



HAL
open science

Wireless body-to-body sensor networks : optimization models and algorithms

Amira Meharouech Ali

► **To cite this version:**

Amira Meharouech Ali. Wireless body-to-body sensor networks : optimization models and algorithms. Networking and Internet Architecture [cs.NI]. Université Sorbonne Paris Cité, 2016. English. NNT : 2016USPCB122 . tel-02147467

HAL Id: tel-02147467

<https://theses.hal.science/tel-02147467v1>

Submitted on 4 Jun 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Wireless Body-to-Body Sensor Networks: Optimization models and Algorithms

By
Amira MEHAROUÉCH ALI

A dissertation submitted in partial fulfillment of the requirements for
the degree of

Doctor of Philosophy

In

COMPUTER SCIENCE

Paris Descartes University, Paris, France

Prepared at LIPADE

<i>Jury :</i>	Professor	Dritan NACE, Université de Technologie de Compiègne
	Dr HDR	Abderrezak RACHEDI, Université Paris-Est Marne La vallée
	Professor	Tijani CHAHED, Institut MINES-TELECOM, Paris
	Professor	Anne WEI, Conservatoire National des Arts et Métiers, Paris
	Professor	Fabio MARTIGNON, Université Paris-Sud
	Professor	Norbert NOURY, Université de Lyon
<i>Thesis Advisor:</i>	Professor	Ahmed MEHAOUA, Université Paris Descartes, Paris
<i>Co-supervisor:</i>	Doctor	Jocelyne ELIAS, Université Paris Descartes, Paris

Abstract

Motivated by the rising demand for remote and improved healthcare, while decreasing the cost of using network infrastructures to ensure time and data rate-constrained applications, Wireless Body Area Networks (WBANs) still form a strongly growing research field. Besides, engineers and researchers are investigating new solutions to supplement mobile communications through developing opportunities for cooperative WBANs. In this context, using network users themselves as relays could complement and extend existing infrastructure networks, while improving network capacity and promoting radio spectrum usage. Yet, network operators, that are already planning for the Internet of Things (IoT) and cloud computing technologies integration, should also think about this new possibility of creating a new type of mobile ad hoc network, where network users themselves are used as simplified ad hoc base stations, to fulfill the desire of sharing real-time information between colocated persons carrying body sensors. This emerging type of network is called Body-to-Body Network (BBN). In a BBN, a radio device situated on one person gathers the sensor data from the sensor nodes worn by that person, and transmit them to a transceiver situated on another person in the nearby area, in order to be processed or relayed to other BBN users. BBNs can find applications in a range of areas such as healthcare, team sports, military, entertainment, as well as exciting social networking experiences. Operating in the popular Industrial, Scientific and Medical (ISM) band, the communication links in a BBN will be heavily susceptible to interference between the different radio technologies sharing the limited radio spectrum. Thus, inter-body interference become an important concern for protocol design and quality of service for the BBN end user. Yet, higher layer MAC and networking mechanisms need to be in place to overcome this interference problem. To date, very few studies, that perform in-depth analysis of this type of body-centric scenario, exist. The interference problem in such distributed system, should be tackled with distributed mechanisms, such as Game Theory. The decision makers in the game are either the WBANs/people forming the BBN or the network operators who control the inter-WBAN communicating devices. These devices have to cope with a limited transmission resource (ISM band) that gives rise to a conflict of interests .

This thesis aims at exploring the opportunities to enable inter-WBAN communications by ensuring feasible sharing of the radio spectrum through two challenging research issues. First, *mutual and cross-technology interference mitigation*, and second, *the design of a BBN specific routing protocol* applied to an epidemic control application within mass gathering areas, such as the airport, as use case in this thesis. In a first phase, a game theoretical approach is proposed to resolve the distributed interference problem in BBNs. The Socially-aware Interference Mitigation (SIM) game performs twofold: at the WBAN stage, it allocates ZigBee channels to body sensors for intra-WBAN data sensing, and at the BBN stage, it allocates WiFi channels to mobile devices for inter-WBAN data transmitting and relaying. Two algorithms, BR-SIM and SORT-SIM, were developed to search for Nash equilibria to the SIM game. The first (BR-SIM) ensures best response solutions while the second (SORT-SIM) attempts to achieve tradeoff between sub-optimal solutions and short convergence time. Then, in order to highlight the social role of BBNs, the second part of this thesis is devoted to propose an epidemic control application tailored to BBNs, in indoor environment. This application implements a geographic routing protocol, that differentiates WBANs traffic and ensures real-time quarantine strategies. Such BBN application could help government agencies like National Institutes of Health (NIH) and authorities such as World Health Organization (WHO) to take swift and timely actions in response to epidemic outbreaks in contaminated areas.

keywords: Body-to-Body Networks, Mutual Interference, Cross Interference, WiFi, ZigBee, Channel Allocation, Game Theory, Nash Equilibrium, Epidemic Model, Geographic Routing.

Résumé

Motivés par la demande croissante de services de santé améliorés et à distance, qui tend à augmenter notamment avec une population de plus en plus âgée, et la réduction du coût de l'utilisation des infrastructures réseaux, afin d'assurer des applications de santé temps-réel et à faible débit de données, les réseaux de capteurs médicaux sans fil (WBANs) forment encore un domaine de recherche en forte croissance, notamment avec le développement de WBANs coopératifs. Dans ce contexte, en utilisant les utilisateurs du réseau eux-mêmes en tant que relais on pourrait étendre les infrastructures réseaux existantes, tout en améliorant la capacité du réseau et optimisant l'utilisation du spectre radio. Ainsi, les opérateurs réseaux, qui planifient déjà pour l'intégration de l'internet des objets (IoT) et l'informatique en nuage (cloud), devraient aussi penser à créer un nouveau type de réseau ad hoc mobile, où les utilisateurs du réseau sont utilisés comme des stations de base ad hoc simplifiées, afin de partager l'information en temps-réel entre des personnes colocalisées portant des capteurs corporels. Ce nouveau type de réseau est appelé réseau corporel sans fil (BBN: Body-to-Body Network). Dans un BBN, un appareil radio, collecte les données des noeuds capteurs attachés ou portés par une personne, et les transmet à un appareil récepteur situé sur une autre personne du voisinage, afin d'être traitées ou retransmises à d'autres utilisateurs du BBN. le BBN peut trouver des applications dans divers domaines tels que la santé, les sports d'équipe, le militaire, les divertissements, ainsi que des expériences passionnantes des réseaux sociaux. Fonctionnant dans la bande Industrielle, Scientifique et Médicale (ISM), les liaisons de communication dans un BBN seront très sensibles aux interférences entre les différentes technologies qui partagent le spectre radio limité. Ainsi, l'interférence entre ces technologies devient une préoccupation importante pour la conception de protocoles pour l'utilisateur final du BBN. À ce jour, très peu d'études existent, qui effectuent une analyse en profondeur de ce type de scénario impliquant le corps humain dans des communications radio. Le problème d'interférence dans un tel système distribué, doit être abordé avec des mécanismes distribués, tels que la théorie des jeux. Les décideurs dans le jeu sont soit les WBANs formant le BBN ou les opérateurs de réseaux qui contrôlent les dispositifs de communication inter-WBAN. Ces dispositifs doivent faire face à des

ressources de transmission limitées (bande ISM) ce qui donne lieu à des conflits d'intérêts.

Cette thèse vise à explorer les opportunités pour permettre des communications inter-WBANs en assurant le partage du spectre radio par le biais de deux approches. D'abord, *l'atténuation des interférences mutuelles et croisées*, et par *la conception d'un protocole de routage spécifique BBN* utilisé dans une application de contrôle de l'expansion d'une épidémie dans les zones de rassemblement de masse, tels que les aéroports. Dans un premier volet, une approche basée sur la théorie des jeux est proposée pour résoudre le problème d'interférence distribué dans les BBNs. Le jeu d'atténuation des interférences socialement conscient des intérêts de la collectivité (SIM) a une double tâche: à l'échelle WBAN, il alloue des canaux ZigBee aux capteurs corporels pour la collecte intra-WBAN des données, et à l'échelle BBN, il alloue les canaux WiFi aux appareils mobiles pour la transmission et le relais des données inter-WBANs. Deux algorithmes, BR-SIM et SORT-SIM, ont été développés pour rechercher les points d'équilibre de Nash du jeu SIM. Le premier (BR-SIM) assure les solutions de meilleure réponse (Best-response) tandis que le second (SORT-SIM) tente d'obtenir un compromis entre des solutions quasi-optimales et un temps de convergence réduit. Ensuite, afin de mettre en évidence le rôle crucial des BBNs, la deuxième partie de cette thèse est consacrée à proposer une application de contrôle épidémique adaptée aux BBNs, dans un environnement "indoor". Cette application met en oeuvre un protocole de routage géographique, qui différencie les classes de service des données WBANs et assure des stratégies de quarantaine en temps réel. Une telle application basée sur BBN pourrait aider les organismes gouvernementaux comme le National Institutes of Health (NIH) et les autorités telles que l'Organisation Mondiale de la Santé (OMS) à prendre des mesures rapides et en temps opportun en réponse aux flambées épidémiques dans les zones contaminées.

Mots-clés: Réseaux corporels sans fils, interférence mutuelle, interférence mixte, WiFi, ZigBee, allocation de canaux, Théorie des jeux, équilibre de Nash, Modèle épidémique, routage géographique.

Acknowledgments

This thesis appears in its current form due to the assistance and guidance of several people. I would, therefore, be very pleased to offer my sincere thanks to all of them.

Professor **Ahmed Mehaoua**, my esteemed **Thesis Advisor**, my cordial thanks go to you for accepting me as a PhD student, for the trust, and for allowing me to grow as a research scientist. Your advises on both research as well as on my career have been priceless. I greatly appreciate your warm encouragement and thoughtful guidance, which have paved me the way to fulfill these results. Especially, I was very honored by teaching with you networking modules for License and Master classes.

Dr **Jocelyne Elias**, my esteemed **Thesis Co-Supervisor**, special thanks go to you for your patience and your valuable feedbacks which made this thesis complete and interesting. I deeply appreciate your critical comments and your detailed reviews and corrections during the whole period of my PhD study, and above all your friendly advises and assistance even for non-thesis related worries. I will never forget the time you devoted to me and the insightful discussions we shared. Without your endless motivation, help, and support, it is doubtful I would have ever finished.

It is my pleasure to thank the examining **Committee Members**, Pr Anne Wei, Pr Dritan Nace, Pr Tijani Chahed, Pr Fabio Martignon, Pr Norbert Noury and Dr Abderrezak Rachedi, for taking time out from your busy schedules to offer your support, guidance and good will throughout the preparation and review of this dissertation.

I would like to thank Pr Pavlos Moraitis, the Director of the Laboratoire LIPADE, especially for the help he provided me when I met an administrative issue on my third PhD college year.

Thanks to the University Paris Descartes and the staff of the Department of Mathematics and Informatics, UFR Math-Info, for their academic assistance, and for giving me the opportunity to gain precious professional experience in teaching beside honorable professors. I am grateful to the administrative staff, especially M. Cristophe Castellani, for handling the paperwork and responding always to my queries within short delays.

My colleagues in the Laboratoire LIPADE, Mohamed Ali, Stanislas Morbieu and Ron-

gRong Zhang, thank you very much for making the atmosphere of our office as friendly as possible.

I cannot finish without thanking my family and close friends. Words cannot express how grateful I am to my parents, Mohamed Meharouech and Cherifa Toumi Ep Meharouech, for all of the sacrifices that you've made on my behalf. Your prayer for me was what sustained me thus far. My sister Safa, my beloved aunt Latifa Toumi who cared always about me, also my aunts Alia Toumi and Souad Toumi for their unceasing encouragements by visits and phone calls.

I warmly thank my beloved daughter, Ihsène, who could embellish, by his childhood magic power, the most difficult moments, also my just arriving son, Iyed, who assisted the writing process by sleepless nights! For both of you, I wish you will be proud of me.

To my dear husband Mehdi, there were times when things were not easy. You were the witness of my moments of fears and joys, you comforted me sometimes, and blamed me other times. Finally I'm convinced it was a valuable experience for both of us. Indeed, if great things were easy, they wouldn't be worth looking for.

I warmly thank my dear friends: Jihen Mahjoubi, Amina Jerbi, Dorra Ben Amara, Imen Khazri, Imen Jaouani, Karima Sebri, Hanen Abidi, Hiba Roihi, Souad Saadi, Hela Sfar, Houda Jmila, for your continuous encouragement for me to strive towards my goal.

I would also like to acknowledge the financial support of my country, Tunisia, and especially the Tunisian Ministry of Higher Education and Scientific Research, during a period of my PhD study.

Above all, I thank almighty God for granting me the strength and resources to achieve this dissertation successfully.

Finally I hope that my defense will be an enjoyable moment for all my welcome attendees.

*To my parents:
It is to you that I owe this success
and I am proud to offer it to you.*

Contents

List of Figures	XII
List of Tables	XIII
List of Acronyms	XV
1 Introduction	1
1.1 Body-to-Body Network concept	2
1.2 Interference mitigation in Body-to-Body Networks	3
1.3 BBN routing: Epidemic control application in mass gathering areas	5
1.4 Summary of Contributions	6
1.5 Thesis Organization	7
2 Moving towards Body-to-Body Networks	8
2.1 Introduction	9
2.2 From WBAN to BBN	9
2.2.1 Overview of WBANs	9
2.2.2 BBN paradigm	11
2.3 BBN Design Considerations	13
2.3.1 Energy-efficient routing in BBNs	14
2.3.2 Interference mitigation in BBNs	18
2.3.3 QoS-aware traffic management for BBN	20
2.3.4 Mobility management for BBN	24
2.3.5 Security policies for BBN	27
2.4 Conclusion	31

3 Interference Mitigation in Body-to-Body Networks: a game theoretical approach	32
3.1 Introduction	33
3.2 Game Theory: the big picture	33
3.3 System models	35
3.3.1 Body-to-Body Network Model	36
3.3.2 Body-to-Body Network Interference Model	39
3.4 Socially-aware Interference Mitigation (SIM) game in Body-to-Body Networks	41
3.4.1 BBN-stage SIM game	43
3.4.2 WBAN-stage SIM game	49
3.4.3 A discussion on social interactions of WBANs in the SIM games	51
3.5 Conclusion	52
4 Socially-aware Interference Mitigation: Game solutions and channel allocation algorithms	53
4.1 Introduction	54
4.2 Best-Response SIM Algorithm (BR-SIM)	54
4.3 Sub-Optimal Randomized Trials for SIM game (SORT-SIM)	56
4.4 Security mechanism - <i>Channel Allocation Time Misuse Attack (CATMA)</i>	59
4.4.1 Misbehavior detection phase	59
4.4.2 Attack prevention phase	62
4.5 Performance evaluation	62
4.5.1 BR-SIM versus SORT-SIM	63
4.5.2 Comparison with power control approaches	70
4.6 Conclusion	76
5 Inter-WBAN Routing Protocol for Epidemic Control in Mass Gathering Areas using Body-to-Body Networks	77
5.1 Introduction	78
5.2 State of the Art	79
5.3 BBN-based Epidemic System models	82
5.3.1 SEIR Epidemic spread model	82
5.3.2 BBN Epidemic control model	84
5.4 Epidemic threshold-based BBN routing protocol	84
5.4.1 Epidemic threshold	85
5.4.2 BB-LAR: Location-Aided BBN Routing	86
5.4.3 BBN Route selector	88
5.4.4 Human trajectory tracing - WBAN selfish strategy	88
5.4.5 Epidemic source tracing - Authority quarantine strategy	89
5.5 Performance Evaluation	89
5.5.1 Performance analysis of BB-LAR	89

5.5.2 Comparison of BB-LAR with other geographic-based routing protocols .	92
5.6 Conclusion	96
6 Conclusion and Future Perspectives	98
Bibliography	99
Appendix	110
A.1 BR-SIM algorithm Scilab source code	111
A.2 SORT-SIM algorithm Scilab source code	119
A.3 BB-LAR Castalia configuration file (omnetpp.ini)	123

List of Figures

1.1	Body-to-Body Network [1]	2
2.1	Example of a patient monitoring using a WBAN	10
2.2	Body-to-Body Network for U-Health monitoring of a group of cyclists.	12
2.3	Application area extension from WBAN to BBN	13
2.4	QoS modules of WBAN QoS protocols suitable for future U-Health BBNs.	22
2.5	Major security requirements in BBNs.	28
3.1	Three-BBN interfering scenario: each BBN is composed of several WBANs which use different transmission technologies (i.e., ZigBee and WiFi) sharing the same radio spectrum.	36
3.2	The 802.11b frequency responses with the raised cosine filter [2].	37
3.3	Extended Conflict Graph of the scenario illustrated in Fig.3.1	41
3.4	Flow chart of bi-level SIM Game.	44
3.5	Delegate and underlying WBANs' WiFi links	45
4.1	Examples of SORT-SIM execution.	58
4.2	CATMA attack scenario and SIM secure mechanism - Reservation of a channel.	60
4.3	CATMA attack scenario and SIM secure mechanism - Extending time of use of a channel.	61
4.4	Simulation scenario for N=40 WBANs	63
4.5	Dynamics of the BR-SIM algorithm for each BBN, with N=20 WBANs	64
4.6	Dynamics of the BR-SIM algorithm for each BBN, with N=40 WBANs	65
4.7	Iterations of the SORT-SIM algorithm for each BBN, with N=20 WBANs	67
4.8	Iterations of the SORT-SIM algorithm for each BBN, with N=40 WBANs	68
4.9	BR-SIM v.s SORT-SIM - Average SIR function of density	69

4.10	BR-SIM: Empirical Cumulative Distribution Function (CDF) of the SIR measured at WiFi and ZigBee interface of all WBANs in the BBN scenario of 40 WBANs with 30 time epochs of 10 s each.	69
4.11	SORT-SIM: Empirical Cumulative Distribution Function of the SIR measured at WiFi and ZigBee interface of all WBANs in the BBN scenario of 40 WBANs with 30 time epochs of 10 s each.	70
4.12	Dynamics of the PAPU algorithm for each BBN, with N=40 WBANs	72
4.13	WBAN configuration for the RSPC algorithm [3].	73
4.14	BR-SIM and SORT-SIM vs PAPU and RSPC. Average WiFi and ZigBee SIR as a function of network density.	74
4.15	Aggregate interference at the Hub/MT.	75
5.1	Air traffic connections from West African countries to the rest of the world: the international spreading risk associated with the 2014 West African Ebola Outbreak [4]	78
5.2	SEIR model flow	83
5.3	BBN and authority levels of the epidemic control model in the airport indoor environment	85
5.4	Structure of RREQ packet	86
5.5	Expected zone and request zone for BBN Location Aided Routing (BB-LAR)	87
5.6	Structure of RREP packet	87
5.7	Flow chart of the BBN-based epidemic control algorithm	88
5.8	Healthy distance and epidemic hazardous zone	89
5.9	Packet delivery ratio of the epidemic data traffic	91
5.10	End-to-end delay of epidemic data packets	91
5.11	Total energy consumed by the epidemic data transmissions	92
5.12	Resource Manager module of a WBAN node in Castalia [5]	93
5.13	Reliable Routing Technique (RRT) in two situations: 1) No disruption of the wireless link (S1 to D1), and 2) Disruption of the wireless link (S2 to D2) [6]	93
5.14	Packet Delivery Ratio: BB-LAR v.s. RRT	95
5.15	End-to-end delay: BB-LAR v.s. RRT	95
5.16	Consumed energy: BB-LAR v.s. RRT	96

List of Tables

2.1 Energy-aware candidate protocols for U-Health BBNs.	15
2.2 WBAN traffic priority according to [7].	20
2.3 Comparative study of mobility prediction methods for U-Health BBNs	25
2.4 Comparison of existing WBAN solutions which can be extended to BBN environment.	30
3.1 Parameters notations for the channel assignment game	42
5.1 Simulation parameters of BB-LAR	90

List of Acronyms

- AODV** Ad hoc On Demand Distance Vector
- APs** Access Points
- BB-LAR** Location-Aided BBN Routing
- BBN** Body-to-Body Network
- BLE** Bluetooth Low Energy
- BR-SIM** Best Response SIM algorithm
- CATMA** Channel Allocation Time Misuse Attack
- ERM** Epidemic Routing Metric
- FIP** Finite Improvement Property
- GPSR** Greedy Perimeter Stateless Routing
- IF** Interference Function
- IoT** Internet of Things
- ISM** Industrial Scientific and Medical band
- LAR** Location Aided Routing
- LOS** Line Of Sight
- MAC** Medium Access Control
- MT** Mobile Terminal

NE Nash Equilibrium
NLOS Non Line Of Sight
OLA OverLap Avoidance
PAPU ProActive Power Update algorithm
PDR Packet Delivery Ratio
POCs Partially Overlapped Channels
PSD Power Spectral Density
PSNs Public Safety Networks
QoS Quality of Service
RF Radio Frequency
RREP Route Reply
RREQ Route Request
RRT Reliable Routing Technique
RSPC Relay Selection and transmit Power Control
RSSI Received Signal Strength Indication
SEIR (Susceptible, Exposed, Infectious, Recovered)
SIM Socially-aware Interference Mitigation
SINR Signal-to-Interference-plus-Noise Ratio
SORT-SIM Sub-Optimal Randomized Trials for SIM game
TDMA Time Division Multiple Access
U-health Ubiquitous Healthcare
WBAN Wireless Body Area Network
WSAN Wireless Sensor and Actuator Network

Chapter **1**

Introduction

Contents

1.1	Body-to-Body Network concept	2
1.2	Interference mitigation in Body-to-Body Networks	3
1.3	BBN routing: Epidemic control application in mass gathering areas	5
1.4	Summary of Contributions	6
1.5	Thesis Organization	7

Future generation wireless networks are characterized by a distributed, dynamic, self-organized architecture. Typical examples include Ad-Hoc/mesh networks, sensor networks, Cognitive Radio networks, etc. These wireless networks could then constitute the infrastructure for numerous applications with growing demands in terms of connectivity, bandwidth, quality of service and energy supply.

In the last years, Wireless Sensor Networks have been considered as one of the key research areas to extend the existing wireless infrastructures, so that using wearable sensors, ordinary people could form a Wireless Body Area Network (WBAN) providing thus "anytime, anywhere" mobile network connectivity. Furthermore, the co-existence of multiple WBANs, the communication and the interactions between them extend the classical concept of WBAN and present a new paradigm, which is referred to as Body-to-Body Network (BBN). Such emerging networks play an important role in enabling ubiquitous communications, creating a huge potential market.

1.1 Body-to-Body Network concept

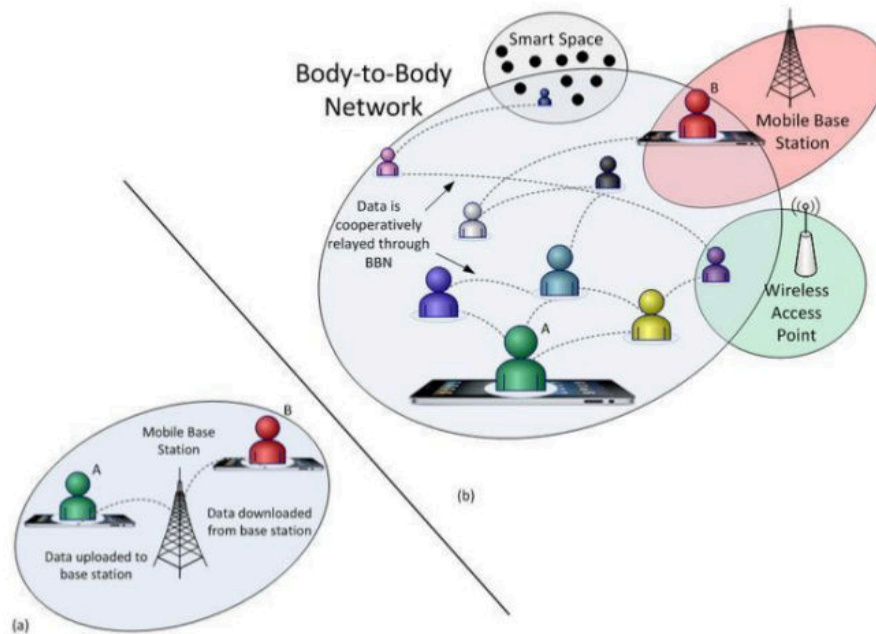


Figure 1.1: Body-to-Body Network [1]

In its simplest form, a body-to-body network (BBN) is a kind of ad hoc network in which mobile nodes are wearable devices, either carried or worn by people [1].

In a BBN, all users should contribute a nominal amount of their bandwidth to relay

data to the other network users, creating thus vast cooperative body-to-body communications, for the great benefit of the network. In densely populated areas, a BBN could allow cellular providers to truly achieve “anytime and anywhere” connectivity and gigabit data rates, especially with the emergence of the Internet of Things (IoT) giving rise to real-time applications with growing demands on data rates.

BBNs are widely adopted in several mission-critical scenarios: (i) rescue teams in a disaster area, (ii) groups of soldiers on the battlefield, and (iii) patients in a healthcare center, whose Wireless Body Area Networks (WBANs) interact with each other. The BBN consists of several WBANs, which in turn are composed of sensor nodes that are usually placed in the clothes, on the body or under the skin [8]. These sensors collect information about the person and send it to the sink (i.e., a Mobile Terminal (MT) or a PDA), in order to be processed or relayed to other networks. The concept of BBN is illustrated by Fig.1.1.

In Fig.1.1(a), two cellular network users wish to exchange data (video, music or social network information) within the same network cell. Using traditional cellular architecture, the data would be routed through the local base station between person A and person B. In Fig.1.1(b), a BBN is used to cooperatively relay the data. Yet, instead of passing through the nearby base station, data would be transmitted over a much shorter distance to the nearby BBN user in local vicinity.

1.2 Interference mitigation in Body-to-Body Networks

Due to the scarce wireless resources, many existing wireless technologies, like IEEE 802.11 (WiFi), IEEE 802.15.1 (Bluetooth) and IEEE 802.15.4 (ZigBee), are forced to share the same unlicensed 2.4 GHz Industrial Scientific and Medical band (ISM). Hence, mutual as well as cross-technology interference may occur between these technologies.

Indeed, the interference issue is already handled by the Bluetooth Low Energy (BLE) standard [9], which defines three channels as advertising channels, used for device discovery and connection establishment, and have been assigned center frequencies that minimize overlapping with IEEE 802.11 channels 1, 6 and 11, which are commonly used in several countries. Then, an *adaptive frequency hopping* mechanism is used on top of the 37 data channels in order to face interference and wireless propagation issues, such as fading and multipath. This mechanism selects one of the 37 available data channels for communication during a given time interval, so as to avoid interference with neighboring wireless links. Furthermore, a number of previous works [10, 11, 12, 13] enhanced the existing frequency hopping mechanism and implemented further schemes, such as the OverLap Avoidance (OLA) proposed in [13].

Number of recent works [14, 15, 16, 17] investigate the inter-WBANs interference problem with different alternatives. For example, in [14], the interference-aware coexistence of multiple WBANs is tackled by considering the mobility of sensor nodes within each WBAN as well as the relative movement of WBANs with respect to each other. Based on social

interaction detection, the proposed protocol, builds the interference model and implements a simple "Sample-and-Hold" channel prediction mechanism that ensures spectral reuse and power efficiency. Besides, specific mechanisms are even proposed such as the interference avoidance method based on Chinese medical band for Wireless Body Area Networks, investigated in [15]. A classification of wireless channels by priority is made based on the distribution of potential interference of the China medical band, then an available channel set is formed at the network initialization phase with respect to the network energy threshold.

Coexistence and interference mitigation between WBANs are also considered by the IEEE 802.15.6 standard. Three mechanisms are defined: *beacon shifting*, *channel hopping* and *active superframe interleaving* [18]. Yet, our choice for ZigBee aims at effectively and theoretically tackling the cross-technology interference problem between WiFi (802.11) and ZigBee (802.15.4) technologies.

Since WiFi transmission power can be 10 to 100 times higher than that of ZigBee, ZigBee communication links can suffer significant performance degradation in terms of data reliability and throughput. In addition to the previously mentioned challenging issues, the mobility of WBANs in their surrounding environment and their interactions with each other make the interference mitigation in body-to-body networks a very interesting and mandatory problem to address. This is indeed the first focus of our work.

In a first step, we consider a dynamic system composed of several Body-to-Body Networks based on wearable technology, and we analyze the joint mutual and cross-technology interference problem due to the utilization of a limited number of channels by different transmission technologies (i.e., ZigBee and WiFi) sharing the same radio spectrum (ISM band). To this end, we propose a game theoretical approach, in order to address the problem of Socially-aware Interference Mitigation (SIM) in BBNs. Our approach considers a two-stage channel allocation scheme: (i) a BBN-stage for inter-WBANs' communications, where special players, called the delegates, decide the allocation of WiFi channels for themselves and the underlying subnetworks based on the optimization of an utility function, which is expressed using Signal-to-Interference Ratios, and (ii) a WBAN-stage that allows players to choose the needed ZigBee channels for intra-WBAN communications, involving mutual and cross-technology considerations at each stage. We demonstrate that the two proposed games have exact potential functions and we develop a Best Response SIM algorithm (BR-SIM) that converges to Nash equilibrium points. A simulation work using Scilab package is conducted and numerical results have shown that the proposed scheme is indeed efficient in optimizing the channel allocation in BBNs interacting between themselves while using different transmission technologies.

A second algorithm, named the Sub-Optimal Randomized Trials for SIM game (SORT-SIM), is then proposed as trade-off between efficient channel allocation and short computation time. SORT-SIM is proved to guarantee a sub-optimal solution to the SIM problem. SORT-SIM is compared to BR-SIM in terms of efficiency and computation time. Numerical results, obtained in several realistic mobile scenarios, have shown that the proposed schemes are

indeed efficient in optimizing the channel allocation in medium-to-large-scale BBNs.

1.3 BBN routing: Epidemic control application in mass gathering areas

We focus then on the interconnection of WBANs. Yet, investigating routing issue goes parallel with energy efficiency, quality of service and mobility considerations.

Among the few inter-WBANs routing protocols proposed in the literature, ZEQoS [19] is an integrated energy and QoS-aware routing protocol that is designed to be used in hospital indoor environments. By calculating the best next hops according to three classes of data packets, ZEQoS ensures optimized path selection while reducing inter-WBAN communication cost and delays, and fulfilling QoS requirements of the different data types. Further candidate protocols for inter-WBAN routing [20, 21, 22] are discussed later in next chapter, and we distinguish the main features to be considered for a specific application: the epidemic control using BBNs.

Thus, we design a routing protocol for inter-WBANs communications within a BBN, considering the aforementioned features: energy, Quality of Service (QoS) and mobility. To implement this routing protocol, we consider the scenario of epidemic control in mass gathering areas (for example the airports). Yet, effective incentives are intended to improve the accuracy of BBN deployment and coexistence within the existing infrastructures, in order to ensure public safety and improve the Quality of Life for future human generations. Indeed, population natural increase and closer public contact make easier the spread of pandemic diseases. Existing epidemic control solutions are unable to gather, simultaneously, people health data and social contact information, neither to analyze those data and proceed in real time for epidemic spread prevention. Most epidemic control solutions [23, 24, 25], proceed off-line by collecting reports on the pandemic spread, which are transmitted later to medical servers for analysis and decision making. Recent researches place Body-to-Body networks as a revolutionary technology, for the monitoring of people behavior with real-time updates of medical records and interactive assistance in emergency situations. In this context, the second part of this work investigates the epidemic control issue using emerging BBNs, in the mass gathering areas, such as the airport use case. Entering people are equipped with Wireless Body Area Networks and they interact with each other forming a BBN inside the test zone. A number of ad hoc routing protocols [26, 27, 28, 29] are investigated to select the more suitable for the epidemic control application. The main drawback of proactive routing protocols is the routing delay caused by the routes discovery broadcasts which corrupts the network performance in emergency situations, in addition to energy inefficiency and bandwidth overload. The delay caused by the route discovery before data transfer is also compromising for reactive ad hoc protocols. Geographical location based routing protocols could avoid the technique of storing and sharing the network topology information, which could have promising effects on delays reduction, energy and

bandwidth efficiency.

Yet, we extend the Location Aided Routing (LAR)[29] to propose a BBN threshold-based routing protocol, referred to as *BB-LAR*, in order to exchange epidemic data and help the authority control unit in detecting and quarantining the infected subjects.

1.4 Summary of Contributions

To the best of our knowledge, this work is the first to propose a game theoretical approach for an interference-aware channel allocation in BBNs. In our model, multiple WBANs could interact among each other within a BBN, as well as with other coexisting networks/BBNs, involving different access technologies (WiFi, ZigBee, Bluetooth..); this can lead to unavoidable heavy interference environment.

The main contributions of our work are the following:

- We propose a novel game theoretical approach for mutual and cross-technology interference mitigation in BBNs.
- We provide a detailed expression of the *Signal-to-Interference Ratio* to define players' payoff functions, capturing all main interference components, namely the co-channel, the mutual, and the cross-technology interferences.
- We demonstrate that our games admit at least one pure strategy Nash Equilibrium (NE) since they are exactly potential, and we develop a best response algorithm (BR-SIM) to compute the channel allocations, which converge fast to NE solutions.
- We propose a second algorithm, called Sub-Optimal Randomized Trials (SORT-SIM), that trades-off between efficient channel allocation process and short computation time, and guarantees a sub-optimal solution to the SIM problem.
- We perform a thorough performance analysis of the BBN- and WBAN-stage SIM games under different system parameters, and compare the two proposed algorithms, i.e., BR-SIM and SORT-SIM to a distributed power control algorithm and a relay-assisted power control algorithm. Numerical results show that the proposed schemes are indeed efficient in optimizing the channel allocations in medium-to-large-scale realistic mobile BBN scenarios.
- We propose an epidemic control application using BBNs in mass gathering areas. We consider the scenario of epidemic spread in the airports and we propose a BBN routing protocol, called BB-LAR, based on geographic routing and an epidemic threshold, to ensure a real-time and self-prevention epidemic control.
- We perform a simulation analysis of BB-LAR protocol to evaluate the different routing parameters, such as the packet delivery ratio, the end-to-end delay and the energy consumption, which are further compared to existing geographic routing protocols.

1.5 Thesis Organization

The rest of this thesis is organized as follows.

- Chapter 2 will generally introduce the Body-to-Body Network paradigm, presenting the design challenges and discussing existing works, focusing on five principal interrelated axes: energy efficiency, interference mitigation, quality of service (QoS), mobility management, and security.
- Chapter 3 presents the two-stage Socially-aware Interference Mitigation (SIM) game theoretical approach. The first section 3.3 presents the BBN system models, including the communication and the interference model. Then, section 3.4 details the BBN-stage and the WBAN-stage SIM games and demonstrate their convergence to Nash Equilibra.
- Chapter 4 investigates the SIM game solutions and the channel allocation algorithms, where section 4.2 details the best-response algorithm (BR-SIM), while section 4.3 handles the sub-optimal solution (SORT-SIM) for the SIM problem, and section 4.5 analyzes numerical results for the proposed solutions in several BBN scenarios.
- Chapter 5 presents an epidemic control application using BBNs, where a QoS-based and energy-efficient geographic routing protocol is proposed to ensure the epidemic information exchange among WBANs.
- chapter 6 concludes this thesis and discusses the open issues that need to be investigated in our future work.

Chapter 2

Moving towards Body-to-Body Networks

Contents

2.1	Introduction	9
2.2	From WBAN to BBN	9
2.2.1	Overview of WBANs	9
2.2.2	BBN paradigm	11
2.3	BBN Design Considerations	13
2.3.1	Energy-efficient routing in BBNs	14
2.3.2	Interference mitigation in BBNs	18
2.3.3	QoS-aware traffic management for BBN	20
2.3.4	Mobility management for BBN	24
2.3.5	Security policies for BBN	27
2.4	Conclusion	31

2.1 Introduction

Smart mobile people have a great potential to extend the existing Internet of Things (IoT) infrastructures by implementing genuine ubiquitous applications, ensuring anywhere and anytime people connectivity. Indeed, the co-existence of multiple WBANs (Wireless Body Area Networks), the communication and interactions between them extend the classical concept of WBAN and present the new paradigm referred to as Body-to-Body Network (BBN). This paradigm supports a number of innovative and interesting applications such as Ubiquitous Healthcare ([U-health](#)), entertainment, interactive gaming, and military applications, to cite a few. Especially, through the forwarding of sensing data from person to person until reaching a connected medical server, or virtually interconnected cloud servers, concrete U-Health becomes true with the emerging of future Body-to-Body Networks.

2.2 From WBAN to BBN

Motivated by the increasing need for remote and improved healthcare solutions, while decreasing the cost of supporting a continuously growing aging population in developed countries, WBANs still form a strongly growing research field, driven by the development of the IEEE 802.15.6 standard. Furthermore, the evolution of single-operating WBANs to a cooperative large-scale BBN, is subject to a number of design challenges, some of which will be addressed in this section.

2.2.1 Overview of WBANs

A Wireless Body Area Network (WBAN) is a wireless network of wearable or implanted computing devices. Sensor devices can be embedded inside the body (implants), surface-mounted on the body in a fixed position (wearable), or carried by humans in different positions.

The development of such technology started around 1995 with the idea of using wireless personal area network (WPAN) technologies to implement communications on, next to, and around the human body.

The WBAN field is an interdisciplinary area which could allow inexpensive and continuous health monitoring with real-time updates of medical records through the Internet. This area relies on the feasibility of fixing (implanting) very small biosensors on (inside) the human body that are comfortable and that do not impair normal activities. The WBAN allows continuous health monitoring in real time and we can access to the medical records remotely. The sensors will collect the different information in order to monitor the patient's health status regardless of his location; this information will be transmitted wirelessly to an external processing unit. If an emergency is detected, an alert will be generated through the computer system to inform the patient and/or the medical staff. [Figure 2.1](#) illustrates an example of a patient monitoring system using a WBAN.

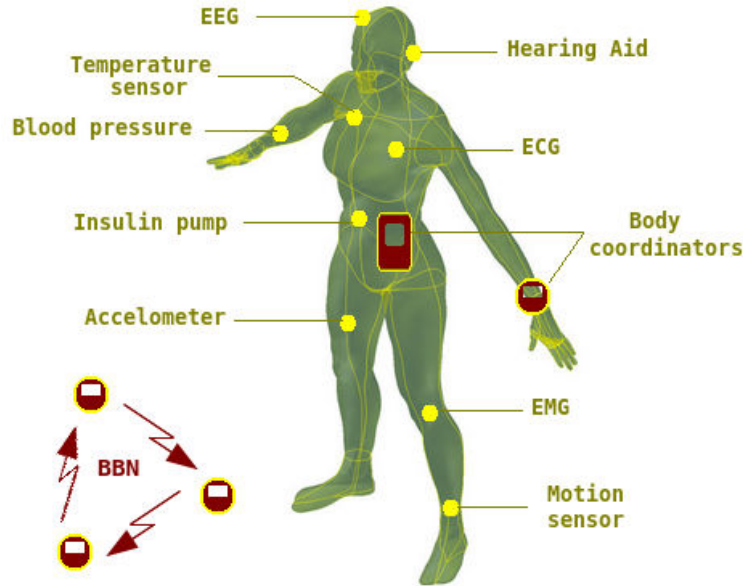


Figure 2.1: Example of a patient monitoring using a WBAN

Architecture

In [19], communication devices in a hospital are classified into three categories, defining three communication models. In communication tier 1, each sensor node of the WBAN collects data and sends them to the WBAN Coordinator. In communication tier 2, the WBAN forwards data for a next hop, which can be a WBAN, a medical display coordinator, a nursing station coordinator, or a cellular device. Finally, communication tier 2 forwards to tier 3 communication devices which can be a 3G tower, a nurse device, an application server, or any cloud servers through the Internet. Other taxonomy used for WBAN architecture talks about intra-WBAN, extra-WBAN and beyond-WBAN communications to designate almost the same communication models.

