EMMON - EMbedded MONitoring

ARTEMIS JU – FP7

D4.5 SPECIFICATION OF MULTILEVEL COMMUNICATION PROTOCOLS

EMMON

Agreement Ref.: *100036*

Date:	*2010-12-07*
Pages:	*56*
Status:	*Approved*
Dissemination Level:	*PU*
Reference:	*FP7-JU-EMMON-2010-DL-WP4-005-D4.5*
Version:	*2*

Customer:

D4.5 SPECIFICATION OF MULTILEVEL COMMUNICATION PROTOCOLS

EMMON

Authors and Contributors				
Name	**Contact**	**Organization**	**Description**	**Date**
Anurag Garg	anurag.garg@cs.tcd.ie	TCD	Author	2010-02-10
Stefano Tennina	sota@isep.ipp.pt	ISEP	Co-author	2010-02-10
Mélanie Bouroche	Melanie.Bouroche@cs.tcd.ie	TCD	Co-author	2010-02-10
Farrukh Mirza	Farrukh.Mirza@scss.tcd.ie	TCD	Co-author	2010-02-10
Mário Alves	mjf@isep.ipp.pt	ISEP	Co-author	2010-02-10
Paulo Gandra Sousa	pag@isep.ipp.pt	ISEP	Co-author	2010-02-10

Dissemination Level

Public

Revision History				
Version	**Revision**	**Date**	**Description**	**Author**
1	0	2010-02-10	Currently In preparation	Anurag Garg, Mélanie Bouroche, Farrukh Mirza
1	1	2010-03-31	Draft for Internal Review	Anurag Garg, Stefano Tennina, Mélanie Bouroche, Farrukh Mirza
1	2	2010-04-07	Final Draft for Submission	Anurag Garg, Stefano Tennina, Mélanie Bouroche, Farrukh Mirza
2	1	2010-05-19	Draft for Internal Review v2	Anurag Garg, Stefano Tennina, Mélanie Bouroche, Farrukh

Revision History				
Version	**Revision**	**Date**	**Description**	**Author**
				Mirza
2	2	2010-05-31	Final Draft for Submission	Anurag Garg, Stefano Tennina, Mélanie Bouroche, Farrukh Mirza
2	4	2011-02-22	Approved version according to the results of the Interim (M18) Technical Review Report, ref: ARTEMIS-ED-21-09 of 2010-12-07	Mélanie Bouroche

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 main objective of this deliverable is to specify the multi-tiered communication architecture to support a large-scale WSN deployment as envisaged by EMMON. This deliverable also proposes a multi-level communication protocol that specifies how messages are exchanged within and between the different tiers in the communication architecture. The first issue of this deliverable was released on 2010-03-31 without sections 8-12.This is the second and final issue of this deliverable and contains the sections 8-12 and revisions to all the other sections.

1.2 Scope

The EMMON project is composed of eight (8) Work-Packages:

- WP1 – Project Management, Procedures and Communication;
- WP2 – Exploitation, Dissemination and standardization;
- WP3 – Study of user environment and definition of requirements and needs;
- WP4 – Research activities on Protocols & Communication Systems;
- WP5 – Definition of HW platforms and sensors;
- WP6 – Research on Embedded Middleware;
- WP7 – Implementation and System Integration;
- WP8 – Operational Testing & Validations.

This deliverable is produced under the scope of Work-package 4 “WP4 - Research on Protocols and Communication Systems” and associated with “T4.3 - Research on multi-level communication protocol”. In this context, it focuses on problems and challenges regarding the design of 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). In addition, this deliverable specifies the design of the multi-level communication protocol for EMMON.

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
ACK	Acknowledge or acknowledgement packet
AD	Applicable Document

Acronyms	Description
C&C	Command and Control Centre
CAP	Contention Access Period
CDMA	Code Division Multiple Access
CEA	Cost-Effectiveness Analysis
CFP	Contention Free Period
CH	Cluster Head
CRC/FCS	Cyclic Redundancy Code/Frame Check Sequence
CSMA	Carrier Sense Multiple Access
DSP	Digital Signal Processor
FDMA	Frequency Division Multiple Access
GPS	Global Positioning System
GTS	Guaranteed Time Slot
GW	Gateway
IEEE	Institute of Electrical and Electronics Engineers
LS-WSN	Large-Scale Wireless Sensor Network
MAC	Medium Access Control
N/A	Not Applicable or Not Available
NES	Networked Embedded Systems
NFP	Non-Functional Property
OTAP	Over The Air Programming
PKC	Public-key cryptography
QoS	Quality-of-Service
RD	Reference Document
SIFS	Short Inter-Frame Spacing time
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.

Section 3, EMMON Project Overview, presents an overview of EMMON project and also of Work Package 4 (communication system and protocols).

Section 4, Methodology Used For Evaluation, aims at introducing the reader with the methodology used.

Section 5, Overview of Solutions Proposed By D4.2, presents a review of the deliverable D4.2 with a brief overview of the network architecture and communication solutions that were proposed.

Section 6, Deployment Considerations, discusses the LS-WSN deployment considerations that must be taken into account in the design of the network architecture and communication protocol.

Section 7, Multi-tiered Architecture, presents the multi-tiered communication architecture.

Section 8, Addressing, discusses the addressing schemes under consideration.

Section 9, Packet Format, discusses the packet format.

Section 10, Routing, discusses routing.

Section 11, Design Choices, fixes some design choices summarizing the output of the present network architecture specification.

Section 12, Additional Issues, presents additional issues to be further addressed in next deliverables in the frame of Work Package 4.

Section 13, General Conclusions, presents the 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] "D4.1 – Study of collected, analysed and classified problems to address in this project", EMMON Project, ARTEMIS Joint Undertaking Call for proposals ARTEMIS-2008-1, Grant agreement no. 100036, 2009-05-29.

[AD-2] "D5.1 – Embedded Systems Hardware Alternatives Document", EMMON Project, ARTEMIS Joint Undertaking Call for proposals ARTEMIS-2008-1, Grant agreement no. 100036, 2010-02-28.

[AD-3] "D3.1 – Operational requirements consolidated from end-users input and opinions", EMMON Project, ARTEMIS Joint Undertaking Call for proposals ARTEMIS-2008-1, Grant agreement no. 100036, 2010-02-26.

[AD-4] "D4.2 – Evaluation report: evaluation of possible solutions, concepts for new communication methods", EMMON Project, ARTEMIS Joint Undertaking Call for proposals ARTEMIS-2008-1, Grant agreement no. 100036, 2010-01-29.

[AD-5] "D5.3 – Device Definition", EMMON Project, ARTEMIS Joint Undertaking Call for proposals ARTEMIS-2008-1, Grant agreement no. 100036, 2010-04-30.

[AD-6] "D6.2 - Middleware Framework", EMMON Project, ARTEMIS Joint Undertaking Call for proposals ARTEMIS-2008-1, Grant agreement no. 100036, 2010-05-31.

[AD-7] "D3.9 – Models and simulations for Fire & pollution propagation", EMMON Project, ARTEMIS Joint Undertaking Call for proposals ARTEMIS-2008-1, Grant agreement no. 100036, 2010-02-28.

[AD-8] "Open-ZB: an open-source implementation of the IEEE 802.15.4/ZigBee protocol stack on TinyOS," A. Cunha, A. Koubaa, R. Severino, and M. Alves, In IEEE Conference on Mobile Ad-hoc and Sensor Systems (MASS'07), Italy, Oct. 2007.

[AD-9] TDBS: a time division beacon scheduling mechanism for ZigBee cluster-tree wireless sensor networks. A. Koubâa, A. Cunha, M. Alves, and E. Tovar. Real-Time Syst. 40, 3 (Dec. 2008), 321-354. DOI=http://dx.doi.org/10.1007/s11241-008-9063-4

[AD-10] MATLAB tool, http://www.open-zb.net/downloads.php, 2008.

[AD-11] Implementation details of the time division beacon frame scheduling approach for ZigBee cluster-tree networks, Cunha A, Alves M, Koubaa A, IPP-HURRAY Technical Report TR070102. http://www.open-zb.net

[AD-12] i-GAME: An Implicit GTS Allocation Mechanism in IEEE 802.15.4, theory and practice, A. Koubâa, A. Cunha, M. Alves, E. Tovar, Published in Springer Real-Time Systems Journal, Volume 39, Numbers 1-3, pp 169 - 204, Springer, August 2008.

[AD-13] "Real-Time Communications over Cluster-Tree Sensor Networks with Mobile Sink Behaviour", P. Jurcik, R. Severino, A. Koubaa, M. Alves, E. Tovar, 14th IEEE

International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA 2008), Kaohsiung, Taiwan, Aug 2008

[AD-14] "Real-Time Communication over Cluster-Tree Wireless Sensor Networks", Petr Jurcik, PhD thesis, Dept. Of Control Engineering, Czech Technical University in Prague, February 2010.

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] Citysense Research Project page, http://www.citysense.net, Accessed on: 2010-05-12.

[RD-2] "CitySense: An Urban-Scale Wireless Sensor Network and Testbed", R. Murty, G. Mainland, I. Rose, A.R. Chowdhury, A. Gosain, J. Bers, M. Welsh, 2008 IEEE International Conference on Technologies for Homeland Security (2008). Available on line at http://www.eecs.harvard.edu/~mdw/papers/citysense-ieeehst08.pdf, Accessed on: 2010-05-12.

[RD-3] "CitySense: An Open, City-Wide Wireless Sensor Network", M. Welsh and J. Bers, Harvard University, November 2007. Available on line at: http://www.eecs.harvard.edu/~mdw/talks/citysense-commnet-nov07.pdf, Accessed on: 2010-05-12.

[RD-4] "Exscal: Elements of an extreme scale wireless sensor network," A. Arora, R. Ramnath, and E. Ertin, 2005. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.59.6739, Accessed on: 2010-05-22.

[RD-5] "Design of a wireless sensor network platform for detecting rare, random, and ephemeral events", P. Dutta, M. Grimmer, A. Arora, S. Bibyk, D. Culler, Proceedings of the 4th international symposium on Information processing in sensor networks.

[RD-6] Creating Ubiquitous Intelligent Sensing Environments, FP6-IST Network of Excellence, http://www.ist-cruise.eu, Accessed on: 2010-05-12.

[RD-7] Reconfigurable Ubiquitous Networked Embedded Systems, FP6-IST integrated project, http://www.ist-runes.org, Accessed on: 2010-05-12.

[RD-8] Very large scale open wireless sensor network testbed, http://www.senslab.info, Accessed on: 2010-05-12.

[RD-9] SensorScope, http://sensorscope.epfl.ch/index.php/Main_Page, Accessed on: 2010-05-12.

[RD-10] Research Project page, http://www.cs.virginia.edu/wsn/vigilnet, Accessed on: 2010-05-12.

[RD-11] "VigilNet: An integrated sensor network system for energy-efficient surveillance", T. He, S. Krishnamurthy, L. Luo, T. Yan, L. Gu, R. Stoleru, G. Zhou, Q. Cao, P. Vicaire, J. A. Stankovic, T. F. Abdelzaher, J. Hui and B. Krogh, ACM Transactions on Sensor Networks (TOSN), Volume 2, Issue 1, pp. 1 - 38, February 2006.

[RD-12] "On Scheduling and Real-Time Capacity of Hexagonal Wireless Sensor Networks", S. Prabh, K.; Abdelzaher, T.F., 2007. ECRTS '07. 19th Euromicro Conference on Real-Time Systems, pp.136-145, 4-6 July 2007.

[RD-13] "A Hexagon-Based Key Predistribution Scheme in Sensor Networks". Li, G., He, J., and Fu, Y., in Proceedings of the 2006 international Conference Workshops on Parallel Processing (August 14 - 18, 2006). ICPPW. IEEE Computer Society, Washington, DC, 175-180.

[RD-14] IEEE Standard for PART 15.4: Wireless MAC and PHY Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs) and amendment 1: Add Alternate PHY. Available on line at http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf and http://standards.ieee.org/getieee802/download/802.15.4a-2007.pdf, Accessed on: 2010-05-12.

[RD-15] "IEEE 802.15.4: a Federating Communication Protocol for Time-Sensitive Wireless Sensor Networks", A. Koubaa, M. Alves, E. Tovar, chapter of the book "Sensor Networks and Configurations: Fundamentals, Techniques, Platforms, and Experiments", Springer-Verlag, Germany, pp. 19 – 49, Jan. 2007.

[RD-16] "On the use of IEEE 802.15.4/ZigBee for Time-Sensitive Wireless Sensor Network Applications", Ricardo Severino, MSc Thesis, Polytechnic Institute of Porto, School of Engineering, October 2008. BEST EWSN/CONET MSc THESIS AWARD, 2009. http://www.cooperating-objects.eu/events/ewsn-2009-awards/.

[RD-17] "Collection Tree Protocol", O. Gnawali, R. Fonseca, K. Jamieson, D. Moss and P. Levis, ACM SenSys 2009 Berkeley, California, November 4-6 2009.

[RD-18] "Energy-efficient communication protocol for wireless microsensor networks". W.R. Heinzelman, A. Chandrakasan and H. Balakrishnan, In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences.

[RD-19] "A survey on routing protocols for wireless sensor networks", K. Akkaya and M. Younis, Ad Hoc Networks, Volume 3, Issue 3, May 2005, Pages 325-349.

[RD-20] ZigBee Alliance, http://www.zigbee.org

[RD-21] 6LoWPAN Standard, http://www.6lowpan.org

[RD-22] "RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks", G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, September 2007. Available at http://tools.ietf.org/html/rfc4944

[RD-23] "RFC 4919: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", G. Montenegro, N. Kushalnagar, C. Shumacher, August 2007, Available at http://tools.ietf.org/html/rfc4919

[RD-24] Berkeley IP implementation for low-power networks (BLIP), 6LowPAN on TinyOS, http://smote.cs.berkeley.edu:8000/tracenv/wiki/blip

[RD-25] 6LoWPAN: The Wireless Embedded Internet, http://6lowpan.net/the-book, Accessed on: 2010-05-02.

[RD-26] ROLL (Routing Over Low power and Lossy networks) Status Pages, http://tools.ietf.org/wg/roll/, Accessed on: 2010-05-02.

[RD-27] Large-Scale Demonstration of Self-Organizing Wireless Sensor Networks, http://webs.cs.berkeley.edu/800demo, Accessed on: 2010-05-23.

[RD-28] "Mobile Enabled Large Scale Wireless Sensor Network," C. Chen, J. Ma, Nokia Research Center, In Proceedings of the 8th International Conference on Advanced Communication Technology, February 2006.

[RD-29] Platform for Autonomous Self-Deploying and Operation of Wireless Sensor-Actuator Networks Cooperating with Aerial Objects, FP6 STREP Project # IST-2006-33579, http://grvc.us.es/aware, Accessed on: 2010-05-12.

