UNIVERSITY OF SOUTHAMPTON

FACULTY OF PHYSICAL AND APPLIED SCIENCES

Electronics and Computer Science

Supervisor: Dr Geoff V. Merrett and Dr Nick R. Harris

Practical Framework for Opportunistic Direct Interconnection between Wireless Sensor Networks with native communication protocols

by

Krongboon Singhanat

Thesis for the degree of Doctor of Philosophy

January 2018

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF PHYSICAL AND APPLIED SCIENCES
Electronics and Computer Science

Doctor of Philosophy

PRACTICAL FRAMEWORK FOR OPPORTUNISTIC DIRECT INTERCONNECTION BETWEEN WIRELESS SENSOR NETWORKS WITH NATIVE COMMUNICATION PROTOCOLS

by Krongboon Singhanat

Wireless Sensor Networks (WSNs) are a key element in IoT as the interface with the physical world. To help integrating WSNs with IoT, this research suggests that co-located WSN domains should be able to engage in collaboration schemes with direct interconnections opportunistically. However, many factors can influence the preferences of communication protocols in each network domain. Therefore, This work studies the practical solution for enabling Opportunistic Direct Interconnections (ODI) between co-located WSNs with different communication protocols by implementing the concept in real hardware. OI-MAC is used as the starting point of the study since the literature is the only the previous work proposing the solution in this direction, according to the best of author knowledge. We propose that WSNs should discovery neighbouring domains and communicate across their boundaries by using a shared MAC protocol. The nodes, which discover a co-located network domain, act as a gateway to communicate with the discovered neighbour.

The practical implementation confirms the feasibility of ODI in the real hardware. This work reformulates the ODI framework in literature. The lessons learned reveal the details of handshake process and reduces the modifications in NET layer.

The investigation leads to the newly proposed shared MAC protocol, which reduces the impacts of ODI on the implemented network. The evaluation shows the reduction of radio occupancy and the improvement of latency and reliability.

This work suggests modelling application data as resources and demonstrates that the connection provided by ODI can support the application exchange in forms of resource discovery and resource access with RESTful services.

Contents

List of Figures

List of Tables

Declaration of Authorship

I, Krongboon Singhanat , declare that the thesis entitled *Practical Framework for Opportunistic Direct Interconnection between Wireless Sensor Networks with native communication protocols* and the work presented in the thesis are both my own, and have been generated by me as the result of my own original research. I confirm that:

- this work was done wholly or mainly while in candidature for a research degree at this University;
- 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;
- parts of this work have been published as: [29, 30]

Signed:.....

Date:.....

Acknowledgements

I would like to express my sincere gratitude to my supervisors Dr Geoff Merrett and Dr Nick Harris for their attention, for the opportunity to carry this research and for their valuable time. I also appreciate help from everyone around me, the staff, fellow researchers, and especially Teng Jiang who provided me with the background of my research. I am grateful for the supports provided by the School of Electronics and Computer Science (ECS). The experiences, I received during my PhD time in Southampton, will be passed on as precious memories to the people, I hold dear and those who need advice on higher education.

I acknowledge the support of Royal Thai Air Force for the sponsorship, which allows me to pursue my personal dream and my PhD research. I feel deeply indebted to my family, especially to my beloved grandmother for the precious time that we must spend far apart. Special thanks to my parents, who are always proud of me either on my success or failures. Many thanks to Kantida Panchareon, my girlfriend, for the deep emotional support, colorful events, and happiness during my stay in the UK. My thesis is dedicated to everyone who involves and supports my works in every aspect. I also wish to share my success later in life to everyone, who contributes to my works during this time.

Abbreviation

ACK	Acknowledgement
ADC	Analog-to-Digital Converter
AODV	Ad-hoc On-demand Distance Vector
ARQ	Automatic Repeat reQuest
APP	Application Layer
BEB	Binary Exponential Backoff
BN	Boundary Node
BW	Back-off Window
CA	Collision Avoidance
CB	Cross Boundary
CBT	Cross Boundary Transmission
CCA	Clear Channel Assessment
CCH	Common Channel
CD	Collision Detection
CDF	Cumulative distribution Function
CoAP	Constrained Application Protocol
CoRE	Constrained RESTful Environments
CRC	Cyclic Redundancy Check
CSMA	Carrier Sense Multiple Access
CSP	Common Sleep Period
CTP	Collection Tree Protocol
CTS	Clear-To-Send Packet
DCF	Distributed Coordination Function
DCH	Data Channel
DST	Destination
DTLS	Datagram Transport Layer Security
EHM	Energy Harvesting Module
FFD	Full Function Device
FCF	Frame Control Field
FCS	Frame Control Sequence
FHSS	Frequency Hopping Spread Spectrum
FIFO	Fisrt-In, First-Out

FTP	File Transfer Protocol
HET	Heterogeneous
HM	Homogeneous
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IRI	Internationalised Resource Identifier
ISM	Industrial, Scientific, and Medical Bands
LAN	Local Area Network
LR-WPAN	Low Rate Wireless Personal Area Network
LPM	Low Power Mode
LPL	Low Power Listening
LPP	Low Power Polling
LQ	Link Quality
M2M	Machine-To-Machine
MAC	Medium Access Control
MCU	Microcontroller Unit
MEMS	Microelectromechanical System
MFR	MAC Footer
MN	Management Node
MQTT	Message Queue Telemetry Transport
MTU	Maximum Transmission Units
NAV	Network Allocation Vector
NET	Network Layer
NDS	Neighbouring Discovery Scheme
ODI	Opportunistic Direct Interconnection
O-QPSK	Offset-Quadrature Phase Shift Keying
OSI-Model	Open System Interconnection Model
P2P	Point-To-Point
PAN	Personal Area Network
PCF	Point Coordination Function
PHY	Physical Layer
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RAM	Random Access Memory
RDF	Resource Description Framework
REQ	Request
REP	Reply
RES	Response
RF	Radio Frequency

RFD	Reduced Function Device
RN	Router Node
RPL	Routing Protocol for Low Power and Lossy Network
RSSI	Received Signal Strength Indicator
RTS	Request-To-Send Packet
Rx	Receiver; Reception
SOA	Service Oriented Architecture
SFD	Start of Frame Delimiter
SN	Sink Node
SRC	Source
SQN	Sequence Number
SYNC	Synchronous
TD	Discovery Period
TCBT	Cross Boundary Transmission Period
TCP	Transmission Control Protocol
TSCH	Time Slotted Channel Hopping
Tx	Transmitter; Transmission
UART	Universal Asynchronous Receiver/Transmitter
UDP	User Datagram Protocol
UWSN	Underground Wireless Sensor Network
VSN	Virtual Sensor Network
WSDL	Web Services Description Languages
WPAN	Wireless Personal Area Network
WQM	Water Quality Monitoring
WSN	Wireless Sensor Network
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

Chapter 1

Introduction

Advances in digital circuitry, wireless communication, and microelectromechanical systems (MEMS) gradually improve efficiencies and performances of hardware, while the form factor and energy consumption have been reduced [31–33]. Integrated sensor systems with the capabilities to sense their surroundings, intelligently detect relevant data, and wirelessly communicate with each other in ad-hoc topology become conceivable [34]. The research interests in this area grow continuously due to the benefits that the technology could bring. In early stage of wireless sensor networks (WSNs) research, the Smart Dust project [35], one of the first attempts to outline the ideal prospects of this technology, promised a device called mote. A mote has abilities to sense its environments and communicate in ad-hoc network topologies. However, at the same time, it is expected to be autonomous, extremely power-efficient, tiny in form factor, and low-cost. At present, many academic achievements are results of the efforts to implement this grand vision of WSNs. However, the technology still has a long way to reach its maturity [36]. As theoretical research is still ongoing, numerous prototypes of potential applications have been successfully deployed and evaluated. WSNs have already been tested in various application domains [37], for example, healthcare [38], surveillance and security [39], environmental monitoring [40], habitat monitoring [41], disaster warning [42, 43], and precision agriculture [10]. As a result, the system design of WSNs becomes application-centric, i.e., the chosen communication protocols depend on the specific requirements of the targeted application [36, 44].

If the usage of WSNs becomes even more widespread, separate WSN domains will be more likely deployed in same areas. For the sake of leveraging the benefits of deployed systems, the interoperation between separate WSNs do-mains should be considered [1, 45–47]. The cooperation between separate systems emerges along with the abundant availability of connected communication systems [48]. The concept of Internet of Things (IoT) [49] describes interactive and cooperative environments building on top of the collaboration between various interactive systems, which can potentially revolutionise conventional approaches with a novel paradigm shifts For example, in health application,

the cooperation between a Wireless Body Sensor Network (WBSN) and a smart home system can offer an integrated healthcare service [44,48]. The smart home system can use the biometric data provided by WBSN to adjust the ambient temperature and airflow. In the absence of the data collection point, WBSN can use an internet access provided by the smart home system to inform the health status of the patient to health care centre as well as to call emergency services if necessary.

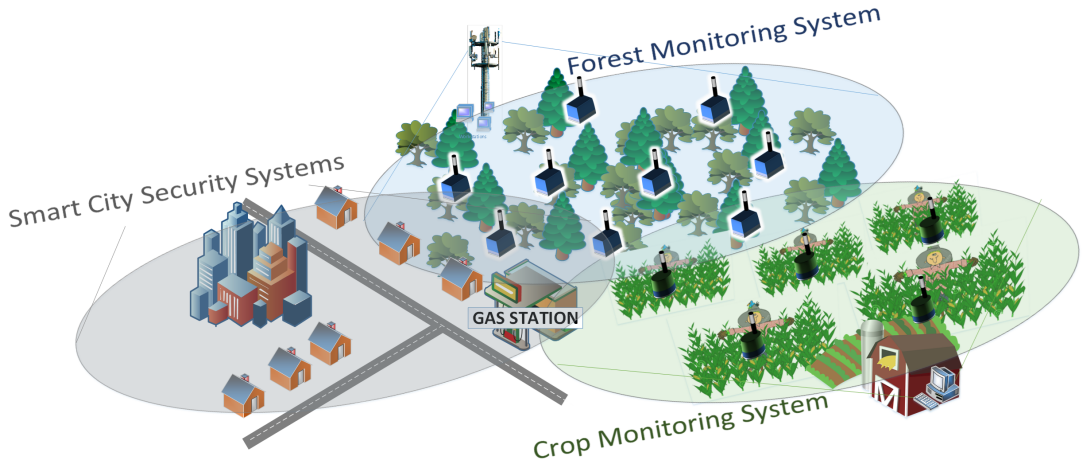


Figure 1.1: Cooperation between forest monitoring system and smart city security systems and nearby WSNs to detect fire disaster.

Another example can be given by the cooperation between fire alarm systems [7]. In Figure 1.1, the forest monitoring system and smart city security system and crop monitoring systems can collaborate sharing data and resource to help achieve the common goal such as fire detection. Sharing data empowers the application level to combine data for the optimisation of the prediction scheme. Fire alarm messages can be allowed to forward across domains to inform the nearby location. The future of IoT is involved technological advances in many research fields. Undoubtedly, WSNs will play a prominent role in manifesting human interactions with the intellectual environments [8, 50].

As WSNs are deployed for specific purposes, there is a high heterogeneity between proprietary solutions. At present, an internet connection is a conventional approach to overcome differences between standards [9]. In the big picture of the IoT development, the proprietary standards should find a way to connect with the global interconnection (Internet) at some point [49]. By adopting universal data and frame format from successfully integrated standards on the internet, the cooperation between separate systems, such as data integration and composite services, could happen in forms of web services [51]. Therefore, many research works in this area assumes the adoption of IP-Based Protocols in WSNs [8, 9]. However, the direct interconnection between local systems still needs to be considered as a fundamental element for cooperation between WSNs [52]. A direct interconnection offers many advantages [11, 45, 53]. The direct interconnection can be established independently from any infrastructure, as WSNs are often deployed in hazardous environments or inaccessible areas, which could limit such

arrangement [11, 12]. Additionally, the direct interconnection can offer the connectivity in cases of opportunistic encounters of associated networks since an encounter could happen without pre-planning. As a result, the Opportunistic Direct Interconnection can give more flexibility in the design process. In a sophisticated system, a completely planned deployment, which foresees all future possibilities of co-located WSNs, cannot be achieved due to many reasons. A case-study of the collaborative water quality monitoring (WQM) in catchment-scale [10] is illustrated in Figure 1.2 to demonstrate the situation,

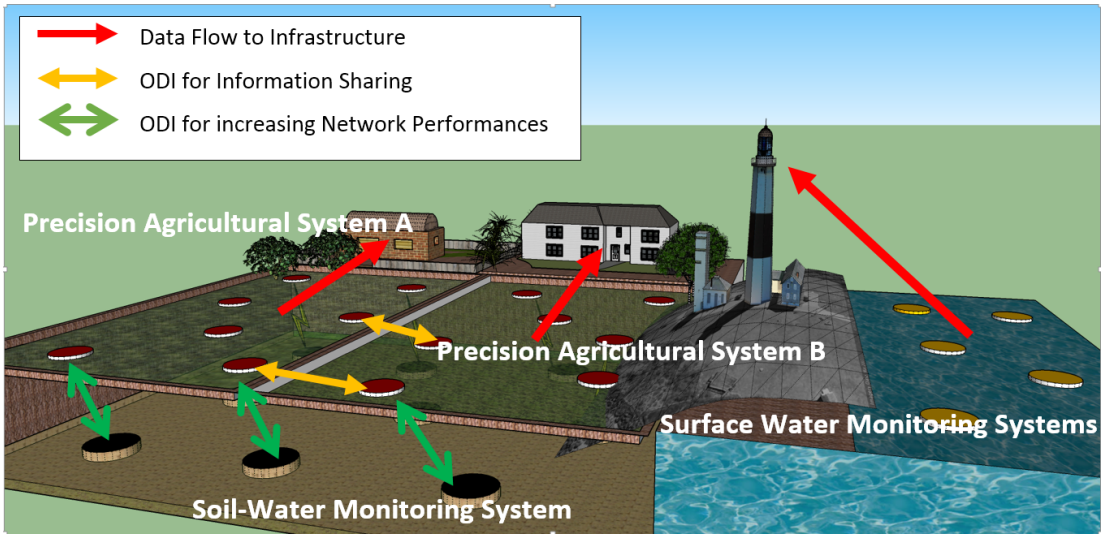


Figure 1.2: Collaborative catchment-scale monitoring of precision agricultural and water quality control systems

Across the water catchment, many co-located monitoring systems are employed. Each of them belongs to different stakeholders, installed for various purposes. The surface water monitoring system may be firstly deployed by the government to observe water qualities. However, precision agricultural systems, owned by farmers to manage fertilisation and irrigation in their field, could take place later. Each stakeholder concerns only with his benefits. However, if they were to build collaboration among all stakeholders, each separate domain could benefit from sharing resources and information, for example, the overview of water qualities and water flows in the catchment scale can be constructed. Lost sections of separate networks can be recovered. By revising load distribution among separate domains network lifetime could be increased. As accesses to shared data or resources from separate domains require the consent of their respective owner, the WSN communication design should be aware of such opportunities and concerns about opportunistic interoperability of separate systems.

According to the vision of Smart Dust [35], WSN hardware should tend to cost efficiency, the quality of the hardware must be compromised [42, 54]. Consequently, accuracy and reliability of the communication and measurement must be sacrificed. As compensation for these low qualities, sensor nodes must be deployed with high spatial density so

that local neighbours can collaborate in sensing and communication tasks [35, 42, 54]. As distributed networks in multi-hop topologies have a scale limitation, depending on the intensity of data traffic [40, 41]. Covering vast geographical space with heterogeneous applications, network deployment would have to split into multiple domains (or at least required more access points). With the presence of neighbouring networks, any non-cooperative strategies (w/o direct interconnections) of each network domain will result in sub-optimal network performances [1, 45, 55, 56]. The cooperation of co-located WSNs will not only be constructive at the information-sharing level [11] but may also be favourable in terms of network qualities, considering the energy constraint [57], loads balancing [1], latency, and reliability [12, 55]. The situation in Figure 1.3 demonstrates the suitable conditions for the opportunistic resource-sharing between multiple-domain WSNs.

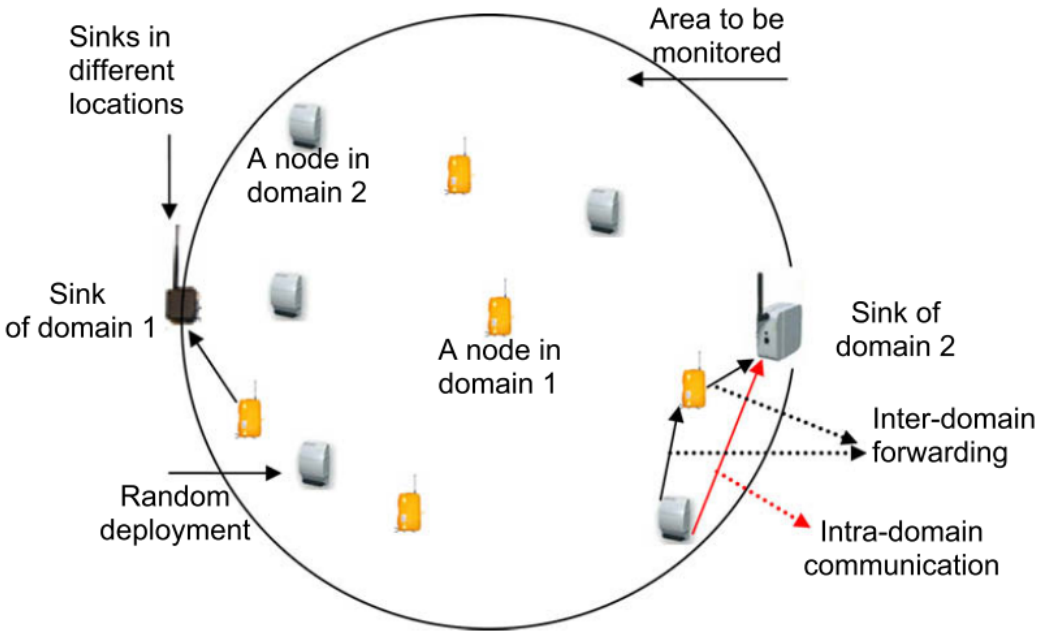


Figure 1.3: Network A and B locate in the same space. Both entities can directly communicate with each other. Due to the symmetry of sink location, the traffic balance is achieved with cooperation (reproduced from [1])

ODI can offer an appropriate solution in specific areas. An example can be seen in Figure 1.2. One of the significant challenges in the development of underground wireless sensor networks (UWSN) is the communication with the base station on the surface. Dynamic soil properties result in the complex path-loss model of UWSNs. Due to this, sophisticated adaptive algorithms must be developed to maintain the connection under/above ground surface [58, 59]. Additionally, direct link to the base station in far distance above ground may lead to inefficient utilisation of energy resource [59]. Alternatively, UWSNs can exploit ODI to inject packets into the neighbouring networks above the ground surface to build the connection with the infrastructure.

Although direct interconnections between WSNs in separate domains can offer two-fold benefits by sharing data and network resources, many obstacles must still be overcome [11, 45]. At present, the development of WSN is still in the transient state. New theoretical proposes still appear continuously, resulting in many proprietary standards [44]. The widely-adopted solution still needs more time to converge. However, the direct cooperation of multiple-domain WSNs can still be investigated with a prudent consideration of the heterogeneity of recommended protocols that exist today.

1.1 Research Justification

The idea of direct interconnection between WSNs is already well aware in the related research communities. A few related terminologies can be specified as cognitive networks [53,60], symbiotic networks [45,61,62], and cooperation in multi-domain WSNs [1,46,47, 55,63]. However, the majority of works assume the connectivity between separate WSNs by adopting IP-based solutions on top of IEEE 802.15.4, which requires every WSN to adopt the same standard. Concerning about the application-centric design of WSNs, an alternative concept, which allows individual WSN to choose its communication protocols, should be considered. Such concept can offer more freedom in network design, which can adapt to the specific purposes of each system. However, Only a few preliminary works in this area focus on the connectivity in the wireless communication level. Furthermore, the proposals in the preliminary works are incomplete and inconclusive. Some parts of the concept are validated by the simulations [11,12]. The empirical experiments are still entirely left out. Therefore, a practical implementation of the concept will clarify the vision, validate the feasibility as well as discovering the missing details of the theoretical works. The practical implementation may also lead to significant improvements and future directions in the same direction. Eventually, the practical implementation will emphasise the values of the concept and provide a template for future research in this area. In this section, the brief review on ODI related research will be provided to give the overview of current progressions and opportunities for future studies.

Many research report benefits of ODI and propose cooperation strategies in the application level. Under the assumption that the wireless connectivity between separate WSN domains is successfully established, and the characteristics of the communication link are known, various applications can be developed on top of the communication link to share data or network resources [11, 12, 57]. Energy trading can be achieved by load redistribution [46, 55–57]. Generally, ODI can offer more spatial balances energy consumption by multi-route connections, resulting in improvement of network lifetime and reliability [1, 55]. Behavioural strategies of each network in established collaborations are already studied [47, 64]. Even without any forced policy on co-located network domains, cooperation between multi-domains can naturally emerge in stationary topologies [63]. Machine-learning applications can be adopted to control

the management policy in cooperation schemes [53]. The cooperation can happen in forms of exchange or composition of services. Service composition schemes have already been studied and proposed [62]. However, all theoretical proposes can be achieved only when the interconnection in lower layers is provided, and the characteristics of the link are well-defined.

There is the trend towards convergence of WSN technology, but the development is still in progress. Even though the elaboration of the same standard becomes visible by promoting the compatibility to IP [9], the differences between individual WSNs may remain after convergence, considering the diversity of WSN application [2]. In the perspective of the wireless communication, the connectivity of separate entities begins with the capability to receive and transmit physical bits. At present, almost every WSN of RF-based WSNs operates on the Industrial Scientific Medical Bands (ISM-Bands). Also, the physical layer of the standard IEEE 802.15.4 is widely accepted in the commercial and research communities [65]. If the tendency towards cooperation between WSN domains gradually develops according to the vision of IoT, the likelihood of compatibility between physical layer (PHY) interfaces will steadily increase.

Lack of practical research on how to overcome differences between communication protocols. Assuming that the PHY connection is out of concerns as its compatibility is forced to gradually developing, most of the current deployed WSNs still employ different communication protocols on top of the PHY layer [3, 4, 6, 66]. Therefore, research on bridging different protocols are the next important step to implement ODI in the real practices. One of the early works in this direction is OI-MAC [11, 12]. Early OI-MAC [11, 29] considers the communication between separate network entities in the MAC protocol. However, the idea enforces the same communication protocol on the network participants. Later, the concept of the heterogeneous OI-MAC (HET-OI-MAC) extends the previous proposal allowing the participants to choose their internal protocol [12]. However, the work remains almost the theoretical contribution, which is only partially validated by simulation. The proposed concept requires multiple MAC protocol to be installed on the platform. The idea of multiple MAC is already considered in the previous works [67, 68] but not intended for this context. Installing multiple protocols may lead to inefficiency on utilisation of memory/computational resources. This aspect must be further investigated by practical implementation.

In conclusion, the vision of direct interconnection is already explored and supported by many research [1, 45, 53, 55, 56, 63, 69–74]. The main constituents of ODI are already developed, but the individual achievements still need further efforts to unite in one direction. Preliminary works often assume wireless connectivity between separate domains by relying on the fact that the development towards IoT will lower differences between domains without consideration on a broad range of applications in WSNs. A solid statement of how ODI supports the mainstream development towards IoT and how to achieve

ODI must be discussed and clarified. This research aims to progress ODI from a theoretical concept to a demonstration by a real hardware implementation. As the first step to realise ODI in a practical application, this research will investigate the existing solutions of the interconnection in communication layers with empirical validation. The actual hardware implementation will lead to well-defined limitations and characteristics of ODI regarding link quality, which can be the basis for new improvements and adjustments. The details of these research objectives are discussed in the next section.

1.2 Research Objectives

The concrete aims of this research can be listed as follows:

Objective 1: Investigate whether the principles of ODI can be practically realised in constrained hardware and real networks. This research aims to achieve the practical solution of the ODI concept by actual implementation from ground-up. The process should reveal the missing details and critical problems of the theoretical proposal. After the system is implemented, further characteristics can be studied, leading to improvements and eventually to the conclusive practical framework.

Objective 2: Investigate and evaluate the performance of protocols used in the ODI framework, identify their short-comings when implemented practically, and overcome these challenges. The ODI concept proposes using a common lightweight embedded MAC protocol to communicate between network entities. Even though OI-MAC proposes the original design in this concept; it is still not proved by a practical implementation. This work aims to implement the performances of the ODI framework by considering an appropriate MAC algorithms based on the realistic assumptions of the data traffic at the network boundary.

Objective 3: Investigate the concept used in the application layer of the ODI framework and demonstrate a example case in real hardware This research aims to design an application protocol for the ODI framework by implementing a functional system in real hardware. After the conceptual design, the workflow of the complete ODI framework will be presented in forms of a case study.

1.3 Research Contributions

The research that has been undertaken to address the objectives in the previous section have led to the following novel contributions:

Contribution 1: This research has practically validated the feasibility of the ODI concept. This work is the first work demonstrating cross-connection between WSNs with different native communication protocols in testbeds. The implementation overcomes issues that are not considered by the simulation and reveals the missing details and shortcomings of the existing theoretical framework. Additionally, the validation confirms the minimal impacts of ODI regarding computational resources (memories), energy consumption. The results of the validation are contributed to the peer reviewed publications [29, 30].

Contribution 2: This research has designed and practically evaluated a new cross-boundary MAC protocol used in the ODI framework. This research systematically analyses the data traffic at the network boundary in the typical operation of ODI. Based on the analysis, this work proposes appropriate MAC algorithms, resulting in the improvement of the critical drawbacks of the previous solution existing in the literature (OI-MAC). This leads to the improved performances regarding radio occupancy and energy consumption.

Contribution 3: This research has formulated the concept of application layer protocol for the ODI framework and demonstrates the complete workflow by a case study on a testbed. The application protocol suggested by this work uses the Constrained Application Protocol (CoAP: RFC7252) as the template to build the application protocol for the ODI framework. The implementing process modifies some concepts in the standard based on the foreseeable constraints from the practical implementation. This implementation is performed on a resource constraints hardware (RAM at 1kB and MCU at 8 MHz) to demonstrate the workflow of the whole process of the proposed solution.

1.4 Research Publication

Early results from the contributions reported in the previous section led to the peer-reviewed publication:

- K. Singhanat, T. Jiang, G. V Merrett, N. R. Harris (2015). Empirical Evaluation of OI-MAC: Direct Interconnection between Wireless Sensor Networks for Collaborative Monitoring. In *2015 IEEE SAS Sensors Applications Symposium (SAS 2015)*, apr 2015, pp1-5.
- K. Singhanat, N. Harris, and G. V. Merrett, Experimental validation of opportunistic direct interconnection between different wireless sensor networks," *in 2016 IEEE Sensors Applications Symposium (SAS) (SAS 2016)*, Catania, Italy, apr 2016.

1.5 Report Structure

This thesis is structured as follows:

- Chapter 2 contains the review of the related literature. This review analyses the related circumstances in the WSN development to pinpoint the motivation, potential contributions and boundaries of the ODI concept, defined by this work. The previous suggestions in the literature are summarised and discussed as the initial point of the implementation.
- Chapter 3 contains the implementation process of the ODI framework in real hardware and the results of the implementation. The missing details, which are not provided by the literature, are pinpointed as well as the possible solutions to the unsolved issues. The operational processes of the framework are captured from the real hardware, compared with the theoretical expectation. The energy expense of the ODI functionality will be analysed.
- Chapter 4 discusses the cross-boundary protocol used between the co-located domain. The prerequisites of such protocol are summarised. The critical problems of the previous suggestion in the literature are discussed. An alternative solution is proposed. The performances of both protocols are evaluated regarding the energy consumption, latency and reliability.
- Chapter 5 elaborates the concepts of the application protocol that can be used on top of the ODI link. The CoAP standard is used as the template to realise the application layer of the ODI framework. This work briefly reviews the data model and the serialisation method to show the potential of using the same concept on top of the ODI link. The proposed concept is evaluated in the testbed. A modelled case study is performed and measured to demonstrate the functionality of the framework.
- Chapter 6 concludes the contents of this thesis and suggests the possibilities of the research in the same direction.

Chapter 2

Literature Review of Opportunistic Direct interconnection

This chapter summarises the existing solutions to integrate WSNs into IoT for pinpointing the role of the Opportunistic Direct Interconnection (ODI) concept in the IoT development. The contents will cover the existing details in the literature regarding enabling ODI. The review begins with the viewpoint of this thesis towards the current situation in the WSN technology. Section 2.1.1 elaborates the early shared vision of WSNs to understand the motives behinds numerous theoretical contributions in WSNs. Section 2.1.2 shows the diversity of the WSN technology in the network design to open the discussion on how the technology will develop and converge. In this research perspective, we think that the likelihood of adopting different communication protocol in each local WSN despite the need for the interoperability provided by direct communication is undeniable. The characteristics of current WSN platforms are considered in Section 2.1.3. This review shows the perspective of the hardware regarding the convergence of the technology. Section 2.2 examines the communication protocols in WSNs that are relevant to understand the motives of this work as well as providing the reference in the technical aspect of further contents. Section 2.3 discusses the cooperation between separate WSNs by presenting the overview of the standardisation using the Internet as the centre to provide the interoperability between heterogeneous systems. The discussion then finds the missing pieces of the development, which reveals the potential contribution of the ODI concept in the big picture. Section 2.4 summarises the existing literature that provides the technical details of the ODI concept. The current progress of the research in this direction will be concluded to provide the starting point for the practical implementation.

Theoretical proposes of communication protocols are constantly released, pursuing the vision of WSNs that describes WSNs as distributed, data-centric, autonomous, and highly energy-efficient wireless networks. Additionally, later implementations in diverse application domains broaden the system design of WSNs. Therefore, even the trend towards the convergence of well-known standards gradually grows significant; the assumption that local systems adopt newly released communication protocols for specific proposes cannot be disregarded. The differences between implemented communication protocols could still exist in the future due to a broad range of system specification in WSNs. In the overview of technology development, there is a global tendency towards cooperation of individual systems to leverage benefits by providing sophisticated services on top of separate elementary services.

The Internet provides the global connection and acts as a mediator between systems from different standards. Therefore, in response to the worldwide trend towards the Internet of Thing (IoT), many research works in the related areas of the cooperation between WSNs continue under the assumption that Internet-related solutions will be adopted in WSNs. Whereas the cooperation in global scales, relying on the connection through the Internet or IP-Based solutions, has been intensively explored, the interconnection in local scales has been left out. Although local collective systems should link to the global connection at some depth level in the network hierarchy, co-located systems can locally connect and opportunistically build a collaborative scheme, which is profitable for each participant. To support opportunistic cooperation between co-located WSNs, the system design should consider distributed wireless connections between platforms of separate network domains.

2.1 Heterogeneity of Wireless Sensor Networks

WSNs have been tested in many fields of potential applications, which have their specific requirements. As a result, the platform design and chosen protocols are present in broad range variety. Thus, the definition of WSN becomes ambiguous. Many of academic achievements are inspired by the early vision of WSNs, which are given at the beginning stage of WSN development [36]. Later exploration and practical implementations of potential applications bring a great diversity of viewpoints on network requirements, system platforms, and protocols in use. This section aims to provide the comprehensive review on the development of the technologies from the theoretical ambitions and the perspectives of the real practices which will show the viewpoint of this work towards the current state of the WSN development.

2.1.1 Vision of Wireless Sensor Networks

The grand vision of WSNs descends from the initial wave of theoretical proposes [36]. WSNs are characterised by a large-scale network of tiny sensors, with moderate costs and qualities. Each platform can sense, do computational tasks, and communicate wirelessly with each other. The system in vision promises intelligently unobtrusive environmental sensing. The described target outlines general requirements, which separate the design framework of WSNs from one of the traditional ad-hoc network [75]. The hardware design of WSN platform is expected to consider low-cost production, the efficiency regarding energy consumption, and the size/outlook, which possesses a low physical footprint [34]. The mentioned viewpoint is philosophical behind later developments of theoretical works in this area. Thus, following sections will summarise the common characteristics of WSNs and their correlations with each other:

- **Data-centric Communication Paradigm**

  While most connections in conventional networks are peer-to-peer, the link architecture of WSNs is asymmetric and data-centric in a tree topology, characterised by tracking and monitoring tasks of WSNs [33, 71, 76]. A large number of nodes is densely installed to overcome the drawbacks of low-quality platforms by the exploitation of spatial collaboration. Consequently, addressing individual nodes in a huge network will be impractical (i.e. may suffer an unacceptable overhead [34]. Therefore, WSN network protocols should focus on retrieving data from spatial-related or event-related sets of nodes, rather than addressing an individual platform [58].

- **Dense Deployment and Trade-off between Cost and Qualities**

  Production cost is an essential requirement, considering the total costs of networks, composed a large number of nodes [34, 42]. The low-cost manufacturing is vital for the feasibility of platform mass production. Mass production leads to the strategic solution, which involves using quantity to compensate for qualities [34, 35] In WSN context, large number deployment permits various advantages:

  1. Using the spatial collaboration of neighbouring nodes to improve the qualities of the communication and measurement of the system [34, 58, 77].
  2. Low-cost manufacturing results in disposable devices, which can be spontaneously deployment in harsh environments or inaccessible areas without maintenance [34, 78].
  3. Generous deployment increases the flexibility and robustness of the network due to redundant nodes [54, 77].

- **Fault Tolerance, Autonomy and Adaptive Network**

Since WSNs use low-cost platforms and operate in harsh environments, malfunctions are originated by both environmental interferences and hardware errors [31, 34]. Also, the system might be randomly deployed in an ad-hoc manner [33]. Thus, WSNs should possess capabilities to autonomously adapt to condition changes [44, 54, 79]. Following terminologies are described adaptive functions of WSNs [80]:

- **self-healing** for the autonomous response to node-failures [44, 75].
- **self-organising (self-managing)** for the ability to manage an ad-hoc topology and adjust with changing in topologies [81]
- **self-optimisation** for adjusting the system characteristics, in responses to dynamic changes of ambient interferences [81, 82].
- **self-protection** that stands for the ability to repel harmful attacks from outside [77]

- **Energy Consumption**

  The power consumption is the primary concern of self-supporting systems. The low-power operation can be seen as a trademark of WSNs that inspired many theoretical proposes. Out of the typical activities of WSNs; sensing, processing, and communicating, the primary energy consumption is dominated by the communication tasks [6, 32, 34]. As a result, many research attempts to address the energy constraint by introducing energy-efficient communication protocols. An example of the power consumption of a WSN platform can be seen in Section A.1. Since the parametric data is assumed in physical phenomena monitoring, the throughput and latency are sacrificed for more energy conservation by introducing the concept of the duty cycle.

Aforementioned key points are assumed and targeted by most of the theoretical works. Clustering and data aggregation protocols and multihop packet forwarding are developed under the assumption of asymmetrical link architecture and dense and large deployments in WSNs. Machine-learning techniques, collaborative or cooperative packet forwarding, and multipath routing are proposed to improve autonomy and fault tolerance. Novel low-power communication protocols focus on minimising energy consumption in distributed and scalable networks. However, as the matter of facts, practical implementations are diverging from these visions, resulting from limitations of current hardware technologies and practical purposes [36]. In the next section, WSN specifications in various application domains will be discussed to analyse the impacts on the system design from practical proposes and give the basic overview of the diversity in WSNs.

2.1.2 Diversity of Wireless Sensor Networks in Practical Applications

In the last section, the key issues considered by theoretical research on communication protocols in WSNs has been given. In controversy from theoretical viewpoints, the practical system design is application-centric [36] (mission-oriented [2]). The relevant problem statements can be different from the conventional theoretical viewpoint of WSNs, discussed in Section 2.1.1. The given tasks of the application determine the main factors of the network design, which can be listed as follows:

- **Data Traffic types** Data traffic type dramatically influences the desired link characteristics and qualities. Following data types are mentioned in the literature:
  - **Periodical monitoring (Sense-only).** This traffic type signifies the underlying cases of WSNs where the unidirectional communication is sufficed, for examples, in typical monitoring application [2, 83].
  - **High rate data.** Such traffic type occurs when the system delivers multimedia data type such as pictures and sounds or when the system engages in a real-time monitoring (Wireless Multimedia Sensor Networks) [2, 33, 44]. This type of WSN is counterintuitive of the early vision mentioned in Section 2.1.1, emphasising the difference between the theoretical vision and the practical implementation.
  - **Query-based.** This traffic type is common in the traditional network depicting the situation of requests and responses [2, 58]
  - **Event-based.** This traffic type will be ignited when certain conditions have been met. The node may need to inform the base station or the relevant endpoints which can react to the situations [2, 83]

  The data traffic type determines the requirement on the communication link. In primary cases, unidirectional communication is sufficed, for examples, in a typical monitoring application, but bi-directional communication could be required if the system needs to respond to some events or queries [2, 76, 83]. Packet forwarding scheme typically involves regularly relaying packets to a single collection point or a defined set of collection points [84], while application requests and responses introduce a sudden burst of data traffic in a peer-to-peer architecture. The communication protocols must, therefore, be suitable for mixed data traffics. In extreme cases, if interactions between nodes are required such as exchanging messages for autonomous collaborative responses, an efficient end-to-end routing protocol may need to be considered [9, 44]. In monitoring tasks, systems with high-rate sampling data could be more tolerant to packet delivery errors than systems with low-rate sampling data. In some applications such as disaster warning, timely responses could be critical. Therefore the travelling duration of the relevant packets must

stay within the acceptable limit [42]. Additional specific requirements such as confidentiality, which requests the network security.

- **Network Scale** Large-scale deployment may involve hundreds of nodes as can be seen in environmental monitoring domain [85, 86], but in other cases, networks in body health monitoring domain may consist of a few nodes. The network topology and link architecture are directly affected by the deployment scale. In a network with a few nodes with moderate capabilities, peer-to-peer links may be preferred more than many-to-one links in a tree topology.

- **Ambient Interferences** The path-loss model and fading effects are varied by the medium, obstacles, and dynamic changes in environments [34, 44, 76]. In some cases, the network may need to operate in special conditions such as under high radioactivity, temperature, pressure, or vibration which can also be used for harvesting energy.

- **Maintenance** If the network is deployed in inaccessible areas, system corrections can be problematical or even impossible [33], for example, the node is deployed in volcanic areas [44], inside human body [38], or in a mechanical part of the manufacturing process [44, 48]. Consequently, to maintain network health in cases of node failures or topology changes, self-adaptive algorithms might be necessary [47, 80, 87] in the compromise with limitations on computational resources. The energy capacity should be able to sustain for the expected network lifetime. The network protocol should be scalable [2, 42, 88] and permit new participants to establish connections without interrupting the network functionality.

- **Operation Time** Operation time intervals of practical implementations are ranged from several weeks to years [36]. Commonly, the network lifetime is limited by the energy capacity, but if ambient energy harvesting can outweigh the energy consumption. The network lifetime could be restricted by the hardware durability and the reliability of the network. Therefore, the priority of energy constraint differs from case to case. In some cases, increasing duty cycle can be used for regaining network qualities [88]. The requirements of the target application must be interpreted into network characteristics, which can be used for designing or choosing the suitable platforms and communication protocols. The network characteristics can be listed as follows:

- **Topology** The network topology is closely related to the network scale and deployment [89]. If the network scale remains in the transmission range, a one-hop star topology can be formed instead of multi-hop topologies such as mesh topology or tree topology. Both sensing coverage and radio coverage change the density of deployment [89, 90]. The outdoor application could prefer a high transmission

range with only relaxed requirements on the form factor [85]. While indoor applications such as industrial process monitoring and body area networks require stringent requirements on form-factor but the transmission range is limited [38].

- **Link Architecture** In large-scale deployment, the link is asymmetric in a tree topology; the data flow more in the direction from sensors to collection points than the control or query messages from the central point [58, 84]. The obtained information from nodes in the same area is correlated. Therefore violations of link fairness in contentions and packet delivery errors are tolerable [31, 76, 86]. However, in cases of networks with few nodes with many activities, the link architecture could resemble the characteristics of traditional ad-hoc networks with regular data transfers in a star topology or mesh topology. If the user interactions from outside are partly provided inside the networks or network needs to support application data flow, i.e., not only sense and send data to collection points, the link architecture design must support both types of traffics.

- **Energy Consumption** Theoretical viewpoints of WSN communication protocol design regard energy constraint as critical, but moderate power consumption is unavoidable if a certain degree of system qualities is required [86, 87]. The energy consumption can be reduced by introducing the radio duty cycle, the ratio between the active/inactive state of the radio. Additionally, ignoring unsuccessful receptions and transmissions in the presence of data redundancy can further negotiate between energy and performances [33]. As the communication is interrupted, the latency of networks is dropped. Therefore the link qualities can be sacrificed for energy [88]. The computational resources can be used to improve the power consumption as well. By introducing sophisticated prediction algorithm or scheduled protocols, the radio module can sleep longer. Therefore the power consumption is decreased.

- **Link Qualities** The application may require the network to perform data delivery in such way that the application can correctly function. The data transfer rate depends on the data type and the sampling rate of the application. The channel capacity can be increased by using a wider bandwidth or higher frequency bands. In observation of the dynamic behaviour of rare events, data losses could be critical. Therefore, data integrity should be increased by exploiting data redundancies or employing sophisticated contention avoidance algorithms [54]. In some application, the latency of data is critical [42], the instability can occur in a feedback system if the duration of the travelling feedback signal is too long. Therefore, link qualities can be simplified by the following viewpoints: 1) Link Capacity (Data Throughput), 2) Link Reliability (Loss Tolerance), and 3) Latency. By using the mentioned viewpoints on link qualities as the criterions, WSN domains can be classified as illustrated in Figure 2.1

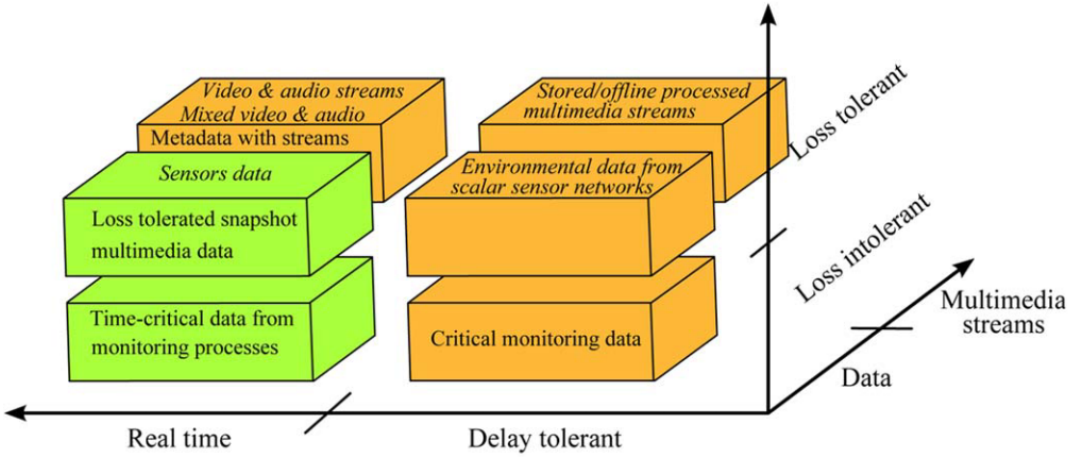


Figure 2.1: Classification of WSN application domains by required QoS (reproduced from [2]

Network characteristics of WSNs depend strongly from the implemented application domains, as this section fundamentally counts the crucial key factors on the network design. Regarding the results of this review, it is doubtful to assume only one universal framework of communication design in WSNs. Even if there seems to be a common practice, adopted by many WSNs developers, the development of communication protocols in WSNs is certainly not conclusive. At present, the potential applications of WSNs are already well defined; we can observe many examples from different application domains [91]. However, most of the practices are still the proof of concept, despite the promising forecasts of the exponential growth of IoT [92]. Many practical implementations still reflect the characteristics of ad-hoc networks rather than the smart dust characteristics (referred to characteristics described in Section 2.1.1). System deployments still need to be pre-planned and observed by the network technicians [36]. The decisive threshold for shifting towards the new approach provided by this technology may require more developments, which offer profound benefits. Currently, the practices concern only about its objectives solving the requirements by using existing wireless technologies. The common viewpoint is that the internet will eventually provide the interoperability between systems. However, if a substantial push is necessary to trigger the scale of the implementation, the interoperability may need to be considered more seriously from the communication viewpoint which could provide the direct cooperation between distributed systems.

2.1.3 Current Development of Platforms

The last section shows the differences in the network design of WSNs which most likely will not converge to a single unified framework. In this section, the platform of WSNs is discussed. This section aims to find the common characteristics of the available platform

to observe the convergence of the technology and also provide the reference for choosing the platform used for the experiments.

In general, a WSN platform consists of three subsystems [31, 34, 38, 58]:

1. *The sensing subsystem* contains various transceivers to translate the observed physical quantity into an electrical signal. An external Analog-to-Digital converter (ADC) could be required to provide a digital form of the measured value. Today, MEMS is widespread in sensor applications, resulting in the reduction of sensor costs.

2. *The computational subsystem* executes bits operations. The microcontroller unit (MCU) and act as the master in serial interfaces between peripheral modules. The microprocessor in WSN platform should be optimised regarding energy consumption, while possesses sufficient computational power. Typically, Reduced Instruction Set Computing (RISC) MCUs are used in WSNs [78]. MCUs commonly possess moderate memory (Flash-Memory, RAM) in the dimension of several kilobytes. However, in cases of data-intensive applications, several options with relatively more powerful MCUs are available. The programmable memory (flash) is ranged from hundreds of kilobytes to several MB.

3. *The communication subsystem* establishes connections to other platforms. Acoustic waves, infrared or typical radio frequency (RF) can provide the physical connection, depending on the context of the communication medium. Since this research focuses on the interoperability, we target the RF-technology for further discussions. The majority of RF-based WSN operates in Industrial Scientific and Medical Bands (ISM) since it is license free. The well-known vendors in this area conform to the PHY definition of IEEE 802.15.4 [26], which is well-accepted as the de facto standard along with several proprietary standards (see details in Section 2.2.2). To suppress energy consumption, the radio chips in WSN platforms commonly can sleep by turning off power-hungry components such as active amplifiers and frequency synthesisers [93, 94]. From sleep states, radios can turn on quickly to the active state for transmissions and receptions. The transmission modes can categorise current radio chips as follows:

   - *Bit-based radios.* This kind of radios offers continuous bit transmissions such as CC2420 [95] and CC1000 [96]. MCU is responsible for protocol transmission processes (such as CRC and Preambles) therefore MCU has manual control on all bit transmissions.
   - *Packet-based radios (packetized radios).* Radios such as CC2500 [14], CC1120 [97], and CC1101 [98] provide hardware optionally performing autonomous packet handling, i.e., conventional processes such as CRC, physical preambles, spread spectrum, channel encoding and encryption.

Except for essential components for core functions of WSNs, the energy harvesting module (EHM) can be integrated, in the power subsystem, in cases of exposure to sunlight or the present of exciting vibration. EHM is responsible for extracting energy from ambient environments to prolong network lifetime (In some cases, with a compromised form-factor, EHM can subsidise the total energy consumption of the platform [85]. In Table 2.1, the features of some well-known available platforms are given to form the primary overview of current platforms.

FEATURE	**MICAZ**	**MICA2-DOT**	**MICA2**	**IMOTE2**	**TELOSB**	**IRIS**	**CRICKET**
MCU	ATmega-128L	ATmega-128L	ATmega-128L	Xscale-PXA271	MSP430	ATmega-128L	ATmega-128L
VOLTAGE SUPPLY	2.7-3.3V	2.7-3.3V	2.7-3.3V	3.2-4.5V	2.7-3.3V	2.7-3.3V	2.7-3.3V
MEMORY	4k EEPROM	4k EEPROM	4k EEPROM	256k SRAM 32M SDRAM	10k RAM 16k EEPROM	4k EEPROM	4k EEPROM
BATTERY	2xAA	2xAA	3 x Coin Cell CR2354	3xAA	2xAA	2xAA	2xAA
AVAILABLE SENSORS	Light, Humidity, Barometric, pressure, accelerometer, GPS, acoustic, video, sounder, magnetometer	Light, Temperature, accelerometer	Light, Humidity, Barometric, pressure, accelerometer, GPS, acoustic, video, sounder, magnetometer	Light, Temperature, humidity, accelerometer	Light, Temperature, humidity	Light, Humidity, Barometric, pressure, accelerometer, GPS, acoustic, video, seismic, sounder, magnetometer	Light, Humidity, Barometric, pressure, accelerometer, GPS, acoustic, ultrasonic, video, sounder, magnetometer
RADIO CHIP	CC2420	CC1000	CC1000	CC2420	CC2420	Atmel RX230	CC1000
FREQUENCY BAND	2.4-2.483 GHz	868/915 MHz	868/915 MHz	2.4-2.483 GHz	2.4-2.483 GHz	2.4-2.480 GHz	868/915 MHz
DATA RATE/- POWER	250 kbps/ -24 -0 dBm	38.4 kbps/ -20 5 dBm	38.4 kbps/ -20 5 dBm	250 kbps/ -24 -0 dBm	250 kbps/ -24 -0 dBm	250 kbps/ 3 dBm	38.4 kbps/ -20 5 dBm
SENSITIVITY	-94	-98	-98	-94	-94	-101	-98

Table 2.1: Features of Well-known Commercial Platforms [23–25]

There are a variety of commercial platforms in WSNs. However, the similarities of the platform design can be tracked. RISC low-cost microprocessors are installed on many models. The same set of radio chips that conform to IEEE 802.15.4 is widespread. This fact encourages the assumption of the compatibility between radio chips in the future. Some new platform even considers the integration of two radio chips in the hardware design to cover 2.4GHz and sub-GHz bands for the sake of the compatibility (RE-MOTE of Zolertia [99]). This tendency may trigger more considerations of the direct cooperation between network domains.

2.1.4 Discussion

The vision of WSNs was proposed in the early stage of WSN research, resulting in a vast number of theoretical works. Each work pursues the same vision by their approach. However, in the viewpoint of the practitioners, the vision of WSNs remains unrealistic. The real practices of WSNs are diverged from the early vision, neglecting some constraints such as form factor, low-cost, low computational power or energy consumption in favour of achieving the application target. The existing technology can be wisely utilised to solve the application demand instead of relying on novel theoretical works. The variety of the application domain delays the maturity of the technology into off-shelf products, resulting in the unclear picture of the platform compatibility. Nonetheless, the interoperability between separate entities may be the crucial key to persuade a casual user to consider a new approach, if it can synthesise the functionality of individual networks into a holistic solution.

All these facts indicate that the WSN technology is still undergoing developments. However, some section of WSN technologies might already begin to saturate. Considering the hardware perspective, some group of available WSN platforms exhibit a same set of characteristics. They consist of middle class low-power MCUs and radio chips, compliant with IEEE 802.15.4. This fact indicates that in some area of the applications, similar platforms may coincidentally be compliant with each other. If the implementation of WSN radio interfaces has reached some same common ground, the first prerequisite of the interoperability between different network entities has been already begun to manifest. However, since WSN needs to adapt to the different application requirements, the optimisation of the communication protocols in use should be necessary. In the next section, the communication protocol in WSNs will be briefly reviewed as a reference for further discussions.

2.2 Diversity of Communication Protocols

As a reference for conceptual discussions on communication protocols, the OSI-Model (Open System Interconnection Model) will be used. OSI-Model is a conceptual model, dividing the communication process into sublayers. Originally, the model consists of seven abstract layers, but only five layers are frequently referred in the WSN context [33, 34, 100]. The Figure 2.2 Protocol Stacks of WSNs according to OSI-Model describes the conceptual definitions and functionality of each protocol stack, which is adopted in WSN context.

In general, the interfaces between distinct layers should be transparent so that every combination of separately-designed protocols on each protocol stack is compatible. However,

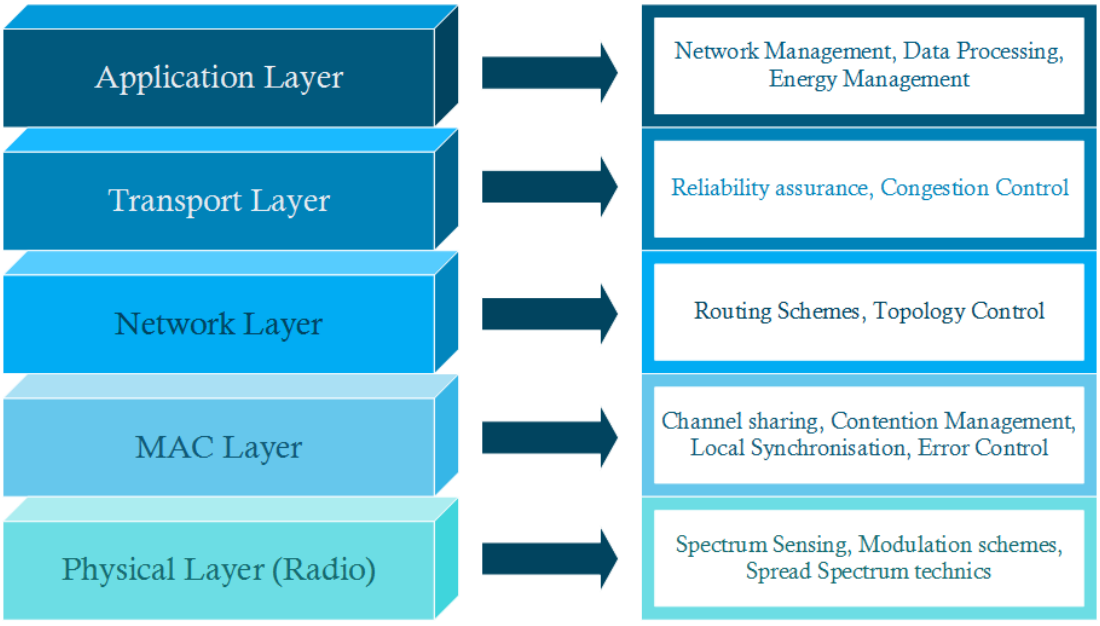


Figure 2.2: Protocol Stacks of WSNs according to OSI-Model

the boundaries between these abstract layers are fuzzy in the case of WSN communication design because of the increased profitability that could arise by exploiting the information from upper/lower layers. A couple of research works proposes a cross-layer design (distinctive binding sub-layers together) [92, 101, 102]. In this works, each layer is referred to the conventional definition of OSI-Model.

