Data Communication Algorithms for Emerging Wearable and Urban Sensing Networks

Dhafer Ben Arbia

Polytechnic School of Tunisia
Qatar Mobility Innovations Center

Doctoral Thesis

Data Communications Algorithms for Emerging Wearable and Urban Sensing Networks

Author
Dhafer Ben Arbia

Supervisors
Prof. Rabah Attia
Dr. Elyes Ben Hamida

Jury

Prof. Mohamed JMAIEL	Head of The Digital Research Centre of Sfax - Tunisia	President
Dr. Fethi TLILI	Associate Professor at SUPCOM - Tunisia	Reviewer
Dr. Fethi FILALI	Head of Applied Research and Technology - QMIC - Qatar	Reviewer
Prof. Rabah ATTIA	Professor at EPT - Tunisia	Thesis Supervisor
Prof. Ridha BOUALLEGUE	Professor at SUPCOM - Tunisia	Examiner
Dr. Takoua ABDELLATIF	Assistant Professor at EPT - Tunisia	Invited Member
Dr. Elyes BEN HAMIDA	R&D & Innovation Manager at IRT SystemX - Paris - France	Thesis Co-Supervisor

A thesis submitted and defended in fulfillment of the requirements for the degree of Philosophiae Doctor (PhD)

in

Electronic, Information and Communication Technologies

June 8, 2018

Declaration of Authorship

I, Dhafer Ben Arbia, declare that this thesis titled, "Data Communications Algorithms for Emerging Wearable and Urban Sensing Networks" and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at Polytechnic School of Tunisia and Qatar Mobility Innovations Center.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

Date:

Version of the manuscript: v1.36

Contact Email: dhafer.benarbia [at] gmail.com

Polytechnic School of Tunisia

Abstract

Philosophiae Doctor (PhD)

Data Communications Algorithms for Emerging Wearable and Urban Sensing Networks

by Dhafer Ben Arbia

Emerging wearable wireless networks (WWNs) are evolving along with the ubiquitous technologies and standards. WWNs are not only used for health-care monitoring, but also in smart home and energy technologies, personal and public security, traffic and transport, environment sensing and industrial controlling. With the recent advances in Industrial Internet-of-Things (IIoT) and Big Data, WWNs have become a key enabling technology to complete the automation chain through which data is collected, transmitted, recorded and analyzed. Moreover, WWNs have been seen as an efficient candidate to substitute wireless networks when networking infrastructures are missing. Obviously, during a disaster, the wireless infrastructure networks are either damaged or over-saturated, however, rescue operations communications must rely on a reliable tactical deployable networks to cover the operations area. To that end, the WWNs could play a key role in establishing a tactical disaster relief wireless network. The established network grants disaster relief operations monitoring (i.e., deployed rescue teams and victims vital signs, air intoxication, ambient temperature, etc.). It enables also remote operations assistance from distant command center (CC) to the deployed rescuing forces (i.e., medical teams, military, police, firefighters, etc.). In this context, an efficient routing approach is important to grant data communication from CC and deployed rescue teams and vice-versa. The scope of this thesis is to address this concern with regards to the disaster relief missions operational and technical requirements. This thesis aims at: First, to study the state-of-the-art of the data communication algorithms in WWNs. Second, to implement and evaluate the existing approaches in order to conclude their limitations for this context. Third, to propose a new communication approach specifically designed for harsh environment and disaster relief operations. Fourth, to evaluate the proposed approach and compare its behavior to the existing routing approaches and validate it by simulation. Finally, to implement the new proposal on real devices as a proof of concept to validate it on a real test-bed within realistic conditions. This thesis was a part of the CROW^2 project conducted by Qatar Mobility Innovations Center and the French Alternative Energies and Atomic Energy Commission (CEA) - Laboratory of Electronics and Information Technology (LETI), over more than three years in order to propose a complete disaster relief reliable communication solution.

Acknowledgements

Firstly, I would like to express my sincere gratitude to my advisors Prof. Rabah Attia and Dr. Elyes Ben Hamida for their continuous support during my Ph.D study and related research, for their patience, motivation, and immense knowledge. Their guidance helped me in all the time of research and writing of this thesis.

Besides my advisors, I would like to thank Dr. Muhammad Mahtab Alam, Associate Professor and ERA-Chair in Tallinn University - Estonia, for his insightful comments, encouragement and support. He was always here for asking the hard questions which helped me to widen my research from various perspectives.

I am deeply grateful to all the members of the jury for agreeing to read the manuscript and to participate in the defense of this thesis: Prof. Mohamed Jmaeil, President of the jury, Dr. Fethi Tlili, reviewer, Dr. Fethi Filali, reviewer, Prof. Ridha Bouallegue, examiner, Dr. Takoua Abdellatif, invited member.

To my dear mother Zakia and to my beloved father Mohammed Bechir who passed away in 2009... I miss you dad.

I would also thank my friends Walid SIDHOM and Belhassen Saddedi for their support during all the three years of my absence overseas.

Last but not the least, I would like to thank my brothers Anis and Achraf and my sisters Hanen and Abir for supporting me spiritually throughout my life in general.

This work was made technically and financially possible by Polytechnic School of Tunisia (EPT), Qatar Mobility Innovations Center (QMIC) and Qatar National Research Fund (QNRF).

Logic will get you from A to B,
Imagination will take you everywhere.

ALBERT EINSHTEIN

Contents

List of Figures

List of Tables

List of Abbreviations

BAN	**B**ody **A**rea **N**etwork
BBN or B2B	**B**ody to **B**ody **N**etwork
BER	**B**it **E**rror **R**ate
BLE	**B**luetooth **L**ow **E**nergy
CC	**C**ommand **C**enter
DBPSK	**D**ifferential **B**inary **P**hase **S**hift **K**eying
DQPSK	**D**ifferential **Q**uadrature **P**hase **S**hift **K**eying
IoT	**I**nternet **O**f **T**hings
IoE	**I**nternet **O**f **E**veryhing
LOS	**L**ine **O**f **S**ight
MAC	**M**edium **A**ccess **C**ontrol layer
NB	**N**arrow **B**and
NLOS	**N**on **L**ine **O**f **S**ight
ORACE-Net	**O**ptimized **R**outing **A**pproach **C**ritical **E**mergency **Net**works
PER	**P**acket **E**rror **R**at
PRR	**P**acket **R**eception **R**ate
PHY	**P**hysical layer
PSN	**P**ublic **S**afety **N**etworks
TG	**T**ask **G**roup
UWB	**U**ltra **W**ide **B**and
WBAN	**W**ireless **B**ody **A**rea **N**etwork
WLAN	**W**ireless **L**ocal **A**rea **N**etwork
WSN	**W**ireless **S**ensor **N**etworks
WSNET	**W**ireless **S**ensor **N**etworks simulator
WWN	**W**earable **W**ireless **N**etworks

This thesis is dedicated to the source of my inspiration, my wife ***Imen****, and my lovely kids* ***Myriam****,* ***Maram*** *and* ***Adam*** *for all their love, support and sacrifices.*

Chapter 1

General Introduction

1.1 Context and motivations

According to the United Nations Office of Disaster Risk Reduction (UNISDR), the financial impact due to natural and man-made disasters are paramount. It is reported that by 2030, the global average of annual losses due to disasters is forecasted to increase and reach 415 billion USD [1]. Most of these losses are due to the damage and/or the over-saturation of the communication infrastructure systems which delays the search and rescue (S&R) operations and makes the decision makers without any visibility on the situation for hours or even for days. According to The Guardian newspaper [2], a "rapid succession of disaster events from January 1st till July 7th 2017 was part of a years-long increase and cost a total of 16 billion USD", going from California flooding in February to hurricane Harvey mid-August. During the latter catastrophe, trapped victims whose still connected to available Base Transceiver Station (BTS) by chance, shared their locations through social media to be reached by the S&R teams within few hours. However, 11 disconnected victims, from a total of 57 deaths, died despite their closeness to the S&R command center but they were out-of-range of any wireless network. It is perceived that these estimated losses are subject to decrease if preventive communication alternatives are ready to be triggered when a disaster occurs. In fact, all emergency and disaster relief responders (i.e., non-government organizations, government bodies and the individuals that work for them providing relief and support during and after natural disasters) and research & development task forces were studying, testing and deploying S&R wireless communication systems. However, based on the diversity of the risk nature basically related to the location of the studied area/country, it is challenging to issue a common standard for all kinds of disasters and threats.

At this point, it is envisioned that Wearable Wireless Networks (WWNs) could play a key role in collecting real-time data from the disaster area [3]. Indeed, WWNs or Wireless Body Area Networks (WBANs) have lately emerged as a key enabling technologies in various kinds of applications, including critical and rescue operations [3], remote monitoring [4], mobile health-care [5], security and authentication [6], sports and entertainment, etc. A Wearable Wireless Sensor Network (or WBAN) consists of one or more intelligent and self-powered sensor devices which can be either sticked on-body, or injected subcutaneous into, humans (or animal or plant) bodies to monitor their vital signs (e.g., cardiogram, blood pressure, stress-level, temperature, oxygen level in the blood, etc.) and motion (e.g., posture, heading, speed, location, etc.); In addition to the sensing devices, a BAN coordinator (i.e., using On-Body / Intra-BANs communications) collects the sensed data and report them back to a distant monitoring or command center for data processing/analysis and decisions making, as depicted by Figure 1.1. The BAN coordinator is generally considered as a resources-rich (i.e., battery, communication range, etc.) device that can interconnect

the on-body sensors to external network infrastructures such as static WSNs, WiFi Access Points or Broadband Cellular Networks (e.g., 4G, 5G, etc.) [7]. The inter-BANs (or Body-to-Body) network could also use the wireless deployed devices (i.e., S&R teams equipments and trapped victims mobile phones) to establish a tactical ad hoc wireless emergency network to grant network extensibility in the victims surrounding areas. Establishing such wireless network allows the decision makers in the command center (CC) to conduct distantly the operations and get feedback of their deployed manpower during and after the disaster.

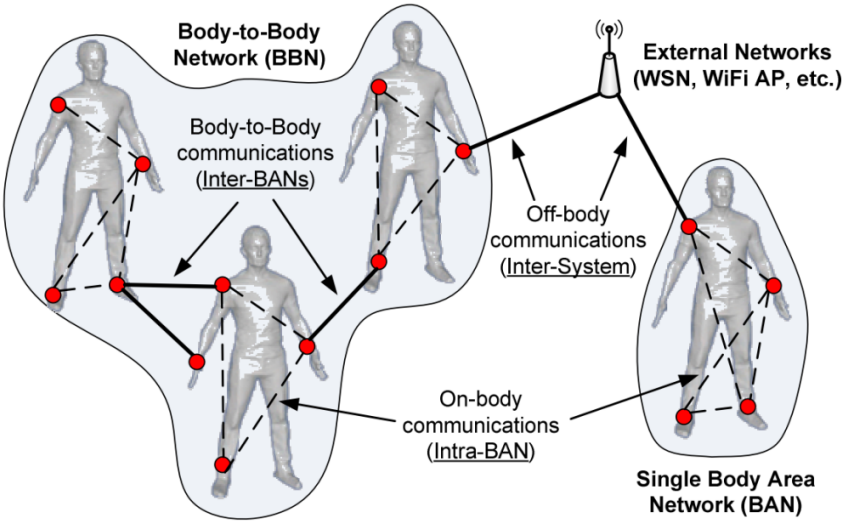


FIGURE 1.1: Wireless Body Area Network (WBAN) and Body-to-Body Network (BBN or B2B) [8].

In fact, in case of infrastructure networks fail (i.e., unavailability, damage, out-of-range), BAN coordinators and/or BAN sensors could rely on cooperative and multi-hoping communications to extend the end-to-end network connectivity (i.e., using Body-to-Body / Inter-BANs Communications). A self-organizing and dynamic Body-to-Body Network (BBN or B2B) will be formed to ensure the end-to-end communications.

The IEEE 802.15.6 task group (TG6) [9] has been established to provide an international standard for BANs. Most of the research efforts have so far been devoted to the design of both contention based (e.g., CSMA/CA, Aloha, etc.) and time division-based (e.g., TDMA) Medium Access Control (MAC) protocols, and Physical (PHY) layers (Narrowband, Ultra Wideband and Human Body Communications) providing efficient communication links for use in close proximity to, or inside, human bodies.

Despites their particularity and specificity especially in terms of requirements, WBANs are relying on existing radio technologies for the design of short-term and ready-to-use WBANs solutions. These radio technologies include Personal Area Networks (PANs), e.g. Bluetooth, Wireless Sensors Networks (WSNs), Zigbee, IEEE 802.15.4 and IEEE 802.15.4a, Wireless Local Area Network (WLAN) and Mobile Ad-hoc Networks (MANET), e.g. WiFi, IEEE 802.11 a/b/g/n.

It is important to note here that the above cited communication standards were designed for other purposes, so, they do not meet the specific requirements of BANs applications, and present major limitations in terms of peak-power consumption, achieved data rates, communication range, generated RF interferences, and efficient on-body routing communications. In addition, the current literature contributions

lack of theoretical and/or implementations and experiment of dedicated routing protocols designed, simulated, implemented and then evaluated on real testbed. Particularly, Inter-WBANs co-existence and interoperability were dimly addressed. So, new autonomous self-organizing and cross-layer communication approaches should be investigated.

The objective of this PhD thesis is to investigate and address the following research challenges related to this context. First, review the state of the art of the existing studies and approaches that investigate the wireless data communication approaches for disaster relief context. Then, evaluate the existing approaches by simulation to understand their weaknesses and failure points. Second, design new networking functionalities for the specific context of On-Body and Body-to-Body networks, including efficient radio link quality estimation, cooperative and multi-hop Intra/Inter-BANs routing protocols, support for dynamic network topologies, infrastructure-less and stable end-to-end connectivity, etc. Third, evaluate the performance of the Cross-layer MAC/Networking communication proposed framework for the specific context (i.e., emergency and disaster relief) of On-Body and Body-to-Body networks, based on simulations and according to different realistic mobility scenarios. Fourth, implement the proposed approach on real testbed and evaluate its performances in realistic conditions. Finally, discuss the overall obtained results and disseminate the technical and scientific outcomes.

1.2 Key Contributions

With regards to the raised research challenges mentioned above and the scope of this PhD thesis, the main contributions of this work can be summarized as follows::

- *State of the art of disaster relief protocols and solutions*: Existing disaster relief routing protocols and communication technologies are investigated. One routing protocol from each routing class (proactive, reactive, geographic-base and gradient-based) is implemented on WSNET simulator [10]. Extensive simulations have been realized to evaluate the behavior of these routing techniques within the disaster scenarios. Limitations of these protocols have been reported and then considered for the proposed approach.

- *New routing approach proposal*: A new routing technique, called Optimized Routing Approach for Critical and Emergency Networks (ORACE-Net), is proposed to overcome existing protocols limitations in the body-to-body wireless communications during disaster relief operations and to ensure reliable routing among the tactical network.

- *Analytical and theoretical analysis*: An analytical analysis is performed to compare the communication overhead of the four identified protocols with our newly proposed approach A lifetime analysis based on the energy consumption is also provided for all the selected approaches.

- *Simulations for performance evaluation*: Based on different mobility traces (static, random way point, disaster mobility model), simulations are conducted to provide a detailed benchmark between the proposed approach and the existing ones. Results showed that ORACE-Net outperformed the other routing protocols in the body-to-body wireless communications in a disaster relief scenario.

- *Implementation and experiment on real testbed with diverse mobile platforms*: OARCE-Net routing protocol is then deployed on real testbed with different operating mobile platforms. Extensive indoor experiments were conducted as one of the rare disaster relief routing approach implementation. Experiments integrated sensing on-body platform connected to a mobile device. Collected data flows through the tactical disaster network (running OARCE-Net protocol) to reach the Internet of Things platform used for recording and analytics.

- *CROW^2 Urban disaster system evaluation*: ORACE-Net routing protocol, as the core of the urban disaster relief system, is evaluated on a real-testbed comprising different operating platforms. Evaluation includes accurate metrics, such as: end-to-end connectivity, end-to-end link quality estimation, end-to-end delay, throughput and jitter.

1.3 Thesis Organization

This thesis is organized as follows:

Chapter Two provides an overview on the literature related to this thesis. First, it covers the data dissemination strategies. Second, the disaster relief routing protocols are presented followed by the wearable communication technologies and systems. Public safety and disaster relief systems state-of-art is then presented. Finally, a survey on the Wireless Body Area Networks (WBAN) standards is detailed.

Chapter Three presents the new proposed routing approach for disaster relief, critical and emergency context in urban area. ORACE-Net routing approach is detailed based on its core algorithms. An analysis of the communication overhead and network lifetime is studied and then presented in order to compare the communication overhead between ORACE-Net and the rest of the considered protocol surveyed among Chapter 2.

Chapter Four focuses on the implementation of ORACE-Net routing approach as a part of the CROW^2 system. The presented implementation integrates sensors connected to a mobile device pushing the real-time data to a cloud IoT platform. The proposed routing approach is implemented on two different platforms, Android (Java/Android) and Linux(C language). Within this chapter also, the overall On-Body, Body-to-Body and Off-Body communications are explained. The last section is about the conducted experiments of the implemented system are detailed in order to evaluate the proposed protocol and the entire system performance. First the experiment setup and scenario are presented, then the results are discussed based on the relevant metrics considered for the urban disaster relief context.

Chapter Five presents the general conclusion and perspectives of this work. This chapter summarizes the overall performed tasks through this thesis. Based on the obtained evaluation of the proposed approach, some perspectives are discussed from research and industrial point of views.

This PhD thesis was proposed within the CROW^2 project, which is a research project conducted over more than three years (Jan, 2014- Feb, 2017) by the: ***Qatar Mobility Innovations Center (QMIC) - Doha, Qatar*** *and the* ***Commissariat à l'énergie atomique et aux énergies alternatives - Laboratoire d'électronique des technologies de l'information (CEA-Leti) - Grenoble, France****.*

"**Info-Box** This info-box is dropped inside some sections to introduce briefly a needed concept/project in the following paragraph ".

1.4 Publications List

1.4.1 Book Chapter

[**B1**] Muhammad Mahtab Alam, **Dhafer Ben Arbia**, and Elyes Ben Hamida, 'Wearable Wireless Sensor Networks for Emergency Response in Public Safety Networks', in *Wireless Public Safety Networks , volume 2*, ISBN: 978-1-78548-052-2, published on July 1st, 2016.

1.4.2 International peer-reviewed Journal Papers

[**J1**] **Dhafer Ben Arbia**, Muhammad Mahtab Alam, Abdullah Kadri, Elyes Ben Hamida, and Rabah Attia 'Enhanced IoT-Based End-To-End Emergency and Disaster Relief System.', *Journal of Sensor and Actuator Networks (Special Issue: Sensors and Actuators in Smart Cities)*, 2017, Aug. 6(3), 19; DOI:10.3390/JSAN6030019.
[**J2**] **Dhafer Ben Arbia**, Muhammad Mahtab Alam, Yanniick Le Moulec and Elyes Ben Hamida, 'Communication Challenges in on-Body and Body-to-Body Wearable Wireless Networks—A Connectivity Perspective.', *Technologies (Special Issue: Wearable Technologies)*, 2017, Jul. 6;5(3):43., 10: 726. DOI:10.3390/technologies5030043.
[**J3**] **Dhafer Ben Arbia**, Muhammad Mahtab Alam, Rabah Attia and Elyes Ben Hamida, 'ORACE-Net: A Novel Multi-hop Body-to-Body Routing Protocol for Public Safety Networks.', *Peer-to-Peer Network Applications Springer*, 2017, 10: 726. DOI:10.1007/s12083-016-0513-9.
[**J4**] Muhammad Mahtab Alam, Elyes Ben Hamida, **Dhafer Ben Arbia**, Mickael Maman; Francesco Mani, Benoit Denis, Raffaele D'Errico. "Realistic Simulation for Body Area and Body-To-Body Networks." *Sensors Journal*, 2016, no. 4: 561.

1.4.3 International Conference Papers

[**C1**] **Dhafer Ben Arbia**, Muhammad Mahtab Alam, Rabah Attia, Elyes Ben Hamida and Abdullah Kadri, 'CROW2: Internet of Humans-based Platform for Disaster Relief and Emergency Communication', in Proceedings of the *14th IEEE Annual Consumer Communications & Networking Conference (IEEE CCNC 2017)*, Las Vegas, USA, January 8-11th 2017.
[**C2**] **Dhafer Ben Arbia**, Muhammad Mahtab Alam, Rabah Attia and Elyes Ben Hamida, 'A New Multi-hop Body-to-Body Routing Protocol for Disaster and Emergency Networks.', in Proceedings of the *international conference on wireless networks and mobile communications (IEEE WINCOM 2016)*, Fez, Morocco, October 26-29th 2016.
[**C3**] **Dhafer Ben Arbia**, Muhammad Mahtab Alam, Abdullah Kadri, Rabah Attia and Elyes Ben Hamida, inpProceedings of the *12th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (IEEE WiMoB 2016)*, Third International Workshop on Emergency Networks for Public Protection and Disaster Relief, New York, USA, October 17-19, 2016.
[**C4**] Muhammad Mahtab Alam, **Dhafer Ben Arbia**, and Elyes Ben Hamida, To appear in Proceedings of the *IEEE Wireless Communications and Networking Conference (IEEE WCNC 2016)*, Doha, Qatar, April 3-6, 2016.
[**C5**] **Dhafer Ben Arbia**, Muhammad Mahtab Alam, Rabah Attia, Elyes Ben Hamida, 'Wearable D2D Routing Strategies for Urban Disaster Management–A Case Study.', *Qatar Foundation Annual Research Conference Proceedings, ARC'16*, ICTPP 2863, Doha, March 22-23, 2016.

[C6] Muhammad Mahtab Alam, **Dhafer Ben Arbia**, and Elyes Ben Hamida, 'Dynamic Scheduled Access MAC for Wearable Applications.', in Proceedings of the *Qatar Foundation Annual Research Conference 2016 (ARC'16)*, March 22-23, 2016.
[C7] **Dhafer Ben Arbia**, Muhammad Mahtab Alam, Rabah Attia, and Elyes Ben Hamida, 'Data Dissemination Strategies for Emerging Wireless Body-to-Body Networks based Internet of Humans.', in proceedings of the *11th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (IEEE WiMoB 2015), First International Workshop on Advances in Body-Centric Wireless Communications and Networks and Their Applications (BCWNets)*, Abu Dhabi, UAE, October 19-21, 2015.
[C8] **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 proceedings of the *11th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (IEEE WiMoB 2015), Second International Workshop on Emergency Networks for Public Protection and Disaster Relief (EN4PPDR)*, Abu Dhabi, UAE, October 19-21, 2015.
[C9] Muhammad Mahtab Alam, **Dhafer Ben Arbia**, and Elyes Ben Hamida, 'Research Trends in Multi-Standard Device-to-Device Communication in Wearable Wireless Network.',in proceedings of the *10th International Conference on Cognitive Radio Oriented Wireless Networks (CrownCom 2015)*, Workshop Cognitive Radio for 5G Networks, Doha, Qatar, April 21–23, 2015.

Chapter 2

Literature Review

This chapter presents a detailed survey on the public safety and urban routing protocols and approaches for wearable technologies. First, data dissemination strategies are presented and benchmarked as a main factor affecting wireless networking performances. Second, routing protocols are investigated with regards to different classes (i.e., proactive, reactive, geographic location-based and gradient-based protocols) as possible candidates for public safety and disaster relief routing techniques. Third, public safety networks are presented based on a real existing system as a case study. Few implemented routing techniques are then detailed according to different levels (i.e., On-Body, Body-to-Body and Off-Body). Finally, a state of the art of the wearable communication technologies and standards used in the public safety and urban emergency networks is presented.

2.1 Data dissemination strategies

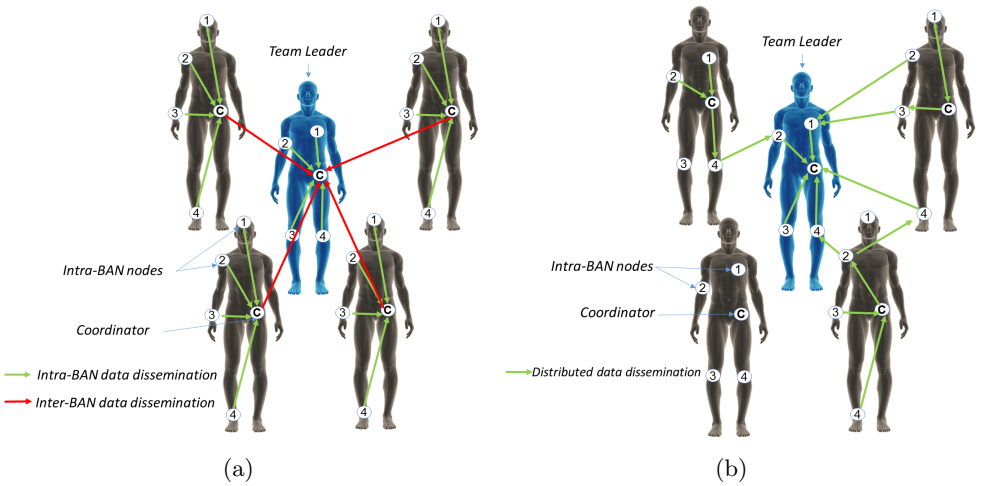
2.1.1 Overview

In the literature, diverse data dissemination protocols have been proposed for Wireless Sensor Networks (WSNs) [11]. WSN is composed by a certain number of sensor devices distributed on an area of interest. Sensor devices are severely constrained in terms of memory, computation capabilities, wireless range and battery power. Sensors (i.e., source-node) sense the environment physical measurements and send them towards a sink (i.e., destination-node). The sensing process could be either triggered by the source-node (i.e., through periodic sensing), or depending on the events (i.e., Event driven) or requested by the sink (i.e., Query Based). Data dissemination strategies for WSN are adopted recently for the Wireless Body-to-Body Networks (WBBNs or WB2BNs) with major restrictions [12, 3]. Based on different strategies, sensed data is disseminated towards the sink node. These strategies are classified with respect to: (i) type of disseminated data, (ii) depending on the destination(s), where both uses the concept of virtual infrastructure [13]. Furthermore, for (i), there are three categories: data dissemination (where the sensed measurements are disseminated), meta-data dissemination (where the sensed measurements are stored locally and a meta-data is disseminated), and Sink location dissemination (where the locations are stored into nodes information, and then data is disseminated depending on events). For (ii), dissemination strategies are categorized as: single node (disseminated information is stored in one node), out-of-group nodes (the information is disseminated out of a defined group of nodes), a set of nodes (information is depicted into a set of nodes). Most known data dissemination protocols in WSNs are Directed Diffusion (DD), Geographic Hash Table (GHT), Two-Tier Data Dissemination (TTDD), Railroad, Locators, etc.

It is important to note that, in Emergency and Critical networks, WSN could be a part of a Wireless Body Area Network (WBAN). A WBAN is a set of miniaturized devices (i.e. sensors, GPS, RFid tags/readers) wirelessly interconnected and attached (or implanted) into body (human, animal, etc.). All these devices are connected with a sink node (i.e. coordinator). Despite the fact that some of the above WSNs protocols were evaluated in a single WBAN context, WBAN still have considerable particularities against WSN [14]. First, mobility in WBAN is more important than WSN (i.e. WSN are considered stationary) therefore, link failure consideration among devices is relevant. Second, in critical operations, devices battery lifetime used in WBAN, is not a crucial requirement (during operations batteries could be replaced or recharged) instead of scattered sensors (in case of WSN) where battery must operate for long time (few years). These particularities impact requirements of data dissemination protocols. Classic data dissemination strategies within single WBAN were based on links lifetime. However, recent dissemination mechanisms tend to be more opportunistic and posture-aware due to the high WBAN dynamic variations especially in tactical operations. Opportunistic dissemination techniques prove energy preservation and network lifetime increase [15]. Moreover, probabilistic routing protocols use the historical link quality estimation and the inertial sensor data to make the best relaying decision. Further researches consist on evaluating Ad hoc routing protocols in a scale of single WBAN. Asogwa *et al.* in [16] evaluated Ad hoc On-demand Distance Vector (i.e. AODV), Dynamic Source Routing (i.e. DSR) and Destination-Sequenced Distance-Vector (i.e. DSDV) routing techniques. The obtained results showed that AODV and DSR have good reliability and performed much better in terms of energy efficiency. Likewise, according to Murthy et al. [17], AODV is the most efficient routing protocol for intra-BAN in terms of energy efficiency and QoS. At an extended level, Ad hoc routing techniques were also used to cover Body-to-Body communications [18]. Even more recent, an interesting layer-2 (i.e., MAC Layer) data forwarding strategy proposed by Kolios et al. with reference to a specific Emergency Ad hoc Network (i.e., ERN) [19]. Explore and Exploit (i.e., EnE) data dissemination strategy is based on new topology-related metric, Local Centrality (i.e., LC). LC computes a node importance rank that classifies the nodes based on their topological properties. Alert Messages (i.e., AM) will be disseminated through the nodes with highest LC. Indeed, no routing calculations, building and maintenance is needed, thus, no network protocol is implemented. LC information is stored into the layer-2 headers. According to the authors, EnE requires trivial communication overhead and includes smart forwarders selection. To conclude, existing data dissemination approaches in WBBNs are primarily based on the operational context (i.e., use cases: critical, emergency, delay-tolerant, etc.), next, on the type of the data to disseminate (i.e., location, data, meta-data). MANET are evidently evaluated in WBBNs, however, data dissemination strategies depending on operational requirements are not yet investigated. An important operational requirement in tactical operations consist on; the team leader has to be able to receive, follow and feedback the operation commanding center of all the information provided by his team. For this, clustered or distributed approaches are investigated in the following section.

During the last decade, most of the studies were focused on to the feasibility of the MANETs in tactical networks. This tendency is justified by the fact that the tactical operations happens in rural and populated areas where networking infrastructures are either absent or shattered, which comply with the specifications of the tactical operations. Furthermore, due to its flexibility to topology changes and its multi-hop routing aspect, Mobile Ad hoc networks are an interesting candidate to be investigated in the tactical WBANs. In this regard, one of the experimental works evaluated

MANETs in rescue and critical operations [20]. However, we introduce the following network architecture which is based on the principle that each team member has to send all the information as One-Way-Converge-Cast traffic towards the unique team leader. It is perceived that the proposed approaches for data dissemination were either classified by type of the disseminated information or based on nodes status (energy, connectivity, etc.). The objective of this part of the work is to evaluate the performance of two data dissemination strategies (clustered and distributed) with specific simulation setup detailed in the next section. The disseminated information towards the team leader could reach it in two different ways:



(a) (b)

FIGURE 2.1: (a): Clustered and (b) Distributed data dissemination strategies.

2.1.2 Clustered data dissemination

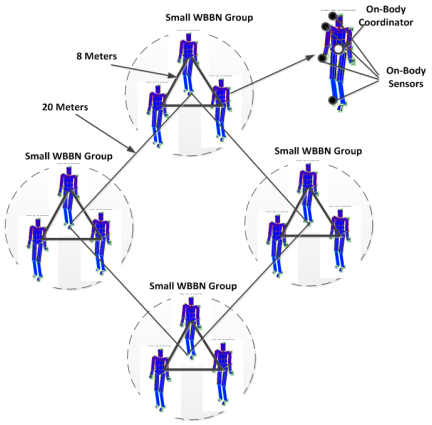
From one-WBAN nodes to their coordinator (i.e., embedded on the same WBAN), and then from that coordinator to the adjacent coordinators until reaching the team leader's coordinator (i.e., a coordinator is a sink node responsible for gathering data from the other On-Body nodes, it is characterized by powerful capabilities comparing to the other nodes). Thus, each WBAN could operate in a single frequency. Figure 2.1 (a) shows in the green color, a communication link between the sensor nodes and a coordinating node during the data dissemination process, whereas, in red color, the Coordinator-to-Coordinator data disseminations are highlighted.

2.1.3 Distributed data dissemination

Covering dissemination going from one-BAN node to the any reachable adjacent node (simple node or coordinator), until reaching the team leader's coordinator. Consequently, all nodes need to share same frequency which could raise an interference issue. Figure 2.1 (b) depicts the distributed data dissemination, any node could send its data to any node, however, the final destination is always the coordinator of the Team Leader.

2.1.4 Benchmarking of the clustered and distributed data dissemination strategies

In order to emphasize the impact of the data dissemination strategy on the performance of the deployed routing protocols in tactical disaster context, a complete evaluation is performed based on realistic scenario simulation. Simulation scenario and results are discussed late in Chapter 4.2.



(a)

FIGURE 2.2: Tactical Wireless Body-to-Body Network Scenario.

2.2 State of the Art of the Mobile Ad hoc Routing Protocols in Public Safety Networks

This section surveys the existing routing protocols which could be possible candidates in wireless sensor networks and wireless body area networks in the urban context.

2.2.1 Proactive Routing Protocols

Protocols that are creating and maintaining continuously their routing tables are called proactive or table-driven. In this routing class, nodes keep exchanging information to learn the network topology. Proactive protocols use one or more tables to store the topology information and routes, exploited later for routing or broadcasting information and data. By these settled routes, optimization algorithms (such as Dijkstra in [21]) can be applied to select best routes to use based on a chosen metric. Proactive protocols differ on the technique used for neighbors sensing and topology update. The difference concerns also the messages used to: discover, maintain and disseminate topology information or routes. Proactive routing protocols are appropriate with small networks, because of the routing overhead caused by the bandwidth consumption due to the continuous broadcasted updates. The most widely known proactive routing protocols are: Optimized Link State Routing protocol (OLSR) [22], Wireless Routing Protocol (WRP) [23] and Destination-Sequenced Distance-Vector (DSDV)[24]. And recently, the latest version OLSRv2[25].

Proactive routing protocols cause network overhead due to the periodic route discovery, but this reduces the routing overhead. Proactive protocols are suitable for small (less number of nodes) networks. The existing routing protocols differs in terms of throughput, packet delivery fraction, end-to-end delay, etc.

2.2.1.1 Optimized Link State Routing Protocol (OLSR)

In OLSR, network discovery and maintenance are based on three steps: neighbor discovery, efficient flooding and calculation of shortest path. Neighbor discovery consists of detecting and maintaining the list of the available neighbors nodes [26] (i.e. neighbors which are present within the communication range). The main optimization introduced by OLSR is to minimize the amount of the control messages which are broadcasted in the network [27]. This optimization is based on the use of the MPR (Multi-Point Relay) technique. Using OLSR, each node selects from its list of neighbors a set of nodes called Multi-Point Relays (MPRs) which will retransmit all its traffic and control messages. The MPRs are the minimum 1st hop neighbors that allows to a given node to reach all its 2nd hop neighbors. Indeed, the choice of these MPRs guarantees available symmetric links with the 2^{nd} hop neighbors.

2.2.1.2 Optimized Link State Routing Protocol Version 2 (OLSRv2)

Research around the OLSRv2 routing protocol started since mid-2005 [28], in order to improve the features of the basic OLSR protocol, based on extensive implementations. OLSRv2 is a proactive link state routing and using periodic local and global signaling for neighbor/link discovery and link state diffusion. Before, OLSR was designed to be extensible and to support hybrid MANET and non-MANET interfaces. Actually, as Clausen exposed in [29] which is based on over than fifty (50) implementations, OLSR wasn't able to support multiple interfaces with addresses in hybrid networks, and is inefficient in IPv6 support. The second version of OLSR brings some significant updates based on the experiments' feedbacks. OLSR uses four types of messages (different messages parser) and uses addressing (no address compression), in addition to the expiration mechanisms of MANET and non-MANET addresses. The format of HELLO message in OLSR could not contain large interfaces addresses (also, it does not support IPv6). OLSR uses two types of messages to manage multiple nodes interfaces and NON-MANET interfaces, these messages are respectively Multiple Interface Declaration (MID) and Host or Network Announcement (HNA). These messages are could not support different hybrid interfaces addresses and different messages formats. Besides, OLSRv2 requires only two messages types: HELLO and TC (internal and external with only one parser for all messages types). It uses also addresses compression with IPv6 support. Finally, OLSRv2 takes into consideration non-MANET nodes as MANET nodes (no more need for HNA and MID messages).

2.2.1.3 Wireless Routing Protocol (WRP)

WRP is a proactive routing protocol based on the path-finding algorithm inherited from Bellman-Ford algorithm with loop free avoidance by forcing each node to perform consistency checks of predecessor information reported by all its neighbors [26]. Four tables are maintained by WRP: Distance Table (DT), Routing Table (RT), Link-Cost Table (LCT) and Message Retransmission List (MRL). DT contains the network view represented by a matrix that contains the distance and the penultimate node to a destination. RT keeps an address for destination given node with distance to it. RT contains also a flag to indicate the path status: correct or erroneous (loop). The LCT contains the number of hops to reach each destination indicated by the relaying messages, it contains also the number of updates period (intervals between two successive periodic updates). The MRL contains entries of all update messages that allows to WRP to detect link breaks. Convergence of WRP is much faster than DSDV.

2.2.1.4 Destination Sequenced Distance Vector (DSDV)

Proposed by Perkins and Bhagwat [30] in 1994. It is based on Bellman-Ford algorithm enhanced by a loop-free. In DSDV, each node has a routing table where entries contain: the destination node and number of hops to it. Each entry is tagged by a sequence number that inform about the freshness of the route and delivered by the destination itself. Each node transmits periodically updates and immediately when new significant modification in topology occurred. The information broadcasted by each node are as follows: i) The destination address; ii) The number of hops to reach it; iii) The sequence number received, basically sent by the destination itself. Once this information is received, the update of the routing table will be based on the sequence number, and then on the better metric used in the case of equal sequence numbers. Stale routes are the routes that are not updated (regarding the sequence number that should be sent by the next hop), will be deleted. As a distance vector protocol, DSDV does not perturb a non-concerned zone by the topology changes; however the regular updates may increase the power consumption and the bandwidth use.

2.2.2 Reactive Routing Protocols

Ad Hoc on-demand routing protocols were designed to reduce the routing overhead caused by the proactive routing protocols. Route Request is always operated by flooding but only in case of needed route. Reactive routing protocols are classified into two categories that uses two different techniques, source routing and distance vector routing. Source routing uses headers data information and don't need routing tables which has high network overhead. Distance vector or hop-by-hop uses next hop and destinations address to route packets. This section overview reactive (on-demand) Ad Hoc routing protocols.

2.2.2.1 Ad Hoc On-Demand Distance Vector (AODV)

In AODV, a node does not perform route discovery or maintenance until it needs a route to another/new node/destination. A route discovery in AODV is initiated by the source node (S) through the broadcast of a specific route request (RREQ) to all its first hop neighbors. This route request is transferred by broadcasting until it reaches the wanted destination. The route request only records the $last_{hop}$ address in the field $Source_{ID}$ and the destination address in the field $Dest_{ID}$. This means that a given node knows only the last node that requested that route and not the originator one. AODV uses also the source and destination sequence number Seq_{Num} to distinguish routes freshness. The $broadcast_{ID}$ or $RReq_{ID}$ is used to avoid processing an already processed request (the pair $Source_{ID}$ and $RReq_{ID}$ is unique). A Time-To-Live (TTL) is also used by AODV to prevent an indefinite routing of a request.The Route Reply (RREP) in AODV follows the same route saved by the nodes while transferring the RREQ. These information will be deleted after a timer if a RREP is not received.

2.2.2.2 Dynamic Manet On-Demand Routing Protocol (DYMO): AODVv2

DYMO [31] routing protocol is considered as an enhancement of AODV, with recourse to some the features of DSR. Indeed, DYMO uses 'path accumulation' from DSR and removes unnecessary Route Reply (RREP), precursor lists and Hello messages (Route exploration messages) [32]. From AODV, DYMO keeps sequence number, hop count and RERR. DYMO has two main operations: route discovery and route management [31]. In DYMO routing protocol, the route discovery process starts with the RREQ (if

no route to destination exists in the source routing table), then, each time the RREQ is forwarded throughout the network, each node will attach its address to the RREQ message. Once the destination reached, The RREP will be sent in unicast to the source node following the accumulation path. DYMO is an energy efficient protocol, then if one node has low energy it does not participate in the route discovery process so it may be disconnected until the RREP is sent back. Now, when while sending data to an intermediate or destination node, and the link breaks or the node is no more available, the generating node multicasts a RERR to only nodes which are concerned with the link failure [33]. Upon the reception of the RERR, the routing table entry containing the unavailable node will be deleted. A new route discovery will be initiated when a destination is needed. Figure 2.3 shows the route discovery process.

