*EMMON - EMbedded MOnitoring*

ARTEMIS JU – FP7

# D4.2 EVALUATION OF POSSIBLE SOLUTIONS, CONCEPTS FOR NEW COMMUNICATION METHODS

## EVALUATION OF POSSIBLE SOLUTIONS

## EMMON

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

| | |
|---|---|
| ***Date:*** | *2010-01-29* |
| ***Pages:*** | *165* |
| ***Status:*** | *Approved* |
| ***Dissemination Level:*** | *PU* |
| ***Reference:*** | *FP7-JU-EMMON-2010-WP4-002-D4.2* |
| ***Version:*** | *1* |

***Customer:***

SEVENTH FRAMEWORK PROGRAMME

# EVALUATION REPORT OF POSSIBLE SOLUTIONS, CONCEPTS FOR NEW COMMUNICATION METHODS

EMMON

| Authors and Contributors | | | | |
|---|---|---|---|---|
| Name | Contact | Organization | Description | Date |
| Stefano Tennina | sota@isep.ipp.pt | ISEP | Author | 2009-11-23 |
| Mário Alves | mjf@isep.ipp.pt | ISEP | Co-author | 2009-11-23 |
| Paulo Gandra Sousa | pag@isep.ipp.pt | ISEP | Co-author | 2009-11-23 |
| Manuel Santos | manuel.j.santos@criticalsoftware.com | CSW | Co-author | 2009-11-23 |
| Pedro Braga | pedro.l.braga@criticalsoftware.com | CSW | Co-author | 2009-11-23 |
| Mélanie Bouroche | Melanie.Bouroche@cs.tcd.ie | TCD | Co-author | 2009-11-23 |
| Gabriella Carrozza | gcarrozza@sesm.it | SESM | Co-author | 2009-11-23 |
| Rui Monica | rs-monica@criticalsoftware.com | CSW | Co-author | 2009-11-23 |
| Filipe Pacheco | ffp@isep.ipp.pt | ISEP | Contributor | 2009-11-23 |
| Ricardo Gomes | rftg@isep.ipp.pt | ISEP | Contributor | 2009-11-23 |
| Anurag Garg | anurag.garg@cs.tcd.ie | TCD | Contributor | 2010-01-07 |
| Ricardo Severino | rars@isep.ipp.pt | ISEP | Contributor | 2010-01-20 |

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

| Revision History | | | | |
|---|---|---|---|---|
| Version | Revision | Date | Description | Author |
| 1 | - | 2009-12-18 | First Draft for internal review | Stefano Tennina, Mário Alves, Paulo Gandra de Sousa, Filipe Pacheco, Manuel Santos, Pedro Braga, Ricardo Gomes, Mélanie Bouroche, Gabriella Carrozza, Rui Monica |
| 1 | 1 | 2010-01-22 | Second draft for approval | Stefano Tennina, Mário Alves, Paulo Gandra de Sousa, Filipe Pacheco, Manuel Santos, Pedro Braga, Ricardo Gomes, Mélanie Bouroche, Gabriella Carrozza, Rui |

| Revision History | | | | |
|---|---|---|---|---|
| **Version** | **Revision** | **Date** | **Description** | **Author** |
| | | | | Monica, Ricardo Severino |
| 1 | 2 | 2010-01-25 | Revision of the second draft for approval | Stefano Tennina, Mário Alves, Paulo Gandra de Sousa, Pedro Braga, Mélanie Bouroche, Gabriella Carrozza |
| 1 | 5 | 2010-01-29 | Version 1, For approval | Stefano Tennina, Mário Alves, Paulo Gandra de Sousa, Filipe Pacheco, Manuel Santos, Pedro Braga, Ricardo Gomes, Mélanie Bouroche, Gabriella Carrozza, Rui Monica, Ricardo Severino |
| 1 | 6 | 2010-06-04 | Approved version according to the results of the Technical Review Report, ref: ARTEMIS-ED-21-09, of 2010-06-04. | Stefano Tennina, Mário Alves, Paulo Gandra de Sousa, Filipe Pacheco, Manuel Santos, Pedro Braga, Ricardo Gomes, Mélanie Bouroche, Gabriella Carrozza, Rui Monica, Ricardo Severino |
| 1 | 7 | 2010-08-15 | Approved version according to the results of the Technical Review Report, ref: ARTEMIS-ED-21-09, of 2010-06-04. Checked according to documentation convention | Stefano Tennina, Mário Alves, Paulo Gandra de Sousa, Filipe Pacheco, Manuel Santos, Pedro Braga, Ricardo Gomes, Mélanie Bouroche, Gabriella Carrozza, Rui Monica, Ricardo Severino |

| 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 assess the most prominent solutions at different layers, like WSN architectures and communication protocols. To do so, a methodology has been defined for evaluating technologies[1] by applying the lessons learned from the analysis of the past and recent projects, which deal with large scale WSN in real world deployments. The composition of these solutions will be the objective of the next deliverable, i.e. the D4.5 – Specification of multilevel communication protocol.

A second objective of this document is to infer the best practices from such real world deployments experiences to be reused in EMMON.

As a final remark, it is of paramount importance to note that this deliverable is not a state of the art review; rather, the available solutions have been evaluated according to a set of criteria to identify the best ones for the EMMON goals of large scale and high density WSNs.

## 1.2 Scope

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

D4.2 will work towards the analysis and proposal of solutions for the problems identified in previous deliverable (D4.1). The strengths and weaknesses of using existing technologies are identified and this drives the direction of this work package. Furthermore, the output of this deliverable, as a set of alternatives feasible solutions, will drive the selection and specification issues addressed first in D4.5, Specification of multilevel communication protocol, and next in D4.3, Simulation results of selected new communication methods.

## 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 |

[1] From now on in this document, for simplicity of exposition, we will call “technologies” the solutions available in literature and described in Sections 7 to 10 for communication protocols and network architectures.

| Acronyms | Description |
|---|---|
| AD | Applicable Document |
| CDMA | Code Division Multiple Access |
| CEA | Cost-Effectiveness Analysis |
| 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 |
| IEEE | Institute of Electrical and Electronics Engineers |
| LS-WSN | Large-Scale Wireless Sensor Network |
| MAC | Medium Access Control |
| MIB | Management Information Base |
| MTTF | Mean Time To Fail |
| MTTR | Mean Time To Recover |
| N/A | Not Applicable or Not Available |
| NES | Networked Embedded Systems |
| NFP | Non-Functional Property |
| 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, while Section 3 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 for identifying the possible alternative stacks described in Section 5, Possible Solutions. As annexes, Section 6, Current and Past Large Scale Solutions, Section 7, Network Architecture, Section 8, WSN MAC and DATALINK Layer, Section 9, WSN Routing and Network Layer, and Section 10, Federated Communication, present the technologies and projects taken into account to identify the solutions proposed in Section 5. In particular, Section 6 aims at reviewing also the solutions and tools used in similar projects and real deployments to be derive the best practices to be efficiently adopted also in EMMON.

Finally, Section 11 provides some general conclusions.

# 2. Documents

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

## 2.1 Applicable Documents

This section presents the list of documents that are applicable to the present document. A document is considered applicable if it contains provisions that through reference in this document incorporate additional provisions to this document.

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

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

[AD-3] “Deliverable 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, 2008-12-08.

[AD-4] “EMMON Scope definition”, FP7-JU-EMMON-2009-O-TSG-008, EMMON Project, ARTEMIS Joint Undertaking Call for proposals ARTEMIS-2008-1, Grant agreement no. 100036, 2009-11-05

[AD-5] “EMMON Glossary”, FP7-JU-EMMON-2009-O-TSG-005, EMMON Project, ARTEMIS Joint Undertaking Call for proposals ARTEMIS-2008-1, Grant agreement no. 100036, 2009-04-28

[AD-6] “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[2].

[AD-7] “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, 2009-07-31

## 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.

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

[2] This is the official date of release that will be on this deliverable. However, at present, preliminary information is available for the goals of D4.2 deliverable.

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

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

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

[RD-6] Ubiquitous Sensing and Security in the European Homeland, FP6-IST (STREP), http://www.ist-ubisecsens.org.

[RD-7] Dirk Westhoff, “The UbiSec&Sens Security and Reliability Toolbox and Selected Applications”, ZigBee Alliance Meeting, Vancouver, BC, 6-9th October 2008. Available on line at http://www.ist-ubisecsens.org/invited_talks/VortragZigBee.pdf

[RD-8] Collaborative Business Items, FP6 STREP Project # IST 004270, http://www.cobis-online.de/index.html.

[RD-9] 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.

[RD-10] L. van Hoesel, T. Nieberg, J. Wu, and P. Havinga. "Prolonging the lifetime of wireless sensor networks by cross-layer interaction". IEEE Wireless Communication Magazine, 12 2004.

[RD-11] M. Marin-Perianu and P. Havinga. "RMD: Reliable multicast data dissemination within groups of collaborating objects". In LCN, pages 656–663, 2006.

[RD-12] M. Horsman, M. Marin-Perianu, P. Jansen and P. Havinga, “A Simulation Framework for Evaluating Complete Reprogramming Solutions in Wireless Sensor Networks”, 3rd International Symposium on Wireless Pervasive Computing, ISWPC 2008, pp 6-10.

[RD-13] P. Gil, I. Maza, A. Ollero and P.J. Marron, “Data centric middleware for the integration of wireless sensor networks and mobile robots”, ROBOTICA 2007 - 7th Conference on Mobile Robots and Competitions, Portugal, April 2007.

[RD-14] R. S. Marin-Perianu, J. Scholten, P. J. M. Havinga and P. H. Hartel, “Cluster-based service discovery for heterogeneous wireless sensor networks”, International Journal of Parallel, Emergent and Distributed Systems, Volume 23, Issue 4 (August 2008), Pages 325-346, 2008.

[RD-15] Taddia, C.; Meratnia, N.; van Hoesel, L.F.W.; Mazzini, G.; Havinga, P.J.M., “MAC support for high density wireless sensor networks”, 15th International Conference on Software, Telecommunications and Computer Networks, 2007. SoftCOM 2007, pp.1-8, 27-29 Sept. 2007.

[RD-16] Y.W. Law, M. Palaniswami, L. van Hoesel, J. Doumen, P. Hartel and P. Havinga, “Energy-Efficient Link-Layer Jamming Attacks against Wireless Sensor Network MAC Protocols”, ACM Transactions on Sensor Networks, Vol. 5, No. 1, Article 6, Publication date: February 2009.

[RD-17] VAN HOESEL, L., DULMAN, S., HAVINGA, P., AND KIP, H. 2003. “Design of a low-power testbed for wireless sensor networks and verification”. Tech. rep. TR-CTIT-03-45, Centre for Telematics and Information Technology, University of Twente, The Netherlands.

[RD-18] Capturing Ambient Intelligence for Mobile Communications Through Wireless Sensor Networks, FP6 IST integrated project IST-FP6-IP-027227, http://www.ist-e-sense.org.

[RD-19] Z. Shelby, A.Gluhak "e-Stack : An adaptive stack architecture for wireless sensing and control" CAPS 2007, Guildford [online] http://www.zurich.ibm.com/pdf/sys/adv_messaging/eSense.pdf.

[RD-20] Deliverable 2.2.2a: "e-SENSE System Architecture", http://www.ist-esense.org/index.php?id=215. Deliverable 2.2.2b: "e-SENSE System Architecture: Protocol stack configurations", http://www.ist-esense.org/index.php?id=215. Deliverable D7.3: "Final Activity Report", http://www.ist-esense.org/index.php?id=215.

[RD-21] Creating Ubiquitous Intelligent Sensing Environments, FP6-IST Network of Excellence, http://www.ist-cruise.eu.

[RD-22] Reconfigurable Ubiquitous Networked Embedded Systems, FP6-IST integrated project, http://www.ist-runes.org.

[RD-23] Smart Messages Project, http://discolab.rutgers.edu/sm.

[RD-24] Borcea, C.; Iyer, D.; Kang, P.; Saxena, A.; Iftode, L., "Cooperative computing for distributed embedded systems," International Conference on Distributed Computing Systems, 2002. Proceedings. 22nd, vol., no., pp. 227-236, 2002.

[RD-25] P. Kang, C. Borcea, G. Xu, A. Saxena, U. Kremer and L. Iftode, "Smart Messages: A Distributed Computing Platform for Networks of Embedded Systems", The Computer Journal 2004 47(4):475-494; doi:10.1093/comjnl/47.4.475, © 2004 by British Computer Society

[RD-26] Energy Efficient Sensor Networks, IST-2001-34734, http://www.eyes.eu.org.

[RD-27] J. Wu, P. Havinga, S. Dulman and T. Nieberg, "EYES Source Routing Protocol for Wireless Sensor Networks" Proceedings of the 1st European Workshop on Wireless Sensor Networks (EWSN 2004) p67. Available on line at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.72.5718&rep=rep1&type=pdf#page=73

[RD-28] Deliverable D1.1: System Architecture Specification, Available online at http://www.eyes.eu.org/publications/d1.1.pdf.

[RD-29] Solving Major Problems in Microsensorial Wireless Networks, FP6 STREP Project # IST 034642, https://www.uswn.eu.

[RD-30] µSWN Research Project Deliverable D8, "Analysis of WSN Deployment Methodologies", November 2007.

[RD-31] µSWN Research Project Deliverable D4, "Clustering and Classification of Application Scenarios", November 2007.

[RD-32] µSWN Research Project Deliverable D52, "µSWN Prototype Plan", February 2008.

[RD-33] µSWN Research Project Deliverable D10A, "WSN Methodology Evaluation".

[RD-34] µSWN Research Project Deliverable D9A, "WSN deployment prototype", August 2008.

[RD-35] µSWN Research Project Deliverable D12c, "uSWN configurable communication protocols", June 2008.

[RD-36] Very large scale open wireless sensor network testbed, http://www.senslab.info.

[RD-37] Deliverable D1.1a: SensLAB node hardware. Available at http://www.senslab.info/index.php/Project_Deliverables.

[RD-38] Deliverable D1.1b: SensLAB node software, ControlNode software and Gateway software. Available at http://www.senslab.info/index.php/Project_Deliverables.

[RD-39] Deliverable D2.4: Software framework package release V1.0. Available at http://www.senslab.info/index.php/Project_Deliverables.

[RD-40] Wireless Sensor Network Testbeds, FP7 Project # 224460; http://www.wisebed.eu.

[RD-41] Deliverables D1.1, D2.1, and D3.1: Design of the Hardware Infrastructure, Architecture of the Software Infrastructure, and Design of Library of Algorithms http://www.wisebed.eu/images/stories/deliverables/d1.1-d3.1.pdf.

[RD-42] Smart-ITS, http://www.smart-its.org; BTnodes - A Distributed Environment for Prototyping Ad Hoc Networks, http://www.btnode.ethz.ch.

[RD-43] ETH Zurich – Smart-Its http://www.vs.inf.ethz.ch/res/show.html?what=smart-its

[RD-44] BTnodes - A Distributed Environment for Prototyping Ad Hoc Networks, http://www.btnode.ethz.ch.

[RD-45] SensorScope, http://sensorscope.epfl.ch/index.php/Main_Page.

[RD-46] G. Barrenetxea, F. Ingelrest, G. Schaefer and M. Vetterli. “The Hitchhiker's Guide to Successful Wireless Sensor Network Deployments”. The 6th ACM Conference on Embedded Networked Sensor Systems (SenSys 2008). Raleigh, NC, USA, 5-7 November 2008.

[RD-47] Shockfish TinyNode, http://www.tinynode.com

[RD-48] WASP, http://wasp.cefriel.it.

[RD-49] Laurent Gomez, Annett Laube, Vincent Ribiere, Alessandro Sorniotti, Christophe Trefois, Marco Valente, Patrick Wetterwald, "Encryption-Based Access Control for Building Management", in the proceedings of the Fifth Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MOBIQUITOUS '08), 2008.

[RD-50] J. Ansari, X. Zhang, P. Mähönen, "Multi-radio Medium Access Control Protocol for Wireless Sensor Networks" Proc. of Workshop on Energy in Wireless Sensor Networks [in conjuction with DCOSS 2008], Santorini Island, Greece, June 2008.

[RD-51] A. Sorniotti, R. Molva, L. Gomez, "Efficient Access Control for Wireless Sensor Data", Ad Hoc & Sensor Wireless Networks, An International Journal, 2009.

[RD-52] Pieter Hogewerf, Wageningen UR, "Do cows and farmers benefit from WSN's?", CEFRIEL, Wireless sensor networks and applications for SMEs, June 2009, Milano/Italy. Available on line at http://wasp.cefriel.it/download/public/publications/05.Hogewerf_Do_cows_and_farmers_benefit_from_WSN.pdf.

[RD-53] WINSOC, http://www.winsoc.org.

[RD-54] Karel Charvat, Zbynek Krivanek, Petr Kubicek, Maneesha V. Ramesh, Rehna Raj T, Joshua D Freeman, Vijay Selvan and Sangeeth Kumar, “Components for sensor nodes and transducers”, IST-2005-2.5.12-WINSOC, 2007/10/10.

[RD-55] COMMON-Sense Net, http://commonsense.epfl.ch and http://commonsense.epfl.ch./COMMONSense/default.htm.

[RD-56] COMMON-Sense Net: Water management for agriculture in semi-arid areas by means of wireless sensor networks, Proposal of the project, September 2003. Available at http://commonsense.epfl.ch./Resources/Docs/WaterSensorsProposal.pdf.

[RD-57] COMMON-Sense Net: Improved Water Management for Resource-Poor Farmers via Sensor Networks, Jacques Panchard, Seshagiri Rao, Prabhakar T.V., H.S. Jamadagni and Jean-Pierre Hubaux, accepted for publication at the International Conference on Information and Communication Technologies and Development (ICTD 2006).

[RD-58] Jacques Panchard: Wireless Sensor Networks for Marginal Farming in India, PhD Thesis Lausanne, EPFL 2008.

[RD-59] SLEWS, http://www.slews.de.

[RD-60] Walter, Kai, Nash, Edward, “Coupling Wireless Sensor Networks and the Sensor Observation Service – Bridging the Interoperability Gap”, In: 12th AGILE International Conference on Geographic Information Science 2009, Hannover, 2009

[RD-61] Research Project page, http://www.cs.virginia.edu/wsn/vigilnet.

[RD-62] 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, “VigilNet: An integrated sensor network system for energy-efficient surveillance”, ACM Transactions on Sensor Networks (TOSN), Volume 2, Issue 1, Pag 1 - 38, February 2006.

[RD-63] TKN Wireless Indoor Sensor network Testbed (TWIST), http://www.twist.tu-berlin.de/wiki/TWIST.

[RD-64] Vlado Handziski, Andreas Kopke, Andreas Willig, Adam Wolisz, ”TWIST: A Scalable and Reconfigurable Testbed for Wireless Indoor experiments with Sensor Networks”,.

[RD-65] T. Nieberg, S. Dulman, P. Havinga, L. van Hoesel and J. Wu, Collaborative Algorithms for Communication in Wireless Sensor Networks.Ambient Intelligence: Impact on Embedded Systems, edited by T.Basten and M.Geilen and H.de Groot, Kluwer Academic Publishers, November 2003

[RD-66] Jun-bin Liang, Ning-jiang Chen and Min-min Yu, “A Cloud Model Based Multi-dimension QoS Evaluation Mechanism for WSN”, in Proceedings of 2009 4th International Conference on Computer Science & Education.

[RD-67] Raman, B. and Chebrolu, K. 2008. Censor networks: a critique of "sensor networks" from a systems perspective. SIGCOMM Comput. Commun. Rev. 38, 3 (Jul. 2008), 75-78. DOI= http://doi.acm.org/10.1145/1384609.1384618

[RD-68] Langendoen, K.; Baggio, A.; Visser, O., "Murphy loves potatoes: experiences from a pilot sensor network deployment in precision agriculture," Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International , vol., no., pp.8 pp.-, 25-29 April 2006. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1639412&isnumber=34366.

[RD-69] Ceriotti, M., Mottola, L., Picco, G. P., Murphy, A. L., Guna, S., Corra, M., Pozzi, M., Zonta, D., and Zanon, P. 2009. "Monitoring heritage buildings with wireless sensor networks: The Torre Aquila deployment". In Proceedings of the 2009 international Conference on information Processing in Sensor Networks (April 13 - 16, 2009). Information Processing In Sensor Networks. IEEE Computer Society, Washington, DC, 277-288.

[RD-70] Min Song; Bei He, "Capacity Analysis for Flat and Clustered Wireless Sensor Networks," Wireless Algorithms, Systems and Applications, 2007. WASA 2007. International Conference on , vol., no., pp.249-253, 1-3 Aug. 2007.

[RD-71] Santa Fe Institute of Complex Systems: www.santafe.edu.

[RD-72] Russell, Monica. Deep Simplicity: Chaos, Complexity and the Emergence of Life [Book Review] [online]. Pacific Conservation Biology; Volume 13, Issue 1; 2007; 75. ISSN: 1038-2097.

[RD-73] Gupta, G.; Younis, M., "Fault-tolerant clustering of wireless sensor networks," Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE, vol.3, no., pp.1579-1584 vol.3, 20-20 March 2003.

[RD-74] Vlajic, N. and Xia D., "Wireless sensor networks: to cluster or not to cluster?", International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2006. WoWMoM 2006.

[RD-75] CONET Research Roadmap on Cooperating Objects.

[RD-76] Bechler, M.; Hof, H.-J.; Kraft, D.; Pahlke, F.; Wolf, L., "A cluster-based security architecture for ad hoc networks," INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies , vol.4, no., pp. 2393-2403 vol.4, 7-11 March 2004.

[RD-77] S. Prabh, K.; Abdelzaher, T.F., "On Scheduling and Real-Time Capacity of Hexagonal Wireless Sensor Networks", 2007. ECRTS '07. 19th Euromicro Conference on Real-Time Systems, pp.136-145, 4-6 July 2007.

[RD-78] Li, G., He, J., and Fu, Y. 2006. "A Hexagon-Based Key Predistribution Scheme in Sensor Networks". In Proceedings of the 2006 international Conference Workshops on Parallel Processing (August 14 - 18, 2006). ICPPW. IEEE Computer Society, Washington, DC, 175-180. DOI= http://dx.doi.org/10.1109/ICPPW.2006.9

[RD-79] M. Yarvis, A. Kushalnagar, H. Singh, Y. Liu and S. Singh, "Exploiting Heterogeneity in Wireless Sensor Networks", Proceedings of IEEE Infocom 2005.

[RD-80] A. Koubaa, M. Alves and E. Tovar, "Modeling and worst-case dimensioning of cluster-tree wireless sensor networks", in RTSS'06 Proc of 27th IEEE Real-Time Systems Symposium, IEEEPress 2006, pp.412-421.

[RD-81] C. Lu, et al., "RAP: A Real-Time Communication Architecture for Large-Scale Wireless Sensor Networks", in the proceedings of the IEEE Real-Time and Embedded Technology and Application Symposium, San Jose, CA.

[RD-82] 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.

[RD-83] A. Koubaa, M. Alves, E. Tovar, "IEEE 802.15.4: a Federating Communication Protocol for Time-Sensitive Wireless Sensor Networks", chapter of the book "Sensor Networks and Configurations: Fundamentals, Techniques, Platforms, and Experiments", Springer-Verlag, Germany, pp. 19 – 49, Jan. 2007.

[RD-84] A. Koubaa, E. Tovar, M. Alves, "Energy/Delay Trade-off of the GTS Allocation Mechanism in IEEE 802.15.4 for Wireless Sensor Networks", published in International Journal of Communication Systems, Vol. 20, No. 7, pp. 791-808, John Wiley & Sons, July 2007.

[RD-85] A. Koubaa, M. Alves, E. Tovar, A. Cunha, "An implicit GTS allocation mechanism in IEEE 802.15.4 for time-sensitive wireless sensor networks: theory and practice", published in Springer Real-Time Systems Journal, Volume 39, Numbers 1-3, pp 169 - 204, Springer, August 2008. Available at: http://www.springerlink.com/content/u203825646vv811r.

[RD-86] A. Koubaa, M. Alves, E. Tovar, "A Comprehensive Simulation Study of Slotted CSMA/CA for IEEE 802.15.4 Wireless Sensor Networks", published in proceedings of the 5th IEEE International Workshop on Factory Communication Systems (WFCS'06), Torino, Italy, June, 2006.

[RD-87] I. F. Akyilidiz, M. C. Vuran, O. B. Akan, W. Su, "Wireless Sensor Networks: A Survey Revisited", Computer Networks Journal, Elsevier Science, 2005.

[RD-88] Martínez, J., Garcí, A., Corredor, I., López, L., Hernández, V., and Dasilva, A. 2007. "QoS in wireless sensor networks: survey and approach". In Proceedings of the 2007 Euro American Conference on Telematics and information Systems (Faro, Portugal, May 14 - 17, 2007). EATIS '07. ACM, New York, NY, 1-8. DOI= http://doi.acm.org/10.1145/1352694.1352715.

[RD-89] A. Koubaa, R. Severino, M. Alves and E. Tovar, "Improving Quality-of-Service in Wireless Sensor Networks by Mitigating Hidden-Node Collisions", IEEE Transactions on Industrial Informatics, vol. 5, n. 3, pp. 299-313, August 2009.

[RD-90] TinyOS, www.tinyos.net.

[RD-91] Texas Instruments, IEEE802.15.4 Medium Access control (MAC) software stack.

[RD-92] Open-zb, Open Source Toolset for IEEE802.15.4 and ZigBee. Available at http://www.open-zb.net.

[RD-93] Ricardo Severino, "On the use of IEEE 802.15.4/ZigBee for Time-Sensitive Wireless Sensor Network Applications", 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-94] WirelessHART Specifications, Available on line at http://www.hartcomm.org/protocol/wihart/wireless_technology.html

[RD-95] Broadcom's Blutonium Silicon (BCM2004), http://www.broadcom.com/products/Bluetooth/Bluetooth-RF-Silicon-and-Software-Solutions

[RD-96] The Mulle, http://www.csee.ltu.se/~jench/mulle.html

[RD-97] Shek, L. L. and Kwok, Y. 2004. An integrated approach to scatternet traffic management in Bluetooth ad hoc networks. Comput. Netw. 45, 2 (Jun. 2004), 99-118. DOI= http://dx.doi.org/10.1016/j.comnet.2003.12.014

[RD-98] Mercier, A. and Minet, P., Introducing Service Differentiation in a Bluetooth Piconet, in NETWORKING 2004, Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications, LNCS 3042, Springer Verlag, 2004.

[RD-99] CARROZZA, G., CINQUE, M.. Modeling and Analyzing the Dependability of Short Range Wireless Technologies via Field Failure Data Analysis. Journal of Software, North America, 4, sep. 2009. At: http://www.academypublisher.com/ojs/index.php/jsw/article/view/0407707716/1105.

[RD-100] J. Eliasson, P. Lindgren, J. Delsing, "A Bluetooth-based Sensor Node for Low-Power Ad Hoc Networks", JOURNAL OF COMPUTERS, ACADEMY PUBLISHER, VOL. 3, NO. 5, MAY 2008.

[RD-101] A. El-Hoiydi and J. D. Decotignie, "Wisemac: an ultra low power mac protocol for the downlink of infrastructure wireless sensor networks," vol. 1, 2004, pp. 244-251 Vol.1. [Online]. Available: http://dx.doi.org/10.1109/ISCC.2004.1358412

[RD-102] Demirkol, I.; Ersoy, C.; Alagoz, F., "MAC protocols for wireless sensor networks: a survey," Communications Magazine, IEEE , vol.44, no.4, pp. 115-121, April 2006.

[RD-103] Yee Wei Law, Lodewijk van Hoesel, Jeroen Doumen, Pieter Hartel, Paul Havinga, “EnergyEfficient LinkLayer Jamming Attacks against Wireless Sensor Network MAC Protocols”. Available online at : http://doc.utwente.nl/57039/

[RD-104] M. Salajegheh, H. Soroush, and A. Kalis, “Hymac: Hybrid tdma/fdma medium access control protocol for wireless sensor networks”, in Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on, 2007, pp. 1-5. [Online]. Available: http://dx.doi.org/10.1109/PIMRC.2007.4394374

[RD-105] A. Rowe, R. Mangharam and R. Rajkumar, “RT-Link: A global time-synchronized link protocol for sensor networks”, in Elsevier Ad Hoc Networks 6 (2008) 1201–1220.

[RD-106] Miroslav Pajic, Rahul Mangharam, "Anti-Jamming for Embedded Wireless Networks". http://www.seas.upenn.edu/~rahulm/Research/Pubs/antijam_ipsn09.pdf

[RD-107] Chipcon CC2420 Datasheet. Available at http://www-inst.eecs.berkeley.edu/~cs150/Documents/CC2420.pdf

[RD-108] Z-MAC: a Hybrid MAC for Wireless Sensor Networks, Injong Rhee, Ajit Warrier, Mahesh Aia and Jeongki Min (Technical Report, Department of Computer Science, North Carolina State University, April 2005).

[RD-109] Li, Y.J.; Chen, C.S.; Song, Y.-Q.; Wang, Z, “Real-time QoS support in wireless sensor networks: a survey”. In Proc of 7th IFAC Int Conf on Fieldbuses & Networks in Industrial & Embedded Systems (FeT'07), Toulouse, France, Nov. 2007.

[RD-110] W. Ye, J. Heidemann, D. Estrin, and Abstract—this, "An energy-efficient mac protocol for wireless sensor networks," 2002. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.16.1535

[RD-111] V. Rajendran, K. Obraczka, and J. Garcia-Luna-Aceves, “Energy-efficient, collision-free medium access control for wireless sensor networks”, Wireless Networks, vol. 12, no. 1, pp. 63-78, February 2006. [Online]. Available: http://dx.doi.org/10.1007/s11276-006-6151-z

[RD-112] O. Gnawali, R. Fonseca, K. Jamieson, D. Moss and P. Levis, “Collection Tree Protocol”, ACM SenSys 2009 Berkeley, California, November 4-6 2009.

[RD-113] Dominik Ślęzak, Tai-hoon Kim, Wai-Chi Fang and Kirk P. Arnett, “Secure Collection Tree Protocol for Tamper-Resistant Wireless Sensors”, Security Technology, International Conference, SecTech 2009.

[RD-114] K. S. J. Pister, L. Doherty, “TMSP: Time Synchronized Mesh Protocol”, In Proc. Of the IASTED International Symposium on Distributed Sensor Networks (DSN), November 2008, >Orlando Florida, USA.

[RD-115] RFC 3610 - Counter with CBC-MAC (CCM), http://tools.ietf.org/html/rfc3610, September 2003. Available on line at http://tools.ietf.org/html/rfc3610.

[RD-116] "RPL: IPv6 Routing Protocol for Low power and Lossy Networks", draft-ietf-roll-rpl-05, December 2009. Available on line at: http://tools.ietf.org/html/draft-ietf-roll-rpl-05

[RD-117] "A Security Framework for Routing over Low Power and Lossy Networks", draft-tsao-roll-security-framework-01, September 2009. Available on line at: http://tools.ietf.org/html/draft-tsao-roll-security-framework-01.

[RD-118] W.R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks". In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences.

[RD-119] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks", Ad Hoc Networks, Volume 3, Issue 3, May 2005, Pages 325-349.

[RD-120] A.-B. Garcia-Hernando et al., “Problem Solving for Wireless Sensor Networks”, Springer-Verlag London, 2008.

[RD-121] Lan Yao, Na An, Fuxiang Gao, and Ge Yu, “A Clustered Routing Protocol with Distributed Intrusion Detection for Wireless Sensor Networks” In Advances in Data and Web Management

[RD-122] Lindsey, S.; Raghavendra, C.S., “PEGASIS: Power-efficient gathering in sensor information systems”, Aerospace Conference Proceedings, 2002. IEEE, vol.3.

[RD-123] Sohrabi, K.; Gao, J.; Ailawadhi, V.; Pottie, G.J., "Protocols for self-organization of a wireless sensor network," Personal Communications, IEEE , vol.7, no.5, pp.16-27, Oct 2000.

[RD-124] Seung Yi, Prasad Naldurg, Robin Kravets, “A Security-Aware Routing Protocol for Wireless Ad Hoc Networks”. In MobiHOC Poster Session, 2001

[RD-125] In-Sung Han, Hwang-Bin RYOU, Seok-Joong Kang, “Multi-Path Security-Aware Routing Protocol Mechanism for Ad Hoc Network”. In 2006 International Conference on Hybrid Information Technology.

[RD-126] W. Heinzelman, J. Kulik, H. Balakrishnan, Adaptive protocols for information dissemination in wireless sensor networks, in: Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'99), Seattle, WA, August 1999.

[RD-127] Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victorwen And David E. Culler, “SPINS: Security Protocols for Sensor Networks” in Wireless Networks journal, vol. 8, 521-534, 2002

[RD-128] Law, Y.W. and Dulman, S. and Etalle, S. and Havinga, P. (2002) Assessing Security-Critical Energy-Efficient Sensor Networks. Internal Report available at http://doc.utwente.nl/38381/1/00000087.pdf

[RD-129] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in MobiCom '00: Proceedings of the 6th annual international conference on Mobile Computing.

[RD-130] R. Shah and J. Rabaey, “Energy aware routing for low energy ad hoc sensor networks”, in Proc. Of IEEE Wireless Communications and Networking Conference (WCNC), Orlando, FL, March 2002.

[RD-131] Sung-Chul Jung; Hyoung-Kee Choi, "An energy-aware routing protocol considering link-layer security in wireless sensor networks," Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on , vol.01, no., pp.358-361, 15-18 Feb. 2009.

[RD-132] Park, P.G.; Fischione, C.; Bonivento, A.; Johansson, K.H.; Sangiovanni-Vincentelli, A., “Breath: A Self-Adapting Protocol for Wireless Sensor Networks in Control and Automation”, Sensor, Mesh and Ad Hoc Communications and Networks, 2008. SECON '08. 5th Annual IEEE Communications Society Conference on , vol., no., pp.323-331, 16-20 June 2008.

[RD-133] Yan Yu, Ramesh Govindan, Deborah Estrin, "Geographical and Energy Aware Routing: a recursive data dissemination protocol for wireless sensor networks", technical report (2001). Available at http://graphics.stanford.edu/courses/cs428-03-spring/Papers/readings/Networking/Estrin_geo-routing01.pdf.

[RD-134] J. N. Al-Karaki and A. E. Kamal. Routing techniques in wireless sensor networks: a survey. IEEE Wireless Communications, 11(6):6-28, 2004.

[RD-135] Brad Karp, H. T. Kung, “GPSR: greedy perimeter stateless routing for wireless networks”, Proceedings of the 6th annual international conference on Mobile computing and networking, Boston, Massachusetts, United States, pg 243 - 254, 2000. Available at: http://portal.acm.org/citation.cfm?id=345953

[RD-136] Atef Abdrabou and Weihua Zhuang, “A Position-Based QoS Routing Scheme for UWB Mobile Ad Hoc Networks”, IEEE J. Sel. Areas Comms. Vol. 24, NO. 4, April 2006.

[RD-137] Tian He, Stankovic, J.A., Chenyang Lu, Abdelzaher, T., "SPEED: a stateless protocol for real-time communication in sensor networks", Proceedings of 23rd International Conference on Distributed Computing Systems, 2003. Page(s):46 - 55.

[RD-138] E. Felemban, Chang-Gun Lee and Ekici, E., “MMSPEED: multipath Multi-SPEED protocol for QoS guarantee of reliability and Timeliness in wireless sensor networks”. IEEE Transactions on Mobile Computing, Volume 5, Issue 6, pages 738-754, June, 2006.

[RD-139] ZigBee Alliance, http://www.zigbee.org

[RD-140] Sun Spots FAQ, http://www.sunspotworld.com/docs/general-faq.php

[RD-141] Motorola neuRFon, http://www.motorola.com/content.jsp?globalObjectId=290

[RD-142] G. Cugola, M. Hellenschmidt, V. Gehrmann, F. Kadhar, N. Mitton, M. Hauspie, J. Carle, D. Simplot-Ryl, S. Schlumbohm, P. van der Stok, M. Aoun, J. Ansari, D. Blasi, J.-D. Decotignie and L. von Allmen, "D4.1: Updated state of the art in communication protocols with associated partner expertise", WASP IST-034963 Public report, 2007

[RD-143] Ken Masica, “Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments”, Lawrence Livermore National Laboratory, U.S. Department of Homeland Security, April 2007. Available online at: http://csrp.inl.gov/Documents/Securing%20ZigBee%20Wireless%20Networks%20in%20Process%20Control%20System%20Environments.pdf

[RD-144] Daintree Networks, “Getting Started with ZigBee and IEEE 802.15.4”, White Paper, Feb. 2008 http://www.daintree.net/downloads/whitepapers/zigbee_primer.pdf.

[RD-145] 6LoWPAN Standard, http://www.6lowpan.org

[RD-146] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, “RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks”, September 2007. Available at http://tools.ietf.org/html/rfc4944

[RD-147] G. Montenegro, N. Kushalnagar, C. Shumacher, “RFC 4919: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals”, August 2007, Available at http://tools.ietf.org/html/rfc4919

[RD-148] Berkeley IP implementation for low-power networks (BLIP), 6LowPAN on TinyOS, http://smote.cs.berkeley.edu:8000/tracenv/wiki/blip

[RD-149] Washington University in St. Louis, 6LowPAN on T-mote Sky, http://www.cse.wustl.edu/~jain/cse567-08/ftp/7lowpan/index.html#sec2

[RD-150] Swedish Institute of Computer Science, 6LowPAN on Contiki, http://www.sics.se/~adam/contiki/docs-uipv6/a01109.html

[RD-151] Joel K. Young, "What a Mesh! Part 2-Networking Architectures and Protocols", December 2008, Available online at: http://www.sensorsmag.com/networking-communications/wireless-sensor/what-a-mesh-part-2-networking-architectures-and-protocols-1544.