This section attempts to summarise the variation of the physical/link layer in WSNs. The review discusses the physical layer to describe the concerns of the interoperability between distinctive platforms. Then, the definition of IEEE 802.15.4 will be briefly mentioned as it is a widely used standard along with the counter-arguments and other proprietary standards. The frequently used algorithms in the MAC layer will be briefly discussed as a reference for the implementation in the next chapters.

2.2.1 Physical Layer

Many types of physical layer are considered in WSNs. Early projects proposed the optical communication as a potential candidate for the physical layer of WSNs [35]. The acoustic wave is also suitable for the medium with a lot of water contents [44, 58]. This work focuses only on the RF-based physical layer. Typically, the RF-Based physical layer is characterised by following aspects:

- **Frequency Bands** WSNs commonly operates in the widely used license-free bands assigned for Industrial, Scientific and Medical (ISM) (433/868/915/ MHz and 2.4 GHz [44]; the regulation differs in each specific region). Largely, the options of the operating frequencies are separated between 1) 2.4 GHz bands [14,95,99] and

2) Sub-GHz bands [96–99]. The first choice possesses more bandwidth, thereby offers more data rate, but covers less Tx range with the same Tx power than the latter option, i.e., the second choice offer more extensive communication range in the trade-off with lower data rate [33,103]. As the length of the antenna must correspond to the half wavelength of the chosen frequency, Sub-GHz bands result in the compromise of the form factor. Based on the characteristics of the wavelength, outdoor applications, e.g., environmental monitoring usually employs Sub-GHz bands because of its energy-efficient coverage [85, 103], while indoor applications choose 2.4 GHz because of the form factor and the higher data rate [33, 44].

- **Modulations** The trade-off between bandwidth and reliability can be achieved by manipulating the cardinality of bits per symbols, depending on the objectives of each system design [33]. Fewer bits per symbol ensures the accuracy of the symbol detection on the constellation diagrams (e.g., OOK BPSK), while more carried bits per symbol offers faster data transfer (e.g., ASK, O-QPSK) [27, 104].

- **Spread Spectrum Techniques** Spread spectrum techniques enhance the robustness of the physical link against narrow-band interferences by exploiting the extra bandwidth [33, 58]. In general, two primary methods to are widely-used to increase the signal bandwidth intentionally: 1) Frequency Hopping Spread Spectrum (FHSS) swaps the communication channel around the available narrow bands (logical channels) or 2) Direct Sequence Spread Spectrum (DSSS) multiplies a transmission signal with a predefined pseudo-random code [33, 51, 104].

The compatibility of the physical layer can only be achieved when all the mentioned aspects are identical. Fortunately, since IEEE 802.15.4 [26] came out in 2003, a considerable number of the released radio chip is manufactured conforming with the physical layer (PHY) of IEEE 802.15.4 standard. The definition covers 2.4GHz and sub-GHz bands. Table 2.2 gives the overview of PHY in IEEE 802.15.4 (2011) as follows

Frequency Band (MHz)	**Modulation**	**Data Rate(kbps)**
779-787	O-QPSK	100
868-868.6	BPSK	20
	ASK	250
	O-QPSK	250
902-928	BPSK	40
	ASK	250
	O-QPSK	250
950-956	GFSK	100
2400-2483.5	O-QSPK	250

Table 2.2: Overview of PHY in IEEE 802.15.4 [26, 27]

As can be seen from the table, the physical link design of IEEE 802.15.4 already offers the trade-off between the data rate and the coverage through the variation of frequency

and modulation. Nonetheless, proprietary standards are diverging from the definition of IEEE 802.15.4. Some of them still use the same physical layer, although the MAC layer definition is modified [9, 51, 76]. In the next section, the well-known link layer standard of WSNs will be discussed.

2.2.2 Related Standards

Commercial and industrial standards, well-known in WSN research are introduced, centring around IEEE 802.15.4. However, the completeness of IEEE 802.15.4 is still sceptical [105, 106].

2.2.2.1 IEEE 802.15.4 (Low Rate Wireless Personal Area Networks: LR-WPANs)

IEEE 802.15.4 [26] is widely recognised as a present solution of WSN application , with considerable arguments on improvements [105]. Principally, this specification modifies the conventional standard by adding a requirement on the energy consumption. The energy saving is improved by introducing the concept of radio duty cycle. The standard defines three operation modes in the MAC layer:

1. **Non-Beacon-Enabled Mode** Non-Beacon-Enabled Mode merely employs CSMA/CA without synchronisation, i.e., each node can content for access the communication channel whenever it has data to transmit [106].

2. **Beacon-Enabled Mode** Beacon-Enabled mode introduces two kinds of platforms: (1) Full Function Device (FFD) and (2) Reduced Function Device (RFD). FFD can act as PAN coordinator, which can initiate communication with every RFD and other FFDs, whereas RFD can communicate only with the assigned FFD. FFD sends a beacon periodically to maintain the duty cycle synchronisation. The beacon interval is divided into three parts: (1) Contention Access Period (CAP) (2) Contention Free Period (CFP) (3) Inactive Period. During CAP, RFPs use CSMA/CA to access the medium. CFP is used for guaranteed time slots, which can be allocated to prioritised traffic to achieve QoS [26, 51].

3. **Time Slotted Channel Hopping (TSCH)** New version of IEEE 802.15.4 (IEEE 802.15.4e [65]), which was released in 2012 [107] try to improve the performances of IEEE on multi-hop networks by using time synchronisation, known as Time Slotted Channel Hopping (TSCH) [9]. The communication pairs will choose the logical channel and time slot based on a pre-defined sequence.

2.2.2.2 Commercial and Industrial Standards

ZigBee [27, 44] is known as the business standard that directly corresponded to IEEE 802.15.4. Both of PHY and MAC directly follow IEEE 802.15.4. ZigBee employs AODV as routing protocol. The star/mesh/tree topology is supported. Many ZigBee compliant products are released in the commercial market

WirelessHart is developed on the PHY definition of IEEE 802.15.4, is widespread in the industrial automation domain [27, 44, 58], gaining attention in wireless control [107]. The concept of its MAC protocol is integrated by IEEE 802.15.4e in 2012 (TSCH) [65].

ISA 100.11a is also developed on top of IEEE 802.15.4 PHY [27, 44, 58]. The standard uses a time synchronisation techniques, interoperable with WirelessHart [44].

Other standards, which operates on 15.4 compliant radio chips are SimpliciTI and WiMi [27, 44]; Although there are other proprietary solutions, which are not developed on top of IEEE 802.15.4, they still operate on the same frequency bands, e.g., Z-wave, ANT, Wavenis, Dash7, EnOcean, and Insteon [8, 27, 44, 58].

2.2.2.3 Arguments on IEEE 802.15.4

Even if IEEE 802.15.4 is widely-accepted in WSN development, there are arguments against the performances of the standard [9, 51, 105]. Some of the critical arguments are given as follows:

1. **Always-On Radio** in Multi-Hop Networks In multi-hop networks, the router nodes must turn on the radio all the time [9] as well as in the non-beacon-enabled mode; the radio must keep active using only CSMA/CA.
2. **Collision between Beacons is intolerable** [51] In multi-hop networks, beacons from different PAN coordinators can collide with each other. These collisions are intolerable because beacons are used for the frame synchronisation.

Fairness problems and hidden-terminal problems are mentioned along with the possible improvements [105]. After the amendment TSCH is integrated into IEEE 802.15.4e [65], efforts to unite the communication protocols can be concretely seen. However, IEEE 802.15.4e only give the definitions of time slots and frames in MAC, the details of implementation such as how to achieve time synchronisation in multi-hop network and scheduling schemes are not provided in the standard [9]. Therefore, many theoretical works are presented as an alternative.

2.2.3 Frequently Used Techniques in MAC layer

Many works are proposed in the area of MAC layer in WSNs. However, they often consider a similar solution to tackle same problems [51, 76]. Therefore, this review focuses on the conventional techniques and the reasons behind its principles. In this way, the convergence of the theoretical concept can be seen [51].

2.2.3.1 Common Problems

In general, the complexity in WSN protocol design arises from the introduction of the duty cycle to save the energy by sleeping radio, resulting in the communication interruption [6, 51]. In the ideal condition, the radio module should be active only when the communication occurs, receives and transmitted only the useful data from the application without any failures. Thus, we can define the common problems as of the in MAC layer as follows:

- **Idle Listening** occurs when radios are active without any communications [4, 6, 58, 76]
- **Overhearing** happens when radios receive irrelevant data traffic such as duplication or data assigned to other participants [4, 51, 58]
- **Contentions** could be a major concern in WSN link architecture, which have many senders (Tx) per one receiver (Rx) as data packets are relayed to collection points [33, 51, 76, 105]. Contentions can cause a delay or congestion in some cases, resulting in packet drops. Unorganised attempts to transmit during contentions may lead to collisions or successful reception but ignoring the transmissions from other participants.
- **Control Overhead** is necessary for organising the medium access [33, 76, 108]. By transmitting extra control bits, the schedule for transmission and reception can be arranged before an actual communication. In this way, the system sacrifices its bandwidth and energy to avoid the problems above proactively.

Fairness [4, 105] and scalability [40, 44] are also additional considerable factors [76], as the centralised management is difficult to achieve in multi-hop topologies [50, 51], unlike the star topology. The following sections discuss common strategies in the literature.

2.2.3.2 Contention-solving techniques

At present, similar concepts to the Carrier Sense Multiple Access (CSMA) in IEEE 802.11 [33, 109] are commonly reused. Such techniques are crucial in asynchronous

duty-cycle protocols [4,6,51], but even synchronous duty cycle may use such techniques to increase bandwidth-efficiency [51, 110, 111]. Other techniques to lessen impacts of collisions are recommended by many works [112,113]. The basic principles of CSMA are briefly described as follows:

- *Carrier Sense (CS) or Clear Channel Assessment (CCA)* [3, 14, 33, 95, 98] The main idea can be described as detecting the availability of the chosen channel, i.e., sensing the channel whether it is free from any other transmissions before sending, called Clear Channel Assessment (CCA) [31,79]. Therefore, interceptions between parallel transmitted signals from different senders can be avoided. CCA can be performed by energy detections, i.e., observing the relative noise floor in the channel as a reference and reporting the channel busy when the detected energy is higher than the programmed threshold. The ratio of fault positive results is strongly depended on the threshold level setting. The accuracy of CCA can be improved by the outlier detection techniques [3]. Therefore, the performance of CCA depends strongly on how the respective radio chip implements the concept.
- *Collision Detection (CD)* [3, 6, 51] CCA is effective when the respective senders are in the sensing range of each other. In cases that the distance between them exceeds the sensing range, CCA yields no benefit, so-called Hidden Terminal Problems [3, 33, 51]. The intended Rx alone can detect collisions by observing an anomaly in the reception process, called Collision Detection (CD). CD can be simply implemented by observing inconsistency in receiving energy level, referred as Received Signal Strength Indicator (RSSI), or by examining whether the received packet is corrupted [112] with algorithms such as Cyclic Redundancy Check (CRC) [113]. After sending, the senders wait for the feedback from the Rx whether the reception is successful. Further instructions could be sent along with the feedback. One of the commonly used techniques is Binary Exponential Backoff (BEB) [6,34,51]. Senders perform BEB will wait before retransmissions in a random interval, which will be exponentially increased each time a consecutive collision happens [51].
- *Collision Avoidance (CA)* CD manages traffic after collisions but cannot prevent collisions from happening therefore in cases of high-density data traffic; collisions should be avoided. Therefore Collision Avoidance (CA) is realised by the initiation of handshake (Request-To-Send: RTS and Clear-To-Send: CTS) before transmissions [109, 111]. Additional information for traffic control can be attached to transmitted packets such as Network Allocation Vector (NAV) how long the channel will be occupied [33, 34, 109]. For further improvements of network reliability, Automatic Repeat reQuest (ARQ) can be considered [34]. ARQ is implemented by implication of an application for retransmission in cases of missing acknowledgement (ACK) [33, 92]. Therefore, incorrect receptions will immediately lead to retransmission of the packet.

2.2.3.3 Procedures for Transmissions and Receptions in Duty Cycling Radio

Since WSN need to turn on an off radio, corresponding to data transmissions (hence duty cycling radios), some regulations need to control the active period of radios, so that data transmissions and receptions can take place when radios from both Rx and Tx are simultaneously active. Roughly, such techniques can be classified into two categories.

Pre-planned Sleep Cycle

Pre-planned Sleep Cycle includes techniques with pre-defined rules or additional information to control sleep periods. Relying on preparations, duty cycling radios could synchronise their active period. In general, pre-planned sleep cycle techniques require two vital elements:

- **Time Synchronisation** Pre-scheduling protocols can only work when associated nodes are time-synchronised, i.e., can count a same defined period. For example, time synchronisation can be achieved by frame mapping, described as associated nodes match its counting parameters (counting rate and target value) with other nodes that count the same defined interval such as Inter Frame Space [9, 76]. An example can be seen in IEEE 802.15.4 beacon-enabled scheme (see details in Section 2.2.2.1). This algorithm needs a central coordinator. Thus network-wide synchronisation is hard to achieve under the assumption of multi-hop networks with limited transmission range [76].
- *Scheduling Algorithms* Channel allocation can be arranged by a centralised coordinator or by local coordinators. If a tree or hierarchical structure of data collection are assumed, then the parent or root nodes can be accounted for this task [9, 102] . Channels can be scheduled by three methods [51, 79]:

  1. ***Scheduling Links between a specific sender and receiver*** There are locally (covered more than 2-hops) or globally an agreement of channel allocation which is exchanged or known by co-located nodes.
  2. ***Scheduling Receivers*** Senders are often the coordinator, which decides a schedule to send packets to different receivers. This method can be efficient in particular situations such as broadcast scheme.
  3. ***Scheduling Senders*** In this category, receivers decide the schedule for senders, often Leaf Nodes in a tree or hierarchical topology. This concept strongly relates to the data collection nature of WSNs

Pre-planned sleep cycle can improve response time and energy consumption, because effects of duty cycling can be predicted, thus reduced. However, scheduling algorithms often involve exchange or negotiation of frame slots, which typically suffer from additional overheads. Nonetheless, recently there are solutions proposed distributed prediction

schemes that contain algorithms to predict behaviours of neighbours [51, 107, 114]. The prediction technique requires less overhead in comparison with exchanging schedules. For example, each node follows a pseudo-random code, described by each unique parameter [114]. Because neighbouring nodes exchange these parameters, wake-up periods or frequency-hopping sequences of neighbours can be predicted.

Unplanned Sleep Cycle

The protocols in this group do not attempt to synchronise the sleep cycle of participating nodes ,i.e., nodes possess asynchronous duty cycle. The Asynchronous duty cycling protocols refer to the concept that each node should possess its individual sleep or duty cycle pattern, asynchronous with any others to avoid collisions. Hence, to initiate a link, the respect sender must wait for the intended receiver to wake up and subsequently some signalling between the sender and receiver is required to start the packet flow. Depended on which side (receiver or sender) in communication link begin signalling, two concepts can be categorised as follows:

- ***Preamble Sampling or Low Power Listening (LPL)***

  If senders signal the request of packet transmissions, signalling must continue until intended receivers wake up and response. This concept is called Preamble Sampling [115]. B-MAC [3] adopts this concept to WSNs. The preamble signal is a pure jamming signal to occupy the channel. In the perspective of receivers, each node only needs to activate its radio, in a concise period to assess the channel occupancy (performed CCA), resulting in very low power expense. Therefore, the same concept can be alternatively called Low Power Listening (LPL) [4, 51, 58]. This simple concept is still profound, especially in wake-on radio such as CC1120 [97]. Nonetheless, Preamble Sampling is further developed by information attachments in preambles such as the address of intended receiver or the remaining time of preamble signalling to reduce idle listening and overhearing [51, 116]. In packetized radios, preambles are mimic by burst transmissions of packets, resulting in strobed preamble techniques [4]. Strobed Preamble is performed by sending packets with an attached destination address in a periodical interval, which Rx can reply and begin the data transmission. Figure 2.3 shows diagrams of LPL variations which reduces the idle listening as the protocol have been improved.

  Nonetheless, the course of novel proposed protocols in asynchronous duty cycle domain has been shifted to receiver-initiated protocols [51], which is discussed in next section.

- ***Low Power Polling or Low Power Polling (LPP)***

  Low Power Polling or Low Power Probing refers to the concept that Rx signals waiting Tx to begin data transmission, resulting in reductions of energy consumption from both Tx and Rx, therefore called Low Power Polling (LPP) [6, 51, 114].

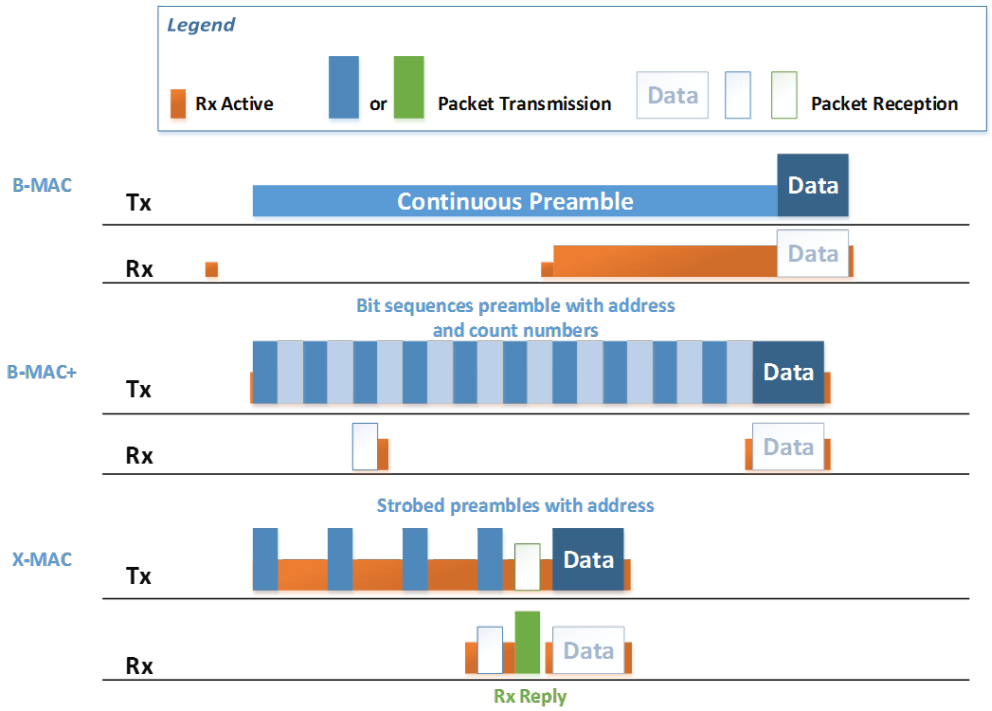


Figure 2.3: Development of LPL Techniques [3–5]

LPP was proposed by RI-MAC (Sun et al. 2008) in contexts of WSNs. The LPP main method can be described as follows: In Rx perspective, nodes in LPP networks broadcast a beacon after waking up and waiting for a defined interval, called dwell time, for incoming packets if any. In cases of any reception of incoming data, a beacon is sent as a response. The beacon invites further transmissions. However, depending on the result of the reception, the beacon may serve as the acknowledgement (ACK) for the correct reception or may indicate that concurrent senders need to perform BEB with the attached back-off windows (BW) to avoid more collisions. Therefore, this concept implies the practice of ARQ. In Tx perspective, any node with packets to send stay awake until receiving a beacon from the intended receiver. However, in case of informed collision, Tx performs BEB and ensure that the channel is unoccupied at least one round trip before retransmission to avoid more collisions. The overview of common LPP process is given in Figure 2.4. Figure 2.5 shows the LPP process to solve collisions, in cases of concurrent senders.

In comparison with LPL, Rx in LPP spend more energy per sampling, but in cases of relatively frequent data transmissions, the absence of preambles spare energy expense and reduces channel occupancy. A significant drawback of LPP is the increasing likelihood of synchronous concurrent senders, which wait for a same signal or beacon [51, 117].

LPP is developed further to reduce idle listening by introduced prediction-scheme, which

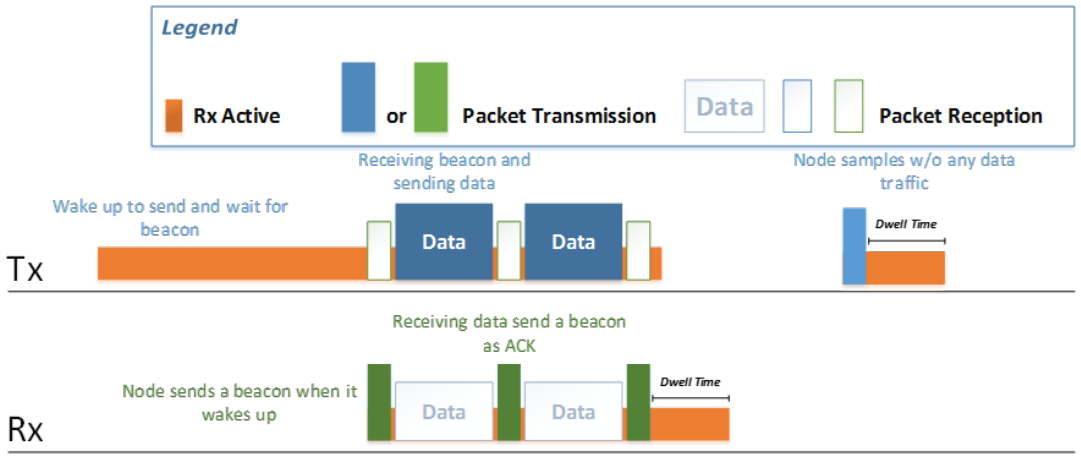


Figure 2.4: Timing diagram shows LPP processes w/o concurrences [6]

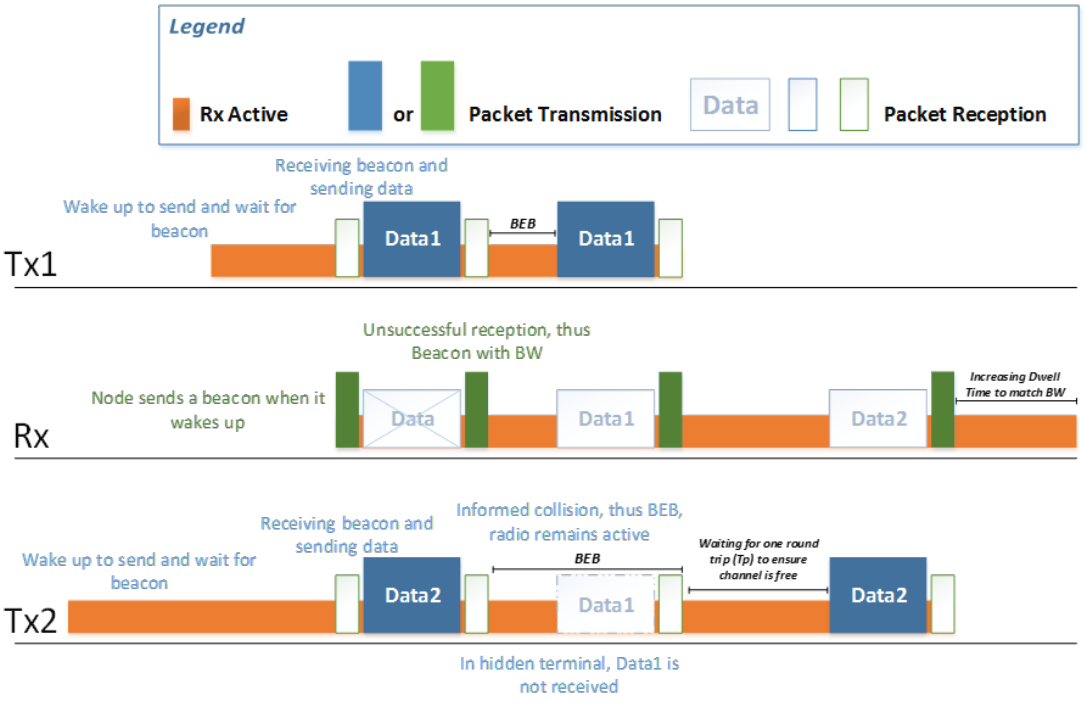


Figure 2.5: Timing diagram shows sequential occurrences when collision happens in LPP [6]

is already discussed in the last section. Recent works on WSN MAC protocols often involves the combination of CSMA and pre-scheduling techniques [51, 110, 111, 118]. This fact shows the convergence between both synchronous/asynchronous duty cycling MAC protocols that intend to take advantages of both CSMA-based/scheduling-based protocols. Therefore, in the practical implementation, if MAC protocols reuse the same algorithms, multiple protocols can potentially be implemented without resource explosion.

2.2.4 Discussion

Since IEEE 802.15.4 is widely accepted in the WSN development, many well-known vendors produce radio chips, compliant with the standards, resulting in proprietary standards and novel theoretical proposes on top of the same radio definition. The standard IEEE 802.15.4 still has significant drawbacks regarding energy consumption in multi-hop topology and the newly released version, IEEE 802.15.4e does not provide the details of the practical implementation of the standard. Even though the significant mass of WSN systems will operate under the MAC protocols or commercial standards that are fully-compliant with IEEE 802.15.4, the possibility of native WSNs, developed by using similar platforms but adopting a proprietary MAC protocol, cannot be disregarded. There are a significant number of theoretical proposes in MAC protocols of WSNs, but the frequently used techniques, regarding same issues in WSNs, can be comprehensively categorised. Similarities of commonly used techniques could lead to practical solutions, which can be implemented in real hardware to build cross connections in HET networks.

2.3 Cooperation between Wireless Sensor Networks

The interoperability between separate systems of smart devices, including WSNs, is improved along with the development of key technologies on the Internet of Thing (IoT) [8, 48, 49]. Cooperation between WSNs in separate domain consequently belongs to essential parts of the vision towards IoT [11].

As WSN systems are diverted in many aspects, the interoperability between separate WSNs is addressed by many research [8]. As the key technologies are united by the Internet connection [49], there is also the research trend to make WSNs compatible with the Internet, as a result many research works suggest that proprietary standards in WSNs should be able to converge around the interoperability with the Internet-based standards [8, 9]. However, this idea remains sceptical in many parts [52]. Even though local systems need a connection to the Internet at some point, this research suggests that the opportunistic collaborations between co-located WSNs in local scales can happen by enabling direct interconnection between them first.

This section discusses the overview of the current research trend on cooperation between WSNs, which is integrated into the big picture of IoT developments. The proposed solutions on the interoperability between WSN in separate domains, involved conforming to the Internet, are described, and the sceptical arguments on the proposed solution are discussed. The standpoint and contributions of supporting Opportunistic Direct Interconnection (ODI) to the mainstream development towards IoT are given. How to enable ODI in heterogeneous networks in previous works will be discussed in details to form the basis for their implementation in the next chapter.

2.3.1 Integration of Wireless Sensor Networks into IoT

Nowadays, almost every computer is connected to global interconnections by the Internet, and the number of mobile platforms such as smartphones and tablets is exponentially increased [9]. As technologies in wireless communication are advancing, wireless connections offer the level of network quality that the handover between wired and wireless connections is almost unnoticeable for users. As the massive connections between smart devices is anticipated [48], the concept of the Internet of Thing (IoT) [49] is emerging with the promise to make significant qualitative changes in how we use the global connection to perceive and interact with the environment [48, 49, 52]. By integrating elementary services from individual smart systems together, composite services can be built (Service-Oriented Architecture or SOA). Consequently, benefits from individual systems are leveraged in the perspectives of users as well as in the perspective of service providers (examples are given in Chapter 1). IoT is an interdisciplinary research topic, in which WSNs will be a key technology [49] to provide data from remote sensing for composite services. The concept of virtualisation of WSNs can be given as an example for the integration of cooperation of WSNs in IoT. The virtualisation means to present raw physical resources in forms of logical units, hidden the resource management from potential users, to provide the resources for multiple concurrent users more efficiently [7,119]. Therefore, by adopting this concept in WSNs, the sensing tasks of the user application is provided by the Virtual Sensor Networks (VSNs), which possess sufficient resources, allocated from physical WSNs. Figure 2.6 explains the virtualisation of WSNs. In *a)* the figure shows the architecture of a general-purpose sensor node, acting as a virtual node for multiple users. In *b)* many VSNs are generated from one large-scale physical WSNs, separated by virtual walls. In *c)* many WSNs are used in one VSN to support the user application.

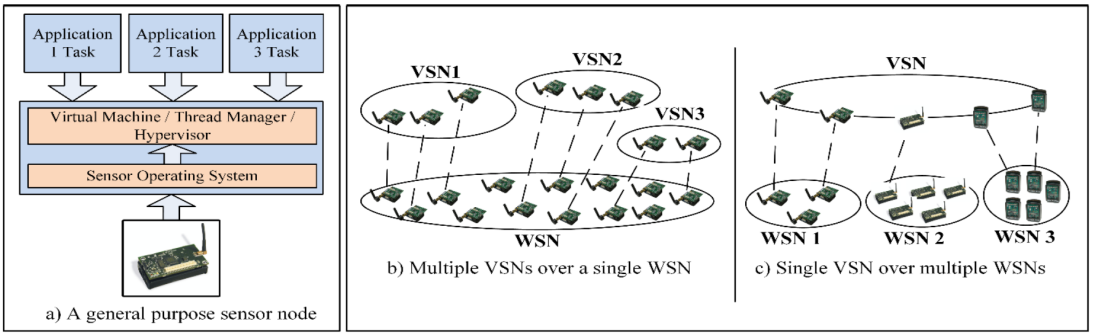


Figure 2.6: Virtualization of WSNs (reproduced from [7])

WSNs can provide their user interfaces, using web services, so that potential users can access globally via the Internet. In this way, the services can be provided by a proxy, using web protocols such as HTTP (Hyper Text Transfer Protocol) [8,9,48,50,52,120]. The remaining question is how deep into the network the Internet connection should/could be reached? Should the services be provided outside the network by gateways [52, 120]

or inside the network by individual nodes or cluster heads [9]? There are many works, discussing the question [7, 9, 52, 120]. Both solutions have advantages and drawbacks. The gateway option has the significant drawback that the connection relies ultimately on the correct functionality of the gateway, which can be unavailable or failed [120], while the implementation of web services on every node may unnecessarily abuse the resource of a constraint platform assuming it is a possible option [52]. Nonetheless, enforcing a unified protocol stack compliant with IP solutions may eradicate the incompatibility between separate systems. Therefore the details of the solution will be further discussed in the next section.

2.3.1.1 IP-Based Solutions

The attempt to integrate Thing with the Internet lead to the framework of IP-Based protocol stacks in WSNs. IP-based solutions suggest assigning a unique IP to each node. The solution involves using IPv6 on top of the well-known standard IEEE 802.15.4 (see details in Section 2.2.2.1). IPv6 frames have the maximum transmission unit (MTU) at 1280 bytes. Therefore, the overhead of IPv6 is practical. However, IEEE 802.15.4 possesses MTU up to 127 bytes [9], so without any modifications, IPv6 is not feasible in WSNs. The 6LowPAN standard was released by Internet Engineering Task Force (IETF) to adopt IPv6 in a Low-Rate Wireless Personal Area Network (LR-WPAN) [19,22]. The overhead of IPv6 is compressed by fragmentation or reassembly of the original header. The compression process begins at the gateway, which is connected to the backbone network [8]. Recently, The Internet Engineering Task Force (IETF) proposes an IP-Based application protocol for constraint devices [8,9], namely Constrained Application Protocol (CoAP) [22]. CoAP consists of a reduced set of HTTP (RESTful Architecture) to support machine-to-machine applications, building on top of the conventional transport protocol, UDP (User Datagram Protocol). CoAP is capable of simple reliability assurances by checking duplicates and request retransmission. This framework is noticeably implemented by well-known middleware such as TinyOS [121] and Contiki [122]. Figure 2.7 illustrates the overview of the mentioned protocol stacks, allowing IP-Based protocols to implement in WSNs.

If all distinctive nodes in separate application domains could follow the mentioned protocol stacks, the compatibility problem would be solved. Since the widespread middleware already supports this framework, it could offer a standard template for future WSN developers. Hence, the future trend of WSN implementation would almost certainly embrace this solution [8,9,123]. Nonetheless, there are sceptical arguments on the complete integration of every WSN platform with the Internet. Some critical arguments are listed as follows [52]:

- **Functionality** The full integration of WSN with IoT in this fashion may overcomplicated, some systems that directly collect data and answer queries.

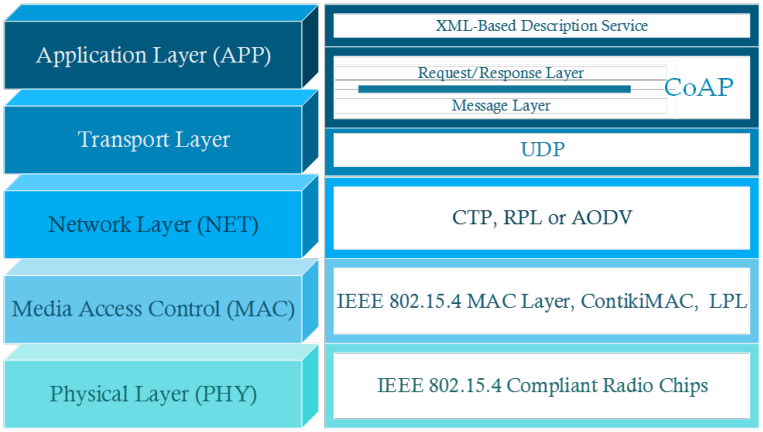


Figure 2.7: Protocol Stacks of IP-Based Solution in WSNs [8, 9]

- **Hardware** Whether it is feasible or efficient to fully connect with IoT and adopt the protocol stack in a large-scale network, consisted of resource-constrained platforms is still not conclusive. In HET networks the capability of platforms can be different therefore it may be more efficient only to integrate high capable platforms to the global connection.
- **WSN Network Redundancy** If terrestrial WSNs in relatively large scales are assumed, redundancy between co-located nodes will be high, most likely they can offer the same services. Thus, representation by cluster head could be more efficient.
- **Protocol Specific Optimisation** By considering the diversity of WSNs regarding relevant application domains and proprietary protocols, a considerable mass of WSNs would prefer its own optimised communication protocols.

Considering the mentioned concerns about the full integration of WSNs, this research believes the IP-Based solution could only reach into a certain depth of the hierarchical structure, probably not cover all of the individual platforms. As an example, if the cluster head adopts the IP-based protocol stack, all Leaf Nodes can use a native protocol to optimise its specific goals inside the locally defined network boundary. Some particular domains may still use the same definition of the physical layer and favour the direct cooperation if it is a possible option. This research intends to contribute to the IoT development by investigating into this direction with a practical implementation to find a practical framework for enabling a direct cooperation between co-located WSNs domains. The existing literature in this direction will be discussed in Section 2.3.2.

2.3.2 Scope of Opportunistic Direct Interconnection

According to the discussion in Section 2.3.1, the physical structure of WSN domains could be seen in a hierarchy. A powerful node will be surrounded by many constraint

nodes, governing a decision on any centralised policy and acting as a gateway or proxy to the Internet. In this work, we refer to this composition as a *domain*. In other words, a domain can refer to a WSN system or subsystem that consist of sensor nodes in a star or multi-hop topology, connected to the Internet by a base station or a powerful platform (Cluster head inside platform-HET networks). In this work, such node will be referred as Management Node (MN). Sometimes, boundaries of the domain can be defined by technical perspectives or by the authority in the user perspective, WSNs are thus separated into multiple domains. In each domain, sensor nodes can choose specific wireless communication protocols for communication in the domain boundary.

The concept of Opportunistic Direct Interconnection (ODI) proposes direct wireless interconnection between separate WSN domains that can be activated opportunistically to support local collaborations between beneficial participants while allowing the individual WSN domain to maintain its preferred algorithms in the communication layers.

ODI positions itself along with the IoT by promoting the connectivity and interoperability between WSNs when the full compatibility provided by the IP-based solution cannot reach into a certain depth of WSNs. Therefore, in the abstract concept, ODI referred in this work targets the domain with highly resource-constraint platforms, which are impractical to implement the IP solution. The network conditions prefer their optimised protocol stack. However, the system design still considers the opportunity to cooperate with the co-located neighbours whenever beneficial. The connectivity provided by ODI offers the robustness and scalability to the cooperation scheme since it is achieved in the distributed manner, independent from the availability of the backbone network/internet connection. However, if the global connection is present, the collaboration scheme of the local domains can be regarded as a local group providing composite services to the outside user in the traditional viewpoint.

2.3.3 Motivations of Opportunistic Direct Interconnection

Previous research studies theoretical benefits of ODI in various perspectives (see Section 1.1). Benefits of ODI can roughly classify into network-based and application-based benefits.

- **Network-based Benefits** The network-based profits describe the advantages, occurring because of network resources sharing between co-located network domains.
  - *Optimising of energy consumption* Mathematical models, game theory, and simulations have proved that the improvement of network lifetime can be

achieved by load balancing [1,55]. Packet forwarding can be optimised in co-operation scheme. The simulation results in [61] has shown that the average cost of the shortest path can be reduced by introduced hybrid nodes, which can connect co-located networks. In [57], the author proposes a case study of energy sharing between common WSN and EH-WSN by load redistributions. To adjust network parameters and to make the strategic decision on the co-operation scheme, the software module in higher layers is needed. [69,82,124] proposed a network management system to optimise the network parameters, based on the feedback signal quality.

- *Improving Reliability and Connectivity* The reliability is enhanced because multi-path connections ensure that packets can relay to respective clients. For example, ODI offers opportunities to reconnect disjoint partitions [55]. Primarily, in a hostile environment, disjoint sections can evolve due to dynamic channel quality of wireless communication. Therefore, ODI will become crucial for packet forwarding from disjoint sections [46, 55]. If neighbouring networks need public access, ODI can provide a possibility for the Internet connections.
- *Promoting Flexibility in Network Planning* In the network planning, the overview of situation development is often not complete in the beginning phase; entrepreneurs may decide to grant new phases of the project after witnessing favorable results. Alternatively, other associated projects may be launched later of the planning phase. New WSN domains can take place by different authorities. If future interconnections between separate domains are considered in the communication design beforehand, the application-level can be developed later without difficulties of collections and redeployments of sensor nodes.

- **Application-based Benefits**

  Collaborations of existing and new networks could leverage the value of individual systems by combining the available services/resources. ODI provides alternative packet routing for exchanging application messages. Because ODI enables wireless connectivity between individual nodes, sharing application data can promptly occur as the associated networks encounter each other in the communication range. Some example can be given as follows:

  - *Case study of collaborative water catchment monitoring* has been proposed in [10], in which data, provided by different types of co-located WSNs is used to predicted water qualities. In Figure 2.8, blue arrows show the water flows in the catchment. Red arrows show the interconnections between WSN domains. In this scenario, the networks are deployed in remote areas. Thus, ODI is more optimal than relying on infrastructure connections.

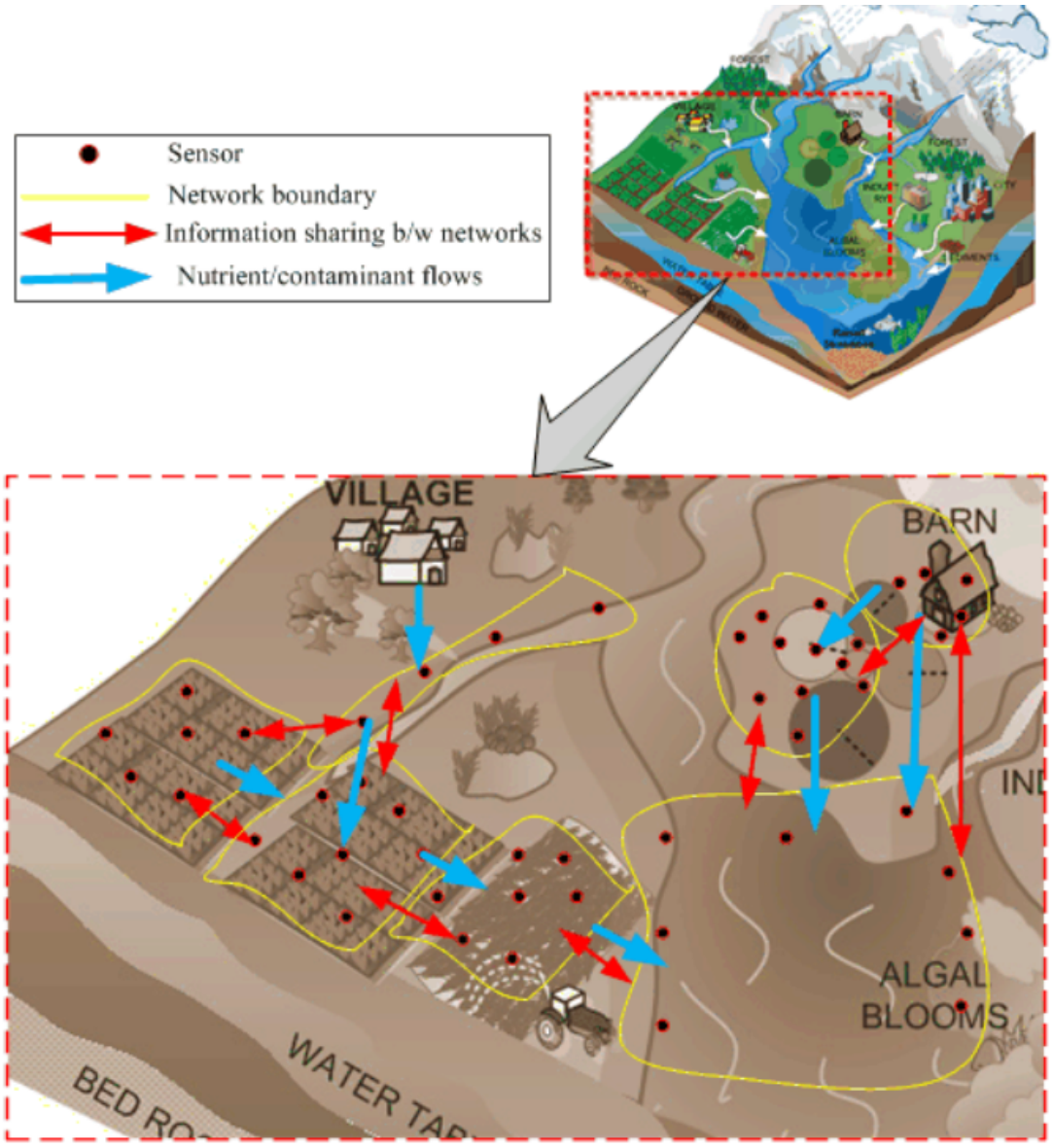


Figure 2.8: Interconnections between WSN domains in collaborative water catchment monitoring (reproduced from [10])

– *Case study of autonomous cargo systems* proposed in [62]. The scenario explains typical check-up process in cargo. Shipping status, monitored by WSNs in transport vehicles, is reported to the infrastructure of the cargo. Because the vehicle is mobile, so instead of relying on Infrastructure connections, ODI could be more optimal.

– *Case Study of collaborative emergency service* [7,49,91]. In emergency warning systems, networks may never produce data until the events occur. However, in the instance of emergency events, a warning message and data capture may explode and require both reliability and latency. Therefore, ODI could offer an alternative way to broadcast the events by using another network infrastructure.

The ODI concept potentially offers an alternative to exchange data without relying on the network infrastructure, especially in the context of WSNs, which may be deployed in the remote area. It can also be used to enhance the reliability by enabling alternative route in the packet forwarding scheme. The discussion reveals huge advantages of the opportunistic direct interconnection between WSNs. However, the critical questions are in the technical perspective whether ODI is feasible and what is the best way to build such a direct connection.

2.4 Conceptual Framework of Opportunistic Direct Interconnection

The cooperation of separate elements in IoT is achieved under the assumption that the interoperability will be provided via the internet connection either by a gateway/proxy that provides the interface to the client from outside [7, 125]. Some works assume the connectivity of the distinctive domains disregarding the technical issues in the communication layers [53, 56, 62, 69, 71]. Thus, only a few works consider the problems in the lower layers in the protocol stack [11, 12, 68, 126]. This section reviews the technical aspects of the ODI concept from the PHY layer to the application layer.

2.4.1 Compatibility in Physical Layer

Using OSI-model as a reference, the compatibility of associated systems must be considered from ground-up at the lowest level, i.e., the PHY compatibility must be first mentioned. In the review of the physical layer in Section 2.2.2 and 2.1.3, there is an apparent tendency towards using IEEE 802.15.4 as the common design for radio chips. Therefore, a certain degree of the PHY compatibility can be expected. For the best of author knowledge, the interoperability between radio chips from different vendors has never been confirmed by practical validation. Following concerns could prevent radios of various vendors to transceive the physical bit from a different model:

- *Physical channel* may differ slightly due to implementation techniques. The frequency synthesising and the channel filtering may need to be finely tuned to match up with other products from different vendors. The frequency/phase errors may dramatically decrease the probability of the successful bit transfer and consequently the whole packet.
- *Different data whitening technics.* The spread spectrum may be used to trade off between robustness and bandwidth. The transceiver must use the same sequences for DSSS for recognising signals from the other end or knowing the sequence of the frequency hopping in FHSS.

- *Capable of detecting the beginning of any transmission.* The sign to begin transmissions may differ in each model. Some may detect energy level; the other may define a preamble sequence to signal a transmission.
- *Synchronising the symbol rate.* The preamble bits may be used as a synchronisation signal. The difference of preamble sequence may be intentional from the vendor to distinguish between similar systems.

Nonetheless, the trend of IoT will eventually enforce the concern on the interoperability between platforms, so that the PHY compatibility should be eventually compulsory for all platform vendors. Therefore, **this research assumes the compatibility of hardware in the physical layer between nodes from different network domains**, instead focusing on the systematically methods to enable ODI in protocol levels.

2.4.2 Process Analysis

Under the assumption of the interoperability of the radio chips, individual networks need additional modifications in their protocol stack to enable the connections. The sequential process of ODI can be analysed by considering the scenario of multiple co-located WSN domains with possible radio links, demonstrated in Figure 2.9.

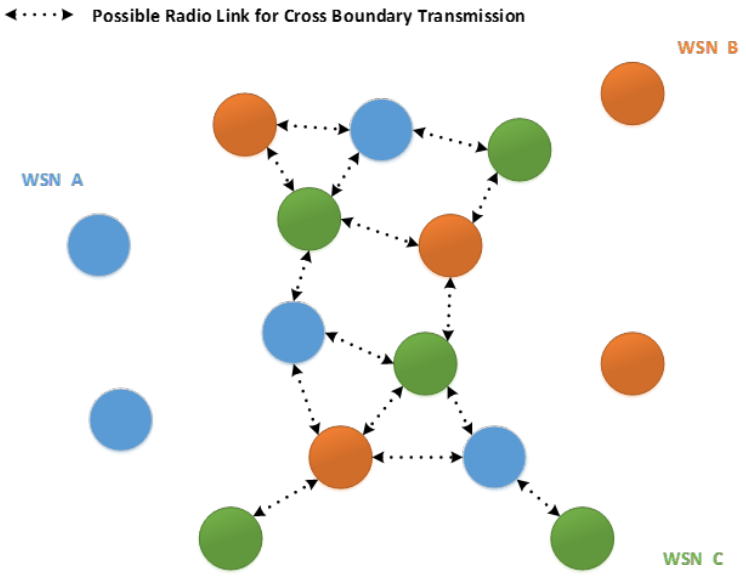


Figure 2.9: Hypothetical scenario, WSN A, B and C are inside each other coverage and able to receive physical bits from each other

ODI can be enabled, if the radio links are correctly regulated, According to the literature [45], the cross-network cooperation can be divided into three phases: 1) Distributed Network Discovery 2) Network Binding (exchange networking parameters) 3) Service Convergence (negotiate the incentives by exchanging possible services). OI-MAC [11]

is another work that explains the process of ODI, and it also comes to the similar conclusion. OI-MAC mentions two phases for initiating ODI as 1) Neighbouring Discovery Scheme (NDS) 2) Handshake process.

From the two mentioned literature, it can be implied that the sequential process of ODI can roughly be separated into two steps: 1) discovering the neighbours and 2) exchanging information.

2.4.2.1 Neighbouring Discovery

Following the literature review in this work, OI-MAC [11, 12] is the only work to discuss the technical details of the neighbour discovery process in WSNs. Therefore, it will be reviewed as a reference. OI-MAC reserves one channel from 16 channels in IEEE 802.15.4 as the common channel (CCH) for NDS and handshake process, while other channels can be used as data channels (DCH). Those networks, which adopts OI-MAC, utilise different data channels to reduce unwanted interferences and to maintain network privacy. The discovery scheme, proposed in OI-MAC [11], is straightforward. It composes of two phases (see details in Figure 2.10):

1. *Active Phase* is performed by actively listening in CCH for a defined time interval, called Discovery Period (TD). Active discovery happens one time in the phase of network establishment. Each node switches to the CCH and keeps listening. Each received discovery beacon will be regarded as an ODI request. Therefore it will be replied by another beacon to answer the request.

2. *Passive Phase* is periodically executed throughout the network lifetime. When TD passes, each node switches to CCH periodically and broadcast a discovery beacon (which contain the initial ODI configuration). Once the broadcast is nished, the node keeps waiting for a response in a defined interval (Dwell Time). If neighbouring networks exist and therefore performing Active Discovery, discovery beacons will be replied. As a result, the nodes will become associated and defined as Boundary Node (BN). The occurrence is referred further in this document as Successful Pairing.

This process is local and performed by each node to discovery nodes from other domains. Therefore, the necessary modifications for NDS are thus contained in the concept of MAC layer. After successful pairing the associated nodes are called Boundary Nodes (BNs), acting as a gateway to other domains. The BN then broadcasts the discovery network-widely. Therefore, the system must support a broadcast scheme. In conclusion, NDS imposes two requirements on the network:

1. The algorithm of NDS must be added to the link layer of each node.

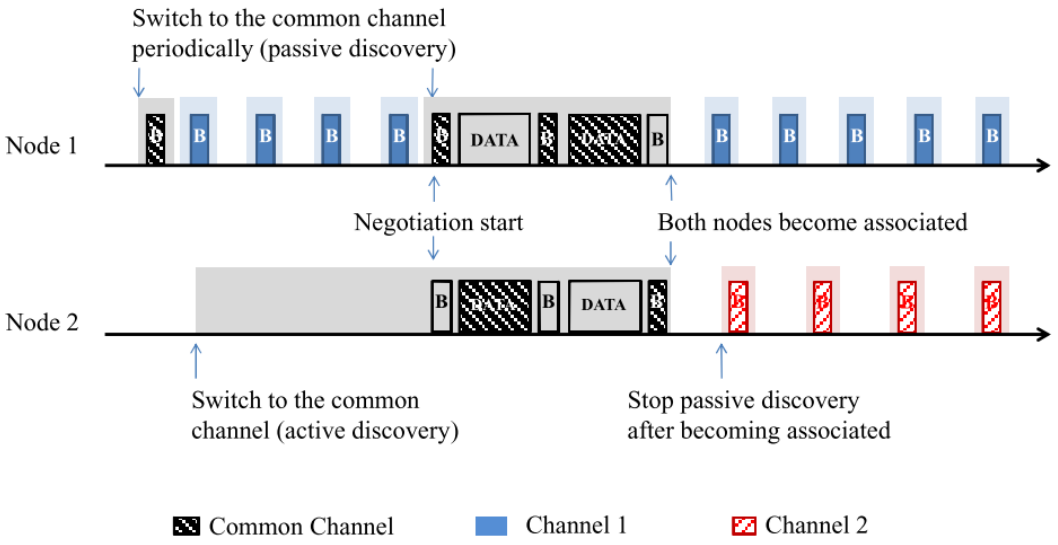


Figure 2.10: Theoretical time diagrams, described the discovery scheme and the handshake process (reproduced from [11])

2. The network needs to support a broadcast scheme

2.4.2.2 Cross Boundary Data Exchange

After neighbouring domains are discovered, the domains will begin exchanging information. The information can be classified into two types:

1. *Network parameter settings for establishing/maintaining the connectivity.* Some of this information are local such as the scheduling for cross-boundary transmission, hop distances to Sink and the link quality. This type of local information can be exchanged immediately after the discovery.
2. *Application data such as query/requests of services or resource contents.* This kind of information may exchange after the reliability of the cross-link between BNs is confirmed locally. In the universal cases, the data could originate from any nodes inside the domain; then the data will be transferred to BNs to send it across the domain boundary. When the data reaches the destination network, the data need to be transferred to a specific destination inside the domain.

From the above discussion, the cross-boundary data transfer will involve all protocol stacks. Figure 2.11 illustrates the diagram, showing the protocol stacks, involved in the transfer process of cross-boundary data.

