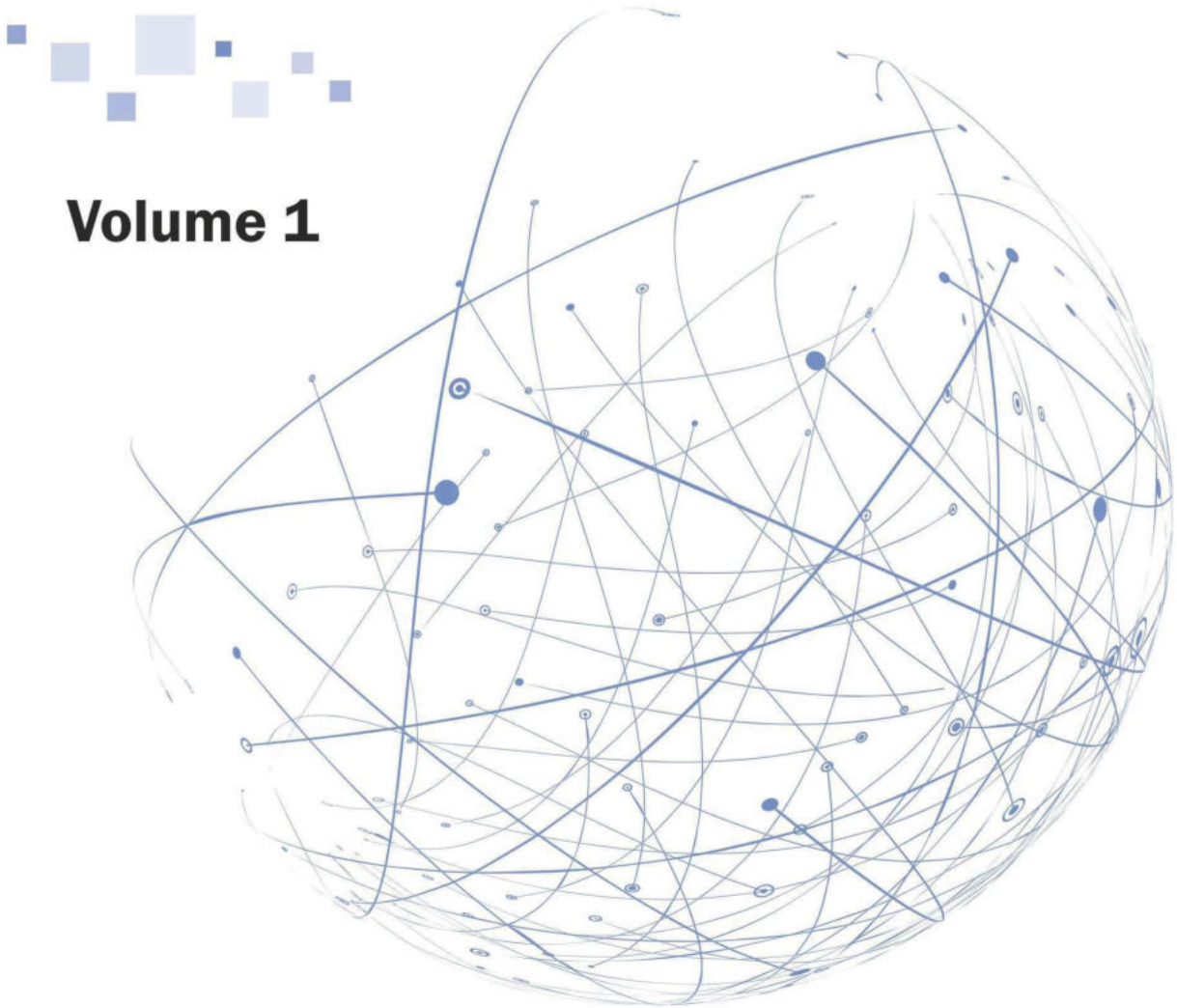
Sergey Y. Yurish
Editor

Advances in Networks, Security and Communications: Reviews

Volume 1



Advances in Networks, Security and Communications: Reviews

Volume 1

Sergey Y. Yurish
Editor

Advances in Networks, Security and Communications: Reviews

Volume 1

International Frequency Sensor Association Publishing

Sergey Y. Yurish
Editor

Advances in Networks, Security and Communications: Reviews
Volume 1

Published by International Frequency Sensor Association (IFSA) Publishing, S. L., 2017
E-mail (for print book orders and customer service enquires): ifsa.books@sensorsportal.com

Visit our Home Page on http://www.sensorsportal.com

Advances in Networks, Security and Communications: Reviews, Vol. 1 is an open access book which means that all content is freely available without charge to the user or his/her institution. Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the articles, or use them for any other lawful purpose, without asking prior permission from the publisher or the authors. This is in accordance with the BOAI definition of open access.

Neither the authors nor International Frequency Sensor Association Publishing accept any responsibility or liability for loss or damage occasioned to any person or property through using the material, instructions, methods or ideas contained herein, or acting or refraining from acting as a result of such use.

ISBN: 978-84-697-8994-0
e-ISBN: 978-84-697-8993-3
BN-20171229-XX
BIC: TJK



Acknowledgments

As Editor I would like to express my undying gratitude to all authors, editorial staff, reviewers and others who actively participated in this book. We want also to express our gratitude to all their families, friends and colleagues for their help and understanding.

Contents

Contents **7**
Contributors **15**
Preface **19**

Networks **21**

1. WSN Routing Improvement Techniques **23**
1.1. Introduction 23
1.2. Architecture of a Wireless Sensor Node 24
1.2.1. The Sensing Unit 24
1.2.2. The Processing Unit 25
1.2.3. The Wireless Transceiver Unit 25
1.2.4. The Power Unit 25
1.3. The Offer of Sensor Manufacturers 26
1.3.1. The Tmote Sky of Moteiv 26
1.3.2. Sun SPOT from Sun Microsystems 27
1.3.3. The WiEye of EasySen 28
1.3.4. The Micaz Mote of Crossbow 28
1.3.5. Jennic Sensors 29
1.3.6. Other Commercial Applications 30
1.4. Wireless Sensor Network Architecture 32
1.4.1. Wireless Sensor Network Architecture 32
1.4.2. Energy Consumption Factors in WSNs 33
1.4.2.1. Collisions *33*
1.4.2.2. Idle Listening *33*
1.4.2.3. Overhearing *33*
1.4.2.4. Overmitting *34*
1.4.2.5. Control Packets Overhead *34*
1.4.2.6. Network Protocols *34*
1.4.2.7. Attacks and Security Issues *34*
1.4.2.8. Cryptography and Security Solutions *34*
1.5. Application Domains of Sensor Networks 35
1.5.1. Military Applications 35
1.5.2. Security and Safety Related Applications 35
1.5.3. Medical Applications 35
1.5.4. Environmental Applications 36
1.5.5. Commercial Applications 36
1.5.6. Cold Chain Monitoring System 36
1.5.6.1. Issues and Challenges *36*
1.5.6.2. Needs and Operating Principles *38*
1.6. Routing Mechanisms for WSN Cold Chain Monitoring System 40
1.6.1. Introduction 40
1.6.2. Backgrounds and Related Works 42
1.6.3. Routes Selection Criteria 43
1.6.3.1. Remaining Energy Level *43*
1.6.3.2. Sensor Proximity with Respect to the Base Station (Proximity-BS) *43*
1.6.3.3. Degree of Connectivity *45*
1.6.3.4. LQI: Link Quality Indicator *45*

1.6.3.5. Composite or Hybrid Metric *46*
1.6.4. Routing Mechanisms 46
1.6.4.1. Simple Routing *46*
1.6.4.2. Round Robin Routing *47*
1.6.4.3. Weighted Round-Robin Routing (W2R routing) *48*
1.7. L2RP: The Link Reliability Based Routing Protocol 50
1.8. Routing Protocol Performance Criteria 51
1.8.1. Average Ratio of the Remaining Energy 51
1.8.2. Average Path Lengths 52
1.8.3. LIF: Load Imbalance Factor 52
1.8.4. Network Lifetime 52
1.8.5. Average Percentage of Lost Packets 52
1.9. L2RP Routing Protocol Performance Evaluation Model 53
1.9.1. Energy Consumption Model 53
1.9.2. Network Deployment and Performance Evaluation Parameters 53
1.9.3. LQI Model for Performance Evaluation Purposes 55
1.10. L2RP Routing Protocol Performance Evaluation 56
1.10.1. Average Path Length 56
1.10.2. LIF: Load Imbalance Factor 59
1.10.3. Average Percentage of Packet Losses 62
1.10.4. Composite or Hybrid Metric 63
1.10.5. Average Network Lifetime 65
1.10.6. Average Ratio of the Remaining Energy 67
1.10.7. Impacts of Increasing the Number of Achtophorous Nodes 68
1.10.8. Impacts of the Unreliability of Wireless Links 69
1.11. Energy Over-Consumption Induced by Securing Routing Operations 72
1.11.1. Introduction and Backgrounds 72
1.11.2. Energy Over-Consumption Induced by Adding an Integrity Key to L2RP 73
1.12. Conclusions 81
Acknowledgements 83
References 83

2. Connectivity Recovery and Augmentation in Wireless Ad Hoc Networks 89
2.1. Introduction 89
2.2. Articulation Nodes and Bridges 91
2.2.1. Definitions and Terms 91
2.2.2. Location of Articulation and Bridges 92
2.2.3. Locating Articulations and Bridges in Wireless Ad Hoc Networks 93
2.3. Cooperative Communication 102
2.4. Connectivity Recovery 104
2.5. Connectivity Augmentation 110
2.6. Conclusion 112
References 113

3. QoS Routing in Ad Hoc Network 115
3.1. Introduction 115
3.2. Routing in Ad Hoc Network 115
3.3. Usual Metrics 117
3.3.1. Hop-Count Metric 117
3.3.2. Delay-Based Metrics 118
3.3.3. ETX Metric 118
3.3.4. BER-Based Metric 119
3.3.5. Retransmission-Based Metric 121
3.4. Taking Into Account the Quality of Links in the Choice of Route 122

3.5. Conclusion 124
Acknowledgements 125
References 125

4. A Knowledge-Based Modeling and Simulation Approach for the Management of Sensor Networks 129
4.1. Introduction 129
4.2. Related Work 130
4.2.1. Modelling and Simulation Tools for Sensor Networks 130
4.2.2. Environment Representation 131
4.2.3. Spatial Behaviours and Knowledge Management 132
4.3. Generation of Informed Virtual Geographic Environments 133
4.3.1. GIS Input Data Selection 133
4.3.2. Spatial Decomposition 134
4.3.3. Map Unification 134
4.3.4. Informed Topologic Graph 134
4.4. From Semantic Information to Environment Knowledge 135
4.4.1. Environment Knowledge 136
4.4.2. Inference Engine 137
4.4.3. Mapping Knowledge Using Environment Knowledge and Inference Engine 138
4.5. From Environment Knowledge to Spatial Behaviors 139
4.5.1. Agent Archetypes 139
4.5.2. Action Archetypes 141
4.6. A Knowledge-Based Approach 141
4.6.1. Agent-Based Simulation Using Informed Virtual Geographic Environments 142
4.6.2. Spatio-Temporal Knowledge 142
4.6.2.1. Representation Formalism 142
4.6.2.2. Knowledge Categories 143
4.7. Case Study: Simulation of a Sensor Network for Weather Monitoring 146
4.8. Discussion 148
4.9. Conclusion and Future Perspectives 149
Acknowledgements 149
References 150

Security 153

5. Reference Monitor-based Security Framework for Trust in Mobile Agent Computing 155
5.1. Introduction 155
5.2. Background Study 156
5.3. Reference Monitor Based Security Framework 159
5.4. Integration and Evaluation of RM-Agent 161
5.4.1. Distribution and Integration of RM-Agent into an AP 161
5.4.2. Verifying Authenticity and Integrity of RM-Agent 162
5.4.2.1. Authentication and Integrity Checking Protocol (AICP) 164
5.5. Experiments and Results 167
5.6. Conclusions and Future Work 167
References 168

6. Risk Assessment Considering Configuration of Hybrid Cloud Computing 171
6.1. Introduction 171
6.2. Overview of Hybrid Cloud Computing Configuration 172
6.2.1. Reference Model of Cloud Computing 172

6.2.2. Hybrid Cloud Computing 172
6.2.3. Related Work 174
6.3. Risk Identification and Analysis: Qualitative Risk Analysis of Hybrid Cloud Computing Configuration 175
6.3.1. Risk Identification: Extraction of Risk Factors in Hybrid Cloud Computing Configuration 175
6.3.2. Risk Analysis: Qualitative Analysis of Risk Factors in Hybrid Cloud Computing Configuration 175
6.3.2.1. Risk Analysis Method 175
6.3.2.2. Risk Analysis Result from Qualitative Viewpoint 176
6.3.2.3. Summary of Risk Analysis Results 176
6.4. Risk Evaluation: Quantitative Risk Evaluation of Hybrid Cloud Computing Configuration 177
6.4.1. Risk Formula 177
6.4.1.1. Approximation of Asset Value 179
6.4.1.2. Approximation of Threat Value 180
6.4.1.3. Approximation of Value of Vulnerability 180
6.4.2. Calculation of Risk Value 181
6.4.3. Discussion 181
6.5. Conclusion and Future Work 184
Acknowledgements 184
References 184

7. The Mathematical Modeling of Road Transport in Context of Critical Infrastructure Protection 187
7.1. Introduction 187
7.2. Critical Infrastructure 188
7.2.1. The Cross-Cutting Criteria 188
7.2.2. The Sectoral Criteria 188
7.3. Critical Road Infrastructure 189
7.4. Mathematical Models of Road Transport 190
7.4.1. Macroscopic Model 191
7.4.2. Macroscopic Model 191
7.5. The Use of Dynamic Modeling of the Impacts of Road Transport 194
7.6. Conclusion 197
Acknowledgements 198
References 198

8. The Assessment of the Soft Targets 201
8.1. Introduction 201
8.2. Methodology of the Solving 203
8.2.1. Deming's Circle Methodology 203
8.2.2. Processes Management 204
8.2.3. Crisis Escalation 204
8.2.4. Failure Mode and Effect Analysis 206
8.3. The Proposed Static Assessment 207
8.4. The Proposed Dynamic Assesment 209
8.5. The Proposal of the Preventive Actions 210
8.6. Conclusions 211
Acknowledgements 212
References 213

Communications 215

9. Performance Analysis of Quadrature Amplitude Modulation Schemes in Amplify-and-Forward Relay Networks over Rayleigh Fading Channels 217
9.1. Introduction 217
9.2. System Model 219
9.3. ASER Performance Analysis 221
9.3.1. ASER of General Order RQAM for MRC Scheme 221
9.3.2. ASER of General Order XQAM for MRC Scheme 223
9.3.3. ASER of General Order XQAM for BRS Scheme 224
9.4. Numerical and Simulation Results 224
9.5. Conclusion 229
Acknowledgements 230
References 230

10. High-Gain Low-Cost Microstrip Antennas and Arrays Based on FR4 Epoxy 233
10.1. Introduction 233
10.2. The Studied Methods 234
10.3. Parameter Study and Performance Comparison 235
10.4. Design Examples 239
10.5. Conclusions 242
References 242

11. Interference Management and System Optimisation for Femtocells Technology in LTE and Future 4G/5G Networks 247
11.1. Introduction 247
11.1.1. Motivation Towards Small Cells 248
11.1.2. Challenges of Vehicular Environment 250
11.2. Related Work 251
11.2.1. LTE Vehicular UEs Penetration Loss 252
11.2.2. Vehicular UEs Performance 252
11.2.3. Small Cells Interference 256
11.3. Mobile Femtocell Technology 259
11.4. Vehicular UEs Performance Analysis in LTE Networks 261
11.4.1. System Model 261
11.4.2. Results and Discussion 271
11.5. Interference Management for Co-Channel and Co-Tire Femtocells Technology 279
11.5.1. Coverage Optimisation 280
11.5.2. Transmission Power Control 283
11.5.3. The Proposed Interference Management Scheme 284
11.5.4. The Proposed Scheme (System Performance Analysis) 288
11.5.5. Results and Discussion 291
11.6. Conclusions and Further Work 302
11.6.1. Conclusion 302
11.6.1.1. Performance Evaluation 302
11.6.1.2. Interference Management Evaluation 303
11.6.2. Future Work 304
References 305

12. The Buffer Delay Correction Algorithm for VoIP Communication 311
12.1. Background 311
12.2. Theatrical Aspects of De-Jitter Buffer 314

12.3. Buffer Delay Correction Algorithm (BDCA) 317
12.4. Implementation and Results 319
12.5. Conclusion 321
References 323

13. Opportunistic Max^2-Degree Network Coding for Wireless Data Broadcasting 325
13.1. Introduction 325
13.1.1. Motivation and Related Work 325
13.1.1.1. WDNC Based WBC 326
13.1.1.2. IDNC Based WBC 326
13.1.2. Contributions 326
13.2. System Model and Parameters 327
13.2.1. Mathematical Description 327
13.2.1.1. Signal Transmission 327
13.2.1.2. Signal Reception 328
13.2.2. Assumptions 328
13.3. The Proposed OM^{2}DNC Based WBC Protocol 329
13.3.1. OM^{2}DNC Strategy 331
13.3.2. Joint Network-RSC Decoding 333
13.4. Performance Analysis 334
13.5. Simulation Results 335
13.6. Conclusions 340
References 340

14. Analytical Model for Vehicular Mobility: A Microscopic Approach 343
14.1. Introduction 343
14.2. Communication Patterns 344
14.3. Information Dissemination 344
14.4. Vehicular Mobility Models 345
14.5. Network Architecture 345
14.6. Microscopic Analysis 347
14.6.1. Joint Poisson Spatial Distribution 347
14.6.1.1. Two-Lane Highway 347
14.6.1.2. K-Lane Highway 352
14.6.2. Conditional Probability of Number of Vehicles 354
14.6.2.1. Two-Lane Highway 354
14.6.2.2. Three-Lane Highway 354
14.6.3. Conditional Expected Number of Vehicles 355
14.6.3.1. Two-Lane Highway 355
14.6.3.2. Three-Lane Highway 356
14.6.3.3. K-Lane Highway 358
14.6.4. Tail Probability of Number of Vehicles 358
14.6.4.1. Two-Lane Highway 358
14.6.4.2. Three-Lane Highway 359
14.7. Conclusions and Future Work 359
References 360

15. USRP-based Implementations of Various Scenarios for Spectrum Sensing 363
15.1. Introduction 363
15.2. Theoretical Aspects 364
15.2.1. Energy Detection 364
15.2.1.1. System Model 364

15.2.1.2. Conventional Energy Detector *365*
15.2.1.3. Energy Detection with Uncertainty *368*
15.2.2. Eigenvalue Based Detection 370
15.2.2.1. Maximum-Minimum Eigenvalue (MME) Detection Method *371*
15.2.2.2. Energy with Minimum Eigenvalue (EME) Detection Method *372*
15.2.2.3. Cooperative Spectrum Sensing *372*
15.2.2.4. Soft Data Fusion *373*
15.2.2.5. Hard Decision Fusion *374*
15.3. Experimental Setup 375
15.3.1. GNU Radio 375
15.3.2. GNU Radio Blocks 375
15.3.3. Results 376
15.3.3.1. Simulation Results *376*
15.3.3.2. Experimental Results for Single Energy Detector *378*
15.3.3.3. Eigenvalue Based Spectrum Sensing *380*
15.3.3.4. Cooperative Spectrum Sensing Results *381*
15.4. Conclusions 387
Acknowledgements 387
References 387

Index 389

Contributors

Ulisses Rodrigues Afonseca
Instituto Federal de Goiás - Campus Luziânia, Luziânia-GO, Brazil,

Mahdi Aiash
Faculty of Science & Technology, Middlesex University, London, United Kingdom

Sandhya Armoogum
Dept. Industrial Systems & Engineering, University of Technology, Mauritius

Vimal Bhatia
Discipline of Electrical Engineering, Indian Institute of Technology Indore, India,

Jacir Luiz Bordim
Department of Computer Science, University of Brasília - UnB, Brasília-DF, Brazil,

Gean D. Breda
Faculty of Electrical and Computing Engineering, University of Campinas, Brazil

Robert H. Colson
Faculty of Science & Technology, Middlesex University, London, United Kingdom

Cherif Diallo
Laboratoire Algèbre, Cryptographie, Codes et Applications (ACCA),
UFR Sciences Appliquées et de Technologies (UFR SAT), Université Gaston Berger,
Saint-Louis, Sénégal

Dharmendra Dixit
Department of Electronics and Communication Engineering, The LNM IIT Jaipur, India,

Lucia Duricova
Tomas Bata University in Zlin, Faculty of applied informatics, Zlín, Czech Republic

Babak Honarbakhsh
Electrical Engineering Department, Shahid Beheshti University, Tehran, Iran

Robinson S. V. Hoto
Mathematics Department, University of Londrina, Brazil

Martin Hromada
Tomas Bata University in Zlin, Faculty of applied informatics, Zlín, Czech Republic

Motoi Iwashita
Chiba Institute of Technology, Japan

Atsushi Kanai
Hosei University, Japan

Tsutomu Konosu
Chiba Institute of Technology, Japan

Nagendra Kumar
Discipline of Electrical Engineering, Indian Institute of Technology Indore, India,

Aboubaker Lasebae
Faculty of Science & Technology, Middlesex University, London, United Kingdom

Jonathan Loo
Faculty of Science & Technology, Middlesex University, London, United Kingdom

Galia Marinova
Faculty of Telecommunications, Technical University, Sofia, Bulgaria

Shinsuke Matsui
Chiba Institute of Technology, Japan

Mehdi Mekni
Department of Computer Science and Information Technology, St. Cloud State University, St. Cloud, MN, USA

Leonardo S. Mendes
Faculty of Electrical and Computing Engineering, University of Campinas, Brazil

Nawaz Mohamudally
Dept. Industrial Systems & Engineering, University of Technology, Mauritius

Jan Mrazek
Tomas Bata University in Zlin, Faculty of applied informatics, Zlín, Czech Republic

Amor Nafkha
Centrale-Supelec SCEE, Avenue de la Boulaie 35576, Rennes, France

Nimal Nissanke
Dept. Industrial Systems & Engineering, University of Technology, Mauritius

Ali Raheem
Faculty of Science & Technology, Middlesex University, London, United Kingdom

Rand Raheem
Faculty of Science & Technology, Middlesex University, London, United Kingdom

Amir Masoud Rahmani
Department of Computer Engineering, Shahr-e-Qods branch, Islamic Azad University, Tehran, Iran

Camila Feitosa Rêgo
Department of Computer Science, University of Brasília - UnB, Brasília-DF, Brazil,

Fábio Sakuray
Computer Science Department, University of Londrina, Brazil

Hiroyuki Sato
The University of Tokyo, Japan

Yoshiaki Seki
Tokyo City University, Japan

Shigeaki Tanimoto
Chiba Institute of Technology, Japan

Zdravka Tchobanova
Faculty of Telecommunications, Technical University, Sofia, Bulgaria,

Jian Wang
Army Engineering University of PLA, China

Wei Xie
Army Engineering University of PLA, China

Kui Xu
Army Engineering University of PLA, China

Tiguiane Yélémou
Polytechnic University of Bobo-Dioulasso, BP 1091, Bobo-Dioulasso, Burkina Faso,

Mani Zarei
Department of Computer Engineering, Shahr-e-Qods branch, Islamic Azad University, Tehran, Iran

Dongmei Zhang
Army Engineering University of PLA, China

Preface

Networks are everywhere, from the Internet to sensor networks. They are used widely for various type of communications. Their safe existence and functioning need deep consideration of different security aspects. It was the reason to combine these three topics such as Networks, Communication and Security in one book volume.