[RD-30] "A survey on clustering algorithms for wireless sensor networks", A. A. Abbasi and M. Younis, Journal of Computer Communications, Special Issue on Network Coverage and Routing Schemes for Wireless Sensor Networks, 30 (2007) 2626-2841.

[RD-31] "First experiences using wireless sensor networks for noise pollution monitoring", Santini, S., Ostermaier, B., and Vitaletti, A. In Proceedings of the Workshop on Real-World Wireless Sensor Networks (Glasgow, Scotland, April 01 - 01, 2008). REALWSN '08. ACM, New York, NY, 61-65. DOI= http://doi.acm.org/10.1145/1435473.1435490

[RD-32] "Wireless Sensor Networks for Environmental Noise Monitoring", S. Santini and A. Vitaletti. In 6. GI/ITG Workshop on Sensor Networks, Aachen, Germany, 2007

[RD-33] "Citizen noise pollution monitoring", Maisonneuve, N., Stevens, M., Niessen, M. E., Hanappe, P., and Steels, L In Proceedings of the 10th Annual international Conference on Digital Government Research: Social Networks: Making Connections between Citizens, Data and Government (May 17 - 20, 2009). S. A. Chun, R. Sandoval, and P. Regan, Eds. ACM International Conference Proceeding Series, vol. 390. Digital Government Society of North America, 96-103.

[RD-34] CrossBow's TelosB mote platform datasheet, available online at http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/TelosB_Datasheet.pdf, Accessed on: 2010-05-12.

[RD-35] Collision-Free Beacon Scheduling Mechanisms for IEEE 802.15.4/Zigbee Cluster-Tree Wireless Sensor Networks", Anis Koubâa, Mario Alves, Melek Attia, Anneleen Van Nieuwenhuyse, available at http://www.dei.isep.ipp.pt/~akoubaa/publications/ASWN2007.pdf, Accessed on: 2010-05-12.

[RD-36] "Fault-Tolerance Mechanisms for Zigbee Wireless Sensor Networks", Skender Ben Attia, André Cunha, Anis Koubâa, Mário Alves, available at http://www.open-zb.net/publications/ECRTS07_WiP_camera%20ready.pdf, Accessed on: 2010-05-12.

[RD-37] Erika Real Time Operating System, http://erika.tuxfamily.org/erikaeducational.html, Accessed on: 2010-05-12.

[RD-38] "Connecting Wireless Sensor Networks to the Internet - a 6lowpan Implementation for TinyOS 2.0", M. Harvan. Master's thesis, School of Engineering and Science, Jacobs University Bremen, May 2007; http://www.eecs.iu-bremen.de/users/harvan/files/6lowpan.tar.gz, Accessed on: 2010-05-12.

[RD-39] "HOLSR: A Hierarchical Proactive Routing Mechanism for Mobile Ad hoc Networks," Luis Villasenor-Gonzalez, Ying Ge, Louise Lamont, IEEE Communications Magazine, July 2005, pg. 118-125

[RD-40] "Using Feedback in Collaborative Reinforcement Learning to Adaptively Optimize MANET Routing," J.Dowling, R.Cunningham, E.Curran, V.Cahill, IEEE Transactions on Systems, Man and Cybernetics-Part A: Systems and Humans, Volume. 35, No.3, May 2005

[RD-41] "SAMPLE: An On-Demand Probabilistic Routing Protocol for Ad-hoc Networks". Curran, Eoin; Dowling, Jim, Dublin, Trinity College Dublin, Department of Computer Science, TCD-CS-2004-03, 2004, pp14, http://hdl.handle.net/2262/13281, Accessed on: 2010-05-21.

[RD-42] "Addressing Techniques in Wireless Sensor Networks: A Short Survey," Uddin, M.Y.S.; Akbar, M.M. , *Electrical and Computer Engineering, 2006. ICECE '06.*

International Conference on , vol., no., pp.581-584, 19-21 Dec. 2006. doi: 10.1109/ICECE.2006.355698

[RD-43] "Z-Cast: A Multicast Routing Mechanism in ZigBee Cluster-Tree Wireless Sensor Networks", Olfa Gaddour , Anis Koubaa, Omar Cheikhrouhou, Mohamed Abid. in the Third International Workshop on Sensor Networks (SN 2010), in conjunction with ICDCS 2010, Genoa, Italy, June 21-25, 2010.

[RD-44] "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and zigbee standards", P. Baronti, P. Pillai, V. Chook, S. Chessa, A. Gotta, and Y. Hu. Computer Communications, 30(7):1655–1695, May 2007.

[RD-45] "Protocols and Architectures for Wireless Sensor Networks", Holger Karl, Andreas Willig, ISBN: 978-0-470-09510-2

[RD-46] "Distributed Localization Algorithms for Wireless Sensor Networks: From Design Methodology to Experimental Validation", S. Tennina, M. Di Renzo, F. Graziosi, F. Santucci, IN-TECH Book chapter in Wireless Sensor Network, ISBN 978-3-902613-49-3

[RD-47] "ESD: A Novel Optimization Algorithm for Positioning Estimation of WSNs in GPS–denied Environments – From Simulation to Experimentation", S. Tennina, M. Di Renzo, F. Santucci and F. Graziosi, International Journal of Sensor Networks, Vol. 6, No. 3/4, pp. 131-156, 2009

[RD-48] "F-LQE: A Fuzzy Link Quality Estimator for Wireless Sensor Networks", Nouha Baccour, Anis Koubâa, Habib Youssef, Maissa Ben Jamâa, Denis do Rosario, Mario Alves and Leandro Becker,, The 7th European Conference on Wireless Sensor Networks (EWSN 2010), Coimbra, Portugal, September 17-19, 2010.

[RD-49] "The ANGEL IEEE 802.15.4 Enhancement Layer: Coupling Priority Queueing and Service Differentiation," Karowski, In Proceedings of 14th European Wireless Conference, Prague, June 2008, pp.1-7.

[RD-50] "Priority-based service differentiation scheme for IEEE 802.15.4 sensor networks." E.-J., Kim, M. Kim, et al. AEU - International Journal of Electronics and Communications 61(2): 69-81.

[RD-51] "An Analytical Model for the Contention Access Period of the Slotted IEEE 802.15.4 with Service Differentiation", Ndih, E D N ; Khaled, N ; De Micheli, G, ICC 2009, International Conference on Communication, Dresden, June 14-18, 2009.

[RD-52] "Improving Quality-of-Service in Wireless Sensor Networks by Mitigating "Hidden-Node Collisions"," Koubaa, A.; Severino, R.; Alves, M.; Tovar, E. *Industrial Informatics, IEEE Transactions on* , vol.5, no.3, pp.299-313, Aug. 2009
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5196849&isnumber=5196841, doi: 10.1109/TII.2009.2026643.

[RD-53] "Adaptive-Compression Based Congestion Control Technique for Wireless Sensor Networks." Lee, Joa-Hyoung; Jung, In-Bum. *Sensors* 10, no. 4: 2919-2945.

[RD-54] "Fault-Tolerant Algorithms/Protocols in Wireless Sensor Networks, in Guide to Wireless Sensor Networks", Liu, H., Nayak, A. and Stojmenović, I, ed. Subhas Chandra Misra, Isaac Woungang and Sudip Misra, Springer London, 2009.

[RD-55] "Adaptive radio channel allocation for supporting coexistence of 802.15.4 and 802.11b", Chulho Won; Jong-Hoon Youn; Ali, H.; Sharif, H.; Deogun, J., Vehicular Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd , vol.4, no., pp. 2522-2526, 25-28 Sept., 2005 doi: 10.1109/VETECF.2005.1559004.

[RD-56] "Multi-Channel IEEE 802.15.4 Packet Capture Using Software Defined Radio", L. Choong, Master's thesis, UCLA, 2009.

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.

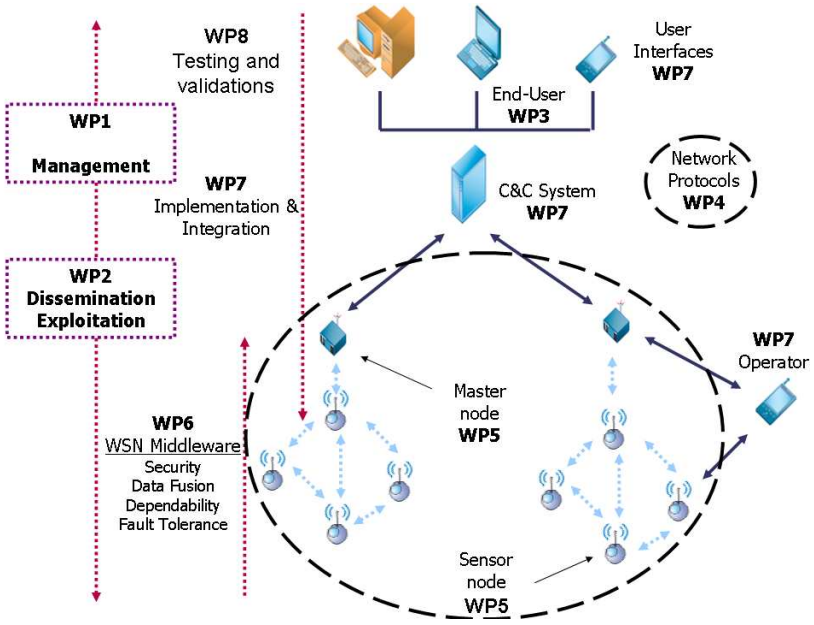

Figure 1 - EMMON system overview and work package decomposition

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.
- T4.4: Data aggregation.
- T4.5: Security.
- T4.6: Communication Test Lab.

4. Methodology Used For Evaluation

In order to evaluate the solutions so far proposed in literature as well as inferring useful information from past and recent projects, we adopted the methodology described in Figure 2.

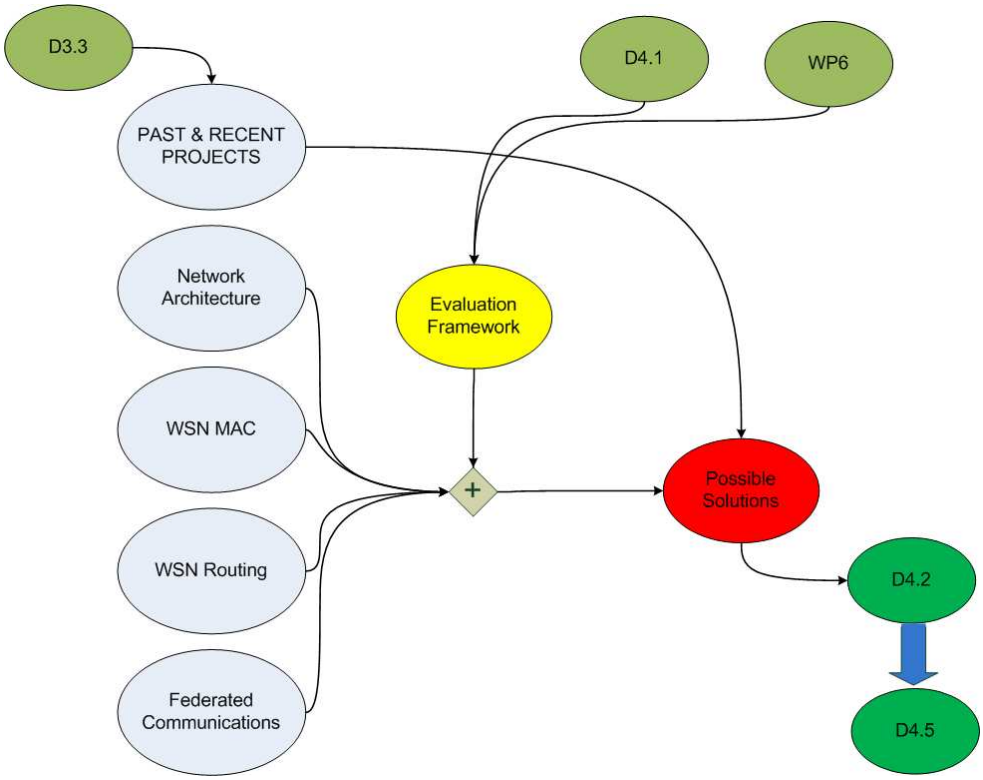

Figure 2 - Methodology used for inputs to this document

D4.2 [AD-4] presented a set of possible communication solutions by composing into a system stack the best options selected from a set of technologies for network architectures, communication protocols and federated communications following the evaluation methodology set out in D4.2. This deliverable, D4.5, builds on the work of D4.2 by evaluating the proposed solutions in the context of the EMMON communication architecture. This document proposes a multi-tier communication architecture for EMMON on the basis of end-user requirements and the lessons learnt from real world deployments of the stack components selected in D4.2. This methodology works as follows. We first present an overview of the technologies and solutions proposed in D4.2 for the network architecture, short-range communication technology, WSN routing protocol and the long-range communication technology. We then consider the end-user requirements to derive some typical deployment scenarios. This is done in order to determine the maximum and minimum deployment densities and the communication range of the nodes in typical deployments. Using this as an input, we then select a multi-tiered communication architecture that will be used in EMMON deciding on the number of tiers, what tiers can communicate with each other directly, the communication technologies used and the approximate ratio of nodes that can to be deployed at each tier. We then decide on addressing and the packet formats used at each tier and we give consideration to additional

issues that may be important such as energy and geographical awareness, traffic differentiation, congestion and flow control and security in the network.

5. Overview of Solutions Proposed By D4.2

This section presents an overview of the technologies and solutions proposed in D4.2 for the network architecture, short-range communication technology, WSN routing protocol and the long-range communication technology.

In the deliverable D4.2 [AD-4], the most prominent solutions at different layers, like WSN architectures and communication protocols, have been evaluated against a set of criteria. To achieve this goal, a methodology has been defined to select and rank such criteria, moving from the definitions presented in the deliverable D4.1 [AD-1] and by applying the best practices derived from the analysis of past and recent projects, dealing with medium to large scale WSN deployments for real world applications. In particular, we have inferred the lessons learned from the most important projects we have found in the literature, which aim at developing applications for medium to large scale WSNs and at addressing issues ranging from environmental monitoring (e.g. CitySense [RD-1], SensorScope [RD-9]) to surveillance systems (e.g. Exscal [RD-4], VigilNet [RD-10], [RD-11]) or disaster recovery (e.g. Aware [RD-29], Runes [RD-7]), or ranging from real world deployments to testbed development (e.g. SensLab [RD-8], Cruise [RD-6]).

The analysis conducted in [AD-4] constitutes the starting point for the present deliverable D4.5 to derive an appropriate network architecture, to achieve efficiency in large scale and dense WSNs for the EMMON purposes. The main output of [AD-4] is summarized in Figure 3. In particular, a set of alternative networking stacks for EMMON have been identified, having the common features to be characterized by

a. A multi-tier (eventually backbone based) architecture, which we showed to be far the best network architecture for our purpose, thanks to the flexibility it offers.

b. The IEEE 802.15.4 and IEEE 802.15.4a communication standards, which we identified as the best options for MAC and Data Link Layer technologies.