- *In MAC layer*, each node performs NDS to find nodes in other domains; potentially each node can become BNs. So, the protocol to send data across the boundary should be integrated into every node.

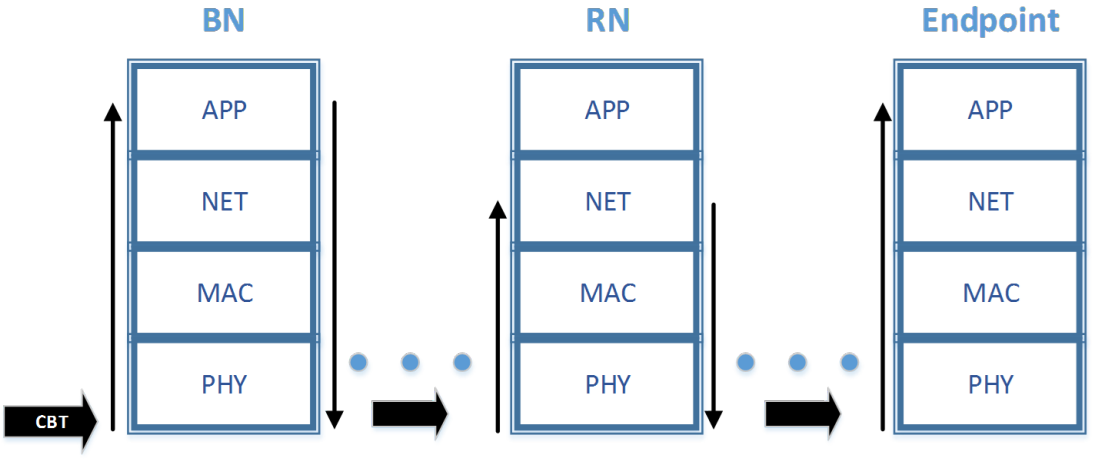


Figure 2.11: Protocol stacks involved in rerouting packets to a specific endpoint in the domain [12]

- *In NET layer*, Router Nodes (RNs) inside each domain must possess an algorithm to determine the next hop for the cross-boundary data.
- *The APP layer* of every node must be able to recognise the content of data, when the data is relevant to them, i.e., they are the specified endpoint. Therefore the uniform format for application data should be specified. In extensions, BNs may also act as a proxy, caching some resources to improve service quality.

2.4.3 Conceptual Design

The analysis of the process of data transferring in the ODI scheme reveals that the communication design of WSNs needs to consider the building blocks of ODI in each protocol stack. This section discusses the requirements in each protocol stack and the principle of the design in each communication layer.

2.4.3.1 MAC Layer

According to the ODI concept, the MAC layer should support three prerequisites:

1. Each domain can choose their own MAC protocol for optimisation purposes.
2. Each node can perform NDS as a distributed algorithm.
3. Each node can become a BN and support a Cross Boundary Transmission (CBT).

Considering these prerequisites, there are two possible design options for MAC layer:

1. Each node supports all possible MAC algorithms of the potential cooperative domains and the algorithm for NDS.

2. Each node maintains their native MAC algorithm but additionally keep an inter-networking MAC algorithm for CBT and NDS.

The design in Option 1) will result in every node maintaining all possible MAC protocol, which will unnecessarily increase the memory footprint, while Option 2) conceptually offers the connectivity with fewer memory usages. However, both solutions point out that the communication design inevitably involves implementing multiple active MAC protocols in the same communication system. The concept of multiple MAC protocols has already been explored by a considerable number of previous works [11, 67, 68, 126]. However, none of the existing works except from OI-MAC [12] follows the idea of introducing an inter-networking MAC protocol to support the connectivity between separate domains. This work thus reviews the concept proposed in the literature as the template for enabling ODI.

Initially, Teng et al. has proposed the first version of OI-MAC in [11]. Back then, OI-MAC imposes the associated domains in the interest to adopt its MAC algorithm, so that the distinctive system can maintain its virtual boundary while offering the possibility to send data across the border. This version of OI-MAC obviously diverges from the concept of ODI defined in this work. Later, the author has released the second version of OI-MAC in his thesis [12]. The proposed concept takes the differences of the MAC algorithm into account. From this point, the discussion will use OI-MAC as a reference for the existing conceptual design in the direction of ODI.

The second version of OI-MAC proposes each distinctive domain to possess two MAC protocols. One of them is used for the internal communication, and another one is used for the interconnection between separate networks. Both MAC protocols coexist simultaneously, but the access to MAC protocols to PHY are authorised to one of them at a time. This algorithm is called the virtual MAC. In CBT, the virtual MAC switches the access to OI-MAC periodically in the interval of CBT Period (TCBT). In this time, the access to PHY is handed over to OI-MAC. OI-MAC then performs LPP in CBT-DCH (Cross Boundary Transmission Data Channel), which is reserved for CBT packets. Therefore, HET-OI-MAC defines two reserved channel: 1) Common Channel (CCH) for NDS and 2) CBT-DCH. The theoretical timing diagram is shown in Figure 2.12.

2.4.3.2 Network Layer

This section also summarises the concept of the network layer in the ODI scheme proposed by Teng et al. [12]. The literature suggests this conceptual design without any practical validation. Therefore, it is necessary to outline the existing concept before

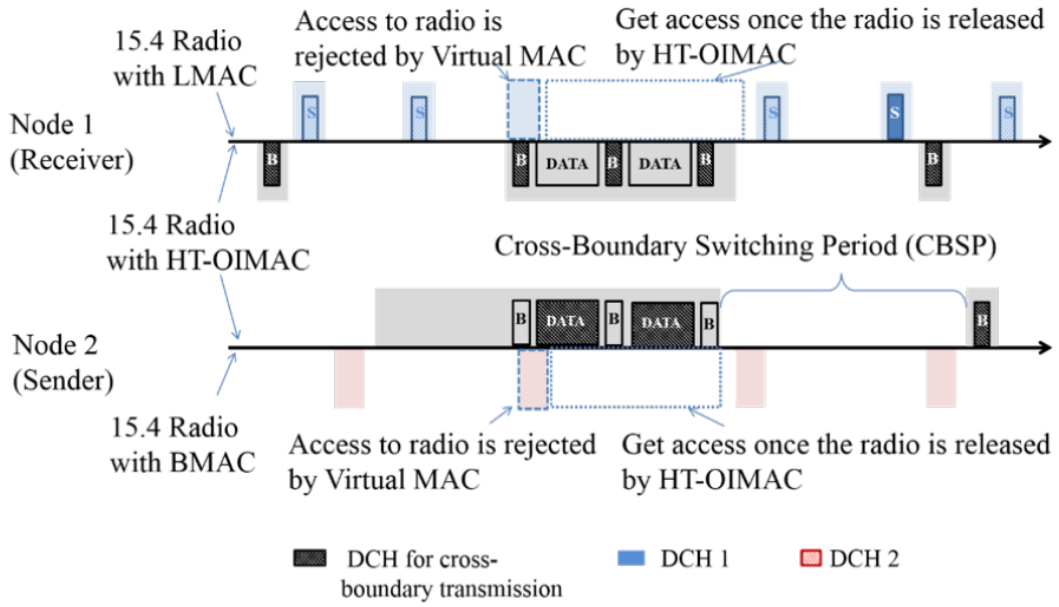


Figure 2.12: Theoretical Timing Diagrams for CBT, performed by OI-MAC (reproduced from [12])

implementation and improvements. To forward ODI frames, the literature suggests all participants adopt a routing protocol based on a routing table. Additionally, the framework imposes the participant to hold an extra table separately for ODI in every node which is only used for forwarding ODI frames. The template of the routing information is shown in Table 2.3.

Pass ID	**DST NET ID**	**Boundary Node List**			**Delivery**	
		`b_addr`	nextHop	`h_Dist`	Priority	`sb_addr`
1	41:01	1	2	12	Low	1

Table 2.3: Routing Information of the ODI routing table [12]

Pass ID is a 2-octet integer given as an entity for any data traffic. *DST NET ID* is the destination domain. The *b_addr* field indicates the address of the *boundary node (BN)*. The *nextHop* field records the next suitable neighbour to receive the frame labelled with the specified *Pass ID*. The *h_Dist* field indicates the hop distance from the destination. The priority may be explicitly specified, and the *sb_addr* field dictates a specific BN in cases that many BNs may be available. However, the literature did not provide the way to exchange this information neither the algorithms to determine the suitable next hop and the suitable BN. Nonetheless, assuming that the headers can be prepared. The conceptual framework suggests the following template for the header of any ODI frame:

```
CBR_Header {
   -  Source Network ID (SRC NET ID): uint16_t
   -  destination Network ID (DST-NET-ID): uint16_t
```

```
    - Passport ID (PASS ID): uint16_t
    - Modified FCF: R_TAG
}
```

R_TAG is inserted in *Frame Control Field (FCF)* of the native frame format to classify any ODI frames from native frames. If *R_TAG* is set, the algorithm will determine the next hop by looking up the ODI routing table instead of the common routing table.

The proposed theoretical concept in the NET layer is sceptical in many parts. It is also doubtful that a high constraint platform can allocate valuable resources to all additional tasks/information assuming that these information headers must be exchanged before each data exchange. Additionally, are all of the extra header necessary? Alternatively, the NET layer can be provided in the entirely different concept. This research will validate the idea by a practical implementation which should lead to a solid conclusion over of this concept is necessary to determine the feasibility of the concept.

2.4.3.3 Application Layer

Teng et al. [12] propose the conceptual design of the protocol used by the APP layer as well. The proposed concept of the APP layer provided by the literature is still highly abstract. Nonetheless, it is a proper starting point to develop the idea of the application layer in the ODI framework. The concept suggests the template of the application message formats in four categories:

- *Service Discovery (SDis)* is used in the process of information exchange to discover a service provided by a participant
- *Service Advertisement (SAdv)* is employed in the process to inform a service to another participant network.
- *Service Negotiation (SNeg)* is used in the subscription or unsubscription of any service from another provider.
- *Service Delivery (SDel)* is used to signify the beginning of any subscribed service and its termination.

In every category, the message can be the initial Request (REQ) or the consequential Reply (REP) Message. The APP layer, therefore, requires further headers to signify the type and function of delivered messages:

```
APP_Header {
    - Function Type: uint8_t
```

```
    - REQ/REP: uint8_t
    - Message Control: uint16_t
    - SRC NET ID: uint16_t
    - DST NET ID: uint16_t
}
```

Function Type can be one of the mention categories (SDis, SAdv, SNeg, Sdel). Message Control is the additional information such as priority or security level. However, some critical details are not provided such as the values of the defined fields, what can be the options that specify in the Message Control, and Is the reserved space for the header is necessary? The practical validation can answer these questions. Nonetheless, the literature provides the general flow of the related process in the application layer. Figure 2.13 shows the sequence diagram of message exchange in different scenarios between associated domains.

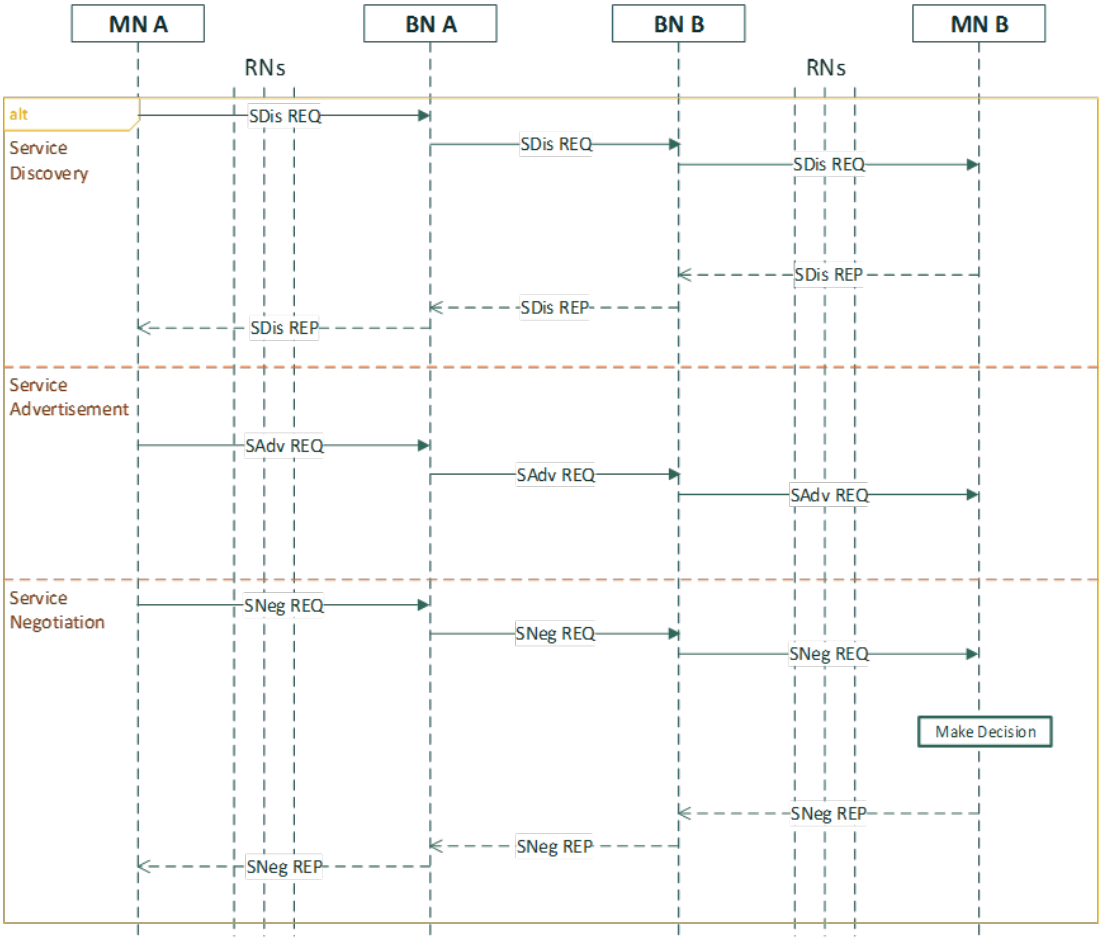


Figure 2.13: Message exchange in Service Discovery/Advertisement/Negotiation schemes [12]

This section briefly describes the theoretical concept proposed by Teng et al. [12]. However, many parts remains an abstract concept lacking critical details for implementation. The foreseeable problems will be discussed in Section 2.4.4

2.4.4 Discussion

Section 2.4 summarises the existing concepts in the technical aspect regarding enabling ODI. Since Teng et al. [12] is the only existing work which elaborates the details of the ODI framework, this thesis uses the conceptual design proposed in the literature as a starting point to develop the practical ODI framework which can provide enough details for real hardware implementation. The ODI framework in this thesis relies on the assumption that the future trend of IoT development will improve the compatibility of the RF module in different platforms. However, the foreseeable concerns regarding the connectivity of the RF modules are discussed. How to achieve the compatibility of the RF module is out of the scope of this thesis. This work then assumes the compatibility of the RF module focusing on the issues in the communication protocol stack.

MAC layer

The original concept of OI-MAC diverges significantly from the definition of ODI in this works because it suggests using OI-MAC for all participants, neglecting the freedom to optimise an individual network in its circumstances. Later, OI-MAC is employed in the virtual MAC concept as a common protocol for Cross-Boundary Transmission (CBT) and Neighbour Discovery Scheme (NDS), while maintaining a native MAC algorithms for internal communication. However, the MAC algorithms proposed in the existing framework must be validated whether it is indeed appropriate for CBT because the MAC algorithms proposed in the current framework (LPP see details in Section 2.2.3.2) is originally designed under the condition that there are low contentions between senders. This work will systematically reanalyse the characteristics of the data traffic at the boundary between domains again and validate the performances of OI-MAC in the desired characteristics. The validation may lead to a significant improvement on the chosen MAC algorithm used at the boundary between separate domains (Internetworking MAC) which lay the foundation for the design of the application layer of the ODI framework.

NET Layer

In NET layer, the fundamental concept is given, but it is still theoretical in many parts. The concept imposes the associated domains to include the routing table with the ODI information. The details are not provided how the headers are exchanged and what should be the algorithms to determine the information. However, maintaining an extra ODI routing table may lead to the robustness and the independence of the ODI process. The actual size of the required header in the NET layer is also not conclusive. Adding

extra bits in the header can be a significant burden in a constraint network particularly when the exchange must often be performed, the communication design must prudently consider the necessity of the extra requirements before proposing significant control traffic to manage the additional functionality. The practical implementation can clarify what is required in this layer and form the concrete concept that bargains the extra benefit with the burden on the resources.

APP Layer

The fundamental concept in the APP layer is defined in the existing literature as well, but it is mostly hypothetical. Nonetheless, it provides a template to develop a real solution in this layer. According to the current framework, the reserving the whole byte for only four variable choices or REQ/REP seems to overly spend the vacancy in the frame. Some of the defined processes may be able to merge into the same functional type. If the introduced headers (4 bytes) are comparable with the promising standard such as Constrained Application Protocol (CoAP) suggested by IETF (4 bytes without option and token), it is plausible to adopt the norm or a reduced functional framework of the standard. If the adoption of a common standard is feasible on top of the connectivity provided by ODI, this will motivate the practices of ODI and also promote the interoperability with other systems and Internet. Therefore, a practical case study of service exchange could reveal the precise conditions of implementing the APP layer compatible with ODI in real practices.

Even though the ODI concept has already been proposed and validated by simulations, some ambiguities and the feasibility of the concept in the real hardware need to be clarified by a practical implementation. Furthermore, the implementation may lead to significant improvements or a more efficient concept to enable ODI.

2.5 Summary

At the beginning of WSN research, WSNs are expected to be distributed wireless networks in multi-hop topology, realised by a large number of low-cost platforms. Consequently, there are a lot of theoretical proposes attempting to achieve the *smart dust* vision. As of today, WSNs have been tested in many application domains. However, the practices are still unlike the previous theoretical assumption. Therefore, a lot of theoretical works potentially wait for proofs with practical implementations.

In the overview of technology developments, WSNs can be seen as part of IoT research. Thus, there is a research trend trying to integrate WSNs with Internet standard. As IEEE 802.15.4 is widely accepted in WSN contexts, other standards are proposed to make data traffic from traditional Internet compatible inside low-resource networks such as 6LowPAN, RPL and CoAP. However, the complete integration of the Internet into

this solution encounter considerable arguments. This research suggests using ODI to promote local collaborations between co-located systems, which could be later integrated into global connections.

The ODI framework attempts to address the heterogeneity of communication protocol in WSNs. ODI can offer the flexibility in the system planning process, as the newly/previously deployed system can communicate with each other to share data or to build network services such as recovering lost sections, cooperative packet forwarding to increase network lifetime or to improve reliability by multipath connections. WSN applications can rely on an ODI to build application services, which only occur when networks are overlapped. The key principle of ODI design is considering the interoperability between WSN domains while limiting modifications and side effects on the original system design. Many words report the benefits of ODI. However, only a few works mention the conceptual design to achieve ODI in the sense that the network legacy to choose its protocol is preserved.

The basic foundation of ODI is established, but real practices of ODI still require more pushes. Most of RF modules in WSNs adopt the PHY definitions of IEEE 802.15.4. Although radio chips from different vendors have never been reported compatible with each other, the interoperability between them will be crucial for IoT developments in the future. If native networks still need to maintain its link protocol, the most efficient answer is the introduction of light-weight common protocol to act as mediator. This concept requires sensor nodes to apply multiple MAC protocols, which are already confirmed by previous works as feasible. Thus, the details of its implementation will be studied and applied in this research.

To enable ODI, there are two major functionalities which are vital in communication design: 1) Neighbouring Discovery Scheme (NDS) and 2) Cross-Boundary Transmission (CBT). OI-MAC is the only work directly focusing on the communication layer. This thesis considers the guideline, proposed by OI-MAC as the starting point of the practical implementation. OI-MAC suggests using a common protocol for cross-communication between domains. LPP (RI-MAC) is employed as base technique. An individual network keeps another protocol for internal communication. Also, OI-MAC provides the guideline for the NET/APP layer, although the proposed framework is a deductive solution providing the general idea of the framework. The details of the concept are still not given for an actual implementation. Nonetheless, OI-MAC is already validated partly by simulations. Therefore, the next critical step of pushing ODI to real practices is to find out the practical framework that provides a guideline for the implementation in the actual hardware and the proof of concept.

Chapter 3

Practical Validation of Opportunistic Direct Interconnection

The previous chapter summarises the related literature and concludes the motivation of the ODI concept and the current progress in the technical perspective. In this chapter, the existing contents of the ODI framework will be interpreted into the implementable details. The existing concepts will be used as the starting point to realising the system on real hardware. The practical solution is formulated by using the findings arising from the practical implementation to complement the existing concept following to the original intentions of the concept. The implementation process will be elaborated to show the process of the developments and the reasons behind amendments or new formulations as well as showing the guideline for the implementation. Then, the implemented systems will be evaluated regarding the correctness of the operations and the impacts on the resource spending.

The chapter is structured in the chronological orders. Section 3.1 elaborates the initial conditions of the implementation consisting of the analysis on the chosen experimental platform and the characteristics of the radio module. Section 3.2 will describe the implementation of the MAC layer, problems and solutions. Section 3.3 will reinvestigate the concept of the ODI framework in the NET layer to propose more realistic solutions in this layer. The implemented system will be used to build an interconnection between two distinctive systems. The operation of the framework will be shown in Section 3.4. Section 3.5 will analyse the energy consumption of the framework.

3.1 Initial Conditions of Implementation

This section discusses the given circumstances of the implementation. The discussion will provide the initial conditions that influence the details of the implementation. Some encountering problems are platform-specific. Nonetheless, the issues are the examples of the differences in the practices and the theoretical concept.

3.1.1 Consideration of Experimental Platform

This section considers the experimental platform, which can demonstrate the conditions of the ODI concept, the specific circumstance where the full standardisation of the IP-based solution is an impractical option. Even though this work aims to show the connection between heterogeneous domains, only one hardware model will be chosen in the beginning. In this work, the compatibility between RF module is assumed, the identical RF module, thus, fulfils this assumption, allowing the implementation to continue focusing on the communication layer.

Since the ODI concept targets the relatively low-level in the network hierarchical structure of IoT when the Internet connection could not reach the individual nodes, a platform with a low computational power and memory will be appropriate for the proof of concept, even though new platforms of WSNs are released with increasing memory and computational powers. Referred to Section 2.1.3, the author assumes that common platforms in WSNs may possess the relatively low-power MCU and a radio chip with PHY layer of IEEE 802.15.4. According to Section 2.4, ODI model by OI-MAC is a multi-channel protocol, using LPP to regulate ODI-related functions. Therefore, ODI poses the following prerequisites on hardware:

1. The transceiver must support carrier sensing algorithm (CS), which is required for Clear Channel Assessment (CCA).
2. The transceiver must support multi-channel protocols and is capable of hopping between frequency bands with acceptable delay and low energy overheads.

Texas Instruments eZ430-RF2500 [13] is one of the applicable options that are already available in the substantial number. This work considers two advantages of using eZ430-RF2500 as the experimental platform:

1. The eZ430-RF2500 device represents a relatively high constraint in the computational power and available memory, which is most likely to be the cases when the practices may diverge from the leading standard seeking a native communication design.

2. The eZ430-RF2500 device offers the opportunity to develop the communication from ground-up, unlike some platforms, which is focused on applications. The manufacturer publishes the software libraries for radio control given the insight into the technical aspect. Since the ODI concept tackles the problem at the low-level communication, it is necessary to possess the total control over the algorithms at the bottom end.

The components of eZ430-RF2500 have following attributes:

- The MSP430F2274 is the microcontroller of eZ430-RF2500. MSP430-F2274 possess maximum speed at 16-MHz. It can enter 5-level Low-Power Modes (LPM), by turning off unused board components [127], as so it signifies typical characteristics of the processor subsystem in WSN platforms. The available memory is very constraint with RAM at one kB and Flash Memory at 32 kB
- Other onboard components consist of an on-chip temperature sensor, ADC, and 12-kHz crystal oscillator. Additionally, it has 21 available development pins (I/O contractors) which separate to 4 digital I/O ports for external and internal functionality, by which I/O and inner workings signals can be easily observed. Using a Universal Asynchronous Serial Port (UART), it can be debugged and communicates with PC.
- It uses 2 AAA-batteries, thus requires voltage supply of 1.8 - 3.6 V with the standard reference value at 3V.

The integrated radio transceiver of eZ430-RF2500 is CC2500. The hardware performs the basic function at Rx/Tx. Hence, CC2500 is a packet-based radio. CC2500 [14] operates in 2.400-2.485 GHz bands. It supports 16 channels with channel hopping in 90 microseconds. The available features in CC2500 are sufficient for a wide range of communication protocols:

- It offers CS with continuous sampling of energy level. The carrier sense indicator can be retrieved from the RSSI status register all time except the reception process.
- CC2500 offers hardware packet handling of CRC (Cyclic Redundancy Check), FEC (Forward Error Correction), and DSSS. CC2500 captures the Link Quality Indicator value (LQI) and the Received Signal Strength Indication (RSSI) at the end of the frame reception. LQI describes the relative level of symbol deviations, which can represent the difficulty of the signal interpretation. LQI and RSSI can be exploited by control algorithm which can improve the link qualities [113].

MSP430F2274 connects with peripheral modules and CC2500 with SPI interface. Digital Port 1 is connected to a push button and LEDs. The push button can generate an MCU interrupt. The physical components of CC2500 are shown in Figure 3.1.

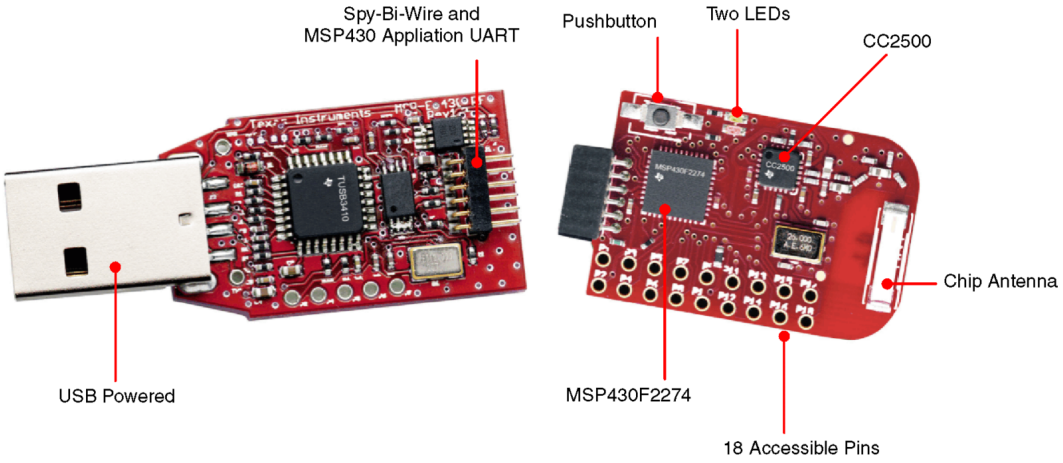


Figure 3.1: Basic architecture and existing features of eZ430-RF2500 [13]

3.1.1.1 Frame Reception and Transmission

The radio configuration leads to the Tx/Rx described by following steps:

1. Transmitting four octets of preambles which are the sequence of 0 and 1 bits (010101). Hardware automatically processes the preambles; the numbers of octets for preambles is configurable.

2. After preambles, four octets of a predefined SYNC WORD are required for byte synchronisations. After SYNC WORD, data will be dewhiten and decoded.

3. Then, Length Field is detected. Length Field indicates the packet length which can be an integer up to 28 in this setting.

4. Address Field follows length Field; the first byte of address field can be used for hardware address filtering. Therefore, packets are dropped in PHY level of Rx process for three reasons: 1) Failure of CRC check 2) Unrecognised Address Field 3) Packet Length Overflows (exceeds maximum length). If the reception is correct, LQI and RSSI will be added at the rear of the packet.

From the described process, the necessary headers of the physical connection are included: 1) Preambles 2) SYNC WORD 3) Length Field. 4) CRC. The physical frame format of CC2500 is illustrated in Figure 3.2. CC2500 positions the Address Field after the Length Field for automatic detection of unauthorised address, but the address filtering is disabled in this implementation because it is incompatible with the frame format of the MAC layer.

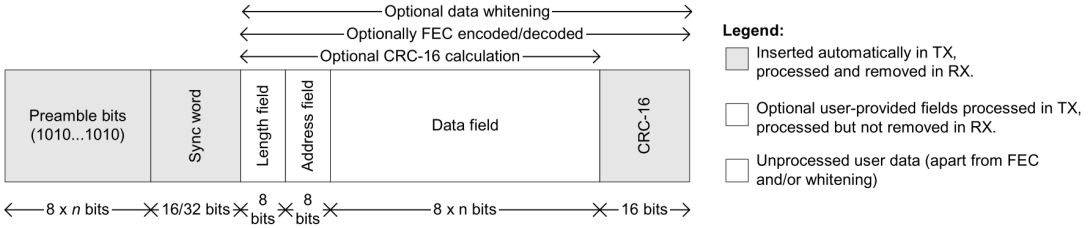


Figure 3.2: Physical Frame Format of CC2500 [14]

3.1.2 Implementation of Physical Layer

Section 3.1.1 elaborates the hardware conditions that influents the physical layer in the implementation. This section will continue explaining the concept of the physical layer and its overall characteristics. The implementation of the physical layer uses the library from the manufacturer (Texas Instruments) to control the radio functions. The library provides the reliable way for MCU to read/write the control registers of the radio chip via Serial Peripheral Interface (SPI) which composes the built-in core functions to control the radio. Following interface are expected from the physical layer:

1. Activation/Deactivation of the radio
2. Carrier Sensing
3. Timing operations (Ransom Back-off and fixed Delay)
4. Transmission control
5. Channel control
6. Reception Service Routine

This interface will be used by the MAC protocol to control the access to the medium by scheduling the Rx/Tx events according to each algorithm. The reception process is realised by an Interrupt Services Routine (ISR), which is invoked by the radio chip after a correct detection of SYNC WORDs (GD0 Interrupt). The flow of the reception routine is organised as shown in Figure 3.3.

According to the flowchart in Figure 3.3, the reception process classifies the outcome into a failure and success by observing the validity of physical frame format. The corruptions of a received frame shown in Figure 3.3 are regarded as a collision between parallel senders, which will activate the routine in the MAC layer to handle the collision. The correct received frame is passed to the MAC layer for further reactions.

Problems and Solutions

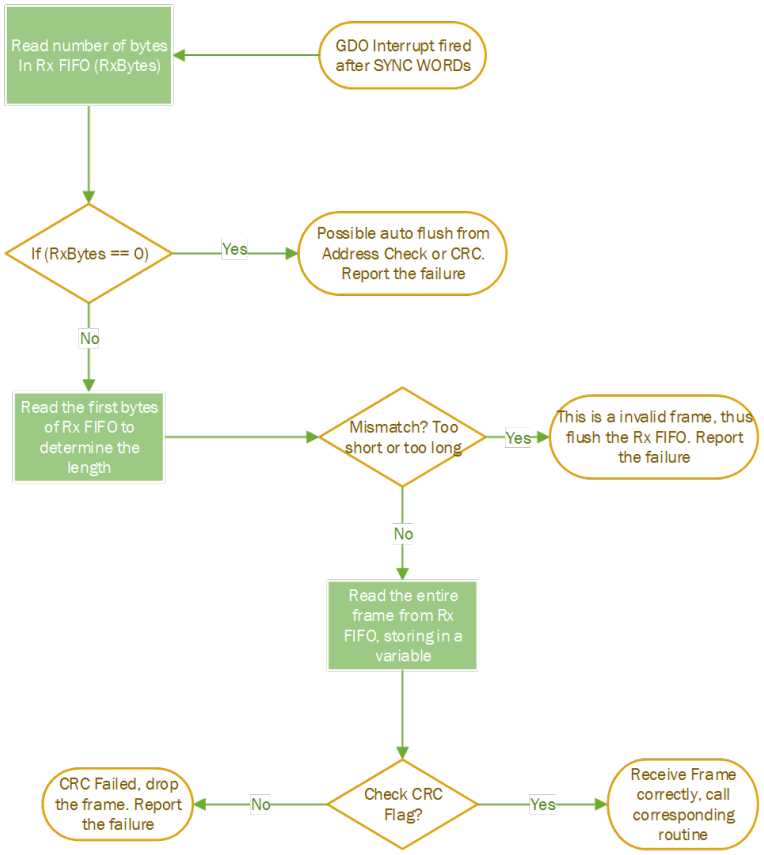


Figure 3.3: Flowchart of the reception routine showing the process to determine the outcome of a reception in different conditions

The discussion by far provides the insight into the concept and concrete details of the implementation in the physical layer. However, the potential problem is detected at this stage of the development. The radio chip relies on the frame corruption to detect the frame collision of the concurrent senders instead of the energy detection. This problem is particularly relevant because the MAC algorithm in the existing framework uses the collision detection technique to solve the contentions. Therefore, the characteristics of the collision detection by this hardware is investigated before progressing on the MAC layer. From the literature review, the radio can receive the frame correctly despite the collisions from different senders; the phenomena are called Capture Effects [112, 113]. According to Section A.2, the radio adjusts the gain control and frequency/phase corresponding to the received signal. Therefore, even another frame disrupts the bit transfer; there is a chance that the received frame will not be corrupted. To understand the circumstances, the experiment is performed by using two parallel contenders. The senders simultaneously send a frame the same receiver and measure the outcome. There are three categories of the outcome: 1) No Frame Detection 2) Frame Corruption 3) Successful Reception. The experimental result is shown in Table 3.1.

The interval (ϵ) is added between the contenders to show the effect of the jitter. When the frame transmissions from the contenders are perfectly aligned, the receiver cannot

Interval ϵ $[\mu s]$	***P_Case1*** [%]	***P_Case2*** [%]	***P_Case3*** [%]
0	99	1	0
128	26	44	30
256	3	55	42
384	0	44	66

Table 3.1: Evaluation of Collision Detection in experimental platform

detect any frame at all because the SYNC WORD is not received correctly corresponding to the radio characteristics in Section A.2. The small delay can increase the probability of detecting collision. Therefore, a small jitter is added before sending any frame to counter the problem.

This mentioned problem reflects one of the differences between real hardware and the concept. According to the discussion in this section, following notices on the physical layer can be implied:

1. The bandwidth of the signal is relatively limited, although the datasheet specifies the baud rate of the radio at 250 kBaud. However, under the consideration of the radio frame format, only 28 octets are available as the payload of the physical frame per transmission. The average transmission time is measured at 1.08 ms by a logic analyser, resulting in the actual physical data rate at approximately 26 kB/s under the ideal condition that all transmission is successfully received.

2. Since the performance of the hardware may vary in this aspect, the protocol design should proactively avoid the contention when possible instead of detecting and solving after it happened.

3. Since the feedback algorithm is used to eliminate the errors in the Tx/Rx process, the physical link may be more stable if the communication partner is not changed continuously allowing the control algorithm to stay on the static behaviour.

4. It should be noticed that several issues are still detected in CC2500 at the hardware level [128], and the manufacturer suggests the application to accept the packet error rate at 1 percent in normal conditions.

This section summarises the circumstances of the physical link provided by specific hardware as well as gives the comprehensive overview of the concept of the implementation along with the problems and its solution. The foundation for communication protocol is established. The details are further discussed in next sections.

3.2 Implementation of MAC Layer

The ODI framework promises to enable the connectivity between participants while allowing each participant to use the native communication protocols internally. The reviewed concept suggests installing a lightweight MAC layer used for inter-networking communication across domains. This section will discuss the principle and its implementation.

3.2.1 Virtual MAC Layer

The concept of Virtual MAC defines two parallel MAC protocols that operate separately by scheduling access to the same radio interface: 1) Internal MAC protocol, referred to the algorithms to control the access to the medium provided inside the domain and 2) Inter-networking MAC, defined as the standard MAC protocol used between participated domains. Two aspects are concerned in the implementation two MAC protocols in the parallel usage:

1. *The algorithms of both MAC protocols should proceed simultaneously without influencing the other.*
2. *The memory footprint of the implemented protocol should be optimised.*

Concerning about the points mentioned above, the MAC layer is applied by following guidelines:

1. The implementation adopts the concept of the event-driven architecture. Each MAC protocol defines the callback functions to handle the event of a frame reception and a frame corruption in the same universal interface. The MAC layer defines two operation modes: INTERNAL_MODE and ODI_MODE controlling the execution flow to mimic the behaviour of parallel protocols.
2. Promoting similar operations of MAC layer into a shared module that can be called by both MAC protocols. Some routines are common thus can be reused such as the random backoff, CS and ARQ.

For the beginning of the proof of concept, LPL with strobed preambles and LPP are chosen as an example of the internal communication protocol because both of them are asynchronous protocol and do not require a synchronisation between nodes. LPL with strobed preambles is selected because this MAC protocol is used by many of the common practices in TinyOS. Additionally, the operations of ContikiMAC [66] also resemble the operations of LPL with strobed preambles as ContikiMAC is a sender-initiated protocol and also repeatedly sends the DATA frame until the intended receiver recognises the

transmission. Both middlewares are common in the academic and commercial areas. Therefore, the ODI scheme with LPL with strobed preambles as the internal communication should approximately reflect many real practices, promoting the possibility of the reimplementation in the other environment.

3.2.2 Opportunistic Direct Interconnection MAC Protocol

The algorithms used by communication between separate domains are at the centre of the ODI framework. Therefore, a careful consideration in this part is crucial to push forward this concept to the practices. In this section, the concept of the ODI protocol is investigated by the implementation. Since OI-MAC (see details in Section 2.4) is proposed as the ODI protocol in the existing literature, this work attempts to implementation OI-MAC from the theoretical concept and discusses the problems and the solutions during the implementation process.

3.2.2.1 Shortcomings of Existing Concept

Before implementation, the theoretical concept must be developed to an implementable model. During the interpretation of the OI-MAC concept into an implementable algorithm, following issues are detected preventing the completion of the practical framework:

1. ***Collision Handling in Discovery Scheme*** As Active Discovery and Passive Discovery are defined now, the collisions in the discovery process are systematic because the neighbouring nodes are waiting for the same advertising packet.

2. ***Details of Handshake Process*** The proposed concept only set a vague definition of handshake process. There are no specific details of how and when exactly this handshake should happen, what type of information should be exchanged, and how to retrieve the relevant information. Before the further process, the precise algorithm must be outlined. The set of relevant information in the handshake process must be clarified.

3. ***Inefficiency of the channel usage*** The proposed concept reserves more logical channels than necessary for its functions. It demands an extra reserved channel for each participant. This strong requirement could be fatal for the systems that use multiple channels for its internal communication.

4. ***Bidirectional or Unidirectional Communication in CBT*** According to the concept of ODI, the data should flow in both directions in one encounter. BN must exchange frames not just be a receiver or sender. However, the original concept of

LPP precisely defines the receiver and sender, thus only let the flow of data in one direction from the sender to the receiver.

5. ***Loss of Connection*** The original content did not explicitly define when and how to deem a loss of connection and how to handle it and what to do after the connection is lost.

To complete the framework, the implementation assumes the best possible options, according to the intention of the ODI concept. Section 3.2.2.2 will discuss the solutions to the mentions issues.

3.2.2.2 Solving Problems and Ambiguity

Considering the necessity and the original intentions of the concept, following solutions are adopted in the implementation:

1. ***Contention in discovery scheme*** The first issue in NDS is the systematic contentions of neighbouring nodes waiting to answer for the same discovery frame. The implementation will reuse the contention solving algorithm of LPP in the neighbour discovery scheme as well.

2. ***ODI reserves only one common channel (CCH)*** Logically, ODI should not use the channel capacity more than necessary since the cooperation is only a secondary objective of the interested participant. Therefore, ODI should impose negligible side effects on the internal communication. Also, by reserving only CCH, the overhearing can be used to inform the new participant about the availability of the neighbouring domains. This solution can reduce not only the requirement on the reserved channel, but it also reduces the complexity and energy consumption.

3. ***Handshake process*** According to the existing concept, the handshake process is only a general definition concerning any information exchange after a neighbour detection. However, this concept must be redefined in the boundary of the MAC layer. Therefore, the information exchange in this context must involve only the information that can be immediately exchanged. This information should come firstly from the PHY/MAC layer in addition to some piggybacking information from the NET layer. Further application exchange must be out of the scope of this concept such as the resource/service discovery. The relevant information captured from the implementation process are summarised in Table 3.2. Some of the information in Table 3.2 can be embedded in the discovery frame depending on the maximum frame length of the discovery frame. At least MTU/PERIOD should be included in the discovery frame. Other remaining information can be transferred later. The handshake process according to the MAC layer concept

FIELD	LAYER	DESCRIPTION
MTU	PHY	Maximum physical frame length.
PERIOD	MAC	Interval between consecutive ODI processes.
CAPACITY	NET	A maximum number of data frames per event.
HOP	NET	Hop distance to the management node.
PREFIX	NET	Network prefix.

Table 3.2: Information exchanged in Handshake process

should end here. However, the negotiation process concerning the application layer can begin if the handshake is deemed as stable. The conditions of the handshake stability are the number of the persistent consecutive detection of the neighbour. BN counts the detection of the same neighbour domain until the count reaches a set threshold before updating the detection to the domain.

4. ***Modification to support a bi-directional link*** Originally, LPP is designed for packet forwarding in WSNs. However, the data exchange is likely expected in ODI. Thus, the implementation modifies the LPP process allowing the bidirectional communication between BNs.

5. ***Set the criteria for the detection of a lost connection in ODI*** This implementation defines the loss of the ODI connection by a specified number of consecutive failures of the data transfer. The node will report the NET layer about the loss after it is a confirmed status.

3.2.2.3 Implementation of OI-MAC

After outlining the details of the framework, this section shows the end stage of the protocol as it is implemented. The contents begin with the frame format definition and the relevant terminology. Then, the process flow of the protocol will be discussed to demonstrate the algorithm in the implementable form.

Frame Format

The protocol defines three distinctive frame types as follows:

- *TYPE_ODI_BEACON (TYPE 01)* is used to begin any conversation including the neighbour discover. The handshake information can be embedded in this frame. It also uses for inviting a transmission from senders.
- *TYPE_ODI_DATA (TYPE 10)* carries the payload contents.
- *TYPE_ODI_ACK (TYPE 11)* confirms the outcome of a DATA reception.

The frame header includes the following information:

- *Frame Type* specifies the function of the frame.
- *ODI_FLAG* is used to identify the ODI frame. It is always set to one in the ODI process. However, this particular field must also be included in some reserved field of the frame definition of the internal protocol to distinguish between the internal DATA frame and the ODI frames.
- *R_FLAG* indicates that the receiving node should expect more DATA frame.
- *D_FLAG* indicates that there is piggybacking data in the control frame.
- *Data Sequence Number (DSN)* is used for the acknowledgement DATA and ACK frames.
- *Tx/Rx Address* specifies the sender/receiver. The ODI framework requires the node of the participant to possess a 2-byte address.
- *ODI PERIOD* indicates the time between two consecutive ODI processes.

Figure 3.4 describes the frame formats covering of the defined frame types.

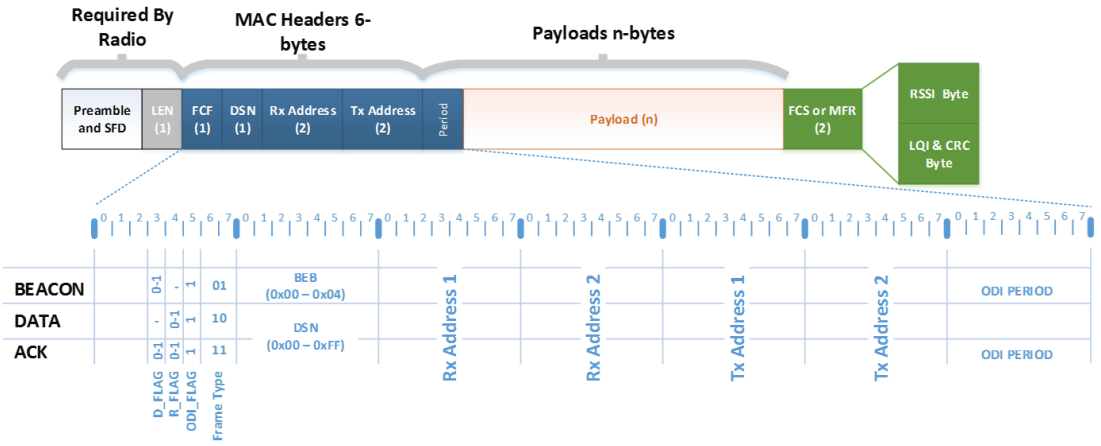


Figure 3.4: Frame formats of each frame type defined in the implementation of OI-MAC

The MAC headers use six octets from the available payload from the physical frame at 28. Therefore, 22 bytes is the payload size of the MAC layer. The control frame types can carry the payload from the NET layer when the NET layer requires an extra information exchange. When the piggybacking payload is available, the D_FLAG field is set, the MAC layer will forward the payload to the NET layer.

Process Flow of ODI related Functions

The ODI process composes of two functions: 1) Neighbour Discovery Scheme (NDS) and 2) Cross-Boundary Transmission (CBT). In principle, the ODI process occurs periodically but should not impose an exact timing of the operation. The node sets a

counter to time the ODI event. However, it will pull an ODI event only when the node is in the sleep state otherwise the ODI event will only set a pending flag waiting for the main thread to pull the process later. When the ODI process is pulled, it will proceed according to the flowchart in Figure 3.5. The flowchart in Figure 3.5 shows the concrete

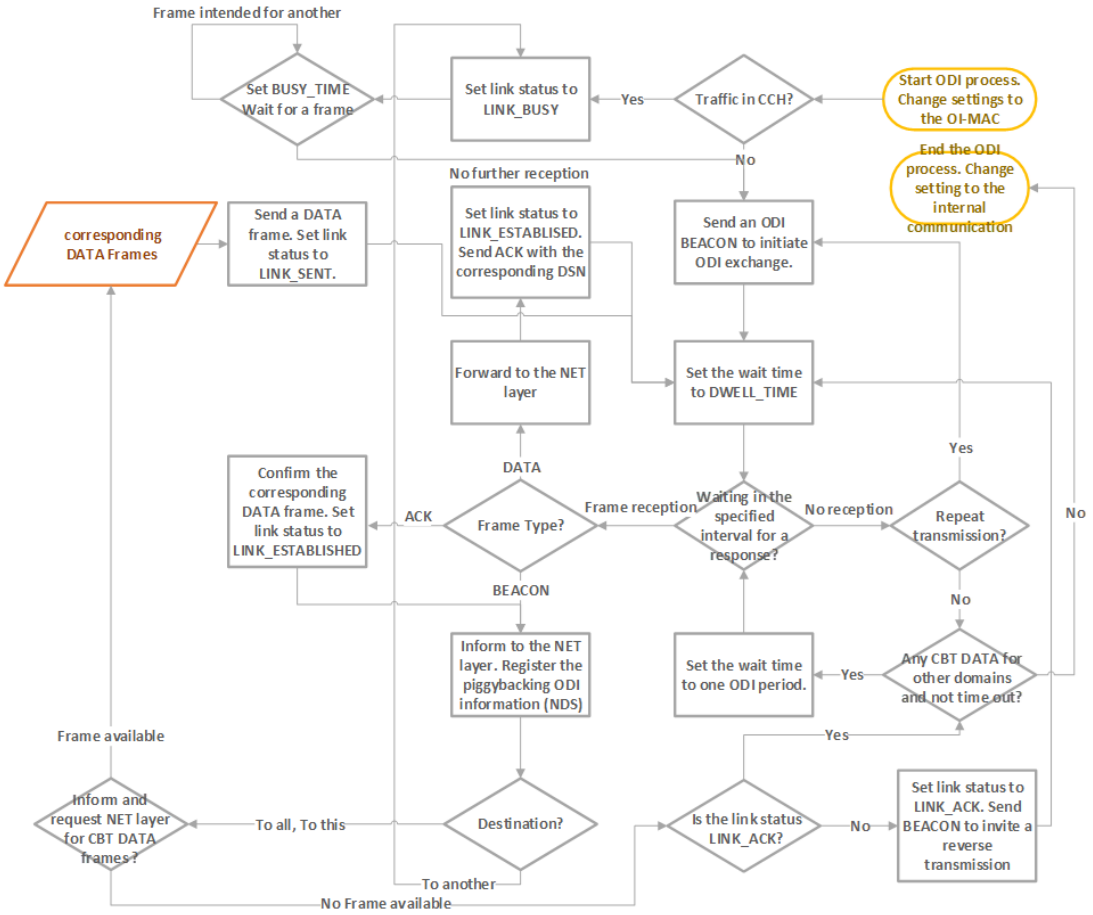


Figure 3.5: The flow chart of the ODI process covering NDS and CBT

form of the algorithms used by the cross-network communication. However, some details must be left out for the sake of the readability. This algorithm covers both mentioned ODI functions. In the overview, the process can be described as follows:

1. In each ODI process, which happens periodically, the node sends an ODI BEACON after sensing the channel to search for any node waiting for an ODI exchange.

2. After sending ODI BEACON, the node actively waits in CCH for any response. If the node receives any ODI BEACON/ODI ACK from another domain, according to the algorithm, it will search for any corresponding DATA frames to send back. Regardless of the data exchange, it always answers once by its ODI BEACON. After answering, the node sets the link status to remind that the BEACON is already answered to prevent the endless loop.

3. Under any circumstance that the frame for another node is received, the node waits until the channel is free by active listening.

4. If there is no response from other nodes in the set time frame, the ODI process comes to an end. At the end process, if the node did not receive any response, this missing encounter will be reported to check for a lost connection.

The described process is universal for NDS and CBT. The BEACON exchange is referred as the handshake process when the node encounters the neighbour domain for the first time. Then, the node may response any ODI BEACON by its available ODI DATA frames. However, it still sends its ODI BEACON at least once to the communication partner.

The MAC layer also keeps the record of the pairing status. When the pairing status is changed, the protocol will set the count to evaluate the certainty of the status change. It reports the NET layer when the pairing status is confirmed for further processes.

3.2.3 Discussion on MAC Layer

This section describes the formulated concept of ODI learned by the implementation. Many ambiguities have been solved in the process. The significant changes in the concept of the MAC layer are the reduction on the reserved channel, the new formulated details of the handshake, the concrete frame definition, the capability to support a bi-directional communication and the procedure for the loss of the connection.

Currently, the validation of the ODI concept implements OI-MAC as the cross-boundary protocol in the existing ODI framework. However, this result shows the considerable differences between the concept and the practices. It, therefore, motivates more validations in the other aspects. Because the protocol of the cross-boundary communication in the MAC layer is the main component that controls the performance of the ODI framework, this research will reconsider the MAC algorithm used for the cross-boundary exchanges in a separate chapter. This chapter will continue on the overview of the framework and discuss the implementation of the NET layer.

In the viewpoint of the MAC layer, the Tx/Rx address implicitly indicates the SRC domain and the DST domain, because the NET layer keeps records of the BN address and the corresponding NET ID, which can be used to refer the identity of the domain. The necessary information about ODI in the NET layer will be discussed in Section 3.3.

3.3 Implementation of NET Layer

According to the implementation, the proposed concept in the NET layer must be reconsidered. The implementation reveals unnecessary requirements in the NET layer that can be avoided. In this section, the concept of the NET layer in the ODI framework will be reformulated to match with the realistic requirements found by the practical implementation. The section also shows an example of a simple routing protocol that conforms to the requirements.

1. In the assumption, that the nodes inside the domain are reduced function platform with constraint resources. The application procedures in ODI schemes should commonly be centralised. Thus, the route between MN to MN should be optimised.

2. Routing algorithms of WSNs are optimised for packet forwarding to a defined set of gathering points rather than a P2P connection as examples of CTP [129] and RPL [130], therefore the default destination of cross-boundary data should be MN.

3. In ODI scheme, overlapping of network coverage is opportunistic. Therefore it should be a logical assumption that the knowledge of the neighbouring topology is unavailable. Therefore, MN should be responsible for the initiation of any services/resources.

4. When a service is already initiated, the application data traffic may involve any specific endpoints in the associated domains.

5. Considering the scope of ODI (see Section 2.3.2), the concept is designed for the cooperation between network domains with a possible direct connection. Therefore, the NET layer should not directly support a routing between hidden network domains.

Figure 3.6 visualises the mandatory route and optional route in the ODI scheme. To realise the formulated requirements, the concept of the NET layer in the ODI framework is defined as follows:

1. BNs must maintain an extra table to record the discovered NET ID in the relation with the 2-octets address of the paired BN. The NET ID must be universally unique. In the assumption that MN possesses a unique IPv6 address as an example (4200 :: 0), the domain prefix (4200 ::/48) in IPv6 may be used as NET ID. A compact 2-byte NAME must be defined inside the domain as a reference to the neighbour. The table also keeps the records of the relevant information including the MTU, the estimated frame capacity of the intermediate node in the domain, and the hop distance. This information is carried along in the ODI BEACON/ACK frame, as shown in Table 3.3.

