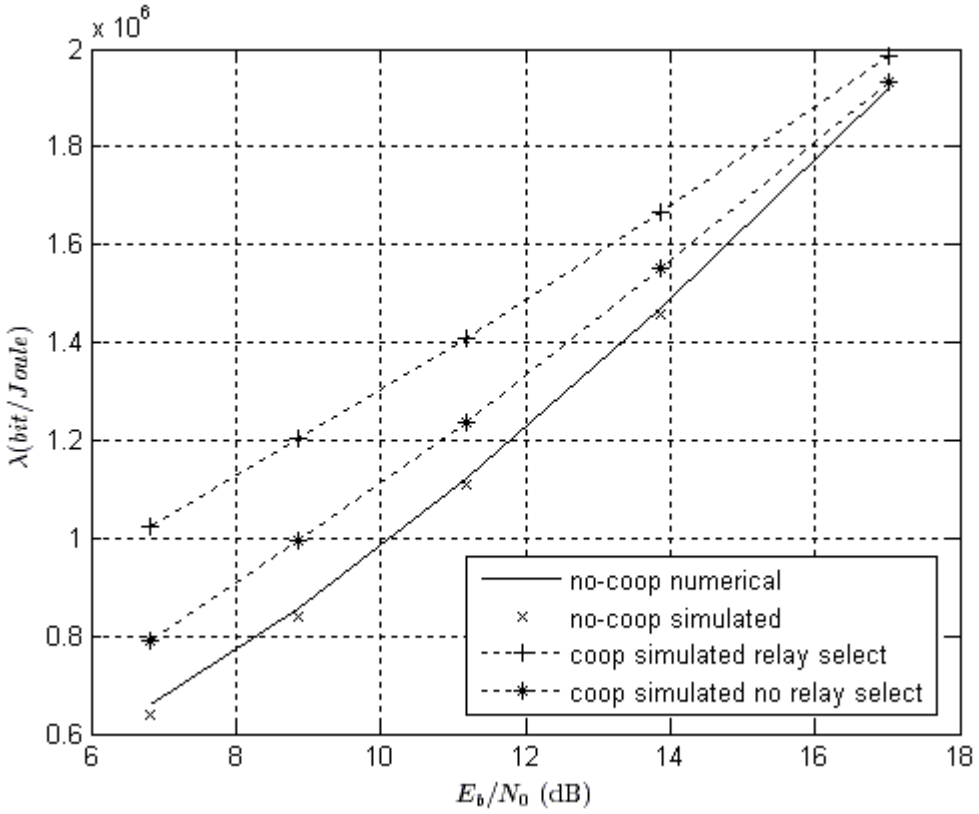

Figure 3.21: Energy efficiency of cooperative and non-cooperative scheme.

This improved energy efficiency translates directly to an extended lifetime of the devices. Just to put some numbers to this conclusion, let us imagine an application where a device has to transmit a total amount of 1000 bytes of information. In the case that the channel between the device and the gateway is such that the value of the E_b/N_0=9dB, then the energy efficiency is of:

1) 1.2Mbits/Joule for the C-ARQ with helper selection.
2) 1Mbit/Joule for the C-ARQ with random helper selection.
3) 0.82Mbits/Joule for the non-cooperative scheme.

If linear battery consumption model is considered, then the C-ARQ with helper selection will attain a normalized lifetime of 1. The C-ARQ with random helper selection will attain a lifetime of 83%, and the non-cooperative approach, a lifetime of 68,3% compared to the C-ARQ with optimal helper selection.

3.2.3.9 Conclusion

Within EXALTED, it has been shown that C-ARQ schemes not only improve the throughput of short-range networks, which had been shown in the past in the literature, but they can also improve the energy efficiency of a capillary M2M short-range network with data rate adaption capabilities (e.g. based on IEEE 802.11). Once proven the energy-efficiency of C-ARQ, it has been shown in the second part of this section that C-ARQ can be applied to low-power low-cost M2M capillary networks based on the IEEE 802.15.4 Standard. By implementing a slight modification to the rules of the MAC layer, it is possible to apply the C-ARQ idea to low-power networks with duty-cycling. In this case, data rate adaptation cannot be exploited, but instead, cooperation can be used to overcome bad channel conditions that remain static for long periods of time due to the time correlation of the channel. The results obtained by

means of theoretical analysis and computer based simulation show that C-ARQ strategies can be applied to capillary M2M networks to overcome severe shadowing in the direct link and thus extend the lifetime of devices in up to 46% with regard to the non-cooperative retransmission approach in the considered scenarios.

In more detail, an energy model based on Markov chain theory and applicable to the PRCSMA protocol has been presented in the first part. This model has been used to assess the energy efficiency of the protocol and it has been compared to the efficiency of a traditional non-cooperative ARQ scheme. The validity of the model has been confirmed by computer-based simulations. The results show that the PRCSMA protocol outperforms non-cooperative ARQ for medium to high packet error rates in the source-to-destination channel. The results also demonstrate that, in the cooperation phase, collisions should be avoided even at the cost of more idle slots to achieve better energy efficiency. This study can be further expanded by introducing sleep states (duty-cycling) and by defining novel techniques that enable the network to have some control over the number of active helpers, and thus run the network in optimal conditions.

In the second part, it is found that a significant improvement in terms of energy efficiency and reliability can be attained in capillary M2M networks by executing a C-ARQ scheme at the MAC layer. The active helpers can be woken up only when needed and thus the energy for overhearing is consumed only when the current channel realization between a source and the destination is unfavorable and likely to be in outage. Moreover, if a smart helper selection procedure is applied to the C-ARQ scheme, the benefits can become even higher. The results show that cooperation is especially suitable for networks with hard reliability constraints since it can significantly reduce the outage probability. C-ARQ enables communication between two remote devices in conditions when traditional non-cooperative schemes cannot operate. Therefore, C-ARQ can extend the communication range with the cost of having a two-hop communication model instead of a single peer-to-peer communication model.

The results obtained in this task of EXALTED have been summarized in two research papers; the results of the first part are described in [49] and the results of the second part can be found in [50].

3.3 MAC Protocol for capillary M2M multi-hop networks

One significant challenge in capillary M2M networks is the bottle-neck effect that appears near to data collector, i.e. the CH or the M2M Gateway. Such an effect appears in situations where network nodes collect data and report them to the collector, which is assumed to be in charge of any collection and processing procedure. This could be the case of an environmental monitoring application, where a large amount of devices have been deployed in order to cover huge geographical areas, and they report their data to the CH or the M2M Gateway in a multihop way of communication. While such an approach simplifies the task of the sensors, it also concentrates most of the traffic near the CH, increasing the chance of congestion, as well as the origination of bottle-neck effects. This leads to increased transit traffic intensity, congestion and high packet loss probabilities, which results in wasted energy and bandwidth. As a result, the sensors that are located nearest to the CH (in the so called *intensity region*), lose a larger number of packets and consume significantly more energy than sensors further away from it, shortening the operational lifetime of the overall network. Hence, mitigating the negative consequences of this bottle-neck effect represents an important challenge and is considered to be the main target of our research.

In this context various hybrid schemes have been proposed, including Zebra-MAC (Z-MAC) [51], Funneling MAC (F-MAC) [52], CSMA/ TDMA [53], [54]). More specifically, focusing on

the hybrid approaches in [52] a hybrid CSMA/TDMA scheme was designed for the intensity region that is controlled by the sink using on demand beaconing. In [53], considering a multihop communication scenario, a traffic scheduling strategy is proposed for improving the network capacity, fairness and packet loss. Finally, in [54], based on the 802.15.4 standard [55], an adaptive hybrid CSMA/TDMA protocol was presented, which dynamically assigns a part of contention access period to TDMA and shares this period among nodes with more packets in buffer. A common observation in all these approaches is that contention based access is used for relatively low traffic conditions, while contention free slot assignments become dominant as traffic density increases. Following a similar approach it has been adopted a *localized, CH-oriented MAC approach* that takes into consideration this bottle-neck effect in its design [53]. This MAC protocol represents a hybrid MAC scheme that supports both TDMA and CSMA with collision avoidance (CSMA/CA) and operates in the intensity region that arises near to the CH. It is worthwhile mentioning that such a hybrid approach, where contention-based access to the medium “co-exists” with contention-free access, is also included in IEEE 802.15.4 [55].

In IEEE 802.15.4 the main reason for including this feature is for supporting time-critical applications. Specifically, employing a guaranteed time slot allocation mechanism it is ensured that time critical data will be delivered to the network coordinator. In our case, the objective of investigating such a hybrid approach, for the MAC protocol, is to deal with the bottle-neck effect, by using local TDMA scheduling in the intensity region. Hence, depending upon the network traffic, sensor nodes may access the channel using contention based or contention free mechanisms. In light traffic scenarios, all sensor nodes perform CSMA/CA, capitalizing on the fact that contention-based protocols are very easy to implement and can efficiently handle sporadic traffic while they are more scalable. However, contention-based protocols suffer from collisions, as the offered traffic load increases, and this causes delivery latency, high rate of retransmissions and hence energy consumption. Thus, scheduling opportunities are provided to the nodes that are located closer to the CH, which typically should handle considerably more traffic than nodes further away from it. The TDMA slots assignment to the nodes is coordinated by the CH using the beacon frame that is periodically broadcasted.

3.3.1 Proposed hybrid CSMA/TDMA coordination algorithm

The mode of operation of our proposed scheme is based on the fact that all nodes use CSMA/CA by default, unless they exceed a predefined threshold. In that case, the CH is being informed by the nodes, using one reserved bit in the data packet, in order to schedule them for future transmissions. The scheduling procedure can be performed using a beacon that is broadcasted by the sink, while this beacon includes information regarding synchronization issues, superframe duration, beacon interval and TDMA scheduling policy [52]. It is worthwhile to note that the nodes that do not receive this beacon continue to employ CSMA/CA as an accessing scheme. Following a similar approach as in [54], the framing structure of the proposed MAC mechanism is based on [1], and is depicted in Figure 3.22. More specifically, several superframes, consisting of CSMA and TDMA frames, are repeated between two beacon periods. Hence, in case of light traffic only access period with contention can be found in a superframe (i.e., CSMA frames), while as traffic gradually increases the contention free period and TDMA frames assignment become dominant. The algorithm of the proposed scheme, which is based on IEEE 802.15.4 with beacon-enabled slotted CSMA/CA, is depicted in Figure 3.23 and can be also found in [55]. In this figure the slotted IEEE 802.15.4 CSMA/CA mechanism is illustrated together with an extension that includes our proposed switching criterion for selecting contention-based or contention-free

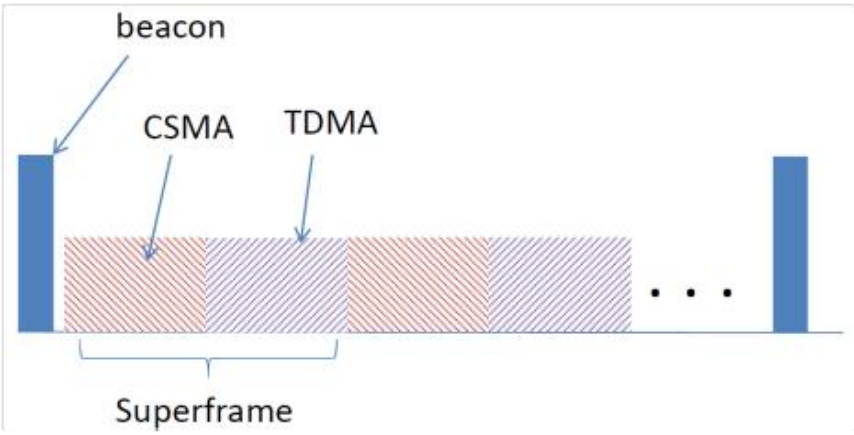

Figure 3.22: Frame structure.

access to the medium. This mode of operation is based on the fact that all devices should keep in their memory a few variables, including the number of backoffs (NB), the contention window length (CW), the backoff exponent (BE), and a threshold. Specifically, NB is the number of backoffs required to be taken while attempting to access to the medium, it is initialized to 0, it gradually increases when the medium is found to be non-idle and in case that it exceeds a maximum value (MaxCSMABackoff) the packet is dropped. CW indicates the number of slot periods that need to be clear of activity before a transmission can start and it is initialized to 2 before its transmission. BE indicates the number of backoff periods that a device should wait before attempting to assess the channel, which in our case is also initialized to 2. Finally, the threshold is related with the cumulative number of times that the medium has been sensed non-idle by a node. The main objective of the proposed algorithm is to determine a threshold criterion for switching between the CSMA and the TDMA modes that optimizes the throughput and minimizes the probability of dropped packets.

. The switching criterion selected that has been found to optimize the throughput is the *ChannelNonIdle*, which is defined as

$$ChannelNonIdle = \frac{numNonIdleChannel}{totNumOfSlots}. \quad (39)$$

In this definition, *numNonIdleChannel* denotes the number of times that a node sensed the medium to be non-idle and *totNumOfSlots denotes* the total number of contention access slots in predetermined period. In this sense in case of light traffic the nodes use pure CSMA/CA mode for accessing the channel. As the traffic increases the probability that a node founds the medium to be non-idle increases and as soon as this probability exceeds the predefined threshold value, the nodes are requesting a non-contenting access to the medium using TDMA. Extensive simulation results have proved that the optimum strategy for maximizing the throughput is to assign TDMA slots mainly to the nodes that are located quite close to the data collector, i.e. one or two hops away.

3.3.2 Simulation setup and results

The algorithm is implemented using matlab, considering a 6x6 grid topology with 36 nodes and the CH located at the bottom right corner of the grid (as shown in Figure 3.24).

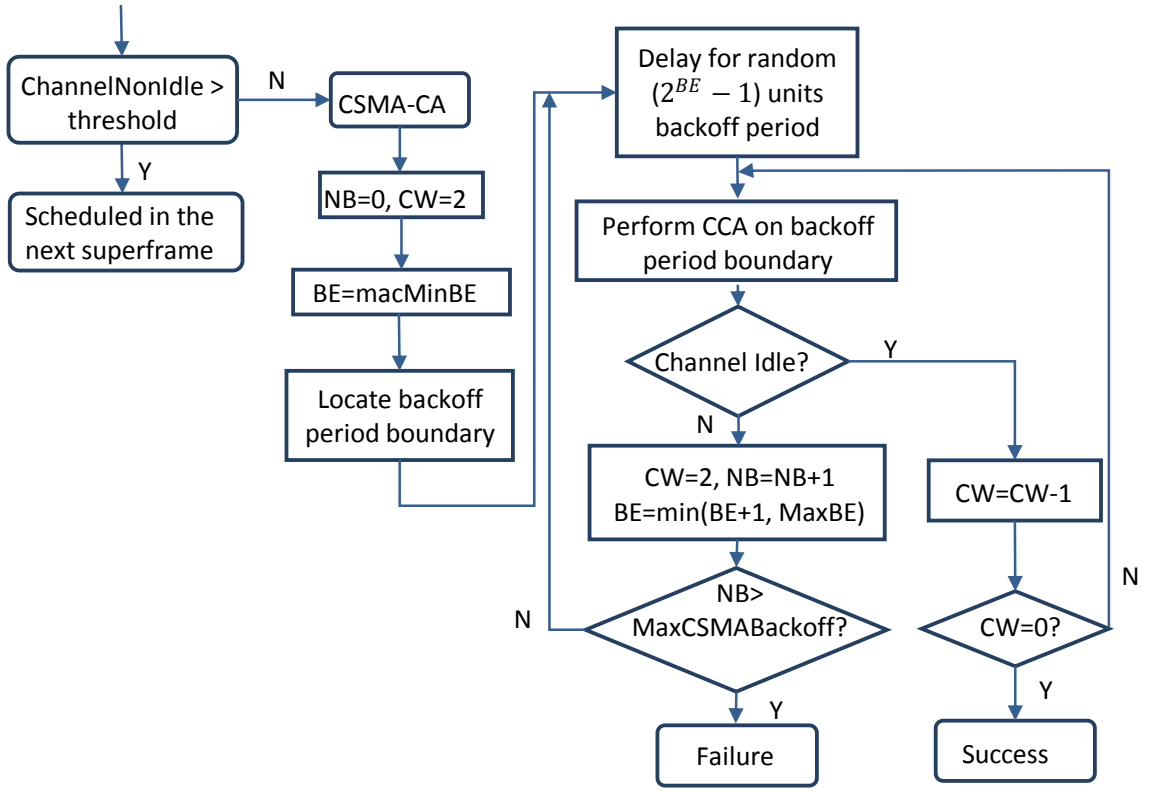

Figure 3.23: Slotted CSMA/CA mechanism extended by a threshold based contention free algorithm.

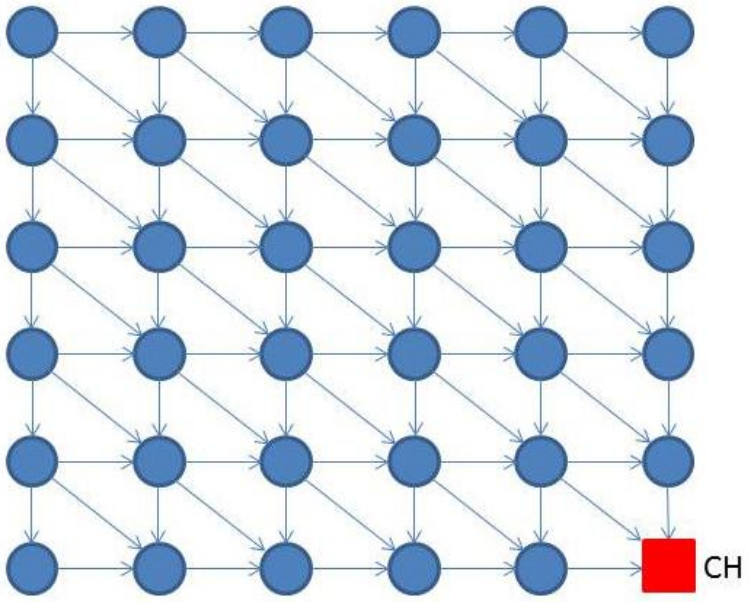

Figure 3.24: Grid topology.

A number of nodes have been randomly selected, throughout the network, for generating data packets, of constant size equal to 1 slot, according to the Poisson distribution. This traffic is routed to the data collector through error free multi-hop paths based on the shortest path routing protocol. Obeying the objective of low complexity devices, it has been considered low storage capabilities for these devices, i.e., with size less than 10 data

packets. Furthermore, the KPIs that have been considered in this study include the throughput, which in our case is defined as the number of successfully received messages per time unit in the CH and the reliability, which is defined as the average number of retransmissions. In all cases, the MaxCSMABackoff has been set equal to 5, the macMinBE equal to 2, CW is set 2, while the TDMA opportunities have been provided only to nodes that are located one hop away from the CH. Here, it is very important to be mentioned that both performance criteria can be optimized by selecting relatively low values for the switching criterion, especially for cases of high traffic, in order to increase the devices (located around the CH) probability of having contention free access.