Every research and development must be started from a state-of-the-art review, and networks, security and communication are not an exception. The review is one of the most labor- and time-consuming parts of research. It is strongly necessary to take into account and reflect in the review the current stage of development, including existing technologies, security aspects and hardware. Many PhD students and researchers working in the same area are doing the same type of work. A researcher must find appropriate references, to read it and make a critical analysis to determine what was done well before and what was not solved till now, and determine and formulate his future scientific aim and objectives. The professionally made state-of-the art must take into account not only open access books, articles and conference papers available online for free, but also traditional monographs and journal articles, which are available only off-line and in print (paper) format.

After very successful publication of our popular Book Series on "*Advances"* from different technical areas in 2012-2017, it was decided to start publication of new Book Series on '*Advances in Networks, Security and Communications: Reviews'*.

It is my great pleasure to present the 1st volume of Book Series titled '*Advances in Networks, Security and Communications: Reviews*' started by the IFSA Publishing in 2017. The volume is published as an Open Access Book in order to significantly increase the reach and impact of this Book Series, which also published in two formats: electronic (pdf) and print (paperback).

The 1st volume of new Book Series contains fifteen chapters submitted by 42 contributors from academia and industry from 13 countries: Brazil, Bulgatia, Burkina Faso, China, Czech Republic, France, India, Iran, Japan, Mauritius, Senegal, UK, and USA. The book is devided into three main parts: Networks (four chapters), Security (four chapters) and Communication (seven chapters). '*Advances in Networks, Security and Communications: Reviews*' provides focused coverage of these three main technologies. It explores practical solutions to a wide range of network, communication and security issues. Chapters are written by experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise. Coverage includes wireless sensor network routing improvement; connectivity recovery, augmentation and routing in wireless Ad Hoc networks; advanced modeling and simulation approach for the sensor networks management; security aspects for mobile agent and cloud computing; various communication aspects (algorithms, coding and hardware design) and others.

Every chapter of this book is independent and self-contained. Fifteen chapters of the book have the similar structure: introduction, state-of-the art, description of advances and list of well selected references, including books, journal articles, conference proceedings and web sites.

This book ensures that our readers will stay at the cutting edge of the field and get the right and effective start point and road map for the further researches and developments. By this way, they will be able to save more time for productive research activity and eliminate routine work.

This book will be a valuable tool in both learning how to design various networks, as well as a reference as an advance in readers' research careers.

Dr. Sergey Y. Yurish

Editor
IFSA Publishing *Barcelona, Spain*

Networks

Chapter 1
WSN Routing Improvement Techniques

Dr. Chérif Diallo

1.1. Introduction

The topics in this chapter detail the structure of sensor devices which are utilized to form wireless sensor networks (WSNs) intended to be used for many applications in various fields. We will be particularly interested in improving the efficiency of routing mechanisms, as well as the impact of securing the routing process.

In a wireless sensor network (WSN), energy efficiency of routing protocols is of primary importance. Embedded with local load balancing mechanisms, the studied L2RP protocol is a Link Reliability based Routing Protocol which aims to help source nodes to exploit the potential capabilities of their respective neighbours. As it is a reliability-oriented protocol, L2RP discards unreliable links to avoid the substantial energy cost of packet losses. We will detail some performance evaluation results to show major efficiency benefits that stem from load balancing which helps in lengthening the network lifetime while minimizing packet losses. In WSN, the choice of a routing protocol and its key parameters depends on the nature of the application and on its primary mission. Lot of works addressed routing issues with more or less effectiveness, some of which pointed out the use of the link quality indicator (LQI) as a route selection criterion (metric). In a previous work, following an experimental study, we have shown, under some conditions, the inefficiency of the LQI based routing.

In this chapter, we propose through L2RP a simple way to improve reliability and efficiency of the LQI based routing in WSN. We also give a comparative study of several metrics including new definitions of LQI based metrics. The performance evaluation results show that our adaptation of the LQI metric is among the best route selection criteria regardless of the performance criterion under consideration [1-3]. Finally, as security has become critical for these networks too, we address in the last part the problem of the additional energy cost induced by solutions used to secure the routing process [4].

Dr. Chérif Diallo
Laboratoire Algèbre, Cryptographie, Codes et Applications (ACCA),
UFR Sciences Appliquées et de Technologies (UFR SAT), Université Gaston Berger, Saint-Louis, Sénégal

1.2. Architecture of a Wireless Sensor Node

A sensor node Fig. 1.1 is mainly composed by four basic units: the sensing unit, the processing unit, the wireless transceiver unit, and the power unit. It can also contain, in accordance with its domains of application, supplementary modules such as a Global Positioning System (GPS) or an energy generator system (solar cell or photovoltaic). There are also sensors, more voluminous, equipped with a mobility system responsible for moving the node in case of need.

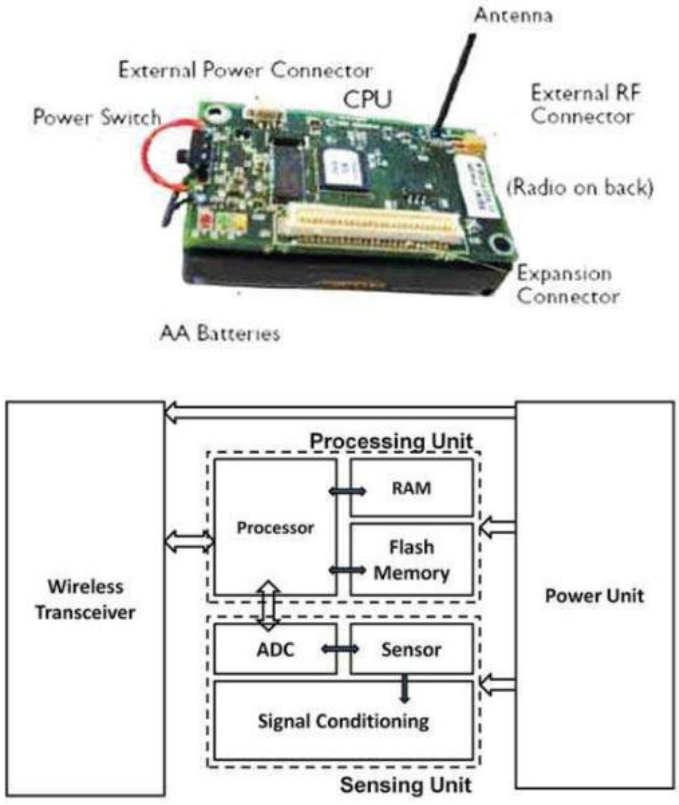


Fig. 1.1. A sensor node and its main units.

1.2.1. The Sensing Unit

The sensing unit is a device transforming the state of an observed physical quantity into a human known quantity such as electrical voltage, luminous intensity or temperature. It is distinguished from the measuring instrument by the fact that it is merely a simple interface between a physical process and manipulable information. The sensing unit is generally composed by two subunits: The sensor itself and the analog-digital converter (ADC) which is responsible for converting the original signal based on the observed phenomenon. ADC transforms these signals in digital signals understandable by the processing unit.

The sensor is characterized according to several criteria. The most common are: the observed physical quantity (light, temperature, noise, humidity, etc.), its transmission range, its sensibility and its functioning temperature range. To use a sensor probe in the best condition, it is often useful to practice a calibration in order to know the uncertainly of measures provided.

1.2.2. The Processing Unit

It includes a processor generally associated to a small storage unit. It works with an operating system specially designed for the sensor (for example: TinyOS). It executes the communication protocols which make it possible to send data to the other nodes of the network, to receive data, and to participate in many network operations such as auto-configuration, auto-organization, clustering process, routing computation, data aggregation and security mechanisms.

1.2.3. The Wireless Transceiver Unit

It carries out all the transmissions and receptions of data on a wireless media. It may be of the optical type (like in the smart dust node), or of radio-frequency type:

- The optical type communications can prevent from electrical interferences. Nevertheless, it's not possible to establish links through the obstacles. Such sensor devices have the disadvantage to requiring a permanent sight of view between the communicating entities.

- The radio-frequency unit transmission types include modulation circuits, demodulation, filtering and multiplexing. This implies an increase in the complexity and cost of the sensor manufacturing.

Designing radio-frequency transmission units to enable large communication range with low energy consumption capabilities is an exciting challenge because powerful signals often consume more energy. An alternative could consist generally to use long antennas, but it is not possible in the domain of wireless sensors because of the small size of the devices.

1.2.4. The Power Unit

A sensor device is provided with an energy source (generally a battery). Considering its small size, this energetic resource is limited and generally not replaceable. What often makes the energy the most precious resource of a sensor network, because it directly affects sensor nodes lifetime and so the entire lifetime of the network. Consequently, the energy control unit constitutes an essential system. It must distribute the available energy to the other modules, in an optimal way, for example by reducing the useless spending by putting components on (deep) sleep mode. This unit can also handle the energy loading systems from the environment via photovoltaic cells for instance.

1.3. The Offer of Sensor Manufacturers

The double protocol stack Bluetooth / ZigBee are among the best standards to be exploited in wireless sensor networks. Bluetooth is a specification of telecommunication industries. It uses a short-range radio technology in order to simplify the connexions between the electronic devices. Initiated in 1994 by Ericsson, The Bluetooth technique has been standardized under the standard IEEE 802.4.15 and it is destined to the creation and the maintain of Personal Area Network (PAN). Such a network is used for the transfer of low data bandwidth and low transmission range between compatible devices. Unfortunately, the big drawback of this technique is its high energy consumption and therefore can not be used by sensors that are powered by non-replaceable battery and that ideally should work without outage for several years.

The standard ZigBee [5] combined with the IEEE 802.15.4 offers features that respond even better to sensor networks needs in terms of energy network saving. ZigBee offers also lower data rates, but it also consumes significantly less than Bluetooth. A small rate of data is not handicapping for a sensor network where the transmission frequencies are not important. Nevertheless, the current tendency of the manufacturers is to use proprietary techniques which have the advantage of being specifically optimized for a specific use, but which have the big drawback of not being compatible between them.

From a hardware point of view, some new techniques will considerably influence the future of the wireless sensor networks. The UWB (Ultra Wide Band) technique is a good example for that. This transmission technique will allow reaching extremely low consumption levels thanks to its simplicity at materiel level.

Moreover, the attenuation of the generated signal by obstacles is lower compared to conventional narrow-band radio systems.

From a software point of view, the field of wireless sensors is therefore moving towards a great rise and many new products continually flooding the sensors market every year. All the more, open-source techniques are now largely used, such as TinyOS [6]. This last one was developed at the University of Berkeley. TinyOS [6] is an open-source operating system designed for wireless sensors and which is used by more than 500 Universities and academic research centers in the world. The realization of programs on the platform is done exclusively in NesC (dialect of the C programming language). The main particularity of this OS is its extremely small size in terms of memory (some kilobytes).

In the following, we review some main devices provided by few sensor manufacturers.

1.3.1. The Tmote Sky of Moteiv

Specifically designed for promoting a rapid deployment of prototypes, the Tmote Sky sensors of Moteiv [7] are adapted to many industrial applications in the fields of light, humidity and temperature control (Table 1.1). These sensors are often equipped with an integrated antenna covering 50 m indoor transmission range and 125 m outdoors. They

are also accompanied by a USB interface to enable interoperability with other devices and peripherals.

Designed with the native support of TinyOS [6], the Tmote Sky sensors of Moteiv offer the advantage of developing innovative technologies related to wireless protocols while also benefiting from the open source software capabilities (Fig. 1.2).



Fig. 1.2. Tmote Sky sensor.

1.3.2. Sun SPOT from Sun Microsystems

Sun SPOT [8] (Sun Small Programmable Object Technology) is a Mote based wireless sensor network developed by Sun Microsystems. This device is based on the IEEE 802.15.4 standard. Contrarily to the others available Mote systems, Sun-SPOT is make on the Java Squawk virtual machine.

The first limited series of Sun-SPOT development kits was launched since April 2007. These first introductive kits have two sensors, one base station, the software development tools and a USB wire. The software is compatible with Windows XP, Mac OS X 10.4, and most common Linux distributions. The SunSPOT sensor node is shown in Fig. 1.3.



Fig. 1.3. SunSPOT sensor node.

Another SunSPOT project is the hardware and software platform developed by Oracle Labs [8]. This project was created to encourage the development of new applications and devices. It is designed from the ground up to allow programmers who never before worked with embedded devices to think beyond the keyboard, mouse and screen and write programs that interact with each other. A Java programmer can use standard Java development tools such as NetBeans to write specific codes [9].

The whole project (hardware, operating environment, java virtual machine, drivers and applications) is available as open source materials.

1.3.3. The WiEye of EasySen

Developed by EasySen, WiEye [10] is a set of modular cards for wireless sensor network applications that meet the needs of professional surveillance and security. The device is based on the IEEE 802.15.4 standard and is particularly adapted to the detection of presence and movement of individuals and/or vehicles. Composed by several sensing units Fig. 1.4, the WiEye components are designed as complementary modules to be connected to the other sensor devices such as Tmote Sky for instance Fig. 1.4.



Fig. 1.4. Illustration of a WiEye sensor node.

1.3.4. The Micaz Mote of Crossbow

The Crossbow Company proposes a hardware system [11] including the process unit (processor and storage), the energy control unit and the transmission unit, which insure data sending to the base station. The Micaz Mote of Crossbow Fig. 1.5 is equipped with a connector allowing the integration of different sensing units.

The MICAz is a 2.4 GHz Mote module used for enabling low-power wireless sensor networks and it is intended for Indoor Building Monitoring and for Security purposes. It enables acoustic, video, vibration and other high speed sensor data applications (Table 1.1). Such devices can also operate in large scale wireless sensor networks including more than one thousand (1000+) nodes [12].



Fig. 1.5. Micaz mote sensors provided by Crossbow.

1.3.5. Jennic Sensors

Equipped with a 32-bit RISC processor, Jennic [13] solutions are designed for both home automation and industrial applications (Fig. 1.6). Characterized by their very low power consumption (Table 1.1), which ensures a long battery lifetime, they specifically target the areas of location, telemetry, remote control, toys and gaming peripherals.



Fig. 1.6. Sensor development kit provided by Jennic.

Based on the well-established IEEE 802.15.4 standard and a 2.45GHz low power radio technology, it adds the self-healing JenNet tree networking stack, the IETF 6LoWPAN IP layer and "JIP", a powerful and flexible application layer enabling interoperability between devices. It is initially targeted at Lighting and Home Automation systems where it is rapidly becoming established as the system of choice, with provision for many different types of devices, all connecting to the same wireless network.

With this solution, every device in the home can have its own IPv6 address, turning the home into a simple extension of the internet and enabling new and exciting innovations to be created in home controls and energy management (IoT, Internet of Things).

The JenNet-IP-EK040 evaluation kit provides all the components needed to allow developers to create these new applications: domestic lighting control, home automation (heating and ventilation control, energy management, access control, blind and window control), building automation (HVAC, access control, security, fire detection and alarm), commercial and outdoor lighting, security systems, etc. [14, 15].

Table 1.1. Main features of some wireless sensors.

	Tmote SKY	**Sun SPOT**	**Crossbow**	**Jennic**
Processor	8 MHz Texas Instruments MSP430	180 MHz 32 bit ARM920T core	MICAz ZigBee Series (MPR2400)	Low power 32bit RISC CPU, 4 to 32MHz clock speed
Data capacity	10 Kb RAM, 48 Kb Flash	512 Kb RAM 4 Mb Flash	4 Kb RAM 512 Mb Flash	128 Kb RAM 128 Kb Flash
Wireless radio	2.4 GHz IEEE 802.15.4 Radio 250 kbps, High Data Rate Radio	2.4 GHz IEEE 802.15.4 Radio	2.4 GHz IEEE 802.15.4 Radio 250 kbps, High Data Rate Radio Outdoor transmission range 150 m	2.4 GHz IEEE 802.15.4 Radio Transmission power 2.5dbm
Sensing feature	Temperature, Humidity, Light	Accelerometer, Temperature, Light	Temperature, Humidity, Light, pressure, acoustic activity, video, seismic movements, magnetic	Temperature, Humidity, Light
Energy	2 AA batteries, 21-23 mA (reception) 19-21 mA (transmission) 5-21 μA (deep sleep mode)	750 mAh Lithium-ion, 3.7 V rechargeable battery 30 μA (deep sleep mode)	2 AA batteries 25 mA (transmission) 15 μA (deep sleep mode)	2 - 3.7 V battery 17.5 mA (reception) 15.0 mA (transmission) 1.25 μA (deep sleep mode)

1.3.6. Other Commercial Applications

There are several other commercial products available on the sensor market:

- ShockFish SA, now Spotme, offers the TinyNode devices Fig. 1.7. Composed of sensors and modular cards for industrial applications [16], this offer is accompanied

by a range of products intended to academic research and is also compatible with TinyOS [6].



Fig. 1.7. ShockFish, BTnode and Silicon Labs products.

- The T-Node products, G-Node and L-Node [17] from SOWNet Technologies are few responses to the several specific needs of academic research and sensor network application developers. This Dutch company offers several TinyOS compatible development kits, allowing easy integration with open source products. It also offers a monitoring application for museums and art objects, which uses remotely managed sensors to provide discrete (invisible) and individual monitoring of each art piece in a museum.

- The Tinynode 584 is an ultra-low power OEM module that provides a simple and reliable way to add wireless communication to sensors, actuators and controllers. The Tinynode evaluation kit contains everything you need to get started. The kit ships with a full TinyOS environment along with demo applications and protocol software [18].

- The BTnode rev3 provides a distributed environment for prototyping Ad Hoc networks and supports different sensor add-ons using the IO provided on the extension connector J1 and J2. There are different UART, SPI, I2C, GPIO, ADC available. The J2 is suitable for prototyping, as you don't need to make a PCB or solder anything. Just connect you sensor(s) to appropriate IO lines. The J1 is suited if you need more IO lines and/or are going to produce sensor boards that can just be plugged in [19].

- Silicon Labs [20] and Microchip [21] solutions are ZigBee-compatible offerings for both industrial applications and academic research.

As we can see, given the enthusiasm of researchers for wireless sensors, the number of manufacturers has increased enormously in recent years to provide concrete answers to both industrial and academic needs.

1.4. Wireless Sensor Network Architecture

1.4.1. Wireless Sensor Network Architecture

A Wireless Sensor Network (WSN) Fig. 1.8 consists of a set of nodes deployed in a given environment (target) for accurate application (temperature, pressure, control, monitoring, intrusion detection, air humidity, agriculture, home automation, medical field, etc.). The sensors communicate with each other to relay information to a Sink node that communicates with the user interface.

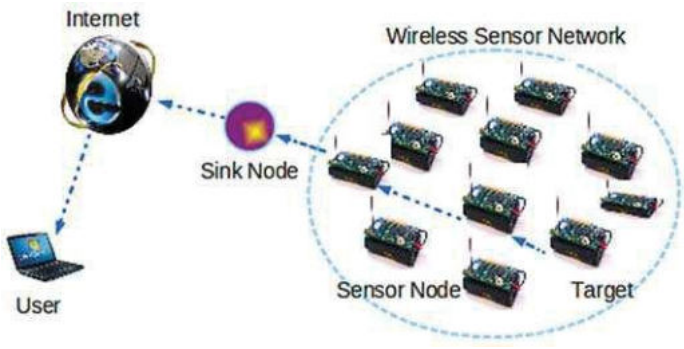


Fig. 1.8. Illustration of a wireless sensor network [22].

A WSN is therefore composed of a number of autonomous sensors capable of collecting and collaborating together to transmit environmental data. The position of these sensors is not necessarily predetermined. They may be randomly dispersed in a geographic area, known as coverage area or target area.

The data collected by the sensors are routed via multi-hops routing to a node considered as a collection point, called a sink node. From the processing center, the user connects to

the Sink using Internet infrastructure or a satellite communication system or other telecommunications systems. The user can, via the Sink, send requests to the other sensors of the network specifying the type of data required and collect and then analyze the events recorded by the sensors in the coverage area.

Wireless sensor networks are designed to collect information related to some events in hostile environments where human presence is not often possible. That is why we consider that once they are deployed, the sensors are autonomous. Their lifetime tightly rely on the manner of their batteries are utilized during network operations. Then, the most critical feature in sensor networks is the hardship of its energy resources because each sensor node has initial low resources in terms of energy and it's not often possible to replace batteries during network operations. That is why it is important to take into account the energy consumption factors when designing wireless sensor networks.

1.4.2. Energy Consumption Factors in WSNs

1.4.2.1. Collisions

Collisions are the primary source of energy loss. When two frames are issued simultaneously and then collide, those become unusable and must be retransmitted. In the same manner, when a node simultaneously receives two packets which have not necessarily been sent at the same time or which have been transmitted by two nodes out of reach one from the other. These two cases require retransmission of frames. MAC protocols, like CSMA, are trying in their own way to avoid collisions in order to backup network performance by reducing packet retransmission.

1.4.2.2. Idle Listening

"Idle listening" or "empty Listening" occurs when listening to the radio channel to receive contingently any data. Its energy cost is particularly high. Many MAC protocols always listen to the channel to the active state, assuming the entire device would be turned off by the user if there is no data to send. The exact cost of the idle listening depends on the hardware radio and on the operation mode. Turning off the radio channel is a solution; nevertheless the cost of the transition between different modes (sleep/deep/active) also consumes energy. Then the frequency of transition between modes must be reasonable when designing protocols.

1.4.2.3. Overhearing

Another common cause of excessive energy consumption is "overhearing". This occurs when a node hears packets that are not destined for it. The cost of "overhearing" can be an aggravating factor of energy losses especially when traffic or node density is notably high during network operations.

1.4.2.4. Overmitting

Overmitting occurs when a source node sends data to a destination node which is not ready to receive. Moreover, if the transmitting node is waiting for an acknowledgment (ACK) from the destination node, it then retransmits the same packet several times because it remains in transmission mode (pending receipt of the eventual ACK frame). This could lead to high energy losses.

1.4.2.5. Control Packets Overhead

Some media access control techniques use specific packets (RTS, CTS) for collision avoidance. Running a network protocol still needs few control packets and necessary headers to encapsulate application data. Sending, receiving, and listening to the control packets consume more energy. As control packets do not carry user data directly, those also reduce the overall effective throughput of the network.

1.4.2.6. Network Protocols

The most protocols designed for network auto-configuration and/or organization, such as routing and clustering algorithms, are also energy consumption factors. Indeed, routing and clustering schemes often involve various message exchanges between sensors before a node processes its routing table or data aggregation operations.

1.4.2.7. Attacks and Security Issues

Many attacks are carried out against the sensor networks in order to exhaust the batteries of the nodes and then to reduce their lifetimes, and consequently that of the network. For instance, with a very high power transmitter node, an attacker can perform Hello Flood attack by broadcasting Hello messages on a large range transmission to some sensors of the network. Then sensors will try to respond to the attacker node which is actually out of range. In such a case, an attacker uses this mechanism to cause energy exhaustion in the hacked network.

1.4.2.8. Cryptography and Security Solutions

Security mechanisms, including cryptography, are aggravating factors of energy consumption in sensor networks. Many works are concerned with the establishment of cryptographic keys without worrying about key lengths. This is the strong point of cryptographic algorithms for wired networks. However, this becomes a major disadvantage in wireless sensor networks where the safeguarding of energy is a sine qua non condition for longer node network lifetime. Moreover, adding integrity key to secure routing protocol exchanges should increase packet size and therefore energy expenditure. In the Section 1.11, we will try to estimate how, that’s to say in what proportion, adding an integrity key will cause energy exhaustion.

1.5. Application Domains of Sensor Networks

The fast evolution of wireless communication media in recent years, the miniaturization, and the low cost of sensor components have enable emergence of large innovative applications of sensor devices (thermal, humidity, optical, vibration, etc.). Sensor networks could also revolutionize the way we understand and build complex physical systems, especially in the military, environmental, domestic, health, security, and so on.