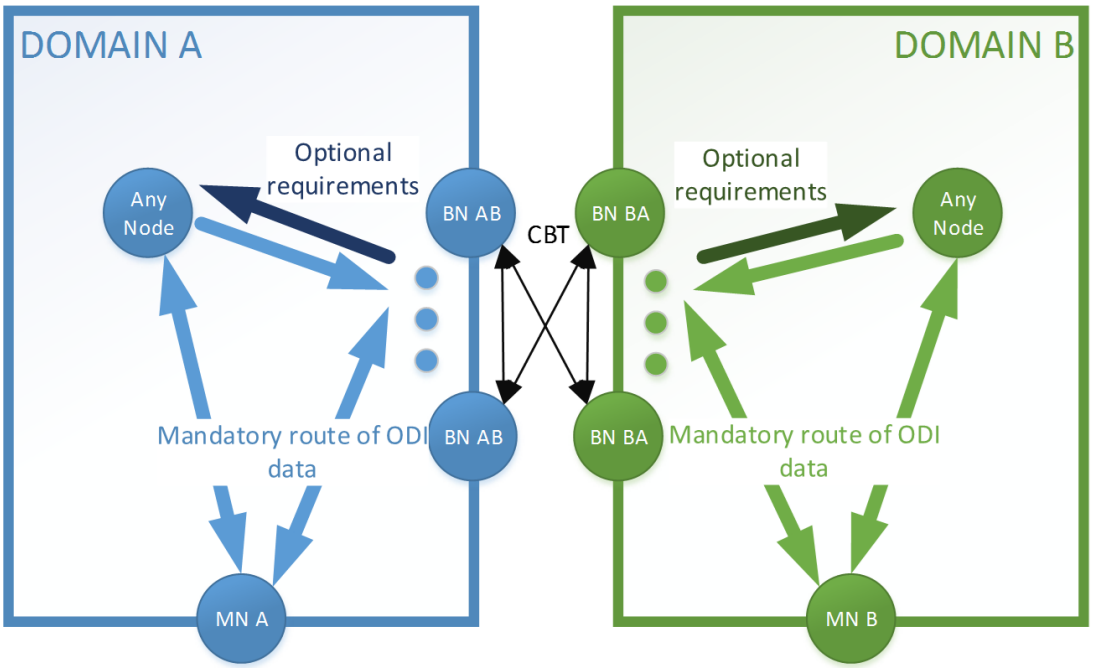


Figure 3.6: The conceptualised requirements on the routing protocol which can be used in ODI schemes

BN	NET ID	NAME	MTU	Capacity	Distance
2 bytes 4105	2 – 14 bytes 4200	2 bytes 4242	1 byte 28	1 byte 10	1 byte 5

Table 3.3: ODI pairing table recorded in BNs

2. The ODI DATA frame includes *passID* in the frame definition. The *passID* specifies the destination of the data. The default value at zero implies the default destination. The cross-boundary data is assigned to MN by default. However, the communication between any endpoints can be achieved by using a unique *passID*. MN performs the concept of the *passID* in a centralised manner.

3. MN can enact *passID* (uint8_t) for a particular traffic (such as observable resources) which specifies the destination other than MN. MN put the *passID* record to the *passID* table stored by BN. The BN must label all ODI DATA sending across the boundary with the *passID* so that the BN from the other side can look up the *passID* table for its associated address (ADDR).

4. Any other node inside the domain communicates only with the MN/BN. There is no need to modify anything in the original NET layer. Any associated endpoint can address to the other domain by assigning data to the BN inside its domain. The ODI data is not forwarded in the same way of the internal data. However, the frame definition must add only 1 bit of the ODI flag in any reserved space, so that the associated endpoint can distinguish ODI frames from the internal frames.

The BN then looks up the PASS table to find the *passID* that matches the node address. BN attaches the *passID* to the ODI DATA before sending the frame across the boundary.

Figure 3.7 shows the following diagram when the passID is used to find the routing destination between domains. In this way, the concept of the NET layer utilises only the

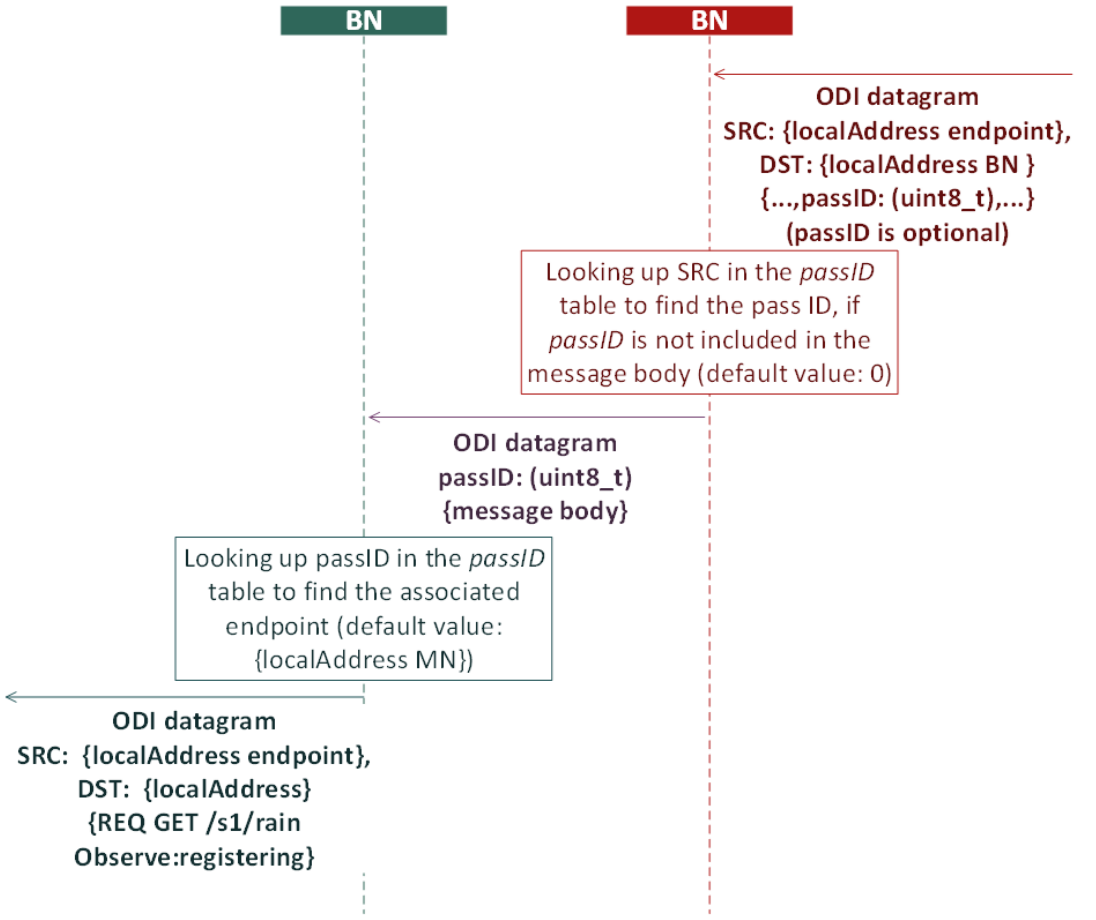


Figure 3.7: BN uses the tagged passID to look up the associated endpoint of ODI datagram that is sent across the boundary.

minimum memory resource and do not require any modifications to the original routing protocol. Almost options of the existing routing protocol fulfil the ODI requirement such as RPL and AODV as long as the forwarding routes between base station and any nodes are supported. However, this concept assumes that the node does not need to know the identity of the partner from the other domain. BN acts as a proxy between endpoints in the other domain. The decision in the security aspect is centralised. The MN must approve the traffic before the P2P connection between nodes is enabled. The routing algorithm used in this implementation is explained in Appendix B. the routing protocol is not the focus of this work. The implemented routing protocol is only an obtainable example in the technical aspect since the implementation must include a functional routing algorithm that can support the traffic in the ODI framework.

This research attempts to build a functional system based on the existing details in the conceptual framework of ODI as far as possible. The lesson learned from the implementation corrects the ambiguities and missing details in some part of the framework and even lead to a formulation of the new concept. The requirements initially claimed by the ODI framework is considerably lessened.

The details of the MAC layer in this current state is consistent enough for a guideline of an implementation. The handshake process is redefined in the boundary of the MAC layer separated from the negotiation process in the application layer. Since the implementation reveals considerable differences from the existing concept, this research decides to proceed the evaluation of the MAC layer further into the aspect of the suitability of the chosen protocol. Chapter 4 will solely discuss this aspect. This chapter continues with the overview of the framework in the order. The concept in the NET layer is redefined to match the actual requirements observed by the implementation. According to the newly defined concept of the NET layer, the burden on the original system is significantly lessened. The intermediate node NET layer is almost untouched except for some nodes that become BN. BN must maintain some extra ODI information to communicate with other nodes in the behave of the neighbouring domain. This chapter discusses only the communication layers up to the NET layer. The application layer is still not covered in this chapter because of its volume of the contents. Chapter 5 will solely focus on the application layer.

3.4 System Evaluation

In the discussion in this chapter so far, the details of the implementation and the concept of the ODI framework is elaborated. This section evaluates the correctness of the system operations and the impacts of the ODI framework regarding the consumed energy.

3.4.1 Experimental Setup

In this experiments, the practical ODI framework is implemented in a testbed with 12 eZ430-RF2500 nodes. The scenario is described by two overlapping domain of WSNs, each of them composes of 6 identical nodes. Each domain uses its protocol stack, modified to support ODI. Each network monitors ambient temperatures in the area. The generated data packets are relayed to its SN, which links to a PC via UART. At the initial phase, each domain is unaware of each other. Figure 3.8 illustrates the scenario in the experiment.

In this experiment, Domain A employs LPP as the internal MAC protocol, while Domain B uses LPL with strobed preambles. Each node in Domain A and B generates a packet in every 6 seconds. Both operate in their separate logical channel. Domain A is already

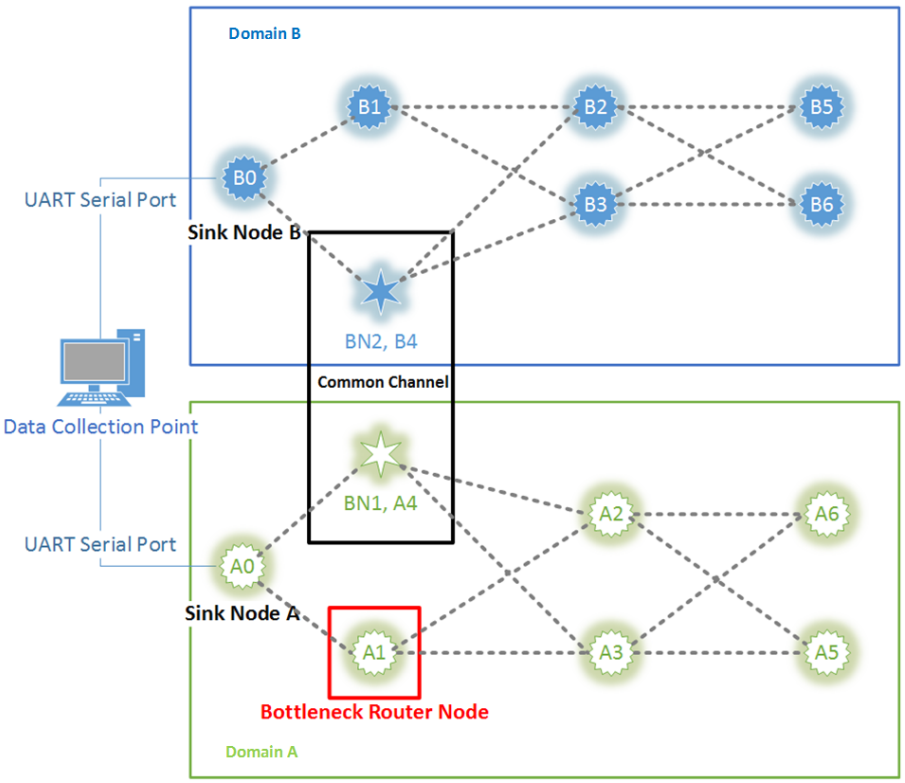


Figure 3.8: Network A and B define its protocol stack, unaware of each other. The experiments observe internal network operations, ODI processes and energy consumption.

deployed; therefore, Domain A periodically performs Passive Discovery in NDS. Domain B is deployed later. At the initial network setup, Domain B performs Active Discovery, one pair of nodes from either side are associated and becomes BN. From this experiment, the obtained results are separated by two aspects:

1. The operation sequence will be observed and analysed. The results are achieved by capturing the digital signal with logical analyser to demonstrate the operation in forms of timing diagrams. The obtained diagram will be analysed, compared with the theoretical expectation (see details in Section 3.4).

2. The energy consumption of ODI will be evaluated. The energy consumption of NDS and CBT process are analysed, compared with internal network activities (see details in Section 3.5). Due to this, relative data flow in CBT is expressed by *injection ratio* (α), which is defined by following expressions:

$$\alpha = \frac{number\ of\ injected\ packet}{number\ of\ generated\ packets} \tag{3.1}$$

However, the collective network performances of the framework are still not formally captured since this thesis intends to reinvestigate and improve the cross-boundary protocol of the framework.

3.4.2 Evaluation of System Operations of Internal MAC Protocols

Since LPP is employed as the internal MAC protocol of Domain A and LPP is also the primary technique in ODI, the operation of nodes, performing LPP, must be observed and analysed. To get the well-covered resolution, Sleep period is relatively shortened and Dwell Time is set relatively longer than the typical operation. Nonetheless, this still maintains the duty cycle of radio at 0.0625. System parameters are set as Table 3.4:

PARAMETER	VALUE
SLEEP PERIOD (CYCLE)	512 [ms]
DWELL TIME	32 [ms]

Table 3.4: Parameter Setting of LPP Operation Testing

Timing diagrams of LPP process are shown in Figure 3.9. The first channel indicates the state of MCU either Active or Sleep. The second and third channel present the state of radio. CC2500 defines 4 states of radio [14]: (1) Receiver-on (Rx-On) (2) Idle-state (3) Radio-sleep (Off-state) (4) On-transmission (Tx-On). The radio can receive packets only when the receiver is turned on (Rx-On in the timing diagrams) since the amplifier is turned on (therefore, consumes more power than the Idle-state). Rx-Off in the diagrams is equivalent to Sleep-state of radio, while Tx-On in the timing diagrams indicates that the radio is sending a packet.

From Figure 3.9, following LPP operations can be tracked.

1. In Process A, Node X performs LPP Scanning Routine. MCU turns on Rx, sending out a beacon. Rx is on for Dwell Time. MCU wakes up and turns off Rx.
2. Process B is performed by Node Y, equivalent to Process A. Node Y then waits for Rx beacon in Process C.
3. In D, Node Y send its data frame after receiving a beacon. Due to technical constraints, the reception cannot be directly captured, since the same port is used for generating several interrupt routine other than the reception. However, the beacon can be seen in the transmission process of Node X. In E, Node X receives the data frame, therefore sends ACK back.

From the timing diagrams, LPP operations are successfully implemented, captured operational sequences followed the theoretical expectations. As the same module of LPP is used for ODI operations as well, therefore the results are positive for NDS and CBT implementation.

LPL with strobed preambles is another internal MAC protocol, chosen by Domain B. To promote reusability, LPL is implemented by using the same elementary functions in MAC module. The parameter setting is chosen as shown in Table 3.5.

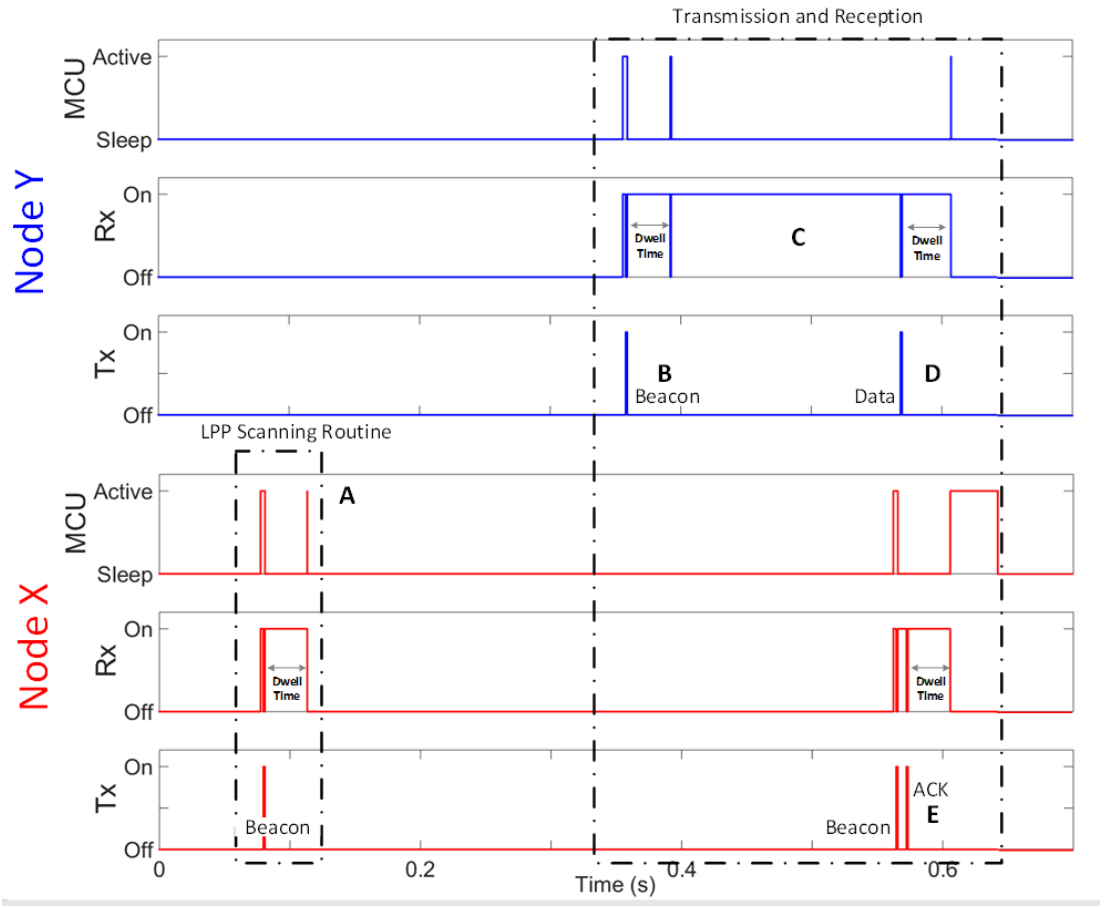


Figure 3.9: Experimentally obtained timing diagrams, showing LPP Operation Sequences in scanning routine and Rx/Tx routine

PARAMETER	VALUE
SLEEP PERIOD (CYCLE)	512 [ms]
SAMPLING TIME	16 [ms]

Table 3.5: Parameter Setting of LPL Operation Testing

Sampling Time is the interval, in which nodes samples channel at waking up. The setting results in the duty cycle of radio at 0.03125. The operations of LPL with strobed preambles are captured and shown in Figure 3.10. The operational sequences Figure 3.10 can be described as follows: 1) In A, Node X samples the signal for 16 milliseconds. MCU wakes up in a very short of time to turn on and off the radio. 2) Process B is equivalent to Process A. The same LPL sampling is performed by Node Y before Node Y transmits a sequence of strobed preambles in C. 3) Node X Replies Node Y with a beacon to signal data transmission. Node Y sends data frame, and in D, Node Y sends ACK as a response. The operations of LPL and LPP exhibits the behaviour of the theoretical as expected. ODI processes reuse LPP modules to implement. In the next Section, NDS and CBT will be observed and investigated.

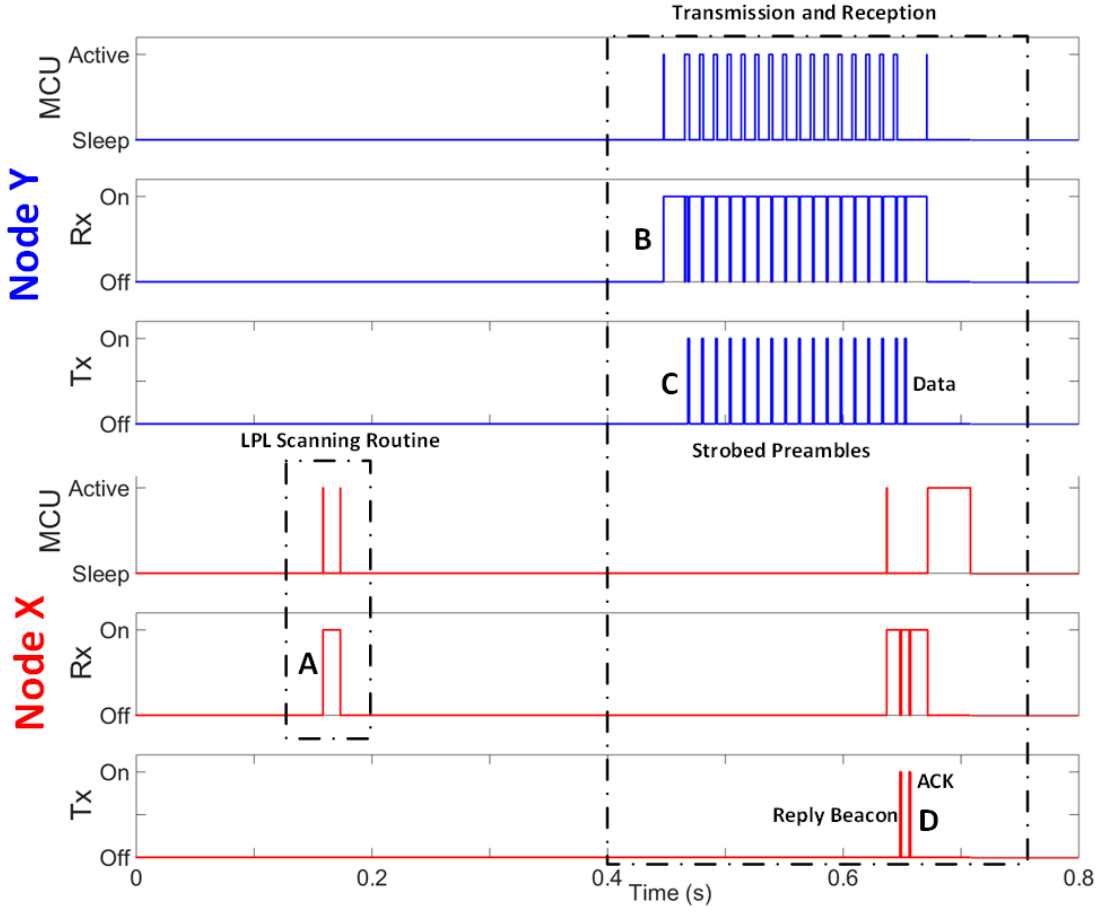


Figure 3.10: Experimentally obtained timing diagrams, showing Operation Sequences of LPL with strobed preambles in scanning routine and Rx/Tx routine

3.4.3 Evaluation of ODI Operations

According to the scenario, Domain A and B are engaged in ODI scheme. A is deployed before therefore each node in A perform Passive Discovery. At the deployment, B executes Active Discovery. A4 (BN1) in Domain A and B4 (BN2) in Domain B are in each other range, demonstrated in Figure 3.8. It is expected that both nodes will be associated and become BNs. To show the explicit sequence in the timing diagram, related system parameters are set as shown in Table 3.6. This parameter setting is

PARAMETER	VALUE
SLEEP PERIOD (CYCLE)	512 [ms]
DWELL TIME	32 [ms]
SAMPLING TIME	16 [ms]
Active Discovery (T_{Active})	20 [s]
Passive discovery ($T_{Passive}$)	12 [s]
ODI period (T_{ODI})	12 [s]

Table 3.6: Parameter setting in ODI experiments

chosen, as it practical to observe the implementation process. However, if the efficiency of energy consumption is considered, the parameter setting of NDS, Active and Passive discovery is calculated, based on the operational period of the system (see details in Section 3.5.2). Passive Discovery is set shorter than Active Discovery to guarantee the overlap of both processes. The ODI period is chosen at 12 seconds in this example, but the ODI period should be adaptive depending on the data traffic.

In the experiment, B4 performs Active Discovery, while A4 executes Passive Discovery in CCH. The pairing event is captured at the time about 7.88 seconds after Domain B is initialised. The captured timing diagram is illustrated in Figure 3.11.

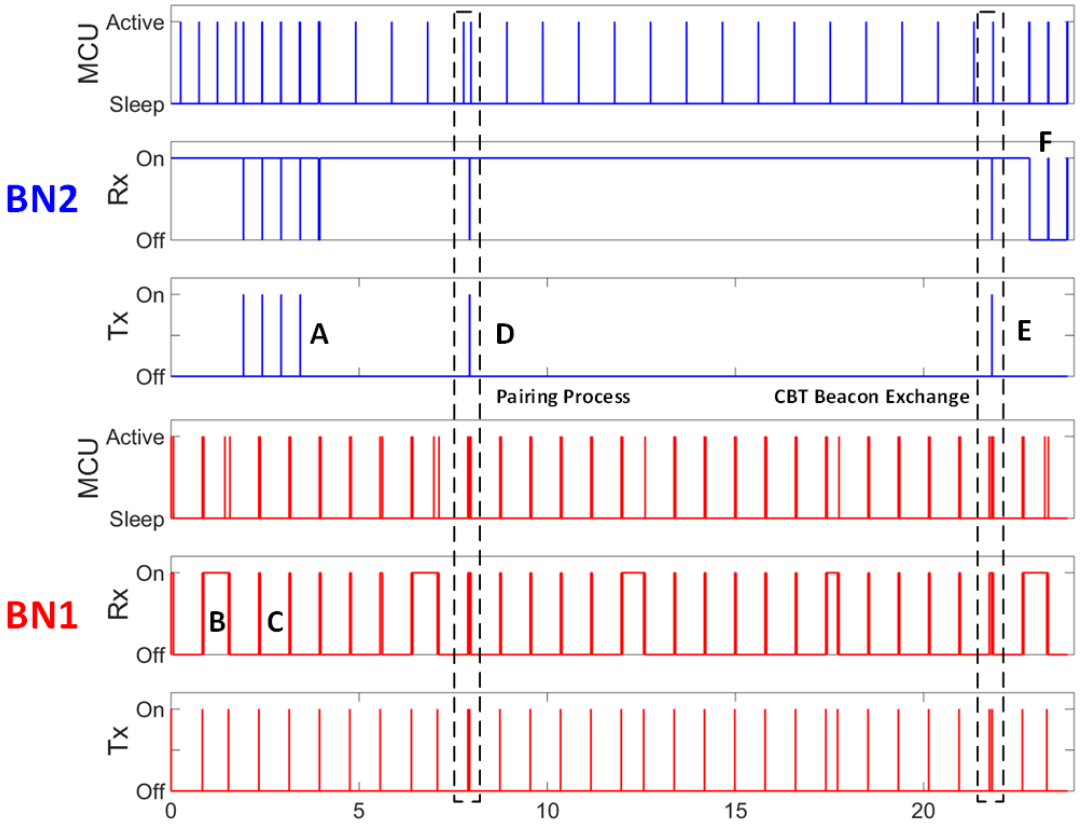


Figure 3.11: Experimentally obtained timing diagrams, showing Operation Sequences of LPL with strobed preambles in scanning routine and Rx/Tx routine

From Figure 3.13, the events can be described as follows:

1. Domain B initialises the routing protocol; broadcast frames can be seen in Process A.
2. After initialisation, BN2 switch to CCH for Active Discovery.
3. Process B and C are the common internal operations in Domain A, which uses LPP inside its domain.

4. The pairing process happens at point D around 7 seconds after B is initialised. The details of pairing process are demonstrated in Figure 3.14. After Event D, BN1 returns to common operations.

5. Around 12 seconds after Event D, BN1 attempts ODI, but because there are no ODI packets, only ODI beacon is exchanged.

Figure 3.12 shows Pairing Process in the smaller scale. The X-axis begins at 0, which equivalent to time 7.88 seconds, in Figure 3.11. Following events happen at the time of

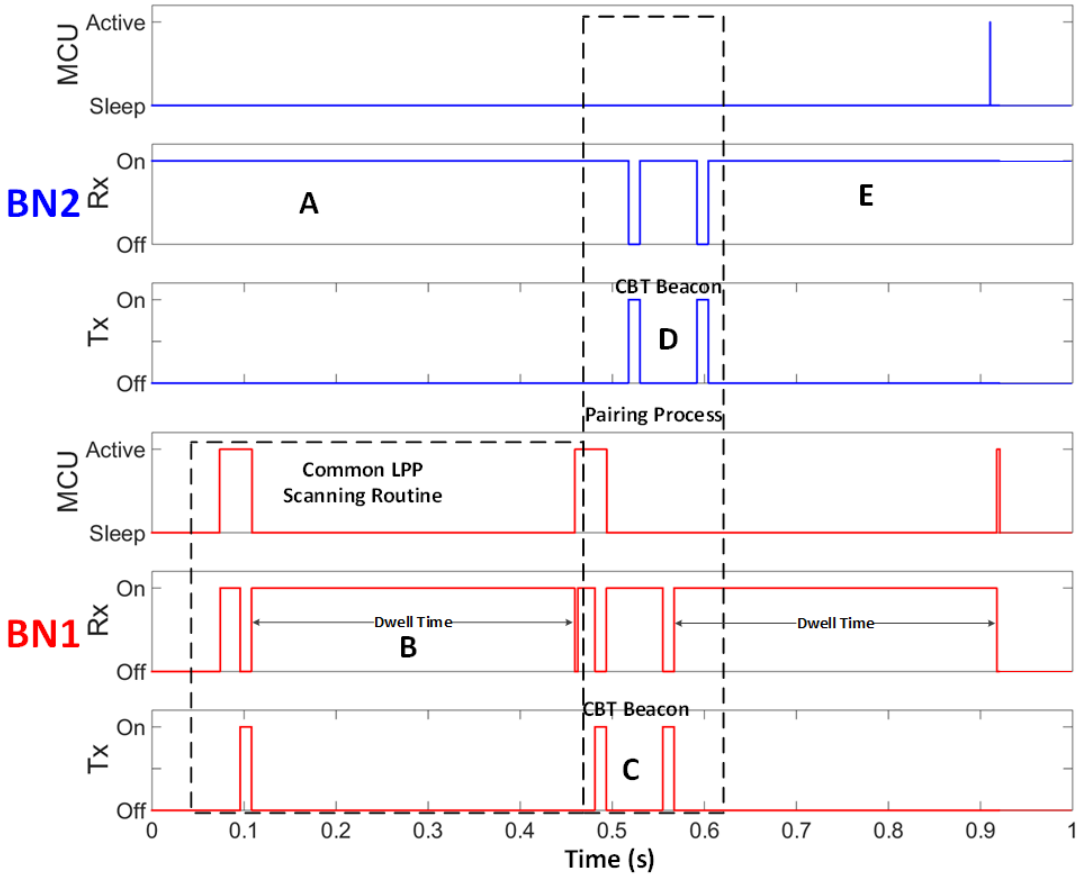


Figure 3.12: Experimentally obtained timing diagram illustrates details of pairing process

pairing process:

1. At Point A, BN2 listens to CCH channel. BN1 wakes up and scan the DCH in Domain A, in Event B.

2. BN1 switch to CCH after performing its ordinary routine, sending ODI Beacon, at Event C. BN2 responses with ODI Beacon. Pairing is successful, at Event D. BN1 sends out another Beacon, which is regards as loads in ODI transmission. BN2 responds with ODI-ACK.

3. After ODI Beacon exchange, BN2 continues performing Active Discovery, while BN1 waits for another Dwell Time, before return to intra-network activities.

After BNs are associated, ODI processes begin in this experiment the injection ratio is set at 0.5. Half of generated packets are ODI packets. The data is generated at the rate of 16 seconds per Sample. BN1 and BN2 are responsible for internal routing and cross-boundary transmission. BN1 is in Domain A, using LPP internally. BN2 is in Domain B, employed LPL with strobed preambles. In regular basis, BN1 and BN2 switch to CCH for ODI activities. In Figure 3.13, the cross-boundary transmission process is demonstrated.

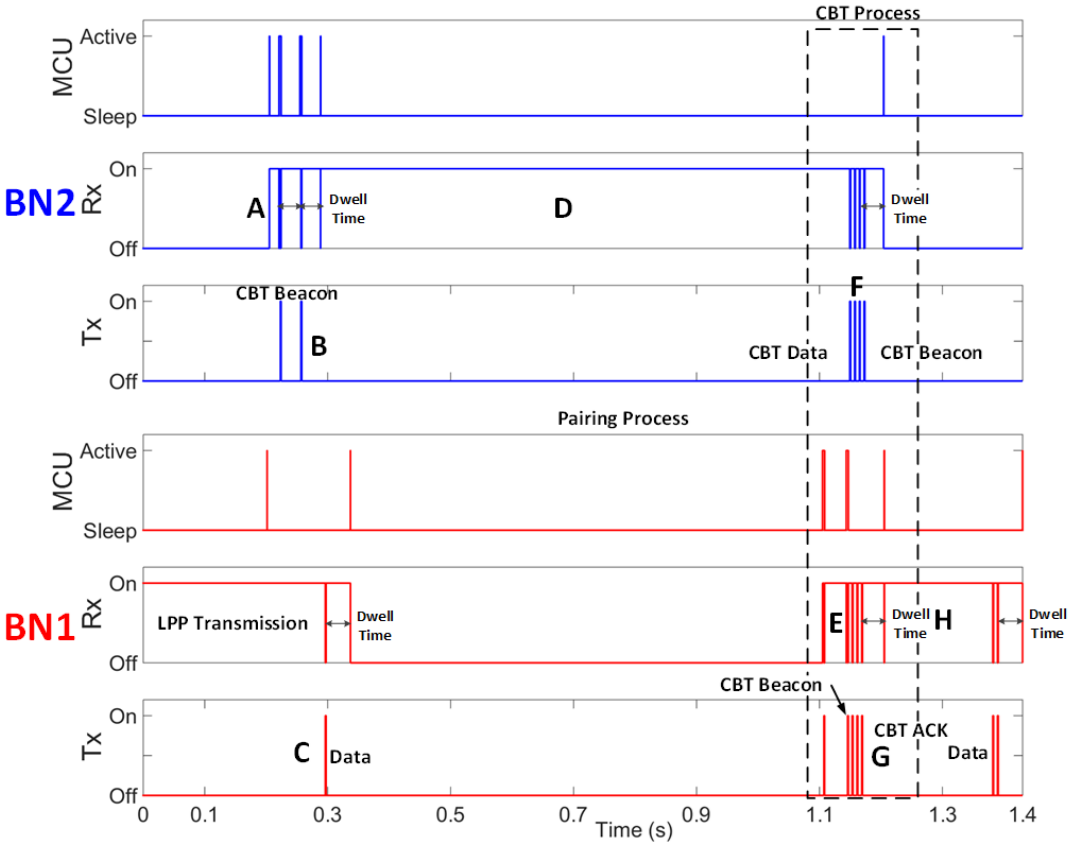


Figure 3.13: Experimentally obtained timing diagram illustrates details of CBT processes

From the above figure, following sequences can be seen:

1. At Point A, BN2 wakes up, sampling CCH for 16 ms, then at Point B switches to CCH and sends out ODI Beacons two times (Double transmission is intentionally set to prevent lost connections because of failures in Tx or Rx processes). It then waits in CCH for cross-boundary transmission with no reply in Event D.

2. At Event C, BN1 is in the Rx process of LPP. It then sleeps for one sleep period. In Event E, BN1 wakes up, performing its scanning routine in DCH-A, then switch to CCH for cross-boundary transmission.

3. BN1 sends ODI Beacon. BN2 receives ODI Beacon, therefore in Event F, BN2 sends ODI Data and The Loop of sending and acknowledging begins in Event G. At the end of Tx process, BN2 sends ODI Beacon to invite ODI packets from another side, but there are no packets incoming.

4. Both of them wait for Dwell Time before returning to intra-network activities. BN2 sleeps at the end of the process, but BN1 begins LPP transmission by waiting for Rx Beacon in Event H.

From the experimental results, the operations of ODI function is successfully implemented. The experimental operations are correctly functioning.

3.4.4 Memory Usage

One major concern of the ODI concept is the impact of the ODI framework on the memory usage since the ODI framework targets a native system with a high constraint in the resources. In this section, the memory usage of the ODI implementation is examined. The memory map of the experimental projects can be used to demonstrate the memory usage of the ODI framework. The results of the implementation are presented in Figure 3.14:

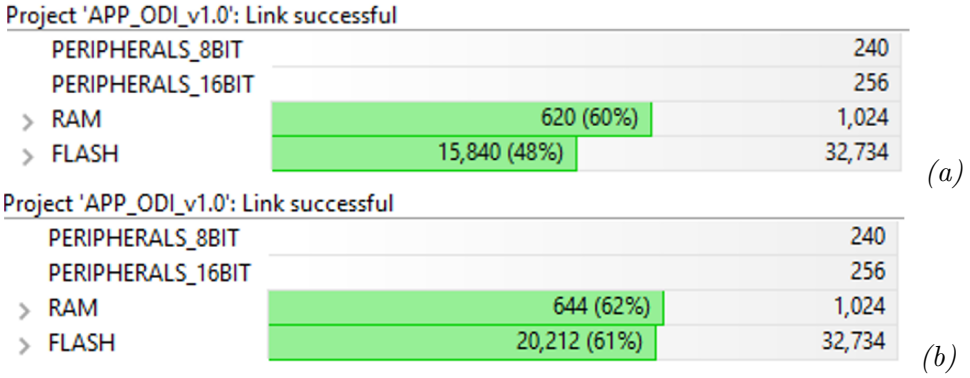


Figure 3.14: Memory map of a platform applied LPP (a) without ODI (b) included ODI functions

Figure 3.14 and 3.15 shows the memory map captured from Code Composer Studio v 6.1 of nodes w/o ODI modules. They illustrates the memory map of the platform with LPL. The memory space in the memory map can be divided into three categories:

1. Peripheral registers (240 + 256). These memories are the specific function registers, defined by the hardware.

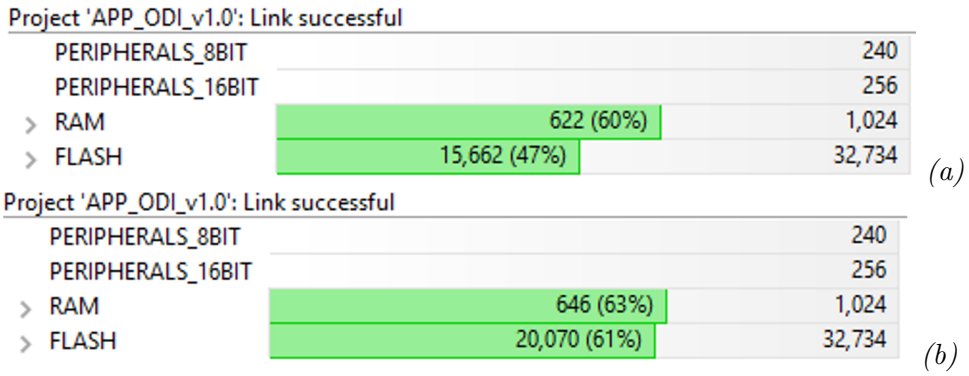


Figure 3.15: Memory map of a platform applied LPL (a) without ODI (b) included ODI functions

2. Random Access Memory (RAM 1,024 bytes). The read/write operation can be performed easily in this segment.

3. Flash Memory (32,734 bytes). The large memory space contains the algorithms and constants. The read operation of the memory section can be separately performed. However, the write operation must be performed segment by segment after the erasure of the whole segment.

The memory usage of the ODI framework can be evaluated by the comparison between the binary codes w/o the ODI framework. According to the memory map, the ODI functions slightly increases the memory usage. It takes 24 bytes of RAM and 4408 bytes of Flash memory. Table 3.7 shows the details of the memory usage concerning ODI modules.

Modules	**Memory [Bytes]**	**Ratio**
Flash Memory	4408	1
ODI MAC Modules	2240	0.51
ODI NET Modules	1804	0.41
Others	364	0.08
RAM	24	1
ODI Pairing Record	6	0.25
ODI Pass Table (4 entries)	13	0.54
ODI Link Status	5	0.21

Table 3.7: Memory usage of ODI modules

The memory usage can be varied depending on the compiler. Nonetheless, the increasing memory usage should be expendable for most of the available platforms.

3.5 Energy Consumption

In this section, the effects of ODI on the energy consumption is analysed. Since the communication process can be represented by a sequence of primary activities of the radio, the energy consumption of each activity is analysed to establish references for further analyses on ODI communication processes in Section 4.1.3. After a discussion about the energy consumption of the radio activities. NDS (see Section 3.5.2) and CBT (see Section 3.5.3) must be separately considered since they use energy for different objectives. Therefore, the viewpoint on the efficient use of energy in each process is different.

3.5.1 Measurement of radio profiles

In this section, Agilent N6705B DC Power Analyser captures the current profile of the radio activities with sampling periods at 0.1024 milliseconds. Observing these current profiles allows the estimation of any communication process that governs the radio. Figure 3.16 shows the current profile of a typical LPP process of scanning for DATA by transmitting a BEACON and waiting for responses.

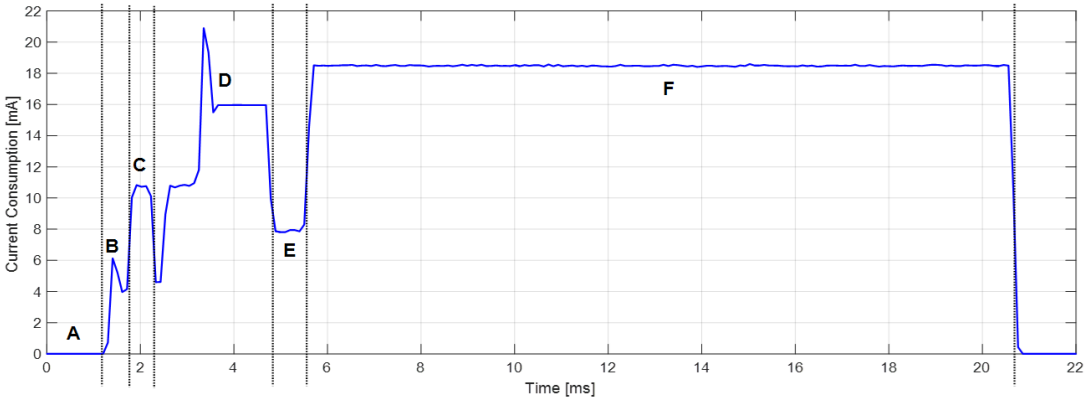


Figure 3.16: Current profile of routine procedures in ODI functions

Following processes are anticipated from comparing the current profiles with technical details from data sheets [13, 14]. The measured current consumptions are compared against the expected values in Section 2.2.3.2:

1. In Process A, CC2500 and MSP430 are in a sleep state, which indicates the sleep state of the node. The node is in the sleep state most of the time. The dimension of the current consumption in the sleep state is around thousands time in compared to the active state. The measured current is averagely 1.4 μA, which is approximately corresponded to the sum values of CC2500 and MSP430F2274 in their sleep state.

2. In Process B, MSP430 wakes up first. CC2500 then starts up its XOSC, which is necessary for the clock signal in CC2500. MCU is in the active state, which consumes 2.7 mA. The current in XOSC start-up is 2.7 mA. In the end, CC2500 is in the Idle state. The measured current consumption approximately corresponds to the reference values.

3. In Process C, CC2500 is calibrating its frequency synthesiser as a part of a startup process. The current consumption in the calibration process is 7.5 mA, MCU is in the active state, consuming 2.7 mA. The measured value approximately corresponds to the reference values.

4. In Process D, CC2500 is calibrating its frequency synthesiser as a part of a Tx process. Then, BEACON is transmitted at -10 dBm (12.2 mA). MCU is in the active state (2.7 mA). However, the measured current in is averagely at 16 mA, which is a bit higher than the sums of the reference values.

5. In Process E, the CC2500 state is changed from Tx to Rx (0.7 ms). The measured value is at 7.8 mA.

6. In Process F, CC2500 listens in the channel for 16 ms, which is corresponding to Dwell Time setting for this experiment. MCU is in a sleep state. The measured current consumption (18.53 mA) is approximately agreed with the reference values.

Each node periodically performs the abovementioned sequence of radio activities. It can be seen as the primary energy expense to sustain LPP, which is the conventional algorithm in ODI. Another unique sequence is the routine of DATA transmission and ACK shown in Figure 3.17. Process F is the action of active listening. In some cases,

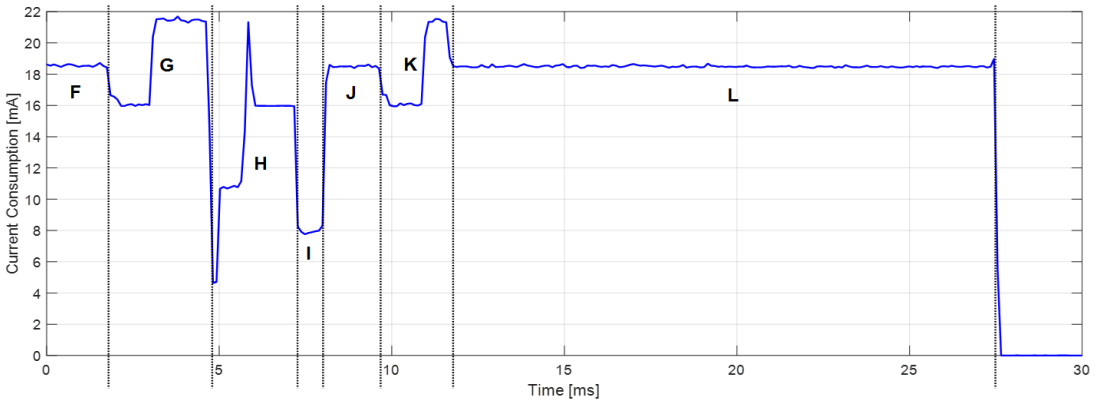


Figure 3.17: Captured current profile of the radio activities including reception of BEACON, DATA transmission and reception of ACK

a BEACON reception (Process G) can occur. Process H is the transmission of DATA frame. In Process I, the radio switches from Tx to Rx (0.7 ms). Process J shows the waiting interval for any response (1.6 ms) followed by a reception of ACK in Process K. Process L is another active listening in DWELL TIME.

From the observation of the current profiles, the energy consumption E can be calculated by the product of the power P and the time interval T, while the power is modelled as constant acquired by the product of the current (I) and the supply voltage at 3V. The following table shows the noticeable empirical values which are used for further references. The measurements are represented by the expected value ($\bar{x}$) and the 95-percent confidential interval, which are calculated by 1.96-fold of the standard deviation of the mean (($\Delta\bar{x} = 1.96\sigma_{\bar{x}}$).

DESCRIPTION	VALUE ($\bar{x} \pm 1.96\sigma_{\bar{x}}$)
Energy of Frame Transmission at -10 dBm (E_{Tx})	0.1036 ± 0.0010 mJ
Energy of LPP Routine (Process A-F: E_{LPP})	0.9802 ± 0.0006 mJ
Energy of Reception Events (Process G: E_{Rx})	0.1668 ± 0.0048 mJ
Avg. Current in Listening State (I_{Rx})	18.53 ± 0.01 mA
Avg. Current in Reception State ($I_{RxFrame}$)	19.05 ± 0.03 mA
Avg. Current in Transmission State (I_{Tx})	13.43 ± 0.11 mA
Transmission Time (T_{Tx})	2.583 ± 0.105 ms
Reception Time (T_{Rx})	2.958 ± 0.071 ms

Table 3.8: Empirical values of radio activities in the common communication procedures

From the measurements, it is noticeable that the reception of frames takes only slightly higher energy than staying listening which can be seen by comparing I_{Rx} and $I_{RxFrame}$. In this case, the transmission consumes less energy than active listening but also depended on the setting of the Tx power. Therefore, the simplified model of the energy usage of any communication protocol can be defined by two metrics:

1. Transmission Rate represents the energy used up by transmission
2. Duty Cycle represents the energy consumed by active listening

These energy metrics will be used further in the analysis of ODI processes in this thesis.

3.5.2 Consumption of Neighbouring Discovery

A mathematical model can describe the behaviour of NDS regarding energy. The observed values from real hardware are used to determine the values of parameters in the model. According to the implemented framework, NDS composes of 2 phases (see details in Section 2.4.2.1):

1. *Active Discovery* is the process when the node listens actively in the common channel for a discovery frame during the initialisation phase. The energy of the

process (E_{Active}) can be modelled by

$$E_{Active} = I_{Rx} T_{NDS} \tag{3.2}$$

where T_{NDS} is the time interval in which the node performs actively listening.

2. *Passive Discovery* is the process after initialisation when the node periodically sends a discovery frame. The energy consumption of this process ($E_{Passive}$) is technically the sum of energy consumed by the discovery routines ($E_{Routine}$) performed in the estimated lifetime of the node (T_{NODE}). The lifetime can be estimated by the quotient of the battery capacity ($E_{Battery}$) and the average current consumption of the node (I_{AVG}).

$$T_{NODE} = \frac{E_{Battery}}{I_{AVG}} \tag{3.3}$$

$$E_{Passive} = \frac{T_{NODE}}{T_{Passive} E_{Routine}} \tag{3.4}$$

where $T_{Passive}$ is the time interval between two consecutive discovery routine defined by $T_{NDS} = (1 + k_{robust}) T_{Passive}$. The coefficient k_{robust} is the safety factor which guarantee the encounter of BNs in CCH ($k_{robust} \geqslant 0$).

The total energy consumption of NDS (E_{NDS}) composes of ($E_{Active}, E_{Passive}$).

$$E_{NDS} = E_{Active} + E_{Passive} \tag{3.5}$$

$$E_{NDS} = I_{Rx} T_{NDS} + \frac{E_{B}attery(1 + k_{robust})}{I_{AVG} T_{NDS}} E_{Routine} \tag{3.6}$$

This model can be further used to calculate the total energy expenditure of NDS. Moreover, the equation can be utilised in the optimisation model. As an example, from Equation 3.6 , finding the minimum likelihood estimation can be used to determine the value of T_{NDS} which yields the minimal energy consumption (E_{NDS}). In this case, the node is supplied by 2-AAA equivalent to 2400 mAh. The average current (I_{AVG}) is measured at 2.4 mA. The k_{robust} is set at 1.5. The relationship between E_{NDS} and T_{NDS} is shown in Figure 3.18.

According to the Figure 3.18, the optimum energy point is at $T_{NDS} = 687.5$, which corresponds to the loss ratio at 0.0029. However, the work point can be shifted to a higher frequency of the discovery routine at the cost of the energy expense. The configuration of T_{NDS} will also impact the case where the neighbour is lost because the waiting interval to discover the neighbour again will also increase with the value of T_{NDS}. Nonetheless, the analysis shows that the neighbouring discovery scheme can be set in the way that the energy consumption for the activity is almost negligible.

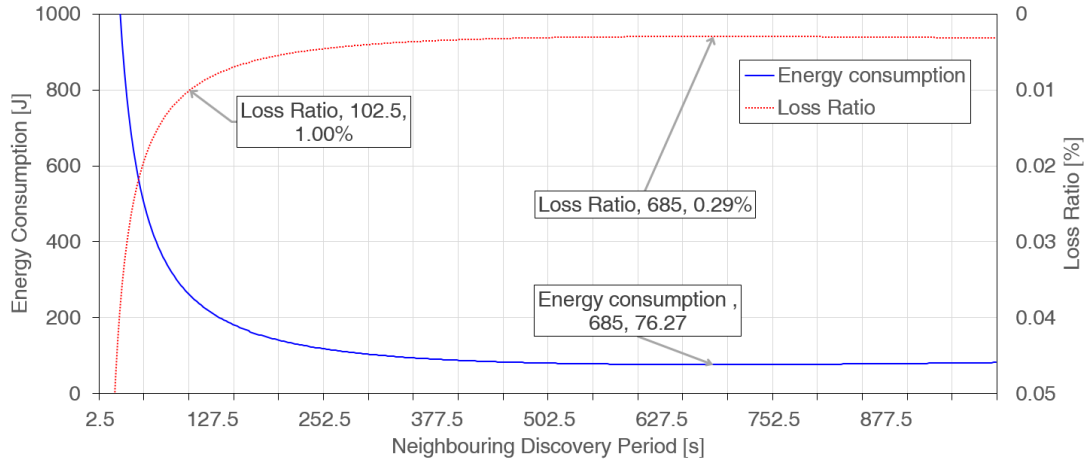


Figure 3.18: The relationship between T_{NDS} and energy consumption at $E_{Routine} = 2.7$ mJ (Transmission 3 ODI BEACON)

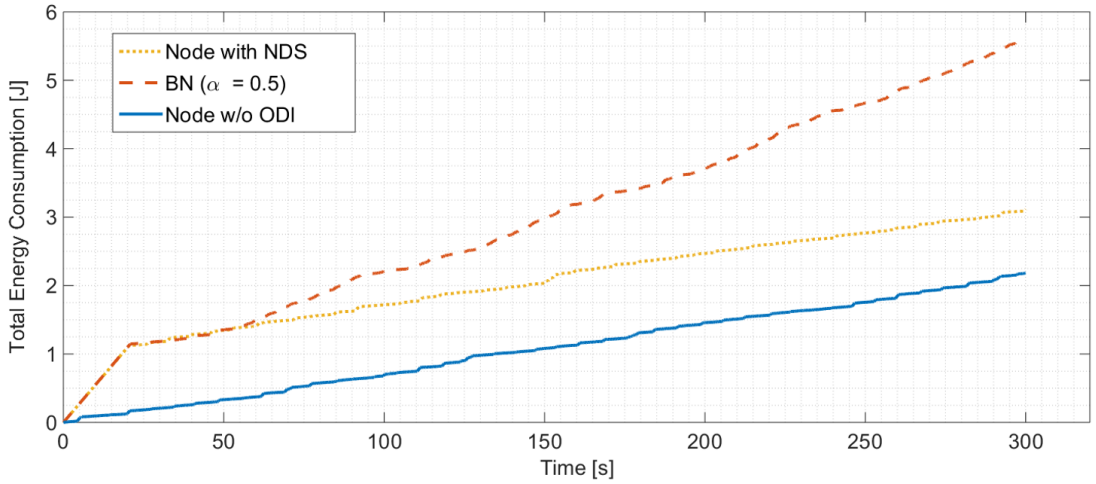


Figure 3.19: Energy consumption of nodes in ODI scheme

Figure 3.19 shows the direct measurement the energy profile from the experiment in Section 3.4.1. The energy profile of Node A1 (RN) is compared to the energy profile of Node A4 (BN, NDS-Node) to estimate the effects of the ODI framework regarding the energy consumption. The energy profile of Node A4 is measured twice to represent the BN performing CBT at $\alpha = 0.5$ and the node that performs NDS without a successful outcome (NDS-Node). According to the graphs in Figure 3.19, the NDS-Node and the BN share a same common energy profile from the beginning to T = 20s. Then, the graphs of RN and NDS-Node possess approximately a same slope, while BN consumes significantly more power. The energy consumption rate can be implied from the slopes of graphs. At the beginning of the graphs of ODI-Nodes (BN and NDS-Node), The power consumption of Active Discovery can be tracked. The measured value is around 1.14 J. Therefore, the offset around 1 J is present between the graphs of RN and NDS-Node. After Active Discovery, however, NDS-Node and RN share the same rate of power consumption. The power consumption of node depends on how often nodes transmit and

receive packets. Therefore, it can be implied that NDS-Node and RN have approximately a same amount of traffic. It can also confirm that the discovery process introduces only minimal packet transmissions and thus consumes relatively insignificant energy. The energy profile of BN shows that CBT introduces significant traffic because half of the packets are assigned for CBT ($\alpha = 0.5$) which will be discussed in details in the next section.