Standards

There are different standards that are used in WBANs in order to permit the communications between the different sensor nodes and between the WBAN coordinator and external devices. The most known and used in the industry are: IEEE 802.15.6 [30][31], which is a low-power and short-range wireless standard used for devices operating inside or around the human body. This standard supports data rates up to 10 Mbps, while simultaneously complying with strict non-interference guidelines. This standard considers effects on portable antennas, radiation pattern shaping to minimize the specific absorption rate (SAR) into the body, and changes in characteristics as a result of the human motions. Then, IEEE 802.15.4 (ZigBee) [32] is a well-known standard for WBANs, which deals with compatible intercon-

nection of communication devices using low-data rate, low-power, but very long battery life, and low-complexity short-range radio frequency (RF) transmissions. Nevertheless, it is possible to use other standards in WBANs, like 802.11 or 4G.

Applications

WBAN applications are classified according to their area of use. In the following, we present the major categories [31].

- *Medical treatment and diagnosis* : there are several cases of WBAN use in diagnostic and treatment of diseases, many researches are conducted in this field. Use case example: cardiovascular disease (CVD), Diabetes, Asthma and Parkinson's disease, etc.
- *Training schedules of professional athletes* : through equipments helping athletes for training and monitoring of the progress and advancement of their performances.
- *Public safety and preventing medical accidents* : Large number of people dies every year due to medical accidents, then, installing a sensor node to maintain a log of previous medical accidents can reduce the number of deaths.
- *Safeguarding of uniformed personnel* : WBAN can be used by firefighters, policeman or military, in order to keep monitored in hazardous environments. Example in the case of the firefighters involved in stopping fire, the WBAN can detect the existence of a dangerous gas and its level in the air, the information will relate to these team members.
- *Consumer Electronics*: WBAN can be integrated in the Electronic equipment, head-mounted displays, microphone, camera, etc.

Yet, WBAN applications have evolved over the time, and new WBAN-based networks have recently emerged, i.e., Body-to-Body Networks (BBNs), that we can define as a set of WBANs, which are able to communicate with each other, in order to ensure various solutions that fulfill real social benefits. However, nowadays this kind of networks present numerous challenges like the energy-efficiency, system devices interoperability, mutual and cross-technology interference, wireless environment properties, the Quality-of-Service, the human mobility prediction and the security of these networks.

2.2.2 BBN paradigm

A Body-to-Body Network (BBN) is composed by several WBANs, each WBAN communicates with its neighbor. The coordinator device plays the role of a gateway that shares the communication information with other WBANs. Alike the single WBAN, a BBN uses the



Figure 2.2: Body-to-Body Network for U-Health monitoring of a group of cyclists.

communication standards such as 802.15.4 (Zigbee), 802.15.6, 802.15.1 (Bluetooth), 802.11 or 4G.

Body-to-Body Network is theoretically a mesh network that uses people to transmit data within a limited geographic area. Using devices such as a BBN-enabled Smartphones or Smartwatches, a signal is sent from the WBAN to the nearest BBN user, which is transmitted to the next-nearest BBN user and so on until it reaches the destination.

BBN is an emerging solution for communication between patients and the medical staff, and exchange of data between WBANs, which provides the possibility to share data in order to perform estimation, statistics or just route to a given destination. Figure 2.2 illustrates an example of BBN network used for the U-Health monitoring of a group of cyclists.

Challenges

The major challenges for BBN are: the energy efficiency, when the coordinators will play the role of cluster head and will transmit the value or vital signs in the case of a medical application to other WBAN within a group. Furthermore, the aforementioned standards used for BBN communications are not optimal and do not provide a secure communication. Thus, implementing a security system that helps to protect data transmitted between the WBAN and the destination is necessary. Then the routing of collected sensor data through neighboring WBANs until the destination, with QoS considerations and ability to support WBANs mobility, is a third issue. Yet, the data generated and transmitted in a BBN must have secure and limited access. Anyway, people can see the BBNs such as a threat sources on their data and private life, their acceptance is the key of the success of BBNs. Finally, all data residing in mobile WBANs or patient sensor nodes must be collected and analyzed in a seamless fashion. The vital patient datasets may be fragmented between some nodes, but if the node does not contain all known information the level of patient care may be not so good.

Applications

Body-to-body networks could represent emerging solutions ensuring real social benefits, such as remote healthcare, precision monitoring of athletes, rescue teams in a disaster area or groups of soldiers on a battlefield, etc. Yet, the BBN can be implemented in both medical and non-medical applications. Especially, BBNs represent the novel trend for the future

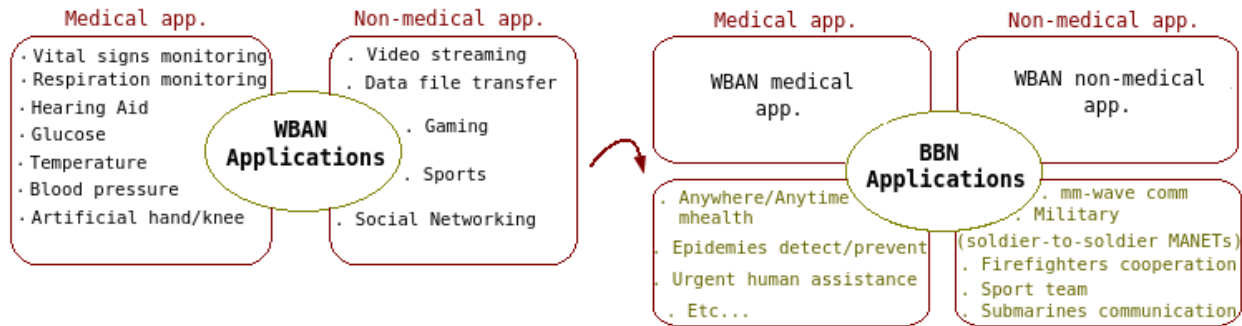


Figure 2.3: Application area extension from WBAN to BBN

ubiquitous healthcare systems, indeed the remote monitoring of patients carrying bodyworn sensors and relaying each other’s physiological data up to the medical center, could greatly reduce the current strain on health budgets and make the Government’s vision of ubiquitous healthcare for distant patients a reality. Hence, the sensors could be embedded into mobile handsets, portable electronic devices, cars, and clothing. People would no longer need to be in range of a cellular tower to make a call or transmit data, apart from the health and environmental red tape associated with cellular peril issues that would be avoided with a low-power body-to-body network.

Figure 2.3 sorts the different WBAN and BBN applications into medical and non-medical classes, and lists the new intended applications by the deployment of BBN networks. We just posit some medical BBN scenarios, for example to ensure remote health monitoring out of the 3G coverage area, this could apply to monitor the vital signs of a rescue team in a disaster area or a group of soldiers in a battlefield. Also, when a patient is at home or far from the medical center, and feels a sudden discomfort, he will be able to broadcast a distress call and bring out an urgent human assistance from his neighborhood.

2.3 BBN Design Considerations

To design new, energy-efficient, QoS-based, and secure mechanisms for BBNs, there is a number of challenges one must overcome. Practically, few mechanisms proposed in the literature for WBANs could apply to BBNs, provided that further specific considerations of BBN applications should be well-respected. Thus, hereafter, we investigate some WBAN solutions and discuss their ability to suit BBN scenarios, focusing on five principal inter-related axes: energy efficiency, interference mitigation, quality of service (QoS), mobility management, and security.

Energy-efficiency: Is one of the foremost challenges of BBNs, the energy efficiency consists in reducing the amount of energy required to provide the different services. In this thesis, we study a number of works that propose solutions, protocols and mechanisms to reduce energy consumption. The main objective of these solutions is to increase the lifetime

of the network, and equilibrate the energy among WBANs/sensor nodes.

Interference and coexistence: To identify and exploit opportunities for cooperation with neighboring WBANs, inter-body interference detection and subsequent mitigation are mandatory. Indeed, we should analyze the joint mutual and cross-technology interference problem due to the utilization of a limited number of channels by different transmission technologies (i.e., ZigBee, WiFi, Bluetooth, etc...) sharing the same radio spectrum.

Quality-of-Service: The quality of service (QoS) is the totality of characteristics of a telecommunication service that bear on its ability to satisfy stated and implied needs of the user of the service [33]. In this thesis, we present the different solutions that are in use today, like the game theory model and also the QoS-aware protocols such as McMAC [22], QPRR [20], RACOON [21] and ZEQoS [19]. These protocols compete in the optimization of the whole network throughput, delay and priority in order to ensure a better QoS in the WBAN communications.

Mobility prediction: The mobile WBANs may follow different mobility patterns that may affect connectivity, and in turn protocol mechanisms and performance. Mobility prediction may positively affect the service oriented aspects as well as the application-oriented aspects of BBN networking. At the network level, accurate WBAN mobility prediction may be critical to routing tasks such as call admission control, reservation of network resources, pre-configuration of services and QoS provisioning.

Security: The security and privacy preoccupations are among major areas of concern of BBN, due to direct involvement of human information. There are different studies that bring out the limitations of the current proposed security solutions that need, therefore, further research. In this survey we present and discuss the different security solutions intended to be applied to the BBN applications.

2.3.1 Energy-efficient routing in BBNs

Stringent resource constraints on devices within a WBAN have been long discussed in the literature. Indeed, while sensors in general are energy constrained, body sensors are more so. Furthermore, the interaction and routing of data among a group of WBANs within a BBN, result obviously in further energy consumption, in order to ensure inter-WBAN communication, and then introduce additional energy constraints.

Authors of [34] presented a comparative study between routing protocols for WBAN healthcare communication networks. The studied scenario consists in a ZigBee network having static IEEE 802.15.4 star topology, taking into account the energy consumption as well as the following QoS metrics: the average end-to-end delay, the throughput, the jitter and the packet delivery rate. The simulation results showed that the Ad hoc On Demand Distance Vector (AODV) protocol produces higher throughput with minimum jitter and delay, with and without mobility of WBANs. Then, AODV was enhanced into an energy-aware routing protocol termed as EAAODV, which is an on-demand routing protocol that

Protocol	Layer	Topology	Advantages	Limitations
EAAODV [34]	Network	Single-hop	On-demand Routing Mobility management	Results only for ZigBee MAC Model.
M-ATTEMPT [35]	Network	Single-hop/ Multi-hop	Mobility management Traffic data priorities Intra-WBAN routing	Disconnection during sensor node mobility.
SIMPLE [36]	Network	Multi-hop	Reliability, High throughput On-demand intra-WBAN routing	No mechanism to handle mobility.
EERS [37]	Network	Multi-hop	Joint Routing and Adaptive power control. Low overhead. Prolong the lifetime of the overall network	Only focus on the energy consumed for data transmission. Sensing and reception energy are assumed constant.
EAWD [38]	Network	Multi-hop	Topology-aware energy-efficiency Minimizing relay nodes Minimizing installation cost Generic (separate energy components)	No consideration of retransmission energy, MAC access energy and signaling energy
Duty-cycle [39]	MAC	Single-hop	Guard time: no overlaps, reliable data transfer. Reduce idle listening Synchronization scheme for TDMA	Hardware dependent

Table 2.1: Energy-aware candidate protocols for U-Health BBNs.

builds routes only on demand by flooding Route Request packets (RREQ). The selection of the neighboring WBAN for forwarding the route request is based on both mobility and the remaining energy.

The EAAODV algorithm is executed over 5 steps. At first, sensor node who wants to send a message must first look if a path exists from source to destination in the routing table. If a route is available, then it forwards the message to the next node. Else, the message is added to the queue and the source sends RREQ packet to the neighbor to start the discovery process. Secondly, the sensor node learns the energy and mobility states of the neighboring nodes and compares them with its current values. In step 3, the sensor node defines energy and mobility thresholds and, at step 4, selects the routing sensor node that presents a maximum energy and minimum mobility. Finally, the sender writes the energy and mobility values in the message, and sends the RREP packet.

In comparison to AODV, EAAODV performs better in terms of energy consumption, and then presents a suitable routing protocol for the energy- and QoS-highly constrained networks of WBANs. Yet, EAAODV could be a candidate routing protocol for BBNs.

In [35], the authors proposed a new energy-efficient routing protocol for heterogeneous WBANs (M-ATTEMPT), defining a prototype to employ heterogeneous sensors on human body. The proposed protocol uses a direct communication with the sink for critical data (real-time) and on-demand data, and uses a multi-hop communication for normal data delivery. The thermal-aware algorithm detects link hot-spots corresponding to implanted

sensors and avoids transmitting on these links in order to minimize energy consumption. Besides, patient mobility causes links disconnections, thus, mobility support and energy management are included in the solution.

A linear programming (LP) model is then defined to maximize routing information extraction and minimize routing energy consumption. There are four phases in the proposed algorithm: at the initialization, the node sends Hello message to discover his neighbors information and distance to the Sink. Then, at the routing phase, M-ATTEMPT differentiates between emergency traffic and normal data to use either single-hop or multi-hop communication to the Sink. Multi-hop allows it to preserve energy consumption, since less energy is required for routing through short distances. Third, at the Scheduling phase, and after the route selection, the sink node creates TDMA schedule for the communication between sink node and root nodes, where the sink allocates time slots to the sensor nodes for the normal data delivery. Finally, at the data transmission phase, sensor nodes send their data to the sink in their assigned time slots. An extra phase is considered in case of node mobility, then extra energy is used to maintain the connectivity of the mobile node.

The M-ATTEMPT protocol was proposed for an energy- and QoS-aware routing in the context of intra-WBAN communication, but it could apply to inter-WBANs routing, i.e., to ensure data forwarding among sinks in a BBN scenario. Nevertheless, the QoS traffic classification and scheduling should be more investigated to fit specific BBN requirements. The negative aspect in this routing protocol is the disconnection during sensor node mobility, which requires the restructuring of the WBAN tree topology. Thus, M-ATTEMPT protocol needs the implementation of a robust mobility management mechanism to be able to ensure inter-WBAN communication within a BBN.

Also in [36], the authors proposed the multi-hop topology to minimize the energy consumption of their routing protocol (SIMPLE), while ensuring higher throughput, more reliable and longer stability period, in comparison to M-ATTEMPT. This multi-hop protocol is based on a cost function to select a parent node or a forwarder.

For the transmission and reception, the authors chose the radio model of Heinzelman [40]. In this model, where d is the separation between the transmitter and the receiver, d^2 models the energy waste due to the transmission channel. This protocol provides better stability of the network for a long time and a large high-speed. The node remains alive for a long period. It is structured on three phases. First, the sink node broadcasts a control message (ID, position of the sink) and each node receiving this message stores the sink information and broadcasts a small message containing its identifier, position and energy status. Thus, every node will have an update of all the other nodes' positions. Selecting the next hop, the election of the parent node or a freight forwarder is based on a set of criteria that each node use to compute its cost function. Finally, the data transmission phase to the parent node or forwarder assigns time slots (TDMA) to each of children to send him data. After sending data, node switches in idle mode.

The SIMPLE routing protocol was proposed for intra-WBAN communications, it optimizes the energy-consumption, reliability and throughput of multi-hop communications

between sensor nodes and the sink. This protocol could be extended to apply to BBN communications with further QoS considerations, where each WBAN sink would represent either the parent or the forwarder for the inter-WBANs routing.

In [37], authors presented a low overhead tree-based Energy-Efficient Routing Scheme (EERS) with a multi-hop routing and low overhead in WBANs based on Collection Tree Protocol (CTP), considering adaptive power control to save energy and keep sensor node for a long time. To evaluate performances of EERS, authors compare it with CTP (collection tree protocol) in terms of packet reception ratio (PRR), collection delay, energy consumption and energy balancing. The simulation results show that EERS exhibits a mean delay 30% lower than the mean delay of CTP and an energy consumption 10% lower than CTP, while achieving at least 0.95 PRR.

The EERS routing protocol is proposed for intra-WBAN multi-hop communications, it ensures a good tradeoffs between reliability, delay and energy consumption. It could be extended to a BBN routing protocol, with adding a mobility management/prediction module and more detailed data traffic classification.

Other works proposed detailed expressions of the power consumption profile of a WBAN node, such as [41], where the authors focused on the MAC layer design to determine the energy profile of a sensor node. Thus, [41] provided the equation defining the total energy consumed by a WBAN node, which implements a number of energy components, each corresponding to a task performed by the node to transmit a packet. The main advantages of this model are:

- Generic: it doesn't depend on the type of MAC protocol and thus, it could be used in a heterogeneous WBAN network, like a BBN scenario.
- Expanded: each energy component appears clearly in the model and could be optimized to minimize the total energy consumed by a sensor node.

Nevertheless, this model did not consider the topology constraints and routing mechanisms that may introduce extra energy components. Yet, in [38] authors provided an Energy-aware Topology Design for Wireless Body Area Networks (EAWD) that takes into consideration the topology problem, minimizing the number of relay nodes and thus the total energy consumption as well as the total network installation cost. Furthermore, the EAWD model explicitly formulates each energy component by displaying both circuitry and amplifier dissipated energy, it also separates the different transmission instances: i) sensors transmitting to relays, ii) relays forwarding to relays and iii) relays forwarding to sinks. As well as the different reception instances: i) Relays receiving from sensors, ii) relays receiving from relays and iii) sinks receiving from relays.

Thereby, EAWD provides more accurate transmission and reception energy values in accordance with topology features, together with sensor roles (node, relay or sink). This is a key feature of EAWD that allows it to apply to BBN context. Indeed, two energy components could be added to the sink energy expression, to specify the transmission and

reception energy between sinks of neighboring WBANs. Also, two further node roles could be specified in a BBN context, namely: i) sinks forwarding to sinks and ii) sinks receiving from sinks.

Nonetheless, EAWD lacks some important components that were considered in [37], namely the retransmission energy, the MAC access energy and the signaling energy.

Another key feature of the energy efficiency in WBANs is the duty cycle considered in [39]. Indeed, this model removes the need of idle listening for clear channel, thus lowering the amount of unnecessary overhead and this by adopting TDMA MAC protocol in such a way to reduce communication time relatively to power down time, and this is the principle of duty cycle. However, the major limitation of this model is the assumption of a static topology of the WBAN, which raises the major problem of TDMA, i.e., the need of a synchronization scheme to collect data efficiently from network sensors. Yet, [39] assumes that synchronization can be simplified since the WBAN has relatively constant network structure and fixed sensor functions. Although the duty cycle mechanism is very useful for a BBN scenario, where minimizing traffic overhead is necessary to ensure an energy-efficient routing among WBANs, this assumption of static topology is unsuited to a dynamic BBN where each WBAN member can join and leave the BBN network seamlessly, and without the need for any centralized infrastructure.

Table 2.1 recapitulates the salient features of the aforementioned energy-aware protocols for intra-WBANs communications.

2.3.2 Interference mitigation in BBNs

We discuss in this section the most relevant works that deal with the problem of interference mitigation between different technologies that share the same frequency spectrum and that could be used by the coexisting WBANs within a BBN (i.e., Bluetooth, ZigBee, WiFi, IEEE 802.15.6, etc...).

Whilst a number of previous interference-aware studies have been based upon power considerations [42, 43], others have chosen different alternatives [44, 45] to deal with this substantial problem which is challenging in WBAN design, and raising even more with the emergence of BBNs.

In [42] the authors propose a distributed power control algorithm which converges to the Nash Equilibrium, representing the best tradeoff between energy and network utility. No transmissions are envisaged among WBANs in [42]; a transmission is either from a WBAN node to its gateway or vice versa, neither access technology assumption is made, it is rather assumed that only mutual interference could happen. However, in a BBN context where WBANs communicate with each other, it is mandatory to consider transmissions among WBANs' gateways and thus investigate cross-interference scenarios where different wireless technologies could be used for intra-WBAN and inter-WBANs transmissions scenarios.

While most power control models provide interference-aware schemes over power adaptation, authors of [43] optimized a transmission scheme given a constant power. They

formulated an interference-aware channel access game to deal with the competitive channel usage by different wireless technologies sharing the ISM band, in both static and dynamic scenarios.

On the other hand, the main idea in [45] is that using only power control to combat this interference might not be efficient; it could even lead to situations with higher levels of interference in the system. Therefore, the work in [45] proposes several interference mitigation schemes such as adaptive modulation as well as adaptive data rate and adaptive duty cycle. Interference Mitigation Factor is introduced as a metric to quantify the effectiveness of the proposed schemes. Based on SINR measurements, these schemes are likely suitable for small-scale WBANs where SINR is function of the transmit power, such as in [42] which uses the SINR metric as a utility function to model the interference problem between neighboring WBANs considering a power control game. In fact, in [42] the network topology is static and no actual communications among WBANs are considered. However, in [46], an experimental study proved the importance of the impact of human body shadowing in off-body communications. Yet, for relatively complex BBNs, SINR is also highly dependent on outdoor conditions and human body effects, and the aforementioned schemes would no longer be efficient, or they should be extended taking into account additional physiological, physical, and environmental parameters. Particularly, in dynamic scenarios, when the SINR is varying due to the fast topology changes with neighboring WBANs movements, relying only on the transmit power in order to keep the desired link quality might not be effective. Indeed, in a BBN scenario with high transmit power from other coexisting wireless networks/WBANs, the interference is significant and the desired link quality cannot be achieved unless considering the surrounding conditions (interference) and the wireless channel characteristics in terms of shadowing, fading, etc., which can be incorporated into the channel gain parameters of the SINR.

Besides, several works investigated the interference mitigation problem with detailed specifications of wireless technologies, especially WiFi, ZigBee, and Bluetooth, which are very popular in the WBAN industry. For example, authors of [47] proposed an approach that accurately characterizes the *white space* in WiFi traffic and develop a ZigBee frame control protocol called WISE, which can predict the length of white space in WiFi traffic and achieve desired trade-offs between link throughput and delivery ratio. The empirical study of ZigBee and WiFi coexistence provided by [47] is useful to understand and model the cross-technology problem. Nevertheless, the WiFi-WiFi and ZigBee-ZigBee mutual interference problems still need to be carefully investigated, especially when coupled with mobility, topology changes and other features related to the complexity of BBN networks, which require more intelligent functions at the WBAN coordinator's (MT) level, in order to ensure an effective channel allocation scheme for BBNs. Further studies [48, 49, 50] have dealt with the solutions that enable ZigBee links to achieve guaranteed performance in the presence of heavy WiFi interference, but almost all of them propose approaches that assume having already established the ZigBee and WiFi links, and try to implement mechanisms to mitigate the interference between them.


Priority	Traffic priority	Traffic designation
Lowest  Highest	0	Background (BK)
	1	Best effort (BE)
	2	Excellent effort (EE)
	3	Controlled load (CL)
	4	Video (VI)
	5	Voice (VO)
	6	Medical data or network control
7	Emergency or medical event report	

Table 2.2: WBAN traffic priority according to [7].

In [51], authors addressed the interference mitigation problem for BBNs considering a centralized approach and formulated it as an optimization problem. To solve efficiently the problem even for large-scale network scenarios, two heuristic solutions were developed, namely, a customized randomized rounding approach and a tabu search scheme. The present work differs from [51] in two main aspects: (1) we formulate the problem of mutual and cross-technology interference mitigation, considering the Signal-to-Interference-Ratio (SIR) and we therefore allocate WiFi/ZigBee wireless channels to communication links optimizing the SIR ratio, while in [51] the interference was only quantified by the binary decision variables; (2) we address the interference mitigation problem using a distributed approach, with concepts and mathematical tools from Game Theory, while this problem was tackled in [51] in a completely centralized way.

2.3.3 QoS-aware traffic management for BBN

In general, the design of a BBN is intended for specific applications (ubiquitous healthcare, sport team, group of firefighters, military, etc.), therefore, the routing protocol to be implemented, in order to ensure inter-WBAN communications within a BBN, should be able to fulfill the QoS demands of the WBAN application by using QoS-aware protocols.

In [7], the authors proposed a game theoretical approach using a QoS-based utility function to resolve the problem of overlapping between coexisting WBANs. The solution, based on the Cournot model, consists in fairly dividing the limited resources among the different players, where the player is the WBAN coordinator. The QoS parameters in this paper are throughput, delay and priority. The player's QoS demands are taken from the traffic specifications of the streams that are carried within the contention free period. The WBAN traffic priorities are detailed in Table 2.2. It was verified that the player's utility

increases with the increase of the throughput and decrease of the delay, according to the Cournot competition model.

Even though the utility function is based on QoS parameters, no energy efficiency parameter is considered and no mobility information is involved, WBANs are assumed fixed and the overlapping problem is only considered in a static topology. The model could be applied to BBN scenario to minimize the interference between neighboring WBANs, with more specific investigations, especially with traffic priorities compliant to the BBN application, for instance, military QoS is different from sport team QoS, also QoS mapping schemes are needed in case of heterogeneous BBN scenarios, where WBANs could use different transmission technologies.

The energy constraint was well-considered in [22], where the authors proposed McMAC which is a MAC protocol with multi-constrained QoS provisioning for heterogeneous traffic in WBANs. Delay and reliability are considered as the most important QoS metrics in WBAN. McMAC classifies the intra-WBAN traffic into four classes, based on the delay and the reliability, as follow:

- **Type 0:** emergency traffic with hard QoS constraints. Both delay and reliability are very important. It's an event-triggered traffic when there is a life-critical situation.
- **Type 1:** both delay and reliability-constrained, but requires soft QoS comparing to traffic 0, requiring hard QoS. It must be delivered with higher reliability in a certain deadline (electrocardiogram for example).
- **Type 2:** reliability-constrained but not delay- constrained. This traffic has strict reliability but can tolerate delay like respiration monitoring.
- **Type 3:** delay-constrained but not reliability- constrained. This traffic can tolerate some packet losses but not delay (for example, telemedicine video streaming applications).
- **Type 4:** no constraints on delay and reliability. This traffic does not have any strict constraints like the measurement of patient's physiological parameters (temperature, pressure, etc.).

The McMAC protocol introduces a novel superframe structure based on the "Transmit-when-ever-appropriate" principle which guarantees multi-constrained QoS. The authors present how McMAC deals with different types of traffic. A handling mechanism for emergency traffic is used to ensure a delivery in the least possible delay and the highest reliability. They described how the BC (wBAN Coordinator) and the nodes respond when there is an emergency packet in both cases, CAP (Contention Access Period) and CFP (Contention Free Period). McMAC is energy-efficient, and provides a QoS classification of the WBAN traffic, but only star topology is considered (single-hop). Multi-hop communications should be considered, especially to be applicable to inter-WBAN communications in BBNs.

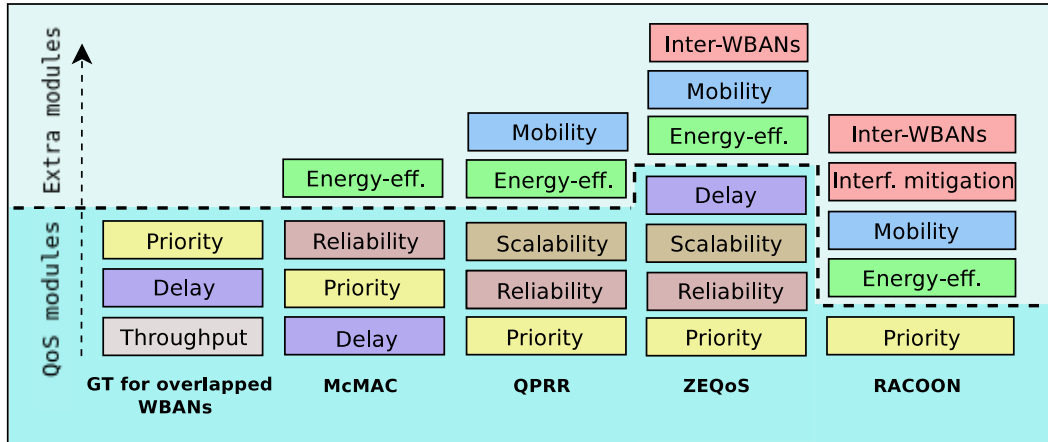


Figure 2.4: QoS modules of WBAN QoS protocols suitable for future U-Health BBNs.

Another existing solution is presented in [20], where the authors proposed a new protocol QPRR (Qos-aware Peering Routing protocol for Reliability). This protocol uses end-to-end path reliability and redundant paths to ensure reliability in the WBAN. They proved that QPRR effectively performs for both stationary and movable patients. This protocol is intended to be employed with indoor-hospital WBAN peering framework. They classify the devices used in WBAN communication into three types considering their energy levels: Nursing Station Coordinator (type 1), which is directly connected to the power source, Medical Display Coordinator (type 2), which uses replaceable batteries, and WBAN Coordinator (type 3), which has limited energy availability. The architecture of QPRR has five main modules:

- Reliability Module (RM): this module monitors the number of packets sent to a neighbor node and the number of acknowledgments received from that node.
- Packet Classifier (PC): it classifies data packets and Hello packets and MAC receiver.
- Hello Protocol Module (HPM): it consists in two sub-modules; the neighbor table constructor and the neighbor table.
- Routing Services Module (RSM): the main functions are to build the routing table, classify data packets and choose the best path for each data class.
- Qos-aware Queuing Module (QQM): after choosing the proper next hop, the RSM sends the data packets to the QQM, which differentiates the data packets in two types and puts them in a separate queue.

The simulations of QPRR protocol verify successful transmission rate, reduced network traffic load, reduced energy consumption and latency. The QPRR reliability is above 88% for low density stationary WBAN nodes and 75% for movable WBAN nodes. The scalability

is also ensured for a large number of nodes and the reliability is above 74%. In this work, the network is infrastructure-based, with a Nursing Station Coordinator (NSC), Medical Display Coordinator (MDC), and mobile WBANs (patients), whereas in a BBN, we consider a completely distributed communication model with only WBANs as source and destination nodes. Furthermore, no specific bandwidth estimation/verification was considered in the path selection procedure, which is a relevant parameter in the QoS-constrained healthcare application. Besides, no fault detection procedure is implemented, the reliability module passes the information of successful data packets' transmission acknowledgments from MAC layer to the network layer to estimate the reliability of a link between the WBAN and its neighbor, and then it does not detect congestion or predict link failures.

In another recent study [19], the authors improved the QPRR protocol by adding a delay module. In this paper the authors propose a novel integrated energy and QoS-aware routing protocol called ZEQoS. This protocol deals with the optimization of energy consumption, end-to-end latency and reliability requirements of the wireless body area network. They classify the data packets into three classes: ordinary packets (OPs), delay-sensitive packets (DSPs) and reliability-sensitive packets (RSPs). It is intended to be used in hospital indoor environment. It calculates the best next hops for the three classes of data packets thanks to its different modules and algorithms. ZEQoS relies on two main layers: MAC layer and network layer. In the MAC layer, ZEQoS implements four modules: MAC receiver, reliability module, delay module and MAC transmitter. In the network layer it implements also four modules: packet classifier (PC), Hello protocol module (HPM), routing services module (RSM) and QoS-aware queuing module (QQM).

In the performance evaluation, the authors measured the throughput by calculating the number of packets successfully received at the destination node. The path selection mechanism of ZEQoS improves throughput for all data types because it considers geographic location, energy availability, end-to-end path delays and end-to-end path reliability. The ZEQoS provides a mechanism which calculates the communication costs, delays and reliability of all possible paths with the help of neighbor table constructor algorithm, routing table constructor algorithm and path selector algorithm and finally choose the best possible path with the consideration of QoS requirement of the different data types.

ZEQoS also offers better performance in terms of higher throughput, fewer packets dropped on MAC and network layers, and lower network traffic than comparable protocols, namely DMQoS [52].

The solution in [21] consists in a Random Contention based Resource Allocation (RACOON) Medium Access Control (MAC) protocol to support the quality of service (QoS) for multi-user mobile wireless body area networks (WBANs). RACOON is a bandwidth control system integrated in medium access control (MAC) layer. To ensure the multi-WBAN QoS, RACOON have two major designs:

RACOON utilizes a centralized control, by the Central Processing Node (CPN), to minimize energy consumption of the WBANs, to early detect inter-WBAN interference and avoid packet collisions. RACOON implements, then, a probing-based inter-WBAN

interference detection to decrease energy waste in the WBANs, which simplifies QoS controls. Therefore, RACOON uses two distinct channels: one for inter-WBAN, to exchange the resource negotiation messages, and the other channel is for intra-WBAN, to transmit polling messages and data packets between the CPN and the sensor nodes. RACOON also implements an iterative bandwidth control according to the users' priority index, so that high priority WBANs get better bandwidth than low priority WBANs.

The advantage of the RACOON protocol is that it considers multi-WBAN designs, with inter-WBAN interference and inter-WBAN priorities considerations, based on polling messages. Moreover, it takes into account the mobility feature of the WBANs in order to encounter the possible collisions and energy waste. Such mechanism could be used in BBNs to assign priorities to WBANs according to their requested services, and their energy status. Nevertheless, RACOON does not consider inter-WBANs communications, which require further QoS considerations and mobility management to ensure the effective inter-WBANs routing.

2.3.4 Mobility management for BBN

Mobility management can positively affect the service-oriented as well as the application-oriented aspects of mobile networks. Especially for BBN ubiquitous healthcare applications, accurate mobility prediction is necessary for critical tasks related to the routing of medical data among mobile WBANs, such as call admission control, congestion control, reservation of network resources, preconfiguration of services and QoS provisioning.

Mobility management is mandatory in a dynamic environment, such as BBNs, where the network topology is changing in a regular or irregular basis, and the mobility of other WBANs should be taken into consideration with respect to a WBAN of interest. Several works have considered the mobility prediction issue in mobile networks context [53, 54, 55, 56, 57].

In the absence of previous works on the mobility management and prediction for BBN scenarios, we review in this section the most relevant studies undertaken for Ad hoc networks, with consideration of specific constraints of BBNs. In [53] the mobility prediction methods are, first, classified into three main categories: movement history based methods, physical topology based methods and logical topology based methods, which are presented in detail and compared in Table 2.3, the possible use cases of each method in the context of U-health BBN applications are also proposed.

Authors of [57] proposed an optimized WBAN handover strategy, a hop-by-hop method to reach the Sink, and a method to maximize the network throughput by using stable routes to avoid inter- and intra-flow interference based on mobility prediction. A joint mobility prediction-based stable and channel assignment approach is used to maximize network throughput.

Category	Advantages	Disadvantages	U-health BBN application
Movement History Based Mobility Prediction			
	Exploit the regularity in human movement behavior within a defined period of time.	Unpredictable changes in user's behavior. Limited feasibility for supporting high quality services.	U-health monitoring for some sports/Athletes
Physical Topology Based Mobility Prediction			
Link expiration time estimation	Estimate the expiration time of the wireless link. Routes are reconfigured before they disconnect.	Support simple node mobility with no sudden changes in the moving directions and speeds	U-health in indoor environments (hospital, rest home)
Link availability estimation	Immediate Rerouting in link failure case. Select more reliable neighbors to form more stable clusters.	Difficulties in learning the changes in link status due to nodes movements. In highly volatile environments, increase of the control overhead.	U-health in accidents and emergencies. (Patient transportation, sharing emergency information, and vital signs monitoring.)
Group mobility and network partition prediction	Prevent disruptions caused by the network partitioning. Low-complexity clustering algorithm accurately determines the mobility groups and their mobility	Assume that group and node velocities are time invariant, which is not a realistic assumption.	U-Health for a rescue team in a disaster area
Cluster change based prediction	Predict the next cluster change depending on the mobile node position in the cluster and its moving direction in the region.	This method needs an accurate location. The method requires the use of a GPS to build the sectors and locate the mobile nodes positions.	U-health monitoring of a group of soldiers. The position and mobility of each soldier are function of those of his neighbors.
Logical Topology Based Mobility Prediction			
Neighboring Nodes Relative Mobility Based Prediction	Based on past measurements. Mobile nodes use a linear model to estimate their future distance from their cluster head (CH).	Do not take node mobility into account during CH election.	U-health in indoor environments (hospitals), or u-health monitoring of a sport team or a rescue team in outdoor/indoor environment.
Information theory based mobility prediction	Assume that a geographical area is divided into virtual clusters. The method does not make any use of a fixed geographical partition. Online learning of the probability model used for predicting the next neighborhood.	Frequent CH changes due to node mobility. The mobility of each node is inferred from how different the neighborhood of the node is over time.	U-health in indoor environments, or U-health monitoring of a sport team or a rescue team in a limited geographical area.
Evidence based mobility prediction	The method does not require the use of a GPS. Accurately predict user traveling trajectory. The signal strength is used to estimate the distances among the mobile nodes. Applied to the Zone Routing Protocol.	This prediction process is performed only on the border nodes, to predict each mobile node's future cluster.	Feasible in outdoor environments, for U-health monitoring of freely moving patients or any group of persons in an outdoor/indoor environment.

Table 2.3: Comparative study of mobility prediction methods for U-Health BBNs

In [55], a distributed Prediction-based Secure and Reliable routing framework (PSR) was proposed for emerging Wireless Body Area Networks (WBANs). It is observed that body sensors may exhibit regular mobility when a user's physical activity (e.g., swimming and jogging) contains repeated motions, and as a result, link quality and a sensor's neighbor set often present periodic changes. Using this model, the sensor node predicts the quality of its incidental links as well as the change of its neighbor set. By the underlying routing protocol, the node selects a subset of incidental links that can be used to forward packets to the sink; among these links, it chooses the one that has the highest predicted quality as next hop.

This framework requires each WBAN coordinator to locally maintain a prediction model and obtain the neighborhood conditions in the immediate future. With the prediction results, the nodes can choose the incidental links of best quality for packet relaying, so as to improve routing reliability and adaptively enable/disable source authentication function to resist data injection attacks.

The study in [56] analyzes two requirements to enable mobility support in mobile WBANs: location independence and clock drifting resilience:

- i) Location independence: means that the different phases of a Time Division Multiple Access (TDMA) transmission should be decoupled, to avoid nodes having to remain in one location. This is reflected, for example, in the requirement to let a subset of WBAN coordinators or BBN routers, transmit acknowledgments rather than only one of them. Doing so; the biological sensors or mobile WBANs, does not have to remain near a specific receiving coordinator or router for an acknowledgment.
- ii) Clock drifting: arises in larger, multi-hop networks with random mobility, namely BBNs. In such networks, the protocol timing becomes more critical and protocol clock drifting resiliency should be added or increased. For example, more acknowledgment slots would improve channel utilization with a very limited impact on energy efficiency.

Yet, the two requirements are applicable to BBN networks to ensure free mobility of patients, in both indoor and outdoor environments. The number of ACKs in the location independence process should be customized according to the BBN application and the different WBANs' QoS demands. Clock drifting is also needed in large scale BBN scenarios.

The work in [54] presents a comprehensive configurable mobility model (MoBAN) for evaluating intra and extra-WBAN communication. It implements different postures as well as individual node mobility within a particular posture. Extra-WBAN protocols take care of communications between a WBAN and its environment, with potentially several wireless body area networks as well as an ambient network. The mobility prediction is based on Markov model. The selected posture also determines the local movement of sensor nodes and the global mobility of the whole WBAN. Therefore, it affects the connection between the nodes in the WBAN and the external network like other WBANs or the surrounding ambient sensor network. Authors use a one-level Markov template to model pattern sequences while maintaining randomness of the posture selection. In any type of location, we may have different posture patterns. As an example, different rooms in a building can be thought of

as having statistically different posture patterns. The posture pattern in a bedroom is surely different from the pattern in the living room or the kitchen. In addition to WBAN topology changes, the BBN topology is also subject to random changes due to WBANs' mobility. The advantage of MoBAN is that it considers both intra- and extra-WBAN movements, and is able to provide mobility information for both scenarios. Such information could be used as a routing parameter for BBNs, and according to WBANs specific needs/applications, this information could represent a mobility prediction parameter.

To maintain the high-quality, data routing should not only take into consideration the change of mobile WBANs locations or topology, as the reactive routing schemes do, but anticipate the movement behavior of mobile nodes employing proactive routing procedures. If each mobile WBAN's future location and network topology can be predicted, then route reconstruction can be done prior to topology changes within BBNs.

