EMMON - EMbedded MOnitoring

Artemis JU – FP7

D4.1 PROBLEMS TO ADDRESS

STUDY OF COLLECTED, ANALYSED AND CLASSIFIED PROBLEMS TO ADDRESS IN THIS PROJECT

EMMON

Agreement Ref.: *100036*

DISCLAIMER
Artemis JU Contract Report
The work described in this report was performed under Artemis JU contract. Responsibility for the contents resides in the author or organization that prepared it.

Date:	*2009-05-27*
Pages:	*31*
Status:	*Approved*
Dissemination Level:	*PU*
Reference:	*FP7-JU-EMMON-2009-WP4-001-D4.1*
Version:	*1*

Customer:

ARTEMIS

SEVENTH FRAMEWORK PROGRAMME

STUDY OF COLLECTED, ANALYSED AND CLASSIFIED PROBLEMS TO ADDRESS IN THIS PROJECT

EMMON

Authors and Contributors				
Name	**Contact**	**Organization**	**Description**	**Date**
Mário Alves	mjf@isep.ipp.pt	ISEP	Author	2009-04-28
Paulo Gandra Sousa	pag@isep.ipp.pt	ISEP	Co-author	2009-04-28
Mélanie Bouroche	Melanie.Bouroche@cs.tcd.ie	TCD	Co-author	2009-04-28
Pedro Braga	plbraga@criticalsoftware.com	CSW	Co-author	2009-04-28
Rui Mónica	rs-monica@criticalsoftware.com	CSW	Co-author	2009-04-28
Gabriella Carrozza	gcarrozza@sesm.it	SESM	Co-author	2009-04-28
Shashi Prabh	ksph@isep.ipp.pt	ISEP	Contributor	2009-05-10
Ricardo Gomes	rftg@isep.ipp.pt	ISEP	Contributor	2009-05-20

Dissemination Level
Public
The contents of this document are under copyright of Artemis JU. it is released on condition that it shall not be copied in whole, in part or otherwise reproduced (whether by photographic, or any other method) and the contents therefore shall not be divulged to any person other than that of the addressee (save to other authorized offices of his organization having need to know such contents, for the purpose for which disclosure is made) without prior written consent of submitting company.

Revision History				
Version	**Revision**	**Date**	**Description**	**Author**
1	1	2009-05-19	Final Draft for internal review	Mário Alves, Paulo Gandra de Sousa, Mélanie Bouroche, Pedro Braga, Rui Mónica, Gabriella Carrozza
1	-	2009-05-26	Final Draft with rework	Mário Alves, Paulo Gandra de Sousa, Mélanie Bouroche, Pedro Braga, Rui Mónica, Gabriella Carrozza
1	2	2009-05-27	For Approval	Mário Alves, Paulo Gandra de Sousa, Mélanie Bouroche, Pedro Braga, Rui Mónica, Gabriella Carrozza
2	5	2010-06-04	Approved version according to the results of the Technical Review Report, ref: ARTEMIS-ED-21-09, of	Mário Alves, Paulo Gandra de Sousa,

Revision History				
Version	**Revision**	**Date**	**Description**	**Author**
			2010-06-04.	Mélanie Bouroche, Pedro Braga, Rui Mónica, Gabriella Carrozza
2	6	2010-08-15	Approved version according to the results of the Technical Review Report, ref: ARTEMIS-ED-21-09, of 2010-06-04. Checked according to documentation convention	Mário Alves, Paulo Gandra de Sousa, Mélanie Bouroche, Pedro Braga, Rui Mónica, Gabriella Carrozza

Change Traceability:			
Paragraph or Requirements Number	**Paragraph or Requirements Number**	**Description & Comments**	**Reference**
Version 01	**Version 02**		

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1. Introduction

1.1 Objective

The objective of this deliverable is to identify the main problems that must be addressed in the EMMON project in what concerns the engineering of Large-Scale Wireless Sensor Networks (LS-WSNs) for embedded monitoring applications. The inherent characteristics of these networks such as huge amount of nodes, large geographical region, harsh environments, processing, memory, energy, radio coverage and bit rate limitations are complex impairments to fulfil requirements such as long network lifetime (node/network energy-sustainability), timeliness (and in some cases real-time communications) and reliability (eventually supporting some redundancy and fault-tolerance mechanisms).

The main challenge is how to engineer large-scale wireless sensor network applications while coping with application/user requirements such as network performance, reliability, security, system lifetime and cost-effectiveness.

1.2 Scope

This deliverable is included in WP4 (“Research on Protocols and Communication Systems”) list of deliverables and associated with T4.1 (“Research on large-scale wireless sensor networks”). In this context, it focuses on problems and challenges related to the EMMON network architecture, particularly for LS-WSNs, where a large number of sensing devices (e.g. >1000) are deployed in a wide geographical region (e.g. > 1 hectare).

T4.1 will work towards the analysis and proposal of solutions for the problems identified in this deliverable (D4.1). The strengths and weaknesses of using existing technologies vs. new proposals will be identified and this will drive the direction of this work package. This analysis will result in “D4.2: evaluation report: evaluation of possible solutions, concepts for new communication methods”, due at T_0+12. This task’s documentation package will also include “D4.3: simulation results of selected new communication methods” (due at T_0+24).

1.3 Audience

- JU and the Commission Services
- WSN research groups
- Consortium participants

1.4 Definitions and Acronyms

Table 1 presents the list of acronyms used throughout the present document.

Acronyms	Description
AD	Applicable Document

Acronyms	Description
CEA	Cost-Effectiveness Analysis
CRC/FCS	Cyclic Redundancy Code/Frame Check Sequence
DSP	Digital Signal Processor
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
LS-WSN	Large-Scale Wireless Sensor Network
MAC	Medium Access Control
MIB	Management Information Base
NFP	Non-Functional Property
PKC	Public-key cryptography
QoS	Quality-of-Service
RD	Reference Document
SOTA	State of the Art
TBC	To Be Confirmed
TBD	To Be Defined
TDMA	Time Division Multiple Access
UTC	Coordinated Universal Time / Temps Universel Coordonné
UWB	Ultra Wide Band
WSN	Wireless Sensor Network

Table 1 - Table of acronyms

1.5 Document Structure

Section 1, Introduction, presents a general description of the contents, pointing its goals, intended audience and structure. Section 2, Documents, presents the documents applicable to this document and referenced by this document, while Section 3 presents an overview of EMMON project and also of Work Package 4 (communication system and protocols).

Section 4 aims at identifying the most relevant properties of WSNs in what concerns the communication system and protocols, within EMMON. These are classified as "non-functional properties", "algorithms" and "network planning and management". For each of these subjects, Section 5 highlights the most relevant problems to be addressed in EMMON, particularly in what is more related to WP4.

Finally, Section 6 provides some general conclusions.

2. Documents

This section presents the list of applicable and reference documents as well as the documentation hierarchy this document is part of.

2.1 Applicable Documents

This section presents the list of documents that are applicable to the present document. A document is considered applicable if it contains provisions that through reference in this document incorporate additional provisions to this document [ECSS-P-001B].