[RD-152] Jonathan Hui, David Culler, Samita Chakrabarti, “6LoWPAN: Incorporating IEEE 802.15.4 into the IP architecture” in Internet Protocol for Smart Objects (IPSO) Alliance. Available online at: http://www.ipso-alliance.org/Documents/IPSO-WP-3.pdf.

[RD-153] 6LoWPAN: The Wireless Embedded Internet, http://6lowpan.net/the-book

[RD-154] ROLL (Routing Over Low power and Lossy networks) Status Pages, http://tools.ietf.org/wg/roll/

[RD-155] WiMAX Forum, http://www.wimaxforum.org

[RD-156] IEEE802.16 Wireless Metropolitan Area Networks standards, http://grouper.ieee.org/groups/802/16

[RD-157] IEEE802.20 Mobile Broadband Wireless Access (MBWA), http://grouper.ieee.org/groups/802/20

[RD-158] G. Nair, J. Chou, T. Madejski, K. Perycz, D. Putzolu, J. Sydir, “IEEE 802.16 Medium Access Control and Service Provisioning”, Intel Technology Journal, Vol. 8, Issue 3, 2004

[RD-159] Intel® WiMAX/WiFi Link 5350 and Intel® WiMAX/WiFi Link 5150, http://www.intel.com/network/connectivity/products/wireless/wimax/wifi/index.htm.

[RD-160] HTC Max4G, http://www.htc.com/www/product/max4g/overview.html

[RD-161] Nokia N810, http://conversations.nokia.com/2008/04/02/wimax-has-landed-update

[RD-162] G.S.V. Radha K. Rao, G. Radhamani “WiMAX: A Wireless Technology Revolution”, Auerbach Publications, ISBN-13: 978-0849370595, 1st edition, 2007/11/19

[RD-163] Wireless sensor network research group, http://www.sensor-networks.org/index.php?page=0823923911

[RD-164] Libelium Wireless Sensor Networks motes, Waspmote, http://www.libelium.com/products/waspmote

[RD-165] Chengyuan Peng, "GSM and GPRS Security", http://www.tml.tkk.fi/Opinnot/Tik-110.501/2000/papers/peng.pdf

[RD-166] Christos Xenakis, "Security Measures and Weaknesses of the GPRS Security Architecture" in International Journal of Network Security, Mar. 2008. http://ijns.femto.com.tw/contents/ijns-v6-n2/ijns-2008-v6-n2-p158-169.pdf.

[RD-167] Ruohonen, T.; Ukkonen, L.; Soini, M.; Sydanheimo, L.; Kivikoski, M., "Quality and reliability of GPRS connections," Consumer Communications and Networking Conference, 2004. CCNC 2004. First IEEE , vol., no., pp. 268-272, 5-8 Jan. 2004 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1286870&isnumber=28685

[RD-168] GainSpan’s low power WiFi module, http://www.gainspan.com

[RD-169] Elecktor WiFi sensor network module, http://www.elektor.com/news/wi-fi-sensor-network-module-has-5-year-battery.925156.lynkx

[RD-170] Explorative Environments: Zigbee WiFi sensor network module, http://www.explorative-environments.net/2006/07/10/zigbee-wifi-sensor-networks

[RD-171] Lewis Adams, "Capitalizing On 802.11 For Sensor Networks: Low-Power Wireless Sensor Networks", White Paper, Gainspan Corporation. Available on line at http://www.gainspan.com/docs2/GS_80211_networks-WP.pdf

[RD-172] Daniel M. Dobkin, Bernard Aboussouan “Low Power Wi-Fi™ (IEEE 802.11) For IP Smart Objects”, White Paper, GainSpan Corporation, 2009. Available online at:

http://www.gainspan.com/docs2/Low_Power_Wi-Fi_for_Smart_IP_Objects_WP_cmp.pdf

[RD-173] Embedded WiSeNts - Project FP6-004400. http://www.embedded-wisents.org.

[RD-174] Large-Scale Demonstration of Self-Organizing Wireless Sensor Networks, http://webs.cs.berkeley.edu/800demo.

[RD-175] First-of-its-kind Ad Hoc/Sensor Network Testbed at Virginia Tech, http://www.ece.vt.edu/news/fall05/sensornetwork.html.

[RD-176] Global Energy Optimisation for Distributed heterogeneous Embedded Systems (GEODES), http://geodes.ict.tuwien.ac.at

[RD-177] tinyLUNAR: tiny Lightweight Underlay Network Ad-hoc Routing, http://www.crysys.hu/~acs/publications/AcsB08pp.pdf, http://www.ist-ubisecsens.org/deliverables/D0.2_310307.pdf

[RD-178] PANEL: Position-based Aggregator Node Election, http://www.ist-ubisecsens.org/publications/ButtyanS07mass.pdf

[RD-179] DTSN: Distributed Transport for Sensor Networks, http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4381601, http://www.ist-ubisecsens.org/publications/DTSN-EuroNGI08.pdf

[RD-180] DSDV - Destination-Sequenced Distance Vector Routing. http://www.cs.virginia.edu/~cl7v/cs851-papers/dsdv-sigcomm94.pdf

[RD-181] NanoTCP - TCP for restricted devices.http://cst.imp.fu-berlin.de/teaching/WS0506/19542-V/documents/nanoip.pdf

[RD-182] GPSR - Greedy Perimeter Stateless Routing. http://www.eecs.harvard.edu/~htk/publication/2000-mobi-karp-kung.pdf

# 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.

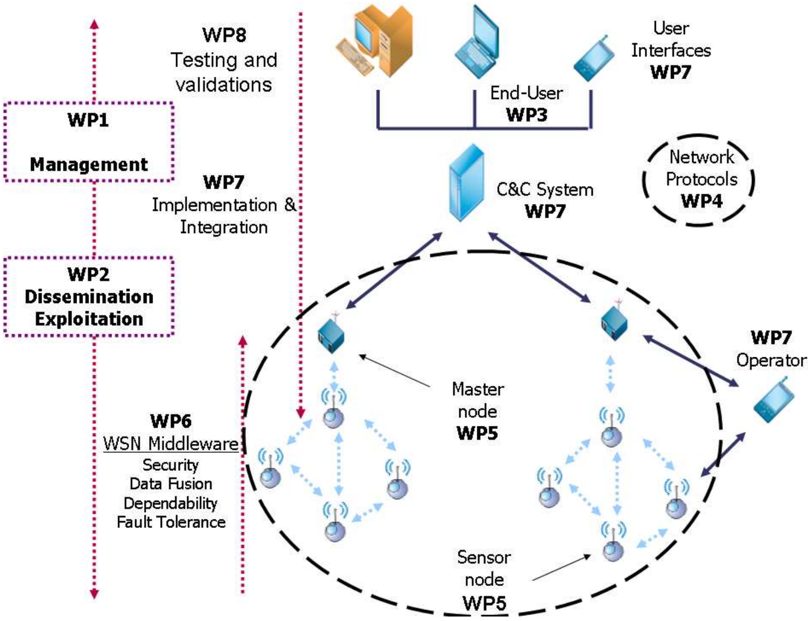

Figure 1 - EMMON system overview and work package decomposition

## 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.

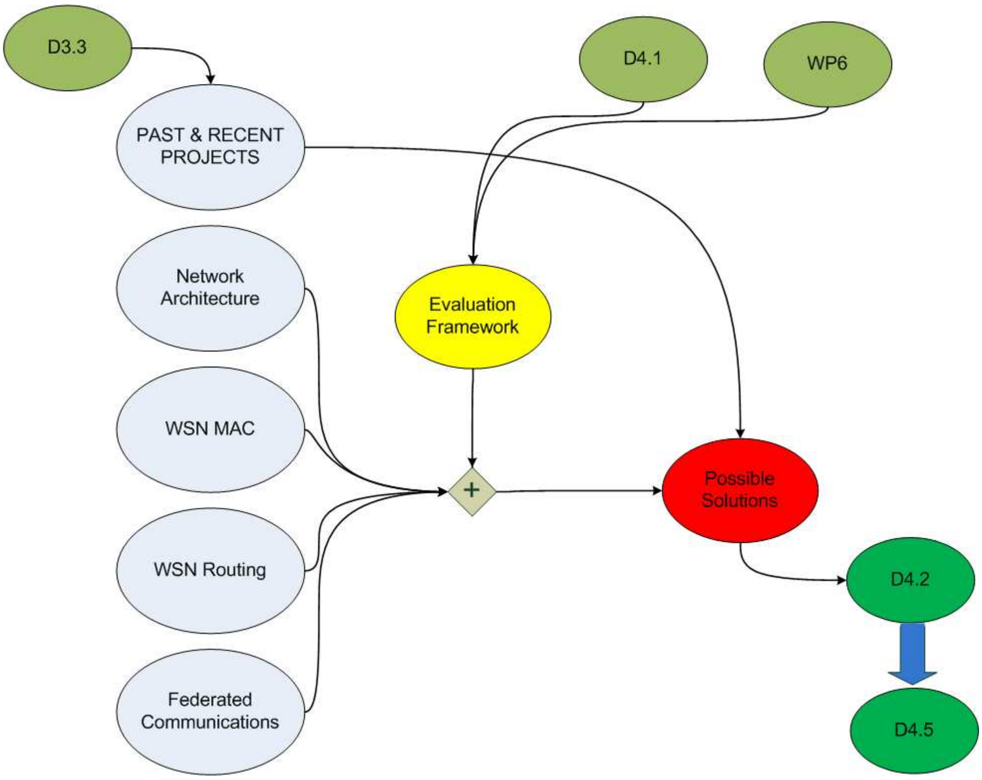

Figure 2 - Methodology used for this document

This methodology works as follows. First we collect a set of technology for network architectures, communication protocols and federated communications. These solutions are evaluated using the framework described next in Section 4.1, Criteria For Evaluating Technologies. In parallel, moving from the inputs of Deliverable D3.3 – Description of research and studies performed before the project, that are considered relevant for the end-user scenarios, we identify a set of past and recent projects, compatible with the EMMON goals, that can be used as a reference for inferring useful information. These projects are evaluated without a specific framework, but with an informal description of their general features and using the scope document [AD-4] as a guideline to identify the most important lessons to be inferred. Combining evaluation of technologies, lesson learned from real world deployments and the requirements suggested by the End Users (first inputs from [AD-7]), which give as a way to weight the criteria, we are able to obtain a set of possible solutions by composing the best ones into a system stack. This represents the main output of this deliverable D4.2 and, in turn, the input of next deliverable D4.5, which should evaluate more quantitatively the proposed solutions, trying to find the best one to be adopted for EMMON.

## 4.1 Criteria For Evaluating Technologies

### 4.1.1 Description

In this section we list the criteria we used to evaluate the available technologies. These criteria are derived from the specific requirements for EMMON, already evidenced in the Deliverable D4.1 [AD-3], as well as from inputs coming from WP6.

The criteria identified are listed and described in what follows.

#### *4.1.1.1 Scalability*

For the WSN, the term “scale” applies to the number (fewer or more nodes in the overall system) or geographical region under coverage (smaller or wider, 2D or 3D). The ability of a WSN system to easily/transparently adapt itself to these dynamic changes in scale is named “scalability”.

In the specific frame of the EMMON project, network architecture should be able to easily/transparently scale up to:

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

#### *4.1.1.2 Heterogeneity*

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

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

The EMMON network architecture must be designed in a way that all these levels of heterogeneity are transparent to the users.

#### *4.1.1.3 Timeliness*

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

In this framework, recalling our intended definition of real-time as in [AD-5]: “data that is only correct if it is provided in a defined time interval since its collection”, we note that each application will impose particular timeliness requirements to the underlying communication/networking infrastructure, so the latter should:

- Enable a minimum data generation rate per sensing node (also considering in-node data aggregation); these minimum data generation rates may be different from node to node;
- Be able to provide deterministic or probabilistic guarantees on the message delays, in a way that both real-time and non real-time applications can be supported;

#### 4.1.1.4 Reliability / Robustness

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

Generally speaking, a component is reliable, robust or fault tolerant, if it provides services complying with their specifications in spite of faults. Therefore, for a WSN network to be reliable, sensor, node and communication failures must be contained so that the overall network is fault-tolerant.

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

In particular, while link reliability mechanisms (e.g. MAC ARQ) can significantly reduce the end-to-end packet loss ratio, some critical WSN applications require high or even total end-to-end reliability, achievable through reliable transport layer protocol. On the other hand, some of these applications require packet-driven reliability (all sent packets must reach the destination) while others only require event-driven reliability (the event must be detected). As a consequence, in this framework we can consider the Mean Time To Fail (MTTF) as a generic reference metric for evaluating reliability.

#### 4.1.1.5 Resiliency

A complementary part of robustness is resiliency, or "fault recovery speed", i.e. the ability of a component or a network to quickly recover from a fault. In this case, we can relate on MTTR, i.e., Mean Time To Recover.

In the case of wireless communication protocols, the acronym also stands for MTTRetransmit in that retransmission is the most common recovery action. In fact, recovery could also concern crashed nodes to replace or faulty links (re-routing): however, retransmission time can be used as the reference metrics in all these cases as well.

#### 4.1.1.6 Energy Efficiency

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

In order to achieve energy-efficiency, in the EMMON project we should address technologies which guarantee the following characteristics:

- Efficient use of processing and radio communication, thus reducing the required energy.
- Maintaining nodes in low-power modes (“sleep”) most of the time. As a consequence, the solutions addressed should avoid the overhearing problem, minimize the idle listening periods and reduce the signal acquisition and processing periods.
- Since the required transmission power increases as the square of the distance between the sender and the receiver, it is preferable to use multiple short hops to transmit a message from a source to a destination in detriment of one long transmission hop,

Achieving a system lifetime that corresponds to end user expectations (and possibly requirements) will also have to take into consideration the available technology in terms of sensor nodes and power supplies.

#### 4.1.1.7 Interoperability

Since the objective of this deliverable is to find two or three possible solutions (i.e. stacks) by composing technologies at different layers, Interoperability criterion concerns the flexibility of the solution under investigation to be efficiently “stackable” with other. In particular it is of paramount importance to recognize that the best solution, e.g., at the MAC layer may not fit the best solution at the routing layer. This mismatch problem leads to delays in the application development.

#### 4.1.1.8 Data Aggregation / Compression Mechanisms

In WSN, sensor measurements at the nodes are usually collected by a node or a set of nodes for further processing and analysis. Since raw sensor data contain redundancies and correlations, the usage of data aggregation can reduce the number of transmissions by reducing the amount of data to be transmitted, thus significantly contributing to achieve energy efficiency

In the EMMON network architecture, the technologies should allow for implementing data aggregation mechanism, i.e. to compute aggregated quantities with a time complexity that is either constant or increases slowly with the number of nodes and the extant of the geographical region of deployment.

#### 4.1.1.9 Traffic Differentiation

In EMMON, based on the application scenario, the network will show both reactive and proactive behaviour. The reactive behaviour will come from alarm condition detection and should generate (high priority) traffic to the collector node according to an event driven delivery model. The proactive behaviour comes from the monitoring of environmental status and should generate (low priority) traffic to the collector node according to a periodic delivery model. Hence, the WSN has to be designed for a combination of at least two traffic types, which should be further supported end-to-end, i.e. across the different network tiers.

#### 4.1.1.10 *Security*

Below are presented the crucial security properties required by sensor networks, and show how they are directly applicable in a typical sensor network.

- **Confidentiality**: The confidentiality service protects system data and information from unauthorized disclosure, keeping information secret from unauthorized parties. Confidentiality of data in a sensor network is achievable only if those with access to network data are authorized to do so. Under no circumstances should sensor readings leak outside the network. The standard approach for preventing this from happening is to use encryption. This requires the use of a secret key that only intended receivers possess.
- **Data authentication**: Prevents unauthorized parties from participating in the network and legitimate nodes should be able to detect messages from unauthorized nodes and reject them. The process of authentication of both network data and users is very important in preserving network data integrity and preventing unauthorized access to the network. Without authenticating mechanisms in place, an attacker can easily access the network and inject dangerous messages without the receivers of the new altered data knowing and making sure that the data being used originates from a malicious source.
- **Data integrity**: The integrity of data in any network means that data in that network is genuine, undiluted without authorization. This implies that data between the sender and the receiver is unaltered in transit by an adversary. Just like data confidentiality, data in transition between the sending and receiving parties is susceptible to many threats like, eavesdropping, disruption, hijacking, and rushing whose goal is to intercept the data and alter it based on their motives.
- **Data Freshness**: In sensor networks, special security requirements such as message freshness are necessary. Data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages [RD-127]. There are two types of freshness: weak freshness, which provides partial message ordering, but carries no delay information, and strong freshness, which provides a total order on a request-response pair, and allows for delay estimation. Weak freshness is required by sensor measurements, while strong freshness is useful for time synchronization within the network

It is not possible to ensure the confidentiality, integrity, authentication, and freshness of data in the communication networks without paying attention to the following issues (especially for wireless sensor networks): Data aggregation, Anti-jamming, Access control, Key management, Link layer encryption, Data replication, Resilience to node capture.

#### 4.1.1.11 *Hardware Support*

When analysing the technologies, and accessing their feasibility when applied to the EMMON project, a very important aspect to consider is the hardware support for a particular technology. Some technologies might present specific hardware requirements (such as the frequency range of the transmitted signals, for example), which in turn imposes restrictions on the hardware platforms available to fulfil those requirements.

This criterion therefore aims to identify any hardware platforms (motes) from among those studied on WP5 [AD-6] that support any of the topics discussed in this deliverable, in order to provide a clear picture of what are the available hardware platforms for each of the technologies under evaluation.

#### *4.1.1.12 Technical Maturity*

EMMON is an industrial project. This leads to evaluate available technologies also based on their maturity and proved efficiency in real (or equivalent) deployments.

As a consequence, this criterion is about the response to the following questions:

- Availability of Simulation code: are simulation codes or simulator available for testing current solution performance?
- Availability of Implementation code: is an implementation code available for the current solution? If yes, for which kind of operating system and platform?
- Availability of Tutorials or technical reports: are technical documents or tutorials available in literature to deeply understand the current solution?

#### *4.1.1.13 Availability of Internal Experience*

This last criterion aims at identifying if there is expertise within the consortium for a given technology, which is a fundamental issue to be able to build a working system.

### 4.1.2 Ranking Scheme

Once established the list of criteria, a scheme for ranking the “goodness” of each technology for each criteria has to be built. Since we move from a set of solutions so far proposed in literature for each technology, it would make sense to evaluate the criteria based on the following scheme.

1. Issue explicitly addressed in the references found:

    a. The solution proposed is an optimal solution also for EMMON, i.e. in large scale densely deployed wireless sensor networks;

    b. The solution proposed is a not very good or a bad solution for EMMON, i.e. in large scale densely deployed wireless sensor networks.

2. Issue not explicitly addressed in the references found:

    a. Easy to implement without affecting remarkably the performance;

    b. Difficult to figure out how to implement or how it impacts other performance.

“Issues” are the criteria listed in the following sections.

Based on this scheme, points ‘1’ and ‘2’ are “objective”, while points ‘a’ and ‘b’ are “subjective” and the evaluation of the criteria strongly rely on the experience of who is judging.

The adopted ranking criterion is in the following scheme:

- 1a -> Score 1 (Best)
- 2a -> Score 2
- 1b -> Score 3
- 2b -> Score 4 (Worst)

Finally, this scheme is summarized in Figure 3.

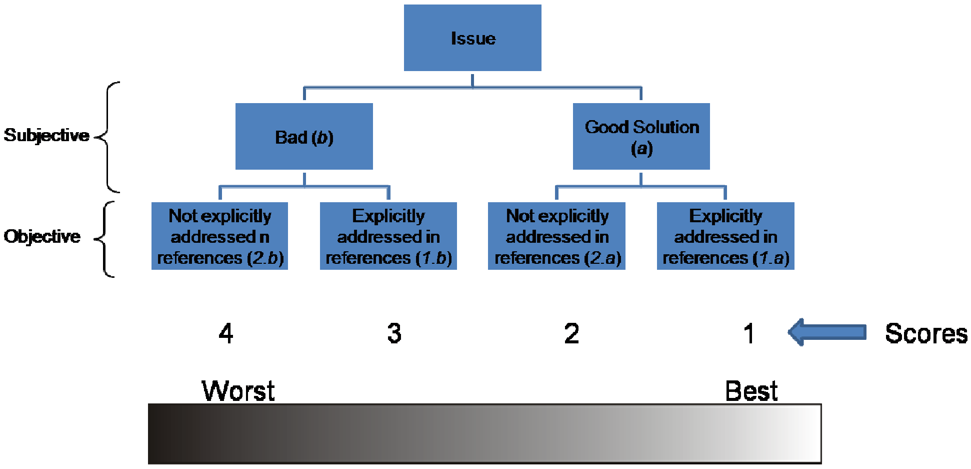
Issue
Subjective
Bad (b)
Good Solution (a)
Objective
Not explicitly addressed n references (2.b)
Explicitly addressed in references (1.b)
Not explicitly addressed in references (2.a)
Explicitly addressed in references (1.a)
4
3
2
1
Scores
Worst
Best

Figure 3 - Criteria evaluation and ranking.

For the specific case of the “Hardware Support” criterion, the ranking system is based on the following rules:

- Scores will be binary, i.e. limited to values “1” or “4”;
- A score of 1 means that there is at least one hardware platform that supports the technology;
- A score of 4 means that there is no hardware platform supporting the technology available, it requires further development, or it is hard to figure out whether the hardware supports it or not;
- The hardware platforms under consideration for this criterion are the one that compose the final shortlist of motes found on deliverable D5.1 [AD-6]. These are the best candidates identified by WP5 on that deliverable.

# 5. Possible Solutions

Based on the evaluation of the available technologies that will be presented in Section 7 to Section 10, and moving from the lessons learned from real deployment experiences summarized in Section 6.19, we can weigh the above requirements based on a set of priority levels, as follows:

1. High priority: a criterion absolutely required by the EMMON final goals or identified as fundamental in Section 6.19. The suggested weight for this priority level is 15.

2. Medium priority: moving from a modular design paradigm, the criteria belonging to this priority class are required to build a platform having the most basic features, which will be further refined in the successive design cycles. The suggested weight for this priority level is 10.

3. Low priority: the criteria belonging to this priority class are required to refine the platform by extending their basic functionalities via add-on features. The suggested weight for this priority level is 5.

It is worth to note that all the criteria we used to evaluate the technologies are required to build the final WSN platform for the EMMON project. Nevertheless, in this phase, by applying the lessons learned about keeping simplicity and using a modular design methodology, we propose to assign each criterion with a priority level as in the following scheme and resumed in Table 2:

- Scalability: this is a high priority criterion because it directly involves the EMMON requirement of large scale deployments.
- Heterogeneity: since we use a modular design methodology, we may consider the feature that the proposed solution can handle different hardware and software components (i.e. heterogeneity) as a low priority requirement.
- Timeliness: since environmental monitoring applications may not require very stringent latency constraints, except in case of some alarms have to be dealt with, this can be a low priority requirement.
- Reliability / Robustness: this is a medium priority requirement because it has to be part of the basic features to be implemented first.
- Resiliency: as for timeliness, this requirement can have a low priority.
- Energy efficiency: this is typically an essential requirement in WSNs, but in some scenarios, the availability of external power sources suggest to consider it as medium priority.
- Interoperability: since our methodology is based on the composition of technologies at several communication layers, as learned from Section 6.19, this must be considered a high priority requirement.
- Data aggregation: since some scenarios may not require stringent constraints on the implementation of data aggregation mechanisms, this requirement can be a low priority.
- Traffic differentiation: this is an important requirement for those scenarios where alarms may be triggered and should be notified to a remote station before other traffic. In our methodology, it can be considered as a low priority requirement.

- Security: this requirement impacts the usefulness of the proposed solutions at different levels[3]. In particular, for an environmental monitoring application, data integrity can be considered an essential feature, while confidentiality may be a useful add-on. Therefore, we have chosen to assign a medium priority level to this requirement.
- Hardware support: this is an important condition since it impacts the feasibility of the proposed solution on the candidate hardware platform, chosen by Work Package 5 in D5.1 [AD-6]. As a consequence, we consider it as a medium priority requirement.
- Technical maturity: as learned from Section 6.19, this must be considered a high priority requirement for the success of a real deployment.

| Criterion | Priority level | Weight value |
|---|---|---|
| Scalability | High | 15 |
| Heterogeneity | Low | 5 |
| Timeliness | Low | 5 |
| Reliability / Robustness | Medium | 10 |
| Resiliency | Low | 5 |
| Energy efficiency | Medium | 10 |
| Interoperability | High | 15 |
| Data aggregation | Low | 5 |
| Traffic differentiation | Low | 5 |
| Security | Medium | 10 |
| Hardware support | Medium | 10 |
| Technical maturity | High | 15 |

Table 2: Criteria to priority levels mapping

Moreover, since we are convinced that the availability of expertise internal to the consortium in some technology is the key for a project to be successful, we assigned a bonus to the final score of a technology in the case when some partner strongly knows it.

Table 3 shows the results of this evaluation framework applied to the technologies presented in Sections 7 to 10. In the following sections, we propose two alternative solutions, which refer to the high level scheme depicted in Figure 4, where the only assumption we made is that IP is explicitly used as the base networking protocol for the higher tiers of the system. Furthermore, in the lower tiers of Figure 4 we have identified two possible alternatives: one is to use a Communication Framework (like 6LoWPAN or ZigBee), the other one is to use a routing algorithm (i.e. one of those presented in Section 9), with eventually added modules to recover the functionalities of a full Network Layer (i.e. network management by implementing addressing mechanisms, fragmentation/reassembly of packets, and so on).

[3] The DoS attack, by jamming, is one of the most common attacks and is easy to implement on WSN. WSN are especially vulnerable to this attack type. To prevent these attacks, some solutions (protocols) are implemented at WSN MAC / Datalink layers and should be considered as necessary features. On the other hand data integrity is very important. Data that is not genuine, as well being useless, may initiate false alarms. In environmental monitoring applications, message freshness is a requirement. Data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages.

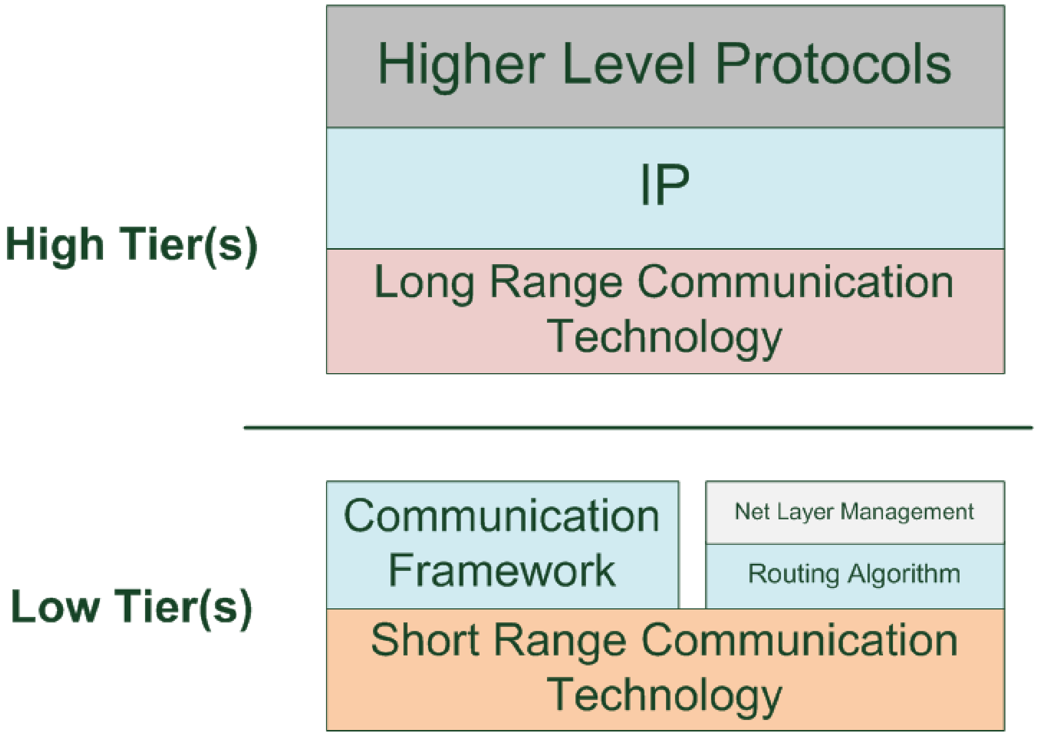

Figure 4: Multi Tier alternative schemes.

## 5.1 Alternative Solution 1

The first solution we can identify is built upon the best[4] solution for each technology:

- Network Architecture: multi-tier or backbone-based (Section 7.2.4).
- Short Range Communication technology: IEEE 802.15.4 or IEEE 802.15.4a (PHY) standards (Section 8.2.1).
- WSN Routing algorithm: Collection Tree Routing protocol (Section 9.2.1).
- Long Range Communication technology: 2G/3G (Section 10.2.4).

In this solution we can imagine that the WSN is composed by a large set of IEEE802.15.4-based nodes grouped into patches. In each group, constituting the lower tier of the network, a simple data gathering protocol as the Collection Tree Protocol (CTP) is used as the routing algorithm at the network layer. Each patch has one or more gateways, constituting the higher tier of the network, composed by e.g. GPRS-enabled devices forming a backbone or able to communicate directly with a remote C&C host over an IP based internet connection.

In a first approximation, the main advantage of this solution is its simplicity.

[4] The best solutions are chosen according to our evaluation framework, summarized in Table 3. These solutions may eventually be slightly modified based on further inputs we might receive from Work Package 5, about the final selected HW/SW platform, and Work Package 3, about the final End User application requirements.

## 5.2 Alternative Solution 2

As an alternative solution[5] we can assume the following:

- Network Architecture: multi-tier or backbone-based (Section 7.2.4).
- Short Range Communication technology: IEEE 802.15.4 or IEEE 802.15.4a (PHY) standards (Section 8.2.1).
- Communication framework: 6LoWPAN-based (Section 10.2.2).
- Long Range Communication technology: 2G/3G (Section 10.2.4).

As before, we can imagine the WSN composed by IEEE802.15.4-based nodes, but the presence of the 6LoWPAN-based framework allows these nodes to be readily connected to other IP-based networks, without the need for intermediate translator entities.

This solution has the advantage of allowing for IP – IP based communications between higher level devices and WSN nodes.

## 5.3 Conclusions

As a general remark, we would like to underline that, moving from the evaluation done in this work, i) the multi-tier backbone based architecture is far the best network architecture and ii) the IEEE 802.15.4 and IEEE 802.15.4a communication standards are the best for MAC and Datalink layer technologies.

Furthermore, while it is expected that the IEEE802.15.4 standard would have been a natural choice for EMMON scenarios, the use of a multi-tiered architecture raises a number of questions, 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).

Moreover, it is important to remark that the solutions presented in Section 5.1 and Section 5.2 are just two alternative starting points for deriving the final communication stack for EMMON. Since both solutions actually present some missing details, e.g. the network management mechanisms (like addressing, framing, …) to be combined with the CTP protocol in solution one or the type of routing algorithm (like CTP or even simpler tree routing protocols) in the 6LoWPAN-based framework of solution two, a deeper investigation is needed along these two proposed directions.

Nevertheless, these details are out of the scope of this deliverable and hence will be investigated in the D4.5 deliverable.

[5] These solutions may eventually be slightly modified based on further inputs we might receive from Work Package 5, about the final selected HW/SW platform, and Work Package 3, about the final End User application requirements.

| Evaluation Framework | | Scalability | Heter. | Timeliness | Reliability / Robustness | Resiliency | Energy efficiency | Interop. | Data aggr. / compr. mechanisms | Traffic differentiation | Security | Hardware support | Technical maturity | Availability of exp. internal to the consortium | TOT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Weights** | | **15** | **5** | **5** | **10** | **5** | **10** | **15** | **5** | **5** | **10** | **10** | **15** | **-10** | SUM(Score *Weight) |
| Net. Arch. | Flat | 4 | N/A | 4 | 4 | 2 | 2 | 1 | 3 | N/A | 4 | N/A | 3 | 1 | 255 |
| | Cluster based | 1 | | 1 | 1 | 1 | 1 | 3 | 1 | | 1 | | 1 | 1 | 110 |
| | Hexagonal | 3 | | 3 | 2 | 2 | 3 | 4 | 3 | | 1 | | 3 | 1 | 240 |
| | Multi-tier (or backbone-based) | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | | 1 | 1 | 80 |
| | Real Time Architecture | 1 | | 1 | 4 | 1 | 4 | 1 | 4 | | 4 | | 4 | 0 | 240 |
| WSN MAC and DATA-LINK Layer | IEEE 802.15.4 / IEEE 802.15.4a | 2 | 3 | 1 | 2 | 2 | 1 | 1 | N/A | 1 | 3 | N/A | 1 | 1 | 145 |
| | Wireless HART | 3 | 2 | 3 | 2 | 2 | 3 | 2 | | 4 | 1 | | 1 | 0 | 205 |
| | BlueTooth low-power | 3 | 3 | 2 | 2 | 2 | 1 | 3 | | 1 | 1 | | 2 | 1 | 190 |

| Evaluation Framework | | Scalability | Heter. | Timeliness | Reliability / Robustness | Resiliency | Energy efficiency | Interop. | Data aggr. / compr. mechanisms | Traffic differentiation | Security | Hardware support | Technical maturity | Availability of exp. internal to the consortium | TOT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Weights** | | **15** | **5** | **5** | **10** | **5** | **10** | **15** | **5** | **5** | **10** | **10** | **15** | **-10** | SUM(Score *Weight) |
| | WiseMAC | 3 | 2 | 3 | 3 | 3 | 3 | 3 | | 3 | 4 | | 3 | 0 | 290 |
| | HyMAC | 1 | 1 | 1 | 2 | 2 | 1 | 2 | | 2 | 4 | | 3 | 0 | 190 |
| | RT-Link | 3 | 2 | 3 | 3 | 3 | 3 | 3 | | 4 | 4 | | 3 | 1 | 285 |
| | Z-MAC | 1 | 2 | 2 | 2 | 4 | 1 | 2 | | 2 | 4 | | 1 | 0 | 180 |
| | S-MAC | 1 | 2 | 4 | 2 | 2 | 1 | 2 | | 4 | 4 | | 1 | 0 | 190 |
| | TRAMA | 1 | 2 | 3 | 2 | 2 | 1 | 2 | | 2 | 4 | | 3 | 0 | 205 |
| | | | | | | | | | | | | | | | |
| WSN Routing and Network Layer | Collection Tree Protocol | 1 | 2 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 | N/A | 1 | 0 | 140 |
| | Time Synched Mesh Protocol | 3 | 3 | 3 | 1 | 2 | 3 | 3 | 4 | 4 | 1 | | 1 | 0 | 235 |

| **Evaluation Framework** | Scalability | Heter. | Timeliness | Reliability / Robustness | Resiliency | Energy efficiency | Interop. | Data aggr. / compr. mechanisms | Traffic differentiation | Security | Hardware support | Technical maturity | Availability of exp. internal to the consortium | TOT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Weights** | **15** | **5** | **5** | **10** | **5** | **10** | **15** | **5** | **5** | **10** | **10** | **15** | **-10** | SUM(Score *Weight) |
| RPL (ROLL routing protocol) | 2 | 1 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | | 4 | 0 | 210 |
| LEACH | 4 | 3 | 3 | 3 | 3 | 3 | 3 | 1 | 1 | 3 | | 1 | 0 | 265 |
| PAGASIS | 3 | 2 | 3 | 4 | 4 | 3 | 4 | 1 | 1 | 3 | | 3 | 0 | 305 |
| SAR | 3 | 1 | 1 | 2 | 2 | 1 | 1 | 2 | 1 | 3 | | 3 | 0 | 200 |
| SPIN | 1 | 1 | 3 | 4 | 4 | 3 | 1 | 3 | 4 | 3 | | 3 | 0 | 250 |
| Directed Diffusion | 3 | 1 | 3 | 4 | 4 | 1 | 2 | 3 | 4 | 4 | | 3 | 0 | 285 |
| Energy aware routing | 3 | 2 | 3 | 4 | 4 | 1 | 1 | 4 | 1 | 4 | | 3 | 0 | 265 |
| Breath | 3 | 2 | 1 | 3 | 3 | 1 | 2 | 4 | 4 | 4 | | 3 | 0 | 270 |

| Evaluation Framework | | Scalability | Heter. | Timeliness | Reliability / Robustness | Resiliency | Energy efficiency | Interop. | Data aggr. / compr. mechanisms | Traffic differentiation | Security | Hardware support | Technical maturity | Availability of exp. internal to the consortium | TOT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Weights | | 15 | 5 | 5 | 10 | 5 | 10 | 15 | 5 | 5 | 10 | 10 | 15 | -10 | SUM(Score *Weight) |
| | GEAR | 3 | 2 | 3 | 2 | 4 | 1 | 1 | 3 | 4 | 4 | | 3 | 0 | 255 |
| | GPSR | 1 | 1 | 3 | 2 | 4 | 4 | 2 | 3 | 1 | 4 | | 3 | 0 | 250 |
| | SPEED | 1 | 1 | 1 | 3 | 3 | 4 | 1 | 4 | 3 | 4 | | 2 | 0 | 230 |
| | MMSPEED | 1 | 1 | 1 | 1 | 1 | 4 | 3 | 4 | 1 | 4 | | 2 | 0 | 220 |
| Fed. Comm. | Zigbee | 3 | 2 | 3 | 2 | 2 | 1 | 2 | N/A | 1 | 1 | 1 | 2 | 1 | 185 |
| | 6LoWPAN | 1 | 1 | 1 | 2 | 2 | 1 | 2 | | 1 | 3 | 1 | 2 | 0 | 170 |
| | WiMAX / Mobile Broad. Wireless Access | 1 | 2 | 1 | 2 | 2 | 1 | 2 | | 1 | 1 | 4 | 3 | 1 | 190 |

| **Evaluation Framework** | Scalability | Heter. | Timeliness | Reliability / Robustness | Resiliency | Energy efficiency | Interop. | Data aggr. / compr. mechanisms | Traffic differentiation | Security | Hardware support | Technical maturity | Availability of exp. internal to the consortium | TOT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Weights** | **15** | **5** | **5** | **10** | **5** | **10** | **15** | **5** | **5** | **10** | **10** | **15** | **-10** | SUM(Score *Weight) |
| 2G/3G (GSM, GPRS, EDGE, UMTS) | 1 | 1 | 1 | 1 | 3 | 1 | 1 |  | 1 | 1 | 1 | 1 | 0 | 115 |
| WiFi (Low Power) | 3 | 2 | 1 | 2 | 4 | 1 | 2 |  | 1 | 3 | 4 | 3 | 0 | 260 |

Table 3: Evaluation framework of the Technologies. The best solution (i.e. the one having the lowest total score) for each technology has been evidenced.