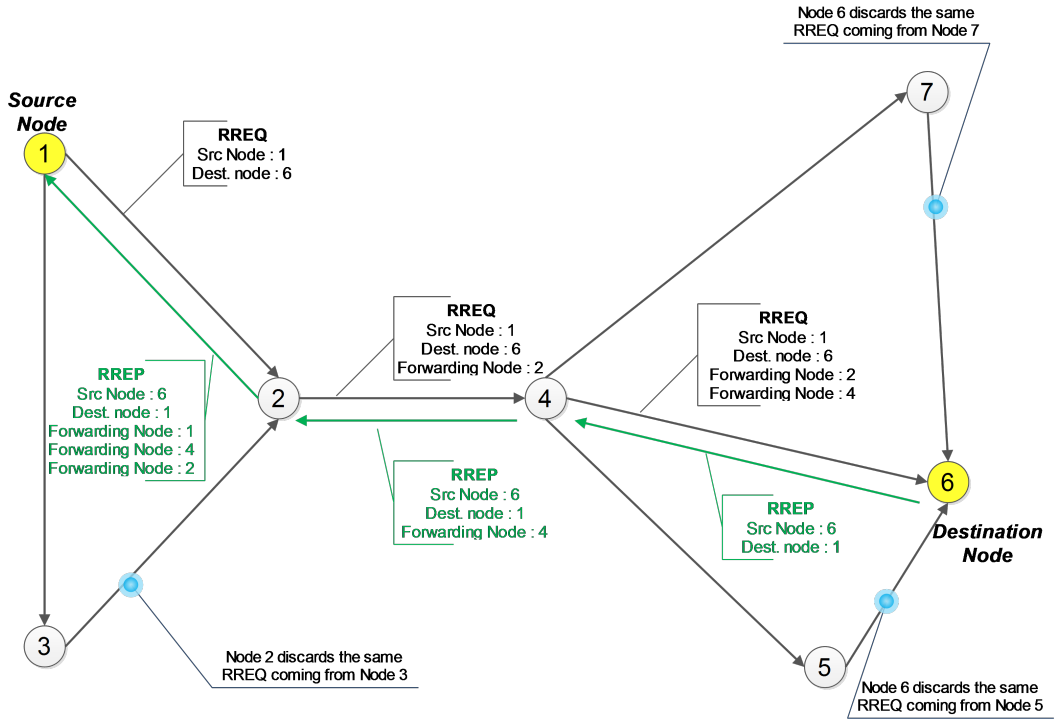


FIGURE 2.3: DYMO Route Discovery Process

2.2.2.3 Dynamic Source Routing Protocol (DSR)

The dynamic source routing (DSR) protocol is based on two mechanisms of route discovery and maintenance. Both are operating only on-demand, and does not have any periodic routing advertisement, link status or neighbor sensing [34]. A specificity of DSR, is that route discovery and route maintenance are designed to allow unidirectional links and asymmetric routes to be easily supported. DSR uses routing caches also, which allows the nodes to react rapidly in case of routes failures. The Route Discovery starts by checking first in the routes cache, if a route already exists to the destination node. In this case, the data will be directly sent using the available route information. Otherwise, a new route request is broadcasted to the neighbor nodes (1st hop). When a node receives the route discovery, if it is the destination, it replies by a route reply through a cached available route or through the recorded list of nodes in the route request (depends on the route efficiency), otherwise it disseminates it to its reachable neighbors. A duplicate reception of route request (known by same route

request id) is discarded. Each intermediate node in the route of the route reply, will check its cache before forward the reply packet, it may have an efficient route better than the recorded in the packet. This technique is appropriate to wireless networks where two uni-directional routes may be efficient than one bi-directional.

2.2.2.4 Temporally Ordered Routing Algorithm (TORA)

TORA is a source-initiated on-demand routing protocol which operates in highly dynamic and mobile multi-hop wireless networks. TORA [35] maintains many routes between given source and destination nodes. TORA is based on the 'link reversal' algorithm (i.e. when a node has no downstream links, it reverses the direction of one or more links). TORA ensure three main operations: route creation, route maintenance and route erasure. The last operation is performed when a route is invalid. These operations are concertized with three types of messages: QRY message for route creation, UPD for route update and CLR for route erasure. Only adjacent nodes' routing information are maintained.

2.2.3 Hybrid Routing Protocols

In order to reduce the traffic overhead of proactive protocols, and to reduce the route convergence delay in reactive protocols, hybrid routing protocols use combined features of both routing protocols categories.

2.2.3.1 Zone Routing Protocol (ZRP)

The ZRP protocol is based on two main routing concepts which were previously discussed, i.e. the proactive and reactive routing approaches. Using ZRP, when nodes are located inside a routing zone (i.e. where a zone is defined by a maximal number of hops, called also range), the routes are created and maintained proactively; whereas for the nodes which are located outside that zone, routes are resolved reactively [27]. ZRP reduces significantly the overhead compared to the original proactive routing protocol. ZRP is an effective routing protocol for groups of small networks where routing between these groups is performed using the nodes located at the boundaries of the different adjacent zones using an on-demand routing protocol. However, in case of dense networks, ZRP behaves as a classic proactive routing protocol.

2.2.3.2 Zone Based Hierarchical Link State Routing Protocol (ZHLS)

ZHLS is a hierarchical routing protocol based on the physical (geographical) location of the nodes with the support of a localization system (e.g. GPS). ZHLS divides the network into disjoint (non-overlapping) zones. Two topological information levels are defined: node level and zone level. The node level topological information informs about how the nodes are connected in that zone. The zone level topological information is shared with all the available nodes; it gives information about the zones inter-connection. Based on these two levels, all ZHLS network nodes construct two types of routing tables: intra-zone and inter-zone. The size of the zone depends on: nodes mobility, network density and power transmission.

2.2.4 Hierarchical Routing Protocols

In spite of the enhancements brought to standards on-demand and table driven routing protocol to increase their performance, these protocols still not adapted for large-scale networks. Hierarchical routing protocols split network into clusters. Most of

hierarchical routing protocol [36] set a particular cluster called Cluster Head (CH) and gateways nodes responsible for communication inter-clusters. Other old routing techniques manage clusters as distributed subnets. Despite of its contribution for the large networks, hierarchical routing protocols still has some drawbacks, especially the centralization of the routes through the cluster leader.

2.2.4.1 Cluster Based Routing Protocol (CBRP)

CBRP is a routing protocol based on the same idea of ZRP with some differences. Portioning the network into group of nodes (called clusters) aims to reduce the updating overhead during the topology changes [37]. CBRP is characterized by its less use of flooding in dynamic route discovery, the exploitation of uni-directional links unexploited by most of routing protocols. CBRP includes also routes repairing and routes shortening processes.

2.2.4.2 Adaptive Routing using Clusters (ARC)

The clustering routing protocols divide the network into sub-nets based on the nodes proximity. At the network initialization, Hello packets are broadcasted, nodes status are undefined. Three (03) different status that a node can hold: cluster leader (cldr), gateway (gateway) or ordinary node (node), depicted by Figure 2.4. When the discovery process starts, each node will be waiting for cluster leader hello message (a hello message sent from a cluster leader giving his status: cldr). Each node that did not receive a declaration of cldr in its neighborhood, will become a cluster leader itself. Each node that receives a hello message from exactly one cluster head, it switches to 'node' status. The third status is filled when a node receive two or more cluster head hello messages. Once the nodes knows their status in the network, the topology learning process starts following four (04) possible scenarios detailed in [36]. In ARC, each node can use one or two tables depending on its status. A non-cluster leader node, manages the Cluster Leader Table. This table contains the Cluster leaders (cldr) of the clusters that this node is a member of. A cluster leader node manages two tables: Node table and Neighbor table. The Node table contains addresses of nodes that contain this cluster leader node in their Cluster Leader Table. The Neighbor table contains the neighbors cluster leader and gateways through which other cluster leader could be reached. ARC exchanges only hello messages, which are used for topology maintenance and neighbors lifetime updating. Nodes status could change through the time, a normal node could become a gateway or joint gateway if it could reach more than one cluster leader. According to [36], ARC is adapted for large networks by centralizing the routing decision in cluster leader, although this feature consist of a disadvantage of all hierarchical routing protocols.

2.2.5 Geographic Location-based Routing Protocols

The drawbacks of Ad hoc networks in terms of continuous routes maintenance, storing of all network topology information into the nodes and network overload by unnecessary routes discovery (in case of proactive techniques), make further approaches come up to exceed these issues. Geographical based routing protocols are one of the proposed approaches. For more than ten years, geographical location based routing protocols avoided the technique of storing and sharing the network topology information. Routing decisions in geographic routing protocols are made hop-by-hop, no end-to-end routes made as in Ad hoc, for that, nodes in geographic routing protocol network store only physically reachable nodes information as detailed in [38]. Hence,

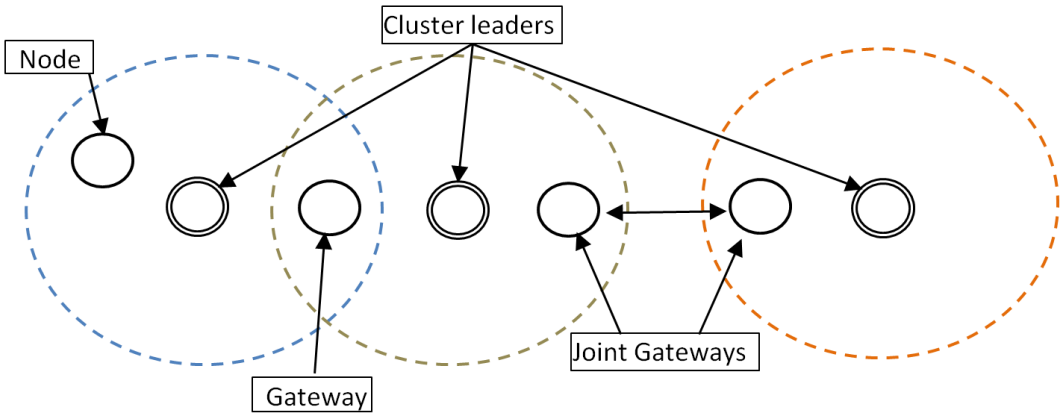


FIGURE 2.4: Cluster-based Topology.

no routes maintenance needed, because packets could follow different paths each time. In PSN, geographic location is an important parameter required regardless the routing approach used. Outdoor geographic locations could be simply obtained based on GPS technology. Indoor localization could be based on anchor nodes or simply tags sending their location. However, basing the routing decisions on geographic location must rely on a high precision available location technology, otherwise, erroneous locations lead on inefficient routing. Most known routing protocols in this class, early in 2000, Greedy Perimeter Stateless Routing (GPSR) [39] followed by Geographic Source Routing (GSR) and Spatially Aware packet Routing (SAR) [40].

For instance, GPSR uses nodes location and the wireless connectivity. It uses two forwarding techniques: greedy forwarding and perimeter forwarding. In greedy forwarding, packets from source node to destination are forwarded throughout the geographically closest next hop towards the destination. When a greedy forwarding is impossible, the protocol routes the packets in the surrounding perimeter of the destination. GPSR returns to the greedy forwarding early when a local maxima (local parameter) is reached. GPSR maintains only its location and locations of neighbors.

2.2.6 Gradient-based Routing Protocols

A gradient routing protocol is interesting to investigate in specific cases of PSN where all the data flow converges towards only one node (e.g. command center). The existing gradient routing approaches are designed for Wireless Sensor Networks as data-centric routing. Quite different from traditional address-centric routing considered as a flat routing, where all nodes have the same interest and importance in the network. In data-centric routing, a sink node collects all data from the other nodes in two main steps. The sink node starts by broadcasting a request to all neighbors until it reaches the concerned node. The response follows back the request path. A node forwarding data may aggregate its own data with the traveling data towards the sink node. Various gradient routing technique exist, most are variants of Directed Diffusion [41].

Indeed, Directed Diffusion (DD) is a data-centric routing protocol designed for WSN. With respect to WSN main requirements, DD is energy efficient, scalable and robust [42]. The routing mechanism in DD follows three steps. At startup, the sink node requests to gather data from one or more nodes. So, the sink node broadcasts the requests called interests towards the concerned node(s). Then, the routes (or gradients) are set up by selecting non-redundant route towards the sink node. This process starts with a low data rate specified by the sink node; afterwards, this data

rate is reinforced by the sink node itself through one selected node. The reinforcement then is propagated throughout all the nodes.

2.2.7 Device-to-device multi-hop routing protocols

The emergency route selection scheme for D2D cellular communications during an urban terrorist attack is presented in [43]. It dynamically selects multi-hop routes for D2D communications in spectrum co-existence with completely congested conventional cellular network (CCN). In this work, different routing algorithms, namely: shortest-path-routing (SPR), interference-aware-routing (IAR), and broadcast-routing (BR) are investigated [43]. The comparison results show that there is a trade-off between different algorithms, for example, for a small D2D communication distances, both SPR and BR achieve slightly higher packet reception ratio (PRR) than IAR, whereas, as the distance increases the impact of interference increases and therefore IAR scheme performs much better.

Another interference-aware routing scheme is proposed in [44]. The scheme minimizes the hop-count in wireless D2D networks which can decrease not only the delay for D2D connections, but also reduces the power consumption. The proposed approach jointly takes the geometric information, interference constraint, and D2D rate requirements into account, and yields low computational complexity. Several routing algorithms are cited in [45], particularly with an emphasis on interference aware routing protocols. For example, shortest path, or shortest hop-counts and farthest neighbor routing approaches are discussed. In these approaches, the algorithm reaches the destination as fast as possible from the current node position with a condition that it achieves the data rate requirements of the D2D communications while maintaining the required QoS [44].

With regards to the load balancing techniques, [46] presents a Load Balancing Based Selective Ad hoc On-Demand Multipath Distance Vector (LBSAOMDV) scheme for disaster recovery. It is an enhancement of the Ad hoc On-Demand Multipath Distance Vector (AOMDV) protocol, which reduces the control traffic by decreasing the number of nodes while maintaining the quality of service (QoS). Further, it intelligently selects the nodes which receives the route requests (RREQ) and optimizes the bandwidth utilization in comparison to AOMDV.

Recently, the concept of multihop smart phone networks based on WiFi-Direct is proposed in [47]. An energy efficient cluster-based routing protocol, called Quasi Group Routing Protocol (QGRP) is developed to address the energy issue which is critical due to high energy costs of the smart phones. In addition, virtual hierarchical distributed cluster algorithm for smart phone networks is introduced. The simulations demonstrate that QGRP can save significant amounts of energy compared to the cases without QGRP.

A brief benchmark on selected routing techniques is given by Table 2.1

2.2.8 Other Routing Protocols

Chen et al. in [48] classify the applications into three main classes: (i) remote health and fitness monitoring, (ii) military and training and (iii) intelligent biosensors for vehicle area networks. Moreover, the authors in [48] discuss a list of research projects and implementations, in particular the Advanced Health and Disaster Aid Network (AID-N) [49], which targets disaster and public safety applications. AID-N uses a wired connection for BAN communication and mesh and ZigBee for the Body-to-Body Network (BBN). Off-body communication in AID-N is fulfilled through WiFi,

Table 2.1: Benchmark on Key Functionalities of Selected Routing Techniques from Different Routing Classes

Parameter	AODV	OLSR	ZRP	CBRP
Routing class	Reactive	Proactive	Hybrid	Hierarchical
Route discovery	On-demand	Triggered at the network startup	*Intra-zone:* at network startup. *Inter-zone:* On-demand.	*Intra-cluster:* at network startup. *Inter-cluster:* On-demand.
Control message	RREQ, RREP, RERR	Hello, TC	*Intra-zone:* Hello. *Inter-zone:* RREQ, RREP.	Hello, RREQ, RREP, RERR.
Link support	Symmetric	*With MPR:* Symmetric. *With others:* Symmetric/Asymmetric	Symmetric	Symmetric/Asymmetric
Centralized administration	No	No	No	Cluster Head

cellular networks and the Internet. AID-N aims to sense pulse, blood pressure, temperature and ECG. Negra et al. in [50] focus more on the following major medical applications: (i) telemedicine and remote patient monitoring, (ii) rehabilitation and therapy, (iii) biofeedback and (iv) ambient assisted living. The latter work discusses also the QoS requirements for the medical context.

Recently, research trends have aimed at relying on large-scale LTE/4G-enabled networks to inter-connect deployed devices during disaster relief operations. For instance, the authors in [51] introduced the Device-to-Device (D2D) communication scheme to allow user equipment (UE) to communicate within the reachable neighborhood. The proposed scheme sets up an ad hoc wireless network, which relies on the base stations evolved NodeBs (eNBs) at the network startup. Therefore, the solution still depends on the 4G network infrastructure. Definitely, the unavailability of the 4G backbone causes the unavailability of the proposed D2D wireless network.

We cite among, other works, approaches that studied and implemented alert messaging systems, such as the Reliable Routing Technique (RRT) [52] and TeamPhone [53]. Both approaches consist of setting up a smartphone messaging system, which is able to send alert notifications by bridging cellular networks or over ad hoc and opportunistic networks. These proposed systems seem to solve the connectivity issues on-the-field between rescuers and trapped survivors. However, devices in the disaster area may only communicate within one hop. Devices select one next hop only, and no neighborhood discovery is done. Thus, RRT and TeamPhone are not topology-aware and do not consider external network extension with the Internet or other networks.

The authors in [54] propose a localization-based and network congestion adaptive approach called "DistressNet". DistressNet is claimed to be efficient in congestion avoidance during disaster relief operations; however, this approach is not appropriate

for indoor rescue operations due to its localization mechanism, which renders multihop algorithms inefficient. The authors in [55] adopted the WiFi Direct standard for the "Emergency Direct Mobile App", which is intended to divide the set of smart phones into groups communicating in peer-to-peer mode assured by WiFi Direct. One of the devices is selected as the Group Owner (GO) and acts as the access point for its group and as a gateway elsewhere. The rest of the devices act as Group Relays (GR). The network topology formation in this strategy causes an important delay. Additionally, with regards to the high mobility imposed by the emergency context, the network topology update (i.e., GO negotiation and election, GR selection) increases data transmissions latency.

The earliest proposed schemes aim to enhance the on-body devices' transmission reliability and to improve the energy efficiency. Chen et al. in [56] proposed a novel Cross-Layer Design Optimization (CLDO) scheme. Indeed, the design of CLDO relies on the three lower layers (i.e., PHY, MAC and network layer). Power consumption is firstly optimized by selecting optimal power relays. Then, the remaining energy in leaf nodes is utilized to increase the lifetime and the reliability. An optimal packet size is given for energy efficiency. Chen et al. claim that an inevitably slight overhead accompanies CLDO processing for different factors. First, during network initialization, complex procedures are run. Second, the algorithm uses a certain number of iterations, which influences the overall performance. Third, CLDO lacks the capacity to manage dynamic location situations.

Another approach presented by Tsouri et al. in [57] relies on Dijkstra's algorithm augmented with novel link cost function designed to balance energy consumption across the network. This latter technique avoids relaying through nodes, which spent more accumulated energy than others. Indeed, routing decisions are made based on the energy optimization. The authors claim that the proposed approach increases the network lifetime by 40% with a slight increase of the energy consumed per bit. However, this work does not fulfill the operational application requirements, which rely on the BBN network for connectivity and routing.

Miranda et al. in [58] implemented and evaluated a complete Common Recognition and Identification Platform (CRIP) for the healthcare IoT. CRIP enables a basic configuration and communication standardization of healthcare 'things'. Security and privacy and health devices' integration are also covered within this approach. Miranda et al. deployed CRIP according to different communication standards, such as NFC, biometrics (fingerprints) and Bluetooth.

The above proposed approaches are limited for various reasons according to two main classes (O: Operational; T: Technical): (O1) the implemented network is not open to be connected to extended networks (i.e., Internet or military communication platforms); (O2) no command center is considered on-the-field for operations conduct, and therefore, nodes only share their status between each other; (O3) limited services (i.e., alert messages, notifications, etc., only); (T1) nodes in the network have no visibility on the neighborhood and the network topology; (T2) routes (which do not exist for some non-multihop approaches) are neither updated according to the quality of the links' variations based on the mobility, nor according to energy efficiency and commanding proximity. To summarize the various protocols and systems, a benchmark comparison is given in Table 2.2.

2.2.9 Summary

A summary of above mentioned protocols is presented in Table 2.3. There is always trade-off between the protocols where different approaches are developed to optimize

TABLE 2.2: Recent implemented disaster management systems benchmark.

Protocols and Systems	Wireless Standard	Multi-Hop	Topology Awareness	Infrastructure Dependency	Network Extensibility	Sensing Devices Integration
RRT [52]	N/A	No	No	No	No	N/A
DistressNet [54]	ad hoc WiFi	Yes	Yes	No	No	N/A
Disaster 4 G [51]	LTE/4G	Yes	Yes	Yes	Yes	N/A
Emergency Direct [55]	WiFi Direct	No	Yes	No	No	N/A
TeamPhone [53]	ad hoc WiFi/SMS	No	No	Yes	No	N/A
CROW^2 (this work)	ad hoc WiFi	Yes	Yes	**No**	**Yes**	**Yes**

TABLE 2.3: Key Performances of the Existing State-of-the-art Multi-hop Routing Protocols.

	Performance Metrics					
Routing Schemes	Energy Efficiency	Delay	PRR	Hop-Count	Load Balancing and Bandwidth Efficiency	Route Set-Up Time
Link State Routing [22], [59]	**Medium**	Low	High	Low	High	**High**
Distance Vector Routing [60], [61], [62]	Low	Low	Medium to High	Low	Low	**High**
Interference-Aware Routing [43], [44], [45]	**High**	**High**	High	Low	High	**High**
Load Balancing-based Routing [46]	NA	**High**	**Low**	Medium to High	High	NA
Energy Efficient Clustered-based Routing [47]	Low	**High**	High	NA	Low	**Medium to High**
Others [52], [53], [63], [64]	**Medium to High**	**Medium to High**	Low to Medium	**One Hop** to Low	**Low to Medium**	High

certain performance metrics. To summarize, multi-hop D2D communication is incapable to connect the whole disaster network. In our latest findings in [65], several multi-hop routing protocols (i.e., AODVv2, OLSRv2, GPSR) were investigated and it is concluded that if we have a location information, geographic-based routing is the best choice both in terms of energy efficiency and higher packet delivery ratio (PDR). Further, it is found necessary to build a bi-directional routes between the PSN command centers and the deployed rescue members in emergency and disaster situations. However, to the best of our knowledge, the aforementioned routing protocols were not optimized for the PSN context and have many limitations.

2.3 Public Safety and Disaster Relief Networks

This section presents a complete case study of a governmental public safety and disaster relief. Operational and technical challenges and requirements of the system

are detailed, then interoperability is discussed.

2.3.1 Wireless Communication for Public Safety and Disaster Networks: A Case Study

National security is a high common interest of every country and this importance is growing along with the evolution of the actual threats. National security programs and organizations are in charge of preventing, planning and assuming protection strategy for civilians from natural disasters, wars, epidemics and so on. Public safety programs must be studied and validated to be used in case of need. These various threats cause a variety of conditions to be considered in extremely cases in order to be most prepared to. Public safety may cover different functions [66]: Law enforcement, emergency medical and health services, border security, environment protection, firefighting, search and rescue and emergency crisis. Other public safety scenarios exist, according to [67]. They are classified according to occurrence space-time:

- Routine or day-to-day operations: EMS (Emergency Medical Services: e.g. heart attack), Fire, Law enforcement.
- Multi-discipline, multi-jurisdiction: Explosion in chemical or nuclear plant.

Planning, triggering and conducting public safety scenario depends on varied circumstances; type of the threat (e.g. natural disaster, war, etc.), location (e.g. land: rural, urban, mountain; sea: ocean, coastline; air; underground), weather conditions, etc. These circumstances are closely related to the mission requirements. Mission requirements are decisive challenges that could guarantee mission success.

To investigate routing protocols in public safety and disaster relief, we consider the following two public safety systems:

"**SAFECOM** is an emergency communications program of the Department of Homeland Security's Office of Emergency Communications (OEC). OEC develops policy, guidance, and future efforts by drawing on SAFECOM member expertise and recommendations. This process has resulted in several key emergency communications initiatives including development of the National Emergency Communications Plan (NECP), the nation's first strategic plan to enhance emergency communications, and the SAFECOM Interoperability Continuum, a tool developed by emergency responders that identifies the five critical elements that must be addressed to achieve optimal inter-operable conditions to respond to an event [67]".

Terrestrial Trunked Radio (formerly, Trans-European Trunked Radio: **TETRA**) is a two ways communication technology, known as Walkie Talkie. It consists of a public safety network designed by governmental institutions for the service of emergency troops, police, firefighters, etc. TETRA is a standard of communication since 1995 [66].

2.3.2 Challenges and Requirements

Public safety is of common interest for governments, scientists, industries and of course all populations. Public safety programs are various, depending on the crisis type, population threatened, location and many other parameters. This variety makes public safety communications capabilities face to migration to new standards that support inter-operability, networks and devices heterogeneity and improve capacities. To accomplish this, there are requirements to fulfill and challenges to face.

After some critical national crisis (natural or man-made), some governments have set special institution intended to study, plan, train and improve public safety programs. In US (Department of Homeland Security), NTPSC (National Public Safety Telecommunications Council) is one of 15 public safety organizations whose mission is to improve public safety communications and interoperability through collaborative leadership [68]. NTPSC manage few programs in order to anticipate the critical telecommunication situations: PSST (Public Safety Spectrum Trust Corporation) and SAFECOM. In Canada (Research and development for defense in Canada), led by the Canadian Interoperability Technology Interest Group (CITIG), there is a program of standardization of public safety operations mechanisms and networking targets that aim to improve Canadian public safety interoperability. This shows the crucial concern provided by governments in public safety context.

Public safety missions and operations depend first on the environment locations and conditions, transportation and emergency equipment (ambulances, helicopters, rescuers equipment, etc.), and then on the communication technologies used with all its specifications (interoperability, coverage, batteries-powers and lifetime, etc.). We will present in the following sections, the current requirements and challenges of the public safety in two parts: Technical and operational requirements. As an example, for a public safety effective program, We consider SAFECOM's [67] studies and deployment to clarify some theoretical concepts. TETRA standard is considered as an example in integration of voice communication with the Long Term Evolution technology proposed in chapter 3 of [69].

2.3.2.1 Public Safety Networks Technical Requirements

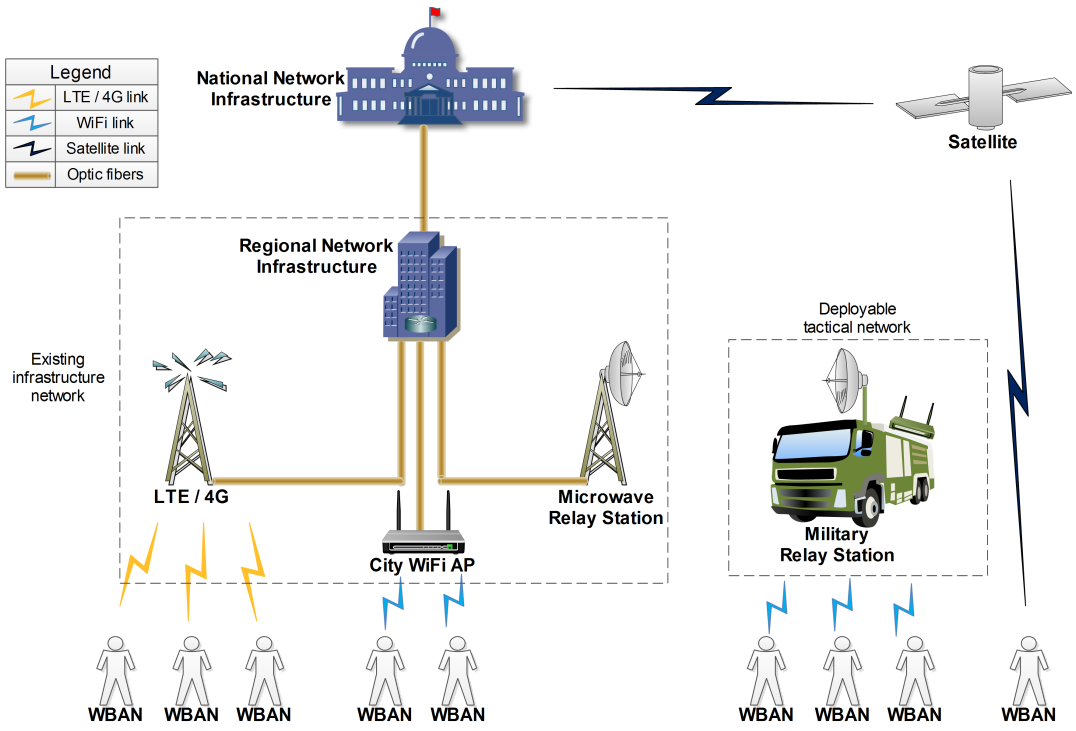


FIGURE 2.5: Infrastructure-based public safety networking architecture.

2.3.2.1.1 Standard Architecture Typical proposed networking architectures are set up based on networking infrastructure which may be either the existing daily useone (LTE/4G, WiFi, etc.) or an appropriated networking infrastructure made for critical and crisis operations. Figure 2.5 presents an example of infrastructure based networking architecture. A typical proposed architecture, defines the following hierarchical networking components:

- WBAN: Wearable Body Area Network: wearable radio system, responsible for: body and body surroundings monitoring, wireless data sharing between near or connected BANs,
- DTR: Deployable Tactical Relays: mobile tactical deployable networks by vehicles. It allows connecting WBANs to distant infrastructure networks or satellite.
- RNI: Regional Networking Infrastructure: Regional network backbone. This network could be particularly dedicated to public safety operations.
- NNI: National Networking Infrastructure: National network backbone.

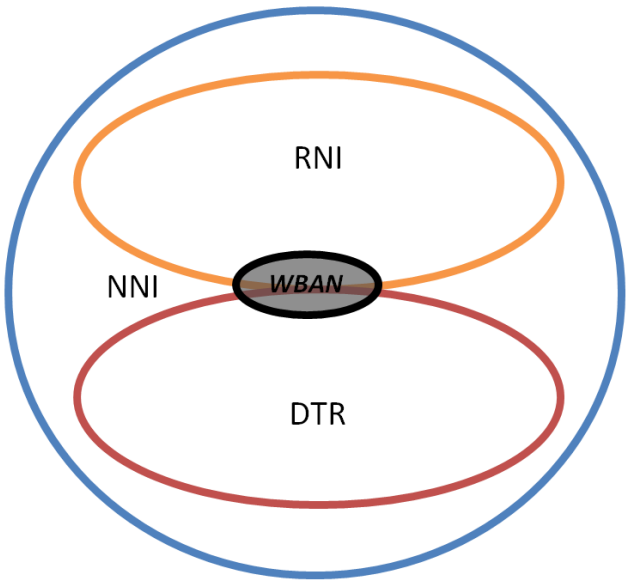


FIGURE 2.6: Networks components Infrastructure-based public safety networking architecture.

By presenting different networking levels and referring to Figure 2.5 and Figure 2.6, the interconnection going from the wearable wireless networks to the infrastructure based networks might be based on various networking technologies, in particular: i) wearable networks technologies, such as IEEE 802.15.6, IEEE 802.15.4j, Zigbee / IEEE 802.15.4, and Bluetooth IEEE 802.15.1, and ii) infrastructure based networks technologies, such as Wifi (IEEE 802.11), and LTE/4G.

SAFECOM, as a complete public safety and disaster relief system, proposes a typical networking architecture based on the existing regional and national networks infrastructure. It designs hierarchical networks into six (06) sub-networks as:

- PSC devices (PSCDs): handheld or wearable radios.
- Personal Area Networks (PANs): human physical and location data monitoring based on sensors.

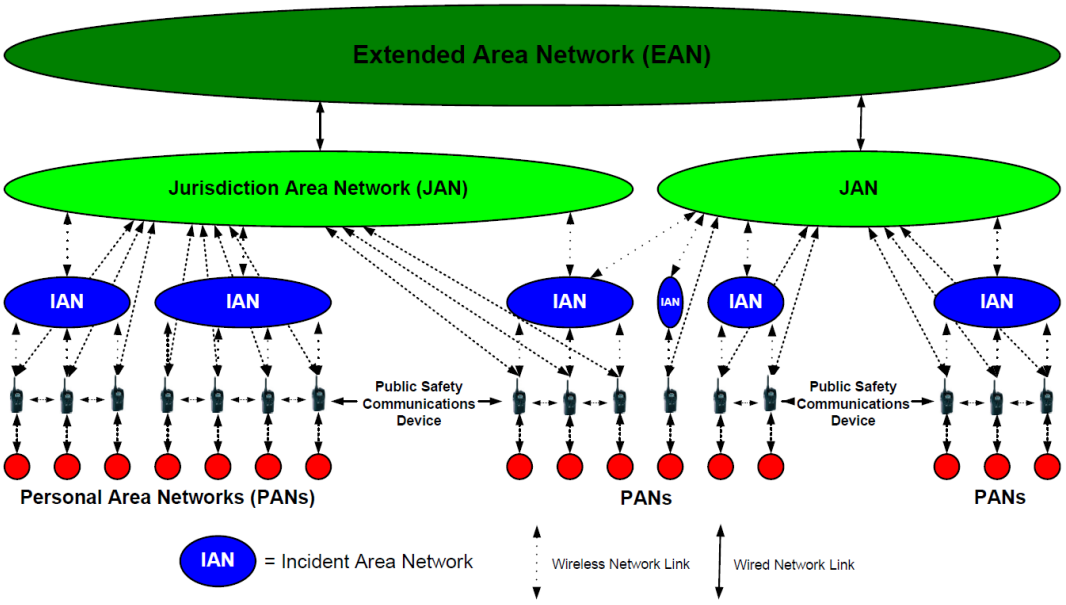


FIGURE 2.7: Infrastructure based architecture according to SAFECOM [67].

- Jurisdictional Area Networks (JANs): regional network infrastructure.
- PSC user groups: authentication systems (devices and personnel).
- Incident Area Networks (IANs): temporary network infrastructures brought especially for the operation.
- Extended Area Network (EAN): regional, state, and national network resources dedicated to public safety operations.

2.3.2.1.2 Tactical Deployable Mobile Networking System On the other hand, we have to consider that the majority of the countries could not implement specific infrastructure networks just for critical and public safety crises, because of its high costs. In addition, the existing infrastructure networks (LTE/4G, Wifi, etc.) will be unavailable in mostly disaster cases: earthquakes, flooding, volcano, etc. An environmental challenge is to face in public safety operations, it is that the location of the action is not known in advance, this means that rescue teams must be ready to act anywhere: mountains, sea, ocean, rivers, forest, etc. These locations, where most of public safety actions take place, are not linked to the infrastructure networks. All these facts prove the necessity of tactical deployable mobile networking system for public safety operations. To satisfy both of mentioned above networking models, there are requirements to consider in terms of *radio coverage*, *interoperability*, *availability*, *voice-data-video transmission*, *energy consumption and security*.

2.3.2.1.3 Radio Coverage No coverage, no life. A lack of coverage in risk study is considered as loss of life in public safety missions. Since all operations need instant communications to report feedbacks, claim support or give orders, an out of coverage element (e.g. casualty, rescuer, vehicle, etc.) is considered lost. However, a complete 100% geographical coverage is too costly. Radio coverage absolutely depends on the area type: indoor, outdoor or other. Indeed, better the radio coverage is, better the rescue missions requirements are fulfilled.

2.3.2.1.4 Interoperability Interoperability has two levels:

2.3.2.1.4.1 Organizational level: standards and procedures must establish the hierarchy of the different involved structures (Firefighting, Police, Army, Navy, Civil authorities, etc.). In addition, these procedures have to present field of intervention of each part. Indeed, orders flow from command center to operational rescuer on the field, the standards shall identify the responsibilities and the roles of each structure, so that in a crisis case, these procedures are ready to be triggered and work with.

> **SAFECOM as Case Study**: goes through the different other levels of interoperability in a concept called "interoperability continuum" which define steps to achieve a complete interoperability system. The first sub-level is Governance, which establishes coordination's practices between different agencies and involved institution. Second sub-level presents joint operating procedures to be engaged. Third sub-level is the technical level explained in the following point. Training and exercises sub-level concerns the joint operational preparation that could be played and replayed many times to improve operational skills of rescuers and emergency teams. The usage sub-level will show the whole system performance with its usage.

2.3.2.1.4.2 Technical level the organizational levels of interoperability depend on the technical level since it is the only effective mean of implementation of all the organizational procedures. NPSTC defines the technical interoperability as follows: "the ability of systems, personnel, and equipment to provide and receive functionality, data, information, and/or services to and from other systems, personnel, and equipment between both public and private agencies, departments, and other organizations, in a manner enabling them to operate effectively together. In addition, it allows emergency management/response personnel and their affiliated organizations to communicate within and across agencies and jurisdictions via voice, data, or video-on-demand, in real time, when needed, and when authorized" [68]. This means that all involved elements (personnel and equipment) in the PS mission should communicate together with regardless to the communication technologies implemented. Indeed, to fulfill this, communication interoperability may require more intermediate equipment to join different technologies; it may also require procedures that specify priorities for each data flow.

Indeed, Figure 2.7 presents many different communication technologies in case of infrastructure-based architecture where WBAN technology must be able to join the WiFi network, the LTE/4G mobile network and the satellite communications. Another aspect of interoperability is discussed in [3]. This aspect concerns the interoperability intra-WBAN and inter-WBAN. According to [3], the public safety context require the support of cooperative and collaborative coexistence mechanisms between WBAN coordinator and sensors, between close WBANs.

2.3.2.1.5 Video, Image and Voice Transmission Sending and receiving video, images and naturally voice in public safety operations is an elementary requirement that allow decision makers in such cases to pan out the right decision at the right time. Nowadays, real-time voice, image and video communications are developed over high band-withed technologies, there is even use of air UAVs to be close and get live videos from the incident zones. Thus, another issue appears in consequence, the security level in such various technologies is a relevant interest, and all the operation depends on it.

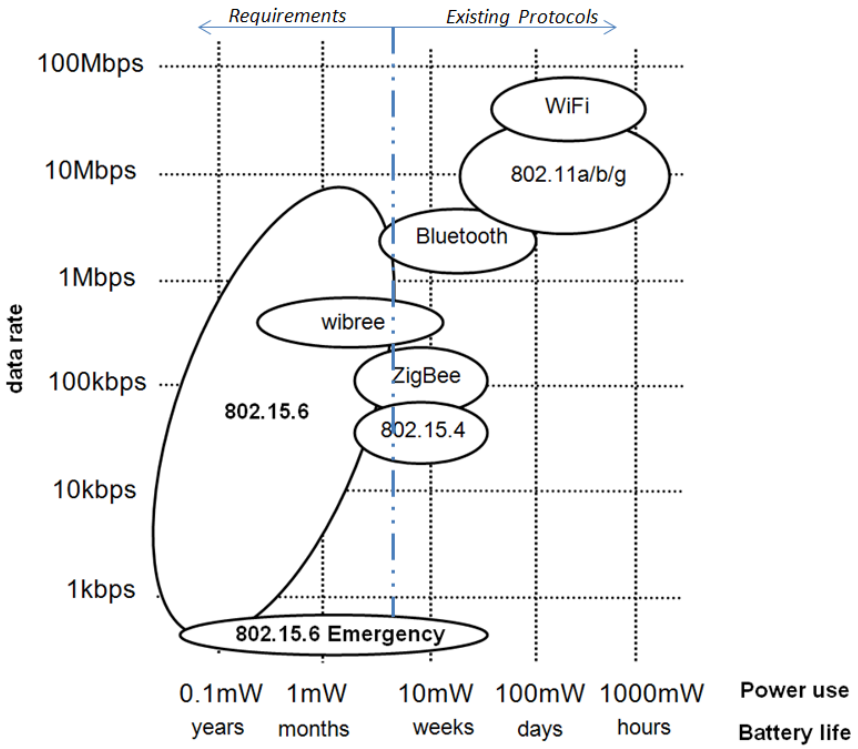


FIGURE 2.8: Power requirements and data rate in WBANs [70].

2.3.2.1.6 Energy Consumption, Security and Data-rate Authors of [3] and [70] surveyed the security requirements intra-WBANs and inter-WBANs, although, in such variety of technologies' standards that may be employed in public safety, it is required that all communication scales and levels must be secured, from the simple WBANs equipment to the monitoring systems in command centers.

The public safety environment is appealing many technologies where interoperability and availability are not the only challenges. In [70], the authors present the power requirements and data rates between the WBANs and the others protocols that may be used in public safety operations. Figure 13 shows that the WBANs in public safety do not meet the required power for critical operations including communicating with other technologies. Rather than the WBANs power limitation, the crisis cases explained in Sub-Section 2.3.1, could persist from few hours to few months, this require a coherent battery life for these type of operations.

2.3.2.2 Public Safety Networks Operational Requirements

In addition to the fact that the public safety technology is continually evolving as detailed in the previous section, also other important components could directly affect the success of the public safety operations.

2.3.2.2.1 Disaster Prevention Information A prevention disaster program covering possible disasters (depends on the region) should be presented, discussed and then published to the public. The fact that the public is aware about possible disasters, evacuation procedures, public safety organizations, etc., reduces the psychological matter of the public and tends to simplify the rescuers missions.

2.3.2.2.2 Rescuers and Equipment Organizations responsible for public safety operations are able to use vehicles, helicopters, aircrafts, and special equipment (snow jet, firefighting aircraft, etc.). Different skilled rescuers could also be appealed to help, since rescuers should be trained for specific environments (e.g. desert, mountains, etc.). To fulfill this, a common command center has to learn all these operational matters in order to manage human resource and equipment in the way of mission's success.

2.3.3 Survey on Routing Protocols for Public Safety and Tactical Networks

In addition to the main known routing protocols (e.g. MANETs, etc.) detailed above in this chapter, other specific routing approaches, which were specifically developed based on specific metrics (temperature, energy, QoS, etc.)