[AD-1] "Technical Annex", EMMON Project, ARTEMIS Joint Undertaking Call for proposals ARTEMIS-2008-1, Grant agreement no. 100036, 2008-12-08.

[AD-2] “Research Roadmap on Cooperating Objects”, CONET Consortium (http://www.cooperating-objects.eu), Draft version, 2009/04. To be officially released by 2009/06

2.2 Reference Documents

This section presents the list of reference documents. A document is considered a reference document if it is referred but not applicable to this document.

The following documents are referenced within this document:

[RD-1] T. He, S. Krishnamurthy, J. Stankovic, T. Abdelzaher, L. Luo, R. Stoleru, T. Yan, L. Gu, G. Zhou, J. Hui, and B. Krogh. *VigilNet: An integrated sensor network system for energy-efficient surveillance*. ACM Transactions on Sensor Networks, 2(1):1–38, February 2006.

[RD-2] Anish Arora, Rajiv Ramnath, Emre Ertin, Prasun Sinha, Sandip Bapat, Vinayak Naik, Vinod Kulathumani, Hongwei Zhang, Hui Cao, Mukundan Sridharan, Nick Seddon, Chris Anderson, Ted Herman, Nishank Trivedi, Chen Zhang, Romil Shah, Sandeep Kulkarni, Mahesh Aramugam, and Limin Wang. *Exscal: Elements of an extreme scale wireless sensor network*. In RTCSA ’05: Proc. of the 11th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, pages 102–108, 2005.

[RD-3] Bhaskaran Raman and Kameswari Chebrolu. *Censor networks: a critique of ”sensor networks” from a systems perspective*. SIGCOMM Comput. Commun. Rev., 38(3):75–78, 2008.

[RD-4] Marius Schlingelhof, David Betaille, Philippe Bonnifait, Katia Demaseure. *Advanced positioning technologies for co-operative systems*. In Intelligent Transport Systems, IET, pages 81-91, 2008.

[RD-5] A. Ward, A. Jones, and A. Hopper. *A new location technique for the active office*. IEEE Personal Communications, Vol.4, Issue.5, pp.42–47, 1997.

[RD-6] A. Savvides, C.-C. Han, and M. B. Strivastava. *Dynamic fine-grained localization in ad-hoc networks of sensors*. In Proceedings of the 7th annual international conference on Mobile computing and networking (MobiCom), pp. 166–179, 2001.

[RD-7] D. Niculescu and B. Nath. *Ad hoc positioning system (APS) using AoA*. In Proceedings of INFOCOM, pp. 1734–1743, 2003.

[RD-8] U. Bischoff, M. Strohbach, M. Hazas, and G. Kortuem. *Constraint-based distance estimation in ad-hoc wireless sensor networks*. In Proceedings of the Third European Workshop on Wireless Sensor Networks (EWSN),pp. 54–68, 2006.

[RD-9] Cristian, F., *Understanding fault-tolerant distributed systems*, Communications of the ACM 34(2), 5678, 1991

[RD-10] Jean-Claude Laprie (Ed.), *Dependability: Basic Concepts and Terminology*, Springer-Verlag, ISBN 3-211-82296-8, 1992

[RD-11] Lynch, N. A., *Distributed Algorithms*, Morgan Kaufmann, 1996

[RD-12] A.A. Abidi, G.J. Pottie, and W.J. Kaiser. *Power-conscious design of wireless circuits and systems*. Proceedings of the IEEE, 88(10):1528{45, October 2000.

[RD-13] Winnie Louis Lee, Amitava Datta, and Rachel Cardell-Oliver , *Network Management in Wireless Sensor Networks*. To appear in Handbook of Mobile Ad Hoc and Pervasive Communications, American Scientific Publishers, USA.

[RD-14] L.B. Ruiz, J.M. Nogueira, and A.A.F. Loureiro, *MANNA: A Management Architecture forWireless Sensor Networks,* IEEE Communications M*agazine, vol. 41, no. 2, pp. 116–125, 2003*

3. *EMMON Project Overview*

3.1 Project Overview

The EMMON project is an European Research and Development (R&D) project, sponsored by the 7th Framework Programme (FP7), ARTEMIS Joint Undertaking (JU) initiative and integrated in the Industrial Priority "Seamless connectivity and middleware".

EMMON motivation is originated from the increasing societal interest and vision for smart locations and ambient intelligent environments (smart cities, smart homes, smart public spaces, smart forests, etc). The development of embedded technology allowing for smart environments creation and scalable digital services that increase human quality of life.

The project goal is to perform advanced technological research on large scale distributed Wireless Sensor Networks, including research and technology development activities in order to achieve the following specific objectives:

- Research, development and testing of a functional prototype for large scale WSN deployments;
- Advance the number of devices by one order of magnitude, by real world validation (10 thousand to 100 thousand nodes);
- Advance the number of devices by two orders of magnitude, by simulation (100 thousand to 1 million nodes);
- Improve reliability, security and fault tolerance mechanisms in WSN;
- Identify and capture end-user needs and requirements, as well as operational constraints;
- Determine a path for exploitation of project results;

EMMON's main objective is the development of a functional prototype for the real-time monitoring of specific natural scenarios (related to urban quality of life, forest environment, civil protection, etc.) using Wireless Sensor Network (WSN) devices. The goal of the project is to develop the technology to effectively monitor and control an area of 50 square km.

Areas of application for the project include a multitude of physical environments where continuous, large scale monitoring and situation analysis are of great interest, such as hydrographical systems (rivers and dam's), urban areas quality of life monitoring (pollution and noise), regional climate/marine monitoring, civil protection (forest fires, pollution propagation, etc), natural resources monitoring, energy production prediction, industrial plant monitoring, personal health monitoring and precision agriculture, just to name a few.

The increased environment awareness and detection of abnormal variations, allied with the possibility to rapidly broadcasting alarms and alerts, improves human quality of life and sustainability.

Project main results include:

- Large scale deployment of a fully-functional system prototype in a real world scenario (composed of thousands of nodes);
- New WSN embedded middleware with better overall energy efficiency, security and fault-tolerance;

- New efficient and low power consumption WSN multilevel communication protocols and reliable middleware for large scale monitoring;
- Simulation models for WSN behaviour analysis;
- Centralized C&C Centre for easy and centralized monitoring;
- Mobile C&C station or device for local access, diagnosing, viewing and troubleshooting of the network;

EMMON is structured in eight (8) work-packages (WP1 to WP8):

- WP1 and WP2 include management, dissemination, exploitation and standardization activities;
- WP3, WP4 and WP6 include the main RTD activities;
- WP5, WP7 and WP8 aggregate all integration, implementation and testing activities.

Figure 1, illustrates the work-packages distribution within project areas and how they are related.