2.3.5 Security policies for BBN

Given their restricted resources, often body sensors are vulnerable to data injection attacks, that aim to consume the resources of a target WBAN by flooding the node with false data. Especially, when a WBAN roams from one BBN to another, handover mechanism takes place increasing the risk of the physical capture of the WBAN. Thus, mostly invasive attacks happen during the mobility of WBANs beyond the BBN borders or AP's coverage zones. Yet, issues related to security must be investigated in BBNs, and security schemes should be designed in accordance with the intended applications and their possible threats. In U-healthcare context, holistic security scheme is, above all, a mandatory requirement for U-health BBN application design, since human lives are definitely at stake. Intrusion detection and prevention techniques are a must in these networks. Due to sensitive nature of healthcare applications, extra measures such as encryption of data, and constant monitoring of the network are necessary. As privacy measures, all WBAN communications over wireless links and Internet are required to be encrypted to protect the user's privacy, thus specific users/WBANs should not be identified unless there is a need.

In [58] the authors proposed a solution based on preloaded keys as well as automatically generated keys from biometrics of the human body. This technique is hybrid because it supports both plug-and-play capability and also pre-deployment of keys in order to ensure the security. It provides an efficient solution for intra-WBAN and inter-WBAN communications.

- Intra-WBAN: in the proposed solution the sensors measure physiological values (PVs) of the human body and then the keys are automatically calculated using those PVs to secure communications.
- Inter-WBAN: the solution is based on preloaded keys. The technique is efficient in terms of memory and also security because we combine auto generation and preloading key to enhance security. Any Personal server (PS) can generate key pool using

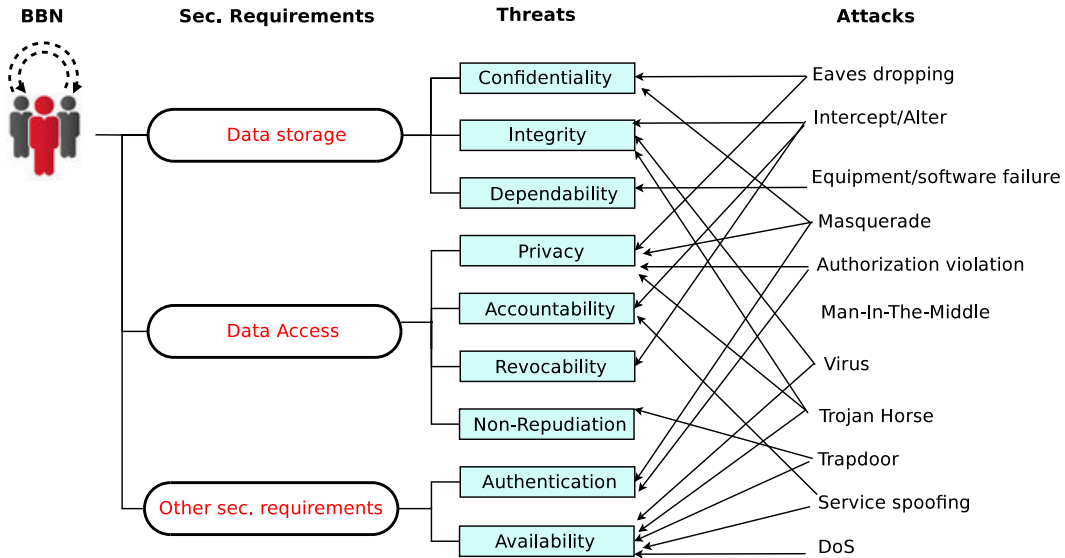


Figure 2.5: Major security requirements in BBNs.

biometric values and then transmit it to the network. The medical server (MS) assigns the responsibility of refreshing the key to any PS generator.

The solution averts from the different attacks like outsider attack, PS compromise, sensor node compromise, KeyGen compromise. The hybrid technique ensures the confidentiality, authentication and integrity of WBAN communications. Authors compared their solution with existing techniques and they demonstrate the improvement in terms of storage, communication, energy overhead and security. This solution is useful for a BBN scenario, since it considers the inter-WBAN communications which include the communication among the Personal Servers of the network WBANs, in order to deal with situations when a PS is out of range of the Medical Server. However the hybrid security mechanism does not consider the dynamic scenarios where WBANs are mobile and, thus, could present further security threats, due to their position changes.

Yet, authors of [59] proposed a cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications, which takes into consideration the mobility of WBANs to the extent that it implements a WBAN neighborhood discovery mechanism, re-clustering in case of cluster head leaving or new arrival WBAN configuration, and WBAN addition or eviction. The proposed security mechanism consists in an energy-efficient key management scheme for WBANs that takes into account the available resources of a node during the whole life cycle of key management. The cluster formation process itself is secured by using electrocardiogram-based key agreement scheme. This framework supports both intra-WBAN and inter-WBAN communications and is then highly suitable for BBN applications.

On the other hand, authors in [60] proposed a new method to improve the security in the WBAN, which objective is to decrease the required memory, control packets complexity, control buffers and mend the existing damages resulting from the high speed of transferring data between nodes. To ensure these goals, [60] proposes a cryptography scheme to secure the communications intra-WBANs, by combining the Advanced Encryption standard (AES) and sensor node bio-signals.

Besides, there are several security proposals in the literature about WBANs and their applications, the work in [61] cites some of them. First, the security mechanism for WBANs must be adjusted to the subsequent major security necessities which are divided into three classes (Figure 2.5):

- Data storage security requirements:
 - i) *Confidentiality*: patient data should be kept confidential during storage periods, using encryption and Access Control Lists.
 - ii) *Integrity*: Patient data must not be modified illegally during storage periods.
 - iii) *Dependability*: Patient data must be retrievable when node failure or data erasure happens.
 - iv) *Privacy*: Data access policy shall be enforced to prevent unauthorized access to patient data generated by the WBAN.
- Data access security requirements:
 - i) *Accountability*: When a WBAN abuses his/her privilege to carry out unauthorized actions on patient's data, he/she should be identified and held accountable.
 - ii) *Revocability*: The privileges of WBANs should be deprived in time if they are identified as compromised or behave maliciously.
 - iii) *Non-repudiation*: The origin of a piece of patient data cannot be denied by the source that generated it.
- Other security requirements:
 - i) *Authentication*: the sender of a patient data should be authenticated, and injection of data from outside the WBAN should be prevented.
 - ii) *Availability*: The patient data should be accessible even under denial-of-service (DoS) attacks.

Then, specific mechanisms should be developed to ensure a secure environment around the WBAN, which will detect, prevent and reinforce the WBAN against attacks. The authors present existing security mechanisms and develop these issues on 7 aspects:

1. **Cryptography**: Cryptographic functions are used to ensure the safety and security of the information collected by sensor nodes (vital signs of a patient). Choosing the cryptographic system depends on the WBAN application and its energy consumption.

Protocol	Energy-eff.	Reliability	QoS	Mobility	Security	Intra-WBAN	Inter-WBAN
EAAODV [34]	✓		✓	✓		✓	
SIMPLE [36]	✓	✓				✓	
EERS [37]	✓	✓				✓	
M-ATTEMPT [35]	✓		✓	✓		✓	
EAWD [38]	✓	✓		✓		✓	
MoBAN [54]				✓		✓	✓
McMAC [22]	✓	✓	✓			✓	
QPRR [20]		✓	✓			✓	
ZEQoS [19]	✓	✓	✓			✓	✓
RACoon [21]		✓				✓	✓
PSR [55]		✓		✓	✓	✓	
MobiHealth [62]		✓	✓	✓	✓	✓	
Hybrid Sec. Mechanism [58]	✓				✓	✓	✓
Cluster-based sec. mechanism [58]	✓			✓	✓	✓	✓

Table 2.4: Comparison of existing WBAN solutions which can be extended to BBN environment.

2. **Key Management:** Key management protocols are used to develop a secure application. especially, to set up and distribute varied forms of cryptographic keys to nodes within the network. There are three types of key management protocols, the trusted server, considering a trusty base station to validate the key agreement, the key pre-distribution, based on the symmetric key cryptography, and finally, the self enforcing, using a public-key infrastructure.

3. **Secure routing:** the sensor node collects physiological information and sends this data to alternative devices. Routing data and message forwarding could be a crucial service of end-to-end communication. There are many routing protocols proposed for sensor network in literature but they suffer from several security vulnerabilities, for example, the associate degree offender may launch denial-of-service attacks on the routing protocol. An assailant may conjointly inject malicious routing information into the network, leading to inconsistencies within the routed packets.

4. **Resilience to Node Capture:** The resilience against node capture is one of the foremost difficult issues in sensor networks. For example, in real time healthcare applications, the medical sensors are placed on a patient's body, who is in a hospital environment that can be accessible by attackers. To resolve this problem, one feasible solution is to use tamper resistant hardware.

5. **Trust Management:** defines the mutual association of any two trustworthy nodes that are sharing their data.

6. **Secure Localization:** to facilitate mobility for patients, the authors specify in [63] the localization systems that are divided into: distance/angle estimation, position computation

and localization algorithms.

7. Robustness to communication Denial-of-Services: The DoS attack can be implemented in the WBAN, by broadcasting high-energy signals. There is a number of potential attacks, for example, an associate in nursing opponent might delay communication by violating medium access management protocol or transmit packets, whereas a neighbor node is transmitting.

Finally, a number of industry and research projects have paid a special attention to the security issue in WBANs. For healthcare applications, the European MobiHealth project presented in [62], provides a complete end-to-end ambulant patient monitoring using a Bluetooth or ZigBee-based communication device, and is a single-hop network. The solution is deployed by UMTS and GPRS networks. The major detailed issues are security, reliability of communication devices, and QoS guarantees.

2.4 Conclusion

In this chapter, we provided a brief overview of the current proposals related to WBANs and their possible application in body-to-body networks design. We mainly discussed the major challenges of inter-WBANs communications focusing on five principal axes: energy efficiency, interference and coexistence, mobility prediction, QoS, and security. At the end, we summarize the aforementioned solutions in Table 2.4. Therewith, BBNs are expected to offer a potential wide range of ubiquitous healthcare benefits to patients, medical personnel and overall society, including numerous community activities. As part of our future work, we plan to design a routing protocol for inter-WBANs communications within a BBN, considering the aforementioned proposals which should be tailored to fit BBN specific requirements. Indeed, effective incentives are intended to improve the accuracy of BBN deployment and coexistence within the existing infrastructures, in order to ensure public safety and improve the Quality of Life for future human generations.

Chapter 3

Interference Mitigation in Body-to-Body Networks: a game theoretical approach

Contents

3.1	Introduction	33
3.2	Game Theory: the big picture	33
3.3	System models	35
3.3.1	Body-to-Body Network Model	36
3.3.2	Body-to-Body Network Interference Model	39
3.4	Socially-aware Interference Mitigation (SIM) game in Body-to-Body Networks	41
3.4.1	BBN-stage SIM game	43
3.4.2	WBAN-stage SIM game	49
3.4.3	A discussion on social interactions of WBANs in the SIM games	51
3.5	Conclusion	52

3.1 Introduction

In this chapter, we identify and exploit opportunities for cooperation between a group of mobile Wireless Body Area Networks (WBANs), forming a Body-to-Body Network (BBN), through inter-body interference detection and subsequent mitigation. Thus, we consider a dynamic system composed of several BBNs and we analyze the joint mutual and cross-technology interference problem due to the utilization of a limited number of channels by different transmission technologies (i.e., ZigBee and WiFi) sharing the same radio spectrum. To this end, we propose a game theoretical approach to address the problem of Socially-aware Interference Mitigation (SIM) in BBNs, where WBANs are “social” and interact with each other. Our approach considers a two-stage channel allocation scheme: a BBN-stage for inter-WBANs’ communications and a WBAN-stage for intra-WBAN communications. We demonstrate that the proposed BBN-stage and WBAN-stage games admit exact potential functions, which led to the conclusion that SIM game converges to Nash equilibrium points.

3.2 Game Theory: the big picture

Game theory has been applied to specific areas, including economics, politics, biology and networking, where decision makers, called the players, have to take actions, or strategies, that have mutual possibly conflicting consequences [64].

Since the radio communication channel is usually shared in wireless networks, the behavior of a wireless device could affect the communication of neighboring wireless devices. In this context, WBAN and BBN communications are subject to such problem, which requires specific and robust mechanisms to deal with routing and resource allocation problems in a competitive environment, especially with the absence of a central unit that monitors the channel utilization within the network.

Game theory is applied in such distributed problems, such as in [44], where the multi-channel usage problem in Wireless Sensor and Actuator Network (WSAN) is modeled as a channel allocation game with the total interference of the whole network as the social objective to minimize. In WSANs, communication and control are highly integrated, even though each node (a sensor, actuator or control unit) is equipped exclusively with one simple half-duplex radio transceiver. However, the major difference with our network model is that BBNs are randomly distributed networks where underlying WBANs are mobile and equipped with two radio antennas to ensure on-body and off-body communications. Yet, WBANs may randomly overlap with each other, which makes BBN a highly dynamic system over time and space, compared to WSNs, apart from the human body environment challenge related to WBANs. Yet, further constraints are to be considered to design an effective channel allocation scheme for BBNs.

Using Game Theory, authors of [43] stated that a decentralized approach is resilient to users’ deviation and ensures the robustness of the network, compared to a centralized approach where the system cannot be easily protected from a selfish deviation to increase,

unilaterally, one's throughput. Alike our BBN model, this game considers nodes concurrently transmitting in nearby clusters, incorporating the Signal-to-Interference-plus-Noise Ratio (SINR) model as wireless communication metric. Nonetheless, the game focuses on the channel access problem under *inter-cluster* interference from nearby Access Points (APs) using the same wireless technology, while the key advantage of our work is to consider both *mutual* and *cross-technology* channel interference problems.

In [65], the authors provided an interesting study that explores the possibility of exploiting Partially Overlapped Channels (POCs) by introducing a game theoretic distributed Channel Assignment (CA) algorithm in Wireless Mesh Networks (WMNs). The proposed CA algorithm aims at increasing the number of simultaneous transmissions in the network while avoiding signal interference among multi-radio nodes. A Cooperative Channel Assignment Game (CoCAG) is implemented, where information is exchanged with neighboring nodes. In fact, by considering neighboring information, nodes can track the instantaneous neighbors' strategies when assigning channels to themselves, which can help in guaranteeing a fair sharing of the frequency band. The major contribution of [65] is that it addresses four different types of interference and their influence on the network capacity: Co-channel Interference, Orthogonal Channels, Adjacent Channel Interference and Self Interference. Nonetheless, one key feature of the WMN is the backbone network composed of Mesh Routers that are usually static and have no constraints on energy consumption, which is not the case for WBANs. Moreover, only IEEE 802.11g was used as wireless technology in [65], and as a consequence no cross-technology scenarios were considered.

Again, in order to cope with the interference issue in WBANs, authors of [66] implemented an intelligent power control game which allows WBANs to improve their performance by learning from history. The proposed power controller implements a genetic algorithm (GA) which enables WBANs to learn from experience and select their power strategies in a distributed manner with no inter-node negotiation or cooperation. Authors state that less inter-node interactions are more attractive for WBANs due to their low overhead and superior scalability. However, such assumption barely adapts to our network model, due to the ever changing topology, the highly dynamic outdoor environment, and the continuously joining and leaving WBANs typical of a BBN scenario.

Apart from WBANs, The spectrum access problem is also tackled from a game theoretical perspective in [67] for cognitive radio networks. A non-cooperative game is proposed to share the wireless channel between licensed/primary users and unlicensed/secondary users (SU), so as to exploit the spectral gaps left available by primary users. To accurately model the channel access game, the interference between SUs is considered as a congestion cost component in the players objective function.

Game theory is also used in [68] for the placement of competing providers' base stations (BS). The game utility function is based on the SINR, to determine the cells where mobile terminals have selective behaviors towards the base stations belonging to different network providers.

In general, a game $G = (\mathcal{N}, \mathcal{S}, \mathcal{U})$ is defined by the following three elements [64]:

- \mathcal{N} is the set of players. For convenience, the subscript $-i$ designates all the players belonging to \mathcal{N} except i himself.
- $\mathcal{S} = S_1 \times S_2 \times \dots \times S_{|\mathcal{N}|}$ designates the set of the strategy spaces of all players, where S_i corresponds to the pure strategy space of player i . The set of selected strategies constitutes a *strategy profile* $s = \{s_1, s_2, \dots, s_{|\mathcal{N}|}\}$, where $s_1 \in S_1, s_2 \in S_2, \dots, s_{|\mathcal{N}|} \in S_{|\mathcal{N}|}$.
- \mathcal{U} designates the set of payoff functions or utilities of all players, where $u_i(s) \in \mathcal{U}$ quantifies the outcome of the game for player i given the strategy profile s .

To solve such distributed problems, the most famous solution is the *Nash equilibrium* [69]. A set of strategies is a Nash equilibrium if each represents a *best response* to the other strategies; each player has, then, no incentive to deviate from his selected strategy to increase his payoff function, since it is the best he can do given what others are doing. The best response $br_i(s_{-i})$ of player i to its opponents strategies s_{-i} is defined as follows :

Definition 1 The best response $br_i(s_{-i})$ of player i to the profile of strategies s_{-i} is a strategy s_i such that:

$$br_i(s_{-i}) = \arg \max u_i(s_i, s_{-i})$$

Then, if all players select their best-response strategies, the concept of Nash Equilibrium is formally defined as follows [64]:

Definition 2: The pure strategy profile s^* constitutes a Nash equilibrium if, for each player i , the payoff function u_i verifies:

$$u_i(s_i^*, s_{-i}) \geq u_i(s_i, s_{-i}), \forall s_i \in S_i$$

In what follows, as a first part of our work in this thesis, we use game theory basics and theorems to model the interference problem in Body-to-Body Networks, and we develop best-response algorithms to resolve the channel allocation issue in two stages: intra-WBAN and inter-WBAN. We finally demonstrate the existence of Nash equilibria in such distributed systems.

3.3 System models

In this section, we present the system models, including the network model and the interference model, arising in body-to-body networks.

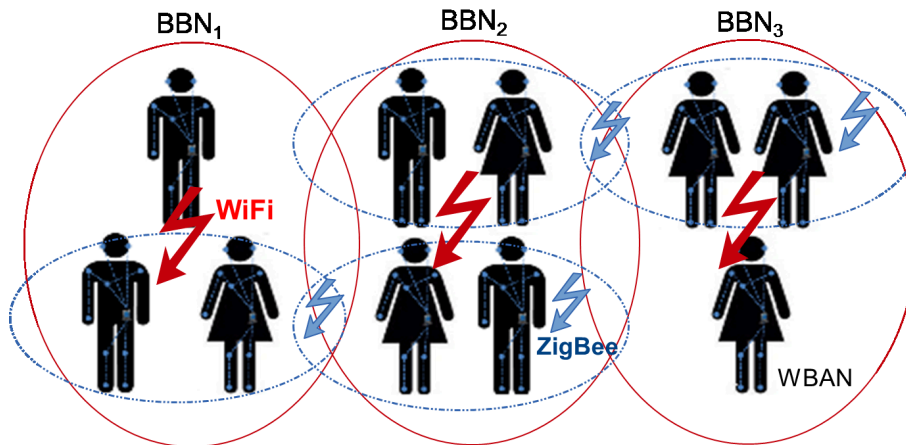


Figure 3.1: Three-*BBN* interfering scenario: each *BBN* is composed of several *WBANs* which use different transmission technologies (i.e., *ZigBee* and *WiFi*) sharing the same radio spectrum.

3.3.1 Body-to-Body Network Model

We consider a *BBN* scenario composed of a set \mathcal{N} of *WBANs*, which are located in the same geographical area (i.e., a medical center, a rest home or a care home), and share the same unlicensed 2.4 GHz ISM band. Let \mathcal{C}^w and \mathcal{C}^z denote, respectively, the set of *WiFi* and *ZigBee* channels in this band.

Each *WBAN* is equipped with a wearable *Mobile Terminal (MT)*¹, that uses both the 802.15.4 protocol (i.e., *ZigBee*) to communicate with the sensor nodes within its *WBAN*, and the IEEE 802.11 wireless standard (i.e., *WiFi*) to create a backhaul infrastructure for inter-*WBANs*' communications (Fig. 3.1).

Since we are assuming that *WBANs* can move and interact with their surrounding environment, we find ourselves in a quite dynamic *BBN* scenario, and therefore, we decide to divide the operating time of the whole system into a set T of consecutive epochs, and during each epoch $t \in T$ we suppose that the network topology and environment conditions do not change.

The set $\mathcal{L}^w(t)$ represents all *WiFi* unidirectional links established by mobile terminals during the epoch $t \in T$; $\mathcal{L}^w(t)$ may vary between two consecutive epochs due to *WBANs*' mobility. On the contrary, the set \mathcal{L}^z , which represents the *ZigBee* unidirectional links used for intra-*WBAN* communication among the sensors, does not change with time, and for this reason, we omitted the parameter t from this set.

Recent works dealing with interference mitigation have considered the binary model to represent overlapping between channels [47, 48, 49, 50, 51]; i.e. a node is either interfered or not, however our idea in this work is to quantify the interference between partially

¹The *WBAN* and his corresponding *Mobile Terminal* will be used as synonyms throughout this thesis.

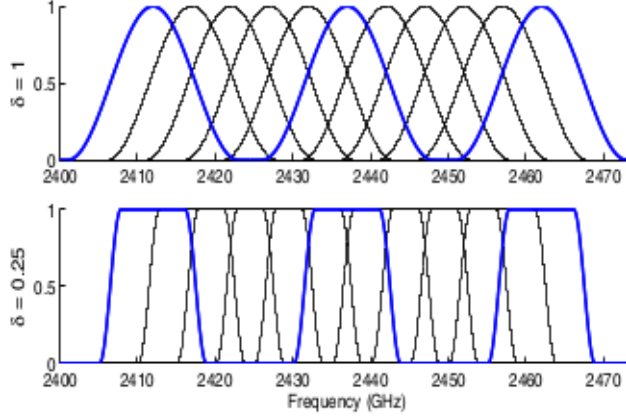


Figure 3.2: The 802.11b frequency responses with the raised cosine filter [2].

overlapped channels. In [70], the authors model the overlapping among different WiFi channels defining a symmetric channel overlapping matrix W , whose element w_{mn} quantifies the degree of interference between channels m and n , and is given as follows:

$$w_{mn} = \frac{\int_{-\infty}^{+\infty} F_m(w)F_n(w)dw}{\int_{-\infty}^{+\infty} F_m^2(w)dw}, \quad (3.1)$$

where $F_m(w)$ and $F_n(w)$ denote the Power Spectral Density (PSD) functions of the band-pass filters for channels m and n , respectively, which can be obtained from the channels' frequency responses. Yet, we need to know which channel filter is being used. As in [70], we assume the use of *raised cosine filters*, whose principle is explained in [2]. Fig.3.2 shows how the PSD function of the IEEE 802.11b depends on the *roll-off factor* δ , which is a key parameter of the raised cosine filter, when it is equal to 1 and 0.25, respectively. Hence, [2] gives a simplified expression of the W matrix :

$$w_{mn} = w_{nm} = \frac{A_o}{A_o + A_{no}} \quad (3.2)$$

where A_o and A_{no} are the overlapping and non-overlapping areas between the power spectral density of channels m and n , respectively. With expression (3.2), the W matrix can be computed off-line and used as a constant matrix while computing the channel allocation variables.

Since different wireless technologies use different signal modulations and access mechanisms, authors of [71] performed an extensive set of experiments to measure the partial overlap of

the IEEE 802.11b standard, using different physical layer modulation methods. First, they considered 1 and 2 Mbps data-rates for the physical layer, using the Binary Phase Shift Keying (BPSK) modulation, to measure the channel overlap. Then, they reported results using the Complementary Code Keying (CCK) modulation, with a data-rate of 11 Mbps. It was concluded that partially overlapped channels can provide much greater spatial re-use if used carefully, depending on the physical separation and/or the channel separation between neighboring links, whatever the modulation scheme in use.

In this work, we model the channel overlapping problem analytically by studying its impact on the signal-to-interference ratio. Yet, although the channel overlapping matrix W has been defined to model the partially-overlapped channels for the 802.11b protocol, it does not depend, actually, on the technology in use, since the expression could involve the PSD functions of any frequency responses, provided that the frequency band presents overlapping behaviors, which is actually not the case for ZigBee and BLE, since both frequency bands present orthogonal wireless channels.

To summarize, our network model will focus on the following relevant elements:

- Every single WBAN's MT, muniequipped with one WiFi antenna and one ZigBee antenna, should dispose of non overlapping WiFi and ZigBee channels.
- No interference is present within a WBAN; we assume a TDMA-based medium access control implemented in each WBAN to deal with collisions. Note in addition that there is no interference between adjacent ZigBee channels since there is no overlapping.
- The interference between overlapping WiFi and ZigBee channels is represented by the matrix A , of size $|\mathcal{C}^w| \times |\mathcal{C}^z|$, whose element $a_{c_1c_2}$ is a binary value: $a_{c_1c_2} = 1$ if WiFi channel c_1 overlaps with ZigBee channel c_2 (0 otherwise).
- As in [70], the degree of interference between overlapping WiFi channels is represented by the matrix W , of size $|\mathcal{C}^w| \times |\mathcal{C}^w|$, whose element $w_{c_1c_2} \in [0, 1]$ is a fractional value, defined by the expression in Equation (3.1).
- To preserve the network connectivity within the BBN, we assume that all WBANs WiFi interfaces are tuned on the same channel. Therefore, we use the $|\mathcal{L}^w| \times |\mathcal{L}^w|$ matrix $B(t)$, whose element b_{ij} is a binary value: $b_{ij} = 1$ if WiFi links i and j belong to the same BBN at time epoch $t \in \mathcal{T}$ (0 otherwise).
- Finally, WBANs use a higher transmission power on the inter-WBAN channel than on the channel used for intra-WBAN communications (i.e. $p^w \gg p^z$). In particular, data transmissions within ZigBee networks can completely starve due to WiFi communications, which use 10 to 100 times higher transmission power [51].

In order to minimize the total interference within BBNs involving several wireless technologies, it is advantageous to observe every interference component separately, thus we can specify two-kind interference scenarios:

- The Mutual interference:
 - WiFi-WiFi interference at the MT receiver, that occurs while receiving collected data from a nearby WBAN of the same BBN and interfering with adjacent BBNs' WiFi links. Such component includes as well the co-channel interference.
 - ZigBee-ZigBee interference at the MT receiver, that happens when a ZigBee link of a WBAN interferes with a ZigBee link of another WBAN belonging to the same or to a different BBN, when they are allocated the same channel.
- The Cross-Technology interference: WiFi-ZigBee, among adjacent WBANs, where each WBAN (MT) is communicating with other WBANs over a WiFi link and is susceptible to interference from nearby ZigBee links, and vice versa.

The *Interference issue* and the *SIR metric* are tightly related. Thus, in this thesis, we would focus on the interference metric (SIR) expressed in decibel format by:

$$SIR_i(t)(dB) = 10 \log \left(\frac{g_{ii}(t)p^i}{\sum_{j \neq i} g_{ij}(t)p_j} \right), \quad (3.3)$$

where p^i is the transmission power of transmitter i , $g_{ij}(t)$ is the link gain from transmitter j to receiver i at time epoch t . Since WBANs can move in their surrounding environment, the links' gains $g_{ij}(t)$ vary over time, and the SIR in turn has been further expressed as a function of time t .

The gain parameters are calculated taking into account the average channel gain evaluated at the reference distance $d_0 = 1 \text{ m}$ and with a path loss exponent $n(\alpha)$, according to the following formula [72]:

$$g_{ij}(t)|_{dB} = G(d_0, \alpha)|_{dB} - 10 \times n(\alpha) \times \log_{10}(d/d_0), \quad \forall i, j \in \mathcal{L}^w(t) \cup \mathcal{L}^z \quad (3.4)$$

Specifically, the average channel gain $G(d_0, \alpha)$, between WBANs' MTs (Tx Right Hip, Rx Right Hip), significantly decreases from -37.88 dB to -66.33 dB when switching from Line Of Sight (LOS) to Non Line Of Sight (NLOS) conditions, which ensures that our BBN scenarios are consistent with a realistic human body environment.

3.3.2 Body-to-Body Network Interference Model

The interference model defines the set of links that can interfere with any given link in the network [73]. There have been various interference models proposed in the literature; the common concept is that two communication links $i = (T_i, R_i)$ and $j = (T_j, R_j)$ are interfering if and only if either T_i or R_i lies within the *interference range* of T_j or R_j , where T_i , T_j and R_i , R_j designate the transmitter and receiver interfaces of links i and j , respectively.

If modeling the interference characteristics in sensor networks is challenging, it is more so for BBNs, because Radio Frequency (RF) characteristics of nodes and environments are

neither known a priori nor computable due to their stochastic, rapidly changing characteristics [74]. Any routing protocol working in high interference environment is incapable of dealing with radio channels suffering from high interference ratios. Thus, sharing channels appropriately according to the interference profiles is mandatory and prior for BBN networks design.

Interference range is the range within which nodes in receive mode will be interfered with an unrelated transmitter and thus suffer from packet loss [75]. For simplicity, ranges are generally assumed concentric which is not necessarily given in physical networks. In [75], the interference range was defined based on SIR, where authors assume a transmission scenario with transmitter-receiver distance as d meters and at the same time, an interfering node r meters away from the receiver, starts another transmission. The received signal is assumed to be successful if it is above a SIR threshold (SIR_{th}).

Conflict Graph Given an interference model, the set of pairs of communication links that interfere with each other, assuming mutual and cross-interference in our model, can be represented using a conflict graph. As done in [51], we depict an extended conflict graph to model the mutual and cross-technology interfering wireless links. We adopt this representation because it will help us in defining the set of neighbors in next sections for our Socially-aware Interference Mitigation game. Therefore, the extended conflict graph $G_c(V_c(t), E_c(t))$ is defined as follows:

- $V_c(t)$: set of vertices corresponding to WiFi and ZigBee communication links in the network, $V_c(t) = \mathcal{L}^w(t) \cup \mathcal{L}^z$.
- $E_c(t)$: set of edges corresponding to the interference relationship among pairs of links. Fig.3.3 depicts the extended conflict graph of the three BBN-scenario illustrated in Fig.3.1. Solid lines represent conflict edges between two vertices using the same radio technology, i.e. $(e_1, e_2) \in E_c(t)$ is a conflict edge if and only if $e_1, e_2 \in \mathcal{L}^w(t)$ or $e_1, e_2 \in \mathcal{L}^z$, and they are interfering with each other. Whereas dashed lines correspond to cross-conflict edges between two vertices using different radio technologies.

Our goal is to minimize the overall network interference. To give an example, let us consider the scenario of Fig.3.1. Each BBN has different interference ranges with its neighboring BBNs. Assuming that only three WiFi orthogonal channels from the 2.4 GHz band are available (1, 6, and 11), one trivial solution would be to assign channels 1, 6 and 11 to BBN1, BBN2 and BBN3, respectively. In this case there would be no interference. Let us assume now that only two WiFi orthogonal channels 1 and 6 are available, in addition to channel 2 overlapping with channel 1. Thus, channels 1, 6 and 2 would be assigned to BBN1, BBN2 and BBN3, respectively. Since BBN1 and BBN3 have disjoint interference ranges,

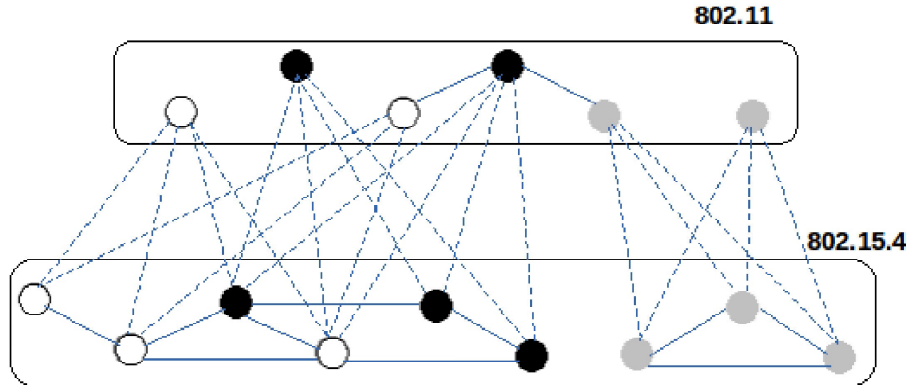


Figure 3.3: Extended Conflict Graph of the scenario illustrated in Fig.3.1

they can use overlapping channels with minimal risk of interference. In practice, the system is more complex, with many more BBNs, and/or more overlapping interference ranges, involving several wireless technologies. Therefore a general approach should be investigated for an appropriate wireless resource sharing according to the interference profiles. Likewise, in such heterogeneous wireless systems, a two-stage channel allocation scheme is needed; a BBN level game for WiFi channel allocation step, then a WBAN level game for ZigBee channel allocation, taking into account the cross-technology features at each stage.

The social information in the BBN and WBAN level games can be collected by using a signaling protocol, like one of those presented in [76, 77], to allow mobile terminals to exchange control messages (or proximity information) among each other in order to build the network topology and the conflict graph, and then compute in a completely distributed fashion the channel assignment that minimizes the mutual and cross-technology interference, or maximizes the SIR at WiFi and ZigBee radio interfaces, based on local information. A detailed description of the information exchange protocol is provided in [76].

3.4 Socially-aware Interference Mitigation (SIM) game in Body-to-Body Networks

In this section, we first define the basic notation and parameters used hereafter, and then we describe in detail the proposed socially-aware interference mitigation game theoretical approach.

The lack of a centralized control and prioritization of access to the radio spectrum, in addition to the restricted knowledge of network information, motivate us to employ local interactions for the WiFi and ZigBee level games, in which players consider their own payoffs as well as those of their neighbors, so as to optimize their strategies while relying on their surrounding network information. Besides, at the BBN-stage game, each group of WBANs (i.e., each sub-BBN) is represented by a special player (a delegate or a leader of the

Notation	Definition
$ \cdot $	Cardinality of a given set.
\mathcal{T}	Set of consecutive time epochs.
\mathcal{C}^w	Set of WiFi channels in the 2.4GHz ISM Band, $\mathcal{C}^w = \{1, 2, \dots, 14\}$
\mathcal{C}^z	Set of ZigBee channels in the 2.4GHz ISM Band, $\mathcal{C}^z = \{11, 12, \dots, 26\}$
$\mathcal{L}^w(t)$	Set of WiFi communication links over a time epoch $t \in \mathcal{T}$, $\mathcal{L}^w(t) = \{1, 2, \dots, \mathcal{L}^w(t) \}$
\mathcal{L}^z	Set of ZigBee communication links corresponding to WBANs' MT ZigBee antennas, $\mathcal{L}^z = \{1, 2, \dots, \mathcal{L}^z \}$
$\mathcal{L}(t)$	Set of players of the SIM game. $\mathcal{L}(t) = \mathcal{L}^w(t) \cup \mathcal{L}^z$
$p_w^l(t)$	Transmit power of a WiFi link l at time epoch $t \in \mathcal{T}$.
p_z^h	Transmit power of a ZigBee link $h \in \mathcal{L}^z$.
g_l	Channel gain of link $l \in \mathcal{L}^w(t)$.
g_{lh}	Inter-network interference gain, between links l and h .
X_w	Channel allocation matrix of WiFi links.
Y_z	Channel allocation matrix of ZigBee links.
$x_{c_1}^l$	X_w -matrix element: WiFi channel c_1 is allocated to WiFi link l .
$y_{c_2}^h$	Y_z -matrix element: ZigBee channel c_2 is allocated to ZigBee link h .
w_{mn}	Interference degree between WiFi channels m and n (continuous metric).
a_{mn}	Binary parameter of cross-interference between WiFi channel m and ZigBee channel n .
$(s^l(t), s^h(t))$	Strategies of WiFi ($x_{c_1}^l$) and ZigBee ($y_{c_2}^h$) channels' allocation, respectively, for the couple of links (l, h) of a single WBAN.
$(s^l(t), s^h(t))^*$	Optimal channel allocation strategies of player/couple (l, h) of a single WBAN.
$S(t)$	Set of channel allocation strategies of all players.
$S^*(t)$	Set of optimal channel allocation strategies of all players.

Table 3.1: Parameters notations for the channel assignment game

group) who decides which WiFi channel to choose. Indeed, to ensure network connectivity all WBANs within the same sub-BBN should be tuned to the same WiFi channel, and we consider this special player that acts on behalf of the entire sub-BBN. To this end, we consider in this work a two-stage socially-aware interference mitigation scheme:

(i) At a first stage, each BBN takes a decision on the WiFi channel that should be assigned to his WiFi transmission links, ensuring minimal interference with his surrounding environment, through a local interaction game with his neighboring BBNs.

(ii) Then, at the second stage, given the WiFi channel assignment for each BBN, a local interaction game takes place among the WBANs belonging to the same BBN. After playing this game, each WBAN (more precisely, each MT) will be assigned a ZigBee channel to his ZigBee radio interface, and such assignment guarantees the minimal interference of the WBAN with his neighboring WBANs.

The overall operations for the time epoch $t \in T$ are represented by the SIM flow chart given in Fig.3.4. In this channel assignment game, the players are the set of links $\mathcal{L}(t) = \mathcal{L}^w(t) \cup \mathcal{L}^z$ associated with the set $\mathcal{N} = \{1, \dots, n\}$ of WBANs occupying either the hospital or a care home for old people, and distributed over a set of coexisting BBNs. Each player

is represented by a couple of links (l, h) , such that $l \in \mathcal{L}^w(t)$ and $h \in \mathcal{L}^z$ are a WiFi and a ZigBee link corresponding to a given WBAN $i \in \mathcal{N}$ assimilated to its MT. At time epoch $t \in T$, each player chooses a couple of strategies $(s^l(t), s^h(t)) \subset S(t)$, such as $s^l(t)$ is the strategy to allocate a WiFi channel $c_1 \in \mathcal{C}^w$ to the WiFi link $l \in \mathcal{L}^w(t)$ at time epoch $t \in \mathcal{T}$, denoted by $x_{c_1}^l$, and $s^h(t)$ is the strategy to allocate a ZigBee channel $c_2 \in \mathcal{C}^z$ to the ZigBee link $h \in \mathcal{L}^z$, denoted by $y_{c_2}^h$. $S(t)$ is obviously the set of the total channel allocation strategies of all players of the BBN scenario. The overall SIM game notations are reported in Table 3.1. To summarize, the WiFi and ZigBee channel assignment variables are :

$$x_{c_1}^l = \begin{cases} 1, & \text{if WiFi channel } c_1 \text{ is assigned to the communication link } l \\ 0, & \text{otherwise} \end{cases}$$

$$y_{c_2}^h = \begin{cases} 1, & \text{if ZigBee channel } c_2 \text{ is assigned to the communication link } h \\ 0, & \text{otherwise} \end{cases}$$

which form the following WiFi and ZigBee channel allocation matrices:

$$X_w = \begin{pmatrix} x_1^1 & \cdots & x_{14}^1 \\ \vdots & \ddots & \vdots \\ x_1^l & \cdots & x_{14}^l \\ \vdots & \ddots & \vdots \\ x_1^{|\mathcal{L}^w(t)|} & \cdots & x_{14}^{|\mathcal{L}^w(t)|} \end{pmatrix}$$

$$Y_z = \begin{pmatrix} y_{11}^1 & \cdots & y_{26}^1 \\ \vdots & \ddots & \vdots \\ y_{11}^h & \cdots & y_{26}^h \\ \vdots & \ddots & \vdots \\ y_1^{|\mathcal{L}^z|} & \cdots & y_{26}^{|\mathcal{L}^z|} \end{pmatrix}$$

Hence, hereafter, we first begin with presenting the first-stage game, to choose a WiFi channel assignment for each MT, and then we describe in detail the second-stage game, where each MT is further assigned a ZigBee channel.