Furthermore, while it is expected that adopting the IEEE802.15.4 standard would have been a natural choice for short range communication technologies, typical in WSNs, the use of a multi-tiered architecture raises a number of questions to be solved in the present work, both in terms of the number of tiers (and therefore the number of communication technologies to choose) and the type of nodes at each tier (and for example, whether those are connected to some kind of external power supplies or not, which affects the available communication technologies).

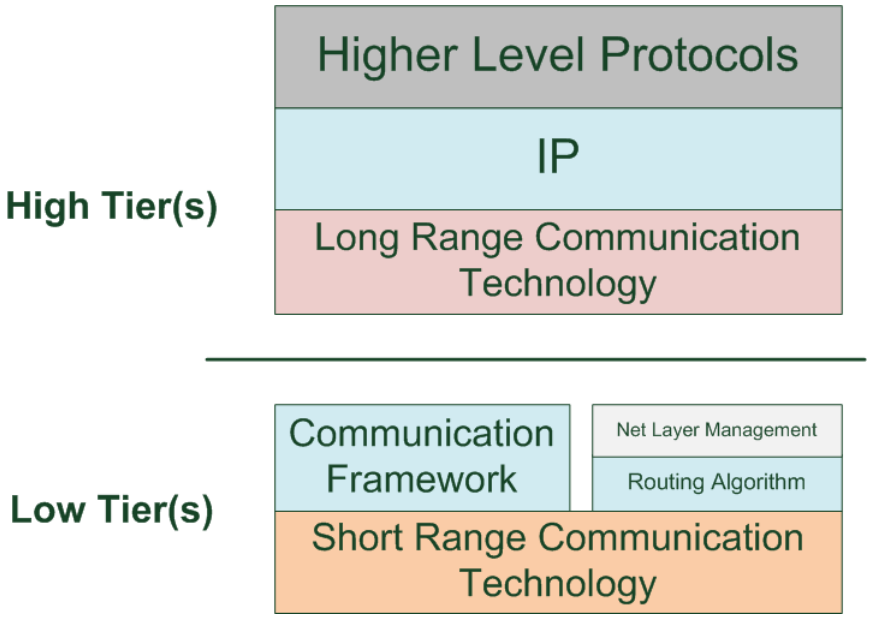

Figure 3 - Multi-tier alternative schemes.

Following the scheme of Figure 3, the communication stacks proposed earlier in D4.2 included the implementation at the low tiers of the Collection Tree routing Protocol [RD-17] or even a simpler cluster-tree routing protocol (e.g. ZigBee-based) at the Network Layer or a 6LoWPAN-based framework [RD-21] above the IEEE802.15.4 Data Link Layer. For the higher tiers of the system, the only assumption we made is that IP is explicitly used as the base networking protocol and one of the alternative solutions foresees one or more gateways, composed by e.g. WiFi or GPRS-enabled devices for long range communications, forming a backbone or able to communicate with a remote C&C host over an IP based internet connection. Nevertheless, the goal of D4.2 deliverable was to explore the advantages of different building block technologies and the alternatives proposed represented only the starting point from which the present deliverable will derive a fully functional network architecture.

6. Deployment Considerations

In this section, we consider typical deployment scenarios and the constraints that are placed on the network architecture and the specification of the multi-level communication protocols due to deployment considerations. There are a number of deployment-related issues that have a bearing on the network architecture and communication protocol design. The answer to some of these questions can be derived from the characteristics of the applications targeted by EMMON. For the others, we endeavour to present what we consider to be the reasonable options that are open to the consortium, how each will affect the design of the communication protocol and architecture and finally what we consider to be the most suitable solution for a large-scale WSN, and the reasoning behind our choice.

6.1 Clustering

We have chosen a clustered architecture for tier 0 nodes because clusters [RD-30]:

a) Help localize routes and reduce the size of the routing table (though this may not be relevant if our solution does not support horizontal routing, see Section 6.6).

b) Conserve bandwidth.

c) Cut the overhead associated with topology discovery and maintenance.

d) Prolong battery life through duty cycling.

e) Result in a reduction in coverage redundancy, medium access collisions, transmission range required and/or number of hops required to reach the sink.

6.2 Node Placement

An important determinant in the design of the communication protocol is whether the physical sensor deployment is going to be deterministic or random. Will the operators have approximate control over where the sensors are placed or will the placement be completely arbitrary? First, none of the requirements gathered from the end users includes random node placement [AD-3]. In addition, all of the large scale deployments we are aware of (such as [RD-4], [RD-27], [RD-5] and [RD-11]) have involved more or less precise control over where sensor nodes are placed. While random deployment of nodes is appealing in theory, in practice there hasn't been any large scale (>100 nodes) deployment that used random scattering of nodes. If nodes are randomly scattered it is quite possible that some nodes are unreachable or have to use a very high transmission power resulting in the battery running out much faster than other nodes. **We therefore assume that in EMMON we will have some control over node deployment and will thus be able to ensure that nodes are relatively evenly spread and that cluster heads in particular are placed in order to maximize network connectivity[1].**

[1] [RD-54] reports an overview of algorithms proposed in literature to solve the Optimal Node Placement problem. The aim of Optimal Node Placement is to calculate how to place further nodes on the field in order to achieve a k-connected newtwork.

6.3 Deployment Area and Density

One of the goals of EMMON is to design protocols that will allow networks of at least 10,000 nodes to be deployed over areas as large as 50km^2. Assuming that the nodes are evenly distributed, a deployment of 10,000 nodes over an area of 50km^2 will result in one node per 70x70m^2. The analysis in D4.2 [AD-4], corroborating the current state of practice in WSNs, concluded that IEEE 802.15.4 or 802.15.4a are the best options for MAC and Data Link layer technologies. However, 802.15.4 is a short-range communication technology and if the sensor network is deployed over a large physical area, network connectivity becomes an issue. While commercial 802.15.4 transceivers claim line-of-sight ranges of up to 500m (and 1450m in the case of Atmel[2]) and this should be sufficient to construct a fully connected network, in practice the operational range of 802.15.4 nodes is much less and obstructions to line of sight significantly reduce the maximum communication distance to a few tens of meters at most.

The deployment density of nodes also affects how many nodes are within radio range of each other and how much energy a node will consume in order to reach its neighbouring nodes. If the deployment is sparse, additional steps may need to be taken to ensure that the network is fully connected. A sparse deployment also increases the chances that the failure of one or a few nodes will cause partitioning in the network. On the other hand, if the nodes are very densely deployed, this also increases the number of sensor nodes that would interfere with each other's transmissions. Thus, the deployment must balance radio range (and transmission power) with the average distance between nodes. While the specific deployment density will be application-specific, EMMON targets dense, large-scale WSNs, and **we therefore assume in this deliverable that a fully connected network (i.e. a network where at least one path exists between any two nodes) can be formed.**

6.4 Impact on Network Topology

The range of the radio transceivers and the distance between nodes also has an impact on the network topology choices that are available at each tier. If nodes are too far apart at any tier, they cannot reach the node at the next higher tier in a single hop. Nodes at this tier could therefore not be arranged in a star topology and communication to the next tier would necessitate a multi-hop strategy. Using multiple hops at any tier adds to the overall delay in the network and conflicts with one of our objectives that is to provide quality of service guarantees and time-bounded delivery of urgent data (i.e. alarm notification) within the network. Hence the density of node deployment can have a bearing on QoS and "real-time"[3] delivery guarantees.

Since EMMON targets applications with dense deployments and timeliness requirements, we will assume in the following that the density is sufficient to warrant the use of star topologies.

6.5 Cluster Head Node Type

As explained in Section 6.1, we have adopted a clustered network architecture at the lowest tier. Another important consideration in the communication protocol design is whether the

[2] http://www.atmel.com/

[3] Here the notion of "real-time" should be intended as "low latency" or equivalently "low end-to-end delay", where the word "low" refers to the requirements in [AD-3], e.g. up to 30s for a notification after an event triggered an alarm.

Cluster Head (CH) is a special node that is more powerful (in terms of processing and memory capabilities and/or other resources such as energy) than ordinary sensor nodes or the CH is selected from ordinary sensor nodes. Selecting the CH from amongst ordinary sensor nodes of the cluster provides us with homogeneity of nodes thus reducing network complexity as well as additional flexibility and fault tolerance as the failure of a CH is not a catastrophic event and another CH can be selected from within ordinary sensor nodes. Many algorithms such as LEACH [RD-18] also provide means for rotating the role of the CH amongst the nodes within a cluster.

If the deployment is deterministic, however, it can be argued that it makes sense to have a more powerful CH as its placement can be decided *a priori* to ensure that the network is connected and clusters of the right size are formed. If the CH is more powerful, it allows for greater processing as it has extra capabilities to perform data aggregation or sensor fusion. It also helps network longevity as all communication from a cluster is routed through a node that is more powerful. However, this topology is more vulnerable to CH failure which can disconnect the entire cluster (unless all nodes in the cluster are within range of adjoining clusters).

A third alternative is to use ordinary sensor nodes as CHs but to fix the ordinary sensor node that is going to act as the CH within each cluster and to equip it with a larger energy reservoir to compensate for the extra functions it has to perform (and thus the extra energy it consumes) in its role as a CH. This option preserves node homogeneity but has the disadvantage of not being as fault tolerant, as well as not having the option for the CH to perform sensor fusion and data aggregation.

Finally, it is possible to use combinations of the above listed alternatives. For example, we could choose the alternative to have a more capable node acting as a cluster head at the beginning but in case of node failure, we could fall back on the alternative where the cluster head is chosen from ordinary sensor nodes.

Given the operational requirements of the project and the final decision on using the TelosB WSN platform as the hardware, we have decided to preserve node homogeneity by using the same hardware for the CH but provide it with a more powerful battery to compensate for the extra communication responsibilities.

6.6 Data Flow

The flow of data within the network plays an important role in determining the optimal communication protocol. In EMMON, we must consider whether data travels horizontally within the same tier. Is there ever any need to route packets from a node in one cluster to another cluster or from one CH to another CH except in order to route the packet to a gateway or the Command and Control centre (C&C)? Given the type of applications targeted by EMMON, and since no end-user expressed any requirements for horizontal communication, [AD-3]**, we will assume that no horizontal data flow is required. Therefore, EMMON will only support communication from nodes to C&C, for sending data, and from C&C to nodes, for queries, commands, OTAP etc.**

7. Multi-tiered Architecture

7.1 Introduction

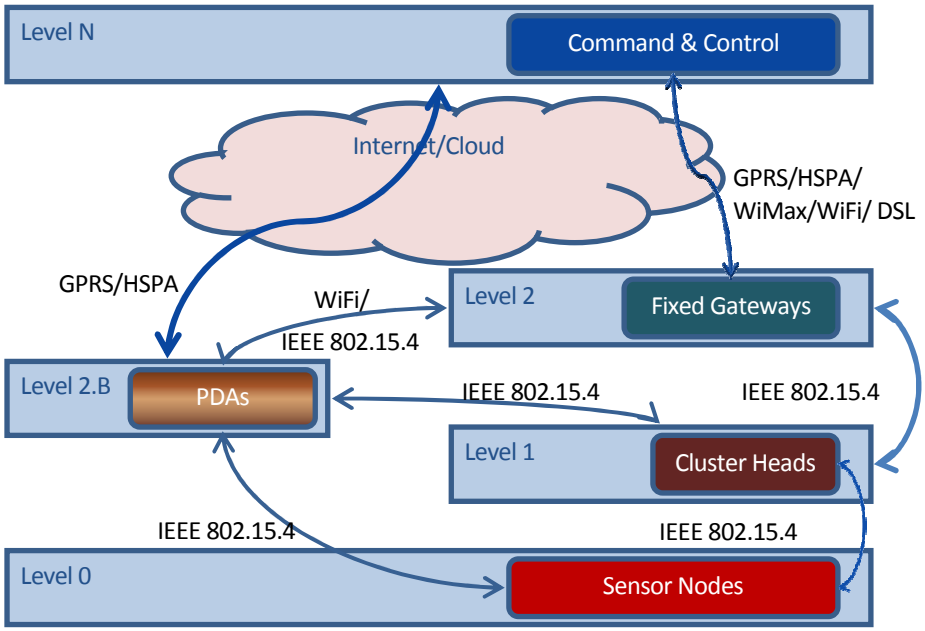

Figure 4 - Multi-tiered communication architecture

We propose the network architecture shown in Figure 4 displaying the different tiers at which devices are present in the network and the communication technology that devices at each tier would use. Level-0 consists of simple wireless sensor nodes, which perform sensing tasks and deliver data to the devices at the next level in the hierarchy using an IEEE 802.15.4 communication stack. These cheap devices cannot communicate using any other communication protocols due to the absence of any other type of radios.

At level-1, cluster heads are responsible for controlling and duty cycling of the sensor nodes within their respective clusters. These cluster heads may also be responsible for data aggregation and sensor fusion. The cluster heads may be somewhat more powerful than ordinary sensor nodes in terms of computational capabilities, and they might have better energy reserves or be powered by an auxiliary energy source such as solar power (see the discussion in Section 6.5). These cluster heads also communicate using IEEE 802.15.4 only.

At level-2 of the network hierarchy, fixed gateways are present. These are devices that have the highest computational capabilities among the devices present in the sensor network field. These fixed gateways are assumed to not be energy constrained (e.g. line-powered or equipped with some sort of long-life batteries and energy scavenging mechanisms). Fixed gateways are assumed to have a direct connection to the C&C at level-N when the C&C is physically close to the sensor field or a connection through the Internet when the C&C is remotely located.

At level-2.B we classify devices like smart phones as portable C&Cs. These devices typically have much better computational capabilities and more power reserves than the level-0 and level-1 devices and are expected to have more than one type of radio. They must have an IEEE 802.15.4 radio so that they can communicate with sensor nodes and cluster heads, but they also have additional communication capabilities to allow them to communicate with fixed gateways and remote servers (e.g., through the Internet) directly.

7.2 LEVEL 0: Sensors Nodes

Starting from the bottom of the network architecture, a WSN Node entity, like in Figure 5, is shown. Based on this view, a communication / computation enabled device is physically linked by wires to a given number of sensors for environmental data readings. These sensors correspond to devices measuring different physical parameters like e.g. ozone, temperature and humidity and are typically on-board on the WSN node. The specification of the required communication primitives at this level is in the WP5 deliverables, in particular D5.3 [AD-5], concerning the integration of HW platforms and SW drivers.