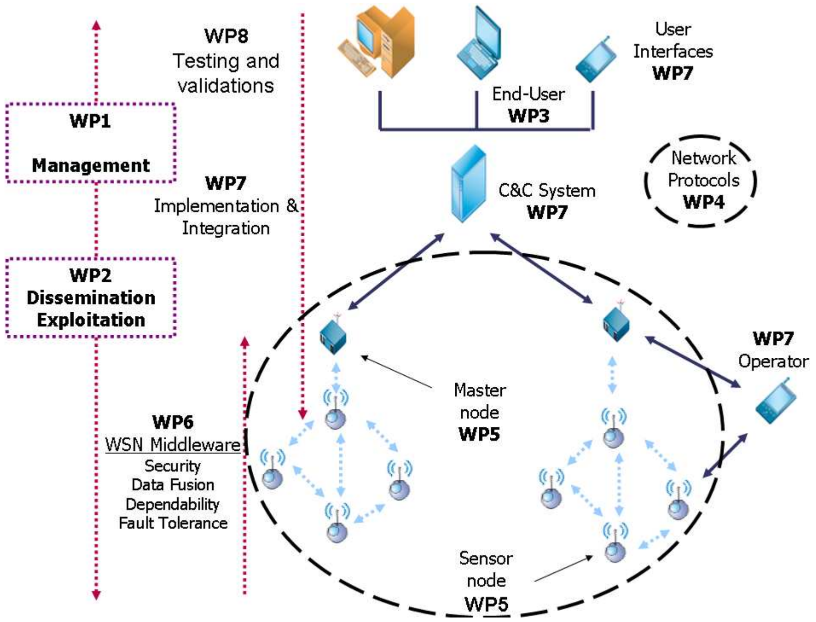

Figure 1 - EMMON system overview and work package decomposition

3.2 Work-Package 4 Overview

WP4 "Research on Protocols & Communication Systems" objective is to design, implement and test the new communication principles, protocols and mechanisms that will support communications in large-scale embedded computing applications and still cope with requirements such as timeliness, reliability, security, energy-efficiency, system complexity and cost-effectiveness. The WP comprises six (6) Tasks:

- T4.1: Research on large scale wireless sensor networks
- T4.2: Robustness and organization
- T4.3: Multilevel-protocol

- TP4.4: Data aggregation
- TP4.5: Security
- TP4.6: Communication Test Lab

4. Envisaged Characteristics of the EMMON Communication Architecture

4.1 Introduction

This section aims at identifying and classifying the most relevant properties of WSNs with respect to the communication system and protocols, within the EMMON network architecture. We have classified these characteristics as follows:

- Non-functional properties:
  - Scalability
  - Heterogeneity
  - Reliability/robustness
  - Timeliness
  - Security
  - Energy-efficiency
  - Cost-effectiveness
- Algorithms
  - Positioning
  - Synchronization
  - Data aggregation
  - Mac and routing
  - Congestion control, load balancing
- Network planning and management
  - Network planning
  - Network management
  - Remote programming/debugging

The remainder of this section presents a short definition of each of these properties and tries to identify their characteristics within the EMMON project, in what concerns WP4, T4.1.

4.2 Non-Functional Properties

The non-functional properties (NFPs) of a WSN system are the properties that do not affect its functionality, but its quality. Therefore, the NFPs can also be considered as the Quality-of-Service (QoS) characteristics of a WSN system, instantiated in properties such as energy-sustainability/system lifetime (involving energy-efficiency, energy conservation, energy harvesting), reliability/robustness (processing, communication, radio links, sensors/calibration), timeliness (throughput, delay, traffic differentiation – real-time/best-effort), security, scalability, heterogeneity and cost-effectiveness.

4.2.1 Scalability

A WSN system may involve different types of network nodes, i.e. sensors/actuators, routers/gateways and/or sinks/controllers and other agents too (e.g. machinery, vehicles, robots, humans/animals). Depending on characteristics such as the application, the environment or the users, a WSN system scale may dynamically change with time. The term "scale" applies to the number (fewer or more nodes in the overall system), spatial density (fewer or more nodes in a restricted region), or geographical region under coverage (smaller or wider, 2D or 3D). The ability of a WSN system to easily/transparently adapt itself to these dynamic changes in scale is named "scalability".

The EMMON network architecture should be able to easily/transparently scale up to:

- Large number of WSN nodes, ranging from thousands to tens of thousands of nodes;
- Wide bi-dimensional regions, ranging from hundreds to several thousand square meters.

It should also be possible to simulate network scenarios featuring one million nodes, although a real deployment for this dimension is not considered within the timeframe of the EMMON project.

4.2.2 Heterogeneity

WSN systems in general and the EMMON architecture in particular will inherently have heterogeneous components, therefore heterogeneity must be appropriately considered both pre-run-time (at design time) and during system operation (e.g. for system management). In what is more related to "communication system and protocols", heterogeneity emerges at different levels, such as:

- Heterogeneity in networking hardware/software
  - Sensor/actuator-level nodes (e.g. different types of platforms)
  - Sensor/actuator-level communication protocols (e.g. IEEE 802.15.4, ZigBee, 6loWPAN)
  - Higher-level nodes (e.g. routers, cluster-heads, gateways)
  - Higher-level communication protocols (e.g. IEEE 802.11, IEEE 802.16)
- Heterogeneity in embedded system nodes hardware/software architecture
  - Hardware: radio transceivers, antennas, microprocessor/controller/DSP, sensors/actuators
  - Software: middleware, operating systems and programming languages

Additionally, heterogeneity may also exist at the application level, as several different applications/services may need to be supported by the same networking infrastructure. In this line, the EMMON network architecture must be designed in a way that all these levels of heterogeneity are transparent to the users.

4.2.3 Reliability/Robustness

In a very large scale WSN, faults (be they of sensors, nodes or communication) can be expected to be common occurrence. This implies that the network should provision for faults and incorporate fault-tolerance mechanisms.

A *failure* occurs when the delivered service no longer complies with its specification. An *error* is an unintended state of the system that is liable to lead to a subsequent failure. The adjudged or hypothesized cause of an error is a *fault*. *Fault containment* deals with preventing the failure of a service from propagating to other components that depend on that service. A component is *fault tolerant* if it provides services complying with their specifications in spite of faults [RD-10] Therefore, for a WSN network to be reliable, sensor, node and communication failures must be contained so that the overall network is fault-tolerant.

Sensors, nodes and communication may fail in many different ways: a sensor or a node might stop (crash failure), might fail to respond (omission failure), might respond outside the specified time interval (timing failure), might give an incorrect response (response failure) or might exhibit more severe failures, where it behaves arbitrarily (Byzantine failures) [RD-9]. Communication failures can include message loss (omission failure) or duplication (response failure) [RD-11].

Fault tolerance requires fault detection and fault recovery. While in a small WSN, these aspects can both be handled by human operators, this approach is not appropriate for a large-scale network. Therefore large-scale networks need to self-manage, i.e., detect faults autonomously and adapt their behaviour and their organization to continue providing services, while also taking appropriate actions for the faults to be corrected, be it autonomously or by notifying an operator.

In particular, large-scale networks are typically hierarchically organized. In this configuration the failure of a node from a higher-tier can imply that all its lower-tier children become unavailable, which can entail that monitoring becomes unavailable in an entire area. Therefore, an essential requirement for EMMON is the ability of the network to handle such failures, either via redundancy in the hierarchical organization, or via self-reorganization of the network.