3.4.1 BBN-stage SIM game

In order to assign a single WiFi channel to each sub-BBN, we opt for a BBN-stage SIM game so that each set of communicating WBANs, forming a sub-BBN, are represented by a specific WiFi link. The representative WiFi link is situated in the center of the sub-BBN and plays the role of the *delegate*, and the other WBANs belonging to the same sub-BBN will be allocated the same WiFi channel (Fig.3.5). Our choice of the representative WiFi link is similar to the one made by Govindasamy et al. in [78]. In fact, the work in [78] presents a technique to find the spectral efficiency of an interference-limited representative

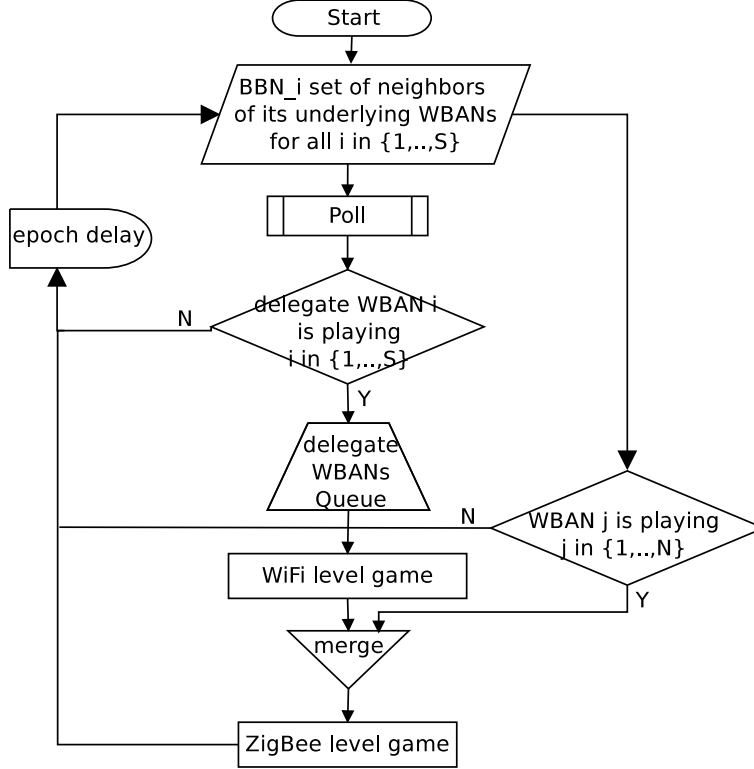


Figure 3.4: Flow chart of bi-level SIM Game.

link with an arbitrary distribution of interference powers, within an ad hoc network with randomly distributed multi-antenna links. This model considers a circular network where the representative receiver is assumed to be at the origin of the circle, and the interferers are links with other receivers whose locations do not impact the representative link. Of course, there exist a variety of different mechanisms/solutions to select the more appropriate delegate/representative link in the network. However, this issue is not the main concern of this thesis and deserves a deep study.

We build the extended conflict graph and we assume that each WBAN has information only about his sub-BBN underlying WBANs, through the exchange of polling messages. Thus, we can identify for each WBAN, the set of interfering neighbors at time epoch $t \in T$ (i.e., the set of edges between a link of such WBAN and transmission links of the others). Let W_l denote the set of links interfering with WiFi link l :

$$W_l(t) = \{k \in L^w(t) : (l, k) \subset E_c(t)\} \cup \{j \in L^z : (l, j) \subset E_c(t)\}$$

Thereby, we can define the BBN-stage game (\mathcal{G}_1) as follows:

- *Players*: the set of BBNs represented by their delegates, such as a delegate player per

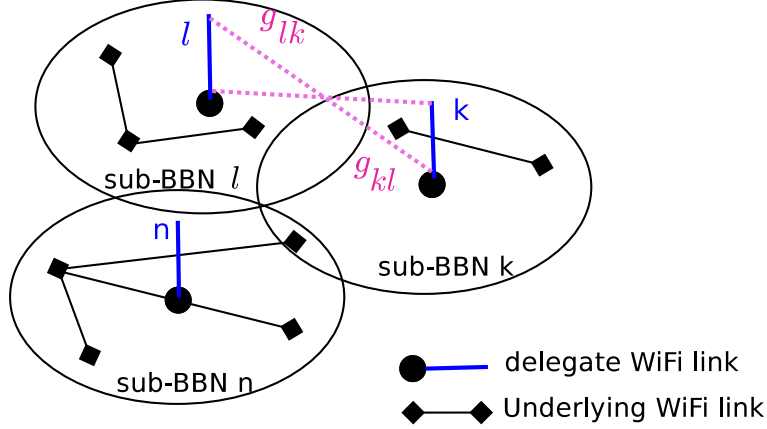


Figure 3.5: Delegate and underlying WBANs' WiFi links

sub-BBN. For the BBN-stage, the player is assimilated to its WiFi link l .

- *Strategies/actions*: $s^l(t) = x_{c_1}^l(t)$, strategy to choose a WiFi channel c_1 for WiFi link l from the set of available channels in \mathcal{C}^w .
- *Utility function*: To ensure a realistic representation of the game, we use the worst SIR values perceived by the two radio interfaces, WiFi and ZigBee, as utility function.

Hereafter, we describe the SIR given in Equation (3.3) that we extend to consider interfering transmitters using different technologies. It is worth noting that Equation (3.5) can be easily extended to more than two radio technologies, considering further for example Bluetooth. However, to simplify the analysis we conduct the study with only two components, corresponding to WiFi and ZigBee, respectively. Whence, the SIR of the player $l \in \mathcal{L}^w$, considering the WiFi interface, is given by:

$$SIR^w(x_{c_1}^l)(t) = 10 \log \left(\frac{g u p_w^l}{I_{c_1}^w(x_{c_1}^l) + I^w(x_{c_1}^l) + I^{wz}(x_{c_1}^l)} \right), \quad (3.5)$$

where

$I_{c_1}^w(x_{c_1}^l)$: Co-channel interference from WiFi links of other sub-BBNs ($b_{kl} = 0$) sharing WiFi channel c_1 with WiFi link l .

$$I_{c_1}^w(x_{c_1}^l) = \sum_{\substack{k \in \mathcal{L}^w \\ b_{kl} = 0}} x_{c_1}^l x_{c_1}^k g_{lk} p_w^k \quad (3.6)$$

$I^w(x_{c_1}^l)$: Mutual interference from WiFi links of other sub-BBNs ($b_{kl} = 0$) using WiFi channels that overlap with c_1 .

$$I^w(x_{c_1}^l) = \sum_{\substack{k \in \mathcal{L}^w \\ b_{kl} = 0}} \left(\sum_{\substack{c \in \mathcal{C}^w \\ c \neq c_1}} w_{c_1 c} x_{c_1}^l x_c^k \right) g_{lk} p_w^k, \quad (3.7)$$

$I^{wz}(x_{c_1}^l)$: Cross-interference from ZigBee links, using ZigBee channels other than c_2 , overlapping with c_1

$$I^{wz}(x_{c_1}^l) = \sum_{\substack{k \in \mathcal{L}^z \\ k \neq h}} \left(\sum_{c \in \mathcal{C}^z} a_{c_1 c} x_{c_1}^l y_c^k \right) g_{lk} p_z^k; \quad (3.8)$$

g_{ll} is the channel gain of link l , g_{lk} the link gain from the transmitter k to the receiver l , p_w^k and p_z^k are the WiFi and ZigBee transmit power, respectively.

Note that in expression (3.8) we use the binary parameter $a_{c_1 c_2}$ to model the cross-technology interference instead of the fractional $w_{c_1 c_2}$ used in Equation (3.7) for mutual WiFi interference. In fact, although in the literature the interference of the IEEE 802.11b has been modeled as an additive white Gaussian noise (AWGN) to the ZigBee signal, the experimental results performed in [79] show a significant performance degradation for ZigBee links in the presence of WiFi transmissions. Specifically, the authors measured a packet loss of 99,75% up to 100% in WBANs used for blood analysis and ECG sensing when a video streaming is executed over an interfering WiFi channel. Therefore, due to the tight constraints on WBANs' transmissions reliability, we consider the worst effect caused by WiFi interference on ZigBee communications, using the binary parameter $a_{c_1 c_2} \in \{0, 1\}$.

1) *Convergence of BBN-stage game: Nash Equilibrium*

Having defined the BBN stage of the SIM game, we then demonstrate that such game indeed admits at least one pure-strategy Nash equilibrium. Thus, we first define the utility function of player l as follows:

$$U_w(x_{c_1}^l) = 10 \log(g_{ll} p_w^l) - 10 \log(IF_l^w(x_{c_1}^l)) \quad (3.9)$$

where $IF_l^w(x_{c_1}^l)$, denoted as the WiFi Interference Function of player l , is the total interference suffered by link l when playing strategy $x_{c_1}^l$, and is expressed as follows:

$$\begin{aligned} IF_l^w(x_{c_1}^l) &= I_c^w(x_{c_1}^l) + I^w(x_{c_1}^l) + I^{wz}(x_{c_1}^l) \\ &= \sum_{k \in W_l \cap \mathcal{L}^w} \sum_{c \in \mathcal{C}^w} f(x_{c_1}^l, x_c^k) + \sum_{j \in W_l \cap \mathcal{L}^z} \sum_{\substack{c \in \mathcal{C}^z \\ c \neq c_2}} g(x_{c_1}^l, y_c^j) \end{aligned}$$

or function of the strategies:

$$IF_l^w(s^l) = \sum_{k \in W_l \cap \mathcal{L}^w} f(s^l, s^k) + \sum_{j \in W_l \cap \mathcal{L}^z} g(s^l, s^j) \quad (3.10)$$

where:

$$f(s^l, s^k) = \begin{cases} 0, & s^l \neq s^k \text{ and WiFi channel } c_1 \text{ of link } l \\ & \text{does not overlap with WiFi channel of link } k. \\ g_{lk} p_w^k, & s^l = s^k \\ w_{c_1 c} g_{lk} p_w^k, & s^l \neq s^k \text{ and WiFi channel } c_1 \text{ of link } l \\ & \text{overlaps with WiFi channel of link } k. \end{cases}$$

and:

$$g(s^l, s^j) = \begin{cases} 0, & \text{WiFi channel } c_1 \text{ of link } l \text{ does not overlap} \\ & \text{with ZigBee channel of link } j. \\ g_l p_z^j, & \text{WiFi channel } c_1 \text{ of link } l \text{ overlaps with} \\ & \text{ZigBee channel of link } j. \end{cases}$$

We observe that the maximization of utility function U_w corresponds to the minimization of the Interference Function IF^w . Due to the property of *monotone transformation*, if the modified game with utility IF^w is a potential game, then the original BBN-stage SIM game with utility U_w is also a potential game with the same potential function. Then, the BBN-stage SIM game (\mathcal{G}_1) is expressed as follows:

$$(\mathcal{G}_1) : \min_{x_{c_1}^l \in S^l(t)} IF_l^w(x_{c_1}^l, x_{c_1}^{-l}) \quad \forall l \in \mathcal{L}^w \quad (3.11)$$

$$s.t. \sum_{c \in \mathcal{C}^w} x_c^l = 1 \quad \forall l \in \mathcal{L}^w(t) \quad (3.12)$$

$$x_{c_1}^l \in \{0, 1\} \quad \forall l \in \mathcal{L}^w(t), c_1 \in \mathcal{C}^w, \quad (3.13)$$

For convenience, we designate by $-l$ all the players belonging to W_l . Constraint (3.12) forces the assignment of a single WiFi channel for a single WiFi link for each player, the connectivity within the sub-BBNs is ensured so that a unique WiFi channel is allocated to every pair of links belonging to the same sub-BBN through the exchange of polling messages between the delegate player and the other players of each sub-BBN. The convergence of the BBN-stage SIM game to a Nash equilibrium is given by the following theorem:

Theorem 1: The BBN-stage SIM game \mathcal{G}_1 is an exact potential game.

Proof: we construct the potential function as follows:

$$\Phi^w(s^i, s^{-i}) = \frac{1}{2} \sum_{i \in L^w} \sum_{k \in W_i \cap L^w} f(s^i, s^k) + \sum_{i \in L^w} \sum_{j \in W_i \cap L^z} g(s^i, s^j) \quad (3.14)$$

Therefore, when player $l \in \mathcal{L}^w$ changes its action at time epoch $t \in \mathcal{T}$, from s^l to s^l , the variation of the potential function subsequent to this player's strategy change is given by:

$$\Phi^w(s^l, s^{-l}) - \Phi^w(\hat{s}^l, s^{-l}) = \frac{1}{2} \sum_{\substack{i \in L^w \\ i \neq l}} \sum_{k \in W_i \cap L^w} f(s^i, s^k) + \sum_{\substack{i \in L^w \\ i \neq l}} \sum_{j \in W_i \cap L^z} g(s^i, s^j) \quad (3.15)$$

$$- \frac{1}{2} \sum_{\substack{i \in L^w \\ i \neq l}} \sum_{k \in W_i \cap L^w} f(s^i, s^k) - \sum_{\substack{i \in L^w \\ i \neq l}} \sum_{j \in W_i \cap L^z} g(s^i, s^j) \quad (3.16)$$

$$+ \frac{1}{2} \sum_{\substack{i \in L^w \\ i \neq l}} f(s^i, s^l) - \frac{1}{2} \sum_{\substack{i \in L^w \\ i \neq l}} f(s^i, \hat{s}^l) \quad (k = l) \quad (3.17)$$

$$+ \frac{1}{2} \sum_{k \in W_l \cap L^w} f(s^l, s^k) + \sum_{j \in W_l \cap L^z} g(s^l, s^j) \quad (i = l) \quad (3.18)$$

$$- \frac{1}{2} \sum_{k \in W_l \cap L^w} f(\hat{s}^l, s^k) - \sum_{j \in W_l \cap L^z} g(\hat{s}^l, s^j) \quad (i = l) \quad (3.19)$$

We can easily see that (3.15)+(3.16)=0. On the other hand, since each player has only interference with his neighboring set, then $\{i \in L^w : i \neq l\} = \{k \in W_l \cap L^w\}$, and we assume that function f is symmetric so as we consider symmetric channel gains ($g_{lk} = g_{kl}$ if $b_{kl} = 0$, Fig.3.5), therefore:

$$\Phi^w(s^l, s^{-l}) - \Phi^w(\hat{s}^l, s^{-l}) = \sum_{k \in W_l \cap L^w} f(s^l, s^k) + \sum_{j \in W_l \cap L^z} g(s^l, s^j) \quad (3.20)$$

$$- \sum_{k \in W_l \cap L^w} f(\hat{s}^l, s^k) - \sum_{j \in W_l \cap L^z} g(\hat{s}^l, s^j) \quad (3.21)$$

$$= IF_l^w(s^l, s^{-l}) - IF_l^w(\hat{s}^l, s^{-l}) \quad (3.22)$$

Accordingly we prove that, when a delegate $l \in \mathcal{L}^w$ deviates from a strategy s^l to an alternate strategy \hat{s}^l , the change in the *exact potential function* Φ^w exactly mirrors the change in l 's utility. Therefore the BBN-stage SIM game is an exact potential game. ■

Thereby, we can rely on the following theorem [80] to confirm the existence of a Nash equilibrium to our game.

Theorem 2: Every potential game has at least one pure Nash equilibrium, namely the strategy s^l that minimizes $\Phi^w(s^l)$.

The result of Theorem 2 motivates us to design the Best Response SIM algorithm in chapter 4 to resolve the BBN-stage SIM game.

3.4.2 WBAN-stage SIM game

We now consider the WBAN-stage game, where each WBAN will be assigned a ZigBee channel to his ZigBee radio interface, that guarantees the minimal interference with his neighbors.

1) ZigBee local interaction game

Similarly to the BBN stage, denote Z_h as the set of neighbors of ZigBee link h , including the set of edges between ZigBee link h and interfering WiFi and ZigBee links, using the conflict graph:

$$Z_h(t) = \{j \in L^z : (h, j) \in E_c(t)\} \cup \{k \in L^w(t) : (h, k) \in E_c(t)\}$$

Hence, we can define the local interaction game of the WBAN stage (\mathcal{G}_2) as follows:

- *Players:* set \mathcal{N} of WBANs. For the WBAN-stage, the player is assimilated to his ZigBee link h .
- *Strategies/actions:* $s^h(t) = y_{c_2}^h(t)$, strategy to choose a ZigBee channel c_2 for ZigBee link h from the set of available channels in \mathcal{C}^z .
- *Utility function:* is, similarly to BBN stage, function of the SIR considering the ZigBee interface which is used for intra-WBAN communications, given by:

$$SIR^z(y_{c_2}^h)(t) = 10 \log \left(\frac{g_{hh} p_z^h}{I^{wz}(y_{c_2}^h) + I^z(y_{c_2}^h)} \right), \quad (3.23)$$

$I^{wz}(y_{c_2}^h)$ represents the *cross-technology* interference caused by mobile terminals using WiFi channels that interfere with the ZigBee channel c_2 on which WBAN link h is tuned.

$$I^{wz}(y_{c_2}^h) = \sum_{\substack{k \in \mathcal{L}^w \\ b_{kl}=0}} \sum_{c \in \mathcal{C}^w} a_{cc_2} x_c^k y_{c_2}^h g_{hk} p_w^k(t). \quad (3.24)$$

$I^z(y_{c_2}^h)$ accounts for the *co-channel interference* of nearby WBANs sharing the same ZigBee channel c_2 of player h .

$$I^z(y_{c_2}^h) = \sum_{k \in \mathcal{L}^z} y_{c_2}^k y_{c_2}^h g_{hk} p_z^k(t). \quad (3.25)$$

Conversely to the BBN stage (Equation (3.5)), in Equation (3.23) only cross and co-channel interference components are considered at the denominator, since all ZigBee channels are completely orthogonal among each other, i.e. no mutual interference is there. In case of sharing the same ZigBee channel, i.e., expression (3.25), the corresponding experimental scenario in [79] measures 18% of packet losses, which led to the conclusion that

the impact of ZigBee co-channel interference may be significant. Therefore, we model our game so that selecting different and non-overlapping ZigBee channels for intra-WBAN communications emerges as the best strategy for all players. Unlike BBN-stage game where a unique WiFi channel is required by a sub-BBN, in WBAN stage, WBANs of the same sub-BBN use different ZigBee channels for intra-WBAN communications. Yet, to ensure a fair sharing of available ZigBee resources within BBNs, we consider local interaction behaviors among players interacting within the same neighboring set, which is translated in the utility function by a local cooperation quantity as a tradeoff to the player selfish attitude. Thus, we define the utility function of player h for the WBAN-stage game as follows:

$$\begin{aligned} U_z(y_{c_2}^h) &= SIR^z(y_{c_2}^h) + \sum_{k \in Z_h} SIR^z(y_c^k) \\ &= 10 \log(g_{hh} p_z^h) + \sum_{k \in Z_h} 10 \log(g_{kk} p_z^k) - IF_h^z(y_{c_2}^h) \end{aligned} \quad (3.26)$$

where: $IF_h^z(y_{c_2}^h) = I_h(y_{c_2}^h) + \sum_{k \in Z_h} I_k(y_{c_2}^h)$

and: $I_k(y_{c_2}^h) = 10 \log(I^{wz}(y_c^k) + I^z(y_c^k))$, $\forall c \in C^z : y_c^k = 1$

$I_k(s^h)$, with $s^h = y_{c_2}^h$, is the total interference suffered by link k of a neighboring WBAN when link h plays strategy $y_{c_2}^h$.

As in [81], using the monotone transformation property, the WBAN-stage SIM game is expressed as follows:

$$(\mathcal{G}_2) : \min_{y_{c_2}^h \in S^h(t)} IF_h^z(y_{c_2}^h, y_{c_2}^{-h}) \quad \forall h \in \mathcal{L}^z \quad (3.27)$$

$$s.t. \sum_{c \in C^z} y_c^h = 1 \quad \forall h \in \mathcal{L}^z(t) \quad (3.28)$$

$$y_c^h \in \{0, 1\} \quad \forall h \in \mathcal{L}^z, c \in C^z \quad (3.29)$$

Constraint (3.28) forces the assignment of a single ZigBee channel for a ZigBee link, for each player.

2) Convergence of WBAN-stage game: Nash Equilibrium

The property of the proposed local interaction game is characterized by the following theorem:

Theorem 4: \mathcal{G}_2 is an exact potential game which has at least one pure strategy NE, and the optimal solution of its potential function constitutes a pure strategy NE.

Proof: we construct the potential function as follows:

$$\Phi^z(s^h, s^{-h}) = \sum_{k \in L^z} I_k(s^h, s^{-h})$$

if we compute the variation of the utility function when player $h \in \mathcal{L}^z$ changes its action at time epoch $t \in T$, from s^h to \hat{s}^h , we obtain:

$$\begin{aligned} & IF_h^z(s^h, s^{-h}) - IF_h^z(\hat{s}^h, s^{-h}) = \\ & I_h(s^h, s^{-h}) - I_h(\hat{s}^h, s^{-h}) + \sum_{k \in Z_h} [I_k(s^h, s^{-h}) - I_k(\hat{s}^h, s^{-h})] \end{aligned} \quad (3.30)$$

On the other hand, the variation of the potential function subsequent to this player's strategy change is given by:

$$\begin{aligned} & \Phi^z(s^h, s^{-h}) - \Phi^z(\hat{s}^h, s^{-h}) = \\ & \sum_{k \in L^z} I_k(s^h, s^{-h}) - \sum_{k \in L^z} I_k(\hat{s}^h, s^{-h}) = \\ & I_h(s^h, s^{-h}) - I_h(\hat{s}^h, s^{-h}) + \sum_{k \in Z_h} [I_k(s^h, s^{-h}) - I_k(\hat{s}^h, s^{-h})] \\ & + \sum_{\substack{k \in L^z \setminus Z_h \\ k \neq h}} [I_k(s^h, s^{-h}) - I_k(\hat{s}^h, s^{-h})] \end{aligned} \quad (3.31)$$

Yet, with the local cooperative nature of WBAN-stage game, h player's action only affects players in its interference range, thus we have:

$$I_k(s^h, s^{-h}) - I_k(\hat{s}^h, s^{-h}) = 0 \quad \forall k \in L^z \setminus Z_h, k \neq h$$

This leads to the following equation:

$$IF_h^z(s^h, s^{-h}) - IF_h^z(\hat{s}^h, s^{-h}) = \Phi^z(s^h, s^{-h}) - \Phi^z(\hat{s}^h, s^{-h})$$

Accordingly we prove that, when a player $h \in \mathcal{L}^z$ deviates from a strategy s^h to an alternate strategy \hat{s}^h , the change in the exact potential function Φ^z exactly mirrors the change in h 's utility.

Therefore the WBAN-stage SIM game is an exact potential game. ■

3.4.3 A discussion on social interactions of WBANs in the SIM games

The social information in the BBN and WBAN level games can be collected by using a signaling protocol, like one of those presented in [76, 77], to allow mobile terminals to exchange control messages (or proximity information) among each other in order to build (and maintain) the network topology and the conflict graph, and then compute in a completely distributed fashion the channel assignment that minimizes the mutual and cross-technology interference, or maximizes the SIR at WiFi and ZigBee radio interfaces, based on local information.

More in detail, we recall that our WiFi and ZigBee utility functions rely on the neighboring sets of a WBAN MT's WiFi and ZigBee pair of links (l, h) , defined as:

$$\begin{aligned} W_l(t) &= \{k \in L^w(t) : (l, k) \subset E_c(t)\} \cup \{j \in L^z : (l, j) \subset E_c(t)\} \\ Z_h(t) &= \{j \in L^z : (h, j) \subset E_c(t)\} \cup \{k \in L^w(t) : (h, k) \subset E_c(t)\} \end{aligned}$$

Link-state messages are used to spread topology information to the entire network. A link-state message contains two lists of WiFi and ZigBee neighbors, each identified by its WBAN and BBN identifiers. Such messages are used by the BBN players to build the network topology and the conflict graph. Then, WBANs' MTs send beacon messages to their neighbors, recognized in their neighboring sets $(W_l(t), Z_h(t))$.

For example, a WiFi beacon message is only sent to the delegates of neighboring BBNs, since a single WiFi channel should be selected by each BBN. Such message contains the identifier of the WBAN, a list of neighbors (from which control traffic has been recently received), and his local information, needed for the utility functions of his neighbors, i.e., $x_{c_1}^k$ and $y_{c_2}^j$, where c_1 and c_2 are the WiFi and ZigBee channels selected by his WiFi and ZigBee links (k, j) . In contrast, the ZigBee beacon message is sent to his neighboring WBANs, within the same BBN, evenly, and contains in addition his SIRz value needed by the local interaction game, as explained hereafter.

Upon receiving a beacon message, the interference mitigation algorithm (BR-SIM) extracts the information necessary to update the utility function. In particular, for each WBAN receiving a ZigBee beacon message from a neighboring WBAN, BR-SIM extracts the SIRz advertised in the beacon message, and updates his utility function, by adding this SIRz value to the local cooperation quantity, as a tradeoff to the player selfish attitude (Equation (25)). A detailed description of the information exchange protocol is provided in [76].

3.5 Conclusion

In this chapter we proposed a novel game theoretical approach for mutual and cross-technology interference mitigation in BBNs. First, we provided a customized expression of the WiFi and ZigBee Signal-to-Interference Ratios to define players' payoff functions for the two-stage game. SIR expressions capture the different interference components, namely the co-channel, the mutual, and the cross-technology interference. Then, using the concepts of exact potential functions and local interaction games, the WBAN-stage and BBN-stage games are demonstrated to admit Nash equilibrium points, proving the convergence of the SIM game to feasible channel assignment solutions.

Chapter 4

Socially-aware Interference Mitigation: Game solutions and channel allocation algorithms

Contents

4.1	Introduction	54
4.2	Best-Response SIM Algorithm (BR-SIM)	54
4.3	Sub-Optimal Randomized Trials for SIM game (SORT-SIM)	56
4.4	Security mechanism - <i>Channel Allocation Time Misuse Attack (CATMA)</i>	59
4.4.1	Misbehavior detection phase	59
4.4.2	Attack prevention phase	62
4.5	Performance evaluation	62
4.5.1	BR-SIM versus SORT-SIM	63
4.5.2	Comparison with power control approaches	70
4.6	Conclusion	76

4.1 Introduction

Using the properties of potential games, we develop in this chapter a Best-Response algorithm for the SIM game (BR-SIM) that converges to Nash equilibrium points. The two-stage model of the game is taken into account and two best-response dynamics are implemented, for both ZigBee and WiFi game stages. A second algorithm, named Sub-Optimal Randomized Trials (SORT-SIM), is then proposed as trade-off between efficient channel allocation process and short convergence intervals, to guarantee a sub-optimal solution to the SIM problem. SORT-SIM and BR-SIM algorithms are then compared in terms of efficiency and computation time. We further compare the BR-SIM and SORT-SIM algorithms to two power control algorithms in terms of signal-to-interference ratio and aggregate interference, and show that they outperform the power control schemes in several cases.

4.2 Best-Response SIM Algorithm (BR-SIM)

Potential games have two appealing properties: they admit at least one pure-strategy NE which can be obtained through a best-response dynamics carried out by each player, and they have the Finite Improvement Property (FIP) [82], which ensures the convergence to a NE within a finite number of iterations. In the following, we propose an iterative algorithm (Algorithm 1) that implements a best response dynamics for our proposed game. Algorithm 1 takes as input the current time epoch $t \in \mathcal{T}$, the set \mathcal{N} of WBANs, the conflict graph $G_c(V_c(t), E_c(t))$, the available WiFi and ZigBee channels ($\mathcal{C}^w, \mathcal{C}^z$), the channel gain, the mutual and cross-technology channel overlapping, and the network connectivity matrices ($\mathcal{G}, \mathcal{W}, \mathcal{A}, \mathcal{B}(t)$). It gives as output the channel allocation matrices $X_w(t)$ and $Y_z(t)$, the minima of the WiFi and ZigBee Interference Functions obtained at the Nash Equilibrium, and the number of iterations NE_{iter} needed to converge to a NE point.

Algorithm 1 starts by forming the coalitions of sub-BBNs whose delegates are representative WiFi links situated in the center with symmetric gains. The delegates and the underlying WBANs are initialized to random WiFi and ZigBee channels with respect to the connectivity criterion within BBNs. Then, the algorithm iteratively examines whether there exists any player that is unsatisfied, and in such case a greedy selfish step is taken so that such player l changes his current strategy $s^l(\tau)$, $\tau < t$, to a better strategy $s^l(\tau + 1)$ with respect to the current action profile of all other players, as follows:

$$s^l(\tau + 1) = \arg \min_{s^l \in \mathcal{C}^w} IF_l^w(s^l, s^{-l}) \quad s.t. \quad (4.1)$$

$$s^{-l} = \{s^1(\tau + 1), s^2(\tau + 1), \dots, s^{l-1}(\tau + 1), s^{l+1}(\tau), \dots, s^{|L^w(t)|}(\tau)\}$$

where s^1, s^2, \dots, s^{l-1} have been updated to their best-responses at iteration $\tau + 1$ and do not change from their selected strategies during the current iteration.

Alike the WiFi Best-response procedure, players iteratively update the ZigBee channels that minimize their Interference Functions, with respect to their WiFi channels selected

at the BBN- (or WiFi-) stage step. Thus, for a ZigBee player h , the strategy domain of the ZigBee channel selection process is delimited to the set of available ZigBee channels $C_h^z(t)$, i.e., not overlapping with his assigned WiFi channel at time epoch t . Therefore, the best-response strategy of ZigBee player h is expressed by:

$$s^h(\tau + 1) = \arg \min_{s^h \in C_h^z(t)} IF_h^z(s^h, s^{-h}) \quad s.t. \quad (4.2)$$

$$s^{-h} = \{s^1(\tau + 1), s^2(\tau + 1), \dots, s^{h-1}(\tau + 1), s^{h+1}(\tau), \dots, s^{|L^z(t)|}(\tau)\}$$

Due to the FIP property, such algorithm is guaranteed to converge in a finite number of iterations to a BBN-stage NE, and then to a local interaction ZigBee NE where no player has an incentive to deviate from his best-response choice.

Algorithm 1: SIM Best Response NE (BR-SIM)

Input : $t \in \mathcal{T}, \mathcal{N}, G_c(V_c(t), E_c(t)), \mathcal{C}^w, \mathcal{C}^z, \mathcal{G}, \mathcal{W}, \mathcal{A}, \mathcal{B}(t)$
Output: $X_w(t), Y_z(t), IF_{min}^w(t), IF_{min}^z(t), NE_{iter}$

- 1 **Initialization**
- 2 Grouping of sub-BBNs and election of the set of delegates: $L_{delegates}^w$;
- 3 Set randomly WiFi and ZigBee action-tuples at $t=0$, $S^w(0) = \{s_0^1, s_0^2, \dots, s_0^{|L^w|}\}$ and $S^z(0) = \{s_0^1, s_0^2, \dots, s_0^{|L^z|}\}$;
- 4 **end Initialization**
- 5 **while** $S^w(\tau)$ is not a Nash equilibrium **do**
- 6 **for** $l \in L_{delegates}^w$
- 7 better response update $s^l(\tau + 1)$: select the WiFi channel that minimizes its Interference Function (**IF**) according to (4.1);
- 8 **end for**
- 9 Set the delegates action profile to $S^w(\tau + 1) = \{s^1(\tau + 1), s^2(\tau + 1), \dots, s^{|L_{delegates}^w|}(\tau + 1)\}$;
- 10 Calculate $IF^w(\tau + 1) = \{IF_1^w(\tau + 1), \dots, IF_{|L_{delegates}^w|}^w(\tau + 1)\}$;
- 11 $\tau = \tau + 1$;
- 12 $NE_{iter}++$;
- 13 **end while**
- 14 $S^w(t) = S^w(\tau)$ is a Nash equilibrium, delegates communicate their WiFi channel selections to WBANs;
- 15 Set the BBN-stage action profile $S^w(t) = \{s^1(t), s^2(t), \dots, s^{|L^w|}(t)\}$ and $X_w(t)$ matrix;
- 16 **while** $\min IF^z(\tau)$ is not reached **do**
- 17 Repeat steps 6-11 for $h \in L^z$ to select the ZigBee channels that minimize the players Interference Function according to (4.2);
- 18 $NE_{iter}++$;
- 19 **end while**
- 20 Set the WBAN-stage action profile $S^z(t) = \{s^1(t), s^2(t), \dots, s^{|L^z|}(t)\}$ and $Y_z(t)$ matrix.

4.3 Sub-Optimal Randomized Trials for SIM game (SORT-SIM)

In large-scale networks with several BBNs, especially in real-time-constrained applications, the exhaustive search of NE can be extremely time consuming. Therefore, we propose, as an alternative solution, the SORT-SIM algorithm to deal with this specific issue. SORT-SIM is based on the principle of ensuring feasible SIR values for all players while allowing them to play simultaneously, and reducing the probability of channel selection conflicts.

Algorithm 2 takes the same inputs as Algorithm 1, and gives the same outputs, i.e., the channel allocation matrices $X_w(t)$ and $Y_z(t)$, the minima of the Interference Functions, and the number of iterations $SORT_{iter}$ needed to reach the sub-optimal solution.

At the beginning, Algorithm 2 describes the main steps relative to the grouping of sub-BBNs, the election of their representative links and the calculation of their corresponding set of neighbors. Then, the WiFi channel allocation is performed, for each delegate l , as follows:

i. First, select randomly a WiFi channel from the list of free WiFi channels, if available, i.e., not allocated in neighboring set of link l (step 8).

$$C_{free}^w(l) = \{c \in \mathcal{C}^w : \forall k \in \mathcal{W}_l(t) \cap \mathcal{L}^w(t), x_c^k = 0\}$$

ii. If no free channel is available, calculate at step 9 the utility (SIR^w) for each delegate and select randomly from the list, WiFi channels that provide an SIR^w above the threshold value (SIR_{th}^w). We denote by C_{th}^w the aforementioned set, defined as:

$$C_{th}^w(l) = \{c \in \mathcal{C}^w : SIR^w(x_c^l) > SIR_{th}^w\}$$

$$c_1 = \begin{cases} Rand(C_{free}^w(l)), & \text{if } C_{free}^w(l) \neq \emptyset \\ Rand(C_{th}^w(l)), & \text{otherwise.} \end{cases} \quad (4.3)$$

iii. To ensure a fair sharing of resources, a WBAN should release his WiFi channel after at most θ s. θ is defined as the maximum time of reservation of the wireless channel, and is assumed as a configurable parameter.

iv. Finally, the WBANs belonging to the same sub-BBN are tuned on the WiFi channel selected by their leader.

The previous operations are iteratively repeated until reaching a number of trials where no WBAN has an incentive to deviate from his channel choice, presenting, thus, a sub-optimal solution for the SIM problem.

Since multiple ZigBee channels could be used within the same sub-BBN, the channel allocation problem is relaxed in the WBAN stage and the aforementioned operations are processed indifferently for each ZigBee link $h \in \mathcal{L}^z(t)$, omitting the last operation (iv.),

Algorithm 2: SIM Sub-Optimal Randomized Trials (SORT-SIM)

Input : $t \in \mathcal{T}, \mathcal{N}, G_c(V_c(t), E_c(t)), \mathcal{C}^w, \mathcal{C}^z, \mathcal{G}, \mathcal{W}, \mathcal{A}, \mathcal{B}(t)$
Output: $\mathbf{X}_w(t), \mathbf{Y}_z(t), \mathbf{IF}^w(t), \mathbf{IF}^z(t), SORT_{iter}$

- 1 Grouping of sub-BBNs and election of the set of delegates $\mathcal{L}_{deleg}^w(t)$
- 2 **for** delegate WiFi link $l \in \mathcal{L}_{deleg}^w(t)$
- 3 Calculate the set of neighbors \mathcal{W}_l ;
- 4 Calculate the set of free WiFi channels $\mathcal{C}_{free}^w(l)$;
- 5 **end for**
- 6 **while** $IF^w(\tau)$ is not a sub-optimal solution **do**
- 7 **for** delegate WiFi link $l \in \mathcal{L}_{deleg}^w(t)$
- 8 **if** $\mathcal{C}_{free}^w \neq \emptyset$ **then** Randomly select WiFi channel c_1 from $\mathcal{C}_{free}^w(l)$;
- 9 **else** Randomly select WiFi channel c_1 such as $SIR^w(x_c^l) > SIR_{th}^w$; **end if**
- 10 **end for**
- 11 Delegates communicate their WiFi channels selections to the underlying WBANs;
- 12 Set the BBN-stage channel allocation matrix $X_w(t)$; Calculate $IF^w(\tau) = \{IF_1^w(\tau), \dots, IF_{L^w}^w(\tau)\}$;
- 13 $\tau = \tau + 1$;
- 14 $SORT_{iter}++$;
- 15 **end while**
- 16 **for** ZigBee links $h \in \mathcal{L}^z(t)$
- 17 Calculate the set of available ZigBee channels for link h , $\mathcal{C}^z(h)$;
- 18 Calculate the set of neighbors \mathcal{Z}_h ;
- 19 Calculate the set of free ZigBee channels \mathcal{C}_{free}^z from $\mathcal{C}^z(h)$;
- 20 **end for**
- 21 **while** $IF^z(\tau)$ is not a sub-optimal solution **do**
- 22 **for** ZigBee links $h \in \mathcal{L}^z(t)$
- 23 **if** $\mathcal{C}_{free}^z(h) \neq \emptyset$ **then** Randomly select ZigBee channel c_2 from $\mathcal{C}_{free}^z(h)$;
- 24 **else** Randomly select ZigBee channel $c_2 \in \mathcal{C}^z(h)$ such as $SIR^z(y_c^h) > SIR_{th}^z$; **end if**
- 25 **end for**
- 26 Set the WBAN-stage channel allocation matrix $Y_z(t)$; Calculate $IF^z(\tau) = \{IF_1^z(\tau), \dots, IF_{L^z}^z(\tau)\}$;
- 27 $\tau = \tau + 1$;
- 28 $SORT_{iter}++$;
- 29 **end while**

		WBAN ₁	WBAN ₂
min IF _w (or IF _z)		c*	c*
SORT-SIM	C _{free}	c _i	c _i
		c _j = c*	c _j = c*
		c _k	c _k
	C _{th}

(a) Available free channels

		WBAN ₁	WBAN ₂
min IF _w (or IF _z)		c*	c*
SORT-SIM	C _{free}	∅	
	C _{th}	c _m	c _l
		c _n = c*	c _n = c*
		c _p	c _q

(b) Non available free channels

Figure 4.1: Examples of SORT-SIM execution.

except some restrictions on the available ZigBee channels. Indeed, for each sub-BBN provided with WiFi channel c_1 , we should delimit the set of available ZigBee channels $\mathcal{C}^z(h)$ eliminating those that overlap with c_1 :

$$\mathcal{C}^z(h) = \{c \in \mathcal{C}^z : a_{cc_1} = 0\} \quad \forall (l, h) \subset \mathcal{L}(t), c_1 \in \mathcal{C}^w : x_{c_1}^l = 1$$

Hence, the algorithm calculates the set of available ZigBee channels for each sub-BBN (step 17), as well as the list of free ZigBee channels (step 19), which is computed with respect to the set $\mathcal{C}^z(h)$.

$$\mathcal{C}_{free}^z(h) = \{c \in \mathcal{C}^z(h) : \forall k \in \mathcal{Z}_h \cap \mathcal{C}^z, y_c^k = 0\}$$

Finally, we define \mathcal{C}_{th}^z , the set of threshold SIR^z values, and the ZigBee channel c_2 is computed similarly to the WiFi part (step 23, 24), as follows:

$$\mathcal{C}_{th}^z(h) = \{c \in \mathcal{C}^z(h) : SIR^z(y_c^h) > SIR_{th}^z\}$$

$$c_2 = \begin{cases} \text{Rand}(\mathcal{C}_{free}^z(h)), & \text{if } \mathcal{C}_{free}^z(h) \neq \emptyset \\ \text{Rand}(\mathcal{C}_{th}^z(h)), & \text{otherwise.} \end{cases} \quad (4.4)$$

We also keep the condition on the fair sharing of resources, so that a WBAN should release his ZigBee channel after at most θ s.