In Figure 3.25, considering pure CSMA/CA and hybrid CSMA/TDMA schemes, the throughput (in terms of packets/sec) is plotted as a function of the average number of generated packets, in packet per second (pps). In this figure, it is clearly depicted the improvement achieved when the hybrid CSMA/TDMA technique is considered for all the range of traffic conditions. It is important to note that as the average number of generated packets increases the improvement in terms of throughput also increases in case of the hybrid approach. Similar observations can be also extracted in Figure 3.26, where the normalized number of retransmissions is also plotted as a function of the average number of the offered load. In this figure it is also verified that employing the proposed hybrid accessing scheme improves the reliability of the system. Hence, this reduction on the amount of retransmissions has as a consequence a decrease to the nodes energy consumption and thus an improvement to the overall network lifetime.

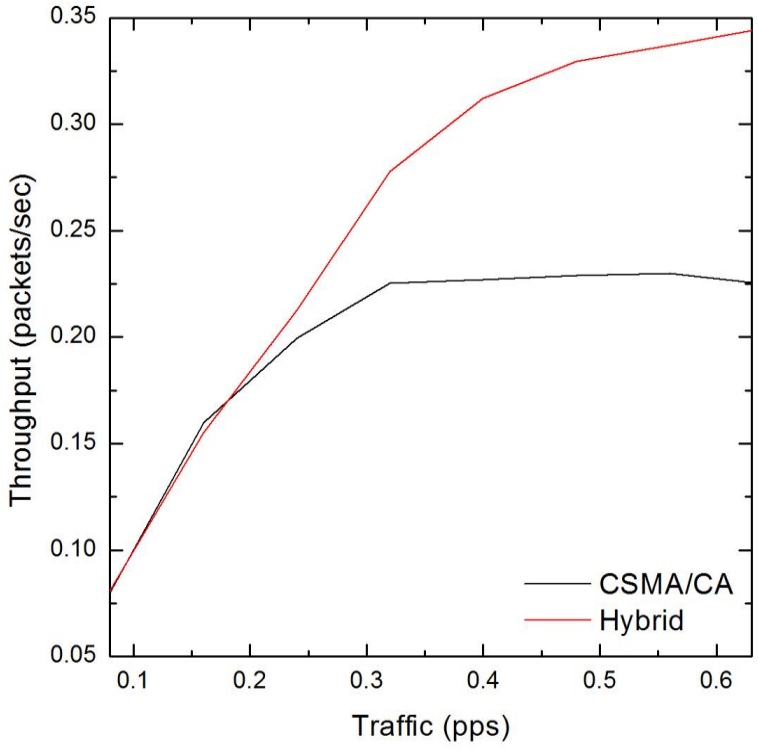

Figure 3.25:Throughput as a function of the offered load.

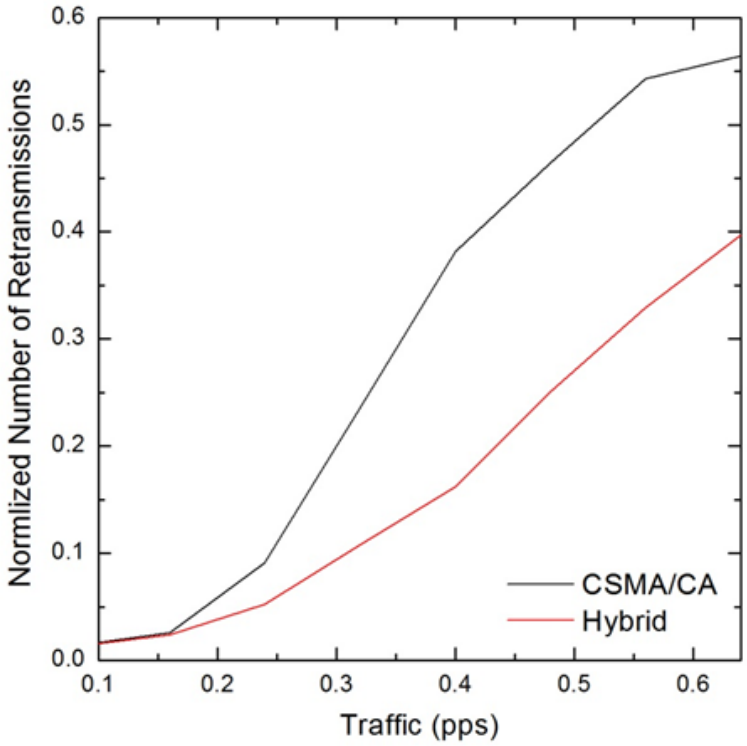

Figure 3.26: Reliability as a function of the offered load.

4. Device Reachability and Addressability for Data Connectivity

As mentioned in the introductory chapter of the document, designing MAC protocols is one of the main tasks regarding the goal of assuring continuous packet data protocols between LTE-M network and capillary networks, but there are some other important aspects to study, such as:

- Heterogeneous connectivity, i.e. the E2E connection across different types of networks. The E2E connection must be established regardless of the access technology used on each network element present in the architecture. For example, one network would be non-IP energy constrained M2M capillary network, and the other network is already deployed IP core network.
- Mobility management so as to handle changes on the capillary network layout, regarding not only single node movement, but also considering group and even whole network mobility.
- Study of higher level (above MAC layer) protocols needed to manage E2E connectivity, aiming to build resource oriented and optimum payload protocols. They aim to define the needed protocols above MAC layer in order to provide a common protocol stack able to deal with the packet continuity while communicating across capillary and LTE-M networks.

All these cited subjects, with a view of the current status and the achievements obtained in the EXALTED are explained in the following subsections.

4.1 Heterogeneous connectivity

The fact that EXALTED is considering a huge number of heterogeneous M2M devices that need to communicate with the LTE-M network, makes it necessary to define proper mechanisms to ensure its interoperability for different types of networks and packet continuity at the higher layers.

On the protocol stack, the focus of this activity can be highlighted as shown in Figure 4.1.

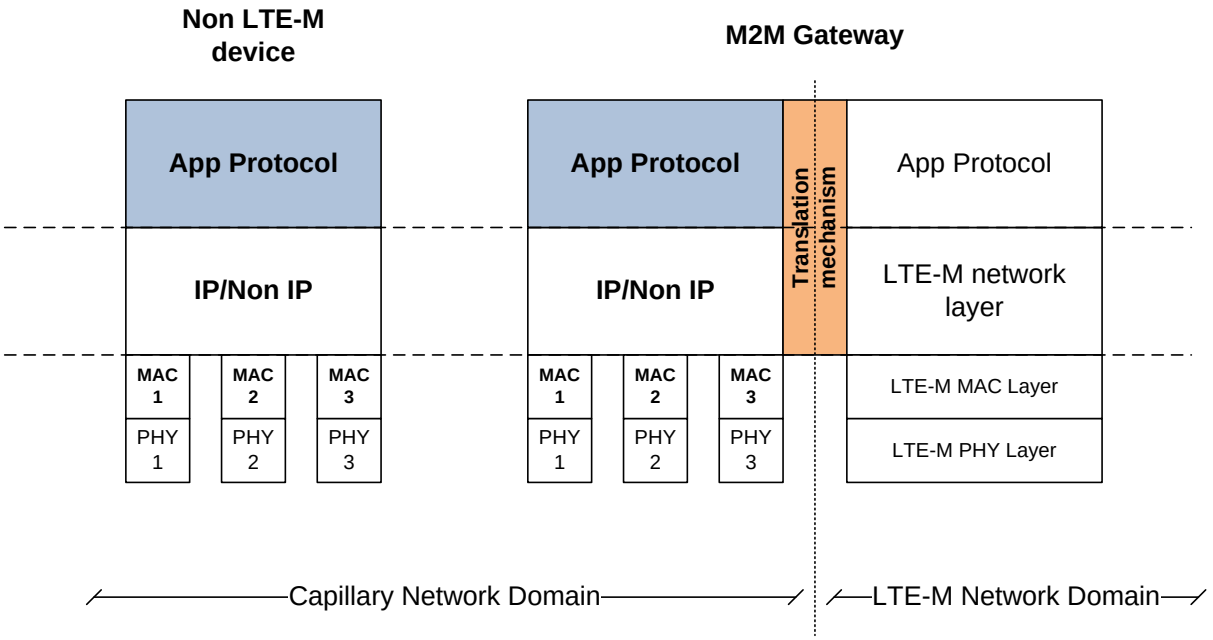

Figure 4.1. Heterogeneous connectivity focus areas: study of application protocols and definition of address translation mechanisms.

The evolution of the Internet of Things (IoT) concept leads to new challenges in terms of heterogeneity in M2M communications. The characteristics of many devices that take part in these scenarios require the optimization of their functionalities and capabilities. The following subsections describe the analysis of different solutions for interconnection between the devices in the capillary networks and the M2M (application) server in the IP core network.

The following subsections describe the theoretical studies carried out for the specification of an optimum algorithm selection regarding address translation between non-IP capillary network elements and IP M2M servers. A use case regarding practical implementation, resource mapping and programming functionalities, and overall system characterization (for such as resultant overhead and memory consumption) can be found in D4.2 [56] deliverable from the EXALTED.

4.1.1 Design considerations

In the design phase of mechanisms for ensuring packet continuity it is mandatory to consider the way that communication is performed. Since in EXALTED it is assumed that capillary networks can be based on non-IP addressing schemes and the application server is located in the IP core network, it is necessary to detect the critical elements from the ones described in 2.3.1 where some the new proposed techniques will be applied.

The elements that participate in this scenario are:

- LTE-M device – Sensors or actuators sending and receiving information from the application server and device management server. This kind of device is able to directly connect through LTE-M network.
- Non LTE-M device - Sensors or actuators sending and receiving information from the application server and device management server. It requires the collaboration of a M2M gateway and could also need other non LTE-M devices for reaching the Gateway in order to access to core network and application server.
- M2M gateway – This element is in charge of managing incoming and outgoing communications from/to capillary network.
- LTE-M network – Long Range wireless network linking devices and gateways to the core network.
- M2M server – Fusion point of the information generated by devices and source of the commands sent to actuators.

Considering these elements of the EXALTED architecture, and due to the scope of this task, there are two scenarios that must be analyzed. The first one is composed of LTE-M devices connected to a M2M Server. In this case, packet continuity is ensured by the characteristics of LTE-M addressing properties (as it implements IP and the addressing is maintained, then, E2E), thus no extra mechanisms must be created for this purpose. The second is more complex, it is composed of non LTE-M devices forming a capillary network and connecting to an M2M server. In this case, the combination of non-IP networks, like some capillary network, and IP core network demands procedures in key points of the architecture so as to ensure packet continuity. As this document aims to propose an address translation mechanism, the second case is deeply studied.

There is a basic assumption made based on the fact that the first communication (bootstrap) is initiated always by the non LTE-M device. The following figures present the data flow in case of TCP and UDP connections are established between non LTE-M end devices and the M2M server.

The first activity of a non LTE-M device when it is switched-on is performing bootstrap and then joining to the capillary network. This step is simplified and depicted in Figure 4.2. After the bootstrapping, and depending on device's own configuration (please refer to strategies described below), the device will start sending data to the M2M server. In this process all elements listed at the beginning of this subsection are involved. As it is an E2E connection, this can be taken as an advantage for "pre-knowing" some key information further employed for maintaining packet continuity. Furthermore, it is possible to keep the communication channel between both ends opened enabling information exchange while environmental conditions keep unaltered.

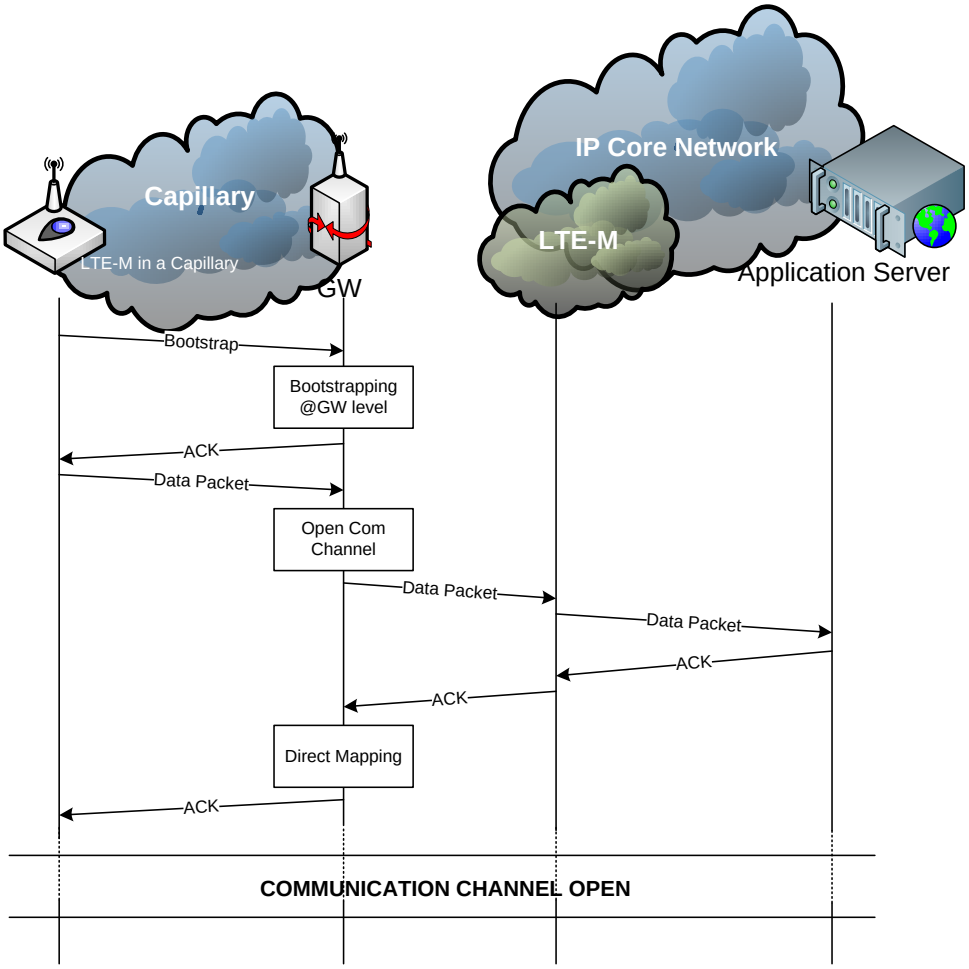

Figure 4.2: TCP connection from non LTE-M device.

Once the communication network level channel (i.e. session) is established and active, the application server is able to send information to devices within the capillary network. Figure 4.3 shows the flow from the server to non LTE-M device. Regardless of how the packet has been triggered the server will connect first the gateway, and once there, it will be able to automatically redirect information to the end device.

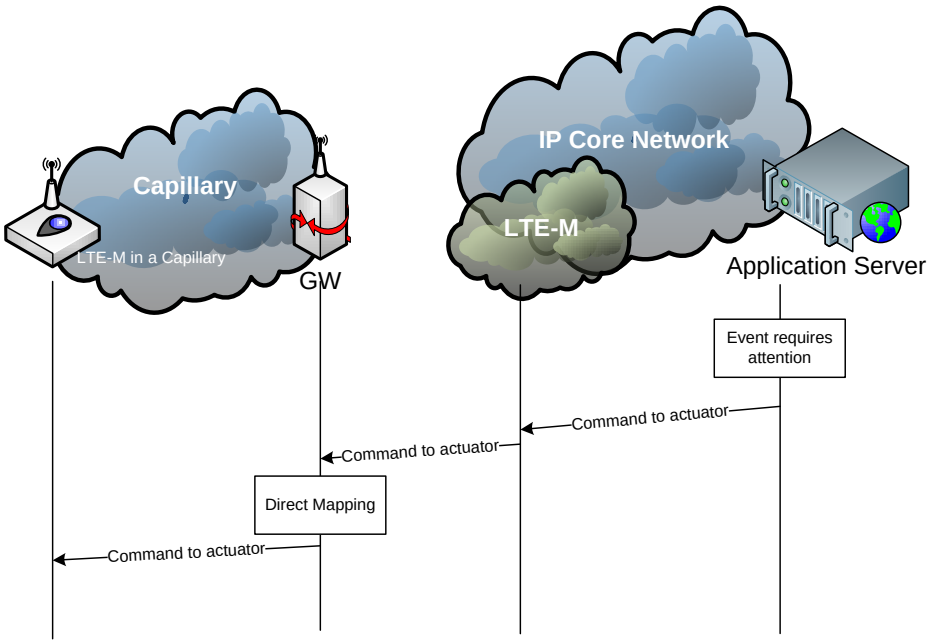

Figure 4.3: Connectivity from Application Server.

The two previous situations are feasible to handle with TCP connections, but unfortunately, UDP protocol is not connection-oriented. This implies that no channel (i.e. session) is kept open after sending a datagram and there is no confirmation about delivery.

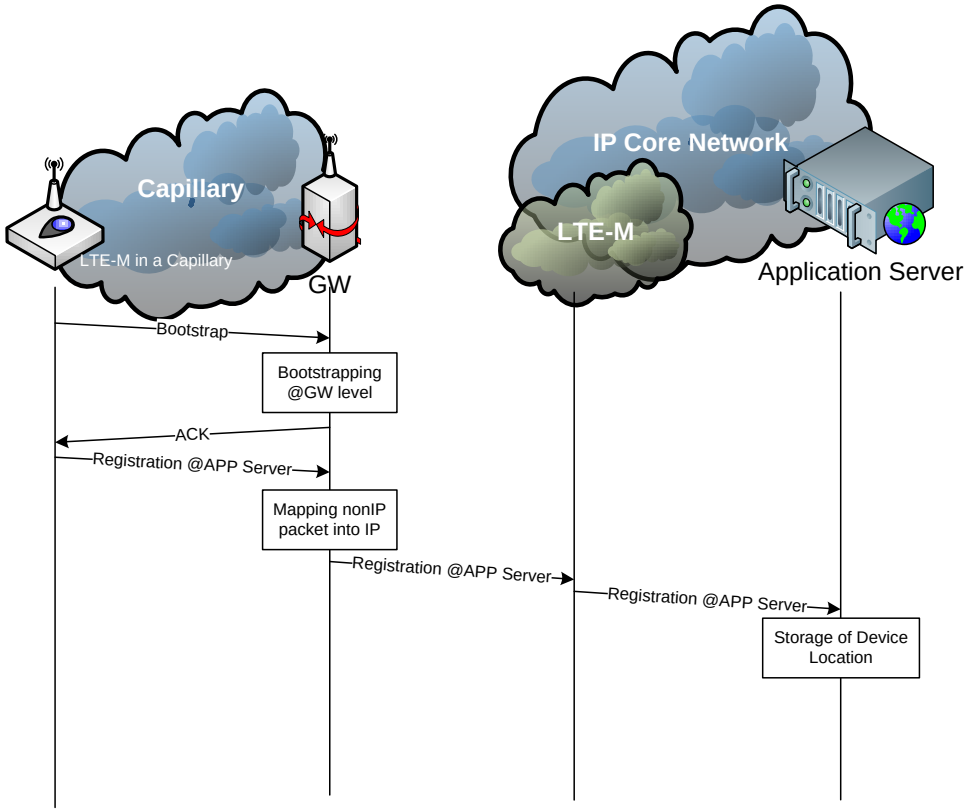

Figure 4.4: UDP Case data transmission.