# 6. Current and Past Large Scale Solutions

This part reviews existing projects, testbeds and applications dealing with large scale WSNs. The goal of this section is to infer tools which can be used also in EMMON, as well as to infer lessons which helped us to evaluate the technologies as described in Section 5.

## 6.1 CitySense

CitySense is an urban scale sensor network testbed that is being developed by researchers at Harvard University and BBN Technologies. CitySense is intended to be an open testbed that researchers from all over the world can use to evaluate wireless networking and sensor network applications in a large-scale urban setting. The status of this project is still open. At present only a few set of nodes have been physically deployed at Harvard University campus and at the BBN Technologies.

This project is a useful reference for EMMON, since urban quality life is one of the most appealing application scenarios among those addressed in the WP3 deliverables.

### 6.1.1 Deployment Details

CitySense will consist of 100 wireless sensors deployed across a city, such as on light poles and private or public buildings; the intended target is to deploy the network in Cambridge, MA. Until now, there are 25 nodes deployed outside and another 32 nodes deployed as part of an indoor testbed at Maxwell Dworkin Hall at Harvard.

Each node will consist of:

- Metrix embedded PC (Soekris single-board PC).
- Pebble Linux OS distribution.
- 133Mhz AMD processor.
- 64MB RAM and flash, 1GB USB flash drive.
- Dual 802.11 a/b/g miniPCI radio cards (one used for “management mesh” and the other for experimental purposes), with high transmit power.
- High gain omni-directional antennas.
- Multiple sensors possible: weather, air quality, bio/chem. agents, webcams, microphones.

### 6.1.2 Network Architecture

Remote nodes form an IEEE802.11-based multi-hop wireless mesh. The network includes a few wired gateway nodes interfacing the mesh with Internet and with the central server at Harvard. This strategy allows a node to download software or upload sensor data to a distant server hub using a small radio with a 1-kilometer range.

### 6.1.3 MAC / Routing Protocols

At the MAC layer an IEEE802.11 ad hoc mesh is used, while at the network layer a multi-hop Optimized Link State Routing (OLSR) protocol, which has been shown to scale well with the number of nodes, is used for management operations. Users are allowed to remotely "install" their own routing protocols over the 802.11 MAC using the network as a test-bed.

### 6.1.4 Federated Communication

IEEE 802.11a/b/g Wi-Fi.

### 6.1.5 Lesson Learned – Problems Solved – Challenges Addressed

**Energy Efficiency**: The system solves a constraint on previous wireless networks—battery life—by mounting each node on a municipal streetlamp, where it draws power from city electricity. As a consequence, energy efficiency is not a stringent constraint.

**Network Planning**: Mounting nodes roughly 10 meters above the ground helps RF reception range by reducing interference from WiFi radios in private laptops and access points. Moreover, the roadways provide a natural line-of-sight path among nodes. To ensure network coverage against unplanned node outages, the inter-node spacing has been chosen roughly less than half the range of the radios and afterwards the nodes have been manually deployed.

**Network Security**: i) WPA encryption used at the link layer; ii) SSL or SSH protocols for communication at the transport layer and iii) new WEP keys distributed periodically using a secure transport protocol.

**Failure detection / recovery**: A node reboots into the baseline configuration when connectivity to the control network is lost for more than a predefined period of time. Furthermore nodes have a software watchdog timer as well as a hardware grenade timer that physically reboots the node at a preset time each day, regardless of its state. The only measure taken is that such timers must be staggered to prevent a total network outage. In this project this timer setting has been fixed at planning time.

**Network Monitoring and Management**: Each node runs periodically a set of scripts to collect information on node state, such as uptime, routing tables and statistics on network performance. Results are routed to the central station and logged to a database. For remote update of the software on each node, a simple approach based on an rsync tree [RD-2], [RD-3] has been used. Basically, this consists in using a spanning tree by which a central server node pushes updates to a selected set of "seed" nodes (passing through the wired gateways), and those nodes push updates over-the-air to their children and so forth. Furthermore, each user will have access rights to an isolated subtree of the node's filesystem, while critical system files can only be updated by the administrator. Updates are not handled on demand, but batched each day into a single bulk operation. Finally, a golden image is maintained in a separate booting partition, so nodes can disable all users' applications and contact the central server for administrative control.

**Resource Management**: Although energy is not a constraint, CPU, memory and bandwidth availability are resource constraints. For instance, in terms of application programming models, since the simplest SSH-based approaches ignore resource and bandwidth limitations, a different set of tools and programming APIs must be supported. For example, even if not already implemented in this project, a set of APIs to expose physical location of each node, the network topology and link characteristics may help application designer to decide where to cache data or perform aggregation.

**Data Stream**: Each node can receive, maintain and compute new state which can then be pushed out to other nodes in the surrounding environment. These capabilities can be used for developing publish/subscribe applications. Furthermore, CitySense nodes could be used as collection and aggregation points for data collected by e.g. a vehicular network, providing not just network connectivity but also localized computational resources.

**Time synchronization**: It is still an open research issue; researchers are trying to investigate about the use of GPS (Global Positioning System) or NTP (Network Time Protocol).

## 6.2 ExScal

Aiming to cover a 10km by 1km perimeter with 10 000 nodes, project ExScal (for **Ex**treme **Scal**e) fielded a more-than-1000[6] node wireless sensor network and a more-than-200 node ad hoc network of 802.11 devices in a 1.3km by 300m remote area in Florida during December 2004. In several respects, these networks were likely the largest deployed networks of either type at the time.

The application targeted by ExScal is the detection and classification of multiple intruder types over an extended perimeter. The project has now been transitioned to a classified setting.

This project organized the biggest deployment to-date and is therefore very relevant to EMMON. The application targeted, however is quite different, and a planned and regular topology make the solutions adopted quite specific. Finally, only little information is available on this project due to its current classified setting.

### 6.2.1 Deployment Details

The ExScal deployment covered an area 1.3km by 300m with about:

- 1000 sensing and actuating nodes, called XSMs (eXtreme Scale Mote, derivative of Mica2 motes, manufactured by CrossBow), running TinyOS and featuring a variety of sensors and actuators including a magnetometer, a microphone, four passive infrared receivers, a photocell, a sounder, and feedback LEDs,
- 200 backbone nodes, called XSS (Extreme Scale Stargates, running the Intel Stargate platform), customized by adding an 802.11b Wireless Networking card with requisite software, an external antenna, a housing for the device, and a battery pack. They have 400Mhz processor, 64MB RAM and 32MB flash memory, and are equipped with a GPS device.

### 6.2.2 Network Architecture

ExScal was organized along a 3-tier architecture [RD-4]:

Tier 1: the sensing and actuating nodes (XSMs)

[6] Although the initial aim is to deploy 10000 nodes, this project really deployed “only” 10%. From the information available, there is not a clear motivation for this. We can only assume operational difficulties (as reported in [RD-4]) or that it was classified before reaching that stage.

Tier 2: the Backbone network nodes (XSS), placed strategically in the topology[7] such that most XSM were able to communicate directly with an XSS.

These nodes ran a controller application that served to orchestrate the localization and reprogramming services at Tier 1. They also facilitated retrieving data from the motes to be analyzed on PC's (Tier 3).

Tier 3: a laptop, or a PC, running the classification, tracking and visualization applications, and also serving as the command and control station for network management.

### 6.2.3 MAC / Routing Protocols

During the main (sensing and intrusion detection) application, the sensor nodes use a routing protocol called GridRouting [RD-4] to communicate to the local base node (tier 2). This protocol uses the node location to conservatively select to which tier-2 nodes a sensor node must transmit its information. This protocol is run over an implicit acknowledgement-based retransmission protocol called ReliableComm [RD-4].

Tier-2 (XSS) nodes use:

- Initid [RD-4], an unstructured broadcast service to initialize the XSS network, constructing a tree used to collect GPS location of nodes,
- LOF [RD-4], a beacon-free convergecast routing protocol, to communicate to the central tier-3 node,
- Sprinkler [RD-4], a structured broadcast service to disseminate bulk data to all XSSs, which constructs a connected dominating set and a transmission schedule.

### 6.2.4 Federated Communication

IEEE 802.11.b, peer-to-peer, ad hoc.

### 6.2.5 Lesson Learned – Problems Solved – Challenges Addressed

The following points illustrate the lessons learned according to the ExScal researchers:

**Successful design principles**

- *Planned architecture to reduce cost*: They argue that a planned, deterministic deployment is feasible in large scale network, and that it allows for more efficient deployment (less nodes required), management and operation and for more predictable overall performance.
- *Multi-phase operation for performance optimization and fault containment*: The operation of ExScal is broken down into several phases (pre-deployment, deployment, reprogramming, localization and Op-Ap for Operator Application, which refers to the sensing and introduction detection application). The ExScal researchers argue that this enables to:
    - manage application complexity,

[7] The topology is quite simple: grid of sensors in open field, with an empirically assumed need of higher density closer to the border of the field to identify the objects.

  - satisfy the processing, communication and memory requirements of each phase,
  - optimize the protocols choice for each phase,
  - benefit from fault containment.
- *Multi-tier design for reliability*: Given that network reliability drops significantly as network size increases beyond 5-6 hops, ExScal uses a multi-tier network design to limit the number of hops travelled by a message at each tier, therefore helping to bind the unreliability in the network.

**Implementation problems**

- *Importance of flexible binding*: A software bug highlighted the importance of separating network functions from device names to be able to bind them flexibly.

**Improving performance**

- *Using available redundancy to increase lifetime*: Lack of prior data lead the ExScal designers to be conservative while choosing sensing and communication coverage. The net yield of ExScal, however, exceeded this planned redundancy. The excess can be used to extend the system lifetime, by using specific power management schemes.
- *Additional services and tools for management*[8]: The unreliability of current protocols for querying network state implies **a lack of information** about the current network state. This was alleviated to some extent by using the application data itself to infer ground truth, but this highlights the need for adequate network monitoring services. Building on this, since different routing protocols are well-suited for different topologies and traffic patterns, the performance of network querying can be improved **by dynamically choosing a routing protocol** that works best for the given network conditions. Similarly, **automated, online filtering of network data** is recommended to extract meaningful information (such as perturbations in network state or patterns in network behaviour) that may be indicators of faults and identify alternate parameters to restore network state. The ExScal researchers also identified the need for greater **local and autonomous management** support. An example of such an autonomous management technique is the use of policy-based monitoring for dealing with false positive, which requires minimal human support for specifying the policy and its associated detection and correction actions. For EMMON, this would suggest having some form of "intelligence" and control at the node level and not only at the C&C station.

[8] Selected software modules of the UbiSec&Sens security and reliability toolbox are available for download at http://www.ist-ubisecsens.org/download.php.

An online demo of configKIT is available at http://www.ist-ubisecsens.org/ckit/ckit_frames.html. configKIT is a security centric configuration tool. It selects modules from the UbiSec&Sens toolbox and combines them to a valid system satisfying application requirements given by the developer. It is claimed that configKIT allows even non-security-expert users to generate fine tuned solution even for rather general formulated application and security requirements, and to experience how even slight modifications of requirements can significantly change the recommended software configuration.

## 6.3 UbiSec & Sens

UbiSec&Sens is a Specific Target Research Project (STReP) in the thematic priority "Towards a global depend-ability and security framework" of the EU Framework Programme 6 for Research and Development.

The motivation for the project can be summarized by the following sentence: "What is needed to kick off the development and exploitation of WSNs is an architecture for medium and large scale wireless sensor networks integrating comprehensive security capabilities right from the concept stage."

UbiSec&Sens goal was to provide a comprehensive architecture for medium and large scale[9] wireless sensor networks with the full level of security that would make them trusted and secure for all applications. In addition UbiSec&Sens provides a complete tool box of security aware components which, together with the UbiSec&Sens radically new design cycle for secure sensor networks, enables the rapid development of trusted sensor network applications.

The project started in January 2006 and had duration of 3 years, meaning it finished at the end of 2008.

Project goals:

- To provide a security and reliability architecture for medium and large-scale WSNs acting in volatile environments,
- Apply a radically new design cycle to protect WSNs,
- To provide a complete toolbox of security and reliability aware components for sensor network application development,
- Focus on the intersection of security, routing and in-network processing,
- Application scenarios of agriculture, road services and homeland security

### 6.3.1 Deployment Details

The project offers various SW modules proposed for Middleware, routing transport, KPD, CDA, xCastAuthentication and crypto modules.

They have used the following tools/technologies [RD-7]:

- Crypto Modules
  - MD5 - MD5 for restricted devices
  - RC5 – RC5 for restricted devices
  - EC-ElGamal - EC-ElGamal space optimised for 8-bit processor
  - NTRUSign - NTRU Signature
  - TinyRNG - Random Number Generator

[9] Vehicular WSN prototype: 15-25 nodes; Agriculture WSN prototype: 50-100 nodes; Homeland Security WSN prototype: 15-25 nodes. The concept of large scale considered in this project is very different from the EMMON goals. This project aims to develop an agriculture WSN prototype with at most 100 nodes.

- Key Distribution
  - RoK - A Robust Key Pre-Distribution Protocol for Mulri-Phase Wireless Sensor Networks
  - TAUK - Topology Aware Group Keying for enhanced CDA with multiple keys
- Convergecast Encoding
  - CDA (DoFe) - Concealed data aggregation for encryption of convergecast traffic based on symmetric group key
  - CDA (CaMyTs) - Concealed data aggregation for encryption of convergecast traffic based on pair-wise symmetric keys
- Authentication
  - ConCastAuthentication - Authentication of Convergecast Traffic
  - MulticastAuthentication - Authentication of Multicast Traffic
  - UnicastAuthentication - Authentication of Unicast Traffic
  - RANBAR - RANSAC-Based Resilient Aggregation in Sensor Networks

UbiSecSens was already applied to:

- Integrated Vehicular & WSN - Detection and distribution of road condition
  - WSN
    - Sensors detect road conditions
    - Data are aggregated and stored in a distribute manner (tinyPEDS)
    - Communication is encrypted
    - 802.15.4
  - VANET
    - Communication uses geographical routing
    - 802.11p
- Vineyard monitoring - Detection and distribution of ground humidity, light
  - 25m distance between sensors

In particular, in the vineyard monitoring scenario, assuming a rectangular deployment area (100m x 200m), the nodes are placed on a grid with the size of a cell 25m x 25m. In total 45 nodes are required. All nodes are equipped with humidity sensors. 15 of them should be equipped with light sensors. The distribution of the sensors in a sample vineyard is schematically shown in Figure 5, where the position and the coverage of the aggregators, the simple nodes and the sink are also shown.

### 6.3.2 Network Architecture

The project is not restricted to one network architecture.

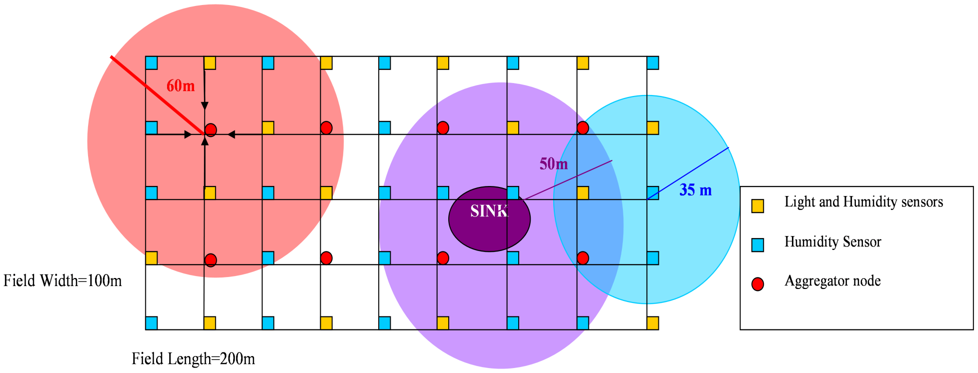

Figure 5: UbiSec&Sens project - distribution of the sensors in a sample vineyard

### 6.3.3 MAC / Routing Protocols

The following Network protocols are considered by the project:

- tinyLUNAR - Reactive end-to-end connection oriented routing protocol based on label switching [RD-177].
- PANEL - Position-based Aggregator Node Election [RD-178].
- DSDV - Destination-Sequenced Distance Vector Routing [RD-180].

The following Transport protocols are considered by the project:

- DTSN - Distributed Transport Protocol for Sensor Networks [RD-179].
- NanoTCP - TCP for restricted devices [RD-181].
- GPSR - Greedy Perimeter Stateless Routing [RD-182].

### 6.3.4 Federated Communication

Not specified.

### 6.3.5 Lesson Learned – Problems Solved – Challenges Addressed

**Network Security:** End-to-end encryption of converge-cast traffic with in-network processing. In this project privacy homomorphism encryption functions are used to aggregate data without the need to decryption and encryption in the aggregate nodes.

**Data Stream**: “CDA” Convergecast encoding.

**Software**: TinyOS and Contiki where considered has the base platform of the system. TinyOS offered a flexible component-based programming model. It also supported the possibility to dynamically update the installed software on sensor nodes at runtime However TinyOS offers less efficient mechanisms than Contiki. On the other hand, TinyOS offers a variety of the existing software modules and drivers that other operating systems cannot offer. After the analysis TinyOS version 2.x has been chosen as the default platform for the UbiSec&Sens software..

**Energy Efficiency:** It can be stated that energy harvesting technologies exist, but their potential application is very dependent on the environment. Anyway, the efficiency of these technologies is still very limited. For example, the conversion of temperature differences directly into electricity, also known as Seebeck effect, was proposed (but we didn't find further information about its effective use).

## 6.4 CoBIs

The project focuses on the development and the integrated application-driven usage of so-called "Collaborative Business Items" (short CoBIs) that utilize a wide spectrum of sensor networks technology. Since these Items are considered to be much "smarter" than items tagged with RFID transponders, they can play a more active role in business processes.

From the business perspective, the approach to handle situations locally can potentially lead to reduced processing and transactional costs, to improved response times in business- or even safety-critical situations, and also to enhanced quality of process results within a given operational environment.

From the more technical point of view, flexible distributed process handling based on services that run on CoBIs nodes can help saving back-end systems' resources, such as CPU-time, memory, network bandwidth, etc., and can thus lead to enhanced reliability, responsiveness and scalability of the overall system.

The major technical outcome of the CoBIs project is a novel distributed service-oriented architecture. This architecture should enable the flexible and, at least partly, automated composition/decomposition and management of services, in order to delegate certain parts of the supported business logic functionality to smart physical entities. Services have the advantage of providing information throughout the enterprise in a platform and language independent manner.

From this project, best practices can be further derived for the design of the middleware in EMMON.

### 6.4.1 Deployment Details

Several trials have been made in the context of this project [RD-8]. As for example:

- *"Smart drums" scenario*: sensors (particles) were attached to drums containing hazardous chemical substances. These sensors monitor and control several rules, including dangerous combinations that are not allowed while storing chemicals in warehouses.

  The use case implemented two processes when handling the drums:

  - in-situ monitoring of a storage limit;
  - in-situ monitoring if incompatible chemicals, i.e. reactive chemicals, are stored together.

  The number of sensors has been very small (2 or 3) in both the cases.

- *Building management scenario*, where 35 sensors have been deployed to control humidity, temperature…. Anyway the focus is not on the WSN but on the integrated framework.

### 6.4.2 Network Architecture

Not specified.

### 6.4.3 MAC / Routing Protocols

Mainly geographical routing.

### 6.4.4 Federated Communication

The project makes use of RFID tagging. No details are provided on the federated communication technology used in the different application scenarios.

### 6.4.5 Lesson Learned – Problems Solved – Challenges Addressed

**Heterogeneity and scalability**: The ultimate goal of a project like CoBIs is to support the operation of a very large number of business items. This concerns all layers of the system, from the networking layer where items interact with each other, to the middleware that connects the items to the back-end system, and the back-end system itself.

On the level of sensor networks, scalable operations of a large number of nodes must be ensured. Since most interactions between nodes take place localized, only a small number of nodes are usually directly involved. Data aggregation, for example, is approached by a hierarchical organization of the network, which facilitates large-scale communication. Multi-hop routing in such networks can become challenging with regard to scalability, therefore often stateless approaches like geographic routing are employed

The developers of CoBIs hope that the project results can be used as the the foundation of a widespread, multi-partner sensor network infrastructure, paving the way for interoperable, commercial, integrated sensor networks.

## 6.5 AWARE

The general objective of the project is the design, development and experimentation of a platform providing the middleware and the functionalities required for the cooperation among aerial flying objects, i.e. autonomous helicopters, and a ground sensor-actuator wireless network, including mobile nodes carried by people and vehicles. The platform will enable the operation in sites with difficult access and without communication infrastructure. Then, the project considers the self-deploying of the network by means of autonomous helicopters with the ability to transport and deploy loads (communication equipment and nodes of the ground network).

The project is closed since August 2009 and a final demonstration to the reviewer of the European Commission has been developed on May 2009. A video of the latter event is available in the project website at http://grvc.us.es/aware [RD-9].

The objective of EMMON is quite different. In EMMON no mobility is considered. Nevertheless, one of the AWARE goals is to develop a scalable and self-organizing ground sensor network and one of its scenarios is strictly related to an EMMON's case study, i.e. the Civil Security/Disaster Management scenario.

### 6.5.1 Deployment Details

Not specified. The demonstration is most related to autonomous vehicles, rather than to WSN elements. In some publications related to this project, like e.g. [RD-13], experimentations have been conducted with MICA2 and Telos motes in small scale networks.

### 6.5.2 Network Architecture

The AWARE platform consists of two different networks, a high bandwidth network (HBN) and a low bandwidth network (LBN). The HBN is composed of personal computers, cameras and mobile robots capable of transmitting data through IEEE 802.3 or IEEE 802.11 networks. A WSN is also present on the system. This second network is formed by nodes with very limited computing and data transmitting capabilities, and it is also called the low bandwidth network (LBN). HBN and WSN are connected through gateway(s). Some mobile robots might be also part of both networks.

At the WSN, the network architecture is cluster-based: the network is data-centric and clusters (groups of nodes identified by a group ID) and cluster heads (group leaders) are dynamically formed and logically move based on the event allowing for tracking.

Moreover, to allow the AWARE system to cope with additional load and to be able to cover a large area of interest while maintaining dependable services, network clustering is usually pursued for multiple sink cases. Multiple gateway nodes are placed and sensors are grouped around them forming a network clusters.

### 6.5.3 MAC / Routing Protocols

AWARE has adopted the Lightweight MAC (LMAC) [RD-10], [RD-15] for the MAC layer. This protocol is a lightweight, energy-efficient TDMA-based medium access control protocol specifically designed for WSN. At the network layer a simple spanning tree based protocol, called FixTree [RD-12], has been adopted. This protocol builds a tree by using the simple metric of number of hops starting from the group leader of each cluster. At the transport layer, the reliable multicast data dissemination protocol (RMD) [RD-11] is adopted. This protocol has been developed in the frame of CoBIs project (see Section 6.4) and is a cross-layer solution, utilizing MAC layer information about neighbourhood and packet losses.

### 6.5.4 Federated Communication

This is related to the High Bandwidth Network (HBN) and it can be IEEE 802.3 or IEEE 802.11.

### 6.5.5 Lesson Learned – Problems Solved – Challenges Addressed

**Data Aggregation**: network is cluster based and each cluster is formed by nodes organized in a spanning tree logical topology. Each node of this tree sums its data to those coming from the child. Only the group leader performs data aggregation, like average or other similar functions, before transmitting to the gateway via the global routing tree [RD-13].

**Network Reprogramming**: In [RD-12] a simulation framework has been presented to analyze the impact of three important parameters (distance, network size and density) on the overall performance of the code dissemination of RMD protocol. This framework is based on MATLAB and SIMULINK simulations, which incorporates a link quality model taken from real data captures and MAC and Routing protocol models. The results indicated that a careful deployment can improve significantly the stability of the reprogramming solution, ensuring more than 98.8% average success rate, but only for small/medium scale networks, i.e. networks with at most 100 nodes.

**Security**: In [RD-16] the authors investigate the effect of radio jamming attacks against a deployed WSN, and in particular the effect on three examples of MAC protocols, i.e. S-MAC, B-MAC and LMAC. Authors define an energy-efficient class of jamming attacks, whose primary goal is to disrupt the network by preventing messages from arriving at the sink node, and the secondary goal is to increase the energy wastage of the sensors. They present simulation results (in OMNET++) which have been validated by measurements obtained from actual implementation of such algorithms on real test-beds (i.e. a home-made WSN node designed in the framework of EYES project and further described in [RD-17]). A careful analysis of other protocols belonging to the respective categories of S-MAC, LMAC, and B-MAC (for instance, slot-based protocols, like T-MAC and DMAC, frame-based protocols, like TRAMA, and random access-based protocols, like WiseMAC) reveals that those protocols are, to some extent, also susceptible to jamming attacks. In particular, authors conclude that among these protocols, frame-based protocols have better resistance to energy-efficient jamming because they spread out transmissions in time. Authors also propose some countermeasures for the analyzed protocols, but they conclude that an effective countermeasure is still lacking. Anyway, by extremely summarizing, it emerges that TDMA protocols are potentially a better choice than other types of protocols.

## 6.6 e-SENSE

e-SENSE provides heterogeneous wireless sensor network solutions to enable Context Capture for Ambient Intelligence, in particular for mobile and wireless systems beyond 3G; thus enabling truly multi-sensory and personal mobile applications and services, as well as assisting mobile communications through sensor information.

The e-SENSE project is finished since December 2007 [RD-18] - [RD-20].

Three classes of applications were investigated:

a) body sensor network applications,

b) wireless sensor network systems deployed in environmental or object sensor network applications requiring localization and positioning and thus having some form of geographic notion

c) wireless sensor network systems deployed in environmental or object sensor network applications not requiring explicit localization support (such as converge-cast applications).

The applications considered by EMMON would most likely fit in category b).

### 6.6.1 Deployment Details

No significant deployment.

### 6.6.2 Network Architecture

The network architecture comprises various possible instantiations of mesh WSNs that are connected via gateways[10] to a core network. The core network can be a beyond 3G mobile communications system or a conventional wired backbone network.

### 6.6.3 MAC / Routing Protocols

A generic communication stack is defined [RD-20] (c.f. Figure 6), and three instantiations, corresponding to the three application classes targeted, are presented [RD-20]. Instantiation A refers to body sensor networks and is not relevant to EMMON.

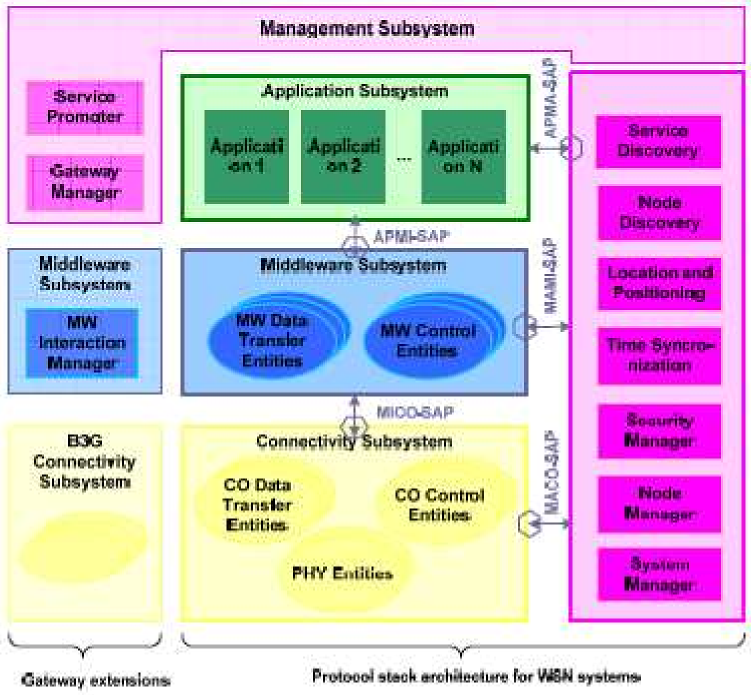

Figure 6: e-SENSE protocol stack architecture

The instantiation B, suited for applications that require localization and positioning (class b above), supports multi-hop communication (of typically up to 10+ hops) and limited mobility of sensor nodes within the WSN system and is further optimized for in-network communication. It builds on the cross-layer RoCoDile component that performs CSMA MAC and routing functionality [RD-20].

The instantiation C, suited for application that do not require localization (class c above), supports multi-hop communication of typically up to 10 hops or more and enables interest dissemination and converge-cast within the multi-hop network. Mobility of both sensor nodes as well as the sinks is supported as well as energy-efficient operation by enabling load-sharing among sensor nodes to prolong the lifetime of the network. It builds on a

[10] This is a conceptual framework. For these devices we were not able to find further details in terms of hardware, software and radio capabilities.

802.15.4 compliant physical layer and the cross-optimized IRIS protocol, performing CSMA MAC with RTS/CTS interest dissemination and converge casting.

While the instantiation B would be the most suitable for EMMON, it is not optimized for scalability or energy efficiency and is therefore not adapted. The stack architecture, however, could potentially be reused for EMMON.

### 6.6.4 Federated Communication

IEEE802.15.4 and B3G.

### 6.6.5 Lesson Learned – Problems Solved – Challenges Addressed

The main problems solved by the e-SENSE project are:

- WSN integration into IP Multimedia Subsystem (IMS) service platform
- Energy efficient air-interfaces for WSN achieving 20nJ/bit;
- Innovative WSN communication mechanisms tailored to the e-SENSE application scenarios in terms of protocol elements for MAC, networking, transport and management;
- Cross-optimization of protocol elements and design of three WSN protocol stack instantiations for specific application scenarios;
- Distributed services, which address common services such as localization/positioning, timing and synchronization and service discovery;
- Distributed data processing, which address mechanisms to enable collaborative processing and context awareness support;
- Data centric resource management, which aims to optimize computing and communication resources in a data-centric network;
- An integrated WSN middleware solution, including service discovery, resource management.

## 6.7 CRUISE

The CRUISE Network of Excellence (NoE) [RD-21] aims to be a focal point in the coordination of research on communication and application aspects of wireless sensor networking in Europe. It brings together a diverse group of partners who will integrate their expertise and knowledge gained in projects on related fields, promoting discussion and strengthening research cooperation between industry and academia, while maintaining an academic nature.

CRUISE partners will closely work on the joint program of activities specified in this project, a crucial part of which is the creation of a state-of-the-art Knowledge Base, available to the general public. The work consists of information collection, comparison, validation and dissemination. CRUISE will focus its research toward the solution of specific theoretical and technological problems that will enable the building of sensor network applications that can significantly affect European society.

**Classification by sector:**

- Industry.
- Retail.
- Logistics.
- Construction.
- Agriculture.
- Medicine, Health Care.
- Military.
- Arts.

The CRUISE consortium will identify short-term and long-term benefit and stimulate open discussion on the issues of standardization, international collaboration, and intellectual property.

CRUISE aims to collaborate with industry and European research initiatives active in this field and will stimulate collaboration by actively disseminating the results of its work. In the joint research work CRUISE partners will establish a framework of common tools and methodologies to accelerate the research process and build sustainable collaboration links. The project's special attention is also given to teaching and training, and novel techniques for knowledge management collaboration and dissemination. For the project leaders, e-learning@CRUISE is the ultimate goal, i.e. promoting the research in sensor networking and spreading results to the general public[11].

### 6.7.1 Deployment Details

**CRUISE ZigBee development environment**

- Micaz Zigbee Motes.
- XBow Sensor Board MTS300/31.
- PC.
- TinyOS.
- nesC.
- AVR-Tools.
- Cygwin.

### 6.7.2 Network Architecture

CRUISE is a general study.

### 6.7.3 MAC / Routing Protocols

CRUISE is a general study.

[11] CRUISE partners on Package 122 ("Integrating Test Beds and Measurements") have collected and disseminated information about their test beds, their experiences with different platforms by means of filling a questionnaire on existing testbeds. For further details refer to "The Approach of European Network of Excellence CRUISE to Heterogeneous Wireless Sensor Networks Design and Integration", available online at http://www.computer.org/portal/web/csdl/doi/10.1109/SENSORCOMM.2007.94.

### 6.7.4 Federated Communication

CRUISE is a general study.

### 6.7.5 Lesson Learned – Problems Solved – Challenges Addressed

**Generic Network Simulators**

Differences between OMNeT++ and NS2:

- NS2 is older than OMNeT++, therefore much more protocols and algorithms have been coded for it;
- In most cases it is easier/faster to code in OMNeT++ and the code is easily reusable due to its hierarchical structure;
- NS2 has scalability problems with large networks.

**Sensor Network Simulators:**

- SENSE
- SENSIM –built over OMNeT++
- EM* (EM Star)
- TOSSIM (TinyOS Simulator)
- ATEMU (Atmel Emulator)

Advantages of using TOSSIM:

- Ease of use - Compiles directly from TinyOS source code, thus reduced efforts and bugs;
- Fidelity - Emulates hardware at component level and simulates network at bit level (fine-grained), thus accurate;
- Scalability - Scales to thousands of nodes;
- Completeness - Captures complete system behaviour and all interactions between individual components;
- Compile application code for actual hardware or TOSSIM as required;
- No change required to the application;
- Deployment can immediately follow testing on TOSSIM;
- Very fine-grained simulation of TinyOS networking stack at bit-level;
- Thus, allows one to do everything on simulator that one can do on mica.

Drawbacks / Possible enhancements:

- Does not include energy modelling;
- Can be improved to run multiple applications at a time;
- Applicable only for TinyOS platform applications.

Advantages of using ATEMU:

- Good graphical debugging environment –Support for arbitrary number of breakpoints and memory watch points;
- Supports multiple sensor nodes in a network, and each node can have different configurations and run different programs.

**Networks Design – Existing TestBeds Features**

CRUISE analyzed thirteen test beds in terms of application scenarios, hardware features and adopted communications protocols.

**Application Area**: The vast majority of the testbeds (9 over 13) have been projected to be applied to for environmental monitoring.

**Observed parameters**: Data sensed are heterogeneous, and almost all of the parameters are focused on environmental conditions. Apart from heart beating for medical purposes, almost all testbeds present temperature sensors, other sensors present are:

- (5/13) Sound sensors.
- (5/13) Accelerometers.
- (4/13) Magnetic sensors.
- (5/13) Light sensors.

Sensing modes are equally divided between synchronous and asynchronous, with some of them working in both modes.

**Networking Aspects:**

Almost all the testbeds are formed by a number of nodes varying between 10 and 30, with some gateways, depending on the application. Particular cases are represented by KU testbed that is constituted by 120 nodes and is conceived for the study of networking issues, and UO testbed, which is composed of 30 gateways, collecting data upon mobile tags.

Topologies are miscellaneous (flat/star/tree/clustered).

**1. Lower layers**

Most (7/13) of the testbeds use 2.4 GHz transmission using IEEE 802.15.4 physical layer, 4/13 use also IEEE 802.15.4 MAC layer (alternatives are S-MAC/BMAC/ StarMAC and proprietary solutions), data rate range from 38.4 to 250 kbps. Heterogeneous layer 3 protocols are used.

**2. Gateway**

Gateway interfaces adopt heterogeneous technologies:

- 6/13 use wired LAN, connected to PCs or to dedicated gateways (Stargate SPB400, MIB600).
- 1 employs a serial connection.
- 1 uses GSM/GPRS.

**3. Security**

Few testbeds approach security issues, implementing symmetric (2/13) or asymmetric (1/13) key inter-node cryptography and authentication of data, or node-gateway authentication.

**Node Characteristics**

1. **Communications protocols**

A possible approach to pilot sites integration could resort to the communications protocols design through the same operative system, namely TinyOS . In particular, Sensinode is releasing a free protocol stack for WSNs called NanoStack. It gives IEEE 802.15.4 and 6LoWPAN support and is easily portable to many different platforms. It is based on FreeRTOS.

2. **Hardware platforms**

The majority of the testbeds (6/13) use different releases of the MICA platforms (MICA2/MICAZ/MICA2DOT), some alternatives are Telos or Intel devices. Most of the nodes run on AA or AAA batteries. Intel/Texas/Atmel/MPR2400CA processors are controlled in the most common case (6/13) by Berkeley TinyOS operative system.

## 6.8 RUNES

The RUNES project [RD-22] has a vision to enable the creation of large-scale, widely distributed, heterogeneous networked embedded systems that interoperate and adapt to their environments. The inherent complexity of such systems must be simplified for programmers if the full potential for networked embedded systems is to be realized. The widespread use of network embedded systems requires a standardized architecture that allows self-organization to suit a changeable environment. RUNES project aims to provide an adaptive middleware platform and application development tools that allow programmers the flexibility to interact with the environment where necessary, whilst affording a level of abstraction that facilitates ease of application construction and use. This allows for a dramatic cut in the cost of new application development and a much faster time to market.

With respect to the EMMON purposes, the approach followed within the RUNES project is more oriented to WSN developers. The developed middleware aims to provide adaptive tools to developers that have to build applications.