1.5.1. Military Applications

The military domain is, as in the most cases of several technologies, a precursor for the development of sensor network applications. The rapid deployment, the reduced cost, the self-organization and fault tolerance of sensor networks are characteristics that make this type of network an appreciable tool in such a field. A WSN deployed in a strategic sector which is often difficult to access, allows for example to monitor all movements (friends or enemies), or to analyze the ground (detection of chemical agents, biological or radiation) before sending troops.

1.5.2. Security and Safety Related Applications

Sensor networks enable real-time monitoring of aircraft, ship, automotive or metro structures, as well as electrical and gas supply and distribution networks. A WSN designed for movement or noise detections can constitute an intrusion detection system in an industrial site or a critical sector. With WSN, it would not be so simple to defeat such a system, since there is no critical point. Prevention of accidents by monitoring roads or railways is one of the envisaged applications of wireless sensor networks.

The evolution of seismic movements, alterations in the structure of a building, a road, a wharf, a railway, a bridge or a hydroelectric dam (following an earthquake or aging) could be detected by sensors. Some sensors that activate only periodically can work for years or even decades.

Another potential area of sensor application use is safety. Experts agree that terrorist threats in the future will be exerted in particular through maritime transport. The cargo containers could thus be monitored and located with sensor devices. The presence of explosives, conventional or nuclear, or even human beings in these containers could be also detected. Consequently, it becomes possible to avoid potential terrorist attacks on cargo ships (90 % of the world's trade passes through the ocean and 200 million containers pass through each year).

1.5.3. Medical Applications

Monitoring the vital functions of a living organism can be facilitated by small sensors swallowed or implanted under the skin. Capsules in the form of sensors or small cameras that can be swallowed already exist and allow, without using surgery, to transmit images

from the inside of a human body. A recent study presents sensors that can function in the human body for the treatment of certain diseases. The monitoring of blood glucose, the monitoring of vital organs or the early detection of certain cancers are intended biomedical applications. Sensor networks would also allow for real-time monitoring of motherhood (detection of babies) or patients.

1.5.4. Environmental Applications

The detection of movements of birds, small animals or insects is one of the possible environmental applications of wireless sensor networks. Thus, it becomes easier to observe the bio-diversity, without disturbing vulnerable animal species, and to propose more effective solutions for the conservation of the fauna and the flora. Thanks to sensor networks, it is also possible to detect environmental problems such as pollution, forest fires and the possibility of assessing the rate of pesticides in water. On industrial sites, such as nuclear or oil tankers, sensors can be deployed in a network to detect leaks of toxic products (gas, chemicals, radioactive elements, petroleum, etc.) in real time in order to alert the users and to enable more rapidly effective intervention.

1.5.5. Commercial Applications

In the field of trading, sensor networks could be used to improve the storage and the delivery process (in particular, as a cold chain monitoring system). Thus, the created network may be used to determine the position, condition and direction of a package, pallet or cargo. Manufacturers, via sensor networks, could follow the production process from the raw material to the delivered product.

In buildings, the home automation system of heating and air conditioning, lighting or water distribution could optimize its efficiency thanks to small sensors. Used on a large scale, such applications would help in reducing global energy demand and indirectly emissions of greenhouse effect gas. For USA, this economy is estimated at around $55 billion per year, with a decrease of $35 million tons of carbon emissions [23].

1.5.6. Cold Chain Monitoring System

1.5.6.1. Issues and Challenges

The cold chain monitoring domain and, more generally, the monitoring of the storage temperature of foodstuffs is becoming increasingly important in the economies of industrialized countries. It concerns frozen products, fishery products, fruit and vegetables but also, and increasingly, pharmaceutical products, vaccines and other biotechnology products. At the same time, the health problems caused by non-compliance with storage conditions are increasing. According to a report published in 1999, the non-respect of the compliance conditions of the cold chain would cause in the United States: 76 million poisonings; 325,000 hospitalizations; and 5,000 deaths per year. That is why the European Community has responded to this social problem by introducing new instructions on the

transport of frozen products (Directive 92/1/EEC) requiring the automatic recording of air temperature in the various stages of the transport (vehicle and warehouse), using fixe devices. However, these devices provide only partial response to the problem because the ambient storage temperature is not necessarily the temperature of the monitored product, and they do not allow control during the loading / unloading phases, where the non-compliance incidents are more likely to be happening Fig. 1.9.

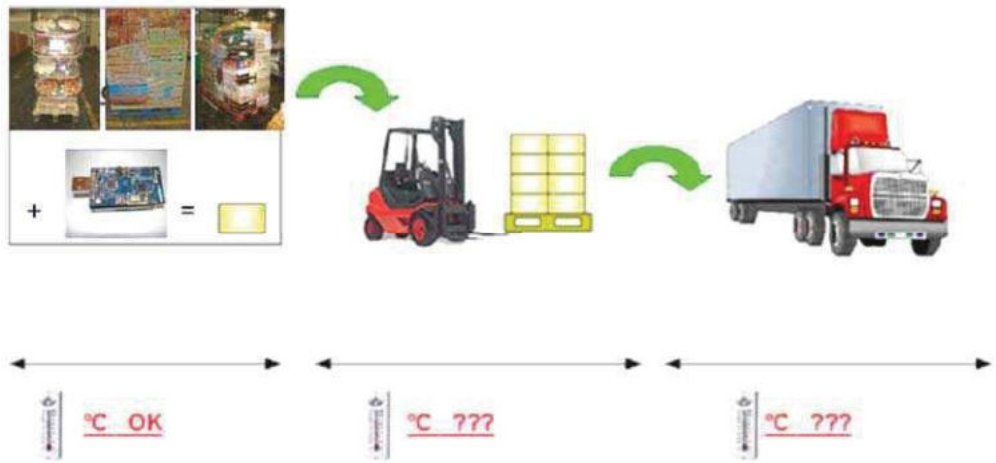


Fig. 1.9. Issues and challenges of a cold chain monitoring system.

Some solutions have been proposed to measure the temperature of the product, or at least its packaging, and throughout the transfer period between the place of manufacturer and the retail outlets. For the monitoring of positive temperatures (storage of fruits and vegetables for example), chemical indicators have been proposed which change their appearance irreversibly when a threshold is exceeded. The transposition of these devices to negative temperatures comes up against many difficulties. The only product of this type that we know consists of labels that become invisible when the cold chain has been broken for a predetermined time. In addition to a delicate implementation, since the labels once manufactured must always be kept below the threshold temperature, this system does not in practice allow intermediate control of the products during their routing. Indeed, no actor in the cold chain can afford to visualize each label when he receives a product and before sending it to the next actor. Thus, only the end user has the knowledge of whether or not the cold chain is respected, which raises the problem of the precise designation of the company responsible for the rupture.

Consequently, the actors in the chain have currently measurements in different regions of a warehouse or in a truck. The consequence of the detection of an incident in a part of the warehouse or in the truck is the destruction of products located in that region or in that truck. For one-off measurement campaigns to qualify a chain, there are portable recorders placed in or near packaging, but these are relatively bulky and costly and are not designed for systematic and extensive use ladder. Indeed, the systematic exploitation of portable temperature recorders encounters a number of problems and constraints. Such solutions

are not suitable for intermediate checks because they have to be connected to a portable reader by a wired link.

This means that these recorders must be located. The cold chain monitoring system implemented by wireless sensor networks aims to solve these different problems. Since recording sensors can communicate wirelessly via a network of sensors, it becomes possible to interrogate a large number of them in a warehouse from a single reading station without having to locate them. Since multiple reading points having Internet connection could be positioned at different storage locations, it becomes possible from a central station to follow the entire logistic chain of the goods and to be warned of any problem in real time. Finally, integrating sensors with transport bins or pallets solves the problem of logistics because there is already a whole activity of leasing and recovery of these packaging elements. The potential market for these devices is important. In addition to the frozen food market, which has millions of pallets per year in the world, fresh products and fisheries, applications in other areas can be considered. For the transport of fragile products, they may be equipped with shock or moisture sensors instead of temperature transducers.

1.5.6.2. Needs and Operating Principles

As part of a cold chain monitoring application, each sensor is associated with a pallet: it records the temperatures as well as it transmits information. The sensors communicate with each other, and then with the base station which sends or receives data from the central server. In addition, an operator can communicate directly with a specific sensor, using a portable terminal, in order to initialize it, identifying, and retrieving, recording or modifying stored information. The data transmitted to the server are then stored in a database. All phases of supply chain is shown in Fig. 1.10.

- ***Phase 1:*** The operator targets the sensor attached to a pallet with a portable terminal in order to empty it of the previous information.

- ***Phase 2:*** The operator places the goods on the pallet. The pallet thus created is associated with an order number and / or pallet reference in the WMS (WMS for Warehouse Management Software) of the supplier. The operator again targets the sensor in order to assign this number to it, then, depending on the nature of the products, he adjusts the temperature according to predetermined approach and exceedance temperature thresholds. Depending on the wishes of the supplier, the operator can send the product data (barcode product, or pallet contain, deadline for sale, etc.) to the sensor. Finally, the operator enables the sensor to operate in networking and then start recording the temperatures.

- ***Phase 3:*** The pallet is placed in stock at an identified location. If during this period the temperature level drops or increases so as to exceed one of the set thresholds, then the sensor sends an alert to a base station (phase 7).

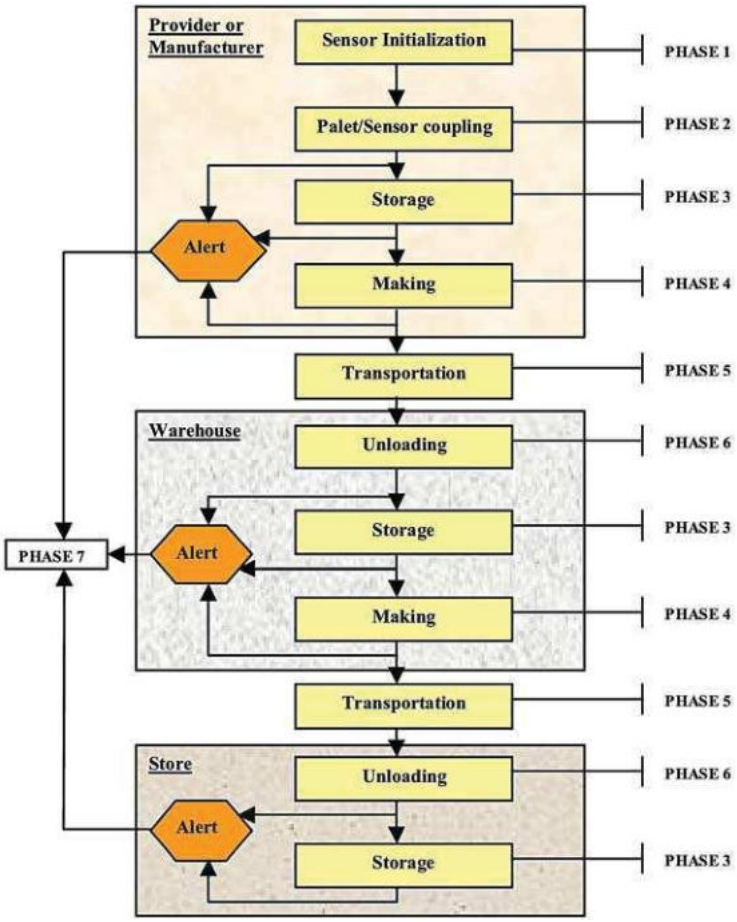


Fig. 1.10. This diagram shows operations carried out on a supply chain.

- ***Phase 4:*** The complete pallet is taken to the preparation area. If during this period the temperature level drops or increases so as to exceed one of the set thresholds, the sensor sends an alert to a base station (phase 7).

- ***Phase 5:*** The pallet is loaded into a truck and routed to the destination logistics platform. During this period, the sensor loses contact with the sender's base stations. If one of the temperature thresholds is reached, the sensor waits to reconnect to the next base station before sending an alert (except, of course, if the truck is equipped with a base station).

- ***Phase 6:*** The pallet is unloaded. If there has been a temperature incident during transportation, the sensor sends the alert as soon as it reconnects to a base station (phase 7). Similarly, if during the unloading phase and waiting for stocking the level temperature decreases or increases so as to exceed one of the thresholds, the sensor sends an alert to a base station (phase 7).

- ***Phase 7:*** The operator recognizes the sensor of the pallet that issued the alert thanks to its portable terminal. It verifies the data recorded by the sensor and controls the pallet. Then, only it takes the appropriate treatment measures.

1.6. Routing Mechanisms for WSN Cold Chain Monitoring System

1.6.1. Introduction

Designing a cold chain monitoring application requires special focus on at least two main phases. In [24], we presented an example of sensor network for cold chain monitoring where sensors are inside pallets. We proposed energy efficient protocols for the transport phase in which the WSN is deployed in trucks with no Base Station (BS) because it would be very expensive to install and maintain Base Stations within each truck. There are a few sensors in the truck.

The second phase concerns the product storage in a warehouse where each pallet is handling temperature sensor. This application specifically collects rare events (alarms) to ensure the proper monitoring of the system. If the temperature is over a threshold, an alarm will be generated; this “interesting event” is then sent towards the BS. Due to the size of a warehouse which hosts large number of pallets, one upon the other, the WSN can reach several hundreds of sensors which collaborate for sending data towards the BS. So, in this environment, the link quality is a key parameter which has many effects on the network performance.

In [25], we used up to 50 Moteiv Tmote Sky [7] sensors, in a small experimental platform, including a 2.4 GHz ZigBee [8, 26] wireless transceiver (chipcon′s CC2420) [27]. On each packet reception, the CC2420 calculates the error rate, and produces a LQI value. To conduct experiments, we used the multiHopLQI routing algorithm [28] along with the Sensornet Protocol (SP) implementation [29]. In this algorithm, nodes sense and send "interesting events" to the BS. Based on the acknowledgement, a sensor decides to retransmit the data or not. If the acknowledgement fails, the sensor selects another node and routes data towards the BS. Under these conditions, the experimental results pointed out that the LQI based routing could have negative effects on the network performance [25].

After all, we think that the link quality might be a key parameter which some routing protocols could rely on in order to increase the network performance. Several works address WSN routing, but only few papers are related to the LQI based routing protocols. Sensors are characterized by their low energy level. Thereby load balancing traffic between different nodes, is also an essential idea to increase the lifetime of nodes and thus of the network. Our work addresses this challenge: improving the LQI based routing protocol by load balancing traffic over multiple paths.

The link quality indicator (LQI) is defined in the IEEE 802.15.4 standard [8, 26] as a measurement of the quality of packet reception between two nodes. The IEEE 802.15.4

standard does not specify the implementation of LQI, which is up to the radio manufacturer. Several works address WSN routing, but only few papers are related to LQI based routing protocols. Sensors are characterized by their low energy level. Thereby load balancing traffic between different nodes, is also an essential idea to increase the lifetime of nodes and thus the network. This work addresses two challenges: improving LQI based routing protocol by load balancing traffic over multiple paths.

When a sensor has to send data towards the Base Station, the load balancing routing consists to elect several nodes as next hop routers depending on the order of packet transmissions and the nodes previously used as the next hop routers. The idea is to involve several sensors in the routing effort to minimize the overall energy consumption and then extend the network lifetime.

The metric is a property of a route in computer networking consisting of any value used by routing algorithms to determine whether one route should perform better than another. Commonly, the route with the lowest metric is the preferred route. However, in this chapter, a metric means the local value associated with a node: for a source node, the highest value, in its neighborhood, may lead to the selection of such a node as the next hop router. For instance, the remaining energy level can be used as a metric to promote the selection of the highest powered nodes as next hop routers.

In this chapter, we propose WSN local load balancing routing mechanisms using the Wait and See (WaS) protocol [24] by comparing the following metrics: the remaining energy level, the degree of connectivity (number of neighbours), the sensor proximity with respect to the Base Station, the link quality indicator (LQI), and a hybrid metric composed of any pairs of these metrics.

The sensor networks are characterized by low energy constituting their batteries. Then energy consumption and some other performance criteria such as the Load Imbalance Factor (LIF), the average path lengths, the network lifetime and the packet loss percentage are taken into consideration to evaluate the effectiveness of routing mechanisms.

Definition of an "Achtophorous Node": we focus on homogeneous WSN where all sensors are participating together in the routing effort. Since all nodes are routers, we prefer using the term "achtophorous node" derived from Greek term ***αχθοφορεω*** which denotes "node handling heavy load". *For each node having data to send, its achtophorous nodes are its next hop sensors which handle the load due to the routing of its packets towards the BS. Each sensor selects among its neighbours one or more achtophorous nodes.* We will also examine the influence of increasing the number of the achtophorous nodes on the routing efficiency. The WSN deployed in a warehouse is pruned to the unreliability feature of the wireless links. Then, we present results pertaining to unreliable links impacts on the network performance.

The rest of this chapter is organized as follows. After presentation of a short background in the next part, the next one gives some topics on studied metrics. Then, we describe load balancing mechanisms and the proposed L2RP routing protocol before presenting a

detailed report of L2RP performance evaluation. Finally, the last part presents the energy over-consumption induced by securing the protocol.

1.6.2. Backgrounds and Related Works

Commonly used by the TinyOS community, MultihopLQI is a routing protocol which employs the cost-based paradigm defined in [30]. Link estimation is viewed as an essential tool for the computation of reliability-oriented route selection metrics. In MultiHopLQI, the link metric is the Link Quality Indicator (LQI) which is used additively to obtain the cost of a given route. MultihopLQI avoids routing tables by only keeping state for the best parent at a given time, drastically reducing memory usage and control overhead. A new parent is adopted if it advertises a lower cost than the current parent.

Many experimental studies related to WSN, some of which are based on MultiHopLQI, [25, 31-37] have shown that high unreliability of wireless links must be explicitly taken into account when designing routing protocols. Papers [32] and [33] address load balancing embedded in reliability-oriented routing protocols and are also using MultiHopLQI.

In [38] and [39] authors address the problem of minimizing the total consumed energy to reach the destination. The performance objective of maximizing the network lifetime was considered in [40] and [41].

Several works are related to WSN and ad hoc networks load balancing routing schemes [42-47]. In [42], authors show that distributing the traffic generated by each sensor node through multiple paths instead of using a single path allows energy savings. Paper [43] defines a network optimization problem used for performing the load balancing in wireless networks with a single type of traffic. In [44], authors study wireless network routing algorithms that use only short paths, for minimizing the latency, and achieve the load balance. In [45], authors introduce collision awareness in multipath routing; while [46] propose a multipath routing protocol to address the congestion control issue in WSN. In [47], the challenge of maximizing the network lifetime by load balancing the traffic is covered. In order to balance the energy consumption among sensor nodes, they deploy multiple sinks simultaneously, which are connected through wired or wireless infrastructure. Papers [48-50] are also related to load balancing routing protocols.

The paper [51] presents a resource-aware and link quality based (RLQ) routing metric. Based on both energy efficiency and link quality statistics, the RLQ metric in [51] is intended to adapt to varying wireless channel conditions, while exploiting the heterogeneous capabilities. This protocol does not include load balancing features.

Some works are taken into account the round-robin cluster based routing [52-54], where cluster heads are selected on a round-robin fashion. In [55] authors propose a source count (packets) based weighted round-robin forwarding algorithm.

Although all these studies provide a valuable and strong contribution in WSN routing, the problems of load balancing routing mechanisms based on local metrics, with special interest on the LQI based metrics, are yet to be addressed. This is the goal of this work. To save energy, we exploit the broadcast nature of wireless links, and the fact that the weights, in our proposed L2RP protocol, are built upon the achtophorous nodes capabilities instead of the ones of the source node. This allows L2RP to avoid doing a per packet load-balancing by the source, as done in [55], where the source node sends its data without being sure that the achtophorous node is able or not to sustain the load assigned. Thus, L2RP helps in reducing packet losses. Moreover, in most of papers addressing the load balancing routing, both experimental studies and simulation models, results are validated for only small sized networks (few tens of nodes), whereas our work addresses large sized networks (several hundreds of sensors). The comparative study of different metrics in L2RP is also a contribution of this work.

1.6.3. Routes Selection Criteria

In this chapter, "metric" is used to refer to local route selection criterion. As previously defined, each time we use "Achtophorous Node" it means next hop router with respect to a specific node having data to transmit towards the BS.

1.6.3.1. Remaining Energy Level

The remaining energy of sensors could be a metric for selecting routes since a node with better battery life seems to be a better candidate for the packet routing from its neighbours. Conversely, if a sensor with low power is selected as an achtophorous node, this can lead to packet losses because it might not have enough batteries to forward packets. We consider that each node knows its energy level.

1.6.3.2. Sensor Proximity with Respect to the Base Station (Proximity-BS)

In a warehouse Fig. 1.11, depending on the nature of their respective contents (frozen foods, fresh produce, etc.), the pallets provided each with a sensor Fig. 1.12 are arranged in fixed locations Fig. 1.13 designated by the Warehouse Management Software (WMS). Thus, during the warehouse WSN initialization, sensors could be initialized with their respective positions without using the GPS technology.

So, we consider a WSN deployed with a Base Station where each node knows its exact position and that of the BS. As the main goal of the application is to send data towards the BS, it seems natural to look at the metric defined as follows:

$$ProximityBS(S_i, BS) = 1/d(S_i, BS), \quad (1.1)$$

where $d(Si, BS)$ is the distance separating the sensor S_i from the BS. We choose inverse of the distance to promote the election of the closest sensor to the BS.



Fig. 1.11. Pallets arrangement inside a warehouse.

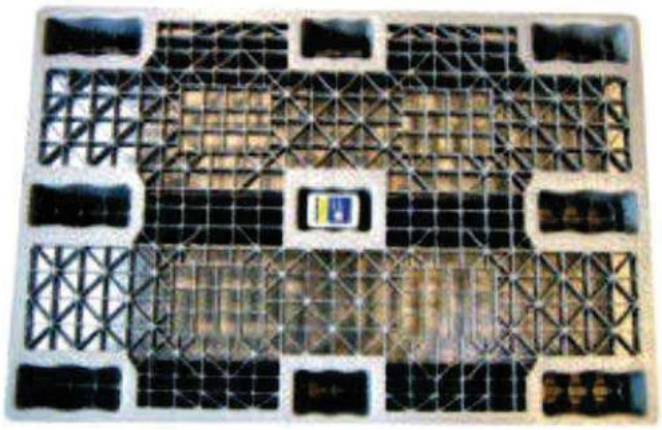


Fig. 1.12. Sensor plugged inside a Pallet.



Fig. 1.13. Location of a pallet: lane, location and level.

1.6.3.3. Degree of Connectivity

The degree of connectivity of a node, i.e., the number of its neighbours, is also a metric that seems interesting to study because, intuitively, the more neighbours a sensor has, the more it seems to be an appropriate candidate as an achtophorous node since a sensor with a low degree of connectivity might have little information, from its neighborhood, to forward to the BS. In the initial phase, each sensor is involved in the neighborhood information exchanges (hello protocol), which allows it to determine its degree of connectivity and the BS position.

1.6.3.4. LQI: Link Quality Indicator

In ZigBee standard [8, 26], the LQI measurement is defined as a characterization of the strength and/or quality reception of a packet. The use of the LQI result by the network or the application layers is not specified in [8, 26]. The LQI measurement is performed for each received packet Fig. 1.14, and the result is reported to the MAC sublayer as an integer ranging from 0 to 255. The minimum and maximum LQI values (0 and 255) are associated with the lowest and the highest quality IEEE 802.15.4 reception detectable by the receiver, and the LQI values in between are distributed between these two limits [8, 26].