Considering the particularities of UDP/TCP transmission schemes, three different solutions are analysed for ensuring packet continuity in M2M scenarios.

1st Strategy

The first approach consists on doing device bootstrap sharing with the gateway the address of the M2M server they must send their information to. This solution requires extra memory at the gateway for storing which is the M2M server linked to each device. The strength of this solution is that the payload of packets is directly encapsulated and sent to the destination server without including extra overhead.

The throughput obtained (considering it as the effective data transferred in comparison to the length of the resultant packet) with this policy can be calculated as

$$Throughput_{S1} = \frac{Payload}{\left\lceil \frac{Payload}{MTU - Overhead} \right\rceil \times Overhead + Payload} \quad (40)$$

Where Payload is the effective data in bits, MTU the maximum transfer unit allowed by the protocol and Overhead the introduced headers due to the protocol used at Network and Transport levels.

And the memory need can be derived from:

$$Memory_{S1} = NumberDevice \times \left(@IP_{Length} + @CapNetwork_{Length} + Port_{Size}\right) \quad (41)$$

Where NumverDevice quantifies the amount of devices in the capillary network, $@IP_{Length}$ is the length in bytes of the IP address of the M2M server, $@CapNetwork_{Length}$ is the size in bytes of the IEEE address of nodes and $Port_{Size}$ is the number of bytes needed to identify the port.

2nd Strategy

The second strategy aims at reducing the extra memory dedicated for mapping devices in the capillary network at the gateway level. This includes that payload starts with IP address of the destination server, this way it is not needed to keep them stored in the gateway reducing in a 50% the requirements imposed in the previous case but increasing overhead, thus reducing throughput.

The throughput obtained with this policy can be calculated as shown:

$$Throughput_{S2} = \frac{Payload}{\left\lceil \frac{Payload}{MTU - Overhead} \right\rceil \times Overhead + Payload + @IP_{Length}} \quad (42)$$

And the memory need can be derived from:

$$Memory_{S2} = NumberDevice \times \left(@CapNetwork_{Length} + Port_{Size}\right) \quad (43)$$

3rd Strategy

Finally, the third approach is getting all information about LTE-M interface of the gateway at non LTE-M device level (by programming end nodes with a default address to authenticate)

and including in the payload a TCP/IP packet, so gateways just have to map it with any requirement in terms of memory.

The throughput obtained with this policy can be calculated as shown:

$$Throughput_{S3} = \frac{Payload}{\left\lceil \frac{Payload}{MTU - Overhead} \right\rceil \times Overhead + Payload + IP_{HEAD} + TCP_{HEAD}} \quad (44)$$

4.1.1.1 Results

In order to provide specific figures for the efficiency and resource requirements of each of the previously mentioned strategies, ZigBee protocol is considered in the capillary networks.

As explained before, there is no need for extra memory. In terms of memory it can be represented as shown in Figure 4.5.

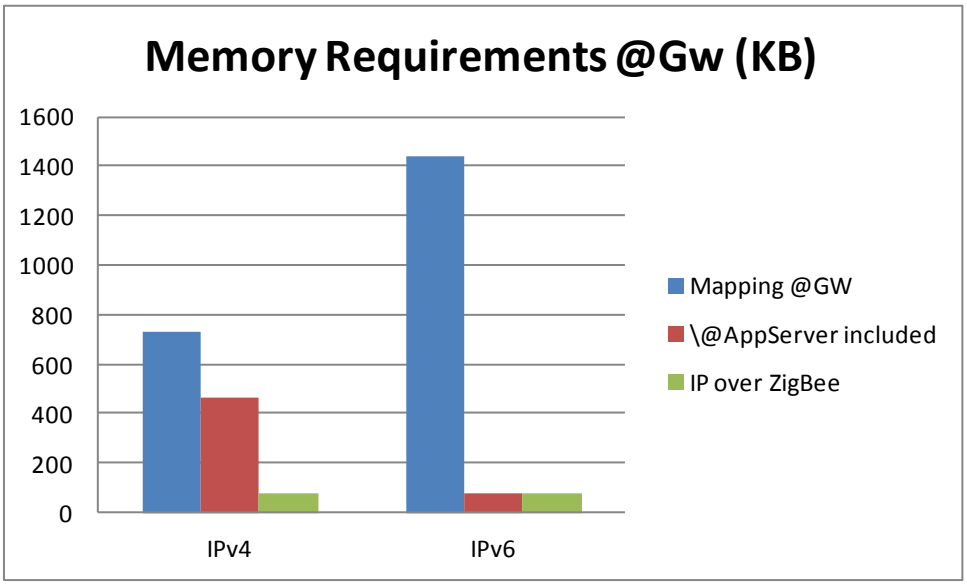

Figure 4.5: Memory requirements at gateway

The result in terms of memory is quite intuitive, the better the throughput, the more inefficient it is in terms of memory needed. It is directly related due to the amount of extra data that is included in the payload of the packet, in case that the extra data were not included it is needed that an initial process informing about destination of packets from each node.

Based on EXALTED target scenarios and the key elements of the strategies already presented, it has been analyzed the performance in terms of efficiency, total bytes sent for a certain payload and radio transceiver transmitting. These results are obtained applying the equations from different strategies for a baseline scenario using ZigBee as capillary protocol and TCP+IP as LTE-M network and transport protocols.

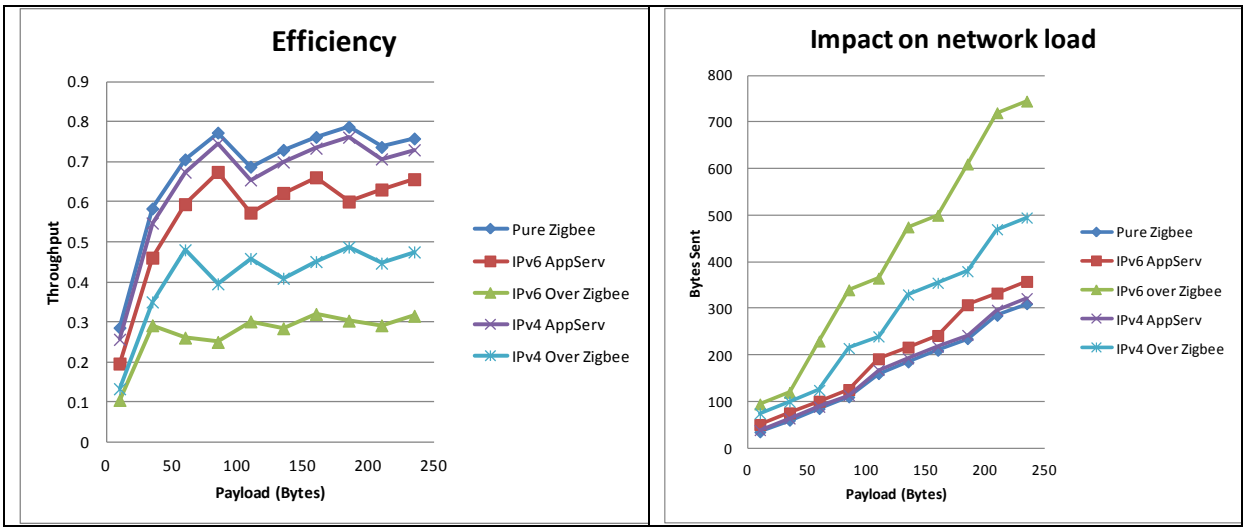

Figure 4.6: Efficiency based on strategy.

Figure 4.6 shows the difference in terms of throughput depending on the strategy chosen. This figure remarks the differences among the strategies enforcing the trade-off between throughput and memory. Depending on the application and gateway location (including the constraints faced) the selection between strategies. For very constrained devices, it is slightly better to reduce throughput but it will be better in terms of devices simplicity. But this is not the case for more powerful devices.

The other critical parameter to be considered is the battery life. In this case strategy also has a strong impact on device life. The translation will be mapped for each manufacturer consulting the amount of energy they need to transmit a certain amount of data. There are some differences (Figure 4.7) for the same payload, so the location of device will determine the decision to be made. This Figure shows the amount of milliseconds that the radio module is working depending on the strategy and the Payload (X-axis) selected.

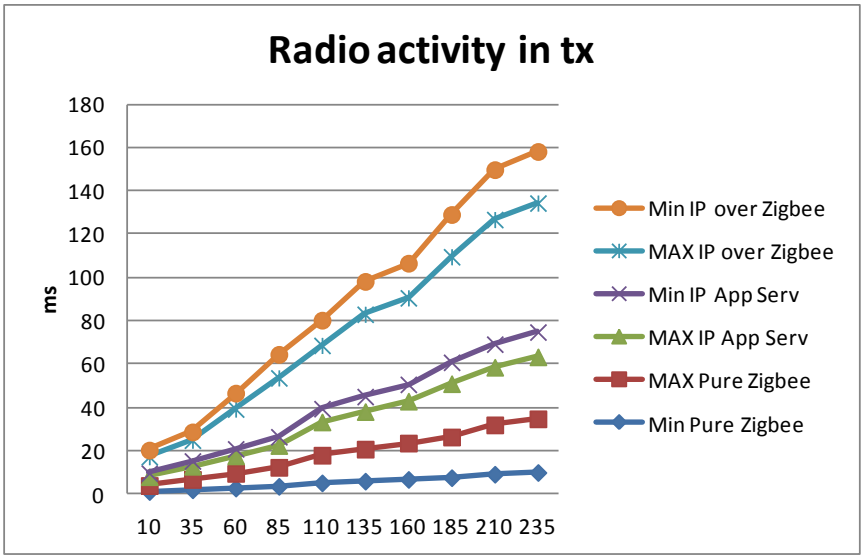

Figure 4.7: Radio Transceiver activity.

4.1.2 Achievements: PoC demos

As an added value provided to heterogeneous connectivity work topic, a couple of hardware demos were set up. The main goal of both of them is to try to implement some of the assumptions made on previous subsections so as to demonstrate the viability of the results provided, not only form a theoretical point of view, but also using real M2M hardwares.

In the following sections, both testbeds are described focusing on the architecture and the features to be proven.

4.1.2.1 E2E connectivity and communication

This is the first demo introduced for proving heterogeneous support. It involves three end devices, two of them on the same capillary network (managed by a Gateway and using ZigBee) and the third one as a standalone device directly connected to the Internet via cellular interface (GPRS).

The two nodes forming a capillary network are conceived to communicate between them. This way, a NFC reader is available on one of them, and a LED array is installed on the other one.

All of them can be remotely monitored by using third-party middleware on the Internet, enabled by installing a small client on each device posting appropriate data towards the M2M server. The connectivity is ensured by the gateway able to gather the information and post it via the GPRS interface.

This way, the following features are proven:

- E2E connectivity between end devices in the same capillary network. Depending on which NFC tag is approached to the device with the NFC reader, the LED array on the other one is illuminated in a certain color. The intelligence is embedded on the gateway, in charge of parsing the data received from the NFC reader and sending the appropriate command to the LED array.
- E2E connectivity between end devices and the M2M server, by means of posting data related to internal sensors into a commercially available application server on the Internet.

Finally, a picture summarizing all previously mentioned features can be shown in Figure 4.8.

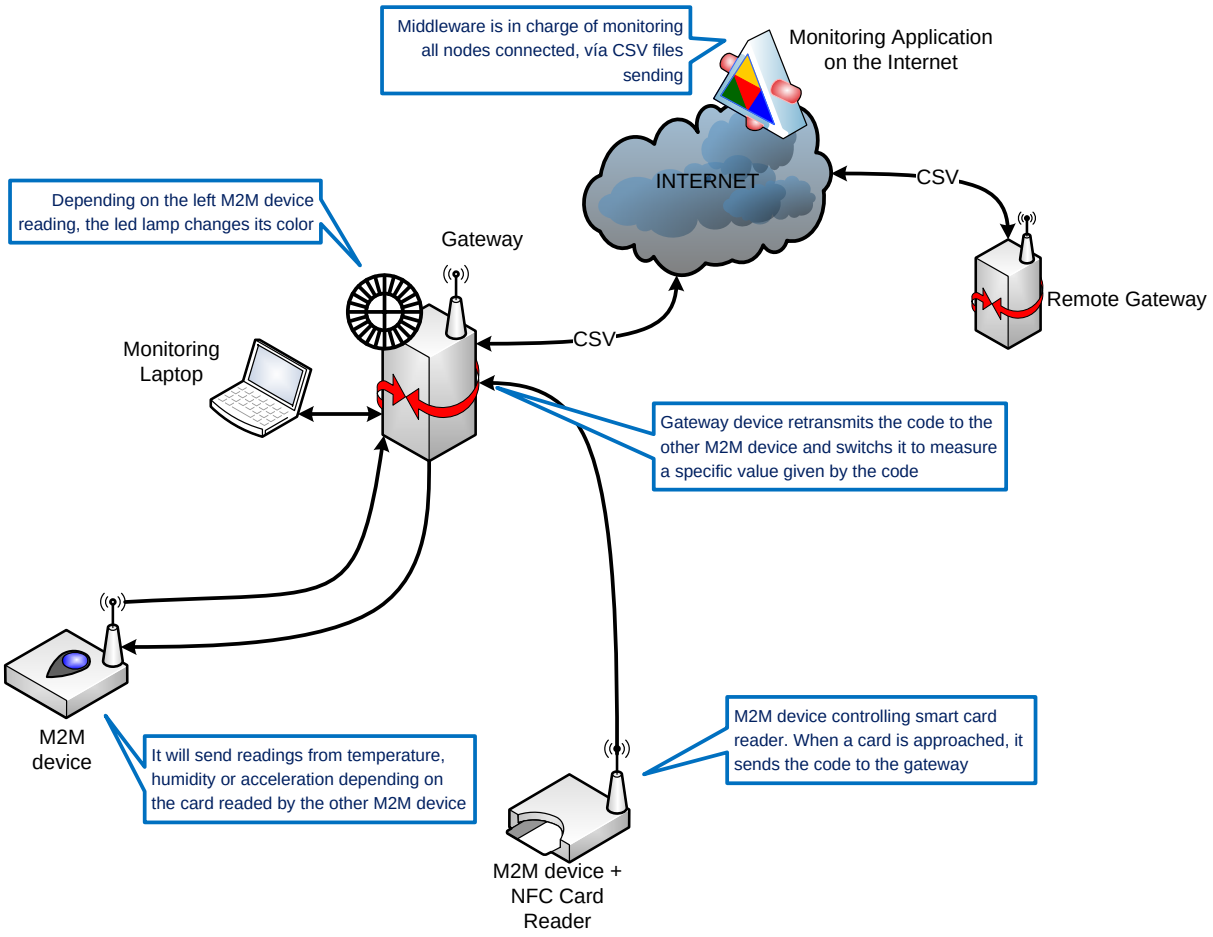

Figure 4.8: E2E connectivity and communication hardware demo architecture.

4.1.2.2 Address translation

The last element regarding E2E connectivity left to be proven (given the fact that previous demo demonstrates E2E connectivity between nodes in the same capillary network and LTE-M enabled nodes to the application server) is the seamless communication between end devices behind a gateway and a M2M server in the Internet.

This work is more complicated than the previous one, as end devices are usually non-IP devices, so some mechanism is needed to reach the application server for registering, and enabling the application server to contact individually the end devices.

For that reason, an address translation mechanism has been developed. The details of this address translation can be found in D4.2 deliverable [56]. In this demo this mechanisms is implemented in order to prove the E2E connectivity.

This way, two non-IP end devices with NFC capabilities are deployed behind a gateway with cellular interface. A specific remote application server is developed this time, in order to handle petitions from the end devices. It is in charge of collecting messages from end devices (conveniently treated by the gateway so as to seamlessly reach the end devices behind it) and replying with orders, flashing a LED depending on the NFC card approached.

Given all these constraints, the main goal of this demo is:

- To provide E2E connectivity between non-IP end devices and remote M2M servers placed in the IP core network.

Finally, the picture describing all elements placed in this demo is shown in Figure 4.9

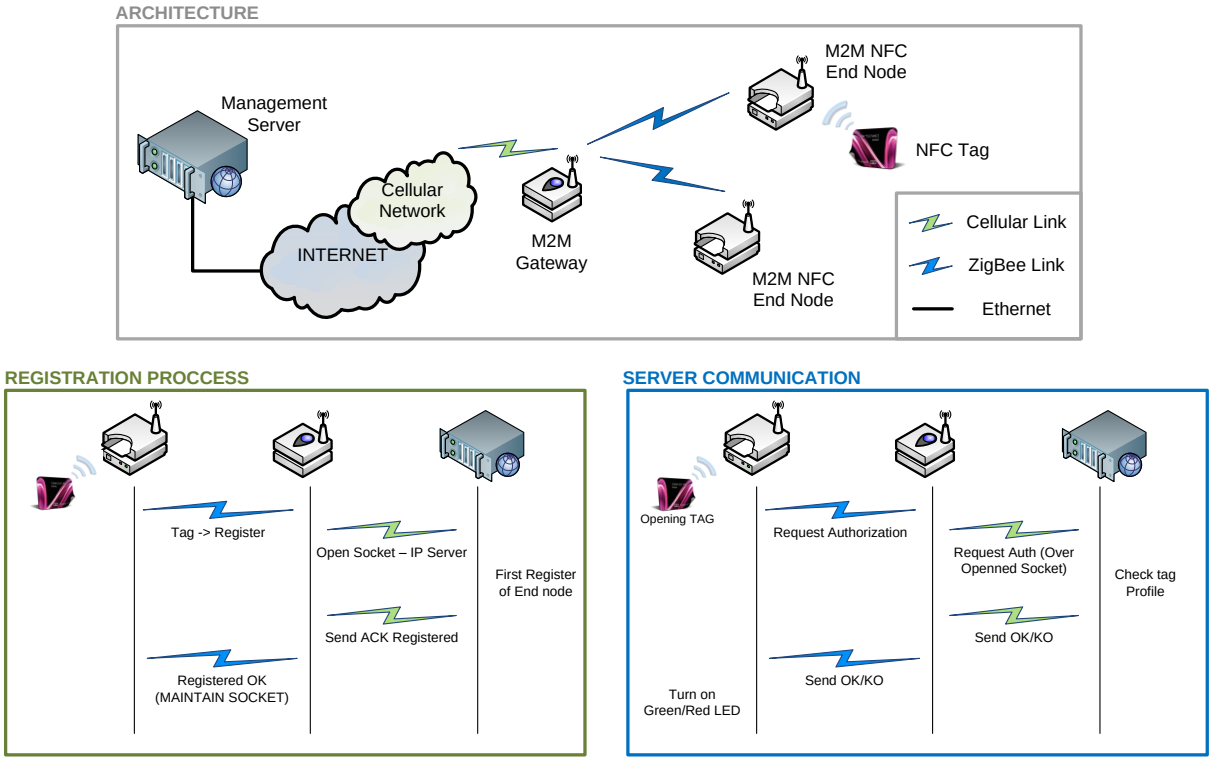

Figure 4.9: Architecture and message exchange for address translation demo.