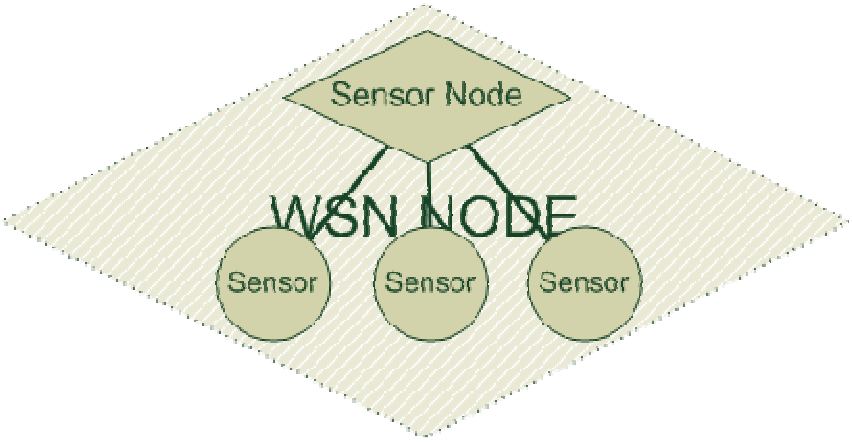

Figure 5 - Network Architecture - WSN Node

Many WSN Nodes are subsequently grouped into one WSN Cluster, like in Figure 6.

To maintain a low level of complexity, at this tier of the Network Architecture we foresee a Star Topology-based scheme among the WSN Nodes and one Router/Cluster Head, i.e. the WSN Nodes do not communicate over a wireless medium directly each other, but are in communication with another device acting as coordinator.

At this tier we intend to use a short range communication technology and, based on the evaluation performed in D4.2 [AD-4], the best candidate solution at this tier is using the IEEE802.15.4 communication standard. In particular, no routing algorithms are needed at this tier and the Cluster Head node acts as a local coordinator.

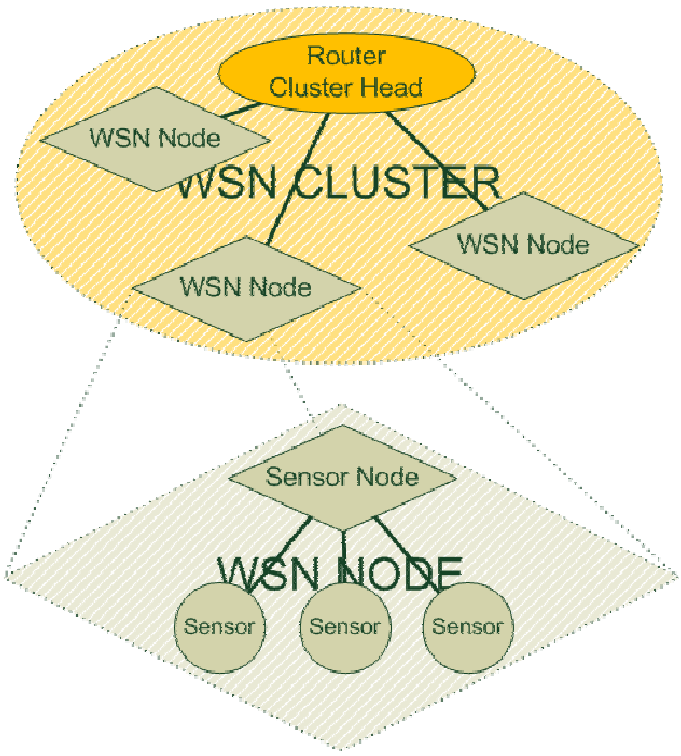

Figure 6 - Network Architecture - WSN Cluster

An example scenario where this architecture is really useful is in a noise monitoring scenario in the frame of Urban Quality of Life[4]. We can imagine that high-quality microphones are placed in strategic points in the city. We know that the main problem in evaluating a noise level is to filter out the additional noise introduced by the wind and rain ([RD-31], [RD-32] and [RD-33]). As a consequence, having a network architecture that provides local values of wind speed and direction, temperature and rain all around a highly-sensitive microphone might help in filtering out such undesirable disturbances from the acquired noise level either in-network (in a sort of sensor fusion mechanism) or off-line.

7.3 LEVEL 1: Cluster Heads

The Star topology adopted in the WSN Clusters has some disadvantages that offset its simple and fully controllable nature with some restrictions in terms of flexibility and a single-point of failure on the central node. To overcome this rigid infrastructure, many WSN Clusters will be connected with each other in a mesh physical topology to form a WSN Patch, where a common Sink/Gateway is in charge of gathering data and sending them over long range communication technology (e.g. WiFi) to a remote C&C (Figure 7).

As a consequence, in terms of HW platforms, the Cluster Head node will be the same platform as a generic WSN Node (e.g. a TelosB [RD-34]), with a larger energy supply. While

[4] Similar considerations may apply also in the ozone monitoring scenario [AD-3], where nodes are deployed all around the already existent monitoring stations.

communication robustness mechanisms are out of scope of the present deliverable and will be dealt in D4.10, in this architecture scheme two basic hypotheses have been assumed[5]:

- Any WSN Node (or at least a very large fraction of them) belonging to a WSN Cluster is able to attach to at least one other neighbour (i.e. one hop distant) Router / Cluster Head;
- Any Router / Cluster Head is able to communicate within the WSN Patch with at least two other Cluster Heads directly (i.e. it is in the communication range of at least two others).

Besides the mesh connectivity graph, which allows the WSN Patch to implement robustness mechanisms for improving the network performance, the logical topology we advocate is tree-based. In particular, from the analysis conducted in D4.2, the following options were identified:

- (ZigBee) Cluster-tree network model;
- 6loW(P)AN framework + Collection Tree routing Protocol (CTP).

The cluster tree protocol has the advantage of being a well-known protocol, with a very simple addressing mechanism, which encodes the node level in the tree. Furthermore, several deterministic analytical tools are available to determine the worst case end-to-end delay and the worst case routers' buffer sizes [AD-13], [RD-16], [AD-14].

Besides its simplicity in networking, the Cluster-tree network model suffers from a rigid infrastructure and the absence of flexible robustness mechanisms for dynamic nodes re-association. In fact, even if this model has a mechanism to overcome the problem of recovering orphan nodes [RD-35], [RD-36], i.e. nodes which do not have a connection to their parent up to the gateway, it doesn't allow for dynamic prevention of this event to occur. In other words, at present it doesn't provide mechanisms to evaluate in real-time, the degradation of the wireless link to the current parent in the tree and switch dynamically to a better neighbour parent before falling into the "orphan status". Such mechanisms fall into the duties of robustness task and are out of scope for the present deliverable.

Furthermore, another drawback of this network model is that the beacon broadcasting strategy for time synchronization is not very reliable as the number of levels in the tree topology grows. Real tests conducted on TinyOS-based platforms [AD-14], have shown that the depth of the tree should be contained to no more than two or three hops for acceptable networking performance. Indeed, this limitation is currently related to the TinyOS operating system running over the test-beds used so far. TinyOS is non pre-emptive, which means that tasks run until completion, and this makes it difficult to handle precise beacon scheduling mechanisms when several beacon periods have to be interleaved with respect to the levels (depths) of the tree[6].

[5] Note that both these hypotheses affect the node deployment strategy and, eventually, the design and implementation of dynamic Cluster Head election mechanisms, by imposing further constraints on the set of eligible nodes.

[6] Novel works are ongoing at this time with a different set of platforms with a real time operating system, like ERIKA [RD-37] but this is out of scope of this deliverable and the current maturity of this technology is still insufficient to be used effectively in this project.

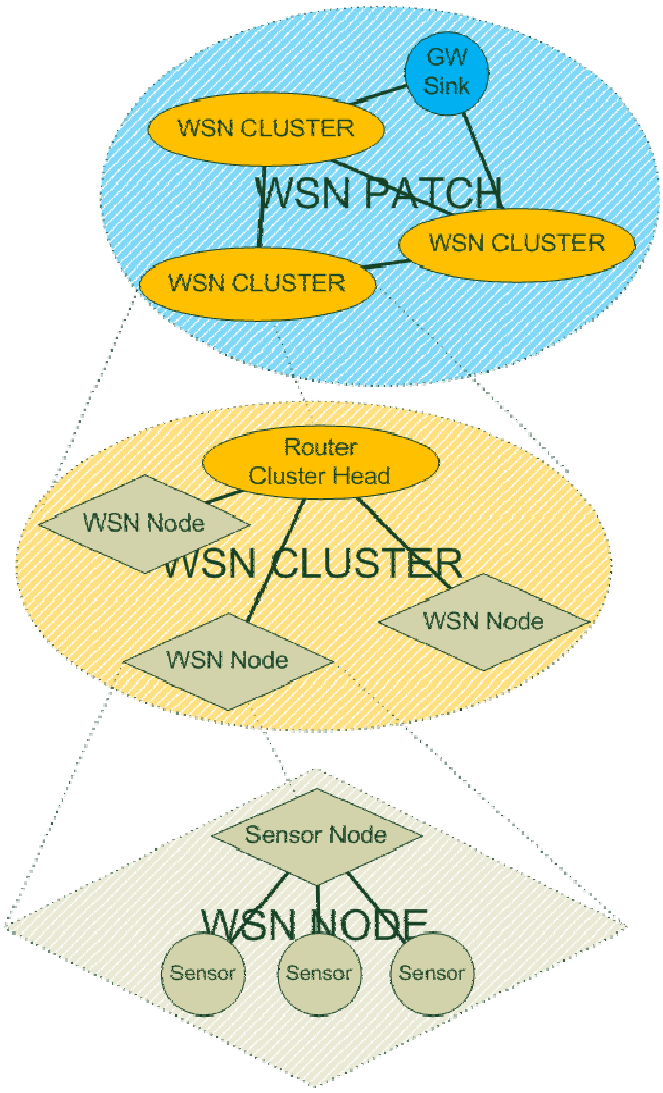

Figure 7 - Network Architecture - WSN Patch

On the other hand, using the CTP routing protocol with 6loW(P)AN allows for a quick and dynamic path re-configuration based on the ETX link quality estimation metric [RD-17], which improves the robustness of the network, but leads also to a lower level of determinism in estimating the bounds for the maximum end-to-end delays and dimensioning node resources. Besides that, there is an intrinsic difficulty to synchronize the nodes: putting them into sleep states at the same time and organizing the inter-clusters and intra-cluster communications based on either time-divided or frequency-divided basis. Furthermore, the standardization of 6loW(P)AN is still in progress and all the implementations found (like [RD-22], [RD-24] and [RD-38]) are subject to limitations.

For these reasons, **we propose to use the Cluster-tree network model, having the GW/Sink as a root[7].**

[7] Actually, in [AD-14], the GW/Sink node might even be a node in the tree without forcing it to be the root of the tree, but at this moment in the frame of this project this is not considered.

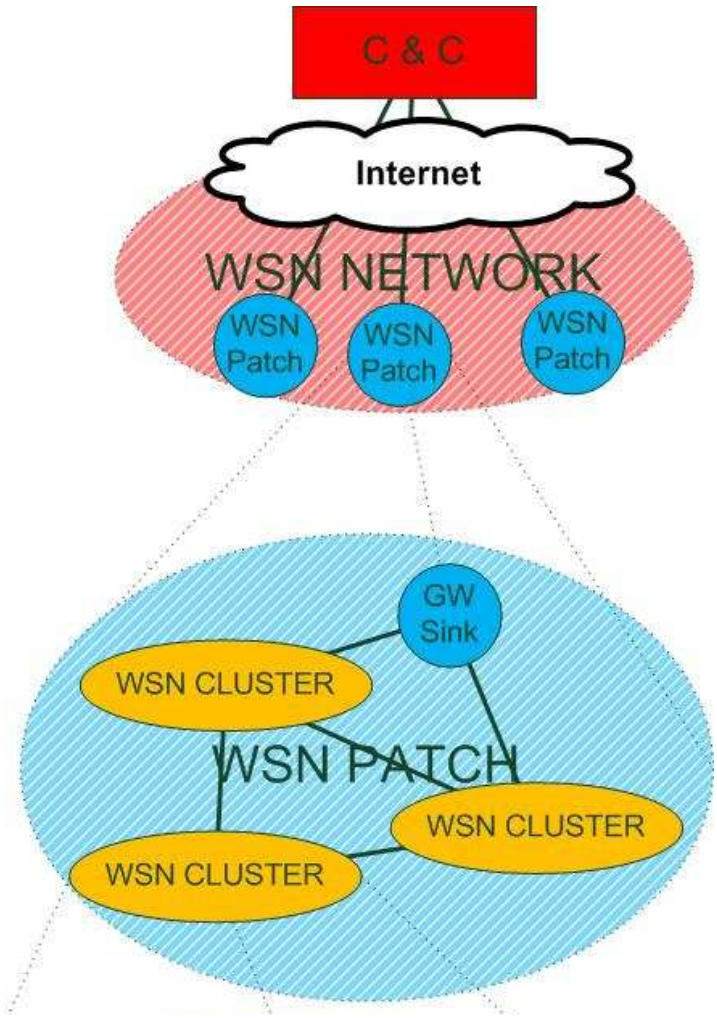

Figure 8 - Gateways connect to the C&C over the Internet

7.4 LEVEL 2: Fixed Gateways

There are two main alternatives for the topology at the highest tiers of our network architecture. The gateways can be connected to the C&C over the Internet using a long-range communication technology which may be a) wireless, such as GPRS or HSPA using a commercial mobile telephony network or b) wired, such as a DSL connection or even a leased line. This is a star topology shown in Figure 8 and is unavoidable in those scenarios where the C&C centre is far away from the sensor network field (e.g., in the forest fire detection or the precision agriculture scenarios). An alternative is to go for some long range wireless radio bridge-based solution. However this may require licenses to use these frequencies and is thus considered unfeasible.