### 6.8.1 Deployment Details

The network has been deployed in tunnels to demonstrate the fire reaction scenario. Small scale demonstration has been done by using:

- 6 Sensor Motes (Tmotes Sky from MoteIV) acting as part of the tunnel infrastructure.
- 1 Laptop with 1 Sensor Mote attached to the USB interface acting as the main tunnel infrastructure gateway.
- 1 connectBlue node acting as secondary gateway.
- 1 Laptop acting as the Tunnel Control PC.

The software components were made up of:

- Tunnel Infrastructure Motes.
- Contiki Operating System (contiki-2.x-snap9.3) with uIP, uAODV, DHCP-light client.
- RUNES Middleware – CRTK.

### 6.8.2 Network Architecture

Because the project deals with scenarios for which emergencies can last from several hours to days and are highly dynamic, the response systems must adapt to the changing conditions, must be robust, must utilize the limited available resources efficiently and must provide accurate, timely, information requirements. A wireless sensor network, comprising low-cost, low-power wireless sensing devices throughout a physical area, can only meet part of the requirements and, therefore, a more complex network that supports an overlay of mobile and fixed wireless networks, existing networking infrastructure, and sensors/robotic services is used.

The proposed network architecture is a mesh basically.

### 6.8.3 MAC / Routing Protocols

The Ad-hoc On-demand Distance Vector (AODV) routing algorithm has been used by RUNES. It is an algorithm for routing data across Wireless Mesh Networks. It is capable of both unicast and multicast routing. It is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. AODV is, as the name indicates, a distance-vector protocol.

### 6.8.4 Federated Communication

The project has been developing a self-organizing ad-hoc wireless standard, able to create point-to-point and mesh networks and adapt to new / out-of-range devices without intervention from a human operator. The project uses anything from GSM, WiFi and Bluetooth and ZigBee, regardless of OS as it is platform agnostic.

### 6.8.5 Lesson Learned – Problems Solved – Challenges Addressed

**Heterogeneity and scalability**: The project proposed a standard, platform agnostic, architecture able to serve heterogeneous networks and devices. In fact, the sensors are of many different types, capabilities and ages; they use different physical and MAC layer protocols; and may require continuous reconfiguration within the network as parts fail.

**Fault tolerance and reliability**: Given the need to adapt response over time, the project provides support for the semi-automatic uploading of software components and the dynamic re-tasking of nodes (robustness).

## 6.9 Smart Messages

The goal of the Smart Messages project [RD-23] is to develop a computing model and a system architecture for networks of embedded systems (NES). The applications running over NES range from as simple as data collection and data dissemination in sensor networks to complex cooperative applications such as cars collaborating to adapt to traffic conditions or robots with intelligent cameras performing distributed object tracking. The main question that this project tries to answer is: How to program user-defined distributed applications over NES?

NES are large scale, ad hoc networks that work unattended. They are composed of resource constrained, heterogeneous, and volatile nodes. Programming NES is a significant challenge due to this unique combination of characteristics which makes traditional distributed computing models difficult, if not impossible, to use in such networks. The solution proposed is Cooperative Computing, a distributed computing model based on execution migration. In this model, applications are dynamic collections of Smart Messages (SMs) and each node cooperates by providing a common system support. Smart Messages are migratory execution units that execute on nodes of interest named by content and reached using self-routing at intermediate nodes. Each node in NES provides a virtual machine for SM execution and a name-based memory, called Tag Space. The Tag Space offers persistent memory across SM executions and a uniform interface to the host OS and I/O system.

This project focuses mainly on the middleware of nodes and the programming by cooperative computing techniques. It is not strictly related with EMMON, but some of these results may constitute useful guidelines to apply in the present project.

### 6.9.1 Deployment Details

They develop a prototype to test the proposed programming framework. This prototype is composed by:

- A modified version of Sun Java KVM (virtual machine for mobile entities).
- HP iPAQs running Linux.
- Processor: 206 MHz Intel StrongARM
- Bandwidth: 11 Mbps (802.11), 1Mbps (Bluetooth)

Simulation activities have been conducted for small-medium scale networks, e.g. 256 nodes uniformly distributed over a 1000m by 1000m square.

### 6.9.2 Network Architecture

This project addresses features like code migration, which are similar to multi agent systems, so the intended network architecture is mainly flat.

### 6.9.3 MAC / Routing Protocols

SMs are self-routing, i.e, they are responsible for determining their own paths through the network. There is no system support required by SMs for routing, with the entire process taking place at application level [RD-24]. As a consequence, authors don’t talk about the used MAC protocol.

### 6.9.4 Federated Communication

Not used/specified.

### 6.9.5 Lesson Learned – Problems Solved – Challenges Addressed

**Routing and Naming**: Smart Messages (SMs) are distributed computing platform for NES based on execution-migration, content-based naming, and self-routing. Instead of passing data end-to-end between nodes, an SM application migrates to nodes of interest named by content and executes there. Each node has a virtual machine for SM execution and a name-based memory, called tag space. The SMs use the tag space for content-based naming and persistent shared memory. An SM carries its own routing code and routes itself at each node in the path toward a node of interest. To perform routing, SMs store routing information in the tag space at nodes.

**Network Reprogram**: since this project addresses code migration issues, it is relatively simple to implement also code re-distribution to the network, by simply update application code agents. The nodes in the network cooperate by providing a common minimal system support for the receipt and execution of Smart Messages.

**Heterogeneity and Scalability**: SMs are distributed applications which overcome the scale, heterogeneity, and volatility encountered in NES by migrating the execution to nodes of interest, using application-controlled routing, instead of using end-to-end communication among nodes [RD-25]. The main feature of the SM programming model is its high flexibility in the presence of dynamic network configurations.

**Security**: Although the security for both mobile agents and ad hoc networks have been extensively studied, in [RD-25] a new and more difficult problem has been faced: how to define a security architecture for a system based on execution migration over (mobile) ad hoc networks? Given the complexity of this problem, the current architecture provides solutions for protecting the hosts against SMs and SMs against each other. However, it is much harder to prevent an SM from being tampered by a malicious host and no efficient solutions still guarantee a sufficient reliability level.

**Application**: To prove that virtually any protocol or application can be written using SMs, authors implemented two previously proposed solutions: Directed Diffusion and SPIN. They present in [RD-25] different paradigms for content-based communication and computation in sensor networks: Directed Diffusion implements data collection and SPIN is a protocol for data dissemination.

**Timeliness**: adopting this new paradigm, the network may become highly responsive for applications where a control action has to be taken locally on the nodes, because the decisions are applied close to the events. However, this paradigm doesn’t really improve classical monitoring application, where an end-user requires data to be collected also for a-posteriori analysis or use.

## 6.10 uSWn

The uSWN project's main objective [RD-29] - [RD-35] is to research generic and reusable Software-Hardware solutions that are common to existent and potential future applications. Moreover, focus is on researching and developing reusable middleware components to ease future development regarding similar systems under real-time restrictions. The research regarding the challenge of WSN architectural design and deployment is focused on obtaining solutions that although generic, allow for further fine-tuning when a given application is considered. Specifically, in this project one of the main goals is to research the optimal deployment systems for the sensors in different generic scenarios and optimal routing and communications protocols under premises of autonomous setting on, low energy use and low memory and bandwidth capacities. A control system based on Agent Technology is assessed.

### 6.10.1 Deployment Details

A deployment methodology has been defined, consisting of consecutive steps to perform in order to make the best choice. The project addressed three different scenarios to which this methodology has been applied:

1. *Surveillance application scenario (outdoors)*: where the WSN system creates a virtual security perimeter to keep intruders out of the sanatorium.

2. *Critical monitoring scenario (indoors + outdoors)*: where the WSN system monitors vital signs to keep track of the health of the visitors.

3. *Multi-tracking application scenario (outdoors)*: where the WSN system targets moving objects inside the limits of the sanatorium to locate them, to store historical data and to obtain statistics regarding the preferred routes of visitors (clients)

For all these scenarios a 50 sensor network has been setup (TelosB motes by Crossbow).

### 6.10.2 Network Architecture

To best suit the application scenario requirements and meet the criteria such as energy efficiency, coverage, scalability, network connectivity, fault tolerance and network performance, the **cluster-based** architecture has been proposed for the uSWN.

### 6.10.3 MAC / Routing Protocols

Hop-by-hop routing is implemented by the µSWN protocol. It is shown that the network behaves efficiently with respect to network performance for up to 5 hops assuming routing and MAC performance. Therefore, the topology selected should tend to minimize the number of hops to the sink, so increasing network performance. Routing enhancements have been proposed considering congestion and remaining power for deciding the next hop, thus leaving more degrees of freedom to the deployment alternatives as long as more than one route exists. Assuming nodes transmitting at maximum power (0dBm), they guarantee that the longest route hops from any network node to the sink has a maximum cost of 3 hops.

The proposed routing algorithm encompasses 4 steps (see [RD-35]):

- Creation of fixed infrastructure routing tree.
- Local advertisement of node status and creation of neighbourhood information table.
- Selection of parent fixed node based on active metrics.
- Communication of packets.

### 6.10.4 Federated Communication

IP, ZigBee basically.

### 6.10.5 Lesson Learned – Problems Solved – Challenges Addressed

**Detection and recovery**: Communication Protocol for Autonomous Setting On and Fault Recovering Protocol of Routing for µSWN with low consumption and auto-location of sensors premises. Each node is identified with an intelligent agent that communicates with other sensors in a multi-agent set-up.

**Reprogramming**: the application at the main Server provides the user with the ability to form clusters of network nodes that he/she needs to reprogram. The clustering may be either data-centric if specific sensors need to be reprogrammed (i.e. environmental temperature sensors) or area-based if a group of sensors in a specific area need to be reconfigured for measuring other attributes. This could help to recover from failures that occur in clusters of nodes (e.g., a part of the network).

**Network Deployment**: Optimal Deployment scheme for the WSN, with the identification of Optimal Deployment Protocols and the design of algorithms capable of automating the generation of Optimal Deployment Prototypes. Metrics are identified that drive the deployment of the network.

**Resource management**: Identification of the Generic and Reusable Middleware Components to use in all range of Application Scenarios. The Middleware Reusable Components which reflect the generalization of all applications scenarios and that lead to low consumption and auto location capable WSN design and deployment solutions have been determined focusing on Reusable Prototype Components that are based on the Agent-Sensor Paradigm.

**Simulation and Prototype Testing**: the modelling and simulations are centred on a Model of WSN considering sensors positions and on the Agent-Sensor Paradigm Validation.

## 6.11 SensLAB

The purpose of the SensLAB project [RD-36] - [RD-39] is to deploy a very large scale open wireless sensor network platform. SensLAB's main and most important goal is to offer an accurate and efficient scientific tool to help in the design, development, tuning, and experimentation of real large-scale sensor network applications.

The SensLAB project is still running and some deliverables are already available to public.

In EMMON the goal is quite similar, even if the network is not developed to be a scientific tool, but to be a real industrial application. As a consequence, the nodes in SensLAB are more powerful than those expected to be deployed in EMMON.

### 6.11.1 Deployment Details

The sensLAB platform will be distributed among 4 sites in France (INRIA-Lille, Strasbourg-LSiiT, INRIA-Rennes and INRIA-Grenoble) and will be composed of 1,024 nodes. Each location will host 256 sensor nodes with specific characteristics in order to offer a wide spectrum of possibilities and heterogeneity. The four test beds will however be part of a common global testbed as several nodes will have global connectivity such that it will be possible to experiment a given application on all 1024 sensors at the same time.

Each SensLAB node is composed of 2 wsn430 boards, and one gateway board [RD-37].In particular, one WSN430 board is an open node, the other is a control node. The aim of this board set is to offer the essential SensLAB features, such as:

- Automated firmware deployment on open node.
- Accurate power monitoring of open nodes (on battery and DC power supply).
- Radio environment monitoring control, (RSSI measures and noise injection), thanks to the control node.
- Configurable sensor polling on control node (temperature, light, acoustic activity).
- Fixed (Ethernet) as well as mobile (WiFi) communication with Node Handler.
- Power over Ethernet support for a standardized and easy power management.
- Sink capability for each open node (in and out characters stream redirection).
- Option for daughter cards on open and control node.
- Remote software update ability for control nodes and gateway.

In the WSN 430 boards there are:

- A micro-controller MSP430F1611.
- Some physical sensors, like temperature, sound and ambient light.
- 2 alternative versions of radio interface:
  - 868MHz Radio interface (wsn430v1.3b). The radio chip is the Chipcon CC1101.
  - 2.4GHz radio interface (wsn430v1.4). The radio chip is the Chipcon CC2420, offering a IEEE 802.15.4 compliant interface

SensLAB developments have been made under NetOS version 7.4 [RD-38]. It consists of:

- packaging of the ThreadX RTOS kernel;
- a BSP for the specic platform/module;
- the Digi ESP IDE.

Digi ESP is based on Eclipse, and packages a gcc/gdb toolchain.

### 6.11.2 Network Architecture

The full network architecture is composed by the four sites wire-linked to each other via a central router station (Renater). Many sites are still works in progress. In Grenoble, sensor nodes are deployed in the robotic hall (15mx15m square) in a 3D mesh (wall & roof).

### 6.11.3 MAC / Routing Protocols

SensLAB is an open platform for building scientific demonstrator, so the communication protocols are open to users. As its basis, each node is a small computer running Linux-based Operating System and adopting IP protocol to access each node.

### 6.11.4 Federated Communication

The federated communication used for this project is essentially a IP-based one.

### 6.11.5 Lesson Learned – Problems Solved – Challenges Addressed

**Remote Programming**: All the firmwares built for SensLAB contains an embedded FTP server. The main goal of this server is to update the "application" sector in the flash memory [RD-38].

**Recovery mechanism from programming**: In case of failure (fault in FTP transfers for example), the module provides an easy mechanism for recovery. Each application image in flash is stored with an header containing a 32 bits CRC. At startup, a small custom bootloader examines the application image flash, and checks if the CRC is the one declared in the header. Thus it can decide if the image is corrupted or not. If it appears as corrupted, a BOOTP procedure is included for recovery (DHCP call, then TFTP transfers for the new image) [RD-38].

**Addressing**: Each testbed needs a DHCP server, allowing to give to each node a unique IP. Addressing is fixed; each MAC is known, and assigned to a defined IP.

## 6.12 WISEBED

The goal of the European project WISEBED [RD-40] is to establish a pan-European WSN of considerable size (more than 2000 sensor nodes in the first phase) which will be accessible by European researchers of all fields for experiments and will also serve as a showcase for European industries. They intend to achieve this goal by bringing together and extending different existing test beds across Europe and forming a federation of distributed test laboratories.

This project started in June 2008 and will last until May 2011.

In terms of its relation to EMMON, it seems that this project might be interesting for the communication test lab.

### 6.12.1 Deployment Details

The project aims to interconnect and extend existing testbeds. Those have different hardware and software characteristics. A detailed description is given in Deliverable D1.1 [RD-41], but the most interesting ones are the two larger-scale deployments:

- At University of Lubeck - Germany, 500 nodes of type Pacemates, CPU 32-bit (60MHz) LPC2136, Memory 256KB, RAM 64KB. Wireless interface Xemnics RF (868 MHz), Interfaces Serial, I2C, Radio Interface, sensors: Heart rate monitor, running iSense
- At Delft University of Technology - The Netherlands, 100 nodes of type TNOde, CPU 8-bit(8MHz) Atmega128L, Memory 128KB, RAM 4KB. Wireless interface CC1000 (868 MHz), sensors: Temperature, Humidity, running TinyOS

### 6.12.2 Network Architecture

A hierarchical architecture is adopted:

- The bottom layer contains the wireless sensor nodes that are running iSense, Contiki, TinyOS, or legacy systems. These devices form wireless networks that constitute the WSN testbeds.

- The testbeds of each partner are controlled by Portal Servers that provide access and expose interfaces to manage and operate them. Users can connect to a single testbed directly via the Internet accessing the interface provided by the particular portal server. In order to do so, users must be aware of the public IP address of the individual portal servers.
- The portal servers of each testbed partner site are interconnected via an overlay network. Peers connecting to the overlay network may access one or more portal servers in order to use multiple testbeds in a distributed manner. In order to do so, users are not required to know the public IP address of the portal servers.

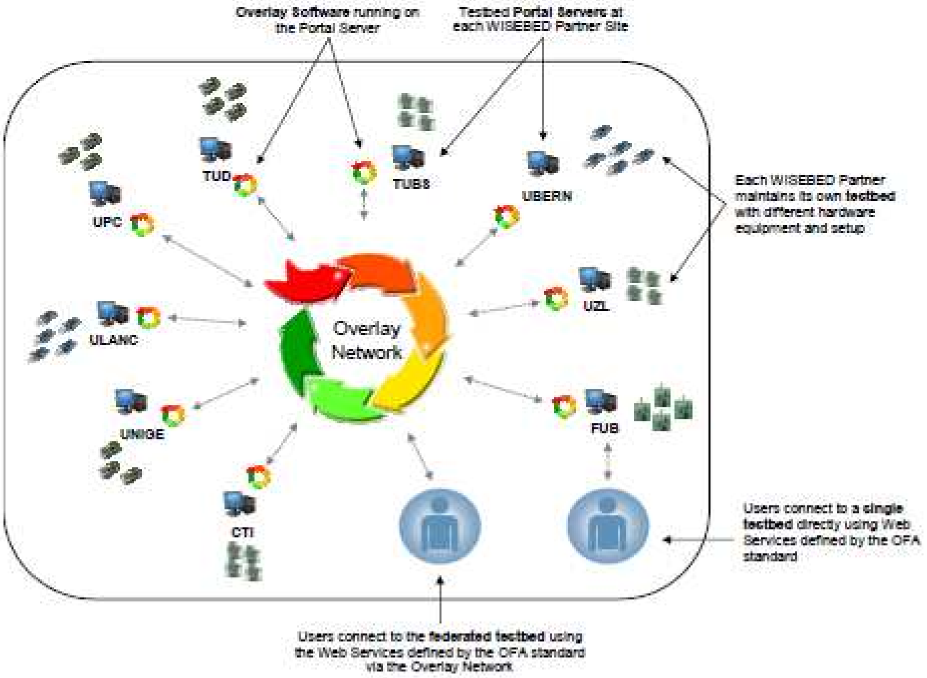
Overlay Software running on the Portal Server
Testbed Portal Servers at each WISEBED Partner Site
TUD
TUBS
UBERN
UPC
Each WISEBED Partner maintains its own testbed with different hardware equipment and setup
Overlay Network
ULANC
UZL
UNIGE
FUB
CTI
Users connect to a single testbed directly using Web Services defined by the OFA standard
Users connect to the federated testbed using the Web Services defined by the OFA standard via the Overlay Network

Figure 7: WISEDED network hierarchical architecture

### 6.12.3 MAC / Routing Protocols

IEEE 802.15.4, IEEE 802.15.1, RS 232.

### 6.12.4 Federated Communication

The portal servers have an internet portal.

### 6.12.5 Lesson Learned – Problems Solved – Challenges Addressed

Since this project is still running, a list of the expect contributions are:

- A multi-platform WSN Software Development Kit (SDK), using the component model OpenCom.
- A testbed management system.
- A simulation system.

- WISELIB, a library that will contain different algorithms for a number of purposes, ranging from standard algorithms to the latest research developments.
- A tailor-made data representation called WiseML (based on GraphML) to record experiment traces.

Three scenarios are targeted:

- Global facility management – building monitoring (fixed sensor nodes measuring static (in terms of location) phenomena),
- Object tracking at borders (fixed sensor nodes measuring a mobile phenomena)
- Sports tracking: track and guide the participants of a large-scale sports event, e.g., a marathon race (mobile devices and a mobile context-situation).

## 6.13 Smart – ITS / Btnode

The Smart-Its project [RD-42] - [RD-44] is interested in a far-reaching vision of computation embedded in the world. In this vision, mundane everyday artefacts become augmented as soft media, able to enter into dynamic digital relationships.

The project aims for small-scale smart devices - "Smart-Its" - small-scale embedded devices, that can be attached to mundane everyday artefacts to augment these with a "digital self". These devices will be as cheap, as unobtrusive and as generic as state-of-the-art smart labels (i.e., RFID tags). Smart-Its nodes are generic smart devices that perceive their environment through a collection of sensors, with peer-to-peer communication, and with customizable behaviour. Collections of such devices will be used to augment and interconnect entire families of artefacts, such as scattered personal belongings, toys in the playroom, and objects in collaborative interactive experiences.

The "Smart-Its" are seen as enabling technology for building and testing ubiquitous computing scenarios, and we will use them to study emerging functionality and collective context-awareness of information artefacts.

This project started in 2001 and ended in 2003. Its objectives were:

- to develop a range of Smart-Its devices, varying in processing power, sensory capabilities, and energy consumption;
- to investigate perceptual computing methods for ad hoc connected sensor devices;
- to develop service infrastructure for interconnected embedded technologies;
- to develop an open architecture for collective context-awareness;
- to explore novel applications and use experiences enabled by Smart-Its technology.

Since it is a very old project, it doesn't seem to have much in common with the EMMON goals, even if as a real world deployment related project some useful lessons can be learned.

### 6.13.1 Deployment Details

The Smart-Its project is based on a philosophy of building and trying fully functional prototypes. The first device prototypes are based on two different microcontroller platforms, Atmel and PIC. The Atmel platform enables to look into Bluetooth integration, while the PIC-based platform is used in conjunction with RFM communication. The overall device architecture is modular so that different sensor boards can be connected to either microcontroller platform.

Smart-Its artefacts are:

- Smart-it based on Atmel's ATmega103L microcontroller with 128kB of in-system programmable flash memory and only 4kB of SRAM. Ericsson's Bluetooth modules allow communication between different devices.
- A device that integrates a PIC 16F876 20 MHz for processing, RFM 868MHz for communication (128kbit/s), on board sensors and an I2C interface for sensor/actor boards. Power is supplied by 3V lithium cell.
- RS232 Add-On is an RS232 interface to Smart-Its, with IrDA physical layer and powered through main board (e.g. Smart-It)
- Sensor board (TDS 0.0-0)
    - Interface: I2C
    - 8 char x 2 line display
    - High-Resolution temperature sensor
    - Piezo sound
    - I/O Test board for input and output
- BTnode
- PC

### 6.13.2 Network Architecture

Network architecture is flat. The communication is based on detection of Smart-Its within sending range.

Handheld devices can serve as mobile gateways to background infrastructure services. Technically, this is achieved by establishing a local short range connection from a smart object to a handheld device, and a long range communication link from the handheld to a background infrastructure server. In this case using a PDA, might be an IEEE 802.11 link to a base station, and a GSM or GPRS connection in case of mobile phones.

### 6.13.3 MAC / Routing Protocols

Mobile ad hoc network, a self-configuring network. They are responsible for determining their own paths through the network. Smart-Its are used for post hoc computational enhancement. Smart-Its allow these artefacts to have digital identity, to perceive their own state and environment, to communicate with peers in ad hoc networks, and to interface with other infrastructures and services.

### 6.13.4 Federated Communication

IEEE 802.11 link to a base station, and GSM / GPRS connection, in case of mobile phones.

### 6.13.5 Lesson Learned – Problems Solved – Challenges Addressed

**Heterogeneity and Scalability**: Sensor networks should employ in network data processing and aggregation in order to reduce the amount of data that has to be transmitted within the network. This is desirable in order to achieve energy efficiency and to match the typically limited capacity of the communication channels.

**Resource Management:** Computing and memory resources of sensor nodes are often too limited to perform typical signal processing tasks (e.g., FFT, signal correlation). Hence, clustered architectures were suggested, where the cluster-heads are equipped with more computing and memory resources. Cluster-heads then process and aggregate sensor data collected from the nodes in their cluster. For example, PDAs with proprietary hardware extensions for wirelessly interfacing the sensor nodes are used for this purpose. With Bluetooth-enabled sensor nodes, off-the-shelf PDAs and laptops can be easily integrated as cluster heads without hardware modification.

**Collaborative Processing:** A typical sensor node has only limited processing power, for these reasons, sensor nodes usually need to cooperate with others. The basic system concept that enables such kind of inter-node interaction in the BTnode system services is a distributed tuple space. The distributed tuple space serves as a shared data structure for a set of sensor nodes which enables them to exchange and process data collaboratively. The main advantage of the tuple space approach is that nodes

## 6.14 SensorScope

SensorScope [RD-45] is developing a large-scale distributed environmental measurement system centred on a wireless sensor network with a built-in capacity to produce high temporal and spatial density measures. This system is composed of multiple solar-powered sensing stations which communicate wirelessly, constituting a sensor network. The sensing stations measure key environmental data such as air temperature and humidity, surface temperature, incoming solar radiation, wind speed and direction, precipitation, soil water content, and soil water suction.

The Research project is now continuing as a spin-off company.

### 6.14.1 Deployment Details

In this project six deployments have been tested, “ranging in size from 6 to 97 stations, from the EFPL campus to high-up in the Alps” [RD-46]. The nodes used are Shockfish TinyNode [RD-47] sensor motes, whose characteristics are as follows:

- CPU MSP430 (16 bit) @8MHz.
- 48kB of ROM, 10kB of RAM and 512kB of Flash memories.
- Semtech XE1205 radio, with frequency band 868-870MHz, bit rate 76kbps and range up to 500m (@15dBm).

To allow for long-term deployments a solar energy system has been designed, composed by a solar panel and two rechargeable batteries. Stations are equipped with seven sensors measuring: air temperature and humidity, surface temperature, solar radiation, wind speed and direction, soil water content and suction, and precipitation [RD-46].

The average price of each station is around €900, and this price has been kept down using lower-end sensors.

### 6.14.2 Network Architecture

The overall network architecture [RD-46] is composed by a multi-hop flat WSN with a single sink. The sink is a GPRS-enabled node that sends gathered data to a remote database server, which makes it available to other servers on internet. Remote management of the sink is possible via GSM text messages.

### 6.14.3 MAC / Routing Protocols

The software node architecture follows the OSI model with five layers (Application – data gathering, Transport – queuing, Network – Routing and Synchronization, MAC – Power management and ACKs, and Physical layer – the Radio).

At the Network layer, motes maintain a neighbourhood table in which they store the neighbours they can hear from. This neighbourhood discovery is not a separated process, but it is performed by listening the data traffic, while the sink starts this process by emitting beacons. Each time a packet is captured, the table is updated with the information about the neighbour's ID, a cost (hop distance to the sink) and a timestamp. With the help of this table, the routing adopted is a randomizing solution: each time a packet has to be routed, the forwarding node randomly selects a next hop between the neighbours closer to the sink. To give priority to better neighbours, a link quality estimation is also used (a measure based on a count of missing sequence numbers of packets).

To allow meaningful exploitation, gathered data must be time-stamped by the nodes. So synchronization among the nodes is needed. In this solution the global sink time is shared across the WSN nodes. The MAC is also based on this mechanism: since the radio has to be turned off most of the time, a network wide synchronization enables nodes to adopt a duty-cycling scheme instead of a low power listening.

### 6.14.4 Federated Communication

Depending on the deployment scenario and the available communication resources, different federating technologies have been used: GPRS/GSM, Wi-Fi, or Ethernet.

### 6.14.5 Lesson Learned – Problems Solved – Challenges Addressed

The lessons learned from the SensorScope project are efficiently collected in the reference [RD-46]. The next paragraphs provide a summary of these.

**Hardware and Software development**:

*Consider local conditions*: you must carefully investigate how local environmental conditions will affect your deployments. In particular it is crucial to simulate the anticipated conditions as accurately as possible to avoid unexpected hardware failures.

*Time Drift*: the crystals used in sensor motes are imperfect and the temperature impacts their precision. In particular the colder is the temperature, the slower the crystal oscillates, and this can have an impact also on day/night cycles in outdoor deployments. As a consequence, protocols should be designed accounting for drifts when waking up the nodes rather than believing in their perfect synchronization.

*Hard shell – soft core*: in outdoor deployments, packaging of sensors is of prime importance. Nodes should be protected from humidity, dust and atmospheric contaminants, even without affecting their sensing capabilities. In this project corrosion of connectors has been identified as the main cause of sensors failures and corrupted measurements. This clearly imposes to accurately choose the best packaging mechanisms in an application-dependent way.

**Keep it small and simple**: to avoid unexpected interactions between software components as much as possible and to realistically think to read and maintain an application code, it is necessary that it is simple even if in some case sub-optimal.

**Remote control**: even in easy-to-access places, the ability to remotely control (reconfiguring parameters or reprogramming nodes) the deployment is highly desirable. In this project the reconfiguration of the sink is possible via GSM text messages and also its reprogram is done via an FTP server. However, until now, reconfiguration or reprogram of the network is still impossible due to the lack of a dissemination mechanism. One foreseen possibility is to use Deluge as an over-the-air programming tool.

**Energy consumptions**: while most solutions approaches the problem by reducing radio activities, don't forget that LEDs are big energy consumers.

**Network management – monitoring nodes**: in this project, besides traditional sensing packets, sensor motes generate some kinds of status packets to monitor the residual energy of the batteries, statistics about the most recent activity of the transport layer (e.g. number of packets sent, number of non-acknowledged packets or the greatest size of the queue) and a dump of the neighbour table. By sending this information few per hour back to the C&C, several other findings can be validated for the network. For instance, in this project it was seen that, since there is energy harvesting via solar panel, the backup battery was never used, even in multiple and consecutive cloudy days, or that the load distribution among nodes is not fair (there are some nodes which act as main hubs for routing packets to the sink). Moreover, it should be planned early what kind of statistics could be more useful to collect from the network nodes, since after deployment it is very hard to implement such additional monitors. Another important aspect is related to the need for performing as many on-site checks as possible. By means of sniffer devices able to interpret the overheard packets, a deployed system can be monitored with the aim of discovering problems as early as possible.

**Network deployment and exploitation**: since data are collected having in mind an application objective, the end-user must be present in all the stages of deployment preparation: from sensor selection, placement and calibration to data analysis. For instance, without such interactions, it is possible to end up with solutions potentially non-working, solving non-existing problems! As an example, in SensorScope, knowing that a sampling rate less than two minutes is useless for an environmental monitoring leads to omit network congestion management. Furthermore, to set up a WSN deployment a preliminary work consist in checking the possible radio interferences and trying to minimize them, by e.g. switching to another unused channel. This is particularly important for indoor or urban deployments. Furthermore since traceability of nodes could be important (e.g. after having identified at the C&C a corrupted node), in this project motes and sensors are in the process to be tagged with RFIDs, in order to allow the full traceability of devices and measures.

**Testing and deployment preparation**: since testing functionalities is composed by many test-it-and-fix-it cycles, the testbed must be easily and quickly accessible. Moreover, replacing batteries is not a good idea even if some slick power saving algorithm is used. If the goal of a testbed is to fix the network code, sensors could be deployed in an indoor environment, plugged into AC power and equipped with some stuff for easy access and reprogram (in the project a Digi Connect module has been used to transparently access the mote via an Ethernet connection [RD-46]).

**Simulation**: instead of using large scale testbeds, a simulation can be efficiently adopted. However, existing network simulators do not provide insights into the quality of the "real" code to be deployed. To overcome this issue, a new class of tools has been considered (like TOSSIM and AVRORA), which enables emulations rather than simulation. Nevertheless, these tools are very platform specific (e.g. TOSSIM is specific for TinyOS motes) and only a few architectures have been ported so far.

**Data Reliability**: packaging sensors may affect the measurements. Once packaged, all sensors should be calibrated comparing their measurements to a high-precision reference station and the bad sensors (i.e. correlation coefficient below 0.98 [RD-46]) must be simply discarded. Moreover, sensory data should be scrutinized as soon as they reach the C&C, to promptly detect arising problems and malfunctions (e.g. broken sensors, failing sink). Often, this could be done by correlating measurements of different and close sensors, but in some cases a strong interaction with the End-User may help identifying problems and bugs when they arises.

## 6.15 WASP

Industries are reluctant to use results coming from academic research in WSNs. A major cause is the magnitude of the mismatch between research at the application level and the node and network level. The WASP project [RD-48] - [RD-52] aims at narrowing this mismatch by covering the whole range from basic hardware, sensors, processor, communication, over the packaging of the nodes, the organization of the nodes, towards the information distribution and a selection of applications. The emphasis in the project lays in the self-organization and the services, which link the application to WSNs.

Two application scenarios have been chosen: herd control (detection of health problems with focus on claw health and locomotion) and elderly care (activities of daily living using wearable/ambient sensors).

The project started on 09/2006 and will run until 08/2010.

### 6.15.1 Deployment Details

We were unable to find any report of neither large scale deployment, nor details about the short testbeds that have been deployed.

Herd control application with 10+ node deployment, telosB and Imote2 are used for the hardware. Custom hardware is used for body sensor networks.

### 6.15.2 Network Architecture

Mesh network is used in the herd control application.

### 6.15.3 MAC / Routing Protocols

A different type has been chosen for each of the two application scenarios. The stack of the Body Area Network (BAN) for elderly care scenario encompasses the following protocols:

- Localization Protocol – RSSI
- MAC Protocol - IEEE802.15.4
- Security Protocol - IEEE802.15.4 Security
- Time Synchronization – FTSP
- Routing – N-SafeLinks.

The herd control stack is composed of the following protocols:

- Localization Protocol - DV-Distance
- MAC Protocol – WiseMAC
- Time Synchronization - time diffusion protocol
- Security Protocol - IEEE802.15.4 Security + Zigbee Security
- Routing OLSR
- Transport - TCP-like protocol
- Service Discovery – SLP

### 6.15.4 Federated Communication

None identified.

### 6.15.5 Lesson Learned – Problems Solved – Challenges Addressed

The tangible results of the project are:

- A consistent chain of energy-sensitive software components.
- Sets of cross optimized software stacks,
- Mobility Framework for OMNeT++ 4.
- Benchmarks and a set of measurements on energy- and code- efficiency.
- Rules for the design of configurable sensor nodes.
- A prototype implementation in two of the three chosen business areas.

The software is built using a service-oriented approach.

## 6.16 WINSOC

The key idea of WINSOC [RD-53], [RD-54] is the development of a totally innovative design methodology, mimicking biological systems, where the high accuracy and reliability of the whole sensor network is achieved through a proper interaction among nearby, low cost, sensors. This local interaction gives rise to distributed detection or estimation schemes, more accurate than that of each single sensor and capable of achieving globally optimal decisions, without the need to send all the collected data to a fusion centre. The whole network is hierarchical and composed of two layers: a lower level, composed of the low cost sensors, responsible for gathering information from the environment and producing locally reliable decisions, and an upper level, composed of more sophisticated nodes, whose goal is to convey the information to the control centres.

Two scenarios have been identified for this project:

- Forest fire detection and fire risk estimation;
- Landslides detection and prediction.

This project, which started on 09/2006 and ended on 02/2009, has some similarities to the EMMON project, namely the target applications. Nevertheless, the technical approach is different. Moreover, although the project is finished there is (yet) not much information about it.

### 6.16.1 Deployment Details

**Forest fire detection and fire risk estimation**

A massive number of small sensors (called level 1 sensor nodes) are deployed by an airplane flying through a fire region, over an area of up to 50km$^2$, and providing a minimum of one sensor node per 100m$^2$ [RD-53]. It is expected that the maximum number of sensor clusters (called level 2 nodes) per squared km is 4. The distance between two level 2 nodes is about 10 meters. There are also level 3 nodes, which are nodes that do not monitor environmental parameters but guarantee communication in the network and are equipped with GPS devices. These level 3 nodes can be as far from each other as 500 meters. Both level 2 and level 3 nodes are human placed.

**Landslides detection and prediction**

The deployment is set for Government College in the Idukki district of the state of Kerala (India), which is a landslide prone site. This site has about 0.5km$^2$ of area. A maximum of 9 sensor columns are placed inside vertical holes drilled in the ground and arranged in a grid pattern. If the worst case transmission distance of the lowest level wireless sensor nodes is insufficient to cover the entire landslide when only 9 sensor columns are used, then relay nodes will be employed to pass data from one sensor to the other. The field deployment will only require around two geophones total due to the ready transmission of large vibrations through the earth. The sensors are placed in a distributed fashion along the length of the sensor column with an average separation of 2 to 3 meters.

A sensor column can have 2 or 3 pore pressure transducers placed a quarter above the bottom and a quarter distance below the top, 3 or 4 single axis inclinometers (tilt meters) and one geophone at the bottom. The sensor tube (typically made of thick wall ABS plastic) having a diameter slightly larger than the size of the sensors, is used for the sensor column. The sensing part (sensors) of the column is underground and the wireless sensor node (processor + radio module) stays above the ground.

### 6.16.2 Network Architecture

**Forest fire detection and fire risk estimation**

- The network will have a multiple hierarchy.
- The monitored area will be covered by two independent ad hoc networks of sensor nodes (level 1 and 2), both communicating with one node from network on level 3. Every level 1 sensor node communicates with more level 1sensor nodes. Level 1 sensor nodes communicate with 0 to n nodes of level 3. The same applies for level 2 sensor nodes. If there is no direct communication between level 1 (or 2) sensor nodes and any node of level 3, then the information has to be transferred through other level 1 (or 2) sensor nodes. There is no guarantee that all level 3 nodes will have access to a public network, so the network of level 3 nodes must ensure the transmission of information among level 3 nodes in order to guarantee communication with the outside world.
- The level 1 sensors nodes self-organize into an ad-hoc network such that information can be transmitted in a multi-hop route to level 3 nodes - The sensors could be destroyed during the fire and this possibility has to be monitored.
- Level 1 sensor nodes are continuously monitoring and are able to communicate with each other and, directly or through other level 1 sensor nodes, with at least one level 3 node (unidirectional communication).