4.2 Mobility models estimator for capillary networks

In most of the use cases considered within the EXALTED project, entities of both M2M capillary networks (non LTE-M devices, non LTE-M CH, M2M gateways) and LTE-M system (LTE-M devices, LTE-M relays) may move after their initial deployment and then change their attachment point over time. One of the main objectives targeted in EXALTED is to maintain connection/transmission integrity across aggregation points through heterogeneous connections (please see [1]). Mobility in capillary networks is then a challenging issue. Energy efficiency is another crucial goal of the project. Consequently, solutions that deal with mobility cannot be based on resource demanding procedures and signalization.

Mobility management is not restricted to a specific layer of the common protocol stack. It is rather a cross-layer task [57][58]. Furthermore, most of the algorithms designed for static scenarios do not apply well to mobile scenarios, and vice versa, whatever the layer is. The novelty proposed in this section is a low complexity tool that estimates and recognizes the model of mobility adopted by mobile entities; this information can then be provided to upper layers if they need it to adapt themselves to mobility. As a possible application by upper layers, an access channel method is proposed. The proposal is consequently not a mobility management method but rather a first step towards it. Regarding the common protocol stack, the work described in this section is application-dependent and could be used by all layers; nevertheless, the work itself is mapped into the following highlighted areas shown in Figure 4.10.

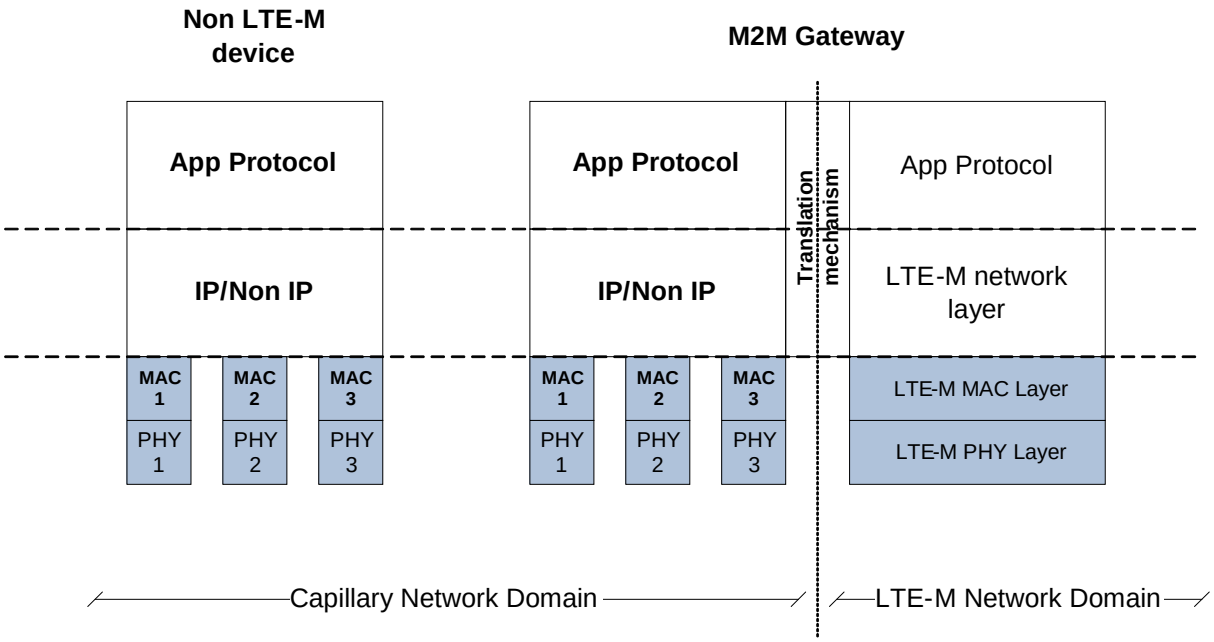

Figure 4.10. Mobility estimator areas: study on PHY and MAC layers.

Next subsections are organized as follows. First it is introduced the main mobility models proposed in literature by sorting them either as “ideal” or “life-like”. Then some metrics that can be useful to characterize mobility models are described. The content of these background sections is then exploited to derive a low complexity algorithm, called “Guess Who estimator” aiming at discriminating the current mobility model among a set of predefined models. Before developing the algorithm itself, it is firstly shown how discrimination between two mobility models may happen. Eventually, it is proposed to use this mobility estimator as input for a mobility aware access channel method.

4.2.1 Mobility models

A mobility model is designed to describe the movement pattern of mobile entities and how their localization, velocity and acceleration change over time. Accurate mobility modeling is necessary to simulate the behavior of mobile entities in targeted real life applications. Several mobility models have been proposed in literature; nevertheless all of them can be classified according to two major philosophies [59]-[62]:

- **Ideal** approach where mobility is characterized by simplified models that reduce the complexity of the model itself,
- **“Life-like”** approach where mobility models are derived from observations of real life behavior of network entities.

4.2.1.1 Ideal mobility models

Such mobility models, also called synthetic mobility models, do not aim at fully characterizing the real behavior of the mobile nodes. These models are well-adapted when a very accurate characterization of the mobility is not requested. Mainly, the movement on a node is characterized by few geometrical/statistical parameters that are related to its history, to other nodes in its neighborhood and to its environment. Depending on some characteristics of mobility models, a non-exhaustive classification can be derived with some of main models, as shown on Figure 4.11 [57].

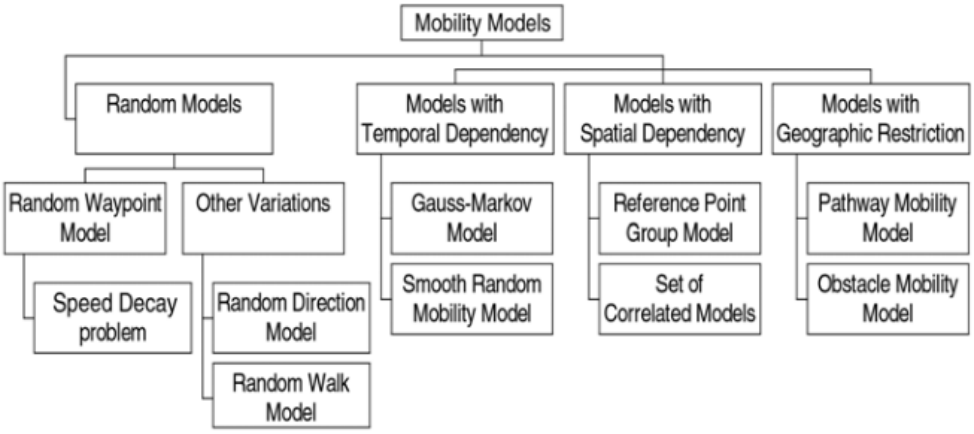

Figure 4.11: Mobility models classification.

A first class of models is characterized by parameters which are randomly set. Then, when the current movement of a mobile node is likely to be affected by its movement history, the related mobility model is said to be led by temporal dependency. On another side, models with spatial dependency refer to mobility scenarios where mobile nodes tend to travel in a correlated manner. The last class stands for mobility models with geographic restrictions and describes movements bounded by streets, freeways or obstacles.

A selection of some mobility models (MM) is proposed below with the main features that characterize them.

- **Random Waypoint MM**: At simulation start each node randomly selects its destination in the simulation field and then travels towards this location with constant speed uniformly and randomly chosen in the range [0; V_{max}], where the parameter V_{max} is the maximum allowable velocity for every mobile node. Velocity and direction are independent between nodes. Upon reaching its destination, the node stops for a duration defined by the pause time parameter T_{pause}. T_{pause}=0 leads to continuous mobility. After the pause, current node chooses again another random destination within the simulation field and moves towards it. The whole process is repeated again and again until the simulation ends.
- **Random Walk MM** was developed to mimic erratic movement. Mobile node moves from its current location to a new location by randomly choosing a direction and speed in which to travel. New speed and direction are respectively chosen from ranges [$speed_{min}$; $speed_{max}$] and [0; 2π] respectively. Each movement in the Random Walk MM occurs in either a constant time interval *t* or a constant distance traveled *d*, at the end of which a new direction and speed are calculated. If a mobile node which moves according to this model reaches a simulation boundary, then it bounces off the simulation borders with an angle determined by the incoming direction and then continues along this new path. It is a Brownian and memory-less mobility model.
- **Gauss-Markov MM** is one of mobility models with temporal dependency. Nodes may be constrained and limited by the physical laws of acceleration, velocity and rate of direction change. Hence, the current velocity of a mobile node may depend on its previous velocity. Thus velocities of single node at different time slots are correlated. This mobility characteristic is called the Temporal Dependency of velocity. Velocity of mobile node is firstly assumed to be correlated over time and modeled as a Gauss-Markov stochastic process [63].

$$\overline{V_t} = \bar{\alpha} \cdot \overline{V_{t-1}} + (1 - \bar{\alpha}) \cdot \bar{v} + \bar{\sigma} \cdot \sqrt{1 - \bar{\alpha}^2} \cdot \overline{W_{t-1}}, \quad (45)$$

where $\overline{V_t}$ and $\overline{V_{t-1}}$ are the velocity vector at time *t* and *t-1*, respectively. $\overline{W_{t-1}}$ is the uncorrelated random Gaussian process with mean 0 and variance σ^2; $\bar{\alpha}$, $\bar{\nu}$ and $\bar{\sigma}$ are the vectors that represent respectively the memory level, the asymptotic mean and the asymptotic standard deviation.
When a node is going to travel beyond the boundaries of the simulation field, the direction of movement is forced to flip 180 degrees. This way, the node remains away from the boundary of simulation field.

- **City Section MM** constraints node movements on a grid road topology where the edges of the graph represent bi-directional, single-lane roads.
- **Manhattan Grid MM** also uses a grid road topology by employing a probabilistic approach in the selection of nodes movements at each intersection.
- **ConstSpeed MM** does not use one of the standard approaches. A specific velocity and an update interval can be defined for each node. If the velocity is greater than zero (mobile node) the module in charge of mobility calculates a random destination for the node. Depending on update interval and velocity, it then calculates the number of steps to reach the destination, as well as the step-size. When the target position is reaches after the computed number of steps, mobility module calculates a new target position.
- **Mass MM**: A mobile node moves within the simulation area according to the following pattern. It moves along a straight line for a certain period of time before it makes a turn. This moving period is a normally distributed random number with expectation μ and standard deviation σ_1. When the node makes a turn, the new direction (angle) in which it will move is a normally distributed random number with expectation equal to the previous direction and standard deviation σ_2. Its new speed is also a normally distributed random number, with an expectation ranging from μ_{min} to μ_{max} (unit/sec) and standard deviation σ_3. This pattern of mobility is intended to model node movement during which the nodes have momentum, and thus do not start, stop, or turn abruptly. When it hits a wall, it reflects off the wall at the same angle.
- **Boundless Simulation Area MM** converts a 2D rectangular simulation area into a torus-shaped simulation area. Thus mobile nodes cannot go outside the simulation field and they do not bounce off borders.
- **Linear MM** is characterized by speed, angle and acceleration parameters. Angle only changes when the mobile node hits a wall: then it reflects off the wall at the same angle.
- **Circle** and **rectangle MM** are geometric mobility models defined within OMNeT++ mobility framework; they define respectively circle and rectangle movement models.

4.2.1.2 "Life-like" mobility models

"Life-like" mobility models are those mobility patterns observed in real life systems. A "life-like" model provides accurate information, especially when large number of nodes is involved and the observation period is long; it appears to be more realistic than ideal mobility models. The two main drawbacks of such an approach are the complexity cost introduced by the higher level of accuracy intrinsically targeted by these models and the large observation time required to achieve the desired accuracy of the model. In practice, depending on the complexity budget of the above process or the time variation of the mobility itself, such models may be suitable or not.

The characterization of wireless channel has to take into account various facets like multi-path, fading and obstacles. Moreover, channel design is stressed by mobility of nodes. For all these reasons it is necessary to choose a simulator that implements mobility models with an effective degree of accuracy if the goal is to mimic realistic behavior of a mobile environment. On one hand there are simplicity and widespread features with ideal mobility

models, on the other hand there are better simulations results with “life-like” mobility models but more work to implement these models. In the remainder, the focus will be put on ideal models.

4.2.1.3 Metrics for characterizing mobility models

In this section the first goal is to investigate how mobility models can be efficiently characterized and second to define the set of best parameters or metrics needed to differentiate mobility models. To that end some mobility metrics have been defined in [64]-[66]. First of all some basic notations are introduced in Table 4-1.

Table 4-1: Adopted notations used in presentation of mobility metrics.

$\vec{V_i}(t)$	Velocity vector of node *i* at time *t*
$\lvert\vec{V_i}(t)\rvert$	Speed of node *i* at time *t*
$\theta_i(t)$	Angle made by $\vec{V_i}(t)$ at time *t* with the X-axis
$\vec{a_i}(t)$	Acceleration vector of node *i* at time *t*
$x_i(t)$	X co-ordinate of node *i* at time *t*
$y_i(t)$	Y co-ordinate of node *i* at time *t*
$D_{i,j}(t)$	Euclidean Distance between nodes *i* and *j* at time *t*
$RD\left(\vec{a}(t),\vec{b}(t')\right)$	Relative Direction (RD) (or cosine of the angle) between the two vectors $\vec{a}(t)$, $\vec{b}(t')$is given by $\frac{\vec{a}(t)\cdot\vec{b}(t')}{\lvert\vec{a}(t)\rvert*\lvert\vec{b}(t')\rvert}$
$SR\left(\vec{a}(t),\vec{b}(t')\right)$	Speed Ratio (SR) between the two vectors $\vec{a}(t)$, $\vec{b}(t')$ is given by $\frac{\min\lvert\vec{a}(t)\rvert,\lvert\vec{b}(t')\rvert}{\max\lvert\vec{a}(t)\rvert,\lvert\vec{b}(t')\rvert}$
R	Transmission range of a mobile node
N	Number of mobile nodes
T	Simulation time
$rand()$	function which returns a uniformly distributed value in the interval [−1;1]

Mobility metrics could be used to differentiate different mobility patterns presented in literature. The basis of differentiation is to analyze spatial dependence, temporal dependence and geographic restrictions.

Degree of Spatial Dependence: It measures similarity of velocity for two close nodes.

$$D_{spatial}(i,j,t) = RD\left(\vec{v_i}(t),\vec{v_j}(t)\right) * SR\left(\vec{v_i}(t),\vec{v_j}(t)\right) \quad (46)$$

$D_{spatial}(i,j,t)$ is high when nodes i and j travel in more or less the same direction and at almost similar speeds. However, $D_{spatial}(i,j,t)$ decreases if RD or SR decreases. Since remote nodes cannot be spatially dependent, there is an additional condition, where $c_1 > 0$ is a constant:

$$D_{i,j}(t) > c_1 * R \Rightarrow D_{spatial}(i,j,t) = 0. \quad (47)$$

Average Degree of Spatial Dependence: $\overline{D}_{spatial} = \frac{\sum_{t=1}^{T}\sum_{i=1}^{N}\sum_{j=i+1}^{N} D_{spatial}(i,j,t)}{P}$, where *P* is the number of tuples (i,j,t) such that $D_{spatial}(i,j,t) \neq 0$. Thus, if mobile nodes move independently of one another, then the mobility pattern is expected to have smaller value for $\overline{D}_{spatial}$. On the other hand, if the node movement is coordinated by a central entity, or

influenced by nodes in its neighborhood, such that they move in similar directions and at similar speeds, then the mobility pattern is expected to have a higher value for $\overline{D}_{spatial}$.

Degree of Temporal Dependence: It measures velocity similarity for a node at two time slots that are not too far apart. It is a function of both acceleration of the mobile node and geographic restrictions.

$$D_{temporal}(i,t,t') = RD\left(\vec{v_i}(t),\vec{v_i}(t')\right) * SR\left(\vec{v_i}(t),\vec{v_i}(t')\right) \quad (48)$$

$D_{temporal}(i,t,t')$ is high when the node moves in more or less the same direction and almost at the same speed over a certain time interval. However, $D_{temporal}(i,t,t')$ decreases if RD or SR decreases. Similarly to $D_{spatial}(i,j,t)$, the following condition appears, where $c_2 > 0$ is a constant:

$$|t - t'| > c_2 * R \Rightarrow D_{temporal}(i,t,t') = 0. \quad (49)$$

Average Degree of Temporal Dependence: $\overline{D}_{temporal} = \frac{\sum_{i=1}^{N}\sum_{t=1}^{T}\sum_{t'=t+1}^{T} D_{temporal}(i,t,t')}{P}$, where *P* is the number of tuples (i,t,t') such that $D_{temporal}(i,t,t') \neq 0$. Thus, if the current velocity of a node is completely independent of its velocity at some previous time step, then the mobility pattern is expected to have a smaller value for $\overline{D}_{temporal}$. However, if the current velocity is strongly dependent on the velocity at some previous time step, then the mobility pattern is expected to have a higher value for $\overline{D}_{temporal}$.

Since networks performance is affected by the network topology dynamics, it is worth to consider some metrics to analyze the effect of mobility on the connectivity graph between the mobile nodes. The connectivity graph is the graph $G = (V,E)$, such that $|V| = N$ and at time *t*, a link $(i,j) \in E$ if $D_{i,j}(t) \leq R$. Let $X(i,j,t)$ be an indicator random variable such that $X(i,j,t) = 1$ if there is a link between nodes *i* and *j* at time *t*.
Let $X(i,j) = \min_{t=1}^{T} X(i,j,t)$ be an indicator random variable which equals '1' if a link exists between nodes *i* and *j* at any time during the simulation, '0' otherwise.

Number of Link Changes: For a pair (i,j) of nodes, it is the number of times the link between them switches from "down" to "up".

$$LC(i,j) = \sum_{t=1}^{T} C(i,j,t) \quad (50)$$

where $C(i,j,t)$ is an indicator random variable such that $C(i,j,t) = 1$ if $X(i,j,t-1) = 0$ and $X(i,j,t) = 1$, i.e. if the link between nodes *i* and *j* is down at time *t−1*, but comes up at time *t*.