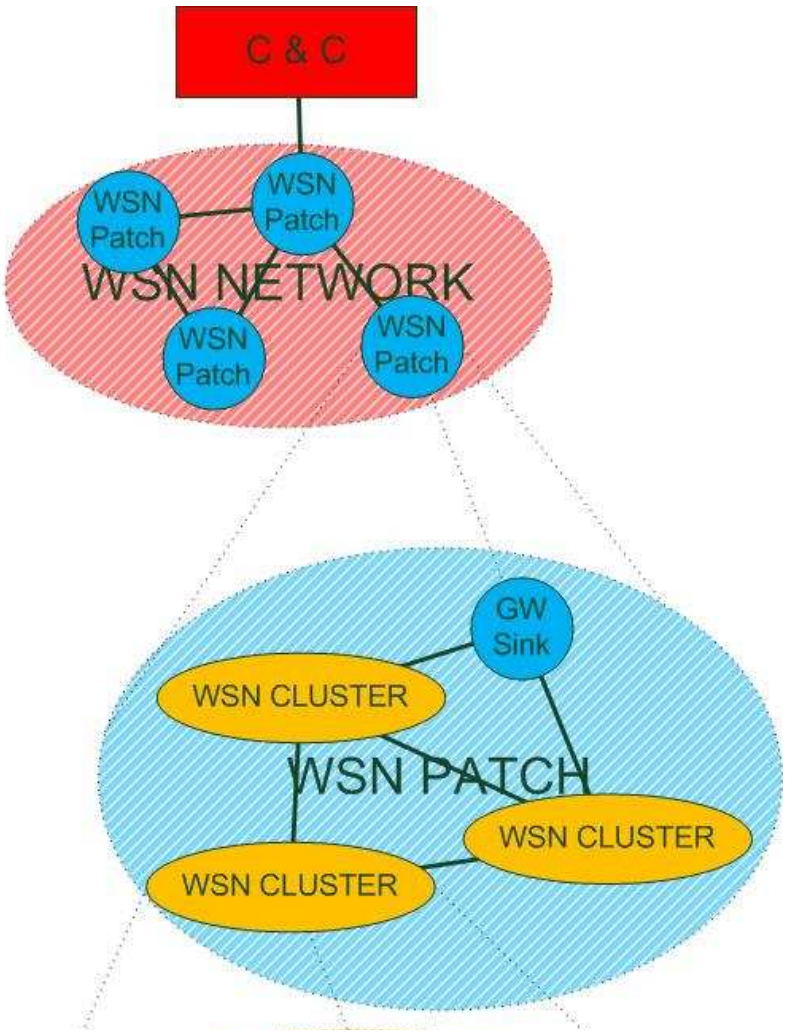

Figure 9 - C&C and gateways form a mesh network

If the C&C centre is located within the sensor field and can be reached using short-range wireless sensor technologies such as WiMax or WiFi, this would result in a mesh topology of gateways shown in Figure 9, when the C&C is *in-situ* with the WSN field (let us imagine the Urban Quality of Life scenario) and the C&C may be able to connect directly with one or more nearby GWs. In this case, all the gateways and the C&C centre together will form a mesh network and use mesh routing protocols. This solution may require some C&C "intelligence" to be implemented on gateways.

Using the Internet to route traffic between the gateways and the C&C leads to some open questions with regard to timeliness as the Internet is a best-effort network and if we have some constraints on the maximum delay in an event being notified to the C&C, we need to get a quantitative measure of the delay incurred in sending this notification from the gateway to the C&C within some confidence intervals. Moreover, sending traffic over the Internet also raises some security considerations. However, in the majority of the cases the Internet will likely be used to send traffic to the C&C. The requirements from WP3 [AD-3] are for a communication protocol from the sensors up to the GW and the final connection with the C&C depends on the specific application scenario and the end-user availabilities such as buying a dedicated service or situating the C&C within the wireless sensor network mesh.

7.5 LEVEL 2.B: PDAs

In a network scenario such as EMMON, PDAs and other portable devices can be used for several purposes. A primary purpose of PDAs would be to perform local maintenance. It could be used to configure individual nodes. It could also be used for Over The Air Programming (OTAP). The PDA could also act as a data sink, so that sensor data may be delivered to it and the user could have a portable C&C centre on his/her PDA. These applications could then be used for decision making or even for some actuation by interacting with the environment and the sensor field locally. An example of this would be the forest fire scenario where a fire-fighter could be equipped with a PDA that collects data from nearby sensor nodes and/or from the main C&C in order to get an understanding of the situation on the ground which is displayed on a portable-C&C on the PDA.

If PDAs are equipped with 802.15.4 transceivers, they can communicate directly with sensor nodes and cluster heads. The PDAs can also communicate directly with gateways and the C&C using a long range communication technology, most likely to be GPRS or HSPA to the mobile telephony network followed by communication over the Internet.

Another purpose for which the portable devices could be utilized is to act as mobile gateways enabling communication with different parts of networks. In the second case, the gateway software works in the background, without intervention from human users or operators, and facilitates data delivery from sensor network to remote sites. [RD-28] reports network capacity gains when such mobile gateways were present in the wireless sensor network. We could use these mobile gateways for packet delivery to improve network performance and maybe even conserve energy consumption of the intermediary nodes, whenever such portable devices are available.

These mobile gateways can also facilitate fault-tolerance mechanisms in situations where a cluster head's battery depletes and the cluster head does not remain operational. In this instance, the sensor data can be acquired using one of the mobile gateways present in the sensor field in an opportunistic manner: i.e., if the sensor nodes are operational themselves but the cluster head has depleted, the sensor node can send data to the destination by using one of the portable devices as gateway or intermediary node.

Following on the conclusions in the deliverable D7.1, it has been decided to consider PDAs as mini C&Cs but only for the role of network management, i.e., to detect anomalous conditions such as low connectivity between nodes, isolated nodes or a partitioned network, to update the firmware or the configuration (such as alarm thresholds) of the sensor network. However, in the case of alarms and emergency conditions PDAs may perform additional roles including some sensing.

7.6 Command and Control

As discussed in the previous section, the Command and Control centre (C&C) can be situated either remotely at a distance from the sensor field and thus only be reached over the Internet or it may be situated within the sensor field so that gateways can communicate with the C&C over a wireless mesh network. In addition to communicating with the gateways, the C&C should also communicate with PDAs either to provide them with data to enable the PDAs to function as portable-C&Cs or to act as a secondary route from the clusters in case of gateway failure. Since the PDAs are likely to be equipped with GPRS/HSPA technologies, the C&C must be connected to the Internet to allow the PDAs to reach it.

8. Addressing

There exists a wide range of devices in a wireless sensor network such as EMMON, ranging from low power sensor nodes to high power fixed gateways, portable devices (PDAs) and Command & Control centre as discussed in section 7 of this document. The problem of addressing however lies chiefly in the addressing scheme for sensor nodes and cluster heads. While allocating addresses to these devices, we must consider that these devices have to be reached from the Command & Control centre as well as fixed gateways and portable devices. The devices at higher tiers (gateways and Command & Control centre) do not use the same communication protocol as the wireless sensor nodes and cluster heads. Therefore, we identify an addressing scheme for the lower tier devices (wireless sensor nodes and cluster heads), which will communicate using the IEEE 802.15.4 standard and the address translation mechanism, such that these lower tier devices could be accessed by the higher tier devices present in the network. The higher tier devices will be allocated IP addresses so that they could be easily integrated with the internet, in order to cover large geographical distances.

8.1 Addressing Scheme

As we decided to use the IEEE 802.15.4 standard as decided in [AD-4] at the lower tier devices in a cluster tree topology, we see two options available for addressing scheme on sensor nodes and cluster heads, based on the aforementioned standard:

- 16 bit PAN/Cluster ID and 16 bit individual node ID
- 16 bit PAN/Cluster ID and 64 bit individual node ID

In the first option, 16 bit addressing for the node seems to be sufficient as a single cluster may only have a limited number of devices associated with a single cluster head and this number may not exceed the upper limit of 65,535 devices per cluster. Theoretically, the number of clusters themselves may become a bottleneck as we can only have 65,535 clusters in the network. While this is unlikely to be the case in EMMON, it is possible to re-use the PAN ID over distant geographical areas, where a geographic area is serviced by a certain fixed gateway. This fixed gateway will be responsible for assigning PAN ID to each cluster, or inversely when a cluster is formed the cluster head (PAN Coordinator) will request a PAN ID from the fixed gateway. The interface of fixed gateway that will communicate with lower tier devices (cluster heads in this case) will be assigned a parent PAN ID either at the time of deployment or dynamically from the centralized Command & Control centre.

In the second option, the problem with the number of clusters that we can have remains the same as before and the recommended solution remains the same as well. However in the second case, we can have a huge number of devices per cluster. This availability of a huge number of devices (2^{64}) may never become a reality in a single cluster, as a single cluster head may never be powerful enough to control that many devices. Also, having this many devices per cluster would require the deployment to be extremely dense, due to the short communication range of devices communicating on IEEE 802.15.4. This dense deployment will however introduce many other problems in communication including frequent packet collisions. Due to these reasons, having 64 bit addressing per device resulting in so many devices per cluster seems like a waste of space in the packet and limited memory per device. These 48 (64-16) additional bits per packet may be utilized elsewhere, resulting in better value.

8.2 Address Translation

As mentioned earlier, using one of the addressing schemes described above, we would need a mechanism to translate the above mentioned addresses into IP addresses. This is due to the fact that the devices at the higher tiers (Fixed Gateways, Mobile Gateways and Command & Control centre) will work on IP (Internet Protocol), whereas sensor nodes and cluster heads will work on ID based addressing scheme. If the addresses of sensor nodes and cluster heads are dealt with as IP addresses as conceived in 6LowPAN ([RD-22], [RD-23]) (64-bit IP), the beacon mechanism and clustering mechanisms may not work properly, although this needs to be investigated in detail. We conclude that using 6LowPAN will add further complexity at all levels of the network.

On the other hand, sensor nodes and cluster heads may not recognize addresses of devices having IP addresses, while trying to send data to such devices, where sensor nodes and cluster heads themselves work on an ID based addressing scheme.

To deal with such issues, we propose using devices with two interfaces at the higher tier (Fixed gateways and mobile devices). One interface will have an IP address, which will be utilized in communication to and from other higher tier devices, while the other interface will have an IEEE 802.15.4 ID based address and will be utilized to communicate with the lower tier devices. The higher tier devices that wish to communicate with lower tier devices through a gateway will specify the address (ID) or lower tier device in the payload of the IP packet that they will send to the gateway. The gateway will then translate the packet for the lower tier device and send the translated packet to the device identified by the ID mentioned in the IP packet payload. The inverse mechanism will work while a packet is to be sent from the lower tier devices to the higher tier devices through the gateway. The Command & Control centre cannot directly communicate with the sensor nodes, having no direct link to the sensor field and must communicate via gateways present in the vicinity. We also assume that the Command & Control centre has knowledge about the geographic location of the gateways.

8.3 Address Assignment

Address assignment is a crucial part of wireless sensor networks. It deals with the mechanism as to how a sensor node or cluster head is assigned an address which uniquely identifies the device, according to the addressing scheme discussed in section 8.1. We have two options for assignment of addresses to individual devices, as listed below:

- The addresses could be pre-programmed before deployment
- The addresses are assigned dynamically by the next higher level device

In the first option, we would be able to identify each device individually without considering the cluster that the device is associated with or the physical location where the device is deployed. However, using this address assignment scheme means that we should be able to identify each device almost globally uniquely before deployment, as we will not be able to re-use addresses because we will not know to which cluster a node will actually belong, when more than one cluster exists in the same vicinity. In order to achieve this, the 16 bit addressing mechanism is not adequate as it does not provide enough unique addresses. Instead, we would be required to use a 64 bit addressing scheme i.e. unless we plan the deployment in detail and then re-use the 16 bit addresses among the devices and even assign clusters to each device before deployment. Using 64-bit addresses however, will increase complexity in routing packets to a certain device, as detailed routing tables would have to be maintained having complete 64-bit addresses of devices in addition to the path to follow in order to deliver packets successfully to the destination node. Note that storing such paths is a memory intensive function in itself, as each device along the path will have a 64-bit address, and many devices may exist along the path. This will increase memory usage by the routing algorithm. If we use 16-bit addressing with duplication of addresses and complete deployment planning in this case, then in our opinion we will not be able to support

portable devices having only 16 bit addresses, because portable devices may arrive in the vicinity where the same address is being used by another stationary or portable device.

In the second option, the size of routing tables could be minimized by keeping only partial information i.e. only keeping addresses of clusters and routing to the cluster head, where the cluster head will know how to deliver data to a particular device. Since we will be using a cluster tree topology as discussed in Section 7, this option seems to be more viable. However in this case, complexity related to dynamic address allocation will be introduced. Addresses to the sensor nodes will be assigned by the cluster heads, addresses to the cluster heads will be assigned by the gateways upon request of association by the cluster heads and addresses to the gateways may be allocated probably by the DHCP server with which the gateway is connected. Using the cluster tree topology and dynamic address assignment also means that all the traffic may have to be routed through the cluster head or next higher tier device [RD-39], resulting in an increase in the load at the next higher tier even when the source and destination exist in the same subnet, probably geographically close or within direct radio transmission range. However, it is reasonable to assume the use of a data centric routing algorithm for query dissemination and sensor reading collection (as with the position based routing assumed in Section 10), while addresses will still remain useful for network management purposes as discussed in [RD-42].

9. Packet Format

In order to achieve successful communication, it is of primary importance that a packet format is defined for a number of packet types. However, the packet types themselves, could only be defined based on the application or middleware requirements. This means that the final definition of packet types and packet format might be subject to change, depending on the functionalities required from the middleware and application. In this manner the input is required from WP6 [AD-6]. However, a few packet types and their sub-types that are envisaged at this stage, are defined below. Later section 9.2 discusses which IEEE 802.15.4 frames will be feasible to deliver certain packet types.

9.1 Packet Types

At the moment, we envisage five major types of packets that will be required in order to establish communication. A short description of these packets and their sub-categories is presented below. The detailed specification of certain types of packets however depends on the requirements generated by the middleware work-package WP6.

9.1.1 Control Packets

Control packets will be used by sensor nodes, cluster heads and other devices present in the network in order to control the network dynamics, behaviour, device discovery, route discovery etc. These control packets are further classified into sub-categories.

9.1.1.1 Active Advertisement

These packets will be used by devices at different levels in the communication hierarchy to advertise themselves. This feature is mostly required by mobile gateways that appear and disappear dynamically, to introduce themselves to the devices that are already present in the vicinity. These packets may also be used by devices that are deployed later than the devices that were deployed initially, so that the network could remain scalable or extendable throughout the network life. If these periodic advertisements are not received by the dependent devices of a certain device, then the dependent devices will assume that the device in question has left the network and probably is inaccessible.

9.1.1.2 Passive Advertisement

This type of packets will be used by the devices that wish to transmit data in order to discover devices that may be offering routes as intermediary nodes. Analogously, these packets could also be called device discovery packets, as their essential purpose is to discover devices in the vicinity before sending packets. This procedure is recommended here, so that new and more efficient routes could be discovered and the routing tables could be updated depending on the changing network environment. However, it should be done periodically and after the appropriate interval, so that the network efficiency and lifetime may not be compromised.

9.1.1.3 Time Synchronization

These packets will be used to synchronize time among the neighbouring nodes. In our opinion, the time at each device should also be synchronized with global time (GMT). Time synchronization is necessary so that alarms and reports may be sent in a timely fashion and if an event occurs somewhere, then the time at which the event occurred must be known as well in order to facilitate meaningful analysis at the C&C. The knowledge of time can also be used in the data aggregation e.g. to filter data and especially to recognize that an event occurred and

has been sensed by several nodes (to avoid sending multiple alarm notifications for a single event).

9.1.1.4 Error Report

These packets will be used for reporting some error in the neighbouring nodes e.g. if invalid sensor readings are detected. In addition, these packets could also be used to tell the neighbouring nodes that limited battery is left and the node which is transmitting this packet should not be picked as intermediary nodes by the neighbouring nodes. Also these packets may be used to convey information about a lost node to the neighbours by the node which has detected a lost node.