4.2.4 Timeliness

The timing behaviour in WSN systems is becoming increasingly important, mainly due to the growing tendency for a very tight integration and interaction between embedded computing devices and the physical environment, via sensing and actuating actions. The “timeliness” NFP concerns the timing behaviour of a system, including issues such as network throughput (effective bit rate), message transmission delay (how long does it take for a message to be transmitted from source to destination) and non/soft/hard real-time characteristics of the messages.

Some WSN applications, or some specific tasks within an application, might also impose to be finished within a certain time limit (deadline). In this case, we usually refer to these as “real-time” applications/tasks, encompassing the need for real-time computation (requiring real-time operating systems and programming languages) and real-time communications (requiring real-time communication protocols).

Each application will impose particular timeliness requirements to the underlying communication/networking infrastructure, so the latter should:

- Enable a minimum data generation rate per sensing node (also considering in-node data aggregation); these minimum data generation rates may be different from node to node;
- Be able to provide deterministic or probabilistic guarantees on the message delays, in a way that both real-time and non real-time applications can be supported;
- Support traffic differentiation, i.e. the EMMON architecture should provide means to distinguish between different traffic classes, e.g. real-time (guaranteed bandwidth) and

best effort (probabilistic); this should be supported end-to-end, i.e. across the different network tiers.

4.2.5 Security

In wireless communications, security is usually a very important aspect. Since the transmitted data travels by air, it is more easily available to anyone having an appropriate receiver to capture the transmitted signals. WSNs also lack physical protection and are usually deployed in open and unattended environments, which increases their vulnerability to attacks. Hence, it is necessary to implement security techniques (such as encryption), in order to prevent sensible data to be obtained by third-parties.

Proposals for securing WSNs have until recently relied on symmetric cryptosystems to provide features such as confidentiality and authentication. This is mainly due to the fact that, because of their resource constraints, nodes cannot afford to run conventional Public Key Cryptography (PKC).

Security decisions made for the EMMON project should aim to fulfil the following points:

- Data confidentiality – this means keeping the information from the WSN secret from any unauthorized parties. This usually means applying some sort of cryptography;
- Data authenticity – the WSN should be secure against injection of data into the network by third parties, especially when it is to be used in any decision making process. Legitimate nodes should be able to detect messages from unauthorized nodes and reject them;
- Data integrity – this is to ensure that the data in transit has not been altered by any third parties. Data authentication can provide data integrity as well;
- Data freshness – it implies that the data received is recent and the no third parties have replayed old messages. A common mechanism to prevent this is the usage of a monotonically increasing counter with every message, thus rejecting any messages with older counter values;
- Robustness and survivability – the EMMON system should be robust against several security attack types, and in case of an attack succeeds, its effects should be minimised. The compromise of a single node should not compromise the entire system;
- Access to the system – decision will need to be made in terms of who will have access to the system. Accounts should be created with the appropriate privileges for all users of the system and an authentication mechanism should be enforced.

4.2.6 Energy-Efficiency

WSNs are characterized by heavy energy and computational constraints. In most cases, sensor nodes are powered by batteries, and in many situations it is not practical to replace these batteries. It is therefore essential to make the best possible use of the available energy, as it is a rare commodity. Energy can be harvested from the surrounding environment (such as sun, thermal or wind power, for example), turning sensor nodes into self-sufficient units. But the topic of energy harvesting will not be addressed here.

In order to achieve energy-efficiency, the EMMON project should envisage the following characteristics:

- Use of efficient processing algorithms and communication protocols, thus reducing the required energy. The routing protocols used should base their decisions on the location of the nodes, required energy to transmit and (current) battery capacity of each sensor node.

- Sensor nodes can be kept in a state of lower power consumption ("sleep" mode), while not transmitting; It seems reasonable to assume that the sensor nodes do not need to be constantly taking measures from the surrounding environment but rather do some readings from time to time. The network can thus be responsible for activating (waking) the sensors nodes at certain intervals, in order to get the readings from the environment.
- The usage of data aggregation/fusion can reduce the number of transmissions by reducing the amount of data to be transmitted. Also, aggregating data in fewer messages will decrease the communication overhead needed. Implementing aggregation/fusion mechanisms can thus significantly contribute to achieve energy efficiency.
- Multiple short message transmission hops should be used in detriment of one long transmission hop, since the required transmission power increases as the square of the distance between the source and the destination.

Achieving a system lifetime that corresponds to end user expectations (and possibly requirements) will also have to take into consideration the available technology in terms of sensor nodes and power supplies, although that is not a topic for this document.

4.2.7 Cost-Effectiveness

Any cost-effectiveness analysis (CEA) consists of comparing costs and effects of several courses of action, to determine which one is the most beneficial. In the EMMON project, energy-efficiency is intimately related to cost-effectiveness, as it directly affects the lifetime of the sensor nodes used. Longer lifetimes mean fewer replacements, which in turn means less sensor nodes purchased over time. The cost of node disposal should also be taken into consideration, due to an increasing concern regarding sustainability and environmental preservation.

One of the main objectives in EMMON should be to use as cheap sensor nodes as possible, in order to be able to build a WSN of sensor nodes that can be considered disposable, due to their price/cost. Nevertheless, sensor node disposal should take into consideration environmental concerns (biodegradability, contamination, etc).

Another important factor is maintenance. "Tele-maintenance" can significantly reduce the maintenance costs, by allowing it to be performed from a centralized point, and without having to deploy a maintenance team to the sensor node's location. This maintenance can be with regards to hardware (repairing of a faulty device, for example) or software (a firmware upgrade, for example).

4.3 Algorithms

WSNs require a number of services to be available. These services, and the algorithms that implement them, must cover the following aspects: node and phenomenon positioning, time and data aggregation, medium access control and message routing, as well as congestion control and load balancing.

4.3.1 Positioning

As sensor data is typically of very little use without corresponding position information, *positioning,* also called *localization*, of both sensor nodes and sensed phenomena is an essential requirement in WSNs. Additionally, positioning can be used to aggregate sensor data (cf. Section 4.3.3), as well as to optimise communication between nodes (e.g., geographical routing, c.f. Section 4.3.4).

Sensor localization is a prerequisite to phenomenon localization. While for small WSNs, the location of each node can be set during deployment, this solution is not realistic for large-scale networks, and nodes therefore need to be able to discover their location autonomously. A simple solution is the use of positioning technology, such as GPS, but the capacity of such technology is limited (e.g., GPS does not work indoors), and the cost and energy expense associated with equipping every node with such technology is typically prohibitive.

For this reason, it is important for a WSN to have a service that allows nodes to devise their position. Such a scheme can provide either *absolute* positioning, or positioning *relative* to some other node. Providing absolute positioning requires that the position of a number of nodes, designated as *anchor* nodes, be known (either via some positioning sensor or set at deployment).

As EMMON deals with WSNs for monitoring, it is expected that absolute positioning of both sensing nodes and phenomenon will be required. It seems realistic to assume that this type of WSNs will encompass a number of nodes whose position is known, and those can be used as anchors.