Average Number of Link Changes: $\overline{LC} = \frac{\sum_{i=1}^{N}\sum_{j=i+1}^{N} LC(i,j)}{P}$, where *P* is the number of pairs (i,j) such that $X(i,j) \neq 0$.

Link Duration: It is the average duration of the link existing between two nodes *i* and *j*. It measures stability of the link between these nodes.

$$LD(i,j) = \begin{cases} \frac{\sum_{t=1}^{T} X(i,j,t)}{LC(i,j)} \; if \; LC(i,j) \neq 0 \\ \sum_{t=1}^{T} X(i,j,t) \cdot LC(i,j) \; otherwise \end{cases} \quad (51)$$

Average Link Duration: $\overline{LD} = \frac{\sum_{i=1}^{N} \sum_{j=i+1}^{N} LD(i,j)}{P}$, where *P* is the number of pairs (i,j) such that $X(i,j) \neq 0$.

Path Availability: It is the fraction of time during which a path is available between two nodes *i* and *j*. The node pairs of interest are the ones that have communication traffic between them.

$$PA(i,j) = \begin{cases} \frac{\sum_{t=start(i,j)}^{T} A(i,j,t)}{T - start(i,j)} \; if \; T - start(i,j) > 0 \\ 0 \; otherwise \end{cases} \quad (52)$$

where $A(i,j,t)$ is an indicator random variable equal to '1' if a path is available from node *i* to node *j* at time *t*, and '0' otherwise. $start(i,j)$ is the time when communication traffic between nodes *i* and *j* starts.

Average Path Availability: $\overline{PA} = \frac{\sum_{i=1}^{N} \sum_{j=i+1}^{N} PA(i,j)}{P}$, where *P* is the number of pairs (i,j) such that $T - start(i,j) > 0$.

4.2.2 Achievements and proposed application

This section starts with a preliminary section including an example to illustrate how aforementioned metrics can help in discriminating two models of mobility. Then the proposed algorithm, called "Guess-Who estimator", is described; it aims at estimating the mobility model that best fits to movement of mobile nodes. In a last subsection we propose a channel access method that exploits this mobility estimator to adapt itself to the mobility scenario.

4.2.2.1 Differentiation of two mobility models

Link duration has been computed for different velocities of nodes and different transmission range among devices. The purpose was to find out differences among average link duration value for mobility models under exams (Random Waypoint and Gauss-Markov models). These two models are synthetic models and of course do not fit very well to realistic movements of mobile nodes that would be better described by "like-like" models, at the expense of harder computation and complexity. These two models are popular models and benchmarks to evaluate MAC and routing protocols in mobile ad hoc networks. Random waypoint model is especially appreciated for its simplicity and its flexibility since no constraint is inherent in this model. Results are shown on Figure 4.12.

For the interpretation of this figure, it is assumed that the transmission range value is not known a priori. To represent how mobility models can be discriminated with help of mobility metrics, two different cases are considered and are illustrated with the two pictures of Figure 4.12. . These two cases differ in the average link duration value along the Y-axis. Contrary to the picture on the left, the picture on the right depicts a combination of parameters for which it is possible to identify the specific mobility model.

Assuming that $\overline{LD}$ and speed of devices are known, the first picture of Figure 4.12 shows a combination of values that does not let discriminate Gauss-Markov and Random Waypoint

models. On the other hand, the second picture of Figure 4.12 illustrates a scenario with which some resolution fields (transmission range) can be found out, once given speed and $\overline{LD}$ values for a group of nodes, which allow us to assign to the group, a specific mobility model.

In most of wireless systems we can assume that transmission parameters such as transmission power are known a priori. This permits to compute the coverage area within which two nodes may interact together. Nevertheless, this area differs from the reliable transmission range since the presence of surrounding nodes which may interfere, the momentary communication scenario and many other systems parameters that add dynamic may affect the transmission area within which two nodes can reliably communicate. Consequently, the use of mobility metrics such as the average link duration $\overline{LD}$ may help in achieving our goal of models discrimination. In next part it is shown that this examination is very interesting to build, step by step, a complete approach to the mobility models valuation.

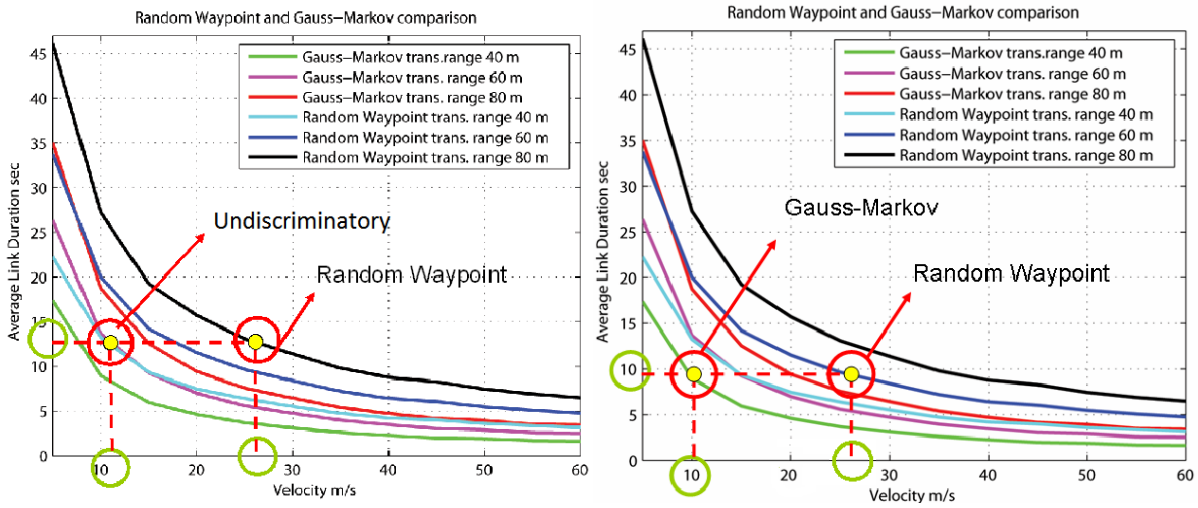

Figure 4.12: Mobility models comparison in terms of Average Link Duration.

4.2.2.2 Mobility model estimator: "Guess Who" algorithm

In the previous section it was shown how it is possible to differentiate two mobility models by processing a single mobility metric. In case that a single mobility metric does not univocally identify a mobility model, a network entity could use several mobility metrics and information to identify the mobility model of a group of devices. In the remaining of this section we introduce our three-step "Guess Who" estimator. This algorithm simply tries to associate a mobility model with a group of mobile nodes. The aim is to provide the mobility information as an input for services and applications that could require it.

The name of the algorithm has arisen from a two-player guessing game, called "Guess Who". In this game each player is given an identical board containing cartoon images of 24 people identified by their first names. The game begins with each player selecting a card of its choice from a separate set of cards containing the same 24 images. The object of the game is to be the first to determine which cards one's opponent has selected; this is done by asking different 'yes' or 'no' questions to eliminate candidates, such as: "Does this person wear glasses". When one's opponent provides the answer, one eliminates those that do not fit the criterion by "flipping down" the cars on one's board.
Referring to our system model, it is possible to associate those 24 images with the different mobility models; mobility metrics help us to discriminate models and let us formulate the "yes

or no" questions. Table 4-2 summarizes some mobility models and mobility metrics used by the "Guess Who" algorithm.

Table 4-2: Discriminatory characteristics of mobility models.

Parameters / Mobility Models	Movement	Speed	Pause Time	Average Link Duration	Degree of Spatial Dependence	Degree of Temporal Dependence	Number of Link Change
Gauss-Markov	No Linear	Changeable	Yes	known	/	/	/
Random Walk	Linear	Constant	No	Unknown	/	/	/
A Boundless Simulation Area	No Linear	Changeable	No	Unknown	/	/	/
City Section	Linear	Changeable	Yes	Unknown	/	/	/
Manhattan Grid	Linear	Changeable	Yes	Unknown	/	/	/
Random Waypoint	Linear	Constant	Yes	Known	/	/	/
Circle	Geometry	Constant	No	Unknown	/	/	/
Rectangle	Geometry	Constant	No	Unknown	/	/	/
Linear	Linear	Changeable	No	Unknown	/	/	/
ConstSpeed	Linear	Constant	No	Unknown	/	/	/
Mass	No Linear	Changeable	Yes	Unknown	/	/	/

All considered mobility models are represented in the first column of the table; whereas, on the first line of the table, it has been divided into two groups the parameters needed to characterize mobility models. Basic mobility information such as speed, co-ordinates and pause-time are blue-colored; these are the first information provided by a supervising entity (e.g. gateway in case of capillary networks). Mobility metrics, such as average link duration, degree of spatial dependence, degree of temporal dependence and number of link change are green-colored; these metrics need a computational process carried out by a devoted mobility entity.

Therefore, the blue-colored parameters are the first values offered to the algorithm; these could be used immediately. If blue-colored parameters are not sufficient for a complete mobility model valuation, it is possible to use also green-colored parameters. In this case, the algorithm has to wait for the necessary time to calculate mobility metrics. This additional time is a negative facet of green parameters. Moreover, the devoted mobility entity that has the responsibility for performing mobility management operation, suffers from an additional charge which is both computational and energetic.

The "Guess Who" algorithm is divided into **two cycles** that correspond to the two colors of the table shown in Table 4-2. Each cycle is performed by a different entity: during the first cycle, the "Guess Who" algorithm is performed by the 'group leader', whereas, execution of second cycle is managed by another network entity. Algorithm proceeds as follow:

Step 1: The algorithm starts to calculate possible locus such as a circumference, a rectangle and a straight curve. If it does not find out any locus, in any case it considers that as a surplus information because it allows to differentiate Circle, Rectangle and Linear (Random Waypoint, Random Walk, etc.) mobility models to Mass, Boundless Simulation Area and Gauss-Markov mobility models.

Step 2: The "black-box" supplies speed and pause-time information. By exploiting the Table 4-2 and reminding the "Guess Who" game, the entity could "flip down" more than the thirty percent of mobility models with a low error percentage.

Step 3: The algorithm goes on to the second cycle where the entity memorizes information in order to compute green-colored mobility metrics. In this phase it is possible to compare results of the first cycle with the ones of second cycle, "flipping down" other mobility models.

For example, after the first cycle, the algorithm has valuated two mobility models, Gauss-Markov and Boundless Simulation Area. Then, thanks to the calculated mobility metrics, at the end of the second cycle it possible to obtain a complete mobility model valuation. Naturally "Guess Who" algorithm recognizes a mobility model only if it has a sufficient characterization.

Figure 4.13 illustrates the 'Guess Who' game employed to discriminate several mobility models.

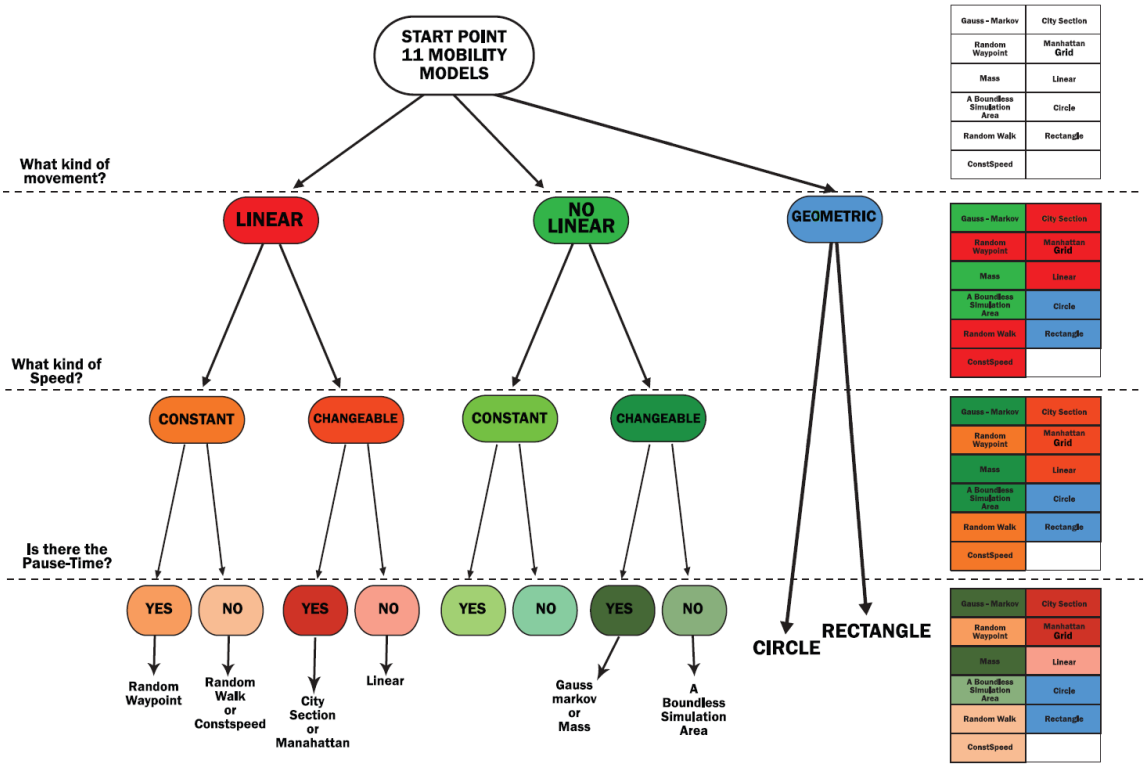

Figure 4.13: Tree Diagram of "Guess Who" algorithm.

4.2.2.3 Mobility aware MAC approach

In this last section we introduce an application of the "Guess Who" estimator for MAC protocols that we are investigating. More precisely, the focus is put on a mobility aware access method for capillary networks. The basic idea is to exploit the "Guess Who" algorithm with DA-MAC access method [67]. DA-MAC stands for Density Aware MAC and proposes efficient forwarding in multi-hop dense and dynamic wireless sensor networks.

DA-MAC is based on the fact that system performance (in case of networks such as wireless sensor networks or capillary networks) highly depends on nodes density. Indeed, because of battery exhaustion, fault or new deployment, nodes may appear or disappear, resulting in highly dynamic topology and then dynamic routes between nodes. The probability of collision between competing transmissions increases with density of nodes. Furthermore, a higher collision probability leads to higher energy consumption due to retransmission mechanisms. Hence DA-MAC offers a configurable channel sensing phase during which nodes request transmission opportunity in a way that avoids collisions. The receiver can thus schedule transmissions so that nodes may return to sleep and only wake up at their scheduled transmission instants. Simulation results have shown that DA-MAC achieves lower latency,

higher delivery ratio and lower energy consumption than other channel access methods proposed in literature (B-MAC, SCP-MAC).
DA-MAC assumes that local density, *i.e.*, the average number of neighbors, is provided for each node by the parent node (which can be the cluster head, the gateway or the LTE-M relay in case of EXALTED). With the knowledge of its local density, each node is able to set efficiently the size of its contention window and its probability of participating to current contention period so as to ensure a probability of success under a given threshold.

Here it is proposed to relate density to mobility. Indeed in dynamic networks, mobility of nodes leads to variation of density. Let us consider a given instant t_0 and realize a 'snapshot' of nodes deployment at this instant. After a given period T during which nodes have moved and potentially left the network and disappeared, a second snapshot of nodes deployment at instant t_0+T can be considered. Between these two consecutive snapshots density of nodes have changed due to mobility.

In DA-MAC, local density of each node is either assumed to be perfectly known, or estimated by the parent node, based on requests for channel opportunity sent by contending neighbors. In this second case nodes that are in idle or sleep state are not considered even if they may request channel opportunity in a close future; besides all contending nodes are not necessarily neighbors in the sense of transmission range. With use of the "Guess Who" algorithm, each node – or possibly an entity devoted to some mobility management tasks such as cluster head, gateway or relay – can guess the current mobility model of mobile nodes to be able to predict future position of mobile nodes and then predict local density variation. In such approaches where a value is regularly updated the accuracy of estimation is a crucial issue since a 'drift' between estimation and accurate value may lead to error propagation. Hence some parameters should probably be periodically synchronized to avoid such a drift leading to bad network performance.

4.3 Analysis of IP address assignment for the LTE terminals and assignment of the IP addresses to M2M devices behind the Gateway

In this section, principles of IP address assignment for the LTE-M devices and assignment of the IP addresses to M2M devices behind the M2M Gateway are proposed and analyzed.

LTE-M devices and M2M gateways are obtaining IP addresses from the LTE-M network, while M2M devices behind the M2M Gateways could obtain addresses from DHCP server which can be located in different parts of the M2M network.

On the common protocol stack, this can be mapped into the following highlighted areas shown in Figure 4.14.

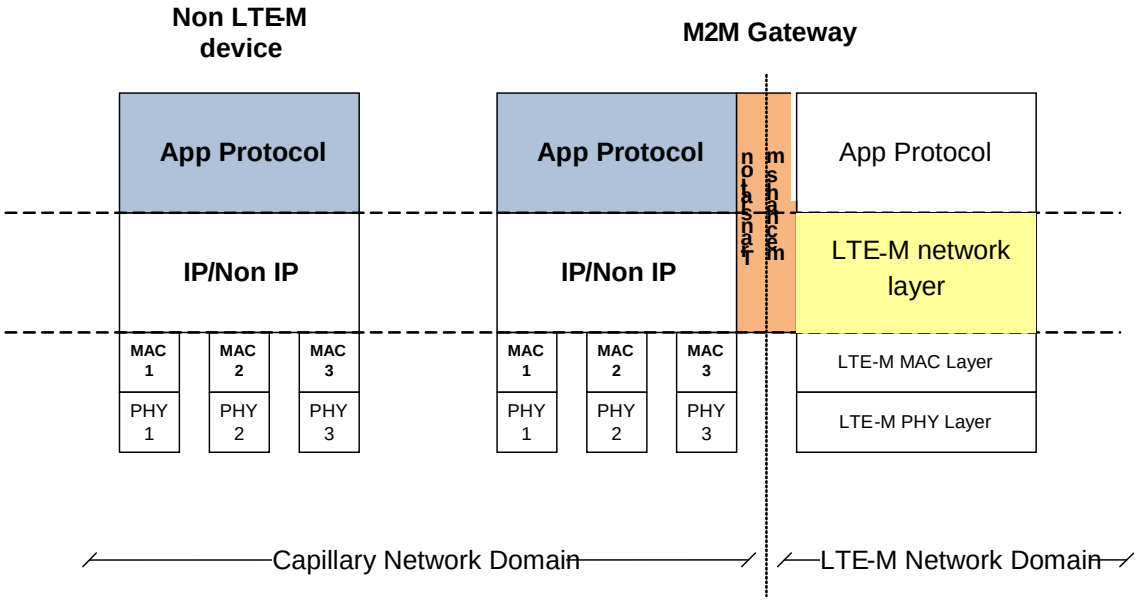

Figure 4.14. IP address assignment focus areas: study of IP address assignment for the LTE terminals and assignment of the IP addresses to M2M devices behind the Gateway

The assignment of IP addresses to LTE-M devices and M2M gateways is performed by the EPC core network. IP address allocation to the terminals in 3GPP Release 10 is explained in detail in the corresponding 3GPP recommendation [86]. A UE (in our case LTE-M device) shall perform the address allocation procedures for at least one IP address (either IPv4 address or IPv6 prefix) after the default bearer activation.