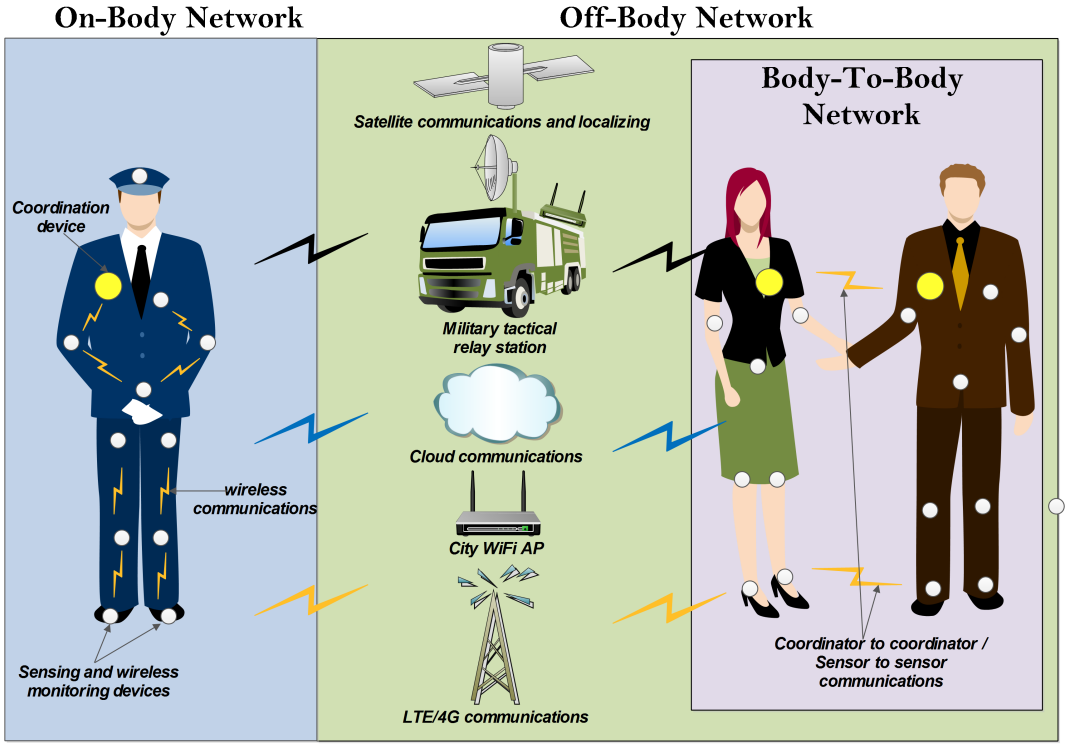


FIGURE 2.9: On-Body, Body-To-Body and Off-Body communications [3].

2.3.3.1 On-Body Routing Protocols

Two recent published studies [71] and [72] detailed the On-Body routing protocols presenting the routing issues first. However, authors in [71] considered in his study the Wireless Body Sensor Network (WBSN) which is a particular (but the implemented technology) case of WBANs. Routing challenges according to both authors are the postural body movements, the limitations of resources (bandwidth, memory, battery), Efficient Transmission Range, Interference and Temperature Rise, and others detailed in [72]. Authors in [71] and [72] studied the intra-WBANs routing protocols and classified them into four (04) main categories according to [72] instead of [71] which added two specific routing protocols to sensor networks. These categories briefly referred in the following section.

2.3.3.1.1 Temperature-based Routing Protocols Temperature based routing protocols where routing protocols are based on the generated radiation caused by the On-Body sensors and which may increase the body temperature and reduce blood flow and more:

- Thermal-aware routing algorithm (TARA): nodes that tend to be overheated are declared as hotspots and the network traffic is routed through other nodes until temperature of these hotspots decrease.
- Least Temperature Routing (LTR): this protocol aims to route traffic through the node that has the lowest temperature. This reduces the optimality of routes.
- Adaptive least temperature routing (ALTR): An optimization of LTR in term of route decisions based on number of hops.
- Least Total Route Temperature (LTRT): In addition to what LTR offers, LTRT uses the shortest path graph theory to optimize bandwidth.
- Hotspot Preventing Routing (HPR): The temperature depends on the number of transmissions. HPR is a biomedical sensor that routes packets from sender to the destination through the shortest path with hotspots avoidance. Others temperature based routing protocols are detailed in [72].

2.3.3.1.2 Cross-Layer Routing Protocols These protocols propose cross-layer routing, by exploiting features offered by upper or lower layers.

- Wireless Autonomous Spanning Tree Protocol (WASP) [73]:divides time into slots and apply a spanning tree algorithm to coordinate routing and medium access.
- Controlling Access with Distributed slot Assignment protocol (CICADA) [74]: low-energy protocol based on Time Division Multiple Access (TDMA). CICADA set up a spanning tree as well as WASP and synchronized slots are distributed between nodes.
- Timezone Coordinated Sleeping Mechanism (TICOSS) [75]: Cross-Layer Message Interface is designed through which information status is sent between MAC and Network layer.

2.3.3.1.3 Cost-Effective Routing Protocol

- Opportunistic routing: The idea of this routing technique is in the used model where the sink node and a relay are placed in a way to increase the communication probability. More details in [72].
- Prediction-based Secure and Reliable routing (PSR): Liang *et. Al* [76] proposed a framework based on a matrix maintained by all nodes where are stored links quality.
- Energy Efficient Thermal and Power Aware (ETPA): A cost function proposed by Movassaghi *et al.* [77], calculated with nodes temperature, energy level and received power from first hop neighbors.

2.3.3.1.4 Cluster based Routing Protocols With different techniques for electing a Cluster Heads, and this aims to reduce direct communications with the coordinator [71].

- Hybrid Indirect Transmission (HIT) : In [78], authors propose this technique which elects clusters heads from clusters and each cluster head is in charge of in and out cluster communications.
- AnyBody: It implements LEACH[79] with density-based cluster head selection method.

2.3.3.2 Body-to-Body Communication

Since a decade, the researchers were tending their studies into the feasibility of the MANETs in the context of public safety. This tendency is justified by the fact that the public safety operations happens in rural and unpopulated areas with absent networking infrastructure which meet with the specifications of the Ad Hoc Mobile Networks. As detailed in Section 3.2, the SAFECOM program [67] provides an entire document called Statement of Requirements that explains the public safety communications conditions and challenges. This document was used later on by Bohannan *et Al.* [80] to propose a QoS enhancement for Ad Hoc routing in the rural public safety. Moreover, a cluster based routing approach is proposed in [81] based on the MANET routing protocol CBRP. These two protocols are detailed below. Rather than Ad Hoc routing approaches, other researchers were focused on different considerations that might be more important in public safety operations, in particular Energy, as given by Fedrizzi *et Al.* in [82]. Bourdena proposed in [83] a mesh and ad hoc based spectrum aware routing protocol with consideration of unavailability of white spaces spectrum resources TVWS. This routing protocol was evaluated over simulated cognitive radio. The following sections highlight the above routing protocol approaches in the public safety context.

2.3.3.2.1 QoS aware Source Routing (QASR) QASR protocol is based on DSR because of the integration of the entire path in the packet. With refer to [84] and [85], authors integrate a bandwidth and delay estimation algorithms in the route discovery process. QASR selects then a path for the route reply RREP from the available paths discovered. QASR estimate the available bandwidth and delay from the collected information from all nodes. Moreover, since the GPS location systems are quite possibly implemented in the most mobile nodes (in public safety operations), the distance between a node and its neighbors is known. Thus, the received message will be re-broadcasted if the calculated distance (between the given node and its neighbors) is higher than the interference range, else the message will be dropped. In case of unknown node position, there will be a random generated number compared with the threshold to decide whether the message will be re-broadcasted or not. Subsequently, three parameters will define the route selection: estimated available bandwidth, estimated delay and the node speed. According to the authors, a cost v is given to nodes with the following Equation 2.1 where:

$$cost(v) = \alpha\frac{(B - A_v)}{B} + \beta\frac{D_v}{D} + \gamma\frac{S_v}{S} \tag{2.1}$$

Where, $\alpha+\beta+\gamma = 1$, A_v is the estimated available bandwidth, B is the channel capacity, D_v is the estimated delay, D is the delay tolerance, S_v is the node average speed and S is the maximum node speed.

The cost of the each path in QASR is given by:

$$cost(path) = \sum cost(nodes) \tag{2.2}$$

This metric leads to a generated path characterized by large available bandwidth, low packet delay and low mobility's nodes will be selected as relays [80]. QASR is compared to DSR and AODV in two public safety scenarios. The simulation conditions are detailed in [80]. The simulation results of both scenarios for QASR are more performant than DSR and AODV in terms of throughput, delay, packet delivery ratio, QoS satisfaction ratio and overhead. QASR was tested and simulated in specific rural safety conditions. QASR intended to increase throughput and delay, although, the most important requirement to be considered in public safety operations is the packet delivery ratio, which is close to AODV behavior.

2.3.3.2.2 Cluster Based Routing Protocol Authors in [81], propose a cluster based routing protocol based on requirements in particular firefighting operations especially reliability and delay. The proposed operational networking model supposes that firefighters act as groups or teams. Each team is led by one firefighter who belongs to that team. CBRP consider that each team represents a cluster and each team leader is a Cluster Head (CH). This CH = Team leader is selected from the 1st hop neighborhood based on least value of path selection variable detailed here [81]. Each team member sends all its sending data to its appropriate CH. The CH is responsible for forwarding data of members that selected him as CH. All CHs data are finally forwarded to a Base Station. Atiq *et al.* in [81] consider the node's residual energy as decisive criteria for packets routing. A simulation of CBRP for public safety rescue operations, with certain simulation parameters shows that the proposed protocol outperforms AODV and DSDV in terms of average end to end delay and packet delivery ratio.

2.3.3.2.3 Energy Aware Routing in Heterogeneous Multi-Hop Public Safety Wireless Networks A recent proposed routing protocol that considers a compromise between the energy consumption and the routing delay as the routes selection criteria. Authors of the proposed routing protocol, present here [82] a strategy for route path selection optimization. This optimization is includes the selection of the minimum energy link cost route path and the maximum network lifetime. An Energy Aware Routing technique based on an on-demand routing protocol in this protocol come up with including the energy related metrics (i.e. remaining battery level, energy cost per bit, etc.). Indeed, a destination node that receives multiple route requests from the same source node, selects the best route based on the optimization strategy for route path selection detailed in [82] and unicasts the route reply through that best route. A hop-limit is considered for the route request to limit the discovery packets flooding. This hop-limit depends on the network size and density. The proposed Energy Aware Routing technique allows also to the destination, of the route request packet, to explore the various networks technologies encountered by the route request while being broadcasted. Such collected information on the network, gives the nodes an overall view to be considered while the routes computation process and the route reply message unicast.

2.3.3.2.4 A Spectrum Aware Routing Protocol for Public Safety Applications over Cognitive Radio Networks This routing protocol is based on the concept of TV White Spaces (TVWS). TVWS are broadcasting allocated frequencies

TABLE 2.4: Key enabling M2M communication protocols for future wearable systems. [5]

Parameter	*HTTP[87]*	*CoAP[88]*	*AMQP[89]*	*MQTT[90]*	*MQTT-SN[91]*
License/Status	IETF Standard	IETF Draft	OASIS Std.	OASIS Std.	Open Std.
Latest Specification	1.2	13	1.0	3.1	1.2
Open Source Librairies	C, C++, DotNET, Java,Python, etc.	Java, C	C, C++, DotNET, Java, Python, etc.	C, C++, DotNET, Java, Python, etc.	C
Protocol Format	Text	Binary	Binary	Binary	Binary
Payload Format	any	any	any	any	any
Max Payload Size	up to 2 GB	1024 Bytes	2^64 Bytes	up to 256 MB	60 Bytes
Target Devices	IP-based	IP / Non-IP based	IP-based	IP-based	IP / Non-IP based
Architecture	REST	REST	Pub/Sub, Queues	Pub/Sub	Pub/Sub
Routing					
Session Oriented	No	No	Yes	Yes	Yes
Network Transport	TCP/UDP/SSDP	UDP	TCP	TCP	UDP
Message Namespace	Hierarchical Resources Space (URL/URI)	Hierarchical Resources Space (URL/URI)	Nodes, Queues, User-Defined	Hierarchical Topic Space	Hierarchical Topic Space
Messaging Reliability	HTTP Response Codes	Basic ACK	QoS 0,1,2	QoS 0,1,2	QoS 0,1,2
Security	SSL/TLS, Basic & Digest auth	DTLS	SSL/TLS, SASL	SSL/TLS, Basic auth	-
Client Complexity	Low (<64 KB)	Low (<188 KB)	Low (<64 KB)	Low (<64 KB)	Low (<64 KB)
Bandwidth Utilization	Medium to High	Low	Medium	Low to Medium	Low

that are not being used by any service. The approach of this protocol is to use cognitive radios to exploit these available frequencies to allow joint operations between different rescue corps (firefighters, police, military, etc.). The recourse to the cognitive radios offers the possibility to cope the interoperability issues especially when various technologies, devices and procedures should be implemented together. Bourdena et al. present a use-case scenario in [86] that adopts Ad Hoc Cognitive Radio network where secondary nodes are able to utilize the available channels left from the primary systems (licensed systems that are allowed to exploit TVWS). A geo-localization database assists the routing process because the selected white channel used for transmission depends on the area where nodes are deployed. The proposed protocol targets the establishment of maximum routing paths and minimum. This process includes the effective coordination of the intermediate routers (forwarding nodes). According to Bourdena *et al.*, this routing protocol is validated for an efficient communication for secondary nodes located in different areas with different TVWS availabilities.

2.3.3.3 Off-Body Communication

Off-Body communication, as a part of the general architecture seems to be the more easiest to deploy. Indeed, military signal corps, press and media equipped trucks could be deployed rapidly near the disaster area to serve as a gateway for the tactical body-to-body and on-body wireless networks. However, relaying deployed tactical network to extended networks (i.e., military, Internet, etc.) is very critical. Indeed, it depends

on the used protocol to transfer real-time data to the extended networks. This subsection reviews the relevant key enabling technologies for Off-Body communications systems (i.e., between the wearable BANs/BBNs and the remote cloud servers).

2.3.3.3.1 Key Enabling Off-Body and Machine-to-Machine (M2M) Protocols for Wearable Systems A Machine-to-Machine (M2M) communication protocol role is to establish a reliable and secure end-to-end wireless communication connection between the deployed on-body devices (e.g. smart phones) and the remote back-end servers (e.g. command centers, cloud servers, etc.). Moreover, all gathered data is transferred to the distant servers by the the M2M protocol. M2M protocols could be classified onto two categories: (1) Representational State Transfer (REST) protocols, such as HTTP [87] and CoAP [88]; and (2) Publish–Subscribe protocols, such as MQTT [90], MQTT-SN [91] and AMQP [89]. A brief overview and a benchmark of the M2M protocols is given below. Sana *et al.* in [5], made a detailed referenced comparative study given by Table 2.4.

2.3.4 Survey on WBAN Communication Standards and Technologies used in Public Safety Networks

Recently, low power standards have been exploited in WBANs research as well as for commercial applications, where most of them partly satisfying the requirements for life vital signs monitoring and public safety missions. Some low power standards designed to support low power sensing that have been adapted for health-care applications, e.g., ZigBee, while others such as IEEE 802.15.6 have been designed specifically for WBANs, not only for mobile health-care monitoring, but also for many more applications. Main standards of WBAN technologies are summarized below in Table 2.6. WiFi IEEE 802.11 standard will be detailed hereafter, because it is the one we have used in our approach, and the IEEE 802.15.6 WBAN Standard is presented as the standard for WBAN.

2.3.4.1 WiFi IEEE 802.11 Standard

The 802.11 standards a.k.a. "WiFi". The most popular are 802.11b and 802.11g protocols using 2.4 GHz band. They respectively use Direct Sequence Spread Spectrum (DSSS) signaling and Orthogonal Frequency Division Multiplexing (OFDM) method.

Wireless connections can be made in ad-hoc mode or infrastructure mode.

- Ad-hoc mode a.k.a "peer-to-peer" mode is simply a group of computers talking wirelessly to each other with no access point (AP). It is limited in range and functionality.
- Basic Service Set (BSS) of Infrastructure mode uses one AP to connect clients. The range of the AP's signal, called microcell, must encompass all clients.

Access Points (APs) are responsible of the following functionalities:

- Guaranty the interconnection
- Manage the extension of the network
- Manage the association of devices in range
- Manage the scheduling of the transmission
- Provide a synchronization through the beacon

- Allow devices to save energy

2.3.4.1.1 WiFi IEEE 802.11 Physical Layer IEEE 802.11b standard specifies one Medium Access Control in addition to several Physical layers:

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)
- Infra-red

As depicted by the following Figures 2.10, 2.11 and 2.12, the formats of the PHY Protocol Data Unit (PPDU) for the 3 IEEE 802.11b Physical layers are

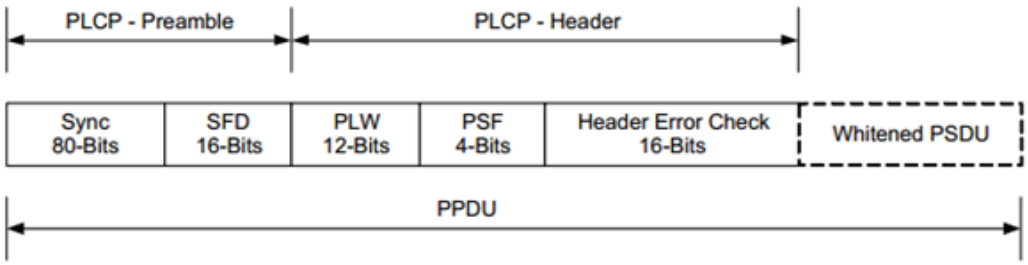


FIGURE 2.10: Format of IEEE802.11 FHSS PPDU[92].

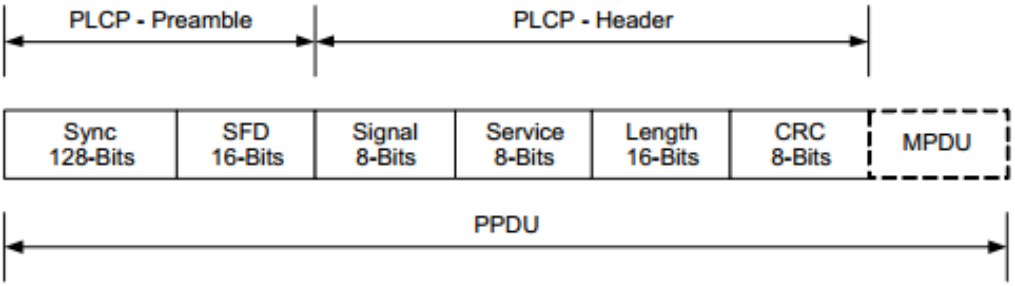


FIGURE 2.11: Format of IEEE802.11 DSSS PPDU[92].

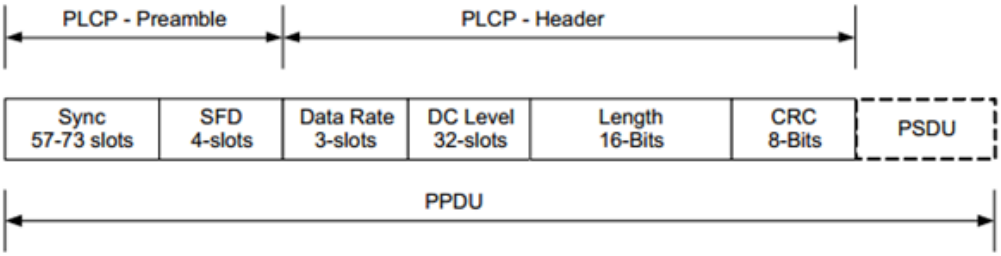


FIGURE 2.12: Format of IEEE802.11 IR PPDU[92].

Figure 2.13 depicts the format of the physical layer protocol data unit (PPDU) for the OFDM Physical layers.

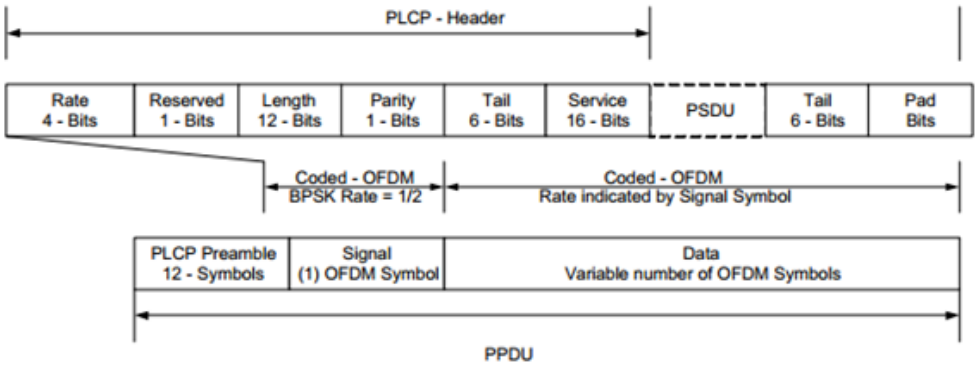


FIGURE 2.13: Format of IEEE802.11 OFDM PPDU[92].

2.3.4.1.2 WiFi IEEE 802.11 Medium Access Layer The services provided by the MAC layer are:

- Transfer of data between nodes: i) asynchronous data transfer limited to 2304 bytes in size, ii) time bounded transfer only if there is an access point.
- Association procedure allowing a node to know the access point,
- Authentication and data confidentiality,
- Manage the frequency band: i) transmitted power control (TPC), ii) dynamic frequency selection (DFS).
- Support applications with QoS constraints,
- Provide precise time synchronization applications.

The access mode is by default a Carrier Sense Multiple Access Collision Avoidance scheme (CSMA/CA). It is a competitive access where collisions are possible. Specifically, a station having a frame to be transmitted, listens to the channel. If the channel is free, it transmits its frame otherwise it defers its transmission frame. The IEEE 802.11 CSMA/CA access mode has additional features:

- Acknowledgement at the MAC level only for a point-to-point transmission.
- Protection against hidden node problem thanks to RTS/CTS exchange. It is reserved for frames larger than a certain threshold. It is performed by two short control frames.

2.3.4.2 Bluetooth IEEE 802.15.1 standard

Bluetooth technology was designed as a short range wireless communication standard, and later widely used for connecting a variety of personally carried devices to support data and voice applications. As a WPAN technology, two or more (up to eight) Bluetooth devices form a short-range network called *piconet*. A synchronization is needed to transfer data and common the the clock on the same physical channel. Bluetooth devices operate in the 2.4 GHz ISM band. The key features of Bluetooth wireless technology are robustness, low power consumption and low cost. There are two forms of Bluetooth technology systems:

Table 2.5: IEEE 802.15.1 Standard Channel Allocation for each RF channel [92]

RF Channel	**RF Center Frequency**	**Channel Type**	**Data Channel Index**	**Advertising Channel Index**
0	2402 MHz	Advertising Channel		37
1	2404 MHz	Data Channel	0	
2	2406 MHz	Data Channel	1	
...	...	Data Channels	...	
11	2424	Data Channel	10	
12	2426	Advertising Channel		38
13	2428	Data Channel	11	
14	2430	Data Channel	12	
...	...	Data Channels	...	
38	2478	Data Channel	36	
39	2480	Advertising Channel		39

- Basic Rate (BR), with optional Enhanced Data Rate (EDR) and Alternate MAC and PHY (AMP) extensions,
- Low Energy (LE)

Although traditional Bluetooth operating in basic data rate (i.e, up to 721.2 kbps) and enhanced data rate (i.e, up to 2.1 Mbps), BT LE data rate could reach up to 1 Mbps now. However, BT LE affords an easy Link Layer design, ultra-low power idle mode, easy neighboring devices discovery. Bluetooth LE technology supports very short data packets (8 octet minimum up to 27 octets maximum) whereas Classic Bluetooth support a maximum packet size of 2971 bits which include a 68-72 bit access code, a 54-bit header and a payload of up to 2745 bits. Using fewer channels for pairing devices, synchronization can be done in a few milliseconds compared to few second for Bluetooth. The topology of Bluetooth LE networks is a star topology. Devices can have 5 roles:

- Advertiser periodically broadcasts advertisements in advertising channels
- Scanner looks for other BTLE devices advertising within range
- Initiator requests LLC with an advertiser
- Master schedules LLC operations. (Multiple LLC possible)
- Slave transmit only upon a reception of packet from the master (only one LLC)

The functioning of the Link Layer can be described in terms of a state machine with five states: i) Standby State, ii) Advertising State, iii) Scanning State, iv) Initiating State, v) Connection State. The transitions from one state to another are directed by the Host. The Standby State is the default state in the Link Layer, where it is not possible to send or to receive packets. Each advertising event is composed of one or more advertising packets sent on proper channels. The advertising event shall be closed after one packet has been sent on each of the used advertising channel indexes or the advertiser may close the event earlier to accommodate other functionalities. There are different types of advertising events: i) connectable undirected event, ii) connectable directed event, iii) scannable undirected event, iv) non-connectable undirected event.

2.3.4.3 IEEE 802.15.4 Standard (ZigBee)

ZigBee is a low-power, short-distance wireless communication standard designed by ZigBee Alliance based on the IEEE 802.15.4 Low-Rate Wireless Personal Area Network (WPAN) standard. It uses the license-free ISM bands either 2.4GHz or 868/915 MHz. Network standard allows unicast, broadcast and groupcast messaging in ad-hoc self-created networks. Based on that messaging scheme, ZigBee defines three different network topologies:

- Mesh: Every node has the possibility of reaching its destination through any of its neighbors. The elements use a simplified version of AODV routing protocol to construct their routing tables.
- Cluster tree: Network routing directs packets up and down the tree structure created through network formation until they reach their destination. This topology demands the links to be active at all times, since the breakage of one may cause re-formation of the tree structure.
- Star: There is a coordinator node which reaches all the other members in a single-hop way, the rest communicates with other nodes by using the coordinator as relaying node in order to deliver their messages to destination.

Nodes within a ZigBee network can play three different roles: Coordinator (stores information about the network and provides connection to other networks), router (capable of running application functions and relaying data from other devices) and end devices (it only communicates the information generated to its neighbors but with no critical role in the network topology).

2.3.4.4 IEEE 802.15.4a Standard (IR-UWB)

The IEEE 802.15 Low Rate Alternative PHY Task Group (TG4a) for Wireless Personal Area Networks (WPANs) was initially created to propose an amendment to the Low Data Rate IEEE 802.15.4 standard, aiming at defining an alternative Physical layer. Over the existing standard, the main goal was to provide:

- Joint communications and high-precision ranging service (typically with submeter accuracy);
- High aggregate throughput ;
- Ultra low power consumption ;
- Scalable bit rates;
- Longer achievable ranges;
- Low cost;
- Compliance with worldwide regulation ;
- Possibility for different receiver architectures (hence tolerating trade-offs between performance and complexity);

2.3.4.5 IEEE 802.15.4j Standard

IEEE802.15.4j, and extended version for IEEE 802.15.4, it is reserved for e-health (Medical BAN). This standard proposes an alternate PHY specified for the 2360 MHz - 2400 MHz MBAN band.

2.3.4.6 IEEE 802.15.6 WBAN Standard

The IEEE 802.15.6 standard is a body area networks protocol. The important features of the standard are detailed below:

2.3.4.6.1 IEEE 802.15.6 Physical Layer Three possible PHY layer specifications including: Human Body Communications (HBC), Narrowband (NB) PHY and Ultra wideband (UWB) PHY. The PHY Protocol Data Unit (PPDU) represents the information that is sent through the propagation medium to the receiver device. It is composed of the physical layer convergence protocol (PLCP) preamble, physical layer convergence protocol (PLCP) header, and physical layer service data unit (PSDU), as illustrated in Figure 2.10, and is briefly explained below:

- **PLCP Preamble**: The purpose of the preamble is to aid the receiver in packet detection, timing synchronization and carrier-offset recovery. Two unique preambles are defined in order to mitigate false alarms due to other networks operating on adjacent channels. Preamble is transmitted at the symbol rate for the desired band of operation and will be encoded using the same modulation parameters as defined for different physical types. More details on the PLCP Preamble can be found in Section 8.2 of the standard [93].
- **PLCP Header**: It is added to convey information about the PHY and MAC parameters that are needed at the receiver side in order to decode the PSDU. Details on the different parts composing the PLCP Header and how to properly set the bits of each field can be found in Section 8.3 for further details in [93].
- **PSDU**: It is formed by concatenating the MAC header with the MAC frame body and Frame Check Sequence (FCS). The PSDU is then scrambled and optionally encoded by a BCH code. The PSDU shall be transmitted using any of the available data rates in the operating frequency band. More details on PSDU construction could be found in [93].

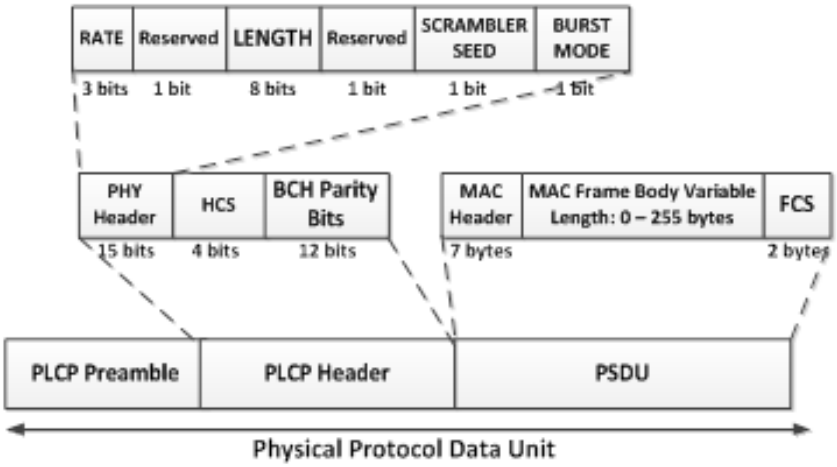


FIGURE 2.14: Physical Frame Format[92].

2.3.4.6.2 IEEE 802.15.6 Medium Access Layer The MAC Protocol Data Unit (MPDU) is an ordered sequence of fields delivered to or from the PHY Service Access Point (PHY SAP). The MAC frame consists of a fixed-length MAC header (7

octets), a variable-length MAC frame body and a fixed-length Frame Check Sequence (FCS) field (2 octets), as shown in Figure 2.11. The MAC frame body has an octet length L_{FB} such that $0 \leq L_{FB} \leq pMaxFrameBodyLength$, and is present only if it has a nonzero length, where *pMaxFrameBodyLength* is the maximum frame body length at the physical layer. The Low-Order Security Sequence Number and Message Integrity Code (MIC) fields are not present in unsecured frames. Management, Control, and Data type are the three MAC frames that are described in detail in the standard. Each of them implies a different composition of the MAC Frame Body, in particular for the Frame Payload Field.

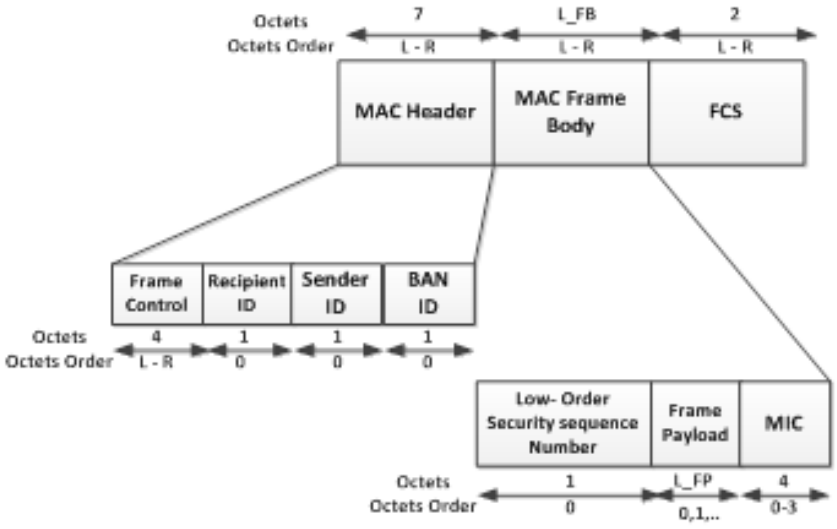


FIGURE 2.15: IEEE 802.15.6 MAC Frame Format[92].

The standard provides greater flexibility on the users to adapt MAC according to their requirements. With regards to medium access mechanisms, WBANs Coordinator can decide to operate in one of the following access modes:

- **Beacon mode with super-frame boundaries**: transmitted at the beginning of every beacon period. Two Exclusive Access Phases (EAP) and two Random Access Phases (RAP) , could be configured together based on the application requirements.
- **Non-beacon mode with super-frame boundaries**: No transmitted beacons, but super-frame and allocation slots boundaries are established.
- **Non-beacon mode without super-frame boundaries**: No transmitted beacons, super-frame and allocation slots boundaries are not established, because no time reference is involved to access the medium.

2.4 Conclusion

Through this chapter we presented a literature review on the related research works and standards. Data dissemination strategies are presented first as communication strategies affecting the overall behavior of wireless wearable systems. A survey on the mobile ad hoc routing protocols used in public safety networks is detailed. The next section of this chapter presented a case study of an existing application where

Table 2.6: WBANs Related Standards

	IEEE 802.11 a/b/g/n (WiFi) [94]	**IEEE 802.15.1 (Bluetooth)[95]**	**IEEE 802.15.4 (Zigbee) [96]**	**IEEE 802.15.4a (UWB) [97]**	**IEEE 802.15.6 (WBANs standard) [93]**
Modes of Operation	Adhoc, Infrastructure	Adhoc	Adhoc	Adhoc	Adhoc
Physical (PHY) Layers	Narrowband	Narrowband	Narrowband	Ultra Wideband (UWB)	Narrowband, Ultra Wideband (UWB), Human Body Communication (HBC)
Radio Frequencies (MHz)	2400, 5000	2400	868 / 915, 2400	75-724, 3128-4859, 3000-5000, 6000-10000	402-405, 420-450, 863-870, 902-928, 950-956, 2360-2400, 2400-2438.5
Power Consumption	High ($\approx$ 800 mW)	Medium ($\approx$ 100 mW)	Low ($\approx$ 50 mW)	Low (<50mW)	Ultra low ($\approx$ 1mW at 1m distance)
Maximal Signal Rate	Up to 150 Mb/s	Up to 1 Mb/s	Up to 250 Kb/s	Up to 27.24 Mb/s	10Kb/s to 10Mb/s
Communication Range	Up to 250m (802.11n)	100 m (class 1 device)	Up to 75 m	Up to 30 m	Up to 10 m (nominal $\sim$2m)
Networking Topology	Infrastructure based	Ad-hoc very small networks	Ad-hoc, Peer-to-Peer, Star, Mesh	Ad-hoc, Peer-to-Peer, Star, Mesh	Intra-WBAN: coordinated, uncoordinated, 1/2-hop star. Inter-WBANs: non-standardized
Topology size	2007 devices for structured WiFi BSS	Up to 8 devices per Piconet	Up to 65536 devices per network	Up to 65536 devices per network	Up to 256 devices per body, and up to 10 WBANs in a volume of 6x6x6 meters
Target Applications	Optimized for Data Networks	Optimized for Voice Links	Optimized for sensor, home automation, etc.	Optimized for short range and high data rates, localization, etc.	Health Monitoring, Sports, Disability Assistance, Body Centric application, etc.

challenges and requirements of such context are discussed. Then, a classification of routing protocols and standards for public safety and tactical networks is given based on the different networking levels. Last section of this chapter surveyed the on-body communication standards which are summarized in Table 2.6. To conclude this state-of-the-art, it is important to emphasize the following limitations in the existing literature, which could be summarized as:

- There is a lack of dedicated disaster relief rescue solutions based on specific designed routing protocols, studied, implemented and evaluated.
- Classic ad hoc routing protocols regardless of their routing class (proactive, reactive, geographic-based, etc.) are limited in performance for the urban disaster relief context, as discussed in [65].
- Some recent proposed implementation offer constrained services: either simple or alert messaging only, one-way communication, one hop capability, etc.

Next chapter presents the new proposed routing approach called: Optimized Routing Approach for Critical and Emergency Networks (ORACE-Net).

Chapter 3

Optimized Routing Approach for Critical and Emergency Networks (ORACE-Net) routing protocol

With regards to the operational perspective, data traffic in Public Safety Networks (PSN) is multi-directional, which means that the command center (CC) collects needed information from the deployed rescue teams and the rescue teams receive real-time instructions to execute from the CC. Additionally, PSN require nowadays real-time video flow (i.e., video streaming) transmission and/or real-time data through Internet. Rescue teams could also ask for assistance from distant medical staff available at the CC. Thus, there are various purposes and requirements at the application layer (e.g., video-streaming, medical assistance, operations conduct, radio communication, Internet connection, etc) which raises the routing functionality challenges.

This chapter presents the newly proposed routing protocol called Optimized Routing Approach for Critical and Emergency Networks (ORACE-Net). ORACE-Net is a Body-to-Body (B2B) and Body-to-Infrastructure (B2I) routing approach. The main objective of ORACE-Net routing protocol is to have instant neighborhood links visibility and establish available optimized dynamic routes according to specific link quality estimation metric based on the the quality and the availability of the links. The first version of ORACE-Net was disseminated within [98], which was based on the signal strength level (SSL) (given by Equation 1 in [98]) as a link quality estimation metric. The following version of ORACE-Net is enhanced where the end-to-end link quality is estimated based on the effective received packets and the expected packets to be received.

> First version of ORACE-Net presented in [98] is based on the received signal strength level as a main factor in calculating the link quality estimation. An enhancement is then made on ORACE-Net algorithms to be more efficient within the complete urban and disaster relief system, disseminated in [99].

3.1 ORACE-Net: Design Principles and Operations

In this section, we present the mechanism of the new routing protocol (i.e.,ORACE-Net). The main objective of ORACE-Net is to have instant neighborhood links visibility and establish available optimized routes according to the specific link quality estimation metrics. The proposed protocol consists of three main phases: 1) Beacons,

Advertisement broadcasts and Link Quality Estimation, 2) Direct Route Establishment (DRE), and 3) Reverse Route Establishment (RRE). These phases are described below.

3.1.1 Beacons, Advertisement broadcasts and Link Quality Estimation

Each node from ORACE-Net network broadcasts continuously periodic $Hello$ packets for neighborhood discovery according to the standard NeighborHood Discovery Protocol (NHDP) [100]. In addition, $Hello$ packets are used in the link quality estimation for the nodes [101]. Each $Hello$ packet has a sequence number. When a node receives the first $Hello$ packet from a neighbor, this neighbor is inserted into the neighbors table with a Link Quality Estimation (LQE) equal to 1.0. Based on the $Hello$ packets broadcasted every 3s, a node can estimate the number of $Hello$ packets supposed to be received during a certain period of time. The LQE of a one hop neighbor is assigned according to the following equation:

$$LQE = \frac{H_R}{H_E} \tag{3.1}$$

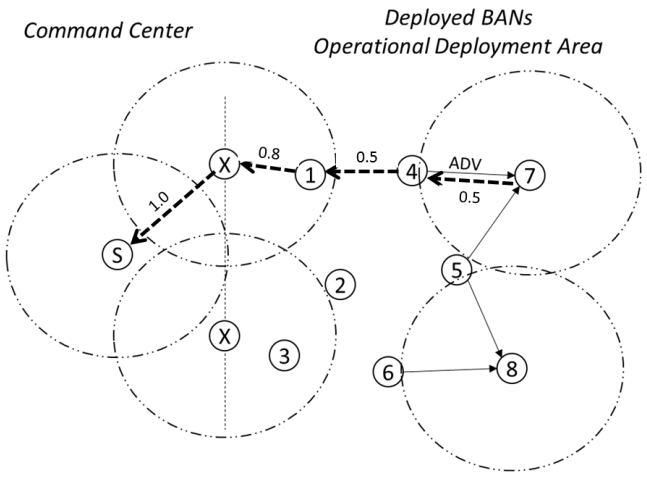
where H_R is the number of received $Hello$ packets, and H_E is the expected number of $Hello$ packets to be received which is equal to:

$$H_E = \frac{T_C - T_S}{P_H} \tag{3.2}$$

where T_C is the current time, T_S is the connection starting time with each specific node, P_H is the $Hello$ period. The *CC node* initializes the connection by broadcasting periodically Advertisement packets (ADV) which are flooded over the entire network to announce the *CC node* to all other nodes in the network. A *CC node* is a node deployed by the command center in the closest safe place to the incident area. A node receiving an ADV, processes it and then rebroadcasts it to all of its reachable nodes. The header of the ADV contains a sequence number which is used to discard the duplicated received ADVs. When a node receives an ADV, a route is established towards the *CC node* with the last visited (traveled) node by the ADV, as the next-hop. The following received ADV will initiate the second phase of ORACE-Net detailed in the next subsection.