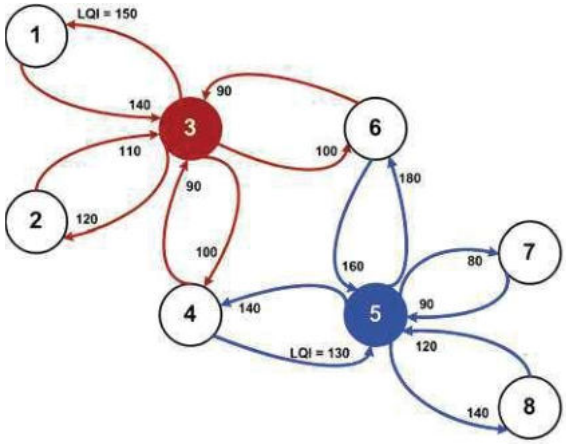


Fig. 1.14. Example of a WSN with Asymmetrical Links.

For Moteiv′s Tmote Sky [7] sensors equipped with chipcon′s CC2420 [27], the LQI values range from 50 to 110. Even so, we stick with the ZigBee standard [8, 26] because some manufacturers, such as SUN-SPOT [8] and WiEye [10], are still using the standard LQI values. Then, we will use the standard values (i.e., [0, 255]), instead of those of CC2420.

In this section, we define three LQI based metrics: AvgLQI, MaxLQI and MinLQI. The AvgLQI metric is the average calculated from the LQI values of all the links between the node and its neighbours. AvgLQI values give a characterization of sensors throughout their respective coverage quality. This metric might be useful in the context of the WSN

deployed in a warehouse which hosts a large number of pallets, one upon the other. Such an environment is proned to high unreliability of wireless links. The MaxLQI metric is the maximum LQI value which matches to the standard definition of the LQI used in the MultiHopLQI routing algorithm [25, 29]. As for the MinLQI, it is the minimum value beyond the given LQI threshold. For example Fig. 1.14, assuming that the LQI threshold for an acceptable link quality is 100, the MinLQI for node 5 is 120 (LQI of link 5-8) instead of 90 (LQI of link 5-7). Thus, Table 1.2 gives LQI metrics values for the WSN in Fig. 1.14.

Table 1.2. LQI metric values related to the WSN in Fig. 1.4.

Sensor ID	1	2	3	4	5	6	7	8
MinLQI	150	120	110	100	120	100	80	140
AvgLQI	150	120	107.5	120	125	140	80	140
MaxLQI	150	120	140	140	160	180	80	140

1.6.3.5. Composite or Hybrid Metric

In this chapter, we define the composite metric (hybrid) as follows:

$$Hybrid(LQI, M_i) = \rho * LQI + (1 - \rho) * Sc(M_i), \quad (1.2)$$

$$Hybrid(M_i, M_j) = \rho * Sc(M_i) + (1 - \rho) * Sc(M_j), \quad (1.3)$$

where $Sc(M_i)$ is the scale function, which returns remaining energy values comparable to the LQI values. This help avoiding the composite metric to be strongly influenced by the M_i component in (1.2):

$$Sc(M_i) = \alpha + \frac{\beta * \log(1 + (M_i - M_{i,min}))}{\log(1 + M_{i,max})}, \quad (1.4)$$

where M_i is the metric, $M_{i,min}$ (resp. $M_{i,max}$) is the minimum (resp. maximum) value ofM_i. If $M_i$is the remaining energy of the node, $M_{i,min}$ represents the value under which, the sensor is considered dead (battery depletion); while $M_{i,max}$is the initial energy value of a new battery. α = 50, β = 255.

Like the LQI metrics definition, we can also define AvgHybrid, MaxHybrid and MinHybrid metrics depending on whether, we are respectively considering AvgLQI, MaxLQI and MinLQI as defined in Table 1.2.

1.6.4. Routing Mechanisms

1.6.4.1. Simple Routing

In the simple routing mechanism, each sensor Si selects an achtophorous node which matches the best metric in its vicinity and located between the sensor Si and the BS. For

each given sensor, a unique achtophorous node plays the next hop role for all its packets until the next election Fig. 1.15.

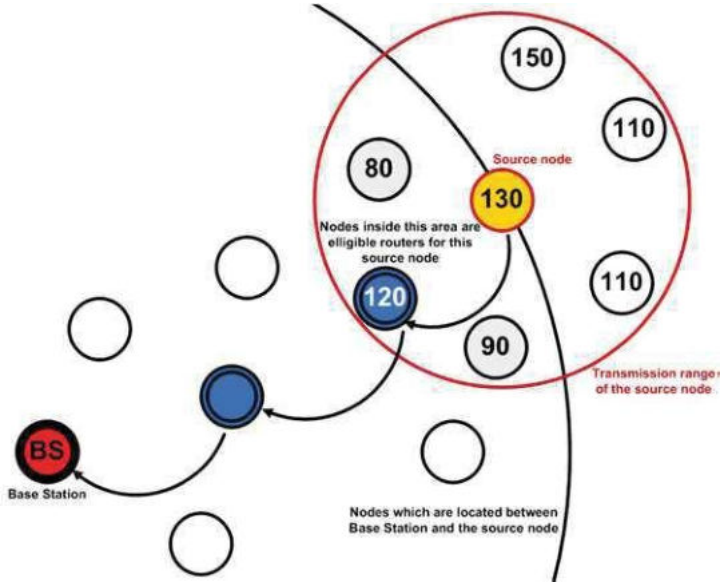


Fig. 1.15. Simple Routing from Source node 130 to the Base Station (BS).

1.6.4.2. Round Robin Routing

In the round-robin routing, each source node has to elect two or more achtophorous nodes. The source node sends data in round-robin fashion, simply taking turns which achtophorous node it routes each packet out Fig. 1.16. This routing mechanism is a per-packet load balancing routing which gives most even distribution across next achtophorous nodes.

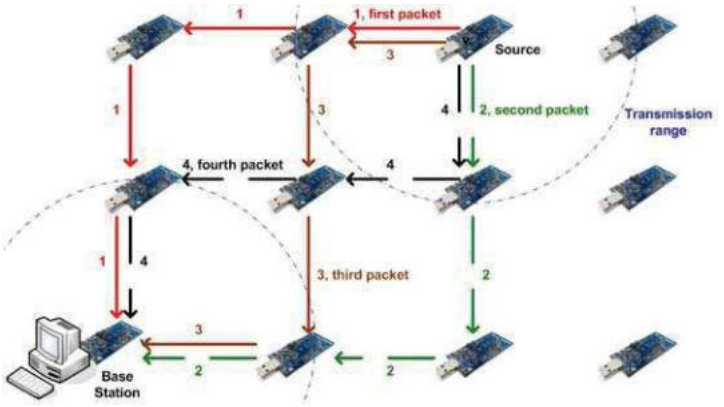


Fig. 1.16. Round-Robin Routing: Multiple routes from each source for different packets.

This per-packet load balancing method means that packets in a particular connection or flow arrive at their destination out of sequence. This does not cause a problem for most applications, but it can cause problems for the increasingly popular streaming media, both video and audio. In this chapter, only data packets are concerned within cold chain monitoring application for which the packet sequence order is not an issue.

1.6.4.3. Weighted Round-Robin Routing (W2R routing)

The weighted round-robin routing (W2R routing) is a load balancing mechanism that involves assigning a weight to each achtophorous node. Weights are proportional to metric values. In the W2R routing, each achtophorous node is assigned a value that signifies, relative to the other achtophorous nodes in the routing table, how the source node performs. The weight determines how many more (or less) packets are sent to that achtophorous node, compared to the other achtophorous nodes Fig. 1.17. The W2R routing is one way addressing some shortcomings. In particular, it provides a clean and effective way by focusing on fairly distributing the load amongst available achtophorous nodes, versus attempting to equally distribute data packets.

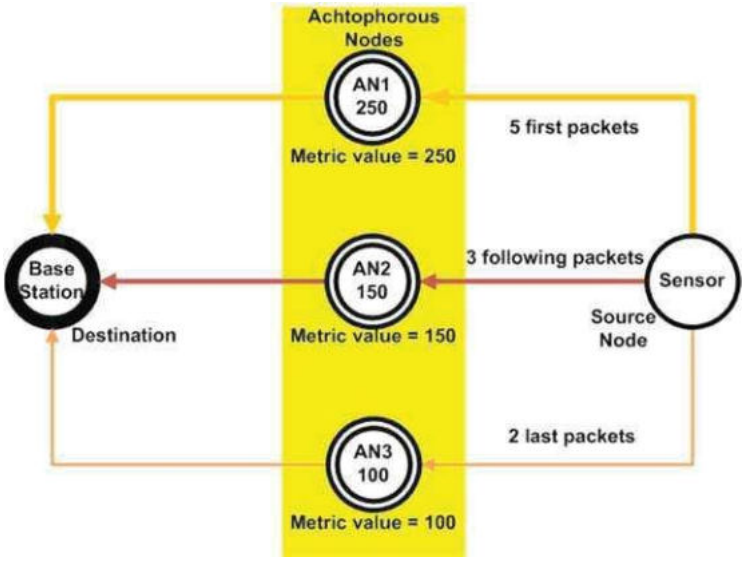


Fig. 1.17. Weighted round-robin routing (W2R routing) mechanism.

Table 1.3. Weights of the achtophorous nodes in Fig. 1.17.

Achtophorous Node	Metric	Weight	Load handled
AN1	250	0.5	50 %
AN2	150	0.3	30 %
AN3	100	0.2	20 %

For example, in Fig. 1.17, the source node routes 50 % of its packets through the achtophorous node AN1, 30 % through AN2 and 20 % through AN3. If the BS is not located within the transmission range of an achtophorous node, this one should apply the same mechanism to retransmit the packet towards the BS.

The weighted round-robin routing mechanism is computed as described in this simple Algorithm 1 which is computed each time a source node has to send a packet. The achtophorous nodes, each with its respective weight, are listed in the routing table of each source node in an ordered manner such that the first achtophorous node matches the highest weight as shown in Fig. 1.17. For each source node, the window interval is the constant length of each stream of consecutive packets to transmit. The weight of each achtophorous node is converted as an integer value based on the window interval parameter. For example, in Fig. 1.17, window = 10 consecutive packets, and weight(AN1) = 5. The use(AN) function returns the number of times the current achtophorous node AN is used during the window interval whereas packet_idx is the index of the current packet during the window interval.

Algorithm 1 : Weighted Round Robin (W2R) Routing

Require: $packet_idx$, $window$, AN, $weight$, use

1: **if** $packet_idx < window$ **then**
2: **if** $use(AN) < weight(AN)$ **then**
3: $Send_packet_to(AN)$
4: $use(AN) \leftarrow use(AN) + 1$
5: $packet_idx \leftarrow packet_idx + 1$
6: **else**
7: $use(AN) \leftarrow 0$
8: $AN \leftarrow Next().achtophorous_node$
9: $\#\ The\ next()\ of\ the\ last\ AN\ is\ the\ first\ AN$
10: $Send_packet_to(AN)$
11: $use(AN) \leftarrow 1$
12: $packet_idx \leftarrow packet_idx + 1$
13: **end if**
14: **else**
15: **for** $each\ achtophorous_node\ AN$ **do**
16: $use(AN) \leftarrow 0$
17: **end for**
18: $AN \leftarrow First().achtophorous_node$
19: $Send_packet_to(AN)$
20: $use(AN) \leftarrow 1$
21: $packet_idx \leftarrow 1$
22: **end if**
23: **return** $packet_idx$, AN, use

1.7. L2RP: The Link Reliability Based Routing Protocol

The proposed (L2RP) routing protocol Fig. 1.18 consists for a sensor having an empty routing table to elect one next hop router (case of simple routing) or more achtophorous nodes (load balancing routings) amongst its neighbours according to the following:

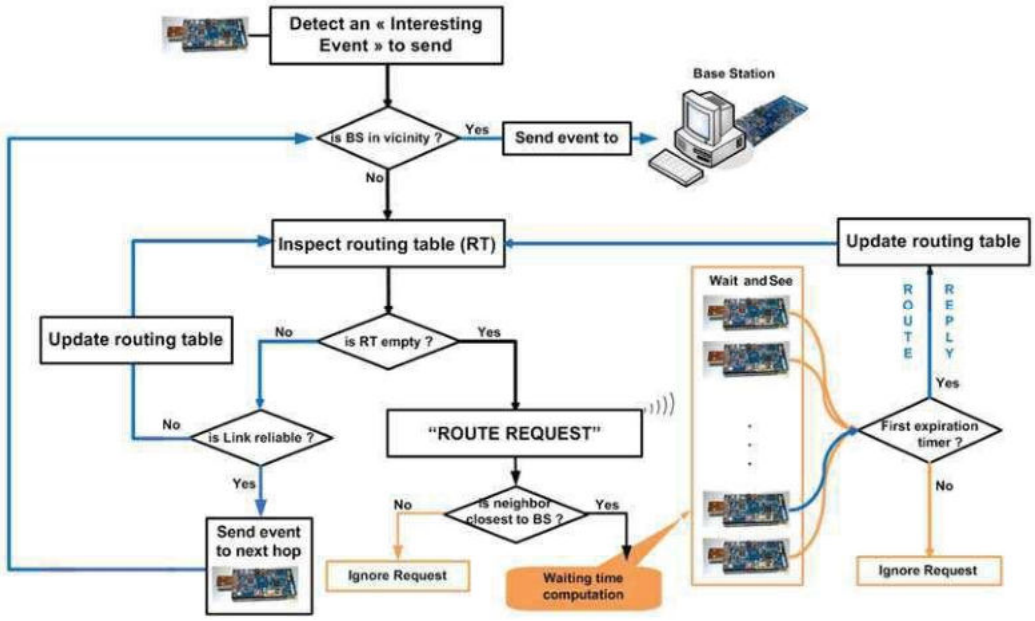


Fig. 1.18. The Link Reliability based Routing Protocol (L2RP) flowchart.

- Initial step: all sensors empty their routing tables.
- The sensors located in the vicinity (transmission range) of the BS send their data directly to it.
- A sensor, located outside of the vicinity of the BS, inspects its routing table:
    - If its routing table is not empty, it checks if the link with the next hop is reliable or not. If the link is unreliable, based on the LQI value, then:
        - Case of simple routing mechanism: it sends a "ROUTE REQUEST" to its neighbours.
        - Case of load-balancing routing: it chooses an alternate route and then checks again if the link with this next hop is reliable or not. If no link with nodes in the routing table is reliable, then it erases its routing table and it sends a "ROUTE REQUEST" to its neighbours.

- If its routing table is empty, it also sends a “ROUTE REQUEST” to its neighbours.

- Each neighbor, located between the BS and the sensor having sent the “ROUTE REQUEST”, computes its own waiting time which is inversely proportional to its metric value. We use the Wait and See protocol (WaS), as in [24], where the only sensor having the best metric sends a “ROUTE REPLY” to the requester node. The other neighbours simply ignore the “ROUTE REQUEST” avoiding useless “ROUTE REPLY” packets. In the case of a load balancing routing, the number (ANs) of achtophorous nodes is a known parameter in the initialization phase of the network. This parameter is used by the WaS protocol that allows ANs sensors having highest metrics in succession to answer to the requester node, and then be elected, for this node, as achtophorous nodes.

- Upon reception of the “ROUTE REPLY” packet, the requester node updates its routing table, which remains valid until the next election. In the case of weighted round-robin routing, each “ROUTE REPLY” packet contains the metric value of the answering node, which allows the requester node to calculate weights associated with each achtophorous nodes.

- At the end of the current cycle, sensors reset their routing tables and go back to the initial step of the next cycle.

Upon receipt of a "ROUTE REQUEST" packet, a sensor S_i computes its own waiting time according to the following formula:

$$Timer(S_i) = \tau + \frac{\zeta}{1+\log(1+M_i+\frac{id(S_i)}{\Gamma}*M_i)}, \quad (1.5)$$

where M_i is the metric value of the sensor S_i. τ and ζ are the nonzero positive constants. Γ is the constant, which is more large than the network size (Γ = 10^6, for example). This timer function avoids collisions between nodes having the same metric value. Since $M_i \geq 0$, if $M_i = 0$ then the sensor S_i can not be an achatophorous node.

As we can see, in this protocol the source node uses the link quality indicator (LQI) to check if the link it forms with the nominated achtophorous node is reliable or not. This helps avoiding sending the packet to an achtophorous with which it forms a link of poor quality which could lead to packet loss.

1.8. Routing Protocol Performance Criteria

1.8.1. Average Ratio of the Remaining Energy

The average ratio of the remaining energy is the ratio of the average remaining energy on the average of initial energy. Multiplied by hundred, this value represents the average

battery life of sensors, in terms of percentage. The higher this value is, the more energy-efficient the routing protocol is.

1.8.2. Average Path Lengths

The average path lengths are calculated in terms of the number of hops traversed by packets before reaching the BS. A large value reflects participation of many sensors in the effort due to the routing, which may increase the overall energy consumption. A good routing protocol is recognized in this performance criterion by a relatively low value. Conversely, too small path length may lead to bad quality link.

1.8.3. LIF: Load Imbalance Factor

The load imbalance factor (LIF) is defined as the root of the squared coefficient of variation of the relative remaining energy. This shows the energy spent by communications:

$$LIF = \sqrt{\frac{Var(E_R^i)}{\bar{E}_R{}^2}}, \tag{1.6}$$

where E_R^i is the ratio of the remaining energy of the sensor S_i; and $\bar{E}_R$ is the average ratio of the remaining energy.

With this performance criterion, the best routing mechanism is among the ones which produce small load imbalance factor. Indeed the lowest LIF value indicates the best evenly distribution of the energy consumption between nodes.

1.8.4. Network Lifetime

In this work, we define the network lifetime as the average number of packets routed until the first time a sensor run out of battery. This could also result in network capacity. We focus on the first battery depletion, which means the instant the network stops fulfilling totally its role, because it leads to packet losses. An ideal network is a network where all packets sent by source nodes are actually transmitted to the recipient (BS). The earlier the first packet loss happened, the more ineffective the routing protocol is.

1.8.5. Average Percentage of Lost Packets

Beyond the first time battery depletion is experienced by the network, a high percentage of packet losses might reflect an unreliable network whose routing protocol is less effective.

The loss of packets is a factor aggravating the overall energy consumption because this causes poor quality of service and retransmissions to guarantee the reliability of some applications.

1.9. L2RP Routing Protocol Performance Evaluation Model

1.9.1. Energy Consumption Model

For the performance evaluation model, we will use this energy consumption model [1-3, 56, 57], Fig. 1.19.

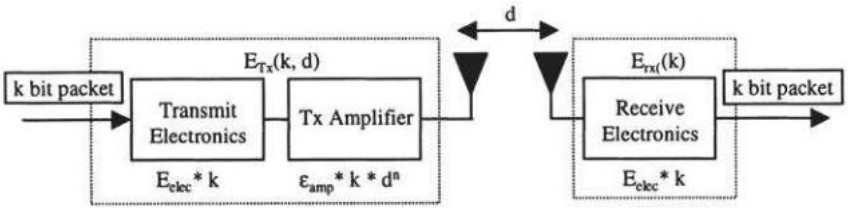


Fig. 1.19. Energy dissipation model.

Let $E_{Tx}(k,d)$ the energy [56, 57] consumed to transmit k bits message over a distance d Fig. 1.19:

$$E_{Tx}(k,d) = E_{elec} * k + \mathcal{E}_{amp} * k * d^2. \quad (1.7)$$

Let $E_{Rx}(k,d)$ the energy consumed to receive a k bits message:

$$E_{Rx}(k,d) = E_{Rx}(k) = E_{elec} * k, \quad (1.8)$$

E_{elec} = 50nJ/bit and $\mathcal{E}_{amp}$ = 100pJ/bit/m2.

1.9.2. Network Deployment and Performance Evaluation Parameters

In the performance evaluation model N nodes are randomly (according to a uniform distribution) deployed over an area of length L=100 m, and width l=100 m (Fig. 1.20). The BS is located at the (0,0) position. Each node generates a sequence of "interesting events", which are sensed data over the temperature threshold T_{min}, following the Poisson process of parameter $\lambda = 10$. For simulation scenarios, the size of each data packet is set to k_{data} = 128 bits, and the "ROUTE REQUEST" and "ROUTE REPLY" packets of the L2RP protocol have a size of k_{rr} = 24 bits. Let us assume that each node knows its position and its remaining energy level at any time.

The initial energy amount of each node is set to a value $E_0 = (1.5 * 10^5 - \mathcal{E})\mu J$, where $\mathcal{E} = rand(0,1) * 10^2 \mu J$. Node battery exhaustion is experienced when the remaining energy level of the node is under the given threshold $E_{min} = E_0 * 0.05$.

All nodes, including the BS, have same the transmission range R = 20 m. The main simulation parameters are listed in Table 1.4.

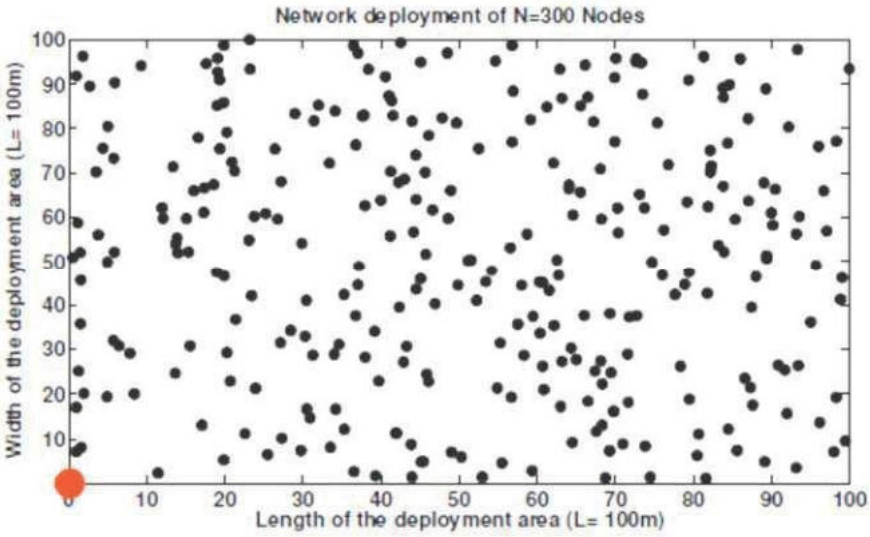


Fig. 1.20. Network deployment of N=300 sensors over an area (100 m × 100 m).

Table 1.4. Simulation parameters.

Parameter	***Value***
Deployment	
Area Length	*L = 100m*
Area Width	*l = 100m*
Base Station Location	*position(SB) = (0, 0)*
Radio range	*R = 20m*
Network Size (number of sensors)	*N = {100, 200, ..., 500}*
Poisson parameter	
Packet sent by each sensor	$\lambda = 10$
Packet sizes (bits)	
Alarms	$k_{data} = 128$
L2RP "ROUTE REQUEST"	$k_{rr} = 24$
L2RP "ROUTE REPLY"	$k_{rr} = 24$
L2RP Achtophorous Nodes	
Number of Achtophorous Nodes	*AN = 3*
Window interval for W2R	*window = 10*
LQI parameters	
Threshold for MinLQI	$LQI \geq 100$
Link Reliability (L2RP)	$LQI \geq 70$
Energy	
Initial Energy Level	$E_0 = (1.404 \times 10^5 - \mathcal{E})\mu J$ $\mathcal{E} = rand(0,1) \times 10^2 \mu J$
Minimum Energy Level	$E_{min} = E_0 \times 0.05$

1.9.3. LQI Model for Performance Evaluation Purposes

The WSN can be modelled as a graph$G = (V, E)$, where two nodes are connected by an edge if they can communicate with each other. Let $x \in V$ be a node in the WSN. $N_1(x)$ is the neighbourhood of the node x. At each given time t, a node x forms with each $y \in N_1(x)$ a link of which the link quality indicator (LQI) value is denoted by $\ell(x, y, t) > 0$. For all other nodes: $\forall z \in V \setminus N1(x), \ell(x, z, t) = 0$. Let ν be a bijective function defined in V which is a totally ordered set. The ν function is defined as follows:

$$\forall x \in V, \nu(x) = \big(f(x), id(x)\big), \tag{1.9}$$

where $f(x)$ is the function which returns the metric value of x, and $id(x)$ returns the address of the node x. The total ordering in V is defined as follows:

$$\forall x, y \in V, \nu(x) > \nu(y) \Leftrightarrow \big(f(x) > f(y)\big) or$$
$$\big(f(x) = f(y) and id(x) > id(y)\big). \tag{1.10}$$

After the WSN deployment in the warehouse, the BS initially broadcasts a message containing its position. This information is then retransmitted to all sensors in the network. In this phase, each node knows its degree of connectivity. At each given time t, the LQI value of the link formed by any pair (x, y) of nodes is calculated by using the $\ell(x, y, t)$ function defined below:

$$\ell(x, y, t) = f(x, y, t) * g(x, y), \tag{1.11}$$

$$f(x, y, t) = 1 - \mathrm{P}_r[link(x, y, t) = Unreliable], \tag{1.12}$$

$$g(x, y) = \alpha + \frac{\beta * \log(1 + (\gamma(x,y) - \gamma_{min}(\mathrm{x})))}{\log(1 + \gamma_{max}(\mathrm{x}))}, \tag{1.13}$$

$$\gamma(x, y) = \frac{1}{d(x,y)}, \tag{1.14}$$

$$\gamma_{min}(x) = \min_{y \in N_1(x)} \gamma(x, y), \tag{1.15}$$

$$\gamma_{max}(x) = \max_{y \in N_1(x)} \gamma(x, y), \tag{1.16}$$

where $\alpha = 50, \beta = 255$ and *d(x, y)* is the distance separating *y* from *x*.