One of the following ways shall be used to allocate IP addresse for the UE:

- The Home Public Land Mobile Network (HPLMN) allocates the IP address to the User Equipment (UE) when the default bearer is activated (dynamic or static HPLMN address);
- The Visited Public Land Mobile Network (VPLMN) allocates the IP address to the UE when the default bearer is activated (dynamic VPLMN address);
- The Packet Data Network (PDN) operator or administrator allocates an (dynamic or static) IP address to the UE when the default bearer is activated (External PDN Address Allocation).

Thus, if the UE is in the in the home or visited network, then HPLMN or VPLMN will through regular LTE procedures allocate IP address to UE, while in the last mentioned case PDN operator/administrator will allocate IP adresses from his own pool of addresses. Addresses could be static or dinamic. The static addresses should be defined and saved on the HSS as UE subscription parameters and retrived from HSS during registration process, and dynamic addresses are assigned from the available DHCPs pools.

The IP address allocated for the default bearer shall also be used for the dedicated bearers within the same PDN connection. A PDN connection consists of one default bearer and, depending on the service for which the connection is used, a number of dedicated bearers. IP address allocation for PDN connections, which are activated by the UE requested PDN connectivity procedure, is handled with the same set of mechanisms as those used within the *attach* procedure (procedure for registering with the network). The purpose of PDN connectivity procedure is to set up a default Evolved Packet System (EPS) bearer between a UE and a packet data network.

PDN types IPv4, IPv6 and IPv4v6 are supported. An EPS Bearer of PDN type IPv4v6 may be associated with one IPv6 prefix only or with both one IPv4 address and one IPv6 prefix. PDN type IPv4 is associated with an IPv4 address. PDN type IPv6 is associated with an IPv6 prefix. PDN types IPv4 and IPv6 are utilised for the UE and/or the PDN Gateway supporting IPv4 addressing only or IPv6 prefix only; or operator preferences dictate the use of a single IP version only, or the subscription is limited to IPv4 only or IPv6 only for this APN. In addition, PDN type IPv4 and IPv6 are utilised for interworking with nodes of earlier releases.

The way that the UE sets the requested PDN type may be pre-configured in the device per Access Point Name (APN). Unless otherwise configured (including when the UE does not send any APN), the UE sets the PDN type during the Attach or PDN Connectivity procedures based on its IP stack configuration as follows:

- A UE which is IPv6 and IPv4 capable shall request for PDN type IPv4v6.
- A UE which is only IPv4 capable shall request for PDN type IPv4.
- A UE which is only IPv6 capable shall request for PDN type IPv6.
- When the IP version capability of the UE is unknown in the UE (as in the case when the Mobile Treminal (MT) and Terminal Equipment (TE) are separated and the capability of the TE is not known in the MT), the UE shall request for PDN type IPv4v6.

Based on the described procedure LTE-M capable device or gateway will obtain IP address from the LTE/LTE-M network. Also, it is up to the operator, if addresses for LTE-M devices/services will be assigned to a separate APN, or they will treat LTE-M devices/gateways as other LTE users.

There are a few options for M2M devices behind the gateway to obtain IP addresses. Overview of the mechanisms for assigning IP addresses could be found in EXALTED deliverable D3.2 [85]. Capillary networks could obtain IP addresses from different DHCP server located in different parts of the overall network.

One possible way would be to communicate with the DHCP server which is located in the network domain of EXALTED, or which is located in the Internet and is accessible to EXALTED. In that case communication with DHCP server is going through LTE-M network, while M2M Gateway runs software implementing DHCP Client functionality, and PDN is acting as DHCP Relay.

Other possibility would be that M2M gateway itself implements DHCP server which will distribute IP addresses to the end devices.

Finally, IP addresses of the capillary network M2M devices could be allocated locally (for example from local DHCP server), and M2M gateway will perform necessary address translation.

In all cases M2M gateway is supposed to perform the maintenance of address translation mapping tables, since IP addresses in capillary networks are not visible for the LTE-M core network.

5. Payload Reduction for Supporting MAC Efficiency

In this section the focus is on application layer, by providing high-level efficiency with light-weight transport protocol and payload reduction methods. The transport protocol can be used in the entire system from end-to-end, or only in capillary network. This option is enabled by interoperability of transport protocol and payload format between M2M Device Domain and LTE Core Network.

On the common protocol stack, this can be mapped into the following highlighted areas shown in Figure 5.15.

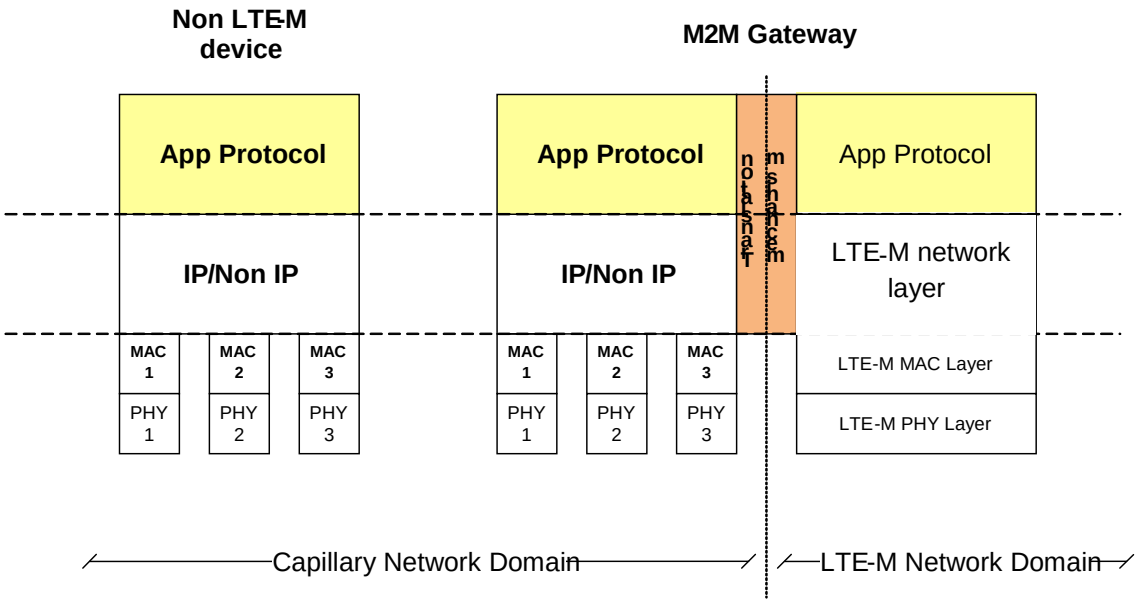

Figure 5.2. High-level transport protocol and Payload reduction focus area

One of the goals of the EXALTED project is to leverage PHY and MAC layer mechanisms for M2M communications over LTE networks. Efficient PHY/MAC protocols/procedure for M2M capillary networks will provide more efficient handling of a large number of M2M devices. Integration of such a large number of devices with varying characteristics and capabilities is a complex task that requires cross-layer optimization. Thus, the PHY/MAC layer optimization for M2M networks need to be accompanied by higher layer optimization such as application protocols oriented on available resources and payload reduction mechanisms in order to achieve overall efficiency [75].

The structure of this section is as follows: In 5.1 state of the art of higher layer protocols for M2M, including design considerations for Constrained Application Protocol (CoAP) is given in order to leverage the higher layer protocols for the EXALTED E2E system. In 5.2, different payloads over CoAP protocol are evaluated.

5.1 State of the art M2M protocols

This section summarizes the state of the art M2M protocols and current efforts in the field of M2M communications. As there are standardization efforts, as well as industrial work, this survey will present and inline the differences and give a comparison of available M2M protocols that can be used in the E2E M2M system foreseen in EXALTED.

The high-level concepts of the M2M protocols are:

- Connecting many devices and many isolated backend solutions
- Hiding the complexity of underlying network and embedded devices
- Providing valuable and simple APIs and open service enabler platform to application/service developers

In this section, the main evaluation criteria for M2M protocols are:

- Architecture - REST (Representational State Transfer) is seen as a suitable global architecture design for resource management for M2M, and is leveraged in ETSI standardization as a key E2E solution. Protocols that are compatible with REST architecture are advantageous over the other architectures
- Network transport – Transport agnostic protocol can be used in any configuration and use case scenario.
- Bandwidth – energy consumption is highly correlated with the number of transferred bytes and bits. Efficient payload format can significantly reduce energy consumption. Protocols that are bounded to a verbose data format are not desirable
- Complexity - Usability of protocol depends of its design complexity. If a certain protocol is “over-designed” to satisfy all possible scenarios, for devices with limited computational resources this means that protocol is too complex and consumes too much resources
- M2M Enablers – Gateway enabler. Gateway has the ability to host user services, acting as Communication Bridge between outside and capillary networks by implementing communication interfaces, (e.g. for Zigbee, 6lowPan).
- License and maturity - If protocol is designed from a small group and it is not maintained from community, the fast development of new software and hardware will make this protocol unusable. Open source protocol have higher chance to continue to exists than closed implementations

In the following subsections, a brief overview of the M2M protocols and design consideration for CoAP are given.

5.1.1 BiTXml

The BitXML [53] is application level protocol that defines commands and control information exchange for specific communication scenarios. The protocol specifies syntax and semantics for data exchange between gateway and M2M devices and between M2M devices itself.

The BiTXml reference model includes Gateway application –software that works as remote execution unit, Controller –software that controls Gateway unit, and sensors and actuator devices. The specification states that BiTXml can use any kind of transport layer; it is assumed that session-less protocol can also use BiTXml because Gateway application supports asynchronous and synchronous processing. BiTXml DNS protocol client is an enabler that allows handling of Gateway with dynamically assigned addresses (e.g. GPRS, WiFi network devices).

Functionalities
Addition functionalities in BiTXml protocol is Condition Monitor that periodically checks conditions and sends events when one or more conditions evaluates to true. This is enabled due the logic in the Gateway application imposed with an XML elements defined with a conditional statements written in a BiTXml V2 scripting language. History monitor generates state values and collects them; Reconfiguration checker verifies that Gateway configuration have possible updates.

BiTXml supports asynchronous and synchronous messaging model. Nevertheless, if synchronous processing is applied for exchanging the messages, only the basic execution of BiTXml commands is possible, which excludes Condition, History and Reconfiguration monitor functionalities.

License and libraries
The BiTXml is open source and there are official libraries releases in Java and .NET. Libraries are outdated and not maintained since 2005.

5.1.2 MQTT-S

MQ Telemetry Transport (MQTT) [73] protocol is an open publish/subscribe protocol designed specifically for remote telemetry applications and optimized for communications over low-bandwidth and it uses TCP/IP as underlying transport. MQTT-S is a version of protocol adapted to WSN networks, preliminary developed for ZigBee. The MQTT-S is also based on bi-directional communication, but it requires only three bytes of overhead to set up a session, compared to 1000 bytes for TCP/IP session initiation.

MQTT does not specify any routing or networking techniques; it assumes that the underlying network provides a point-to-point, session-oriented, auto-segmenting data transport service with in-order delivery (such as TCP/IP) and employs this service for the exchange of messages [63]. In contrast to MQTT, MQTT-S does require connection service, and does not rely on message segmentation, nor does it deliver those segments. MQTT-S is agnostic of the underlying networking services - any network which provides a data transfer between two end points and a particular gateway should be able to support MQTT-S.

The MQTT-S architecture is based on three components: MQTT-S clients, MQTT-S gateways, and MQTT-S forwarders and MQTT broker. These components can be mapped to architecture of many required WSN application where the above mentioned components corresponds to an M2M devices, Gateways and Relays. MQTT is using publish/subscribe approach, that requires broker as a component that allows data to be collected from WSN and advertized to other interested parties. This architecture is not universal for M2M domain, but in WSN it can be efficiently exploited.

MQTT-S clients connect to a MQTT broker via a MQTT-S Gateway using the MQTT-S protocol. A MQTT-S GW may or may not be integrated with a MQTT broker.
All traffic that is going towards the server must be translated. The syntax translation is actually translation between MQTT-s and MQTT as the lightweight version of protocol is intended only for the constrained clients' devices.

Functionalities
The main concern of this protocol is its usability in other systems than M2M, because addressability is questionable due the publish/subscribe approach that delivers data based on interests rather than individual device addresses.
The paper [63] evaluates the MQTT-s protocol and presents the implementation and reveals problems with the broker in certain use cases. Therefore protocol maturity is still in its early stage unlike its older version.

Libraries and licenses
There are no MQTT-S official/unofficial library releases. This protocol is still in its initial phase, followed with a specification derived from an original MQTT implementation.

5.1.3 M2MXML

The M2MXML [57] protocol is an XML based messaging protocol designed for a M2M communication. This protocol defines an XML semantic for commands, addressability and communication by using XML namespace elements that can be optional or mandatory.
Protocol is straight forward and does not provide reference architecture elements, but rather semantics model for telemetry devices and transducers.

Functionalities
M2MXML specifies models and XML encoding that provide a framework for the M2M communication, measurements and device configuration. Message semantics is defined for request/response model with batch sensor readings, device configuration (i.e. device turn on/off/reboot as well as for querying sensor properties).
As any M2M device is composed of one or more transducers (sensors or actuators), these devices are addressed by using namespace that contain alphanumeric address unique for each device. Transducer addresses are arbitrary strings with a maximum length of 128 characters and may contain any valid unicode characters. Address is optional and if specified; this indicates that the message is intended to apply to a transducer. If not specified, the message applies to the telemetry device. Messages may also contain a sequence number attribute that can be used to match queries to responses [1].

Licenses and libraries
M2MXML is licensed and distributed under the terms of the GNU Library or Lesser General Public License (LGPL). There is Java open source library implementation available, but it is not well supported by community and latest update was 2006.

5.1.4 CoAP

CoAP (Constrain Application Protocol) [56] is a light-weight application layer protocol that utilizes patterns from HTTP for URIs, Resource abstraction and RESTful interaction and extensible header options. The one of crucial differences from a HTTP is that CoAP uses UDP transport protocol that enables one-to-many and many-to-many communication.

The CoAP is REST based protocol that provides request/response interaction model for asynchronous message exchanges. The Request/Response layer and the Message layer are just features of the CoAP header, and therefore it is a single layer protocol. The UDP layer receives a message from the message layer, packs it into a datagram and sends it to the IP layer of the OSI or the TCP/IP architecture. Similarly, in the opposite direction, the UDP layer receives a datagram from the IP layer and unpacks it into a message readable by the application layer.

Functionalities
The main capabilities are resource discovery, multicast, simple proxy and caching. CoAP employs unreliable, asynchronous UDP protocol that does not provide reliability on transport layer. This is overcome with lightweight reliability mechanisms based on confirmation of a message reception with an acknowledge response. Every message contains ID number for duplicate detection but also, for reliability. If no ACK message was received in some time, the message is retransmitted. RESPONE_TIMEOUT and MAX_RETRANSMIT determine how to retransmit.

A proxy is a CoAP end-point that can be tasked by CoAP clients to perform requests on their behalf. This may be useful, for example, when the Proxy is caching information in order to reduce response time or for CoAP-HTTP bidirectional mapping. A CoAP CON or NON requests that go over a Proxy has a Proxy-Uri Option (that is an absolute URI). A Proxy-Uri

Option defines the target server. When Proxy receives a message with this option, it retransmits it to a different Proxy or the end server defined by the Proxy-Uri.

Licenses and libraries
The CoAP is IETF draft protocol that strives to become a standard. There are commercial as well as open source releases of this protocol with libraries in Java, C, and other languages.

5.1.5 M2M overview and design consideration

The BitXML and M2MXML are protocols strictly related to an XML message format. Despite the fact that both of these protocols have extra M2M capabilities, the resources inefficiency that comes with verbose payload is criterion that excludes these formats from the further consideration. The MQTT-s is designed for low-end and battery-operated devices and uses pub/sub model that fits many communication requirements in WSNs, but not in EXALTED architecture. In addition, to our knowledge, there is no available library implementation of this protocol, nor open source or commercial.

Most of the existing M2M protocols are originated from industrial environments or are designed for a specific use case. EXALTED system is rather complex and it is beyond the scope of these individual M2M implementations.

The leveraged EXALTED M2M protocol must be able to support all communication scenarios and to provide reachability and addressability of LTE-M and Non-LTE-M devices and M2M gateways, and to be resource efficient. The constrained LTE-M and Non-LTE-M devices will most likely be connected over the gateway with the rest of the system, to avoid triggering device in a sleep mode. However, the gateway must have permanent connection from one side (i.e. with the M2M Application Server) and asynchronous connectionless state between itself and the end device on the other side. In addition, there is a need for direct communication from the M2M Server to a non-constrained LTE-M devices.

The CoAP supports all these communication scenarios as it is interoperable with HTTP. Therefore, connection between the M2M server and the gateway can be maintained using the HTTP/TCP, followed with a bidirectional translation at the gateway that enables utilization of the CoAP protocol behind the gateway in the capillary network. The CoAP is also payload format agnostic, and provides addressability of the M2M devices/ gateways with a multicast enabler for capillary network.

Considerations for including the CoAP in the EXALTED design are next:

- M2M device behind the M2M gateway - HTTP transport from the server to the M2M gateway, and then HTTP-CoAP translation with Proxy on the M2M gateway itself. For the device to communicate with the server, a bidirectional proxy is required to allow flow of data in both directions.
- For direct communication scenarios CoAP can be utilized E2E.

Table 5-1: Comparison between payload formats over CoAP

Protocol	Session oriented	Network transport	Architecture	Gateway API	Payload format	License/ Status	Libraries	Functionalities
BitXml	Optional	Any	/	Yes	XML	Open source	Java, .NET	Gateway Enabler DNS client
MQTT-s	No	Any	Publish/	Yes	Any	Open	C,C++,C	Gateway

			Subscribe			source	#, Java, Delphi, Erlang, .NET, PHP, Phyton, Ruby…	Enabler
CoAP	No	UDP	Representational State Transfer (REST)	No	Any	Open Source/IETF Draft	C, Java	Multicast, Subscription, Light-weight Reliability
M2MXML	No	Any	/	No	XML	Open source	Java	Multicast, Gateway Enabler

There are also other systems, standards and M2M efforts that are out of the scope of this survey as they represents the complete systems and M2M platforms, including SCADA [64], UPnP [65], DPWS [66], Modbus [68], Telenor Object's [69], Mango [70], NORS [71], Pachube [72], Axeda [73], Sedona [74], etc.