9.1.1.5 Route Request

The purpose of this type of packets is essentially to request for available routes for a given destination by the node that wishes to transmit data. However, as we are assuming a cluster tree topology, we might not need this type of packets because the communication will take place only through the next higher tier device, which will already know which nodes are in contact with it.

9.1.1.6 Route Reply

If a route to a certain destination was requested and the route is known by the neighbouring nodes, those neighbouring nodes will notify the requesting node of known and available routes to the destination using this type of packets. The availability of this type of packets in the communication protocol depends on the routing protocol and will only be implemented if the route request packets are implemented.

9.1.1.7 Cluster Membership

The availability of this type of packets is not decided yet as well. These packets will be used by cluster heads to advertise the nodes that are controlled by that cluster head (which is sending this packet) to other cluster heads. This is done, so that routes to nodes in other clusters may be built via cluster heads.

9.1.2 Acknowledgment Packets

These acknowledgement packets are not IEEE 802.15.4 acknowledgement frames. The IEEE 802.15.4 acknowledgement frames are used for acknowledging reception of data by the next immediate node. The acknowledgment packets defined in this section will be used for end-to-end feedbacks and acknowledgements.

This means that when a message is sent to a destination by a source node, the final destination node will acknowledge the reception of the message using this type of acknowledgement and this acknowledgement will be received by the original source node. By doing so, the routing algorithm will be able to validate a complete path and probability of choosing the same path again for the same destination node will increase.

This type of packets will also contain information such as:

- How much energy was used by a given path in order to deliver the packet
- How much time it took to deliver the packet to the destination from the given source

Using such end-to-end feedback will also enable a source node to infer the probability by which packets to a certain destination are delivered successfully.

Such acknowledgements are further subdivided into two categories:

9.1.2.1 Positive Acknowledgement

This positive acknowledgement will be sent by the final destination only upon successfully receiving a packet. This positive acknowledgement will hold the information that is mentioned above. The positive acknowledgement may take a path other than the path through which the original data packet was delivered. It will allow the source nodes to make better informed decisions in the future and will allow the routing algorithm to learn success rates through this feedback. In addition to this, we will be able to perform end-to-end optimization in terms of:

- Network energy consumption
- Average round trip time
- Data loss

Hence, routes that will minimize the above parameters and will be able to achieve multiple optimization objectives in terms of above mentioned parameters will have more probability to be selected.

9.1.2.2 Negative Acknowledgement

This type of acknowledgements will be used to identify broken links and propagate that information backwards along the path. This means that having this negative acknowledgement will reduce the probability by which broken routes may be selected, hence optimizing routing decision.

Since the purpose of this type of feedback is to report broken routes and links, such packets will have to follow the same path as that of original data packets.

9.1.3 Alarm Packets

These packets will be used to generate alarms at the sensor nodes and cluster heads as soon as an event of interest has occurred. The interest will be propagated by the Command & Control centre for a particular phenomenon and for a given geographic area. The geographic area may be resolved into a Cluster/PAN ID and a Device/Node ID by either Command & Control centre or gateway servicing the designated area or both. As discussed in section 10, this resolution of the geographic area into Cluster/PAN ID and Device/Node ID may be not be required when routing for data gathering is position based with no need for specifically addressing single nodes or groups of nodes by their addresses.

9.1.3.1 Set Alarm

These packets will be responsible for propagating interest for a particular phenomenon. For example, this packet may contain interest for fire detection or smoke detection in a particular geographic location. The interest or alarm could be defined to be triggered either at the sensor node level, cluster head level or even the gateway level. In this way, aggregated event trigger mechanisms may be incorporated over a geographic region. These packets may also be used to renew interests (e.g. changing the threshold limit for a particular alarm, say temperature, for a given area).

9.1.3.2 Remove Alarm

These packets will be used to remove interest for a particular phenomenon from a certain geographic region. This removal functionality may be required because the user's interests in a particular phenomenon has faded or may be because the alarm has become too redundant,

meaning a lot of nodes are reporting the same alarm. In each case, the interest in the given alarm may be removed from a subset of nodes, reporting it.

9.1.3.3 Alarm Triggered

These packets will be used by sensor nodes, cluster heads and gateways to report alarms to the Command & Control centre. The alarms will be triggered based on the interests propagated by the Command & Control centre using packets described in section 9.1.3.1.

9.1.4 Report Packets

These packets will be used to leverage the necessary data to generate reports from the sensor nodes and cluster heads periodically for particular phenomenon and for a given geographic area. The geographic area may be resolved into Cluster/PAN ID and Device/Node ID by either Command & Control centre or gateway servicing the designated area or both. This functionality will be used to acquire periodic information from the field especially when no alarms are generated and no user has queried the sensor network, thus keeping up-to-date sensing information in the system.

9.1.4.1 Set Report

These packets will allow the applications and middleware to configure sensor nodes, cluster heads and gateways to send periodic information about a particular phenomenon in a given geographic region. If the reports are required from the cluster heads and/or gateways, they will deliver aggregated information periodically for the geographic area that they are servicing.

9.1.4.2 Remove Report

These packets will allow the applications and middleware to remove the configuration from the sensor nodes, cluster heads and gateways as described in section 9.1.4.1. Once these configurations are removed, the devices will no longer generate periodic reports for the particular phenomenon in the given geographic region.

9.1.4.3 Triggered Report

These packets will be generated by the sensor nodes, cluster heads and gateways periodically depending on the configuration sent earlier as described in section 9.1.4.1. The report configuration will also hold the criterion upon which the report will be triggered. This criterion will possibly include the time interval after which a report should be generated and sent to the Command & Control centre.

9.1.5 Data Query Packets

These packets will be used by the application or middleware to query data from the sensor field in special circumstances. For example, when some details are required or more fine grained information is required where as no report provides that information. This functionality can also be used to make a one-off query or a query for fresh information, whereas reports may only arrive later or the reports already delivered may only contain old information. These packets can also be used by the devices in the sensor field to query other devices in the sensor field or by third party devices that require a type of sensing information for which the third party devices don't have their own sensors.

9.1.5.1 Data Request

These packets will be sent by the devices that wish to request fresh information from a particular node. As discussed above, this functionality will not be used to gather information periodically but will be used to request information that is not present in periodic reports or information from a different granularity level for the purpose of further analysis.

9.1.5.2 Data Response

These packets will be similar to report packets generated periodically. However these will be solicited messages, which will only be generated if requested. These packets are a consequence of the "Data Request" packets outlined in section 9.1.5.1.

9.2 Mapping Packets to IEEE 802.15.4 Standard

The packets that need to be delivered to destinations connected through a multi-hop connection to the source of the packet will be delivered using "Data Frames" of the IEEE 802.15.4 standard. However, the packets that have to be delivered only to the neighbouring nodes will be delivered using "Command Frames" of the IEEE 802.15.4 standard. Thus, routing will not be performed on Command frames, but only to the Data Frames.

In this way Alarm, Report, Data Query and Acknowledgement packets will be delivered using IEEE 802.15.4 Data Frames. Whereas, Control and Negative Acknowledgement packets will be delivered using IEEE 802.15.4 Command Frames.

9.2.1 Data Frame

Table 2 shows the fields that are required in order to deliver a packet. The fields in gray are the MAC layer header and footer fields of the Data Frame of the IEEE 802.15.4 standard. The description of these fields can be found in [RD-14]. The rest of the fields before the MAC layer footer (FCS) will be introduced by the network layer, in order to deliver data across multiple levels in the communication hierarchy.

Header - Data Packet				
Field Name	**Size(Bytes) Case 1**	**Size(Bytes) Case 2**	**Size(Bytes) Case 3**	**Comments**
Frame Control	2	2	2	
Sequence Number	1	1	1	
Destination PAN ID	0	2	2	Next Hop probably. Depends on routing.
Destination Address	0	2	8	Next Hop probably. Depends on routing.
Source PAN ID	0	2	2	original source
Source Address	0	2	8	original source
Auxiliary Security	0/5/6/10/	0/5/6/10/	0/5/6/10/	

Header	14	14	14	
Final Destination PAN ID	0	2	2	
Final Destination Address	0	2	8	
Time To Live	1	1	1	
MsgTypeAndFlags	1	1	1	Alarm/Report/Data/ACK
Fragment Sequence No.	1	1	1	Depends if fragmentation and reassembly is supported
MsgLen	1	1	1	In Bytes
Estimated Energy Consumed	1	1	1	Needed for end-to-end routing optimization
PAYLOAD - Data	n	n	n	Variable
FCS	2	2	2	
Total	10	22	40	
Max Size	127	127	127	
Remaining	117	105	87	Without Aux Security Header
Remaining Worst Case	103	91	73	With Aux Security Header

Table 2 - IEEE 802.15.4 Data Packet Header Format

Table 2 shows the number of bytes remaining for the data payload after the space used by the header and the footer in different circumstances. The security header is optional i.e. if the security is enabled at the MAC layer, it could occupy 5, 6, 10 or 14 bytes depending on the security features used by the packet. According to the IEEE 802.15.4 standard there are three modes of addressing (as discussed in Section 8.1), one of which is address free mode, which may not be very useful in the context of EMMON. Whichever addressing scheme is used, it should remain common across all types of addresses present in the packet and should not yield discrepancy among different address fields.

The final destination PAN ID and final destination address will uniquely identify the destination, which may be connected via a number of intermediary devices, whereas the destination address and PAN ID will identify the next hop device. In the case where a packet needs to be delivered to the gateway, the final destination address and PAN ID will identify the network interface of the gateway that communicates on the IEEE 802.15.4 standard.

The TimeToLive field identifies the number of hops or time duration after which the packet will be dropped if un-delivered.

The higher order 4 bits of MessageType and Flags field will specify the type and subtype of the packet contained in the payload. The lower order 4 bits will specify certain flags, e.g. bit-0 will be used to specify if the packet is fragmented or not, bit-1 will specify if this is the last fragment when the packet is fragmented. Bits 2 and 3 are reserved for future purposes.

The Fragment Sequence Number will hold the incremental sequence of the fragments, so that they could be re-assembled at the destination. This field will only be present in the packet, if the packet is fragmented and if fragmentation is supported.

The MsgLen field will contain the number of bytes in the payload being transmitted in the current frame or fragment.

The Estimated Energy Consumed field will contain the estimate of energy consumed by this frame at any given time. This field will be used to improve efficiency of the network, so that routes that consume less energy while forwarding a packet to a particular destination may be utilized more often.

9.2.2 Command Frame

Table 3 shows the fields that are required in order to deliver a packet. The fields in gray are the MAC layer header and footer fields of Command Frame of the IEEE 802.15.4 standard. The description of these fields can be found in [RD-14]. The command payload field will be used by the IEEE 802.15.4 MAC layer. In addition it will also be used by EMMON's customized network layer to deliver Control and Negative Acknowledgement packets to the neighbouring nodes.

Header - Command Packet

Field Name	Size(Bytes) Case 1	Size(Bytes) Case 2	Size(Bytes) Case 3	Comments
Frame Control	2	2	2	
Sequence Number	1	1	1	
Destination PAN ID	0	2	2	Next Hop probably. Depends on routing.
Destination Address	0	2	8	Next Hop probably. Depends on routing.
Source PAN ID	0	2	2	original source
Source Address	0	2	8	original source
Auxiliary Security Header	0/5/6/10/14	0/5/6/10/14	0/5/6/10/14	
Command Frame ID	1	1	1	
PAYLOAD - Command	n	n	N	Variable
FCS	2	2	2	
Total	6	14	26	
Max Size	127	127	127	
Remaining	121	113	101	Without Aux Security Header
Remaining Worst Case	107	99	87	With Aux Security Header

Table 3 - IEEE 802.15.4 Command Packet Header Format

Table 3 also shows the number of bytes remaining for the data payload after the space used by header and footer in different circumstances. The security header is optional i.e. if the security is enabled at the MAC layer, it could occupy 5, 6, 10 or 14 bytes depending on the security features used by the packet.

For the command frames, we assume that these packets will only be sent to the neighbouring nodes as discussed earlier in section 9.2 and therefore do not require final destination address as part of the packet. In this case the destination address and PAN ID will specify the neighbour node for which the packet is intended.

It can be seen that in the worst case where the maximum security is used along with 64-bit device addresses, 87 bytes are still available to carry the command payload, which is more than enough for the purpose of the control packets discussed in section 9.1.1. The IEEE 802.15.4 standard command frames use only a few bytes themselves in each of the available commands specified in the standard. Although as the discussion in section 8.1 suggests, we will be using 16-bit PAN ID with 16-bit device addresses, which means that even if maximum security header is used, the command payload will have 93 bytes, which seems to be sufficient at this stage.

10. Routing

In wireless sensor networks, while at the MAC and PHY levels of the classical ISO/OSI stack, the protocols and algorithms are now well standardized, at the upper tiers of the protocol stack there are still open issues and only recommendations from alliances like the ZigBee alliance exist (see [RD-20], [RD-43] and [RD-44]).

However, in our network architecture, we are assuming that the flow of the messages is only a point-to-multipoint downlink flow from the GW to the rest of the nodes (e.g. for asking the nodes for sensor readings or even propagate the new firmware for reprogramming purposes) and a multipoint-to-point uplink flow backward (e.g. for sensor readings report). Thus, only parent-child communication is really necessary[8] and simple solutions for routing can be applied, like the one proposed for ZigBee cluster tree, possibly enhanced with geographic awareness. In this case, a network like the one depicted in Figure 10[9] is proposed. We assume the Gateway is the root of the tree, and in general this device may also act also as a special CH, having its own WSN Nodes associated with it. For performance limitations, especially due to the beacon scheduling mechanism [AD-9], the depth of the tree should be constrained to no more than 3 hops. In Figure 10 we have considered a two hop tree where each vertex of the tree is a Cluster Head / Router (CH) node. As a consequence, each vertex is composed by a cluster of WSN Nodes, each of them having its own CH.