#### Landslides detection and prediction

The wireless sensor network used in this scenario has three levels of nodes: low level nodes, cluster heads, and the sink node (or gateway node). The lower level wireless nodes are connected to the sensor column comprising the geological sensors. The low level nodes coming under each cluster head are allowed to communicate with each other and arrive at a consensus on the parameter values. The consensus value will then be forwarded to the cluster head. No processing is done in any of the cluster heads. All of the higher level nodes will be receiving the data from the lower nodes and transmitting it to the successive higher level nodes. The cluster heads transmit the data to the sink node, which will then forward the data via TCP/IP (possibly over WiFi) to a local analysis computer. From there, it is transmitted via a satellite link to a more sophisticated landslide data processing and modelling centre located at Amrita University.

### 6.16.3 MAC / Routing Protocols

No relevant information was found regarding this topic.

### 6.16.4 Federated Communication

The potential communication technologies could be GPRS, WIFI, WIMAX and VSAT. Possibly, Wi-Fi technology will be used.

### 6.16.5 Lesson Learned – Problems Solved – Challenges Addressed

No conclusions were found for this project and therefore it was not possible to determine any lessons learned, problems solved or addressed challenges. This project is on-going and this situation might change in the future.

## 6.17 EFPL – COMMON-Sense Net

The COMMON-Sense Net system (for Community-Oriented Management and Monitoring Of Natural Resources via a Sensor network) [RD-55] - [RD-58] aims at designing and developing an integrated network of sensors for agricultural management in the rural semi-arid areas of developing countries. On top of having an impact on yield and efficiency at the local level, the system will allow the collection of extensive data that can be reused to better understand the effects of water and other environmental parameters on agriculture, and thus to develop replicable strategies.

COMMON-Sense Net consists in a wireless network of ground-sensors that will record periodically the water content of the soil. Weather stations will also be used to get an improved picture of the field-environment. In the intended model, sensors record data on a periodic basis, and send them in a multi-hop fashion to a centralized processing unit, which performs statistical computations and correlates them with meteorological and ground-water data to assess the optimal farming strategy. The centralized processing unit can be linked to external meteorological servers to help in its decision process. This can be done, depending on the environment, through a wired or wireless connection, or a satellite link.

The project ended in August 2008. Even if this project is quite old, it has a good overlapping with the intended EMMON goals, especially regarding continuous environmental monitoring and data collection from a WSN to a C&C station.

### 6.17.1 Deployment Details

The area of interest is a cluster of villages in India, consisting of mostly marginal and small farmers. The proposed project area (radius of 25km) encompasses approximately 25 villages, out of which eight have already been identified as benchmark locations. This area encompasses around 100.000 inhabitants. However, the pilot application deployed in Pavagada consisted of about 20 wireless sensors, deployed in geographical clusters corresponding to the assignment to one base station, which is connected to a centralized server via an 802.11 (wi-fi) link.

The intended sensor network platform has been chosen in 2004 to be the MICA2 [RD-57], while in 2006 it has been decided to migrate to the TinyNode platform, which ensures longer radio range and lower power consumptions (in all radio state, but TX) [RD-58]. For meteorological parameters, MTS400 weather board designed for use with Mica2 has been used, integrating temperature and humidity (Sensirion SHT11), ambient light (TAOS TSL2550D), and barometric pressure (Intersema MS5534AM). Soil moisture is a parameter of higher variability. The ECH2O probes, which can be plugged to Mica2 motes via a data acquisition board, have been chosen [RD-57].

Enclosure: FIBOX [RD-58]

- Boxes: PC 150/50 LG
- 2 x PG 16 cable glands
- 1 x MB 10894 pressure equalizer plug
- Cables going in the soil need to be protected up to 1 meter above the ground

As an operating system, TinyOS-2.x is used, with proprietary MAC plus Routing protocol Dozer by Shockfish (instructions on how to use it are available with the code) [RD-58].

### 6.17.2 Network Architecture

The solution proposed in this project is to rely on a two-tiered network composed of several, possibly disconnected clusters of sensors, linked by an overlay network of 802.11 access points using as a power source the numerous electrical poles present even in the most remote rural areas in India [RD-57].

### 6.17.3 MAC / Routing Protocols

TinyOS standard implementations of the communication protocols: firstly a B-MAC and the default multihop routing at the Network layer. In a successive refinement, the adopted solution was the Dozer protocol, which is a joint TDMA-based MAC and tree-based Routing [RD-58].

### 6.17.4 Federated Communication

Firstly, an IEEE 802.11 WiFi bridge was used, because GSM connectivity was poor in the deployment area. GPRS was used as soon as base stations were deployed, because the range limitations of 802.11 proved to be severe [RD-58].

### 6.17.5 Lesson Learned – Problems Solved – Challenges Addressed

**Network behaviour model**: Data can be generated periodically or as a response to an event. In this project, since agricultural scientists are curious to observe fine-grained data in order to determine what level of granularity is significant, as much data as possible should be generated, while not compromising the lifetime of the network, so that it remains operational throughout a full season at the minimum [RD-58]. In particular, for the deficit irrigation use case, a hybrid strategy has been followed: a periodic data collection model, with a variable rate of emission depending on the data variability at the time. For instance, it is not necessary to collect soil moisture data at more than one sample per hour, or even per day, when no rain is falling. However, when water is brought in either by precipitation or irrigation, a finer resolution might be desirable.

**Network deployment issues**: Memory corruption of motes contributes to the overall unreliability of the system. The experience in live deployment resulted in unpredictable node ID changes. Although the node ID may be brought back to its original value by a software reboot of the running code, a node freeze proved to be a corruption of the flash memory. Maybe, high package temperatures are the cause for the flash corruption seen in the field deployment [RD-58]. Furthermore, the general lessons to be drawn from the connectivity issues, faced in the field, is the pressing need of an appropriate deployment and maintenance support tool that helps with the deployment of a wireless sensor network. Moreover, such a tool, if it is to be put in the hands of a non-specialist user, has to be intuitive and must not require a priori knowledge of networking.

**Sensory data reliability**: The measurements appeared to be noisier than hoped, although they remain in the 5% range specified in the ECH2O user manual. This problem can be solved by averaging over a larger number of samples (which is what is done a traditional data logger), but this increases the power consumption and decrease the lifetime significantly. Instead, when the Tinynode platform has been used, a new data acquisition board was designed in collaboration with Shockfish, filtering out high frequency signal variations. This proved to reduce significantly the effect of noise, while not compromising on the accuracy.

**Network lifetime**: An average lifetime of only two weeks was observed in preliminary tests. Failed links might indeed cause numerous retransmissions, exchange of resynchronization packets and undue active-radio time. Further investigations on this were still running at the time of [RD-58], but no further results are available.

## 6.18 VigilNet

VigilNet [RD-61], [RD-62] is one of the major efforts in the sensor network community to build an integrated sensor network system for surveillance missions. The focus of this effort is to acquire and verify information about enemy capabilities and positions of hostile targets. Such missions often involve a high element of risk for human personnel and require a high degree of stealthiness. Hence, the ability to deploy unmanned surveillance missions, by using wireless sensor networks, is of great practical importance for the military. Because of the energy constraints of sensor devices, such systems necessitate an energy-aware design to ensure the longevity of surveillance missions.

The goal of VigilNet is to develop an operational self-organized wireless network to provide tripwire-based surveillance with a sentry-based power management scheme, in order to achieve minimum 3–6 months life time with current hardware capability. The system should also support timely detection, tracking and coarse granular classification of vehicle and personnel targets over all kinds of terrain. The main deployment scenario is actually along a road for detecting vehicular passing.

The application scenario of VigilNet is not related to EMMON, but the developed energy-aware design methodology for large scale networks may be of potential interest, as well as the solutions adopted for timely reporting of detected events.

### 6.18.1 Deployment Details

VigilNet currently consists about 40,000 lines of NesC and Java code, running on XSM, Mica2 and Mica2dot platforms, above TinyOS operating system. The complete system is designed to scale to at least 1000 XSM motes and cover minimal 100x1000 square meters to ensure operational applicability.

### 6.18.2 Network Architecture

The architecture is cluster-based. Nodes are grouped in patches (sections) at deployment time, based on the road under monitoring. Each section is provided with a base station, i.e. a powerful device able to long-range communications to a distant collector point. In each section a backbone is then formed to route information to the base station.

### 6.18.3 MAC / Routing Protocols

Based on the system overview presented in [RD-62], at the MAC level a B-MAC protocol is adopted, while at the Network level, a robust diffusion tree, which is a routing algorithm very similar to the directed diffusion.

### 6.18.4 Federated Communication

Not specified. In the WSN, communications are based on MAC and Routing protocol up to the “base station”, which is able to send remotely the reports.

### 6.18.5 Lesson Learned – Problems Solved – Challenges Addressed

**Network behaviour**: this project focuses on surveillance system, so only reactive behaviour is considered, i.e. no periodic measurements report.

**Time Synchronization**: fine grained clock synchronization achieved by costly periodic beacon exchanges may not be suitable for the energy-constrained surveillance system. In this project time synchronization is performed periodically via beacons, but only once per day.

**Failure detection**: failure detection systems at link layer in bandwidth constrained platforms like MICA2 is too costly and leads to a reduction of the effective data rate by nearly 50%. In this project the solution proposed is to introduce a soft-state into the diffusion tree, i.e. the diffusion tree is refreshed per system cycle to prune failed links and discover new routes.

**Radio link asymmetry**: low power radio exhibits very irregular/anisotropic communication patterns especially when sensor nodes are placed on the ground. Discovering such link asymmetries via a link layer handshaking is very expensive. In this project the solution proposed foresees a local beaconing only in the initial phase. A node inserts in the beacon the nodes' IDs of its identified neighbours. A node receiving this beacon checks whether its ID is in it or not. In the former case the link is symmetric, while in the latter case it identifies a link asymmetry. By repeating this process more times to have a sufficient statistical significance, symmetric links are identified and only those links are effectively used after.

**Network deployment**: nodes are manually placed and position information is sent to each node at the same time of its placement. In particular, in this project a GPS assisted mote is used to deploy the network nodes. When a node is physically placed, the GPS mote sends to it the actual position with a configuration message.

**Network reprogramming**: in this project there is not a reprogramming feature, but only a reconfiguration process; i.e. nodes can receive a new set of parameters embedded in the time synchronization beacon messages, but this doesn't lead to a reboot of the nodes.

**Data aggregation**: in the hypothesis that no simultaneous events may occur, i.e. different event are far enough, in-network aggregation of reports into a digest reduces transmissions and energy consumptions. The system in this project respond to an event by forming groups of sensors, i.e. all the sensors which sense the event are grouped each other. Moreover, this group logically moves as the event moves. A group is further represented to the external world by a leader which collects reports and, if the confidence level of detecting an event is higher than a threshold, sends a digest of the reports back to the base station.

**Reliability**: since lower layers often lack of domain-specific knowledge (i.e. the retransmission of a frame can be driven by an application-specific knowledge of the content of that frame), in this project an important lesson learned is that to achieve energy efficiency it is better to implement reliability mechanisms at the application layer.

**False alarm reduction**: false alarm may be transient or persistent. While a simple exponential weighted moving average (EWMA) on the mote is sufficient often to deal with transient false alarms, network aggregation relative to a threshold value can eliminate the persistent false alarms. In the worst case, when multiple persistent false alarms are generated simultaneously, persistent false alarm may be eliminated by analyzing spatial-temporal correlations patterns among the consecutive reports at the base station. Furthermore, a faulty node detection algorithm is proposed to shut down misbehaving nodes automatically.

## 6.19 Comments

In this section we have listed 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, SensorScope) to surveillance systems (e.g. Exscal, VigilNet) or disaster recovery (e.g. Aware, Runes), or ranging from real world deployments to testbeds development (e.g. SensLab, Cruise).

Several other projects have been investigated in our analysis (EYES [RD-26], [RD-28], Embedded Wisents [RD-173], a Large Scale Demonstrator at Berkeley [RD-174], First-of-its-kind Ad Hoc/Sensor Network Testbed [RD-175], SLEWS [RD-59], [RD-60], TWIST [RD-63], [RD-64] and GEODES [RD-176]). However, the information gathered from these projects is not sufficient, either because they are old projects (e.g. 2001 in the case of the demonstrator at Berkeley) or because not enough documentation is available yet (e.g. for GEODES, which started in the first quarter of 2009).

Basically, for each project we have identified a set of solutions and lessons learned to solve the problems of real world deployments. We think that some of these best practices may be further investigated, to be successfully used in EMMON.

In order to infer useful guidelines to evaluate the technologies and identifying a design methodology, the main lessons learned from the majority of these projects [RD-46], [RD-67], [RD-68], [RD-69] are reported below.

1. **Keep it simple**: simple solutions are the best ones. Simple solutions are also easier to handle and debug than complex solutions. Moreover, by interacting with the end-user will help identifying the appropriate requirements, hence allowing a reduction on the number of features and the solution’s complexity. For example, it can be useless to design a complex congestion control algorithm if the probability of congestions is negligible.

2. **Embed tests in the design cycles**: using a testbed is important and tests have to be included in the design refinement cycles (test-it-fix-it), because many properties and problems appear only in the real world deployment. So it is important to have the possibility of a fully controlled environment where to deploy the testbed.

3. **Modular design**: it is of paramount importance to proceed by steps using a modular design. In the first phase, it is important to include the most basic features in the design cycle, assessing their correctness by means of evaluation with both simulation and testbed activities. In the second and the subsequent steps, the other functionalities have to be added and validated iterating the design cycles and assessments.

4. **APIs are not enough**: i.e. the best MAC may not fit the requirements of the best routing, so it is important to focus the attention to the interoperability criterion to evaluate each technology.

5. **Technical maturity**: it is important to choose technologies that are mature enough, especially those that have been implemented, preferably having been used for a long time and by many people.

6. **Availability of expertise**: gluing components together takes a lot of effort and requires in-depth knowledge of individual components. It is therefore important to have this knowledge available in the consortium.

7. **Auto diagnosis**: each software component should be capable of dumping its status and provide statistics about its internal operation, so debugging via in-node monitoring and statistics reporting is essential to identify faults early. Moreover, even if it is strongly required to use some form of reprogramming feature, it should be planned early what kind of statistics could be more useful to collect from the network nodes, since after deployment it is very hard to implement such additional monitors.

8. **Enclosures**[12]: especially for outdoor, a well designed enclosure (against humidity and environmental agents) will avoid many hardware faults. This is really important to avoid them, because e.g. some hardware faults should not be confused with communication faults. Finally, this is related to the problem of finding a good trade-off between the cost of each node and the hardware reliability. It is also important to make sure that the enclosures do not interfere with the communications otherwise they can compromise the operation of the system, thus becoming counterproductive.

9. **Data reliability**: sensory data should be scrutinized as soon as they reach the C&C, to promptly detect arising problems and malfunctions. Often, this could be done by correlating measurements of different and close sensors, but in some cases a strong interaction with the End-User may help identifying problems and bugs when they arise.

[12] This will be addressed by Work Package 5 in the deliverable D5.3.

# 7. Network Architecture

## 7.1 Requirements/Evaluation Criteria

Moving from the methodology presented in Section 4, the applicable criteria for network architectures are listed in what follows.

- Scalability (see Section 4.1.1.1).
- Timeliness (see Section 4.1.1.3).
- Reliability / Robustness (see Section 4.1.1.4).
- Resiliency (see Section 4.1.1.5).
- Energy efficiency (see Section 4.1.1.6).
- Interoperability (see Section 4.1.1.7).
- Data aggregation / compression mechanisms (see Section 4.1.1.8).
- Security (see Section 4.1.1.10).
- Technical Maturity (see Section 4.1.1.12).
- Availability of internal experience (see Section 4.1.1.13).

## 7.2 Existing Solutions

### 7.2.1 Flat

In a flat architecture, all sensor nodes transmit their own data and relay data for other nodes to the sink [RD-70]. Typically the protocols and algorithms adopted in this architecture are fully distributed and don't rely on any central coordination.

Another kind of maximally flat network architecture is conceivable by adopting the newest paradigm of complexity theory [RD-71], [RD-72], or chaos theory, of fully distributed systems. In the consortium there is expertise in such a field and some improvements in applying such technology to networking and WSN is in the roadmap of the EMMON project. Nevertheless, it is our opinion that this theory at present has a too low technical maturity, especially in terms of real deployments.

#### *7.2.1.1 Scalability*

Score: 4

Even if a flat network architecture is easy to deploy, the scarce availability of fully distributed algorithms and protocols is a severely limiting factor to the use of such architecture. Moreover, as the density of nodes increases, the absence of a local coordination reduces significantly the performance of such solutions.

#### *7.2.1.2 Timeliness*

Score: 4

Flat network architectures show higher latencies due to multi-hop nature of the communications in Wireless Sensor Networks. Moreover this is further exacerbated in the case of large scale WSNs.

#### 7.2.1.3 Reliability / Robustness

Score: 4

A flat network architecture is not designed with reliability and robustness in mind, especially in the case of large networks. It is hard to imagine replication strategies to duplicate nodes when there is not any hierarchical organization and/or cluster. If all the nodes are in charge of providing the same services, i.e., they are functionally equivalent, the network may not be robust the failure of any single node acting as service provider. This is true with respect to every kind of failure (node, link…)

#### 7.2.1.4 Resiliency

Score: 2

In a flat architecture, resiliency strongly depends on the replication style and node restart strategy (e.g., cold restart).

#### 7.2.1.5 Energy Efficiency

Score: 2

Without coordination among nodes in the network, difficulties may arise when handling collisions in communications, nodes duty cycles and efficient data aggregation schemes.

#### 7.2.1.6 Interoperability

Score: 1

The key advantage and challenge of flat architectures is the ability for a single access gateway to inter-operate with a wide range of radio technologies simultaneously on a common hardware and software platform, scalable to multiple cost and traffic profiles.

#### 7.2.1.7 Data Aggregation / Compression Mechanisms

Score: 3

Without coordination among nodes in the network, difficulties may arise when handling collisions in communications, nodes duty cycles and efficient data aggregation schemes.

#### 7.2.1.8 Security

Score: 4

Secure routing is difficult to achieve in a flat, non-hierarchical network.

Flat architecture in LSWSN might pose a problem for security key distribution, which would have to be performed in a centralized fashion (as for other network management issues).

This architecture imposes also non-flexible security mechanisms, since all links have the same mechanisms.

#### 7.2.1.9 Technical Maturity

Score: 3

The maturity of the paradigms for fully distributed flat networks is still low. Moreover, several projects and real deployments explicitly avoid using such a kind of extreme network architecture.

### 7.2.2 Cluster Based

Cluster-based architectures organize WSNs into a set of disjoint groups. Each cluster has a designated leader, the so-called clusterhead (CH). Nodes in one cluster do not transmit their gathered data directly to the sink, but only to their respective cluster head. Accordingly, the cluster head is responsible for:

- coordination among the cluster nodes and aggregation5 (i.e. compression) of their data, and
- transmission of the aggregated data to the sink, directly or via multi-hop transmission.

#### 7.2.2.1 Scalability

Score: 1

Clustered networks organizations have the potential to outperform their non-clustered counterparts, e.g. they allow for scalability of MAC and routing [RD-70]. However, for this potential to be realized, certain conditions need to be met. For example, the degree of correlation between inter-cluster nodes' readings must be quite high to ensure full performance superiority of clustered over non clustered WSNs [RD-74].

#### 7.2.2.2 Timeliness

Score: 1

Comparing with the flat network, it has been showed in [RD-70] that clustering is the major factor to improve network capacity.

#### 7.2.2.3 Reliability / Robustness

Score: 1

Based on the approach presented in [RD-73], in this architecture is possible to perform run-time recovery of the sensors from the clusters in which the gateway has experienced some faults. The mechanism is divided in to two phases; detection and recovery. In order to recover the sensors from the failed cluster it is important to detect whether a fault has occurred in the system. A consensus model of the gateways is followed to agree on a particular fault in the system. A consensus is required to maintain the synchronization in the network with respect to the status and cardinality of a gateway. The cardinality of a gateway device "A" is the number of sensor nodes that belong to the cluster having "A" as gateway.

The second phase of fault tolerance identifies the type of fault and performs recovery of the sensors.

#### 7.2.2.4 Resiliency

Score: 1

Once the gateways reach a consensus about the presence of fault, the next step is to identify the type of faults and allocate the sensors to new clusters. When a gateway is identified as completely failed all the sensors in its cluster are recovered.

Clustering is based on the distance between the sensors and gateways.

#### 7.2.2.5 Energy Efficiency

Score: 1

Clustering keeps network traffic local and reduces energy dissipation of long distance transmissions [RD-75]. Clustering can further conserve energy by employing cluster heads to perform local data aggregation or sensor fusion (refer to [AD-5] for the definitions).

#### 7.2.2.6 Interoperability

Score: 3

Clustering is a form of physical organization of nodes and clustered WSNs don't seem to have any major interoperability issues with other network layers. However, the physical organization and duty cycling does impose some constraints on when the data can be transmitted and how it is routed.

#### 7.2.2.7 Data Aggregation / Compression Mechanisms

Score: 1

Cluster heads naturally serve as aggregation or fusion points to process data, reducing the amount of transmitted bits to the sink [RD-70].

#### 7.2.2.8 Security

Score: 1

Hierarchical based architectures allow for differentiation in security mechanisms: we might have no security (or lighter) in lower tiers, where the data is still too local and with less meaning, and have higher security in upper tiers when the data is merged and starts to have a global sense and, hence, is more critical. Moreover, if one cluster has a security leakage, it might be detected when merging.

With clusters we have isolation: one attack or security failure can be limited to one cluster [RD-76].

#### 7.2.2.9 Technical Maturity

Score: 1

The cluster based approach is the most widely used paradigm for WSNs and real world deployments strongly rely on it, or equivalently, on the multi-tier one.

### 7.2.3 Hexagonal

For densely deployed wireless sensor networks, a hexagonal architecture is typically a two-tiered cluster-based network topology [RD-77]. At the first tier, the cluster heads collect sensed data in their neighbourhood. At the second tier, cluster heads send and route data packets to their destination.

Afforded by the techniques of ad-hoc networks topology control, hexagonal meshes enable trivial addressing and routing protocols. In such networks, it is showed in [RD-77] that it is possible to design conflict free transmission scheduling algorithms.

In the consortium (at ISEP), there is some experience available concerning this kind of network architecture.

#### *7.2.3.1 Scalability*

Score: 3

As specified above, this is a two-tier network architecture: this leads to good performance in terms of scalability. However, appropriate node placement at deployment time and topology control algorithms at run-time are essential to fully take advantage of the abstraction of a hexagonal network topology.

#### *7.2.3.2 Timeliness*

Score: 3

CDMA is used to communicate in intra-clusters in a collision-free fashion, while a scheduling algorithm is proposed for the inter-clusters communications. However, appropriate node placement at deployment time and topology control algorithms at run-time are essential to ensure the abstraction of a hexagonal network topology.

#### *7.2.3.3 Reliability / Robustness*

Score: 2

In [RD-77] the proposed algorithms are shown to be robust to link failures. Long links refer to those that arise when the interference range of a node is larger causing it to interfere with neighbours that it would not normally reach in a hexagonal topology.

#### *7.2.3.4 Resiliency*

Score: 2

The paper [RD-77] presents a constant time routing algorithm for hexagonal topology networks. This allows the network to be resilient to the long links failures, and to recover from them promptly assuring that packet deadlines are almost always met.

#### 7.2.3.5 Energy Efficiency

Score: 3

High energy efficiency is achievable via trivial MAC and routing schemes in hexagonal networks. However, appropriate node placement at deployment time and topology control algorithms at run-time are essential to ensure the abstraction of a hexagonal network topology.

#### 7.2.3.6 Interoperability

Score: 4

Topology control algorithms must be implemented. Also, the sensor nodes need to be deployed carefully to enable hexagonal network. The network in [RD-77] was simulated with irregularities in the links.

#### 7.2.3.7 Data Aggregation / Compression Mechanisms

Score: 3

Data aggregation mechanisms are compatible with the hexagonal topology. However, appropriate node placement at deployment time and topology control algorithms at run-time are essential to ensure the abstraction of a hexagonal network topology.

#### 7.2.3.8 Security

Score: 1

In [RD-78], a hexagon-based key pre-distribution scheme is presented and is showed that it can improve the key management in sensor network, through the use of the bi-variate polynomial in a hexagonal coordinate system, based on deployment information about expected locations of the sensor nodes. The scheme presented in [RD-78] can improve the probability of establishing pair-wise keys between sensor nodes of up to two hops apart by more than 40% over previous schemes.

#### 7.2.3.9 Technical Maturity

Score: 3

Some results exist about simulations and theoretical framework analysis and also commercial WSN platforms implementations. However, real deployments results are lacking.

### 7.2.4 Multi-tier (or Backbone Based)

A multi tier WSN is typically a heterogeneous network, where more powerful nodes (mostly IP-based) compose a backbone which helps to increase network reliability, timeliness and lifetime. Typically, resource-aware MAC and routing protocols are needed to utilize those resources [RD-79].

Moreover, there is a lot of experience available for some of these architectures in the consortium.

#### 7.2.4.1 Scalability

Score: 1

Generally, these protocols allow for using multi-tier networks architectures which improve scalability by often introducing high power devices as local collectors, like in cluster based architectures. Furthermore, in [RD-80] a cluster-tree network is proposed as a solution for hierarchically organize the WSN to overcome small range inter-sensor distances while maintaining low the traffic volume by exploiting aggregation among the cluster heads.

#### 7.2.4.2 Timeliness

Score: 1

Methodology proposed in [RD-80] provides a practical tool to choose the adequate settings of cluster-tree WSNs, for applications with real-time requirements, depending on the available resources (e.g. buffering at each node and bandwidth available), and the delay bound requirement.

#### 7.2.4.3 Reliability / Robustness

Score: 1

Using heterogeneous nodes is a very effective mean to increase network reliability at a reasonable cost.

#### 7.2.4.4 Resiliency

Score: 1

Heterogeneity can help into the implementation of customized recovery mechanisms aiming at achieving low TTR.

#### 7.2.4.5 Energy Efficiency

Score: 1

By hierarchically organize the network, nodes can remain in low power modes when their group (cluster) is not involved in the communication process and scheduling protocols can be efficiently used at the inter-cluster level. Moreover, since in-network computation is feasible and encouraged, further energy savings can be achieved.

#### 7.2.4.6 Interoperability

Score: 1

A backbone based network architecture guarantees the maximum of the flexibility for the Wireless Sensor Networks and is the most widely used architecture also because it allows the composability of several solutions using gateway devices.

#### 7.2.4.7 Data Aggregation / Compression Mechanisms

Score: 1

These architectures are specifically tailored to allow for exploiting data aggregation and compression mechanisms, i.e. in-network computations.

#### 7.2.4.8 Security

Score: 1

Hierarchical based architectures allow for differentiation in security mechanisms: we might have no security (or lighter) in lower tiers, where the data is still too local and with less meaning, and have higher security in upper tiers when the data is merged and starts to have a global sense and, hence, is more critical. Moreover, if one portion of the network exposes some security leakages, it might be detected when merging data at the upper tiers.

#### 7.2.4.9 Technical Maturity

Score: 1

The cluster based approach is the most widely used paradigm for WSNs and real world deployments strongly rely on it, or equivalently, on the multi-tier one.

In particular, in [RD-80] the methodology has been successfully applied to ZigBee networks and was implemented in commercial WSN platforms.

### 7.2.5 Real Time Architecture

RAP is a new real-time communication architecture for large-scale sensor networks [RD-81]. RAP provides convenient, high-level query and event services for distributed micro-sensing applications. The RAP packet scheduling policy is particularly suitable for communication scheduling when a large number of wireless devices are seamlessly integrated into a physical space to perform real-time monitoring and control.

#### 7.2.5.1 Scalability

Score: 1

RAP is a fully distributed architecture and so it scales well in large scale sensor networks because it is composed of efficient and localized protocols and algorithms at every layer. No per-flow state is maintained inside the network.

#### 7.2.5.2 Timeliness

Score: 1

The architecture includes a Velocity Monotonic packet Scheduling module which addresses exactly the timing requirements of a query. In particular RAP increases the number of packets meeting their end-to-end deadlines by prioritizing the transmission of contending packets based in their requested velocities.

#### 7.2.5.3 Reliability / Robustness

Score: 4

In [RD-81] authors propose two mechanisms for increasing reliability at MAC level by modifying original version of the 802.11 standard. However, the reference metric is the deadline miss ratio hence reliability is not explicitly addressed in the paper.

#### 7.2.5.4 Resiliency

Score: 1

The low deadline miss ratio shown in [RD-81] means that a low number of retransmissions is needed to complete packet delivery. Hence, MTTR should be low as well.

#### 7.2.5.5 Energy Efficiency

Score: 4

In [RD-81] RAP actually evidences good performance on timeliness requirements only and also data aggregation details, which impacts severely on the energy efficiency, are still missing.

#### 7.2.5.6 Interoperability

Score: 1

[RD-81] implemented GF, VMS & 802.11 extensions on GloMoSim. Network parameters were tuned in reference to Berkeley motes. The simulation covered an area of 136 X 136 m^2, with 100 nodes randomly placed throughout the grid. Each grid cell was 13.6 X 13.6 m^2. The radio coverage in these experiments were limited to 30.5 m radius with packet sizes of 32-160 Bytes out of which 28 Byte overhead was due to UDP/IP header. In these experiments DSR (ID based) and GF (Location based) were used for routing.

#### 7.2.5.7 Data Aggregation / Compression Mechanisms

Score: 4

In the RAP architecture, described in [RD-81], there is a coordination service which is responsible of dynamic management and data aggregation among sensors. Anyway it is still a not addressed topic in [RD-81] and so quite difficult to evaluate its impact over large scale WSNs.

#### 7.2.5.8 Security

Score: 4

In the RAP architecture, described in [RD-81], security is not addressed and so quite difficult to evaluate its impact over large scale WSNs.

#### 7.2.5.9 Technical Maturity

Score: 4

In [RD-81] no results have been showed about implementation over any real testbed.

## 7.3 Conclusions

To summarize, Table 4 collects all the scores of the Network Architectures technologies analyzed in this section.

| **SCORES** | Scalability | Heterogeneity | Timeliness | Reliability / Robustness | Resiliency | Energy efficiency | Interoperability | Data aggregation / compression mechanisms | Traffic differentiation | Security | Hardware support | Technical maturity | Availability of experience internal to the consortium |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Flat | 4 | N/A | 4 | 4 | 2 | 2 | 1 | 3 | N/A | 4 | N/A | 3 | 1 |
| Cluster based | 1 | | 1 | 1 | 1 | 1 | 3 | 1 | | 1 | | 1 | 1 |
| Hexagonal | 3 | | 3 | 2 | 2 | 3 | 4 | 3 | | 1 | | 3 | 1 |
| Multi-tier (or backbone-based) | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | | 1 | | 1 | 1 |
| Real Time Architecture | 1 | | 1 | 4 | 1 | 4 | 1 | 4 | | 4 | | 4 | 0 |

Table 4: Network Architectures Technologies evaluation

# 8. WSN MAC and DATALINK Layer

## 8.1 Requirements/Evaluation Criteria

Moving from the methodology presented in Section 4, the applicable criteria for network architectures are listed in what follows.

- Scalability (see Section 4.1.1.1).
- Heterogeneity (see Section 4.1.1.2).
- Timeliness (see Section 4.1.1.3).
- Reliability / Robustness (see Section 4.1.1.4).
- Resiliency (see Section 4.1.1.5).
- Energy efficiency (see Section 4.1.1.6).
- Interoperability (see Section 4.1.1.7).
- Traffic differentiation (see Section 4.1.1.9).
- Security (see Section 4.1.1.10).
- Technical Maturity (see Section 4.1.1.12).
- Availability of internal experience (see Section 4.1.1.13).

## 8.2 Existing Solutions

### 8.2.1 IEEE 802.15.4/a

The IEEE802.15.4 and its amendment 802.15.4a [RD-82] are communication standards for a Low Rate Wireless Personal Area Network (LR-WPAN), which is a simple, low-cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements. The main objectives of a LR-WPAN are ease of installation, reliable data transfer, short-range operation, extremely low cost, and a reasonable battery life, while maintaining a simple and flexible protocol.

A system conforming to this standard consists of several components. The most basic is the device. A device may be a Reduced Function Device (RFD) or a Full Function Device (FFD). Two or more devices within a Personal Operating Space (POS) communicating on the same physical channel constitute a WPAN. However, this WPAN shall include at least one FFD, operating as the PAN coordinator.

The amendment IEEE802.15.4a provides an international standard for an ultra-low complexity, ultra-low cost, ultra-low power consumption alternate Physical Layer (PHY) for IEEE802.15.4. To satisfy an evolutionary set of industrial and consumer requirements for WPAN communications, the precision ranging capability will be accurate to one meter or better, and the communication range, robustness, and mobility improved over IEEE802.15.4. The requirements to support coexisting networks of sensors, controllers, and logistic and peripheral devices in multiple compliant co-located systems are addressed.

Finally, ISEP is studying this technology for a long time and has gained expertise in the field of simulation and experimentation of solutions based on IEEE802.15.4.

#### 8.2.1.1 Scalability

Score: 2

In the Non Beacon Enabled mode scalability is easy to achieve, because all nodes are completely independent from the PAN Coordinator. However to address timing and reliability requirements of real world applications, peer-to-peer paradigm becomes controversial.

So a scalability/latency paradox in peer-to-peer networks arises. This can be partially solved by resorting to a two-tier cluster based network architecture [RD-83], with an overlay network at the tier 2 acting as a backbone for the underlying WSN .

#### 8.2.1.2 Heterogeneity

Score: 3

The standard addresses the two lowest layers of the ISO-OSI reference protocol stack, i.e. the MAC sub-layer and the PHY layer. At the PHY layer, i.e. the radio, there are a specific set of rules to be met, so heterogeneity in the radio platforms is out of the scope, even if there is already a wide availability of different radio devices which are compatible with the standard.

In terms of protocols, there are several works in literature which address the performance of e.g. routing protocols over the IEEE802.15.4 MAC layer.

In terms of operating systems, even if there are a set of functions to be implemented to be compliant with the standard, many solutions for wireless sensor networks explicitly embed the needed functions.

Since, this is an IEEE standard, most of the low powered devices support it. Also, the upper tier devices e.g. Smart Phones, can be made compatible by attaching a 802.15.4 device through USB port (http://www.libelium.com/tienda/catalog/product_info.php?cPath=25&products_id=57). Nevertheless, many devices available today only implement the 2003 version of the standard, which does not take UWB (Ultra-wide band) into account.

#### 8.2.1.3 Timeliness

Score: 1

The IEEE 802.15.4 protocol provides real-time guarantees by using the Guaranteed-Time Slot (GTS) mechanism, which is quite attractive for time-sensitive WSNs. In fact, when operating in beacon-enabled mode, i.e. beacon frames are transmitted periodically by a central node called the PAN Coordinator for synchronizing the network, the IEEE 802.15.4 protocol allows the allocation/deallocation of GTSs in a superframe for nodes that require real-time guarantees. Hence, the GTS mechanism provides a minimum service guarantee for the corresponding nodes and enables the prediction of the worst-case performance for each node's application [RD-84], [RD-86].

#### 8.2.1.4 Reliability / Robustness

Score: 2

At the MAC layer the standard has the most common features for link reliability, like ARQ and Retransmissions of not acknowledged frames. On the contrary, end-to-end reliability and network fault tolerance are up to the routing layer which is not addressed in the standard. Anyway, the standard also provides low level measurements like Received Signal Strength and Link Quality (with different algorithms and metrics, like ETX, 4-bit and a novel LQE based on Fuzzy logic recently proposed), which could be efficiently used by the upper layer protocols.

One of the open issues is to resolve the hidden-node problem in IEEE 802.15.4, since its MAC protocol does not use any RTS/CTS mechanism. Nowadays, the proposed solutions groups nodes according to their hidden-node relationship, such that all nodes in each group are not hidden to each other, and assign to the PAN Coordinator the task of detecting the hidden node situation and performing grouping procedure if necessary [RD-89].

#### *8.2.1.5 Resiliency*

Score: 2

The standard is about MAC, hence resiliency is related to the retransmissions at the link layer. However the standard is specifically designed for low data rate networks and this affects also the Mean Time To Retransmit performance index.

Acknowledgements are optionally used and the number of retransmissions (macMaxFrameRetries) is configurable. If the originator does not receive an acknowledgment after some period (macAckWaitDuration symbols, which depends on the currently selected PHY), it assumes that the transmission was unsuccessful and retries the frame transmission. If an acknowledgment is still not received after several retries, the originator can choose either to terminate the transaction or to try again. When the acknowledgment is not required, the originator assumes the transmission was successful.

#### *8.2.1.6 Energy Efficiency*

Score: 1

This standard is specifically addressing energy efficiency issues, allowing duty cycles down to 0.01% and so long (multi-month) network lifetimes.

#### *8.2.1.7 Interoperability*

Score: 1

With the mechanism of Beacons, this standard can guarantee Quality of Service and prioritization while maintaining low energy consumptions, but it requires a cluster-based topology, which may not be applicable to some WSN scenarios [RD-87]. Without beacons, i.e. in Non-Beacon Enabled mode, the standard works also on flat networks. Consequently, this standard is flexible enough to be adopted in several different network architectures, and higher levels protocols.

Furthermore, with intrinsic ranging accuracy (and positioning, in turn), IEEE802.15.4a shows to be an optimal starting point for enabling geographical based routing protocols, which are intrinsically scalable.

FFD is used as PAN Coordinator in star topology and the leaf nodes are RFDs. However, in Peer-to-peer and MESH topologies, all devices are supposed to be FFDs, since every node should be capable of communicating with every other node in the radio coverage. Motorola has been involved in projects using this technology under the trademark **Conformables**.

#### *8.2.1.8 Traffic Differentiation*

Score: 1

This standard can guarantee Quality of Service and prioritization while maintaining low energy consumptions, but it requires a cluster-based topology, which may not be applicable to some WSN scenarios [RD-87].