In the context of a cold chain monitoring application, the warehouse hosts hundreds of pallets, one upon the other. Each pallet is provided with a temperature sensor. This environment is subjected to the unreliably feature of the wireless links. So, in the formula (1.12), $\mathrm{P}_r[link(x, y, t) = Unreliable]$ denotes the probability that the link *ℓink(x, y, t)* becomes unreliable at a given time t. This probability is used in some simulation scenarios, in order to evaluate the behaviour of our L2RP protocol with respect to the unreliability aspect of the wireless links.

The choice of this model, formula (1.13) similarly to the scale function $\mathrm{S_c}$ defined in the composite metric, is guided by experimental results shown in [58] and [31] which stated that the LQI decreases when the distance between nodes increases in ZigBee-based WSN.

As we can see, $\ell(x, y, t) \neq \ell(y, y, t)$, because of the formulas (1.15) and (1.16). Hence, the model allows taking into account asymmetrical aspects of the wireless links.

For Moteiv′s Tmote Sky [7] sensors equipped with chipcon′s CC2420 [27], the LQI values range from 50 to 110. Even so, we stick with the ZigBee standard [26, 8] because some manufacturers, such as Sun-SPOT [8] and WiEye [10], are still using the standard LQI values. Then, we use the standard values (i.e. [0, 255]) increased by $\alpha = 50$, instead of those of CC2420. The use of $\alpha = 50$ allows to keep the null value, $\ell(x, y, t) = 0$, only for the two cases where the node y is not in the transmission range of the node x, or when the $\ell ink(x, y, t)$ becomes unreliable i.e. $P_r[link(x, y, t) = Unreliable] = 1$.

This LQI model is only used for simulation purposes, so sensor nodes do not compute these above formulas.

1.10. L2RP Routing Protocol Performance Evaluation

Performance evaluation, using Matlab, are run for a network size ranging from 100 to 500 nodes. The performance results presented here are obtained by averaging the results for 50 different simulations for each scenario comparing the route selection criteria. In each scenario where the three routing mechanisms are compared, 25 different simulations were run. For each simulation, a new random node layout is used.

In all simulation results presented below, ρ = 0.5 for the composite metric as defined in formulas (1.2) and (1.3). If it's not specified, the number ANs of Achtophorous Nodes is set to ANs = 3 for each load balancing mechanism.

In all performance evaluation scenarios, except those in Section 1.10.8, links are considered reliable, i.e.:

$$\forall t, \forall x \in V, \forall y \in N_1(x), P_r[link(x, y, t) = Unreliable] = 0. \quad (1.17)$$

For some results, the related confidence intervals for a confidence coefficient of 95 % are computed as detailed in the Section 1.3.3 of [59].

1.10.1. Average Path Length

The Fig. 1.21 shows the average path length for the simple routing, and the Fig. 1.22 its related confidence interval.

The results of Fig. 1.21 show, in the case of simple routing mechanism, the average path lengths in terms of the average number of hops obtained with the different studied metrics when the node density is increasing in the deployment area. This result shows that routes are longer for the MaxLQI and degree of connectivity metrics. The remaining energy, AvgLQI, MinLQI and "Proximity with respect to the BS" metrics have better average path lengths. The gap is more important for the MaxLQI metric with respect to the other metrics. Moreover, for MaxLQI, the average number of hops is a monotonically

increasing function of the network density. This reflects the fact that the routing according to the metric MaxLQI consists of choosing as an achtophorous node the node having the best link quality with the source node. In the absence of obstacles and other phenomena like interferences, the best link quality is determined by the shortest distance separating a node from the source node. So, routing according to the MaxLQI metric is equivalent to a multihop "step by step" routing which is characterized by a great number of hops due to small distances separating each source node and its achtophorous node.

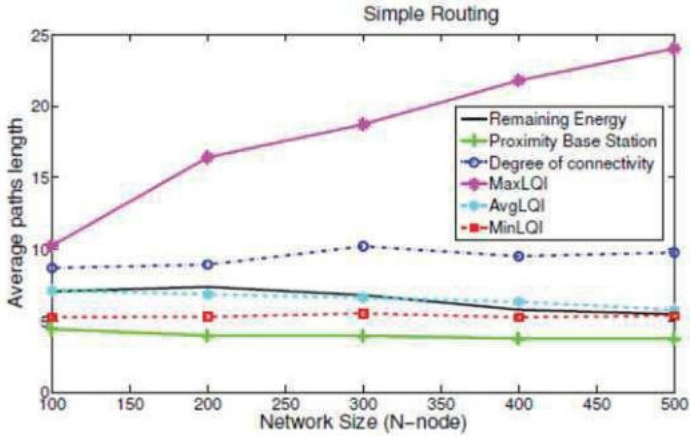


Fig. 1.21. Average path length: Comparison of metrics in simple routing mechanism.

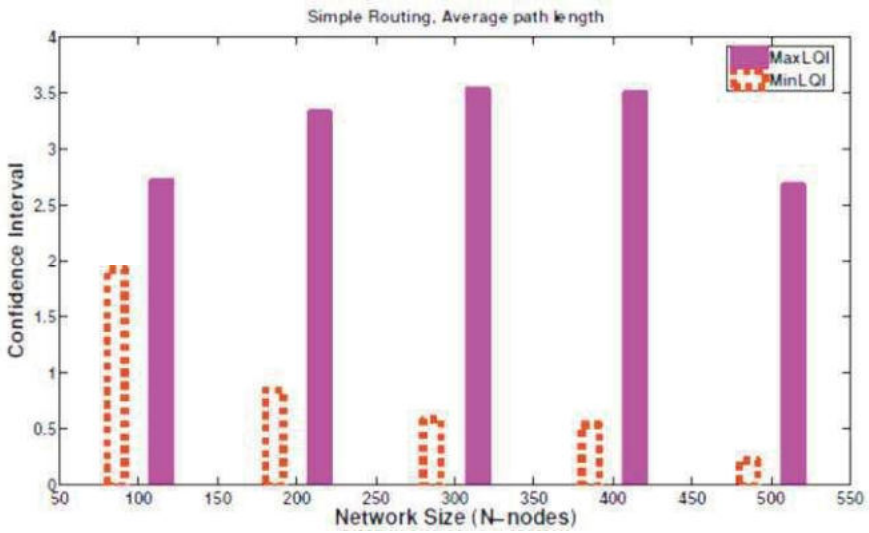


Fig. 1.22. Confidence interval, for the result of Fig. 1.21, for a confidence coefficient of 95 %.

When the network density is increasing, the distances separating sensors decrease. Thus, the distances separating each source node and its achtophorous node also decrease, as well. So, from any source node towards the base station, the number of hops of each sent

packet becomes increasingly high when the MaxLQI is used. By multiplying the number of hops, in this manner, the sensor network could not claim to have a good performance. This result explains the low performance of the MultiHopLQI routing algorithm which is used today in many TinyOS based empirical WSN analysis. Indeed, MultiHopLQI uses the LQI metric as defined in the ZigBee standard [26, 8], that is to say the MaxLQI metric.

Conversely, the Proximity-BS and MinLQI metric have the lowest average path lengths Fig. 1.21. For any given source node, the selected Proximity-BS based achtophorous node matches the farthest neighboring node towards the Base Station. Therefore, the routing according to the Proximity-BS metric is equivalent to the shortest geographical path routing. Accordingly, packets are transmitted from the source node to the base station requiring the minimum number of hops. This result Fig. 1.21 is also interesting for the MinLQI metric. Indeed, this metric promotes the use of the links of intermediate quality. Links of good quality are synonymous with the nearest nodes multiplying the number of hops, whereas the links of poor quality stand for lot of packet losses. This explains why MinLQI is a good metric.

The Fig. 1.23 compares the average path length related to the "Proximity with respect to the BS" metric when it is used in the simple routing and load balancing routing mechanisms.

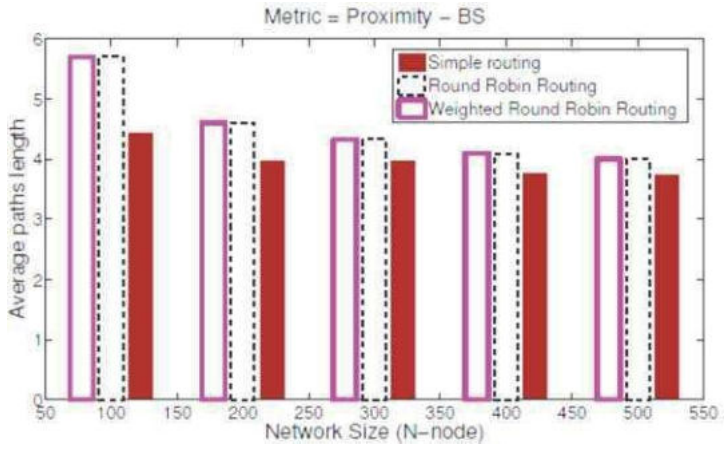


Fig. 1.23. The average path length in the three routing mechanisms (Proximity-BS).

For the Proximity-BS metric, the load balancing mechanisms have the effect of increasing the average path lengths which is almost the same average for the weighted round robin routing and the round robin one Fig. 1.23. In the case of load balancing mechanisms, each sensor has in its routing table several achtophorous nodes of which only one exactly corresponds to the achtophorous node used by the simple routing. The other achtophorous nodes are necessarily more distant from the base station. So, the average path lengths slightly increase for load balancing mechanisms with respect to the simple routing using the Proximity-BS metric Fig. 1.23. For any given source node, the selected achtophorous nodes are identical for both load balancing mechanisms, their use only differs by the

weight introduced in the weighted round robin routing. This leads to an average number of hops almost identical Fig. 1.23.

Unlike the Proximity-BS and MinLQI metrics, the MaxLQI one has an average path length which is reduced by the load balancing mechanisms Fig. 1.24. In this case, the weighted round robin routing mechanism has an average number of hops closer to the one of the simple routing mechanism than the round-robin one. Indeed in the case of W2R, the achtophorous node which forms the better link quality (MaxLQI) is also the one which has the highest weight. Thus, depending on the weight value, the sensors choose to send their packets more frequently to that achtophorous node. Therefore, W2R leads to an average number of hops closer to the one of the simple routing mechanism Fig. 1.24.

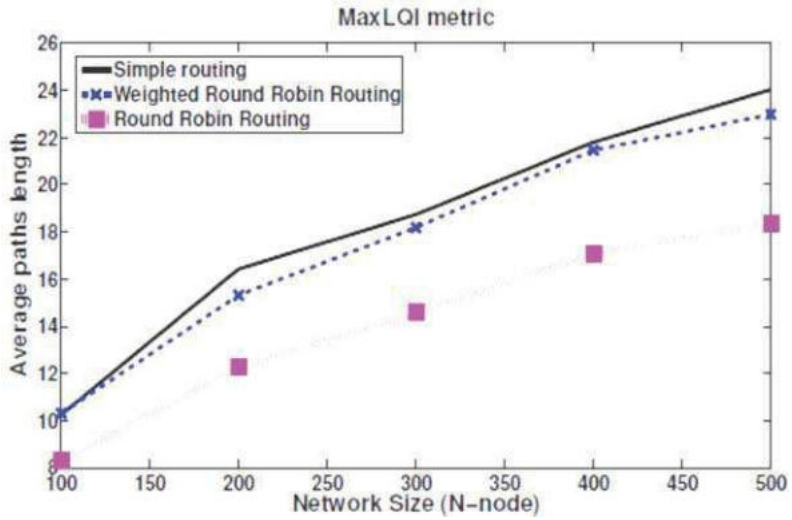


Fig. 1.24. The average path length in the three routing mechanisms (MaxLQI).

1.10.2. LIF: Load Imbalance Factor

The Fig. 1.25 shows the LIF when the "Proximity with respect to the BS" is used as metric. It displays results for the simple routing and load balancing mechanisms. The Fig. 1.26 for MaxLQI and the Fig. 1.27 for MinLQI also display the LIF for the three routing mechanisms.

The lowest LIF value indicates the best evenly distribution of the energy consumption between nodes. It would be redundant to say that the load balancing mechanisms (round robin and W2R) help evenly balancing the load. That is to say that the average LIF values are lower for load balancing mechanisms compared to the simple routing, whatever the chosen metric Fig. 1.25, Fig. 1.26 and Fig. 1.27. But the gap is more important for MaxLQI than other metrics.

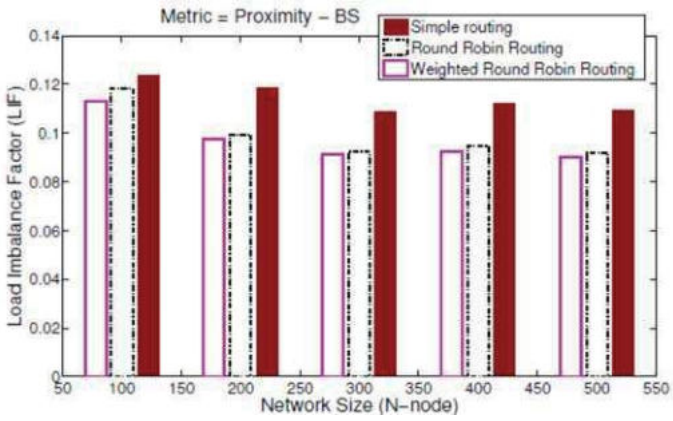


Fig. 1.25. LIF in the three routing mechanisms (Proximity-BS).

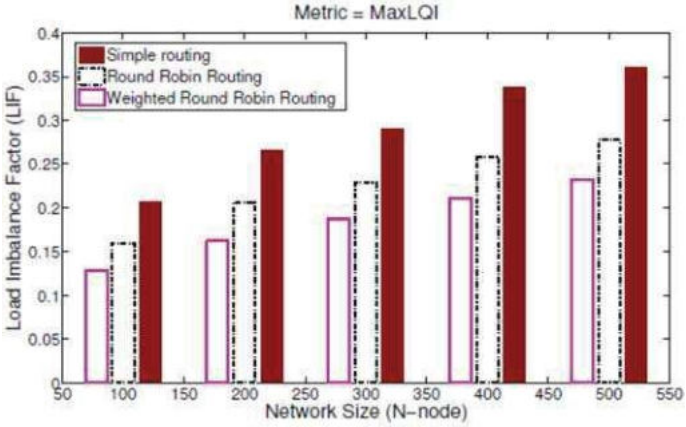


Fig. 1.26. LIF in the three routing mechanisms (MaxLQI).

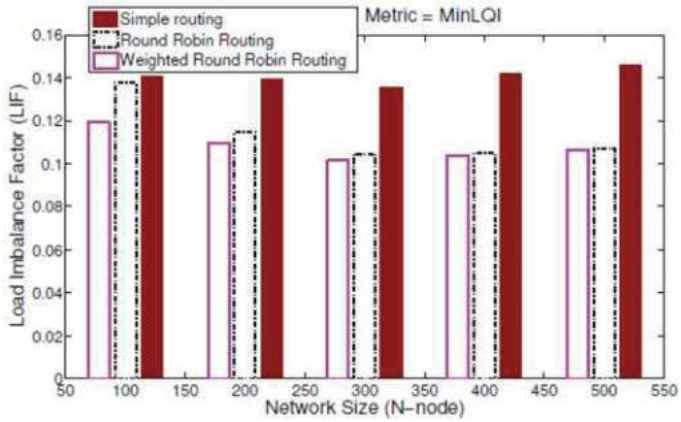


Fig. 1.27. LIF in the three routing mechanisms (MinLQI).

Moreover, when the network density is increasing, the difference between round robin and W2R tend to vanish for the Proximity-BS metric and for the MinLQI metric Fig. 1.25 and Fig. 1.27. For these two metrics, it would be more suitable in dense wireless sensor networks to use the round robin mechanism than the W2R one. Therefore, in doing so, one saves the power required, mainly by the processor, for the achtophorous weight computations Fig. 1.17 and Table 1.3.

These results confirm that load balancing mechanisms help in the distribution of the load across the nodes, because whatever the metric used: the W2R routing produces lower LIF than the round-robin routing which is followed by the simple routing Fig. 1.25, Fig. 1.26 and Fig. 1.27.

As for the result of Fig. 1.28, it compares the average LIF of different metrics in the W2R routing. The "Proximity with respect to the BS" and MinLQI metrics produce lower LIF values Fig. 1.28. The remaining energy metric has an intermediate LIF, while the degree of connectivity and MaxLQI metrics tend to imbalance the energy consumption on the network: some sensors exhaust their batteries while others have a little participation in packet routings towards the BS. This negative phenomenon is much more important for the MaxLQI metric when the network size is increasing Fig. 1.26 and Fig. 1.28.

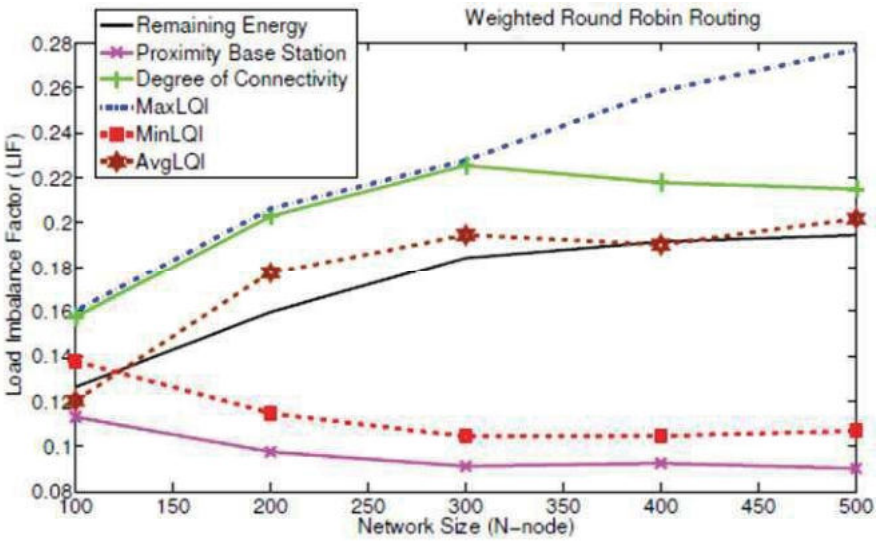


Fig. 1.28. LIF: Comparison of different metrics in the Weighted Round Robin Routing (W2R).

This reflects the fact that the degree of connectivity and the MaxLQI metrics are the ones for which packets arrive at the Base Station by routes using the largest number of hops as shown in Fig. 1.20 and explained in the last section. Thus, along each route, the WSN experiences more retransmissions and then more energy wastage due to the effects of overhead, latency and overhearing phenomena which are more important when the average number of hops is increasing.

1.10.3. Average Percentage of Packet Losses

The result of Fig. 1.29 displays, for each metric, the average percentage of packet losses experienced by the network when the simple routing is run. The three routing mechanisms are compared Fig. 1.30 using the degree of connectivity metric.

Generally, the loss percentage is quite low. This reflects the fact that, in L2RP, losses are mainly due to the node battery exhaustion. The first result Fig. 1.29 compares the different criteria in the mechanism of simple routing.

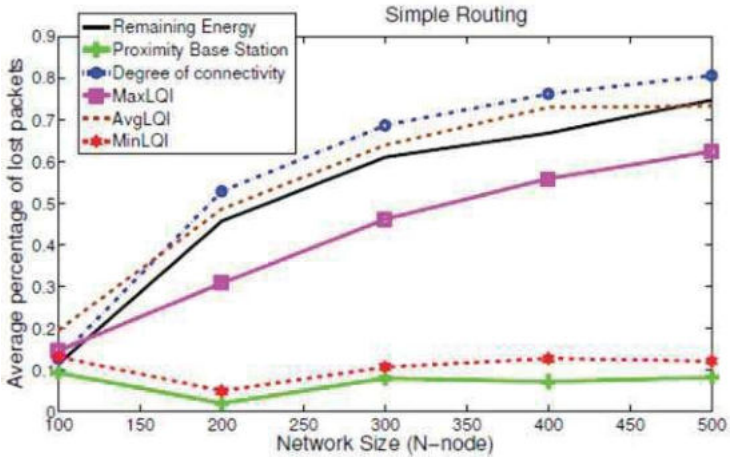


Fig. 1.29. Average percentage of lost packets: Comparison of the different metrics in the Simple Routing mechanism.

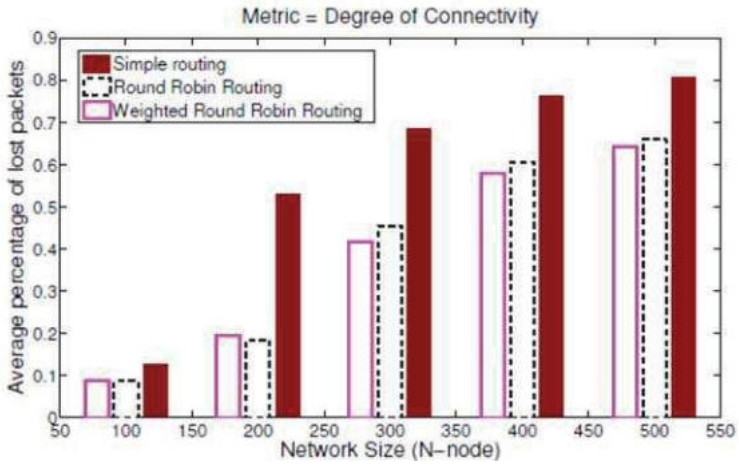


Fig. 1.30. Average percentage of lost packets: Comparison of the three routing mechanisms with the Degree of connectivity metric.

Here again, best results are produced by MinLQI and "Proximity with respect to the BS" metrics. MaxLQI has an intermediate average percentage of packet losses, while the remaining energy and degree of connectivity metrics have higher percentages. For the Proximity-BS metric this result is easy to understand, because according to the previous results Fig. 1.20, Proximity-BS is the metric which produces the shortest path lengths. Accordingly, as the overhearing phenomenon and the overhead induced by routing are reduced when the number of hops is minimal, then the node battery exhaustion occurs later (in time) leading to a low loss percentage for the metric Proximity-BS.

Conversely, the degree of connectivity metric has the highest percentage of packet losses Fig. 1.29. By choosing to route packets according to this metric, any given sensor which has data to transmit chooses its achtophorous node, in simple routing, as its neighbor which has the highest number of neighbours. Therefore whenever an achtophorous node is requested to route a packet, the overhearing phenomenon causes more energy consumption which leads to a greater packet loss percentage.