In our proposed approach, ADV broadcasting process has three key roles: 1) it contributes in the conventional neighbors discovery process, 2) it provides routes establishment towards the command center node(s) (*CC node(s)*), 3) it provides also the $E2E_{LQE}$. The proposed approach relies on two main metrics: $E2E_{LQE}$ and the Hop_{Count}. The first metric can be calculated based either on the *Signal Strength Level* (SSL), the *link quality indicator* (LQI), or the *signal to noise ratio* (SNR) measurements [102] [101]. To that end, each ADV contains specific header's entries to track the hop count and the $E2E_{LQE}$ along the traversed route. When an ADV is rebroadcasted, the $E2E_{LQE}$ field in the packet header is updated by multiplying the LQE values recorded at each hop. Figure 3.1 depicts an example of the ADV broadcasting process. The $E2E^{SD}_{LQE}$ between a source node S and a destination node D is calculated according to the following equation:

$$E2E^{SD}_{LQE} = \prod_{S}^{D} LQE_{ij} \tag{3.3}$$



Routing Table for Node 7

DST	Next_Hop	Hops	E2E-LQE	Link_Lifetime
S	4	4	0.7	3s

Routing Table for Node 5

DST	Next_Hop	Hops	E2E-LQE	Link_Lifetime
S	2	2	0.9	4s

Routing Table for Node 8

DST	Next_Hop	Hops	E2E-LQE	Link_Lifetime
S	6	3	1.0	2s

FIGURE 3.1: Routing tables after DRE phase (for Nodes 7, 5 and 8) when the 1^{st} wave of ADV reaches all nodes. Please note that, Nodes Xs are base stations deployed by the rescue teams while they are moving towards the incident area. Route from Node 7 to the *CC node* is represented by the bold dashed line.

where: S is the source of the E2E route, D is the destination, i and j are the visited nodes from the source to the destination. LQE_{ij} is the Link Quality Estimation between node i and j (i.e., on one hop only).

The proposed ORACE-Net routing protocol operates based on two different algorithms. Algorithm 1 is triggered upon the reception of ADVs (i.e. DRE phase), while Algorithm 2 is executed upon receiving a $DATA$ packet (i.e. RRE phase).

3.1.2 Direct Route Establishment: DRE

The *CC node* broadcasts an ADV, then it waits for a predefined period (i.e., 3s used during the simulation and the implementation) to broadcast the next ADV with a new sequence number. In the other side, when a node receives an ADV, it updates both its neighbors and routing tables. Then it rebroadcasts the ADV only once. The DRE algorithm is presented in Algorithm 1.

The routing table is only updated when the received ADV has better $E2E_{LQE}$ than the one (i.e.,$E2E_{LQE}$) of the current used route. According to Algorithm 1, all the ADV packets are considered (even duplicated), but each ADV is re-broadcasted only one time (based on the sequence number). Indeed, the $E2E_{LQE}(ADV)$ is compared with the $E2E_{LQE}(Route)$. If the first value is higher, then the current route is updated as follows: First, the last visited node by the ADV becomes the next-hop of the route. Second, the $Hop_{Count}(Route)$ gets the value of the $Hop_{Count}(ADV)$, and the destination remains always the *CC node*. If the $E2E_{LQE}(ADV)$ is equal to the $E2E_{LQE}(Route)$, then, the shortest or equal path is considered. For the rest of the cases, the current route is maintained until the route lifetime expires. If it is the case, a new route is created based on the next first ADV received. It is important to note here, that as soon as an ADV is re-broadcasted, the upcoming received ADV (with delay) with the same sequence number are then dropped (Step 3 of Algorithm 1). This feature will trigger the multi-path functionality in the upcoming versions of ORACE-Net. The DRE phase of the protocol ends up by a fresh route towards the *CC node* at every involved node with only one way routes (i.e., from nodes to the *CC node*) as depicted in Figure 3.1. As a reply to the ADV packets, nodes send back a

Algorithm 1 Direct Route Establishment Algorithm (Node 'i')

1- RX (SRC, DST, Sender, ADV_{Packet})
2- Update Neighbors Table(ADV_{Packet})
if ($E2E_{LQE}(ADV_{Packet}) > E2E_{LQE}(Route)$) OR ($E2E_{LQE}(ADV_{Packet}) == E2E_{LQE}(Route)$ AND $Hop_{Count}(ADV_{Packet}) \leq Hop_{Count}(Route)$) **then**
  Update $E2E_{LQE}(ADV_{Packet})$
  Update $Hop_{Count}(ADV_{Packet})$
  Update $Routing_{Table}(ADV_{Packet})$
end if
if ($ADV_{Packet}(Seq_{Number})$ == already broadcasted) **then**
  3- Drop Duplicated $ADV_{Packet}(Seq_{Number})$
  4- Go To 1.
else
  5- TX (SRC=CC-node, DST=Bcast, Sender=i, ADV_{Packet});
  6- Go To 1.
end if{Where: "SRC" is the originator of the packet, and "Sender" is the last visited node.}

Algorithm 2 Reverse Route Establishment Algorithm (Node 'j')

1- RX (SRC, DST, Sender, $DATA_{Packet}$)
2- Update Neighbors Table($DATA_{Packet}$)
if ($E2E_{LQE}(DATA_{Packet}) > E2E_{LQE}(Route)$) OR ($E2E_{LQE}(DATA_{Packet}) == E2E_{LQE}(Route)$ AND $Hop_{Count}(DATA_{Packet}) \leq Hop_{Count}(Route)$) **then**
  Update $E2E_{LQE}(DATA_{Packet})$
  Update $Hop_{Count}(DATA_{Packet})$
  Update $Routing_{Table}(DATA_{Packet})$
end if
if ($DATA_{Packet}(Seq_{Number})$ == already broadcasted) **then**
  3- Drop Duplicated $DATA_{Packet}(Seq_{Number})$
  4- Go To 1.
else
  5- TX (SRC, DST=CC-node, Sender=j, To Nexthop, $DATA_{Packet}$)
  6- Go To 1
end if

data packet towards the originator *CC node*, this data packet triggers the next phase called Reverse Route Establishment (i.e., *RRE*).

3.1.3 Reverse Route Establishment: RRE

ORACE-Net proposes bi-directional path establishment for efficient routing in PSN networks. Indeed, the data packets are forwarded hop-by-hop until they reach the *CC node*. The $DATA$ packet header records the $E2E_{LQE}$, Hop_{Count}, the last visited node, and the originator of the packet. If the routing table does not contain a route to the originator of the packet, then a new route is created. Otherwise, if the route already exists and the $E2E_{LQE}(DATA)$ is higher than $E2E_{LQE}(Route)$, or, they are equal and the $Hop_{Count}(DATA)$ is less or equal than $Hop_{Count}(Route)$, fields are extracted from the header to create or update route as follows:

1. The originator of the $DATA$ packet becomes the final destination in this route.

2. The last visited node is the next-hop to reach that final destination.

3. The $E2E_{LQE}$ is updated with the LQE (given by Equation 3.2) of the link (Current node, last visited node) according to Equation 3.3, then inserted into the route.

4. The Hop_{Count} is incremented and inserted within the route.

Figure 3.2 illustrates the data packets flow towards the *CC node*. When a node receives a data packet, the node updates its routing table then forwards the packet. A duplicated $DATA$ packet is used to update the routing table and then dropped based on the sequence number. Similarly to the DRE phase, the $E2E_{LQE}$ is calculated and updated using the same process as detailed in Algorithm 2.

3.2 ORACE-Net vs Other Protocols: A Qualitative Comparison

Table 3.1 summarizes the differences between ORACE-Net, and the rest of the studied routing protocols from the different routing classes, reactive, proactive, and geographic-based. As given in the summarizing Table 3.1, ORACE-Net has an optimized-proactive mechanism, which means that the ADV/DATA packets are utilized by the nodes for neighborhood discovery, CC node announcement and data transmission. ORACE-Net is a hierarchical with regards to the operational disaster context, means that the CC node is considered as a master trusted node in the network, responsible of collecting/diffusing data of the network. Additionally, ORACE-Net has a control packet (i.e., ADV). Energy-awareness and the overhead are detailed later in Table 3.7.

Table 3.1: Routing Protocols Benchmark.

	Specifications					
Routing Protocol	Strategy	Beacon-less (optional)	Control-Packet	PSN-Architecture	Scalability	Energy-aware
AODVv2	Reactive	No	Yes	Flat	Scalable	No
OLSRv2	Proactive	No	Yes	Flat	Scalable	No
GPSR	Geographic-Based	No	No	Flat	Depends on Positioning system	No
ORACE-Net	**Optimized-Proactive**	No	Yes	**Hierarchic (CC-node, simple nodes)**	Scalable	Yes

In order to evaluate the studied routing protocols (one from each routing class) in order to learn the drawbacks of each in the context of urban sensing critical operations, we decided to consider a realistic simulation. The next subsection details the scenario and the performance evaluation.

3.2.1 Investigation of the Studied Protocols through Realistic Disaster Scenario with Different MAC/PHY Standards

The previous section provides a qualitative comparison of the studied routing protocols (i.e., OLSRv2, AODVv2, GPSR, DD and ORACE-Net). In order to emphasize

the drawbacks of these protocols, selected as one from each routing class (i.e., Proactive, ereactive, geographic-based and gradient-based), among the disaster context, hereafter, we evaluate them in realistic discrete simulation.

The evaluation of a routing protocol in a specific context, strongly depends on the accurate mobility models. Mobility models metrics are classified as follows [103]:

- Random based: no dependencies or restriction,
- Temporal dependencies: current movements depend on the past ones,
- Spatial dependencies: movements depend on the movements of the surrounding units,
- Geographical restrictions: geographic restriction on the movements,
- Hybrid structure: Integration of two or more models.

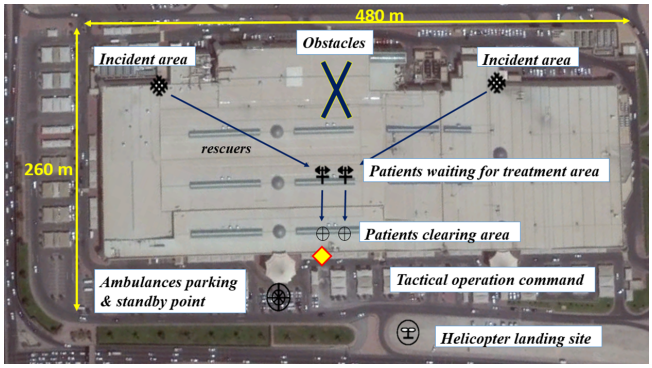


FIGURE 3.3: Overview of the Disaster Scenario in the Landmark Shopping Mall.

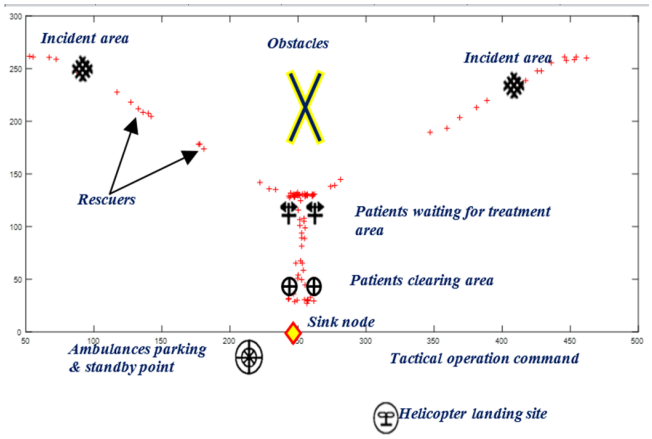


FIGURE 3.4: Disaster Area Nodes Locations, Areas and Obstacles.

An hybrid structured disaster area model designed by Aschenbruck in [104] divides the catastrophe area into four different sub-areas. First, incident site contains one or more incident area(s) that represent(s) the exact incident location (e.g., coordinates of aircraft crash, coordinates of a fire trigger, etc.). Second, casualties treatment area contains one or more patients waiting for treatment area and casualties clearing station. Then, the transport zone with ambulances and eventually rescue helicopter(s).

The last sub-area is the hospital zone, which is often not represented, because size constraints, so arriving to the transport zone, casualties are considered cleared and safe. The last and important component in this model is the location of the command center responsible for conducting the rescue and emergency operations.

In this sub-section we investigate a disaster scenario (fire triggering as a case study) in the "Landmark" shopping mall in the State of Qatar as depicted by Figure 3.3. The mobility model used is generated by the BonnMotion tool. Let us first consider some logistic aspects for the mobility scenario. We consider that the incident is caused by a fire in two opposite sides in the mall (Figure 3.3). Then rescuers are called to react along with firefighters and medical teams. Firefighters are divided into 3 groups of vehicles with 26 firefighters in each group. Medical emergency teams that probably could reach the mall just after the incident, are consisting of 6 ambulances with 5 medical staff in each ambulance (30 personal in total).

Further, police officers and civil defense personals are also considered to support the emergency teams (we have considered 18, to have a total of 100 rescuers). We consider all the rescuers as moving nodes and sending their gathered information to one main sink node placed at the main-gate of the mall (shown as yellow diamond in Figure 3.3). Data sent could be rescuers and/or victims health status, ambient rescuing conditions, special medical requests, etc., based-on simple data, voice, images and/or video.

We provide, area perimeter coordinates, obstacles coordinates, number of nodes (i.e., personal in our case) in each incident area, transported nodes in each group of nodes, etc., as an input parameters to BonnMotion. As an output, we obtain a mobility trace file containing the movement of all the nodes during the observation time. The generated mobility trace file is used as an input for the comparative evaluation of the routing protocols (as illustrated in Figure 3.5) discussed in the following part.

3.2.1.1 Performance Evaluation

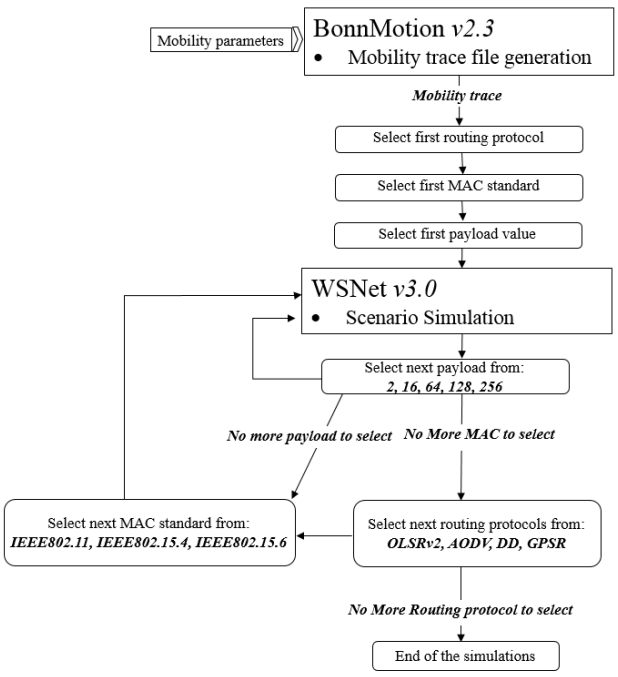


FIGURE 3.5: Simulation Methodology.

3.2.1.1.1 Simulation Setup In this section, proactive (i.e., OLSRv2), reactive (i.e., AODV), geographic based (i.e., GPSR) and gradient based (i.e., DD) routing protocols are evaluated using a realistic disaster mobility model. In addition, we consider various communication technologies including WiFi (i.e., IEEE 802.11 standard), WBAN (i.e., IEEE 802.15.6 standard) and WSN (i.e., IEEE 802.15.4 standard). These wireless technologies (i.e., MAC and PHY layers), are selected especially to analyze and evaluate inter-body communication (i.e., realized through WBAN coordinator). Subsequently, each of these technologies is implemented using above selected routing protocols for comprehensive evaluation. We are using an event-driven, packet-oriented network simulator called WSNet (version 3.0), for systems level simulations. The simulations are executed based on a realistic mobility model for 100s. We considered 10 iterations for every simulation and the 95% confidence intervals are provided. All the parameters at each layer are configured though an XML configuration file, where we vary the routing protocols for each technology.

For the performance metrics, we consider the Packet Reception Rate (PRR), Communication Delay and Energy Consumption as the main metrics. The complete simulation process as shown in Figure 5 is a set of operations iterated for 10 times to converge to the realistic behavior of the evaluated routing protocols. At first, the mobility generation tool BonnMotion with specific parameters of the studied disaster scenario generates Mobility trace file. The output file is then converted into a proper format before being parsed by the simulator WSNet. A routing protocol is then selected with a specific communication technology and an initial payload. These parameters are entered through the "XML" configuration file.

Table 3.2: LIST OF SIMULATIONS PARAMETERS AND CORRESPONDING VALUES

Standard	**MAC Layer**	**PHY Layer**	**Battery Parameters (mA)**		
			TX	**RX**	**IDLE**
WiFi IEEE 802.11	CSMA/CA DCF with ACK	Modulation BPSK, Sensitivity = -92dBM, TX Power = 0dBm, 2.4GHz	160	53	0.69
WSN IEEE 802.15.4	CSMA/CA without ACK	Modulation O-QPSK, Sensitivity = -85dBM, TX Power = 0dBm, 2.4GHz	17.4	19.7	0.9
WBAN IEEE 802.15.6	CSMA/CA with ACK	Modulation DQPSK, Sensitivity = -85dBM, TX Power = 0dBm, 2.4GHz	17.4	19.7	0.9

3.2.1.1.2 Application & Routing Layers At the application layer, we consider 99 moving nodes (i.e. WBANs coordinators) inside the shopping mall sending data packets to one sink node (i.e. command center), here node 0, which is placed at the main gate of the mall. Distance between nodes, movements, directions and speed are calculated according to the mobility model. A Constant Bitrate Rate (CBR) application is used to generate the traffic (with one packet/s), with available data payload ranging from 2 bytes to 256 bytes. At the network layer, a routing protocol detailed in the previous sub-section is selected as illustrated in the simulation process (cf. Figure 3.6). The routing layer receives the packets from the application layer, depending on the routing protocol; all the configuration parameters are equally affected. Each routing approach will be evaluated with individual technology detailed in Table 3.2.

3.2.1.1.3 MAC & PHY Layers At the MAC layer, we are employing unified distributed CSMA/CA protocol for the three wireless technologies. It includes DCF IEEE 802.11 (for Wifi) which employs a CSMA/CA with binary exponential back-off algorithm. It uses CTS/RTS control signals for better reliability. IEEE 802.15.4-based CSMA/CA (for WSN) is implemented with maximum back-off exponent set as 3; maximum back-off is 5 without any re-transmission. Finally, IEEE 802.15.6 (for WBAN) CSMA/CA MAC protocol with immediate acknowledgment policy is implemented. We have exploited the higher emergency level feature of this standard (i.e. 2) for the transmitted packets. The maximum back-off is set as 5 and re-transmission limit is 3. Along with the selected MAC layers, corresponding modulation schemes, physical configuration parameters including transmit power levels and corresponding current consumptions (of the widely used radio transceivers i.e., cc2420 for WSN/WBAN, and cc3100 for WiFi) are detailed for various states in Table 3.2.

3.2.1.2 Simulation Results

In this sub-section, the performance of OLSRv2, AODVv2, GPSR and DD are investigated with the WiFi, WSN and WBAN technologies (i.e. IEEE 802.11, IEEE 802.15.4 and IEEE 802.15.6 standards). Parameters settings were configured for the context of PSN.

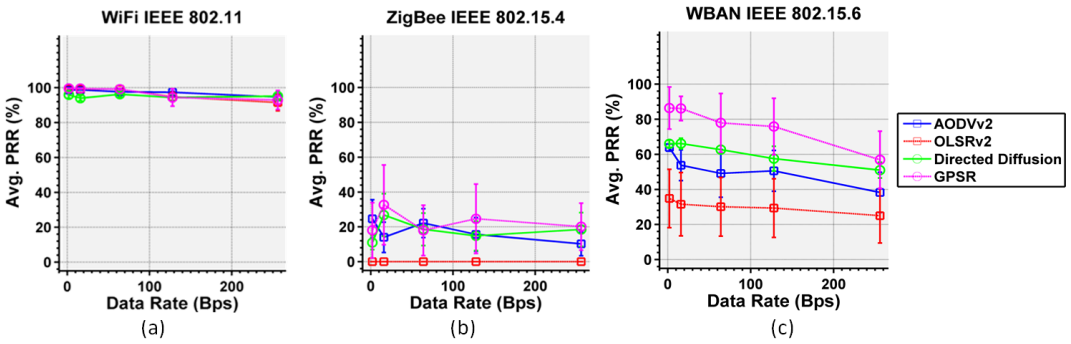


FIGURE 3.6: Average Packet Reception Rate for AODVv2, OLSRv2, DD and GPSR using the three WiFi, WSN and WBAN Technologies.

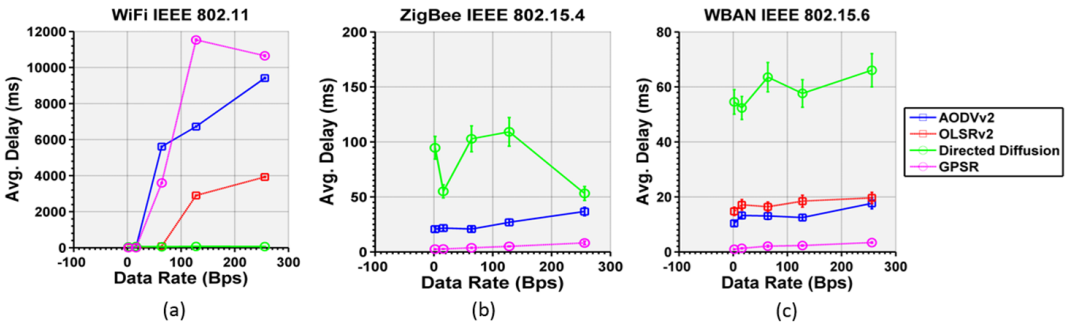


FIGURE 3.7: Average Communication Delay for AODVv2, OLSRv2, DD and GPSR using the three WiFi, WSN and WBAN Technologies.

3.2.1.2.1 Packet Reception Rate (PRR) The results of average PRR for the four selected protocols and three technologies are shown in Figure 3.5. Generally, the evaluated routing protocols perform much better using WiFi in comparison to the

others technologies, overall it achieves more than 92% of PRR. In particular, with low payloads (i.e. 2 and 16 bytes), only DD PRR is below 96% whereas, OLSRv2, AODVv2 and GPSR are all able to achieve above 99% PRR. Starting from 64 bytes and higher payload, DD performance also starts improving to exceed others protocol performance as can be seen in Figure 3.5-a. GPSR and OLSRv2 showed similar performance. AODVv2 has best performance with WiFi at 128 bytes payload, and performs similar as DD with 256 bytes payload. Finally, GPSR shows slightly lower performance with more than 128 bytes payload. This is due to the perimeter forwarding technique which may occur several times due to the obstacles located in the mobility model. For the case of WSN IEEE 802.15.4 (ZigBee), in general, all the protocols are under-performed as shown in Figure 3.5-b. As the best case, 33% of average PRR was achieved using GPSR. Even with the lowest payloads, the performance remained very low. OLSRv2 was not able to deliver any packet at all with the various payload values. WSN is a short-range communication technology, with high mobility nodes such as defined in the mobility model and according to the nodes density in the shopping mall; evaluated routing protocols are unable to perform well with WSN. Additionally, by using CSMA/CA MAC without any acknowledgment policy the performance further degrades. WBAN (i.e., IEEE 802.15.6) is mainly an intra-BAN communication technology, but recently, research trends are tend to evaluate this standard in inter-BAN context [105]. For this reason, we are investigating IEEE 802.15.6 standard to achieve the potential limits studied in [106]. In WBAN generally, most of the protocols perform much better in comparison to WSN technology. In particular, GPSR outperforms the other routing approaches again, it achieves up to 88% PRR under low payloads (2 and 16 bytes). However, by increasing the payload, GPSR starts to gradually degrade in performance same as the case in other technologies however,GPSR remains the best protocol. OLSRv2 has the worst performance, whereas both DD and AODVv2 also reach below 50% average PRR with 256 bytes. As we analyzed the performance given by combining one of the evaluated routing protocols with WBAN IEEE 802.15.6, GPSR meets the disaster scenario requirements with low payload, the rest of protocols are inconclusive. It is necessary to notice that while considering WBAN technology, the low data rate is a limitation in terms of image and video transfer. Finally, the evaluated routing protocols used with WiFi are convincingly better than the two counterparts in terms of average PRR. Only, GPSR performed well with WBAN.

3.2.1.2.2 Latency We considered latency as the average packet delay between the source node and the final destination over a multi-hop BBN. Generally, the results of the delay are inter-related with PRR, if PRR is higher then, delay will be lower. Focusing onto WiFi technology, with low payloads (i.e. 2 and 16 bytes), all routing protocols delay is below 80ms which satisfy our application context. Figure 3.7-a shows an exponential increase in delay for AODVv2 and GPSR starting from 16 bytes of payload, while OLSRv2 delay remains slightly lower than 80ms until 16 bytes. DD is the most efficient and has almost negligible delay among all protocols and therefore is considered as the most effective protocol in terms of delay using WiFi technology.

In comparison to the other evaluated protocols, DD has very low calculation for data routing. While, AODVv2 with an on-demand routes lookup technique and GPSR which also bases its routing table on geographic locations calculations which require more time to route calculation before data transfer which adds an additional significant delay. Figure 3.7-b, shows the average delay for WSN. It is clear that comparatively, it is extremely (i.e., 100 times) better than WiFi. AODVv2, DD and GPSR all perform very well even at higher payloads sizes. Exceptionally, OLSRv2

performance is the worst one since it was unable to transmit any packet and had zero average PRR, therefore the delay is irrelevant for it. Although, DD shows slightly more delay comparing to the other two protocols, but overall it is below 100ms as well. With WBAN technology, in addition to the respectable PRR recorded by GPSR with low payload, all the routing approaches perform much better in term of delay with WBAN technology than with the rest of the communication technologies. Results in Figure 3.7-c, show that delays are very low in comparison to the delays recorded with WiFi and WSN technologies. Finally, concerning the delay, WBAN and WSN outperformed WiFi in most of the protocols. Only in case of GPSR with WBAN, the results are comparable and it is the most effective protocol for optimized delay performance.

3.2.1.2.3 Energy Consumption The energy consumption for each transmitted packet is calculated as follows: $E_{packet} = T_{packet} \times 3_{volts} \times I_{mA}$

where, T_{packet} is the duration in ms which is based on the effective packet length (including all the PHY and MAC headers[106]). The current consumption values for two different considered radio transceivers are mentioned in Table 3.2. For WiFi, approximately linear increase in energy consumption is observed with an increase in payload size for all the protocols as shown in Figure 3.7–a. There is hardly any difference between the protocols for 2 and 16 bytes of payload. However, for higher payloads it is notable that AODVv2 consumes the highest energy, whereas GPSR is the most energy efficient protocol.

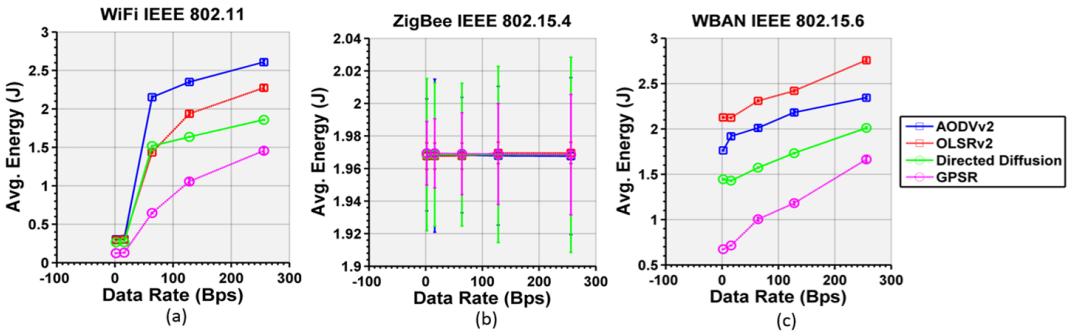


FIGURE 3.8: Average Energy Consumption for AODVv2, OLSRv2, DD and GPSR using the three WiFi, WSN and WBAN Technologies.

In general, all routing protocols have performed much better with WSN for energy efficiency. By increasing the payloads, the energy consumption decreases for AODVv2, DD and GPSR. It seems that OLSRv2 performed very well in terms of energy consumption, but since it does not able to transmit any data packet, this reflection is not for a successful transmission and hence irrelevant In addition, the behavior of OLSRv2 is a reflection of continuous routes maintenance operations, which increases energy consumption even without packet receptions. Despite of that OLSRv2 improves OLSR features, though, it still not scalable and destined for small networks with small data traffic. Using WBAN, routing protocols, except AODVv2 and GPSR have similar pattern, i.e., energy consumption slightly decrease with the increase in payload. OLSRv2 performs better than the other routing protocols. A slight difference of energy consumption is noticed between the evaluated routing protocols. Finally, in terms of energy efficiency, WBAN communication technology is most suitable with the evaluated routing protocols.

To summarize, definitely WiFi is the most relevant for the reliable communication but at an expense of significant increase in delay. In this aspect WBAN technology is most effective and by using GPSR routing protocol it can be a considerable option for BBN. GPSR with both WiFi and WBAN is able to achieve high packet reception and consumes relatively much lower energy with low delay. Referring to our network topology (i.e., converge cast) and mobility scenario, GPSR is one of the most favorable protocol as reflected in Table 3.3. Finally, for small-scale rescue and critical operations using BBN, both WiFi and WBAN can be considered based on the given constraint, either PRR or delay.

TABLE 3.3: COMPARATIVE TABLE FOR ROUTING PROTOCOLS BEHAVIOR WITH DIFFERENT WIRELESS TECHNOLOGIES

Standards	Routing	PRR	Delay	Energy
WiFi IEEE 802.11	AODVv2	High	High	High
	OLSRv2	High	High	Medium
	DD	Medium	Low	Medium
	GPSR	**High**	High	**Low**
WSN IEEE 802.15.4	AODVv2	Low	Low	Low
	OLSRv2	Worst	Worst	Worst
	DD	Low	High	Low
	GPSR	Low	**Low**	Low
WBAN IEEE 802.15.6	AODVv2	Low	Low	Low
	OLSRv2	Low	Low	**Low**
	DD	Medium	Medium	Low
	GPSR	**High**	**Low**	**Low**

3.2.1.3 Summary

In this section, a particular emphasis is given to the emerging body-to-body communication whilst evaluating best wireless technologies and routing strategies under realistic mobility scenario for public safety and disaster relief operations. Three technologies (i.e., WiFi IEEE 802.11, WSN IEEE 802.15.4 and WBAN IEEE 802.15.6) and four different class of routing protocols are considered including mobile Ad hoc (i.e., OLSRv2 and AODVv2), data centric (directed diffusion) and geographical location-based (GPSR). It is concluded that WiFi is the best technology for both packet reception ratio and energy efficiency performance metric. Whereas, as far as the packets delay is concerned, WBAN is the most effective technology. Among the protocols, by assuming that we have location information, then GPSR performed the best in comparison to all other protocols using WiFi IEEE 802.11. The only exception is with delay results, where DD outperformed all other protocols. If location information is not available, then DD especially with WBAN IEEE 802.15.6 can be considered as a favorable choice. However, it is important to note that WBAN has maximum payload limit of 256 bytes which limits it to the transmission of real-time audio or video.

3.3 Analytical study of the existing routing protocols vs ORACE-Net

This chapter provides the analytical analysis based on the preliminary investigation of the various routing approaches as discussed in Chapter 2, including AODVv2, OLSRv2, GPSR and newly proposed ORACE-Net protocol.

The objective of this analytical analysis is to evaluate the different routing protocols in terms of their communication costs (or overheads, such as neighbor discovery process, path establishment and finally the data communication). To achieve this objective, we model the wireless communication links between the PSN nodes (i.e., D2D or B2B links) and we analyze the network lifetime for the above mentioned routing protocols. In this regard, we extend the analytical framework presented in [11].

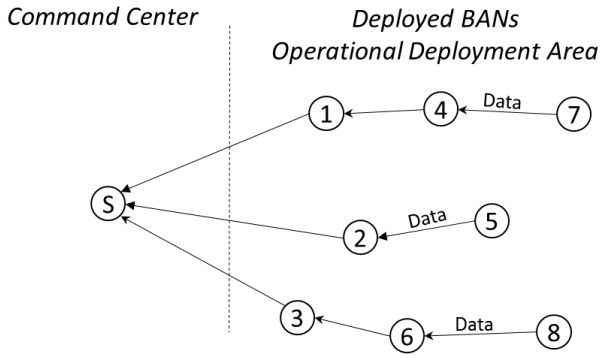
For simplicity, we assume that we have an ideal medium access (MAC) layer and radio channel (i.e., no packets loss or re-transmissions). However, later in Section 3.4, we will consider realistic IEEE 802.11 physical and MAC models for the evaluation of these routing protocols. Finally, the total communication cost of the various routing protocols and the numerical results of the lifetime are presented. Tables 3.4 and 3.5 present all the variables and symbols being used in the following study.

TABLE 3.4: Various nomenclature being used throughout the analytical analysis

Nomenclature	**Representation**
Transmitted hello packets	$H^{TX}_{Protocol}$
Received Hello packets	$H^{RX}_{Protocol}$
Transmitted Route Establishment Packets	$RE^{TX}_{Protocol}$
Received Route Establishment Packets	$RE^{RX}_{Protocol}$
Transmitted data packets	$D^{TX}_{Protocol}$
Received data packets	$D^{RX}_{Protocol}$
Total transmitted overhead cost	$C^{TX}_{Protocol}$
Total received overhead cost	$C^{RX}_{Protocol}$
Total Energy	$E^{Total}_{Protocol}$

3.3.1 Scenario

Let us consider a disaster scenario which consists of N number of nodes including a command center node (*CC-node*). More details about the disaster incidents area can be found later in Section 3.4. The overall communication is established in three steps. During the first step, periodic hello packets of size ($i.e., HELLO_s$) are broadcasted for the neighbor discovery process (if applicable). Once all the neighbor nodes are identified, route establishment (i.e., RE) process starts with periodic transmission of the control packets followed by the data packets transmission of size $DATA_s$. To represent the communication costs for the protocols in the different processes (i.e., Neighbor Discovery, Route Establishment and Data Communication), we use the notations as illustrated in Table 3.4 where each protocol is termed with its associated name in each equation.



Routing Table for CC-Node S

DST	Next_Hop	Hops	E2E_LQE	Link_Lifetime
1	1	1	0.9	2s
2	2	1	1.0	1s
3	3	1	1.0	5s
4	1	2	0.95	2s
5	2	2	1.0	1s
6	3	2	0.9	4s
7	1	3	0.92	1s
8	3	3	0.95	3s

Routing Table for Node 4

DST	Next_Hop	Hops	E2E_LQE	Link_Lifetime
S	1	2	0.9	3s
7	7	1	1.0	3s

Routing Table for Node 2

DST	Next_Hop	Hops	E2E_LQE	Link_Lifetime
S	S	1	1.0	4s
5	5	1	1.0	3s

FIGURE 3.2: Reverse Route Establishment (i.e., RRE) based on data packets.

TABLE 3.5: Various used parameters and their corresponding symbols.

Symbols	**Description**	**Symbols**	**Description**
N	Number of nodes	Υ	Average number of neighbors nodes
r	radio range	λ_0	Spatial intensity
h	number of hops	D	Euclidean Distance
α	scaling factor	$HELLO_s$	Hello Packet size
$RREQ_s$	Route Request Packet of size	$RREP_s$	Route Request Packet size
H_{period}	Hello period	RE_{period}	Route Establishment period
W	Time	D_{period}	Data period
t_B	Time to transmit one byte	I_{mA}^{Tx}	Transmit current
I_{mA}^{Rx}	Receive current	I_{mA}^{Idle}	Idle current
V_{volts}	Voltage	$MPRs_{Avg}$	Average multi-point relay selection
TC_s	TC packet size	I_{mA}^{GPS}	Current consumption of GPS transceiver
ADV_s	Advertise packet size	E_{DISP}	Energy consumed to display (screen)
E_{CPU}	Energy consumed by the CPU		

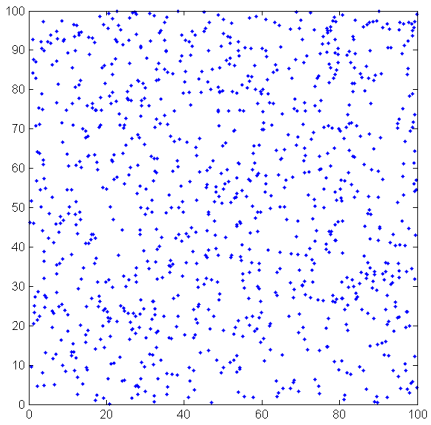


FIGURE 3.9: Poisson point distribution over $100m \times 100$m geographical area with $\lambda_0 = 0.1$.

3.3.2 Network Models

For simplicity of the analytical analysis, we assume a static network topology with a large number of nodes (N), which are deployed in a square field of size 100×100 (as shown in Figure 3.9). We consider that the nodes are uniformly and independently distributed in this region. The network is modeled by a two-dimensional *Poisson point process* ϕ_0 of constant spatial intensity λ_0 (i.e., the mean number of nodes per unit area).

In order to evaluate the average number of neighbors (Υ), we use a stochastic geometry modeling of the network based on the aforementioned Poisson point process. With such a process, first, the number of points (i.e., independently and uniformly distributed) lying in a region R of the plane follows a discrete Poisson law. If $\psi_0(R)$ is the random variable which counts the number of points laying in R, then we have,

$$P(\psi_0(R) = k) = \frac{(\lambda_0 |R|)^k}{k} \times e^{-\lambda_0 |R|} \tag{3.4}$$

where k is a positive integer.

Let us assume that r is the circular communication range of each node, consequently, the average number of neighbors per node (Υ) can be calculated as;

$$\Upsilon = \pi \times r^2 \times \lambda_0, \tag{3.5}$$

where, λ_0 is the spatial intensity of the Poisson point process.

Finally for the average number of hops, let us consider h as the number of hops on a path between two arbitrary nodes X and Y such that $(D = |X, Y|)$ is the Euclidean distance of the path between the two nodes [11]. For a given routing protocol, the average hop count, between two arbitrary nodes, can be approximated as:

$$h = \alpha \frac{D}{r} \tag{3.6}$$

where, r is the communication range, D is the Euclidean distance between the two nodes, and α is a scaling factor [11] which vary depending on the spatial node density λ_0 and it is often greater than one (i.e., $\alpha \geq 1$) [11]. For numerical simplifications, we will assume that $\alpha = 1$.

3.3.3 Communication Overhead

The communication overhead cost of the routing protocols is computed based on the three steps (i.e., neighbor discovery, route establishment and the data transmission) as explained in Section 3.3.1. For example, AODVv2 protocol requires, hello packet (i.e., $HELLO_s$) for neighbor discovery, route request packet (i.e., $RREQ_s$) and route reply packets (i.e., $RREP_s$) for route establishment (RE) and the data packet ($DATA_s$). The route establishment process in OLSRv2 is achieved through TC packets (TC_s), whereas, GPSR does not require route establishment since it rely on the location information. Finally, ORACE-Net establishes the path through advertisement packets (ADV_s). The packet sizes are different in various standards and protocols, please note that, we consider the packets being used for the route establishment process as control packets.

TABLE 3.6: List of Parameters and their corresponding values.

Parameters	**Values**	**Parameters**	**Values**
λ_0	100%	Area	500×300
N	100	Υ	5.26
r	$50m$	h	5.2
hello period	$3s$	RE period	$5s$
Data period	$2s$	$MPRs_{Avg}$	50%
Battery Capacity (C)	$2300mAh$	V_{volts}	3
I_{mA}^{IDLE}	$0.69mA$	I_{mA}^{TX}	$233mA$
I_{mA}^{RX}	$53mA$	I_{mA}^{GPS}	$47.7mA$
t_B	$6.93 \times 10^{-7}s$	Data rate	$11Mb/s$
E_{DISP}	$259mA$	E_{CPU}	$462mA$
$Transmitpower$	$0dBm$		

3.3.3.1 AODV-v2 Routing Protocol

In AODV, a node does not perform route discovery or maintenance until it is needed. A route discovery in AODV is initiated by the source node (S) through the broadcast of a specific route request (RREQ) to all its first hop neighbors. This route request is transferred through broadcast until it reaches the destination. The protocol is based on a process with three steps as explained below.

In the first step (i.e., neighborhood discovery), the total number of bytes transmitted by the hello packets (H_{AODV}^{TX}) and the total number of bytes received by the hello packets (H_{AODV}^{RX}) can be calculated as;

$$H_{AODV}^{TX} = N \times HELLO_s, \tag{3.7}$$

and

$$H_{AODV}^{RX} = N \times \Upsilon \times HELLO_s. \tag{3.8}$$

Where, N is the number of nodes, Υ is the average number of neighbor nodes and $HELLO_s$ is the size of hello packet.

The second step consists in the route establishment (RE) and during this phase, each node transmits a route request packet (where the packet size is $RREQ_s$) to all reachable nodes. This route request is forwarded by the receiving node to its

reachable neighbors. It is assumed that each node has explored all the neighbors before sending data, this process is assured by all nodes of the network by N times. Thus, the total number of transmit (RE^{TX}_{AODV}) and receive (RE^{RX}_{AODV}) packets (in terms of bytes) respectively during the route establishment process can be calculated as;

$$RE^{TX}_{AODV} = N \times (N \times RREQ_s + h \times RREP_s), \tag{3.9}$$

and

$$RE^{RX}_{AODV} = ((N \times N \times RREQ_s) + (N \times h \times RREP_s)) \times \Upsilon. \tag{3.10}$$

Where, $RREQ_s$ and $RREP_s$ are the control packets sizes.