#### *8.2.1.9 Security*

Score: 3

The cryptographic mechanism in this standard is based on symmetric-key cryptography and uses keys that are provided by higher layer processes. The establishment and maintenance of these keys are outside the scope of this standard.

Cryptographic frame protection may use a key shared between two peer devices (link key) or a key shared among a group of devices (group key), thus allowing some flexibility and application-specific tradeoffs between key storage and key maintenance costs versus the cryptographic protection provided. If a group key is used for peer-to-peer communication, protection is provided only against outsider devices and not against potential malicious devices in the key-sharing group.

#### *8.2.1.10 Technical Maturity*

Score: 1

The IEEE802.15.4 is a ratified mature standard. There exist already several physical platforms which are compliant with this standard, as well as a plethora of network simulators which embed models adherent with the standard.

Moreover, several stacks are available, like for TinyOS [RD-90] and Texas Instruments [RD-91], some of them also open-source, like [RD-92], [RD-93]. There is also additional ongoing implementation work at the 15.4 TinyOS working group.

### 8.2.2 WirelessHART

WirelessHART [RD-94] is a wireless mesh network communications protocol for process automation applications. It adds wireless capabilities to the HART Protocol while maintaining compatibility with existing HART devices, commands, and tools.

Each WirelessHART network includes three main elements:

- Wireless field devices connected to process or plant equipment. This device could be a device with WirelessHART built in or an existing installed HART-enabled device with a WirelessHART adapter attached to it.

- Gateways enable communication between these devices and host applications connected to a high-speed backbone or other existing plant communications network.
- A Network Manager is responsible for configuring the network, scheduling communications between devices, managing message routes, and monitoring network health. The Network Manager can be integrated into the gateway, host application, or process automation controller.

#### 8.2.2.1 Scalability

Score: 3

As specifically detailed for its TMSP protocol (Section 9.2.2), it is not clear if the good performance in terms of scalability may remain available in environments other than industrial automation.

#### 8.2.2.2 Heterogeneity

Score: 2

WirelessHART network uses 802.15.4, so it could be easy to implement. However, as per our observation the devices available are mostly targeted towards industrial monitoring. Although to use this protocol, probably HART Communication Foundation's membership is required.

#### 8.2.2.3 Timeliness

Score: 3

As specifically detailed for its TMSP protocol (Section 9.2.2), it is not clear if the good performance in terms of scalability may remain available in environments other than industrial automation.

#### 8.2.2.4 Reliability / Robustness

Score: 2

WirelessHART includes several features to provide reliable communications in all industrial environments. Moreover, it is specialized for industrial plants but it seems to work well even in large outdoor environments. It’s based on 802.15.4 at MAC layer but it actually implements a communication protocol, hence it takes care of end-to- end connections as well.

#### 8.2.2.5 Resiliency

Score: 2

The protocol is able to perform recovery at communication level by means of redundant routing paths for maximum reliability and managed latency.

#### 8.2.2.6 Energy Efficiency

Score: 3

As specifically detailed for its TMSP protocol (Section 9.2.2), it is not clear if the good performance in terms of scalability may remain available in environments other than industrial automation.

#### 8.2.2.7 Interoperability

Score: 2

WirelessHART is designed to work in MESH device network which are connected to server systems using Gateways.

#### 8.2.2.8 Traffic Differentiation

Score: 4

It is not clear how traffic differentiation can be performed in WirelessHART.

#### 8.2.2.9 Security

Score: 1

WirelessHART employs robust security measures to protect the network and secure the data at all times. These measures include the latest security techniques to provide the highest levels of protection available. Wireless HART is built on top of 802.15.4 DSSS (Direct Sequence Spread Spectrum), but it adds a more deliberate frequency-hopping algorithm. Security includes encryption and authentication.

Protects Valuable Information:

- Robust, multi-tiered, always-on security;
- Industry standard 128-bit AES encryption;
- Unique encryption key for each message;
- Data integrity and device authentication;
- Rotate encryption keys used to join the network.

Protects Wireless Network:

- Channel hopping
- Adjustable transmit power levels
- Multiple levels of security keys for access;
- Indication of failed access attempts;
- Reports message integrity failures;
- Reports authentication failures;
- Safe from Wi-Fi type Internet attacks.

#### *8.2.2.10 Technical Maturity*

Score: 1

WirelessHART is a standard focusing industrial applications and features strongly mature.

### 8.2.3 BlueTooth Low Power

TCP/IP has recently taken promising steps toward being a viable communication architecture for networked sensor nodes. Furthermore, the use of Bluetooth can enable a wide range of new applications. The number of Bluetooth-enabled consumer devices on the market is increasing, which gives Bluetooth an advantage compared to other radio technologies from an interoperability point of view. Bluetooth-enabled networked sensor node can achieve an operating lifetime in the range of years using a total volume of less than 10 cm$^3$ [RD-43], [RD-44], [RD-95], [RD-96].

Finally, SESM has some experience in this technology.

#### *8.2.3.1 Scalability*

Score: 3

Scalability of Bluetooth based networks over large scale sensor number of nodes still has strong limitation [RD-100].

#### *8.2.3.2 Heterogeneity*

Score: 3

Although a number of devices are available today that support BlueTooth but most of them are either embedded in mobiles or are supposed to be used with mobiles. Secondly, we are only aware of very few BlueTooth sensor nodes. Also, the range of a BlueTooth device is limited to 10 meters and could be extended to 100 meters by providing higher power. BlueTooth also restricts the number of slave nodes, a master node can have to up to seven.

#### *8.2.3.3 Timeliness*

Score: 2

Bluetooth radios normally achieve higher bandwidth than classical WSN radios in a single-hop network, i.e. a STAR-based network architecture, hence timeliness in large scale multihop networks is still hard to achieve.

#### *8.2.3.4 Reliability / Robustness*

Score: 2

Bluetooth is initially designed with reliability in mind and there several concepts used helping to achieve this.

- Frequency-hopping Code Division Multiple Access (FH-CDMA).

- Error Correction. Bluetooth includes both Forward Error Correction (FEC) and packet retransmission. This is a shortened Hamming code and able to automatically correct all one bit errors and detect all two bit errors An ARQ packet retransmission scheme is applied. Retransmission is done if packets are lost or NAKed. This allows for safe transmission of data.
- Received Signal Strength Indicator (RSSI)-based power control ensures that excessive power not is used to fulfil communication between a pair of nodes.

Concerns remain when dealing with thousands of nodes. [RD-99] reveals packet payload corruptions even with a low number of nodes in a single piconet (this is the same, if no worse, for low energy version).

#### 8.2.3.5 Resiliency

Score: 2

The error correction and control mechanisms used by BT at MAC/routing level revealed some pitfalls due to the simple CRC implemented [RD-99]. MTTR is good, given that the fault (corruption) is recognized.

#### 8.2.3.6 Energy Efficiency

Score: 1

In [RD-100], authors showed that the high power consumption of classical Bluetooth-based sensor nodes can be reduced by order of magnitudes while still enabling interoperability with existing infrastructure. Authors claim that a system lifetime in the range of months to years is made feasible by an efficient and extensive use of the available low-power modes.

#### 8.2.3.7 Interoperability

Score: 3

Usually BlueTooth network is deployed in STAR or TREE topology, because of the fact that these networks have a MASTER and several SLAVE nodes in a single piconet.

#### 8.2.3.8 Traffic Differentiation

Score: 1

A number of scheduling protocols that allow traffic differentiation in a Bluetooth network exist. These include Class-Based Earliest Deadline First (CB-EDF) and Traffic Differentiation Queueing (TDQ) [RD-97], [RD-98].

#### 8.2.3.9 Security

Score: 1

Bluetooth devices can advertise all of the services they provide. This makes using services easier because more of the security, network address and permission configuration can be automated than with many other network types. For security reasons Bluetooth uses a process called pairing. Two devices need to be paired once to communicate with each other. Pairing mechanisms have changed significantly with the introduction of Secure Simple Pairing in Bluetooth 2.1.Secure Simple Pairing has two security goals: protection against passive eavesdropping and protection against man-in-the-middle (MITM) attacks (active eavesdropping).

#### 8.2.3.10 Technical Maturity

Score: 2

Bluetooth is a standard communication technology widely adopted for networked personal systems, but not yet in large scale embedded devices.

http://www.btnode.ethz.ch/ hosts the BTNUT platform (code and tutorials) for Linux.

### 8.2.4 WiseMAC

WiseMAC is an ultra low power MAC protocol for the downlink of infrastructure wireless sensor networks. WiseMAC is a novel energy efficient medium access control protocol based on synchronized preamble sampling [RD-101].

#### 8.2.4.1 Scalability

Score: 3

The hidden terminal problem accompanies the WiseMAC model as in Spatial TDMA and CSMA with Preamble Sampling algorithm, That is because WiseMAC is also based on non-persistent CSMA. This problem will result in collisions when one node starts to transmit the preamble to a node that is already receiving another node's transmission where the preamble sender is not within range [RD-102]. This problem is further exacerbated when the number of nodes and density is high.

#### 8.2.4.2 Heterogeneity

Score: 2

WiseMAC is a MAC protocol for WSNs and as such does not make any specifications that would impact heterogeneity.

#### 8.2.4.3 Timeliness

Score: 3

Decentralized sleep-listen scheduling results in different sleep and wake-up times for each neighbour of a node. This is an important problem especially for broadcast-type, since they will be buffered for neighbours in sleep mode and delivered many times as each neighbour wakes up. However, this redundant transmission will results in higher latency and power consumption [RD-102].

#### 8.2.4.4 Reliability / Robustness

Score: 3

Preamble Protocols are well suited to lightly loaded energy limited sensor networks as they can save more energy compared to common sleep/wakeup protocols.

However, they also present some drawbacks that come from the overhead of preamble transmission/reception. Besides minimizing energy consumption, a good MAC protocol should also provide reliable communication between neighbour nodes. However, these are antagonistic requirements in general, because reliability may increase energy consumption.

Reliability should be a major concern in environmental monitoring.

#### *8.2.4.5 Resiliency*

Score: 3

There are no studies that explicitly evaluate MTTR for WiseMac networks. Anyway error control mechanisms are implemented that fit the need for resiliency.

As for reliability, it is not the main strength of this (downlink) protocol.

Resiliency should be a major concern in environmental monitoring.

#### *8.2.4.6 Energy Efficiency*

Score: 3

Decentralized sleep-listen scheduling results in different sleep and wake-up times for each neighbour of a node. This is an important problem especially for broadcast-type, since they will be buffered for neighbours in sleep mode and delivered many times as each neighbour wakes up. However, this redundant transmission will results in higher latency and power consumption [RD-102].

#### *8.2.4.7 Interoperability*

Score: 3

WiseMAC is a MAC protocol and does not impose any constraints on Physical layer protocols and upper layer protocols other than the physical layer must be wireless. However, for energy efficiency and timeliness, WiseMac imposes some limitations to routing when a “diffusion”-like solution is selected.

#### *8.2.4.8 Traffic Differentiation*

Score: 3

WiseMAC does not support traffic differentiation.

#### *8.2.4.9 Security*

Score: 4

In the documents that were analysed, security issues are not addressed, whether explicitly or implicitly.

However, in [RD-103], a study concerning jamming-style DoS attacks over three representative MAC protocols, S-MAC, LMAC and B-MAC is presented. In it, the authors develop jamming attacks that (1) work on encrypted packets, (2) are as effective as constant /deceptive/reactive jamming, and (3) are at the same time more energy-efficient than random jamming or reactive jamming. A careful analysis of other protocols belonging to the respective categories of S-MAC, LMAC, and B-MAC - for instance, slot-based protocols (like T-MAC and DMAC), frame-based protocols (like TRAMA), and random access-based protocols (like WiseMAC) - reveals that those protocols are, to some extent, also susceptible to jamming attacks. Authors also propose some countermeasures for the analyzed protocols, but they conclude that an effective countermeasure is still lacking. For WSNs that require high security against link-layer jamming the recommendations are: (1) encrypting link-layer packets to ensure a high entry barrier for jammers, (2) the use of spread spectrum hardware, and (3) the use of a TDMA protocol.

#### 8.2.4.10 Technical Maturity

Score: 3

No significant results have been found about large scale real world deployments.

### 8.2.5 HyMAC

HyMAC, a new hybrid MAC layer protocol for wireless sensor networks that is the first effort to combine the strengths of both TDMA and FDMA schemes in these constrained networks [RD-104].

#### 8.2.5.1 Scalability

Score: 1

The base station is responsible to assign an appropriate frequency as well as specific time slot(s) to each node by running an appropriate algorithm: hence the solution is centralized. However, even in an extreme case where 900 nodes are presented in the network each of which having 90 neighbours, simulation results showed that the total number of required frequencies will not be more than 14. In addition, it is important to note that HyMAC is practically adjustable according to the exact number of frequencies that user specifies employing suitable number of time slots [RD-104].

Moreover, HyMAC supports denser networks with higher number of nodes - and thus a higher throughput - than RT-Link is potentially able to; thanks to its use of multiple available frequencies [RD-104].

#### 8.2.5.2 Heterogeneity

Score: 1

It can work with a variety of hardware platforms such as Telos, MICAZ and Firefly. The functionality of HyMAC does not depend on the type of its underlying synchronization service, its creators believe that it best performs in presence of a hardware-based out-of-band time synchronization such as FireFly.

#### 8.2.5.3 Timeliness

Score: 1

HyMAC is the first sensor-net MAC protocol that schedules the network nodes in a way that eliminates collisions and provides small bounded end-to-end delay and high throughput while taking advantage of multiple frequencies available in current sensor node hardware platforms such as MICAZ, TELOS and FireFly [RD-104].

#### 8.2.5.4 Reliability / Robustness

Score: 2

The HyMAC ability to reduce collisions makes reasonable to suppose that delivery packet ratio is increased if compared to TDMA and FDMA separately. However, there is a lack of experiments showing this.

#### 8.2.5.5 Resiliency

Score: 2

The fact that more frequencies are available makes higher the probability of successful retransmissions, i.e., a lower number of retransmission attempts is needed to complete packet delivery. However, there are no studies confirming such an intuition.

#### 8.2.5.6 Energy Efficiency

Score: 1

The small bounded end-to-end delay and high throughput achieved by HyMAC as well as its energy efficiency due to minimization of idle listening, elimination of overhearing and its collision-free operation make it an appropriate candidate for the newly emerging sensor network applications such as real-time voice streaming.

#### 8.2.5.7 Interoperability

Score: 2

HyMAC does not make any explicit statements about interoperability but as a MAC protocol it should be inter-operable with a wide variety of lower layer protocols.

#### 8.2.5.8 Traffic Differentiation

Score: 2

While traffic differentiation is not provided out of the box, it should be easy to implement in the scheduler.

#### 8.2.5.9 Security

Score: 4

Security aspects have not been found at all for this protocol.

#### 8.2.5.10 Technical Maturity

Score: 3

No significant results have been found about large scale real world deployments.

### 8.2.6 RT-link

For real-time wireless communication in industrial control, surveillance and inventory tracking, RT-Link, a time-synchronized link protocol, has been proposed in [RD-105]. RT-Link provides predictable lifetime for battery-operated embedded nodes, bounded end-to-end delay across multiple hops, and collision-free operations.

#### 8.2.6.1 Scalability

Score: 3

RT-Link assigns the time slots centrally at the base station and similar to TRAMA it supports contention slots employing Slotted-ALOHA rather than CSMA. However, in spite of using CC2420 radio provided in FireFly, RT-Link does not take any advantage of the multiple frequencies provided which could noticeably increase the network throughput and reduce the delay [RD-104].

Finally, there are some experiences with this protocol at ISEP.

#### 8.2.6.2 Heterogeneity

Score: 2

RT-link is a MAC layer protocol and as such does not put any restrictions on hardware/software or the application layer.

#### 8.2.6.3 Timeliness

Score: 3

RT-Link assigns the time slots centrally at the base station and similar to TRAMA it supports contention slots employing Slotted-ALOHA rather than CSMA. However, in spite of using CC2420 [RD-107] radio provided in FireFly, RT-Link does not take any advantage of the multiple frequencies provided which could noticeably increase the network throughput and reduce the delay [RD-104].

#### 8.2.6.4 Reliability / Robustness

Score: 3

The protocol is based on TDMA, hence it’s collision free in principle. It has been shown in [RD-105] that, with a jammer solution, the RT-link has a very high packet success rate at different distances. However, hop length increases, reliability decreases which causes time synchronization degradation and increased energy consumption in the form of extended synchronization wait times.

Concerns remain when dealing with thousands of nodes and distance. Do we need to deploy the nodes at more than 30 meters one from the other?

#### 8.2.6.5 Resiliency

Score: 3

The resiliency in terms of MTTR is something strictly related to end-to-end latency at this level. In [RD-105] has been shown that RT-Link exhibits flat (constant) latency in a multihop scenario.

#### 8.2.6.6 Energy Efficiency

Score: 3

RT-Link achieves a practical lifetime of over 2 years. However, the small bounded end-to-end delay and high throughput achieved by HyMAC as well as its energy efficiency due to minimization of idle listening, elimination of overhearing and its collision-free operation make it a more appropriate candidate for the newly emerging sensor network applications such as real-time voice streaming [RD-104].

#### 8.2.6.7 Interoperability

Score: 3

RT-link is a MAC layer protocol and while the referenced work only uses 802.15.4 transceivers in the demonstration, it should be easy to implement and work with alternative network layer implementations and architectures.

#### 8.2.6.8 Traffic Differentiation

Score: 4

It is not addressed in the work.

#### 8.2.6.9 Security

Score: 4

In the documents that were analysed, security issues are not addressed, whether explicitly or implicitly.

However, in [RD-106], a study concerning jamming-style DoS attacks over three representative MAC protocols, S-MAC, LMAC and B-MAC is presented. For WSNs that require high security against link-layer jamming the authors recommendations are: (1) encrypting link-layer packets to ensure a high entry barrier for jammers, (2) the use of spread spectrum hardware, and (3) the use of a TDMA protocol. RT-Link is a TDMA-based link layer protocol.

RT-Link utilizes an out-of-band synchronization mechanism using an AM broadcast pulse. As the out-of-band sync pulse is a high-power (30W) signal with no encoded data, it is not easily jammed by a malicious sensor node. In general, RT-Link outperforms B-MAC which in turn out-performs S-MAC [RD-106].

CC2420 radio provided in FireFly [RD-105] includes a digital direct sequence spread spectrum baseband modem [RD-107] which is resistant to RF interference and provides inherent data security.

#### 8.2.6.10 Technical Maturity

Score: 3

No significant results have been found about large scale real world deployments.

### 8.2.7 Z-MAC

Z-MAC [RD-108] is a medium-access control (MAC) protocol designed for wireless sensor networks which combines the strengths of TDMA and CSMA while offsetting their weaknesses. Z-MAC uses an efficient TDMA channel reuse schedule from a distributed implementation of RAND, as a hint to enhance performance of CSMA, especially during high contention.

#### 8.2.7.1 Scalability

Score: 1

This protocol can adapt itself to different scales like other similar MACs (e.g. S-MAC). It requires the knowledge of topology and a loosely synchronized clock as hints to improve MAC performance under high contention; otherwise it behaves like a classical CSMA protocol [RD-109].

#### 8.2.7.2 Heterogeneity

Score: 2

Z-MAC is a MAC layer protocol and as such does not put any restrictions on hardware/software or the application layer.

#### 8.2.7.3 Timeliness

Score: 2

This is a hybrid protocol, which dynamically switch between CSMA and TDMA. So, although it is not specifically designed for RT QoS services, the idea of switching behavior is inspiring [RD-109].

#### 8.2.7.4 Reliability / Robustness

Score: 2

Z-Mac implements transmission control mechanisms to be robust to the packet loss. As stated in [RD-108] it has been realized to tolerate time synchronization errors, as well as Radio interferences from unreachable nodes.

#### 8.2.7.5 Resiliency

Score: 4

There are no studies that deal with Z-MAC resiliency explicitly.

#### 8.2.7.6 Energy Efficiency

Score: 1

Z-MAC is a hybrid protocol able to adapt its behaviour between CSMA and TDMA like protocols. Like most MAC protocols for WSN, it is specifically designed to conserve energy while trying to allow good performance in other fields (like QoS).

#### 8.2.7.7 Interoperability

Score: 2

While implemented on MicaZ motes and TinyOS, it should be possible to inter-operate with other layers and architectures.

#### 8.2.7.8 Traffic Differentiation

Score: 2

Traffic differentiation is not addressed. The referenced work addresses issues of fairness and the protocol may be modified to allow traffic differentiation.

#### 8.2.7.9 Security

Score: 4

In the documents that were analysed, security issues are not addressed, whether explicitly or implicitly.

#### 8.2.7.10 Technical Maturity

Score: 1

Z-MAC is implemented in TinyOS and NS-2 http://www4.ncsu.edu/~rhee/export/zmac/software/zmac/zmac.htm

### 8.2.8 S-MAC

In WSNs, individual nodes remaining largely inactive for long periods of time, but then becoming suddenly active when something is detected. These characteristics of sensor networks and applications motivate a S-MAC [RD-110] that is different from traditional wireless MACs in almost every way: energy conservation and self-configuration are primary goals, while per-node fairness and latency are less important.

#### 8.2.8.1 Scalability

Score: 1

The solution proposed in S-MAC is fully distributed.

#### 8.2.8.2 Heterogeneity

Score: 2

S-MAC is a MAC layer protocol and as such does not put any restrictions on hardware/software or the application layer.

#### 8.2.8.3 Timeliness

Score: 4

S-MAC and its variants like T-MAC and B-MAC, as CSMA/CA based protocols, only provide best effort service, but not Real Time QoS guarantees [RD-109]. To be a Real Time MAC, either deterministic or statistical delay bound is required.

#### 8.2.8.4 Reliability / Robustness

Score: 2

S-MAC has been extended adding a “reliable unicast” extension (see the link below). In this version, RTS-CTS-DATA-ACK packet exchange handles collisions and hidden terminal problems, and enables fast error recovery through retransmissions.

#### 8.2.8.5 Resiliency

Score: 2

Error recovery is enabled by retransmission. It is fastened by message fragmentation.

#### 8.2.8.6 Energy Efficiency

Score: 1

S-MAC, as a CSMA/CA based protocol, uses periodic listening and sleeping to save energy consumptions. There are also some variants, like T-MAC and B-MAC, which try to improve the energy efficiency and throughput.

#### 8.2.8.7 Interoperability

Score: 2

While not explicitly addressed in the paper, as a MAC layer protocol, there are no restrictions to inter-operability.

#### 8.2.8.8 Traffic Differentiation

Score: 4

Traffic differentiation is not explicitly addressed but may be hard to implement. The S-MAC protocol assumes that most communication will be between sensor nodes as peers, the nodes will be deployed casually rather than carefully positioned and that the entire network will be dedicated to a single or a few collaborative applications so that system-wide performance is more important than individual node fairness. There is no support in the protocol for different traffic classes and while it may be possible to implement traffic classes on a per node basis using multiple queues, the S-MAC protocol does not provide a way to allow traffic differentiation in the network.

#### 8.2.8.9 Security

Score: 4

In the documents that were analysed, security issues are not addressed, whether explicitly or implicitly.

However, in [RD-103], a study concerning jamming-style DoS attacks over three representative MAC protocols, S-MAC, LMAC and B-MAC is presented. In it, the authors develop jamming attacks that (1) work on encrypted packets, (2) are as effective as constant /deceptive/reactive jamming, and (3) are at the same time more energy-efficient than random jamming or reactive jamming. A careful analysis of other protocols belonging to the respective categories of S-MAC, LMAC, and B-MAC - for instance, slot-based protocols (like T-MAC and DMAC), frame-based protocols (like TRAMA), and random access-based protocols (like WiseMAC) - reveals that those protocols are, to some extent, also susceptible to jamming attacks. Authors also propose some countermeasures for the analyzed protocols, but they conclude that an effective countermeasure is still lacking. For WSNs that require high security against link-layer jamming the recommendations are: (1) encrypting link-layer packets to ensure a high entry barrier for jammers, (2) the use of spread spectrum hardware, and (3) the use of a TDMA protocol.

#### 8.2.8.10 Technical Maturity

Score: 1

S-MAC is implemented in TinyOS and using a dedicated communication protocol stack. Available at http://www.isi.edu/ilense/software/smac/.

There also exists an ns-2 implementation here: http://www.isi.edu/ilense/software/smac/.

### 8.2.9 TRAMA

The traffic-adaptive medium access protocol (TRAMA) [RD-111] is introduced for energy-efficient collision-free channel access in wireless sensor networks. TRAMA reduces energy consumption by ensuring that unicast and broadcast transmissions incur no collisions, and by allowing nodes to assume a low-power, idle state whenever they are not transmitting or receiving.

#### 8.2.9.1 Scalability

Score: 1

TRAMA, as a TDMA-based protocol, tries to allocate a slot for each node based on its real need to transmit. In doing so, it considers the two-hop neighbourhood of each node to avoid the hidden terminal problem. Moreover, since the intended receivers are indicated by a bitmap, less communication is performed for the multicast and broadcast types of communication patterns, compared to other protocols [RD-102].

#### 8.2.9.2 Heterogeneity

Score: 2

TRAMA is a MAC layer protocol and as such does not put any restrictions on hardware/software or the application layer.

#### 8.2.9.3 Timeliness

Score: 3

Analytical models for the delay performances of TRAMA protocol are presented and supported by simulations in [RD-111]. Delays are found to be higher, as compared to those of contention-based protocols, due to a higher percentage of sleep-times [RD-102].

#### 8.2.9.4 Reliability / Robustness

Score: 2

In [RD-111] the protocol has been tested in a WSN scenario where one of the nodes was designated as the sink and the sink starts sending a broadcast query. All nodes receiving a non-duplicate query add the sender of the query as the next hop for data forwarding, establishing a reverse-shortest path tree with the sink node as the root. Results show that the average packet delivery ratio is nearly constant as the packet generation load increases.

It must be also considered that whenever a node assumes that a neighbour is transmitting a data to it, the schedules are updated only after receiving the data from the neighbour using the schedule summary. Hence, packet losses due to transmission errors can cause the schedules to be unsynchronized and forces a node to listen whenever the unsynchronized neighbour is elected for transmission. This continues until the node receives a data packet from the unsynchronized neighbour, and also prevents invalid state assignment. Hence, TRAMA is correct even when the schedules are not synchronized.

It seems that TRAMA behaves well without serious impacts on performances.

#### 8.2.9.5 Resiliency

Score: 2

The resiliency in terms of MTTR is something strictly related to end-to-end latency at this level. In [RD-111] it has been shown that TRAMA has a constant delay as the traffic increases.

#### 8.2.9.6 Energy Efficiency

Score: 1

Higher percentage of sleep time and less collision probability are achieved, as compared to CSMA-based protocols. Moreover, since the intended receivers are indicated by a bitmap, less communication is performed for the multicast and broadcast types of communication patterns, compared to other protocols [RD-102].

#### 8.2.9.7 Interoperability

Score: 2

While not explicitly addressed in the paper, as a MAC layer protocol, there are now restrictions to inter-operability.

#### 8.2.9.8 Traffic Differentiation

Score: 2

Traffic differentiation should be easy to implement as prioritization of packets is supported in the protocol.

#### 8.2.9.9 Security

Score: 4

In the documents that were analysed, security issues are not addressed, whether explicitly or implicitly.

However, in [RD-103], a study concerning jamming-style DoS attacks over three representative MAC protocols, S-MAC, LMAC and B-MAC is presented. In it, the authors develop jamming attacks that (1) work on encrypted packets, (2) are as effective as constant /deceptive/reactive jamming, and (3) are at the same time more energy-efficient than random jamming or reactive jamming. A careful analysis of other protocols belonging to the respective categories of S-MAC, LMAC, and B-MAC - for instance, slot-based protocols (like T-MAC and DMAC), frame-based protocols (like TRAMA), and random access-based protocols (like WiseMAC) - reveals that those protocols are, to some extent, also susceptible to jamming attacks. Authors also propose some countermeasures for the analyzed protocols, but they conclude that an effective countermeasure is still lacking. For WSNs that require high security against link-layer jamming the recommendations are: (1) encrypting link-layer packets to ensure a high entry barrier for jammers, (2) the use of spread spectrum hardware, and (3) the use of a TDMA protocol.

#### 8.2.9.10 Technical Maturity

Score: 3

No significant results have been found about large scale real world deployments

## 8.3 Conclusions

To summarize, Table 5 collects all the scores of the MAC Protocols technologies analyzed in this section.

| **SCORES** | Scalability | Heterogeneity | Timeliness | Reliability / Robustness | Resiliency | Energy efficiency | Interoperability | Data aggregation / compression mechanisms | Traffic differentiation | Security | Hardware support | Technical maturity | Availability of experience internal to the consortium |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IEEE 802.15.4 / IEEE 802.15.4a | 2 | 3 | 1 | 2 | 2 | 1 | 1 | N/A | 1 | 3 | N/A | 1 | 1 |
| Wireless HART | 3 | 2 | 3 | 2 | 2 | 3 | 2 |  | 4 | 1 |  | 1 | 0 |
| BlueTooth low-power | 3 | 3 | 2 | 2 | 2 | 1 | 3 |  | 1 | 1 |  | 2 | 1 |
| WiseMAC | 3 | 2 | 3 | 3 | 3 | 3 | 3 |  | 3 | 4 |  | 3 | 0 |
| HyMAC | 1 | 1 | 1 | 2 | 2 | 1 | 2 |  | 2 | 4 |  | 3 | 0 |
| RT-Link | 3 | 2 | 3 | 3 | 3 | 3 | 3 |  | 4 | 4 |  | 3 | 1 |
| Z-MAC | 1 | 2 | 2 | 2 | 4 | 1 | 2 |  | 2 | 4 |  | 1 | 0 |
| S-MAC | 1 | 2 | 4 | 2 | 2 | 1 | 2 |  | 4 | 4 |  | 1 | 0 |

| **SCORES** | Scalability | Heterogeneity | Timeliness | Reliability / Robustness | Resiliency | Energy efficiency | Interoperability | Data aggregation / compression mechanisms | Traffic differentiation | Security | Hardware support | Technical maturity | Availability of experience internal to the consortium |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| TRAMA | 1 | 2 | 3 | 2 | 2 | 1 | 2 |  | 2 | 4 |  | 3 | 0 |

Table 5: WSN MAC and DATALINK Layer Technologies evaluation

# 9. WSN Routing and Network Layer

## 9.1 Requirements/Evaluation Criteria

Moving from the methodology presented in Section 4, the applicable criteria for network architectures are listed in what follows.

- Scalability (see Section 4.1.1.1).
- Heterogeneity (see Section 4.1.1.2).
- Timeliness (see Section 4.1.1.3).
- Reliability / Robustness (see Section 4.1.1.4).
- Resiliency (see Section 4.1.1.5).
- Energy efficiency (see Section 4.1.1.6).
- Interoperability (see Section 4.1.1.7).
- Data aggregation / compression mechanisms (see Section 4.1.1.8).
- Traffic differentiation (see Section 4.1.1.9).
- Security (see Section 4.1.1.10).
- Technical Maturity (see Section 4.1.1.12).
- Availability of internal experience (see Section 4.1.1.13).

## 9.2 Existing Solutions

### 9.2.1 Collection-Tree Routing Protocol

In [RD-112] two principles for wireless routing protocols are presented and evaluated. The first is datapath validation: data traffic quickly discovers and fixes routing inconsistencies. The second is adaptive beaconing: extending the Trickle algorithm to routing control traffic reduces route repair latency and sends fewer beacons.

#### *9.2.1.1 Scalability*

Score: 1

This protocol is fully distributed.

#### *9.2.1.2 Heterogeneity*

Score: 2

CTP has been tested with a wide variety of MAC protocols and PHY platforms. However, at present, it has been implemented only onto the TinyOS operating system.

#### *9.2.1.3 Timeliness*

Score: 1

This protocol explicitly addresses mechanisms to prevent self-interference on a route, by rate-limiting the transmissions at each node. By this way, edge conditions due to MAC backoff or synchronized transmissions are prevented [RD-112].

#### 9.2.1.4 Reliability / Robustness

Score: 1

The mechanisms proposed in [RD-112] maintain an average delivery ratio above 90%: it meets the reliability goal, in all the cases and across several testbeds.

#### 9.2.1.5 Resiliency

Score: 1

Results in [RD-112] show that the proposed mechanisms are able to guarantee a very fast recovery from faults (e.g., nodes turned off to simulate crashes).

#### 9.2.1.6 Energy Efficiency

Score: 1

In [RD-112] authors claim that low energy profiles are achieved by CTP because, even if no multipath is allowed, it is able to dynamically selects efficient paths, avoids unnecessary control traffic and actively monitors the topology using the data plane.

#### 9.2.1.7 Interoperability

Score: 2

Interoperability is guaranteed by the fact that there is an implementation over TinyOS operating system and this protocol has been tested on a wide variety of MAC protocols and PHY platforms. However, CTR assumes that the data link layer provides four things:

1. Provides an efficient local broadcast address.

2. Provides synchronous acknowledgments for unicast packets.

3. Provides a protocol dispatch field to support multiple higher-level protocols.

4. Has single-hop source and destination fields.

CTR also assumes that it has link quality estimates of some number of nearby neighbours.

#### 9.2.1.8 Data Aggregation / Compression Mechanisms

Score: 2

Data aggregation is not addressed in [RD-112], but the proposed routing protocol is multi-hop and when an efficient path is selected it is maintained without unnecessary control traffic. So, classical data aggregation mechanisms are allowed at intermediate nodes.

#### 9.2.1.9 Traffic Differentiation

Score: 2

Even if no mechanisms for priority traffic differentiations are addressed in [RD-112], it seems quite simple to implement it using classical multiple queues mechanisms.

#### 9.2.1.10 Security

Score: 2

Security aspects have not been found at all for this protocol. However, in [RD-113], authors proposed modifications of Collection Tree Protocol suitable for wireless sensors with tamper resistant module. This platform provides better security, however ordinary protocols cannot utilize its features. Their goal was to offer secure routing protocol with similar behaviour and efficiency to the original protocol. Both protocols were simulated to prove that adding security to protocols does not necessarily lead to higher demands to data transfer and thus power consumption.

#### 9.2.1.11 Technical Maturity

Score: 1

This protocol has been tested for long time and it is implemented in the TinyOS v2 network stack.

### 9.2.2 Time Synchronized Mesh Protocol

The Time Synchronized Mesh Protocol (TSMP) [RD-114] enables reliable, low power, secure communication in a managed wireless mesh network. TSMP is a medium access and networking protocol designed for the recently ratified Wireless HART standard in industrial automation.

#### 9.2.2.1 Scalability

Score: 3

Even if TMSP requires a centralized control approach at the access point, it has been demonstrated in multi-hop networks exceeding 250 nodes per access point and thousands of nodes with multiple access points (at least a two tier network architecture). However, it not clear if this solution could remain feasible in environments other than industrial automation.

#### 9.2.2.2 Heterogeneity

Score: 3

Developed for the WirelessHART technology TMSP does not support heterogeneity.

#### 9.2.2.3 Timeliness

Score: 3

TMSP protocol foresees a high synchronization among nodes in the network and generally high throughput and low latencies. However, it not clear if this solution could remain feasible in environments other than industrial automation.

#### 9.2.2.4 Reliability / Robustness

Score: 1

To maximize reliability, TSMP uses frequency diversity, time diversity, and spatial diversity on a fully redundant routing scheme.

Reliability is further improved by temporal and spatial diversity routing. Nodes attempt to maintain connectivity with at least two neighbouring nodes, and forward packets on a FIFO-basis at the next available transmission opportunity. Should communication with one parent fail (for example, due to poor channel conditions), the next transmission attempt will be to another parent (and most likely on another channel), effectively using another path, realizing both spatial and temporal diversity.

#### 9.2.2.5 Resiliency

Score: 2

Although no explicit results are available on resiliency, it is reasonably high since a reliable mesh network is encompassed. Moreover, results refer only to the implementation of TMSP over IEEE802.15.4 MAC protocol.

#### 9.2.2.6 Energy Efficiency

Score: 3

TMSP has been demonstrated with radio duty cycle of 0.01%. Moreover, high synchronization among nodes allows to conserve energy by avoiding collisions. However, it not clear if this solution could remain feasible in environments other than industrial automation.

#### 9.2.2.7 Interoperability

Score: 3

TMSP is not very interoperable as it requires a mesh network architecture running WirelessHART. Moreover, results refer only to the implementation of TMSP over IEEE802.15.4 MAC protocol.

#### 9.2.2.8 Data Aggregation / Compression Mechanisms

Score: 4

Data aggregation is not explicitly addressed, and even if the network is multi-hop and aggregation may be performed at the access point, it is not clear if in-network computation is compatible with the high synchronization requirement.

#### 9.2.2.9 Traffic Differentiation

Score: 4

The references do not make explicit whether traffic differentiation is supported[13].

#### 9.2.2.10 Security

Score: 1

TSMP has two security layers managed by a centralized application. The transport layer encrypts the application payload and authenticates the payload and network and transport headers. The DLL authenticates the entire packet or ACK. Keys are 128 bits, and use the AES-128 block cipher in CCM [RD-115] mode.

#### 9.2.2.11 Technical Maturity

Score: 1

TMSP is the joint Medium Access and Networking protocol of the WirelessHART standard.

### 9.2.3 RPL (ROLL Routing Protocol)

Low Power and Lossy Networks (LLNs) are made largely of constrained nodes (with limited processing power, memory, and sometimes energy when they are battery operated). Such networks may potentially comprise a large number of nodes and traffic patterns are not simply unicast. The IETF ROLL WG has defined application-specific routing requirements for a LLN routing protocol.

In particular, the IPv6 Routing Protocol for LLNs (RPL) [RD-116] provides a mechanism whereby multipoint-to-point traffic from devices inside the LLN towards a central control point, as well as point-to-multipoint traffic from the central control point to the devices inside the LLN, is supported. Support for point-to-point traffic is also available.