For all metrics, load balancing significantly reduces the average percentage of packet losses Fig. 1.30. Load balancing mechanisms produce lower packet losses than the simple routing; differences are more important when load balancing is run with the degree of connectivity metric, the remaining energy metric or the MaxLQI metric.

Indeed, for the degree of connectivity metric of which the overhearing phenomenon is the most important, Load balancing requires the selection of different achtophorous nodes for each source node. So, in the routing table there is exactly one node which has the highest number of neighbours: this the one used by the simple routing mechanism. Then, in load balancing when the other achtophorous nodes with fewer neighbours are used, this helps reducing the overhearing phenomenon. This justifies why load balancing reduces the percentage of packet losses compared to simple routing which always requires the highest degree of connectivity as achtophorous node Fig. 1.30.

1.10.4. Composite or Hybrid Metric

The Fig. 1.31 (simple routing) and the Fig. 1.32 (W2R routing) display the average percentage of packet losses including the hybrid metric which is a combination of the remaining energy metric and the "Proximity with respect to the BS" metric.

These results show that the hybrid metric composed of 50 % of the remaining energy and 50 % of "Proximity with respect to the BS" (i.e. $\rho = 0.5$ in Formula (1.3)) is a very good metric. It has a percentage of packet losses which is relatively low, especially when it is used with load balancing mechanisms. As we can see, there are fewer lost packets when the simple routing is run with the MinLQI metric than the W2R routing run with the remaining energy metric, MaxLQI or the degree of connectivity metric Fig. 1.31 and Fig. 1.32.

These results show that compared to the "remaining energy level" metric, the hybrid metric helps mitigating losses particularly in load balancing (W2R Routing) where the

average packet loss percentage is less than 0.1 % for this metric. This kind of metric is very interesting to consider because depending on the specific WSN application purposes, it may be useful to consider several criteria for selecting routes by computing a single hybrid metric.

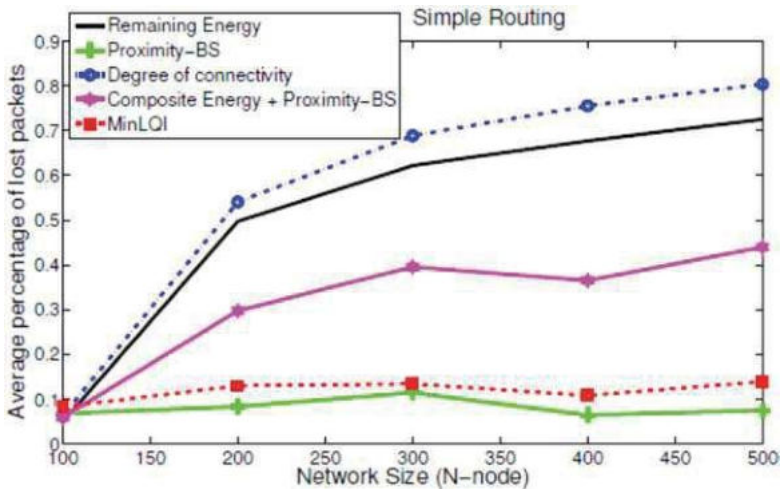


Fig. 1.31. Average percentage of lost packets: Comparison of different metrics including the hybrid metric (remaining energy level + Proximity-BS) in W2R Routing.

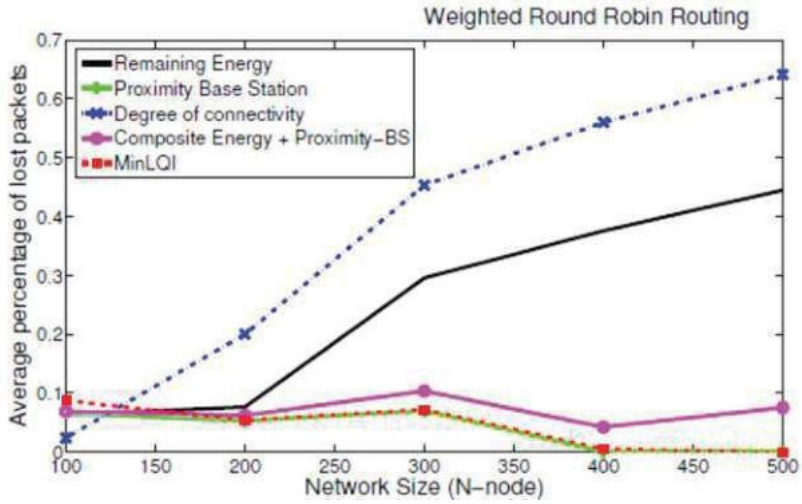


Fig. 1.32. Average percentage of lost packets: Comparison of different metrics including the hybrid metric (remaining energy level + Proximity-BS) in W2R Routing.

In this result, it is more beneficial to route jointly depending on the distance and the remaining energy than to route only along with the remaining energy criterion. This reflects the fact that the "remaining energy level" criterion is not a good metric for route

selection. Because in our simulation scenario Table 1.4 each node is deployed with an initial energy level $E0$ which is randomly and slightly lower than a reference value $E_0 = (1.5 \times 10^5 - \mathcal{E})\mu J$, where $\mathcal{E} = rand(0,1) \times 10^2 \mu J$. This scenario is very realistic, because even if the AA batteries powering the sensors are new, they also have slightly different energy levels in real world scenario.

Although the average percentage of packet losses is generally too low, the load balancing helps reducing the packet loss percentage for the hybrid metric similarly to all other studied metrics.

1.10.5. Average Network Lifetime

The Fig. 1.33 displays the average network lifetime for the simple routing, and the Fig. 1.34 shows its related confidence interval for a confidence coefficient of 95 %. The Fig. 1.35 shows the average network lifetime when MinLQI is used in each routing mechanism.

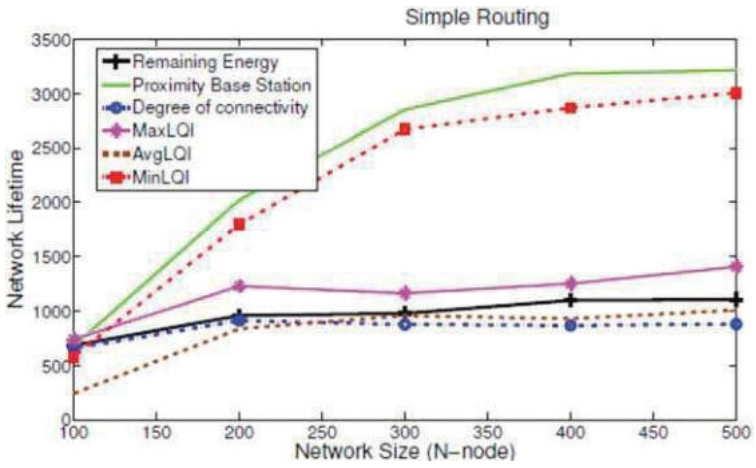


Fig. 1.33. Average network lifetime: Comparison of different metrics in the simple routing.

Firstly, these results show that more dense networks have better lifetime. The MinLQI and "Proximity with respect to the BS" metrics produce better network lifetime. MaxLQI is better than the remaining energy metric which is followed by the degree of connectivity metric Fig. 1.33. Load balancing mechanisms significantly increase the average network lifetime which is larger than the one of the simple routing with more differences for MinLQI (Figs. 1.35, 1.36) and "Proximity with respect to the BS" metrics.

The time of first packet loss occurs earlier for the degree of connectivity metric. As we explained in the previous sections, this result is also caused by the overhearing phenomenon of which effects are more important for the degree of connectivity metric with respect to other metrics. The Proximity-BS metric improves the network lifetime by minimizing the number of hops Fig. 1.33.

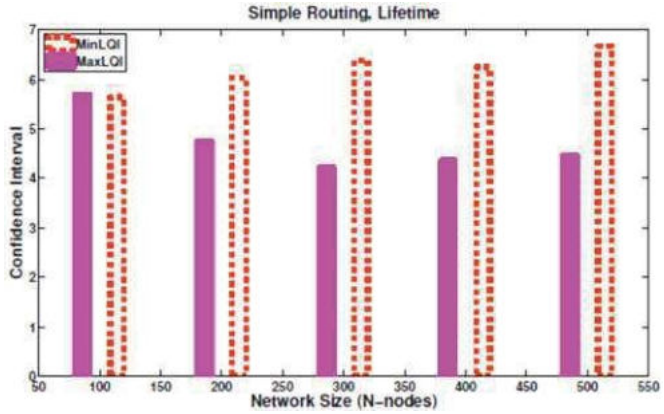


Fig. 1.34. Average network lifetime: confidence interval related to Fig. 1.33 for a confidence coefficient of 95 %.

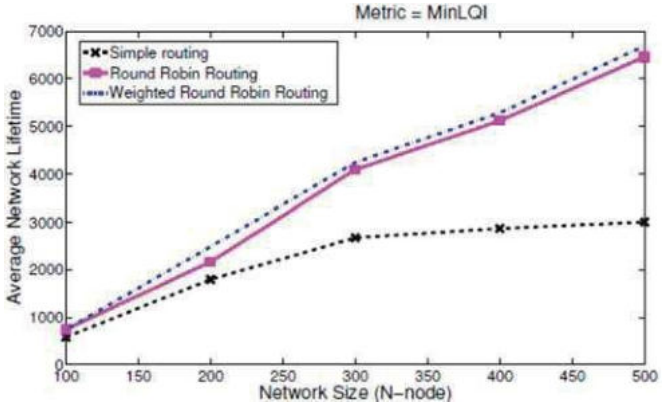


Fig. 1.35. Average network lifetime: Comparison of the three routing mechanisms using the MinLQI metric.

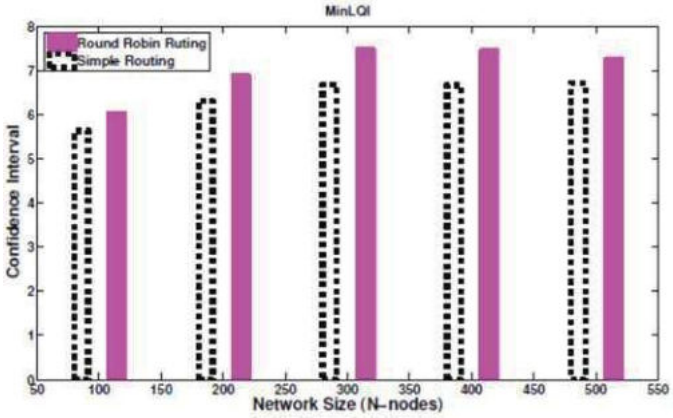


Fig. 1.36. Average network lifetime: confidence interval related to Fig. 1.35 for a confidence coefficient of 95 %.

Compared to the simple routing, the load balancing mechanisms Fig. 1.35 significantly increase the WSN lifetime. However, even if the weighted round robin routing leads to a better WSN lifetime than the round robin routing, the gap between the two load balancing mechanisms is not significant for the MinLQI metric Fig. 1.35.

By rotating the achtophorous node this helps splitting the load among different sensors. So, load balancing helps delaying the moment of the first node battery depletion of and therefore extending the lifetime of the network: Load balancing adds lifetime benefits to the WSN.

1.10.6. Average Ratio of the Remaining Energy

The Fig. 1.37 and Fig. 1.38 display the evolution average remaining energy after a complete cycle, when the network density is increasing. The cycle is constituted by: the network deployment, the detection of alarms and the data routing towards the base station where each source node uses L2RP to build its routing table. The cycle ends when all nodes have sent their alarms.

The degree of connectivity and MaxLQI metrics are the least energy efficient metrics Fig. 1.37. In contrast, Proximity-BS and MinLQI are the metrics that ensure better energy efficiency.

The weighted round-robin routing (W2R) leads to less energy consumption than the round-robin routing which is better than the simple routing whatever the metrics used. The Fig. 1.38 shows the result for the MaxLQI metric.

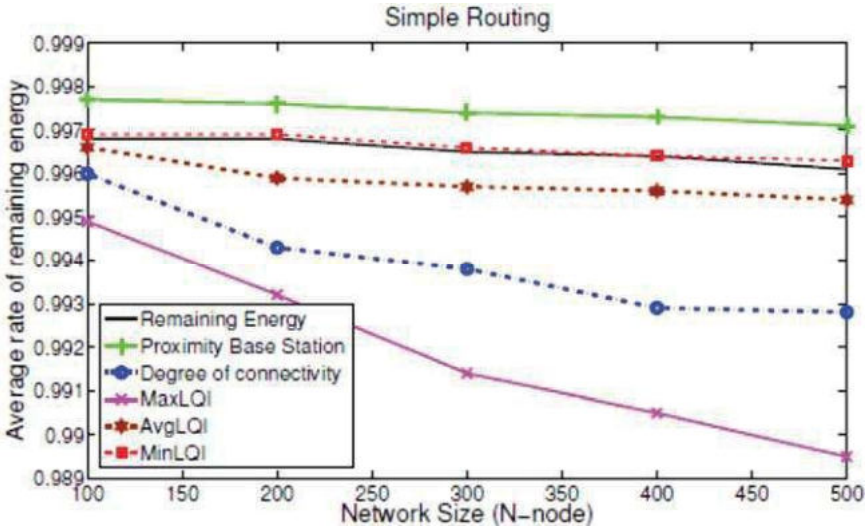


Fig. 1.37. The average ratio of the remaining energy: Comparison of the different metrics in the Simple Routing mechanism, after one cycle of which all sensors had sent their alarms towards the Base Station.

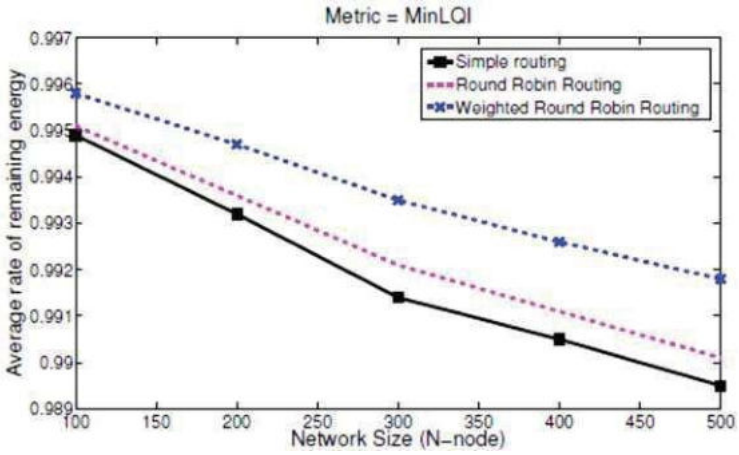


Fig. 1.38. The average ratio of the remaining energy: Comparison of the three routing mechanism with the MaxLQI metric, after one cycle of which all sensors had sent their alarms towards the Base Station.

In summary, these results are natural consequences of the previous ones. Indeed, for the MaxLQI metric of which the average number of hops (average path length) is high, the energy consumption is also large because of the increasingly overhearing, latency, and overhead phenomena.

1.10.7. Impacts of Increasing the Number of Achtophorous Nodes

The Fig. 1.39 shows the influence of the number (ANs) of the achtophorous nodes on the network lifetime performance criterion by comparing the results for *ANs = 3* and *ANs = 5*, when the remaining energy and MinLQI metrics are combined with the round-robin routing.

The Fig. 1.40 shows the influence of increasing the number (*ANs*) of the achtophorous nodes on the average percentage of lost packets by comparing results for *ANs = 3* and *ANs = 5*, when the W2R routing is run with the remaining energy and MinLQI metrics.

These two results Fig. 1.39 and Fig. 1.40 show that the average percentage of lost packets decreases for the MinLQI metric. The network lifetime increases for both metrics when the number of achtophorous nodes varies from 3 to 5. This is not obvious to predict, because increasing the number of achtophorous nodes might increase the risk of using low-energy sensors in routing process, which could cause more packet losses.

From a given number of achtophorous nodes, the result should be reversed. Nevertheless, until the value *AN = 5*, it remains within reasonable limits for a cold chain monitoring application.

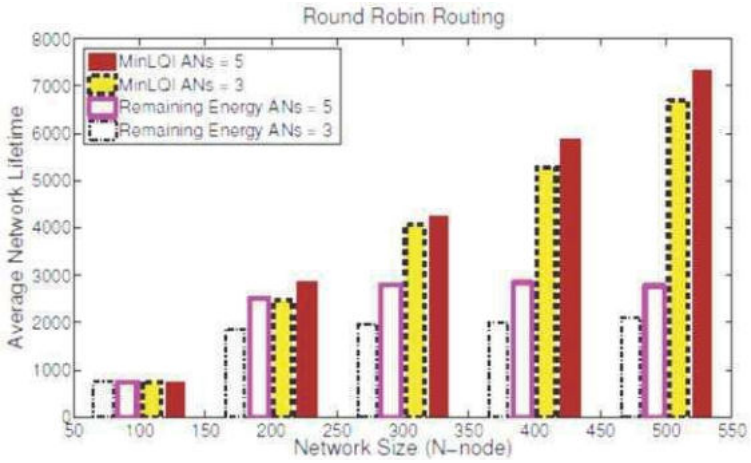


Fig. 1.39. Impacts of increasing the number of achtophorous nodes on the average network lifetime for the round-robin routing mechanism.

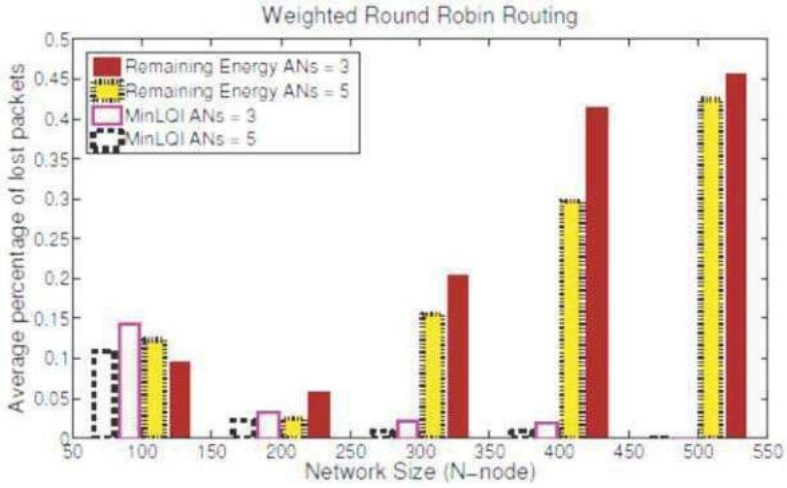


Fig. 1.40. Impacts of increasing the number of achtophorous nodes on the average percentage of packet losses for the W2R Routing mechanism.

1.10.8. Impacts of the Unreliability of Wireless Links

In the context of our application, the warehouse hosts hundreds of pallets, one upon the other. Each pallet is provided with a temperature sensor. This environment is subjected to the unreliably feature of the wireless links. In this section we take into account such a phenomenon. At any given time t, for a sensor S_i, its unreliable links ($P_r[\ell(i,j,t) = Unreliable] = 1$ in Formula (1.12)) with some neighbours are modelled by the Poisson process of parameter $\gamma(S_i,t)$ calculated as follows:

$$\gamma(S_i,t) = \frac{\mu}{\delta(S_i)}, \tag{1.17}$$

where $\delta(S_i)$ is the number of nodes located between the node S_i and the BS. If $\delta(S_i) = 0$, then the nodeS_i has no eligible achtophorous node.

At any given time t, for each sensor S_i, $\gamma(S_i, t)$ is too small, then the Poisson process returns a series T_i of integers T_i, in which nonzero values $T_i[j]$ denote the unreliable links formed by S_i with some of its neighbours S_j i.e. ($P_r[\ell(i,j,t) = Unreliable] = 1$ in Formula (1.12).

The Fig. 1.41 shows the effect of the unreliability of the wireless links on the WSN lifetime by comparing results for μ = 0.01 (low unreliability) and μ = 0.1 (high unreliability), when the MinLQI metric is used in the simple routing and in the round-robin routing. The Fig. 1.42 (resp. the Fig. 1.43) shows impacts on the average path length (resp. on the LIF) by comparing results for μ = 0.1 (high unreliability), when MinLQI metric is used in the three routing mechanisms.

The first result in Fig. 1.41, shows that the network lifetime is smaller in high unreliable WSN (μ = 0.1). In this case, the load balancing also increases the network lifetime. Indeed, the round-robin routing in high unreliable WSN (μ = 0.1) is much better than the simple routing in low unreliable links environment (μ = 0.01), even if the simple routing produces lower average path length Fig. 1.42 than load balancing mechanisms. Even in the context of high unreliable links, the load balancing routing produces better LIF than the simple routing Fig. 1.43, which means that the load is more evenly shared between nodes.

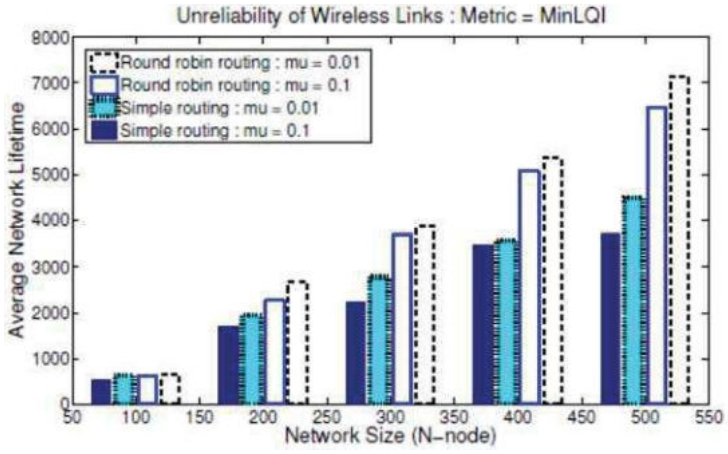


Fig. 1.41. Impacts of the unreliability of the wireless links on the average network lifetime (MinLQI, μ = 0.01 and μ = 0.1) for both simple and round robin routing mechanisms.

This result pertained to the MinLQI metric, clearly shows that the unreliability of the wireless links phenomena reduce the WSN lifetime because of more retransmissions needed in such an environment. But the key point of this result relies on the fact that load balancing mechanisms also add lifetime benefits in high unreliable environment. Indeed, in the case of simple routing, a weak link between a sensor and its achtophorous node involves the sending of a new "ROUTE REQUEST" message. In contrast, for load

balancing mechanisms, each sensor has several achtophorous nodes in its routing table. If a link between a sensor and its achtophorous node were to be unreliable, the source node first examines the quality of the link it forms with the next achtophorous node listed in its routing table. So, if this link is reliable, it simply sends the packet without having to request a new route.

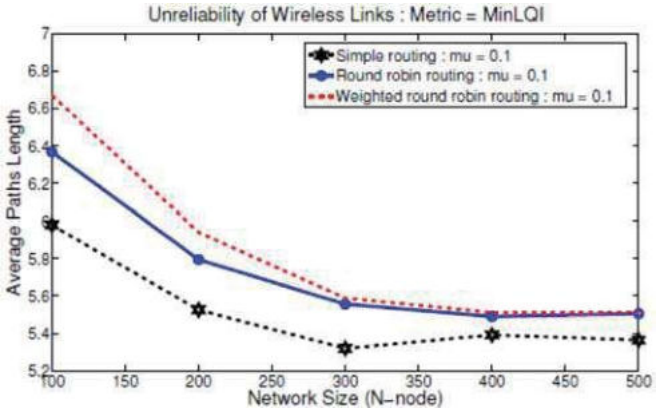


Fig. 1.42. Impacts of the unreliability of the wireless links on the average path length (MinLQI, μ = 0.1) for the three routing mechanisms.