On one hand, the accuracy requirements on the positioning are likely to depend on the specific application considered. On the other hand, a more accurate system is likely to require more energy. Therefore, the positioning system should offer an adaptive service, whose accuracy can be tailored to meet applications' requirements while minimizing energy consumption.

4.3.2 Synchronization

Aggregation of data from different sensors is essential for deriving higher-level information in WSNs. This, however, requires that the nodes have a common notion of time to fuse the sensor readings. Similarly, synchronization is also required to coordinate potential actuators in a WSN, to coordinate medium access (c.f. Section 4.3.4), as well as for some methods of positioning (such as time of arrival difference c.f. Section 5.3.1).

The many uses of synchronization make it critical. The diversity of these roles, however, also makes it a difficult problem to solve. Application requirements may vary widely along many axes, such as precision, lifetime, scope, availability, and energy requirements. For example, localization might require a precision of a few milliseconds, while sensor tasks allocation might work at the level of several hours. Moreover, some applications based on local collaboration will require a pair of neighbours to be tightly synchronized, while global operations might place requirements on the synchronization of the entire WSN. Also, operations such as event triggers might require only momentary communication, while data logging often require an eternally persistent time scale. Finally, while relative synchronization (where the time of different nodes are synchronized) might be sufficient for some applications, other applications will have requirements on external synchronization, i.e., with an external time scale such as UTC.

This vast array of potential requirements highlights the need for an adaptive synchronization technique that can provide different guarantees at different levels of scale (i.e., better precision with closer neighbours), and also can achieve better synchronization during some period of time if required, so that synchronization is always “just precise enough” for the current needs of application, while saving as much energy as possible.

4.3.3 Data Aggregation

In WSN, sensor data collected at the nodes are usually collected by a node or a set of nodes for further processing and analysis. Raw sensor data contain redundancies and correlations.

Since communication is quite resource consuming as compared to computation in WSN nodes, computing data summaries before communication results in an efficient – and sometimes necessary – approach.

Data aggregation protocols provide parent sensor nodes with a single value or a small set of values that represent all sensor data in the area according to the interests of higher tiers and of the application.

In the EMMON network architecture, the data aggregation protocols should be able to compute aggregated quantities with a time complexity that is either constant or increases slowly with the number of nodes and the extant of the geographical region of deployment.

4.3.4 MAC and Routing

Since wireless channel is a shared medium, its access must be coordinated. The Medium Access Control (MAC) protocols determine the channel accesses by nodes. Routing protocols determine the routes that the packets take in multi-hop transmissions.

The EMMON communication system should feature:

- A MAC protocol with a prioritization mechanism; it should be contention-free for real-time traffic; the MAC may also support contention-based medium access for non real-time (best-effort) traffic;
- A routing protocol that guarantees bounded (at least with high probability) end-to-end message delays, for high-priority real-time traffic;
- MAC and routing protocols must be as much as possible, simple, scalable, decentralized and energy-efficient.

4.3.5 Congestion Control and Load Balancing

Because of the limited capacity of WSNs nodes, congestion control and load balancing is a crucial problem in these settings. In wireless networks, congestion can happen at the *node level*, like in traditional networks, when a node receives too many messages, and its buffer overflows, but also at the *link level*, when messages collide or the number of messages to be sent exceeds the available capacity. Both cases lead to message loss, hence decreasing fidelity (the proportion of messages delivered), or, in the case where retransmission mechanisms are in place, increasing energy consumption, message latency, and traffic volumes.

These problems are particularly rife in WSNs because typically nodes either send messages only when an event of interest occurs, or increase the reporting frequency in these cases. As several nodes typically detect the same event either simultaneously or within a short time period, this leads to message storms during crisis periods, i.e., very high traffic load when some event of interest occurs. Importantly, it is often during these periods that it is the most important to deliver data.

In addition, recurring traffic patterns might imply that some nodes, typically close to a sink or higher in a hierarchical topology, handle significantly more traffic than others, making it likely that these particularly important nodes be depleted of energy very quickly and die. Therefore, network topology and routing, should take into account the energy resources of the different nodes, and potentially change configuration periodically, so that the load be balanced among the nodes. Moreover, a congestion control and load balancing algorithm should be tuneable to the specific trade-off point between fidelity, and packet delay, throughput, and energy expenditure to suit an application's needs, i.e., provide the required message QoS while using as little energy as possible.

4.4 Network Planning and Management

4.4.1 Network Planning

Network planning tools assume an extreme importance in WSNs. In the EMMON context, we consider that network planning tools include modelling and simulation tools that can be used for network analysis and dimensioning, network (parameters) setup and network deployment.

Particularly for large-scale WSNs, it is of paramount importance to analyse, prior to run-time, the performance limits of the network, as well as, how the network parameters can be setup (e.g. MAC, routing, clusters' duty-cycle, routers' buffer size) in a way that QoS metrics such as throughput, message delay, security and system lifetime can be properly balanced.

WSN deployment is also a very complex task, for which adequate methodologies and tools must be used. How to deploy the WSN nodes? Where, how many, with what functionalities (sensing, processing, routing, gateway)? How to balance sensing accuracy (geographically), transceiver power (RX/TX) and network connectivity?

Therefore, EMMON should provide appropriate models, methodologies and tools to:

- Perform pre-run-time analysis, and dimensioning of the network (particularly for computing performance limits, system lifetime);
- Set all network parameters (e.g. MAC/routing/security-related);
- Deploy the nodes (e.g. location, number, functionalities);
- Simulate the network (preferably based on COTS simulation tools).

4.4.2 Network Management

After the network deployment it is necessary to monitor and control the network itself. Several things contribute to this need, namely: initial assumptions on network planning that might not reflect the true reality; environmental conditions that might change over time; active network components of a WSN that might reduce their performance over time due to unexpected deterioration; the network might be extended, with new components being deployed.

The main parameters to monitor are related to network availability and network efficiency. The goal should be to guarantee the best level of functionality and availability possible, without losing data and keeping the best performance possible (efficiency). In a traditional wired network, management focuses mainly on network responsiveness and bandwidth. In

WSNs, the energy efficiency claims all the focus over these traditional parameters. The management of the network should consider the energy level in each network node and control the network to efficiently use the energy capacity available in the network.

Network management of large-scale WSNs will differ greatly from traditional wired network management, not only on the wireless energy efficiency field, but also on the unmanageable amount of network actors monitored by a single point of monitoring.

The EMMON system should provide monitoring and control tools that: provides aggregate and comprehensible information about the network health; provide reports on automatic control operations or modifications on the network; allow for sensors configuration by aggregation (geographical areas, sensor type, etc)

A network management system designed for WSNs shall take the following into account [RD-13]:

- **Lightweight operation** - The operation of the network manager shall have light impact on the sensors' energy consumption and not interfere with the normal sensor operation (processing and communicating);
- **Robustness and fault tolerance** - The network management system shall be able to handle the dynamics inherent to WSN. Nodes becoming inactive, environment's drastic changes forcing packet loses, new nodes being added to the network, etc. The management system shall be able to reconfigure the network to handle all these kinds of events;
- **Minimal data storage** - The data model representing the management data must have a minimal core and be extensible to address different implementation management needs so it can be used in a modular way minimizing the data storage needed and complying with memory constraints of WSNs;
- **Scalability** - A management system should operate efficiently in any network size.