Because WSN's requirements are heterogeneous and sometimes incompatible in nature, the approach for RPL is first taken to design a protocol capable of supporting a core set of functionalities corresponding to the intersection of the requirements. As the RPL design evolves optional features may be added to address some application specific requirements. This is a key protocol design decision providing a granular approach in order to restrict the core of the protocol to a minimal set of functionalities and to allow each implementation of the protocol to be optimized differently.

[13] Even if in [RD-114] it is claimed that TMSP has been demonstrated for different time-varying traffic patterns, it does not capture the notion of QoS or traffic differentiation. All authors claim in [RD-114] is that nodes can dynamically request more bandwidth from the manager. We presume that this can somehow be used along with traffic queues to support QoS, but the manager and the network isn't really aware of different traffic classes.

A network may run multiple instances of RPL concurrently. Each such instance may serve different and potentially antagonistic constraints or performance criteria. RPL is a generic protocol that is to be deployed by instantiating the generic operation described in [RD-116] with a specific objective function (OF) (which ties together metrics, constraints, and an optimization objective) to realize a desired objective in a given environment.

#### 9.2.3.1 Scalability

Score: 2

The protocol works on a tree-like topology (using the definition of DAG: Directed Acyclic Graph) and using a fully distributed algorithm to construct it. Moreover, to meet different requirements as goal functions, in the same network, multiple DAG instances are allowed and a single node may belong to multiple DAGs. However, at this moment, in [RD-116] only a single instance is addressed.

#### 9.2.3.2 Heterogeneity

Score: 1

As RPL is a routing protocol, it of course does not rely on any particular features of a specific link layer technology. RPL should be able to operate over a variety of different link layers, including but not limited to low power wireless or PLC (Power Line Communication) technologies.

#### 9.2.3.3 Timeliness

Score: 2

Traffic is bound to a specific DAG Instance by a marking in the flow label of the IPv6 header. Traffic originating in support of a particular application may be tagged to follow an appropriate DAG instance, for example to follow paths optimized for low latency or low energy. The role of the Objective Function is to advertise routing metrics and constraints in addition to the objectives used to compute the (constrained) shortest path. However, at this moment, in [RD-116] only a single instance is addressed.

#### 9.2.3.4 Reliability / Robustness

Score: 2

Retry mechanism is mainly based on timers at receivers side. The mechanisms sounds appealing and easy to implement (see section 6.8.1.1.1 Destination Advertisement Timer in [RD-116]).

#### 9.2.3.5 Resiliency

Score: 2

Retransmission mechanisms should be easy to implement; since the protocol assures low collisions they should also perform well in terms of TTR.

#### 9.2.3.6 Energy Efficiency

Score: 2

Traffic is bound to a specific DAG Instance by a marking in the flow label of the IPv6 header. Traffic originating in support of a particular application may be tagged to follow an appropriate DAG instance, for example to follow paths optimized for low latency or low energy. The role of the Objective Function is to advertise routing metrics and constraints in addition to the objectives used to compute the (constrained) shortest path. However, at this moment, in [RD-116] only a single instance is addressed.

#### 9.2.3.7 Interoperability

Score: 1

As RPL is a routing protocol, it of course does not rely on any particular features of a specific link layer technology. RPL should be able to operate over a variety of different link layers, including but not limited to low power wireless or PLC (Power Line Communication) technologies.

#### 9.2.3.8 Data Aggregation / Compression Mechanisms

Score: 2

Data aggregation mechanisms can be applied like in the classical tree-based topologies. However, this feature has not been addressed in [RD-116].

#### 9.2.3.9 Traffic Differentiation

Score: 2

Not addressed in the references but should be possible with separate queues for separate packet classes.

#### 9.2.3.10 Security

Score: 2

Security Considerations for RPL are to be developed in accordance with recommendations laid out in, for example [RD-117]. At the conceptual level, security within an information system in general and applied to ROLL in particular is concerned with the primary issues of Confidentiality, Integrity, and Availability (CIA).

#### 9.2.3.11 Technical Maturity

Score: 4

Actually this technology is still in the draft proposal stage; hence it is mature enough for academic purposes but not to be applied in industrial projects.

## 9.2.4 LEACH

Low-energy adaptive clustering hierarchy (LEACH) [RD-118] is one of the most popular hierarchical routing algorithms for sensor networks. The idea is to form clusters of the sensor nodes based on the received signal strength and use local cluster heads as routers to the sink. This will save energy since the transmissions will only be done by such cluster heads rather than all sensor nodes. In each cluster a TDMA approach is used for each node to communicate with the actual cluster head. Optimal number of cluster heads is estimated to be 5% of the total number of nodes.

### *9.2.4.1 Scalability*

Score: 4

The hypothesis that each node is able to communicate directly with the sink does not make LEACH very feasible for large scale wireless sensor networks deployed in wide zones [RD-120].

### *9.2.4.2 Heterogeneity*

Score: 3

LEACH uses single hop routing to the cluster head and sink. So it is not useful in WSNs deployed over large regions.

### *9.2.4.3 Timeliness*

Score: 3

LEACH uses single hop routing where each node can transmit directly to the cluster head and the sink [RD-119]. However, the idea of dynamic clustering brings extra overhead which diminishes the gain in throughput and latency. Furthermore, single-hop routing is difficult to achieve in large deployment.

### *9.2.4.4 Reliability / Robustness*

Score: 3

LEACH includes redundancy in the system by periodically selecting a cluster-head from the sensors in the network but suffer from overhead of re-clustering. However reliability and FT are not the properties for which it was designed.

### *9.2.4.5 Resiliency*

Score: 3

Re-clustering takes long time, then MTTR is reasonably too long. However a run time recovery mechanisms has been proposed in [RD-73] that can improve resiliency.

### *9.2.4.6 Energy Efficiency*

Score: 3

The purpose of LEACH is to randomly select sensor nodes cluster-heads, so the high energy dissipation in communicating directly with the base station is spread to all sensor nodes in the network. As a consequence, LEACH achieves over a factor of 7 reduction in energy dissipation compared to direct communication [RD-119]. However, LEACH assumes that every node can transmit with sufficient power to reach the sink in a single hop and that every node is computationally prepared to house the different MAC protocols required [RD-120].

#### 9.2.4.7 *Interoperability*

Score: 3

LEACH was tested in ns (Network Simulator) by the others [RD-118], in cluster based network architecture. In this protocol nodes communicate with cluster heads and cluster heads are assumed to be able to communicate directly to the BS. It Uses CSMA for advertising cluster heads and during cluster joining phase by the sensor nodes. In steady state TDMA is used.

#### 9.2.4.8 *Data Aggregation / Compression Mechanisms*

Score: 1

Sensor fusion and data aggregation are local to the cluster [RD-119].

#### 9.2.4.9 *Traffic Differentiation*

Score: 1

In a novel paper [RD-66], a QoS strategy for LEACH called LEACH-QoS has been implemented. So traffic differentiation in LEACH is possible and relevant for EMMON.

#### 9.2.4.10 *Security*

Score: 3

Essentially, LEACH doesn't include any security mechanism [RD-121]. The communications between BS (Base Station) and CHs (Cluster head selection) in LEACH are in single hop way, which prevent intruders from performing some kinds of relay attacks. However, a MCH (Malicious Cluster Heads) may broadcast its adv message with a large power, which leads to non-CHs' confusion. Non-CHs will select the MCH as the only CH (Cluster Head) in this WSN. Under this condition, the whole network is seized

#### 9.2.4.11 *Technical Maturity*

Score: 1

LEACH is a well investigated protocol and several implementations are in literature over common network simulators.

### 9.2.5 PEGASIS

Power-efficient GAthering in Sensor Information Systems (PEGASIS) [RD-122] is an improvement of the LEACH protocol. Rather than forming multiple clusters, PEGASIS forms chains from sensor nodes so that each node transmits and receives from a neighbour and only one node is selected from that chain to transmit to the base station (sink). Gathered data moves from node to node, aggregated and eventually sent to the base station. The chain construction is performed in a greedy way.

#### 9.2.5.1 Scalability

Score: 3

PEGASIS improves upon LEACH protocol, allowing nodes to form chains and multi-hop methods used for routing [RD-120]. However, in large scale sensor networks it is still difficult to have a node in the chain able to directly communicate with the sink.

#### 9.2.5.2 Heterogeneity

Score: 2

PEGASIS allows multi-hop routing so can be deployed in large scale networks. It requires information on link quality and transmission strength but it is not clear what the impact on heterogeneity is.

#### 9.2.5.3 Timeliness

Score: 3

PEGASIS introduces excessive delay for distant node on the chain and the single leader can become a bottleneck [RD-119].

#### 9.2.5.4 Reliability / Robustness

Score: 4

The problems of PEGASIS routing protocol:

- PEGASIS introduces excessive delay for distant node on the chain;
- The single leader can become a bottleneck.

#### 9.2.5.5 Resiliency

Score: 4

Due to the lack of re-election mechanisms, it is reasonable to suppose that recovery cannot be fast. However re-configurability is encompassed for new nodes entering into the network.

#### 9.2.5.6 Energy Efficiency

Score: 3

PEGASIS improves the energy efficiency of the LEACH protocol by reducing the number of long-range transmissions (i.e. those directed to the sink) and allowing in-network computation along the chain. However, in large scale sensor networks it is still difficult to have a node in the chain able to directly communicate with the sink.

#### 9.2.5.7 Interoperability

Score: 4

PEGASIS was tested in simulation environment, where base station (BS) was located at least 100m away from the nearest sensor node. It uses sensor fusion to produce a single packet that will be transmitted to the BS. The only cluster head becomes the single designated point of contact between BS and sensor network. The simulation was executed in 50m X 50m and 100m X 100m grids. Because of single point of contact, it may affect data throughput especially in emergency response or disaster management scenarios.

#### 9.2.5.8 Data Aggregation / Compression Mechanisms

Score: 1

In network computation can be performed along the chain and at the node which is responsible to communicate with the base station.

#### 9.2.5.9 Traffic Differentiation

Score: 1

PEGASIS is an improvement over LEACH and due to the reasons cited in Section 9.2.4.9, PEGASIS can implement traffic differentiation in a way that is useful for EMMON.

#### 9.2.5.10 Security

Score: 3

PEGASIS is an improvement of LEACH. Regarding security, PEGASIS is better than LEACH, but it is still a very poor protocol level security. PEGASIS with one chain, a compromised node can influence the entire network

#### 9.2.5.11 Technical Maturity

Score: 3

No significant results have been found about large scale real world deployments.

### 9.2.6 SAR

Sequential assignment routing (SAR) [RD-123] is the first protocol for sensor networks that includes the notion of QoS in its routing decisions. It is a table-driven multi-path approach striving to achieve energy efficiency and fault tolerance. The SAR protocol creates trees rooted at one-hop neighbours of the sink by taking QoS metric, energy resource on each path and priority level of each packet into consideration. By using created trees, multiple paths from sink to sensors are formed. One of these paths is selected according to the energy resources and QoS on the path. Failure recovery is done by enforcing routing table consistency between upstream and downstream nodes on each path.

#### 9.2.6.1 Scalability

Score: 3

The protocol assumes the knowledge of multi-path routing tables and suffers from certain overhead when tables and nodes states must be refreshed [RD-88].

#### 9.2.6.2 Heterogeneity

Score: 1

As a routing protocol, it does not have any requirements to the homogeneity of the layers and network architecture.

#### 9.2.6.3 Timeliness

Score: 1

QoS planned for each path is one of the factors based on which SAR makes routing decisions [RD-88].

#### 9.2.6.4 Reliability / Robustness

Score: 2

Failure recovery is done by enforcing routing table consistency between upstream and downstream nodes on each path. SAR maintains multiple paths from nodes to BS.

#### 9.2.6.5 Resiliency

Score: 2

Although, this ensures fault-tolerance and easy recovery, the protocol suffers from the overhead of maintaining the tables and states at each sensor node especially when the number of nodes is huge.

#### 9.2.6.6 Energy Efficiency

Score: 1

Efficient use of the energy resources for each path is one of the factors based on which SAR makes routing decisions [RD-88].

#### 9.2.6.7 Interoperability

Score: 1

SAR can interoperate with a number of other layers.

#### *9.2.6.8 Data Aggregation / Compression Mechanisms*

Score: 2

In network computation is not addressed, but the protocol assumes a tree-based topology, with the sink as root; hence the standard data aggregation mechanisms can take place.

#### *9.2.6.9 Traffic Differentiation*

Score: 1

SAR provides implicit Quality of Service support in its routing decisions. The type of traffic (implemented by means of a priority mechanism) to which the packet belong to for each path is one of the factors based on which SAR makes routing decisions [RD-88].

#### *9.2.6.10 Security*

Score: 3

SAR (Security Aware Routing) [RD-124] protocol is an Ad Hoc network protocol that finds a secure path using the security level of mobile nodes. SAR incorporates security attributes as parameters into ad hoc route discovery that enables the use of security as a negotiable metric to improve the relevance of the routes discovered by ad hoc routing protocols.

However, the SAR protocol sometimes transfers data through inefficient transmission paths because it always tries to find secure nodes for a safe transmission. Since it is a protocol based on AODV, the new routing path will be searched from the very beginning when a transmission fails. Obviously it will cause transmission delay. Also during the new routing path search, the connection could not established when the security level of intermediate node is lower than the level requested by a source node [RD-125].

In conclusion, SAR enables the discovery of secure routes in a mobile ad hoc environment. Its integrated security metrics allow applications to explicitly capture and enforce explicit cooperative trust relationships. In addition, SAR also provides customizable security to the flow of routing protocol messages themselves. Routes discovered by SAR come with “quality of protection” guarantees. The techniques enabled by SAR can be easily incorporated into generic ad hoc routing.

#### *9.2.6.11 Technical Maturity*

Score: 3

SAR is one of the first protocols for WSN that has considered QoS issues for making routing decisions.

### 9.2.7 SPIN

SPIN [RD-126] is among the early work to pursue a data-centric routing mechanism. The idea behind SPIN is to name the data using high-level descriptors or meta-data. Before transmission, meta-data are exchanged among sensors via a data advertisement mechanism, which is the key feature of SPIN. Each node upon receiving new data, advertises it to its neighbours and interested neighbours, i.e. those who do not have the data, retrieve the data by sending a request message

#### 9.2.7.1 Scalability

Score: 1

One of the advantages of SPIN is that topological changes are localized since each node needs to know only its single-hop neighbours [RD-119].

#### 9.2.7.2 Heterogeneity

Score: 1

SPIN supports a wide range of hardware and software platforms.

#### 9.2.7.3 Timeliness

Score: 3

SPIN protocol doesn’t implement any concrete QoS mechanism; it is based on an interesting data negotiation mechanism. This increases the available bandwidth [RD-88]. However, SPIN’s data advertisement mechanism cannot guarantee the delivery of data [RD-119]. For instance, if the nodes that are interested in the data are far away from the source node and the nodes between source and destination are not interested in that data, such data will not be delivered to the destination at all [RD-119]. Therefore, SPIN is not a good choice for applications which require reliable delivery of data packets over regular intervals [RD-119].

#### 9.2.7.4 Reliability / Robustness

Score: 4

SPINs data advertisement mechanism cannot guarantee the delivery of data. To see this, consider the application of intrusion detection where data should be reliably reported over periodic intervals and assume that nodes interested in the data are located far away from the source node and the nodes between source and destination nodes are not interested in that data, such data will not be delivered to the destination at all.

#### 9.2.7.5 Resiliency

Score: 4

Since there is no guarantee that data are delivered, it becomes difficult to think that good and fast recovery can be performed in case of failure.

#### 9.2.7.6 Energy Efficiency

Score: 3

Data negotiation mechanism increases lifetime of the network [RD-88]. However, the format of the exchanged meta-data has to be carefully designed in order not to make the nodes transmit very voluminous information [RD-88]. This is strongly application-dependent.

#### 9.2.7.7 Interoperability

Score: 1

SPIN is interoperable with many layer implementations. It is a data-centric protocol.

#### 9.2.7.8 Data Aggregation / Compression Mechanisms

Score: 3

The format of the exchanged meta-data has to be carefully designed in order not to make the nodes transmit very voluminous information [RD-88]. This is strongly application-dependent.

#### 9.2.7.9 Traffic Differentiation

Score: 4

SPIN does not implement any concrete QoS mechanism. It does not support multiple traffic classes.

#### 9.2.7.10 Security

Score: 3

SPINS has two secure building blocks: SNEP and $\mu$TESLA. SNEP provides the following important baseline security primitives: Data confidentiality, two-party data authentication, and data freshness. A particularly hard problem is to provide efficient broadcast authentication, which is an important mechanism for sensor networks. $\mu$TESLA is a new protocol which provides authenticated broadcast for severely resource-constrained environments. The above protocols were implemented, and show that they are practical even on minimalistic hardware: The performance of the protocol suite easily matches the data rate of our network. It was demonstrated that the suite can be used for building higher level protocols [RD-127].

**Contributions & Merits**

- Combines two unique methods SNEP & μTESLA;
- Gives actual performance numbers on extremely resource-constrained environments
- Some limited analysis on energy consumption
- Simple yet effective design choices:
  1. Use of a single block cipher for all operations;
  2. Counter mode encryption.
- SPINS is relatively universal and extensible to many other embedded applications
- Two application examples:
  1. Authenticated routing in ad-hoc networks using key disclosure packets as routing beacons
  2. Secure node-to-node key agreement using symmetric cryptography

- A nice feature of the above protocol is that the base station performs most of the transmission work.

**Weaknesses & Drawbacks**

- Weak mobility model. Sensor networks assumed to have a base station
  1. What if they don't?
  2. Lots of other papers assume nodes take turns being the base station, negating the "supernode" assumption.
- It appears mobility is limited or infrequent. If it isn't, the overhead from the routing beacons might be significant.
- Time synchronization is a key assumption
  1. Clock drift is actually a major problem in sensor networks using crystal oscillators
  2. Packet loss is also potentially a major issue in wireless environments
- Both can be mitigated by re-synchronizing the counter or sending it with the message. But this leads to huge (and potentially devastating) overhead in sensor networks.
- Clock drift could lead to attacks
- No non-repudiation
- No study of compromised nodes
- No study of the effects of error rates on energy consumption
- SPINS use only symmetric cryptography. The disadvantage is that once a node is compromised, forward secrecy is broken, therefore tamper-resistance becomes crucial [RD-128].

#### 9.2.7.11 Technical Maturity

Score: 3

SPIN is among the early work to pursue data-centric routing mechanism. However, there is not a standard format of the exchanged meta-data [RD-88].

### 9.2.8 Directed Diffusion

Directed Diffusion [RD-129] is an important milestone in the data-centric routing research of sensor networks. The idea aims at diffusing data through sensor nodes by using a naming scheme for the data. The main reason behind using such a scheme is to get rid of unnecessary operations of network layer routing in order to save energy. Direct Diffusion suggests the use of attribute-value pairs for the data and queries the sensors in an on demand basis by using those pairs.

#### 9.2.8.1 Scalability

Score: 3

Among the characteristics of this paradigm, there is the caching of data (generally attribute-value pair's interests). This feature can increase scalability of coordination between sensor nodes [RD-88]. However, being based on a query driven data delivery model, the applications that require continuous data delivery to the sink will not work efficiently with this model. So this paradigm is not a good choice as a routing protocol for environmental monitoring [RD-119].

#### 9.2.8.2 Heterogeneity

Score: 1

Directed Diffusion does not place restrictions on hardware and software components.

#### 9.2.8.3 Timeliness

Score: 3

This paradigm allows for data aggregation which reduces the number of transmissions, leading to allow higher bandwidth near to the sing node. This could be decisive to provide QoS for real-time applications [RD-88]. However, being based on a query driven data delivery model, the applications that require continuous data delivery to the sink will not work efficiently with this model. So this paradigm is not a good choice as a routing protocol for environmental monitoring [RD-119].

#### 9.2.8.4 Reliability / Robustness

Score: 4

As all the flat routing protocols, this has not been designed with reliability in mind. The main idea of the DC paradigm is to combine the data coming from different sources enroute (in-network aggregation) by eliminating redundancy, minimizing the number of transmissions; thus saving network energy and prolonging its lifetime. Unlike traditional end-to-end routing, DC routing sends routes from multiple sources to a single destination that allows in-network consolidation of redundant data. It is not suitable for applications (e.g., environmental monitoring) that require continuous data delivery to the base station).

#### 9.2.8.5 Resiliency

Score: 4

Since there is no guarantee that data are delivered, it becomes difficult to think that good and fast recovery can be performed in case of failure.

#### 9.2.8.6 Energy Efficiency

Score: 1

The main goal of this paradigm is to aggregate data eliminating redundancy. This leads to network savings and lifetime extension [RD-88].

#### 9.2.8.7 Interoperability

Score: 2

Primarily directed diffusion was implemented in ns-2. It assumes MESH like topology, where interest for event(s) are propagated through the network for a particular region and gradients are set, so that events could be propagated at regular intervals along these gradients towards the sink. The sink is considered to be the node that generated an interest for a given event. In this protocol, a sink can generate multiple interests from the same area or from different areas for the same event type. Also, multiple sinks can initiate propagating interest for the same event type from the same region. However, this routing protocol is closely associated with the application, since it depends on the event definitions that may be used by sink nodes.

#### 9.2.8.8 Data Aggregation / Compression Mechanisms

Score: 3

Directed Diffusion, unlike traditional end-to-end routing, tries to find routes from multiple sources to a single destination which allows redundant data aggregation [RD-88]. Hence, the objective of this protocol is specifically to aggregate data coming from different sources, by deleting redundancy. However, being based on a query driven data delivery model, the applications that require continuous data delivery to the sink will not work efficiently with this model. So this paradigm is not a good choice as a routing protocol for environmental monitoring [RD-119].

#### 9.2.8.9 Traffic Differentiation

Score: 4

Directed Diffusion does not support multiple traffic classes.

#### 9.2.8.10 Security

Score: 4

Security aspects have not been found at all for this protocol.

#### 9.2.8.11 Technical Maturity

Score: 3

A directed diffusion implementation is available at http://www.isi.edu/scadds/testbeds.html.

However, being based on a query driven data delivery model, the applications that require continuous data delivery to the sink will not work efficiently with this model. So this paradigm is not a good choice as a routing protocol for environmental monitoring [RD-119].

### 9.2.9 Energy Aware Routing

Shah and Rabaey [RD-130] proposed to use a set of sub-optimal paths occasionally to increase the lifetime of the network. These paths are chosen by means of a probability function, which depends on the energy consumption of each path. Network survivability is the main metric that the approach is concerned with. The approach argues that using the minimum energy path all the time will deplete the energy of nodes on that path. Instead, one of the multiple paths is used with a certain probability so that the whole network lifetime increases. The protocol assumes that each node is addressable through a class-based addressing which includes the location and types of the nodes.

#### 9.2.9.1 Scalability

Score: 3

The protocol requires a setup phase and a less frequent route maintenance phase, where a localized flooding occurs to find the routes and create the routing tables with the energy cost metrics and nodes' positions. This means that this approach requires gathering the location information which complicates the route setup [RD-119].

#### 9.2.9.2 Heterogeneity

Score: 2

The protocol makes assumptions on how the network is addressed.

#### 9.2.9.3 Timeliness

Score: 3

Timing requirement is addressed only in the sense that the cost metric includes the closeness to the final intended destination. However, the probabilistic approach used doesn't make any guarantee on throughput and latency.

#### 9.2.9.4 Reliability / Robustness

Score: 4

Reliability/fault tolerance aspects have not been faced at all. However, the availability of several alternative paths is good in the case of node failures (e.g., low energy or crash), in that real packets can be easily forwarded on alternative paths. However, it should be verified how this could impact on the performance of the network.

#### 9.2.9.5 Resiliency

Score: 4

Reliability/fault tolerance aspects have not been faced at all. However, the availability of several alternative paths is good in the case of node failures (e.g., low energy or crash), in that real packets can be easily forwarded on alternative paths. However, it should be verified how this could impact on the performance of the network. Moreover, no experiments have been done to evaluate recovery speed.

#### 9.2.9.6 Energy Efficiency

Score: 1

Energy cost for each path is explicitly considered as the main routing metric.

#### 9.2.9.7 Interoperability

Score: 1

The protocol in [RD-130] and other similar protocols mainly focus towards energy conservation and balancing the energy usage across the network. Usually these protocols perform better in MESH like networks where nodes are redundant and multiple transmission paths are present, such that less energy consuming path can be selected while transmitting.

#### 9.2.9.8 Data Aggregation / Compression Mechanisms

Score: 4

Data aggregation is not considered and difficult to implement since each node sends different packets to different paths, in a probabilistic way.

#### 9.2.9.9 Traffic Differentiation

Score: 1

Energy-aware routing supports two traffic classes, real-time and best-effort. So the traffic differentiation is limited but of relevance to EMMON.

#### 9.2.9.10 Security

Score: 4

Security aspects have not been found at all for this protocol. Transform Energy Aware Security Routing (TEASR) [RD-131] protocol which provides the mutual authentication of between nodes

#### 9.2.9.11 Technical Maturity

Score: 3

No significant results have been found about large scale real world deployments.

### 9.2.10 Breath

Energy-efficient, reliable and timely data transmission is essential for wireless sensor networks (WSNs) employed in control applications. To reach a maximum efficiency, cross layer interaction is a major design paradigm to exploit the complex interaction among the layers of the protocol stack. Breath [RD-132] ensures a desired packet delivery and delay probabilities while minimizing the energy consumption of the network.

#### 9.2.10.1 Scalability

Score: 3

The protocol is a cluster based approach and it assumes that each node belonging to a cluster is able to communicate with each node of the neighbour clusters.

#### 9.2.10.2 Heterogeneity

Score: 2

Breath is a cross-layer solution where MAC, routing and duty-cycling functions are implemented together.

#### 9.2.10.3 Timeliness

Score: 1

Protocol parameters are chosen at deployment phase by formulating and solving an optimization probabilistic problem which try to minimize the total network energy under the constraints of maximum end-to-end delay and successful packet delivery ratio.

#### 9.2.10.4 Reliability / Robustness

Score: 3

Results presented in [RD-132] show that Breath behaves well in the presence of reliability and latency constraints, even if compared to 802.15.4. However, available results refer only to indoor control networks.

#### 9.2.10.5 Resiliency

Score: 3

Results presented in [RD-132] show that Breath behaves well in the presence of reliability and latency constraints, even if compared to 802.15.4. However, available results refer only to indoor control networks.

#### 9.2.10.6 Energy Efficiency

Score: 1

Protocol parameters are chosen at deployment phase by formulating and solving an optimization probabilistic problem which try to minimize the total network energy under the constraints of maximum end-to-end delay and successful packet delivery ratio.

#### 9.2.10.7 Interoperability

Score: 2

Breath [RD-132] was implemented on T-mote Sky nodes, in a non line of sight environment. In the experiments, it is compared against 802.15.4. It assumes clusters of intermediate nodes, while forwarding data from designated cluster of source nodes towards the cluster of sink or destination nodes. But since, it does not implement acknowledgment (ACK) or re-transmission of lost packets, the probability of data loss is higher in scarce deployments where only limited number of nodes, are present. This may happen because the intermediate node, responsible for forwarding packets, may be in sleep mode during the transmission.

#### 9.2.10.8 Data Aggregation / Compression Mechanisms

Score: 4

No data aggregation is foreseen in this protocol.

#### 9.2.10.9 Traffic Differentiation

Score: 4

Breath does not provide explicit support for traffic classes.

#### 9.2.10.10 Security

Score: 4

Security aspects have not been found at all for this protocol.

#### 9.2.10.11 Technical Maturity

Score: 3

This solution has been recently proposed, but it has been validated both via simulation in OMNeT++ and experimentation on TMote Sky platform (for a small scale indoor network).

### 9.2.11 GEAR

Geographic and Energy-Aware Routing (GEAR) [RD-133] uses energy aware and geographically informed neighbour selection heuristics to route a packet towards the target region. The idea is to restrict the number of interests in Directed Diffusion by only considering a certain region rather than sending the interests to the whole network. GEAR compliments Directed Diffusion in this way and thus conserves more energy.

#### 9.2.11.1 Scalability

Score: 3

The protocol uses energy aware and geographically informed neighbour selection heuristics to route a packet towards the target region. Each node uses only local information. However, even if this protocol has been simulated with 48000 nodes, it revealed limited scalability [RD-134].

#### 9.2.11.2 Heterogeneity

Score: 2

While not explicitly addressed, GEAR does not have any restrictions on heterogeneity.

#### 9.2.11.3 Timeliness

Score: 3

Packets are routed to the target regions by using geographic information: this means that at each step the set of neighbours closest to the destination is chosen. However, in the case of holes in the network, i.e. a node identify that all its neighbours are farther than itself to the target region, there isn't any guarantee on the packet delivery time.

#### 9.2.11.4 Reliability / Robustness

Score: 2

Using local flooding, holes in a local region do not constitute a serious problem; hence the protocol can be considered robust to crash/node failures. Additionally in [RD-133] and [RD-134] GEAR is shown to perform well in terms of packet delivery.

#### 9.2.11.5 Resiliency

Score: 4

No recovery mechanisms are explicitly implemented.

#### 9.2.11.6 Energy Efficiency

Score: 1

Energy is one metric cost to choose the relay neighbour. Moreover, when the packet reaches the target region, it can be diffused to nodes in that region via restricted flooding (more energy efficient in low density regions) or recursive geographic flooding (more energy efficient in high density regions).

#### 9.2.11.7 Interoperability

Score: 1

The algorithm was implemented in a discrete event simulator and compared against GPSR. However, in the simulation the transmission or queuing delay was not taken into account. Also, the MAC layer was assumed to turn off itself when it is not actively transmitting or receiving. These assumptions were made to compare the overhead incurred by the algorithm only with rest of the available algorithms. The source and target regions of the data traffic were randomly distributed throughout the network in the first case. However, in the second case sources and destinations were clustered near each other. This means that all the sources were near each other and destinations were placed near each other.

#### 9.2.11.8 Data Aggregation / Compression Mechanisms

Score: 3

Since GEAR is a compliment of Directed Diffusion, it has the same score as in Section 9.2.8.8).

#### 9.2.11.9 Traffic Differentiation

Score: 4

GEAR does not provide explicit support for traffic classes.

#### 9.2.11.10 Security

Score: 4

Security aspects have not been found at all for this protocol.

#### 9.2.11.11 Technical Maturity

Score: 3

No significant results have been found about large scale real world deployments

### 9.2.12 GPSR

Greedy Perimeter Stateless Routing (GPSR) [RD-135], a routing protocol for wireless datagram networks that uses the positions of only local neighbours and a packet's destination to make packet forwarding decisions. GPSR is one of the earlier works in geographic routing that uses planar graphs to solve the problem of holes. In case of GPSR, the packets follow the perimeter of the planar graph to find their route. Although GPSR decrease the number of states a node should keep, it has been designed for general mobile ad hoc networks and requires a location service to map locations and node identifiers.

#### 9.2.12.1 Scalability

Score: 1

The protocol uses geographically informed neighbour selection heuristics to route a packet towards the target region. Each node uses only local information.

#### 9.2.12.2 Heterogeneity

Score: 1

GPSR was designed for general purpose ad hoc networks and is therefore applicable to a wide range of networks.

#### 9.2.12.3 Timeliness

Score: 3

Packets are routed to the target regions by using geographic information: this means that at each step the set of neighbours closest to the destination is chosen. However, in the case of holes in the network, i.e. a node identify that all its neighbours are farther than itself to the target region, there isn't any guarantee on the packet delivery time.

#### 9.2.12.4 Reliability / Robustness

Score: 2

Simulations with up to 200 nodes over a full IEEE 802.11 MAC demonstrate that GPSR consistently delivers upwards of 94% of data packets successfully. It also encompasses mechanisms for MAC failures catching that are very robust.

#### 9.2.12.5 Resiliency

Score: 4

No recovery mechanisms are explicitly implemented.

#### 9.2.12.6 Energy Efficiency

Score: 4

Differently from GEAR, in GPSR energy is not a metric cost to choose the relay neighbor.

#### 9.2.12.7 Interoperability

Score: 2

This algorithm was simulated in ns-2 and was compared against DSR (Dynamic Source Routing). In the experiments, it uses IEEE 802.11 MAC and PHY layers and considers mobile or moving nodes in the simulation. The movement of nodes is simulated using random waypoint model. Although it requires less state information than many non-geographic routing protocols, but it does not take energy awareness into account. The protocol was successfully simulated for 50, 112 and 200 nodes, where each node has a communication range of 250m. The nodes' velocity was variable with maximum velocity being 20m/s.

#### 9.2.12.8 Data Aggregation / Compression Mechanisms

Score: 3

Since GPSR is similar to GEAR, it has the same score as in Section 9.2.11.8.

#### 9.2.12.9 Traffic Differentiation

Score: 1

While GPSR does not support traffic classes and traffic differentiation, an improvement called QoS-GPSR [RD-136] does provide QoS support.

#### 9.2.12.10 Security

Score: 4

Security aspects have not been found at all for this protocol.

#### 9.2.12.11 Technical Maturity

Score: 3

Some publications are available at http://www.icir.org/bkarp/gpsr/gpsr.html, as well as simulation code in NS2. However, no implementation code has been found.

### 9.2.13 SPEED

SPEED [RD-137] is a QoS routing protocol for sensor networks that provides soft real-time end-to-end guarantees. The protocol requires each node to maintain information about its neighbours and uses geographic forwarding to find the paths. In addition, SPEED strive to ensure a certain speed for each packet in the network so that each application can estimate the end-to-end delay for the packets by dividing the distance to the sink by the speed of the packet before making the admission decision. Moreover, SPEED can provide congestion avoidance when the network is congested.

#### *9.2.13.1 Scalability*

Score: 1

SPEED is a Real Time routing protocol for soft-end-to-end deadline guarantee. It works in a localized way, which makes it scalable [RD-109].

#### *9.2.13.2 Heterogeneity*

Score: 1

SPEED is stateless and applicable to a wide variety of platforms.

#### *9.2.13.3 Timeliness*

Score: 1

SPEED is a Real Time routing protocol for soft-end-to-end deadline guarantee. The core module is the stateless non deterministic geographic forwarding which sends packet to node capable of maintaining the desired delivery speed. At the same time, a backpressure packet re-routing around large delay links is used to reduce or divert the traffic injected to a congested area. The desired network wide speed is maintained such that Soft Real Time end-to-end delivery is obtained with a theoretical delay bound [RD-109].

#### *9.2.13.4 Reliability / Robustness*

Score: 3

SPEED is a real time protocol, hence its main concern is the deadline hitting. If faults are associated to congested links that can cause deadline miss, SPEED has very good performances thanks to the proposed cross-layer approach. However, it is not the best choice for EMMON hence it outperforms other protocols especially for highly dense network deployed on a medium size geographic area.

#### *9.2.13.5 Resiliency*

Score: 3

Congestion control and reconfiguration mechanisms implemented by SPEED are shown to work well (re-routing).

#### 9.2.13.6 Energy Efficiency

Score: 4

It can be reasonable that a protocol specifically designed for (Soft) Real Time WSN may sacrifice energy efficiency in order to achieve message delivery timeliness. So, energy consumption metric has not been taken into account [RD-109].

#### 9.2.13.7 Interoperability

Score: 1

The algorithm was implemented on GloMoSim and Berkeley motes. It is an almost stateless protocol, which requires information only about the neighbouring nodes. It doesn't require real-time or QoS (Quality of Service) aware MAC as its variant “MMSPEED”. Hence, it is compatible with most of the best effort MAC layers. This algorithm provides congestion control and avoids ‘voids’ by feedback loops and back pressure re-routing. MAC layer used in simulation was 802.11 that covered an area of 200m X 200m with 100 nodes uniformly distributed, and each node having radio range of 40m.

#### 9.2.13.8 Data Aggregation / Compression Mechanisms

Score: 4

It is interesting to consider in-network data aggregation to allow a faster information delivery after data redundancy elimination. However, this leads to extra delay due to the processing time for aggregation [RD-109].

#### 9.2.13.9 Traffic Differentiation

Score: 3

SPEED is QoS aware and provides end-to-end service guarantees but does not provide multiple traffic classes so it does not support traffic differentiation.

#### 9.2.13.10 Security

Score: 4

Security aspects have not been found at all for this protocol.

#### 9.2.13.11 Technical Maturity

Score: 2

The protocol should be quite simple to implement, even if no implementation are already available.

## 9.2.14 MMSPEED

MMSPEED [RD-138] is an extension of SPEED which supports service differentiation and probabilistic QoS guarantee.

### *9.2.14.1 Scalability*

Score: 1

Like SPEED, since all mechanisms in MMSPEED work locally without global network state information and end-to-end path setup, it is scalable and adaptive to network dynamics [RD-109].

### *9.2.14.2 Heterogeneity*

Score: 1

MMSPEED, like SPEED, can be used on a wide range of platforms.

### *9.2.14.3 Timeliness*

Score: 1

Like SPEED, the desired network wide speed is maintained such that Soft Real Time end-to-end delivery is obtained with a theoretical delay bound [RD-109].

### *9.2.14.4 Reliability / Robustness*

Score: 1

Routing decisions in MMSPEED are also made taking the reliability requirements of traffic class into account. Regarding the reliability domain, MMSPEED implements a complex mechanism that duplicates the packets sending them through several routes to the sink. To determine next nodes for a packet, MMSPEED takes into account the frame loss ratio of each link to neighboring nodes. This information is directly obtained from link layer.

The score also refers to the optimality in Urban Quality of Life and Traffic monitoring scenarios.

### *9.2.14.5 Resiliency*

Score: 1

Routing decisions in MMSPEED are also made taking the reliability requirements of traffic class into account. Regarding the reliability domain, MMSPEED implements a complex mechanism that duplicates the packets sending them through several routes to the sink. To determine next nodes for a packet, MMSPEED takes into account the frame loss ratio of each link to neighbouring nodes. This information is directly obtained from link layer.