The average current consumptions, corresponding to data in Figure 3.19 are shown in Table 3.9.

Node		**Avg. Current [mA]**
RN (Node without ODI)		2.41
NDS-Node (Node with NDS)	Time (0-20)	19
	After Time = 20s	2.37
BN ($\alpha = 0.5$) (Node with CBT)	Time (0-20)	19
	After Time = 20s	5.33

Table 3.9: Current consumption of nodes performing basic ODI functions

In conclusion, this section has shown that the current empirical profile can be used to optimise NDS and the impact of NDS can be modelled and proved that it is insignificant in comparison with internal network activities. The analysis on the energy consumption of CBT will follow in the next section.

3.5.3 Consumption of Cross-Boundary Transmission

CBT is the process when BN exchange DATA frames across the boundary. Considering the theoretical concept, the energy expenses can be separated into following parts:

1. The energy spent on the common routine of checking a potential sender from other domain ($E_{Routine}$)
2. The energy spent on Tx/Rx of DATA frames exchanged across the boundary ($E_{DATA} = E_{TX_{DATA}} + E_{Rx_{DATA}}$)
3. The energy lost by failures on Tx/Rx ($E_{Failures}$)
4. The energy lost by idle listening during waiting for intended partner (E_{idle})

So, the energy consumption of CBT (E_{CBT}) can be comprehensively modelled as follow:

$$E_{CBT} = E_{Routine} + E_{TX_{DATA}} + E_{RX_{DATA}} + E_{Failure} + E_{idle} \tag{3.7}$$

From Equation 3.7, E_{CBT} is obviously depended on the data rate which should be considered under the ODI concept. However, the worthiness of the transferred data is not a concern of the communication protocol but, it is for the application layer to decide therefore at this point all DATA frames are considered mandatory. As a result, $E_{Routine}$ and E_{DATA} are the prerequisite of CBT in terms of energy expenses, while $E_{Failures}$ and E_{idle} represents the nonideal behaviours which should be minimised. This consideration is universally true for the design of any MAC protocol. But, in cases of CBT, the effects from the nonideal behaviours will be multidimensional as it will impact the internal communication as well. The comprehensive overview of the energy tradeoff in CBT can be understood by considering each distinctive part of E_{CBT} separately as follows:

- The amount of $E_{Routine}$ is effected by the setting of the CBT interval. This is the energy tradeoff with the collective network performances, i.e., reliability of the data transfer and latency of the data transfer. This part can be analysed in the same way as NDS.
- E_{DATA} is directly effected by the data rate. This strongly coupled with the application tasks but may limit by the capacity of the CBT link. Both parts are equivalent to the product of the data rate and the measured values of Tx/Rx (E_{Tx}, E_{Rx}) from the radio.
- $E_{Failure}$ is actually strongly related to the stabililty of the PHY layer and the potential of concurrency. The MAC protocol should minimise the contentions by considering the actual amount of data traffic an provide a backup algorithm to correct the errors of the PHY layer.
- E_{idle} is the direct concern of the MAC protocol in terms of resources either energy and bandwidth. The algorithm uses in CBT should consider more weight into this part because the idle listening in CCH will cut off the node from all internal communication and activities.

Considering from this discussion, the measured current of Node with CBT in Table 3.9 shows a relatively high duty cycle at approximately 29 percent. This is because LPP is asynchronous protocol. The communication partner must wait for signal from the other. It raises the question that OI-MAC which uses LPP as its main algorithm is well suitable for CBT since LPP is not designed to actively avoid the concurrency assuming that the potential of contentions is low or moderate. Furthermore, the idle listening in an asynchronous duty cycle protocol is randomised by several influential factors such as topology, the setting of the sleep period. Therefore, further analysis of the characteristics and the potential issues in the algorithm will be further discussed.

3.6 Discussion

Since the concept of ODI has never been implemented in real hardware, the conceptual design of the ODI framework must be expanded enough in the details so that the implementable algorithms can be derived. This research uses the existing concept as the initial point of the implementation and reconstructs the concept of the ODI framework considering the lesson learned from the implementation while maintaining the original intentions of the concept. After this work, the concept should possess enough details as a guideline for implementing a system with the ODI capabilities.

This chapter has mentioned the details of the implementation case from the PHY layer to the NET layer, which is applied in a high constraint device. In the communication layer, this research validates the existing concept by using OI-MAC to connect two distinctive domains, which uses a different MAC protocol. One employs LPL with strobed preambles (X-MAC), and another one adopts LPP (RI-MAC) as the MAC protocol. The concept of the MAC layer is interpreted into implementable algorithms including the exact definition of the frame format that retains only the necessary additions. Also, the handshake process is redefined separating the information exchange of the communication layers from the application exchange. The implementation reveals the realistic concept of the NET layer that lessens the requirements and the modification of the NET layer. An example of a routing protocol, which conforms to the requirements, is given.

The implemented system is tested by setting a scenario in which two network domains exchange packets via the connection provided by ODI. The system operation is observed by capturing digital signals from real hardware to confirm the correctness of the operations by comparing the obtained results with the theoretical expectation. Then, the energy consumption of the system is analysed by mathematical models and experimental measurements. The analysis on the energy consumption of the ODI framework leads to sceptical arguments on the suitability of the protocol used by the framework.

Chapter 4

Design and Evaluation of Cross-Boundary Protocol in Opportunistic Direct Interconnection Framework

The last chapter formulates the practical ODI framework from the existing concepts. The implementation is fundamentally evaluated regarding the operations of the framework and its memory/energy expenses. Upon the implementation and evaluation process, the results open a deeper question on the suitability of the cross-boundary protocol that used by the framework whether it is appropriate for the conditions of the data traffic at the boundary between domains. In all probability, other alternatives can improve the collective performances of the framework, if the careful consideration and practical investigation of the situation are carried out.

To answer the question, in this chapter, the conditions of the cross-boundary transmission will be analysed to formulate the conceptual design of the cross-boundary protocol. The newly formulated protocol will be compared to the OI-MAC in various aspects to confirm the suitability of the algorithms used by the cross-boundary exchanges.

4.1 Link Characteristics and Issues of Existing Protocol

In Section 3.5.3, the CBT process has been analysed regarding energy consumption. The energy expense is separated into the useful parts ($E_{Routine}, E_{DATA}$) and the nonideal parts ($E_{idle}, E_{Failure}$). The preferred characteristics of the CBT link thus should allow the tradeoff between the useful parts of the energy expense with the better performances while minimising the nonideal parts in the common scenario of CBT. Therefore, in this

section the common scenario will be firstly deduced from the known information. Then, the implemented protocol will be discussed based on the characteristics of the deduced characteristics and the practically obtained results.

4.1.1 Assumption of Cross-Boundary Transmission

The typical scenario in CBT can be approximately described as follows:

1. The data traffic could be periodicals such as cooperative packet forwarding or event-driven resources query and acquisition.
2. The ODI period (T_{ODI}) should be adjustable since the period should correspond to the intensity of data traffic and the requirements on the network performances.
3. CBT should be less frequent than the internal communication since ODI is the secondary objective of all participants, which possess their primary objectives.
4. The ODI processes should be executed in a precise and concise manner to lessen the impact on the original system.

All of the above statements point out the assumption on the traffic at the boundary as follows:

1. If T_{ODI} is set to suit the data traffic while considering the energy expense and impacts on the internal communication, BNs will frequently have pending DATA frames. As a result, CBT should induce a high probability of contentions.
2. Following from the first argument, the pending DATA frames could be correlated originated from the fragments of the application payload.

Therefore, according to the available information, the data traffic between the boundary is expected to exhibit the characteristics of burst transmissions with high contention.

4.1.2 Issues of existing protocol

Since the common scenario in CBT could involve a burst traffic with a high potential of contentions. The contention solving mechanism of the existing protocol is the vital point. In situations with a dense data traffic, LPP introduces the concurrency because contenders wait for the same BEACON to begin a transmission. The contention solving of LPP involves:

1. *Clear Channel Assessment (CCA) or Carrier Sense (CS).* This is a prevention technique, which functions well under the condition that the contenders are in range.

2. *Binary Exponential Backoff (BEB)* after Collison Detection (CD). This algorithm solves the contention after the receiver detects it.

To investigate both algorithms practically, the scenario is set by introducing a varied number of LPP contenders which sending DATA frames to the same Sink in a star topology. The Packet Error Rate ($PER = N_{Loss}/N_{Total}$) is measured to show the efficiency of the algorithm. The PER is defined as follows:

$$PER = \frac{N_{Loss}}{N_{Total}} = (1 - PDR) \tag{4.1}$$

where N_{Loss} : Number of the lost frames, N_{Total} : Number of the total transmitted frames and PDR : Packet delivery rate.

The results of the experiments are shown in Figure 4.1.

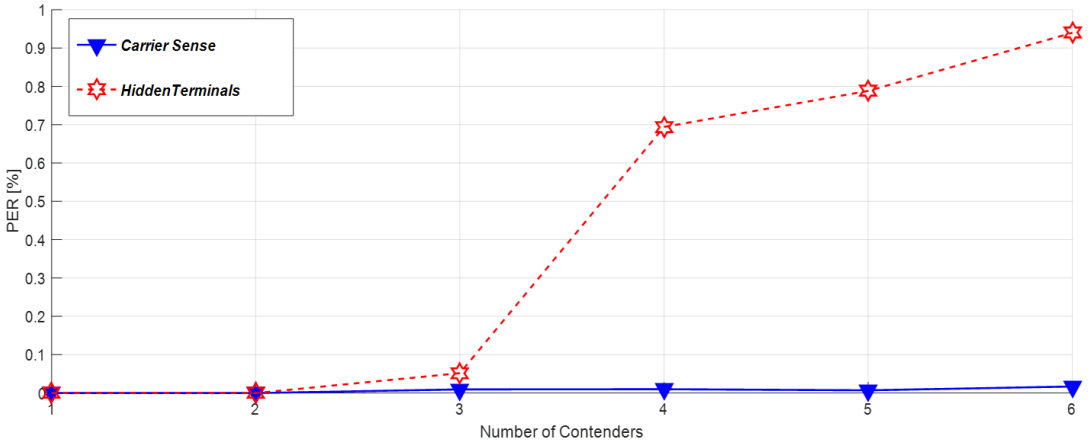


Figure 4.1: Packet loss vs number of contenders in LPP scheme, imitating CBT scenarios

The PER is the metric reflecting the reliability of any communication system. Thus, it will be the primary requirement of the CBT. The data generation and the sleep period are set equally at every second to simulate the scenario in which all transmitters always have DATA frames to send. The results show that if CCA is working correctly, the reliability of the link is high because the concurrency is actively avoided. However, the hidden terminal shows the big gap between 3 nodes and four nodes. This could be caused by the effectiveness of the collision detections since CC2500 cannot directly detect the change of the energy level while receiving [14]. If the parallel contenders send a DATA frame simultaneously, the receiver will not even detect the transmission because the SYNC WORDs which signals a frame reception in the hardware setting are corrupted.

To avoid this outcome, a small random jitter must be added before sending. The setting of this jitter leads to the sudden change in the probability of the frame detection in the concurrency scenarios.

While this measurement represents only one case of the LPP implementation, the measurement also points out the vital concern in CBT. CCA between two distinctive domains may not function accurately because the effectiveness of CCA is depended on the knowledge of the PHY characteristics. Additionally, CD can be even less dependable because the detection rate is affected by many factors. Thus, the dependence on the PHY layer to solve the concurrency should be proactively avoided in CBT as much as possible. Regarding energy consumption, the concurrency is avoided, the failures of the data transmission will be dropped along with the idle time in CCH resulting in the reduction of the wasteful expense.

Another big concern is the randomness of the idle time (T_{idle}) in CCH. This characteristic is crucial because not only it will affect the CBT behaviours but also impact the internal communication. The nodes idling in CCH will not response to any internal communication resulting in the declines in the network performances of the original system. Furthermore, the collective performances of CBT cannot be sharply defined resulting in the difficulty to support any link requirements. Figure 4.2 shows a measured current profile of the BN with $T_{ODI} = 12$.

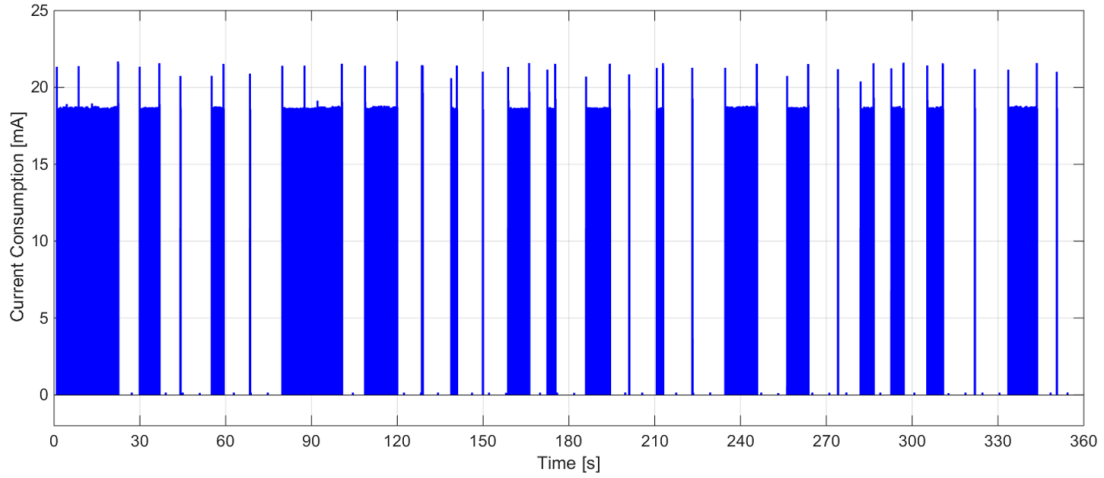


Figure 4.2: Current profile of CBT at $T_{ODI} = 12$ demonstrating duty cycle of radio

The current profile shows an example of the idle time in the random interval of LPP protocol. The maximum interval is equal to the twice of the specified sleep period assuming that all BEACON frames are received correctly. Therefore, T_{idle} is a random variable that scales with the setting of T_{ODI}. Additionally, the waiting time will be shorter if the number of the receivers is increased, therefore the protocol depended on the assumption that the overlapping area will cover many nodes from the associated domain.

However, this behaviour should be decoupled from the unrelated factor such as the topology or the setting of T_{ODI} because those two factors are changed by circumstances. As an example T_{ODI} can be set to a long interval to save the energy should not affect the idle time in CCH. If only a few nodes are detected, the idle time in CCH should not be affected. In conclusion, two major concerns are noticed in the existing protocol based on the common assumption of the CBT traffic:

1. Contention Management
2. Randomness of idle intervals

To observe the issues closely, more details of the link characteristics will be investigated in the next section.

4.1.3 Link Characteristics

To evaluate the link characteristics, the interesting aspects must be first defined. Then, the measurable metrics to show the tendency of the evaluated quality will be selected. According to the discussion so far, the relevant aspects of the link characteristics are the contention management and the idle listening which is related to the effectiveness of the energy usage. To reflect the features in the interests, following evaluation metrics are considered:

- **Packet Delivery Ratio (PDR)** This is defined by the ratio of data generation and the correctly arriving data at the base station. This metric is the fundamental requirement for the link communication. The sharp decline of PDR can be used to determine the saturation of the channel, i.e., channel capacity, which reveals the key characteristic of a MAC protocol.
- **Packet Latency (LAT)** This is defined by the time interval between the point where the packet is arriving at BN to the point where the packet reaches the base station. This metric can express the time-related quality of services which reflect the impact of the idle listening.
- **Duty Cycle** This is defined by the ratio between active/inactive states of the radio chip. The metric directly shows the behaviour of the idle listening. Additionally, it also allows the estimation of the energy profile.

To reflect the condition change, following parameters are chosen as a controlled variable:

- **Number of associated BNs** This variable reflect the diverse topology. By varying this parameter, the behaviour of the link in contentions can be investigated.

- **CBT Period** (T_{ODI}) This parameter reflects the setting change and also can demonstrate the variations in respect to the rate of data traffic since increasing or decreasing T_{ODI} will change the number of pending DATA frames.

The CBT occurs at the boundary of two distinctive domains. However, the effect of the internal communication should be minimised to decouple the measurement results from the internal communication so that the measurement results reflect the behaviours of CBT. Therefore, the experimental setup assumes the ideal internal communication that can deliver DATA frames promptly and correctly. The overview of the experimental setup is illustrated in Figure 4.3.

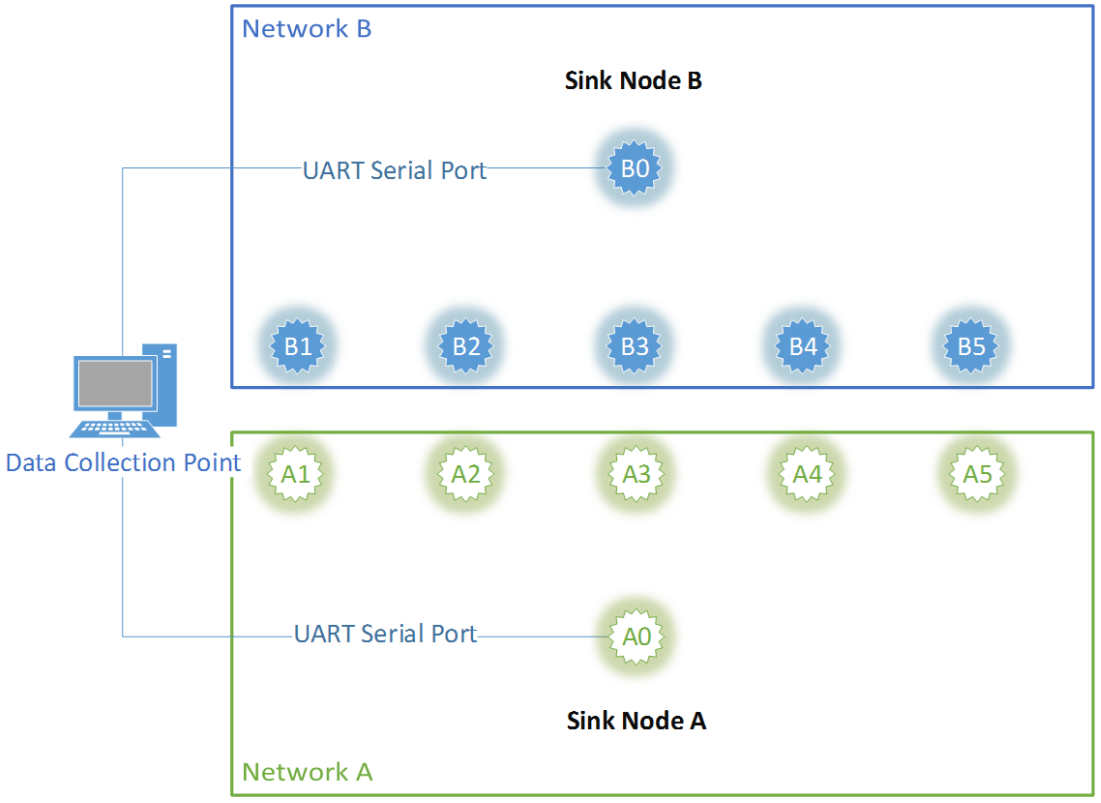


Figure 4.3: Experimental setup to measure the characteristics of CBT while reducing the effects of the internal communication

The details can be briefly described as follows:

- Two distinctive networks in the star topology discover each other and send packets across the boundary.
- Each network operates in each own DCH with X-MAC. This allows Sink Node to receive the transmission immediately by keeping the radio active all the time.
- Sink Node ideally stays awake without duty cycle to receive packets. This scenario simulates the ideal internal communication.

- Every node in the network has a very stable and robust wireless connection to their Sink Node.
- The number of nodes in CBT is varied, and every node in the boundary area can discover nodes of the neighbouring network.

The common values of the relevant parameters are shown in Table 4.1.

PARAMETERS	**VALUE**
Transmission Power	-10 [dBm]
Sleep Period Of Sink Node	0
Sleep Period Of Remote Node	1024 [ms]
Data Generation	1024 [ms]
Injection rate (α)	0.5
Dwell Time	16 [ms]
ODI Configuration	
Discovery Period (T_{NDS})	12 [s]
CBT/ODI Period (T_{ODI})	6 [s]

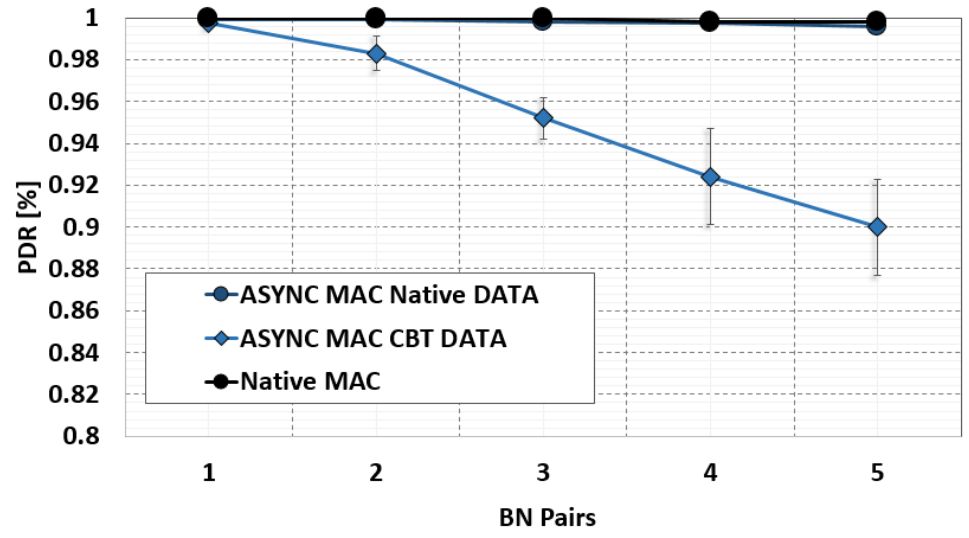
Table 4.1: Parameter setting of the experiments on CBT characteristics

The details of the measurement process are described as follows:

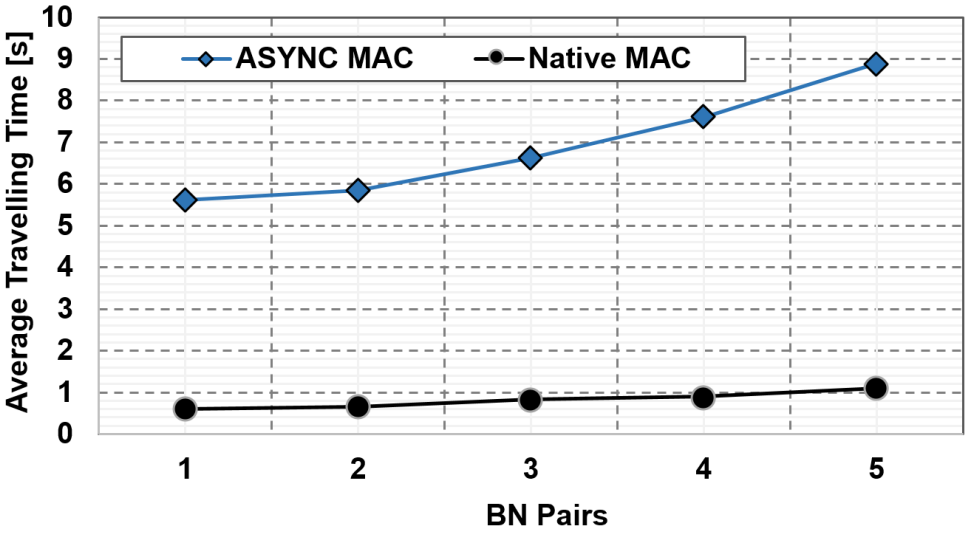
- PDR value is evaluated after a number of the collected packets reaches 1000 packets. The measured value comes from 10 measurements with the 95-percent confidence interval.
- LAT is evaluated every 100 packets. The average value is chosen to represent the measured data.
- Duty cycle [%] is measured in every 5 minutes. The presented value comes from 10 measurements with a 95 percent confidence interval assuming a normal distribution.

Figure 4.4 shows the results obtained from the experiments as the number of BNs are varied. Figure 4.5 illustrates the results obtained regarding the setting of the CBT period (T_{ODI}).

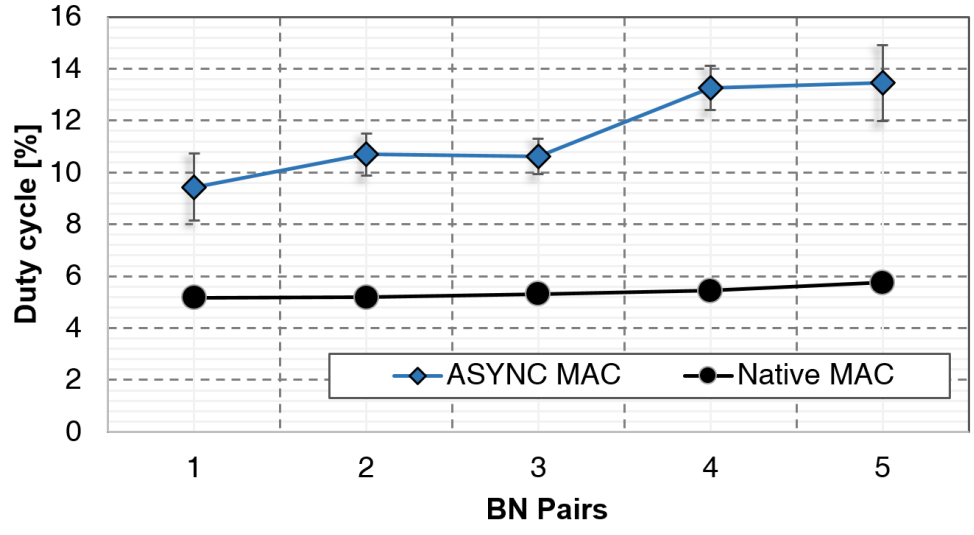
The native MAC is the measurement of the internal communication (X-MAC with the always-on Sink Node). The results of the native MAC is shown here to be the reference point so that the impacts of CBT on the original system can be seen. The internal communication is relatively stable concerning the increasing number of associated nodes. However, the effects of the concurrency can be obviously noticed regarding the CBT link. These nodes are in coverage of each other, so the CCA is working correctly,



(a)

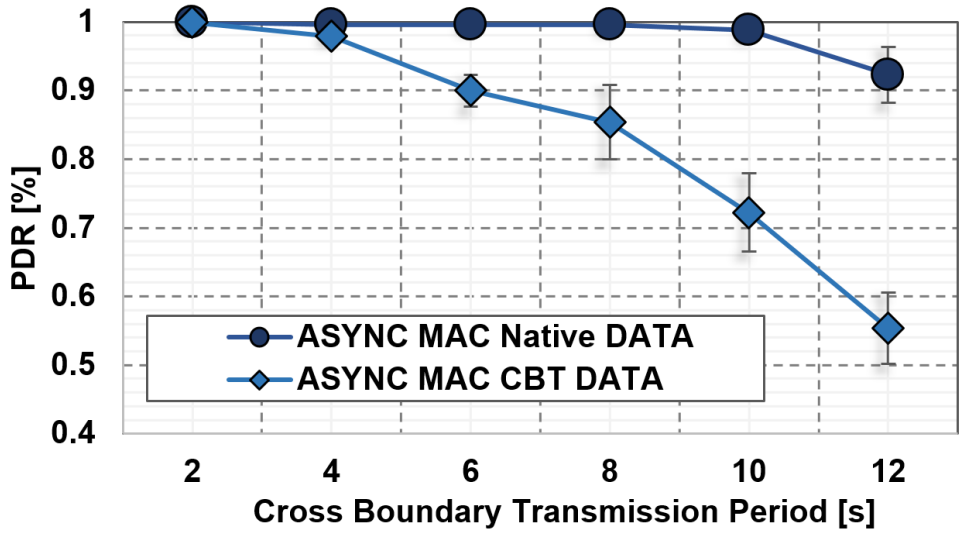


(b)

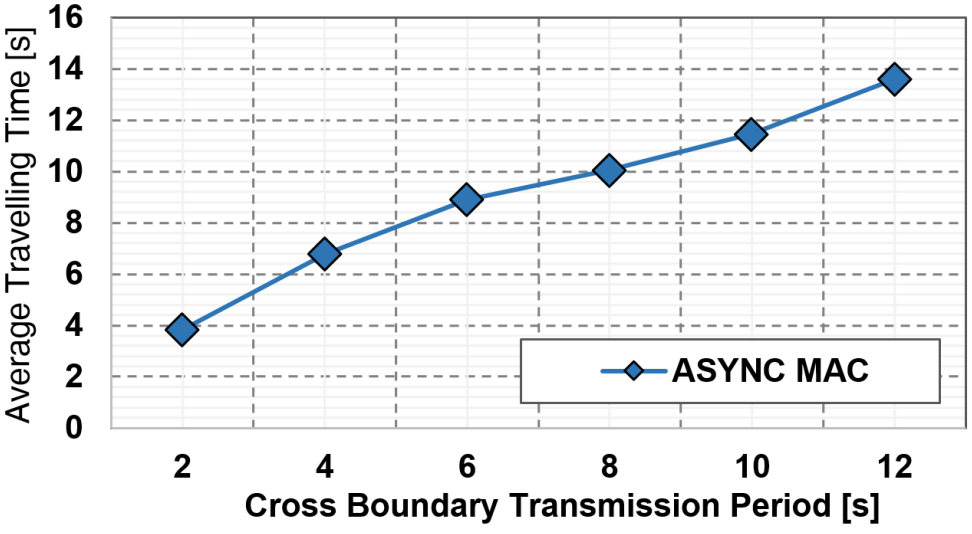


(c)

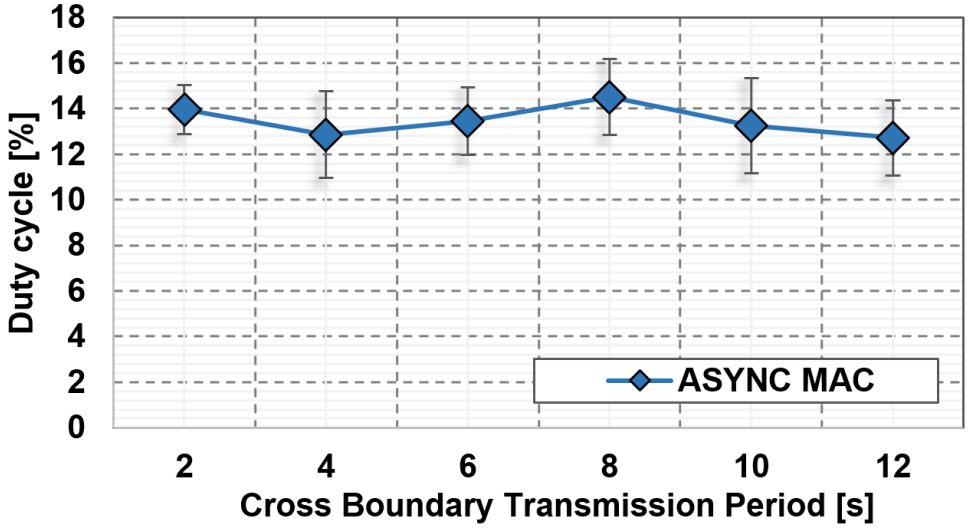
Figure 4.4: The relationship between the number of associated nodes and the evaluation metrics(a) PDR (b) LAT (c) Duty Cycle



(a)



(b)



(c)

Figure 4.5: The relationship between the varied T_{CBT} and the evaluation metrics(a) PDR (b) LAT (c) Duty Cycle

but the failures of the transmission attempt are increased with the probability of the contentions. This results in the higher LAT, the lower PDR and the increased duty cycle. In a), the PDR of the internal frames are not declined at the same rate with the CBT frames because the internal is very strong, but on rare occasions, the pending CBT frames can overwrite the internal frames results in the loss of the internal frames contrary to the quality of the internal link. The empirical results regarding the effects of the concurrency confirm the discussion in the last section. Another relevant factor is the setting of the CBT period (T_{ODI}). T_{ODI} changes the number of pending frames in each CBT event which is equivalent to change the effect of the increasing incoming rate.

With the increasing T_{ODI}, the number of pending DATA frames is increased resulting in the declination of PDR and the higher LAT. The LAT is approximately in the linear proportional relationship with T_{ODI} since BNs need to wait longer before each CBT event. The function of duty cycle with T_{ODI} is approximately a constant around 0.13. This also mean that the setting of T_{ODI} only scales each idle interval but the total energy consumption will not be effected by the setting of T_ODI in cases that BNs always have pending frames to exchange in every CBT event.

In conclusion, the link characteristics implied by the results of the experiments show the positive confirmation on the concerns of the existing protocol. Therefore, the performances of the CBT link should be improved if the chosen algorithm is designed particularly for the CBT traffic.

4.1.4 Discussion

The ODI concept is evidently proved feasible regarding memory and energy constraints. The available RAM space is much tighter than the external memory such as flash memory. The RAM usage of Virtual MAC, which allows multiple MAC protocols inside one node, is insignificantly different from usual networks with only one MAC protocol. The programming space can be significantly reduced by emphasising on the code reusability. From this experiment, the fact that NDS requires only relatively insignificant energy confirms that the energy constraint will not obstruct the feasibility of ODI. The energy consumption of CBT is depended on the intensity of CBT traffic, but the technique in CBT still need improvements. LPP is not originally designed to be optimised in such scenarios. According to literature reviews and experimental results, following critical issues are detected in the current framework, which uses LPP as a basis:

1. Time intervals that BNs remain in CCH are inconsistency and unpredictable as CBTs occurs when BNs randomly detect each other, this induces packet loss and congestion as well as make resynchronisation of local protocols harder resulting in excessive energy losses.

2. Furthermore, performances of ODI by LPP depends strongly on the network condition. Two critical factors can be given: 1) T_{ODI} as this become longer, the link quality sharply drops 2) numbers of BNs as this directly introduces higher probability of the contentions.

3. LPP invites contentions and collisions in its core principle by requesting multiple senders to send their data to the same receiver simultaneously after receiving the polling beacon. In ODI schemes, BNs are the destination of packet collections. Therefore, BNs always have packets to transmit.

4. Randomly distributed cycles are reflected by high variances of packet latency. Therefore, hard QoS requirements on latency could be challenging to serve.

In Section 4.2, the algorithm of the link layer in CBT will be redesigned by using the assumption of the CBT traffic.

4.2 MAC Algorithms for Cross-Boundary Protocol

In Section 4.1, the issues of the currently used algorithms in CBT are pinpointed. In this section, the alternative solution for the MAC algorithms in CBT will be discussed.

4.2.1 Analysis on Solution

4.2.1.1 Objectives

Considering the assumptions of the data traffic in CBT (see details in Section 4.1.1), following characteristics of MAC protocol are required:

1. *Contention management*: The protocol should be designed under the assumption of concurrent burst transmission between a pair of BNs, therefore actively prevent contentions before transmission.

2. *Optimal for burst transmission*: The protocol should be designed to save energy in burst transmission such as avoid idle listening of other BNs.

3. *The configurable frequency of cross-boundary transmission*: Because the frequency of application load in ODI is uncertain, depends on the application. Therefore, the period to perform cross-boundary transmission should be adjustable.

4. *Minimal radio occupancy*: The MAC protocol used in cross-boundary transmission co-exist with the internal MAC protocol inside the network. Therefore, it seizes the radio control and interrupts the internal communication. Thus, minimising idle listening in ODI must be considered more severe than in common scenarios.

4.2.1.2 Methods

Following methods are reviewed to improve the desired characteristics (see details in Section 4.1.1):

1. *Improving contention management*: This involves Carrier Sensing or Clear Channel Assessment [3, 51] (Sampling channel energy level before sending), Collision Avoidance (CA) [109,117] (Receiver sends signal CTS before transmission), Scheduling [51, 76] (Sending agreement scheme to all potential contenders).
2. *Network Allocation Vector (NAV)* can be used to save energy by sending the duration of transmission to surrounding nodes [109,116]. 3. Scheduling and Synchronisation are commonly used to reduce idle listening and set a defined characteristic according to the requirements of quality of services [51, 76].

Following considerations are involved in the design of the algorithms:

- The traffic conditions of CBT are similar to the conditions in the traditional network which use CSMA/CA algorithms (IEEE802.11 [109]). However, the duty cycle of radio is the additional concept to conserve the energy.
- CSMA/CA works under the assumption that all participants are constantly listening to the channel which not applicable for WSNs and the ODI scheme [31]. ODI must be sharply optimised regarding the radio occupancy otherwise; the internal communication will be affected. Therefore, the duty cycle must be synchronised.
- The requirement of ODI on a swift radio control and the configurable period can only be provided by the synchronisation of the radio duty cycle. However, it could introduce more overheads and the typical problem of the synchronisation such as the clock accuracy.
- When the synchronisation fails, an asynchronous algorithm must be available as the substitute.

The considerations result in the pragmatic solution of ODI, which is described in Section 4.2.2.

4.2.2 Details of Algorithms

According to the analysis in the last section, the MAC algorithms of CBT should employ the algorithms to avoid contentions and idle listening including CCA, CA and NAV with the synchronisation of the radio duty cycle. The details of the process can be described as follows:

- After a successful discovery, BNs usually remain with a fixed partner in cross-boundary transmission, unless any condition changes. The partner synchronises the intervals in which they are absent/active in the common channel (CCH). Therefore, there are no extra overheads on the scheduling for multiple nodes.
- The period can be regulated according to an additional header, sending in beacon packets. This will allow the adjustment of cross-boundary transmission period according to data traffic.
- The transmission (CCA mode) of data loads begins after receiving a signal from the receiver as described in typical Polling Technique [6, 11]. Every beacon is treated as a Clear-To-Send signal to the surrounding nodes; therefore, it will prevent transmission of another beacon from other nodes to avoid contentions. (Integrated CA)
- Every received packet must be acknowledged. Any ACK is treated as a BEACON.
- Each node sends a BEACON (with CCA) after listening to channel for one slot of transmission to detect any BEACON in cases that channel is occupied. After sending BEACON, the node waits for a short period (Dwell Time) and then releases the radio control.
- To remain synchronised with the partner, BNs must exchange beacons when the ODI period is reached, but the setting of ODI period must consider the intensity of the traffic. (The setting of ODI is out of concerns of the MAC layer).
- After any sender sends all the available data packets, each node must send a BEACON to invite data from the other side.
- If CCA is failed, the node performs a back off for one slot and retry the transmission for three times before termination.
- NAV can be introduced in the packet header to tell how much time left until the transmission will finish.

Figure 4.6 shows the overview of the proposed algorithms with the sequence diagram.

All other details about the frame definitions and process are similar with the OI-MAC, referred to Section 3.2.2. The BEACON frame realises ODI SYNC BEACON and ODI CTS addressed to the paired partner. In this way, other unintended nodes received the BEACON will know that the medium is busy as they check the address of the received frame. The accuracy of the synchronisation can be controlled by a Euler feedback loop to reduce the wait time in CCH under the limit setting.

While these algorithms should significantly improve the target performances, the potential drawbacks should be considered as well so that the gaining benefits are not

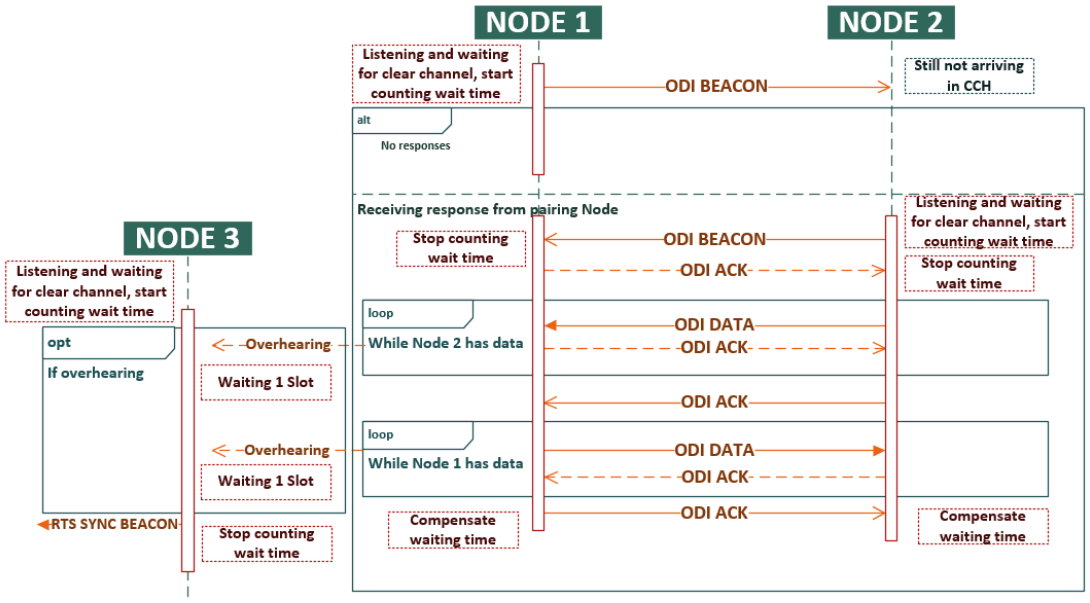


Figure 4.6: Sequence diagram illustrates the outline of the improved MAC algorithm used in CBT

outweighed by the drawbacks of the improvement. In Section 4.2.3, the drawbacks and advantages of this solution against the previous one will be discussed.

4.2.3 Potential Benefits and Drawbacks

The synchronous MAC protocol described in the last section is expected to gain following benefits over asynchronous version (OI-MAC):

- *The long-term tendency to eliminate collisions and interferences.* As BNs only response to messages from its pairing partner, while avoiding any messages from other pairs, the channel usage is automatically adjusted to prevent interferences between BN pairs in the long term.
- *The radio occupancy by ODI in each round will remain constant and low.* As BNs can use feedback control to compromise the difference between clock rate thus reducing waiting time in CCH
- *Because the ODI partner is fixed, the physical connection should be more static.* The radio chip can use a feedback loop to compensate the frequency offset and phase offset, caused by the mismatch of PLL between Tx and Rx and also to control the reception gain.
- *The method to emphasise any desired Quality of Services (QoS) can be comprehensively outlined.* Because the CBT period is configurable, the trade-off between

quality metrics, i.e., trading between energy consumption and network qualities can be achieved by setting the CBT period.

- *Loss of connection is readily determined and can be handled locally* because the ODI partner is fixed and synchronised. Losing partner can consecutively be used as an indicator to find any new partner. If a new partner is not found, then the connection to the neighbouring network is lost.

Following drawbacks of the synchronous protocol can be recognised, compared with OI-MAC:

- *The increasing overheads due to synchronisation may overthrow the gaining benefits.* BNs need to exchange beacons to check the availability and synchronise the ODI cycle. Therefore, the efficiency of energy spending depends on the accuracy of the synchronisation as well as the configuration of the ODI period.
- *Random error in physical layer may lead to fatal consequences.* Missing beacon exchange may result in massively increased radio occupancy, as BNs always wait for the response from the partner.
- *Some nodes in the boundary areas may not be utilised as a BN.* Pairing with only one fixed partner limits the numbers of BNs, even though some network may possess nodes in the boundary region more than the neighbour may have.

According to the above consideration on the benefits and drawbacks, there are the possibilities that the newly proposed protocol underperforms the previous OI-MAC despite the careful analysis so far. Therefore, an evaluation of the performances of both variations of MAC protocols in ODI will be needed to choose a more pragmatic solution, which will be discussed in further sections.

4.2.4 Performance Comparison of MAC Algorithms in CBT

The target in these experiments is to compare the performances of the deduced solution and OI-MAC in the common environments of CBT. Considering the objectives of the experiments, the experimental conditions in Section 4.1.3 are still valid as the comparison should show the behaviours of the algorithms in the target characteristics. Therefore, the identical experiment setup is used for the comparison of the performances between both protocols. Two network domain with an ideal internal communication is deployed to study the CBT between them (see Figure 4.3).

The previous evaluation metrics from Section 4.1.3 are still valid as they cover the most important aspects of the collective network performances regarding reliability, latency and energy consumption. However, the extra overhead is included as one of the

foremost concerns when employing a synchronous protocol instead of asynchronous protocol. Therefore, another metric must be added into the evaluation metric to compare the overhead of both algorithms. The average transmission rate [frames/s] is measured by counting the transmitted frames in 5 minutes to calculate the average rate of the frame transmission. In the controlled environments, this metric can indicate the significance of the increasing overhead The evaluation results are collected in two aspects: 1) Contention Management 2) Variation of ODI period

The evaluation assumes the situation when BNs are in the constant contention. Therefore, all BNs are assumed to receive an incoming CBT frame in every second, i.e., all of them always contends for the access to the CCH. The number of the BNs will be varied to see the effects of the contention and the ODI period is varied to see the effects of the parameter setting.

4.2.4.1 Contention Management

Figure 4.7 shows the results of the measurement of the evaluation metrics as the number of contenders is varied. Overall, the synchronous algorithm improves the network qualities in every criterion. While OI-MAC is affected by the contention, the synchronous protocol remains relatively unaffected. The probability of successful receptions of OI-MAC is approximately proportional to the number of pairs involved in the scenario as it can be seen in the decline of PDR and the increased delay of the transmitted frames. When using OI-MAC, the PDR of the CBT frame is decreased by 0.02 with one additional pair. This can only be caused by the buffer overflow because the node is programmed to overwrite the new coming frames with the oldest frame in the buffer. The results of the latency measurement show the same trend as the PDR. As the number of BNs is increased, the latency of the CBT frames in OI-MAC is also increasing because some queuing frames cannot be successfully transmitted in one cycle due to collisions. The latency of the synchronous protocol is relatively stable unaffected from the increasing number of BNs

The experimental results confirm the prediction that the proposed synchronous protocol is more suitable to the condition of CBT than the asynchronous protocol as the contention of BNs in CBT should be high. After the benefit is confirmed, the energy consumption should be simultaneously considered. Figure 4.8 results are obtained regarding the energy consumption.

According to Figure 4.8, the increasing trend of the consumed energy can be observed in both synchronous and asynchronous protocol. However, the increasing rate of the synchronous protocol is much lower than that of OI-MAC. Since the CBT period is fixed, the duty cycle of the radio is depended on the systematic pattern of the encounters

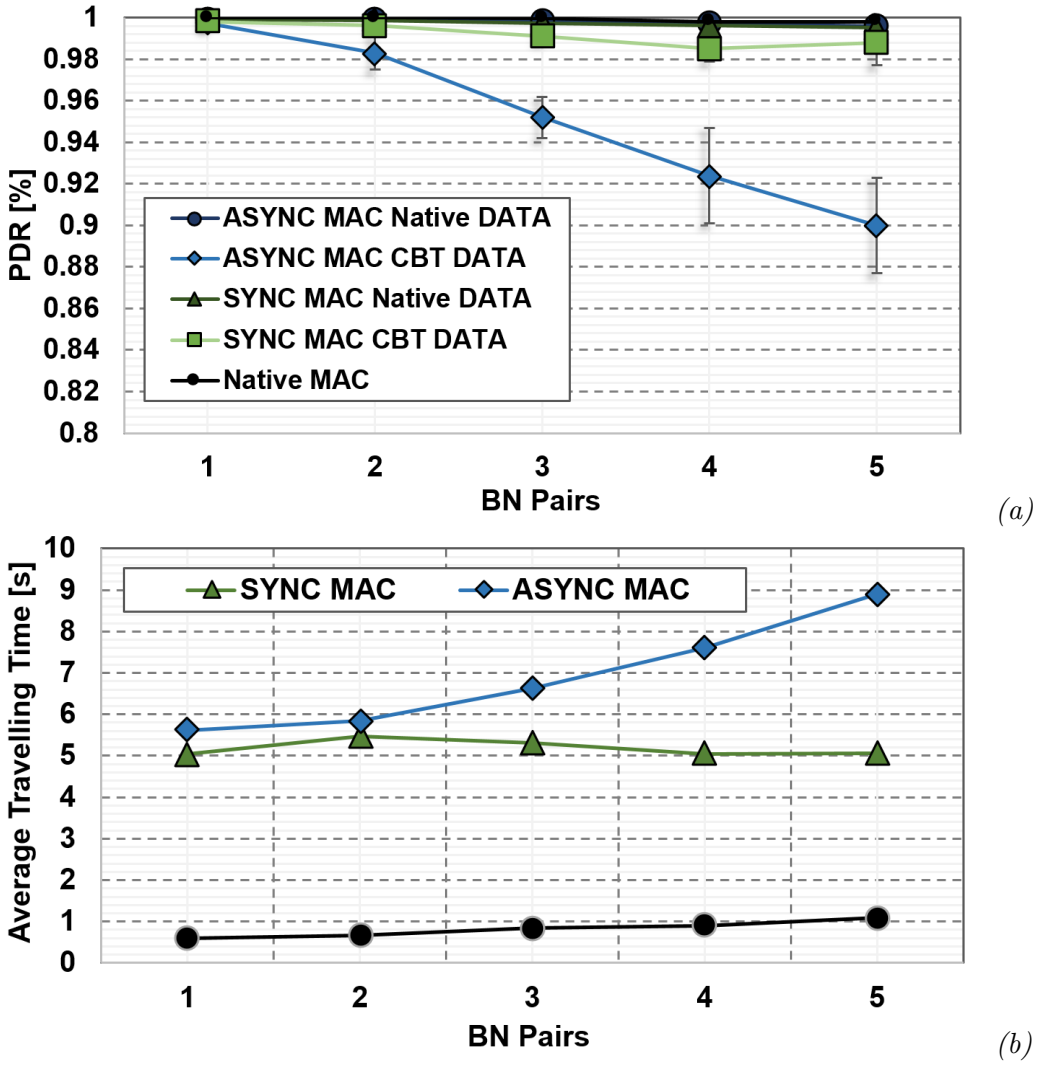


Figure 4.7: Experimental results show relationship between number of BNs and collective network performances (a) PDR (b) Latency

between the associated nodes. However, the synchronous protocol fixes the communication partner of BNs and adjusts the difference of the clock rate with a feedback control by simply reducing the waiting time of the node waiting for its partner more than an acceptable interval. As a result, the duty cycle of the synchronous protocol is relatively constant which also corresponding to the results obtained from the latency. From the measurement, the duty cycle is improved up to 7 percent. This confirms the multiple benefits of the synchronous protocol in CBT which saves energy, improves the network quality, reduces the radio occupancy.