Tables 4.1(a) and (b) give two examples of the worse-case SORT mode, where neighboring players (WBAN₁ and WBAN₂) would select the same optimal solution c^* that minimizes their respective Interference Functions, whereas SORT-SIM algorithm provides them with feasible solutions (those in the circles) that may be the optimal for the one (WBAN₂) and a sub-optimal for the other (WBAN₁), in both cases where free channels are available or not.

Although the proposed SORT-SIM algorithm does not provide the optimal solution for SIM game, it guarantees, at the worst cases, an appropriate strategy with feasible SIR value, i.e. $SIR > SIR_{th}$, while reducing the probability to select the same channel by neighboring WBANs. Furthermore, the simplicity of implementation of SORT-SIM algorithm is a major feature for such highly constrained BBN environment.

4.4 Security mechanism - *Channel Allocation Time Misuse Attack (CATMA)*

Within the context of our BBN channel allocation scheme, we define a new attack which is referred to as Channel Allocation Time Misuse Attack (**CATMA**), joining the NEPA (Network Endo-Parasite Attack), CEPA (Channel Ecto-Parasite Attack) and LORA (Low-Cost Ripple Effect Attack) attacks identified in [83] for the channel assignment in MRMC-WMN (multi-radio multi-channel wireless mesh networks), with consideration of BBN specific constraints. Indeed, this attack exploits the possibility of reservation of the allocated WiFi/ZigBee channel for a threshold period θs , so that to allow stationary players to keep their channel and cut down the game overall computation time. Therefore, a malicious player could:

- i. Extend the time of use of his channel over θs .
- ii. Select a channel that is not yet released by his neighboring WBAN, at $t < \theta s$, in order to reserve this channel for the future; he will minimize his utility in the future to the cost of increasing the overall interference of his neighboring domain at present.

Dealing with such new paradigm (BBN), and in absence of previous works on the channel assignment problem for such networks, we rely on studies undertaken for MRMC-WMN in securing the channel assignment, with consideration of specific constraints of BBN networks.

Noticing that all the known dynamic channel assignment algorithms in WMN require a *channel allocation message exchange*, for the purpose of information dissemination and channel change respectively [84, 85], our security scheme will also require WBANs to transmit the messages similar to CHNL_USAGE (Channel Usage message), CHNL_CHANGE (Channel Change message) and REQ_MONITOR (Request Monitoring Message), to control the secure operation of the SIM game.

Similarly to the channel allocation phase, security mechanism is also based on the concept of neighbor monitoring, and is twofold; a detection phase and a prevention phase:

4.4.1 Misbehavior detection phase

- Each WBAN maintains two counters for CATMA detection and prevention: the *reservation_time* and the *bad-credit* counters for each channel (WiFi and ZigBee), with initial value of 0, for all neighboring WBANs.

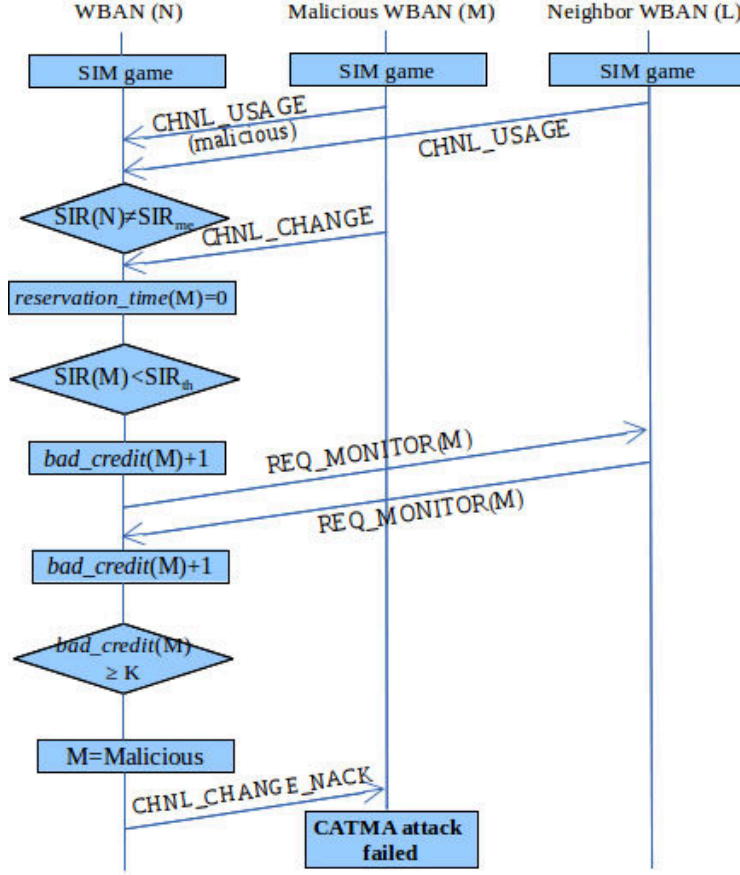


Figure 4.2: CATMA attack scenario and SIM secure mechanism - Reservation of a channel.

- The neighbors of the WBAN (M) receive the CHNL_USAGE message containing the information about the WiFi and ZigBee allocated channels, at time epoch $t \in \mathcal{T}$.
- To verify the correctness of the information contained in the CHNL_USAGE message, each neighbor (N) collects CHNL_USAGE messages from all his neighbors and calculate his utility functions ($SIR^z(N)$, $SIR^w(N)$) with the expressions defined in this thesis including channel allocation variables, and compare them to the measured values (SIR_{me}^z , SIR_{me}^w).
- If the two values match (for each technology), then no misbehavior is detected. If, otherwise, utility and measured values don't match, so there's at least one misbehaving neighbor. Then, WBAN should verify the CHNL_CHANGE messages.
- The $reservation_time$ of each WBAN from which a CHNL_CHANGE message is

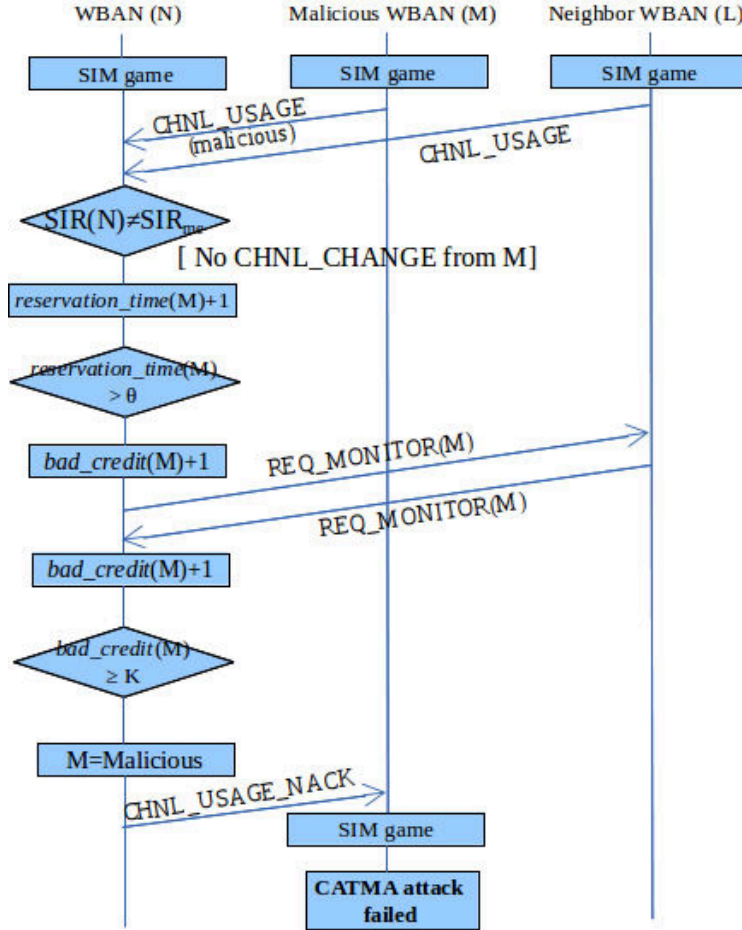


Figure 4.3: CATMA attack scenario and SIM secure mechanism - Extending time of use of a channel.

received, would be reset to 0. With the reception of CHNL_CHANGE message the recipient WBAN (N) would check if the new SIR of the sender (M) (sent for the local interaction game purpose) is above the threshold value (SIR_{th}^z or SIR_{th}^w), if not then the WBAN (M) is trying to reserve the channel to guarantee maximizing his utility in the future. Then the *bad-credit* of the misbehaving WBAN (M) would be incremented marking him as suspicious (Fig.4.2).

- If no CHNL_CHANGE message is received from some WBANs, their *reservation_time* would be incremented up to θ s. If *reservation_time* of WBAN (M) exceeds θ s, the *bad-credit* would be incremented marking the WBAN (M) as suspicious (Fig.4.3).
- The anomalies detected upon the examination of channel allocation messages are reported to the WBANs of the neighboring set of the WBAN (N), in the REQ_MONITOR

message, alerting of the misbehaving WBAN(s).

- If REQ_MONITOR message(s) is(are) received within a waiting time duration (T_w) the *bad-credit* is incremented by number of messages for each suspicious WBAN, and up to the cap value K of *bad-credit*, the corresponding WBAN(s) is(are) marked as malicious.

4.4.2 Attack prevention phase

- If the malicious player corresponding *reservation_time* is over θ s, then a CHNL_USAGE_NACK message is returned, preventing him from keeping the channel over θ s. Upon reception of CHNL_USAGE_NACK the WBAN is forced to play WiFi/Zigbee level game and get a new channel.
- Else, a CHNL_CHANGE_NACK is returned to the misbehaving WBAN, preventing him from reserving this channel. Upon reception of CHNL_CHANGE_NACK the WBAN is forced to release this channel and keep his old channel.
- If at a later time epoch, the misbehaving WBAN starts behaving well, the *bad-credit* is decremented until it reaches 0 when the information from that WBAN is trusted again by its neighbors.

4.5 Performance evaluation

This section illustrates and discusses the numerical results obtained in different network scenarios of both algorithms BR-SIM and SORT-SIM, which have been implemented using the Scilab software package [86]. Then, we compare our algorithms with two existing power control approaches [3, 42], which handle almost the same problem we tackle in this work, i.e., the interference mitigation for nearby WBANs. The mobile WBANs, which number varies in the range [20,50], are randomly deployed in a $1000 \times 1000m^2$ area, and grouped into four overlapping BBNs. The mobility is simulated using the common *random way-point model* [87] (Fig.4.4). We consider the first five overlapping WiFi channels of the ISM band ($\mathcal{C}^w = \{1, 5\}$) and the whole band of ZigBee channels ($\mathcal{C}^z = \{11, 26\}$) in order to simulate the WiFi mutual interference and the cross-technology scenarios. To compute channel gains, we refer to the BBN-specific channel gain model in [72]. The WiFi and ZigBee transmission powers are set to 100 mW and 1 mW, respectively. To prove and compare the effectiveness of our two distributed solutions, we successively evaluate the effect of the WBANs density on the dynamics of the BR-SIM channel selection algorithm and then on the performance of the SORT-SIM algorithm. More specifically, we evaluate the WiFi and ZigBee signal-to-interference ratios for each BBN, proving that the BR-SIM algorithm guarantees a fair sharing of wireless resources, while SORT-SIM presents quickness benefits in some BBN scenarios. SIR_w and SIR_z, in Equations (3.5) and (3.23), respectively, are

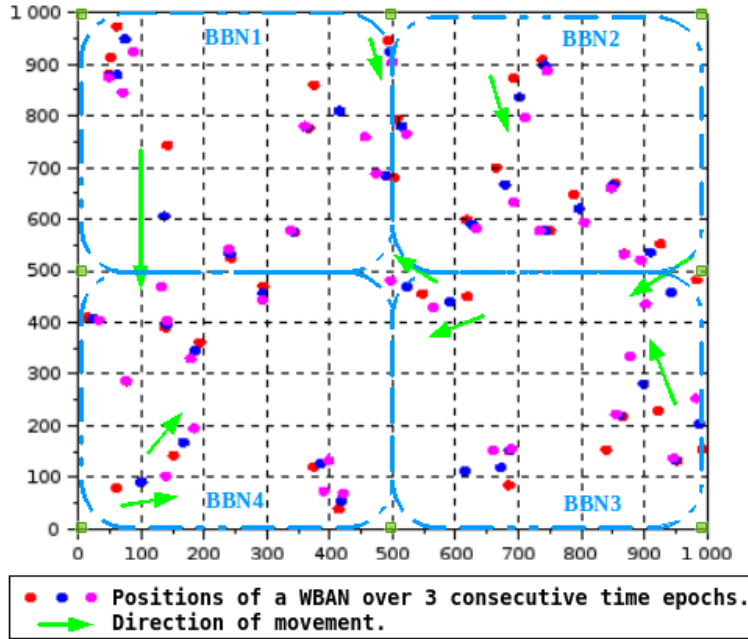


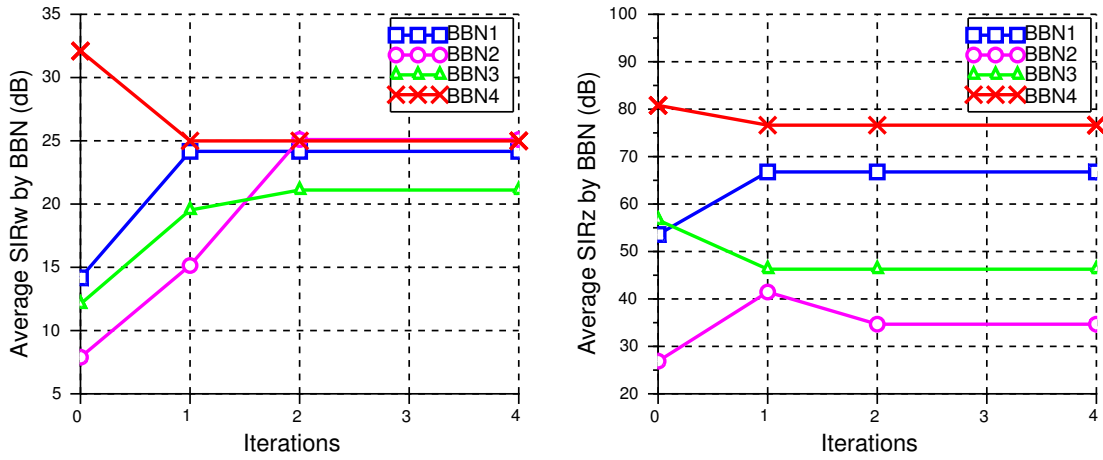
Figure 4.4: Simulation scenario for $N=40$ WBANs

indeed our original utility functions that are obtained after the computation of the WiFi and ZigBee Interference Functions.

4.5.1 BR-SIM versus SORT-SIM

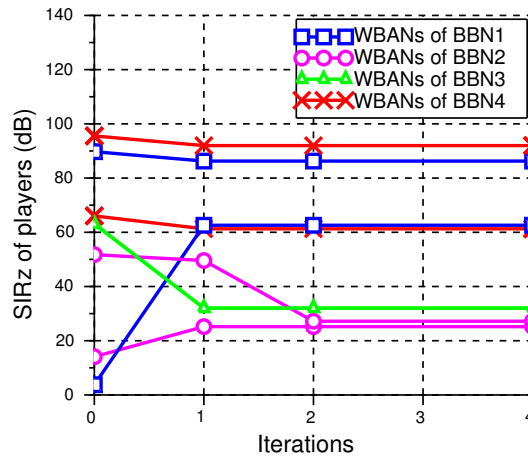
The curves on Fig.4.5 and Fig.4.6 illustrate, respectively, the dynamics of the BR-SIM algorithm for different BBN densities, namely for the number of WBANs $N=20$ and $N=40$. More specifically, Fig.4.5a and Fig.4.5b show the average WiFi SIR and ZigBee SIR, respectively, for $N=20$. Fig.4.5c further shows the convergence of the SIR at the ZigBee interface of a subset of players under the BR-SIM algorithm. Similarly, Fig.4.6a, Fig.4.6b and Fig.4.6c display, respectively, the evolution of the average SIR and the actual SIR values for a subset of players by each BBN, so as to show the effect of the network density on the convergence of the BR-SIM algorithm. As expected, increasing the BBN density results in increasing the network overall interference and the number of iterations to reach an equilibrium.

Besides, we notice at the Nash Equilibrium that the worst WiFi SIR (21 dB for $N=20$ and 9 dB for $N=40$), measured with the standard transmission power of 20 dBm (100 mW) is always above the receiver sensitivity of most commercial cards (the lowest receiver sensitivity for the Atheros chipset is -95 dB), even considering other effects like fading and thermal noise. The same conclusions are observed for the worst ZigBee SIR measured by all four BBNs (i.e., the WBAN that experiences the worst SIR in a BBN), which varies



(a) Average WiFi SIR.

(b) Average ZigBee SIR.



(c) SIRz of a subset of players.

Figure 4.5: Dynamics of the BR-SIM algorithm for each BBN, with $N=20$ WBANs

between 25 and 30 dB for $N=20$ and $N=40$ respectively. Note that the worst SIR measured at the ZigBee interface is higher than the value measured at the WiFi interface due to the restricted number of overlapping WiFi channels used in the simulation in order to enable mutual and cross-technology interferences, thus resulting in conflicting transmissions using the WiFi technology.

Naturally, within a BBN only WiFi transmissions coming from surrounding BBNs are considered in the computation of the WiFi interference, since we assume the utilization

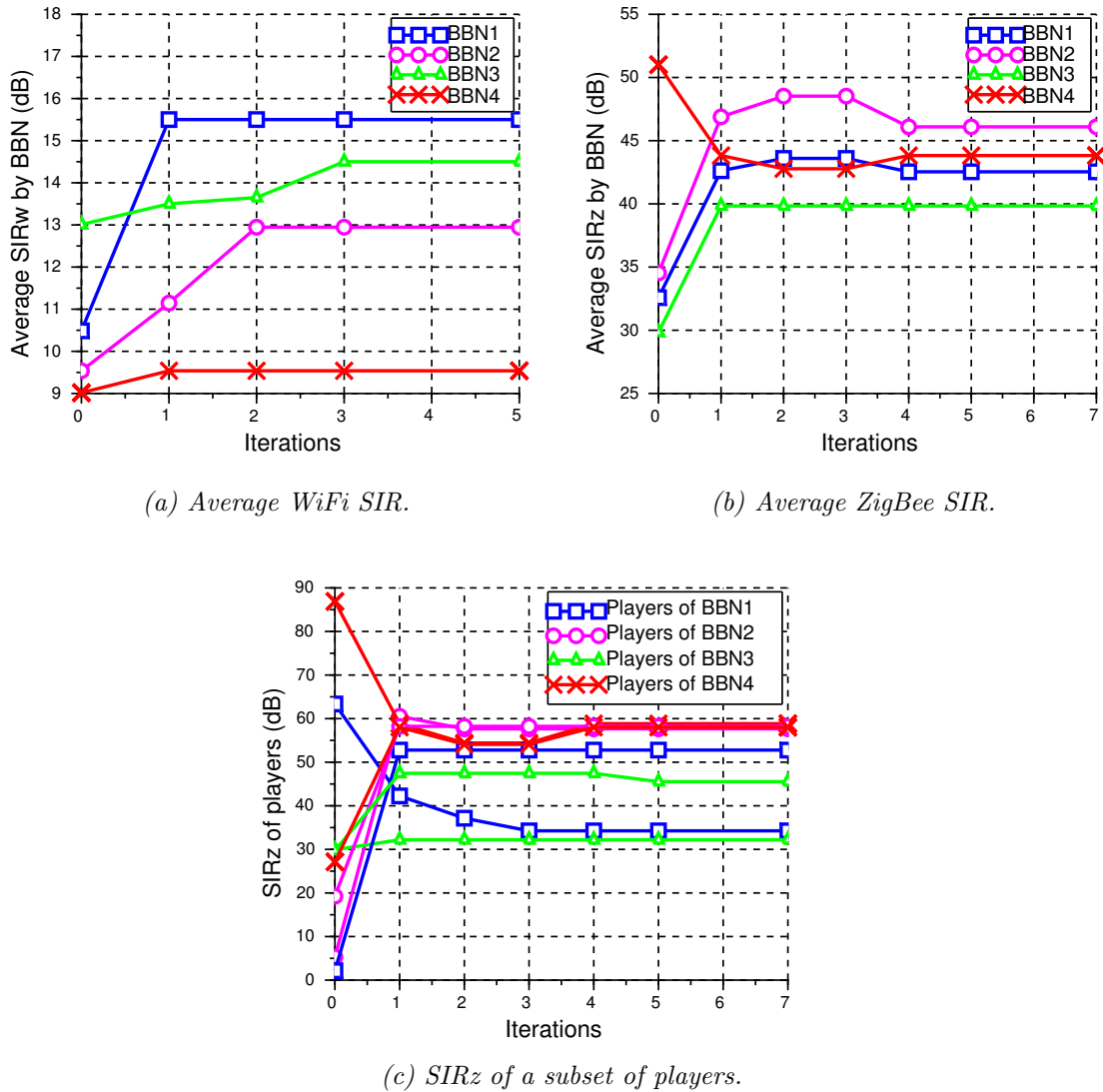


Figure 4.6: Dynamics of the BR-SIM algorithm for each BBN, with $N=40$ WBANs

of a coordination scheme for intra-BBN communications, whereas the ZigBee interface of any WBAN experiences both intra-BBN and inter-BBN interference. Thereby, further experiments with non-overlapping WiFi channels would reverse the previous conclusions and assess higher values of WiFi SIR versus ZigBee SIR.

Yet, the performance of BR-SIM is ensured since it provides a rather fair, socially-aware channel allocation, so that both WiFi and ZigBee signal-to-interference ratios tend to be quite close to a mean value at the Nash Equilibrium. Nevertheless, a noticeable decrease

in the range of SIR values (mainly SIRz), at the NE point, is observed when the density of the WBANs is high ($N=40$), and the SIR curves are tightly close. Indeed, higher densities occasion a more fair spreading of players over the neighboring BBNs, that will suffer from relatively fair interference environment. This explains why, for lower densities, the average SIR values for each BBN are spread out over a larger range of values.

On the other hand, Fig.4.7 and Fig.4.8 illustrate the signal-to-interference ratios at WiFi and ZigBee interfaces obtained by the SORT-SIM algorithm for the same topology configurations (i.e., $N=20$ and $N=40$). Almost the same conclusions can be made for SORT-SIM, as far as BR-SIM results, in terms of the evolution of SIR metrics as a function of WBANs density, wherein we can observe the degradation of both WiFi and ZigBee SIR values while increasing the BBN density. However, if we observe the average SIR of the whole network we can notice the main differences between the behaviour of the two algorithms. Indeed, Fig.4.9a and Fig.4.9b show a more accentuated steepness of SORT-SIM curves compared to that of BR-SIM, which means that the effectiveness of SORT-SIM is more density-sensitive, while BR-SIM seems to be more robust to density changes. In fact with higher densities, i.e., beyond $N=30$ players, SORT-SIM presents more severe degradation in SIR values for both WiFi and ZigBee transmission links, whereas BR-SIM shows a smooth decrease while preserving good SIR ratios.

Now, if we observe the performance of each algorithm separately, we notice rather similar behaviours at low densities (Fig.4.5 and Fig.4.7), where few players are spread out over the simulation area. Both algorithms compete in allocating feasible, near optimal, WiFi and ZigBee channels to all players. However, for high densities we notice that BR-SIM curves merge around the average SIR, while SORT-SIM still presents great divergences among players' SIR values. This can be explained by the usefulness of the cooperative component of BR-SIM, where the local interactions among neighbors allow it to fairly share the wireless resources. Whereas, SORT-SIM proceeds in a completely non-cooperative manner, thus some players get maximal SIR values, while others settle for channel allocations with minimal SIR values, just above the threshold.

Yet, the SIR values at both WiFi and ZigBee interfaces under the BR-SIM and SORT-SIM algorithms are illustrated in detail in Fig.4.10 and Fig.4.11, respectively. More specifically, these figures show the empirical Cumulative Distribution Function (CDF) of the SIR when the total number of WBANs $N=40$ and for a time duration of 300 s, which is divided in 30 time epochs of 10 s each. Let us first focus on the SIR metric for WiFi obtained with BR-SIM (Fig.4.10a) and SORT-SIM (Fig.4.11a). It can be observed that the SIR values under both algorithms are quite similar and range from 0 to ≈ 40 dB. However, it is not hard to see that BR-SIM guarantees for the majority of the players fair values of SIR (in the range $[10,25]$), while SORT-SIM performs WiFi channel assignment to transmission links in a much more aggressive way, where some players enjoy high values of SIR while others suffer from very low values. Similarly, for the SIR value measured at the ZigBee interface, Fig.4.10b and 4.11b show that in more than 50% of the scenarios, the SIR is higher than approximately 50 dB. However, note that in the case of SORT-SIM and for the 6 considered

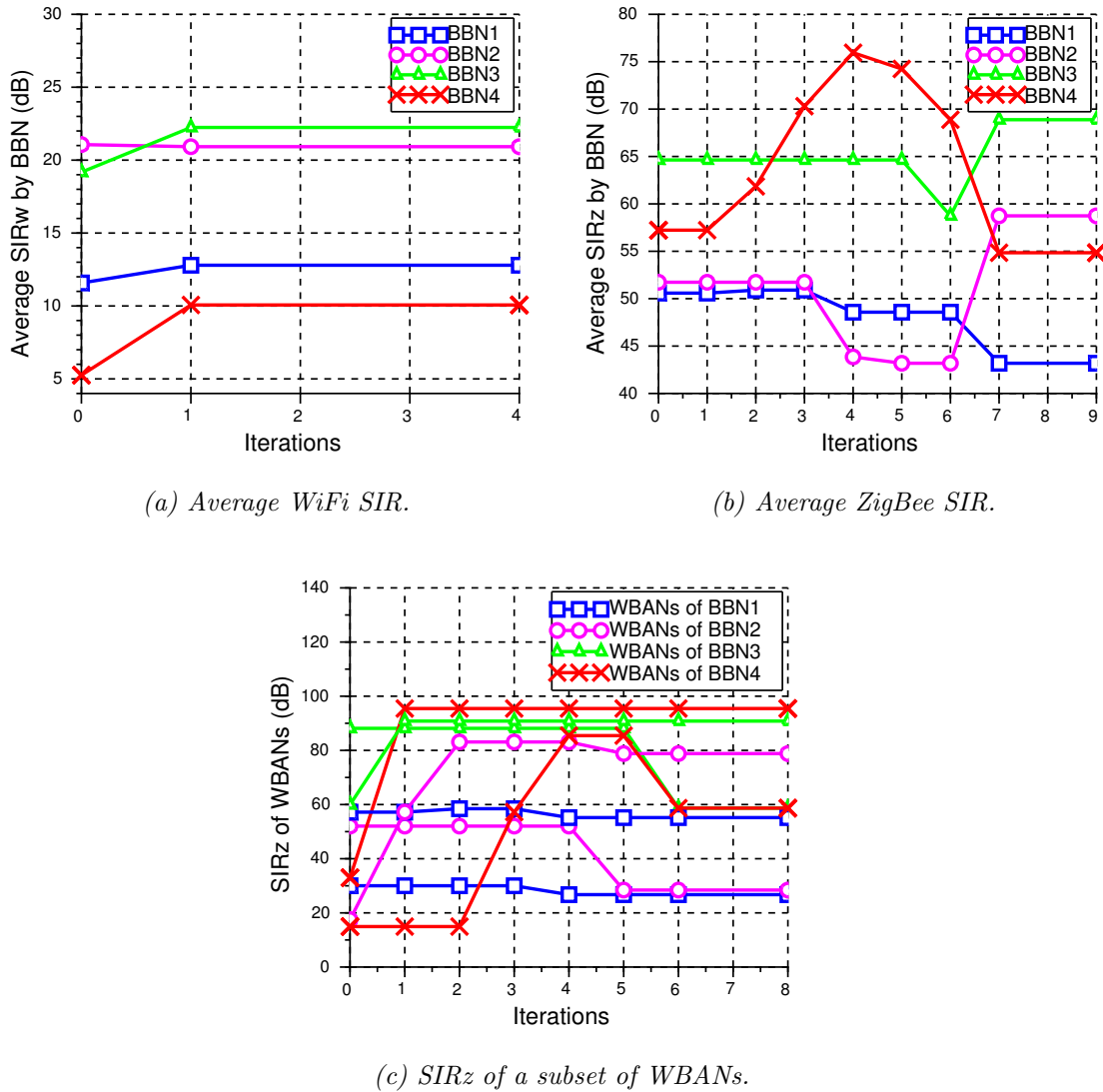
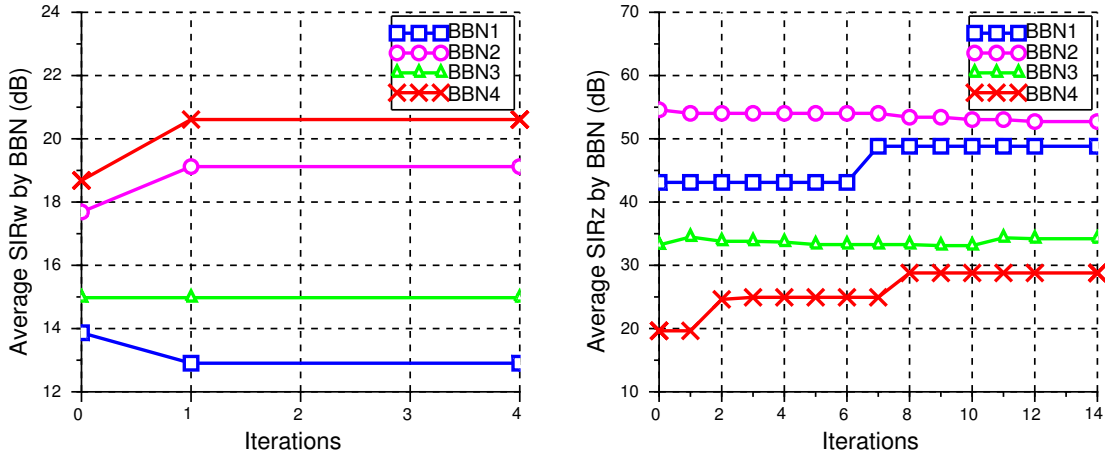


Figure 4.7: Iterations of the SORT-SIM algorithm for each BBN, with $N=20$ WBANs

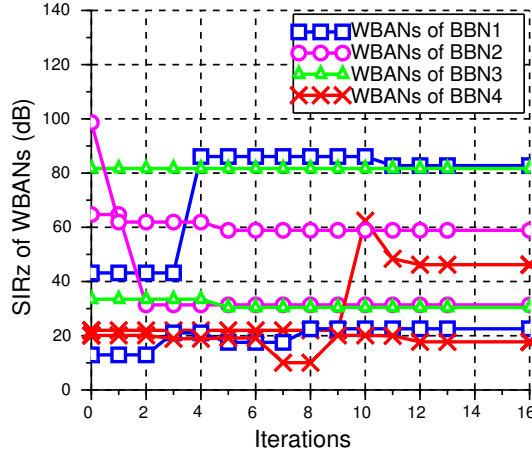
WBANs the percentage of players getting a value of SIR below 20 dB is larger than the one obtained with BR-SIM. Hence, this trend confirms the fact that BR-SIM guarantees at the same time some fairness along players and good performance.

Besides, we calculate with Scilab the computation time (CPU time) for both algorithms and we find noticeable difference between them. Indeed, the BR-SIM computation time is about four times larger than that of the SORT-SIM execution instance. For example, the maximum computation time we measured to solve the BR-SIM algorithm over 30 consecu-



(a) Average WiFi SIR.

(b) Average ZigBee SIR.



(c) SIRz of a subset of WBANs.

Figure 4.8: Iterations of the SORT-SIM algorithm for each BBN, with $N=40$ WBANs

tive time epochs was approximately equal to 1060 seconds, for $N=50$ WBANs. Conversely, SORT-SIM takes less than 228 seconds to find the sub-optimal solutions for the SIM problem, under the same network instances and parameters' settings. Furthermore, it can be observed that the BR-SIM algorithm converges to a stable operational point in few iterations, in particular, all BBNs converge to their best WiFi and ZigBee channel allocations in at most 3 and 5 iterations, respectively, while SORT-SIM performs with greater number of iterations (up to 15), but within less computation time.

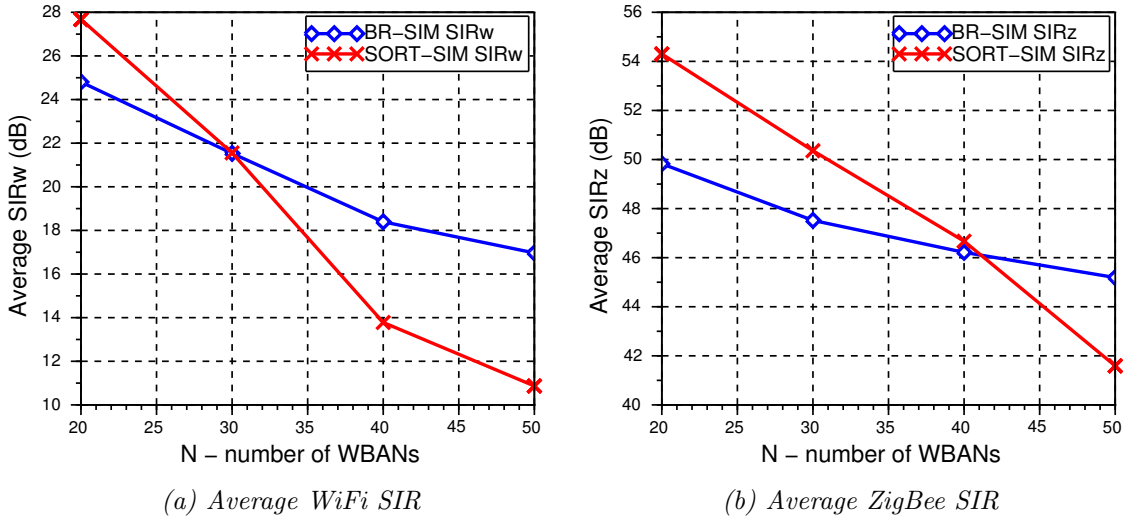


Figure 4.9: BR-SIM v.s SORT-SIM - Average SIR function of density

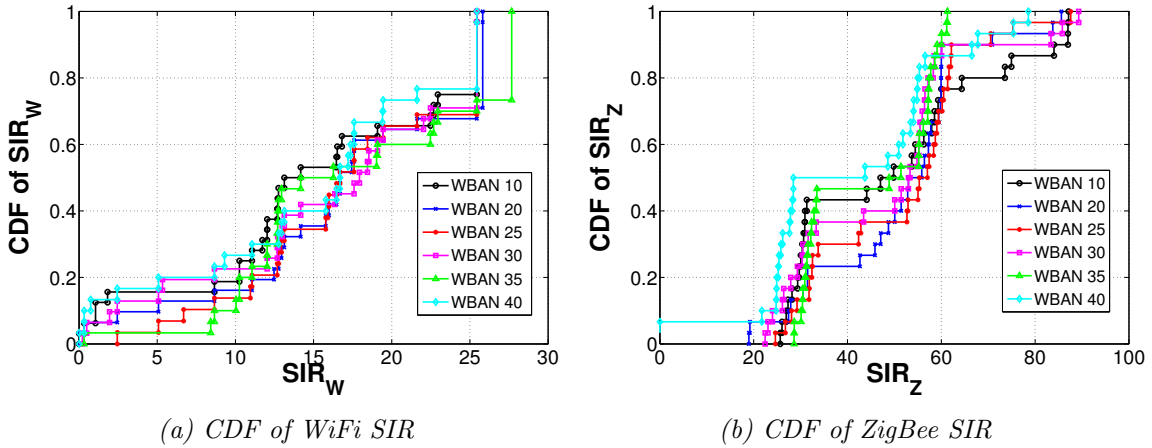


Figure 4.10: BR-SIM: Empirical Cumulative Distribution Function (CDF) of the SIR measured at WiFi and ZigBee interface of all WBANs in the BBN scenario of 40 WBANs with 30 time epochs of 10 s each.

Finally, BR-SIM outperforms in terms of fairness and robustness the SORT-SIM algorithm, especially at higher densities, thus representing a practical solution for interference mitigation in realistic BBN scenarios. However, SORT-SIM presents simplicity and rapidity benefits which makes it useful, under specific BBN scenarios, mainly at low densities and low QoS requirements.

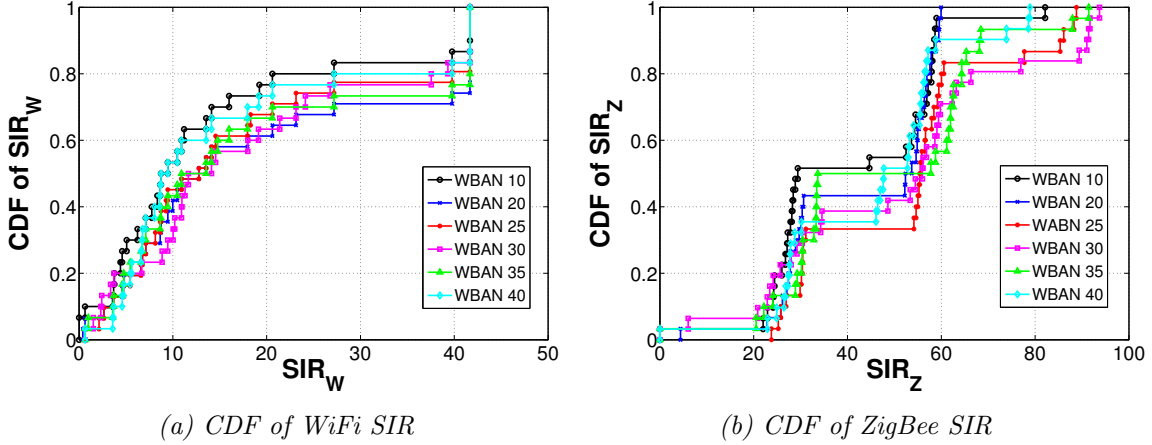


Figure 4.11: SORT-SIM: Empirical Cumulative Distribution Function of the SIR measured at WiFi and ZigBee interface of all WBANs in the BBN scenario of 40 WBANs with 30 time epochs of 10 s each.

4.5.2 Comparison with power control approaches

In this section, we compare our BR-SIM and SORT-SIM algorithms to the distributed power control algorithm proposed in [42] and to the joint relay selection and transmit power control algorithm proposed in [3].

Authors of [42] formulated a power control game considering interference between neighboring WBANs and energy-efficiency. They derived a distributed power control algorithm, called the ProActive Power Update algorithm (PAPU), to reach a unique Nash Equilibrium (NE) representing the best tradeoff between energy-efficiency and network utility. As in our model, PAPU assumes a TDMA-based MAC protocol to deal with intra-WBAN interference avoidance, and uses the SINR metric to define the utility function of the power control game. However, neither WBAN mobility is considered, nor wireless technologies are specified. Alike our SIR metrics defined by expressions (3.5) and (3.23), respectively, for WiFi and ZigBee received signals, the SINR was defined in [42] without consideration of heterogeneous wireless technologies. This will be reflected in the final SINR values, as we will show hereafter.

Indeed, we have implemented the PAPU algorithm with the same network configuration of our BR-SIM and SORT-SIM algorithms, and with the following definition of the power best-response performed by each WBAN/player:

$$b_i(p_{-i}) = \frac{1}{c_i} - \frac{\sum_{j \neq i} h_{ji} p_j + n_0}{h_{ii}} \quad (4.5)$$

where p_j is the transmission power of player j , h_{ji} represents the channel gain between transmitter j and receiver i , h_{ii} the intra-network gain, n_0 is the background white noise power (which is ignored in our simulations since we calculate the SIR), and c_i the power

price. The obtained (average) SIR values are reported in Fig.4.12 and Fig.4.14.