The score also refers to the optimality in Urban Quality of Life and Traffic monitoring scenarios.

#### 9.2.14.6 Energy Efficiency

Score: 4

It can be reasonable that a protocol specifically designed for (Soft) Real Time WSN may sacrifice energy efficiency in order to achieve message delivery timeliness. So, energy consumption metric has not been taken into account [RD-109].

#### 9.2.14.7 Interoperability

Score: 3

This routing algorithm depends heavily on the MAC layer protocol to provide QoS guarantees. It relies on the MAC layer to provide prioritized access to shared medium, reliable (at least partially) delivery of multicast packets, measurement of average delay to neighbours & measurement of loss rate to neighbours. Extends IEEE 802.11e MAC and uses this MAC layer in EDCF (Enhanced Distributed Coordinate Function) mode. The algorithm was simulated in J-SIM and compared against SPEED. The area used in the experiments was 200m X 200m with 100 nodes uniformly distributed in the area, each node having a radio range of 40m.

#### 9.2.14.8 Data Aggregation / Compression Mechanisms

Score: 4

It is interesting to consider in-network data aggregation to allow a faster information delivery after data redundancy elimination. However, this leads to extra delay due to the processing time for aggregation [RD-109].

#### 9.2.14.9 Traffic Differentiation

Score: 1

This algorithm provides traffic differentiation at MAC layer by introducing multiple speeds for various types of traffic having different end-to-end deadlines. In this way, it provides traffic guarantees and end-to-end reliability.

#### 9.2.14.10 Security

Score: 4

Security aspects have not been found at all for this protocol.

#### 9.2.14.11 Technical Maturity

Score: 2

The protocol should be quite simple to implement, even if no implementation are already available.

## 9.3 Conclusions

To summarize, Table 6 collects all the scores of the Routing Protocols technologies analyzed in this section.

| **SCORES** | Scalability | Heterogeneity | Timeliness | Reliability / Robustness | Resiliency | Energy efficiency | Interoperability | Data aggregation / compression mechanisms | Traffic differentiation | Security | Hardware support | Technical maturity | Availability of experience internal to the consortium |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Collection Tree Protocol | 1 | 2 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 | N/A | 1 | 0 |
| Time Synched Mesh Protocol | 3 | 3 | 3 | 1 | 2 | 3 | 3 | 4 | 4 | 1 | | 1 | 0 |
| RPL (ROLL routing protocol) | 2 | 1 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | | 4 | 0 |
| LEACH | 4 | 3 | 3 | 3 | 3 | 3 | 3 | 1 | 1 | 3 | | 1 | 0 |
| PAGASIS | 3 | 2 | 3 | 4 | 4 | 3 | 4 | 1 | 1 | 3 | | 3 | 0 |
| SAR | 3 | 1 | 1 | 2 | 2 | 1 | 1 | 2 | 1 | 3 | | 3 | 0 |
| SPIN | 1 | 1 | 3 | 4 | 4 | 3 | 1 | 3 | 4 | 3 | | 3 | 0 |
| Directed Diffusion | 3 | 1 | 3 | 4 | 4 | 1 | 2 | 3 | 4 | 4 | | 3 | 0 |

| **SCORES** | Scalability | Heterogeneity | Timeliness | Reliability / Robustness | Resiliency | Energy efficiency | Interoperability | Data aggregation / compression mechanisms | Traffic differentiation | Security | Hardware support | Technical maturity | Availability of experience internal to the consortium |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Energy aware routing | 3 | 2 | 3 | 4 | 4 | 1 | 1 | 4 | 1 | 4 | | 3 | 0 |
| Breath | 3 | 2 | 1 | 3 | 3 | 1 | 2 | 4 | 4 | 4 | | 3 | 0 |
| GEAR | 3 | 2 | 3 | 2 | 4 | 1 | 1 | 3 | 4 | 4 | | 3 | 0 |
| GPSR | 1 | 1 | 3 | 2 | 4 | 4 | 2 | 3 | 1 | 4 | | 3 | 0 |
| SPEED | 1 | 1 | 1 | 3 | 3 | 4 | 1 | 4 | 3 | 4 | | 2 | 0 |
| MMSPEED | 1 | 1 | 1 | 1 | 1 | 4 | 3 | 4 | 1 | 4 | | 2 | 0 |

Table 6: WSN Routing and Network Layer Technologies evaluation

# 10. Federated Communication

## 10.1 Requirements/Evaluation Criteria

Moving from the methodology presented in Section 4, the applicable criteria for network architectures are listed in what follows.

- Scalability (see Section 4.1.1.1).
- Heterogeneity (see Section 4.1.1.2).
- Timeliness (see Section 4.1.1.3).
- Reliability / Robustness (see Section 4.1.1.4).
- Resiliency (see Section 4.1.1.5).
- Energy efficiency (see Section 4.1.1.6).
- Interoperability (see Section 4.1.1.7).
- Traffic differentiation (see Section 4.1.1.9).
- Security (see Section 4.1.1.10).
- Hardware support (see Section 0).
- Technical Maturity (see Section 4.1.1.12).
- Availability of internal experience (see Section 4.1.1.13).

## 10.2 Existing Solutions

Thinking at the scheme depicted in the Figure 4, in this section we have introduced the evaluation of the two most important communication frameworks for WSN, i.e. ZigBee and 6LoWPAN, and that of three solutions for long range communication technologies, i.e. WiMAX, 2G/3G and WiFi.

### 10.2.1 ZigBee

IEEE 802.15.4 [RD-82] and ZigBee [RD-139] are standards-based protocols that provide the network infrastructure required for wireless multi-hop network (including WSN) applications. IEEE 802.15.4 itself defines the physical and MAC layers, whereas ZigBee defines the network and application layers. ZigBee defines three types of devices: ZigBee coordinator devices, ZigBee router devices and ZigBee end devices. Every network must contain only one ZigBee coordinator, whose primary responsibility is to set up the parameters for building a network and to start that process. ZigBee routers can be used to extend the range of a network by acting as relays between devices that are too far apart to communicate directly. ZigBee end devices do not participate in routing [RD-142].

ZigBee specifies an algorithm that provides address ranges to routers and coordinators, to be assigned to joining devices (i.e. 'child' nodes) in a systematic manner. As result of this process, a tree structure spanning the whole network is created: the coordinator is designated as the root of the tree and the end devices become the leaves of the tree. In tree-routing, a node can communicate with a remote node by sending frames along the tree. The basis of tree routing is that each node can determine if it needs to forward a packet, destined to a particular node, up to its 'parent' node or down to one of its child nodes, by simply looking at the destination address: if it belongs to a descendant, the packet is passed down to the child node leading to the destination, otherwise the packet is sent upward [RD-142].

Finally, ISEP is studying this technology for a long time and has gained expertise in the field of simulation and experimentation of solutions based on IEEE802.15.4 (and in particular ZigBee).

#### *10.2.1.1 Scalability*

Score: 3

The network density allowed by the Tree Routing mechanism allowed in ZigBee is typically low and the number of nodes is in the order to tenths [RD-142].

#### *10.2.1.2 Heterogeneity*

Score: 2

As ZigBee is not a standard, rather an industry alliance, hence manufacturers like SUN have not implemented it in their radio stack [RD-140]. However, the stack could be implemented or existing open source implementations could be found, if available. Although implementing ZigBee stack means that if EMMON would be commercialized, then first EMMON Consortium would have to join ZigBee Alliance as outlined by ZigBee license.

#### *10.2.1.3 Timeliness*

Score: 3

Since tree routing follows the structure of a tree rather than taking the shortest path, routes may be longer than necessary (thus generating extra traffic) and are more likely to fail. To improve routing efficiency, the ZigBee algorithm also lets routers discover shortcuts by using AODV [RD-142].

#### *10.2.1.4 Reliability / Robustness*

Score: 2

ZigBee offers a range of techniques to ensure reliable communications. These are described below.

- Listen Before Send. The transmission scheme used in ZigBee avoids transmitting data when there is activity on the chosen channel – this is known as Carrier Sense, Multiple Access with Collision Avoidance (CSMA-CA). Put simply, this means that before beginning a transmission, a node listens on the channel to check whether it is clear. If activity is detected on the channel, the node delays the transmission for a random amount of time and listens again. If the channel is now clear, the transmission can begin, otherwise the delay-and-listen cycle is repeated.

- Acknowledgements. An acknowledgement mechanism is built into ZigBee to ensure that messages reach their destinations. When a message arrives at its destination, the receiving device sends an acknowledgement to say the message has been received. If the sending device does not receive an acknowledgement within a certain time interval, it resends the original message (it can resend the message several times until the message has been acknowledged).

- Alternative Routes. In a Mesh topology, the network has built-in intelligence to ensure that messages reach their destinations. If the default route to the destination node is down, due to a failed intermediate node or link, the network can "discover" and implement alternative routes for message delivery.

#### *10.2.1.5 Resiliency*

Score: 2

Congestion control and reconfiguration mechanisms implemented are shown to work well (re-routing).

#### *10.2.1.6 Energy Efficiency*

Score: 1

Low power modes and low duty cycles are the main goals of ZigBee.

#### *10.2.1.7 Interoperability*

Score: 2

A range of home automation and home patient care products are available today in the market which implement Zigbee stack. Motorola has been involved in projects implementing this protocol stack under the trademark NeuRFon [RD-141].

#### *10.2.1.8 Traffic Differentiation*

Score: 1

Traffic differentiation has been implemented on ZigBee though the results have not been as good as expected. The packet loss ratio for higher priority packets was not that much better.

#### *10.2.1.9 Security*

Score: 1

ZigBee security, which is based on a 128-bit AES algorithm, adds to the security model provided by IEEE 802.15.4. The ZigBee protocol defines methods for implementing security services such as cryptographic key establishment (it uses three types of keys to manage security: Master, Network and Link), key transport, frame protection (it uses frame counters to assure message freshness.), and device management. The ZigBee security architecture includes security mechanisms at three layers of the protocol stack - MAC, Network, and Application. Each layer has services defined for the secure transport of their respective frames. Security for applications is typically provided through Application Profiles [RD-143].

The Trust Center, which is usually the network coordinator, is defined in the ZigBee protocol and is responsible for the following security roles [RD-144]:

- Trust Manager, to authenticate devices that request to join the network;

- Network Manager, to maintain and distribute network keys;
- Configuration Manager, to enable end-to-end security between devices.

The current stack release contains two stack profiles:

- Stack profile 1 - simply named ZigBee - for home and light commercial use;
- Stack profile 2 – named ZigBee Pro - offers additional features, such as multi-casting, many-to-one routing and high security with Symmetric-Key Key Exchange (SKKE).

#### *10.2.1.10 Hardware Support*

Score: 1

The ZigBee protocol builds up on the IEEE 802.15.4 protocol, which specifies the physical layer and media access control for Low-Rate Wireless Personal Area Networks (LR-WPANs).This means that motes that support the protocol 802.15.4 also support the ZigBee protocol. This is the case for the TelosB, IRIS, Mulle v5.2, RedBee and Waspmote motes (see [AD-6]).

#### *10.2.1.11 Technical Maturity*

Score: 2

The technology is mature enough, even if mostly for home and industrial automation rather than for very large scale wireless sensor networks.

### 10.2.2 6LoWPAN

6LoWPAN is the International Open Standard that enables building the Wireless "Internet of Things". It enables using 802.15.4 and IP together in a simple well understood way. It brings IP to the smallest of devices - sensors and controllers [RD-145], [RD-146].

The application of IP technology is assumed to provide the following benefits [RD-147]:

- The pervasive nature of IP networks allows use of existing infrastructure.
- IP-based technologies already exist, are well-known, and proven to be working.
- An admittedly non-technical but important consideration is that IP networking technology is specified in open and freely available specifications, which is favourable or at least able to be better understood by a wider audience than proprietary solutions.
- Tools for diagnostics, management, and commissioning of IP networks already exist.
- IP-based devices can be connected readily to other IP-based networks, without the need for intermediate entities like translation gateways or proxies.

#### *10.2.2.1 Scalability*

Score: 1

This standard is explicitly related to large number of devices, which are expected to be deployed during the lifetime of the technology. This number is expected to dwarf the number of deployed personal computers, for example [RD-147].

#### *10.2.2.2 Heterogeneity*

Score: 1

RFC 4944 or 6LoWPAN is viable for heterogeneous sensor networks, composed of a number of different devices, for example, TinyOS motes and Sun SPOTS. Some open source implementations are available but they might not support all options of 6LoWPAN [RD-148], [RD-149], [RD-150]. This makes it feasible to communicate between devices of different levels in the network hierarchy. For instance, if 6LoWPAN is implemented, then the sensor node will be able to communicate directly with Smart Phones, PDAs and remote Command & Control servers. In addition to the above mentioned ability, each device may have a globally unique IP address, based on which the sensor data may be queried from any part of the world.

#### *10.2.2.3 Timeliness*

Score: 1

If each device in the network is provided by an IPv6 address, it will be able to communicate directly with any other kind of device and using standard communication interfaces. This leads to an improvement by avoiding gateways delays, i.e. protocol adaptors.

#### *10.2.2.4 Reliability / Robustness*

Score: 2

Reliability and robustness issues are not explicitly addressed neither in the 6LoWPAN book [RD-153] nor in all the other references available. However, since 6LoWPAN lies on IP and 802.15.4, reliability mechanisms should be easy to implement.

#### *10.2.2.5 Resiliency*

Score: 2

Idem as above.

#### *10.2.2.6 Energy Efficiency*

Score: 1

Energy efficiency strongly relies on the underlying IEE802.15.4 protocol.

#### *10.2.2.7 Interoperability*

Score: 2

6LoWPAN was implemented by [RD-149] on T-mote sky using TinyOS implementation by Berkeley [RD-148]. [RD-150] implements it on Contiki 2.2.1. All of these 6LoWPAN implementations are done on top of IEEE 802.15.4 stack. Nevertheless, these implementations are excellent platform for supporting a number of device types and operating systems.

However, implementation of 6LoWPAN means that location aware or geographic routing, especially in three dimensions may not remain feasible, as the packets may not be capable of handling location information in addition to the payload.

#### 10.2.2.8 Traffic Differentiation

Score: 1

QoS is supported in 6LoWPAN.

#### 10.2.2.9 Security

Score: 3

The most powerful strength is that 6LoWPAN can take advantage of the existing TCP/IP suite of Internet protocols, all of which are well understood due to the proliferation of the Internet. For this reason it can capitalize on existing protocols, existing quality of service requirements and functions, and security framework supported by the IETF, enabling seamless routing of message payloads [RD-151].

Security can be provided at the application, transport, network, and/or at the link layer, i.e., within the 6LoWPAN set of specifications. In all these cases, prevailing WSN inherent constraints will influence the choice of a particular protocol.

Given these constraints, first, a threat model for 6LoWPAN devices needs to be developed in order to weigh any risks against the cost of their mitigations while making meaningful assumptions and simplifications. Some examples for threats that should be considered are man-in-the-middle attacks and denial of service attacks.

A separate set of security considerations apply to bootstrapping a 6LoWPAN device into the network (e.g., for initial key establishment). Beyond initial key establishment, protocols for subsequent key management as well as to secure the data traffic do fall under the purview of 6LoWPAN. Here, the different alternatives (TLS, IKE/IPsec, etc.) must be evaluated in light of the 6LoWPAN constraints [RD-147].

6LoWPAN takes advantage of the strong AES-128 link-layer security mechanisms provided by IEEE 802.15.4. Transport layer mechanisms have also been shown to be feasible on 6LoWPAN networks. However, while network-layer security mechanisms such as IPsec and Secure Neighbour Discovery are becoming mature, their feasibility on 6LoWPANs is still being questioned [RD-152]. This system is still very new and is only a proposed standard. Because it is officially in the public review stage, it will most likely undergo a number of changes. In fact, the mesh routing working groups are still being formed, which means that wide-scale adoption is still a few years away. As such, interoperability is a nice concept that has not yet been proven. Finally, because it is still new, it has not yet been ported to a large group of chipsets [RD-151].

#### 10.2.2.10 Hardware Support

Score: 1

Similarly to the ZigBee protocol, the 6LoWPAN builds up on the IEEE 802.15.4 protocol, which means that motes that support the protocol 802.15.4 also support the 6LoWPAN protocol. This is the case for the TelosB, IRIS, Mulle v5.2, RedBee and Waspmote motes (see [AD-6]).

#### 10.2.2.11 Technical Maturity

Score: 2

There are already available technologies for embedding 6LoWPAN in WSN, like [RD-148], [RD-149], [RD-150]. However, this system is still very new and is only a proposed standard. Because it is officially in the public review stage, it will most likely undergo a number of changes. In fact, the mesh routing working groups are still being formed, which means that wide-scale adoption is still a few years away. As such, interoperability is a nice concept that has not yet been proven. Finally, because it is still new, it has not yet been ported to a large group of chipsets [RD-151].

### 10.2.3 WiMAX / Mobile Broadband

WiMAX Forum [RD-155] is an industry-led, not-for-profit organization formed to certify and promote the compatibility and interoperability of broadband wireless products based upon the harmonized IEEE 802.16/ETSI HiperMAN standard. MBWA's scope [RD-157] is about the specification of physical and medium access control layers of an air interface for interoperable mobile broadband wireless access systems, operating in licensed bands below 3.5GHz, optimized for IP-data transport, with peak data rates per user in excess of 1Mbps.

Finally, TCD is a partner with some knowledge on this field.

#### 10.2.3.1 Scalability

Score: 1

IEEE 802.16 WiMAX broad band standard [RD-156] is quite scalable, as quite many subscriber stations can be connected to a base station. The range of the network with a single base station according to the specifications could be as wide as 40Km. If the network coverage is to be increased beyond that upper bound, then MESH networking mode of the standard could be employed to do so. However, practically due to interference and absorption of transmission, achieved range of network for fixed WiMAX varies between 7Km and 12Km, and for mobile WiMAX, it varies between 1Km and 3Km.

The standard allows the base station to employ time division and frequency division duplexing for servicing as many subscriber stations as possible with the required quality of service guarantees.

#### 10.2.3.2 Heterogeneity

Score: 2

There are many devices available today that support WiMAX (IEEE 802.16d and IEEE 802.16e) and are WiMAX Forum certified. But most of such devices require much power and the protocol is mainly designed for last mile connectivity with respect to home/office networks.

WiMAX may not be suitable for sensor network itself; however it may be appropriate to use WiMAX to connect the base station to the internet for connectivity with C&C. The mobile version of the standard (IEEE 802.16e) could be used on mobile gateways like smart phones compatible with this standard. The usage of this technology however depends on the service provider's availability in the area where the sensor network is deployed.

The major problem is that it works on licensed bands, mostly in 2.3GHz, 2.5GHz and 3.5 GHz bands, which means that the equipment installed must be compatible to the band for which license is obtained. Also, it is worth mentioning that the fixed version and the mobile version of the standard are not compatible to each other. This means if service provider has deployed the fixed version of the standard (IEEE 802.16d) in the target region, then only the fixed base stations could use it.

#### *10.2.3.3 Timeliness*

Score: 1

The network architecture of WiMAX supports simultaneous use of flexible and diverse set of IP services, each of which having different timeliness requirements. At the coarse grain, these service provisioning could be at user or terminal level and at the finer grain, it could be at per user/terminal per service flow level. The base station is responsible for allocating bandwidth to subscribers and different service flows originating from different or same subscriber stations and allocating bandwidth as per requirements of the service flow used.

The standard is capable of providing up to 70Mbps of bandwidth; however to the best of our knowledge, most of the service providers only provide 2.5Mbps per subscriber station. In practice the subscriber station may only get between 1.5 and 2.0Mbps.

#### *10.2.3.4 Reliability / Robustness*

Score: 2

IEEE 802.16 [RD-158] protocol is a connection oriented protocol, in which the subscriber stations or mobile stations establish their connections to the base station through a network entry and registration process. Within the duration of an established connection, if any data units are lost, the receiving node sends a negative acknowledgement to the transmitter, hence notifying the transmitter of lost, garbled or un-received data units. Upon reception of any such negative acknowledgements, the transmitter will send the lost data units again until it receives a positive acknowledgement for those data units. In this manner, the standard provides a reliable connection between the subscriber and base station. End-to-end reliability, where the data packets may travel through a number of different channels or gateways, is out of the scope of this standard protocol. For the purpose of end-to-end reliability, referring to transport layer protocol (for example, TCP/IP) seems like a rather obvious choice.

#### *10.2.3.5 Resiliency*

Score: 2

IEEE 802.16 [RD-158] is a connection oriented protocol; it optionally calculates CRC and performs both fragmentation and packing of MAC Service Data Units (SDU). Because air link is a precious resource, hence 802.16 fills the air link with small SDUs and fragments the large SDUs when they don't fit in the air link allocation. The standard employs automated repeat request (ARQ) for re-transmission of lost or garbled data units. IEEE 802.16 uses a simple sliding window approach to deal with lost data units. The transmitter can transmit up to a pre-negotiated number of blocks with receiving an acknowledgement. Upon completion of these blocks, the receiver sends acknowledgements for the data units that were received successfully and negative acknowledgement for the lost service data units. If negative acknowledgements are received, the transmitter then re-transmits these lost service data units and moves the sliding window forward when acknowledgements are received for all the data units.

#### 10.2.3.6 Energy Efficiency

Score: 1

IEEE 802.16e (Mobile WiMAX) implements Sleep mode and Idle mode to facilitate energy conservation in mobile stations. Sleep modes are the periods which are pre-negotiated with the base station and in these periods, the mobile station remains absent from the serving base station's air interface. From base station's perspective, in the sleep period the mobile station is unavailable for any communication. The sleep period allows the mobile stations to conserve energy and minimize the usage of serving base station's air interface. The mobile stations also scan other base stations during this period to facilitate hand-over.

Idle mode allows mobile stations to become periodically available for the downlink broadcast traffic without registering with any specific base station. This period benefits base stations and network interface by minimizing network handoff traffic from essentially inactive mobile stations, while still providing timely alerts to the mobile stations about pending downlink traffic.

#### 10.2.3.7 Interoperability

Score: 2

Usually WiMAX is deployed in a way that end devices (leaf nodes or subscriber stations) communicate with base station (BS). However the standard allows the network to be deployed in MESH configuration, mainly to extend the range of the network. The standard implements the PHY, MAC and Data link layers. The communication takes place in a connection oriented fashion. Hence, it is not suitable for ad hoc networks.

#### 10.2.3.8 Traffic Differentiation

Score: 1

WiMAX implements QoS at the MAC layer which prioritizes the network traffic depending on the nature of the application. The standard provides QoS guarantees by service flows, which are uni-directional flow of packets associated with a particular set of QoS parameters. During the transmission of a packet, each packet is associated with a particular service flow.

The QoS parameters define transmission ordering and air interface scheduling. These parameters include guarantees for maximum latency tolerance, maximum sustained rate, jitter tolerance, traffic priority, throughput etc.

#### 10.2.3.9 Security

Score: 1

The security sub-layer of IEEE 802.16 provides users with confidentiality, authentication and integrity by applying cryptographic transforms to the payload. It also provides strong protection against service theft by securing the service flows across the network. This sub-layer employs an authenticated client/server key management protocol in which base station controls the distribution of keying material to the subscriber stations.

The encapsulation protocol for securing packet data across the network employs a set of cryptographic suite for data encryption and authentication, and rules for applying those algorithms to the payload. The key management protocol provides secure distribution of keying data from the base station to the subscriber stations. This key management protocol enables the base station and subscriber station to synchronize the keying data and using this protocol, the base station can limit the access to network services.

For device or user authentication the security sub-layer of IEEE 802.16 employs IETF EAP protocol. The subscriber can be authenticated using X.509 digital certificates issued by its manufacturer. The base station could also employ authentication by using SIM (Subscriber Identification Module) based approach.

All base stations and subscriber stations must implement DES in CBC mode for data encryption. However, if the base station and subscriber station, both are capable, they can also use AES in CCM mode for data encryption. All devices guarantee data integrity by using HMAC with secure hash algorithm SHA-1.

In spite of these security features, there are several potential attacks open to adversaries, including rogue BSs, DoS attacks, man-in-the-middle attacks, and network manipulation with spoofed management frames. The real test will come when providers begin wide-scale network deployments, and researchers and attackers have access to commodity customer premises equipment (CPE). Other attacks, including WiMAX Protocol fuzzing, may enable attackers to further manipulate BSs or SSs. Until then, the security of WiMAX is somewhat limited to speculation. Recognizing the importance of security, the 802.16 working groups designed several mechanisms for authentication and encryption to protect the service provider from theft of service and to protect the customer from unauthorized information disclosure [RD-162].

#### *10.2.3.10 Hardware Support*

Score: 4

Requirements for the physical layer and for the MAC layer for this protocol are specified by the protocol IEEE 802.16. None of the motes selected by WP5 provide support for this protocol off the box.

#### *10.2.3.11 Technical Maturity*

Score: 3

IEEE 802.16 standard was formalized in 2004 for fixed subscriber stations, while for mobile stations was formalized in 2005. Since then a number of devices have appeared in the market including cellular phones which provide WiMAX chips on board. Also, this technology has been deployed worldwide mostly in 2.3GHz, 2.5GHz and 3.5GHz licensed bands. But due to the differences in the fixed and mobile versions of the standard, their incompatibility and un-guaranteed availability of devices for the band licensed by the service provider, it may be safe to say that the technology is not quite mature or not readily available.

The subscriber devices available today include Intel 5350 board [RD-159] that has WiMAX and Wi-Fi both on the chip, aimed primarily at computers. In phones, this technology is available on HTC Max4G [RD-160] and Nokia N810 WiMAX addition [RD-161].

### 10.2.4 2G/3G (GSM, GPRS, EDGE, UMTS)

A WSN node [RD-163] can be equipped with GSM/GPRS radio transceiver [RD-164] to be able to directly connect to this public wide area network and eventually sends alarms over internet or via SMS/email. However, the costs of this kind of nodes make difficult to implement large scale networks using a huge number of such devices.

#### *10.2.4.1 Scalability*

Score: 1

With this solution each node is a most powerful station, able to perform networking via e.g. IEEE802.15.4 or directly using public wide area networks [RD-164].

#### *10.2.4.2 Heterogeneity*

Score: 1

Most of the smart phones available today come with GSM/GPRS/HSDPA/HSPA devices on board. This means that it could be used for connecting base stations and/or mobile devices to the command and control centre via internet, from the areas where these services are available. However, these technologies are not suitable for MESH networking.

Since, these technologies are widely available today in a number of devices; hence in our opinion it is better to use these technologies than using WiMax as a backhaul. The base stations (embedded PCs) can be connected to the internet by using a GPRS modem with the base station.

#### *10.2.4.3 Timeliness*

Score: 1

From the part of WSN nodes, when some kind of real time communication or alarm has to be sent, the availability of a connection to public and wide area networks is a key factor.

#### *10.2.4.4 Reliability / Robustness*

Score: 1

GPRS allows to set different QoS levels and reliability is encompassed among them. In [RD-167] the good quality of GPRS connection is stated in terms of lost packets.

### 10.2.4.5 Resiliency

Score: 3

Results in [RD-167] show that many retransmissions are made unnecessarily at different MTU sizes. This compromises MTTR.

### 10.2.4.6 Energy Efficiency

Score: 1

Since this kind of node has hybrid communication radios, it can exploit the efficiency of multi-hop networking (e.g. using IEEE 802.15.4) most of the time and eventually send messages over long distance by exploiting a short time connection to the public network [RD-164].

### 10.2.4.7 Interoperability

Score: 1

Usually base stations are thought of as the only devices that connect to the internet via GPRS/WiMAX or Wi-Fi (in infrastructure mode) becoming the gateway between sensor network and rest of the world, however [RD-163] explains how a GPRS module could be connected to SquidBee mote, so that it could connect directly to the internet. Also, recently WaspMote [RD-164] has been released, which is a modular sensor mote and a number of different chipsets (modules) can be attached to it, including GPRS modem. Although in these cases power consumption of a mote may increase, resulting in shorter network life time.

### 10.2.4.8 Traffic Differentiation

Score: 1

Traffic differentiation is supported in GPRS/EDGE networks.

### 10.2.4.9 Security

Score: 1

The GSM system provides solutions to a few important aspects of security: subscriber authentication, subscriber identity confidentiality and confidentiality of voice and data over the radio path. However the GSM system defined in the standard is not perfect. There are still some potential threats posed [RD-165]. In subscriber authentication procedure, a collision attack on the A3 or A8 algorithm is one example. The microwave links to the BSSs are extensively used when the operator opens its service. The voice and cipher keys Kc can be intercepted on these links. From the standard introduced, it is known that the encryption of voice and use data is only on the radio interface between the MS and the BTS. It does not provide any protection method on the user traffic and signalling data transferred through the fixed parts of network. The ciphering keys should also be protected when transferred between and with networks on ss7 signalling link.

Although GPRS have been designed with security in mind, it presents some essential security weaknesses, which may lead to the realization of security attacks that threaten network operations and data transfer through it. These weaknesses are related to [RD-166]:

- The compromise of the confidentiality of subscriber's identity, since it may be conveyed unprotected over the radio interface;
- The inability of the authentication mechanism to perform network authentication;
- The possibility of using COMP128 algorithm (which has been crypt analyzed) for A3 and A8 implementations;
- The ability of reusing authentication triplets; (e) the possibility of suppressing encryption over the radio access network or modifying encryption parameters;
- The lack of effective security measures that are able to protect signaling an user data transferred over the GPRS backbone network.

#### 10.2.4.10 Hardware Support

Score: 1

Generally, WSN motes (like e.g. the WaspMote [RD-164]) do not come with GSM/GPRS support, but in some cases an optional board can be purchased in order to provide support for this technology. The same applies to devices (e.g. micro PC) which can may as gateways.

#### 10.2.4.11 Technical Maturity

Score: 1

Even if these devices [RD-164] are quite new on the market, they are hybrid and composed by very well known technologies, like IEEE802.15.4 and GSM/GPRS radios.

### 10.2.5 Wi-Fi Low Power

GainSpan [RD-168], a low power Wi-Fi semiconductor company and spin-off of Intel, provides an ultra low power Wi-Fi single chip solution for battery-powered or energy-harvesting-based sensor applications that can run sensor devices for up to 10 years on a single AA battery. Furthermore, low-power Wi-Fi devices have the advantages of native IP-network compatibility and well-known protocols and management tools.

Actively participating in the green revolution and leveraging the very large installed base of Wi-Fi access points, GainSpan and its ecosystem partners reduce energy consumption and carbon footprint as well as the operation and installation costs of residential, commercial, industrial, and municipal sensor network applications.

#### 10.2.5.1 Scalability

Score: 3

Scalability is directly related to the maximum data rate of a particular network architecture [RD-171]. Consequently, the ability to add new sensors and utilize higher data rate sensors is directly proportional to the maximum data rate supported by the physical channel.

Therefore, 802.11 can scale to a great number of nodes and faster data rates. However, this relationship between available bandwidth and scalability is quite too simplistic at very large and dense sensor networks.

#### 10.2.5.2 Heterogeneity

Score: 2

Many commonly used and most popular sensor network devices (mica2, micaZ, telosB, Sun Spots, iMote2) do not support Wi-Fi or low power Wi-Fi. However, recently Gain Span [RD-168] has introduced a low power Wi-Fi chip that is incorporated by a few newly designed sensor nodes [RD-169], [RD-170]. Although these nodes are not as popular as the nodes mentioned earlier, that are commonly used in sensor networks.

Wi-Fi is however widely available today in mobile devices like smart phones, net books, laptops, embedded PCs, desktops and other high end devices.

#### 10.2.5.3 Timeliness

Score: 1

The availability of higher data rate allows for transfer more (possibly aggregated) data at the same time.

#### 10.2.5.4 Reliability / Robustness

Score: 2

Low Power Wi-Fi leverages the reliability/robustness mechanisms already implemented in the original version of 802.11. Hence, it implements retransmission mechanisms for facing collisions and interferences (recall that it works in unlicensed band), only related to unicast traffic (no reliability support to broadcast and multicast traffic). In particular, a station transmits the packet and waits for an ACK. If the receiver successfully receives the packet, it waits for a Short Inter-Frame Spacing time (SIFS) and then transmits an ACK frame. If the sender does not receive an ACK (e.g., due to a collision or poor channel condition), it retransmits the packet using binary exponential back-off, where its contention window is doubled every time after a failed transmission until it.

#### 10.2.5.5 Resiliency

Score: 4

Depending on the channel load, the number of retransmission increases and the MTTR increases consequently. On a large scale network, with thousands of nodes this can be serious, especially in the case of high node density.

#### 10.2.5.6 Energy Efficiency

Score: 1

Implementing silicon orders of magnitude more efficient at conserving power for sensor nodes, along with adding more intelligence in the network to accommodate a new class of 802.11 clients that are often in low power standby mode to conserve power is the key to achieve energy efficiency. By utilizing such technologies, 802.11 WSN solutions are on par with other WSN solutions, achieving 5-10 years of battery life using one AA battery. Such performance is achieved by designing silicon from the ground up specifically for low power consumption applications, utilizing methodologies such as extremely low sleep currents and fast transitions to active and back to standby states [RD-171].

#### *10.2.5.7 Interoperability*

Score: 2

Wi-Fi is a tested and widely available technology today in Smart Phones, PDAs, NetBooks, Laptops and Desktop PCs. Most of these devices can be used in both Infrastructure and Ad hoc networking modes. This means that such devices when used in infrastructure mode can connect to the internet, but requires a gateway to do so. When such devices are used in ad hoc networking mode, they can be utilized to form a mobile ad hoc network, using which the data can be shared among a number of mobile devices which are a part of the network.

#### *10.2.5.8 Traffic Differentiation*

Score: 1

Multiple implementations of Low power Wi-Fi offer support for QoS and traffic differentiation.

#### *10.2.5.9 Security*

Score: 3

The Wi-Fi low power protocol derives from the Wi-Fi protocol, but is oriented towards energy efficiency. This means that, although this protocol focus on reducing energy consumption, it conforms to the IEEE 802.11 standard and benefits from the standards' evolution in areas such as security (802.11i), meshing (802.11s) and Quality of Service (QOS, 802.11e). Relative to other technologies for low-power applications such as ZigBee/802.15.4, low power Wi-Fi takes advantage of the benefits conferred by the well established IP and Wi-Fi protocols.

As far as security is concerned, the Wi-Fi protocol supports well proven Wi-Fi link-layer encryption and authentication and related Wi-Fi Protected Access (WPA/ WPA2). For example, Pre-Shared Key (PSK), Extensible Authentication Protocol (EAP), as well as Transport layer security (TLS/SSL) are all supported by GainSpan's [RD-168] SOC product.

Since this protocol is oriented towards energy saving, and in order to minimize the power consumed during the vast majority of the time – when no data is being transferred - the device must be highly integrated to shorten connections, minimize capacitances and inductances and reduce overall energy consumption. All major system functions, including application programming, task management and network functions, radio management, encryption, MAC and baseband processing, and the radio transceiver itself, should ideally be incorporated on a single die [RD-172].

However, and mostly due to the extensive usage of wireless communications nowadays, it is important to mention that the security mechanisms provided by the Wi-Fi protocol have (and will continue to be) subject to attacks and exploits. For example, the WEP (Wired Equivalent Privacy) and the WPA (Wi-Fi Protected Access) encryption mechanisms have already been thoroughly exploited and their flaws exposed.

#### *10.2.5.10 Hardware Support*

Score: 4

Requirements for the physical layer and for the MAC layer for this protocol are specified by the protocol IEEE 802.11. None of the motes selected by WP5 provide support for this protocol off the box.

#### *10.2.5.11 Technical Maturity*

Score: 3

The Wi-Fi low power technology is very attractive since re-using of existent infrastructure is really appealing. However, this technology is relatively new and it should be verified its suitability especially for very large scale and dense wireless sensor networks. Moreover, not all the intended scenarios for EMMON are compatible with a Wi-Fi pre-existing coverage.

## 10.3 Conclusions

To summarize, Table 7 collects all the scores of the Federated Communications technologies analyzed in this section.

| **SCORES** | Scalability | Heterogeneity | Timeliness | Reliability / Robustness | Resiliency | Energy efficiency | Interoperability | Data aggregation / compression mechanisms | Traffic differentiation | Security | Hardware support | Technical maturity | Availability of experience internal to the consortium |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ZigBee | 3 | 2 | 3 | 2 | 2 | 1 | 2 | N/A | 1 | 1 | 1 | 2 | 1 |
| 6LoWPAN | 1 | 1 | 1 | 2 | 2 | 1 | 2 |  | 1 | 3 | 1 | 2 | 0 |
| WiMAX / Mobile Broadband Wireless Access | 1 | 2 | 1 | 2 | 2 | 1 | 2 |  | 1 | 1 | 4 | 3 | 1 |
| 2G/3G (GSM, GPRS, EDGE, UMTS) | 1 | 1 | 1 | 1 | 3 | 1 | 1 |  | 1 | 1 | 1 | 1 | 0 |
| Wi-Fi (Low Power) | 3 | 2 | 1 | 2 | 4 | 1 | 2 |  | 1 | 3 | 4 | 3 | 0 |

Table 7: Federated Communications Technologies evaluation. The first two are about Communication Framework, while the remaining three are about Long Range communication technologies.

# 11. General Conclusions

In this deliverable, a methodology to infer best practices from past and recent projects about real world deployments of Wireless Sensor Networks and evaluate the technologies available in literature has been presented.

This work addressed a very broad spectrum of technologies, which have been filtered and evaluated in order try to identify a set of alternative networking stacks for EMMON, having the common features to be characterized by i) a multi-tier and backbone-enabled network architecture  and ii) a IEEE802.15.4 short range communication technology. Both proposed stacks are only indicative solutions to be deeper analyzed in the frame of deliverable D4.5, whose main goal will be finding one complete stack, to be further evaluated by performing a quantitative analysis in deliverable D4.3, based on the recognized application requirements.