The third step is data propagation. A data packet communication overhead consists in the number of times the data packet is forwarded from a node to another which is the average number of hop counts from a random source node to a *CC-node*. The total number of transmit (D^{TX}_{AODV}) and receive (D^{RX}_{AODV}) data packets (in terms of bytes) can be calculated respectively as;

$$D^{TX}_{AODV} = N \times h \times DATA_s, \tag{3.11}$$

and

$$D^{RX}_{AODV} = N \times h \times \Upsilon \times DATA_s. \tag{3.12}$$

The total communication overhead from (3.7) to (3.12) (i.e., hello, route establishment and data communication) for a time period of W and their periodic transmission interval, is the sum of transmit, receive and idle states. Thus, the total overhead cost can be expressed as;

$$\begin{aligned} C^{TX}_{AODV}(W) = \frac{W}{H_{period}} \times H^{TX}_{AODV} + \frac{W}{RE_{period}} \times \\ RE^{TX}_{AODV} + \frac{W}{D_{period}} \times D^{TX}_{AODV}, \end{aligned} \tag{3.13}$$

and

$$\begin{aligned} C^{RX}_{AODV}(W) = \frac{W}{H_{period}} \times H^{RX}_{AODV} + \frac{W}{RE_{period}} \times \\ RE^{RX}_{AODV} + \frac{W}{D_{period}} \times D^{RX}_{AODV}. \end{aligned} \tag{3.14}$$

Where; H_{period}, RE_{period} and D_{period}, is the periodic interval of the hello, route establishment and data packets, respectively.

It is important to point here that AODVv2 is a reactive routing protocol where the route establishment (RE) phase is only launched when there is data to send. But based on the dynamic mobility models we used (i.e., Random Waypoint and Disaster Area Scenario) and to raise a fair comparison between the protocols, we specified the same period of RE for all of the protocols.

Finally, the total energy consumption (E^{Total}_{AODV}) is the sum of the above communication overheads (i.e., number of bytes) in TX, RX and IDLE states, times the amount of time required to transmit one byte (t_B). Further, various current consumption levels (I^{TX}_{mA}, I^{RX}_{mA}, I^{IDLE}_{mA}) are used for respective states along with the used battery voltage (i.e., V_{volts}). Thus, the total energy consumed during a period of W of time can be expressed as;

$$\begin{aligned} E^{Total}_{AODV}(W) = (C^{TX}_{AODV}(W) \times t_B \times I^{TX}_{mA} \times V_{volts}) \\ +(C^{RX}_{AODV}(W) \times t_B \times I^{RX}_{mA} \times V_{volts}) \\ + \Big[W - (C^{TX}_{AODV}(W) \times t_B + C^{RX}_{AODV}(W) \times t_B)\Big] \\ \times I^{IDLE}_{mA} \times V_{volts}. \end{aligned} \tag{3.15}$$

3.3.3.2 OLSR-v2 Routing Protocol

OLSRv2 is a proactive link state routing protocol that uses periodic local and global signaling for neighbor/link discovery and link state diffusion. There are three main steps which are followed in this routing approach i.e., neighborhood discovery, Multi-Point Relay (MPR) selection, routing table calculation and maintenance.

The total number of bytes being transmitted (i.e., H^{TX}_{OLSR}) and received (i.e., H^{RX}_{OLSR}) by the hello packets can be calculated with the same equations as (3.7) and (3.8), with only modification to the hello packet size being used in OLSRv2 standard.

In the MPR selection step, the total number of transmission and reception is based on two steps according to [107]. We consider that, 50% similar to in[108] of the first hop neighbors are considered as MPRs, ($MPRs_{Avg} = 50\%$). The total number of transmit and receive packets (in terms of bytes) in the route establishment phase (i.e., RE^{TX}_{OLSR} and RE^{RX}_{OLSR}) can be calculated as;

$$RE^{TX}_{OLSR} = N \times N \times MPRs_{Avg} \times TC_s, \tag{3.16}$$

and

$$RE^{RX}_{OLSR} = N \times N \times MPRs_{Avg} \times \Upsilon \times TC_s. \tag{3.17}$$

Where TC_s is the size of the Topology Control packet of OLSR During the data propagation, the total number of transmit and receive data packets (in terms of bytes) (i.e., D^{TX}_{OLSR} and D^{RX}_{OLSR}) respectively can be calculated using Eq. 3.11 and Eq. 3.12, with only modification to the data packet size. Further, the cost of the total communication overhead (for the transmission i.e., C^{TX}_{OLSR}) for a time period of W and periodic transmission interval of above packets can be expressed as;

$$\begin{aligned} C^{TX}_{OLSR}(W) = \frac{W}{H_{period}} \times H^{TX}_{OLSR} + \frac{W}{RE_{period}} \times \\ RE^{TX}_{OLSR} + \frac{W}{D_{period}} \times D^{TX}_{OLSR}. \end{aligned} \tag{3.18}$$

Whereas, for the reception (C^{RX}_{OLSR}), it can be calculated as;

$$\begin{aligned} C^{RX}_{OLSR}(W) = \frac{W}{H_{period}} \times H^{RX}_{OLSR} + \frac{W}{RE_{period}} \times \\ RE^{RX}_{OLSR} + \frac{W}{D_{period}} \times D^{RX}_{OLSR}. \end{aligned} \tag{3.19}$$

Where; H_{period}, RE_{period} and D_{period}, is the periodic interval of the hello, route establishment,and data packets respectively. Finally, the total energy consumption (E^{Total}_{OLSR}) is the sum of the above communication overheads in TX and RX states along with IDLE state which can be computed as;

$$\begin{aligned} E^{Total}_{OLSR}(W) = (C^{TX}_{OLSR}(W) \times t_B \times I^{TX}_{mA} \times V_{volts}) \\ +(C^{RX}_{OLSR}(W) \times t_B \times I^{RX}_{mA} \times V_{volts}) \\ +(\Big[W - (C^{TX}_{OLSR}(W) \times t_B + C^{RX}_{OLSR}(W) \times t_B)\Big] \\ \times I^{IDLE}_{mA} \times V_{volts}). \end{aligned} \tag{3.20}$$

3.3.3.3 GPSR Routing Protocol

GPSR uses the nodes location and the wireless connectivity. It uses two forwarding techniques i.e., greedy forwarding and perimeter forwarding. In greedy forwarding, packets from source node to destination are forwarded throughout the geographically closest next hop towards the destination. When a greedy forwarding is impossible, the protocol routes the packets in the surrounding perimeter of the destination. GPSR returns to the greedy forwarding early when a local maxima (local parameter) is reached. GPSR maintains only its location and locations of its neighbors.

With GPSR, nodes broadcast their geographical position within a known interval. After this specified interval of time, a node is considered unreachable (or disconnected). Thus, if we have N nodes in the network, we have N broadcasts. The total number of transmit and receive hello packets (in terms of bytes) (i.e., H^{TX}_{GPSR} and H^{RX}_{GPSR}) can be calculated with the same equations i.e., (3.7) and (3.8), with only modification to the hello packet size being used in GPSR (as shown in Table 3.5).

For the routing establishment process in GPSR, packets are routed (or forwarded) to the nearest neighbor towards the direction of the destination. This is simply calculated based on the geographic location of the nodes collected within the neighborhood discovery phase. For the data propagation, the total number of bytes being transmitted and received by the data packets (i.e., D^{TX}_{GPSR} and D^{RX}_{GPSR}) can be calculated using equations (3.11) and (3.12), with only modification to the data packet size. Further, the cost of the total communication overhead for the transmission (C^{TX}_{GPSR}) for a time period of W and periodic transmission interval of hello (H_{period}) and data packets (D_{period}) can be expressed as;

$$C^{TX}_{GPSR}(W) = \frac{W}{H_{period}} \times H^{TX}_{GPSR} + \frac{W}{D_{period}} \times D^{TX}_{GPSR}. \tag{3.21}$$

Whereas, for the reception (C^{RX}_{GPSR}), it can be calculated as;

$$C^{RX}_{GPSR}(W) = \frac{W}{H_{period}} \times H^{RX}_{GPSR} + \frac{W}{D_{period}} \times D^{RX}_{GPSR}. \tag{3.22}$$

Where; H_{period} and D_{period}, are the periodic interval of the hello and data packets respectively. Finally, the total energy consumption ($E^{Total}_{GPSR}(W)$) is the sum of the above communication overheads in TX and RX states along with IDLE state. In addition, the energy cost of the GPS receiver is also added for a realistic evaluation of GPSR protocol. The total energy can be computed as;

$$\begin{aligned} E^{Total}_{GPSR}(W) = (C^{TX}_{GPSR}(W) \times t_B \times I^{TX}_{mA} \times V_{volts}) \\ +(C^{RX}_{GPSR}(W) \times t_B \times I^{RX}_{mA} \times V_{volts}) \\ +(\Big[W - (C^{TX}_{GPSR}(W) \times t_B + C^{RX}_{GPSR}(W) \times t_B)\Big] \\ \times I^{IDLE}_{mA} \times V_{volts}) + C^{GPS}_{GPSR}(W). \end{aligned} \tag{3.23}$$

Where; $C^{GPS}_{GPSR}(W)$ is the total consumed energy by the GPS receiver during a W period of time.

3.3.3.4 ORACE-Net Routing Protocol

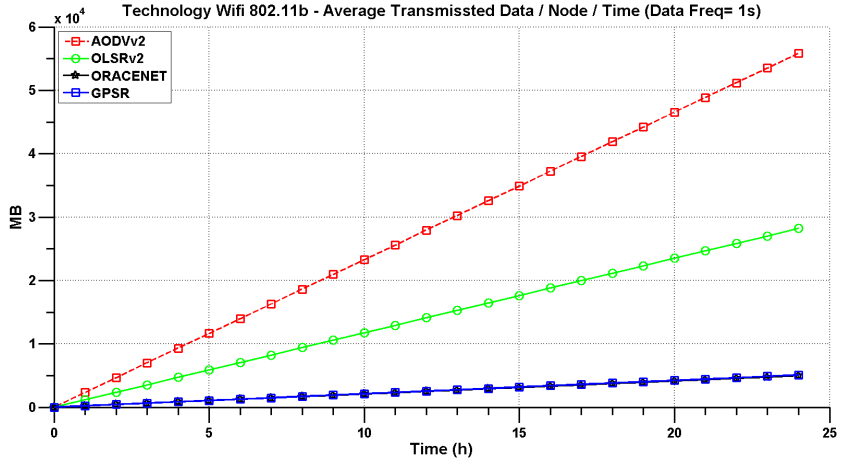


FIGURE 3.10: Average Transmitted Packets per node over 24 hours in MBytes.

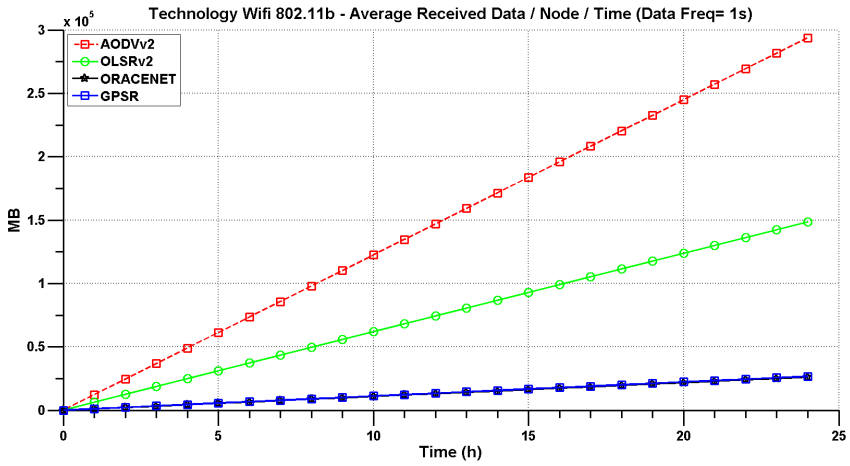


FIGURE 3.11: Average Received Packets per node over 24 hours in MBytes.

The total number of transmitted and received hello packets (in terms of bytes) (i.e., $H^{TX}_{ORACE-Net}$ and $H^{RX}_{ORACE-Net}$) can be calculated with the same equations i.e., (3.7) and (3.8). However, we are considering, in the analytical study, that ORACE-Net is beacon-less. Indeed, beacons are option to be activated in ORACE-Net depending on the network density. ADV packets are broadcasted every period (i.e., 3s), thus, they play a main role in the neighbor discovery phase.

The direct route establishment process is achieved by sending waves of advertisements packets (i.e., ADV_s) as mentioned in Section 3.1.2 and it consists of two steps, direct or forward routes are established from the *CC-node* to the source nodes in the first step, whereas, reverse route establishment is achieved in the second step. The total number of transmitted and received packets (in terms of bytes) in the route establishment phase (i.e., $RE^{TX}_{ORACE-Net}$ and $RE^{RX}_{ORACE-Net}$) are calculated as;

$$RE^{TX}_{ORACE-Net} = N \times ADV_s, \tag{3.24}$$

and

$$RE^{RX}_{ORACE-Net} = N \times \Upsilon \times ADV_s. \tag{3.25}$$

In the data packet propagation, the total number of transmit and receive data packets (in terms of bytes) (i.e., D^{TX}_{OLSR} and D^{RX}_{OLSR}) can be calculated using equations (3.11) and (3.12), with only modification to the data packet size. Further, the cost of the total communication overhead (for the transmission i.e., $C^{TX}_{ORACE-Net}$) for a time period of W and periodic transmission interval of route establishment (RE_{period}) and data packets (D_{period}) can be expressed as;

$$\begin{aligned} C^{TX}_{ORACE-Net}(W) = \frac{W}{RE_{period}} \times RE^{TX}_{ORACE-Net} \\ + \frac{W}{D_{period}} \times D^{TX}_{ORACE-Net}. \end{aligned} \tag{3.26}$$

Whereas, for the reception ($C^{RX}_{ORACE-Net}$), it can be calculated as;

$$\begin{aligned} C^{RX}_{ORACE-Net}(W) = \frac{W}{RE_{period}} \times RE^{RX}_{ORACE-Net} \\ + \frac{W}{D_{period}} \times D^{RX}_{ORACE-Net}. \end{aligned} \tag{3.27}$$

Finally, the total energy consumption is the sum of the above communication overheads in TX and RX states along with IDLE state which can be calculated as;

$$\begin{aligned} E^{Total}_{ORACE-Net}(W) = (C^{TX}_{ORACE-Net}(W) \times t_B \times I^{TX}_{mA} \times V_{volts}) \\ + (C^{RX}_{ORACE-Net}(W) \times t_B \times I^{RX}_{mA} \times V_{volts}) \\ + (\Big[W - (C^{TX}_{ORACE-Net}(W) \times t_B + C^{RX}_{ORACE-Net}(W) \times t_B)\Big] \\ \times I^{IDLE}_{mA} \times V_{volts}). \end{aligned} \tag{3.28}$$

3.3.3.5 Routing Protocols Comparison

Table 3.7 summarizes all the addressed protocols and compare them intuitively. The costs of neighbor discovery (ND), route establishment (RE) and data transmission (DT) of the protocols are highlighted. Specific expressions required to compute these costs which are also referred in Table 3.7. It can be observed that, the comparison is in line with the life-time results presented later in Fig. 3.15 in Sec. 3.3.4.

3.3.4 Lifetime Analysis

In this section we present the numerical results of the energy consumption and the lifetime of routing protocols discussed above. The smart phones are considered to enable D2D or B2B communications.

We use the analytic expressions which are developed in section 3.3.2 and section 3.3.3. The packets size being used for neighbor discovery, route establishment and data transmission packet are shown in Table 3.8. During the route establishment, for example, in AODVv2, the control packet represents route request and route reply packets, in OLSRv2, it is called TC packet and in ORACE-Net it is an advertisement packet. It is important to note that, the MAC overhead is constant (i.e., 40 bytes

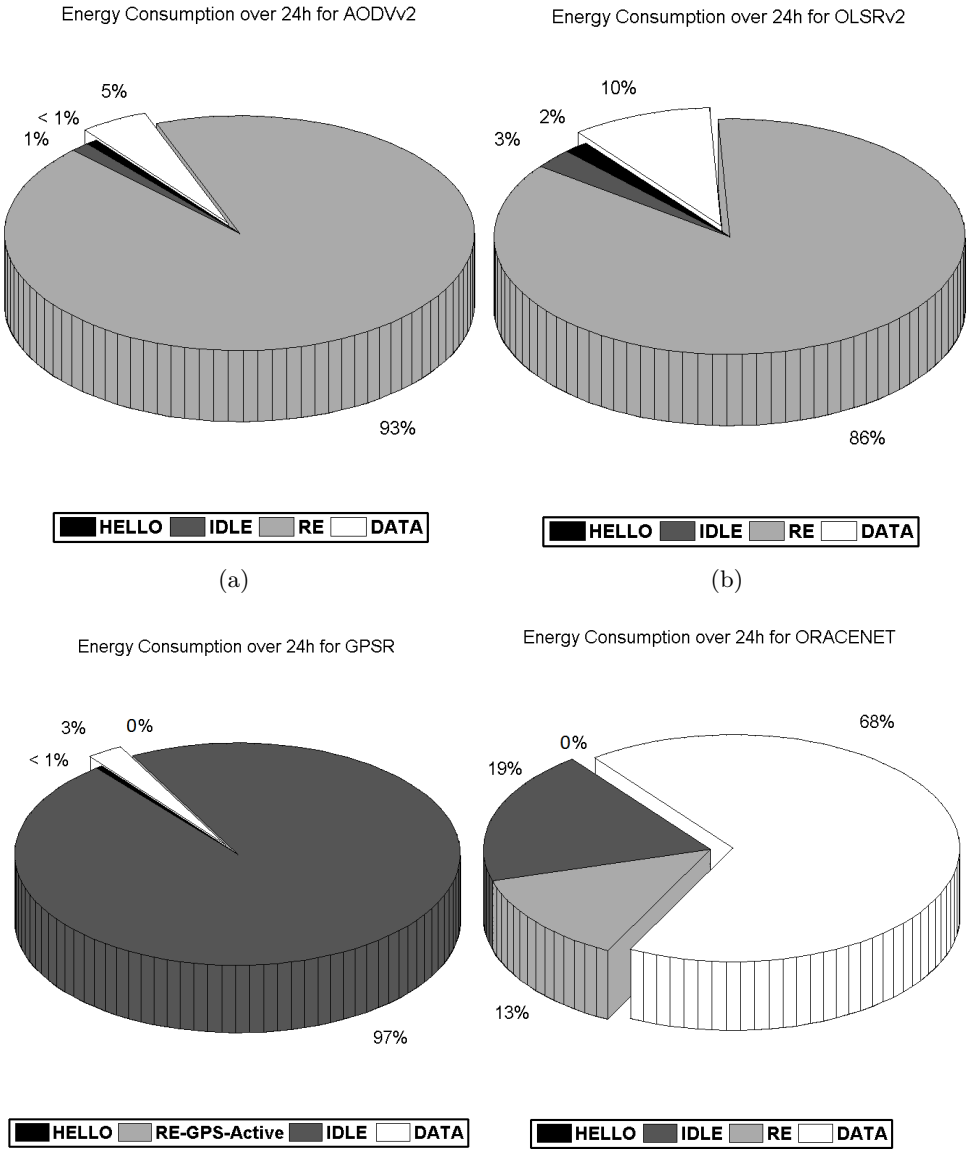


FIGURE 3.12: Average energy distribution in (a): AODVv2 (b): OLSRv2, (c): GPSR, (d): ORACE-Net.

TABLE 3.7: Routing Protocols Comparison Summary. ND: Neighbor Discovery; RE: Route Establishment; DT: Data Transmission.

	Cost						
Protocol	**ND**		**RE**		**DT**		**Total Cost**
AODVv2	Very Low		High		Medium		Medium
	TX: eq. 5	*RX: eq. 6*	*TX: eq. 7*	*RX: eq. 8*	*TX: eq. 9*	*RX: eq. 10*	*Eq. 13*
OLSRv2	Low		High		Medium		Medium
	TX: eq. 5	*RX: eq. 6*	*TX: eq. 14*	*RX: eq. 15*	*TX: eq. 9*	*RX: eq. 10*	*Eq. 16*
GPSR	Very Low		NULL		Low		Low
	TX: eq. 5	*RX: eq. 6*	-	-	*TX: eq. 19*	*RX: eq. 20*	*Eq. 21*
ORACE-Net	NULL		Medium		High		Low
	-	-	*TX: eq. 22*	*RX: eq. 23*	*TX: eq. 24*	*RX: eq. 25*	*Eq. 26*

TABLE 3.8: Packet types and sizes (in bytes) of various routing protocols (including 40 Bytes of MAC layer overhead).

Routing Protocols	Packet Types and Sizes		
	Hello ($Hello_s$)	Control	Data ($Data_s$)
AODVv2	60	64 ($RREQ_s$) / 60 ($RREP_s$)	65
OLSRv2	60	(TC_s) 60	65
GPSR	60	N/A	65
ORACE-Net	60	65 (ADV_s)	65

[109]) and it is included in all the packets sizes represented in Table 3.8. The time required to transmit one byte is (t_B). The t_B can be derived from the physical layer data rate (i.e., $11Mb/s$ for WiFi 802.11b) and is equal to $6.93 \times 10^{-7}s$ in our analysis. The periodic transmission interval of hello, route establishment and data packets are 3 seconds, 5 seconds and 1 seconds respectively. The detailed parameters list is provided in Table 3.6.

The total communication costs over 24 hours per node are illustrated by Figure 3.10 and Figure 3.11. Please note that the received traffic is higher than the transmitted one, it is due to the fact that the calculations are computed at the routing layer where all the received traffic is included (i.e., broadcasted, forwarded, etc.) as part of received packets. AODVv2 and OLSRv2 exchanged traffic is much higher than ORACE-Net and GPSR. ORACE-Net and GPSR are closely identical in terms of exchanged quantity of data. This shows that in the given scenario (detailed in **??**), ORACE-Net and GPSR are more efficient in communication overhead in comparison to AODVv2 and OLSRv2. This becomes clear when one examines the pie-charts in Figure 3.12. These pie-charts present the average energy consumption distribution over 24 hours for the considered protocols. The distribution break-down is based on the energy consumed in idle states, neighbor discovery, route establishment and finally the data communications. It can be seen that both AODVv2 and OLSRv2 (i.e., typical ad-hoc routing protocols) consumes most of the energy during route establishment (i.e., 93% and 86% respectively), whereas, GPSR has less energy consumption in RE, and it is mainly dominated by idle energy consumption. Finally, ORACE-Net optimizes RE consumption as well as the idle consumption and 86% of the energy is consumed during the actual transmission of data.

In order to have realistic numerical analysis, we have added the baseline energy consumption of the smart phones as proposed by the authors of [110] which provide a separate energy consumption averages for the different smart phones functionalities (i.e., Screen Display, CPU Usage, RAM Usage, etc.). Thus, in addition to the total energy consumption of four routing protocols expressed in equations (3.15), (3.20), (3.23), and (3.28), respectively, we have also considered the CPU (i.e., E_{CPU}) and Display (i.e., E_{DISP}) energy consumption [110].

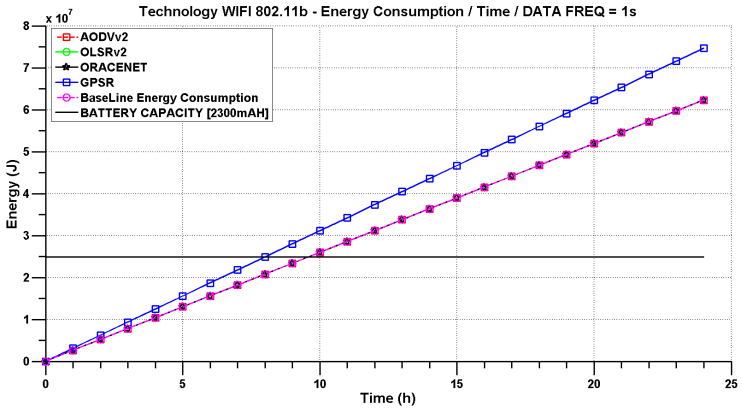


FIGURE 3.13: Protocols Average Energy Consumption in Joules per Node by Time (over 24 hours).

Figure 3.15, shows the lifetime results and comparison between the routing protocols. A typical smart phone battery capacity being used is 24840 mW (2300 mAh) [111]. It can be seen that all the studied protocols have approximately the same average of energy consumption per node, except for GPSR. The high value of the energy consumption for the case of GPSR is due to its additional receiver energy consumption. GPSR lifetime is around 8 hours, whereas the rest of the protocols lifetime is around 9 hours and 30 minutes. Particularly, AODVv2, OLSRv2 and ORACE-Net have a slight difference in the lifetime, whereas ORACE-Net remains the one with the higher lifetime compared to the others. Figure 3.14 is an enlargement of the intersection zone for ORACE-Net, AODVv2, OLSRv2 and the Baseline energy consumption with the battery capacity.

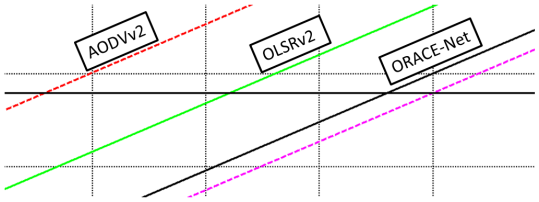


FIGURE 3.14: Intersection of the routing protocols lifetime curves with the battery lifetime (lower curve is the baseline smart phone consumption). It is a zoomed version of Figure 3.15

3.4 Extensive simulation studies

In this section we present, discuss and compare the simulations results of the four routing protocols focused mainly in the network level performance. Particularly, the new proposed routing protocol (i.e., ORACE-Net) is intended to route data traffic in disaster context. The best routing protocol is selected from each relevant class of routing protocols (i.e., Reactive routing, Proactive routing, and Geographic-based

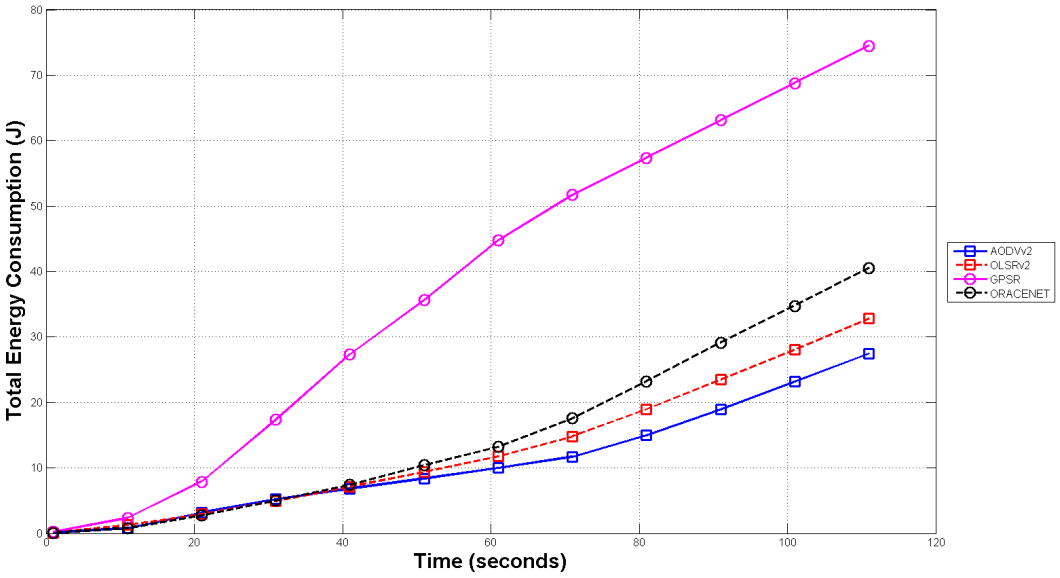


FIGURE 3.15: Average Energy Consumption with Activated GPS for All Protocols.

routing. The eligible selected candidates to be investigated and compared to ORACE-Net are the most widely used routing protocols AODVv2, OLSRv2 and GPSR. In one of our recent works [65] we have evaluated the above mentioned protocols in a realistic disaster context. In this work, we evaluate and compare these protocols with the new proposed routing protocol (i.e., ORACE-Net) based on the different mobility models. It is crucial to reproduce the realistic critical and disaster relief environment for the realistic performance evaluation. Therefore, several essential factors must be considered. First, a realistic mobility model (spatial and temporal consideration, mobility pattern, unpredictable crowd behavior, multiple incidents areas, etc.). Second, command and control operational requirements (e.g., CC location, rescue groups formation, logistic and medical resources, etc.). Third factor, simulated dynamic information generation (data flow in two ways: from CC to the incident area and vice versa). Moreover, first and second factors are related to the mobility modeling tool features, whereas, third factor depends on the network simulator used which will be detailed in the following section (i.e., 3.4.1).

3.4.1 Simulation Setup and Mobility Modeling

"**BonnMotion [112]** is a Java software which creates and analyzes mobility scenarios and is most commonly used as a tool for the investigation of mobile ad hoc network characteristics. The scenarios can also be exported for several network simulators, such as ns-2, ns-3, GloMoSim/QualNet, COOJA, MiXiM, and ONE. BonnMotion is being jointly developed by the Communication Systems group at the University of Bonn, Germany, the Toilers group at the Colorado School of Mines, Golden, CO, USA, and the Distributed Systems group at the University of Osnabrück, Germany. Several mobility models are supported, namely: the Random Waypoint model, the Random Walk model, the Gauss-Markov model, the Manhattan Grid model, the Reference Point Group Mobility model, the Disaster Area model, the Random Street model, and more."

The mobility scenario generation and analysis tool called Bonnmotion [112] implements widely used existing models. In order to assess the protocols' behaviors in different contexts, we consider the following three diverse mobility models: 1) Static Network Topology, 2) Random Waypoint Mobility and 3) Disaster Area Mobility. We assume that at the beginning of an emergency case, first, people are moving in all directions as a panic behavior, then, they follow the emergency exists and start receiving the first aids, finally, the mobility reduces significantly in the area. In *Static Network Topology* nodes are randomly dispatched over the deployment area and remain static. *Random Waypoint Mobility* consists of randomly and freely moving nodes. Destination, directions and speed are randomized but the speed limit could be specified. This model could represent a happening incident (especially the case when the incident area is not identified exactly) where individuals are running to different directions with different speeds. Whereas, *Disaster Area Mobility* is designed and implemented specifically for the crisis and disaster context (e.g., Earthquake, Air crash, storm, etc.). Indeed, this model provides a realistic pattern of real disaster theater that composed of incident area(s), casualties clearing area(s), transport and medical evacuation zone(s). In our recent work, We provided a sample of disaster area pattern [65].

Table 3.9: Simulation Setup Parameters - WSNET v3.0

Parameters	**Values**
Area	500m/300m
Number of nodes	100
Number of CC-nodes	1 (located in the left corner of the area with the coordinates [0 , 0 , 0])
Simulation Duration	300s/iteration
Mobility Modeling	Static, Random Waypoint and Disaster Scenario
Application Layer	Constant Bit Rate(CBR) with 1 packet/s
Routing Layer	AODVv2, OLSRv2, GPSR and ORACE-Net
MAC-Layer Standard	IEEE802.11b CSMA/CA DCF with ACK
PHY-Layer	Modulation BPSK, Sensitivity = -92dBM, TX Power = 0dBm, 2.4GHz , Range = 50m
Packets Sizes	detailed in Table 3.8
Number of iterations	15

In this section, we detail the simulation setup and respective parameters. We explain also the entire simulation process. First, we generate the mobility trace files according to the three mobility models as explained above. For systems level simulations, we have used an event-driven, packet-oriented network simulator called Wireless Sensor Networks (WSNet) version 3.0 [10]. Once, the mobility trace file is converted into the input file format of WSNet, we start the simulations in the following

order. We select one of the routing protocol (i.e., ORACE-Net, AODVv2, OLSRv2 or GPSR), then, we select the first value of application layer payload (200, 400, 600, 800 or 1000 bytes per second (Bps), we run the simulation for multiple number of iterations and 95% confidence interval is considered. Once a specific routing protocol simulation is completed with all the payload values for the considered iterations, the next routing protocol is selected, and so on. This process is coordinated by scripts that select, run and save the results. Finally, Table 3.9 presents the specific time and energy parameters being used in the simulations. It is important to note here that for our simulations, we have considered only one *CC-node* in order to simplify the concept of the protocol. However, in reality, more than one *CC-node* could be deployed for two main reasons: 1) to filter the data traffic based on the data type, where each *CC-node* could be dedicated to a specific concern (*CC-node* for Internet connection, *CC-node* for medical support, *CC-node* for media, etc.), 2) to replace any defected of attacked *CC-node*.

"**WSNET [10]** is an event-based node simulator for wireless networks, which is used for node and environment simulation and it is developed by the INRIA research center, France. In WSNet, the simulated nodes are built as an arbitrary assembly of blocks which represent a hardware component, a software component or a behavior/resource of the node. There is no restriction in the number of blocks or the relation between the blocks. The blocks may model the Physical Layer, Radio interface, Antenna, Mobility, Application, MAC and Routing Protocols and energy resources.
Each block is formally called as bundle, whereas each component is called as entity. WSNet does not have big community support but it is based on a simple modular approach and fundamental modules are available at each entity which are useful for comparing the algorithm or protocol. The construction of a new module is also simple, there are some modular functions which provide interface between the layers as well as for the formation of a node.
One of the key advantages of using WSNet simulator is that there is an associated node platform simulator WSIM, which allows simulating different components of the sensor node. It relies on cycle accurate full platform simulation using microprocessor instruction driven timings. The simulator is able to perform a full simulation of hardware events that occur in the platform and to give back to the developer a precise timing analysis of the simulated software. WSNET simulator is actively updated (reached version 9.07). WSNET has been committed with more than 1,227 updates and 395 adds."

3.4.2 Simulations Results

The performance metrics considered for the evaluation of the protocols are:

1 *Average Packet Reception Rate* (i.e., PRR) which consists of the number of received packet divided by the number of the transmitted packets at the application layer.

2 *Average Communication Delay*, which is the average packet delay between the source node and the final destination over a multi-hop communication.

3 *Average Energy Consumption per delivered packet*, with reference to textcolorgreen-the considered radio transceiver parameters detailed in Table 3.9.

4 *Average Hop Count*, which consists of the average number of hops starting from the source to the destination in the network.

The performance results of the studied protocol are investigated according to various mobility models including the *Static network topology*, *Random Waypoint mobility model* and finally, *Disaster mobility model*.

3.4.2.1 Static Network Topology

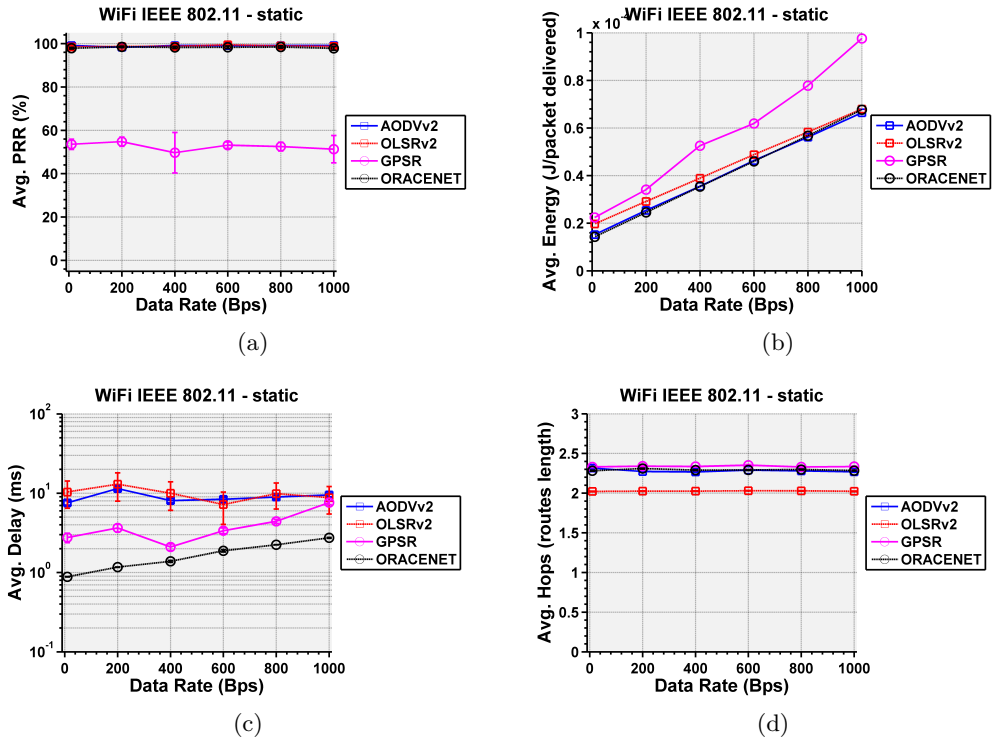


FIGURE 3.16: ORACE-Net Behavior with static network topology.

The *Static Network Topology* is a set of dispatched nodes in the deployed area where the nodes are static during the whole simulations. Thus, if a route is established between certain nodes, it will be considered as available during the entire simulation, unless the battery of the node is down. The static topology simulates the pattern of the nodes in the disaster area after the search and rescue operations. We assume that after these operations, we still have some base stations dispatched in the area and still communicating.

3.4.2.1.1 Packet Reception Rate: The results of the average packet reception rate for the four studied protocols are depicted by the Figure 3.16(a). Overall, all the routing protocols except GPSR achieves more than 97% of PRR for all the payloads. In contrast, GPSR achieves around 56% of average PRR. For GPSR, routes are not necessarily optimized, they are established based on the nodes geographic location. When the route is established by GPSR, then the nodes location does not change, routes are not updated. This point is particularly relevant when the routes lifetime is reached or the nodes are disconnected.

3.4.2.1.2 Energy Consumption: The results of the average energy consumption per delivered packet are shown in the Figure 3.16(b). It can be seen (as expected) that the energy increases linearly with the data generation rates. Best energy consumption results are achieved by ORACE-Net and AODVv2 protocols followed by OLSRv2, (from 0.22×10^{-4} Joules at 200Bps to 0.69×10^{-4} Joules at 1000Bps). In

the case of ORACE-Net, the absence of neighbor discovery process represents a major advantage in terms of energy optimization. Along with ORACE-Net, AODVv2, consumes similar amount of energy, this is due to the fact that AODVv2 is a reactive routing protocol, so the reactive mechanism saves energy. OLSRv2 consumes slightly higher than ORACE-Net and AODVv2 from 200 to 800 Bps, and has the same energy consumption with the highest data rate payload ($0.68 \times 10^{-4} Joules/packet_{delivered}$). Finally, GPSR presents the highest energy consumed per delivered packet since it is using a considerable amount of energy for nodes' localization.

3.4.2.1.3 Communication Delay: Figure 3.16(c) shows the average communication delay achieved by the four studied protocols. The best delay is achieved by ORACE-Net due to routes optimization that increases the end-to-end PRR and decreases the delay. Nearly 10 times higher than ORACE-Net, AODVv2 and OLSRv2 have almost the same average communication delay behavior against different data rate payloads. Since the network overhead of the AODVv2 and OLSRv2 are higher than ORACE-Net mainly because of the network control packets and the beacons utilization, this impacts the communication delay. GPSR, as shown in Figure 3.16(a), with the lowest PRR, thus, the communication delay in Figure 3.16(c) has no significant information to add even GPSR has better performance than OLSRv2 and AODVv2.

3.4.2.1.4 Average Hop Count: The average hop count results are shown in Figure 3.16(d). Shortest routes are realized by OLSRv2 with average hop count almost around 2 hops with all the payload variations. OLSRv2 is a proactive routing protocol, thus, the network topology is continuously maintained. The rest of the routing protocols have similar hop count (i.e., on average around 2.3 hops). The average hop count realized by ORACE-Net is similar to AODVv2 and GPSR. As can be seen, by varying the data rate, there is no impact on the average hop count, because if routes are established, how much is the amount of data to be routed, it is routed according to the established routing table. The average hop count is related to the mobility model, in a static topology, the difference between the protocols is not really noticeable, but later on with the random way point and the disaster mobility models, it becomes clearly visible.

3.4.2.2 Random Waypoint Mobility Model

The Random Waypoint mobility is considered as a mobility pattern that reflects the panic situation where movements of the nodes are in diverse directions to various destinations with distinct speed. We consider the random waypoint mobility model as a generic disaster model because of the nodes' velocity and acceleration change over the time. This made the mobility of the nodes comparable to the behavior of the individuals in the incident area when the disaster just happened. Speed of the nodes vary from 0 m/s to the maximum specified speed (i.e., 1.3 m/s which is constraint to humans mobility). The Results of the studies protocols using Random Waypoint mobility model are explained below.