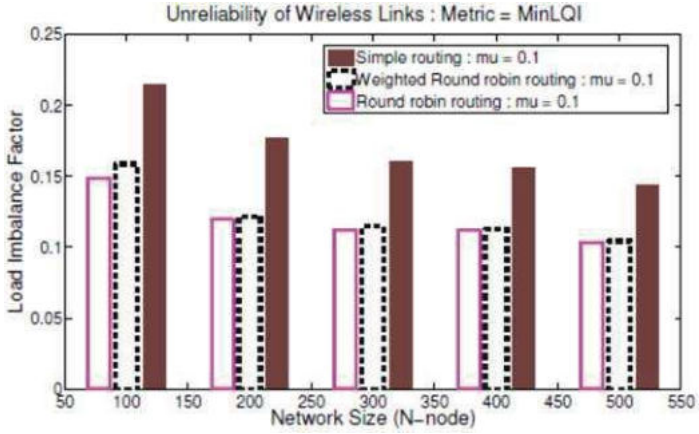


Fig. 1.43. Impacts of the unreliability of the wireless links on the Load Imbalance Factor (MinLQI, μ = 0.1) for both simple and load balancing routings.

Therefore, in load balancing mechanisms, a source node has to send a new "ROUTE REQUEST" message, if and only if all the links it forms with all the achtophorous nodes listed in its routing table were to become unreliable at the same time.

In the scenarios which do not take into account the unreliability of the wireless links, the L2RP protocol leads to identical routes for the two load balancing mechanisms Fig. 1.23. The Fig. 1.42 shows the impacts of the unreliability of the wireless links on the average

path lengths (number of hops) in an environment subjected to high unreliable links (μ = 0.1). In this result, we observe that the routes obtained with the round robin mechanism are now different from those obtained with the weighted round robin routing (W2R) Fig. 1.42. This is due by the fact that link quality parameters are very fickle and time variant and are greatly dependent on the poison parameter $\gamma(S_i, t)$ in formula (1.17).

The Fig. 1.43 plots, for μ = 0.1, the impacts of high unreliability of the wireless links on the LIF criterion performance. This still confirms the effectiveness of the load balancing mechanisms in unreliable environments. Indeed, the load imbalance factor (LIF) is lower for the round robin and W2R routing compared to the simple routing. Contrary to the previous result Fig. 1.27, this one Fig. 1.43 shows that the gap between the average LIF of the simple routing mechanism and those obtained via the load balancing routings decreases as the network density is increasing. Indeed, the unreliability of the wireless links become more and more important when the density of the WSN is increasing [3]. Consequently, load balancing mechanisms gradually begin to lose some of their interest.

1.11. Energy Over-Consumption Induced by Securing Routing Operations

1.11.1. Introduction and Backgrounds

Considering the fact that sensors are often dispersed in unprotected environments, WSNs are vulnerable to several types of intrusions and attacks. Thus, the proper functioning of the network might be compromised. In such hostile environments, the information exchanged between two communicating parties can include highly sensitive data that must be secured when sent through intermediate nodes. In the state of the art, there are currently several security mechanisms to ensure a good level of data protection as it flows from one source toward one (or more) destination(s) in the network.

Security solutions are usually based on cryptographic routines which help to ensure traditional security requirements such as confidentiality, integrity, availability and authentication [61]. Even for wireless sensor networks, cryptographic techniques [62-64] are used for protection purposes. But calculating crypto keys could push down WSNs performance. Security protocols designed for wired networks (such as DES, 3DES, AES, RSA, TLS, MD5, SHA-1, etc.) are generally not suitable for WSNs, because in such wireless networks, nodes have restricted capacity calculation (CPU), scanty capacity of memorization (RAM) and small energy supply. Thereby, security solutions must be custom sized and tightly adapted for wireless environments and especially for WSNs.

In this way, related works propose several security mechanisms for WSNs without caring about energy overconsumption induced by adding cryptography keys. We agree that such security solutions could naturally decrease network performance, but the real question is to understand in what proportion adding cryptography keys could affect network lifetime. Accordingly, in this chapter, we will evaluate the energy consumption induced by increasing the size of the packet when establishing cryptographic keys for wireless sensor networks, and then estimate the decrease rate of network performance.

We call unnecessary over-consumption of energy the consumption that can be avoided to maintain the energy of a sensor node. Energy efficiency is one of the most important issues in wireless sensor networks. Whatever the TCP/IP network layer (network access, internet, transport or application) considered, we must always take into account factors of energy consumption in order to develop an energy efficient protocol for WSNs. As a matter of fact, the major causes of energy losses are [3]: Collisions, Idle listening, Overhearing, Overmitting, Control packets overhead, Network protocols, Attacks and security issues, Cryptography and security solutions, etc.

Many attacks [65] are carried out against the sensor networks in order to exhaust the batteries of the nodes and then to reduce their lifetimes, and consequently that of the network. For instance, with a very high power transmitter node, an attacker can perform Hello Flood attack by broadcasting Hello messages on a large range to certain sensors of the network. Then sensors will try to respond to the attacker node which is actually out of range. In such a case attack, an attacker uses this mechanism to consume energy.

Security mechanisms, including cryptography [66-69], are aggravating factors of energy consumption in sensor networks. Many works are concerned with the establishment of cryptographic keys without worrying about key lengths. This is the strong point of cryptographic algorithms for wired networks. However, this becomes a major disadvantage in wireless sensor networks where the safeguarding of energy is a sine qua non condition for longer node and network lifetime.

Moreover, adding integrity key to secure routing protocol exchanges should increase packet size and therefore energy expenditure. In the next section, we will try to estimate how, that's to say in what proportion, adding an integrity key will cause energy exhaustion.

1.11.2. Energy Over-Consumption Induced by Adding an Integrity Key to L2RP

For routing protocols [70], nodes compute their routing table by exchanging messages in order to compare selection criteria also called metric [1-4, 71]. Then the node which has the lowest metric is chosen as next hop router. The network convergence is the fact that all nodes have successfully completed computing their routing table. Generally, the convergence occurs when all the routers in the routing domain agree on the routes that are available. Convergence time is the time that it takes for every router's routing table to synchronize after there has been a change in the network topology. It is important to ensure that the time taken is as short as possible because while the routers disagree on the available network, they cannot route data correctly or efficiently.

So, a commonly used WSN attack is to introduce malicious nodes in the network which will play the role of next hop routers by sending lowest criterion values (after a small period of sniffing network communications). In this way, traffic could be hijack toward the attacker platform. To avoid this type of security issue, one mechanism is to add integrity keys in order to secure communications between nodes. Integrity keys help ensuring authentication and message integrity in such a way that a malicious node will

not be able to perform this kind of attack. Most of algorithms providing integrity keys are designed for wired network and are not suitable for wireless sensor network operations because provided integrity keys are often too long. In this section, we aimed to show that integrity keys have non negligible energy cost and we'll estimate the rate of energy depletion induced by adding an integrity key in order to secure routing protocol processes. Firstly, we will present in the next section some types of common deployment WSN topologies we are using to run simulations.

The size of messages exchanged in the network has an effect on power consumption of transmitter and receiver nodes. Thus packet size should be neither too high nor too low. While it is small, the number of control packets (acknowledgment) increases. Otherwise, more transmission power is necessary for larger packet size.

In this work, we consider two routing different scenarios in which each sensor need to send a fixed number of packets before reaching network convergence:

- ***Scenario 1:*** each sensor node has to send 3 packets before network convergence. This is common to the most of the many WSN routing protocols, such as L2RP (with hello packet), in which sensors often exchange 1, 2 or 3 messages before computing its routing tables [2, 71].

- ***Scenario 2:*** each sensor node has to send 10 packets before network convergence. This scenario is not common to WSN routing protocols, but it's not an exaggeration if we consider all control packets needed for network auto-organization such as: initialization and authentication phase [72, 73], routing process, clustering formation [74, 75], data aggregation computation [76, 77], other security mechanisms [78-80], etc.

In each scenario, each packet has a fixed size length of 128 bits. Adding an integrity key whose length is equal to 5 % of the initial packet size, we obtain the results of the additional energy expenditure for the first scenario Fig. 1.46 to Fig. 1.48 following different deployment strategies and those of the second scenario in Fig. 1.49 to Fig. 1.51.

For all these results displayed in Fig. 1.46 to Fig. 1.51, the height of each bar highlights the energy over-consumption (in Joule) of a sensor node induced by adding an integrity key which size (7 bits) is equal to around 5 % of the initial package size (128 bits). The abscissa represents the number-id of each sensor. The energy consumption model used for simulations is the same than the Section 1.9.1 of this chapter, and can also be found in [1-3, 56, 57, 60, 81].

First of all, for the random deployment topology, it should be noted that the bars have different heights as shown in the Fig. 1.46 and Fig. 1.49. This results from the fact that each node has a number of neighbours that could be different from that of the other nodes. Because the deployment is random, some areas could be much more densely populated (so more neighbours) than others.

On the other hand, in the two scenarios, for the grid topology, the bars are grouped by several sets of bars having the same height Fig.1.47-1.51. This means that for each group, the concerned nodes have the same average power consumption. By zooming on each of the results concerning the type of grid topology, we obtain, for example, the Fig. 1.44. This will help us better understand these results.

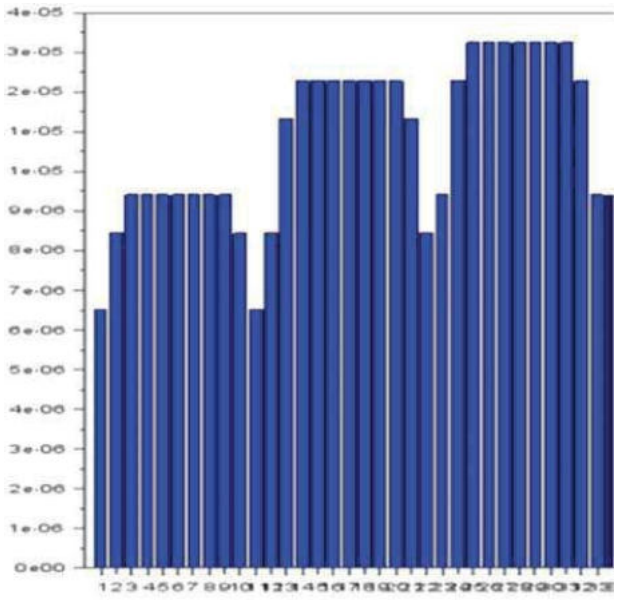


Fig. 1.44. A part of the zoom of the Fig. 1.48.

This results from the inherent properties of the uniform grid topology, where the nodes are numbered from the first row (which is defined by: $\forall x \in [0,100], y = 0$) to the last one ($\forall x \in [0,100], y = 100$), and for each row form the left ($x = 0$) to the right ($x = 100$). In fact, by observing the example illustrated in the Fig. 1.45.

- The first node and the last node of each row have the same number of neighbours. This explains why the node number 1 and the node number 11 have the same energy expenditure in the Fig. 1.44, Fig. 1.48 and Fig. 1.51.

- The second node and the penultimate node of each row have the same number of neighbours. This explains why the node number 2 and the node number 10 have the same energy expenditure in the Fig. 1.44, Fig. 1.48 and Fig. 1.51.

- For the first line, the nodes within the green rectangle (dashed line) Fig. 1.45 have the same number of neighbours. The same applies to the corresponding nodes for each of the other lines of the grid. This explains why all the nodes from the node number 3 to the node number 9 have the same energy expenditure in the Fig. 1.44, Fig. 1.48 and Fig. 1.51.

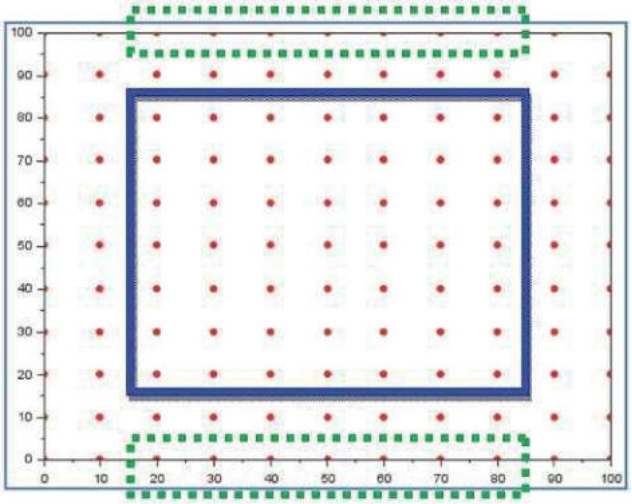


Fig. 1.45. Case of a uniform grid topology (X_{step} = Y_{step} = 10 m).

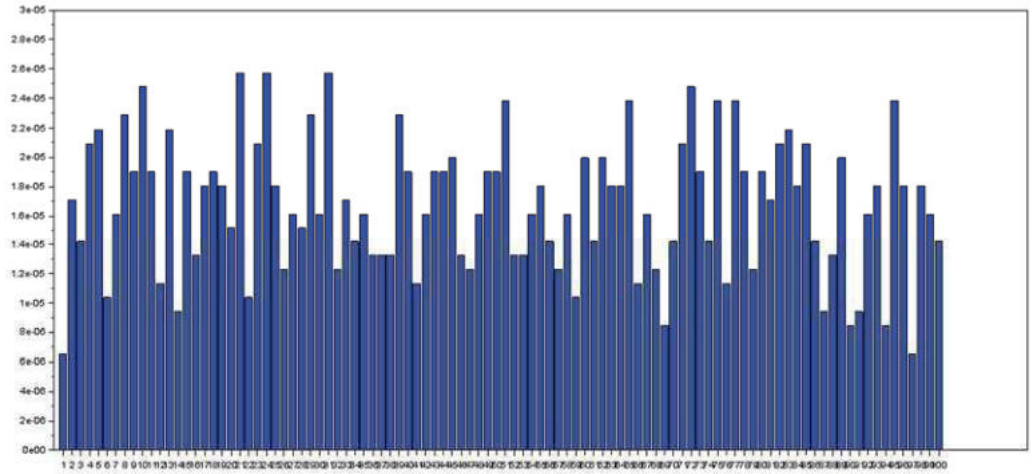


Fig. 1.46. Scenario 1: The energy over-consumption of each sensor node induced by adding an integrity key which size is equal to 5 % of the initial package size, in the case of a random deployment topology as described in Section 1.9.2. The simulation parameters are summarized in Table 1.5.

- All the nodes inside the blue rectangle (solid line) Fig. 1.45 have the same number of neighbours. Moreover, it is the nodes with the greatest number of neighbours in the grid. As a result, all lines affected by the blue rectangle (i.e. from the 3rd row to the 9th row) have the same average energy expenditure. This corresponds to the seven sets of bars having the highest height in the Fig. 1.48 and Fig. 1.51.

- The first set (and then the 11th set) of bars corresponds to the nodes of the first line (and then the 11th line) of the grid. Similarly, the 2nd set (and then the 10th set) of bars

corresponds to the nodes of the 2nd line (and then the 10th line) of the grid Fig. 1.48 and Fig. 1.51.

Table 1.5. Simulation parameters for random deployment topology.

Parameter	Value
Area Length	L = 100 m
Area Width	l = 60 m
Base Station Location	position(SB) = (0, 0)
Sensor transmission radio range	R = 20 m
Initial packet size	128 bits
Length of the added key integrity	7 bits

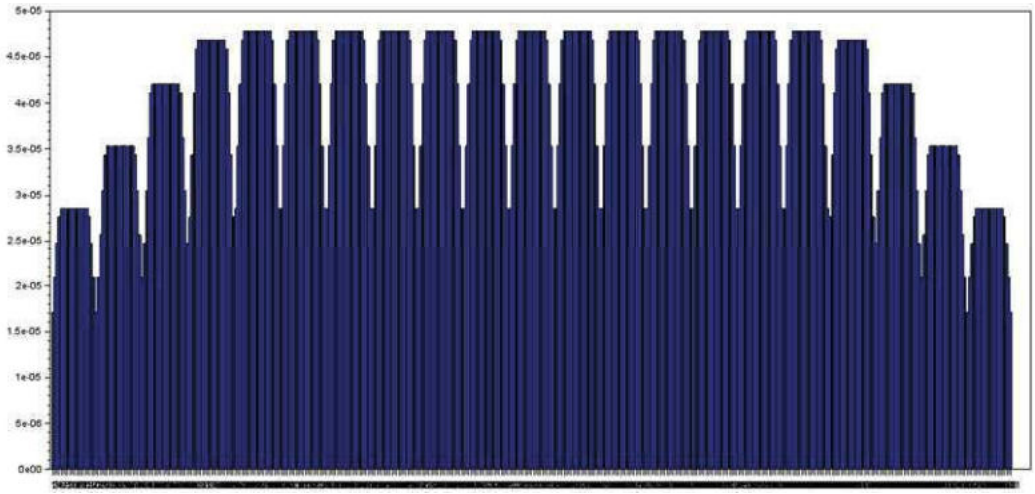


Fig. 1.47. Scenario 1: Energy over-consumption of each sensor node induced by adding an integrity key which size is equal to 5 % of the initial package size in the case of an uniform grid topology ($X_{step} = Y_{step} = 5$ m). The simulation parameters are summarized in Table 1.6.

Table 1.6. Simulation parameters for a uniform grid topology.

Parameter	Value
Area Length	L = 100 m
Area Width	l = 100 m
Base Station Location	position(SB) = (0, 0)
Sensor transmission radio range	R = 20 m
Initial packet size	128 bits
Length of the added key integrity	7 bits
Uniform grid topology	$X_{step} = Y_{step} = 5$ m

In each case of deployment topology specified in Fig. 1.46 to Fig. 1.51, we calculated the energy over-consumption of each sensor node induced by adding an integrity key which

size is equal to 5 % of the initial package size. The integrity key is added to each of the 3 or 10 packets exchanged during routing process before reaching the network convergence. Results show that the average rate of energy over-consumption per sensor is high despite the smallness of the integrity key.

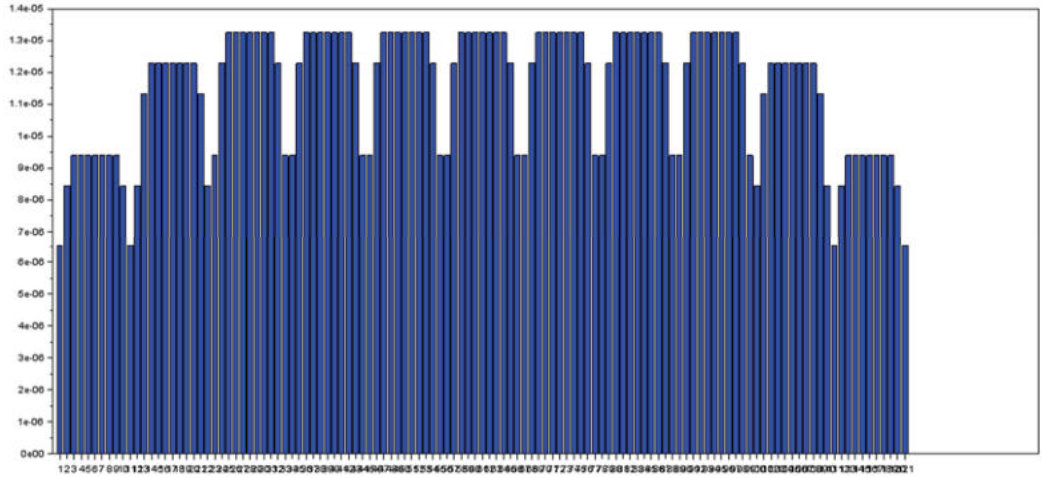


Fig. 1.48. Scenario 1: Energy over-consumption of each sensor node induced by adding an integrity key which size is equal to 5 % of the initial package size in the case of an uniform grid topology ($X_{step} = Y_{step} = 10$ m). The simulation parameters are summarized in Table 1.7.

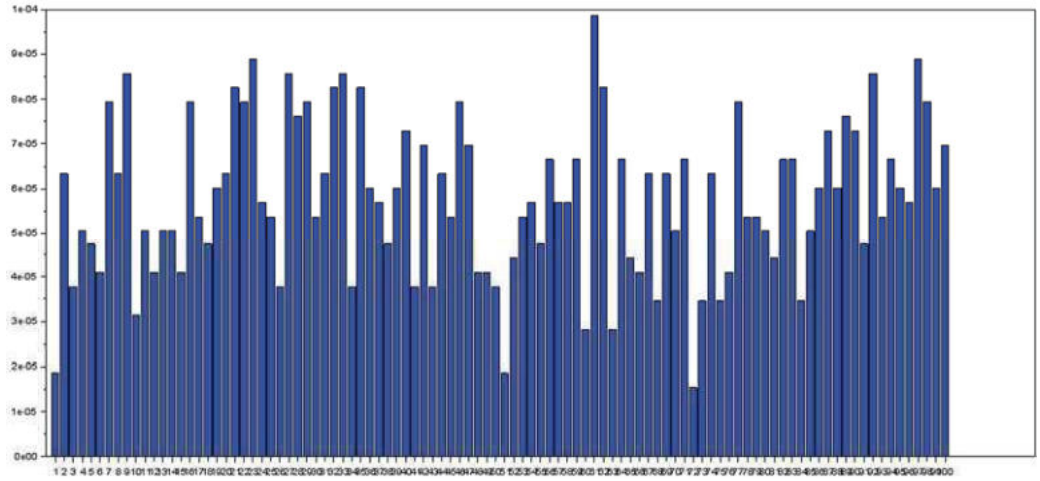


Fig. 1.49. Scenario 2: The energy over-consumption of each sensor node induced by adding an integrity key which size is equal to 5 % of the initial package size in the case of the random deployment topology. The simulation parameters are summarized in the Table 1.5.

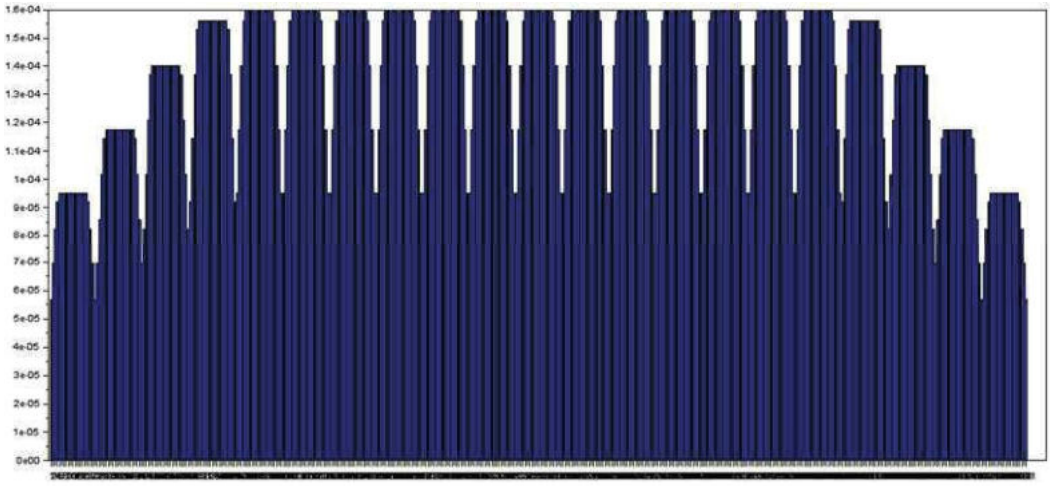


Fig. 1.50. Scenario 2: Energy over-consumption of each sensor node induced by adding an integrity key which size is equal to 5 % of the initial package size in the case of an uniform grid topology (X_{step} = Y_{step} = 5 m). The simulation parameters are summarized in the Table 1.6.