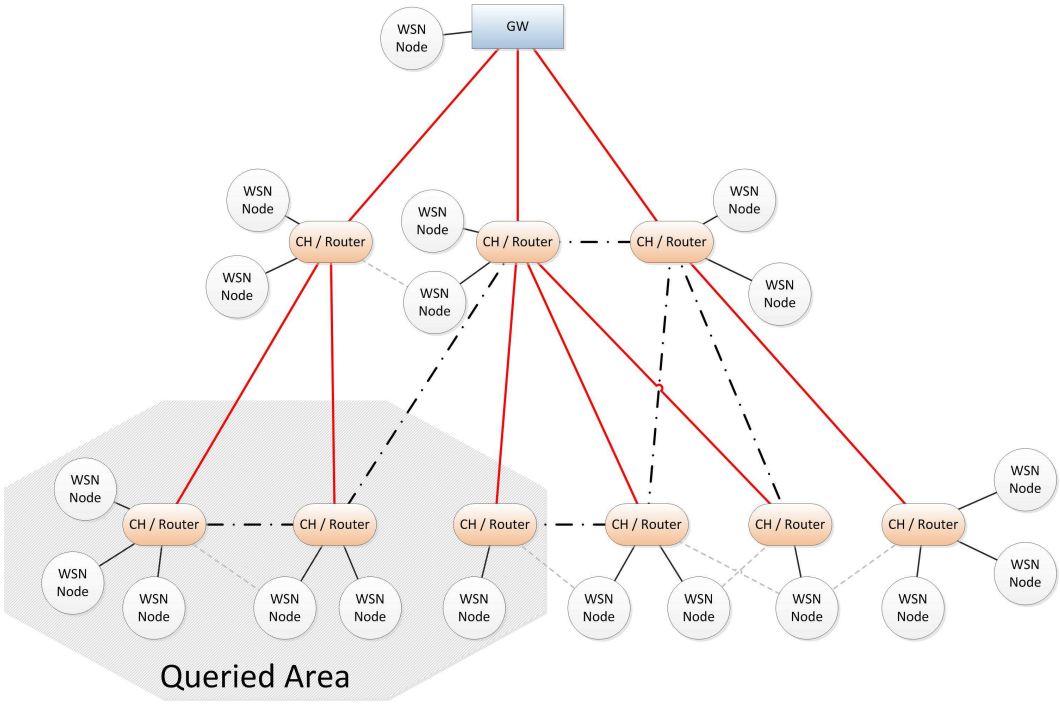

Figure 10 - Position based routing over a cluster tree topology within a WSN Patch

[8] If a node wishes to communicate with another node in the same WSN Patch, the message will follow the rigid structure of parent-child only communications, so reaching the appropriate level in the tree before to be sent to the final destination.

[9] The role of the Queried Area in Figure 10 will be clarified later in the document.

In Figure 10 we have represented the connections among the nodes using for the edges of the graph two different line types: i) the continuous lines indicate the final cluster tree topology, while ii) the dashed lines indicate that the nodes are in the communication range of each other, but they currently are not using that link. The presence of such redundancy in the links among the nodes constitutes the basis to implement any form of robustness for communication protocols against link and node failures. This issue will only be further addressed later in the deliverable D4.4 about communication robustness.

As a consequence, we might have some CH in the communication range with more than one CH and the same applies to the WSN Nodes. As a matter of fact, the final tree, where each node must choose only one parent among the alternatives it might have, would be formed assuming some convenient metrics, like the link quality (such as based on the LQE metric [RD-48]) and the energy available on the nodes. Nevertheless, we are convinced that this network architecture is flexible enough to allow us to foresee mechanisms for dynamically rebuilding the tree topology by periodically checking the status of nodes and links.

The association of WSN Nodes within a cluster and among the CH with each other up to the gateway will be performed following the standard procedures defined for the IEEE 802.15.4 protocol, where a cluster head is elected as a local WSN Cluster coordinator and starts transmitting beacon signals to keep its child nodes synchronised. At present, any decision whether to implement a dynamic cluster head (re-)election mechanism or to plan the role of the nodes at the deployment phase has not yet been taken.

In this work, instead of having a map which associates statically at deployment time the position of the nodes with their IDs somewhere in the network devices, it is assumed that each node knows its own position[10] and communicates it when it tries to perform an association procedure within a cluster. Given these assumptions, a simple and efficient position aware tree based routing algorithm can be implemented in our architecture as follows.

For the sake of simplicity in the exposition, let us suppose using coordinates in a bi-dimensional reference system, i.e., each node has its own position expressed as:

$P_i = (x_i, y_i)$, $i = 1, ..., N$,

where N is the number of nodes in the network and x_i and y_i are the coordinates of the node i, which can be either absolute (e.g. GPS coordinates) or relative (e.g. to the position of the gateway).

When a WSN Node tries to associate to a CH in a WSN Cluster, it communicates its own position P_i to the CH, so that the CH can compute its served area, by simply computing the rough area as a box B:

$B = [(x_s, y_s), (x_e, y_e)]$,

where:

[10] This can be done in several ways, either by preprogramming the nodes with their own position or by configuring them at the deployment time (like done e.g. in [RD-11]) or by implementing a kind of position discovery algorithm ([RD-45], [RD-46], [RD-47]). In any case how each node would get its own position estimation is out of scope of the present deliverable.

$$x_s = \min_{i \in N_c}\{x_i\}$$

$$x_e = \max_{i \in N_c}\{x_i\}$$

and N_c is the number of nodes in the WSN Cluster. y_s and y_e are computed in a similar fashion.

This mechanism can be iterated up to the gateway, i.e. when a Cluster Head tries to associate to its parent, or as soon as it has computed its served area B, it communicates the coordinates of B to its parent which can determine its served area A as follows (Figure 11):

$A = [(x_{sA}, y_{sA}), (x_{eA}, y_{eA})]$,

where:

$$x_{sA} = \min_{s \in N_r}\{x_s\}$$

$$x_{eA} = \min_{e \in N_r}\{x_e\}$$

and N_r is the number of child router nodes.

As a consequence, each node of the WSN Patch is aware of its own served area B and in particular, the gateway can communicate the coordinate of A to the remote C&C.

When the C&C queries the network for sensor readings, as defined in the Deliverable D6.2 [AD-6], it uses high level APIs which include the position information of the interested area as a parameter for querying the network for specific readings or for instructing the nodes about the alarm or report generation conditions. In Figure 10, we presented an example of the queried area from the C&C. By knowing the served area of each WSN Patch and the IP addresses of their gateways, the C&C sends the query message Q to the appropriate gateway (or gateways, if the queried area includes, even partially, the served area of more than a WSN Patch). As soon as the gateway receives the message Q, it checks if the queried area is overlapping with its served area and forwards the message to its child nodes in the tree using e.g. the command frame defined in the IEEE 802.15.4 standard. In particular, it may include in the beacon the “message pending” information so that each child node asks for this message during the contention access period in the super-frame ([RD-14], [RD-15]). Each child router will forward Q down to its sub-tree only if the queried area is overlapping, even partially, to its served area, and this mechanism will be repeated at each step along the tree, until all the nodes in the interested area will be reached. As an alternative, the Z-Cast protocol [RD-43] for multicast routing in cluster tree networks, already tested and implemented in the frame of OpenZB [AD-8], can be more efficiently used to propagate the message.

Nevertheless, the collection of the sensor readings, i.e. the flow back from the WSN Nodes up to the sink gateway, can be implemented in the usual way along the tree, by simply recognizing that each node communicates only with its parent. This mechanism easily allows also for implementing data aggregation or even sensor fusion at each vertex in the tree, but this topic will be addressed in the Deliverable D4.7.

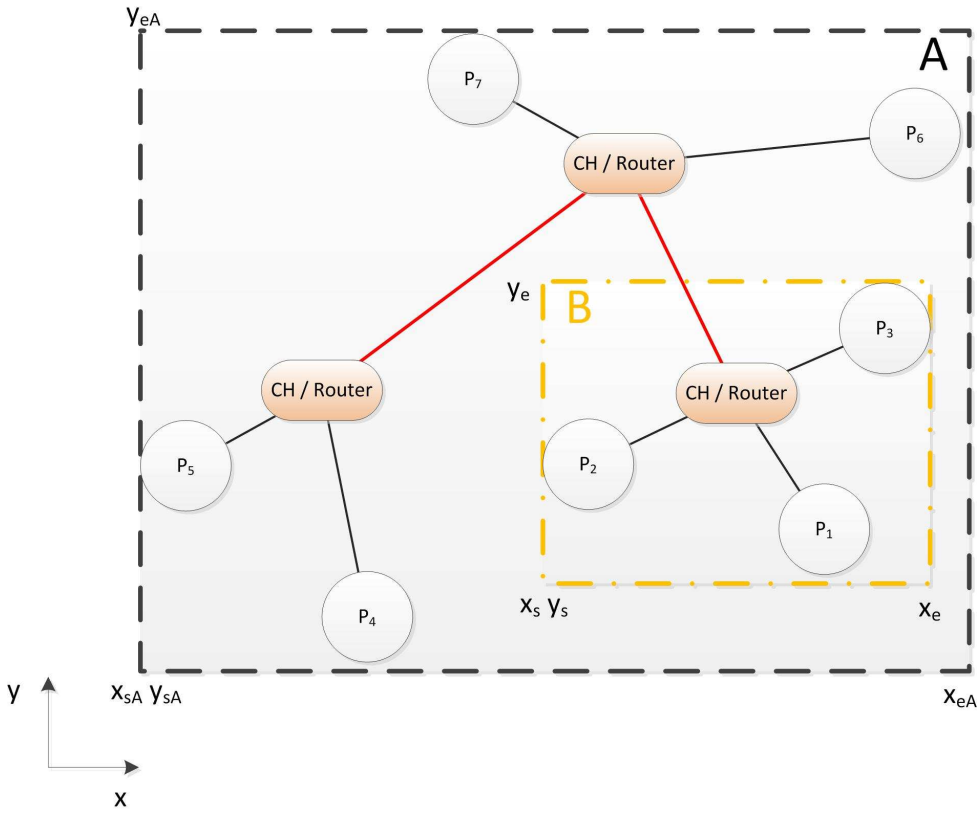

Figure 11 - Position based routing – nodes association and served area

11. Design Choices

Following on from the specifications made in sections 8-10, this section aims to summarize the choices made by the consortium to achieve scalability in the proposed network architecture, highlighting our scientific contribution.

It is clear that introducing a hierarchical and modular design, where blocks are composed together to form the whole network, is the only way to guarantee the necessary level of scalability in our EMMON network architecture. Furthermore, even if the option of using 6LoWPAN is appealing in this framework, at this time the standard is not mature enough to provide the necessary guarantees that such a technology succeed in the EMMON scenarios. As a consequence, **current proposal is to opt for a cluster tree network architecture, based on the Open-ZB approach [AD-8]**.

In this frame we'll solve a number of technical challenges as briefly summarized in next subsections.

11.1 Synchronization

The key to achieving scalability while maintaining quality of service is to apply a design methodology characterized by a "divide et impera" approach, moving from the basic building blocks of the IEEE802.15.4 standard in its beacon enabled version. Multiple independent WSN Patches compose the whole EMMON network. Within each Patch, due to the necessary nodes density requirement, the assumption that a transmission from any node can affect any other node is real.

To solve this problem, the IEEE 802.15.4 standard suggests to schedule the activity portions of the super-frames into time windows for all the clusters so that they are mutually exclusive. In other words, when a cluster is active the neighbours must be sleeping to avoid inter-cluster collisions/interference. However, the standard doesn't define any mechanism to achieve this goal.

In this project we propose to adopt our defined Time Division Beacon Scheduling algorithm as summarized in Deliverable D6.2 [AD-6] (Section 6.3) and in more detail in [AD-8], where this solution has been tested both in simulation and experimental activities with a network composed by up to 15 clusters. Briefly, the idea in this algorithm is to find a scheduling of the beacon intervals of each cluster within a WSN Patch with non-overlapping windows. In this framework there is an obvious trade-off between scalability and network responsiveness, as already highlighted in [AD-6]: the longer the beacon intervals, the more cluster activity periods can be scheduled in the inactivity periods of the other ones, but the longer the responsive time of each cluster. However, for preliminary results in terms of time bounds and resources on the Router/Cluster Heads a set of tools have been developed [AD-10] and further implementation details on can be found in [AD-8] and [AD-11].

11.2 GTS Usage

To handle at least two traffic classes, as requested in [AD-3], with different quality of service needs, i.e. sensor measurements reports and alarm notifications, the idea is to use Guaranteed Time Slots (GTS) defined in the IEEE802.15.4 standard and further addressed next in Section 12.1, Traffic Differentiation, to enable the timely notifications of the alarms, meeting the goals defined in [AD-3] on the maximum end-to-end delay.

However, the standard defines a procedure to explicitly allocate these slots on-demand to a single node, which typically leads to wasted bandwidth. Our proposal is to improve the guaranteed bandwidth usage by sharing the same GTS slots among several nodes, which is a new mechanism not defined in the standard. This mechanism, named i-GAME, foresees an implicit allocation mechanism and has been proposed and validated in [AD-12], demonstrating that the proposed solution is feasible in practice on real COTS WSN platforms and confirming the improvement resulting from using the implicit GTS allocation mechanism over the classical explicit GTS allocation in terms of bandwidth utilization.

11.3 Dimensioning Of A WSN Patch And Interference

Based on the available experiences of real cluster tree networks within the EMMON consortium, there is a common understanding that for performance reasons in terms of time synchronization and beacon propagation among the nodes running the TinyOS operating system, like the ones chosen in [AD-5], the best way to make the system works is to limit the depth of a tree to no more than 3 hops.

However, this is not really a limitation in terms of the scalability of the network, since a single WSN Patch can be composed easily by a dozen of clusters (experiments succeeded with 15 clusters) and it is possible to imagine something like ten nodes per cluster, resulting in a WSN Patch composed by a few hundreds of nodes. In this scenario, the chosen communication protocol, based on a time division beacon scheduling mechanism, will still work and guarantee that no collisions occur among the clusters. Experiments and simulation activities aiming at stress more the system with an increased number of nodes are currently running in the frame of this project.

Furthermore, to increase the number of nodes in the whole network, it is possible to deploy multiple WSN Patches in the area under monitoring. To maintain the independence in terms of the communication protocol among different WSN Patches, which might be even partially co-located in the same area, since time division mechanisms are used within each WSN Patch, the idea is to exploit the frequency division, i.e. using different IEEE802.15.4 channels.

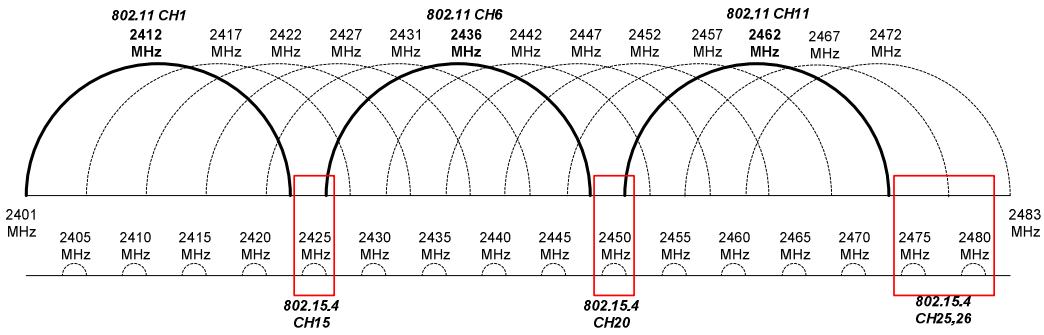

Figure 12 - Spectrum overlap of WLAN (IEEE802.11) and IEEE802.15.4

While in some EMMON envisaged scenarios like the forest fire monitoring, one can imagine that all the 16 IEEE802.15.4 channels are available in the 2.4GHz band allowing co-existence of multiple WSN Patches, in practice the real available spectrum is limited to the interference considerations. Especially in Urban scenarios, the main source of interference is the WLAN spectrum, which is formally spread over all the 802.15.4 frequencies. The WLAN standard suggests using non overlapping channels, which means to restrict the

number of channels available to only three, as shown in Figure 12. By comparing the spectrum of the two systems, it is evident that the number of available 802.15.4 channels for EMMON is reduced to only four.