3.4.2.2.1 Packet Reception Rate: The average PRR of the four routing protocols is depicted by the Figure 3.17(a). The graph shows that, in terms of PRR, ORACE-Net outperforms the rest of the routing protocols and achieves almost 80% of PRR with the different payload variations. ORACE-Net exploits the data packets to maintain and update its neighbors and routing tables, therefore, no control packets are needed and routes are always up to date because the data traffic is continuous during the disaster. Due to its reactive mechanism, AODVv2 achieves the worst

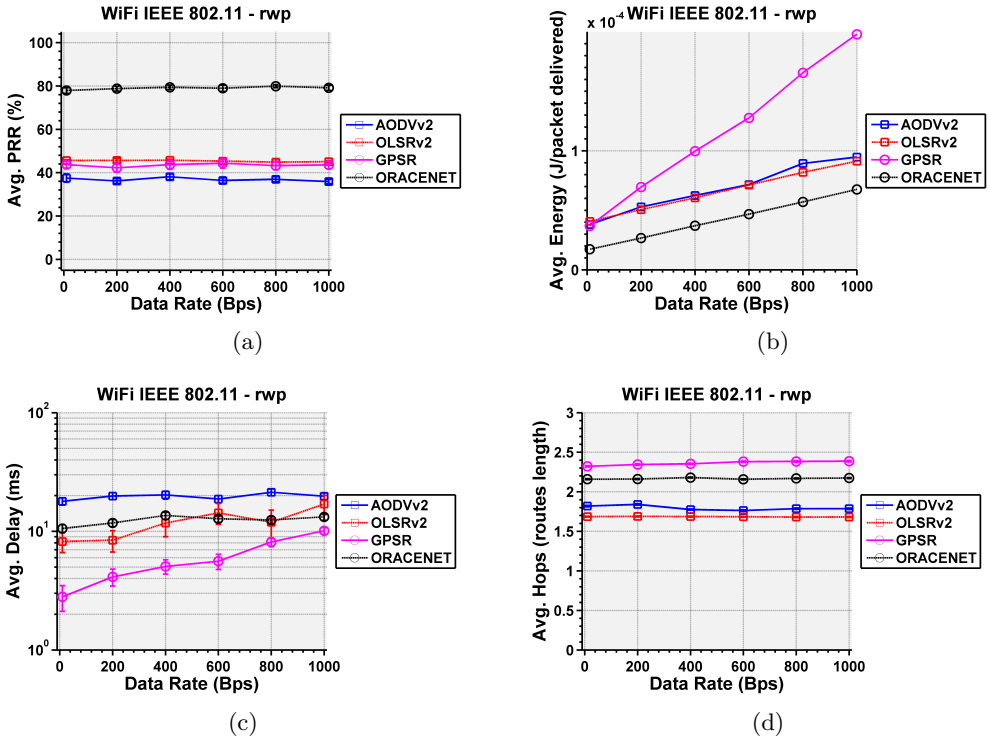


FIGURE 3.17: ORACE-Net Behavior with Random Waypoint mobility model.

performance for an average PRR around 40% during the entire simulation with the various payloads. AODVv2 looks up for the route only when it needs to route the data. Routes update is not continuous in AODVv2, so when a route is broken, the sender receives a Route Error (RERR) message, during this time the packet did not reach the destination yet. This explain also the delay results of AODVv2. OLSRv2 and GPSR achieved approximately the same results in terms of average PRR (i.e., between 48 and 50 %). OLSRv2 is slightly better than GPSR because of its proactive mechanism.

3.4.2.2.2 Energy Consumption: Figure3.17(b) shows the energy consumption of the protocols against varying data rates. Comparatively with the worst performance in terms of energy noticed with the static network topology, GPSR again has the highest energy consumption compared to the rest of the protocols. Whereas, ORACE-Net is the best with lowest energy consumption results. ORACE-Net broadcasts less topology control packets than the rest of the protocols, then the energy consumption is relatively lower. With mobile topology, protocols need to update their network topology information along with the topology variation. AODVv2, has a higher energy consumption, from 0.5×10^{-4} Joules at 200Bps to 0.9×10^{-4} Joules at 1000Bps. In addition to that, AODVv2 achieved lowest results in terms of PRR. So, having an energy consumption average near to OLSRv2, does not mean that AODVv2 has a comparable behavior according to the other metrics.

3.4.2.2.3 Communication Delay: Figure 3.17(c) shows that GPSR performs much better than the other routing protocols in terms of communication delay, although, with regards to the average PRR, GPSR achieves the best delay because it has low amount of exchanged data traffic. AODVv2 has the highest communication delay. With regards to the average PRR, having the lowest values, AODVv2 was

not able to establish efficient routes because the number of the delivered packets is very low. As the data packets do not reach destination, the protocol keeps updating the routes and re-transmitting the packet which impacts the communication delay. Compared to the other routing protocols, ORACE-Net and OLSRv2 performance is fairly conclusive. Communication delay results must be interpreted with regards to the recorded average PRR, which shows that ORACE-Net has the most stable communication delay behavior with regards to the average PRR.

3.4.2.2.4 Average Hop Count: Figure 3.17(d) depicts the hops count for the four studied routing protocols with the Random Waypoint mobility model. OLSRv2 establishes the shortest routes with an average of 1.7 hops. While GPSR achieved the longest routes with around 2.4 hops. ORACE-Net shows a stable average of hop count, around 2.18 hops with the different data rates. GPSR has the highest average of hop count (i.e., 2.35) but the difference with the other routing approaches is not significant.

Finally, results with Random Waypoint mobility model make a significant difference between the behavior of the routing protocols. Overall, ORACE-Net achieved by far the best performance in terms of average PRR and average energy consumption per delivered packet, further, it also shows comparable results in terms for average communication delay.

3.4.2.3 Disaster Mobility Scenario

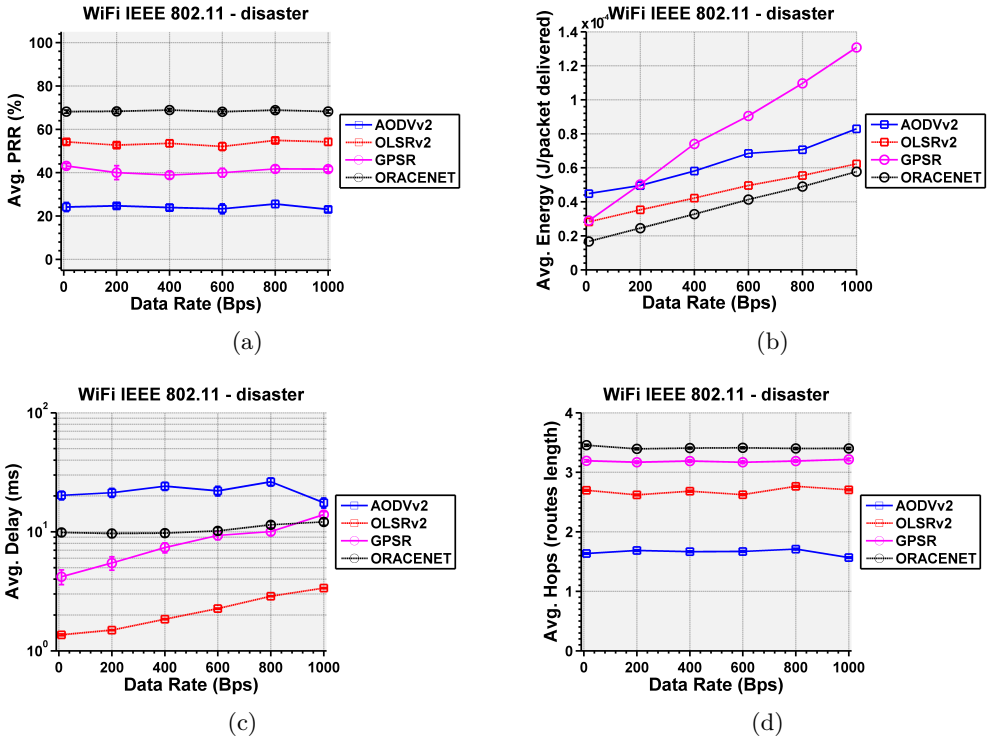


FIGURE 3.18: ORACE-Net Behavior with Disaster Scenario mobility model.

Disaster scenario mobility model is the most appropriate model to use in case of critical and emergency simulation. Thus, in similar context, the average PRR is the most important metric to investigate. Second, the communication delay has a direct impact on rescue operation. Finally, the energy consumption and the average hop

count are metrics to be considered as well. In particular, the variations of the PRR results compared to the other mobility models is quite different as explained below..

3.4.2.3.1 Packet Reception Rate: Figure 3.18(a) shows the average PRR for the different studied protocols. ORACE-Net achieved the best performance with near 70% of PRR while OLSRv2 has a difference of more than 10% of PRR lower than ORACE-Net. ORACE-Net performed much better than the other protocols with the disaster mobility model because it relies on reliable routes established based on the shortest path first then on highest signal strength level. These routes are continuously updated based on the received data packets. On the other hand, AODVv2, achieves the worst performance with 23% of PRR mainly due to the high number of re-transmissions and the non-resolved destinations. Indeed, a route in AODVv2 is established on-demand, when the route is set, and the nodes have a high mobility behavior (which is the case here), the route must be updated continuously, if AODVv2 keeps on using an old route where intermediate nodes moved away, that route is no more available, a Route Error (i.e., RERR) is received by the sender, and a new request is flooded into the network. All this process has an impact on the average PRR, communication delay and the energy consumption.

3.4.2.3.2 Energy Consumption: The energy consumption with a disaster scenario is shown in the Figure 3.18(b). As we detailed in the previous paragraph, AODVv2 has a variant energy performance due to the low average PRR. Meanwhile, the energy consumption for the rest of the routing protocols linearly increases over time. Despite the similitude of the curves of ORACE-Net, OLSRv2 and GPSR in the Random Waypoint and Disaster Area scenarios, the energy consumption in the Disaster Area scenario is lower than the one recorded with the Random Waypoint model. A small difference may have a large impact in terms of battery lifetime.

3.4.2.3.3 Communication Delay: Figure 3.18(c) depicts the average communication delay for the four studied routing protocols with a Disaster Area mobility model. It can be seen that AODVv2 has the highest and variable results. The unstable behavior of AODVv2 is due to the high topology change, so, consequence of the low average PRR recorded, the communication delay has the highest value compared to other protocols. However, OLSRv2 and GPSR have better performance in terms of delay accordingly with the low PRR noted in the previous subsection. Thus, if the PRR is low, there is not much data traffic to communicate, consequently, there will be lower communication delay. Similarly to the results achieved with the Random Waypoint mobility model, average communication delay of ORACE-Net is around 10 ms. ORACE-Net recorded a higher average delay than OLSRv2 and GPSR because it has higher average PRR. Moreover, the quantity of processed data packets with ORACE-Net is much higher than the rest of the protocols.

3.4.2.3.4 Average Hop Count: Figure 3.18(d) shows the average hop count with a disaster mobility scenario. All the routing protocols except AODVv2 have approximately the same performance in terms average hop count. The average hop count is one more aspect to expose the inefficiency of AODVv2 in a disaster mobility scenario.

Finally, ORACE-Net is the most performant routing protocol simulated with realistic disaster mobility scenario. OLSRv2 is close to ORACE-Net in terms of energy

consumption and average hop count, but far in terms of PRR. Whereas, it is concluded that AODVv2 and GPSR are not intended to be deployed in disaster mobility network. Regarding the average PRR and the average energy consumption per delivered packet ORACE-Net is the most appropriate routing protocols from the studied approaches to be considered in the disaster scenarios.

3.5 Conclusion

Through this chapter, ORACE-Net mechanism has been presented based on its three main phases: Beacons and Advertisement Broadcast, Direct Route Establishment, and Reverse Route Establishment. ORACE-Net communication overhead, is compared to the studied ad-hoc routing protocols communication overheads. A comparison is then discussed based on simulations according to different mobility traces (static, random waypoint and disaster mobility models).

Chapter 4

Implementation and Experimentation of an End-to-End Solution based on ORACE-Net: CROW^2

The Critical Rescue Operation using Wearable Wireless sensor networks (CROW^2) is a standalone ORACE-Net based end-to-end system that enables a wireless ad hoc network in order to connect human beings (rescuers, trapped survivors, civilians, media and press, etc.) to each others from a side and to Internet (or any extended network) from the other side, during disaster relief operations. The overall objectives and challenges to be addressed are initially described in [8].

4.0.1 Overview of the CROW^2 Project

The CROW^2 system is realized under the CROW^2 project. Among the contributions of the project, notably, we proposed realistic channel models and simulation environment for Body Area Networks (BAN) and Body-to-Body Networks (BBN or B2B) [113]. We evaluated the IEEE 802.15.6 WBAN standard under the realistic channel, radio and mobility models; in particular, the proposed MAC protocols were compared for application-specific design; additionally, new dynamic MAC protocols were proposed in [114, 115]. Furthermore, at the MAC layer, the IEEE 802.15.6 standard's proposed coexistence schemes for co-channel were evaluated in order to investigate the impact of interference from co-located BANs [113].

For that, we studied and compared the effectiveness of distributed and cluster-based architectures for Body-to-Body communications (BBNs or B2B). Then, various routing protocols among different classes including proactive, reactive, geographic-based and gradient-based were simulated and evaluated in [98]. Finally, we proposed a new optimized routing protocol specifically designed for the emergency and disaster relief communication networks. The routing protocol was implemented and evaluated on the WSNet [10] simulator within a realistic disaster mobility pattern. Finally, we implement the entire system on real mobile devices (smart phones and Raspberry Pi devices) for performance evaluation in real testbed.

4.0.2 CROW^2: The ORACE-Net-based End-to-End System Architecture

The CROW^2 system is a set of wireless distributed devices equipped with wireless sensors intended to collect real-time data (i.e., vital signs, stress level, locations, ambient intelligence [116], etc.) from Wireless Body Area Network (WBAN) nodes towards

a cloud IoT platform. Figure 4.1 depicts the general architecture of the next generation WBAN. A node in the proposed system could be either: (i) tactical (deployed by rescuers while moving inside the disaster area) or (ii) mobile (carried on-body by rescuers or trapped survivors). Tactical nodes establish a wireless tactical backbone, which extends the network coverage. Mobile nodes, being in proximity of the tactical backbone, could route packets through it as depicted in Figure 4.2b. We call these tactical devices ORACE-Net Tactical Devices (OTDs). Mobile devices carried on-body rely on both the OTDs and the other mobile devices to route data. Data collected from deployed nodes (i.e., tactical and mobile) are routed through the network towards the Command Center node (CC node). The CC node is a tactical command center deployed as a gateway allowing the emergency network to be linked to wide infrastructure networks (e.g., Internet, military platforms, other emergency networks, etc.). The CC node is also the node through which the operations' commanders send their instructions to the rescuers and the rescuers send back their feedback to the CC node. It is important to note here that multiple CC nodes could be deployed and activated in the case of single CC failure.

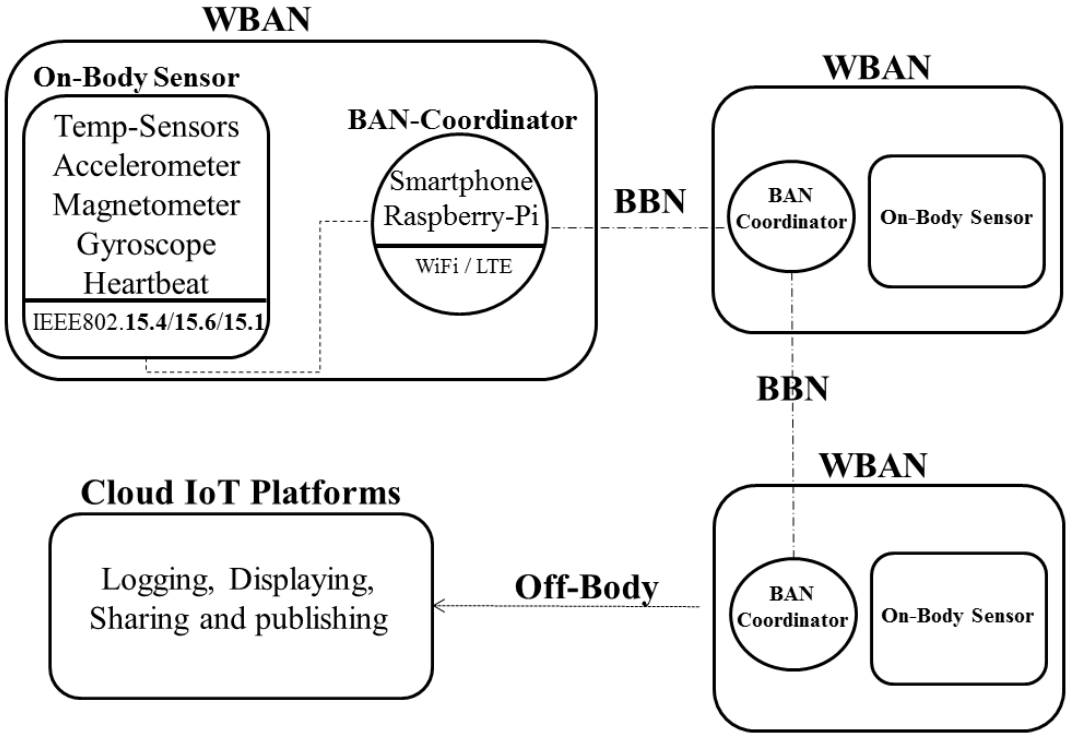
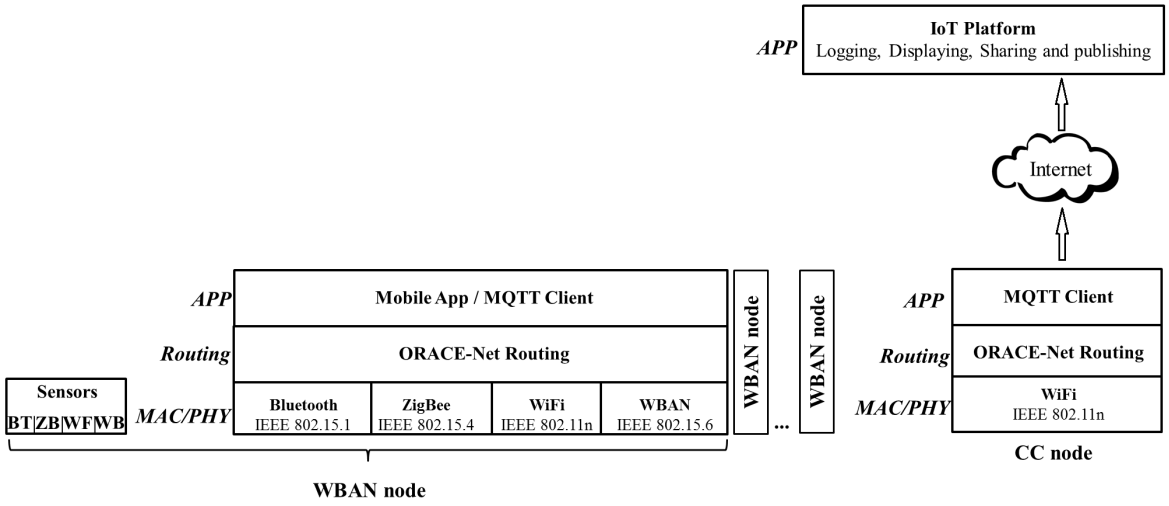
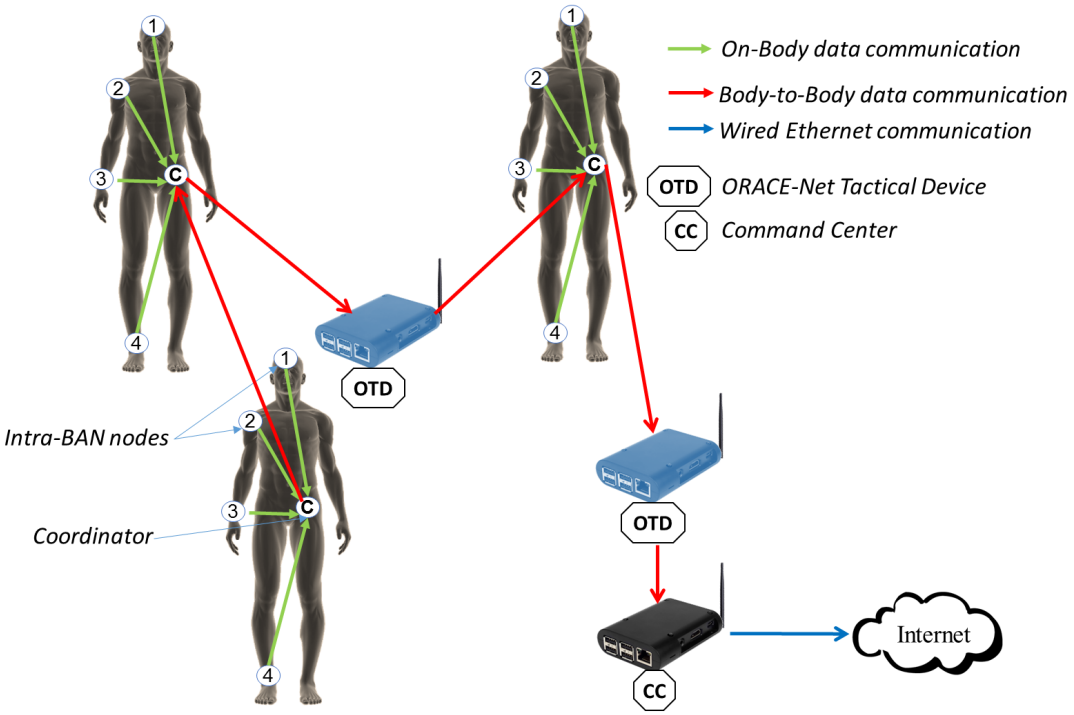


FIGURE 4.1: General architecture of the wireless body-area-network system. BAN: Body-Area-Network, BBN: Body-to-Body communication, Off-Body communication: all non-BAN and non-BBN communications.



(**a**)

FIGURE 4.2: (**a**) CROW² system layer-based architecture. BT: Bluetooth, ZB: ZigBee, WF: WiFi, WB: WBAN. For the CROW² system, we considered Bluetooth between sensors and the coordinator and WiFi IEEE802.11n between WBANs and the Command Center node (CC node)



(**b**)

FIGURE 4.2: (**b**) Multi-hop aspect in CROW²; Data is routed from/through mobile/tactical nodes towards the Internet. MQTT, Message Queuing Telemetry Transport.

4.0.3 CROW^2 Solution Enhancement

As depicted in the layer-based architecture in Figure 4.2a, CROW^2 consists of two Wireless Body Area Networks (WBANs), or more, connected to a cloud IoT platform through the CC node. Each WBAN node is composed of: (i) a WBAN coordinator, which is a wireless device with advanced energy and communication features, (ii) on-body sensors, which may feature different communications technologies (i.e., Bluetooth IEEE802.15.1, WiFi IEEE802.11a/b/g/n, ZigBee IEEE802.5.4 and WBAN IEEE802.15.6). Sensors are connected among one of the previous technologies to the WBAN coordinator. The BBN routing is assured by the ORACE-Net routing protocol according to the architecture depicted in Figure 4.1. As a payload at the application layer, we deployed an Message Queuing Telemetry Transport [117] client (on tactical and mobile devices) to push data to the IoT platform.

An improvement to the CROW^2 system has been proposed through this work [99]. Compared to our previous work [118], we have installed on-body sensors provided by Shimmer [119]. Therefore, the current system payload consists of real sensed vital sign data from the human body towards the IoT platform. To improve connectivity and mitigate interference, we reduced the tactical devices (OTDs) to four. Additionally, we reduced the number of active indoor wireless access points, since we assume that during the disaster, they will be damaged.

4.1 ORACE-Net-based CROW^2 Solution Implementation

In this section, we explain how the CROW^2 system is implemented. We present first the on-body communication; then, we present the body-to-body communication implementation. Finally, we describe the off-body components' implementation, in particular the Labeeb-IoT platform.

4.1.1 On-Body Communication

WBAN covers the communication between the coordinator (which is the main on-body device responsible for communication with other BANs and off-body devices) and the rest of the on-body or under skin sensors. For the CROW^2 system, on-body communication is established between sensors (i.e., Shimmer [120]) and the Android mobile application (i.e., Labeeb-IoT Shimmer Sensing Android App).

Shimmer sensors [120] are sensing devices capable of measuring physical quantities (e.g., acceleration, gyroscope X, Y, Z and angle, triple axis magnetic field, pressure, etc.) and sharing them via Bluetooth. Shimmer provides a Service Development Kit (SDK) that affords the possibility to read real-time data from the sensor by an Android or IOS mobile application. We place the Shimmer sensor on-body as shown in Figure 4.3. Once connected via Bluetooth, our mobile application (Labeeb-IoT Shimmer Sensing Android App) starts reading data from the sensor and sharing them with the IoT platform.

The Labeeb-IoT Shimmer Sensing Android App is responsible for collecting data from sensors and transmitting them onto the Labeeb-IoT platform using the Message Queuing Telemetry Transport (MQTT) protocol [117]. Figure 4.4 (a) depicts a screenshot from the live activity of the mobile app with the different real-time sensed parameters before being pushed to the Labeeb-IoT platform.

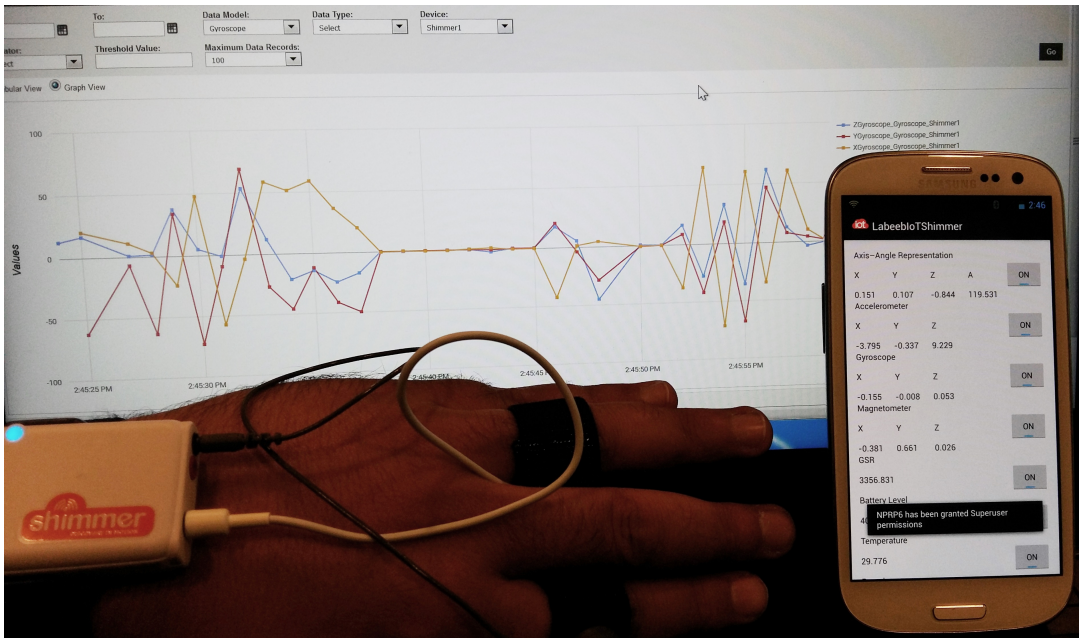
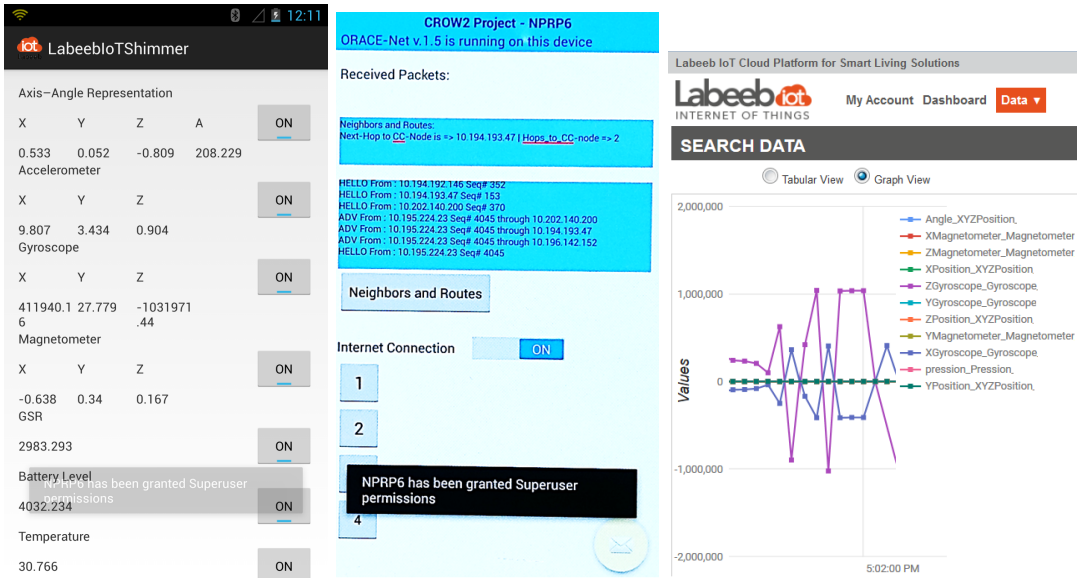


FIGURE 4.3: Real-time data collected by the ORACE-Net Mobile Device (OMD), routed through the ORACE-Net network and then displayed on the Labeeb-IoT platform.



(a) (b) (c)

FIGURE 4.4: (**a**) A screen-shot from the Labeeb-IoT Shimmer sensing mobile app, which collects data from Shimmer [120] sensors and pushes them to the Internet of Things platform (Labeeb-IoT). (**b**) Testbed: a photo of the ORACE-Net mobile devices displaying the real-time events (received "Hello" and Advertisement ("ADV") packets) and the current route. (**c**) The Labeeb-IoT [121] interface shows the variation of the sensed data from the Shimmer sensor connected to the mobile node.

4.1.2 Body-To-Body Communication

Body-to-body communications consist of the communications between coordinators (i.e., mobile devices) carried by the rescuers, survivors and also the communications between coordinators and tactical devices, as shown in Figure 4.2b. The ORACE-Net routing protocol assures routing between CROW^2 devices. With regards to the operational requirements of a disaster relief mission, we assume that the first rescue teams reaching the incident area deploy wireless tactical devices (i.e., OTDs) to enable a wireless ad hoc tactical network on site. We describe these in the two following subsections. The implementation of the ORACE-Net routing protocol is describe for: (i) ORACE-Net Tactical Devices (OTDs) (ii) and ORACE-Net Android Mobile Device (OMD). Both devices are depicted in Figure 4.5.

4.1.2.1 Android Mobile Devices

These devices are designed based on the ORACE-Net Android application, which is a mobile app coded in Java and deployed on Android v4.2.2 CyanogenMod 10.0 distribution. This mobile app is dedicated to route data through the emergency network based on the ORACE-Net routing protocol. The ORACE-Net Android application is implemented at the user level as depicted in Figure 4.6a. It exploits the features of the Linux operating system at the kernel layer through the Dalvik Virtual Machine. Figure 4.6b depicts the ORACE-Net mobile application components, which are: (1) events listener, (2) broadcast receivers, (3) services, (4) content providers and (5) display activities. The relevant component in the architecture is the events listener, which triggers the rest of the tasks. An events listener is used to catch events (e.g., unicasted, multicasted or broadcasted packets, clicked button, typed text, etc.). In the ORACE-Net Android application, the events listener is implemented as a socket with a multi-cast IP address/Port: 224.0.0.1/10000. A similar socket is implemented with the C-language on Linux for the tactical deployed devices. Received packets through the events listener are handled by the broadcast receivers component to be hulled. Particularly, the content provider allows the application to share the application output with other servers or platforms. Figure 4.4b is a screenshot of the ORACE-Net mobile app showing the received/transmitted Hello and Advertisement (ADV)packets, the next-hop and the hop count to the CC node.

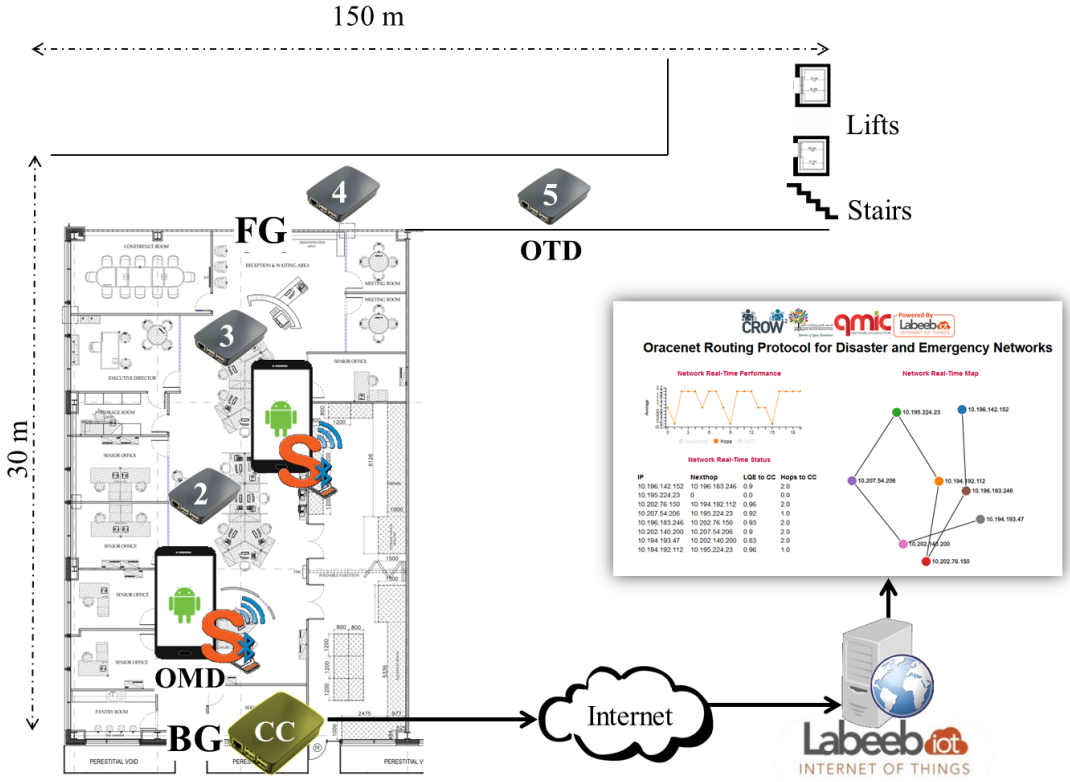


FIGURE 4.5: Experimentation scenario and data flow from deployed nodes to the Labeeb-IoT platform. The Command Center (CC node) is placed at the Back Gate (BG); ORACE-Net Mobile Devices (OMD) are mobile devices carried by the rescuers to which Shimmer sensors are connected via Bluetooth. The tactical ORACE-Net network is established through ORACE-Net Linux Tactical Devices (OTD). All collected data go through the CC node to the Labeeb-IoT platform. A real-time dynamic topology website instantly displays the network topology.

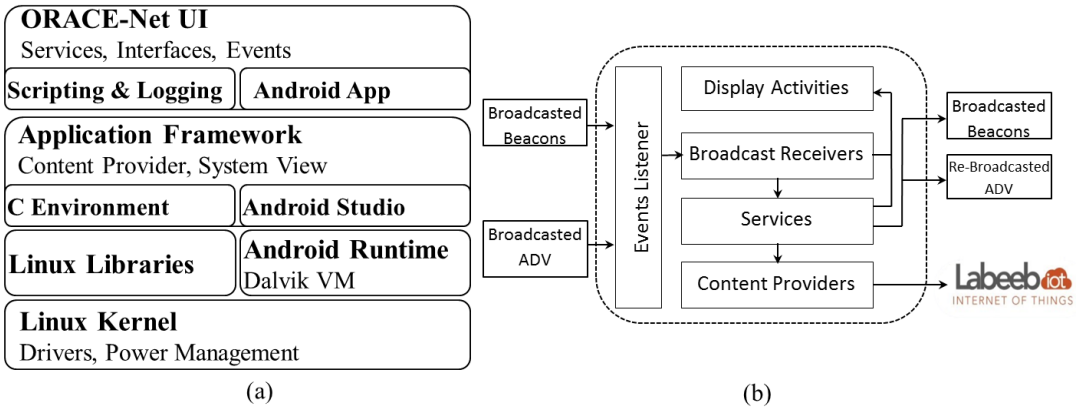


FIGURE 4.6: (**a**) ORACE-Net system-oriented stack over Linux and Android. (**b**) ORACE-Net Android application architecture.

4.1.2.2 ORACE-Net Tactical Devices

These tactical devices are implemented based on Linux applications. Indeed, we implemented the ORACE-Net protocol on Raspbian v8.0, a free operating system

based on Debian optimized for the Raspberry Pi hardware. Linux libraries are used to operate various protocol events (i.e., socket connections, packets encapsulation, multicasting and broadcasting). We use shell scripts to display the status and statistics and to manage the processes of the protocol. The logging system in the tactical devices is based on the operating system logging service "Syslog". Finally, data are pushed to the Labeeb-IoT platform via the MQTT protocol client installed on every OTD.

4.1.3 Off-Body Communication

Communication between the CC node and the Labeeb-IoT platform covers the off-body communication of the CROW^2 system, as depicted in Figures 4.1 and 4.5.

The Internet of Things (IoT) is an emerging technology developed for smart living solutions. IoT solutions are online platforms capable of receiving sensed real-time data from diverse types of devices (including sensors, actuators, coordinators, gateways, etc.) that could be deployed in a vast geographic area. Such platforms are able to collect, store, publish and analyze data according to many parameters. With respect to the MQTT standard [117], the Labeeb-IoT platform uses a publish/subscribe architecture in contrast with the HTTP request/response paradigm architecture. Publish/subscribe is event-driven and enables messages to be pushed by clients using the MQTT protocol. The MQTT client communicates with the broker using predefined methods (e.g., connect, disconnect, subscribe, publish). Labeeb-IoT offers various APIs and RESTful and/or JavaScript Object Notation (JSON) web services.

In our experiments, ORACE-Net devices (mobile and tactical) push continuously and instantly the following data to the Labeeb-IoT platform: (1) device identifier ($Device_{Id}$), (2) device location ($Location$), (3) device neighbors' list ($Neighbors$), (4) next-hop to the CC node (NH_{CC}), (5) $E2E_{LQE}$ and (6) Hop_{count} to the CC node. Data are stored in the platform database and then could be extracted and displayed on Labeeb-IoT as shown in Figure 4.4c.

4.2 Performance evaluation of ORACE-Net and CROW^2 system

This section presents the complete evaluation of the proposed ORACE-Net routing protocol within the complete CROW^2 system. In this chapter, first, an evaluation of the different dissemination strategies (presented in Chapter 2) is discussed. Second, the performance of ORACE-Net routing protocol is simulated and evaluated among realistic scenario setup. Finally, the implemented CROW^2 system presented in Chapter 4 is evaluated and the experiment results are discussed.

4.2.1 Routing Protocols Evaluation According to the Data Dissemination Strategies

4.2.1.1 Simulation Setup, Radio Link and Mobility Modeling

The radio-link modeling metric is based on SINR (signal-to-interference-noise-ratio), which considers the mutual interference from multiple WBANs [122]. This metric rely on accurate path loss calculations using enhanced IEEE 802.15.6 channels models [123]. Then, bit error rate is calculated based on the specific modulation schemes (i.e., DQPSK and DBPSK) proposed in the IEEE 802.15.6 standard, followed by the evaluation of packet error rate (PER) [122].

In WBANs there are different mobility patterns depending upon the posture positions during sitting, standing, walking, running swimming etc., scenarios. In addition, body shadowing, orientation and rotations make the radio-link consistently time-varying. Our modeling methodology is based on real-time mobility traces from the motion captured system which provides diverse mobility patterns such as walking, sitting, standing and running. These mobility patterns coincide with our application scenario which are imported in a packet-oriented event-drive network simulator, called WSNet [10], for performance analysis. Further, we have developed bio-mechanical models (for on-body) communication and group mobility model (for body-to-body) communications which reflect and satisfy our application context. The detailed steps of the bio-mechanical modeling and transformation are explained in [123]. In this work we have considered three levels of hierarchy as shown in Figure 4.7. At the top level, there are 12 bodies (WBANs), then, 3 WBANs form a small group (for inter-WBAN mobility) and finally each body consists of five on-body nodes. Concerning the separation distance between these WBANs, the WBANs inside a small WBANs group are separated by 8 meters, whereas, 20 meters separation is considered between the groups. Five on-body nodes are placed as; head (node 1), right shoulder (node 2), right wrist (node 3), stomach (node 0), and right ankle (node 4).

The bodies' mobility patterns include sitting, standing, walking (i.e., 0.5m/s) and running (i.e., 3m/s). We consider two different nodes architectures based on the aforementioned data dissemination strategies. In the distributed data dissemination strategy, all on-body sensors (including WBANs coordinators) are running on top of an IEEE 802.15.6 compliant MAC and PHY layers, with the power consumption characteristics of the CC2420 RF transceiver [124].