4.4.3 Remote Programming/Debugging

In general terms, remote programming/debugging consists of debugging (or programming) a program which is run on a system other than the system where the debugger is being run. The debugger connects to the remote system where the program to be debugged is being run, and is able to take control of its operation and get information about its state.

Envisaged characteristics for the EMMON network architecture:

- The sensor nodes will most likely be in areas with difficult physical access and possibly far away from each other. It will be important for sensor nodes to be remotely programmable. This will avoid having to send technician teams to the field to program the sensor nodes one by one, which would be very expensive and extremely time-consuming. In some cases, where there is no physical access to the sensor nodes, this would not even be possible at all.
- Being able to remotely replace code modules would also add flexibility to the system. This would allow the replacement of only part of the software, without the need to reconfigure and whole system or having to stop the sensor node from working during this period.
- Usage of sniffers to monitor the network traffic, providing insight on how the network is operating.

- Allow synchronization services, such as clock synchronization among nodes in the network.

5. Problems to Address

5.1 Introduction

This section aims at identifying the most relevant problems to be addressed in EMMON, particularly in what concerns the aspects related to WP4 (communication system and protocols). Most of the problems derive from:

- The large-scale nature of the WSN systems envisaged within EMMON, both in terms of number of nodes and also in terms of geographical region under coverage
- Severe resource limitations of (most) WSN nodes, such as the ones related to their energy, computational and communication capabilities

These are impairments to fulfil the objectives that were identified in Section 4.1:

- **Non-functional/QoS properties** - In addition to functional correctness, computation and communication must be secure and produced “on time” in accordance with application’s requirements. It is highly desirable to minimize energy consumption. Systems must also be cost-effective, maintainable and scalable. So, while fulfilling each individual QoS property in WSNs is difficult *per se*, addressing all these contradictory QoS attributes is even more complex.
- **Algorithms** - MAC, routing, positioning, synchronization, data aggregation and congestion control are some extremely important mechanisms to most WSN applications. Large-scale and nodes’ resource limitations strongly influence the way in which these mechanisms must be designed. For instance: MAC and routing protocols must be designed in a way that energy-efficiency is optimized, but fault-detection, message latency, security must not be significantly affected; positioning and synchronization must be achieved in a way that network throughput and system lifetime are not dramatically affected.
- **Network planning and management** - Network planning (e.g. network dimensioning, setup and deployment), network management and remote programming (over-the-air) and debugging are also quite challenging issues when WSN are concerned. Especially for large-scale systems, it gets increasingly complex to carry out these tasks while mitigating the impact on energy consumption or useful (data) network throughput. Appropriate network modelling, simulation and management tools must be devised in order to help system designers.

EMMON (and particularly WP4) will investigate standard and COTS wireless communication technologies as a baseline for the EMMON network architecture. Examples of wireless technologies to be explored are IEEE 802.15.4, ZigBee or 6loWPAN for the lower and IEEE 802.11 or IEEE 802.16 for the higher network tiers.

5.2 Non-Functional Properties

5.2.1 Scalability

Scalability and energy-efficiency have probably been the most important topics to drive WSN research, in the last few years. Nevertheless, to our best knowledge, real WSN deployments were only up to a few hundred (e.g. [RD-1]) to one thousand nodes ([RD-2]). Within EMMON, we envisage to build a real deployment one order of magnitude larger (several thousands of nodes), which is a significant advancement on the state of the art itself. Moreover and very importantly, our objective is to encompass several QoS properties at the same time.

Some of the problems that need to be addressed are:

- Investigate on MAC, routing, congestion control, load balancing and data aggregation mechanisms that are scalable, either designed from scratch or based on (adapting) already available ones (c.f. Sections 5.3.3 – 5.3.5)
- Investigate hierarchical multiple-tiered architectures, since they can support scalability without compromising other QoS metrics (e.g. throughput, delay, reliability); the communication architecture is composed of a more powerful (e.g. processing, energy, communication) network technology serving as a backbone to low-cost, low-power (sub)networks at the sensor/actuator level;
- Explore the use of geographically distributed (multiple) sinks, in a way that traffic bottlenecks may be more easily mitigated (a multiple-tiered architecture may be seen as a particular case of "multiple sinks", since data converges to separate "sink" nodes that may act as gateways to a higher level network.

5.2.2 Heterogeneity

In terms of "networks and protocols", heterogeneity is mostly related with the need for interoperability between different networks protocols, at the different tiers of the EMMON network architecture. Additionally, heterogeneity also emerges from the existence of different types of network nodes, namely sensor/actuator, router/cluster head, gateway, each one with specific characteristics.

In this context, the following problems were identified:

- Check how the required levels of QoS (e.g. timeliness, reliability, energy-efficiency) can be achieved using the communication technologies previously referred in Section 5.2.1, with a particular concern in achieving end-to-end QoS (across network tiers);
- Investigate and design the architecture of a gateway between "backbone" and sensor networks; interoperability between the two tiers; synchronous/asynchronous message relaying behaviour, traffic classes (and mapping into MAC traffic differentiation schemes in both tiers), functional blocks and data structures, frame/address/speed conversion issues (across tiers);

5.2.3 Reliability/Robustness

The challenges associated with ensuring reliability of a large-scale WSN network include sensors, nodes and wireless communication inherent unreliability, programming errors and updates, as well as failure accumulation.

Wireless communication is inherently unreliable, due to varying signal strength caused by reflection, diffraction and scattering. Moreover, signal collisions can lead to message loss. This is a particularly relevant problem in WSN where the simultaneous detection of an event by several sensors might trigger a broadcast storm. Therefore communication protocols and in particular network access scheduling is of particular importance in WSNs (cf. Section 4.3.4). In addition, radio transceivers themselves might be very unreliable especially when they have to fulfil cost, size and power-consumption constraints.

In a large-scale WSN, a software error might lead to complex errors very challenging to diagnose (c.f. Section 4.4.3). In addition, once an error is detected, the node update process might be very challenging for this reason, it is important that nodes be designed so that they can easily be reconfigured, updated, or replaced (c.f. Section 4.4.2).

Finally, failures might be propagated along the network and accumulate, with potentially dramatic results. This is particularly challenging problem for very large-scale networks.

5.2.4 Timeliness

As already referred, one of the biggest challenges in LS-WSNs is to optimize all QoS properties simultaneously, knowing a priori that some (most) of them are contradictory. In what concerns the “timeliness” QoS property, the following problems were identified and deserve to be addressed:

- How to design protocols and algorithms in an optimized light and cross-layered approach; analyse trade-offs in terms of flexibility and interoperability, since the software structure becomes more difficult to update and maintain;
- How to build system/network planning and dimensioning tools for achieving optimal QoS trade-offs, e.g. timeliness vs. energy-efficiency;
- Consider timeliness (and real-time) both at the node level (hardware and software) and at the network level; the timing performance of a WSN depends on node hardware design, on the operating system (if any), programming language and style, as well as on the network protocol;

5.2.5 Security

Applying encryption algorithms to the data that travels through the network means extra processing on all that data. This represents an increase on data processing and power consumption that needs to be taken into consideration. Therefore, it is essential to choose these encryption algorithms (and level) wisely.