First, it can be observed from Fig.4.12 that PAPU is rather efficient with respect to WiFi SIR maximization; results are almost in the same range as the BR-SIM and SORT-SIM algorithms. This can be explained by the fact that PAPU's WiFi SIR does not consider the cross-technology interference from ZigBee on WiFi links. Only intra-WBAN channel gains are involved, whereas in real BBN scenarios the cross-technology channel gains introduce further interference components to the SIR denominator.

However, the difference mainly appears in the second-stage game (Fig.4.14b), where PAPU provides less efficient SIR values for the ZigBee signal. Whilst BR-SIM and SORT-SIM provide ZigBee SIR values over 20dB (up to 80dB), PAPU's maximum ZigBee SIR is around 20dB (up to 40dB for lower network densities). Yet, as its authors explained, PAPU requires limited information exchange between WBANs, and as a consequence the player strategy is purely selfish, without any consideration of neighboring WBANs' utilities. With local interactions of our SIM game, BR-SIM and SORT-SIM achieve better SIR values, and thus stronger wireless signal. This also explains the regularity of PAPU curves, whereas the negotiations among players are better observed on the BR-SIM and SORT-SIM curves. It is worth noting that the reduced number of iterations of the PAPU algorithm within our network configuration, compared to that of the original paper, is also due to the local interaction behavior among players, which allows a rapid convergence to the NE.

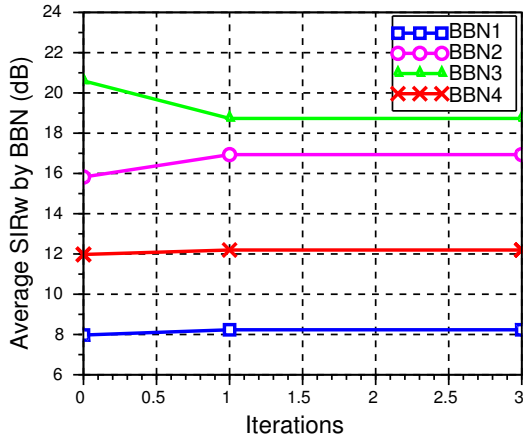
We now compare BR-SIM and SORT-SIM to the joint Relay Selection and transmit Power Control (RSPC) algorithm, proposed in [3].

In [3], each WBAN has the following configuration (see Fig.4.13): a hub at the chest, two relays at the right and left hips, and three sensors at other suitable locations. The hub, the sensor and the two relays are denoted as H , S , R_1 and R_2 , respectively. Time division multiple access (TDMA) and asynchronous TDMA are respectively used as intra- and inter-WBAN access schemes, since it has been shown in [88] that they provide better interference mitigation than other access schemes in terms of power consumption and channel quality.

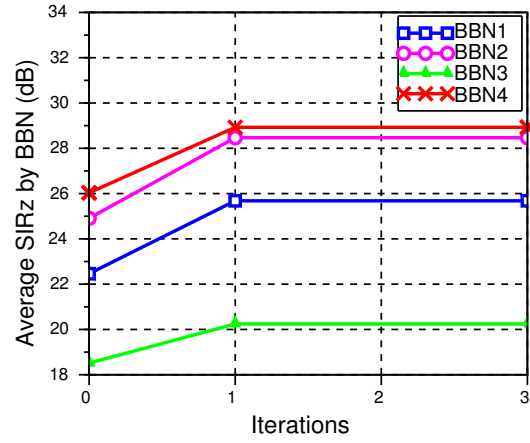
The major contribution of the RSPC algorithm is the use of opportunistic relaying with no cooperation between WBANs to provide inter-body channel gain measurements, in order to improve reliability (decrease the outage probability) and reduce the power consumption. RSPC uses the on-body and inter-body channel data sets in [89], obtained through exhaustive scenarios performed in realistic environments, over several hours of normal everyday activities. In each experiment, sensors transmit in a round-robin fashion with 5 ms separation between each other.

Thereby, the RSPC algorithm can be summarized in the three following steps:

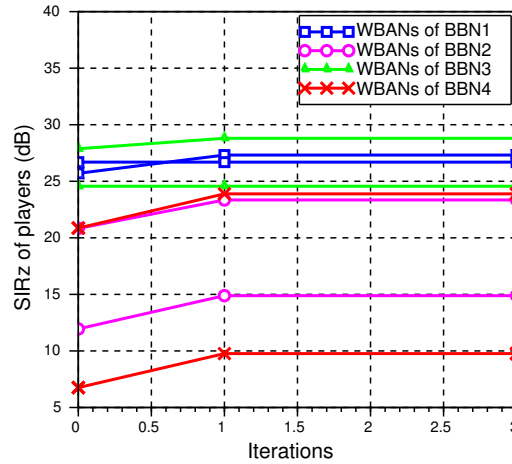
1. Power control at the sensor level: the sensor performs power control on a channel at time epoch τ using the value at time epoch $\tau - 1$, and selects the one-hop relay: StoH (Sensor-to-Hub), StoR1 (Sensor-to-Relay1) or StoR2 (Sensor-to-Relay2).
2. Power control at the relay level: select the relay transmit power to the hub, in the transmit range.



(a) Average WiFi SIR.



(b) Average ZigBee SIR.



(c) SIRz of a subset of WBANs.

Figure 4.12: Dynamics of the PAPU algorithm for each BBN, with $N=40$ WBANs

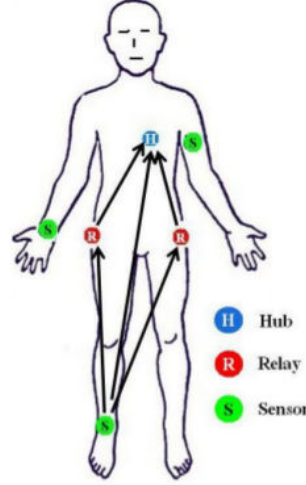


Figure 4.13: WBAN configuration for the RSPC algorithm [3].

3. Branch selection at the hub: the hub selects the path (StoH, StoR1-R1toH or StoR2-R2toH) that gives the best SINR.

The authors of [3] assert that relay-assisted communications can reduce co-channel interference from neighboring WBANs, by increasing the SINR of the packets transmitted by the sensor node and received at the WBAN coordinator (the hub/the MT in our model), expressed by:

$$SINR = \frac{T_x \times |h_{TxRx}|^2}{\sum T_{x_{int,i}} |h_{int,i}|^2} \quad (4.6)$$

where T_x is the sensor/relay transmit power obtained by the Power Control function (step 1 or 2 of the RSPC algorithm). $|h_{TxRx}|$ represents the average channel gain across the duration of the sensor/relay transmitted signal, while $|h_{int,i}|$ is the channel gain between the interferer int , which is the neighboring WBAN sensor, and the sensor or selected relay i . Finally, $T_{x_{int,i}}$ denotes the interfering power of neighboring WBAN sensor int to the sensor/relay i . The instantaneous noise at the receiving node has been omitted, since we compare SIR metrics.

For the one-hop relay selection, we consider the WBAN configuration given in Fig.4.13. Since TDMA is used as access scheme, sensors cannot transmit simultaneously within a WBAN. Yet, to adapt the RSPC algorithm to our network model, we focus on a WBAN's sensor-of-interest, and we assimilate the neighboring interferer sensor to its corresponding MT. The one-hop relay process will be considered while selecting the intra-WBAN transmit power, i.e. in the ZigBee stage. We further assume that WBANs use a WiFi channel for inter-WBAN exchanges. Power control will also be performed for WiFi transmissions in a

way to maximize the MT WiFi SIR, using the ZigBee power vectors of neighboring WBANs, computed at the previous time epoch.

We run our simulations and we calculate the WBAN's SIR (SIR_w and SIR_z), considering the aggregate interference due to transmit powers of the neighboring WBANs.

It can be observed from Fig. 4.14a that, in general, the RSPC WiFi SIR curve lies between BR-SIM and SORT-SIM curves. Even though RSPC does not perform iterations to reach the best SIR, unlike the game models, it optimizes once the sensor/relay transmit power with its Power Control algorithm and achieves rather efficient SIR values. These

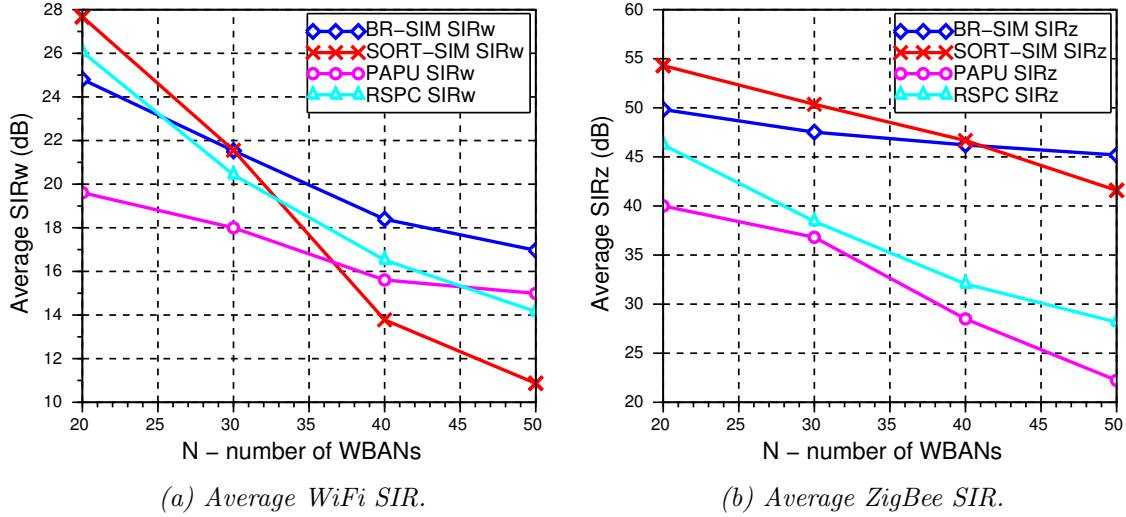


Figure 4.14: BR-SIM and SORT-SIM vs PAPU and RSPC. Average WiFi and ZigBee SIR as a function of network density.

results can be explained by analyzing, as we do hereafter in Fig. 4.15, the aggregate interference, calculated as the sum of interference suffered by the hub/MT, due to WiFi and ZigBee transmissions of neighboring WBANs.

In Fig. 4.15, we notice an important gap between the RSPC aggregate interference and the one obtained by our algorithms (BR-SIM and SORT-SIM) and PAPU. Specifically, IN_{BR-SIM} and $IN_{SORT-SIM}$ are always lower than those of PAPU and RSPC, even though sometimes the WiFi SIR of RSPC is higher than the one achieved by BR-SIM or SORT-SIM (Fig. 4.14a). This can be explained as follows:

- The aggregate interference values of the BR-SIM and SORT-SIM algorithms are considerably lower than those of PAPU and RSPC, because in our interference mitigation model we assign WiFi/ZigBee channels to wireless links in a way to reduce the co-channel and cross-interference components. Therefore, neighboring interfering

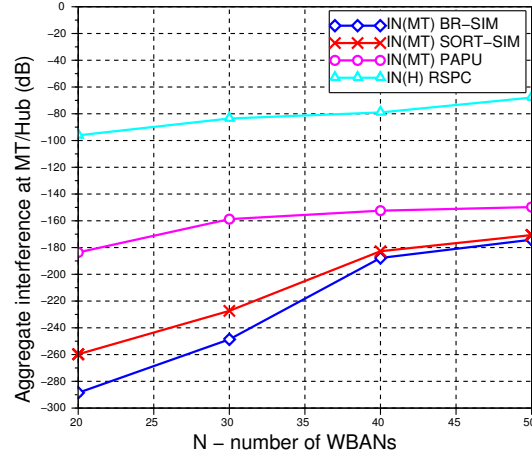


Figure 4.15: Aggregate interference at the Hub/MT.

WiFi/ZigBee links are omitted (by allocating them orthogonal channels) or reduced by the w_{mn} scalar, to ensure minimum mutual interference.

- The gap is less important for the SIR values, because the MT/Hub channel gains and transmit powers are far larger than the interference component in the four algorithms, either with power control (PAPU and RSPC), or with constant transmit power (BR-SIM and SORT-SIM). Indeed, the four algorithms achieve efficient interference mitigation, ensuring feasible SIR values. However, the advantage of BR-SIM and SORT-SIM mainly appears when we compare the aggregate interference (Fig. 4.15) and the ZigBee SIR (Fig. 4.14b). This can be explained by the fact that our algorithms give some privilege to ZigBee links w.r.t. WiFi links; WiFi interference on ZigBee links is considered more crucial than ZigBee interference on WiFi links. In other words, our algorithms make sure that WiFi links (which use a transmit power 100 times higher than that of ZigBee) will not prevent ZigBee transmissions and deteriorate the BBN system performance.

Although the aggregate interference $IN(MT)$ of BR-SIM and SORT-SIM is significantly lower than that of RSPC $IN(H)$, it increases more rapidly for higher densities, because the use of orthogonal channels is no more possible, and BR-SIM and SORT-SIM start using channels with minimum mutual interference, with constant WiFi and ZigBee powers. However, RSPC maintains approximately the same level of interference by adjusting the transmit power of the sensor/relay nodes. Hence, it would be interesting in future work to consider a control power mechanism together with the channel assignment to further improve the efficiency of the SIM game.

4.6 Conclusion

In this chapter we evaluated and compared our SIM game theoretical approaches to relay-assisted power control schemes (i.e., PAPU and RSPC) in realistic BBN scenarios. We first showed that the BR-SIM algorithm converges quickly and achieves feasible values for the utility functions, while SORT-SIM presents some practicability benefits under specific network scenarios. Then, we demonstrated that BR-SIM and SORT-SIM outperform PAPU and RSPC in terms of SIR and Aggregate Interference in several cases, and especially when the network density is quite low.

Chapter 5

Inter-WBAN Routing Protocol for Epidemic Control in Mass Gathering Areas using Body-to-Body Networks

Contents

5.1	Introduction	78
5.2	State of the Art	79
5.3	BBN-based Epidemic System models	82
5.3.1	SEIR Epidemic spread model	82
5.3.2	BBN Epidemic control model	84
5.4	Epidemic threshold-based BBN routing protocol	84
5.4.1	Epidemic threshold	85
5.4.2	BB-LAR: Location-Aided BBN Routing	86
5.4.3	BBN Route selector	88
5.4.4	Human trajectory tracing - WBAN selfish strategy	88
5.4.5	Epidemic source tracing - Authority quarantine strategy	89
5.5	Performance Evaluation	89
5.5.1	Performance analysis of BB-LAR	89
5.5.2	Comparison of BB-LAR with other geographic-based routing protocols	92
5.6	Conclusion	96

5.1 Introduction

The penetration of BBN solutions for monitoring and remote control in a wide range of markets, generates great social benefits. Especially, the BBN technology paves the way for new possibilities of ubiquitous health applications.

In this context, we will consider the scenario of preventing epidemic spread in mass gathering areas. We consider the airport indoor environment, in order to ensure public safety and prevent the insurgence of pandemics inside the local population as well as the epidemic diffusion due to the migration of people across the countries.

Indeed, recent studies name 40 airports most likely to spread diseases (Fig.5.1). Researchers used real traveler patterns, geographical information and airport waiting times to find out that these airports are disease-spread hot spots, and even the most likely to facilitate the diffusion of a major pandemic from its origin. Some of those findings are reported in [4, 90].



Figure 5.1: Air traffic connections from West African countries to the rest of the world: the international spreading risk associated with the 2014 West African Ebola Outbreak [4]

Yet, a lot of epidemic models have been developed and analyzed, and mathematical modeling of infectious disease spreading has been extensively studied for a long time. Nev-

ertheless, these approaches suffer from their inability to gather health data and social contact information simultaneously, namely in dynamic scenarios where the assumptions about human motions and social contacts are barely efficient. Indeed, these models process offline treatments, using medical surveys or medical records, while the epidemic keeps spreading continuously in time which makes the control policies harmfully time-delayed.

The above issues stress the imperative need for developing novel approaches that deal with the epidemic control problem more efficiently, to successfully avert adverse outcomes. The weaknesses of traditional approaches place BBN systems on the spotlight of attention, due to their ability to ensure real-time health data sensing and support dynamic networks so that to control the face-to-face contact when mobile people can enter and leave the network randomly. Moreover, real-time interactions among cooperative WBANs may allow each person to choose an instant selfish strategy to ensure auto-preventive actions, even before the quarantine strategies are taken by the BBN authorities.

Another issue that our work focuses on is the inter-WBAN routing of the aggregated epidemic data. Then, our epidemic control model relies primarily on an inter-WBAN routing protocol which represents the skeleton of our model.

Investigating routing issues goes parallel with energy efficiency, QoS and mobility considerations. Indeed, the information stream consists of short packets of data that are passed from person to person and routed to the destination WBAN (or remote server). The other WBANs in the BBN all contribute a little of their energy and bandwidth to relay the packets. A BBN like any sensor network suffers limited energy resources, hence preserving the energy of the nodes is of great importance. In addition, in a BBN scenario, network topology changes frequently especially when the WBAN user keeps encountering other WBAN users. Then, the quality of the links between the WBANs keeps changing frequently due to the moving nature of the body, hence the ability to foresee the mobility of the WBANs is crucial. All these issues are taken into account in this chapter which is organized in the following manner. In section II, we discuss the existing works. In section III, we present the epidemic spread and control models. In section IV, we introduce our epidemic threshold-based BBN routing protocol which we evaluate in section V through targeted simulations. Finally, section VI concludes the chapter.

5.2 State of the Art

Few recent works [23, 24, 25] are worthy of mention, as they have already focused on the epidemic control solutions using WBANs.

In [23], authors show up the inconvenience of the existing information systems for epidemic control. Based on delayed reports of epidemic cases provided by hospitals and doctors, they are unable to give timely and precise estimations of epidemic situations. Yet, the authors introduce the use of *Social Networks* in their information system for Epidemic control, called EPIC, to accurately describe social interactions between individuals in a

community infected by a pandemic. Prediction algorithms are developed to model health conditions and social interactions of individuals, which allows to predict how epidemic diseases spread in a community. EPIC algorithm is based on the fusion of collected health information from WBANs and social information from social networks, and it articulates around three steps: i) data collection from WBANs and social networks, ii) data interpretation and information fusion, and iii) epidemic prediction by authorities. Even it provides timely and accurate predictions, this algorithm does not consider traffic classes, so that to transmit sensor data with priorities relative to the individuals' health status. On the other hand, EPIC algorithm doesn't not share the epidemic information among the community, only authorities take quarantine strategies, whereas susceptible individuals ignore the epidemic threats around them.

The same authors implemented, then in [24], an Epidemic Source Tracing Algorithm which integrates WBANs technology for body vital signs collection with mobile phones for social interaction sensing. Based on the SIR (Susceptible, Infected, Recovered) epidemic model, the epidemic source tracing used genetic algorithm based search and dominating set identification algorithms to achieve epidemic source identification and inhibit epidemic spread. In some pandemics there exist an intermediate status between the susceptible and the infected status, where the individual catches the disease and stay in latent period, he is said to be infected but not infectious, i.e., not transmitting the infection yet. If we consider a timely epidemic control model, it would be interesting to consider the intermediate state, in order to anticipate the quarantine strategy, before reaching the infected status. Indeed, in our work, we consider this intermediate status, called the Exposure status.

Furthermore, the epidemic control in distributed systems such as BBNs, needs the participation of all network nodes in order to achieve timely and accurate epidemic detection, where no central coordinator is monitoring the network. Yet, a routing protocol is required to ensure epidemic information exchange among the network nodes, equipped with WBANs. Actually, not many research works have focused on inter-WBAN communications and routing. Some of them are discussed hereafter.

In order to increase the lifetime of the WBAN network, Ali et al. in [59] used an energy-efficient secure cluster formation technique for inter-WBAN communication, based on the residual energy of the Personal Server (the sink node) and the distance between two communicating WBANs. Ali et al. also stated that securing intra-WBAN and inter-WBAN communications means securing the human lives since such communications involve the human personal data. Hence, clustering is further made secure by using a preloading-based lightweight key management scheme. By clustering, more powerful sensors act as Cluster Heads (CH) while other sensors are Cluster Members (CM). Modeling inter-WBAN communications as a hierarchical structure has the advantage of local data processing, which reduces the network overhead and provides a scalable solution.

Again, to enable inter-WBAN communications, Mittal et al. in [57] implemented the network clustering SCAN (Structural Clustering Algorithm for Networks), proposed in [91], which detects meaningful clusters and helps in the delimitation of communities in large

social networks, so that for example, two people who share many friends would be clustered in the same community. According to IEEE 802.15 TG6 [92], the standard task group of WBAN, it is required that the WBAN protocol should support at least the sensor density of 60 sensors in a 63 m³ space. Such BBN density gives rise to a high probability of mutual interference. Then, Mittal et al. also proposed an inter-WBAN scheduling (IWS) that rapidly detects and responds to every inter-WBAN interaction and allow an optimal channel-utilization reuse.

Another concern for epidemic data aggregation and routing is the BBN topology which is subject to random changes due to WBANs' mobility. The work in [54] presents a comprehensive configurable mobility model (MoBAN) for evaluating intra and extra-WBAN communication. It implements different postures as well as individual node mobility within a particular posture. The selected posture also determines the local movement of sensor nodes and the global mobility of the whole WBAN. Therefore, it affects the connection between the nodes in the WBAN and the external network like other WBANs or the surrounding ambient sensor network. The advantage of MoBAN is that it considers both intra and extra-WBAN mobility, and is able to provide mobility information for both scenarios.

In another work [55], a distributed Prediction-based Secure and Reliable routing framework (PSR) was proposed for emerging WBANs. It is observed that body sensors may exhibit regular mobility when a user's physical activity (e.g., swimming and jogging) contains repeated motions, and as a result, link quality and a sensor's neighbor set often present periodic changes. Using this model, the sensor node predicts the quality of its incidental links as well as the change of its neighbor set.

Ben Arbia et al. [93] investigated the inter-WBAN routing in an urban critical and emergency scenario, where a BBN is considered as an extension or "add-on" to existing Public Safety Networks (PSNs), in order to enhance QoS and ensure ubiquitous coverage during and after a disaster. Hence, routing protocols were evaluated with different communication technologies (i.e., WiFi IEEE 802.11; ZigBee IEEE 802.15.4; WBAN IEEE 802.15.6). A mobility model was also generated by a simulation tool to serve as a realistic environment for the evaluation of various classes of routing protocols. The Optimized Link State Routing protocol version 2 (OLSRv2) [27], Ad-hoc On-Demand Distance Vector (AODVv2) [26], Directed Diffusion and Greedy Perimeter Stateless Routing (GPSR) [94] protocols were then selected from proactive, reactive, gradient-based and geographical-based routing classes, respectively. It has been proved that, in addition to energy inefficiency and bandwidth overload, the drawbacks of proactive routing protocols in PSNs is also the routing delay caused by the routes discovery broadcasts which corrupts the network performance in emergency situations. On the other hand, reactive routing protocols solve the bandwidth and energy issues using on-demand routing request, i.e., the route discovery procedure is invoked when it is needed, but the delay caused by the route discovery before data transfer is still compromising for PSN's requirements. Whence, hybrid routing protocols class, merging both reactive and proactive routing techniques, seems to aggregate the usefulness of both. Then, proactive routing could be applied for nearby nodes and reactive routing for faraway

nodes. Besides, geographical location based routing protocols could avoid the technique of storing and sharing the network topology information, since nodes store only physically reachable nodes, i.e., routing decisions are made hop-by-hop, no end-to-end. Then, the authors concluded that geographic routing protocols could be a considerable candidate for BBNs.

Yet, to the best of our knowledge, this work is the first to propose a location-based routing for BBNs, in order to ensure real-time epidemic control within a limited area. Our routing protocol is based on an epidemic spread model that specifies the different stages of the pandemic evolution. The epidemic control is then ensured by the epidemic message exchange among WBANs and with the authority's wireless infrastructure, so that each WBAN informs the network of his health status in order to facilitate the quarantine strategy.

5.3 BBN-based Epidemic System models

In this section we present, first, the epidemic spread model, which specifies the epidemic metrics used thereafter by the routing protocol to ensure epidemic control in the BBN environment. Then we present the epidemic control model, which consists in a two-level control architecture, in order to ensure both self-control by WBANs themselves, and quarantine actions by authorities.

5.3.1 SEIR Epidemic spread model

The establishment and spread of infectious diseases is a complex phenomenon with many interacting factors. For example, the *epidemiology compartmental models* serve as a mathematical framework for understanding the complex dynamics of these systems, by abstracting the population into compartments under certain assumptions, which represent their health status with respect to the epidemic specific features. These compartments, in the simplest case, can stratify the population into two health states: susceptible to the infection (often denoted by S); and infected by the pathogen (given the symbol I).

In this work we consider a dynamic system where individuals can enter and leave the network with different rates and we intermediate in real-time preventing the contact with the infectious individuals, and in providing rapid quarantine strategies based on real-time health information exchanged between cooperative WBANs and with the medical staff, as explained later in 5.3.2.

In our scenario, in order to ensure a real-time detection of the epidemic outbreak during the incubation period of the disease, we should consider the *Exposure* state, where the infected individuals should be quarantined as rapidly as before reaching the infectious stage. We divide the operating time of the whole system into a set \mathcal{T} of consecutive epochs. Thus,

we model the epidemic spread evolution in the airport indoor environment as the (Susceptible, Exposed, Infectious, Recovered) (SEIR) compartmental model [95, 96], represented by Figure 5.2.

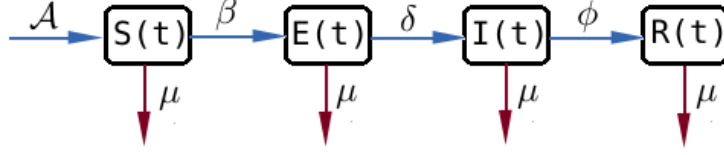


Figure 5.2: SEIR model flow

$S(t)$ is used to represent the number of individuals not yet infected with the disease at time $t \in \mathcal{T}$, or those susceptible to the disease. $E(t)$ represents the Exposed individuals in the latent period, during which the individual is said to be infected but not infectious. $I(t)$ denotes the number of individuals who have been infected with the disease and are capable of spreading the disease to those in the susceptible category. $R(t)$ is the compartment used for those individuals who have been infected and then removed from the observed area, either due to immunization or due to death; in our scenario the recovered status corresponds to the quarantined individuals who are just discarded from the airport zone. \mathcal{A} represents the average arrival rate, β the contact rate between susceptible and infectious individuals, δ the average transition rate from the exposed to the infectious status, $\frac{1}{\delta}$ denotes then the average latent period. Accordingly, $\frac{1}{\phi}$ models the average infectious period, and μ the average departure rate.

The mathematical framework of SEIR model has been thoroughly investigated in the literature [95, 97, 98], through differential equations derived from the fundamental equation:

$$S(t) + E(t) + I(t) + R(t) = N(t) \quad (5.1)$$

Where the population $N(t)$ is considered constant because of the rough assumption that arrival and departure rates are equal, whereas in realistic scenarios, $N(t)$ is variable. Yet, the differential equations derived from Equation (5.1) barely represent the realistic epidemic spread scenario of SEIR model. Accordingly, we do not rely on the mathematical model proposed in the literature, instead we propose an epidemic-threshold-based routing protocol that aims at routing packets using an epidemic-based metric which consists of the following epidemic components:

$$\beta S(t)I(t), \quad \forall t \in \mathcal{T} \quad (5.2)$$

$$\delta E(t), \quad \forall t \in \mathcal{T} \quad (5.3)$$

$$\mu(E(t) + I(t)), \quad \forall t \in \mathcal{T} \quad (5.4)$$

The goal is to guarantee a low epidemic spread of the disease. Then, expression (5.2) aims to minimize the contact between Susceptible WBANs and Infected WBANs in order to reduce the contact rate and the epidemic spread in the indoor airport zone. Expression (5.3) will anticipate the translation of the incubator WBANs to the Infectious stage, by quarantine strategies during the latent period. Finally, Expression (5.4) helps in preventing the diffusion of the disease to the external population, so that individuals who already show symptoms, either in latent period or in infectious stage, should be tracked and quarantined before leaving the airport control zone.

5.3.2 BBN Epidemic control model

To ensure an efficient epidemic control under the considered SEIR model, we propose a two-level system architecture (illustrated in Fig. 5.3), based on a dynamic BBN network and a Wireless Network infrastructure:

- BBN-level control: The real-time interactions between WBANs within the airport indoor BBN play an important role in the self-prevention phase, where each WBAN will be able to i) sense health status of his neighboring WBANs and broadcast his own health status, ii) participate in the diffusion of the epidemic alerts to the BBN nodes to allow them to take self-prevention measures, and iii) use the collected health status of the network to trace his own trajectory while avoiding the hazardous zones, using an indoor localization application [99], to get accurate positions of the infected individuals carrying mobile terminals. In our SEIR model, the BBN level performs the optimization of the expression (5.2), guaranteeing a minimum level of infection.
- Authority-level control: The existing wireless infrastructure is provided for the authority staff, to collect sensor data from the mobile terminals (smartphones) carried by the WBANs within the indoor airport zone, using WiFi links, and process real-time analysis to detect Exposure (E) and Infectious (I) subjects. The principal role of the wireless access points (APs) is to provide specific health data transmitted by the mobile terminals, coupled with localization information to help the authorities in epidemic source tracing and quarantine strategies. The authority level is then responsible of the optimization of expressions (5.3) and (5.4).

5.4 Epidemic threshold-based BBN routing protocol

This section presents the different modules of our epidemic control mechanism. First, the *epidemic threshold* metric is introduced, upon which the epidemic data routing is based. Then, the proposed geographic routing protocol is detailed, especially the message exchange

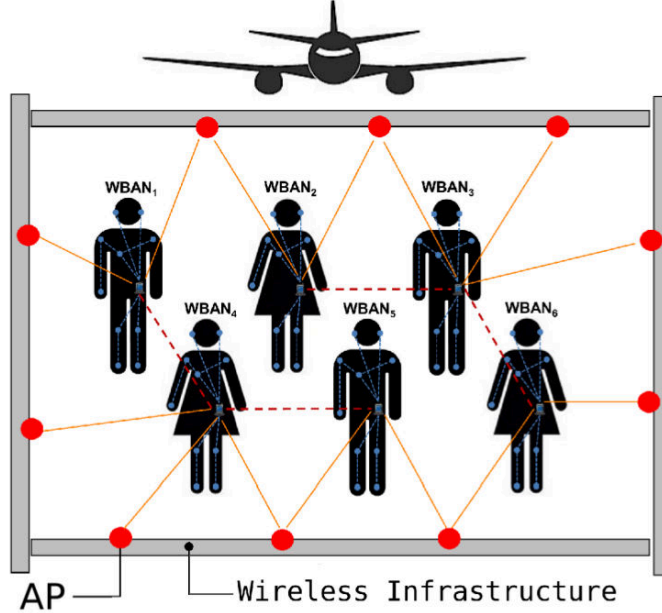


Figure 5.3: BBN and authority levels of the epidemic control model in the airport indoor environment

within a BBN indoor environment, considering the epidemic control application specific requirements. The route selector module is described, thereafter in paragraph 5.4.3, introducing the *epidemic routing metric* which determines how the epidemic data is routed among WBANs, with respect to a number of parameters, such as the residual energy, the contact rate with infected individuals, the transition rate to exposure status, the departure rate of exposed and infected individuals, and the health status of the communicating WBANs. Finally, paragraphs 5.4.4 and 5.4.5 present the epidemic control actions, according to the epidemic control model described in 5.3.2.

5.4.1 Epidemic threshold

The concept of epidemic threshold, denoted hereafter as EP_{th} , is core in our SEIR model. Both BBN and the authority level epidemic control actions articulate around this configurable parameter. In our model, each WBAN $n \in N$ should be able to detect his own health status and broadcast an epidemic alert to the other WBANs in case of incubating or infectious status. We define the health status $H_n(t)$ of WBAN $n \in N$, at time epoch $t \in \mathcal{T}$, as the function $f(\Gamma_n, t)$ of the correlated sensor data $\gamma_i(t) \in \Gamma_n$ of WBAN n , according to the epidemic detection predefined algorithm, where Γ_n represents the set of collected sensor data of WBAN n :

$$H_n(t) = f(\Gamma_n, t), \quad \Gamma_n(t) = \{\gamma_i(t), \forall \text{ sensor } i \in \text{WBAN } n\} \quad (5.5)$$

In order to keep the SEIR model practically tractable, we use the discrete representation of the health status as follows:

$$H_n(t) = \begin{cases} 2, & \text{if } f(\Gamma_n, t) > EP_{th}; & \text{Infectious WBAN (I)} \\ 1, & \text{if } \epsilon < f(\Gamma_n, t) < EP_{th}; & \text{Exposed WBAN (E)} \\ 0, & \text{otherwise;} & \text{Susceptible WBAN (S)} \end{cases}$$

5.4.2 BB-LAR: Location-Aided BBN Routing

A neighborhood discovery module should be implemented to deal with WBANs' mobility and discover the dynamic routes to each other as well as to the wireless AP that will forward the sensor data to the medical servers. Yet, we opt for a reactive (on-demand) routing for inter-WBAN communications and epidemic control information exchange.

However, due to the energy and delay high-constrained nature of BBN networks, it is required that BBN nodes (WBANs) do not deplete their energy in continuous routes maintenance, sharing and storing all network topology information and unnecessary routes discovery. This network overload could be avoided by implementing geographical location based routing. Thus, we select the Location Aided Routing (LAR) protocol which combines reactive routing, based on DSR (Dynamic Source Routing), and geographic routing by limiting the propagation of Route Request (RREQ) packets to a geographic region where it is most probable for the destination to be located [100]. Such location information may be obtained using indoor Location-Based Services (LBS), as proposed in [99], which offer ubiquitous positioning of mobile terminals in pervasive environments, in order to reduce the search space for a desired route, which results in fewer route discovery messages.

Yet, LAR is extended to the Location-Aided BBN Routing (BB-LAR) which is an epidemic threshold-based BBN routing protocol that performs as follows: When a source WBAN $n \in N$ needs to send data to the authority-level control or send a message to another WBAN $m \in N$, he/she broadcasts a Route Request (RREQ) message. The RREQ message contains several key bits information: the source, the destination, their respective location information, the lifespan of the message, a sequence number which serves as a unique ID, and the $H_n(t)$ index specifying the health status generated by the WBAN n , which determines the priority of the data he will send (see Fig. 5.4).

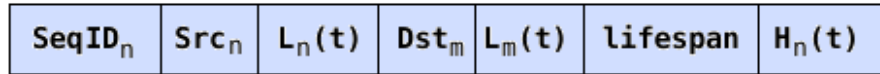


Figure 5.4: Structure of RREQ packet

WBAN n defines a *request zone* for the route request. Assume that the current time is t_1 . WBAN n can determine the request zone based on the knowledge that WBAN m was at location $L_m(t_0)$ at time t_0 . For instance, if WBAN n knows that WBAN m travels

with average speed v , then the expected zone is the circular region of radius $v(t_1 - t_0)$, centered at location $L_m(t_0)$; an illustration is given in Fig. 5.5. Then, a neighbor of WBAN n forwards a route request only if it belongs to the request zone.

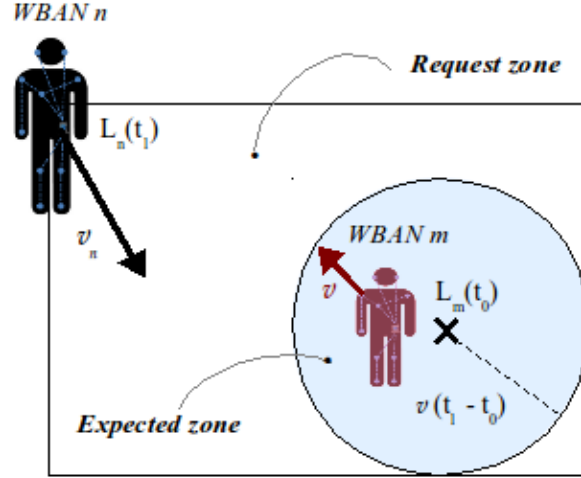


Figure 5.5: Expected zone and request zone for BBN Location Aided Routing (BB-LAR)

When a neighbor of WBAN n receives the RREQ message he/she has two choices:

- If he is the destination m or if he knows a route to the destination, he sends a Route Reply (RREP) message back to WBAN n , he adds his health status $H_m(t)$, his residual energy $E_{res}(m)$ and the number of susceptible, exposed and infectious WBANs; $s_m(t)$, $e_m(t)$ and $i_m(t)$, respectively, he has already exchanged with them (see Fig. 5.6).
- Otherwise, and if it belongs to the request zone, he/she will rebroadcast the RREQ to his neighbors. The message keeps getting rebroadcasted until its lifespan is up.

SeqID _m	Src _m	L _m (t)	Dst _n	L _n (t)	s _m (t)	e _m (t)	i _m (t)	H _m (t)	E _{res} (t)	Q _{id} (t)
--------------------	------------------	--------------------	------------------	--------------------	--------------------	--------------------	--------------------	--------------------	----------------------	---------------------

Figure 5.6: Structure of RREP packet

If WBAN n does not receive a reply in a threshold waiting time, he rebroadcasts the RREQ with a longer lifespan and a new SeqID number. All WBANs use the Sequence number in the RREQ to ensure that they do not rebroadcast a RREQ. The BBN routing protocol, as well as the different epidemic control modules, are summarized in the flow chart given by Fig.5.7.

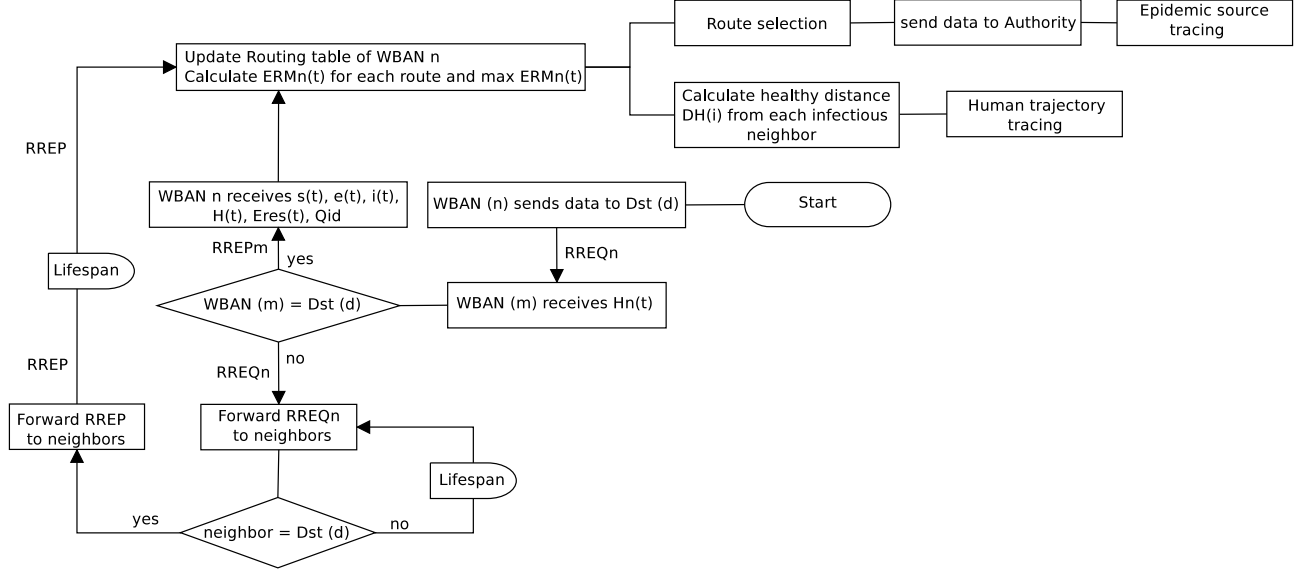


Figure 5.7: Flow chart of the BBN-based epidemic control algorithm

5.4.3 BBN Route selector

To select the route to his destination, the source WBAN n will use the network information collected in his routing table. The purpose is to trade off between the health data transmission priorities and the network resources. By expression (5.6), we define the Epidemic Routing Metric (ERM) of WBAN n as $ERM_n(t)$ which allows the WBAN n to broadcast his health status or send his sensor data to the authority control, at time epoch $t \in \mathcal{T}$, while maximizing the alerts about the critical health status of BBN nodes collected from the RREP messages, according to the expressions (5.2), (5.3) and (5.4).