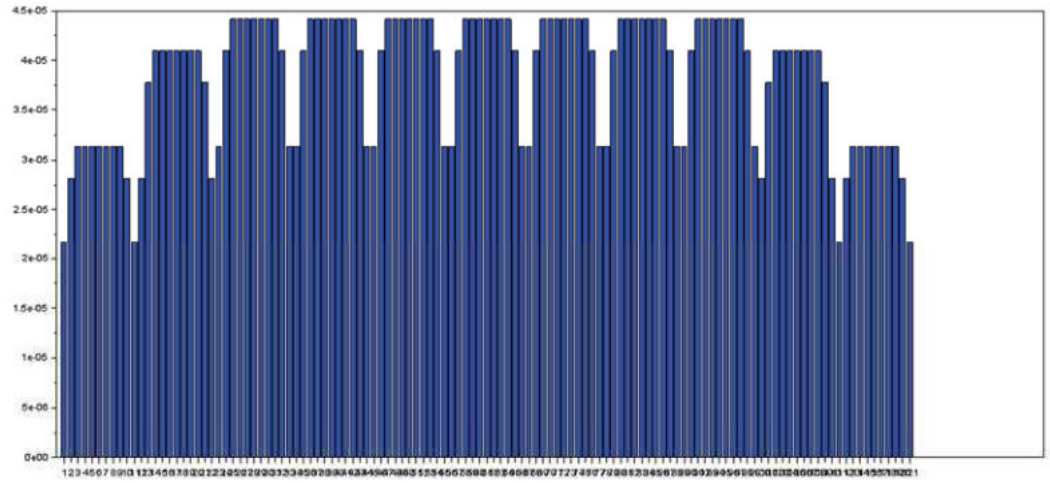


Fig. 1.51. Scenario 2: Energy over-consumption of each sensor node induced by adding an integrity key which size is equal to 5 % of the initial package size in the case of an uniform grid topology (X_{step} = Y_{step} = 10 m). The simulation parameters are summarized in the Table 1.7.

Consequently, we calculated Table 1.8 the average number of additional packets each sensor would be able to send with this amount of energy over-consumption in the absence of the integrity key.

Table 1.7. Simulation parameters for a uniform grid topology.

Parameter	Value
Area Length	L = 100 m
Area Width	l = 100 m
Base Station Location	position(SB) = (0, 0)
Sensor transmission radio range	R = 20 m
Initial packet size	128 bits
Length of the added key integrity	7 bits
Uniform grid topology	Xstep = Ystep = 10 m

Table 1.8. The average number of additional packets that each sensor would be able to send if the routing protocol were not being secure with the integrity key.

Deployment topology			Scenario 1	Scenario 2
Random deployment topology		Average number of additional packets	4	16
		computed from the results displayed in the figures	Fig. 1.46	Fig. 1.49
Uniform grid topology	Xstep = Ystep = 5 m	Average number of additional packets	8	25
		computed from the results displayed in the figures	Fig. 1.47	Fig. 1.50
	Xstep = Ystep = 10 m	Average number of additional packets	4	7
		computed from the results displayed in the figures	Fig. 1.48	Fig. 1.51

These results point out that in both scenario and for the two deployment topologies, the energy required for the added integrity key is sufficient to run the routing protocol again. That's to say that it is more energy-expensive to secure the routing protocol than running it again.

The energy over-consumption of each sensor node is more important as the network density becomes larger (Fig. 1.47 and Fig. 1.48 in comparison with Fig. 1.50 and Fig. 1.51). Moreover, when the average number of neighbours is increasing in the network, as a consequence of the increase of the network density, the eavesdropping and the overhearing phenomena could then constitute aggravating factors in energy consumption. For uniform grid deployment topologies, moving from $\{X_{step} = Y_{step} = 10$ m$\}$ to $\{X_{step} = Y_{step} = 5$ m$\}$ has the effect to increase the average number of neighbours in the network. This explains the fact that the energy expenditure is almost multiplied by a factor of 2 in the results Fig. 1.47 with respect to Fig. 1.48 and Fig. 1.50 with respect to Fig. 1.51.

Thus, as we can see, providing a small integrity key, whatever the type of the deployment topology considered, greatly increases energy consumption. On the other hand, even if

decreasing the node deployment density results in a decrease in average energy consumption due to Collisions, Idle listening, Overhearing, Overmitting, etc., one must still avoid in exaggeratedly swerving the positions of the nodes on the deployment area. As this may result in increased loss of connectivity due to the unreliability feature of the wireless links, which could increase the phenomenon of packets losses and retransmissions, and then annihilates quality of service while increasing energy exhaustion. So one should be careful with this, and operate to moderately swerve the positions of the sensors in a real environment.

1.12. Conclusions

In this work, we have proposed the L2RP routing protocol (Link Reliability based Routing Protocol) which takes into account the quality of the links formed by any source node with the achtophorous nodes listed in its routing table. This avoids sending data over a link disrupted, unreliable or unstable.

The L2RP protocol also includes load balancing mechanisms where the source node, based on "ROUTE REPLY" packets, is able to estimate the load sustainable by each of its achtophorous node. This property allows L2RP to avoid doing a per packet load-balancing by the source, as done in [55], where the source node sends its data without being sure of the capacity of the achtophorous node to sustain the load assigned. Thus, by doing so, L2RP helps to reduce packet losses.

Applications often have their specific objectives and constraints, so it is essential to have the choice between several possible settings when deploying a wireless sensor networks. Thus, in its design, the L2RP protocol can use any chosen metric. This allows L2RP to be able to support different applications by offering the choice of the metric which ensures the best performance in the specific context of each application.

We therefore evaluated the L2RP performance based on routing mechanisms (simple or load balancing) and then presented a comparative study of the different metrics in each routing mechanisms. This work has shown that:

The degree of connectivity metric is the metric that leads to the highest percentage of packet losses. This metric also has the lowest network lifetime. Indeed, it is the metric which is the most sensitive to the overhearing phenomenon.

The Proximity-BS metric provides better energy efficiency. With this metric, the alarms sent by any sensor reach the Base Station in fewer hops. By minimizing the number of hops, it helps in reducing energy wastefulness due to overhearing, overhead and latency.

The LQI used as a metric by considering the best link quality (the MaxLQI metric) leads to an inefficient routing regardless of the performance criterion considered. This confirms our previous experimental results obtained in [25]. The MaxLQI metric matches the standard definition of the LQI used in the MultiHopLQI routing algorithm [29]. Indeed, this metric is characterized by a relatively high average number of hops. In the absence of

obstacles and any interference, the best link quality is often observed for the nodes which are located relatively close to each other. By multiplying the number of hops, the MaxLQI metric has the effect to increase energy wastefulness due to overhearing, overhead and latency.

Accordingly, despite its popularity in WSN empirical analysis based on TinyOS platforms, the MultiHopLQI routing algorithm is not suitable for WSN applications, because it uses the MaxLQI metric for route selection.

By setting a given LQI threshold, i.e. a value of acceptable LQI, and considering the lowest LQI value beyond this threshold (the MinLQI metric), we obtain an optimal LQI based metric which highly enhances the energy efficiency. As the LQI decreases when the distance between the nodes increases, the average path length is larger for MaxLQI than for MinLQI: this explains why MinLQI is more energy-efficient than MaxLQI. Then, the average percentage of packet losses is larger for MaxLQI. There is a trade-off between routes consisting of good links quality and small average path length (i.e. without too many retransmissions).

This interesting result shows that it is better for LQI based routing algorithm to promote links of intermediate quality (such as MinLQI metric) to avoid:

The better links which are synonymous of nodes located relatively close to each other and also synonymous of higher number of routing hops which are responsible for excessive energy consumption;

The bad links (low quality) which are synonymous of higher percentage of packet losses.

The load balancing mechanisms significantly improve the routing efficiency by extending the network lifetime, while minimizing the average percentage of packet losses. The load balancing also helps evenly splitting the load on all nodes in the WSN.

Increasing the number of achtophorous nodes improves the network performance: a low average of packet losses and a longer network lifetime.

The composite metric, resulting of the remaining energy metric combined with the Proximity-BS metric, offers good routing performance. This metric is interesting, as each node ignores the settings of its neighbours (such as the remaining energy, the position) when selecting its achtophorous nodes.

Since it is LQI based routing algorithm, the question that naturally arises is how L2RP behave in an environment subjected to high unreliability of the wireless links. Simulation results have shown that, such an environment slightly impacts the L2RP efficiency. Generally, packet loss percentage is relatively low because in L2RP a source node avoids sending data to an achtophorous node with which it forms an unreliable link at the moment it has data to transmit.

Embedded with load balancing mechanisms, L2RP adds lifetime benefits to the wireless sensor network. Nevertheless, it would be more profitable to combine L2RP with aggregation techniques like cluster formation and data aggregation in order to gain more scalability and lifetime. So, in [60] we have used L2RP in a cold chain monitoring application where regular sensors send alarms to their respective clusterheads, which aggregate received alarms and then forward the aggregated data towards the BS using the L2RP routing protocol. In this application L2RP is run with the weighted round robin load balancing mechanism using the "MinLQI" metric.

On the other hand, in this report, we show that how the energy over-consumption induced by securing network operations is high. We added a small integrity key (7 bits) which length is equal to 5 % of the initial packet size (128 bits) in order to secure the routing tables' computation process. Simulation results for two deployment strategies allow us to conclude that adding integrity key, for network operations security, significantly increases the energy consumption of sensors and therefore reduces network performance. Even if there is lot of works on lightweight cryptography [61] and [82], which concerns the science of small cryptography keys, it is still found that many works continue offering relatively long keys with respect to the size of the protected data without caring about energy over-consumption.

Acknowledgements

This research was supported by:

- SAMOVAR CNRS Research Lab – UMR 5157; Dept. Réseaux et Services de Télécommunications (RST); Télécom & Management SudParis, Evry, France. I would like to thank Prof. Monique Becker and Prof. Michel Marot of Télécom & Management SudParis. I am more than grateful to them for their help. (http://www.telecom-sudparis.eu/);

- Centre d'Excellence en Mathématiques, Informatique et TIC (CEA-MITIC); UFR Sciences appliquées et de Technologies (UFR SAT), Université Gaston Berger, Saint-Louis, Sénégal. (http://www.ceamitic.sn/).

References

[1]. C. Diallo, M. Marot, M. Becker, Efficiency benefits through load-balancing with link reliability based routing in WSNs, *Journal on Advances in Networks and Services*, Vol. 3, No. 3&4, 2010, pp. 430-446.

[2]. C. Diallo, M. Marot, M. Becker, Link quality and local load balancing routing mechanisms in wireless sensor networks, in *Proceedings of the 6th Advanced International Conference on Telecommunications (AICT'10)*, Barcelona, Spain, May 2010, pp. 306-315.

[3]. C. Diallo, Techniques d'amélioration du routage et de la formation des clusters multi-*sauts* dans les réseaux de capteurs sans fil., PhD Thesis, *Télécom & Management SudParis*, Evry, France 2010.

[4]. M. T. Sow, C. Diallo, Energy over-consumption Induced by securing network operations, in *Proceedings of the 2nd International Conference on Frontiers of Sensors Technologies (ICFST'17)*, Shenzhen, China, April 2017.
[5]. ZigBee Specificationv1.0, *ZigBee Alliance*, USA, June 2005.
[6]. TinyOs Community Forum, http://www.tinyos.net/
[7]. Tmote Sky datasheet, http://www.moteiv.com/products/docs/tmote-skydatasheet.pdf
[8]. Sun SPOT World, http://www.sunspotworld.com
[9]. Sun SPOT, smartsantander, http://www.smartsantander.eu/wiki/index.php/Main/Sunspot
[10]. EasySen WiEye Sensor Board, http://www.easysen.com/wieye.htm
[11]. Crossbow sensor platform, http://www.xbow.com/)
[12]. Micaz datasheet, http://www.openautomation.net/uploadsproductos/micaz_datasheet.pdf
[13]. Jennic Wireless Microcontrollers, http://www.jennic.com/index.php
[14]. Jennic Wireless Microcontrollers, http://www.glyn.com.au/HF_Opto_Jennic.htm
[15]. Jennic Wireless Microcontrollers, http://www.glyn.com.au/PR01062007_Jennic.htm
[16]. TinyNode Sensors, http://www.tinynode.com/
[17]. T-Node de SOWNet, http://www.sownet.nl/
[18]. TinyNode 584, http://www.tinynode.com/?q=product/tinynode584/tn-dev584
[19]. BTnode rev 3, http://www.btnode.ethz.ch/Documentation/BTnodeRev3SensorGuide
[20]. Silicon Labs, http://www.silabs.com/Pages/default.aspx
[21]. Microchip Wireless Devices, http://www.microchip.com/
[22]. WSN architecture illustration, http://vlssit.iitkgp.ernet.in/ant/ant/8/theory/
[23]. I. F. Akyildiz, S. Weilian, Y. Sankarasubramaniam, E. Cayirci, A survey on sensor networks, *IEEE Communications Magazine*, Vol. 40, Issue 8, 2002, pp. 102-114.
[24]. C. Diallo, A. Gupta, M. Becker, M. Marot, Energy aware database updating protocols for autoconfigurable sensor networks, in *Proceedings of the 8th International Conference on Networks GlobeNet 2009(ICN'09),* Cancun, Mexico, Mar. 2009, pp. 138-143.
[25]. A. Gupta, C. Diallo, M. Marot, M. Becker, Understanding topology challenges in the implementation of wireless sensor network for cold chain, in *Proceedings of the IEEE Radio and Wireless Symposium(RWS'10)*, New Orleans, LA, USA, 2010, pp. 376-379.
[26]. Wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (wpans), IEEE Std 802.15.4-2006, *IEEE Computer Society*, 2006.
[27]. CC2420 Radio, http://www.chipcon.com redirect to http://www.ti.com
[28]. MultiHopLQI, http://www.tinyos.net/tinyos-1.x/tos/lib/MultiHopLQI
[29]. J. Polastre, J. Hui, J. Z. P. Levis, D. Culler, S. Shenker, I. Stoica, A unifying link abstraction for wireless sensor networks, in *Proceedings of the 3rdInternational Conference on Embedded Networked Sensor Systems (SenSys'05)*, 2005, pp. 76-89.
[30]. A. Woo, T. Tong, D. Culler, Taming the underlying challenges of reliable multihop routing in sensor networks, in *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems(SenSys'03)*, Los Angeles, CA, USA, 2003, pp. 14-27.
[31]. M. Becker, A.-L. Beylot, R. Dhaou, A. Gupta, R. Kacimi, M. Marot. Experimental study: Link quality and deployment issues in wireless sensor networks, in *Proceedings of the 8thInternational IFIP-TC 6 Networking Conference (NETWORKING'09)*, LNCS 5550, Aachen, Germany, 2009, pp. 140-25.
[32]. D. Puccinelli, M. Haenggi, Lifetime benefits through load balancing in homogeneous sensor networks, in *Proceedings of the IEEE Wireless Communications and Networking Conference(WCNC'09)*, Budapest, Hungary, April 2009.
[33]. D. Puccinelli, M. Haenggi, Arbutus: Network-layer load balancing for wireless sensor networks, in *Proceedings of the IEEE Wireless Communications and Networking Conference(WCNC'08)*, Las Vegas, NV, USA, March 2008, pp. 2063-2068.

[34]. D. Lal, A. Manjeshwar, F. Herrmann, E. Uysal-Biyikoglu, A. Keshavarzian, Measurement and characterization of link quality metrics in energy constrained wireless sensor networks, in *Proceedings of the IEEE Global Communications Conference(Globecom'03)*, San Francisco, USA, 2003, pp. 446-452.

[35]. J. Zhao, R. Govindan, Understanding packet delivery performance in dense wireless sensor networks, in *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys'03)*, CA, USA, 2003, pp. 1-13.

[36]. D. Son, B. Krishnamachari, J. Heidemann, Experimental analysis of concurrent packet transmissions in low-power wireless networks, in *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys'06)*, Colorado, USA, 2006, pp. 237-250.

[37]. G. Zhou, T. He, J. Stankovic, T. Abdelzaher, Rid: Radio interference detection in wireless sensor networks, in *Proceedings of the IEEE24th Annual Joint Conference of the IEEE Computer and Communications Societies (Infocom'05)*, Miami, USA, 2005, pp. 891-901.

[38]. S. Singh, M. Woo, C. Raghavendra, Power-aware routing in mobile ad hoc networks, in *Proceedings of the 4thAnnual ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom'98)*, Dallas, Texas, USA, 1998, pp. 181-190.

[39]. K. Scott, N. Bamboos, Routing and channel assignment for low power transmission in pcs, in *Proceedings of the 5th IEEE International Conference on Universal Personal Communications (ICUPC'96)*, Cambridge, USA, 1996, pp. 498-502.

[40]. R. Shah, J. Rabaey, Energy aware routing for low energy ad hoc sensor networks, *In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC'02)*, Orlando, Florida, USA, March 2002, pp. 350-355.

[41]. J. Chang, L. Tassiulas, Maximum lifetime routing in wireless sensor networks, *IEEE/ACM Transactions on Networking*, Vol. 12, 609619.

[42]. F. Othman, N. Bouabdallah, R. Boutaba, Load-balanced routing scheme for energy -efficient wireless sensor networks, in *Proceedings of the IEEE Global Telecommunications Conference (Globecom'08)*, New Orleans, LA USA, 2008, pp. 1-6.

[43]. S. Toumpis, S. Gitzenis, Load balancing in wireless sensor networks using Kirchhoff's voltage law, in *Proceedings of the IEEE INFOCOM'2009*, Rio de Janeiro, Brazil, 2009, pp. 1656-1664.

[44]. J. Gao, L. Zhang, Load balanced short path routing in wireless networks, in *Proceedings of the IEEE INFOCOM 2004*, Hong Kong, China, 2004.

[45]. Z. Wang, E. Bulut, B.K. Szymanski, Energy efficient collision aware multipath routing for wireless sensor networks, in *Proceedings of the IEEE International Conference on Communications (ICC'09)*, Dresden, Germany, 2009.

[46]. L. Popa, C. Raiciu, I. Stoica, D.S. Rosenblum, Reducing congestion effects by multipath routing in wireless networks, in *Proceedings of the 14th IEEE International Conference on Network Protocols(ICNP'06)*, Santa Barbara, USA, 2006, pp. 96-105.

[47]. C. Wu, R. Yuan, H. Zhou, A novel load balanced and lifetime maximization routing protocol in wireless sensor networks, in *Proceedings of the IEEE Vehicular Technology Conference (VTC'08)*, Singapore, 2008, pp. 113-117.

[48]. K. Sha, J. Du, W. Shi, Wear: A balanced, fault-tolerant, energy aware routing protocol for wireless sensor networks, in*ternational Journal of Sensor Networks*, Vol. 1, Issue 3-4, 2006, pp. 156-168.

[49]. I. Raicu, L. Schwiebert, S. Fowler, S.K.S. Gupta, Local load balancing for globally efficient routing in wireless sensor networks, in*ternational Journal of Distributed Sensor Networks*, Vol. 1, 2005, pp. 163-185.

[50]. R. Vidhyapriya, P.T. Vanathi, Energy efficient adaptive multipath routing for wireless sensor networks, *IAENGInternational Journal of Computer Science*, Vol. 34, Issue 1, 2007.

[51]. V.C. Gungor, C. Sastry, Z. Song, R. Integlia, Resource-aware and link quality based routing metric for wireless sensor and actor networks, in *Proceedings of the IEEE International Conference on Communications(ICC'07)*, Glasgow, Scotland, 2007, pp. 3364-3369.

[52]. S. Hussain, A. W. Matin, Hierarchical cluster-based routing in wireless sensor networks, in *Proceedings of the IEEE/ACM International Conference on Information Processing in Sensor Networks (IPSN'06)*, Nashville, TN, USA, 2006, pp. 335-344.

[53]. D. Nam, H. Min, An energy -efficient clustering using a roundrobin method in a wireless sensor network , in *Proceedings of the 5thACIS International Conference on Software Engineering Research, Management & Applications(SERA'07)*, 2007, pp. 54-60.

[54]. D. Choi, J. Shen, S. Moh, I. Chung, Virtual cluster routing protocol for wireless sensor networks, in *Proceedings of the International Conference on Parallel and Distributed Computing and Networks (PDCN'09)*, Innsbruck, Austria, 2009.

[55]. M.O. Rashid, M.M. Alam, A. Razzaque, C.S. Hong, Reliable event detection and congestion avoidance in wireless sensor networks, in *Proceedings of the High Performance Computing Conference(HPCC'07)*, Houston, Texas, USA, 2007, pp. 521-532.

[56]. W.B. Heinzelman, A. Chandrakasan, H. Balakrishnan, An application-specific protocol architecture for wireless microsensor networks, *IEEE Transactions on Wireless Communications*, Vol. 1, Issue 4, October 2002, pp. 660-670.

[57]. C. Diallo, A. Gupta, M. Marot, M. Becker, Virtual base station election for wireless sensor networks, in *Proceedings of the 8thInternational Conference on New Technologies in Distributed Systems (NOTERE'08)*, Vol. 2, Lyon, France, Jun. 2008.

[58]. J. Blumenthal, R. Grossmann, F. Golatowski, D. Timmermann, Weighted centroid localization in ZigBee-based sensor networks, in *Proceedings of the IEEE International Symposium on Intelligent Signal Processing(WISP'07)*, 2007.

[59]. M. Becker, A.L. Beylot, Simulation des Réseaux (Traité IC2, Série Réseaux et Télécoms), *Hermes*, 2006.

[60]. C. Diallo, M. Marot, M. Becker, Single-node cluster reduction in WSN and energy -efficiency during cluster formation, in *Proceedings of the 9th IFIP Annual Mediterranean Ad Hoc Networking Workshop(Med-Hoc-Net'10)*, Juan-Les-Pins, France, June. 2010.

[61]. C. Manifavas, G. Hatzivasilis, K. Fysarakis, K. Ranto, Lightweight cryptography for embedded systems - a comparative analysis, in *Proceedings of the 8th International Workshop on Data Privacy Management and Autonomous Spontaneous Security* , Vol. 8247, 2014, pp. 333-349.

[62]. Y. Lu, L. Li, H. Peng, Y. Yang, An energy efficient mutual authentication and key agreement scheme preserving anonymity for wireless sensor networks, *Sensors*, Vol. 16, Issue 6, 2016, E837.

[63]. M. Turkanovi´c, B. Brumen, M. Hölbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion, *Ad Hoc Networks*, Vol. 20, 2014, pp. 96-112.

[64]. R. Amin, G. P. Biswas, A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks, *Ad Hoc Netw.*, Vol. 36, Issue P1, January 2016, pp. 58–80.

[65]. J. Vijay, Daniel K.Venkatraman, G. Murugaboopathi, Various attacks in wireless sensor network: survey, in*ternational Journal of Soft Computing and Engineering*, Vol. 3, 2013.

[66]. H. K. Patil, S. A. Szygenda, Security for Wireless Sensor Networks using Identity-Based Cryptography, *CRC Press*, 2012.

[67]. C. Alcaraz, R. Roman, J. Lopez, A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes, *Mobile Networks and Applications*, Vol. 12, Issue 4, 2007, pp. 231-244.

Advances in Networks, Security and Communications: Reviews, Volume 1

Sergey Y. Yurish, Editor

The 1st volume of new *'Advances in Networks, Security and Communications: Reviews'* Book Series contains 15 chapters submitted by 42 contributors from academia and industry from 13 countries: Brazil, Bulgatia, Burkina Faso, China, Czech Republic, France, India, Iran, Japan, Mauritius, Senegal, UK, and USA. The book is divided into 3 main parts: Networks (4 chapters), Security (4 chapters) and Communication (7 chapters). The book provides focused coverage of these 3 main technologies.

Chapters are written by experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise. Coverage includes wireless sensor network routing improvement; connectivity recovery, augmentation and routing in wireless Ad Hoc networks; advanced modeling and simulation approach for the sensor networks management; security aspects for mobile agent and cloud computing; various communication aspects (algorithms, coding and hardware design) and others.

This book ensures that our readers will stay at the cutting edge of the field and get the right and effective start point and road map for the further researches and developments. By this way, they will be able to save more time for productive research activity and eliminate routine work.

This book will be a valuable tool in both learning how to design various networks, as well as a reference as an advance in readers' research careers.

ISBN 978-84-697-8993-3