When encryption key pairs (a public key and a private key) are generated, two large prime numbers are selected (in a random manner), in a process that takes time. Since there are very few prime numbers to select from, when comparing to the whole range of integer numbers, the number of bits used for the public keys must be very large, in order to match the key space used for symmetric encryption, which uses integers (and not just prime numbers). The encryption level chosen for the EMMON system will therefore depend on the key space, which in turn depends on the algorithm and number of bits used to generate the keys.

Symmetric cryptosystems face the key distribution problem (they must decide on a shared key to communicate separately), although they are more efficient than PKC (Public-key Cryptography) systems. On the other hand, the usage of PKC might constitute a problem, since it is too expensive to be used on the resource constrained WSNs.

In a two-party communication system, data authentication mechanisms can be achieved with a purely symmetric mechanism: both the sender and the receiver share a secret key to compute a message authentication code (MAC) of the communicated data. The receiver knows that the message has been sent by the correct sender, if it has the correct MAC. However, for broadcast messages, authentication requires stronger trust assumptions with regards to the network nodes. If one sender wants to transmit authentic data to mutually untrusted receivers, using a symmetric MAC is not secure as any of the receivers knows the MAC key and can thus impersonate the sender and forge messages and send them to other receivers.

With regards to data freshness, using a monotonically increasing counter with every single message and reject any messages with old counter values might constitute a problem. For RAM constrained sensor nodes, this becomes problematic even for modestly sized networks. Assuming that the nodes devote just a small fraction of their RAM for this neighbour table, an adversary replaying broadcast messages from several different senders might fill up the table. At this stage, two options are available to the recipient: ignore any messages from senders that are not in its neighbour table, or purge entries from the table. None of these options is desirable: the first one creates a Denial of Service (DoS) attack, and the second allows replay attacks.

Scalability might also pose a problem. The majority of the security protocols used in WSNs are based on point-to-point handshaking procedures (to negotiate link dependent keys), but this affects the scalability of the network. Also, not all applications of WSNs will require the same security levels, but even in applications that do, different types of messages might require different security levels. This will add to the complexity of the security protocols to be implemented.

5.2.6 Energy-Efficiency

Energy-efficiency is one of the biggest challenges of any WSN project and one of the most difficult obstacles to overcome. Using sensor nodes with their own power supplies (typically batteries) is a common approach, but these have limited lifetimes. Often enough, these lifetimes are considerable shorter than what would be expected.

The use of a “sleep mode” may present a problem. If there is no a priori knowledge about when is a sensor node expected to receive a particular transmission, it will have to be listening all the time or will risk missing out on important information.

While using multiple short message transmission hops requires less power than one long hop, it increases the number of used sensor nodes, which in turn increases the total cost of the network.

The security related encryption mechanisms present a problem in terms of energy efficiency. The extra processing that is required for the encryption and decryption procedures consumes additional energy, as does sending an encryption key along with every message. The level of security itself also influences energy issues: if message integrity is only checked at the final destination, the network may be routing packets that were injected by third parties, many hops before they are eventually detected. This (as well as other attacks) represents a waste of energy (as well as bandwidth).

There will always have to be a trade-off between energy-efficiency and the system’s characteristics/functionalities (processing capacity, security level, amount of data handled, timeliness, synchronization accuracy, robustness, etc).

5.2.7 Cost-Effectiveness

Several factors influence the total costs associated to a WSN. The cost of the individual sensor nodes plays an important role, but over time, other factors such as maintenance costs or possibility of updates will also be very significant.

A solution cannot be to simply get the cheapest sensor nodes in the market. Cheaper nodes usually have more limited resources, including battery lifetime. In most cases, the choice of which devices to use will always have to be a trade-off between price and functionality/resources.

5.3 Algorithms

This section presents the challenges that must be tackled to derive and implement each of the algorithms identified in Section 4.3.

5.3.1 Positioning

As mentioned in Section 4.3.1., it is realistic to assume that the positions of a (limited) number of nodes of a very large-scale WSN will be known. Positioning technology, however, only provides position with a limited accuracy (from several meters for standalone GPS to sub-metre accuracy for differential GPS [RD-4]). In addition, calibration and deployment errors might further lower the accuracy of the nodes' positions. Anchor-based localization schemes use these known locations to position other nodes. This positioning, however, is also of limited accuracy, which adds up to the anchor's position inaccuracy and propagates through the network. This makes ensuring positioning with a specified accuracy throughout an entire large-scale network particularly challenging.

Localization algorithms can be categorized as *range-based* or *range-free*. Range-free algorithms use only connectivity information and the number of hops between nodes. Range-based algorithms, however, make use of an approximation of the distance between nodes by using either time of arrival (TOA) [RD-5], time difference of arrival (TDOA) [RD-6], angle of arrival (AOA) [RD-7], or received signal strength (RSSI) [RD-8]. While range-based algorithms should yield more accurate results, most of them require extra hardware to achieve the measurement, which implies extra energy consumption and cost. Therefore, one of the most salient challenges to address by the positioning system is how to achieve optimal accuracy using available hardware.

Most positioning schemes assume isotropic networks (i.e., networks that have the same density of nodes in every direction), which may not be an appropriate assumption for a WSN whose shape maps some physical feature (e.g., a forest). Furthermore, the possibility of obstacles obstructing some of the transmissions is most often not considered.

Another aspect that is likely to prove challenging is the positioning of measured phenomena (as opposed to the nodes themselves), as these phenomena can potentially move over time and be observed by a varying set of sensors. Considering the possibility of mobile nodes would also make the positioning problem significantly more challenging.

Finally, any solution to the positioning problem should both scale well for a very large-scale network, and limit the number of messages to limit traffic congestion (c.f. Section 4.3.5) and power consumption (c.f. Section 4.2.6)

5.3.2 Synchronization

In traditional distributed systems, the creation of a synchronization scheme that satisfies such a broad spectrum of requirements as identified in Section 4.3.2 is already challenging. The task becomes particularly daunting in sensor networks, in light of their additional domain requirements, and in particular energy efficiency and scalability through localized interactions.

Nodes in WSNs typically have very low energy budgets, therefore communication, which is traditionally used for synchronization in distributed systems but is very costly in terms of energy, should be kept to a minimum. Energy consumption can also depend on the synchronization precision indirectly via the energy cost of MAC protocols. This means that there is a trade-off between avoiding energy expenditure during synchronization at the cost of precision, and aiming for higher precision to allow recurrent energy gains during the WSN's lifetime.