The measurement of the transmission rate indicates that the introduced overheads of the synchronous protocol are less than the wasted transmission introduced by contentions. When a few BNs are involved in the CBT, the transmission rates of OI-MAC and that of the synchronous protocol are approximately equal, the tiny difference between the transmission rate could come from the transfer of BEACONs to begin the transmission

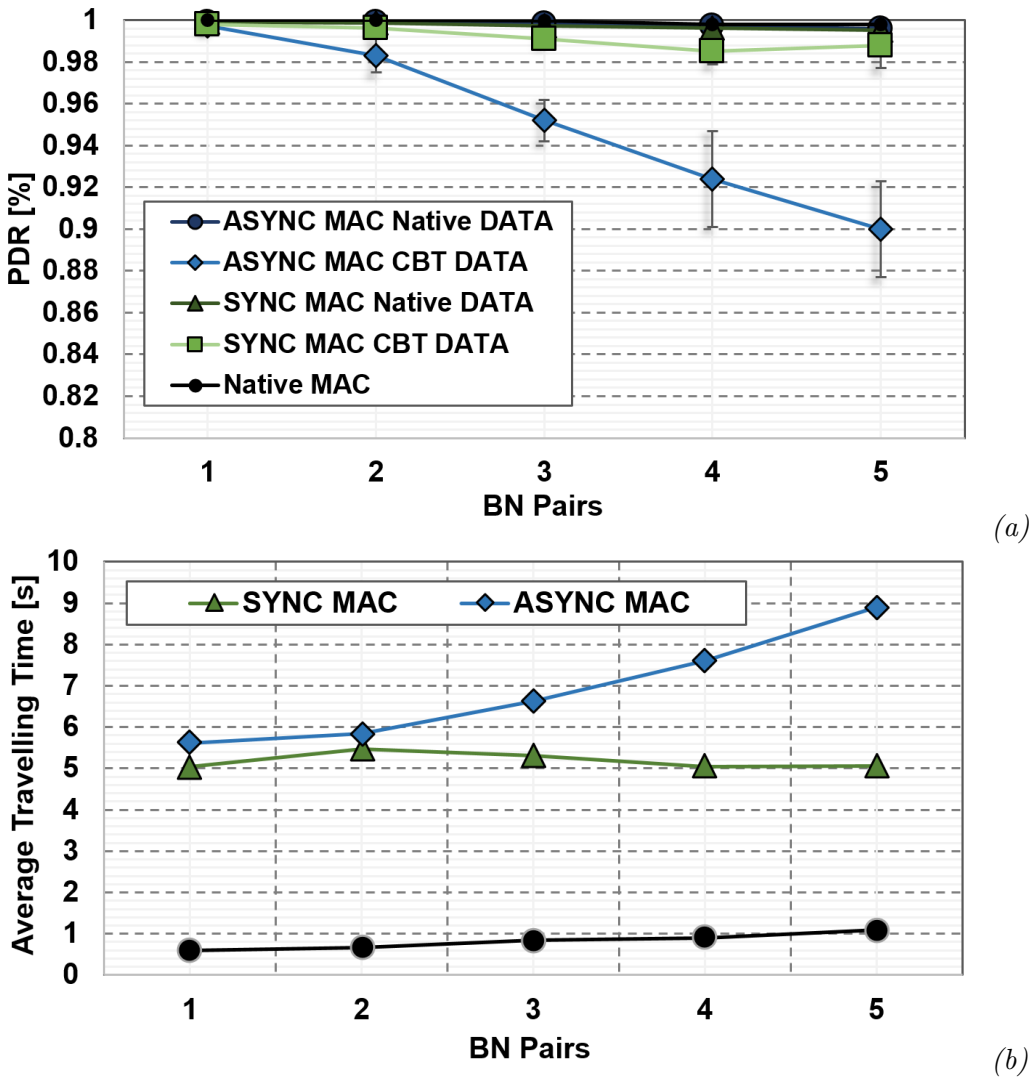


Figure 4.8: Experimental results show relationship between number of BNs and collective network performances (a) PDR (b) Latency

of the internal DATA frames. The experimental results so far confirm the expected benefits of the synchronous protocol over OI-MAC. In the next section, the behaviours of both protocols on the different amount of data traffic will be studied.

4.2.5 Variation of CBT period

In this section, the evaluation metrics are measured as the CBT period is varied. Varying CBT period shows the effects of the basic parameter setting of CBT on the network qualities. Additionally, the amount of the data traffic can be indirectly simulated by changing the CBT period. Figure 4.9 shows the experimentally obtained results as the evaluation metrics are measured as the CBT period is varied.

When the CBT period is set at the larger value, the number of pending DATA frames is increased. If the pending data can be transferred before a buffer overflow, there is no lost

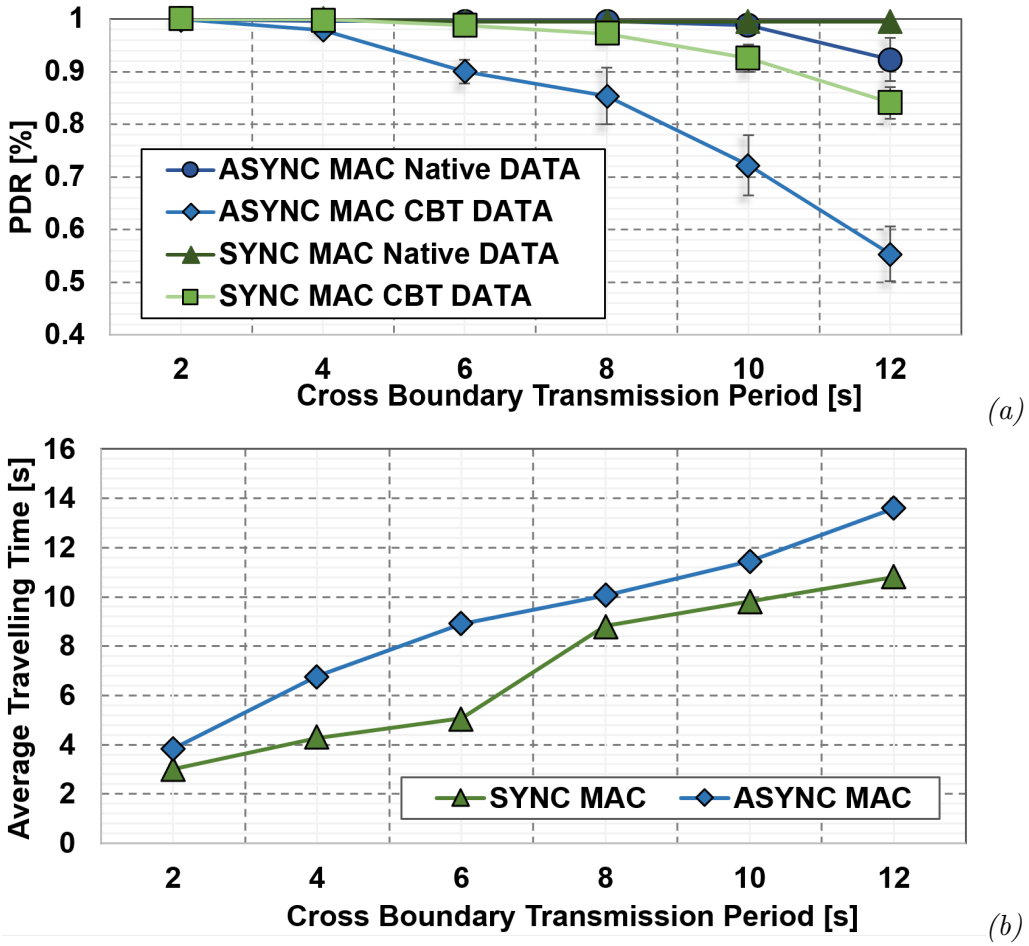
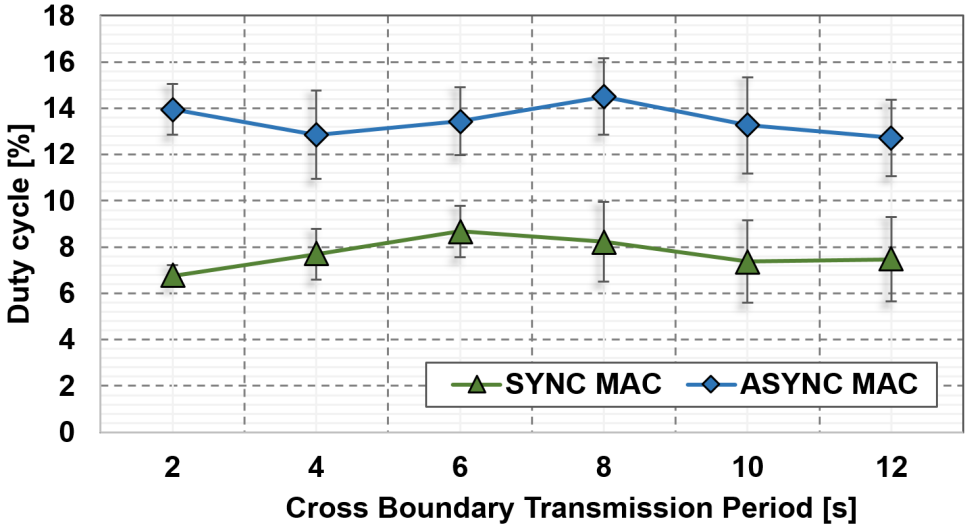


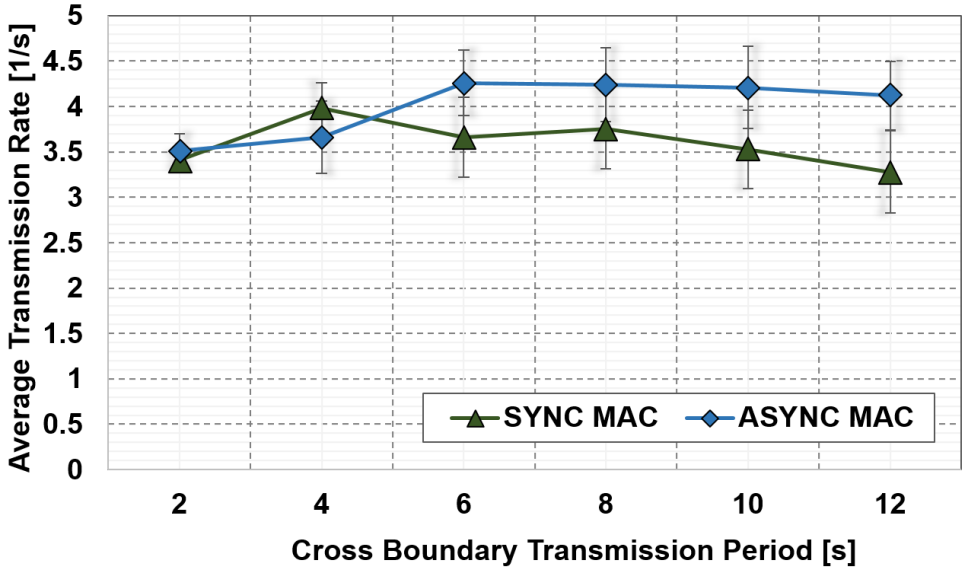
Figure 4.9: Experimental results show relationship between CBT period and network qualities in different aspects (a) PDR (b) Latency

frame, i.e., PDR is 1. The point when the PDR begin to decline noticeably shows the point of the saturation when the incoming frame rate overrun the outgoing frame rate. When the amount of data traffic exceeds the saturation point, the rate of overwritten frames, i.e., PER is equal to the number of the exceeding frames. Therefore, the PDR declines linearly with the increasing CBT period as seen in the PDR of the native frames in the case of OI-MAC. The PDR of the synchronous protocol shows that the channel is saturated at the significant more incoming data rate. Therefore, the synchronous protocol will allow a more extended CBT period as a possible option to trade off with the energy.

The latency is directly proportional to the duration of the CBT period as the CBT data is stacked longer before an opportunity for the next transmission. However, because collisions and radio occupancy are reduced in the synchronous protocol, the latency is improved averagely about 2.1 seconds. Overall, the experimental results show the improvements on network qualities as expected. However, the energy consumption should be considered along with the network qualities. The results from experiments in the aspect of the energy consumption are illustrated in Figure 4.10



(a)



(b)

Figure 4.10: Experimental results show relationship between CBT period and energy consumption (a) Duty Cycle (b) Transmission Rate

It is apparent from the measured duty cycle that the duty cycle is relatively constant with the varied CBT period. This is because the increased CBT period only scales the dynamic behaviours of the radio occupancy since the probability of encountering the intended receiver stay unchanged regardless of the setting of the CBT period. OI-MAC yields the average duty cycle at 13.46 percent, while the synchronous protocol results in the duty cycle at 7.7 percent. The improvement of the radio occupancy is approximately improved by 5.76 percent.

In the aspect of the overhead, the results from the measurement of the transmission rate show that contentions caused more wasteful transmission than the overheads introduced by the synchronous protocol. While the channel is still not saturated, the transmission rate rises along with the increasing CBT period. After the saturation point, the transmission rate stops increasing at about 4.2 frames per second. This is because the

circumstances of the transmission remain unchanged regardless of the interval of the CBT period as all participants always request for transmission and the probability of successful transmission is unchanged depended on the characteristics of the physical channel. Contrary, the transmission rate of the synchronous protocol remains approximately constant at around 3.6 frames per second.

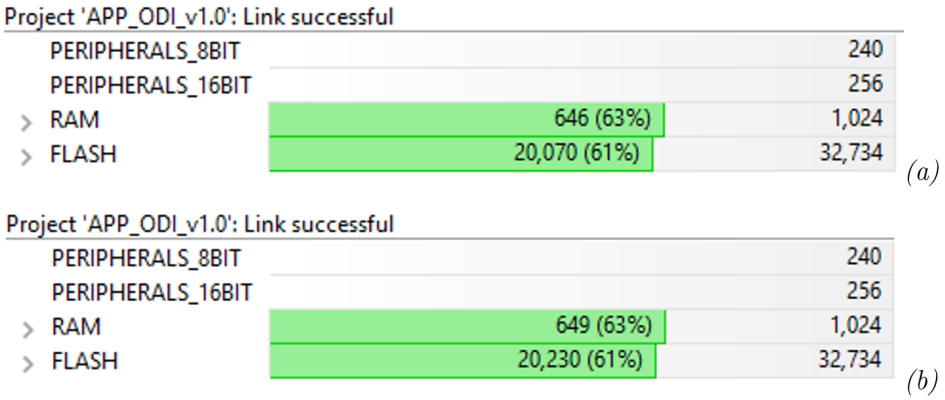


Figure 4.11: Memory map of a platform applied LPP (a) OI_MAC (b) Synchronous protocol

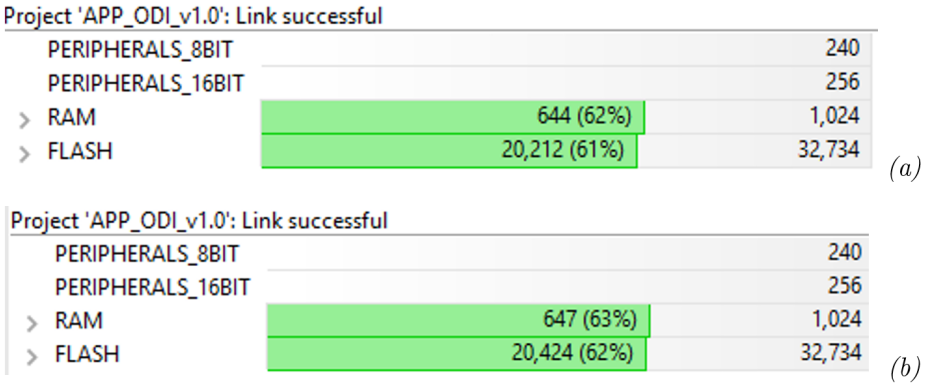


Figure 4.12: Memory map of a platform applied LPL (a) OI_MAC (b) Synchronous protocol

From Figure 4.12 and Figure 4.11, The synchronous protocol requires extra memories for synchronisation algorithms and pairing status. However, the difference of memory usage between the versions of cross-boundary protocols is insignificant. The experimental results confirm the expected benefits as mentions in Section 4.2.3 while the concern about the overhead is disproved as insignificant. Moreover, the results also show that the synchronous protocol can offer a more extended set of the CBT period which can be used for trading off the network qualities with the energy consumption.

However, it is important to note that both cross-boundary protocols contain many similarities in the implementation perspective. In fact, almost every module of OI-MAC is used to create the new synchronous protocol. The additional condition is that the BN will only respond to the recorded partner and not exchange with other nodes from the

neighbouring domains. Other routines of frame type transmissions and receptions are identical. Therefore, the code size will not significantly increase if both versions of the cross-boundary protocol are embedded. Then, the cross-boundary transmission can be switched to adapt for the condition of the cross-boundary traffic. However, the conditions and the details of the process to switch between both versions of the cross-boundary protocols are one of the possible future work in this direction.

4.3 Discussion

The evaluation of the ODI framework has led to a question on the suitability of OI-MAC as the cross-boundary protocol of the ODI framework. According to the reconsideration of the network conditions, the expected data traffic of in the ODI connection scheme should be a burst transmission with a high potential for collisions. The initial measurements of the collective performance of OI-MAC confirm the hypothesis from the pre-analysis. The asynchronous protocol (LPP) employed by OI-MAC is marginally usable in the common scenario of CBT since the contention solving algorithms of LPP is passive. Moreover, LPP induces irregular duty cycles in forms of a random variable. However, the radio occupancy of the ODI processes should be minimal and predictable. The CBT period should be one of the controllable parameters that the system can use as a tool to a tradeoff between the ODI performances and the energy expense.

Considering the conditions of the CBT scenario, this research proposes an alternative solution. Essentially, the new concept suggests a synchronous pair between BNs. A BN from one domain can only connect with another BN from another domain to reduce radio occupancy and avoid contentions. While the concept is diverse, the frame definition and most of the implemented modules can be reused from the modules of OI-MAC.

The comparison of the newly proposed synchronous protocol and OI-MAC has shown considerable improvements regarding network qualities as well as the energy consumption. Moreover, the initial investigation on the concerns about the introduced overheads indicates that the transmission costs are lower than the wasteful transmission in cases of contentions and collisions. Nonetheless, the implementation of both protocol is almost the same concept. Therefore, the cross-boundary protocol can use both synchronous and asynchronous MAC algorithm depending on the circumstances. This topic require more investigation, which can be a future work in this direction.

This chapter concludes the MAC layer of the ODI framework. However, the communication layers only provide a data link between endpoints. The application must exchange data in the regulated format, so that each participant domain can interpret the application data from its neighbours. This topic must be further discussed to enable the actual cooperation via ODI.

Chapter 5

Demonstration of Application Exchange in Opportunistic Direct Interconnection Framework

So far, this thesis has reformulated the ODI framework from the theoretical domain to a practical domain based on a real implementation. Chapter 3 and Chapter 4 have discussed the communication layer that involves the parts of the framework implemented on the resource-constraint platform. However, the ODI framework assumes a centralised model because of the hierarchical structure of heterogeneous networks in WSNs. The framework is formulated under the assumption that resource-constraint platform is governed by a full function platform (Management Node: MN) that manages the sophisticated tasks. Therefore, the fully-functional ODI framework must include the model of the application exchange performed by the MN. In the next step, this research will formulate the concept of the application layer governed the exchange of the application message.

The contents of this chapter are divided into two parts. The first part will analyse the given circumstances of the communication layer together with the existing solutions of the application protocol in a resource-constraint device to derive a feasible solution from the given conditions. The application protocol will be evaluated to show its reliability and the feasibility of using the protocol to support exchanges of the application payload. After the concept of the framework is complete, the second part of this chapter will present a case study of a modelled scenario to explain the details of the complete process.

5.1 Application Protocol in ODI Framework

This section aims to formulate the concept of the application protocol in the ODI framework. The section begins with the reviews of the suggestion from the literature on the application layer of the constraint protocol. Then, the conditions given by the communication layers will be summarised to understand the constraints imposed on the application layer. The application protocol will be designed based on the feasible options, advantages and drawbacks.

5.1.1 Consideration of Application Protocol

The application protocol in this context is referred to the common procedure of the message exchange between the applications of the individual domain. In the traditional sense, the application may include web services, instant message delivery, file transfer etc. The transfer protocol such as HTTP, CoAP [17] and FTP regulates the message transfer of each end-user application on the internet [92, 132]. If the services provided by WSNs are formulated in some forms of web services, the application protocol will correspond to the transfer protocol in the traditional sense. On a broader perspective, the WSN application exchange can be realised in some general form of message exchange. In this case, the application protocol can include other alternatives such as MQTT [15, 123] and XMPP [20, 92]. Following candidates are mentioned in the literature regarding the application protocol of IoT:

1. Advanced Message Queuing Protocol (AMQP) [123, 133, 134] is an open standard for messaging in the RESTful architecture. It is intended for the business area.
2. Extensible Messaging and Presence Protocol (XMPP) [20, 92] is a standard from IETF for message exchanging and XML streaming.
3. Message Queue Telemetry Transport (MQTT) [15, 123, 132, 135] a standard (ISO/IEC PRF 20922) for application messaging in IoT.
4. Constraint Application Protocol (CoAP) [9, 17, 92, 123, 136–138] a standard from IETF for application message in constrained devices.

All of the mentioned options are implemented on top of an IP transport protocol, so they cannot directly implement in the ODI framework, which possesses a different communication stack. However, their concept may be used as a guideline for the application layer of the framework. In this context, the implementation is involved a highly constrained device, so AMQP and XMPP are unsuitable since it natively requires TCP/IP [20, 133]. Moreover, their focus is the chat application on the internet instead of the communication between constrained devices [134, 137]. Moreover, MQTT is unsuitable as it is also

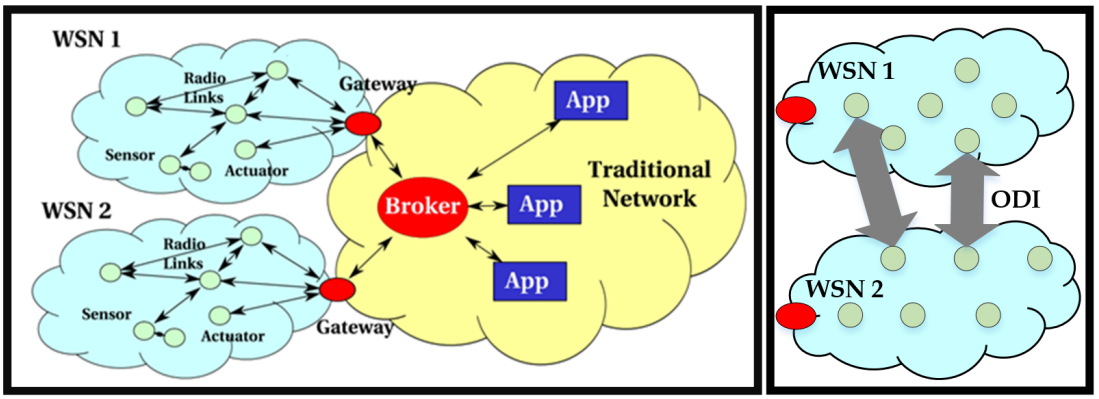


Figure 5.1: (a) MQTT structure for integration of WSNs with the Internet (reproduced from [15])(b) Prospect of WSN local connection with ODI framework

designed on top of TCP/IP [135]. However, there is an update version MQTT-S [15] mainly targeting sensor networks and constraint devices. In the concept, the architecture of the communication provided by MQTT is presented in Figure 5.1.

According to Figure 5.1, the structure of MQTT is converse from the ODI perspective. MQTT defines a broker to coordinate the traffic from subscribers and publishers [15]. Since the traditional network provides the broker, it will violate the idea of ODI that suggests providing the connectivity in the absence of the backbone network. Therefore, this research uses CoAP (RFC 7252 [17]) as a guideline for its application protocol of the ODI framework. As the only option, using CoAP as the guideline can offer the following additional advantages [17]:

1. *CoAP may promote the interoperability of the framework with another system.* As a web transfer protocol in RESTful architecture, CoAP provides a systematic way to map with HTTP [17, 122]. A considerable number of related works also considers CoAP as the future standard of the application protocol in constrained devices [9, 92]. Therefore, if the result is not sharply diverged from the standard, the message of the framework can be mapped back to a CoAP message. This will be the key to promote the interoperability of the ODI framework

2. *CoAP introduces only a small initial overhead.* The fixed header of CoAP is four octets which should be tolerable for the available bandwidth of the communication link.

3. *CoAP is designed for UDP which is the basic transport protocol.* The function of UDP should be conceivable with the available resource.

4. *CoAP proposes an option to perform the block-wise transfer (RFC 7959)* [139]. Considering the constraint of the MTU, the application protocol must offer the fragmentation method. The block-wise transfer in CoAP may be solved the MTU

problems in the ODI framework or at least confirms the possibility of the fragmentation when using the protocol.

It is important to note that this work does not implement the application protocol conforming to RFC 7252 [17] since the conditions of the communication stack differ from the specification. However, the aim is to follow the same concept as far as possible to open the opportunity for the interoperation.

5.1.2 Protocol Design

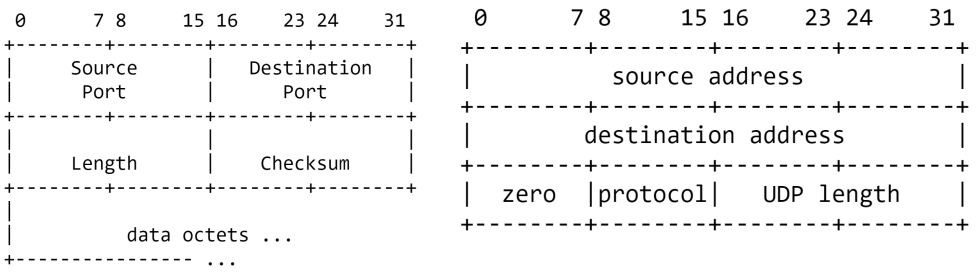
The initial conditions concerning the application protocol are the results of the link characteristics provided by the communication layer. Because the communication layer of the ODI framework uses the same radio chip and the similar concept of the MAC/routing protocol from the original systems, the performances of the ODI communication layer should be in the same dimension of the common system in the term of packet exchange/forwarding. Thus, the concept of CoAP should be reusable in the ODI framework. However, the limitation of the available frame length is the main obstacle to the direct adoption of CoAP. Originally, CoAP is designed for IP-based protocol stack on top of IEE 802.15.4 (see detail in Section 2.3.1). The standard supports the physical frame length of 127 bytes [65, 140, 141]. On the contrary, the available physical frame length in this implementation is 28 bytes which are only one-fifth (21.9 percent) of the specified space. Then again, the assumption of a deficiency of MTU should be a plausible concern, if the ODI framework were to target a native system with a highly constrained device that cannot conform to the standard. Therefore, the protocol design must optimise the frame space while attempting to maintain the main functionality.

5.1.2.1 Datagram Format

In the overview, CoAP [17] is designed for message exchanges in forms of the confirmable/non-confirmable requests/responses of a resource that is provided by a server and accessed by a client. CoAP is designed to use UDP as the transport protocol. The UDP datagram is presented in Figure 5.2(a).

The UDP header is straightforward. It contains the SRC/DST port. CoAP specifies the default port number at 5683 [17]. The Length field gives the length of the payload. A checksum is a 2-octets number required for the integrity check. The general IP datagram format includes SRC/DST address, the padding zero octets, the Protocol field (the value is fixed at 17 when using UDP [16]) and the UDP length (sum of the length of UDP headers and data).

Because the primary concern is the compactness of the design, the redundancy in the header will be elided, and the field with a fixed value will be left out. However, there



(a) UDP Format (b) IPv4 Datagram

Figure 5.2: UDP datagram format (a) UDP header (b) IP datagram format (reproduced from [16])

should be a way to reconstruct the UDP datagram to promote the interoperability. If the datagram is reconstructed in the form of the original UDP datagrams, the default values will be assumed. Figure 5.3 shows the compressed results which are used in the ODI framework.

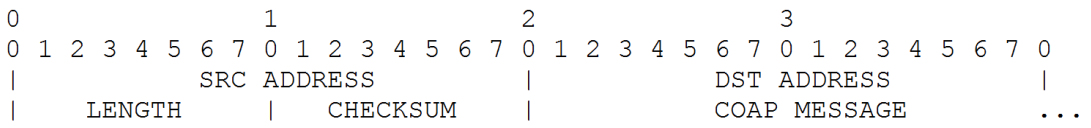


Figure 5.3: ODI Datagram format

The SRC/DST port, zero padding, UDP length, and the protocol number are omitted. The SRC/DST addresses are compressed to 2-octets assuming that the address prefix (NET prefix) is known and exchanged in the handshake process (see Section 3.2.2.2). The Length field uses only one octet since the frame length cannot exceed 255 (1280 supported by IP Datagram, 576 is recommended). The checksum is also reduced to one octet since the frame is more compact than the supported standard. The UDP length and the protocol number are redundant because there is no other option of the transport protocol. The result is a primitive datagram provided only the required functionality illustrated in Figure 5.3.

The designed datagram carries ODI messages as the payload. The ODI messages are defined based on the concept of CoAP. Therefore, the format of CoAP Messages is illustrated in Figure 5.4 for the reference.

The format is already very concise. However, some of the fields can still be modified in favour of the bandwidth conservation. The *VER* field indicates the version of the standard; this field indicates the revision of the standard which may provide a backward compatibility for a future revision. Since the ODI framework is still in the development, this field is omitted assuming the current version at 01. Message ID is defined as a unique 16-bits number for matching corresponded messages together. The *T* field indicates the

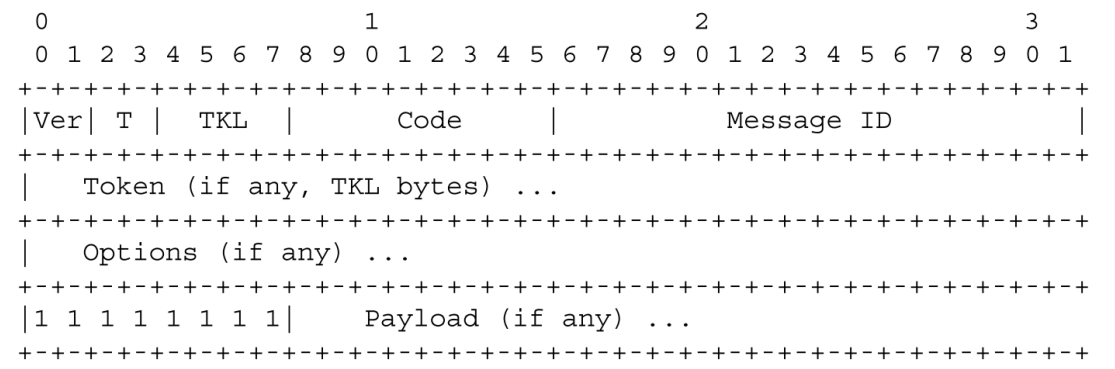


Figure 5.4: CoAP Message format (reproduced from [17])

message type which is critical for the functionality. Therefore this field is preserved and function the same way as the standard. There is four message type defined by CoAP also adopted by the ODI framework as follows [17]:

- *Confirmable Message (CON: 00)* used for requests/responses that must be acknowledged by the recipient with ACK carrying the identical Message-ID.
- *Non-confirmable Message (NON: 01)* used for messages that must not be acknowledged. However, the sender can retransmit the message for the robustness.
- *Acknowledgement Message (ACK: 10)* used for the acknowledgement of CON with the identical Message-ID.
- *Reset Message (RST: 11)* used for a rejection of the CON message and for stopping the retransmission of the NON-message with the identical Message-ID.

The definitions of the message type are defined for message transmission w/o reliability. The transmission with reliability involves the exchange of the corresponding CON and ACK. The retransmission of CON follows the principle of BEB to avoid congestion. The transmission without reliability uses the exchange of NON ensuring the success rate with retransmission under a bandwidth limitation. The application exchange occurs in the form of requests/responses to an operation on a resource. The *Code* field indicates the type of requests/responses in the format of c.dd. The c part contains 3 bits from (0-7) indicating the category of the message. The dd part containing 5 bits shows the details of the particular detail of the request/response. In general, the c part of a request is zero. The dd part indicates the request type. There are four types of requests in CoAP [17]:

- GET (0.01) used for obtaining the specified resource.
- POST (0.02) used for adding new information to the server.
- PUT (0.03) used for an idempotent change or creation the resource (including a creation of the resource).

- DELETE (0.04) used for deleting the specified resource.

Regarding the categories of the response, there are three main categories as follows [17]:

- Positive responses (2.xx) shows the results of the request execution such as Content (2.05), Changed (2.04), Created (2.01), Deleted (2.02) etc.
- Client errors (4.xx) shows that the error originated from the client side such as a Bad request (4.00), Bad options (4.02), Not found (4.04), etc.
- Server errors (5.xx) shows that the error originated from the server side such as Internal server errors (5.00), Not implemented (5.01), Timeout (5.04) etc.

As an example, the client may send a CON (MSG ID: 1)-GET (0.01) to a server to obtain a resource representation. The server may respond with an empty ACK, or the piggybacking response such as ACK (MSG ID: 1)-Content (2.05) or ACK (MSG ID: 1)-Not found (4.04). In the case of an empty ACK, the server may send CON (MSG ID: 2)-Content (2.05) or CON (MSG ID: 2)-Not found (4.04) later.

The *TKL* field in Figure 5.4 indicates the token length in the header. The token is an opaque sequence of 0 to 8 bytes used by the client to match a request and response. It is also one of the security measures in CoAP. For the security, CoAP encourages the client to generate a non-trivial token to guard against spoofing. Nonetheless, the token can be left out with the default value at zero. The ODI framework shortens the max length of the token to four bytes to the limitation of the available space. However, this will also compromise the security concern in favour of the bandwidth. The appropriate tradeoff should be debated in the future. The *options* fields in Figure 5.4 are predefined fields of additional information that are frequently used in the request/response such as the location of the resource, the size, the maximum age, the entity tag (ETAG) etc. The ODI framework adopts all of the definitions of the options from CoAP. After the options, the message must contain a PAYLOAD MARKER (0xFF) to indicate the beginning of the payload. Figure 5.5 summarises the format of the ODI message designed based on the concept of CoAP.

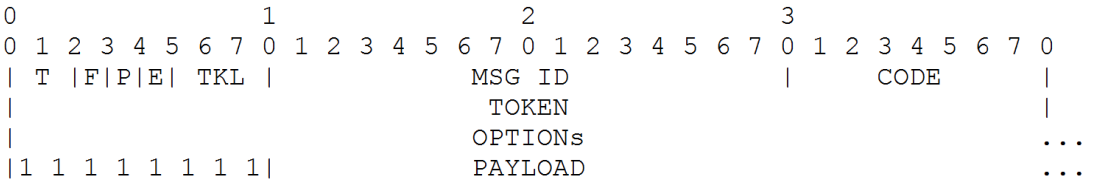


Figure 5.5: ODI Message format

In general, the ODI message adopts every field of the CoAP format except for the version field and the modified token field. However, three extra fields are added in the message format, which is vital for the functionality:

E: 1-bit flag. The *E_FLAG* indicates whether the message is encrypted. This flag provides an interface for the application layer to notify associated endpoints of encryption.

P: 1-bit flag. The *P_FLAG* indicates whether the message is prioritised. The communication layer can check this flag to deliver messages in a prioritised manner if a service for a prioritised traffic exists.

F: 1-bit flag. The *F_FLAG* indicates whether this message is fragmented and containing only one fragment of the CoAP message. This flag is related to the fragmentation defined by this framework. (see details in Section 5.1.2.2).

The security in the CoAP framework is mainly provided by a Datagram Transport Layer Security (DTLS) [17, 142]. However, DTLS cannot be implemented in the ODI framework. The security aspect of the ODI framework is still not deeply covered in this thesis. The author believes the application should handle the encryption of the payload because the application is implemented on the MN which possesses more resources than the leaf nodes inside the network. So, the message format reserves the E_FLAG field for this purpose. However, the detail discussion in this aspect should be considered again in the future work.

The primary concern in this protocol design is the high limitation on the MTU, which is approximately one-fifth of the IEEE 802.15.4. Even if the headers of the ODI datagram are already carefully considered, the remaining spaces in the physical frame are still much less than that specified by CoAP.

5.1.2.2 Message Layer and Fragmentation

To solve the problem of the limited frame space, this work resorts to the message fragmentation. CoAP already possesses two options to accommodate a large payload:

1. IP Fragmentation in 6LowPAN [17, 143]
2. Block-wise transfer in RFC 7959 [139]

However, both solutions cannot be used in the context of the ODI framework because they are designed for a different purpose. Both of them extends the capacity of the communication link that possesses the MTU at 127 to accommodate the IP datagram in the three digits order [17, 139]. In contrary, the ODI framework just only aims to cover an average size payload that can be delivered by a single CoAP message. Regarding the reusability of the conceptual design of both solutions, the consideration undergoes as follows. The IP fragmentation concept is designed for the compression of the IPv6 headers. Therefore, the principle cannot be reused in this context. The concept of RFC

7959 is straightforward; it suggests that the payload should be divided into fragments and the client/server request each fragment individually by using the options BLOCK1 and BLOCK2 [139]. The advantage of this concept is the minimal modifications/burdens on the original purposes, and the robustness since every fragment is requested individually. This concept also opens the freedom to for each system to leave the implementation of the block-wise transfer [139]. However, the considerable bandwidth will be consumed since the number of the extra frames is double as the fragment count increases and as well as the repeated headers of the request, that must be sent in every conversation. This method is more beneficial with the increasing datagram length.

In the context of the ODI framework, the fragmentation is compulsory for its functionality. Also, the considerable number of the fragments is expected. Therefore, the bandwidth usage per fragment must be reduced. To accomplish the target, the framework uses the most straightforward approach. The main principle is the separation of the message layer and the request/response layer. The message layer straightforwardly divides the transmitted body until it fits into the available MTU. The body is defined as the message payload referred to a complete request/response as shown in Figure 5.6.

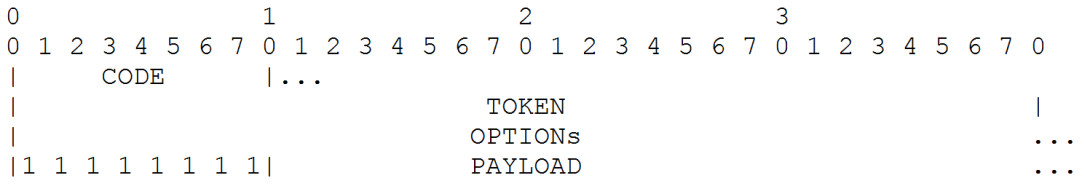


Figure 5.6: The format of requests/responses defined as the message payload transmitted after divided into fragments

The network with more MTU will reduce its frame length to match with the one that possesses less MTU, which is already exchanged in the handshake process. The message containing a fragment is labelled with the fragment number and the full count. The message layer waits until all fragments are retrieved and compose the request/response as if it was sent in one piece. Figure 5.7 briefly illustrates the concept.

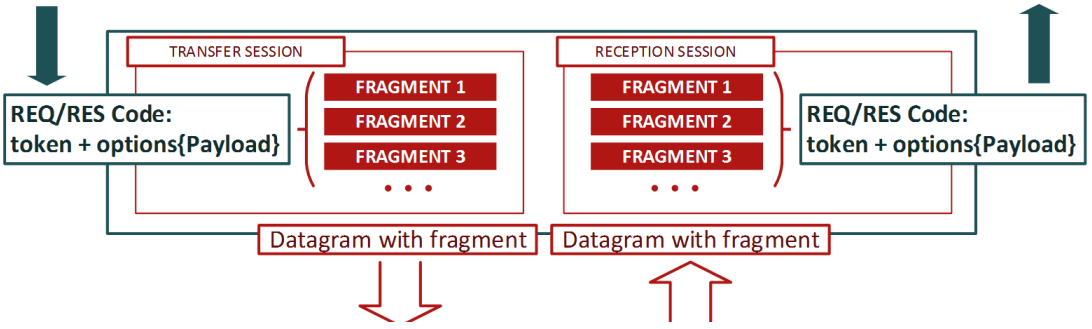


Figure 5.7: Concept of message fragmentation

To perform this task, some modifications are necessary for the message header. Figure 5.8 shows the headers of the fragmented message.

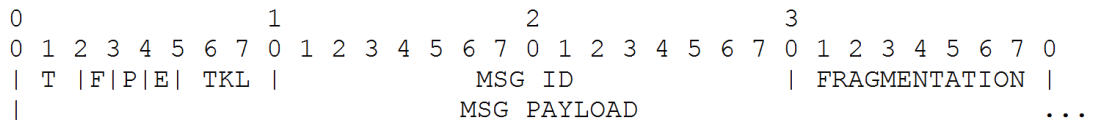


Figure 5.8: Headers of the fragmented message

According to Figure 5.7, the recipient must check the F_FLAG at the reception to distinguish between fragmented/non-fragmented messages. In cases of the fragmentation, the recipient looks at the fragmentation header to identify the fragment number and the full count of the available fragments. The fragmentation header is constructed in the following form:

$$FRAGMENTATION = (FRAGMENT\_NUM << 4) + FRAGMENT\_COUNT \tag{5.1}$$

This formulation straightforwardly divides the fragmentation header into two parts with an equal space at four bits. FRAGMENT_NUM indicates the sequence number of the fragment and FRAGMENT_COUNT indicates the number of the available fragments. All fragments are sent with the same message header, i.e., the same message type and the same MSG-ID. In this way, the original ODI message can be reconstructed even in the format of the CoAP message. Therefore, the message layer proposed in this section could offer an opportunity to send a CoAP message by a communication link which possesses much less MTU than that of IEEE 802.15.4.

However, the fragmentation also results in the concern of the reliability. The success rate of the packet delivery will drop exponentially as the fragment count is increasing. Following equations can show the estimation: Let PER be the packet error rate of the end-to-end communication. $PDR = (1 - PER)$ where PDR is the successful packet delivery rate. The message will be correctly retrieved if and only if all fragments are correctly delivered. Let n be the number of the available fragments.

$$P_{success} = PDR^n = (1 - PER)^n = 1 - P_{failed} \tag{5.2}$$

$$P_{failed} = 1 - (1 - PER)^n \tag{5.3}$$

is the probability of the successful message. P_{failed} is the probability of the message reception failures. A sharp decline of P_{failed} is expected, if the quality of communication link is worsened, i.e., PER is increased. To counter this problem, the message layer maintains the state of the reception to request lost fragments individually (selective acknowledgement) [144]. The procedure is described as follows:

1. A transmission session is created by the sender to set a time for the first transmission by a uniform random variable $[T_{ACK}/2, 3T_{ACK}/2]$ where T_{ACK} is the estimated waiting interval for am response message ACK/RST.
2. At the first transmission time, the sender sends all fragments together and set the ACK time out for a retransmission.
3. The recipient creates a reception session when a fragmented message is received. The session sets a counter for a reception time out.
4. When all fragments are received, the reception session reconstructs the request/response for the application.
5. At the reception timeout, the session will send a fragment request per each required fragment and set another reception time out. At the third reception timeout, the message reception is regarded as a reception failure, and the session is ended.
6. The sender is receiving a fragment request sends the corresponding fragment again.
7. At the retransmission time, the sender repeats all fragments. The transmission session is ended after the retransmission quota is empty and T_{ACK} for that retransmission round is reached or at the reception of the corresponding ACK/RST.

The fragment request used the RST message with the fragmentation header as described in Figure 5.8. By this method, the framework requires the system to maintain a reception state, which can be considered as a drawback. However, the process is necessary for delivering a sensible message size for the application payload. This method also limits the size of the message payload because the fragmentation header uses only four bits to encode the fragment count resulting in the limitation at 15 fragments. The limitation of the fragmentation comes from the following considerations:

1. The probability of the success is exponentially lower as the fragment count is increased.
2. The shortage of RAM in the intermediate constrained platforms, which can store only a limit number of datagrams.

If the real exchange flows as the consideration in this session, the concept in this section should provide a way to deliver the application message with the similar functionality of a CoAP message as long as the end-to-end PER of the system is low enough.

5.1.2.3 Message Size

To accommodate an application message by a datagram with very small MTU, the fragmentation concept is proposed according to Section 5.1.2.2. Considering the fragmentation method, this section will analyse the result of the concept.

From the available physical frame length at 28, the native MAC/routing protocol uses 7-8 bytes for their headers. The ODI datagram occupies six bytes, and the fragmented message headers take four bytes. Therefore, a single ODI datagram can carry 10-11 bytes of the message payload (FRAGMENT_SIZE). In consideration of the fragmentation, the body size (MSG_SIZE) is equal to the product of FRAGMENT_COUNT and FRAGMENT_SIZE, i.e., up to 150 bytes.

FRAGMENT_COUNT tells the allowed number of the datagram fragment of one message. The suitable value of FRAGMENT_COUNT is depended on the system conditions such as the quality of the communication link and the available memory of the implemented platform. The FRAGMENT_SIZE can also be varied if the physical frame length or the communication headers size are changed in other implementations. The result of the permitted message size in this implementation is 50 bytes (FRAGMENT_COUNT = 5, FRAGMENT_SIZE = 10). The MTU in this implementation should already reflect one of the outermost cases. The application should be aware of the limitation on the MTU to ensure the reliable network capacity.

5.1.3 Application Exchange

In Section 5.1.2, the application protocol of the ODI framework governing the message exchange is discussed using the concept of RFC 7252 as the template. In this section, the overview of the application exchange will be discussed. The aim of this section is just to present the broad notion of how data exchange in the limited bandwidth can offer the useful information exchange in the application logic. The exact solution regarding the proper semantics, representation and management of data in the constrained device is still an open research question, which is out of the scope of this research.

5.1.3.1 Data Model in Constrained Networks

There is two architectural design of the applications mentioned in the contexts of IoT [145]: 1) Service-oriented architecture (SOA) [49, 125, 146] 2) Resource-oriented architecture (ROA) [19, 137]. Choosing the architectural design is domain-dependent because the design concept is linked to the preferred application protocol, semantics, representation and serialisation. SOA often uses the semantics defined by Web Service Description Language (WSDL) serialised by XML-based Simple Object Application Protocol (SOAP) [19,20,147]. Alternatively, ROA presents data as a web resource, which is accessed and manipulated by the common interfaces provided REST operations [19,145]. The advantages and drawbacks of both architectures are debatable. Some mention the standardisation and rigidity as the advantages of SOAP, while REST offers the simplicity with less computational resources and overheads [19, 92]. This work develops a

highly constrained system based on REST operation, thus choosing the concept design of ROA due to its background.

In ROA, the web resource uses the semantics defined by the Resource Description Framework (RDF) [18] to express the relationship between data in a resource model. An IRI (previously URI) uniquely identifies a resource and the method to access the resource. The RDF statement is expressed in the form of the triple composed of *Subject node predicate Object node* [18,148]. An IRI can represent all components of the triple. However, a node can semantically include a blank node or a literal. Combining many statements allows the description of a structured data such as a class and its properties. Figure 5.9 visualises the structure obtained by the concept.

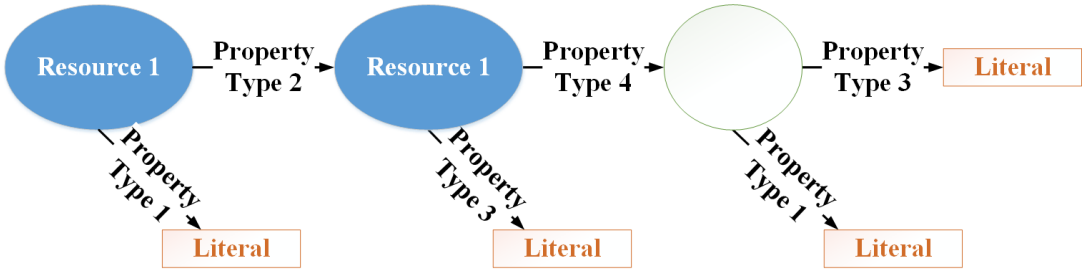


Figure 5.9: Generic RDF graph notations described structured data with a resource model [18]

Figure 5.9 shows how the data structure can be formed by assigning the property value as a literal (primitive data types) or a nested resource, which possesses its own properties [148]. It should be noted that the property type could also be used as a subject node or an object node in other definition. This concept is widely used in traditional web services and increasingly adopted in constrained networks. However, some contexts may need to be revised. An abstract RDF model can be serialised in many forms. The well-known formats include the XML-based document (RDF/XML) and the JavaScript Object Notation (JSON) [18,149]. JSON is the simplified lightweight option in comparison to the XML counterpart in the plain text form, while XML offer more standardised features at the cost of its verbosity [150]. Figure 5.10 shows an example of the serialisation of a resource in JSON.

Even though the abstract data model is identical, the method of the serialisation strongly influences the size of the output stream [150, 151]. In M2M interface, the serialisation method can sacrifice the human readability in favour of the compactness using compression or binary encoding [152]. Many works propose the solution in this direction such as Efficient XML Interchange (EXI) for XML documents [150], CBOR for JSON [153] and other binary formats [151]. However, it is still an open research question in the area of constrained networks. Some works propose resource naming schemes [122, 141], generally suggesting the compact name of resources/properties [17,136]. The suggestion also includes using binary strings as URI instead of a readable text [92, 122].

```
Client: REQ GET /ODI

Server: RES 205 Content
ContentType: Application/JSON
        [   {   "Uri-reference" = "/ev",
                "rt" = "fire-alarm-ev",
                "if" = "observe"
            },
            {   "Uri-reference" = "/temp",
                "rt" = "temperature-c",
                "if" = "sensor"
            }...
        ]
```

Figure 5.10: Response message obtained by a GET request on a root URI of a sensor node [19–21]

5.1.3.2 Data Access

The defined request in the form of the REST operations (GET, POST, PUT and DELETE) is the standard interface to access the data in RESTful web services [17]. In general, the GET request with a specific URI is used by the client to obtain the resource representation from the server such as the sensing data, services or status of the physical/logical node. As an example, GET /temp is used to obtain the temperature data on the physical device [17, 154]. If a binary string expresses the URI, the output stream of the request message can be further shortened (GET /temperature-resource-ID (1-2 byte)) [122]. CoAP also provides a method to subscribe to an observable resource using the observe message option [155]. As an example, GET /temp Observe: Registering will register the client to the observer list of the server. The client is subject to be notified when the state of the resources is changed. The PUT request can be used to control the system parameters [17, 155] such as changing the frequency of the sensing samples or setting a new duty cycle. As an example, PUT /dev data-interval: 30 may set a new interval between two consecutive routine reports. The application should concern about the limitation on the communication link [17] to avoid degradation of the network qualities due to congestion or fragmentation. The block-wise transfer can also be used to accommodate a bulk payload [139].

Before accessing the available resources hosted by any server, the client must know the URIs of the resources and necessary information about the resources. Exchanging the meta-data describing the available resources is defined as Resource Discovery. In the ODI framework, the ODI resources must be exchanged in the negotiation process. The ODI resources are referred to the specific resources that participants can trade with each other via the ODI link. The Constrained RESTful Environments (CoRE) or RFC 6690 [22] provides the guidelines for exchanging the meta-data of the resources in the form of web linking. The process is performed by a GET request to the well-known interface (GET /.well-known/core). A similar concept can be employed for discovering ODI resources in

the negotiation process. Figure 5.11 shows one of the possible suggestion on the resource discovery used in ODI.

```
Client: REQ GET /ODI

Server: RES 205 Content
ContentType: application/link-format
        </ev>;rt="threshold-ev";if="event";sz=64;obs,
        </temp>;rt="temperature-c";if="sensor";obs;
```

Figure 5.11: example of message exchange in the negotiation process [17, 22]

In general, the principle of the resource discovery described in the RFC 6690 [22] is applied. The *rt* field describes the resource type of the dereferenced URI. If the client reads this field, it supposes to learn about the type of the resource with a predefined semantic description. It may also contain a link to the resource description. In the same way, the *if* field declares the interface for the resource. Reading the field should lead to the understanding of the standard procedure on the resource. The value of this field is expected to be reused on multiple resources with the same interface. The *sz* field tells the estimated size of the resource, this is useful information for the application layer to assess and manage the data exchange in the concerns of the network/computational resources. It may be used to decide on the method of requests and responses or whether the client can process the resource with the available memory. The field can be omitted if the size can be contained in one MTU. The *obs* field indicates that the resource is observable. Any client can register to the resource by a GET request with the *observe* option [155].

Even though this section reviews the data model and its representation, this topic is outside the scope of this thesis. However, the topics must be mentioned and reviewed since this thesis intends to demonstrate the framework by using a case study. The demonstration cannot be achieved without involving a basic form of the application payload. Therefore, the general idea of the concepts mentioned in this section will be used in the case study. The technical aspects of implementing the full capabilities of web APIs on top of the ODI link require more research works, which will be suggested as the research opportunity in the same direction. In this implementation, the request and response payloads are hard-codings, only some functionality relevant to the project are implemented to simulate the real application exchange.

5.1.4 Discussion

As the study on the opportunistic direct interconnection between WSNs continues, this research reaches the point of the application protocol design. At the level of the application layer, the design of the application protocol is heavily influenced by the constraints of the communication layer. As a result, the priority of the design is shifted to the

conservation of the bandwidth/frame space usage since the MTU of the communication is highly limited. Although the implementation is case-specific, it leads to the different viewpoint on the implication of the application protocol that could benefit some related area in the future.

Using CoAP in the RESTful architecture as a guideline, this research attempts to accommodate the sizable payload on the highly limited MTU. The attempts lead to the suggestion on the elimination of the redundancy of the message headers while maintaining the concept of the request and response provided by the REST system. The message fragmentation is also reviewed and proposed as the solution for a network with a limit MTU. This section also gives the overview of how the application data is modelled and exchanged. In general, this thesis supports the idea of adopting the web semantics in ROA design into the context of constrained networks. However, some significant improvements may be possible if the contexts of constrained networks are attentively considered in the design. For example, the bandwidth usage of the application data could be decreased under the assumption that the human readability of the data representation can be compromised in M2M interfaces.

In this section, this thesis has already formulated the concept of the application protocol for the ODI framework, which covers the whole structure of the protocol stack. Therefore, the next step is the evaluation and demonstration of the proposed concept.

5.2 System Evaluation

In this section, the ODI framework will be evaluated to understand the effects of the network conditions on the performances of the framework. This section only aims to show the qualitative relationships between the collective network qualities and the network conditions over the quantitative results because a single implementation can not evaluate the performance of the concept. Preferably, it should be evaluated in many cases. Although the exact values of the measurements in this implementation cannot represent the actual performance of the framework, it still shows the relationships between quantitative metrics, which promotes the understanding of the system characteristics.

5.2.1 Experimental Setup

For the experiments, the PC connected with an eZ430-RF2500 platform by UART acts for the central platform, which plays a role of a Management Node (MN) and the Sink Node (SN). The remote nodes are composed of up to 12 eZ430-RF2500 platforms depending on the set conditions in the evaluation method. The reduced function of the RESTful interface is programmed by a Java application on the PC following to the concept described in Section 5.1.