5.2 Evaluation of data formats over CoAP

In preliminary tests CSV and Protobuf payload was evaluated for HTTP protocol. With CoAP proposal as an EXALTED higher layer protocol. The main goal here is to evaluate the data formats and payload encoding over CoAP protocol. Benchmark is written in Java programming language and executed on an Android powered mobile device with 1GHz processor and 512 Mb of RAM. Each data format has different usability (implementation complexity, debug features) and resource consumption (CPU, memory, battery) that can impact deployment. The memory and battery consumption are calculated for message parsing process that is being sent from the server. A large amount of messages are sent (5000 messages) and parsed on the device. This is repeated for 50 times. CoAP californium server was used and modified for this benchmark. The battery and memory and parsing utilization is measured for one repeat of 5000 parsed messages on Android device. The evaluation should influence the choice of payload format utilized in the system for different use cases, with a CoAP as a transport; by providing information of how much resource efficient each format is.

For the subsequent evaluation, next libraries were used:

- XML: SAX parser
- JSON: json-lib-2.4-jdk15 http://sourceforge.net/projects/json-lib/files/
- EXI: EXIficient v0.8 http://exificient.sourceforge.net/
- CSV: Custom file parse (read from an array)
- Protobuf: Protobuf 2.4.1 http://code.google.com/p/protobuf/downloads/list
- CoAP Californium Java https://github.com/mkovatsc/Californium

The evaluation criteria is measurement of resource consumption (i.e. battery and memory) for parsing the messages on device sent from the server. The testing involved parsing of the message for the following data formats:

- CSV (Comma Separated Values)
- XML
- JSON
- EXI
- Protobuf

The Android application sends GET request to a server that responds with a message (file sitting on the server). In order to avoid impact of the I/O operations on the measurements, the messages were buffered before parsing. The messages were at first fetched from a remote server over a wireless network and the Internet, and then parsed and finally corresponding Java objects required by the application was created. The exclude external influence for message transferred over the Internet, 50000 messages was sent for every test, and the final number of repeats was 50 for each test.

The representation of a given XML message in Figure 5.3 was made for each data format.

```
<?xml version="1.0" encoding="UTF-8"?>
  <senml xmlns="urn:ietf:params:xml:ns:senml"
        bn="http://[2001:db8::2]/"
        bt="1320078429"
        ver="1">
    <e n="temperature" u="degC" v="27.2" />
    <e n="humidity" u="%RH" v="80" />
  </senml>
```

Figure 5.3: XML Message used for evaluation.

5.2.1 Data formats, evaluation results and discussion

The Extensible Markup Language (XML) has been used for a long time for payload encoding. It brought the benefits of portability, extensibility, broad support by tools and libraries. Nevertheless, embedded systems rarely have enough memory and processing power to run an XML parser. The XML is not suitable due its verbosity that increases RAM, bandwidth usage and operating costs.

The requirement for message structure acknowledgement of both sender and receiver of the Protobuf messages makes this format hard for implementation and debugging. Protobuf have among all evaluated formats at the best bandwidth, memory, parsing and power consumption results. In the preliminary test [75], a CSV format was better as the evaluation was not performed over CoAP and for batch (array) readings, but for HTTP and regular messages. The message with an array data is used in this case to simulate the environment with multiple data sent over one CoAP message.

JSON was chosen for evaluation as it is widely available and represented format and offers possible message interchange with MessagePack binary libraries [76]. This can be valuable between Application interface (where JSON data format is applicable) and the end device, which can run MessagePack libraries for encoding JSON messages. MessagePack showed even better compression than Protobuf, but reported error for MessagePack encoder prevented us to give further evaluation of this juvenile payload format in time of writing this document.

EXI JAVA library requires a lot of resources for serialization/deserialization compare to other formats. The results of the test can be significantly different for other EXI libraries implementations.

Nevertheless, this evaluation gives a straightforward answer and advises CoAP utilization with a CSV payload, which is resource efficient, needs no additional implementations and provides interoperability between Capillary and LTE-M Network.

Table 5-2: Comparison between payload formats over CoAP.

Data format	Av. parsing time (ms)	Total battery drain (%)	Max memory used	Message size [bytes]
XML	14,9585966	3,72	19161188,84	267
JSON	13,8477374	3,58	19025289,72	188
EXI	35,36446864	9,7	19245712,66	137
CSV	10,7656934	2,96	19079675,82	94
Protobuf	10,2260024	2,72	18898773,54	56

6. Conclusion

EXALTED presents novel MAC protocols suitable for capillary networks, tackling different challenges of M2M communications that can arise in different applications, namely, handling a high number of devices, improving energy-efficiency by exploiting cooperative retransmissions, and combating the funneling problem in multi-hop networks. One of these protocols is a cooperative MAC (DPCF), which is suitable for highly-dense M2M capillary networks and capable of providing sustainable throughput. The protocol is shown to be scalable to the number of contending devices. It is found that by letting devices cooperate with each other when the channel conditions are poor, it is possible to boost the energy-efficiency of the communications, and thus extend the lifetime of the M2M networks (K39). Another MAC protocol uses a hybrid approach to avoid the negative consequences of the bottle-neck around CH nodes. A decision threshold for switching between the CSMA and the TDMA mechanisms is developed. Throughput can be optimized by selecting relatively low values for this switching threshold, especially for cases of high traffic, in order to increase the probability of having contention free access for those devices that are located around the CH. Furthermore, it has been discovered that contention free slots should be mainly assigned to those nodes that are located quite close to the sink, i.e. one or two hops.

Device reachability, addressability, and data connectivity are mutually dependent topics mentioned in this document, and some conclusive remarks are provided. First, heterogeneous connectivity in capillary networks is demonstrated via testing multiple schemes (NFC + ZigBee + GPRS). These technologies have been tested for accessing and communicating M2M end devices. In addition, the constraint of not having IP at this kind of devices is overcome by the introduction of an address translation scheme. Another task is related with IP address assignment for the LTE-M terminals and assignment of the IP addresses to M2M devices behind the M2M Gateway. It is concluded that LTE-M capable terminal or gateway should obtain its IP address from the LTE-M network, and M2M devices behind the gateway can obtain IP addresses from DHCP server located in application domain of EXALTED, or alternatively the DHCP server can be implemented on M2M gateway. IP addresses of the capillary network M2M devices can also be allocated locally. In all these cases, the M2M gateway is supposed to perform the maintenance of address translation mapping tables since IP addresses in capillary networks are not visible from the LTE-M core network point of view.

The document also outlines the issue of mobility management, which is a cross-layer topic. A solution to support mobility in a system involves modification and adaptation of individual algorithms at each layer of the protocol stack such that they each intrinsically deal with mobility. Nevertheless this is complex and resource demanding. A better solution is to design procedures that support mobility of devices and to provide inputs about mobility to all algorithms and procedures of the protocol stack that actually require it. To this end, an algorithm is derived to select among a set of mobility models; the one that best fits the current movement of entities. This algorithm is finally transformed into a channel access method that adapts the parameters of the contention phase to the local density of nodes so as to ensure low latency, low energy consumption and successful transmissions.

Finally, payload reduction for supporting MAC efficiency is another topic addressed in the document. Evaluation of payload encoding and different payload methods over light-weight CoAP transport for resource utilization has been completed. The performances of five different payloads that offer interoperability between device domain and LTE network domain have been evaluated in live network conditions for their battery, memory, parsing, and bandwidth consumption levels sent from CoAP server.

ANNEX: List of EXALTED KPIs

This Annex introduces a preliminary list of performance indicators used for the evaluation of the different EXALTED solutions. It aims at collecting the various KPIs for the sake of completeness, giving a short description and the aim towards a specific EXALTED objective.

KPIs		EXALTED objective
Generally valid	**(K1) BER**: Bit error rate at the output of the decoder. **(K2) Packet Error Rate (PER)**: A packet represents the information block protected by CRC at the MAC layer. **(K3) Packet Loss Rate (PLR)**: As PER, but it only counts erroneous packets due to excessive latency. **(K4) Frame Error Rate (FER)**: A frame represents the information block protected by CRC at the RLC layer. **(K5) Outage probability**: probability of being excluded from the network either for battery or route reconfiguration.	General evaluation not limited to certain objective
Evaluation of TX signal processing	**(K6) Peak-to-Average Power Ratio (PAPR):** Ratio of peak power and average power of the transmitted signal in the time domain. **(K7) Out-of-band radiation (OOB)**: ratio of power within given spectral mask to power out of spectral mask	Complexity reduction Improved resource management Energy efficiency
Evaluation of retransmissions schemes (ARQ, HARQ)	**(K8) Average number of retransmissions**: In case of erroneous transmissions, ARQ and HARQ mechanisms are used to retransmit packets until they are successfully received. **(K9) Reliability**: Average Number of Retransmissions.	Energy efficiency Signaling overhead reduction
Evaluation of transmission schemes with feedback	**(K10) Feedback bandwidth**: Required feedback data rate in bit/s.	
Evaluation of broadcast/multicast services	**(K11) Redundancy overhead** spent per user for reliable multicast message reception.	Energy efficiency

Evaluation of achievable data rates and spectral efficiency	**(K12) Throughput**: number of successfully received bits or messages per time unit in bit/s or messages/s. **(K13) Average packet call throughput** defined as $R_{pktcall}(i) = \frac{\sum_k good\ bits\ in\ packet\ call\ k\ of\ user\ i}{\sum_k t_{end\_k} - t_{arrival\_k}}$ w here k denotes the k[th] packet call from a group of K packet calls where the K packet calls can be for a given user i , $t_{arrival\_k}$ is the first packet of packet call k arrives in queue, and t_{end_k} is the last packet of packet call k is received by the UE. **(K14) Spectral efficiency (sum-rate)**: Number of successfully transmitted bits per time unit per frequency unit per cell in bit/s/Hz/cell.	Energy efficiency Signaling overhead reduction Improved resource management
Evaluation of achievable delays	**(K15) Average packet delay per sector**: The averaged packet delay per sector is defined as the ratio of the accumulated delay for all packets for all devices received by the sector and the total number of packets. The delay for an individual packet is defined as the time between when the packet enters the queue at transmitter and the time when the packet is received successively by the device. **(K16) E2E Delay/jitter**: Round trip time. **(K17) Access delay**: Needed time in order to join the network. **(K18) Bandwidth delay product**: Total available bandwidth * round trip time. Used for estimating the minimum buffer length needed in order to assure non-lossy transmission (it defines the maximum amount of data to be transmitted before receiving ACK or NACK confirmations). **(K19) Addressing translation delay**: Delay introduced by the needed processing time in order to map from IP to IEEE addresses. **(K20) Number of addresses mapped**: Maximum number of addresses supported when mapping IP addresses to non-IP ones on the M2M Gateway. **(K21) Handover delay**: Amount of time needed to leave a network and join another one. **(K22) Percentage of satisfied users**: The percentage of users whose packets arrive at the destination within their maximum delay tolerance time interval	Complexity reduction Energy efficiency Heterogeneous network access management
Evaluation of number of supported users	**(K23) User per cell capacity**: Maximal number of simultaneously active users per cell. **(K24) CDF of number of served multicast users**.	Signaling overhead reduction Improved resource management

Evaluation of coverage and range	**(K25) Range**: Maximal possible distance between a M2M device and base station to enable communication with a given QoS, either directly or via a gateway or relay. **(K26) Coverage**: Percentage of area, where M2M devices can connect to a base station, either directly or via a gateway or relay.	Het. network access management Mobility management
Particular evaluation of signalling overhead	**(K27) PHY Control channel and pilot overhead**: Percentage of radio resources utilized for signalling, control channels and pilots on PHY layer. **(K28) Paging efficiency**: Percentage of specific control channel information for paging procedures in bit/user. **(K29) Mobility management efficiency**: Percentage of specific control channel information for mobility procedures in bit/user. **(K30) Transmission Payload Size**: Size of the message exchange between 2 peers (e.g. device, cluster head, gateway, device management server). The size depends on the data encoding scheme, compression. **(K31) Payload Encoding**: Specify how device attributes, data are encoded and presented in the payload. **(K32) Actual Payload Size**: Size of the received message after decoding or decompression.	Mobility management Signalling overhead reduction Complexity,cost reduction
Particular evaluation of energy efficiency	**(K33) Mean power per signalling bit per user:** watt/bit. Specifies how many power (energy) is saved with signaling reduction procedures per signaling bit per user. **(K34) Ratio between transmitted power and achieved throughput (energy efficiency)**: watt/(bit/s)=joules/bit **(K35) Consumed energy per message**: Sum of energy spent for signal processing and transmitted energy required for one message. **(K36) Standard Deviation of node energy levels**: This is an indicator of the variety of residual energy levels of nodes. We monitor this indicator to see how much energy equalization is achieved over time. **(K37) Average node energy levels**: This is an indicator that is used to monitor the network's overall energy consumption over time. **(K38) Coefficient of variation**: the ratio of (Standard Deviation of node energy levels/ Average node energy levels). **(K39) Network lifetime**: The time period until the first node depletes its battery energy.	Signaling overhead reduction Complexity reduction
Particular evaluation of complexity	**(K40) Complexity of encoding and decoding**, i.e. number of required multiplications. **(K41) Distortion**: Distortion is the performance metric used to measure how close an estimate is to its	Improved resource management

	actual value. Typically, the distortion is measured by the Mean Squared Error (MSE). **(K42) Number of CSI estimation:** the number of channel state information (CSI) estimation per decoded data bit. **(K43) Number of active antennas**: number of activated antennas compared to the available ones	
Evaluation of Radio resource management	**(K44) Radio resource consumption**: autodiagnostic aims at reducing the amount of data exchanged between the remote device management server and the device moving one source of data transaction from the server side to the device side. **(K45) System resource consumption**: moving diagnostic to the device side introduces a new set of work in the device which means the system will run longer in order to perform the autodiagnostic task. Energy wise, this is a cost and it should be minimized.	Benefits of autodiagnostic compared to a standard diagmon
Evaluation of Security	**(K46) Computational energy consumption :** This is the computational energy required to insure privacy, confidentiality and integrity of the data transmitted. It is related to the computational complexity of the algorithms involved **(K47) Radio energy consumption:** the radio energy required to insure privacy, confidentiality and integrity of the data transmitted. It is related to the data overhead required by the security process. **(K48) Infrastructure energy consumption:** This is the energy consumption required by the overall security layers adding up. It can be reduced by collapsing when possible different security layers into one**.** **(K49) Flexibility of the security enrolment process for capillary devices:** this indicator takes several parameters into account to reflect the overall flexibility of the security enrolment process for capillary devices **(K50) Total cost per user of the security solution:** This indicator(s) take(s) in to account the overall cost of the deployment of a security solution and (per client+infrastructure costs) and reflects it per user.	
Network Monitoring	**(K51) Query size:** Size of a query message exchange between two M2M elements (e.g. M2M device, cluster head, gateway, eNodeB, and network monitoring server). **Objective:** Shall be as small as possible. **Benefits**: Requires minimal memory, processing time and reduce transmission time (impacts: lower device cost, less energy consumption). **(K52) Passive monitoring:** Human manager submit the queries and perform analysis and management tasks). **Objective:** Monitoring should not be limited to passive monitoring and not depends on human intervention. **Benefits**: Passive monitoring	Device / node monitoring mechanism to ensure that a response-to-demand datum is authentic reliable and secure

	introduces less overhead, minimal impact of memory and network traffic. **(K53) Centralized / hierarchical monitoring:** Centralized-processing approach requires continues polling of network health data from managed each sensor node in the network to the sink. **Objective:** Hierarchical monitoring (tasks are distributed among network managers, each manager reports to a higher level manager). **Benefits**: Centralized monitoring increases high data overhead, and this limits its scalability. Since individual node information is important, aggregation solutions may not be applicable. In addition, in case of network partitioning, the nodes that are unable to reach the central sink are left without any management functionality. Local management tasks can be done at a lower level that reduces communication costs. Meanwhile global view of the network can still be available by reporting lower-level managers to higher level sink which can enable sink to make network-wide management control decisions. **(K54) Frequency of queries:** How often the queries need to be disseminated. **Objective:** For better energy-efficiency should be less frequent as possible. For more accuracy should be more frequent.	