As a consequence, the choices available to cope with the interference problem are basically two:

- Configuring the operating channels of each WSN Patch at deployment time, by measuring the interference level, or
- Embedding in the nodes some robustness mechanisms to dynamically choose the free channel.

While the latter option seems the most appealing and even if in literature there exist some proposals to address this issue at the protocol level, like e.g. [RD-55], or by relating to more sophisticated mechanisms, like software defined radio [RD-56], the former one appears at this moment more feasible.

12. Additional Issues

In this section we aim at giving an overview of the traffic differentiation, congestion control and security mechanisms that would be implemented in our chosen network architecture. Deeper analysis of these issues is deferred to next deliverables, i.e. D4.4 for communication robustness and D4.10 for security mechanisms.

12.1 Traffic Differentiation

Although some classical WSN applications, like environmental monitoring for sensor reports, do not impose stringent timing requirements on data delivery, there are a number of added value services in which timeliness is of great importance. In the case of raising alarms and subsequent control actions, computations and communications must not only be logically correct, but also be delivered on time.

The standardization efforts of the IEEE Task Group 15.4 have already tried to solve this problem within the frame of the IEEE 802.15.4. In our architecture, we have chosen to implement the beacon-enabled mode of the standard, which provides two Medium Access Protocol (MAC) mechanisms to nodes for accessing the medium: i) slotted CSMA/CA in the Contention Access Period (CAP) and ii) Guaranteed Time Slots (GTS) in the Contention Free Period (CFP) (Figure 13). These two mechanisms enable a natural differentiation in the traffic for the nodes allowing at least two classes.

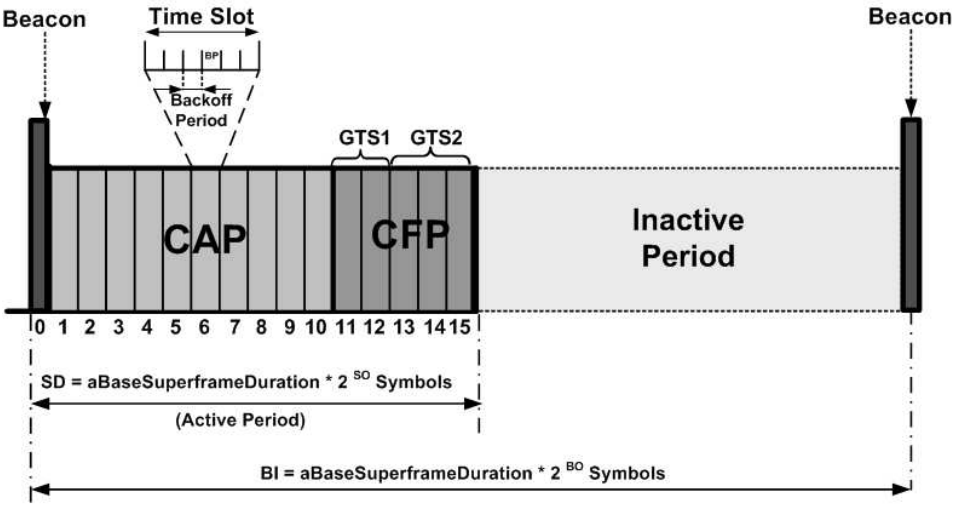

Figure 13 - IEEE 802.15.4 Superframe

However, even if the GTS mechanism is a good solution for the QoS requirement of the low-rate WPAN applications and it will be considered as the basis for implementing our EMMON architecture in the first step, it shows some limitations.

The first one concerns the restriction on the distribution and amount of traffic that this service can avail. In a superframe, a maximum of seven GTS slots can be allocated, implying that in each cluster a maximum of seven nodes can have guaranteed communication slots in any superframe. The remaining nodes may only transmit in the CAP, nominally without QoS support.

Second, as highlighted previously in Section 11.2, the GTS slots allocation must be preceded by an allocation request message transmitted using the CAP, and when collisions occur, this request may fail, delaying its service. This is unequivocally a bad scenario for high priority traffic.

Therefore, in the recent past several works dealt with building mechanisms to provide QoS to the CAP part of the superframe ([RD-49], [RD-50] and [RD-51]). The integration of these mechanisms easily provides increased QoS to higher priority messages, requiring only minor add-ons and ensuring backward compatibility with the IEEE 802.15.4 standard protocol. In particular, the CSMA/CA protocol behaviour is mostly affected by three parameters: i) the minimum backoff exponent (*macMinBE*), ii) the maximum backoff exponent (*aMaxBE*) and the initial value of the contention window CW (*CWinit*). Changing the values of any of these parameters will have an impact on the performance.

Instead of having the same CSMA/CA parameters for e.g. two different traffic types, each class can be assigned with its own attributes, like ($macMinBE_{HP}$, $aMaxBE_{HP}$, CW_{HP}) for the High Priority traffic class and ($macMinBE_{LP}$, $aMaxBE_{LP}$, CW_{LP}) for the Low Priority one.

In addition to the specification of different CSMA/CA parameters, Priority Queuing can be applied to reduce queuing delays of high priority traffic (Figure 14). In this case, slotted CSMA/CA uses priority scheduling to select frames from queues, and then applies the adequate parameters corresponding to each service class.

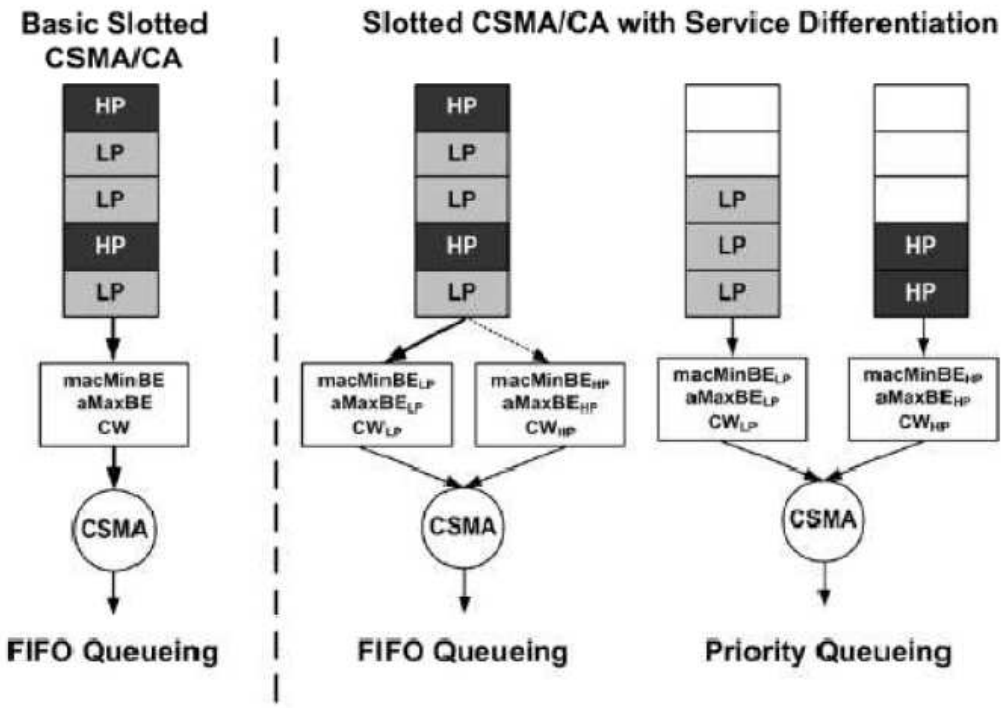

Figure 14 - Differentiated service strategies

In conclusion, the heuristics for adequately setting these parameters may be the following. Intuitively, a first differentiation consists in setting CW_{HP} lower than CW_{LP}. It results that low priority traffic has to assess the channel to be idle for a longer time before transmission. A second differentiation is related to the backoff interval: providing lower backoff delay values

for high priority traffic by setting $macMinBE_{HP}$ lower than $macMinBE_{LP}$ would improve its responsiveness without degrading its throughput.

However, as a final note, since this traffic differentiation method is probabilistic, it doesn't have guarantees in terms of quality of service. As a consequence, in the frame of this project we will first evaluate the performance when using a standard implementation of the beacon-enabled mode of the IEEE 802.15.4 protocol, differentiating traffic classes between the CAP and the CFP.

12.2 Congestion Control

In this project sensor nodes are required to send data on a periodic basis and they should conform their duty cycle when an event is detected which may potentially trigger an alarm notification to a remote C&C. With fast continuous transmissions, the variation of any phenomenon in the environment can be monitored precisely; however, the energy consumption can increase drastically. For energy savings and detailed monitoring, sensor nodes should adapt the data transmission interval, i.e. their communication duty cycle, in an inverse proportion to the phenomenon's variation. Therefore, the transfer rate in case of alarms should be varied according to the event occurrence or the input from the forecasts provided by the event propagation tool running on the C&C host [AD-7]. However, such a variable transfer rate for different part of the network causes network congestion due to concentrated packets in case of a concurrent occurrence of multiple events. During congestion, routers usually drop the overflowed packets; however packet drops lead to data loss and unnecessary energy consumption [RD-53].

In order to reduce congestion, the routing protocol should reduce the number of packets in the network; however, simply dropping overflowed packets will reduce the data fidelity and increase the energy consumption. As a consequence, in literature two kinds of works are present and they try to tackle the congestion control problem under two perspectives: i) proactively trying to determine the pre-conditions under which the occurrence of this problem might have a low probability of occurrence, i.e. like congestion avoidance mechanisms, or ii) reactively adjusting some parameter, like the packet generation rate or the compression level of the source information, to avoid the need to drop packets.

In the first class we can mention the work done in [RD-52], [AD-13]. In particular, in [AD-13] an analytical model has been developed having in mind the following objective: "Having a WSN organized in a cluster-tree topology, with a given number of nodes, a given number of routers, and a given depth, and provided that a minimum service is guaranteed to every node and router, what are the delay bounds for flows originated from nodes at a given depth in the WSN, and what are the minimum resource requirements in each router?". As a by-product of this work, an estimation of the minimum resources needed in each router in terms of queues length is made available.

In the second class, the works like [RD-53] and the references therein try to build adaptive compression schemes or source rate limiting for packet reduction in case of congestion.

Some solutions often referred for mitigating this problem in WSNs rely on the possibility to use different paths in multipath routing. However, in our simple network architecture, these mechanisms are difficult to implement, since we foresee only communications among parent-child in the tree. On the other hand, this architecture easily allows for exploiting data aggregation and sensor fusion mechanisms, which greatly helps in reducing the packets along the tree and as a consequence the probability of occurrence of congestions.

Nevertheless, we think that by combining the first solution, i.e. planning accurately the nodes' resources, with an adequate aggregation/fusion algorithm, e.g. compressing the information at the source nodes and aggregate it along the tree, we may guarantee a sufficient level of QoS even in the presence of high loads of traffic. Both mechanisms will be further investigated as communication robustness methods in next D4.4 deliverable, while data aggregation will be addressed in D4.7.

12.3 Security

Security mechanisms will be addressed in detail in next Deliverable D4.10. In this section we aim at giving only a general overview of the security features provided by the IEEE 802.15.4 standard, while the choice to enable or disable them along with their correct use is demanded to the higher levels of the ISO/OSI stack, i.e. the Network and the Application layers.

In general, when we talk of security requirements we mean[11] [RD-44]:

- Freshness: devices maintain incoming and outgoing freshness counters to maintain data freshness. In the ZigBee specifications these counters are reset every time a new key is created. Devices that communicate once per second will not overflow their freshness counters for 136 years.

- Message Integrity: ZigBee specifications provide options of providing 0-, 32-, 64- or 128-bit data integrity for the transmitted messages. The default is 64-bit integrity.

- Authentication: Network level authentication is achieved by using a common network key. This prevents outsider attacks while adding very little in memory cost. Device level authentication is achieved by using unique link keys between pairs of devices. This prevents insider and outsider attacks but has higher memory cost.

- Encryption: ZigBee uses 128-bit AES encryption. Encryption protection is possible at network level or device level. Network level encryption is achieved by using a common network key. Device level encryption is achieved by using unique link keys between pairs of devices. Encryption can be turned off without impacting freshness, integrity, or authentication as some applications may not need any encryption.

The MAC layer uses the Advanced Encryption Standard (AES) as its core cryptographic algorithm and describes a variety of security suites that use the AES algorithm. The MAC layer does the security processing, but the upper layers, which set up the keys determine the security levels to use. In particular, the MAC Layer adds an auxiliary header along with the MAC Layer header for carrying security information. The message integrity code (MIC) may take the values 0, 32, 64 or 128 and determines the level of data integrity. When the MAC layer transmits (receives) a frame with security enabled, it looks at the destination (source) of the frame, retrieves the key associated with that destination (source), and then uses this key to process the frame according to the security suite designated for the key being used. Each key is associated with a single security suite and the MAC Layer frame header has a bit that specifies whether security for a frame is enabled or disabled. The security processing of the outgoing and incoming MAC Layer frames with MAC Layer security is explained in [RD-20].

[11] As a reference, we inserted the general directives defined in the ZigBee specifications.

As a general remark, since using the security features involves extra overhead both in the packets transmitted and received and in the computations performed by the nodes, it is of paramount importance to adapt the security level to the criticality of the information, trading off this with the available computation and storage resources at each tier of our network architecture. For instance, we may imagine that a single sensor reading will be sent to the Cluster Head with an appropriately low level of encryption, while the flows of the aggregated data that traverse the tree up to the sink and which constitutes even more important information, will be protected with more sophisticated techniques. Finally, at the gateway, where computational and storage resources should not be a limitation, more complex security mechanisms will be adopted to protect the transfer of the gathered data to the C&C.

13. General Conclusions

This document is the second and final issue of deliverable D4.5 that specifies a multi-tiered communication architecture to support large-scale WSN deployments for EMMON on the basis of end-user requirements and the lessons learnt from previous large-scale real world WSN deployments. In particular, we discuss the constraints placed on the architecture design by the end-user requirements and the rationale behind the design decisions that are made. We then discuss the various tiers of the communication architecture, the topology chosen at each tier and the role of the nodes at each tier. We then address issues relating to addressing, packet format, routing, traffic differentiation, congestion control and security.

We are confident that adopting a hierarchical network architecture with local coordinators, greatly helps in solving problems at different tiers, while trying to maintain a level of complexity adequate to the resources available at each tier, i.e. rigid but simple mechanisms where there are more resource constrained nodes and flexibility where powerful nodes are.