α is a weighting coefficient that permits to scale the energy consumption beside the epidemic rates (β , δ and μ) and the health status ($H_n(t)$). The health status permits also to scale the consideration of the QoS metrics of the available routes, so that priority increases with data criticality ($H_n(t)=2$ for status (I), 1 for (E) and 0 for (S)).

$$ERM_n(t) = \alpha E_{res}(t) + \beta s_n(t) i_n(t) + \delta e_n(t) + \mu (e_n(t) + i_n(t)) + H_n(t) Q_{id} \quad (5.6)$$

5.4.4 Human trajectory tracing - WBAN selfish strategy

Based on the information collected from the RREP messages, WBAN n updates his routing table with the total number of susceptible, infectious and exposed individuals in his neighborhood, the total residual energy and the QoS metric of each route. Then, he calculates the Healthy Distance $D_H(i)$ from each infectious neighbor $i \in I(t)$. Based on *mobility pre-*

diction algorithms [53], he calculates the hazardous zones around these critical WBANs, as illustrated in Fig. 5.8. WBAN n uses these location parameters to trace his own trajectory, while avoiding the hazardous zones, so as to minimize his contact with infectious WBANs and ensure his real-time self prevention.

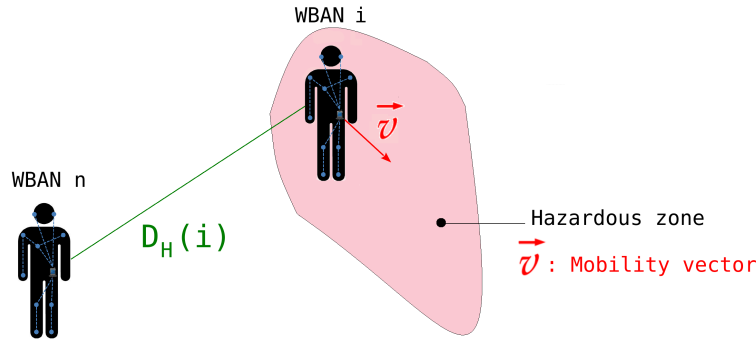


Figure 5.8: Healthy distance and epidemic hazardous zone

5.4.5 Epidemic source tracing - Authority quarantine strategy

To effectively identify epidemic sources and inhibit epidemic spread, an accurate and real-time source tracing algorithm is needed. The wireless APs main task is to collect specific sensor data coupled with WBANs locations and forward these information datasets to the medical servers, where online analysis and identification algorithms based search are performed to detect epidemic outbreaks and quarantine the epidemic WBAN sources.

5.5 Performance Evaluation

In this section we analyse, first, the BB-LAR protocol performance by evaluating three routing parameters: the Packet Delivery Ratio (PDR), the end-to-end delay and the energy consumption. Then, we provide a comparison between our protocol and another proposal in the literature.

5.5.1 Performance analysis of BB-LAR

The OMNet++ based simulator Castalia-3.2 [101] is used to evaluate the performance of our proposed BBN routing protocol, especially in ensuring public safety and preventing the insurgence of the epidemy inside and outside the mass gathering area, i.e. the airport. A number of mobile WBANs, varying in the range [20,100], are randomly deployed in a $200 \times 200m^2$ area and moving according to the common *random waypoint mobility model* [87]. The

transmit power used in our simulations is $-15dBm$ for all WBANs and the initial WBAN energy is 18720 Joules, which is the equivalent of 2 AA batteries [20]. The transmission data rate is set to 5 packets per second, and the Received Signal Strength Indication (RSSI) transmission threshold to $-89.3dBm$. The network parameters used in the simulations are reported in Table 5.1.

Parameter	Value
Area	$200 \times 200m^2$
Number of WBANs	[20..100]
Mobility model	Random Waypoint Mobility
WBAN's MT transmit power	$-15dBm$
Initial WBAN's MT energy	18720 Joules
Transmission data rate	5 pkt/s
RSSI threshold	$-89.3dBm$
MAC	IEEE 802.15.4

Table 5.1: Simulation parameters of BB-LAR

In this work, we evaluate the effect of the WBANs' density on three key performance metrics of routing protocols: the PDR, the end-to-end Delay and the total consumed energy. We further compare these metrics between the three health-type traffic components, I(t), E(t) and S(t), so as to prove the effectiveness of the epidemic control function of our routing protocol. A simulation time of 2000s is run for every WBAN density configuration, and results are reported and discussed hereafter.

The curves on Fig.5.9 illustrate the effect of WBAN density on the packet delivery ratio for the three health-type data traffic. The PDR metric is defined as the ratio of the average data packets received by the WBAN destinations to those generated by the WBAN sources. We define the PDR metric, for example for I(t), as follows:

$$PDR(I(t)) = \frac{\sum \text{Received I(t) data packets}}{\sum \text{Sent I(t) data packets}} \quad (5.7)$$

As expected, the PDR metric decreases with WBAN density, for the three health-type traffic components. Nevertheless, Infectious, I(t), and Exposed, E(t), status packets are delivered with higher PDR, because they are prioritized: $H(t) = 2$ and $H(t) = 1$, respectively, while ordinary health status packets of S(t) traffic, $H(t) = 0$, are less reliably delivered. Besides, with higher densities, beyond 40 WBANs, we notice that the PDR metric dramatically decreases for S(t) traffic, because the network resources become entirely occupied by Infectious and Exposed data traffic, which represent the hazardous individuals to be quarantined.

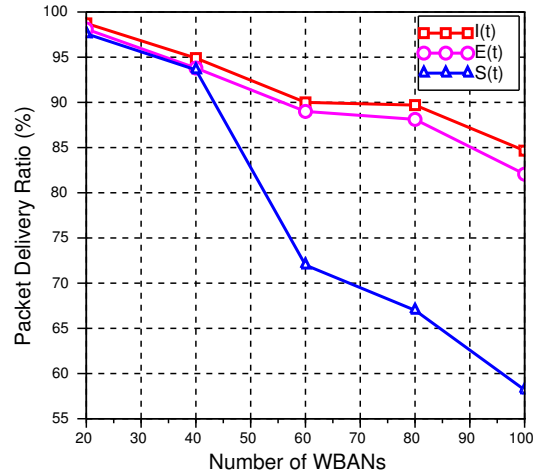


Figure 5.9: Packet delivery ratio of the epidemic data traffic

End-to-end delay specifies the average time that a data packet takes to reach the destination WBAN, including all delays caused by route discovery, buffering and queuing at each WBAN queue. End-to-end delay naturally increases with WBAN density, as shown by Fig.5.10. I(t) and E(t) packets are delay sensitive and then achieve less transmission delay compared to ordinary packets S(t).

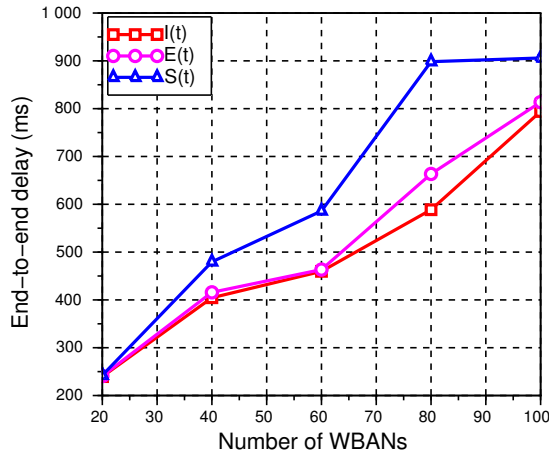


Figure 5.10: End-to-end delay of epidemic data packets

In accordance to what was observed for the PDR metric, the S(t) status latency notably increases with higher densities (above 60 WBANs), since network queues become overloaded

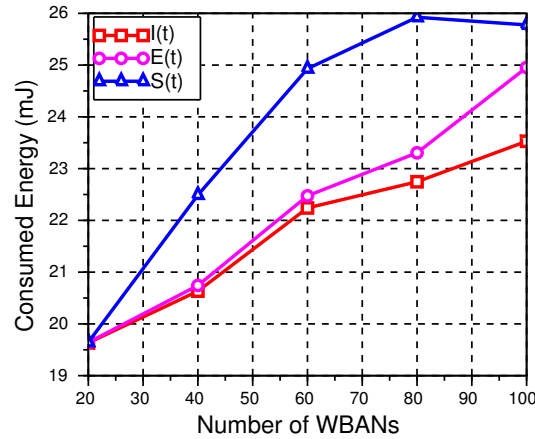


Figure 5.11: Total energy consumed by the epidemic data transmissions

with $I(t)$ and $E(t)$ traffic.

Finally, Fig.5.11 points out how the energy consumption increases with WBAN density. The consumed energy is calculated for each WBAN by the Resource Manager of the simulator, as the sum of transmission, buffering, reception and idle energy amounts. Average total consumed energy values are represented. Fig.5.12 depicts the internal structure of a sensor node in Castalia, where we can see that most of the modules call a function of the resource manager to signal that energy has been consumed. In practice, the different sensor node modules, that model the hardware devices (i.e, the radio, MAC, CPU...) send messages to the resource manager to notify about how much power they currently use. Thus, the resource manager has a complete view of the total power drawn in the WBAN [5].

It can be observed that $I(t)$ and $E(t)$ packets are less energy consuming since they are associated with high priorities and hence face less packet retransmissions, while $S(t)$ packets need more retransmissions especially with higher densities, and hence higher packet collisions.

5.5.2 Comparison of BB-LAR with other geographic-based routing protocols

In order to assess the efficiency of our BB-LAR protocol for BBN communications, and given the scarcity of inter-WBAN routing protocols in the literature, we compare our protocol with the Reliable Routing Technique (RRT) proposed in [6], which is also a geographic routing protocol, based on GPSR [94], that aims to establish reliable and continuous communications between the officers, the rescue team and the people in disaster situations, without the use of the communication infrastructure that could be completely or partially

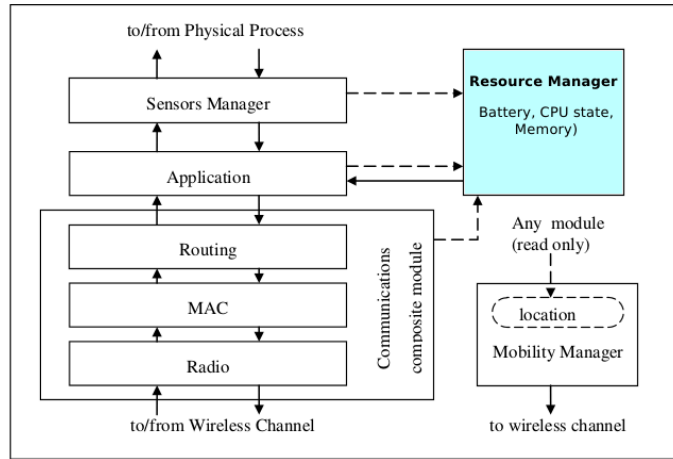


Figure 5.12: Resource Manager module of a WBAN node in Castalia [5]

damaged. Thus, authors of [6] use ad hoc networks as one of the best techniques for establishing communication during disaster relief operations, which make it possible to compare this protocol with BB-LAR since it ensures routing among BBN nodes that form an ad hoc network.

The RRT protocol is then proposed to ensure reliable data delivery among mobile devices like mobile phones and personal computers. The technique is based on priority concept of the mobile devices, so that the nearest mobile device to the destination is given the highest priority and is first selected to route the data packet. If ever a forwarder device is unable to forward the data packet due to movement of mobile devices, the next priority device forwards the data packet to the destination, ensuring thus the reliability of data delivery in the ad hoc network.

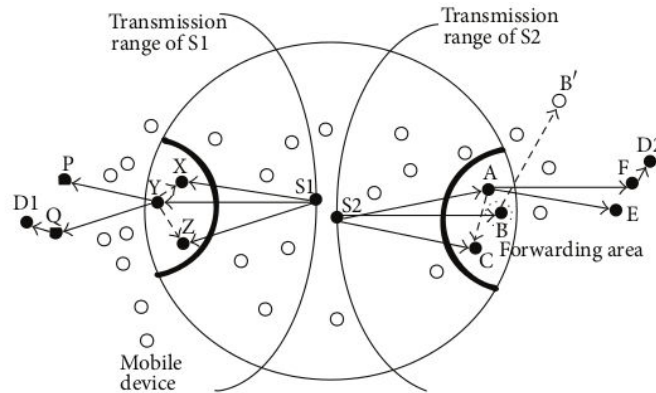


Figure 5.13: Reliable Routing Technique (RRT) in two situations: 1) No disruption of the wireless link (S1 to D1), and 2) Disruption of the wireless link (S2 to D2) [6]

Thereby, the RRT algorithm can be summarized in the following steps:

1. The source device (S) of a rescue officer broadcasts the data to the network.
2. The nearest device to the destination (D) is the forwarder (F), it has the priority to forward the packet. Then, two situations are envisaged (Fig.5.13):
 - Mobile device (F) forwards the data to the destination (D) and to the mobile nodes in its transmission range. The neighbors receives then a second copy of the packet and realize that the data has been already forwarded by a prior node, then they drop that packet.
 - Mobile device (F) moves outside the transmission range of the source node (S) and does not receive the packet. Upon a timer (T), the second priority node, having not received a copy of the packet broadcasted by the source, becomes the forwarder (F), and so on till reaching the destination (D).

The main contribution of the RRT protocol is the guarantee of reliability and continuous communication in emergency situations, it ensures the delivery of packets in dynamic scenarios where rescue workers move throughout the focus zone during disaster recovery.

The difference with respect to BB-LAR is that in RRT protocol the rescue officers are not equipped with WBANs, just communicating mobile devices (smartphones, laptops,...) are considered. BB-LAR protocol further considers traffic classes, with respect to the different data priorities transmitted by the sensors, which is not the case of RRT protocol. Another issue that RRT should deal with is the traffic overhead due to the multiple transmissions of data packets for reliability ensurance, which can have a dramatical effect on the energy consumption and the data delivery delays.

Yet, RRT simulations are run with Castalia simulator under the same parameters configuration as BB-LAR, but without considering traffic classes relative to the different health status. Since RRT does not consider traffic classes, we obtain a single curve for each evaluation parameter: we calculate a single PDR value for the total traffic sent and received, according to equation 5.7, and we obtain single delay and consumed energy values for each network density.

Firstly, and thanks to the reliability module, RRT protocol achieves successfull PDR, which can be observed from Fig.5.14. It is even clear that PDR performance of RRT protocol is better than BB-LAR, staying above 90%, for network sizes of less than 70 WBANs. Then I(t) and E(t) components of BB-LAR perform better for greater network sizes. Indeed, for higher densities, a great number of packets, that correspond to susceptible WBANs traffic S(t) are delayed, and prior I(t) and E(t) packets are transmitted, so that to ensure that the requested PDR is met, while RRT keeps transmitting, with much more overhead due to the reliability mechanism, the whole data traffic which results in a harmful effect on the packet delivery ratios.

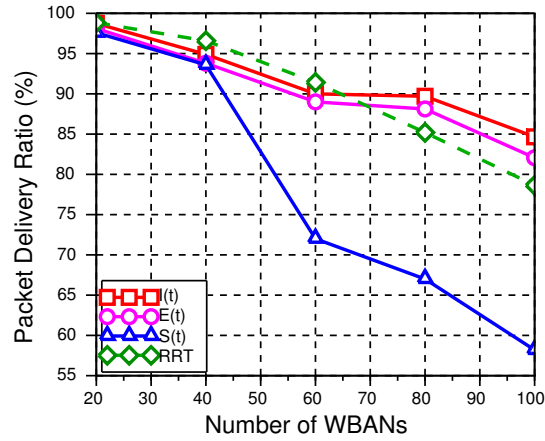


Figure 5.14: Packet Delivery Ratio: BB-LAR v.s. RRT

Noticeable gaps are then observed for end-to-end delay and energy consumption curves, between RRT and BB-LAR, in Fig.5.15 and Fig.5.16. Due to the traffic overhead, RRT is subject to excess delay compared to BB-LAR, but its curve approaches that of I(t) and E(t) for network sizes above 80 WBANs. Then, for bigger networks, RRT performs slightly similar to BB-LAR.

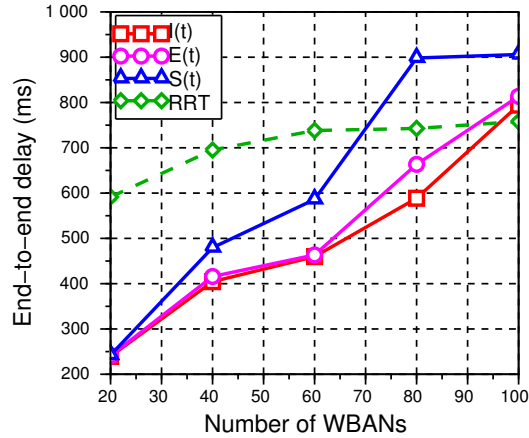


Figure 5.15: End-to-end delay: BB-LAR v.s. RRT

This could be explained by the difference between GPSR and LAR protocols, and their respective behaviors for higher network densities. Both geographic protocols limitate the destination zone, and even if RRT seems to perform efficiently for large-scale networks,

our enhanced BB-LAR protocol performs better for any network size, thanks to the traffic classification that differentiates the $S(t)$ traffic which is not delay sensitive, and transmit within short delays the more constrained data packets, $I(t)$ and $E(t)$.

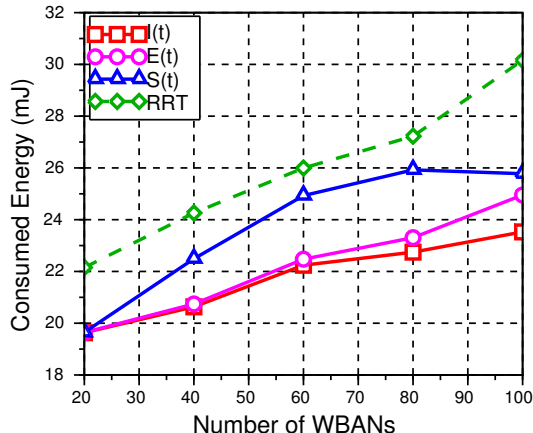


Figure 5.16: Consumed energy: BB-LAR v.s. RRT

The gap between RRT and BB-LAR is then more evident for the energy curves (Fig.5.16). Especially for big sized networks of above 80 WBANs, packets need to pass through more nodes to reach the destination, which generates further energy consumption, and with all packets retransmissions, as required by the RRT reliability mechanism, this energy amount would be double or even more.

Despite the routing cost due to the overhead packets of the epidemic information exchange, BB-LAR achieves better results than RRT. Yet, BB-LAR traffic overhead can be regarded as negligible, compared to the improvement it provides in terms of delay and energy consumption.

5.6 Conclusion

In this chapter we proposed an epidemic threshold-based routing protocol (BB-LAR) to ensure a real-time and self prevention epidemic control. Our approach is based on the SEIR epidemic spread model that allows to introduce the intermediate exposure status, so that to limitate the epidemic spread during the incubation period of the disease. The epidemic threshold is then used to detect the incubating or infectious status and send a RREQ message to warn the authority control unit. The RREQ message routing, based on location information, would inform the neighboring WBANs of the nearby peril. Finally, we evaluate our BBN routing protocol, BB-LAR, in realistic BBN scenarios in order to show that

the protocol achieves accepted PDR, end-to-end delay and consumed energy values, and differentiates between the three-type epidemic traffic. Nevertheless, to effectively identify epidemic sources and inhibit epidemic spread, an accurate and real-time source tracing algorithm is needed, which will be considered as part of our future work.

Chapter 6

Conclusion and Future Perspectives

In this thesis we studied the distributed interference mitigation problem in BBN scenarios from a game theoretical perspective. In particular, our work made three main contributions. First, we formulated the problem as a game considering the Signal-to-Interference Ratio, which accurately models the channel capacity that can be achieved in the presence of mutual and cross-technology interference.

Second, we studied the properties of our game proving the existence of a Nash Equilibrium, which represents channel allocations that minimize the mutual and cross-technology interference.

Third, we proposed a two-stage algorithm (called BR-SIM) based on the best-response dynamics to compute the Nash Equilibria in a distributed fashion. We further developed an alternative approach (SORT-SIM) that reaches a sub-optimal solution in less computational time than BR-SIM.

Finally, we evaluated and compared our approaches in realistic BBN scenarios showing that the BR-SIM algorithm converges quickly and achieves feasible values for the utility functions, while SORT-SIM presents some practicability benefits under specific network scenarios.

Then we proposed an epidemic threshold-based routing protocol, BB-LAR, to ensure a real-time and self prevention epidemic control. The simulation results of our proposed epidemic model and BBN routing protocol are promising and provide insights in the design of powerful frameworks for epidemic control using BBNs.

Our perspectives for the future work consist, first, in a real-time source tracing mech-

anism to track the Infectious and Exposed subjects, either by the susceptible WBANs to perform their self-prevention strategies, or by authorities to catch and isolate them. Then we intend to implement a security module for the epidemic threshold-based BBN routing protocol, in order to ensure inter-WBAN data privacy, and provide legacy for epidemic source tracing and quarantine by the authorities.

Further BBN issues have not been inspected in this work and are of significant concern, to cite a few:

- *Wireless channel propagation challenges:* At present, very little is known about the characteristics of wireless signal propagation between wireless wearable devices forming a human body-to-body network. Recent narrowband studies at 2.45 GHz [1, 72, 102], have tried to establish some propagation models based on user's physical characteristics, including mobility and human bodies' effects (LOS, NLOS, shadowing, fading...). In fact, a greater understanding of the physical layer characteristics, the reliability and connectivity of wireless data paths will help in the design of upper layers, for example when allocating resources at the link layer or performing routing at network layer.
- *Storage and privacy of health data in a cloud environment:* The data exchange among a group of persons within a BBN could be motivated by the rapid growth of cloud-computing market. Nevertheless, the thought of one's sensitive health data, traveling from person to person until reaching a virtual server, is a bit unsettling, and it introduces further security issues for U-health applications.
- *Heterogeneous devices and traffic:* BBNs should be able to handle heterogeneous traffic, ranging from plain messages to real-time audio and video contents, and support diverse transmission rates, especially between the WBANs' coordinators. Moreover, special mechanisms should be implemented to handle new devices in the WBAN neighborhood, enabling the seamless addition or removal of WBANs during roaming or link failures, without affecting the BBN operation.
- *Ethical challenges:* whereas Medicine is a profession which is heavily regulated by government authority, Computer Science and ICT services are notoriously lacking in such regulations. Therefore, a number of ethical considerations, including privacy, equity, liability and responsibility to the error, are involved [103].

Bibliography

- [1] SimonL Cotton and WilliamG Scanlon. Using smart people to form future mobile wireless networks. *Microwave Journal*, 54(12):24–40, 2011.
- [2] Vincent WS Wong et al. Joint optimal channel assignment and congestion control for multi-channel wireless mesh networks. In *Communications, 2006. ICC'06. IEEE International Conference on*, volume 5, pages 1984–1989. IEEE, 2006.
- [3] Jie Dong and David Smith. Joint relay selection and transmit power control for wireless body area networks coexistence. In *IEEE International Conference on Communications (ICC)*, pages 5676–5681. IEEE, Sydney, Australia, June 2014.
- [4] Marcelo FC Gomes, Ana Pastore y Piontti, Luca Rossi, Dennis Chao, Ira Longini, M Elizabeth Halloran, and Alessandro Vespignani. Assessing the international spreading risk associated with the 2014 west african ebola outbreak. *PLOS Currents Outbreaks*, 2014.
- [5] Athanassios Boulis. Castalia user manual. *Online: <http://castalia.npc.nicta.com.au/pdfs/Castalia-User Manual.pdf>*, 2009.
- [6] Varun G Menon, Joe Prathap Pathrose, and Jogi Priya. Ensuring reliable communication in disaster recovery operations with reliable routing technique. *Mobile Information Systems*, 2016.
- [7] Sangbae Shin, Su Weidong, and Jinsung Cho. A game theory model to support qos in overlapped wban environment. In *Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication*, page 47. ACM, 2012.
- [8] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V.C.M. Leung. Body area networks: a survey. *Mobile Networks and Applications*, 16(2):171–193, April 2011.

- [9] Carles Gomez, Joaquim Oller, and Josep Paradells. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors*, 12(9):11734–11753, 2012.
- [10] Alex Chia-Chun Hsu, David SL Wei, C-C Jay Kuo, Norio Shiratori, and Chung-Ju Chang. Enhanced adaptive frequency hopping for wireless personal area networks in a coexistence environment. In *IEEE GLOBECOM 2007-IEEE Global Telecommunications Conference*, pages 668–672. IEEE, 2007.
- [11] M Cho-Hoi Chek and Yu-Kwong Kwok. On adaptive frequency hopping to combat coexistence interference between bluetooth and ieee 802.11 b with practical resource constraints. In *Parallel Architectures, Algorithms and Networks, 2004. Proceedings. 7th International Symposium on*, pages 391–396. IEEE, 2004.
- [12] Nils Langhammer and Ruediger Kays. Enhanced frequency hopping for reliable interconnection of low power smart home devices. In *2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 305–310. IEEE, 2012.
- [13] Carla F Chiasserini and Ramesh R Rao. Coexistence mechanisms for interference mitigation between ieee 802.11 wlans and bluetooth. In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 2, pages 590–598. IEEE, 2002.
- [14] Samaneh Movassaghi, Akbar Majidi, Abbas Jamalipour, David Smith, and Mehran Abolhasan. Enabling interference-aware and energy-efficient coexistence of multiple wireless body area networks with unknown dynamics. 2016.
- [15] Weixia Zou, Chao Guo, Fengyuan Kang, and Chunqing Zhang. An interference avoidance method of wireless body area network based on chinese medical band. *International Journal of Distributed Sensor Networks*, 2015:4, 2015.
- [16] Roy C Park, Hoill Jung, and Sun-Moon Jo. Abs scheduling technique for interference mitigation of m2m based medical wban service. *Wireless Personal Communications*, 79(4):2685–2700, 2014.
- [17] Dakun Du, Fengye Hu, Feng Wang, Zhijun Wang, Yu Du, and Lu Wang. A game theoretic approach for inter-network interference mitigation in wireless body area networks. *China Communications*, 12(9):150–161, 2015.
- [18] IEEE Standards Association et al. Ieee standard for local and metropolitan area networks-part 15.6: wireless body area networks. *IEEE Std*, 802(6):2012, 2012.

- [19] Zahoor Ali Khan, Shyamala Sivakumar, William Phillips, and Bill Robertson. Zeqos: A new energy and qos-aware routing protocol for communication of sensor devices in healthcare system. *International Journal of Distributed Sensor Networks*, 2014, 2014.
- [20] Zahoor A Khan, Shyamala Sivakumar, William Phillips, and Bill Robertson. A qos-aware routing protocol for reliability sensitive data in hospital body area networks. *Procedia Computer Science*, 19:171–179, 2013.
- [21] ShihHeng Cheng, ChingYao Huang, and Chun Chen Tu. Racoon: A multiuser qos design for mobile wireless body area networks. *Journal of medical systems*, 35(5):1277–1287, 2011.
- [22] Muhammad Mostafa Monowar, Mohammad Mehedi Hassan, Fuad Bajaber, Musaed Al-Hussein, and Atif Alamri. Mcmac: Towards a mac protocol with multi-constrained qos provisioning for diverse traffic in wireless body area networks. *Sensors*, 12(11):15599–15627, 2012.
- [23] Zhaoyang Zhang, Ken CK Lee, Honggang Wang, Dong Xuan, and Hua Fang. Epidemic control based on fused body sensed and social network information. In *Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on*, pages 285–290. IEEE, 2012.
- [24] Zhaoyang Zhang, Honggang Wang, Xiaodong Lin, Hua Fang, and Dong Xuan. Effective epidemic control and source tracing through mobile social sensing over wbans. In *INFOCOM, 2013 Proceedings IEEE*, pages 300–304. IEEE, 2013.
- [25] Zhaoyang Zhang, Honggang Wang, Chonggang Wang, and Hua Fang. Cluster-based epidemic control through smartphone-based body area networks. 2014.
- [26] Stan Ratliff, John Dowdell, and Charles Perkins. Dynamic manet on-demand (aodvv2) routing. 2013.
- [27] Thomas Clausen, Christopher Dearlove, Philippe Jacquet, and Ulrich Herberg. The optimized link state routing protocol version 2. Technical report, 2014.
- [28] Chalermek Intanagonwiwat, Ramesh Govindan, and Deborah Estrin. Directed diffusion: a scalable and robust communication paradigm for sensor networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 56–67. ACM, 2000.
- [29] Young-Bae Ko and Nitin H Vaidya. Location-aided routing (lar) in mobile ad hoc networks. *Wireless networks*, 6(4):307–321, 2000.
- [30] Kyung Sup Kwak, Sana Ullah, and Niamat Ullah. An overview of ieee 802.15. 6 standard. In *Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on*, pages 1–6. IEEE, 2010.

- [31] IEEE Standards Association. 802.15.6-2012 IEEE Standards for Local and Metropolitan Area Networks–Part 15.6: Wireless Body Area Networks. Available online: <http://standards.ieee.org/findstds/standard/802.15.6-2012.html>.
- [32] IEEE Standards Association. 802.15.4-2011 IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs). Available online: <http://standards.ieee.org/findstds/standard/802.15.4-2011.html>.
- [33] ITU-T Recommendation E.800 (09/08): Definitions of terms related to quality of service. Available online: <http://www.itu.int/rec/T-REC-E.800-200809-I/en>.
- [34] Jayanthi K Murthy and V Sambasiva Rao. Improved routing protocol for health care communications. *Open Journal of Applied Biosensor*, pages 51–56, 2013.
- [35] Nadeem Javaid, Z Abbas, MS Fareed, ZA Khan, and N Alrajeh. M-attempt: A new energy-efficient routing protocol for wireless body area sensor networks. *Procedia Computer Science*, 19:224–231, 2013.
- [36] Q Nadeem, Nadeem Javaid, SN Mohammad, MY Khan, S Sarfraz, and M Gull. Simple: Stable increased-throughput multi-hop protocol for link efficiency in wireless body area networks. In *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2013 Eighth International Conference on*, pages 221–226. IEEE, 2013.
- [37] Liang Liang, Yu Ge, Gang Feng, Wei Ni, and Aung Aung Phyto Wai. A low overhead tree-based energy-efficient routing scheme for multi-hop wireless body area networks. *Computer Networks*, 70:45–58, 2014.
- [38] Jocelyne Elias. Optimal design of energy-efficient and cost-effective wireless body area networks. *Ad Hoc Networks*, 13:560–574, 2014.
- [39] Stevan Jovica Marinkovic, Emanuel M Popovici, Christian Spagnol, Stephen Faul, and William P Marnane. Energy-efficient low duty cycle mac protocol for wireless body area networks. *Information Technology in Biomedicine, IEEE Transactions on*, 13(6):915–925, 2009.
- [40] W Heinelman, Anantha Chandrakasan, and Hari Balakrishnan. Energy-efficient communication protocol for wireless microsensor network. In *Proc, of the Hawaii International Conference on System Sciences*, 2000.
- [41] Jamil Yusuf Khan, Mehmet R Yuce, Garrick Bulger, and Benjamin Harding. Wireless body area network (wban) design techniques and performance evaluation. *Journal of medical systems*, 36(3):1441–1457, 2012.

- [42] G. Fang, E. Dutkiewicz, K. Yu, R. Vesilo, and Y. Yu. Distributed inter-network interference coordination for wireless body area networks. In *IEEE GLOBECOM'10*, pages 1–5, Miami, Florida, USA, Dec. 2010.
- [43] H.J. Lee, H. Kwon, A. Molskin, and L. Guibas. Interference-aware mac protocol for wireless networks by a game-theoretic approach. In *IEEE INFOCOM'09*, pages 1854–1862, Rio de Janeiro, Brazil, April 2009.
- [44] J. Chen, Q. Yu, P. Cheng, Y. Sun, Y. Fan, and X. Shen. Game theoretical approach for channel allocation in wireless sensor and actuator networks. *IEEE Transactions on Automatic Control*, 56(10):2332–2344, 2011.
- [45] W.-B. Yang and K. Sayrafian-Pour. Interference mitigation for body area networks. In *22nd IEEE PIMRC'11*, pages 2193–2197, Toronto, Canada, September 2011.
- [46] S.L. Cotton, A. McKernan, A.J. Ali, and W.G. Scanlon. An experimental study on the impact of human body shadowing in off-body communications channels at 2.45 ghz. In *Proceedings of the 5th IEEE European Conference on Antennas and Propagation (EUCAP)*, pages 3133–3137, Rome, Italy, April 2011.
- [47] J. Huang, G. Xing, G. Zhou, and R. Zhou. Beyond co-existence: Exploiting wifi white space for zigbee performance assurance. In *18th IEEE International Conference on Network Protocols (ICNP'10)*, pages 305–314, Kyoto, Japan, 2010.
- [48] S.Y. Shin, H.S. Park, S. Choi, and W.H. Kwon. Packet error rate analysis of zigbee under wlan and bluetooth interferences. *IEEE Transactions on Wireless Communications*, 6(8):2825–2830, 2007.
- [49] C.-J.M. Liang, N.B. Priyantha, J. Liu, and A. Terzis. Surviving wi-fi interference in low power zigbee networks. In *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems (SenSys'10)*, pages 309–322, Zurich, Switzerland, November 2010.
- [50] J. Hou, B. Chang, D.-K. Cho, and M. Gerla. Minimizing 802.11 interference on zigbee medical sensors. In *Proceedings of the Fourth International Conference on Body Area Networks (BodyNets'09)*, page 5. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels, Belgium, 2009.
- [51] S. Paris, J. Elias, and A. Mehaoua. Cross technology interference mitigation in body-to-body area networks. In *IEEE WoWMoM'13*, pages 1–9, Madrid, Spain, June 2013.
- [52] Md Abdur Razzaque, Choong Seon Hong, and Sungwon Lee. Data-centric multiobjective qos-aware routing protocol for body sensor networks. *Sensors*, 11(1):917–937, 2011.

- [53] Damianos Gavalas, Charalampos Konstantopoulos, and G Pantziou. Mobility prediction in mobile ad hoc networks. *Next Generation Mobile Networks and Ubiquitous Computing*, pages 226–240, 2010.
- [54] Majid Nabi, Marc Geilen, and Twan Basten. Moban: A configurable mobility model for wireless body area networks. In *Proceedings of the 4th International ICST Conference on Simulation Tools and Techniques*, pages 168–177. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2011.
- [55] Xiaohui Liang, Xu Li, Qinghua Shen, Rongxing Lu, Xiaodong Lin, Xuemin Shen, and Weihua Zhuang. Exploiting prediction to enable secure and reliable routing in wireless body area networks. In *INFOCOM, 2012 Proceedings IEEE*, pages 388–396. IEEE, 2012.
- [56] Bart Braem and Chris Blondia. An analysis of requirements to supporting mobility in body area networks. In *Computing, Networking and Communications (ICNC), 2012 International Conference on*, pages 89–93. IEEE, 2012.
- [57] Manisha Mittal and Dr DK Chauhan. Secured solutions for mobility in wireless body area networks. *International Journal of Emerging Technology and Advanced Engineering*, 4(2):157–161, 2014.
- [58] Sarah Irum, Aftab Ali, Farrukh Aslam Khan, and Haider Abbas. A hybrid security mechanism for intra-wban and inter-wban communications. *International Journal of Distributed Sensor Networks*, 2013, 2013.
- [59] Aftab Ali and Farrukh Aslam Khan. Energy-efficient cluster-based security mechanism for intra-wban and inter-wban communications for healthcare applications. *EURASIP Journal on Wireless Communications and Networking*, 2013(1):1–19, 2013.
- [60] Reza Khalilian, Abdalhossein Rezai, and Ehsan Abedini. An efficient method to improve wban security. 2014.
- [61] Ramesh Kumar and Rajeswari Mukesh. State of the art: Security in wireless body area networks. *International Journal of Computer Science & Engineering Technology (IJCSET) Vol*, 4:622–630, 2013.
- [62] K Wac, R Bults, B Van Beijnum, I Widya, V Jones, D Konstantas, M Vollenbroek-Hutten, and H Hermens. Mobile patient monitoring: the mobihealth system. In *Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE*, pages 1238–1241. IEEE, 2009.
- [63] Azzedine Boukerche and Yonglin Ren. A secure mobile healthcare system using trust-based multicast scheme. *Selected Areas in Communications, IEEE Journal on*, 27(4):387–399, 2009.

- [64] Mark Felegyhazi and Jean-Pierre Hubaux. Game theory in wireless networks: A tutorial. Technical report, Technical Report LCA-REPORT-2006-002, EPFL, 2006.
- [65] Pedro BF Duarte, Zubair Md Fadlullah, Athanasios V Vasilakos, and Nei Kato. On the partially overlapped channel assignment on wireless mesh network backbone: A game theoretic approach. *Selected Areas in Communications, IEEE Journal on*, 30(1):119–127, 2012.
- [66] Ramtin Kazemi, Rein Vesilo, and Eryk Dutkiewicz. A novel genetic-fuzzy power controller with feedback for interference mitigation in wireless body area networks. In *Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd*, pages 1–5. IEEE, 2011.
- [67] Jocelyne Elias, Fabio Martignon, Antonio Capone, and Eitan Altman. Non-cooperative spectrum access in cognitive radio networks: a game theoretical model. *Computer Networks*, 55(17):3832–3846, 2011.
- [68] Eitan Altman, Anurag Kumar, Chandramani Singh, and Rajesh Sundaresan. Spatial sinr games combining base station placement and mobile association. In *INFOCOM 2009, IEEE*, pages 1629–1637. IEEE, 2009.
- [69] John F Nash et al. Equilibrium points in n-person games. *Proc. Nat. Acad. Sci. USA*, 36(1):48–49, 1950.
- [70] A.H. Mohsenian Rad and V.W.S. Wong. Partially overlapped channel assignment for multi-channel wireless mesh networks. In *IEEE ICC'07*, pages 3770–3775, Glasgow, Scotland, June 2007.
- [71] Arunesh Mishra, Vivek Shrivastava, Suman Banerjee, and William Arbaugh. Partially overlapped channels not considered harmful. In *ACM SIGMETRICS Performance Evaluation Review*, volume 34, pages 63–74. ACM, 2006.
- [72] Ramona Rosini, Raffaele D’Errico, and Roberto Verdone. Body-to-body communications: a measurement-based channel model at 2.45 ghz. In *Personal Indoor and Mobile Radio Communications (PIMRC), 2012 IEEE 23rd International Symposium on*, pages 1763–1768. IEEE, 2012.
- [73] Anand Prabhu Subramanian, Himanshu Gupta, Samir R Das, and Jing Cao. Minimum interference channel assignment in multiradio wireless mesh networks. *Mobile Computing, IEEE Transactions on*, 7(12):1459–1473, 2008.
- [74] Monty Beuster, Michael Beigl, Daniel Rohr, Till Riedel, Christian Decker, and Martin Berchtold. Matrix routing—an interference range insensitive routing protocol for wireless sensor networks. In *Applications and the Internet, 2008. SAINT 2008. International Symposium on*, pages 137–140. IEEE, 2008.