List of Acronyms

Acronym	Meaning
3G	Third Generation
3GPP	3rd Generation Partnership Project
ACK	Acknowledge
ADC	Analog to digital converter
AMR	Automated Metering Reading
API	Application Programming Interface
APN	Access Point Name
ARM	Advanced RISC Machine
ARQ	Automatic Retransmission Request
C-ARQ	Cooperative Automatic Retransmission Request
CAN	Controlled Area Network
CDMA	Code division multiple access
CE	Cluster End
CFP	Contention-Free Period
CH	Non-LTE-M Cluster Head
COPD	Chronic Obstructive Pulmonary Disease
CoAP	Constrained Application Protocol
CP	Contention Period
CTS	Clear to Send
CSMA	Carrier Sensing Multiple Access
CVD	Cardiovascular Diseases
DAC	Digital to Analog Converter
DCF	Distributed Coordination Function
DD	M2M Device Domain
DHCP	Dynamic Host Configuration Protocol
DI	Device Identifier
DM	Device Management
DMT2	Diabetes Mellitus Type 2
DPCF	Distributed Point Coordination Function
DSL	Digital Subscriber Line
DSO	Distribution System Operator
DQCA	Distributed Queuing Collision Avoidance
DQMAN	Distributed Queuing for Mobile Ad Hoc Networks
E2E	End to end
ECG	Electrocardiogram
eNodeB	evolved NodeB
EPS	Evolved Packet System
ETSI	European Telecommunications Standards Institute
EXALTED	Expanding LTE for Devices Project
GFDM	Generalized Frequency Division Multiplexing
GPIO	General Purpose In/Out
GPRS	General packet radio service
GPS	Global Positioning System
GSM	Global System for Mobile
GUI	Graphical User Interface
GW	M2M Gateway
HDP	Health Device Profile
HLR	Home Location Register
HPLMN	Home Public Land Mobile Network

HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
HW	Hardware
I/O	In/Out
I2C	Inter-Integrated Circuit
ICCID	International Circuit Card ID
IF	Intermediate Frequency
IG	Intelligent Gateway
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
IR	Internal Report
ITS	Intelligent Transportation System
ITU	International Telecommunication Union
JTAG	Joint Test Action Group
KPI	Key Performance Indicator
LAN	Local Area Network
LC	Number of Link Changes
LD	Link Duration
LTE	Long Term Evolution
LTE-A	Long Term Evolution Advanced
LTE-M	Long Term Evolution Network with M2M enhancements
LTE-X	LTE, LTE-A, or LTE-M
M2M	Machine to Machine
MAC	Media Access Control
MCAP	MultiChannel Adaptation Protocol
MedWG	Medical Working Group
MIMO	Multiple-Input, Multiple Output
MISO	Multiple-Input, Single Output
MM	Mobility Model
MSISDN	Mobile Station Integrated Services Digital Network
MT	Mobile Terminal
MTC	Machine type communication
MTO	Master Time-Out
NAT	Network Address Translation
ND	M2M Network Domain
NFC	Near Field Communication
OBU	On Board Unit
OEM	Original Equipment Manufacturer
OFDMA	Orthogonal Frequency-Division Multiple Access
OS	Operating System
P/BAN	Personal/Body Area Network
PA	Path Availability
PC	Personal Computer
PDN	Packet Data Network
PCF	Point Coordination Function
PHY	Physical Layer
PoC	Proof of Concept
RD	Relative Direction
RF	Radio Frequency
RFID	RF Identification
RIA	Rich Internet Application
RRM	Resource Radio Management

RTS	Request to Send
SC-FDMA	Single Carrier Frequency Division Multiple Access
SDIO	Secure Digital I/O
SDRAM	Secure Digital Random Access Memory
SIG	Special Interest Group
SIM	Subscriber Identity Module
SIMO	Single-Input, Multiple Output
SISO	Single-Input, Single Output
SMM	Smart Metering and Monitoring
SMS	Short Message Service
SPI	Serial Peripheral Interface
SR	Speed Ratio
SW	Software
TBD	To Be Determined
TDMA	Time Division Multiple Access
TCP	Transmission Control Protocol
TMSI	Temporary Mobile Subscriber Identity
UART	Universal Asynchronous Receiver-Transmitter
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
URI	Uniform Addressed Identifier
USB	Universal Serial Bus
TDMA	Time Division Multiple Access
TE	Terminal Equipment
VPLMN	Visited Public Land Mobile Network
WCDMA	Wideband Code Division Multiple Access
WP	Work Package
WWRF	Wireless World Research Forum
XML	Extensible Markup Language

References

[1] FP7 EXALTED: “D2.1 – Description of baseline reference systems, scenarios, technical requirements & evaluation methodology,” project report, May 2011.
[2] FP7 EXALTED "D2.3 - The EXALTED system architecture", project deliverable, August 2012
[3] FP7 EXALTED "D2.4 - The EXALTED system concept and its performance", project deliverable, February 2013
[4] IEEE, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. 802.11 – 2007.
[5] IEEE, "Std 802.15.4-2006: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)," 2006.
[6] S. Tozlu, “Feasibility of Wifi-Enabled Sensors for Internet of Things,” in proc. of the IEEE IWCMC, July 2011.
[7] G. Bianchi, L. Fratta, and M. Oliveri, “Performance Evaluation and Enhancement of the CSMA/CA MAC protocol for 802.11 Wireless LAN’s,” in Proc. of the IEEE PIMRC 1996, Taipei, Taiwan, pp. 392 – 296, Oct. 1996.
[8] J. Weinmiller, M. Schläger, A. Festag, and A. Wolisz, “Performance Study of Access Control in Wireless LANs-IEEE 802.11 DFWMAC and ETSI RES 10 HIPERLAN,” Mobile Networks Appl., vol. 2, pp. 55 – 67, 1997.
[9] F. Cali, M. Conti, and E. Gregori, “Dynamic Tuning of the IEEE 802.11 Protocol to Achieve a Theoretical Throughput Limit,” IEEE/ACM Transactions on Networking, vol. 8, no. 6, pp. 785 – 799, Dec. 2006.
[10] S. Agarwal, S. Krishnamurthy, R. H. Katz, and S. D. Kao, “Distributed power control in ad hoc wireless networks,” in Proc. of the IEEE PIMRC, 2001.
[11] E. S. Jung and N. H. Vaydia, “A Power Control MAC protocol for ad hoc networks,” in Proc. of the ACM Mobicom, Atlanta, GA, pp. 36– 47, Sep. 2002.
[12] Z. Tang and J. J. Garcia-Luna-Aceves, “A protocol for topology-dependant transmission scheduling in wireless networks,” in Proc. of the IEEE WCNC, vol. 3, New Orleans, LA, pp. 1333 – 1337, Sep. 1999.
[13] S. Toumpis and A. Goldsmith, “Performance, optimization, and cross-layer design of media access control protocols for wireless ad hoc networks,” in Proc. of the IEEE ICC, Anchorage, AK, pp. 2234 – 2240, May 2003.
[14] D. J. Goodman, R. A. Valenzuela, K. T. Gayliard, and B. Ramamurthi, “Packet Reservation Multiple Access for Local Wireless Networks,” IEEE Trans. on Communications, vol. 37, no. 8, Aug. 1989.
[15] Chlamtac, A. Faragó, A. D. Myers, V. R. Syrotiuk, and G. V. Záruba, “ADAPT: A dynamically self-adjusting media access control protocol for ad hoc networks,” in Proc. of the GLOBECOM, pp. 11 – 15, Dec. 1999.
[16] Rhee, M. Warrier, and J. Min, “ZMAC: A hybrid MAC for wireless sensor networks,” in Proc. of Sensys 2005, San Diego, California.
[17] M. Shakir, I. Ahmed, P. Mugen, and W. Wang, “Cluster Organization based Design of Hybrid MAC Protocol in Wireless Sensor Networks”, in Proc. of the Third International Conference on Networking and Services, pp. 78 – 83, Jun. 2007.
[18] Muir and J. J. Garcia-Luna-Aceves, “An efficient packet sensing MAC protocol for wireless networks,” Springer Mobile Networks and Applications, vol.3, no. 2, pp. 221–234, Aug. 1998.
[19] Kanjanavapastit and B. Landfeldt, “A performance investigation of the modified PCF under hidden device problem,” in Proc. of the ICCCAS 2004, vol. 1, pp.428 – 432, Jun. 2004.
[20] Anjum, S. Mushtaq, A. Hussain, “Multiple Poll Scheme for Improved QoS Using IEEE 802.11 PCF,” in Proc. of the IEEE INMIC’05, pp.1 – 6, Dec. 2005.

[21] Ping, J. Holliday, A. Celik, “Dynamic scheduling of PCF traffic in an unstable wireless LAN,” in proc. of the CCNC. 2005, pp. 445 – 450, Jan 2005.
[22] K. Byung-Seo, K. Sung Won, W. Yuguang Fang, “Two-step multipolling MAC protocol for wireless LANs, ” IEEE Journal on Selected Areas in Communications, vol. 23, no. 6, pp. 1276 – 1286, Jun. 2005.
[23] K. Young-Jae and S. Young-Joo, “Adaptive polling MAC schemes for IEEE 802.11 wireless LANs,” in Proc. of the VTC 2003, vol. 4, pp. 2528 – 2532, Apr. 2003.
[24] Kanjanavapastit and B. Landfeldt “An analysis of a modified point coordination function in IEEE 802.11,” in Proc. of the IEEE PIMRC’03, vol. 2, pp. 1732 – 1736, 2003.
[25] Y. Tiantong, H. Hassanein, H. T. Mouftah, “Infrastructure-based MAC in wireless mobile ad-hoc networks,” in Proc. of the 27th Annual IEEE Conference on Local Computer Networks, pp. 821 – 830, 2002.
[26] Crespo, J. Alonso-Zárate, L. Alonso, and Ch. Verikoukis, “Distributed Point Coordination Function for Wireless Ad hoc Networks,” in proc. of the VTC Spring 2009, Barcelona, SPAIN.
[27] J. Alonso-Zárate, E. Kartsakli, L. Alonso, and Ch. Verikoukis, "Performance Analysis of a Cluster-Based MAC Protocol for Wireless Ad Hoc Networks," EURASIP Journal on Wireless Communications and Networking, Special Issue on Theoretical and Algorithmic Foundations of Wireless Ad Hoc and Sensor Networks, vol. 2010, Article ID 625619, 16 pages, March 2010.
[28] J. Alonso-Zárate, E. Kartsakli, A. Cateura, C. Verikoukis, and L. Alonso, "A Near-Optimum Cross-Layered Distributed Queuing Protocol for Wireless LAN," IEEE Wireless Communication Magazine, Special Issue on MAC protocols for WLAN, vol. 15, no. 1, pp. 48-55, February 2008.
[29] The MAC Simulator for Wireless Networks (MACSWIN). Available online at: http://wikienergy.cttc.es/index.php/MACSWIN.
[30] M. Dianati, Xinhua Ling, K. Naik, and Xuemin Shen, "A node-cooperative ARQ scheme for wireless ad hoc networks," IEEE Transactions on Vehicular Technology, vol. 55, no. 3, pp. 1032-1044, 2006.
[31] Pei Liu, Zhifeng Tao, and S. Panwar, "A cooperative MAC protocol for wireless local area networks," in IEEE International Conference on Communications, 2005.
[32] Hao Zhu and Guohong Cao, "rDCF: A Relay-Enabled Medium Access Control Protocol for Wireless Ad Hoc Networks," IEEE Transactions on Mobile Computing, vol. 5, no. 9, pp. 1201 -1214, 2006.
[33] J. Alonso-Zarate, L. Alonso, and C. Verikoukis, "Performance analysis of a persistent relay carrier sensing multiple access protocol," IEEE Transactions on Wireless Communications, vol. 8, no. 12, pp. 5827 -5831, 2009.
[34] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," IEEE Journal on Selected Areas in Communications, vol. 18, no. 3, pp. 535 -547, 2000.
[35] P. Serrano, A. Garcia-Saavedra, M. Hollick, and A. Banchs, "On the energy efficiency of IEEE 802.11 WLANs," in European Wireless Conference (EW), 2010.
[36] J. Yin, Xiaodong Wang, and D.P. Agrawal, "Energy efficiency evaluation of wireless LAN over bursty error channel," in IEEE Global Telecommunications Conference, 2005.
[37] M. Ergen and P. Varaiya, "Decomposition of Energy Consumption in IEEE 802.11," in IEEE International Conference on Communications, 2007.
[38] J. Alonso-Zarate et al., "Energy-Efficiency Evaluation of a Medium Access Control Protocol for Cooperative ARQ," in IEEE International Conference on Communications, 2011.
[39] A. Ben Nacef, S.-M. Senouci, Y. Ghamri-Doudane, and A.-L. Beylot, "A Cooperative Low Power MAC Protocol for Wireless Sensor Networks," in IEEE International Conference on Communications, 2011.
[40] M. Zorzi and R.R. Rao, "Energy constrained error control for wireless channels," in IEEE Global Telecommunications Conference, 1997.

[41] L.M. Feeney and M. Nilsson, "Investigating the energy consumption of a wireless network interface in an ad hoc networking environment," in IEEE International Conference on Computer Communications, 2001.
[42] Andrea Goldsmith, Wireless Communications., 2005.
[43] M. Zuniga and B. Krishnamachari, "Analyzing the transitional region in low power wireless links," in IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004.
[44] Marvin K. Simon Alouini and Mohamed-Slim, Digital Communication over Fading Channels.: Wiley, 2005.
[45] R.M. Radaydeh and M.M. Matalgah, "Results for Infinite Integrals Involving Higher-Order Powers of the Gaussian Q-Function with Application to Average SEP Analysis of D-QPSK," IEEE Transactions on Wireless Communications, vol. 7, no. 3, pp. 793-798, 2008.
[46] P. Mary, M. Dohler, J.-M. Gorce, G. Villemaud, and M. Arndt, "M-ary symbol error outage over Nakagami-m fading channels in shadowing environments," IEEE Transactions on Communications, vol. 57, no. 10, pp. 2876-2879, 2009.
[47] Trung-Kien Nguyen et al., "A Low-Power RF Direct-Conversion Receiver/Transmitter for 2.4-GHz-Band IEEE 802.15.4 Standard in 0.18-micro CMOS Technology," IEEE Transactions on Microwave Theory and Techniques, vol. 54, no. 12, pp. 4062 -4071, 2006.
[48] http://www.ti.com/lit/ds/symlink/cc2430.pdf. (2011) CC2430 datasheet.
[49] T. Predojev, J. Alonso-Zarate, Alonso L., and Verikoukis C., "Energy Efficiency Analysis of a Cooperative Scheme for Wireless Local Area Networks," in submitted to Globecom, 2012.
[50] T. Predojev, J. Alonso-Zarate, and M. Dohler, "Energy Efficiency of Cooperative ARQ Strategies in Low Power Networks," in INFOCOM Workshop on Green Networking and Smart Grids, 2012.
[51] I. Rhee, A. Warrier, M. Aia, and J. Min, “ZMAC: a hybrid MAC for wireless sensor networks,” in In Proc. of 3rd ACM Conference on Embedded Networked Sensor Systems (SenSys 2005), Nov. 2005.
[52] G.-S. Ahn, E. Miluzzo, A.T. Campbell, S.G. Hong, F. Cuomo, Funneling-Mac: A Localized, Sink-Oriented Mac For Boosting Fidelity In Sensor Networks, In: Proc. 4th Acm Conference On Embedded Networked Sensor Systems, Sensys, Boulder, Co, Usa, Nov. 2006.
[53] A. Ouni, H. Rivano And F. Valois, “Joint TDMA/CSMA Scheduling For Solving The Bottleneck Issue in Wireless Mesh Networks, Technical Report, Institut National de Recherche en Informatique et en Automatique
[54] M. H. S. Gilani, I. Sarrafi, And M. Abbaspour, “An Adaptive CSMA/TDMA Hybrid Mac For Energy And Throughput Improvement Of Wireless Sensor Networks,” Elsevier Ad Hoc Networks, Doi:10.1016/J.Adhoc.2011.01.005, Pp. 1-8, Available Online: Jan. 11th, 2011.
[55] IEEE Standard 802.15.4, Part 15.4: Wireless Medium Access Control And Physical Layer Specification For Low Rate Wireless Personal Area Networks. IEEE Std. 802.15.4, 2006
[56] FP7 EXALTED: “D4.2 - IP Networking System for M2M communications for EXALTED use cases”, project deliverable, June 2012.
[57] A. Raja and X. Su, “Mobility handling in MAC for wireless ad hoc networks,” Wireless Communications and Mobile Computing, Wiley Online Library, vol. 9, no. 3, pp. 303-311, 2009.
[58] M. Ali, T. Voigt and Z.A. Uzmi, “Mobility management in sensor networks,” MSWSN / DCOSS, pp. 131-140, 2006.
[59] T. Camp, J. Boleng and V. Davis, “A survey of mobility models for ad hoc network research,” Wireless Communication and Mobile Computing, Wiley Online Library, vol. 2, no. 5, pp. 483-502, 2002.

[60] G. Lu, G. Manson and D. Belis, “Mobility modeling in mobile ad hoc networks with environment-aware,” Journal of Networks, vol. 1, no. 1, pp. 54-63, 2006.
[61] A. Jardosh, E.M Belding-Royer, K.C. Almeroth and S. Suri, “Towards realistic mobility models for mobile ad hoc networks,” in Proc. Of Mobile Computing and Networking, 2003.
[62] F. Bai, A. Helmy, "A Survey of Mobility Modeling and Analysis in Wireless Adhoc Networks," Book Chapter in the book "Wireless Ad Hoc and Sensor Networks", Springer, October 2006, ISBN: 978-0-387-25483-8.
[63] B. Liang, Z. J. Haas, "Predictive Distance-Based Mobility Management for PCS Networks," in Proc. of IEEE INFOCOM 1999, Apr. 1999.
[64] F. Bai, N. Sadagopan, B. Krishnamachari, A. Helmy, "Modeling path duration distributions in MANETs and their impact on reactive routing protocols," IEEE Journal Selected Areas in Communications, vol. 22, no. 7, Sept. 2004, pp. 1357-1373.
[65] N. Sadagopan, F. Bai, B. Krishnamachari, A. Helmy, "PATHS: analysis of PATH duration statistics and their impact on reactive MANET routing protocols," Proc. of the 4th ACM Int. Symp. on Mobile ad hoc networking & computing, 2003, pp. 245-256.
[66] F. Bai, N. Sadagopan and A. Helmy, "The IMPORTANT framework for analyzing the Impact of Mobility on Performance Of RouTing protocols for Adhoc NeTworks", Elsevier, Ad Hoc Networks, vol. 1, no. 4, Nov. 2003, pp. 383-403.
[67] G. Corbellini, E. Calvanese-Strinati, E. Ben Hamida, A. Duda, “DA-MAC: Density Aware MAC for Dynamic Wireless Sensor Networks,” IEEE PIMRC’11, Toronto, Sept. 2011.
[68] BiTXml M2M Communication Protocol V2.0.1 Protocol Specification , http://www.bitxml.org/doc/BITXml_protocol_EN_2.0.1.pdf
[69] Andy Stanford-Clark and Hong Linh Truong, “MQTT For Sensor Networks (MQTT-S) Protocol Specification”, http://mqtt.org/MQTT-S_spec_v1.2.pdf
[70] http://m2mxml.sourceforge.net/v1.1/M2MXML_Spec.html
[71] Constrained Application Protocol (CoAP) draft-ietf-core-coap-07 http://tools.ietf.org/html/draft-ietf-core-coap-07
[72] M2MXML Open Source Project, http://m2mxml.sourceforge.net
[73] Urs Hunkeler, Hong Linh Truong, Urs Hunkeler, Hong Linh Truong, “MQTT-S – A Publish/Subscribe Protocol For Wireless Sensor Networks”, 2nd Workshop on Information Assurance for Middleware Communications "IAMCOM'08," Bangalore, India, January 2008 Availabe online: http://www.zurich.ibm.com/pdf/sys/adv_messaging/mqtts_iamcom08.
[74] Supervisory Control and Data Acquisition (SCADA) Systems, Techical Information Bulletin 04-1, National Communication Systems, 2004
[75] UPnP Forum, http://www.upnp.org/
[76] Devices Profile for Web Services (DPWS) v1.1, OASIS Standard, 2009. http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01
[77] http://www.modbus.org/specs.php
[78] Telenor Objects, http://www.telenorobjects.com
[79] Mango Open Source M2M, http://mango.serotoninsoftware.com/
[80] Dirk Trossen, Dana Pavel, NORS: An Open Source Platform to Facilitate Participatory Sensing with Mobile Phones, Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking&Services (MobiQuitous), 2007
[81] Pachube, a realtime data brokerage platform for the Internet of Things, https://pachube.com/docs/
[82] Axeda Developer Connection, Product documentation http://developer.axeda.com/learn/by-type/product-documentation
[83] Sedona Framework, http://www.sedonadev.org/doc/index.html
[84] MessagePack, Extremely efficient object serialization library for cross-language communication. http://msgpack.org/
[85] FP7 EXALTED “D3.2 - Study of commonalities and synergies between LTE-A and the heterogeneous network (WP4)”, project deliverable, February 2012

[86] 3rd Generation Partnership Project, “General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 10)”, section 5.3.1 “IP address allocation”, 3GPP TS 23.401, V10.4.0 (2011-06), Technical Specification, June 2011. Accessed on July 21st, 2011, at http://www.3gpp.org/ftp/Specs/archive/23_series/23.401/23401-a40.zip