Regarding the PHY layer parameters, the transmission power was set to 0dBm, two frequencies were evaluated (i.e., 2450MHz and 900MHz), and for each frequency two different data rates are considered, i.e. 101.2Kbps (DBPSK) and 404.8Kbps (DQPSK) for 900MHz, and 121.4Kbps (DBPSK) and 971.4Kbps (DQPSK) for 2450 MHz. The MAC layer is based on the CSMA/CA protocol with immediate acknowledgement, where all WBANs nodes are operating under the same channel frequency. On top of the MAC layer, the AODV version 2 (DYMO) was implemented with a neighbor discovery frequency of 3s and a timeout of 9s. Finally, a Constant Bit Rate (CBR) application is generating data traffic on all WBANs nodes using different data payloads (i.e. from 16Bytes to 256 Bytes) and frequencies (i.e. 250ms, 500ms and 1s).

Figure 4.8 shows the node architectures (for both sensors and coordinator) under distributed and clustered approaches. In the clustered data dissemination strategy, each WBAN coordinator device is based on a multi-standard communication stack, where one MAC/PHY interface is used to communicate with the on-body sensors through a dedicated channel frequency (each WBAN uses a different channel frequency to avoid interferences with other WBANs), whereas the second MAC/PHY interface is used to communicate with the surrounding WBANs coordinator using a same channel frequency. In this case, the communication between the on-body sensors and their coordinator is performed using CSMA/CA, whereas AODV version 2 is only implemented at the coordinator node to discover the surrounding coordinator devices from the other WBANs, and to route the collected data to the WBANs group leader. We considered 10 iterations for each simulation scenario, and the 95% confidence intervals were computed and reported in the below simulation results.

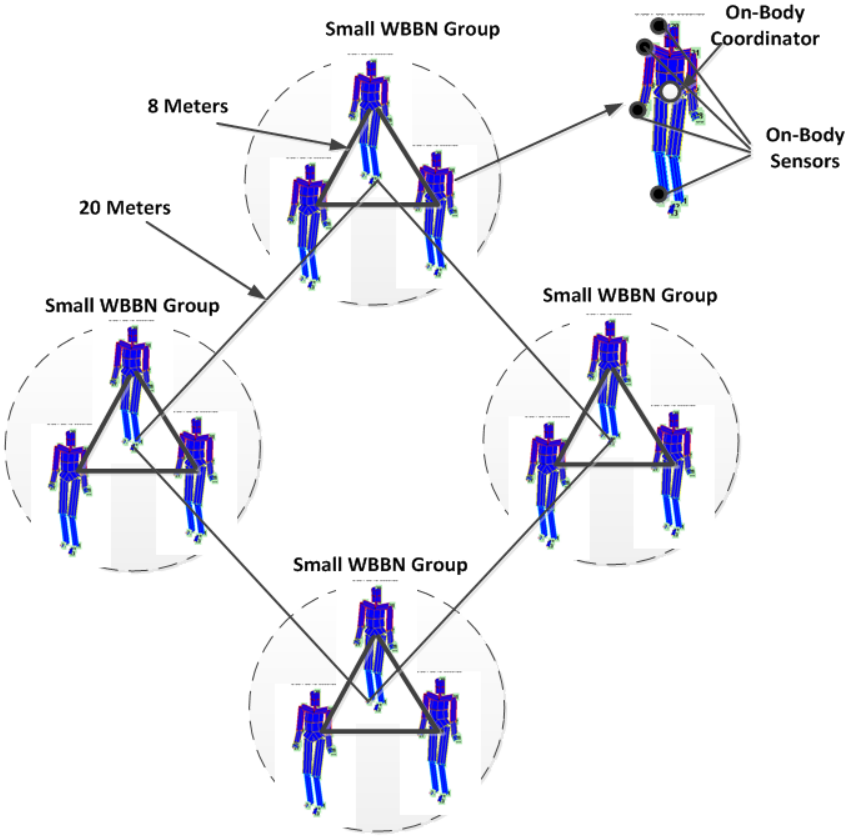


FIGURE 4.7: Tactical Wireless Body-to-Body Network Scenario for Data Dissemination Strategies Evaluation.

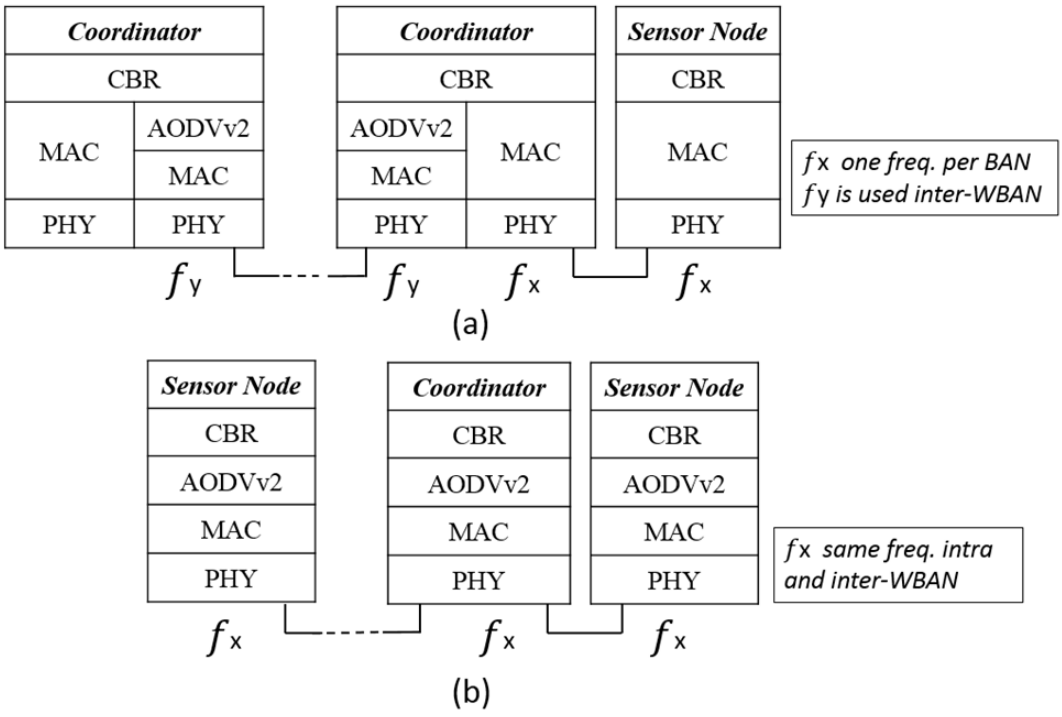


FIGURE 4.8: (a) Clustered approach where one frequency is used per BAN and a different frequency is used for inter-WBAN. (b) Distributed approach where same frequency is used from any node to any node (even coordinator).

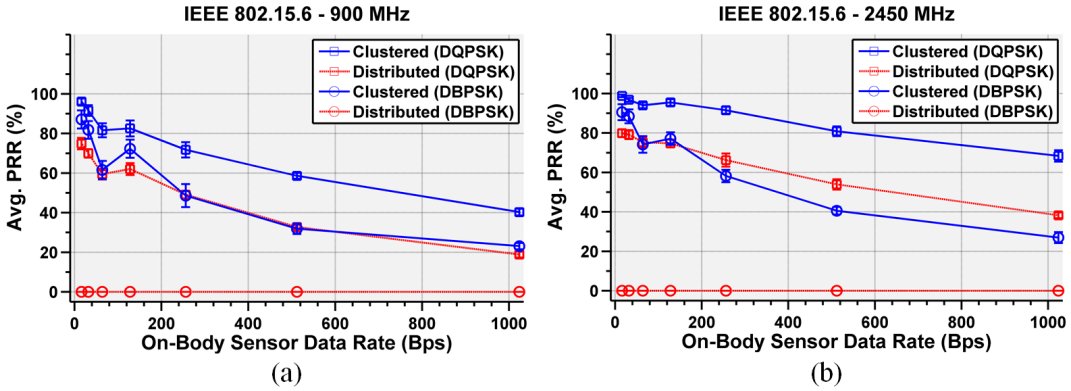


FIGURE 4.9: Average Packet Reception Ratio for Clustered and Distributed Data Dissemination Strategies for IEEE 802.15.6 with (a) 900 Mhz and (b) 2450 MHz.

4.2.1.2 Simulation Results Discussion

Collected results among the simulations, are discussed in the following subsections according to the following metrics: packets reception rate (PRR), latency, energy consumption.

4.2.1.2.1 Average Packet Reception Rate (PRR) Figure 4.9, shows the results of average PRR against varying payload (i.e., from 16-to-1024 bytes) transmitted per second for the application layer by each of the four sensors and coordinator connected on the body. In addition, 900 MHz and 2450 MHz narrow-band frequencies are utilized with lowest and highest data rates as specified earlier. In general it can be seen that clustered-based approach achieves much better PRR under both frequencies with DQPSK (i.e., highest rate). Whereas, DBPSK (i.e., lowest data rate), in distributed approach achieves the lowest performance in both frequency under all payloads variations. Further, it can be seen in both Figure 4.9 (a) and Figure 4.9 (b), that there is a gradual decrease in PRR performance with an increase in the payloads. In specific, with low payload, clustered approach achieves almost 97% PRR; however, the performance degrades relatively more with the higher payloads especially when operating at 900 MHz frequency. The best performance of the clustered-based strategy at the maximum payload (i.e., 256 bytes) is with DQPSK at 2450 MHz, where the PRR drops up to 75%. On the other hand, distributed approach with the highest rate is comparable with clustered approach (lowest rate) at 900 MHz, though it performs slightly better in 2450 MHz frequency. However, the results are always below 80% PRR even at 2 bytes of payload.

4.2.1.2.2 Average Latency As per the packet delay performance, Figure 4.10 shows the average of packet transmission delay. Payload is varied as from 16-to-1024 bytes are transmitted per second. As well, 900 and 2450 MHz are the utilized frequencies. Generally, the results of the delay are inter-related with PRR, if PRR is higher then, delay will be lower due to higher successful transmissions and lower retransmissions. It is clear that both clustered and distributed-based approaches have similar behavior with DQPSK with different variation of the payload and frequencies. Best average delay is given by the distributed-based approach with 64 bytes payload at both utilized frequencies. Accordingly to the PRR, worst performance is noticed for distributed-based dissemination strategy for all payload values and frequencies.

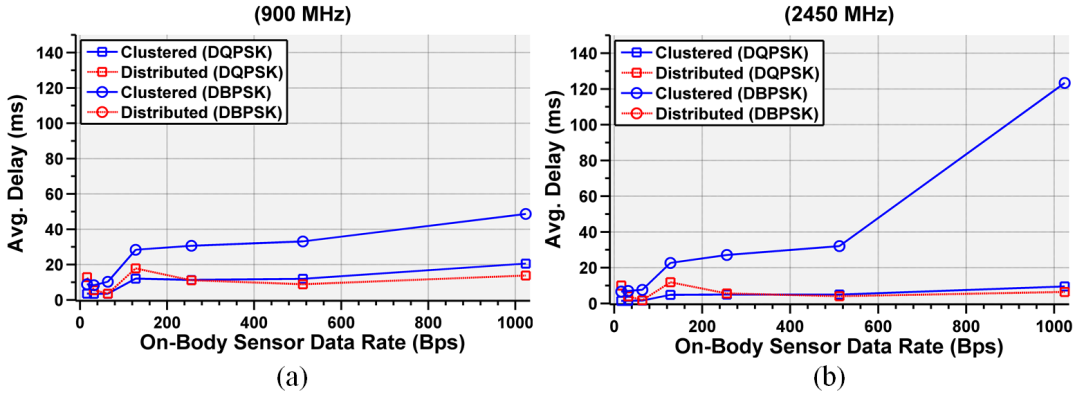


FIGURE 4.10: Average Latency for Clustered and Distributed Data Dissemination Strategies for IEEE 802.15.6 with (a) 900 Mhz and (b) 2450 MHz.

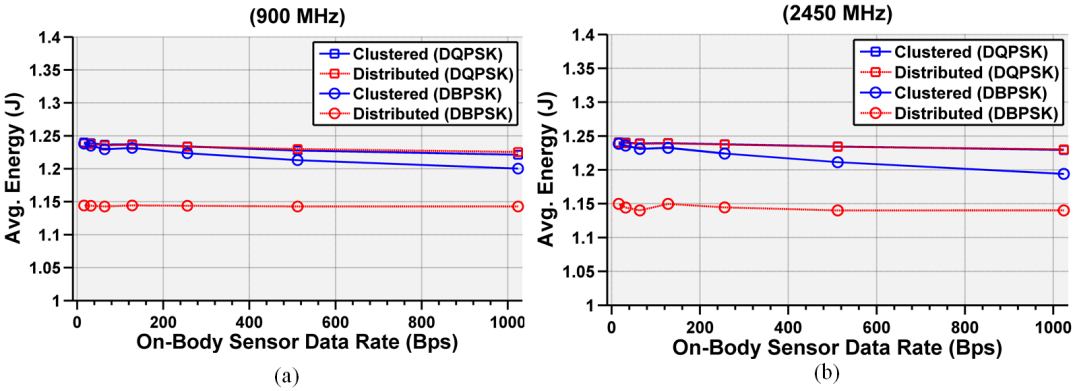


FIGURE 4.11: Average Energy Consumption for Clustered and Distributed Data Dissemination Strategies for IEEE 802.15.6 with (a) 900 Mhz and (b) 2450 MHz.

Specifically, with low payload and high rate (i.e. DQPSK), distributed and clustered-based approaches latency is interesting with a delay under 10ms. In contrast, for distributed dissemination strategy, delay is infinite with DPSK, which is relatively expected based on the PRR average results (around 0%). DBPSK in clustered-based approach, has a linear increase to reach 50ms with highest payload. (i.e. 1024 bytes).

4.2.1.2.3 Energy Consumption Concerning the energy consumption, Figure 4.11 shows the energy consumption for clustered and distributed data dissemination approaches with low and high rate (i.e. DBPSK and DQPSK). The energy consumption is shown with two graphs respectively for 900 and 2450 MHz as utilized frequencies. The energy consumption for each transmitted packet is calculated as follows,

$$E_{Packet} = T_{Packet} \times 3_{Volts} \times I_{mA}. \tag{4.1}$$

where, T_{Packet} is the duration in ms which is based on the effective packet length (including all the PHY and MAC headers [125]). It can be seen that in general similarly for both utilized frequencies, with DQPSK (i.e. highest rate) energy consumption follows the same curve for the two investigated data dissemination strategies.

TABLE 4.1: Hop Count Statistics (Computed Across all Data Payloads and Iterations)

PHY Layer	Routing Layer	Hop Count		
		Min	Average	Max
2450 Mhz + DQPSK	**Distributed**	1	2.44	7
	Clustered	1	2.24	6
2450 Mhz + DBPSK	**Distributed**	N/A	N/A	N/A
	Clustered	1	1.21	3
900 Mhz + DQPSK	**Distributed**	1	2.48	7
	Clustered	1	2.25	5
900 Mhz + DBPSK	**Distributed**	N/A	N/A	N/A
	Clustered	1	1.26	4

Distributed approach with DBPSK for both frequencies (900 and 2450 MHz) shows the lowest values for energy consumption, this is explained by the null PRR average depicted in Figure 4.9. Indeed, there is no packets sent in this case (Distributed with DBPSK), so the energy consumption will be consequently the lowest. Clearly, clustered approach with DBPSK consumes slightly low energy compared to DQPSK for both dissemination approaches. However, even though clustered approach with DBPSK is performing with lowest energy consumption, according to the delay discussed based on Figure 4.10, is not the most performant approach. Finally, DQPSK digital modulation has the same energy consumption behavior for both dissemination strategies.

4.2.1.2.4 Average Hop Count Table 4.1 shows the hop count for different data dissemination approaches with high and low rate and the utilized frequencies detailed above. Hop count is an important metric in tactical networks. Hence, it is considered as the relevant routing decisive parameter. In general, with the digital modulation DQPSK and both utilized frequencies, clustered and distributed dissemination approaches have almost the same hop count average (i.e., from 2,24 to 2,48). With DBPSK, clustered dissemination approach has the same hop count average with both frequencies. Distributed approach with DBPSK with both utilized frequencies is not considered based on the PRR average. Specifically, digital modulation DQPSK is most appropriate for clustered and distributed dissemination approaches in terms of hop count.

To conclude, Figure 4.12 and Figure 4.13 depict the network topology obtained with the clustered and distributed dissemination approaches (2450 MHz, DQPSK, and Payload of 16 bytes). Figures show clearly that number of hops for most of the nodes is much better with the distributed approach (Figure 4.12). However, the PRR average (for 2450 MHz, DQPSK and Payload of 16 bytes) is more important with clustered approach (i.e., 89%). Thus, there is a clear trade-off between both data dissemination approaches. Hence, the choice of the data disseminations strategy should be maid with regards to the networking context and the network density.

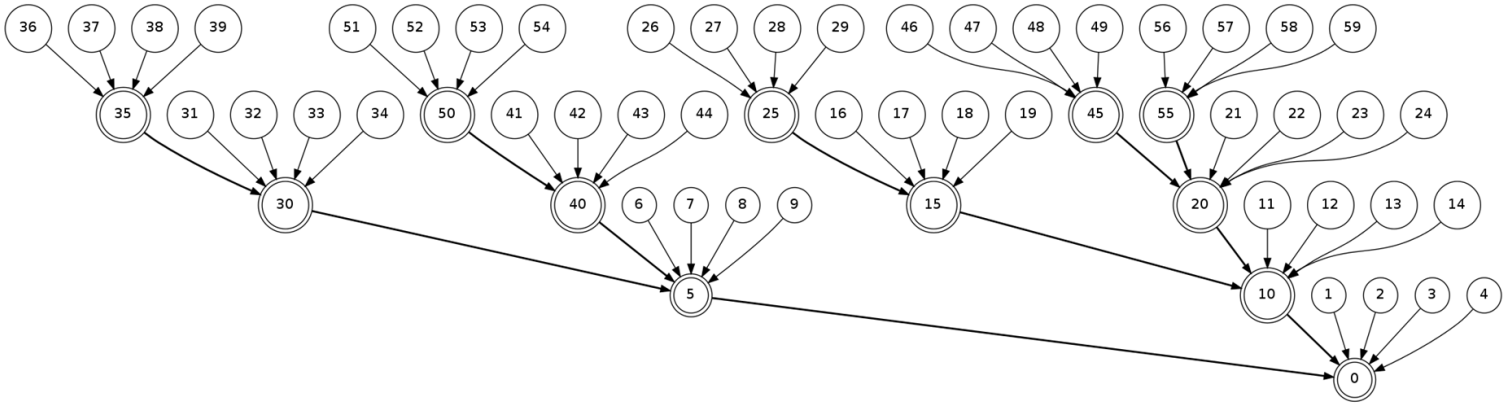


FIGURE 4.12: Network topology obtained with the clustered routing approach (2450Mhz, DQPSK, and Payload of 16 bytes).

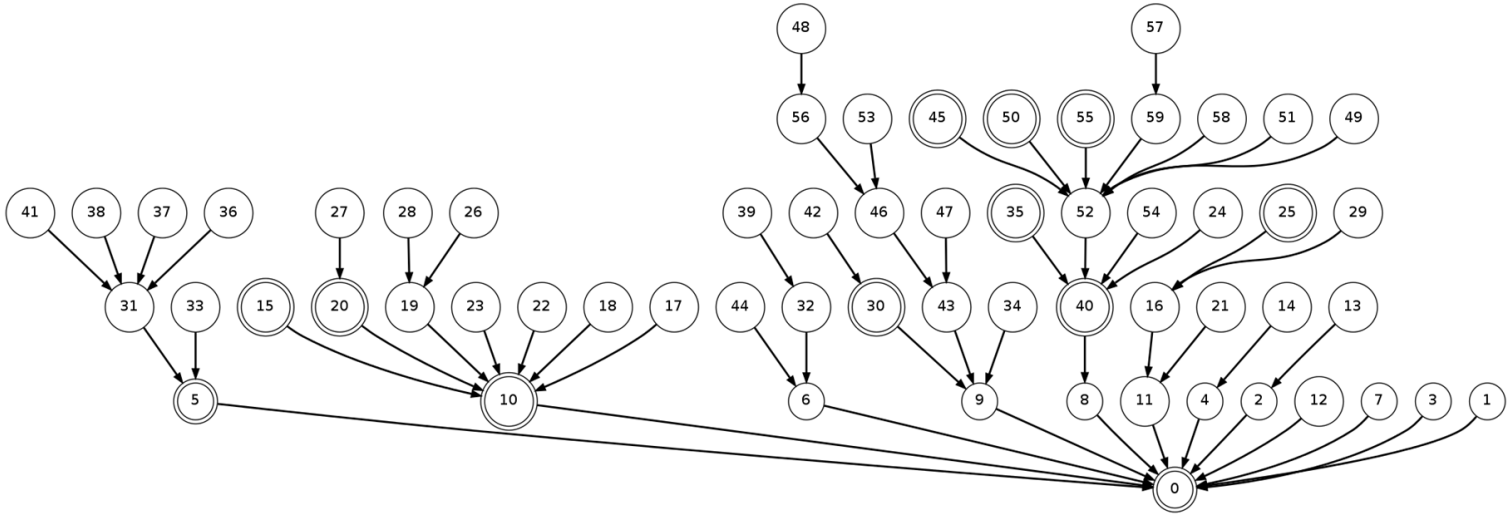


FIGURE 4.13: Network topology obtained with the distributed routing approach (2450Mhz, DQPSK, and Payload of 16 bytes).

4.2.2 CROW^2 System Experimentation Setup and Scenario

TABLE 4.2: Experimental parameters and configuration settings. ORACE: Optimized Routing Approach for Critical and Emergency Networks; CC: command center node.

General Settings	
Parameter	**Settings**
Number of WBANs	2
ORACE-Net Tactical Devices	4 (raspberry pi 2) OS: Raspbian v8.0
Mobile nodes (coordinators)	2 (Samsung Galaxy S3-I9300 - rooted) OS: Android 4.2.2 CyanogenMod 10.0
Wireless mode	Ad hoc
ESSID	CROW2
Wireless standard	IEEE 802.11n/2.412 GHz (Channel 1)
Transmission power	0 dBm
Experiment area	30 m × 150 m
CC-node connection	Ethernet to Internet Ad hoc WiFi to ORACE-Net network
Number of iterations	3
Experimentation duration	60 min/iteration
ORACE-Net Protocol and Application Layer Settings	
Application layer	MQTT client used for pushing data to the IoT platform
MQTT msg size/intervals	30 Kb/1s
Hello/ADV packet size	20/25 Bytes
Hello/ADV intervals	3 s
Multicast address/port	224.0.0.0/10000
Shimmer [120] Sensing Device Settings	
Wireless standard	Bluetooth IEEE 802.15.1
Sensed data	Pressure, Temperature, Gyroscope $(x, y, z$, axis-angle), Acceleration (x, y, z), Magnetometer (x, y, z), Battery level
Device/Body	1 (with multiple embedded sensors)
Buffer [120]	1024 bytes
Message interval	1 s

In our experiments, we consider a disaster scenario in our office Qatar Mobility

Innovations Center (QMIC) in Qatar Science and Technology Park (QSTP). Our test-bed consists of four raspberry-pi devices model 2-B and two Samsung galaxy S3-I9300 smart phones with ORACE-Net routing protocol implemented on-board. The office map is shown in Figure 4.5. The scenario is as follows: rescue teams access to the office from the back-gate (BG). First, they deploy the *CC node* in a trusted and safe location at the gate to be connected to Internet through an Ethernet or WiFi access point (these links could be provided with military microwave or satellite connections). Upon their entrance inside the office, rescuers start deploying tactical devices (OTD) as base stations in order to have the maximum network wireless coverage above all the operations area. OTDs are deployed as shown in Figure 4.5 from 2 to 5. Mobile nodes (smart phones) carried by the rescuers are connected through the tactical network to the CC node. Shimmer sensors are connected to ORACE-Net Mobile Devices via Bluetooth. Since the experimentation area is limited, we reduced the raspberry-pi's and smart phone's WiFi antennas transmission power to 0 dBm. Experimentation parameters and configuration settings are detailed in Table 4.2.

4.2.2.1 Results and Discussion

In this subsection, we present the results of the experiment aimed to evaluate the CROW^2 system performance based on the ORACE-Net routing protocol on a real test-bed. To do so, we consider the following metrics: throughput and jitter, End-to-End delay ($E2E_{delay}$) and End-to-End Link Quality Estimation ($E2E_{LQE}$). Throughput is the maximum amount of data processed for sending from the source node (i.e., ORACE-Net mobile device) to the destination node (i.e., Labeeb-IoT platform). "Jitter" is the amount of variation in latency/response time (typically in milliseconds). Reliable connections consistently report back the same latency over and over again. Much variation (or 'jitter') is an indication of connection issues. Jitter is a relevant indicator of the network performance because it defines what kind of applications the network is able to support. The $E2E_{LQE}$ is calculated by the ORACE-Net protocol to estimate end-to-end links. The $E2E_{delay}$ is the round trip time delay recorded from the source node to the destination node. This latter metric informs also about nodes' disconnections. In addition to the above performance metrics, we discuss the collected data from the IoT platform to detect motions and prevent unavailability. Finally, we discuss the overall approximate interference and noise affecting the indoor signal using an academic version of the AirMagnet software.

4.2.2.1.1 Throughput and Jitter The average throughput and jitter recorded on the mobile device over the time during the experiment plotted by UDP/TCP packets is depicted in Figure 4.14. These results are collected using local Linux logging tools, runnable also on Android (i.e., iptraf and trafshow). It can be seen that the UDP throughput is higher than the TCP throughput. Indeed, the TCP protocol uses connected mode, and it is highly optimized to make reliable use of the link. Therefore, this decreases the throughput and increases the jitter compared to UDP because of the handshake mechanism for the pre-/post-connection process. However, UDP is used for real-time data (e.g., voice and video over IP) and recommended for high-latency links.

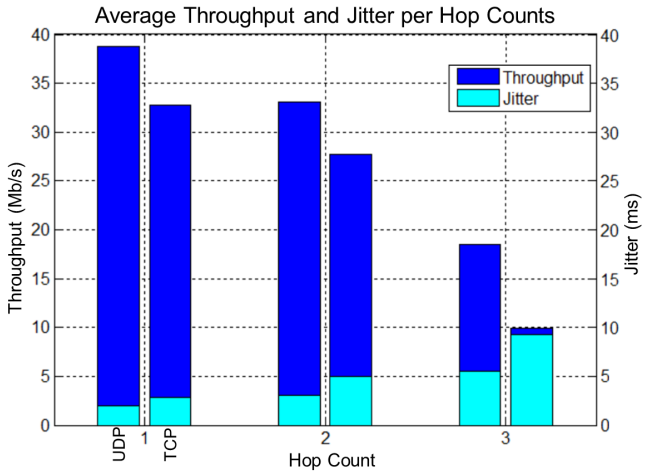


FIGURE 4.14: Average TCP and UDP throughput (Mbit/s) and jitter (ms) per hop count.

Now, with regards to the hop counts, UDP and TCP throughput averages within one hop are 38.8 and 32.71 Mb/s, respectively. Throughput decreases when the hop count increases to reach 18.47 and 9.87 Mb/s for UDP and TCP, respectively, within three hops. According to the authors of [126], a minimum data rate of 10 Mb/s is required for audio, medical imaging and video and hundreds of kbps for other WBAN applications. It is perceived that CROW^2 achieved a real throughput higher than the data rate requirements. It is also important to note that the throughput is expected to decrease significantly starting from four hops based on the behavior shown in Figure 4.14. The average throughput reduction is accompanied by jitter increase. Recorded jitter values increase also following the same pattern as the throughput. It is important to note here that the maximum accepted jitter for the video streaming application must be less than 40 ms according to [127] and under 30 ms according to Cisco for interactive video (video-conferencing) [128]. Indeed, jitter reaches 9.227 ms with TCP mode within three hops, which stays under the limits of the use of video-streaming. According to the results of throughput and jitter, we conclude that the recommended hop count that guarantees throughput for audio/video streaming and files (i.e., photos, reports, etc.) might be less than or equal to three hops, according to the standard definition video (3 Mb/s). The CROW^2 system assures an acceptable throughput and jitter for routes less than or equal to three hops with regards to the required thresholds cited above.

4.2.2.1.2 End-To-End Delay and Link Quality Estimation The WBAN node behavior during the experiment is observed as depicted by Figure 4.15. The end-to-end link quality estimation (i.e., $E2E_{LQE}$) is a real-time metric calculated between a mobile node and the CC node.

The bottom curve of Figure 4.15 illustrates the $E2E_{LQE}$ results over the time. There is a strong correlation between $E2E_{LQE}$ and the HOP_{Count}. It is observed that when the mobile node reaches more than 3 hops away from the CC node, and maintains that HOP_{Count} for more than 2 s, the $E2E_{LQE}$ decreases sharply. When the $E2E_{LQE}$ decreases significantly, connection latency increases and leads to mobile node disconnection. This is due to many factors: (1) signal degradation caused by the fact of being out of range (and no closed node can relay the mobile's data); and (2) the unstable links between the nodes are caused by the interference effected by WiFi access points, wireless extenders and devices inside the office. Equally important, indoor obstacles raised major signal attenuation [129]. It is noteworthy that the delay in milli-seconds (ms) depicted in Figure 4.15 is reset to zero when a mobile

node is disconnected (we consider that a delay higher than 1000 ms is an immediate disconnection). Hence, this leads us to investigate the accuracy of the delay and disconnection times. For that, we have set up a process to ping the distant CC node every millisecond.

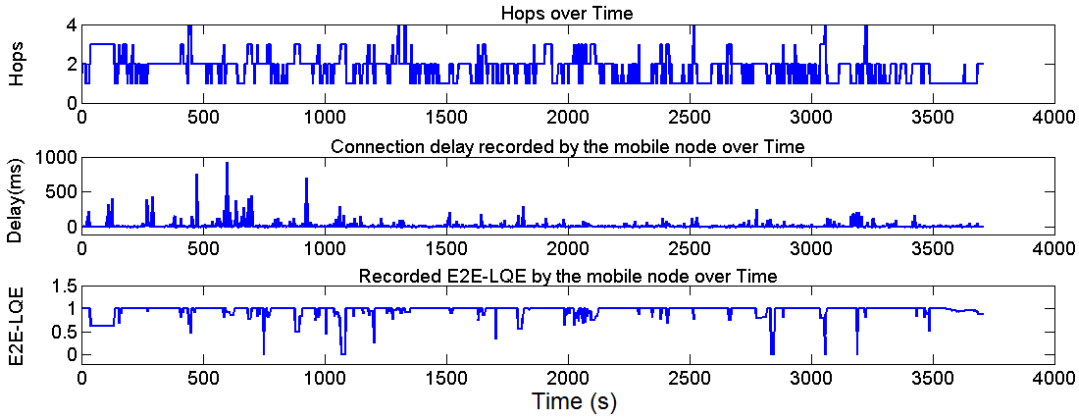


FIGURE 4.15: Hop count, instant delay and end-to-end link quality estimation variation during one hour of experimentation for WBAN node in an indoor scenario.

.

Figure 4.16 depicts the average round trip time delay ($E2E_{delay}$) recorded from the OMD to the Labeeb-IoT platform versus $E2E_{LQE}$. It can be seen that the $E2E_{LQE}$ decreases with the rise of $E2E_{delay}$. Indeed, $E2E_{delay}$ exceeds 1 s when $E2E_{LQE}$ reaches less than 0.7 between 1030 and 1070 s. The same behavior appears between 1155 and 1175 s. $E2E_{LQE}$ and $E2E_{delay}$ are proportional. An $E2E_{LQE}$ equal to zero means that the link is disconnected; the same link shows an infinite $E2E_{delay}$. Figure 4.16 shows also the effectiveness of the metric used in the ORACE-Net routing protocol (i.e., $E2E_{LQE}$). The route update mechanism based on the optimal $E2E_{LQE}$ then is validated by our experiment. Indeed, ORACE-Net prevents the link quality degradation, then looks for a better route with optimized link quality, delay and disconnection avoidance.

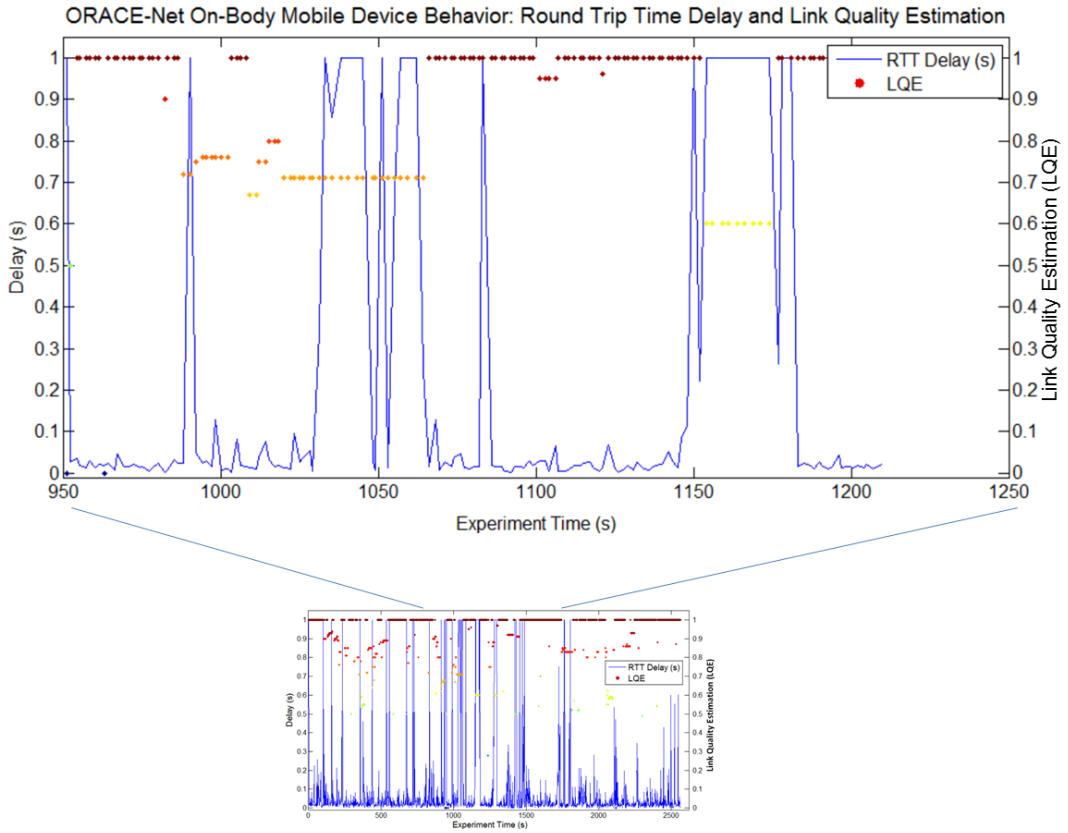


FIGURE 4.16: ORACE-Net on-body mobile device behavior: round trip time delay and link quality estimation.

4.2.2.1.3 Average Disconnections and Round Trip Time Delay for WBAN

The resulted average round-trip time delay and the average end-to-end disconnections per hop count are illustrated in blue and red respectively in Figure 4.17.

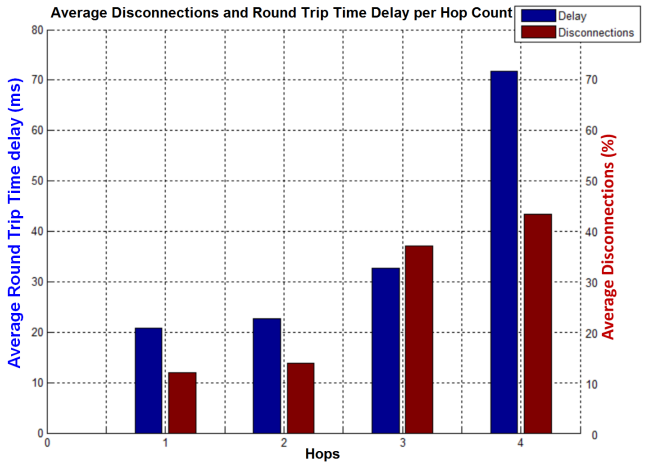


FIGURE 4.17: Average disconnections and round-trip time delay per hop count for WBAN (android smart phone mobile node with ORACE-Net protocol-enabled) in an indoor scenario.

What is important to know is that the average percentage of end-to-end disconnections and average round trip time delay increase accordingly with the hop count. With regards to the mobile smartphones used in the experiment (Samsung Galaxy S3 I9300-Battery: 2300 mAh-WiFi IEEE 802.11n), the experimental range is around 100 m. The experiment shows that the best performance is recorded within 1 hop

(from the mobile node to the CC node) where average disconnection is around 12% and average round-trip time delay is equal to 21 ms. However, a connection within 4 hops (approximate distance between two nodes is 45 m) makes the average end-to-end disconnections exceed 43% as illustrated in Figure 4.17. The average round trip delay increases also to reach 72 ms. It is perceived that for more than 4 hops, average disconnection is expected to exceed 50%.

4.2.2.1.4 Motion Detection and Link Unavailability Anticipation On-body sensors carried by the rescuers push data regularly to the IoT platform. Based on the type of recorded data, we can extract several human behaviors. For instance, gyroscope data recorded and depicted by the Labeeb-IoT platform in Figure 4.18 inform about human mobility. Sensors placed on the hand detect and send gyroscope variations tending to zero when the human has stopped and is not moving. Small variations may be distinguished in the first part of the figure when the human is walking and higher variations of the gyroscope when he/she is running. Figure 4.19 depicts the gyroscope angle variations over more than 2000 s. The gyroscope angle informs about the movement direction. Furthermore, some vital sign information may help the command center to switch rescue teams and send support there; we cite for example magnetometer and heart beat variations reflecting the stress level. All collected data on the IoT platform side could provide also the connectivity status for every deployed node, as can be seen in Figure 4.19. Disconnected nodes inform about the unavailable intermediate links or network over-saturation.

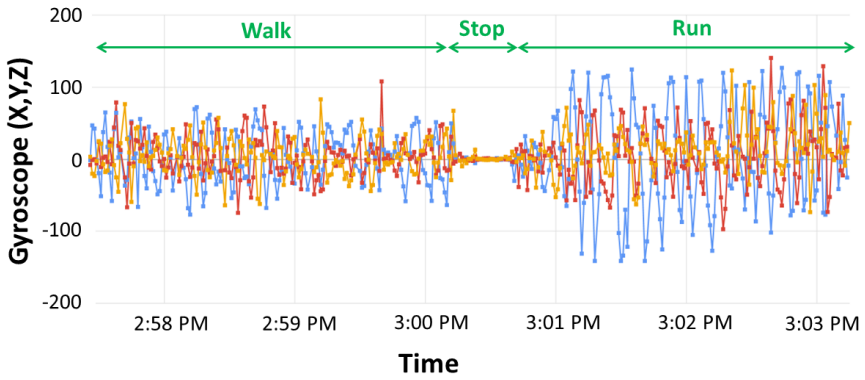


FIGURE 4.18: Gyroscope records over 5 min during the experiment. The X-axis is real time.

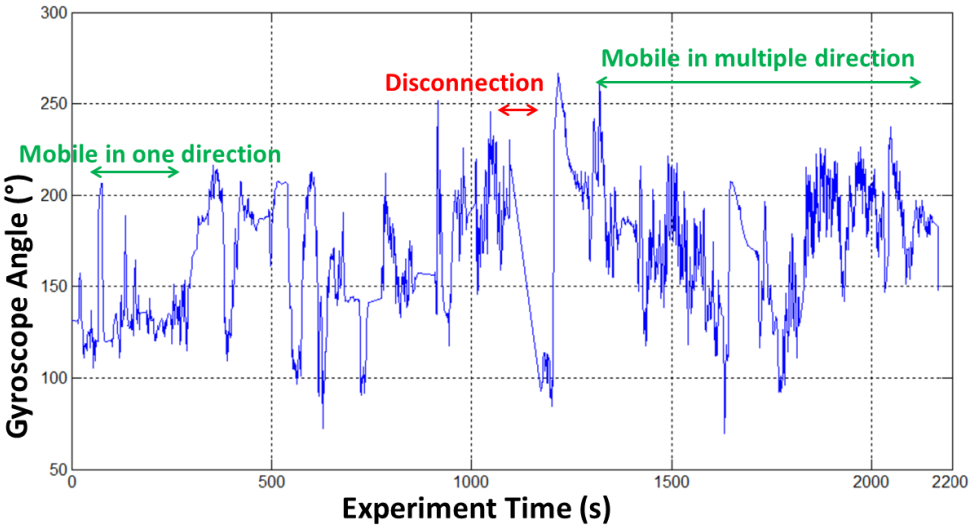


FIGURE 4.19: Gyroscope angle variation over 2200 s of the experiment.

4.2.2.1.5 Interference Score and Noise As given by Table 4.2, the CROW^2 ad hoc network is configured on WiFi Channel 1. Figure 4.20a shows a sample of the interference score recorded indoors along 25 s. Interference varies from 0–53 dBm (as the maximum peak recorded). We assumed during our previous work [118] that the overall network achievements were affected by the indoor interference caused by WiFi access points, microwaves, etc. Thus, we have recorded the interference score and noise to verify whether these facts affect the overall behavior of the emergency network or not. The recorded interference is important compared to the Received Signal Strength Indicator (RSSI), so the signal is notably affected by the interference. However, the overall interference score is likely to decrease because the wireless infrastructure devices and access points are mostly out-of-order post-disaster. Figure 4.20b shows a sample of real-time variation for signal and noise strength as a percentage for Channel 1 during 50 s. The noise floor is given by the red curved waves, and the Signal-to-Noise Ratio (SNR) is depicted in yellow color. The figure shows that the signal strength varies between 3 and 50%. To conclude, interference clearly affects the RSSI and, then, the overall performance of the system. Interference is an important factor that must be considered in indoor emergency operations.