- [75] Kaixin Xu, Mario Gerla, and Sang Bae. Effectiveness of rts/cts handshake in ieees 802.11 based ad hoc networks. *Ad Hoc Networks*, 1(1):107–123, 2003.
- [76] Jocelyne Elias, Stefano Paris, and Marwan Krunz. Cross technology interference mitigation in body area networks: an optimization approach. *IEEE Transactions on Vehicular Technology*, September 2014.
- [77] Zhaoyang Zhang, Honggang Wang, Chonggang Wang, and Hua Fang. Interference mitigation for cyber-physical wireless body area network system using social networks. *Emerging Topics in Computing, IEEE Transactions on*, 1(1):121–132, 2013.
- [78] Siddhartan Govindasamy, Daniel W Bliss, and David H Staelin. Asymptotic spectral efficiency of multiantenna links in wireless networks with limited tx csi. *Information Theory, IEEE Transactions on*, 58(8):5375–5387, 2012.
- [79] N. Golmie, D. Cypher, and O. Rebala. Performance analysis of low rate wireless technologies for medical applications. *Elsevier Computer Communications*, 28(10):1266–1275, 2005.
- [80] N. Nisan, T. Roughgarden, E. Tardos, and V. V Vazirani. *Algorithmic game theory*. Cambridge University Press, 2007.
- [81] X. Chen and J. Huang. Game theoretic analysis of distributed spectrum sharing with database. *Proceedings of the IEEE 32nd International Conference on Distributed Computing Systems (ICDCS)*, pages 255–264, Macau, China, June 18-21, 2012.
- [82] Dov Monderer and Lloyd S Shapley. Potential games. *Games and economic behavior*, 14(1):124–143, 1996.
- [83] Anjum Naveed and Salil S Kanhere. Nis07-5: Security vulnerabilities in channel assignment of multi-radio multi-channel wireless mesh networks. In *Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE*, pages 1–5. IEEE, 2006.
- [84] F Kaabi, S Ghannay, and F Filali. Channel allocation and routing in wireless mesh networks: A survey and qualitative comparison between schemes. *International Journal of Wireless and Mobile Network*, 2(1):132–151, 2010.
- [85] Mihui Kim and Peng Ning. Seca: A framework for secure channel assignment in wireless mesh networks. *Computer Communications*, 34(4):567–576, 2011.
- [86] INRIA. Scilab software package.
- [87] David B Johnson and David A Maltz. Dynamic source routing in ad hoc wireless networks. In *Mobile computing*, pages 153–181. Springer, 1996.

- [88] Jie Dong and David Smith. Opportunistic relaying in wireless body area networks: Coexistence performance. In *IEEE International Conference on Communications (ICC)*, pages 5613–5618. IEEE, Budapest, Hungary, June 2013.
- [89] D Smith, L Hanlen, D Rodda, B Gilbert, J Dong, and V Chaganti. Body area network radio channel measurement set. URL: <http://www.opennicta.com/datasets>. accessed December, 2012.
- [90] Christos Nicolaides, Luis Cueto-Felgueroso, Marta C Gonzalez, and Ruben Juanes. A metric of influential spreading during contagion dynamics through the air transportation network. *PloS one*, 7(7), 2012.
- [91] Xiaowei Xu, Nurcan Yuruk, Zhidan Feng, and Thomas AJ Schweiger. Scan: a structural clustering algorithm for networks. In *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 824–833. ACM, 2007.
- [92] Ieee 802.15 wpan task group 6 body area networks, 15-08-0644-09-0006-tg6 technical requirements document,.
- [93] Dhafer Ben Arbia, Muhammad Mahtab Alam, Rabah Attia, and Elyes Ben Hamida. Behavior of wireless body-to-body networks routing strategies for public protection and disaster relief. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on*, pages 117–124. IEEE, 2015.
- [94] Brad Karp and Hsiang-Tsung Kung. Gpsr: Greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 243–254. ACM, 2000.
- [95] Guihua Li, Wendi Wang, and Zhen Jin. Global stability of an seir epidemic model with constant immigration. *Chaos, Solitons & Fractals*, 30(4):1012–1019, 2006.
- [96] Fred Brauer. Compartmental models in epidemiology. In *Mathematical epidemiology*, pages 19–79. Springer, 2008.
- [97] Herbert W Hethcote. The mathematics of infectious diseases. *SIAM review*, 42(4):599–653, 2000.
- [98] Dejen Ketema Mamo and Purnachandra Rao Koya. Mathematical modeling and simulation study of seir disease and data fitting of ebola epidemic spreading in west africa. *Journal of Multidisciplinary Engineering Science and Technology (JMEST) ISSN*, pages 3159–0040.

- [99] Halgurd S Maghdid, Ihsan Alshahib Lami, Kayhan Zrar Ghafoor, and Jaime Lloret. Seamless outdoors-indoors localization solutions on smartphones: implementation and challenges. *ACM Computing Surveys (CSUR)*, 48(4):53, 2016.
- [100] Atekeh Maghsoudlou, Marc St-Hilaire, and Thomas Kunz. A survey on geographic routing protocols for mobile ad hoc networks. *Carleton University, Systems and Computer Engineering, Technical Report*, 2011.
- [101] Athanassios Boulis et al. Castalia: A simulator for wireless sensor networks and body area networks. *NICTA: National ICT Australia*, 2011.
- [102] Simon L Cotton, William G Scanlon, and Bhopinder K Madahar. Millimeter-wave soldier-to-soldier communications for covert battlefield operations. *Communications Magazine, IEEE*, 47(10):72–81, 2009.
- [103] Ian Brown, Andrew A Adams, et al. The ethical challenges of ubiquitous healthcare. *International Review of Information Ethics*, 8(12):53–60, 2007.

Appendix

A.1 BR-SIM algorithm Scilab source code	111
A.2 SORT-SIM algorithm Scilab source code	119
A.3 BB-LAR Castalia configuration file (omnetpp.ini)	123

A.1 BR-SIM algorithm Scilab source code

```

//*****
//***** BR-SIM Algorithm *****
//***** Author: Amira Meharouech *****
//***** July 2014 *****
//*****

//*****
//***** Inputs: Initialization *****
//*****

scf(1); //creation of a graphic window
clf(1);
f=gcf();
f.figure_name='MANET' ;
f.pixmap='on'; //set the pixmap mode
//creation of the network boundaries
plot2d(0,0,-1,"011", " ",style=5,rect=[0,0,1000,1000]);
xgrid;
r=10; //display radius of moving nodes
rf=15; //display radius of fixed nodes
rs=19; //display radius of the moving nodes belonging to the connection under studies
n=19; //quantity of moving nodes =nbr of WBANS =nbr of Zigbee links
nf=1; //quantity of fixed nodes (medical server)
L=1000; //network square area side
ts=20; //maximum time break
vm=20; //maximum speed
Tlim=300; //simulation duration
Tmax=50 //maximal waiting time
dmax=180; //Locality radius for the links attribution
Cw=1:5; //{{1,6,11} //1:5//1:14; // Wifi channels
Cz=11:26; //11:18//11:26; //Zigbee channels
Pw=100; // wifi power
Pz=1; // zigbee power
Xw = []; // wifi channels matrix
Yz = []; // zigbee channels matrix
SIR_w_th = 13; // wifi SIR threshold
SIR_z_th = 13; // zigbee SIR threshold
NE_it_nb=0; // number of iterations to reach NE

// A= Cz x Cw
A=[1 0 0 0 0 0 0 0 0 0 0 0 0 0 0;...
 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0;...
 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0;...
 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0;...
 0 1 1 1 1 0 0 0 0 0 0 0 0 0 0;...
 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0;...
 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0;...
 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0;...
 0 0 0 0 0 1 1 1 1 0 0 0 0 0 0;...
 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0;...
 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0;...
 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0;...
 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0;...
 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1;...
 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1;...
 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1];

```



```

// 1 2 3 4 5 6 7 8 9 10 11 12 13 14
W=[ 0. 0.8 0.6 0.4 0.2 0. 0. 0. 0. 0. 0. 0. 0. 0. ;...
    0.8 0. 0.8 0.6 0.4 0.2 0. 0. 0. 0. 0. 0. 0. 0. ;...
    0.6 0.8 0. 0.8 0.6 0.4 0.2 0. 0. 0. 0. 0. 0. 0. ;...
    0.4 0.6 0.8 0. 0.8 0.6 0.4 0.2 0. 0. 0. 0. 0. 0. ;...
    0.2 0.4 0.6 0.8 0. 0.8 0.6 0.4 0.2 0. 0. 0. 0. 0. ;...
    0. 0.2 0.4 0.6 0.8 0. 0.8 0.6 0.4 0.2 0. 0. 0. 0. ;...
    0. 0. 0.2 0.4 0.6 0.8 0. 0.8 0.6 0.4 0.2 0. 0. 0. ;...
    0. 0. 0. 0.2 0.4 0.6 0.8 0. 0.8 0.6 0.4 0.2 0. 0. ;...
    0. 0. 0. 0. 0.2 0.4 0.6 0.8 0. 0.8 0.6 0.4 0.2 0. ;...
    0. 0. 0. 0. 0. 0.2 0.4 0.6 0.8 0. 0.8 0.6 0.4 0. ;...
    0. 0. 0. 0. 0. 0. 0.2 0.4 0.6 0.8 0. 0.8 0.6 0. ;...
    0. 0. 0. 0. 0. 0. 0. 0.2 0.4 0.6 0.8 0. 0.8 0.4 ;...
    0. 0. 0. 0. 0. 0. 0. 0. 0.2 0.4 0.6 0.8 0. 0.6 ;...
    0. 0. 0. 0. 0. 0. 0. 0. 0. 0.2 0.4 0.6 0.8 0.6 ;...
    0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.4 0.6 0.6 0.];

// Cz=11:26 all channels, Cz_no: non-overlapping channels
Cz_no=list([15:26],...
           [11,16:26],...
           [11,12,17:26],...
           [11:13,18:26],...
           [11:14,19:26],...
           [11:15,20:26],...
           [11:16,21:26],...
           [11:17,22:26],...
           [11:18,23:26],...
           [11:19,24:26],...
           [11:20,25,26],...
           [11:21,26],...
           [11:22],...
           [11:24]);

//Tx, Rx on body's right hip LOS/NLOS positions
//(see paper: Body-to-Body Communications:a Measurement-based Channel Model At 2.45 GHz)
g0=[3.33 -37.88;...
    1.15 -66.33]

function ch_bw = wifi_ch_bandwidth(dist, tx_dBm)
// dist = distance [meter]
//
// Receive Sensitivity
// IEEE 802.11a:
// -88 dBm @ 6 Mbps
// -87 dBm @ 9 Mbps
// -85 dBm @ 12 Mbps
// -83 dBm @ 18 Mbps
// -80 dBm @ 24 Mbps
// -75 dBm @ 36 Mbps
// -73 dBm @ 48 Mbps
// -71 dBm @ 54 Mbps
//
// IEEE 802.11b:
// -95 dBm @ 1 Mbps
// -94 dBm @ 2 Mbps
// -92 dBm @ 5.5 Mbps
// -90 dBm @ 11 Mbps
//
// IEEE 802.11g:
// -90 dBm @ 6 Mbps
// -89 dBm @ 9 Mbps
// -87 dBm @ 12 Mbps
// -85 dBm @ 18 Mbps
// -82 dBm @ 24 Mbps
// -79 dBm @ 36 Mbps
// -76 dBm @ 48 Mbps
// -74 dBm @ 54 Mbps
//
// Free Space Model:
// Pr(d) = (lambda / (4 * pi))^2 * (1 / d)^eta * Pt
// lambda = c / f

// Values of sensitvity are in dBm, therefore I can consider directly the
// Path Loss without correction factors

```

```

sensitivity = [-90 6; -89 9; -87 12; -85 18; -82 24; -79 36; -76 48; -74 54];
rate = 0;
c = 3*10^8;
freq = 2.4*10^9;
eta = 2;
lambda = c / freq;
path_loss = 10 * log10((lambda / (4 * %pi))^2 * (1 / dist^eta)); //negative value

// Rx_Pwr = Tx_Pwr - path_loss - Fading (20 dB)
rx_dBm = tx_dBm + path_loss - 20;

for s=1:size(sensitivity,1)
    if (rx_dBm > sensitivity(s,1))
        rate = sensitivity(s,2);
    end
end
if (rx_dBm <= sensitivity(1,1))
    // SNR too low for establishing a wireless link
    rate = 0;
end

ch_bw = rate;

endfunction

function MobilityModeBBN(r,rf,rs,n,nf,L,ts,vm,Tlim,Tmax,dmax)
timer()
    [n_play,nfin]=MobilityRandom_i_j_nf(n,nf);//connection extremal nodes: player i
    v=vm*rand(1,n);//velocity
    nodex=L*rand(1,n+nf);//current x-coordinate of all nodes
    nodey=L*rand(1,n+nf);//current y-coordinate of all nodes
    destx=L*rand(1,n+nf);//destination x-coordinate of all nodes(not used for fixed nodes)
    desty=L*rand(1,n+nf);//destination y-coordinate of all nodes(not used for fixed nodes)
    d=sqrt((nodex-destx).^2+(nodey-desty).^2);//initialization of the distance vector
    //display the initial state
    MobilityGraph2Plot(nodex(nf+1:$),nodey(nf+1:$),r,5);//mobile nodes in red (5)
    MobilityGraph2Plot(nodex(1:nf),nodey(1:nf),rf,2);//fixed nodes in blue (2)
    f=gcf();//get the figure properties
    i=n_play-nf;//emission node in purple (6): player i
    f.children.children($-1).children(n-i+1).data(3:4)=[rs rs];//node i
    f.children.children($-1).children(n-i+1).foreground=6;//node i
    f.children.children($-1).children(n-i+1).background=6;//node i
    drawnow();//display
    t=0;
    Tnodes=zeros(1,n);//initialization of breaking time parameters
    he=[];//link head vector
    ta=[];//link tail vector =nbr of Wifi links

while (t<Tlim) //observation over time epochs t+5 till Tlim

    B=list();
    B(1)=[]; B(2)=[]; B(3)=[]; B(4)=[];
    b=[];
    mt_w_l=[];
    d_link=0;
    g_wv=[];
    g_zw=[];
    g_zz=[];

for i=1:n
    fr=f.children.children($-1).children(n-i+1);//node i
    //displacement of the node i
    [fr.data(1) fr.data(2) destx(i) desty(i) d(i) v(i) Tnodes(i)]=
    MobilityNodeRWP(fr.data(1),fr.data(2),destx(i),desty(i),d(i),v(i),Tnodes(i),Tmax,vm,L);
end

if (length(he)<>0)//presence of network links
//remove old links before the performance of the current topology
delete(f.children.children(1:$-3));

end
[nodx,nodey]=MobilityXYExtraction(f,n,nf);//extraction of the nodes coordinates
[ta,he]=MobilityLocality(nodx,nodey,dmax);//topology performance
//calculation of the shortest path between the connection nodes n_play and nfin
[dist,pred]=MobilityDijkstra(nodx,nodey,he,ta,n_play);
[mx my]=min(dist(1:nf));
[path]=RoutingPredRoute(pred,dist,n_play,my);

// positioning of WBANs within BBNS
for i=1:(n+nf)
    if nodx(i)< L/2 & nodey(i)< L/2 then 113
        B(1)=[B(1) i]; b(i)=1;
    elseif nodx(i)< L/2 & nodey(i)>= L/2 then
        B(2)=[B(2) i]; b(i)=2;
    elseif nodx(i)>= L/2 & nodey(i)>= L/2 then
        B(3)=[B(3) i]; b(i)=3;
    else
        B(4)=[B(4) i]; b(i)=4;
    end
end
end

```

```

// Wifi links within each BBN
tot_link=0;
tmp_link=eye(n+nf,n+nf)
for i=1:(n+nf-1)
    for j=(i+1):(n+nf)
        if b(i)==b(j) then
            d_link = sqrt((nodx(i)-nodx(j)).^2 + (nody(i)-nody(j)).^2);
            ch_bw = wifi_ch_bandwidth(d_link, wifi_dBm)
            if(ch_bw > 0)
                tmp_link(i,j)=1;
                tmp_link(j,i)=1;
                tot_link = tot_link+1;
                mt_w_l = [mt_w_l ; i j b(i)] // b(i)=b(j)
            end
        end
    end
end
//calculate Wifi-Wifi gains, select randomly LOS or NLOS position for each link
for k=1:(tot_link-1)
    for j=(k+1):tot_link
        d_link=sqrt((nodx(mt_w_l(k,1))-nodx(mt_w_l(j,1))).^2 + (nody(mt_w_l(k,2))-nody(mt_w_l(j,2))).^2);
        n_pos = round(rand(1)*1)+1;
        g_db = g0(n_pos,2) - 10 * g0(n_pos,1) * log10(d_link/d0);
        g_ww(k,j)=10^(g_db/10);
        g_ww(j,k)=g_ww(k,j);
    end
end
//calculate Zigbee-Wifi gains for all WBANs zigbee channels
for k=1:(n+nf)
    for j=1:tot_link
        d_link=sqrt( (nodx(k)-nodx(mt_w_l(j,1))).^2 + (nody(k)-nody(mt_w_l(j,2))).^2);
        n_pos = round(rand(1)*1)+1;
        g_db = g0(n_pos,2) - 10 * g0(n_pos,1) * log10(d_link/d0);
        g_zw(k,j)=10^(g_db/10);
    end
end
//calculate Zigbee-Zigbee gains
for k=1:(n+nf-1)
    for j=(k+1):(n+nf)
        d_link=sqrt((nodx(k)-nodx(j)).^2+(nody(k)-nody(j)).^2);
        n_pos = round(rand(1)*1)+1;
        if d_link==0 then
            end
            g_db = g0(n_pos,2) - 10 * g0(n_pos,1) * log10(d_link/d0);
            g_zz(k,j)=10^(g_db/10);
            g_zz(j,k)=g_zz(k,j);
        end
    end
end
// calculate g_ww(l,l) wifi gain of all players
for l=1:(n+nf)
    g_ww(l,l) = 0
    for k=1:tot_link
        if mt_w_l(k,1)==l | mt_w_l(k,2)==l then
            d_g = sqrt((nodx(mt_w_l(k,1))-nodx(mt_w_l(k,2))).^2+(nody(mt_w_l(k,1))-nody(mt_w_l(k,2))).^2);
            n_pos = round(rand(1)*1)+1;
            g_db = g0(n_pos,2) - 10 * g0(n_pos,1) * log10(d_g/d0);
            g_ll_tmp=10^(g_db/10);
            if g_ll_tmp < g_ww(l,l) | g_ww(l,l) == 0 then
                g_ww(l,l) = g_ll_tmp;
            end
        end
    end
end
end
//calculate g_zz(h,h) Zigbee gain of all players
for h=1:(n+nf)
    d_g = 1; //assumption (Stefano)
    n_pos = round(rand(1)*1)+1;
    g_db = g0(n_pos,2) - 10 * g0(n_pos,1) * log10(d_g/d0);
    g_zz(h,h)=10^(g_db/10);
end
// Select delegates of BBNs
L_deleg = []; // Matrix of delegates WiFi links
for i=1:4
    deleg = 0;
    deleg_rand=[];
    n_deleg=[];
    if size(B(i),2)>0
        for j=B(i)
            for k=1:tot_link
                if mt_w_l(k,1)==j
                    n_deleg=[n_deleg j];
                end
            end
        end
    end
end
end

```

```

if size(n_deleg,2)>0
    deleg_rand = grand(1,'prm',n_deleg');
    deleg = deleg_rand(1);
end
g_ww_worst=0;
if deleg<>0
    for k=1:(tot_link)
        if mt_w_l(k,1)==deleg
            if g_ww_worst==0 | g_ww(k,k) < g_ww_worst
                g_ww_worst = g_ww(k,k);
                L_deleg(i,1)=mt_w_l(k,1);
                L_deleg(i,2)=mt_w_l(k,2);
                L_deleg(i,3)=mt_w_l(k,3);
                L_deleg(i,4)=g_ww_worst;
                L_deleg(i,5)=k;
            end
        end
    end
end // END select delegates
// Initialization: Random Xw and Yw

Xw=Initial_W_Alloc(L_deleg, B, b, Xw);
Yz=Initial_Z_Alloc(L_deleg, B, b, Yz);

//*****
//***** BR-SIM *****
//*****
S_w_0=linspace(0, 0, n+nf);
S_w_1=linspace(0, 0, n+nf);
S_z_0=linspace(0, 0, n+nf);
S_z_1=linspace(0, 0, n+nf);

for i=1:(n+nf)
    for c=Cw
        if Xw(i,c)==1
            S_w_0(i)=c; // vecteur initial des stratégies Wifi
            for j=1:tot_link
                if mt_w_l(j,1)==i
                    IFw_0(j) = IF_w_func(j,Xw,Yz,c);
                end
            end
        end
    end
    for c=Cz
        if Yz(i,c-10)==1
            S_z_0(i)=c-10; // vecteur initial des stratégies zigbee
        end
    end
end

S_w_1 = S_w_0;
S_z_1 = S_z_0;

// Nash Equilibrium for WiFi stage
//Dynamics of SIRw at initial random status
for i=1:size(L_deleg,1) //analysis by each BBN
    sum_SIRw=0;
    nb_links= 0;
    for j=B(i) // average SIRw by each BBN
        SIRw(j) = SIR_w_func(j, Xw, Yz);
        sum_SIRw = sum_SIRw + SIRw(j);
        nb_links= nb_links+1;
    end
    Avg_SIRw(i) = sum_SIRw/nb_links;
end

while (NE<size(L_deleg,1))
    NE=0;
    for l=1:size(L_deleg,1) // l= delegate link of BBN l =(Tx,Rx)=(L_deleg(l,1), L_deleg(l,2))
        IFw_tmp=0;
        IFw = 0;
        if L_deleg(l,1) <> 0 // we have at least one established link in BBN l
            for c1=Cw // argmin IFw
                IFw_tmp = IF_w_func(L_deleg(l,5),Xw,Yz,c1);
                if IFw_tmp < IFw_1(L_deleg(l,1))
                    IFw_1(L_deleg(l,1))=IFw_tmp;
                    S_w_1(L_deleg(l,1))=c1;
                end
            end
            Xw(L_deleg(l,1), S_w_1(L_deleg(l,1)))=1;
            for j=B(l) //allocate c1 to all WBANs under BBN l.
                Xw(j,S_w_1(L_deleg(l,1)))=1;
                for c_null=Cw
                    if c_null<>S_w_1(L_deleg(l,1))
                        Xw(j,c_null)=0;
                    end
                end
            end
        end
    end
end // loop on representative links (delegates)

```

```

//Dynamics of SIRw
for i=1:size(L_deleg,1) //analysis by each BBN
sum_SIRw=0;
nb_links=0;
if L_deleg(i,1) <> 0
    for j=B(i) // average SIRw by each BBN
        SIRw(j) = SIR_w_func(j, Xw, Yz);
        sum_SIRw = sum_SIRw + SIRw(j);
        nb_links= nb_links+1;
    end
Avg_SIRw(i) = sum_SIRw/nb_links;
end
end

tau=tau+1;
end //while

sum_sirw_epoch=0;
for i=1:size(Avg_SIRw,1) //at NE
sum_sirw_epoch = sum_sirw_epoch + Avg_SIRw(i);
end
Avg_SIRw_epoch(t/10+1)=sum_sirw_epoch/size(Avg_SIRw,1);

printf("_____ WiFi Nash REACHED _____\n");

// Nash Equilibrium for ZigBee stage
while (NE<(n+nf))
NE=0;

for p=1:(n+nf) // loop on all WBANS
IFz_tmp=0;
for c=Cw
    if Xw(p,c)=1
        c1=c;
    end
end
//argmin IFz, select Zigbee channel non overlapping with WiFi channel
for c2=Cz_no(c1)
    IFz_tmp = IFz_z_func(p,Xw,Yz,c2);
    if IFz_tmp < IFz_1(p)
        IFz_1(p)=IFz_tmp;
        if IFz_1(p) < IFz_0(p)
            S_z_1(p)=c2-10;
        else
            IFz_1(p)=IFz_0(p);
            S_z_1(p)=S_z_0(p);
        end
    end
end
Yz(p, S_z_1(p))=1;
for c_null=Cz
    if c_null-10<>S_z_1(p)
        Yz(p,c_null-10)=0;
    end
end
end // loop on WBANS/players

//Dynamics of SIRz
for i=1:size(L_deleg,1) //analysis by each BBN
sum_SIRz=0;
nb_links=0;
for j=B(i) // average SIRz by each BBN
    SIRz(j) = SIR_z_func(j, Xw, Yz, S_z_1(j)+10);
    if SIRz(j)<>0
        sum_SIRz = sum_SIRz + SIRz(j);
        IN_MT = IN_MT + 10*log10(g_zz(j)*Pz) - SIRz(j);
        nb_links= nb_links+1;
    end
end
end

tau=tau+1;
end //while
printf("\n_____ ZigBee Nash REACHED _____\n\n");

//***** END BR-SIM *****
//*****

```

```

//display the network links
if (path<>[]) then
    l = [n_play,path(length(path)-1)]; //Wifi link
end
h=n_play; //Zigbee link

for k=1:length(he)
    if (he(k)<>h) then
        distg_z(k)=sqrt((nodx(h)-nodx(he(k))).^2+(nody(h)-nody(he(k))).^2);
    end
end

for j=1:tot_link
    xpolys([nodx([mt_w_l(j,1) mt_w_l(j,2)])+r/2]',[nody([mt_w_l(j,1) mt_w_l(j,2)])-r/2]',1);
end

drawnow();//display the graph
t=t+10;//time increment : time epoch = 10ms

end // while(t<Tlim)

endfunction //MobilityModeBBN

//***** BR-SIM functions *****//

function SIRw = SIR_w_func(p, Xw, Yz)

// channel c1 of player p
for c=Cw
    if Xw(p,c) == 1
        c1=c;
    end
end

// wifi link of player p
g_ww_worst==0
for k=1:(tot_link)
    if mt_w_l(k,1)==p
        if g_ww_worst==0 | (g_ww(k,k) < g_ww_worst & g_ww(k,k)<>0)
            g_ww_worst = g_ww(k,k);
            L_p = [mt_w_l(k,1) mt_w_l(k,2) mt_w_l(k,3) g_ww_worst k];
        end
    end
end

// set of neighbors of player p
W_l_w = set_w_neighbors(p); //[[Tx Rx BBN n°link]
W_l_z = set_z_neighbors(p); //[[WBAN BBN]

if size(W_l_w,1)>0
    for k=1:size(W_l_w,1)
        if Xw(W_l_w(k,1),c1) == 1
            Iw_c1 = Iw_c1 + g_ww(L_p(5), W_l_w(k,4)) * Pw; // n° links
        else
            for c=Cw
                if Xw(W_l_w(k,1),c) == 1
                    c_k = c;
                end
            end
            if c_k<>0 & W(c1, c_k)<>0
                Iww = Iww + W(c1,c_k) * g_ww(L_p(5), W_l_w(k,4)) * Pw;
            end
        end
    end
end

if size(W_l_z,1)>0
    for j=1:size(W_l_z,1)
        for c=Cz-10
            if Yz(W_l_z(j,1),c) == 1
                c_k = c;
            end
        end
        if A(c_k, c1) == 1
            Iwz = Iwz + g_zw(W_l_z(j,1), L_p(5)) * Pz;
        end
    end
end

SIRw = 10*log10(g_ww(L_p(1),L_p(1))*Pw/(Iw_c1+Iww+Iwz));

endfunction

```

```

function SIRz = SIR_z_func(p, Xw, Yz, c2)
// set of neighbors of player p
Z_h_w = set_w_neighbors(p); //[Tx Rx BBN n°link]
Z_h_z=set_z_neighbors(p); //[WBAN BBN]

if size(Z_h_z,1)>1
for k=1:size(Z_h_z,1)
if Yz(Z_h_z(k,1),c2-10) == 1
Iz_c2 = Iz_c2 + g_zz(h, Z_h_z(k,1)) * Pz;
end
end
end
if size(Z_h_w,1)>0
for j=1:size(Z_h_w,1)
for c=Cw
if Xw(Z_h_w(j,1),c) == 1
c_k = c;
end
end
if A(c2-10, c_k) == 1
Iwz = Iwz + g_zw(p, Z_h_w(j,4)) * Pw;
end
end
end
SIRz = 10*log10(g_zz(p,p)*Pz/(Iz_c2+Iwz));
endfunction

function [Z_h_z] = set_z_neighbors(p)
Z_h_z=[];
for i=1:(n+nf) // search for interfering zigbee links
r1= sqrt((nodx(p)-nodx(i)).^2 + (nody(p)-nody(i)).^2); // distance to the WBAN i
if r1 < RIz
Z_h_z=[Z_h_z; i b(i)]; //[WBAN BBN]
end
end
Z_h_z=Z_h_z;
endfunction

function [W_l_w] = set_w_neighbors(p)
W_l_w=[];
for i=1:tot_link // search for interfering wifi links
r1= sqrt((nodx(p)-nodx(mt_w_l(i,1))).^2 + (nody(p)-nody(mt_w_l(i,1))).^2);
r2= sqrt((nodx(p)-nodx(mt_w_l(i,2))).^2 + (nody(p)-nody(mt_w_l(i,2))).^2);
if r1 < RIz | r2 < RIz
W_l_w=[W_l_w; mt_w_l(i,1) mt_w_l(i,2) mt_w_l(i,3) i]; //[Tx Rx BBN n°link]
end
end
//end
W_l_w=W_l_w;
endfunction

function [Xw]=Initial_W_Alloc(L_deleg, B, b, Xw)
for i=1:4
c_rand=grand(1,'prm',Cw');
c=c_rand(1);
for j=B(i)
Xw(j,c)=1;
for c_null=Cw
if c_null<>c
Xw(j,c_null)=0;
end
end
end
if c<>size(Cw,2) // fill in the matrix till last column
Xw(j,size(Cw,2))=0;
end
end
Xw=Xw;
endfunction

function [Yz]=Initial_Z_Alloc(L_deleg, B, b, Yz)
for i=1:(n+nf)
c_rand=grand(1,'prm',Cz');
c=c_rand(1)-10;
Yz(i,c)=1;
for c_null=Cz
if c_null-10<>c
Yz(i,c_null-10)=0;
end
end
if c <> size(Cz,2)
Yz(i,size(Cz,2))=0;
end
end
end
Yz=Yz;
endfunction

```

A.2 SORT-SIM algorithm Scilab source code

```

//*****
//***** SORT-SIM algorithm for WBAN i=(l,h) *****
//***** Author: Amira Meharouech *****
//***** December 2014 *****
//*****

//*****
//***** Inputs: Initialization *****
//*****

//Please refer to the Input: Initialization section of BR-SIM algorithm

//*****
//***** SORT-SIM *****
//*****
S_w_0=linspace(0, 0, n+nf);
S_w_1=linspace(0, 0, n+nf);
S_z_0=linspace(0, 0, n+nf);
S_z_1=linspace(0, 0, n+nf);

for i=1:(n+nf)
    for c=Cw
        if Xw(i,c)==1
            S_w_0(i)=c; // vecteur initial des stratégies Wifi
        end
    end
    for c=Cz
        if Yz(i,c-10)==1
            S_z_0(i)=c-10; // vecteur initial des stratégies zigbee
        end
    end
end

S_w_1 = S_w_0;
S_z_1 = S_z_0;

// Nash Equilibrium for WiFi stage

for l=1:size(L_deleg,1) // l= delegate link of BBN l =(Tx,Rx)
//Calculate set of neighbors
W_l_w(l)=set_w_neighbors(l); //[Tx Rx BBN n°link]
W_l_z(l)=set_z_neighbors(l); //[WBAN BBN]

//Calculate Cw_free
Cw_free(l)=[];
for c=Cw
    free = 1;
    if size(W_l_w(l),1)>0
        for k=size(W_l_w(l),1)
            if Xw(W_l_w(l)(k,1),c) == 1
                free = 0;
            end
        end
    end
    if free == 1
        Cw_free(l) = [Cw_free(l) c];
    end
end
end //loop delegates

```



```

//SORT
if size(Cw_free(l),1)>0
c1_rand = grand(1,'prm',Cw_free(l));
c1 = c1_rand(1);
Alloc(c1)=1;
SIRw_sort(L_deleg(l,1)) = SIR_w_func(L_deleg(l,1), Xw, Yz);
    if (SIRw_sort(L_deleg(l,1)) > SIRw_1(L_deleg(l,1)))
        SIRw_1(L_deleg(l,1)) = SIRz_sort(L_deleg(l,1));
        if SIRw_1(L_deleg(l,1)) > SIRw_0(L_deleg(l,1))
            S_w_1(L_deleg(l,1)) = c1;
            Alloc(c1)=1;
        else
            SIRw_1(L_deleg(l,1)) = SIRw_0(L_deleg(l,1));
            S_w_1(L_deleg(l,1)) = S_w_0(L_deleg(l,1));
        end
    end
else
printf("No free wifi channels\n");

//Calculate Cw_th
for c1=Cw
    SIR_w = SIR_w_func(L_deleg(l,1), Xw, Yz);
    if SIR_w > SIR_w_th
        Cw_th = [Cw_th ; SIR_w c1];
        sir(c1)=SIR_w;
    end
end

if size(Cw_th, 2)>0
c1_rand = grand(1,'prm',Cw_th(:,2));
c1 = c1_rand(1);
SIRw_sort(L_deleg(l,1))=sir(c1);
    if (SIRz_sort(L_deleg(l,1)) > SIRz_0(L_deleg(l,1)))
        S_w_1(L_deleg(l,1)) = c1;
        SIRw_1(L_deleg(l,1)) = SIRw_sort(L_deleg(l,1));
        Z_Alloc(c1)=1;
    else
        S_w_1(L_deleg(l,1)) = S_w_0(L_deleg(l,1));
        SIRw_1(L_deleg(l,1)) = SIRw_0(L_deleg(l,1));
    end
end

end //SORT

end // loop on representative links (delegates)

//Dynamics of SIRw
for i=1:size(L_deleg,1) //analysis by each BBN
sum_SIRw=0;
nb_links=0;
    for j=B(i) // average SIRw by each BBN
        SIRw(j) = SIR_w_func(j, Xw, Yz);
        if SIRw(j) > SIR_w_th
            sum_SIRw = sum_SIRw + SIRw(j);
            nb_links= nb_links+1;
        end
    end
    Avg_SIRw(i) = sum_SIRw/nb_links;
end
printf("_____ WIFI NE reached _____\n");

// Nash Equilibrium for ZigBee stage

// loop on all Zigbee links to calculate Cz_h(h), set of neighbors and Cz_free(h)
for h=1:(n+nf)
Z_h_w(h)=set_w_neighbors(h);
Z_h_z(h)=set_z_neighbors(h);

//Calculate Cz_h(h) from Cz_no(c1), depending on used channels Cz
for c=Cw
    if Xw(h,c)==1 //Xw
        c1 = c;
    end
end

if c1==0
    Cz_free(h) = Cz;
else

```

```

    for c=Cz_no(c1)
        for c_available=Cz
            if c == c_available
                Cz_h(h) = [Cz_h(h) c];
            end
        end
    end
end

//Calculate Cz_free(h)
for c=Cz_h(h)
    free = 1;
    if size(Z_h_z(h),1)>0
        for k=size(Z_h_z(h),1)
            if Yz(Z_h_z(h)(k,1),c-10) == 1
                free = 0;
            end
        end
    end
end

if free == 1
    Cz_free(h) = [Cz_free(h) c];
end
end
end //if c1==0

end //loop on all zigbee links (Sets calculated)
//Allocate ZigBee channels, sub-optimal randomized trials=iterations
while (NE<(n+nf))
    NE=0;

    for p=1:(n+nf) // loop on all WBANS

        for c=Cw
            if Xw(p,c)=1
                c1=c;
            end
        end

        //au lieu d'une boucle, on va choisir un canal randomly si available free ou > SIRth
        //si le nouveau SIR > à la valeur précédente on le prend

        if size(Cz_free(p),1)>0 //SORT
            c2_rand = grand(1,'prm',Cz_free(p));
            c2 = c2_rand(1);
            SIRz_sort(p) = SIR_z_func(p, Xw, Yz, c2);
            if (SIRz_sort(p) > SIRz_1(p))
                SIRz_1(p) = SIRz_sort(p);
                if SIRz_1(p) > SIRz_0(p)
                    S_z_1(p) = c2-10;
                    Alloc(c2)=1;
                else
                    SIRz_1(p) = SIRz_0(p);
                    S_z_1(p) = S_z_0(p);
                end
            end
        else
            printf("No free zigbee channels\n");
        end
        //Calculate Cz_th
        for c2=Cz_h(p)
            SIR_z = SIR_z_func(p, Xw, Yz, c2);
            if SIR_z > SIR_z_th
                Cz_th = [Cz_th ; SIR_z c2];
                sir(c2)=SIR_z;
            end
        end
    end // calculate Cz_th

    if size(Cz_th, 2)>0
        c2_rand = grand(1,'prm',Cz_th(:,2));
        c2 = c2_rand(1);
        SIRz_sort(h)=sir(c2);
        if (SIRz_sort(h) > SIRz_0(p))
            S_z_1(p) = c2-10;
            SIRz_1(p) = SIRz_sort(p);
            Z_Alloc(c2-10)=1;
        else
            S_z_1(p) = S_z_0(p);
            SIRz_1(p) = SIRz_0(p);
        end
    end
end //SORT

```

```
//Dynamics of SIRz
for i=1:size(L_deleg,1) //analysis by each BBN
sum_SIRz=0;
nb_links=0;
    for j=B(i) // average SIRz by each BBN
        SIRz_0(j) = SIR_z_func(j, Xw, Yz, S_z_1(j)+10);
        if SIRz_0(j)>0
            sum_SIRz = sum_SIRz + SIRz_0(j);
            IN_MT = IN_MT + 10*log10(g_zz(j)*Pz) - SIRz_0(j);
            nb_links= nb_links+1;
        end
    end
    Avg_SIRz(i) = sum_SIRz/nb_links;
    IN_MT = IN_MT/nb_links;
end
printf("\n_____ ZIGBEE Nash reached _____\n\n");

//***** END SORT-SIM *****/
//*****

//display the network links

// For the rest of the program, please refer to the corresponding sections in
// BR-SIM algorithm.
```

A.3 BB-LAR Castalia configuration file (omnetpp.ini)

```

[General]
# =====
# Always include the main Castalia.ini file
# =====
include ../Parameters/Castalia.ini

sim-time-limit = 2000s

SN.field_x = 200 # meters
SN.field_y = 200 # meters

SN.numNodes = 100
include node_locations.ini

SN.node[*].ResourceManager.initialEnergy = 18720

SN.wirelessChannel.pathLossMapFile = "../Parameters/WirelessChannel/BANmodels/pathLossMap.txt"
SN.wirelessChannel.temporalModelParametersFile = "../Parameters/WirelessChannel/BANmodels/TemporalModel.txt"
SN.wirelessChannel.onlyStaticNodes = false

SN.node[*].ResourceManager.baselineNodePower = 0
SN.node[*].Communication.Radio.RadioParametersFile = "../Parameters/Radio/BANRadio.txt"
SN.node[*].Communication.Radio.TxOutputPower = "-15dBm"

SN.node[*].Communication.RoutingProtocolName = "BBLARRouting"
SN.node[*].Communication.Routing.neighbor_RSSIThreshold = -89.3 # in dBm

SN.node[*].Communication.MACProtocolName = "Mac802154"
SN.node[*].Communication.MAC.phyDataRate = 1024

SN.node[*].ApplicationName = "ThroughputTest"
SN.node[*].Application.startupDelay = 1 #wait for 1sec before starting sending packets
SN.node[*].Application.packet_rate = 5

# =====
# WBANs mobility configuration
# We assume that all WBANs are moving to the emergency issue
# at point (x,y)=(200,200)
# =====

SN.node[*].MobilityManagerName = "LineMobilityManager"
SN.node[*].MobilityManager.updateInterval = 100
SN.node[*].MobilityManager.xCoordDestination = 200
SN.node[*].MobilityManager.yCoordDestination = 200
SN.node[*].MobilityManager.zCoordDestination = 0
SN.node[*].MobilityManager.speed = 2 # m/s

[Config VaryHealthStatus]
SN.node[*].Application.priority = ${H=1,2,3}

```