The JSSC libraries are used to program the UART connection in the Java platform. The received frames from the serial communication are reconstructed in the form of ODI datagrams (in Figure 5.3). The message layer collects/requests the fragments of the message payload according to the procedure described in Section 5.1.2.2. The characteristics of the implemented application interface can be described as follows:

1. The application interface can send a GET/PUT with simple message options such as Observe, URI-Path, Content-format and Size1 specified in RFC7252.
2. The response codes that use the interface are 205 Content, 204 Changed, 404 Not found and 400 Bad requests.
3. The client can perform the resource discovery by sending GET /ODI to the server. The server sends a resource list in a binary-encoded core link format.
4. The request and response are carried by CON messages. CON messages are marked with P_FLAG, i.e., they are prioritised by the associated networks. The prioritised datagrams are excluded from buffer overflows. The datagram carried CON messages can be overwritten with the messages at the same priority level. NON-messages send all regular generate data traffic such as the sensing data and observable contents without priority.
5. The application interface limits the number of sessions and the number of fragments that are sent in parallel to be less than the capacity of the intermediate node.

The experiments aim to understand the characteristics of the ODI framework regarding the reliability and the latency. Many factors in the communication link can influence the reliability and latency. However, the fragmentation and the hop distance are chosen as the network conditions in the scope of the evaluation since both variables show the direct effect of the application protocol design.

1. The fragmentation is necessarily proposed in this design as the compensation of the limited MTU. However, this experiment can prove the usefulness of such strategy for individual domains that possess the physical frame length less than specified by the standard.
2. The hop distance can represent the scale of the network if errors of the routing protocol are decoupled from the experiments. Under the assumption that the routing protocol can find an optimal forwarding route to the required destination, the hop distance will grow with the size of the network. Measuring the effects of the hop distance should approximately tell the effects when the participant network scales.

The measurement is designed as follows to answer the objectives of the experiments:

1. The reliability and latency are measured in this experiment. The evaluation metrics involved the success rate of the data transfer and the message travelling time.
   - The success rate is represented by the expected value and the 95-confidential interval ($\bar{x} \pm 1.96\sigma_{\bar{x}}$). The samples of the success rate are calculated from the ratio of arriving messages and the total number of the sending request in every 100 messages.
   - Travelling time [ms] is measured at the application front-end using timestamp. The client will send GET /time to the server. The server send 205 Content t: timestamp (8 bytes).
2. The hop distance between message endpoints (MNs) is varied by increasing the number of the intermediate nodes, while the request and response of the resource representing the system time are executed the statistics of the success rate and the travelling time will be recorded. The routing protocol is disabled in the experiment; a static table determines the forwarding route to fix the hop distance and eliminate the effects of fuzzy route changing from the routing protocol.
3. The size of the resource representation (10-50 bytes) is varied to change the number of fragments (1-5). The statistics of the evaluated metrics (PDR and travelling time) are recorded.

Figure 5.12 shows the hardware setup in the experiments discussed in this section.

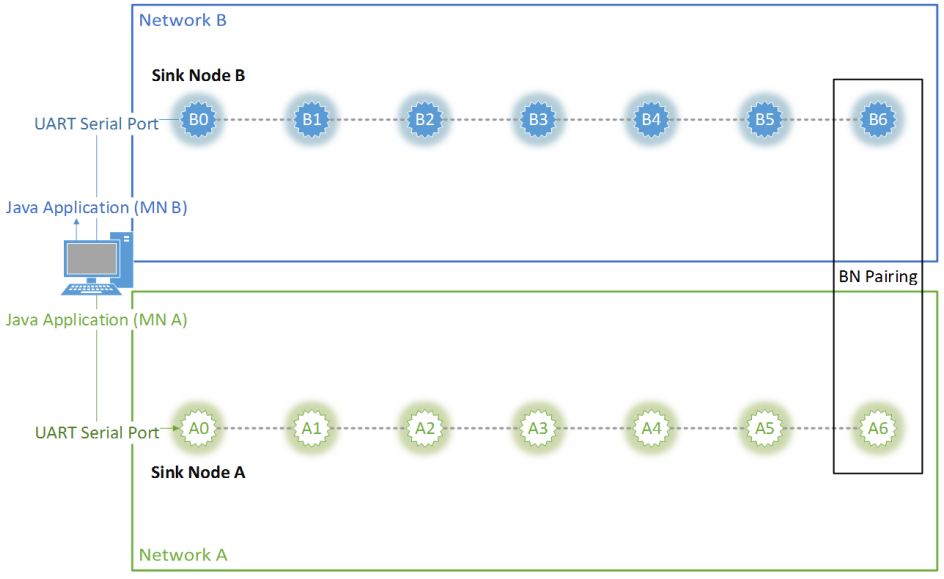


Figure 5.12: The experimental setup for evaluating the effects of the fragmentation and the hop distance on the reliability and latency of the framework.

5.2.2 Hop Distance

The hop distance represents the network scale, which is the important factor for network qualities. In this experiments, the acknowledgement is used in hop-to-hop communication. Therefore, only the buffer overflows can cause the packet loss. Moreover, requests and responses are carried by CON messages which are protected from the packet overflows; this means every node refuses to overwrite the datagrams with CON messages, instead of overwriting the routine reports or NON-messages, in cases of buffer overflows. Therefore, it is expected that the success rate of the delivery should be very close to 1.0. However, the delivery error can happen if the datagrams are delivered very late, and the transmission session ends before the response comes or the CON messages are duplicated because of the hop-by-hop retransmission. Not only the success rate of the ODI messages but the impacts on the internal communication should also be concerned. In usual cases where the network bandwidth is sufficient, carrying ODI messages do not affect the success rate of the internal data. However, the worst case that the network bandwidth is already exhausted by the internal communication is investigated. In this experiment, each node generates a sensing data message in every second. The results in Figure 5.13 are obtained from the measurements:

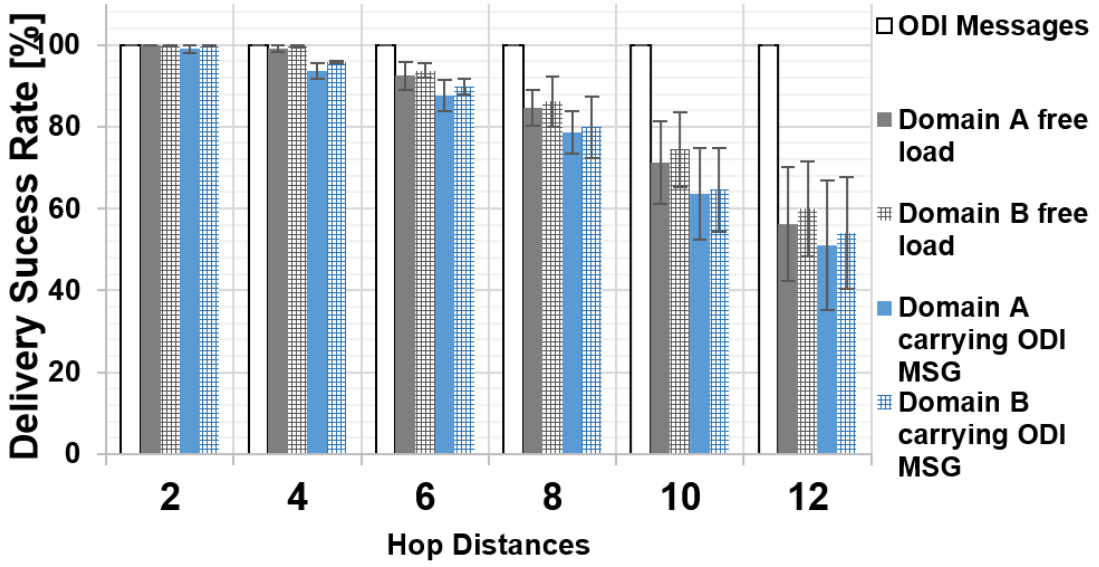
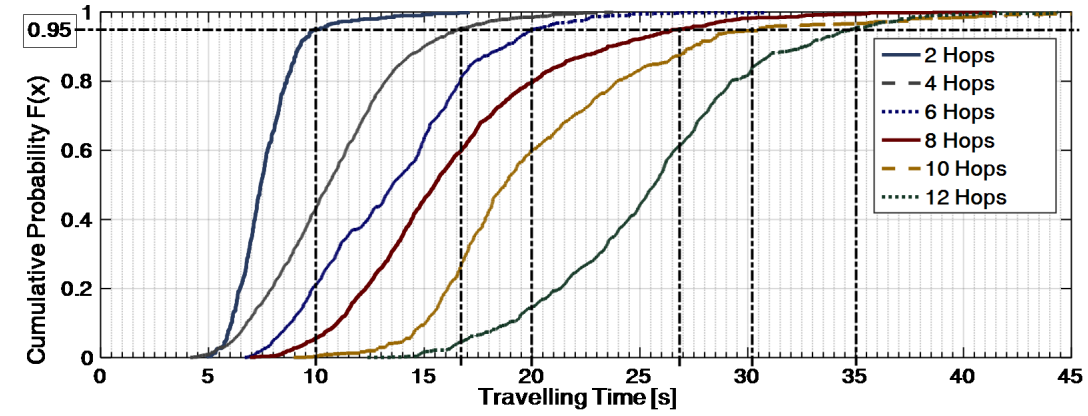


Figure 5.13: Delivery success rate (1000 messages) of associated domains in ODI scheme showing the impacts of ODI messages when network bandwidth is entirely used.

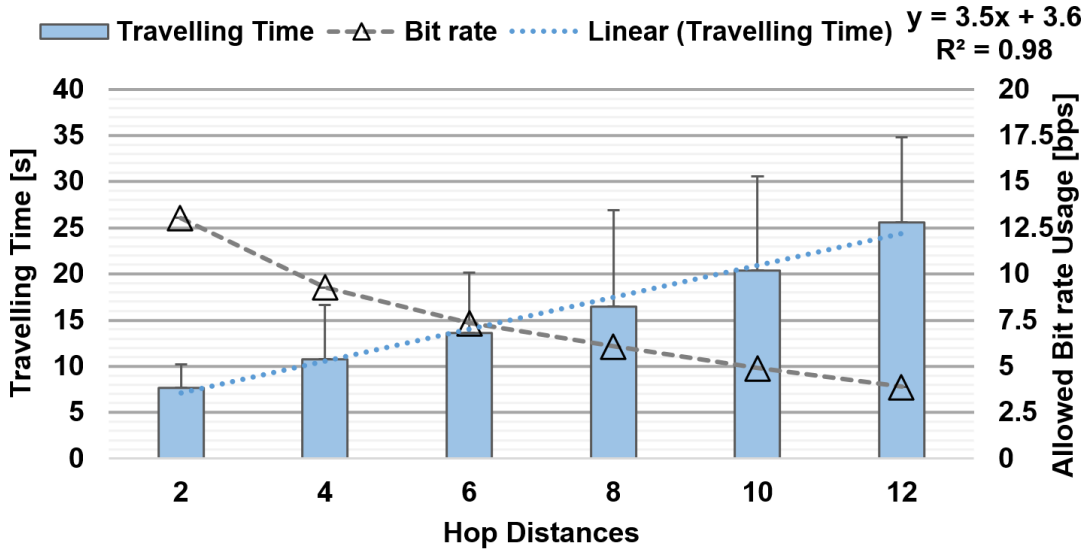
The experimental results show the expected trend of the delivery success rate all request and response is delivered successfully in any hop distances, even though the regular data rate already saturates the available bandwidth. This result implies that the error rate of the ODI message delivery in this setting is lower than 0.001 since one thousand message are collected in the measurements. However, this method assumes the associated networks possess a scheme for QoS differentiation and willing to give priority to the ODI

messages. The success rate of the internal routine data is decreased gradually with the hop distances since the additional data are generated by the increasing number of nodes. Contrary, the bottleneck effect reduces the network bandwidth causing the probability of the buffer overflow. However, the number of sessions is limited by the application interface below the full buffer capacity of the intermediate node. Therefore, only limited numbers of ODI datagrams are in the forwarding route at a time (ten datagrams in this experiments) resulting in the controlled impact scale of the ODI exchange on the implemented systems. Figure 5.13 shows that the delivery success rate of the internal data is marginally lower than the original delivery rate.

If the reliability is acceptable, other network qualities can be further considered. In this experiments, the latency of the ODI message represented by the end-to-end travelling time. The results in Figure 5.14 are obtained from the measurements, regarding the latency of ODI messages:



(a)



(b)

Figure 5.14: a)Cumulative distribution function of travelling time of messages between Sink Node A and Sink Node B (b) Expected value of travelling time in a 95-percentile range in a relationship with hop distances.

The latency of any system is usually defined by cascading random variables, which are subprocesses of the whole process. In this cases, the process includes the processing time, the serial communication, the hop-by-hop transfers and the cross-boundary transmission. As the hop distance increases, more random variables of the hop delay are cascaded to the process, resulting in the higher deviation of the samples as can be observed from the CDF slopes in Figure 5.14. The expected values and the 95-percentile of the samples show the approximately linear relationship with the hop distances (3.5 seconds per hop and 4.94 seconds per hop) since increasing hop distance adds more random variables with approximately the same characteristics. Because the application interface limits the number of simultaneous datagrams, the upper boundary of the bit rate usage (D_RATE_{upper}) can be mathematically implied from the latency as follows:

$$D\_RATE_{upper} = \frac{(N_l B_d)}{T_d} \tag{5.4}$$

where N_l is the limitation of the allowed datagrams, B_d is the bit capacity of the datagrams and T_d is the delivery time (travelling time) of datagrams. In this case, there is no fragmentation expected. Therefore, five sessions of requests are allowed in parallel resulting in the maximum number of the travelling datagrams. Therefore, the exploitation of the bandwidth allowance, in this case, is very close to the maximum limits. The bit rate usage of the ODI messages is illustrated in Figure 5.14. The allowed digital bandwidth usage of ODI application is lower as the hop distance decreases. This recommendation improved the reliability and reduced the impacts on the original system at the same time.

5.2.3 Fragmentation

In this implementation, the fragmentation is necessary. However, if this concept is feasible, it may benefit other systems, which possesses low MTU of datagrams. Using fragmentation should be avoided whenever possible. In this section, the effects of the fragmentation will be evaluated. The automatic session is set to request the resource with different sizes ranging from 10 to 50 bytes. The delivery success rate is recorded along with the travelling time measured from the point where the server receives the request until the response body is reconstructed at the client side. The hop distance is set at 12 hops to see the effects of the fragmentation at the considerable scale. The measurement of the delivery success rate is shown in Figure 5.15.

Some losses of the ODI messages is detected in the fragmentation cases. This result is caused by the stability of the pairing between BNs. The conversation is disrupted by the BN temporarily loses the connection with its partner, These occurrences seem to repeat in a long period, when it happens the ODI messages overwrite each other at the boundary. Regarding the impacts on the original systems, the fragmentation does

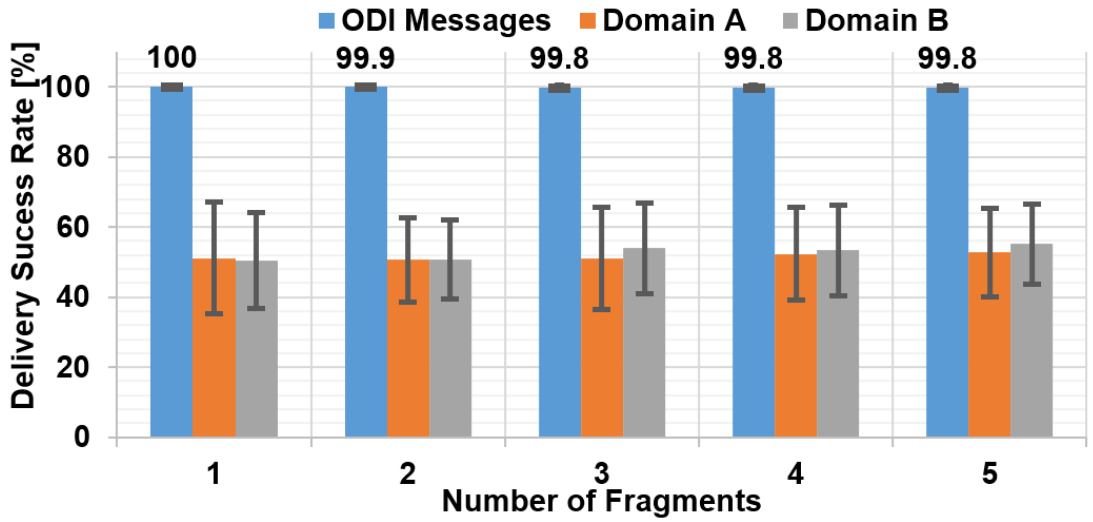


Figure 5.15: Delivery rate of ODI messages when the messages is fragmented at 12 hops between endpoints and the impacts of ODI messages on the original systems

not worsen the success rate of the internal communication since the numbers of the simultaneous datagrams is limited. In fact, there is a slight improvement in this aspect as the fragments are increased because some fragments must be extra requested and retransmitted resulting in the lower bandwidth usage of the ODI conversation. This results can be seen more clearly in Figure 5.16.

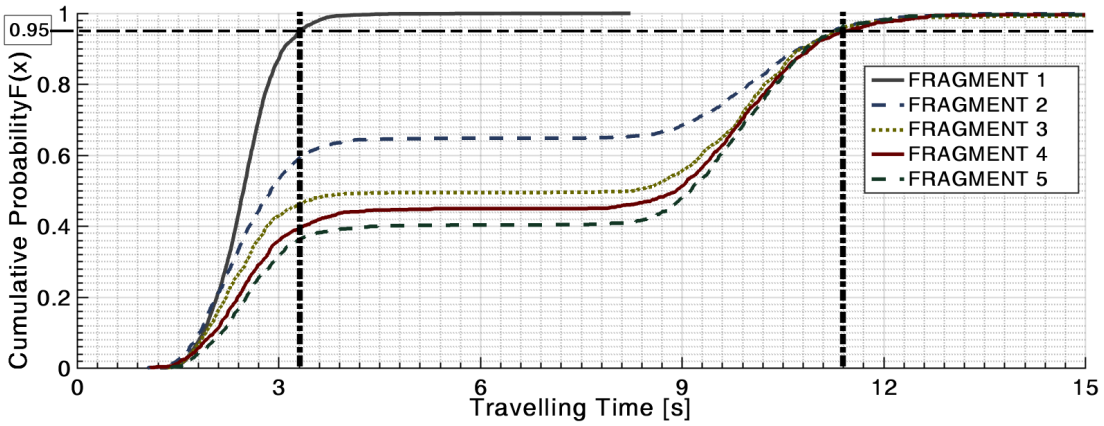


Figure 5.16: Cumulative distribution of fragmented ODI messages

In Figure 5.16, the cumulative of the experimental captured frequency of data samples show the significant effects of the fragmentation. If the messages are fragmented, the probability that the completion of the messages requires an extra round trip is high. The horizontal lines in the graphs of the CDF show the probability when some fragments are lost at the initial responses. The 95-percentiles of all fragmentation cases located at approximately the same point. Figure 5.17 shows the expected value and the data rate of fragmentation cases.

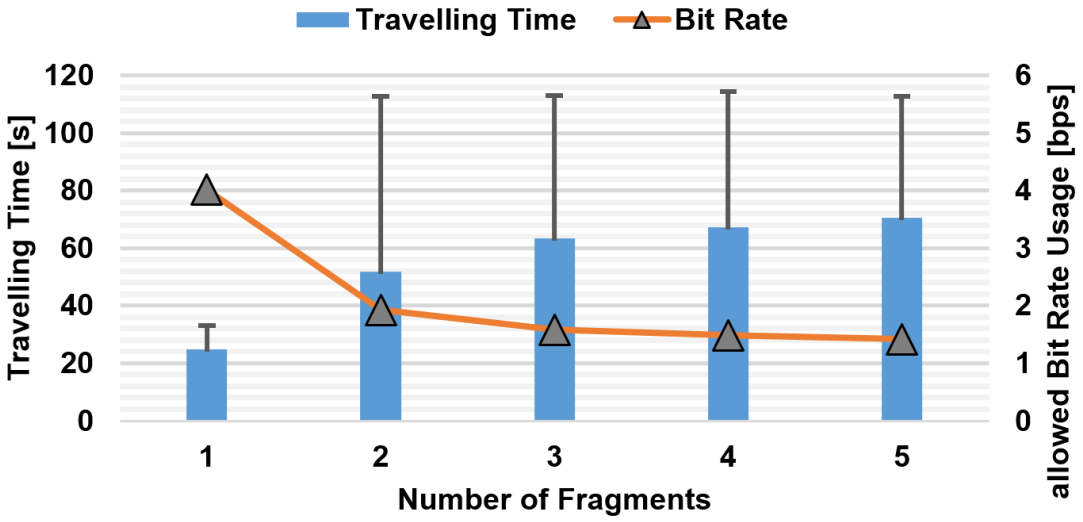


Figure 5.17: Expected values and 95-percentiles of travelling times and allowed bit rate usage of ODI messages in cases of fragmentation.

This fact confirms when the fragmentation is executed, the quality of the data transfer is dramatically decreased. The bit rate decreases approximately by half when messages are fragmented because messages may require another round trip to complete the lost fragments. However, the differences between a high and a low number of fragments are marginal since the messages can be completed in the second request.

5.2.4 Discussion

In this section, the effects of the hop distances and the fragmentation are chosen as the conditions for the evaluation since both are important factors in the design of the protocol used in the lossy constrained networks. The hop distances increases and spread the delay time of the messages. The limitation of parallel datagrams can enforce the reliability. However, this reliability comes with the costs of the available bandwidth, which is relatively low at 4 bps (12 hops). Further investigation is performed to observe the reliability of the fragmented messages at the furthest distances in this setting. While the reliability of the delivery is acceptable with the error rate of the delivery under 0.01, the QoS is dramatically decreased whenever the fragmentation is executed. However, in comparison among the cases of fragmentation, the number of fragments does not significantly change the network qualities.

5.3 Case Study

So far, this thesis has formulated the ODI framework by learning from an actual implementation. Although the components of the framework are evaluated in certain aspects

to point out the functionality and the characteristics of the system, the overall process may be unclear as the components of the framework are mentioned separately. A case study should provide the comprehensive overview of the operational processes and also highlight the benefits of the framework at the same time. Therefore, this section uses a case study to perform the full operations of the ODI framework by supporting the conversation of the cooperation between WSNs that employs the ODI framework in their system.

5.3.1 Scenario

For the demonstration, the cooperation between environmental monitoring systems is constructed. A testbed of 12 EZ430-RF2500 platforms performs all communication process in the experiments. It is important to note that the focus of the implementation in this section is the communication processes, not the evaluation of the real application functionality of the systems. The implementation does not intend to evaluate the exact performance of a particular case, but to show the feasibility to support the application exchange of the cooperation scenario to enable the cooperation scheme. Figure 5.18 illustrates the background of the scenario.

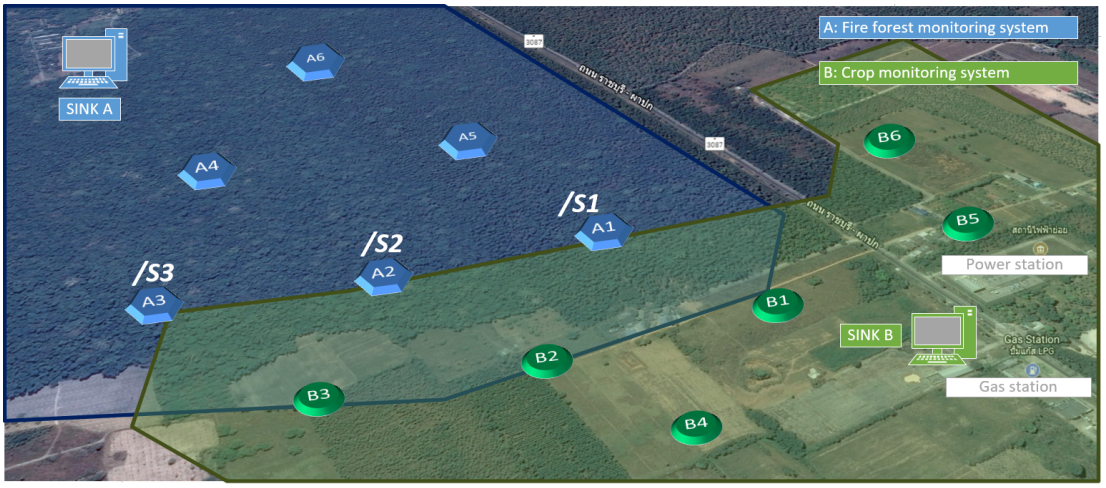


Figure 5.18: Scenario used for case study of cooperation between forest monitoring system and crop monitoring system

The scenario in Figure 5.18 is used to explain the situation and the motive of the cooperation. The topology of the sensor nodes is constructed at the approximate scale 1:100. The modelled scenario is described as follows; the forest monitoring system is first deployed by a government sector to observe the conditions of forest and detect wildfires. System A depicts a cluster of the deployed WSNs, which covers the area around a square kilometre near the residential and agriculture area. Later, the local community decides to deploy a crop monitoring system (System B) close to the forest area to monitor the soil moister and the chemical substances in the fields. The sensor nodes are located

approximately 300-500 meters apart from its neighbour in which the reliable radio link of sub-GHz bands between the next neighbours should be reliable.

Both systems have preinstalled the ODI modules according to the ODI framework to support the opportunistic direct interconnection with a co-located neighbour. Since some of the sensor nodes in both domains are in the reliable radio coverage of each other, both domains will discover each other and negotiate the cooperation scheme. In the user level, both domains gain some benefits from cooperation. In the viewpoint of the government sector, the reliability of the wildfire alarm will be improved if the alarm message is directly established. However, since the gas station and power station of the local community are stationed in the proximity of the forest, the wildfire event can potentially inflict significant damages to the infrastructure. Therefore, the local community will cooperate with the government and allow the wildfire message to be forwarded across their network domain. Moreover, some information provided by the forest monitoring system may be useful to the farmer, which can be used to regulate their agriculture activities. The sequential process in the cooperation scheme will be described in Section 5.3.2.

5.3.2 Processes in Communication Layers

System A employs LPL with strobed preambles as its MAC algorithms. Platforms in System A harvest energy with a solar panel enough to power its operations. System B uses LPP as the MAC protocol. Both are assumed to use its specific routing algorithm that satisfies the prerequisites for the ODI framework (see Section 3.3). However, in the experiments, the routing algorithm described in Appendix B is used. The parameters setting is recorded in Table 5.1.

The transmitted power is set at -10 dBm to create the topology in Figure 5.18 (two multi-hop domains with six nodes) on the 1:100 scale. The duty cycle of System A is set higher than System B. System A periodically sends the ODI BEACON periodically in every 30 seconds ($T_{NDS}/(1 + k_{Robust})$) to search for the potential neighbour. Then, System B is later deployed in the radio coverage, and each node in System B listens for CCH in the T_{NDS} interval, thus receives an advertising frame from System A. The details of the exchange is described in Section 3.2. After the successful neighbouring discovery, the handshake process begins. The associated node samples the CCH periodically in every 12 seconds to exchange ODI BEACON to exchange some update information such as hop distance and ODI period. The encounter between paired BNs must continue consecutively until the stability count is reached. If the connection persists, the status of the ODI link is regarded as paired. Every time, the stability counter is saturated (at 10 in this case study); the synchronisation error will be adjusted. BN stores only the minimum waiting time for its partner in every round of the stability count. The minimum waiting time is considered as the synchronisation error. If it is out of the

Parameter	System A	System B
Physical layer Setting		
Retransmission Attempt	3	3
Tx Power [dBm]	-10	-10
MAC Setting		
Dwell Time [ms]	16	16
Average Wakeup Period [s]	1	2
Sink Wakeup Period [s]	0.5	0.5
MAC Algorithm	LPL	LPP
Application Setting		
Average data generation period [s]	10	30
Cross-boundary data generation [s]	60	-
ODI Setting		
Neighbour Discovery (T_{NDS})[s]	60	
Robust Coefficient (K_{Robust})	1	
Repetition of ODI BEACON	1	
ODI period (T_{ODI})[s]	12	
Synchronisation error range [ms]	100	
Stability Count	10	

Table 5.1: Parameter configuration of the case study is presenting the cooperation scheme between two network domains.

setting synchronisation error range. The counter rate of the ODI event will be adjusted. The associated nodes then put the information of the discovered neighbouring domain to the MN. MN responses the put message with the local name (2-byte address) of the network domain. After the reception of the response from MN, the status of the cross-boundary connection is confirmed. The associated node then becomes the legitimate BN ready for the exchange of the application payload across the domain boundary. The routing protocol will be informed to configure a new forwarding route to this node as the intermediate endpoint to the neighbouring domain. Figure 5.19 illustrates the overview of the low level communication process.

The BN sends the status of the ODI connection whenever the stability count is reached. The status is an unsigned character containing binary flags indicating the paired/unpaired status, the pending/no_pending status, etc. A PUT request will be sent with a confirmable message if the status of the ODI connection is changed between paired and unpaired. Otherwise, the status report will be sent with a non-confirmable message. When MN has received the PUT /BN request, it reads the NET ID. In the case that the NET ID exists, it updates the resource properties included in the request body, otherwise, create a new neighbouring domain record. Upon creating a new neighbouring domain record, MN pings the neighbouring domain with an empty message to check for the end-to-end connection. As the end-to-end connection between MNs of the associated domains is confirmed, the handshake process ends, and the negotiation process can begin. In the cases that the BN partner is unresponsive, the stability counter will keep

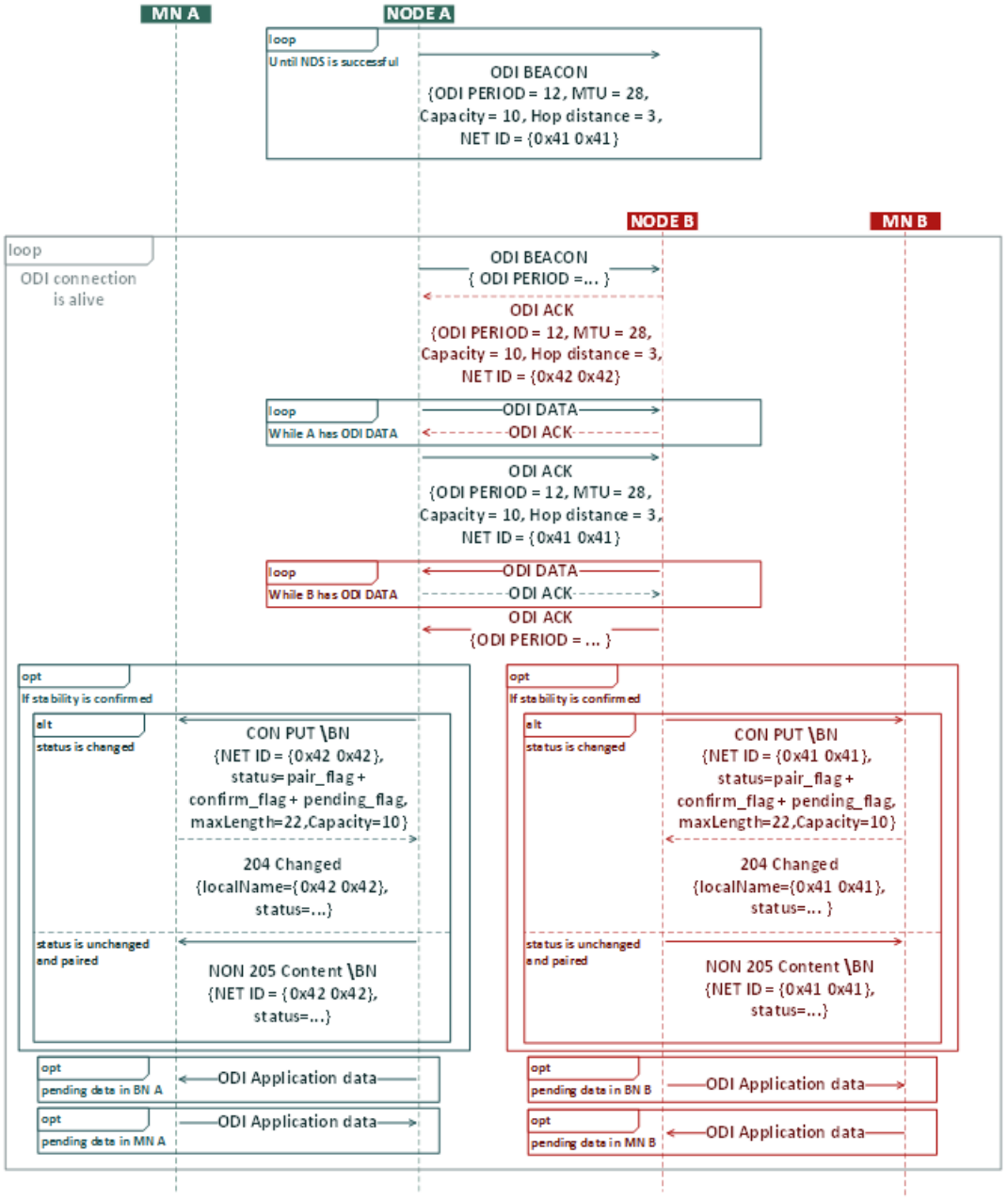


Figure 5.19: Diagram of communication process between BNs and MNs

adding up until the stability count is reached. Then, the ODI connection is regarded as unpaired, and the BN demotes itself from the BN status. The routing protocol will be informed to float the forwarding route. The new status will be put to the MN. The node still keeps sending ODI BEACON to perform the neighbouring discovery.

5.3.3 Negotiation Process

The application uses the handshake information to estimate the limitation of the payload size. In this case, the application payload per ODI datagram is 11 bytes, and

the intermediate node can approximately hold ten datagrams in its buffer. Only half of the available space should be used since the remaining space may be used by the communication from the other end. Therefore, the limitation of application payload is 55 bytes. The application must find the formulation of the request and response in the limitation. *The application payloads mentioned in this section are created and sent by the real hardware* to simulate the exchange in the mentioned scenario. The contents of the payloads are considered from the RFC 6690 standard concerning the resource discovery process [22] and other related literature [28, 138, 155, 156].

As the negotiation process begins, MN sends a GET request to /ODI. The URI contains the information of the resources that can be provided by the ODI connection. The fire forest monitoring system is assumed to possess the following resources according to examples in literature: 1) relative humidity 2) luminosity 3) rain volume 4) temperature 5) wind speed 6) risk assessment level of wildfire events 7) the fire alarm notification. The crop monitoring system hosts the resources related to soil and water conditions such as soil moisture, irrigation events, pH level, Nitrate level and Phosphate level. The domain that receives the advertising frame is always allowed to initiate the communication within a set time limit. This procedure is intended to avoid simultaneous requests for a large payload from both endpoints. In this case, System B is allowed to initiate the conversation. The data exchange in the negotiation is described as follows:

```
MN B: REQ GET /ODI
MN A: RES 205 Content
</dev>;ct=43;sz=130,</ala>;rt="fire-alarm";if="event";sz=16;obs
```

MN B sends a GET /ODI request. This URI always contains the metadata of the available resources that can be traded by the ODI link. MN A responses the requests by sending the core link format of the available resources. However, in this implementation, the payload is not sent in the plain text as shown in the dialogue. The payload is binary encoded by the Type-Length-Value in the similar method with the message options in CoAP [17] under the assumption that the binary tag for each core link attribute is predefined. As an example, instead of sending *</dev>*, the URI-reference tag (4 bits) and the length (4-bits) are sent in the same octet followed by */dev* as the value. The details of the encoding scheme is described in Appendix C. After encoding, the output stream of the 66-bytes payload is reduced to 36 bytes. If the values of the *rt* and *if* fields were to be also encoded, the size of the output stream could be further reduced. This content type is considered as a content-encoding of the core link format assumed to be registered with ID = 43. Under the assumption that the attributes defined by the core link format and their common values will be widely used as the M2M interface for the resource discovery in the future, a small set of the predefined binary coding scheme for the core link format in the similar idea is likely possible. One of the examples is encoded the core link format with CBOR [28, 153], which still a draft document of the IETF.

After retrieving the data of the ODI resources, MN B is informed of two URIs. One of them is a fire alarm notification, which can be observed. Another is the URI, which contains more information in the core link format. MN B then sends a GET request to /dev for further information.

```
MN B: REQ GET /dev
MN A: RES 205 Content
</s1>;ct=43;if="core.ll";sz=168;location=[13617123 99645878],
</s2>;ct=43;if="core.ll";sz=168;location=[13618721 99647490],
MN B: RES 204 Changed /dev
MN A: REQ POST /dev
</s3>;ct=43;if="core.ll";sz=168;location=[13620594 99650278],
</s4>;ct=43;if="core.ll";sz=168;location=[13620594 99650278],
MN B: RES 204 Changed /dev
MN A: REQ POST /dev
</s5>;ct=43;if="core.ll";sz=168;location=[13620594 99650278],
</s6>;ct=43;if="core.ll";sz=168;location=[13613695 99652250]
MN B: RES 204 Changed /dev
```

The */dev* path contains a link list. Each link contains further information of each environmental sensor node. The tagged location may be used in the decision scheme for obtaining the further data. Upon reading the sz field, MN B knows that the resource representation is incomplete and waits for further content. MN A listens for the regular report from BN A when BN A reports no pending data consecutively; MN A then sends POST requests for more contents. MN B responds all POST requests so that MN A can track the outcome of the sending message. However, the process should be aware of the case where the POST request is repeated so that the request is processed only once. In this case, the repetition of URI reference is ignored by the server. This procedure is used by the case study as the workaround for the limitation of the datagram size. Alternatively, a block-wise transfer in RFC 7959 [139] can be employed. If the block-wise transfer is used, MN B will keep sending a GET request with the BLOCK2 option (1-2 bytes) to receive each block of the resource representation. Since each block does not contain a semantical meaning, it cannot be processed separately. However, the method can strictly fix the message size and decouple the application concerns from the limitation of MTU.

After processing the meta-data of the available sensors, System B decides that the data at the locations [13.617123 99.645878], [13.618721 99.647490] and [13.620594 99.650278] is beneficial since the location locates next to the area of System B. Therefore, it then requests the information stored in the path /s1, /s2 and /s3.

```
MN B: REQ GET /s1
```

```
MN A: RES 205 Content
</s1/temp>;rt="temperature-c";if="core.s";obs,
MN A: REQ POST /s1
</s1/light>;rt="light-lux";if="core.s";obs,
MN B: RES 204 Changed /s1
MN A: REQ POST /s1
</s1/hum>;rt="himidity-rel";if="core.s";obs,
MN B: RES 204 Changed /s1
MN A: REQ POST /s1
</s1/wind>;rt="wind-mps";if="core.s";obs,
MN B: RES 204 Changed /s1
MN A: REQ POST /s1
</s1/rain>;rt="rain-mm";if="core.s";obs,
MN B: RES 204 Changed /s1
MN A: REQ POST /s1
</s1/risk>;rt="fire-assess";if="core.rp";obs
MN B: RES 204 Changed /s1
```

After receiving the information of the s1 sensor, System B retrieves the information of the s2 and s3 sensor by the same method. In this way, System B can recognise the tradable resources hosted by System A. MN A set a random integer as the threshold for resource discovery by counting the status report (pending=false) from BN A. When the threshold is reached, MN A assumes that MN B does not initiate further requests. MN A sends a GET request at */ODI* to discover the ODI resources from System B as follows:

```
MN A: REQ GET /ODI
MN B: RES 205 Content
</ssr>;ct=43;sz=150,
</evt>;ct=50;rt="irrigation-volume";if="event";obs,
MN A: REQ GET /ssr
MN B: RES 205 Content
</n1>;ct=43;if="core.ll";sz=110;location=[13616778 99642750],
</n2>;ct=43;if="core.ll";sz=110;location=[13618937 99644203],
MN B: REQ POST /ssr
</n3>;ct=43;if="core.ll";sz=110;location=[13620776 99646504],
</n4>;ct=43;if="core.ll";sz=110;location=[13618668 99641585],
MN A: RES 204 Changed
MN B: REQ POST /ssr
</n5>;ct=43;if="core.ll";sz=110;location=[13613737 99641244],
</n6>;ct=43;if="core.ll";sz=110;location=[13611546 99643525],
MN A: RES 204 Changed
```

```
MN A: REQ GET /n1
MN B: RES 205 Content
</n1/1>;ct=50;rt="phosphate-ugL";if="core.s";obs,
MN B: REQ POST /n1
</n1/2>;ct=50;rt="nitrate-ugL";if="core.s";obs,
MN A: RES 204 changed /n1
MN B: REQ POST /n1
</n1/3>;ct=50;rt="pH";if="core.s";obs,
MN A: RES 204 changed /n1
MN B: REQ POST /n1
</n1/4>;ct=50;rt="soil-moisture-rel";if="core.s";obs,
MN A: RES 204 changed /n1
```

System A is informed of the available ODI resources of System B. At this point, it is still not required additional information, so it remains silent. *The deployed testbed can perform the above conversation correctly using binary encoding scheme and separated request sessions to reduce the payload size per transfer session.*

In summary, this work shows that the negotiation process of the interconnection can be achieved by using a core link format. This method potentially can achieve the interoperability other systems at the application level. Moreover, if the bandwidth usage is strictly concerned, the payloads can be binary-encoded to attain a more concise form of the output stream. The payload may be exchanged in the block-wise transfer. Alternatively, the application can attempt to create a conversation that is not exceeded the available space.

5.3.4 Resource Access

In this section, the process of enabling data traffic flow between domains will be elaborated using the situation in the case study. After processing the available ODI services of System A, System B considers receiving the data from System A as follows: 1) rain data from three sensors (s1, s2 and s3) near the agriculture area 2) fire alarm alert message. The data are exchanged according to the following steps:

1. MN B sends the ODI datagram containing REQ GET /ala Observe: registering to BN B.
2. BN B sends the datagrams across the boundary to BN A.
3. BN A forwards the datagram containing the request.
4. MN A sends back RES 205 Content Observe: registering passID:1 to MN B, using the same route.

Observing resource can be achieved by using the observe option [155]. After MN A receives a request with (Observe: registering), the client (MN B) is registered to the state changes of the resources. In this case, MN A will send a message to MN B when the fire alarm is alerted. Additionally, in the ODI framework, any request that could involve further data traffic from other endpoints must include the *passID* attribute (uint8_t) in the response body. The server domain generates this field and sends to MN as a tool to manage the routing scheme. If the endpoint of the signified data traffic, which is generated by the corresponding request is always MN, the *passID* field can be ignored. The *passID* is relevant when another node, except MN, is the endpoint of the cross-boundary data. MN will put the pair of the associated endpoint address and the *passID* to BN. BN holds the *passID* records to look up for the associated endpoint of the incoming/outgoing ODI datagrams to/from the neighbouring domain (see Section 3.3). Another example shows the case when the sensing data is sent from the endpoint, other than MN. System B applies to the rain data from the sensor. The conversation is described as follows:

1. Using an ODI link, MN B sends REQ GET /s1/rain to MN A.
2. MN A sends back the RES 205 Content n: "s1", v: uniform random (uint8_t), u: mm, passID: 2.
3. MN B receives the response with the passID value from MN B and remains silent.
4. MN A send PUT /pass passID: 2, address: local address of Sensor s1 to BN A to update the passID table.
5. MN A sends a request to subscribe BN A to the client list of Sensor s1.
6. Sensor s1 send a response body to BN A.
7. BN A looks up the passID table to label the passID associated with the data traffic and send the datagram to BN B.
8. BN B looks up the passID value and does not find an entry. Therefore, the response body is labelled to MN B.

In this case study, the rain data payload is generated with a pseudo-random unsigned integer (0-40 mm) to simulate the possible reading from an actual rain gauge in 60 seconds, according to the statistics of rainfall volume [157].

5.3.5 Performances

Table 5.2 shows the measurement results of the energy consumption of the set case study.

Node	**Duty Cycle [%]**	**Transmission Rate [1/s]**
Leaf Node B	4.707 ± 0.079	0.707 ± 0.013
Leaf Node B performed NDS	4.710 ± 0.077	0.766 ± 0.015
Leaf Node B performed CBT	5.044 ± 0.087	0.974 ± 0.016
Leaf Node A	4.011 ± 0.021	2.114 ± 0.025
Leaf Node A performed NDS	4.027 ± 0.032	2.213 ± 0.033
Leaf Node A performed CBT	5.872 ± 0.230	2.346 ± 0.045

Table 5.2: Measured duty cycle and transmission rate demonstrating an example case of neighbouring discovery

The results shown in Table 5.2 are the statistical reference from 100 samples of measurements ($\bar{x} \pm 1.96\sigma_{\bar{x}}$). The duty cycle and transmission rate of the sensor nodes in the setting scenario are measured. The NDS is expected to increase by 2 ODI BEACON in every 30 seconds or 0.067 frames per second. However, the measured values of the show that the transmission rate is increased by 0.059 frames per second in the case of System B and 0.99 frames per second in the case of System A. the experimental results are slightly different from the estimation. This outcome is caused by the clock drift due to the inaccuracy of the 12-kHz RC circuit used as the clock source in the lower power mode. Because this implementation still not include the algorithm to calibrate the clock rate. The expected increasing value of the duty cycle due to the neighbouring discovery is equal to 0.0012 (4 ms (Tx) + 32 ms (Listening)/30 s). The measured duty cycle is increased by 0.003 percent. However, the difference is still relatively small in comparison to the statistical fluctuation. Nonetheless, the experimental results confirmed that the neighbouring discovery activities take a negligible energy from the original system. The energy consumption of the cross-boundary transmission is depended on the rate of data transfer and the waiting time CCH. The transmission rate is expected to ideally increase by 0.1 frames per second due to the data transfer. The results of the measurement show some deviations which can be caused by the transmission errors. The marginal increase of the duty cycle in the case of cross-boundary transmission is caused by the waiting time in CCH due to the imperfection of the synchronisation of the paired BNs. Leaf node B suffers more from the synchronisation errors since Leaf node B always wait for A for the cross-boundary transmission.

The delivery rate of data frame generated by each node in the case study is captured by counting the message ID. The results are shown in Table 5.3.

From Table 5.3, the success rate of the internal data transfer of the nodes without CBT duty is slightly higher than the success rate of the paired BNs. These results show the effects of CBT, which reduces the delivery rate of the internal data of the paired BNs. The success rate of the CBT data transfer in this case study is approximately 0.98. In this scenario, all paired BNs are in the transmission range of the other pairs. Thus, the synchronisation can be disrupted when the other BN pair attempt to access CCH.

Node	System A (Value)	System B (Value)
Internal Data		
1(paired)	0.986 ± 0.004	0.987 ± 0.005
2(paired)	0.984 ± 0.005	0.982 ± 0.008
3(paired)	0.988 ± 0.004	0.986 ± 0.008
4	0.997 ± 0.002	0.998 ± 0.003
5	0.997 ± 0.003	0.994 ± 0.006
6	0.996 ± 0.002	0.996 ± 0.005
CBT Data		
/s1	-	0.982 ± 0.009
/s2	-	0.981 ± 0.011
/s3	-	0.984 ± 0.010

Table 5.3: Delivery success rate of sensor nodes resulted from the experiments

Sometimes, the situation results in a temporary loss of the communication partner which result in an extended stay in ODI operations. However, this issue can be significantly reduced when a proper algorithm to synchronise the clock rate of BN pair is implemented.

This section shows that the ODI framework can at least support the primary form of the application payload exchange with a fairly reliable delivery rate if the design of the application layer considers the limitation of the link layer by attempting to minimise the size of the message in each transfer session.

5.4 Discussion

This chapter proposes the application layer of the ODI frameworks by considering the given solutions in the research communities. CoAP in RESTful architecture is chosen as the template due to its conciseness and its interoperability. However, because of the severe constraint in the MTU of the datagram, the ODI framework proposes various methods in attempts to accommodate a sizable payload for the application routine. The datagram headers are carefully considered to omit the redundancy. Additionally, the message fragmentation layer is proposed. The ODI message format is slightly adjusted from CoAP. However, the format still stays very close to the original CoAP message, which should permit the reusability of the standard libraries related to CoAP and RESTful services in the future with more research works.

While this research does not focus on the application payload, the semantics and the methods of the data exchange in the constrained network is briefly reviewed to clarify the outline of the system functionality supported by the framework. The resource-oriented design is mentioned in the context of the constrained network. However, the serialisation of the resource representation should be redesigned to optimise with the constraint of the

bandwidth. Typically, the output stream can be binary-encoded to shorten the required space significantly in the cost of the human readability. This aspect is highly relevant because of the reduction of the fragmentations, affecting the reliability and network performances as a whole. This work implements its small REST interfaces with a Java application as a proof of concept.

The proposed framework is evaluated to show its reliability and latency in the relation of the hop distance and the increasing fragment counts. A case study is set up with real hardware to show the operational process and to assess the functionality of the frameworks. The evaluation results have shown that the ODI framework has a low impact on the original system and offer a fairly reliable connectivity in common operations.

Chapter 6

Conclusions and Future work

6.1 Conclusions

Advancing The IoT vision involves developing various types of the M2M cooperation. The diversity of specifications and purposes also leads to different approaches and solutions, resulting in the problem of interoperability. While sensors and actuators are the core elements of IoT as interacting tools with the physical world, they must operate together to enable meaningful service in the higher abstract layer. The interoperability of IoT components is usually achieved at the application level under assumptions that the common interface to access the data exists using the internet standard such as Web APIs. Therefore, the compatibility problem in the low-level connection is still neglected, while a considerable number of research works mention the benefits of the cooperation between separate entities.

Similarly, the convergence of the communication in WSNs can be tracked with the increasing adoptions of IP standards on top of IEEE 802.15.4. However, the possibility that some groups of network domains prefer to use their native communication protocols is considerable according to the diversity of the application domain and engineering conditions. Concerning this fact, this research attempts to find the practical way to enable the interconnection between separate domains, while still maintaining the options to choose the preferred communication protocol. This thesis aims to contribute to the IoT development by investigating the interoperability between co-located WSNs in a holistic view of the low-level connection to the communication in the application layer with the real hardware, as called Opportunistic Direct Interconnection in this thesis.

The physical bits transfer is the first concern in this viewpoint. This work performs all experiments under the assumption that the radio chips from different domains can send/receive physical bits from other domains while discussing the possibility of the assumption. Nonetheless, this work focuses on the heterogeneity in the communication

layers since the trend of IoT should force the platform compatibility. In the perspective of the low-level communication, the capability of switching multiple MAC protocol is the key concept to build such a connection between systems adopting different protocols. According to the literature review, some works already report implementing multiple MAC protocol in a constrained platform. Some provide theoretical concepts of the interconnection between WSNs. However, OI-MAC is the only existing literature that provides concrete details in the technical perspective. OI-MAC proposes using a common MAC protocol for communication between domains. Even though the concept of OI-MAC is later extended mentioning the theoretical concept of the NET layer and the application layer, the concept is only validated with the simulation in OMNET++. Therefore, this work uses the concept of OI-MAC as the initial point to deepen the outline of the concept and find the actual solution with a practical implementation.

In this research, EZ430-RF2500 is used as the experimental platform to demonstrate the solution in a highly constrained model with 1kB of RAM, 32 kB of flash memory. As the results, the research proposes the practical ODI framework that can be briefly described as follows:

1. The ODI framework reserves one logical channel for ODI activities.
2. The associated WSN domains in the ODI scheme must possess a common MAC protocol for the cross-boundary transmission. This common protocol uses synchronous duty cycle.
3. The conversation between domains is centralised, governed by cluster heads, sink node, or base station (called management node)
4. The native routing protocol forwards ODI messages in the same way the internal payload is delivered. However, the boundary node must know the address of the associated endpoint to label the destination of the message from the neighbour.
5. The concept of the application protocol is mainly adopted from CoAP and RESTful interface. However, the method to deliver the message must be changed slightly to shift the focus of the protocol design more towards the space reduction while maintaining the equivalent functionality as far as possible.

The results of this work change many major technical aspects of the ODI framework proposed by OI-MAC. To clarify the advances achieved by this research, the details of the development of the ODI framework apart from the concept of OI-MAC are listed as follows:

1. **Handshake Process.** This work redefines the outline of handshake process and gives the details of the process along with other details that are not mentioned in the previous solution.

2. **Cross-boundary protocol.** The critical drawbacks of the proposed MAC protocol used in the cross-boundary in the previous solution are discussed. The alternative solution is provided and evaluated.

3. **Formulation of the concept of the ODI framework in the NET layer.** This work reformulates the necessary modifications in the NET layer for the ODI link, according to the real conditions, the proposed concept dramatically reduces the prerequisites of the framework imposed on the original system.

4. **Formulation of the concept of the ODI framework in the Application layer.** This works reviews the existing literature to propose an application protocol that can be used on top of the implemented ODI link by using CoAP as a template. In an attempt to accommodate a sizeable payload with a very limit MTU, the headers of the datagram are reconsidered, and the message fragmentation is implemented. As a result, the header of CoAP message must be slightly modified. However, the designed message format is still easily translated to CoAP. This method should allow the ODI link to carry messages with the equivalent functionality. Therefore, the solution may allow other details of the standard to apply with careful consideration. This fact still needs more proof of concept in the future since the implementation still not use standard libraries of web API to generate the message payload. However, a custom Java interface is built to measure the fundamental characteristics of the designed protocol, and the equivalent payloads of the necessary functionalities are investigated by using a basic case study.

Instead of relying on the adoption of a communication standard, the concept of ODI can promote the interoperability in local scale while maintaining the native communication protocol. This work shows the first proof of the concept of ODI on real hardware, even though the implementation only shows the feasibility of the concept in a limited scale. This work should provide an evidence for the stakeholders that the ODI concept is practical. The ODI framework proposed by this work also intents to encourage the interoperability with the application outside the framework by using the similar interface for the data exchange. However, this vision still need more proof of concept. This research direction should connect the ODI framework with other implementation concepts allowing ODI to help the integration of WSNs with IoT.