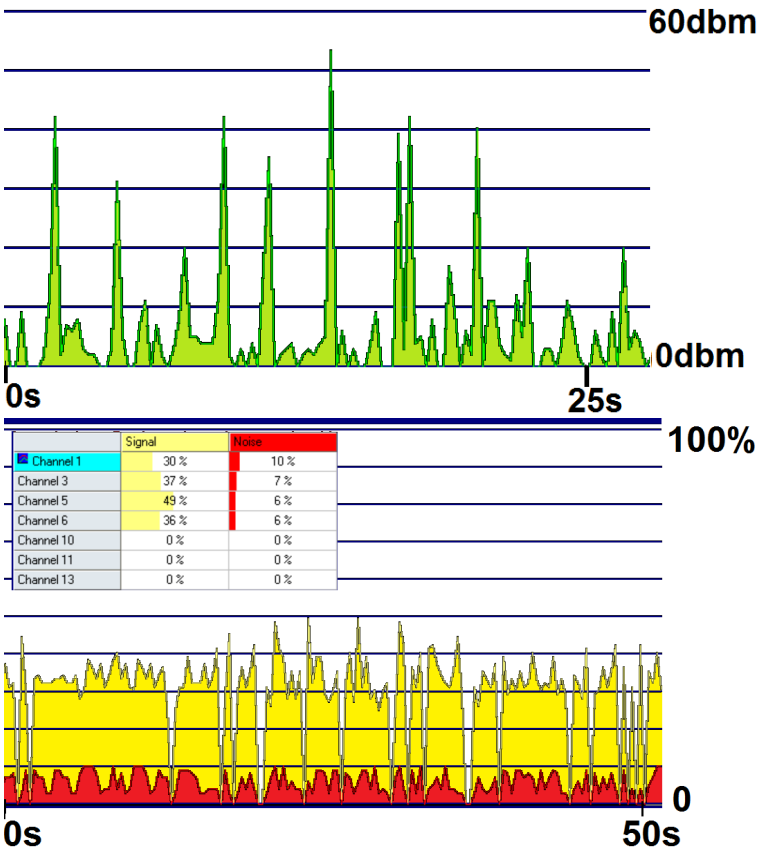


FIGURE 4.20: (**a**) Interference score (in dBm) recorded over 25 s on the channel at 2.412 GHz (AirMagnet WiFi Analyzer Limited Edition). (**b**) Screen-shot of signal and noise (as a percentage) recorded over 50 s (AirMagnet WiFi Analyzer Limited Edition).

4.3 Conclusion

In this chapter, we presented the CROW^2 system, an IoT end-to-end emergency and disaster relief system. CROW^2 is implemented based on ORACE-Net routing protocol, which is especially designed for the disaster context. To evaluate the performance of the proposed system, we deployed the routing protocol and the payload applications on two different platforms (Raspberry Pi and Android smart phone). We equipped a rescuer with on-body sensors connected to a smart phone via Bluetooth. The entire system uses an IoT platform as a back-end to push, record, publish and analyze sensed data. The performance of the system is investigated according to the following relevant metrics: average throughput and jitter, average end-to-end delay and average link quality estimation. We emphasized also motion detection and links' unavailability prevention based on the collected data. Finally, we sampled the indoor interference score and noise to estimate its impact on the system behavior. It can be concluded that the CROW^2 system outperformed the given requirements for the urban wireless wearable body-to-body communications in terms of throughput and jitter. However, being effected by the indoor environment, the behaviors of $E2E_{LQE}$ and $E2E_{delay}$ are moderately fair.

Chapter 5

General Conclusion and Perspectives

5.1 Conclusion

The overriding purpose of this thesis is to cover five main concerns. First, review the state of the art of the existing studies and approaches that investigates the wireless data communication approaches for disaster relief context. Evaluate the existing approaches by simulation to understand their weaknesses and point of failures. Second, design new networking functionalities for the specific context of On-Body and Body-to-Body networks, including efficient radio link quality estimation, cooperative and multi-hop Intra/Inter-BANs routing protocols, support for dynamic network topologies, infrastructure-less and stable end-to-end connectivity, etc. Third, evaluate the performance of the Cross-layer MAC/Networking communication proposed schema for the specific context (i.e., emergency and disaster relief) of On-Body and Body-to-Body networks, based on simulations and according to different realistic mobility scenarios. Fourth, implement the proposed approach on real testbed and evaluate its performances in realistic conditions. And finally, discuss the overall obtained results and disseminate the technical and scientific outcomes.

To achieve these goals, it was necessary to reach some prerequisite goals. First, a deep understanding of the Mobile Ad Hoc routing protocols was mandatory to acquire advanced knowledge of routing operating techniques. While studying different protocols from various routing classes (i.e., proactive, reactive, geographic-based, gradient-based, QoS-aware,etc.) based on their issued standard references and Request For Comments (RFCs), a specific learning of the networking layer functionalities has been acquired. Second challenge, was to master a network simulation software and a numerical computing environment, in order to implement existing standards in one hand, then, design and implement new proposed approach in the other hand. Thirdly, the proposed routing approach (Optimized Routing Approach for Critical and Emergency Networks: ORACE-Net) which is the scope this work, is designed with regards to the limitations concluded from the other studied protocols. Indeed, ORACE-Net was implemented on the latest operating open platforms (Linux, Android), and was deployed on various devices within the CROW^2 system. Finally, an Internet of Things (IoT) platform was used in the back-end of the solution to exploit real-time data collected from sensors and deployed devices for analysis purposes.

The outcomes of this work fall into two categories:

1. Research Contributions:

    - This thesis, as a part of the CROW^2 project, was an opportunity to disseminate several research works (book chapter, journal papers, conferences,

workshops, etc.). Within the scope of this thesis, a book chapter has been written about the state-of-art of the routing protocols for public safety networks. Four journal papers have been disseminated to present ORACE-Net routing and then its enhanced version. Nine conference papers have been published to disseminate the results of the analytical study, simulations and experiments of ORACE-Net routing protocol and CROW^2 project.

- Within this work, the state-of-the-art of the existing standards and recent proposals related to the thesis have been investigated and discussed.
- Based on the learned limitations from the existing disaster relief and emergency routing approaches from one hand, and the disaster management operational requirements on the other hand, we have proposed ORACE-Net as a new approach to overcome the limitations.
- An analytical study has been performed to evaluate theoretically the communication overhead of the proposed approach compared to the other studied protocols.
- The proposed approach (i.e., ORACE-Net) was implemented on WSNET 3.0 network simulator and compared to the other body-to-body routing candidate approaches from different classes.

2. Proof of Concept:

   - This work has been validated by simulation and then implemented on real testbed.
   - As the core of the CROW^2 system, ORACE-Net routing approach outperformed the existing proposals and standards, in particular in terms of the end-to-end link quality estimation and end-to-end delay in the context of disaster relief operations.
   - ORACE-Net is a multi-hop ORACE-Net approach implemented on open source operating platforms, portable on various devices configurations. Based on our experiments, ORACE-Net increases connectivity efficiency and reduced average disconnection.

5.2 Perspectives

This work can not be seen within an academic perspective only, but industrial also. In fact, it contributes to the nodes mobility experimentation according to different mobility patterns, where the nodes' wireless connectivity behavior is investigated and discussed. The existing research and implementation works lack of similar real analysis. In addition, the implemented applications on different platforms (i.e., Linux, Android and WSNET simulator), could be tested on-board of different wireless devices such as Unmanned Aerial Vehicles (i.e., drones) for instance, as proposed recently by authors in [130]. Indeed, UAVs have become essential components in the critical applications, such as border surveillance, disaster response, traffic monitoring, and the transportation of goods, medicine, and first aid [131]. As a matter of fact, the next-generation of Aerial Medical Assistance, a top trending remote assistance use case where UAVs are not only able to carry and deliver first aid packs to urban areas but also to inaccessible conflict areas. As a complimentary mission, the UAVs can ensure the first aid assistance using on-body sensors (placed by the wounded person himself, any surrounding person or even the UAV itself). On-body vital signs data

is then gathered and routed from UAV to UAV/infrastructure to reach the conflict management center. Within the explained above context, the here presented thesis could be extended and the proposed protocol could be deployed as a routing technique in the Aerial Medical Assistance.

Furthermore, many commercial applications have been announced recently integrating wireless communication networking, positioning, and IoT. Given as an e.g., during a cars rally happening usually in non-urban zones, a wireless safety mesh network is deployed to inter-connect the various mobile nodes (i.e., cars, motorbikes, drones, helicopters, etc.). Relying on such network, all nodes could be monitored and real-time data could be routed using ORACE-Net or any other adapted routing protocol. Moreover, data gathered from smart things (smart watches, smart TVs, broadband devices, etc.) could be integrated within this scope as a rich source of information to be considered during a disaster. Now, as recently the 5G specifications are issued, 5G could be investigated as a communication alternative among which this proposal could be also evaluated, especially with the advanced Industrial Internet-of-Things developed features coming within the Industry 4.0. Undoubtedly, some major sensing limitations are still to overcome, such as the limited range for instance, but the main challenge is to consider the emergency response system as an available network over which devices could switch and connect efficiently during pre and post disaster times.

If we assess this thesis findings, we can conclude that the studied, proposed and implemented approach is above the fourth level according to the Technology readiness levels (TRL) method estimating technology maturity of Critical Technology Elements (CTE) of a program during the acquisition process [132]. Indeed, this thesis fulfilled TRL 4 called: "Component and/or breadboard validation in laboratory environment", called also "Research to Prove Feasibility" phase where first, the state of the art is studied and discussed. Second, the concept of the technology is designed and formulated, and finally simulated. After that, the proposal is implemented to be then analyzed and evaluated to come up finally with the proof-of-concept (PoC) presented through the previous chapter of this work. As a next chapter according to the TRL cycle, the TRL 5 could be tackled, the upcoming related works could target the technology development for the approach maturing through the following points of interest: i) This PoC could be reimplemented on different platforms and evaluated during a real disaster incidents during which the collected data is compared with the data gathered from the existing solutions. ii) Different data flow types could be tested among an ORACE-Net based architecture (i.e., video streaming, live video broadcasts, etc.). iii) Manufacturing of ORACE-Net devices and integration of this approach as an emergency protocol running when mobile users switch to the emergency mode.

Bibliography

[1] UNISDR. *UNISDR - ANNUAL REPORT*. Tech. rep. United Nations Office of Disaster Risk Reduction, 2015.

[2] Joanna Walters. *The Guardian @ONLINE*. Sept. 2017. URL: *https://www.theguardian.com/world/2017/sep/01/hurricane-harvey-us-billion-dollar-weather-disasters-2017*.

[3] Muhammad Mahtab Alam and Elyes Ben Hamida. "Surveying Wearable Human Assistive Technology for Life and Safety Critical Applications: Standards, Challenges and Opportunities". In: *Sensors* 14.5 (2014), pp. 9153–9209. ISSN: 1424-8220. DOI: *10.3390/s140509153*.

[4] Giacinto Luigi Cerone. "Development of a wireless system for the remote monitoring of muscular activity". In: *Gait & Posture* 57 (2017), pp. 34–35.

[5] Sana Tmar-Ben Hamida, Elyes Ben Hamida, and Beena Ahmed. "A New mHealth Communication Framework for Use in Wearable WBANs and Mobile Technologies". In: *Sensors* 15.2 (2015), pp. 3379–3408. ISSN: 1424-8220. DOI: *10.3390/s150203379*. URL: *http://www.mdpi.com/1424-8220/15/2/3379*.

[6] Bin Liu, Hao Luo, and Chang Wen Chen. "A Novel Authentication Scheme Based on Acceleration Data in WBAN". In: *Connected Health: Applications, Systems and Engineering Technologies (CHASE), 2017 IEEE/ACM International Conference on*. IEEE. 2017, pp. 120–126.

[7] Jaime Lloret et al. "An architecture and protocol for smart continuous eHealth monitoring using 5G". In: *Computer Networks* 129 (2017). Special Issue on 5G Wireless Networks for IoT and Body Sensors, pp. 340–351. ISSN: 1389-1286. DOI: *https://doi.org/10.1016/j.comnet.2017.05.018*. URL: *http://www.sciencedirect.com/science/article/pii/S1389128617302189*.

[8] Elyes Ben Hamida et al. "Wearable Body-to-Body Networks for Critical and Rescue Operations, The CROW² Project". In: *procedding of the Workshop on the Convergence of Wireless Technologies for Personalized Healthcare in IEEE PIMRC 2014*. Sept. 2014, pp. 2145–2149. DOI: *10.1109/PIMRC.2014.7136527*.

[9] *IEEE 802.15 WPAN™ Task Group 6 (TG6) Body Area Networks*. *http://www.ieee802.org/15/pub/TG6.html*. Accessed: 2017-04-11.

[10] *WSNET 3.0 Simulator*. *http://wsnet.gforge.inria.fr/*. Accessed: 2015-11-30.

[11] Elyes Ben Hamida and Guillaume Chelius. "Analytical Evaluation of Virtual Infrastructures for Data Dissemination in Wireless Sensor Networks with Mobile Sink". In: *proceedings of the First ACM Workshop on Sensor and Actor Networks*. 2007, pp. 3–10. DOI: *10.1145/1287731.1287734*.

[12] S. Movassaghi, M. Abolhasan, and D. Smith. "Interference Mitigation in WBANS: Challenges and Existing solutions". In: *Workshop on Advances in Real-time Information Networks, 2013*. 2013, pp. 1–4.

[13] Elyes Ben Hamida and Guillaume. Chelius. "Strategies for data dissemination to mobile sinks in wireless sensor networks". In: *Wireless Communications, IEEE* 15.6 (Dec. 2008), pp. 31–37. DOI: 10.1109/MWC.2008.4749745.

[14] Daojing He et al. "Lightweight and Confidential Data Discovery and Dissemination for Wireless Body Area Networks". In: *Biomedical and Health Informatics, IEEE Journal of* 18.2 (Mar. 2014), pp. 440–448. DOI: 10.1109/JBHI.2013.2293620.

[15] Elyes Ben Hamida et al. "Short-term link quality estimation for Opportunistic and Mobility Aware Routing in wearable body sensors networks". In: *proceedings of the IEEE 10th International Conference on Wireless and Mobile Computing Networking and Communications (WiMob)*. Oct. 2014, pp. 519–526.

[16] ClementOgugua Asogwa et al. "Experimental Analysis of AODV, DSR and DSDV Protocols Based on Wireless Body Area Network". English. In: *Internet of Things*. Vol. 312. Communications in Computer and Information Science. 2012, pp. 183–191. ISBN: 978-3-642-32426-0. DOI: 10.1007/978-3-642-32427-7_25. URL: http://dx.doi.org/10.1007/978-3-642-32427-7_25.

[17] JayanthiK. Murthy, P. Thimmappa, and V. Sambasiva Rao. "Investigations on the Routing Protocols for Wireless Body Area Networks". English. In: *Proceedings of International Conference on Advances in Computing*. Ed. by Aswatha Kumar M., Selvarani R., and T V Suresh Kumar. Vol. 174. Advances in Intelligent Systems and Computing. Springer India, 2012, pp. 483–490. ISBN: 978-81-322-0739-9. DOI: 10.1007/978-81-322-0740-5_59. URL: http://dx.doi.org/10.1007/978-81-322-0740-5_59.

[18] C. Bohannan et al. "QoS Enhancement and Performance Evaluation of Ad-Hoc Routing Protocols for Rural Public Safety". In: *Communications, 2009. ICC '09. IEEE International Conference on*. June 2009, pp. 1–5. DOI: 10.1109/ICC.2009.5199377.

[19] P. Kolios et al. "Qualifying explore and exploit for efficient data dissemination in emergency adhoc networks". In: *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2014 IEEE International Conference on*. Mar. 2014, pp. 303–307. DOI: 10.1109/PerComW.2014.6815222.

[20] Richard Wolff et al. *Ad Hoc Routing for Rural Public Safety*. Tech. rep. DHS-06-ST-086-006. Nov. 2008, pp. 1–149. URL: http://www.westerntransportationinstitute.org/documents/reports/%204w1566_final_report.pdf.

[21] Jiazi Yi et al. "Implementation of multipath and multiple description coding in OLSR". In: *arXiv preprint arXiv:0902.4781* (2009).

[22] T. Clausen and P. Jacquet. *Optimized Link State Routing Protocol (OLSR)*. Tech. rep. Oct. 2003, pp. 1–75.

[23] Shree Murthy and Jose Joaquin Garcia-Luna-Aceves. "An efficient routing protocol for wireless networks". In: *Mobile Networks and applications* 1.2 (1996), pp. 183–197.

[24] Charles E Perkins and Pravin Bhagwat. "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers". In: *ACM SIGCOMM computer communication review*. Vol. 24. 4. ACM. 1994, pp. 234–244.

[25] Yi Jiazi et al. "Implementation of Multipath and Multiple Description Coding in OLSR". In: *proceedings of the Fourth OLSR Interop/Workshop*. Feb. 2009, pp. 1–5.

[26] Anuj K Gupta, Harsh Sadawarti, and Anil K Verma. "Review of various routing protocols for MANETs". In: *International Journal of Information and Electronics Engineering* 1.3 (2011), p. 251.

[27] Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz. "A review of routing protocols for mobile ad hoc networks". In: *Ad Hoc Networks* 2.1 (2004), pp. 1–22. DOI: *http://dx.doi.org/10.1016/S1570-8705(03)00043-X*.

[28] Thomas Clausen et al. "Securing the OLSR routing protocol with or without compromised nodes in the network". PhD thesis. INRIA, 2005.

[29] Thomas Heide Clausen and Ulrich Herberg. "Security issues in the optimized link state routing protocol version 2 (OLSRv2)". PhD thesis. INRIA, 2010.

[30] Charles E Perkins and Pravin Bhagwat. "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers". In: *ACM SIGCOMM computer communication review*. Vol. 24. 4. ACM. 1994, pp. 234–244.

[31] C. Perkins et al. "Ad Hoc On-demand Distance Vector version 2 (AODVv2) Routing". In: IETF. May 2016. URL: *https://tools.ietf.org/html/draft-ietf-manet-aodvv2-16*.

[32] Narendran Sivakumar and Satish Kumar Jaiswal. "Comparison of DYMO protocol with respect to various quantitative performance metrics". In: *Department of Computer Science, Malardalen University* (2009).

[33] Anuj K Gupta, Harsh Sadawarti, and Anil K Verma. "Implementation of DYMO routing protocol". In: *arXiv preprint arXiv:1306.1338* (2013).

[34] David B Johnson, David A Maltz, and Josh Broch. "DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks". In: *Ad hoc networking* (2006), p. 139172.

[35] Vincent Douglas Park and M Scott Corson. "A highly adaptive distributed routing algorithm for mobile wireless networks". In: *INFOCOM'97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution., Proceedings IEEE*. Vol. 3. IEEE. 1997, pp. 1405–1413.

[36] Elizabeth M Belding-Royer. "Hierarchical routing in ad hoc mobile networks". In: *Wireless Communications and Mobile Computing* 2.5 (2002), pp. 515–532.

[37] Naveen Chauhan et al. "A distributed weighted cluster based routing protocol for MANETs". In: *Computer Networks and Information Technologies* (2011), pp. 147–151.

[38] Fraser Cadger et al. "A survey of geographical routing in wireless ad-hoc networks". In: *IEEE Communications Surveys & Tutorials* 15.2 (2013), pp. 621–653.

[39] 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*. ACM. 2000, pp. 243–254.

[40] Kuk-Hyun Cho and Min-Woo Ryu. "A survey of greedy routing protocols for vehicular ad hoc networks". In: *SmartCR* 2.2 (2012), pp. 125–137.

[41] 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*. ACM. 2000, pp. 56–67.

[42] Deepak Goyal and Malay Ranjan Tripathy. "Routing protocols in wireless sensor networks: A survey". In: *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on*. IEEE. 2012, pp. 474–480.

[43] Yuan Hu, Weisi Guo, and Siyi Wang. "Emergency Route Selection for D2D Cellular Communications During an Urban Terrorist Attack". In: *CoRR* abs/1403.6923 (2014). URL: *http://arxiv.org/abs/1403.6923*.

[44] Pinyi Ren, Qinghe Du, and Li Sun. "Interference-aware routing for hop-count minimization in wireless D2D networks". In: *Communications in China - Workshops (CIC/ICCC), 2013 IEEE/CIC International Conference on*. Aug. 2013, pp. 65–70. DOI: *10.1109/ICCChinaW.2013.6670569*.

[45] L. Babun. "Extended Coverage for Public Safety and Critical Communications Using Multi-hop and D2D Communications, M.Sc Dissertation, Florida International University, USA." In: (2015).

[46] C. Tata and M. Kadoch. "Multipath routing algorithm for device-to-device communications for public safety over LTE Heterogeneous Networks". In: *Information and Communication Technologies for Disaster Management (ICT-DM), 2014 1st International Conference on*. Mar. 2014, pp. 1–7. DOI: *10.1109/ICT-DM.2014.6918583*.

[47] A. Laha et al. "An energy efficient routing protocol for device-to-device based multihop smartphone networks". In: *Communications (ICC), 2015 IEEE International Conference on*. June 2015, pp. 5448–5453. DOI: *10.1109/ICC.2015.7249190*.

[48] Min Chen et al. "Body Area Networks: A Survey". In: *Mobile Networks and Applications* 16.2 (Apr. 2011), pp. 171–193. ISSN: 1572-8153. DOI: *10.1007/s11036-010-0260-8*. URL: *http://dx.doi.org/10.1007/s11036-010-0260-8*.

[49] Tia Gao et al. "The advanced health and disaster aid network: A light-weight wireless medical system for triage". In: *IEEE Transactions on biomedical circuits and systems* 1.3 (2007), pp. 203–216.

[50] Rim Negra, Imen Jemili, and Abdelfettah Belghith. "Wireless Body Area Networks: Applications and Technologies". In: *Procedia Computer Science* 83 (2016). The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016) / The 6th International Conference on Sustainable Energy Information Technology (SEIT-2016) / Affiliated Workshops, pp. 1274–1281. ISSN: 1877-0509. DOI: *http://dx.doi.org/10.1016/j.procs.2016.04.266*. URL: *http://www.sciencedirect.com/science/article/pii/S187705091630299X*.

[51] K. Gomez et al. "Enabling disaster-resilient 4G mobile communication networks". In: *IEEE Communications Magazine* 52.12 (Dec. 2014), pp. 66–73. ISSN: 0163-6804. DOI: *10.1109/MCOM.2014.6979954*.

[52] Joe Prathap Pathrose Varun G. Menon and Jogi Priya. "Ensuring Reliable Communication in Disaster Recovery Operations with Reliable Routing Technique". In: *Mobile Information Systems* (2016), p. 10. DOI: *10.1155/2016/9141329*.

[53] Guohong Cao Zongqing Lu and Thomas La Porta. "Networking Smartphones for Disaster Recovery". In: *Proceedings of IEEE PerCom, 2016* (2016).

[54] S. M. George et al. "DistressNet: a wireless ad hoc and sensor network architecture for situation management in disaster response". In: *IEEE Communications Magazine* 48.3 (Mar. 2010), pp. 128–136. ISSN: 0163-6804. DOI: *10.1109/MCOM.2010.5434384*.

[55] Marco Di Felice, Luca Bedogni, and Luciano Bononi. "The Emergency Direct Mobile App: Safety Message Dissemination over a Multi-Group Network of Smartphones Using Wi-Fi Direct". In: *Proceedings of the 14th ACM International Symposium on Mobility Management and Wireless Access*. MobiWac '16. Malta, Malta: ACM, 2016, pp. 99–106. ISBN: 978-1-4503-4503-3. DOI: *10.1145/2989250.2989257*. URL: *http://doi.acm.org/10.1145/2989250.2989257*.

[56] Xi Chen, Yixuan Xu, and Anfeng Liu. "Cross Layer Design for Optimizing Transmission Reliability, Energy Efficiency, and Lifetime in Body Sensor Networks". In: *Sensors* 17.4 (Apr. 2017), p. 900. ISSN: 1424-8220. DOI: *10.3390/s17040900*. URL: *http://dx.doi.org/10.3390/s17040900*.

[57] Gill R Tsouri, Alvaro Prieto, and Nikhil Argade. "On increasing network lifetime in body area networks using global routing with energy consumption balancing". In: *Sensors* 12.10 (2012), pp. 13088–13108.

[58] Jorge Miranda et al. "An Open Platform for Seamless Sensor Support in Healthcare for the Internet of Things". In: *Sensors* 16.12 (2016), p. 2089.

[59] T. Clausen et al. "RFC7181: The Optimized Link State Routing Protocol Version 2 (Proposed Standard)". In: (Apr. 2014). DOI: *http://dx.doi.org/10.17487/RFC7181*. URL: *http://www.rfc-editor.org/info/rfc7181*.

[60] C. Perkins and E. Royer. "Ad-hoc on-demand distance vector routing". In: *proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications*. Feb. 1999, pp. 90–100. DOI: *10.1109/MCSA.1999.749281*.

[61] C. Perkins, S. Ratliff, and Dowdell J. "Dynamic MANET On-demand (AODVv2) Routing draft-ietf-manet-dymo-26". In: (Apr. 2013). URL: *https://datatracker.ietf.org/doc/draft-ietf-manet-dymo/*.

[62] David B. Johnson, David A. Maltz, and Josh Broch. "Ad Hoc Networking". In: Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2001. Chap. DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks, pp. 139–172. ISBN: 0-201-30976-9. URL: *http://dl.acm.org/citation.cfm?id=374547.374552*.

[63] Tipu Arvind Ramrekha and Christos Politis. "A Hybrid Adaptive Routing protocol for Extreme Emergency Ad Hoc Communication". In: *Proceedings of 19th International Conference on Computer Communications and Networks (ICCCN)*. 2010. DOI: *10.1109/ICCCN.2010.5560057*.

[64] T. A. Ramrekha et al. "Energy Efficient and Scalable Routing Protocol for Extreme Emergency Ad Hoc Communications". In: *International Journal of Mobile Networks and Applications* 17.2 (Apr. 2012), pp. 312–324. DOI: *10.1007/s11036-011-0336-0*.

[65] Dhafer Ben Arbia et al. "Behavior of Wireless Body-to-Body Networks Routing Strategies for Public Protection and Disaster Relief". In: *proceedings of the Workshop on Advances in Body-Centric Wireless Communications and Networks and Their Applications (BCWNets 2015), in 11th IEEE WiMob Conference*. Oct. 2015.

[66] Gianmarco Baldini et al. “Survey of wireless communication technologies for public safety”. In: *IEEE Communications Surveys & Tutorials* 16.2 (2014), pp. 619–641.

[67] Leonard E Miller. “Wireless Technologies and the SAFECOM SoR for Public Safety Communications”. In: *NIST Technical Report, http://www. antd. nist. gov/wctg/manet/docs/WirelessAndSoR060206. pdf (accessed February 2006)* (2005).

[68] *A NPSTC Public Safety Communications Report-Defining Public Safety Grade Systems and Facilities*. Tech. rep. May 2014, pp. 1–112.

[69] Raul Aquino Santos. *Broadband Wireless Access Networks for 4G: Theory, Application, and Experimentation: Theory, Application, and Experimentation*. IGI Global, 2013.

[70] Samaneh Movassaghi et al. “Wireless body area networks: A survey”. In: *IEEE Communications Surveys & Tutorials* 16.3 (2014), pp. 1658–1686.

[71] Javed Iqbal Bangash et al. “A survey of routing protocols in wireless body sensor networks”. In: *Sensors* 14.1 (2014), pp. 1322–1357.

[72] S Movassaghigilani, Mehran Abolhasan, and Justin Lipman. “A review of routing protocols in wireless body area networks”. In: *Journal of networks* (2013).

[73] Bart Braem et al. “The wireless autonomous spanning tree protocol for multihop wireless body area networks”. In: *Mobile and Ubiquitous Systems: Networking & Services, 2006 Third Annual International Conference on*. IEEE. 2006, pp. 1–8.

[74] Bart Braem et al. “Improving reliability in multi-hop body sensor networks”. In: *Sensor Technologies and Applications, 2008. SENSORCOMM'08. Second International Conference on*. IEEE. 2008, pp. 342–347.

[75] Anirban Bag. *Medium access control protocols and routing algorithms for wireless sensor networks*. University of Central Florida, 2007.

[76] Xiaohui Liang et al. “Exploiting prediction to enable secure and reliable routing in wireless body area networks”. In: *INFOCOM, 2012 Proceedings IEEE*. IEEE. 2012, pp. 388–396.

[77] Samaneh Movassaghi, Mehran Abolhasan, and Justin Lipman. “Energy efficient thermal and power aware (ETPA) routing in body area networks”. In: *Personal Indoor and Mobile Radio Communications (PIMRC), 2012 IEEE 23rd International Symposium on*. IEEE. 2012, pp. 1108–1113.

[78] Benjamin J Culpepper, Lan Dung, and Melody Moh. “Design and analysis of Hybrid Indirect Transmissions (HIT) for data gathering in wireless micro sensor networks”. In: *ACM SIGMOBILE Mobile Computing and Communications Review* 8.1 (2004), pp. 61–83.

[79] Wendi B Heinzelman, Anantha P Chandrakasan, and Hari Balakrishnan. “An application-specific protocol architecture for wireless microsensor networks”. In: *IEEE Transactions on wireless communications* 1.4 (2002), pp. 660–670.

[80] Chad Bohannan et al. “QoS enhancement and performance evaluation of adhoc routing protocols for rural public safety”. In: *Communications, 2009. ICC'09. IEEE International Conference on*. IEEE. 2009, pp. 1–5.

[81] Mahin K Atiq, Hyung Seok Kim, and Kamran Manzoor. “Cluster based routing protocol for public safety networks”. In: *ICT Convergence (ICTC), 2013 International Conference on*. IEEE. 2013, pp. 435–439.

[82] Riccardo Fedrizzi et al. "Energy aware routing in heterogeneous multi-hop public safety wireless networks". In: *Communications Workshops (ICC), 2014 IEEE International Conference on*. IEEE. 2014, pp. 218–224.

[83] Athina Bourdena et al. "A spectrum aware routing protocol for public safety applications over cognitive radio networks". In: *Telecommunications and Multimedia (TEMU), 2012 International Conference on*. IEEE. 2012, pp. 7–12.

[84] Yaling Yang and Robin Kravets. *Achieving delay guarantees in ad hoc networks using distributed contention window adaptation*. Tech. rep. 2005.

[85] Yaling Yang and Robin Kravets. "Throughput guarantees for multi-priority traffic in ad hoc networks". In: *Ad Hoc Networks* 5.2 (2007), pp. 228–253.

[86] A. Bourdena et al. "A spectrum aware routing protocol for public safety applications over cognitive radio networks". In: *Telecommunications and Multimedia (TEMU), 2012 International Conference on*. July 2012, pp. 7–12. DOI: *10.1109/TEMU.2012.6294737*.

[87] Roy Fielding et al. *Hypertext transfer protocol–HTTP/1.1*. Tech. rep. 1999.

[88] Zach Shelby, Klaus Hartke, and Carsten Bormann. "The constrained application protocol (CoAP)". In: (2014).

[89] *OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0; OASIS Standard*. *http://docs.oasis-open.org/amqp/core/v1.0/os/amqp-core-complete-v1.0-os.pdf*. Accessed: 2015-06-25.

[90] Urs Hunkeler, Hong Linh Truong, and Andy Stanford-Clark. "MQTT-S—A publish/subscribe protocol for Wireless Sensor Networks". In: *Communication systems software and middleware and workshops, 2008. comsware 2008. 3rd international conference on*. IEEE. 2008, pp. 791–798.

[91] Andy Stanford-Clark and Hong Linh Truong. "Mqtt for sensor networks (mqtt-sn) protocol specification". In: *International business machines (IBM) Corporation version* 1 (2013).

[92] Muhammad Mahtab Alam and Elyes Ben Hamida. "Wearable Wireless Sensor Networks: Applications, Standards, and Research Trends". In: *Emerging Communication Technologies Based on Wireless Sensor Networks: Current Research and Future Applications* (2016), p. 59.

[93] "IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks". In: *IEEE Std 802.15.6-2012* (Feb. 2012), pp. 1–271. DOI: *10.1109/IEEESTD.2012.6161600*.

[94] IEEE 802.11 Working Group et al. "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications". In: *IEEE Std* 802.11 (2010).

[95] "Approved IEEE Draft Standard for Information Technology– Telecommunications and Information Exchange Between Systems– Local and Metropolitan Area Networks– Specific Requirements Part 15.1Reva: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs) (Replaced by IEEE 802.15.1-2005)". In: *IEEE Std P802.15.1/D6* (2004).

[96] "IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)". In: *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)* (Sept. 2011), pp. 1–314. DOI: 10.1109/IEEESTD.2011.6012487.

[97] "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirement Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)". In: *IEEE Std 802.15.4a-2007 (Amendment to IEEE Std 802.15.4-2006)* (2007), pp. 1–203. DOI: 10.1109/IEEESTD.2007.4299496.

[98] Dhafer Ben Arbia et al. "ORACE-Net: A novel multi-hop body-to-body routing protocol for public safety networks". In: *Peer-to-Peer Networking and Applications* (2016), pp. 1–24. ISSN: 1936-6450. DOI: 10.1007/s12083-016-0513-9. URL: http://dx.doi.org/10.1007/s12083-016-0513-9.

[99] Dhafer Ben Arbia et al. "Enhanced IoT-Based End-To-End Emergency and Disaster Relief System". In: *Journal of Sensor and Actuator Networks* 6.3 (2017), p. 19.

[100] C. Clausen T. Dearlove and J. Dean. *Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP),* 2011. URL: https://tools.ietf.org/html/rfc6130.

[101] Elyes Ben Hamida et al. "Short-term link quality estimation for Opportunistic and Mobility Aware Routing in wearable body sensors networks". In: *proceedings of the IEEE 10th International Conference on Wireless and Mobile Computing Networking and Communications (WiMob)*. Oct. 2014, pp. 519–526.

[102] E. Ben Hamida and G. Chelius. "Investigating the impact of human activity on the performance of wireless networks: An experimental approach". In: *WoWMoM 2010 Conference*. June 2010, pp. 1–8. DOI: 10.1109/WOWMOM.2010.5534913.

[103] Santosh Kumar, SC Sharma, and Bhupendra Suman. "Mobility metrics based classification & analysis of mobility model for tactical network". In: *International Journal of Next-Generation Networks* 2.3 (2010), pp. 39–51.

[104] Nils Aschenbruck, Elmar Gerhards-Padilla, and Peter Martini. "Modeling mobility in disaster area scenarios". In: *Performance Evaluation* 66.12 (2009), pp. 773–790.

[105] Muhammad Mahtab Alam and Elyes Ben Hamida. "Interference mitigation and coexistence strategies in IEEE 802.15. 6 based wearable body-to-body networks". In: *International Conference on Cognitive Radio Oriented Wireless Networks*. Springer. 2015, pp. 665–677.

[106] Muhammad Mahtab Alam, DB Arbia, and Elyes Ben Hamida. "Device-to-Device Communication in Wearable Wireless Networks". In: *10th CROWNCOM Conf.* 2015.

[107] Anthony Busson, Nathalie Mitton, and Eric Fleury. "Analysis of the Multi-Point Relays selection in OLSR and consequences". In: *Mediterranean Ad Hoc Networking Workshop (MedHocNet'05)*. Ed. by ACM. ACM. France, 2005.

[108] Mounir Frikha. *Ad Hoc Networks: Routing, QoS and Optimization*. John Wiley & Sons, 2013.

[109] Matthew Gast. *802.11ac: A Survival Guide*. 2013. URL: *http://chimera.labs.oreilly.com/books/1234000001739/ch03.html*.

[110] G.P. Perrucci, F.H.P. Fitzek, and J. Widmer. "Survey on Energy Consumption Entities on the Smartphone Platform". In: *Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd*. May 2011, pp. 1–6. DOI: *10.1109/VETECS.2011.5956528*.

[111] Device Specifications Copyright. *Mobile Devices Specifications*. 2016. URL: *http://www.devicespecifications.com/en/model-battery/d1332bee*.

[112] Nils Aschenbruck et al. "BonnMotion: A Mobility Scenario Generation and Analysis Tool". In: *proceedings of the 3rd International Conference on Simulation Tools and Techniques*. 2010, 51:1–51:10. DOI: *10.4108/ICST.SIMUTOOLS2010.8684*.

[113] M. Mahtab Alam and Elyes (in press) Ben Hamida. "Performance Evaluation of IEEE 802.15.6-based WBANs under Co-Channel Interference". In: *International Journal of Sensor Networks* (2016).

[114] M. M. Alam, E. Ben Hamida, and D. Ben Arbia. "Joint Throughput and Channel Aware (TCA) Dynamic Scheduling Algorithm for Emerging Wearable Applications". In: *2016 IEEE Wireless Communications and Networking Conference (WCNC)*. Apr. 2016.

[115] M. Maman et al. "Evaluation of Multiple Coexisting Body Area Networks Based on Realistic On-Body and Body-to-Body Channel Models". In: *In the Proceedings of 10th International Symposium on Medical Information and Communication Technology (ISMICT'16)*. Mar. 2016.

[116] Francisco E Martinez-Perez et al. "Activity inference for ambient intelligence through handling artifacts in a healthcare environment". In: *Sensors* 12.1 (2012), pp. 1072–1099.

[117] *Information technology Message Queuing Telemetry Transport (MQTT) v3.1.1 - ISO/IEC 20922:2016*. Geneva,CH. July 2016.

[118] Dhafer Ben Arbia et al. "Implementation and Benchmarking of a Novel Routing Protocol for Tactical Mobile Ad-Hoc Networks". In: *proceedings of the Third International Workshop on Emergency Networks for Public Protection and Disaster Relief (EN4PPDR 2016), in 12th IEEE WiMob Conference*. Oct. 2016.

[119] *Shimmer Sensing*. www.shimmersensing.com, accessed: 2016-10-30.

[120] A. Burns et al. "SHIMMER : A Wireless Sensor Platform for Noninvasive Biomedical Research". In: *IEEE Sensors Journal* 10.9 (Sept. 2010), pp. 1527–1534. ISSN: 1530-437X. DOI: *10.1109/JSEN.2010.2045498*.

[121] Qatar Mobility Innovations Center. *Labeeb IoT Platform and Solutions,* 2016. URL: *www.labeeb-iot.com,%20accessed%202016-09-01*.

[122] Muhammad Mahtab Alam and Elyes Ben Hamida. "Interference mitigation and coexistence strategies in IEEE 802.15.6 based wearable body-to-body networks". In: *proceedings of the 10th CROWNCOM Conference, Springer LNICST, Vol. 156*. Apr. 2015, pp. 1–12. DOI: *10.1007/978-3-319-24540-9-55*.

[123] Muhammad Mahtab Alam and Elyes Ben Hamida. "Towards accurate mobility and radio link modeling for IEEE 802.15.6 Wearable Body Sensor Networks". In: *proceedings of the IEEE 10th International Conference on Wireless and Mobile Computing Networking and Communications (WiMob)*. Oct. 2014, pp. 298–305. DOI: 10.1109/WiMOB.2014.6962186.

[124] I. Texas. *2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver*. 2008. URL: http://www.ti.com/product/cc2420.

[125] Muhammad Mahtab Alam and Elyes Ben Hamida. "Performance evaluation of IEEE 802.15.6 MAC for Wearable Body Sensor Networks using a Space-Time dependent radio link model". In: *proceedings of the IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA)*. Nov. 2014, pp. 441–448. DOI: 10.1109/AICCSA.2014.7073232.

[126] Chinmay Chakraborty, Bharat Gupta, and Soumya K Ghosh. "A review on telemedicine-based WBAN framework for patient monitoring". In: *Telemedicine and e-Health* 19.8 (2013), pp. 619–626.

[127] Basem Al-Madani, Anas Al-Roubaiey, and Zubair A. Baig. "Real-Time QoS-Aware Video Streaming: A Comparative and Experimental Study". In: *Advances in Multimedia* (2014), p. 10. DOI: 10.1155/2014/164940.

[128] *Quality of Service Design Overview*. http://www.ciscopress.com/articles/article.asp?p=357102&seqNum=2. Accessed: 2017-02-20.

[129] Daniel B Faria et al. "Modeling signal attenuation in ieee 802.11 wireless lans-vol. 1". In: *Computer Science Department, Stanford University* 1 (2005).

[130] Celia Yasmine Tazibt et al. "Wireless sensor network clustering for UAV-based data gathering". In: *Wireless Days, 2017*. IEEE. 2017, pp. 245–247.

[131] I. Guvenc et al. "Wireless communications, networking, and positioning with unmanned aerial vehicles [Guest Editorial]". In: *IEEE Communications Magazine* 54.5 (May 2016), pp. 24–25. ISSN: 0163-6804. DOI: 10.1109/MCOM.2016.7470931.

[132] *Technology Readiness Level NASA*. https://www.nasa.gov/directorates/heo/scan/engineering/technology/txt_accordion1.html. Accessed: 2018-01-30.