Scalability is another significant challenge that needs to be addressed to achieve synchronization in a large-scale wireless network. Many synchronization schemes adopt a *master/slave* approach, where a node is assigned to be a master, and the other nodes try to synchronize with it. Such a centralized approach, however, might prove both inefficient and not robust enough in a large-scale WSN. Therefore, *peer-to-peer* approaches, where every node is treated equally, or hybrid approaches, where nodes synchronize within a cluster, need to be considered. Scalability also raises accuracy problems as errors might propagate within the network and potentially aggregate leading to very poor accuracy in some parts of the network.

5.3.3 Data Aggregation

Within EMMON, scalability is the most important issue to be considered for a data aggregation protocol. It is important to investigate appropriate routing and packet scheduling (for deterministic MAC) designs in conjunction with a data aggregation protocol for the performance improvement of the latter.

Processing and memory limitations must also be considered when designing data aggregation mechanisms. Additionally, the problem of information loss should be minimized in a way that application requirements are respected.

Holding transmission for data aggregation from as many nodes as possible leads to better aggregation but implies delays. This trade-off needs to be studied. Ideally, the aggregation mechanism will be both order and duplicate insensitive.

There exist a number of aggregation protocols that are tree-based. Such protocols are not suitable for a large scale WSN since loss of one packet can result in the loss of data from an entire sub-tree. Graph based or other fault-tolerant mechanisms need to be considered.

5.3.4 MAC and Routing

MAC and routing are affected by network layout. Accordingly, it will be useful to consider these issues together. The characteristics of these two protocols are affected by duty-cycle. In order to improve system lifetime, WSN nodes switch to lower power consumption status as often as possible, usually according a certain periodicity (that can dynamically change over time/space); this is called duty-cycle and it may refer to both node processing (turning processor off) and communications (turning transceiver off) status decisions.

Energy-efficiency of MAC and routing protocols is an important problem to be considered. Designing a MAC mechanism that is able to guarantee acceptable levels of network throughput and message delays but still be energy-efficient (e.g. supporting mechanisms for mitigating the hidden-node problem, duty-cycling, traffic differentiation, optimal utilization of TDMA slots), guaranteeing an optimal trade-off between flexibility and complexity.

Existing routing protocols and WSN models, particularly “mesh-like” (probabilistic routing, but more flexible, scalable and redundant) and “clustered-like” approaches (deterministic routing, but less flexible and redundant), deserve investigation, in a way that their positive features can eventually be merged.

It will be important to design a scalable routing protocol that makes routing decisions locally and thus provides complexity that is independent of the size of the network. Robust routing in the case of node failures must also be addressed.

5.3.5 Congestion Control and Load Balancing

Congestion arises when the traffic volume exceeds the resources' capacity. Therefore congestion can be avoided by two strategies: traffic control, i.e., reducing the amount of traffic, and resources control, i.e., increasing available resources. Traffic control can be achieved by three methods:

- Dropping messages (in which case, the fidelity requirement, c.f. Section 4.3.5, is typically violated),
- Optimising message routing (as discussed in Sections 4.3.4 and 5.3.4);
- Aggregating data (c.f. Sections 4.3.3 and 5.3.3), but this is limited by the amount of processing and memory available at each node and is often at the expense of data timeliness.

While traffic control is the only approach available in traditional networks, in WSNs, resource control can also be used, by turning on nodes that would otherwise be sleeping to save energy. Increasing the number of modes increases the network capacity, hence enabling fidelity and timeliness requirements to be met, though at the expense of the energy factor. This approach, however, requires nodes to be aware of the congestion type, traffic pattern and network topology, which might not be fully predictable.

While all of these approaches can be combined, the main challenge lies in assessing how to combine them to best fit an application's requirements, and potentially adapt them as application requirements evolve.

5.4 Network Planning and Management

5.4.1 Network Planning

Network planning, (e.g. network dimensioning, setup and deployment), will be extremely important for the EMMON project, particularly at the time the EMMON application scenarios are to be engineered.

Therefore, the following problems related to Network Management should be addressed:

- How to devise appropriate models, methodologies and tools to perform pre-run-time analysis and dimensioning of the network;
- How to use these tools to easily and transparently set all network parameters and also for an optimal nodes deployment;
- Investigate the way pre-run-time analysis and simulation tools can be combined to achieve a better network planning; check how these models can be tuned and optimized by using experimental data.

5.4.2 Network Management

Currently there is no generalized solution for WSN management [RD-14]. However, network management is important to maintain WSN health. Commercial WSN implementations might be unviable without it. Nevertheless, it is a big challenge to develop a generalised, full featured and addressing all requirements WSN monitoring system.

Most of the existing solutions manage the network within the application protocols. The creation of WSN management layer protocols is still work in progress. Furthermore, the creation of a Management Information Base (MIB) specific for WSNs that is able to express management policies and information exchanged between sensor nodes, managers, and end users is also another area with work in progress. This shall address the modularity and data storage constraints on sensors.

The main difficulties foreseen to achieve WSN management system can be summarized in two points:

- Address the new network monitoring paradigm based on energy state of the WSN nodes,
- Minimize the overhead of the monitoring system in the WSN energy consumption and bandwidth not to interfere with the normal operation of the network.

5.4.3 Remote Programming/Debugging

Usually the operation of loading a new firmware into a device has a level of risk associated. This is because the routine to load the new firmware is part of the firmware being replaced. If the process of loading fails in the middle it might leave the device with part of the old and part of the new firmware, resulting in an unpredictable outcome.

Considering that WSNs have many sensor nodes, the risk of loading new firmware to every single one of them successfully is even higher. This would have to be dealt with techniques like double memory to hold the old firmware on one memory while loading the new one to another (no overwriting while loading) - this would make the device more expensive.

Also because we are always talking about several devices – mainly on LSWSN – the communication of the new firmware from the network manager to the devices would definitively occupy a large bandwidth. The impact would be to have the WSN not operating during some time while loading the new firmware into all devices. Furthermore this would be a big drain for network nodes responsible to relay the firmware to several devices and other routers.

Broadcast techniques might be used to mitigate the impacts of distributing new firmware in the energy consumption and bandwidth. It still has a considerable impact though.

6. General Conclusions

This deliverable aimed at classifying and identifying the main problems and challenges to be addressed within WP4 (Research on Protocols and communication systems), thus related to the EMMON communication system.

This document has been written at a very early stage of the EMMON project, even before the first WP3 deliverables (T0+4) on end-user requirements have been released. Therefore, Section 4 presented the characteristics of the EMMON communication system in a generic fashion, in a way that these can then be fine-tuned according to application-specific requirements.

As it can be inferred from this document and from the state-of-the-art in [AD-1], engineering large-scale wireless sensor network applications while coping with application/user requirements such as scalability, timeliness, reliability, security, system lifetime and cost-effectiveness is quite challenging. Mature solutions to some of these problems might only emerge beyond the timeline of the EMMON project, as precluded in [AD-2].

Lots of problems to address were identified in this deliverable (Section 5). According to the end-user requirements resulting from WP3 deliverables and also from the more specific requirements of the EMMON target application, the problems to address identified in this deliverable will eventually need to be revisited and readjusted.