6.2 Future Work

Even though this work accomplishes the ODI framework in the real hardware, its objectives only cover finding the practical solution of ODI and demonstrating its functionality and operational processes in real hardware. Many related parts are left out of the consideration to let the research remain in the boundary of its objectives. Following works can advance the research in this direction:

1. **Optimising cross-boundary protocol.** This work discusses the requirements of the cross-boundary protocol and proposes the cross-boundary protocol using the concept of the synchronous duty cycle. This protocol logic is suggested by this research to be used by default. However, upon the implementing and evaluating processes, it is observed that there are only tiny differences between code sizes and algorithm logics between the asynchronous and synchronous duty cycle protocols. If BNs fix their communication partner, the link automatically becomes synchronous. Otherwise, the communication is asynchronous when the partner is not fixed. This fact is the opportunity to reduce the expenses of the ODI framework and improve the network quality in the broader set of scenarios. Additionally, the procedure to determine the dynamic setting of ODI period can be studied since the parameter can be used to trade the channel capacity with the energy consumption. Therefore, there should be a decision algorithms to set the parameter matching with the ODI frame rate.

2. **Advancing application protocol.** This work already includes the concept of the application layer. However, the technical areas in this layer can be further developed. This work shows that the equivalent conversation of the necessary functionalities can be supported with the implemented ODI link despite the highly limited MTU of datagrams. This laid out a solution already builds a strong foundation to use CoAP/RESTful interfaces on top of the native link layer (customised MAC/routing protocol). If this concept is solidly proved possible by a practical implementation, the ODI framework will significantly benefit the research communities. This is because the laid out evidence will encourage the network practitioners to optimises their networks by implementing their customised link protocols, while still aiming to achieve the compatibility at the application level using the same interface with IP standards.

3. **Implementing Application logics used in cooperation scheme.** Many scenarios of ODI can be modelled and studied to form the cooperation strategies. The cooperation scheme in the boundary of the ODI concept can be specialised by considering the direct interconnection between participants. This research direction can continue further to the implementation level as it can take advantage of the fact that web APIs are implementable by the ODI link.

4. D**esign and Evaluation of Scalability.** Even though there is no foreseeable issue in the proposed concept opposing the scalability of the concept, this aspect is still not proven in this work. The evaluation shows that the provided end-to-end application connectivity is still reliable, even if datagrams travel for 12 hops under the condition that the forwarding route is stable. This fact should allow the ODI framework to scale in the network size. In the perspective of the increasing number of neighbouring domains in contact, the framework should be able to support this aspect without further technical works. However, it still needs a concrete evidence.

5. **Security.** This topic is one of the key element in this topic. This is because the conversation between unknown systems is prone for intrusive attackers. The setting of physical layer is effectively used for avoiding interferences and maintaining the security from ground-up. The concept of ODI contrary proposes to open the hole in the physical layer. Therefore, the security concepts are necessary before this idea can be meaningful proposed to real practitioners.

6. **Proof of concept in broader perspectives.** Apart from accomplishments in this work, other factors can be taken into the consideration. Future works may consider more factors as following examples:

   (a) **Differences of Platforms.** Many WSN platforms (such as MICAZ, TELOSB see details in Section 2.1.3) uses the same model of radio chips, which should provide the compatibility of the physical connection. However, the compatibility between radio chip can be checked as the foundation to allow more realistic, scenario.

   (b) **Increasing protocol diversity.** Since the cross-boundary protocol currently uses synchronous duty cycle technique, the native MAC protocol with synchronous duty cycles should effortlessly coexist together as long as the setting period is correspondingly aligned. Therefore, future works can incorporate synchronous MAC algorithms in the investigation. Moreover, the routing protocol compliant to the ODI requirement can be chosen differently.

   (c) **Case study of Deployment.** Some necessary elements inside and outside the scope of this research are still under developments for the real case deployment. It requires more times before WSN domain will spatially co-locate by chances and the details of the payload contents and their standard interface will be well established. A realistic case study of the cooperation using a direct connection, providing the data in forms of web resources via web interfaces should help the community building the real picture in this direction.

Appendix A

Hardware Profile

A.1 Power Profile

The energy consumption can be obtained by a direct measurement with a power analyser or by measuring the intervals in which the hardware stay in different states, as the power [mW] is equal to the product of current (I [mA]) and voltage (V [V]). In this experiment, MCU spends most of the time in LPM3 (sleep state with disabled CPU, DCO but ACLK is enabled for timer interrupts). MCU is shortly on LPM0 in the sensing routine and active to run ordinary routine and packet receptions. CC2500 needs PLL calibration in its wake-up routine. In this research Tx power is set at -10 dBm and Rx Mode is set at Sensitivity Optimised Mode. For further references, the current profiles of eZ430-RF2500 are given in Table A.1.

The configuration of the radio module dramatically influences the characteristics of the physical layer. This section summarises the relevant information on the radio setting and Rx/Tx process to show the details of the implementation as a reference. Mostly, the default configuration of the radio module is maintained. However, the important settings of the physical module are discussed in this section.

Board Component	***State***	***Current [mA]***
MSP430F2274	LPM0	1.1
	LPM3	0.0009
	Active (8MHz)	2.7
CC2500	Rx (Sensitivity limits)	18.8
	Tx (-10 dBm)	12.2
	Idle	1.5
	PLL Calibration	7.5
	Sleep	0.0004

Table A.1: Current Profile of eZ430-RF2500 at voltage supply of 3V [13, 14]

A.2 Radio Setting

The configuration of the radio can be changed by setting a predefined value in the control registers responsible for the specified functions. The register is accessed via Serial Peripheral Interface (SPI). Table A.2 records the values of noticeable control registers that influent the specification of the PHY layer. Further details can be found in the datasheet of CC2500 [14].

Table A.2: Register configurations of CC2500 for ODI implementation.

Register	***Value***	***Descriptions***
PKTCTRL0	0000 0101	CRC is enabled. PKT length is varied. Data whitening is off.
PKTCTRL1	0000 0100	LQI, RSSI and CRC are automatically generated. Address checking is disabled. AUTOFLUSH is off.
FIFOTHR	0000 0111	Tx and Rx FIFO are 33, 32 bytes.
MDMCFG1	0010 0011	FEC is disabled. 4 bytes of SYNC WORD are transmitted.
MDMCFG2	0111 0011	DC Filter is on. 30/32 bits of SYNC WORD must be correctly received to signal a reception of a frame.
MCSM0	0001 1000	Recalibrating frequency synthesiser when changing the status from IDLE to Tx or Rx.
MCSM1	0011 1100	CCA in THRESHOLD MODE. Remain in the Rx Status after frame reception.
AGCCTRL0	1011 0000	32 Samples are accumulated before new gain adjustment.
AGCCTRL2	1100 0111	The third highest level of DVGA (coefficient of gain) cannot be used. The signal level at 33 dB is targeted at the demodulator.
FOCCFG	0001 1101	The gain for controlling the frequency offset is 4K. After the SYNC WORD is detected, reducing the gain to K/2.

Overall, the registers on the list can be roughly separated into three groups:

1. Packet Handling Control (PKTCTRL, MDMCFG) configures the reception process when a signal is sensed.
2. Radio Control (MCSM) handles the component in the radio chip.

3. Feedback Control (AGCCTRL, FOCCFG) set the parameters for the feedback loop to retrieve the normalised form of the signal.

From Table A.2, the automatic packet handling is set active at with a varied packet size. Following consequences can be implied from the radio set:

1. The maximum physical frame length is limited 32 according to the setting of FIFOTHR. The available physical load is 28 octets.

2. Some dynamic behaviours of the physical layer can be the result of the feedback control algorithm to compensate the signal strength and phase/frequency. Because the signal from different senders arrives with the differences in the energy level, phase and frequency offsets, the updating parameters of the radio may be a favour for some communication partners at any given instance.

Appendix B

Example of Routing Algorithms

Since this implementation is the implementation from ground-up, the widely used routing protocol cannot be applied due to the technical aspect. Instead, the simple routing algorithm is invented to demonstrate the function of a routing protocol in the ODI framework. In further experiments that involving the routing algorithms, following details are applied in the system. The principle of the routing protocol is gradient-based, i.e., each node is assigned a RANK for each registered destination. Nodes only allow sending DATA frames only to another with the lower RANK than them. In this way, the data will eventually find the destination with the RANK at zero. However, each node changes its RANK based on the outcome of the transmission and the connected neighbour. The routing protocol keeps the records of the neighbouring nodes and uses the information to choose the parent with a higher success rate.

In the implementation, each node keeps a routing table as shown in Table B.1.

DST ADDR	PARENT	RANK	FRESHNESS
4100	4105	0b00111111	255

Table B.1: Route entry recorded by routing table

The FRESHNESS (max. at 255) is reduced every time the routing table is looked up but will be replenished when the record is used. In the case that a new DST ADDR is registered when the table is already full, the record with the smallest value of FRESHNESS will be overwritten. DST ADDR is the destination address of the route. Because this simple protocol only maintains the most optimum route for each DST, the DST ADDR can use as the unique entity of the route. PARENT is the next receiver which the DATA frames will be sent towards. The RANK is defined as follows:

$$RANK = HOPDISTANCE(0x10 - 0xF0) + UNCERTAINTY(0x01 - 0x0F) \quad \text{(B.1)}$$

The RANK contains the hop distance (maximum at 15). The node positions its hop distance considering the hop distance of its parent. If the transmission succeeded, the node lowers its hop distance but not equal or less than the parent. When the transmission to the parent failed, the hop distance is increased. This will allow more probability of an attempt to send data to another neighbour. However, the node will permanently change the parent only when the situation is persistent. The UNCERTAINTY field and the REPUTATION field are defined to determine when a new neighbour node should replace the current parent.

The UNCERTAINTY field reflects the success rate of the communication with the parent. The UNCERTAINTY (0-15) is increased when the data transmission is failed and decreased when the data transmission is succeeded. When the UNCERTAINTY value is bigger than a threshold level, the parent is regarded as inefficient. The routing protocol then attempts to change the parent. The rate of increasing and decreasing UNCERTAINTY can be adjusted to secure the preferred success rate.

Also, the routing protocol maintains the NEIGHBOUR table to record the surrounding neighbours as follows: The PREFERENCE is defined to evaluate the connection

ADDRESS	FRESHNESS	LQ	PREFERENCE
0x4105	255	17	0b11011111
0x4106	234	23	0b00100111

Table B.2: Neighbouring table for evaluation of the surrounding nodes

of each neighbour. The BLACKLIST_FLAG is set to ignore the link with the respective neighbour. This flag is defined to mark the parent with a high concurrence. The blacklist status can be undone when the neighbour gains enough reputation. The PARENT_FLAG (1 bits) indicates that this neighbour is a parent in the routing table. The REPUTATION (0-64) is used to evaluate the performance of the neighbour. The REPUTATION is increased when a signal is received from the respective neighbour and when the data transmission is succeeded. The REPUTATION is decreased when the data transmission is failed and when the DATA frames assigned to the neighbour is overflowed. In this way, the REPUTATION reflects the performance of the neighbour regarding the outcome of data transfer.

Each node occasionally attempts to send data to another neighbour that is not the current parent when some aspect of the neighbour is better than the current parent. However, if the transmission attempt is failed, the neighbour is set in the blacklist to prevent further attempt until the neighbour is out of the blacklist. The parent can be changed by following conditions:

1. The current parent is evaluated as inefficient by the UNCERTAINTY field.

2. Another neighbour possesses a lower RANK and higher REPUTATION than the current parent.

3. The routing record is overwritten or erased.

In this way, the chosen parent for each destination is dynamically changed based on the connection performance of the surrounding nodes using REPUTATION as an objective function. The routing protocol requires the MAC layer to advertise the available DST ADDR and its RANK periodically. In this implementation, the NET payload is carried by BEACON and ACK. The details of the NET payload is shown as follows:

```
1               2               3
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
|--ENTRY COUNT--|...
|------------DST ADDR-----------|-----RANK----|...
```

The ENTRY COUNT byte tells how many records are expected in the payload. The following bytes are the details of the DST ADDR and the RANK of the sender in the route. The record with high FRESHNESS will gossip more frequently than the records with low FRESHNESS.

For the DATA frame, the routing algorithm adds the information of the HOP COUNT and FRAME COUNT into the frame headers. Each intermediate node will increase the HOP COUNT. The FRAME COUNT tells how many frames are pending in the queue.

Appendix C

Binary Encoding Scheme

This thesis suggests using REST interfaces for cooperation between local WSNs with different native communication protocols. Therefore, the proof of concept includes application payload exchanges in the similar concept. The serialisation method of the application payload can significantly influence the size of the data stream. Therefore, this work serialises the application payload by encoding the payload with the following encoding scheme:

1. The encoding scheme uses the Type-Length-Value (TLV) in the similar format with the message option specified by RFC 7252 [17]. Type and Length are contained in a single octet describing the encoded value.
   (a) Type (4 bits) specifies the identity of the encoded value.
   (b) Length (4 bits) specifies the length of the value field. Length at zero (0000) means the length is more than 15. Therefore, the Length field is specified in the next octet.
   (c) Value contains the encoded information.
2. In the negotiation process, Table C.1 contains the defined types of the CoRE web linking format according to the suggestion of IETF [28]
3. In the data flow models resulted from the resource access, the basic concept of SenML [156] is adopted as the format of the application payload. Table C.2 defines the types of the data involving in the data flows.

Attribute	Value
href	1
rel	2
anchor	3
rev	4
hreflang	5
media	6
title	7
type	8
rt	9
if	10
sz	11
ct	12
obs	13
(Additional)location	14

Table C.1: Integer Encoding of common attribute names in CoRE link format [28]

Attribute	Label	Value
Name	n	0
Units	u	1
Value	v	2
String Value	vs	3
Boolean Value	vb	4
Value Sum	s	5
Time	t	6
Update Time	ut	7
Data Value	vd	8
Link	l	9
(additional) PassID	-	A
(modified) Base Name	bn	B
(modified) Base Time	bt	C
(modified) Base Units	bu	D
(modified) Base Value	bv	E
(modified) Base Sum	bs	F

Table C.2: Types of data in sessions of resource access

References

[1] K. Bicakci and B. Tavli, "Prolonging network lifetime with multi-domain cooperation strategies in wireless sensor networks," *Ad Hoc Networks*, vol. 8, no. 6, pp. 582–596, aug 2010. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1570870509001164

[2] L. M. Borges, F. J. Velez, and A. S. Lebres, "Survey on the Characterization and Classification of Wireless Sensor Network Applications," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 4, pp. 1860–1890, jan 2014. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6805127

[3] J. Polastre, J. Hill, and D. Culler, "Versatile low power media access for wireless sensor networks," *Proc. 2nd Int. Conf. Embed. networked Sens. Syst. SenSys 04*, vol. 3, no. 4, p. 95, 2004. [Online]. Available: http://dl.acm.org/citation.cfm?id=1031508

[4] M. Buettner, G. V. Yee, E. Anderson, and R. Han, "X-MAC: a short preamble MAC protocol for duty-cycled wireless sensor networks," *Proc. 4th Int. Conf. Embed. networked Sens. Syst. (SenSys 2006)*, p. 307, 2006. [Online]. Available: http://dl.acm.org/citation.cfm?id=1182807.1182838

[5] J. M. Gilbert and F. Balouchi, "Comparison of energy harvesting systems for wireless sensor networks," *Int. J. Autom. Comput.*, vol. 5, no. 4, pp. 334–347, oct 2008. [Online]. Available: http://link.springer.com/10.1007/s11633-008-0334-2

[6] Y. Sun, O. Gurewitz, and D. B. Johnson, "RI-MAC: A Receiver-Initiated Asynchronous Duty Cycle MAC Protocol for Dynamic Traffic Loads in Wireless Sensor Networks," in *Proc. 6th ACM Conf. Embed. Netw. Sens. Syst. - SenSys '08*, vol. 81 LNICST. New York, New York, USA: ACM Press, 2008, p. 1. [Online]. Available: http://dl.acm.org/citation.cfm?id=1460414

[7] I. Khan, F. Belqasmi, R. Glitho, N. Crespi, M. Morrow, and P. Polakos, "Wireless sensor network virtualization: early architecture and research perspectives," *IEEE Netw.*, vol. 29, no. 3, pp. 104–112, may 2015. [Online]. Available: http://arxiv.org/abs/1501.07135

[8] L. Mainetti, L. Patrono, and A. Vilei, "Evolution of wireless sensor networks towards the Internet of Things: A survey," *Software, Telecommun. Comput. Networks*, pp. 1–6, 2011. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp={&}arnumber=6064380

[9] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the internet of (important) things," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 3, pp. 1389–1406, jan 2013. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6380493

[10] H. Zia, N. R. Harris, G. V. Merrett, M. Rivers, and N. Coles, "The impact of agricultural activities on water quality: A case for collaborative catchment-scale management using integrated wireless sensor networks," *Comput. Electron. Agric.*, vol. 96, pp. 126–138, aug 2013. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S0168169913001063

[11] T. Jiang, G. V. Merrett, and N. R. Harris, "Opportunistic direct interconnection between co-located wireless sensor networks," in *Proc. - Int. Conf. Comput. Commun. Networks, ICCCN*. IEEE, jul 2013, pp. 1–5. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6614166

[12] T. Jiang, "Opportunistic Direct Interconnection and Cooperation Between Co-Located Wireless Sensor Networks," Ph.D. dissertation, University of Southampton, 2015.

[13] "eZ430-RF2500 development tool user's guide," 2009. [Online]. Available: http://www.ti.com/lit/ug/slau176d/slau176d.pdf

[14] "CC2500 Low-Cost Low-Power 2.4 GHz RF Transceiver," pp. 1–89, 2009. [Online]. Available: http://www.ti.com/lit/ds/swrs040c/swrs040c.pdf

[15] U. Hunkeler, H. L. Truong, and A. Stanford-Clark, "MQTT-S A publish/subscribe protocol for Wireless Sensor Networks," *2008 3rd Int. Conf. Commun. Syst. Softw. Middlew. Work. (COMSWARE '08)*, pp. 791–798, 2008. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4554519

[16] J. Postel, "User Datagram Protocol," pp. 1–3, 1980. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/B978012374541550016X

[17] Z. Shelby, K. Hartke, and C. Bormann, "RFC 7252The Constrained Application Protocol (CoAP)," pp. 1–112, 2014.

[18] R. Cyganiak, D. Wood, and M. Lanthaler, "RDF 1.1 Concepts and Abstract Syntax," *W3C Recomm. 25 Febr. 2014*, no. February, pp. 263–270, 2014. [Online]. Available: http://www.w3.org/TR/2014/REC-rdf11-concepts-20140225/

[19] D. Guinard, V. Trifa, and E. Wilde, "A resource oriented architecture for the Web of Things," *Proc. 2010 Internet Things*, pp. 1–8, 2010. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5678452

[20] M. Liyanage, C. Chang, and S. N. Srirama, "Lightweight Mobile Web Service Provisioning for Sensor Mediation," in *2015 IEEE Int. Conf. Mob. Serv.*, vol. 32, no. 1. IEEE, jun 2015, pp. 57–64. [Online]. Available: http://ieeexplore.ieee.org/document/7030172/http://ieeexplore.ieee.org/document/7226672/

[21] K. Li, "Representing CoRE Formats in JSON and CBOR," pp. 1–17, 2016.

[22] CoRE Working Group, "Constrained RESTful Environments (CoRE) Link Format," Tech. Rep., 2012.

[23] "IRIS OEM Edition Hardware REFERENCE MANUAL," 2010. [Online]. Available: http://www.memsic.com/userfiles/files/User-Manuals/iris-oem-edition-hardware-ref-manual-7430-0549-02.pdf

[24] M. Johnson, M. Healy, P. van de Ven, M. J. Hayes, J. Nelson, T. Newe, and E. Lewis, "A comparative review of wireless sensor network mote technologies," in *2009 IEEE Sensors*. IEEE, oct 2009, pp. 1439–1442. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5398442

[25] Aqeel-Ur-Rehman, A. Z. Abbasi, N. Islam, and Z. A. Shaikh, "A review of wireless sensors and networks' applications in agriculture," *Comput. Stand. Interfaces*, vol. 36, no. 2, pp. 263–270, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.csi.2011.03.004

[26] IEEE Computer Society, "Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," New York, Tech. Rep. September, 2011.

[27] K. Gravogl, J. Haase, and C. Grimm, "Choosing the best wireless protocol for typical applications," *24th Int. Conf. Archit. Comput. Syst. (ARCS)*, p. 6, 2011. [Online]. Available: http://www.vde-verlag.de/proceedings-en/563333040.html

[28] K. Li, A. Group, A. Rahman, and InterDigital, "Representing Constrained RESTful Environments (CoRE) Link Format in JSON and CBOR," pp. 1–19, 2017.

[29] K. Singhanat, T. Jiang, G. V. Merrett, and N. R. Harris, "Empirical evaluation of OI-MAC: Direct interconnection between wireless sensor networks for collaborative monitoring," in *2015 IEEE Sensors Appl. Symp.* IEEE, apr 2015, pp. 1–5. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7133594http://ieeexplore.ieee.org/document/7133594/

[30] K. Singhanat, N. R. Harris, and G. V. Merrett, "Experimental validation of opportunistic direct interconnection between different Wireless Sensor Networks,"

in *2016 IEEE Sensors Appl. Symp.* IEEE, apr 2016, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/7479814/

[31] W. Dargie, C. Poellabauer, and Wiley InterScience (Online service), *Fundamentals of wireless sensor networks theory and practice.* Hoboken, NJ, USA: John Wiley & Sons, 2010. [Online]. Available: http://public.eblib.com/EBLPublic/PublicView.do?ptiID=543019

[32] I. Akyildiz and M. Can Vuran, *Advanced Texts in Communications and Networking : Wireless Sensor Networks.* Hoboken, NJ, USA: John Wiley & Sons, 2010.

[33] F. Breu, S. Guggenbichler, and J. Wollmann, *WIRELESS SENSOR NETWORKS Technology, Protocols, and Applications*, 2008.

[34] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Comput. Networks*, vol. 38, no. 4, pp. 393–422, mar 2002. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1389128601003024

[35] J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Next century challenges: Mobile Networking for "Smart Dust"," in *Proc. 5th Annu. ACM/IEEE Int. Conf. Mob. Comput. Netw. - MobiCom '99.* New York, New York, USA: ACM Press, 1999, pp. 271–278. [Online]. Available: http://dx.doi.org/10.1145/313451.313558

[36] E. Gauna, L. Girod, J. Brusey, and M. Allen, *Wireless sensor network: Deployments and Design Framework.* Newyork: Springer, 2010.

[37] T. Arampatzis, J. Lygeros, and S. Manesis, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks," *Proc. 2005 IEEE Int. Symp. on, Mediterrean Conf. Control Autom. Intell. Control. 2005.*, pp. 719–724, 2005.

[38] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," *Comput. Networks*, vol. 54, no. 15, pp. 2688–2710, oct 2010. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1389128610001398

[39] A. Arora, R. Ramnath, E. Ertin, P. Sinha, S. Bapat, V. Naik, V. Kulathumani, Hongwei Zhang, Hui Cao, M. Sridharan, S. Kumar, N. Seddon, C. Anderson, T. Herman, N. Trivedi, Chen Zhang, M. Nesterenko, R. Shah, S. Kulkarni, M. Aramugam, Limin Wang, M. Gouda, Young-ri Choi, D. Culler, P. Dutta, C. Sharp, G. Tolle, M. Grimmer, B. Ferriera, and K. Parker, "ExScal: Elements of an Extreme Scale Wireless Sensor Network," in *11th IEEE Int. Conf. Embed. Real-Time Comput. Syst. Appl.* IEEE, pp. 102–108. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1541065

[40] Yunhao Liu, Yuan He, Mo Li, Jiliang Wang, Kebin Liu, Lufeng Mo, Wei Dong, Zheng Yang, Min Xi, Jizhong Zhao, and Xiang-Yang Li, "Does wireless sensor

network scale? A measurement study on GreenOrbs," in *2011 Proc. IEEE INFOCOM*, vol. 24, no. 10. IEEE, apr 2011, pp. 873–881. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5935312

[41] R. Szewczyk, A. Mainwaring, J. Polastre, J. Anderson, and D. Culler, "An analysis of a large scale habitat monitoring application," in *Proc. 2nd Int. Conf. Embed. networked Sens. Syst. - SenSys '04*, vol. 2. New York, New York, USA: ACM Press, 2004, p. 214. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1031495.1031521

[42] D. Chen, Z. Liu, L. Wang, M. Dou, J. Chen, and H. Li, "Natural Disaster Monitoring with Wireless Sensor Networks: A Case Study of Data-intensive Applications upon Low-Cost Scalable Systems," *Mob. Networks Appl.*, vol. 18, no. 5, pp. 651–663, oct 2013. [Online]. Available: http://link.springer.com/10.1007/s11036-013-0456-9

[43] P. Kułakowski, E. Calle, and J. L. Marzo, "Performance study of wireless sensor and actuator networks in forest fire scenarios," *Int. J. Commun. Syst.*, vol. 26, no. March, pp. 515–529, 2012. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1002/dac.2760/epdf

[44] P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, "Wireless sensor networks: a survey on recent developments and potential synergies," *J. Supercomput.*, vol. 68, no. 1, pp. 1–48, apr 2014. [Online]. Available: http://link.springer.com/10.1007/s11227-013-1021-9

[45] E. De Poorter, B. Latré, I. Moerman, and P. Demeester, "Symbiotic Networks: Towards a New Level of Cooperation Between Wireless Networks," *Wirel. Pers. Commun.*, vol. 45, no. 4, pp. 479–495, jun 2008. [Online]. Available: http://link.springer.com/10.1007/s11277-008-9490-5

[46] M. Felegyhazi, J.-P. Hubaux, and L. Buttyan, "Cooperative Packet Forwarding in Multi-Domain Sensor Networks," in *Third IEEE Int. Conf. Pervasive Comput. Commun. Work.* IEEE, 2005, pp. 345–349. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1392864

[47] M. Shamani, H. Gharaee, S. Sadri, and F. Rezaei, "Adaptive Energy Aware Cooperation Strategy in Heterogeneous Multi-domain Sensor Networks," *Procedia Comput. Sci.*, vol. 19, pp. 1047–1052, jan 2013. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1877050913007552

[48] J. a. Stankovic, "Research Directions for the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, feb 2014. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6774858

[49] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, sep 2013. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S0167739X13000241

[50] S. B. Qaisar, S. Ali, and E. A. Felemban, "Wireless Sensor Networks in Next Generation Communication Infrastructure: Vision and Challenges," in *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*. Springer International Publishing Switzerland 2014, 2014, vol. 8582 LNCS, no. PART 4, pp. 790–803. [Online]. Available: http://link.springer.com/10.1007/978-3-319-09147-1{_}58

[51] P. Huang, L. Xiao, S. Soltani, M. W. Mutka, and N. Xi, "The Evolution of MAC Protocols in Wireless Sensor Networks: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 1, pp. 101–120, jan 2013. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6188353

[52] C. Alcaraz, P. Najera, J. Lopez, and R. Roman, "Wireless Sensor Networks and the Internet of Things : Do We Need a Complete Integration ?" *1st Int. Work. Secur. Internet Things*, no. July 2015, pp. 1–8, 2010. [Online]. Available: https://www.nics.uma.es/system/files/papers/calcaraz10.pdf

[53] M. Rovcanin, E. D. Poorter, I. Moerman, and P. Demeester, "A reinforcement learning based solution for cognitive network cooperation between co-located, heterogeneous wireless sensor networks," *Ad Hoc Networks*, vol. 17, pp. 98–113, jun 2014. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1570870514000201

[54] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Comput. Networks*, vol. 47, no. 4, pp. 445–487, mar 2005. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1389128604003457

[55] K. Bicakci, I. E. Bagci, B. Tavli, and Z. Pala, "Neighbor sensor networks: Increasing lifetime and eliminating partitioning through cooperation," *Comput. Stand. Interfaces*, vol. 35, no. 4, pp. 396–402, jun 2013. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S0920548912001250

[56] N. Inoue, K. Kinoshita, T. Watanabe, K. Murakami, Y. Tanigawa, and H. Tode, "A cooperative routing method with shared nodes for overlapping wireless sensor networks," in *2014 Int. Wirel. Commun. Mob. Comput. Conf.* IEEE, aug 2014, pp. 1106–1111. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6906509

[57] T. Jiang, G. V. Merrett, and N. R. Harris, "Opportunistic energy trading between co-located energy-harvesting wireless sensor networks," in

Proc. 1st Int. Work. Energy Neutral Sens. Syst. - ENSSys '13. New York, New York, USA: ACM Press, 2013, pp. 1–6. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2534208.2534212

[58] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Comput. Networks*, vol. 52, no. 12, pp. 2292–2330, aug 2008. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1389128608001254

[59] X. Dong, M. C. Vuran, and S. Irmak, "Autonomous precision agriculture through integration of wireless underground sensor networks with center pivot irrigation systems," *Ad Hoc Networks*, vol. 11, no. 7, pp. 1975–1987, sep 2013. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1570870512001291

[60] R. Thomas, D. Friend, L. Dasilva, and A. Mackenzie, "Cognitive networks: adaptation and learning to achieve end-to-end performance objectives," *IEEE Commun. Mag.*, vol. 44, no. 12, pp. 51–57, dec 2006. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4050101

[61] B. Karaoglu, I. Demirkol, and W. Heinzelman, "Exploring the Benefits of Symbiotic Routing," in *2011 Proc. 20th Int. Conf. Comput. Commun. Networks*. IEEE, jul 2011, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6005905

[62] T. De Pauw, B. Volckaert, A. Hristoskova, V. Ongenae, and F. De Turck, "Symbiotic Service Composition in Distributed Sensor Networks," *Int. J. Distrib. Sens. Networks*, vol. 2013, pp. 1–22, 2013. [Online]. Available: http://www.hindawi.com/journals/ijdsn/2013/684563/

[63] G. Crosby and N. Pissinou, "Evolution of Cooperation in Multi-Class Wireless Sensor Networks," in *32nd IEEE Conf. Local Comput. Networks (LCN 2007)*, no. i. IEEE, oct 2007, pp. 489–495. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4367879

[64] V. Jelicic, D. Tolic, and V. Bilas, "Consensus-based decentralized resource sharing between co-located Wireless Sensor Networks," in *2014 IEEE Ninth Int. Conf. Intell. Sensors, Sens. Networks Inf. Process.*, no. April. IEEE, apr 2014, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6827662

[65] IEEE Computer Society, *IEEE Standard Part 15.4e: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer*. New York: IEEE STANDARDS ASSOCIATION, 2012, vol. 2012, no. April. [Online]. Available: http://standards.ieee.org/findstds/standard/802.15.4e-2012.html

[66] A. Dunkels, "The ContikiMAC Radio Duty Cycling Protocol," *SICS Tech. Rep. T201113 , ISSN 1100-3154*, pp. 1–11, 2011. [Online]. Available: http://dunkels.com/adam/dunkels11contikimac.pdf

[67] M. Sha, R. Dor, G. Hackmann, C. Lu, T.-S. Kim, and T. Park, "Self-Adapting MAC Layer for Wireless Sensor Networks," in *2013 IEEE 34th Real-Time Syst. Symp.* IEEE, dec 2013, pp. 192–201. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6728874

[68] E. De Poorter, I. Moerman, and P. Demeester, "An Information Driven Sensornet Architecture," in *2009 Third Int. Conf. Sens. Technol. Appl.* IEEE, jun 2009, pp. 553–561. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5210857

[69] D. Plets, W. Joseph, E. Poorter, L. Martens, and I. Moerman, "Concept and framework of a self-regulating symbiotic network," *EURASIP J. Wirel. Commun. Netw.*, vol. 2012, no. 1, p. 340, 2012. [Online]. Available: http://jwcn.eurasipjournals.com/content

[70] J. Nagata, K. Kinoshita, and Y. Tanigawa, "A Routing Method for Co-operative Forwarding in Multiple Wireless Sensor Networks," in *ICNS 2012, Eighth Int. Conf. Netw. Serv.*, no. c, 2012, pp. 43–46. [Online]. Available: http://www.thinkmind.org/index.php?view=article{&}articleid=icns{_}2012{_}2{_}30{_}10108

[71] E. De Poorter, P. Becue, I. Moerman, and P. Demeester, "Exploring a Boundary-Less Cooperation Approach for Heterogeneous Co-Located Networks," in *2011 IEEE Int. Conf. Commun.* IEEE, jun 2011, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5963028

[72] E. De Poorter, P. Becue, M. Rovcanin, I. Moerman, and P. Demeester, "A negotiation-based networking methodology to enable cooperation across heterogeneous co-located networks," *Ad Hoc Networks*, vol. 10, no. 6, pp. 901–917, aug 2012. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1570870511002149

[73] M. Garcia, S. Sendra, J. Lloret, and A. Canovas, "Saving energy and improving communications using cooperative group-based Wireless Sensor Networks," *Telecommun. Syst.*, vol. 52, no. 4, pp. 2489–2502, aug 2011. [Online]. Available: http://link.springer.com/10.1007/s11235-011-9568-3

[74] T. De Pauw, N. Matthys, B. Volckaert, V. Ongenae, S. Michiels, and F. De Turck, "Design of an autonomous software platform for future symbiotic service management," in *2012 IEEE Netw. Oper. Manag. Symp.* IEEE, apr 2012, pp. 1195–1198. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6212050

[75] C. Buratti, A. Conti, D. Dardari, and R. Verdone, "An Overview on Wireless Sensor Networks Technology and Evolution," *Sensors*, vol. 9, no. 9, pp. 6869–6896, aug 2009. [Online]. Available: http://www.mdpi.com/1424-8220/9/9/6869/

[76] M. A. Yigitel, O. D. Incel, and C. Ersoy, "QoS-aware MAC protocols for wireless sensor networks: A survey," *Comput. Networks*, vol. 55, no. 8, pp. 1982–2004, jun 2011. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1389128611000703

[77] W. Li, J. Bao, and W. Shen, "Collaborative wireless sensor networks: A survey," in *2011 IEEE Int. Conf. Syst. Man, Cybern.* IEEE, oct 2011, pp. 2614–2619. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6084070

[78] L. M. Oliveira and J. J. Rodrigues, "Wireless Sensor Networks: a Survey on Environmental Monitoring," *J. Commun.*, vol. 6, no. 2, pp. 143–151, apr 2011. [Online]. Available: http://ojs.academypublisher.com/index.php/jcm/article/view/4233

[79] A. Bachir, M. Dohler, T. Watteyne, and K. K. Leung, "MAC Essentials for Wireless Sensor Networks," *IEEE Commun. Surv. Tutorials*, vol. 12, no. 2, pp. 222–248, 2010. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs{_}all.jsp?arnumber=5451759

[80] J. M. T. Portocarrero, F. C. Delicato, P. F. Pires, and T. V. Batista, "Reference Architecture for Self-adaptive Management in Wireless Sensor Networks," in *Adapt. Intell. Syst.* Springer International Publishing Switzerland, 2014, pp. 110–120. [Online]. Available: http://link.springer.com/10.1007/978-3-319-11298-5{_}12

[81] K. Sohrabi, J. Gao, V. Ailawadhi, and G. Pottie, "Protocols for self-organization of a wireless sensor network," *IEEE Pers. Commun.*, vol. 7, no. 5, pp. 16–27, 2000. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=878532

[82] M. Rovcanin, E. D. Poorter, O. Yaron, I. Moerman, D. Plets, W. Joseph, and L. Martens, "Elaboration of Cognitive Decision Making Methods in the Context of Symbiotic Networking," in *Sixth Int. Conf. Sens. Technol. Appl. Elabor. (SENSORCOMM 2012)*, no. c, 2012, pp. 229–234.

[83] L. Mottola and G. P. Picco, "Programming wireless sensor networks," *ACM Comput. Surv.*, vol. 43, no. 3, pp. 1–51, apr 2011. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1922649.1922656

[84] O. Gnawali, R. Fonseca, K. Jamieson, M. Kazandjieva, D. Moss, and P. Levis, "CTP: An Efficient, Robust, and Reliable Collection Tree Protocol for Wireless Sensor Networks," *ACM Trans. Sens. Networks*, vol. 10, no. 1, pp. 1–49, nov 2013. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2555947.2529988

[85] P. Corke, T. Wark, R. Jurdak, W. Hu, P. Valencia, and D. Moore, "Environmental Wireless Sensor Networks," *Proc. IEEE*, vol. 98, no. 11, pp. 1903–1917, nov 2010. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs{_}all.jsp?arnumber=5597912

[86] D. Chen and P. K. Varshney, "QoS Support in Wireless Sensor Networks: A Survey," *Int. Conf. Wirel. Networks, (ICWN '04), Las Vegas*, vol. 13244, no. 0749-503; 10, pp. 227–233, 2004. [Online]. Available: http://pdf.aminer.org/000/369/962/qos{_}support{_}in{_}wireless{_}sensor{_}networks{_}a{_}survey.pdf{%}5Cnhttp://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.91.3594{&}rep=rep1{&}type=pdf

[87] F. Xia, "QoS Challenges and Opportunities in Wireless Sensor/Actuator Networks," *Sensors*, vol. 8, no. 2, pp. 1099–1110, feb 2008. [Online]. Available: http://arxiv.org/abs/0806.0128

[88] J. Bhar, "A Mac Protocol Implementation for Wireless Sensor Network," *J. Comput. Networks Commun.*, vol. 2015, pp. 1–12, 2015. [Online]. Available: http://www.hindawi.com/journals/jcnc/2015/697153/

[89] A. Eslami, M. Nekoui, H. Pishro-Nik, and F. Fekri, "Results on finite wireless sensor networks," *ACM Trans. Sens. Networks*, vol. 9, no. 4, pp. 1–22, jul 2013. [Online]. Available: http://dl.acm.org/citation.cfm?id=2489268

[90] M. Li, Z. Li, and A. V. Vasilakos, "A Survey on Topology Control in Wireless Sensor Networks: Taxonomy, Comparative Study, and Open Issues," *Proc. IEEE*, vol. 101, no. 12, pp. 2538–2557, dec 2013. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6570755

[91] B. Rashid and M. H. Rehmani, "Applications of wireless sensor networks for urban areas: A survey," *J. Netw. Comput. Appl.*, vol. 60, pp. 192–219, 2016. [Online]. Available: http://dx.doi.org/10.1016/j.jnca.2015.09.008

[92] Z. Sheng, C. Mahapatra, C. Zhu, and V. C. M. Leung, "Recent advances in industrial wireless sensor networks toward efficient management in IoT," *IEEE Access*, vol. 3, no. Oma Dm, pp. 622–637, 2015.

[93] J. Tollefson, "The Truth about Power Consumption in PIC MCUs with XLP Technology vs. TI's MSP430," pp. 1–8, 2010.

[94] B. Finch and W. Goh, "MSP430 Advanced Power Optimizations : ULP Advisor Software and EnergyTrace Technology," Texas Instruments, Tech. Rep. June, 2014.

[95] "CC2420 2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver Applications," Texas Instruments, Tech. Rep., 2006. [Online]. Available: http://www.ti.com/lit/ds/symlink/cc2420.pdf

[96] Chipcon A.S., "CC1000 Single Chip Very Low Power RF Transceiver," pp. 1–55, 2004. [Online]. Available: http://www.ti.com/lit/ds/symlink/cc1000.pdf

[97] "CC1120: High-Performance RF Transceiver for Narrowband Systems," 2013.

[98] "CC1101 — Sub-1 GHz — Wireless Connectivity — Description & parametrics." [Online]. Available: http://www.ti.com/product/cc1101/description

[99] Zolertia , "Zolertia RE-Mote platform Datasheet," vol. 001, no. December, pp. 1–2, 2015.

[100] F. Ingelrest, G. Barrenetxea, G. Schaefer, M. Vetterli, O. Couach, and M. Parlange, "SensorScope," *ACM Trans. Sens. Networks*, vol. 6, no. 2, pp. 1–32, feb 2010. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1689239.1689247

[101] A. A. Kumar S., K. Ovsthus, and L. M. Kristensen., "An industrial perspective on wireless sensor networks-a survey of requirements, protocols, and challenges," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 3, pp. 1391–1412, jan 2014. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6728782

[102] H. Karvonen, C. Pomalaza-Ráez, and M. Hämäläinen, "A Cross-Layer Optimization Approach for Lower Layers of the Protocol Stack in Sensor Networks," *ACM Trans. Sens. Networks*, vol. 11, no. 1, pp. 1–30, jul 2014. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2648771.2590810

[103] "Key Priorities for Sub-GHz Wireless Deployment," p. 6. [Online]. Available: http://www.silabs.com/pages/DownloadDoc.aspx?FILEURL=SupportDocuments/TechnicalDocs/Key-Priorities-for-Sub-GHz-Wireless-Deployments.pdf

[104] J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," in *IECON 2007 - 33rd Annu. Conf. IEEE Ind. Electron. Soc.* IEEE, 2007, pp. 46–51. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4460126

[105] M. Khanafer, M. Guennoun, and H. T. Mouftah, "A Survey of Beacon-Enabled IEEE 802.15.4 MAC Protocols in Wireless Sensor Networks," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 2, pp. 856–876, jan 2014. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6687312

[106] S. Brienza and D. D. Guglielmo, "Strategies for optimal MAC parameter setting in IEEE 802.15. 4 wireless sensor networks: A performance comparison," in *Comput. Commun. (ISCC), 2013 IEEE Symp. on. IEEE*, 2013, pp. 898–903. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs{_}all.jsp?arnumber=6755063

[107] D. Chen, M. Nixon, S. Han, A. K. Mok, and X. Zhu, "WirelessHART and IEEE 802.15.4e," in *2014 IEEE Int. Conf. Ind. Technol.* IEEE, feb 2014, pp. 760–765. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6895027

[108] M. A. Mahmood, W. K. Seah, and I. Welch, "Reliability in wireless sensor networks: A survey and challenges ahead," *Comput. Networks*, vol. 79, pp. 166–187, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2014.12.016

[109] B. Crow, I. Widjaja, L. Kim, and P. Sakai, "IEEE 802.11 Wireless Local Area Networks," *IEEE Commun. Mag.*, vol. 35, no. 9, pp. 116–126, 1997. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=620533

[110] a. Warrier, M. Aia, and M. Sichitiu, "Z-MAC: A Hybrid MAC for Wireless Sensor Networks," *IEEE/ACM Trans. Netw.*, vol. 16, no. 3, pp. 511–524, jun 2008. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4453818

[111] L. Sitanayah, C. J. Sreenan, and K. N. Brown, "A hybrid MAC protocol for emergency response wireless sensor networks," *Ad Hoc Networks*, vol. 20, pp. 77–95, sep 2014. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1570870514000638

[112] K. Whitehouse, A. Woo, F. Jiang, J. Polastre, and D. Culler, "Exploiting the Capture Effect for Collision Detection and Recovery," in *Second IEEE Work. Embed. Networked Sensors, 2005. EmNetS-II.*, vol. 2005. IEEE, 2005, pp. 45–52. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1469098

[113] Z. A. Eu, P. Lee, and H.-P. Tan, "Classification of Packet Transmission Outcomes in Wireless Sensor Networks," in *2011 IEEE Int. Conf. Commun.* IEEE, jun 2011, pp. 1–5. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5962637

[114] L. Tang, Y. Sun, O. Gurewitz, and D. B. Johnson, "PW-MAC: An energy-efficient predictive-wakeup MAC protocol for wireless sensor networks," in *2011 Proc. IEEE INFOCOM.* IEEE, apr 2011, pp. 1305–1313. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5934913

[115] A. El-Hoiydi, "Aloha with preamble sampling for sporadic traffic in ad hoc wireless sensor networks," in *2002 IEEE Int. Conf. Commun. Conf. Proceedings. ICC 2002 (Cat. No.02CH37333)*, vol. 5, no. C. IEEE, 2002, pp. 3418–3423. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=997465

[116] H. Singh and B. Biswas, "Comparison of CSMA based MAC protocols of wireless sensor networks," *Int. J. AdHoc Netw. Syst.*, vol. 2, no. 2, pp. 1–10, may 2012. [Online]. Available: http://arxiv.org/abs/1205.1701

[117] X. Fafoutis, C. Orfanidis, and N. Dragoni, "Altruistic Backoff: Collision Avoidance for Receiver-Initiated MAC Protocols for Wireless Sensor Networks," *Int. J. Distrib. Sens. Networks*, vol. 2014, pp. 1–11, 2014. [Online]. Available: http://www.hindawi.com/journals/ijdsn/2014/576401/

[118] I. Demirkol, C. Ersoy, and F. Alagoz, "MAC protocols for wireless sensor networks: a survey," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 115–121, apr 2006. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1632658

[119] A. P. Jayasumana, H. Qi, and T. H. Illangasekare, "Virtual sensor networks - A resource efficient approach for concurrent applications," in *Proc. - Int. Conf. Inf. Technol. Gener. ITNG 2007*. Ieee, apr 2007, pp. 111–115. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4151668

[120] D. Christin, A. Reinhardt, P. S. Mogre, and R. Steinmetz, "Wireless Sensor Networks and the Internet of Things : Selected Challenges," in *Proc. 8th GI/ITG KuVS Fachgespräch Drahtlose Sensornetze*, 2009, pp. 31–34.

[121] J. G. Ko, A. Terzis, S. Dawson-Haggerty, D. Culler, J. Hui, and P. Levis, "Connecting low-power and lossy networks to the internet," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 96–101, 2011.

[122] Z. Sheng, H. Wang, C. Yin, X. Hu, S. Yang, and V. C. Leung, "Lightweight Management of Resource-Constrained Sensor Devices in Internet of Things," *IEEE Internet Things J.*, vol. 2, no. 5, pp. 402–411, 2015. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7080876

[123] K. Rose, S. Eldridge, and C. Lyman, "The internet of things: an overview," *Internet Soc.*, no. October, p. 53, 2015. [Online]. Available: http://www.internetsociety.org/doc/iot-overview

[124] D. Plets, W. Joseph, E. De Poorter, L. Martens, and I. Moerman, "Cognitive symbiotic network planning for energy consumption reduction in wireless sensor networks," in *2012 6th Eur. Conf. Antennas Propag.* IEEE, mar 2012, pp. 69–72. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6205839

[125] S. Li, L. D. Xu, and S. Zhao, "The internet of things: a survey," *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, 2015.

[126] E. De Poorter, E. Troubleyn, I. Moerman, and P. Demeester, "IDRA: A flexible system architecture for next generation wireless sensor networks," *Wirel. Networks*, vol. 17, no. 6, pp. 1423–1440, aug 2011. [Online]. Available: http://link.springer.com/10.1007/s11276-011-0356-5

[127] Texas Instruments, "Mixed Signal Microcontroller," pp. 1–122, 2013. [Online]. Available: http://www.datasheetarchive.com/SLAS504G-datasheet.html

[128] "ERRATA NOTES CC2500," pp. 1–17.

[129] O. Gnawali, R. Fonseca, K. Jamieson, and P. Levis, "CTP : Robust and Efficient Collection through Control and Data Plane Integration Technical Report SING-08-02," Stanford Information Networks Group SING-08-02, Tech. Rep., 2008.

[130] J. P. Vasseur, N. Agarwal, J. Hui, Z. Shelby, P. Bertrand, and C. Chauvenet, "RPL: The IP routing protocol designed for low power and lossy networks," 2011.

[131] M. Veeraraghavan, "Analysis of error control and flow control schemes," pp. 1–16, 2004.

[132] R. Sutaria and R. Govindachari, "Making sense of interoperability: Protocols and Standardization initiatives in IOT," *2nd Int. Work. Comput. Netw. Internet Things held conjunction with 14th Int. Conf. Distrib. Comput. Netw. (ICDCN 2013)*, pp. 2–5, 2013. [Online]. Available: http://rsutaria.net/wp-content/uploads/2013/02/Low{_}power{_}IoT{_}ComNet{_}2013{_}Mindtree.pdf

[133] L. Nastase, "Security in the Internet of Things: A Survey on Application Layer Protocols," *2017 21st Int. Conf. Control Syst. Comput. Sci.*, no. July 2016, pp. 659–666, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7968629/

[134] J. L. Fernandes, I. C. Lopes, J. J. P. C. Rodrigues, and S. Ullah, "Performance evaluation of RESTful web services and AMQP protocol," *Int. Conf. Ubiquitous Futur. Networks, ICUFN*, no. April 2014, pp. 810–815, 2013.

[135] D. Thangavel, X. Ma, A. Valera, H. X. Tan, and C. K. Y. Tan, "Performance evaluation of MQTT and CoAP via a common middleware," *IEEE ISSNIP 2014 - 2014 IEEE 9th Int. Conf. Intell. Sensors, Sens. Networks Inf. Process. Conf. Proc.*, no. April, pp. 21–24, 2014.

[136] S. K. Datta and C. Bonnet, "A lightweight framework for efficient M2M device management in oneM2M architecture," *2015 Int. Conf. Recent Adv. Internet Things, RIoT 2015*, no. April, pp. 7–9, 2015.

[137] N. Correia, A. Mazayev, G. Schütz, J. Martins, and A. Barradas, "Resource design in constrained networks for network lifetime increase," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1611–1623, 2017.

[138] Z. Shelby, M. Vial, and M. Koster, "Reusable Interface Definitions for Constrained RESTful Environments," *IETF*, vol. CoRE Draft, pp. 1–27, 2017. [Online]. Available: https://tools.ietf.org/html/draft-ietf-core-interfaces-04

[139] C. Bormann and Z. E. Shelby, "RFC 7959: Block-Wise Transfers in the Constrained Application Protocol (CoAP)," pp. 1–37, 2016. [Online]. Available: https://tools.ietf.org/pdf/rfc7959.pdf

[140] IEEE Computer Society, "Part 15 . 4 : Low-Rate Wireless Personal Area Networks (LR-WPANs)," New York, 2012.

[141] E. Vogli, M. B. Alaya, T. Monteil, L. A. Grieco, K. Drira, P. Bari, C. Roche, and F. Toulouse, "An efficient resource naming for enabling constrained devices in SmartM2M architecture," 2015.

[142] N. Modadugu and E. Rescorla, "Datagram Transport Layer Security," Tech. Rep., 2006.

[143] J. Melorose, R. Perroy, and S. Careas, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," *Statew. Agric. L. Use Baseline 2015*, vol. 1, pp. 1–24, 2015.

[144] C. A. Kent and J. Mogul, "Fragmentation Considered Harmful," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 17, no. 5, pp. 390–401, 1987. [Online]. Available: http://portal.acm.org/citation.cfm?doid=55483.55524

[145] R. Lucchi, M. Millot, and C. Elfers, "Resource Oriented Architecture and REST," *Assess. impact advantages INSPIRE, Ispra Eur. Communities*, pp. 5–13, 2008.

[146] L. Lan, F. Li, B. Wang, L. Zhang, and R. Shi, "An Event-Driven Service-Oriented Architecture for the Internet of Things," *2014 Asia-Pacific Serv. Comput. Conf.*, pp. 68–73, 2014. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7175497

[147] F. Curbera, M. Duftler, R. Khalaf, and W. Nagy, "Unraveling the Communication : SOAP," *IEEE Internet Comput.*, no. April, pp. 86–93, 2002. [Online]. Available: http://tele1.dee.fct.unl.pt/rit2{_}2009{_}2010/teo/soap.tutorial.pdf

[148] E. Miller, "An Introduction to the Resource Description Framework," *Bull. Am. Soc. Inf. Sci. Technol.*, vol. 25, no. 1, pp. 15–19, jan 2005. [Online]. Available: http://doi.wiley.com/10.1002/bult.105

[149] J. D. Fernández, M. A. Martínez-Prieto, C. Gutiérrez, A. Polleres, and M. Arias, "Binary RDF representation for publication and exchange (HDT)," *J. Web Semant.*, vol. 19, pp. 22–41, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.websem.2013.01.002

[150] F. Pacini, F. A. Aderohunmu, S. Bocchino, P. Pagano, A. Azzara, and M. Petracca, "Performance Analysis of Data Serialization Formats in M2M Wireless Sensor Networks," *12th Eur. Conf. Wirel. Sens. Networks*, no. FEBRUARY, pp. 7–8, 2015.

[151] K. Maeda, "Performance evaluation of object serialization libraries in XML, JSON and binary formats," *2012 2nd Int. Conf. Digit. Inf. Commun. Technol. its Appl. DICTAP 2012*, pp. 177–182, 2012.

[152] N. Gligorić, I. Dejanović, and S. Krčo, "Performance evaluation of compact binary XML representation for constrained devices," *2011 Int. Conf. Distrib. Comput. Sens. Syst. Work. DCOSS'11*, 2011.

[153] C. Bormann and P. Hoffman, "Concise Binary Object Representation (CBOR)," Tech. Rep., 2013. [Online]. Available: https://www.rfc-editor.org/info/rfc7049

[154] M. Ruta, F. Scioscia, A. Pinto, E. D. Sciascio, F. Gramegna, S. Ieva, G. Loseto, D. E. I. Politecnico, and E. Orabona, "Resource annotation , dissemination and discovery in the Semantic Web of Things : a CoAP-based framework," no. January 2008, pp. 527–534, 2013.

[155] K. Hartke, "Observing Resources in the Constrained Application Protocol (CoAP)," Tech. Rep., 2015. [Online]. Available: https://www.rfc-editor.org/info/rfc7641

[156] C. Jennings, Z. Shelby, J. Arkko, A. Keranen, and C. Bormann, "Media Types for Sensor Measurement Lists (SenML)," *IETF Stand. Track Internet-Draft*, no. draft-ietf-core-senml-10, pp. 1–46, 2017. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-core-senml/

[157] "World Records-HDSC/OWP." [Online]. Available: http://www.nws.noaa.gov/oh/hdsc/record{_}precip/record{_}precip{_}world.html