Integrated Framework for Mobile Low Power IoT Devices

Yaarob Mahjoob Nafel Al-Nidawi

Submitted in accordance with the requirements for the degree of

Doctor of Philosophy

University of Leeds

School of Electronic and Electrical Engineering

Institute of Integrated Information Systems

June 2016

Declaration

The candidate confirms that the work submitted is his own, except where work which has formed part of jointly authored publications has been included. The contribution of the candidate and the other authors to this work has been explicitly indicated below. The candidate confirms that appropriate credit has been given within the thesis where reference has been made to the work of others. Most materials contained in the chapters of this thesis have been previously published in research articles written by the author of this work (Yaarob Al-Nidawi), who appears as lead (first) author in all of them.

The research has been supervised and guided by Dr. Andrew H. Kemp, and he appears as a co-author on these articles. All the materials included in this document is of the author's entire intellectual ownership.

A) Details of the publications which have been used (e.g. titles, journals, dates, names of authors):

In chapter 2:

"Mobility of Low Power IoT Devices: The State of The Art", *IEEE Internet of Things Journal*, Under Review. Co-authors: Andrew H. Kemp.

In chapter 3:

1- "Mobility of Low Power IoT Devices: The State of The Art", *IEEE Internet of Things Journal*, Under Review. Co-authors: Andrew H. Kemp.

2- "Impact of Mobility on The IoT MAC Infrastructure: IEEE 802.15.4e TSCH and LLDN Platform," in *Proceedings of IEEE 2nd World Forum on Internet of Things (WF-IoT),* pp.478-483, Milan, 14-16 Dec. 2015. Co-authors: Harith Yahya, Andrew H. Kemp.

In chapter 4:

"Mesh-Under Cluster-Based Routing Protocol for IEEE 802.15.4 Sensor Network," in *Proceedings of 20th European Wireless Conference;* pp.1-7, Barcelona, 14-16 May 2014. Co-authors: Naveed Salman, Andrew H. Kemp.

In chapter 5:

“Mobility Aware Framework for Timeslotted Channel Hopping IEEE 802.15.4e Sensor Networks," in *IEEE Sensors Journal,* vol.15, no.12, pp.7112-7125, Dec. 2015. Co-authors: Andrew H. Kemp.

In chapter 6:

"Tackling Mobility in Low Latency Deterministic Multihop IEEE 802.15.4e Sensor Network," in *IEEE Sensors Journal*, vol.16, no.5, pp.1412-1427, March, 2016. Co-authors: Harith Yahya, Andrew H. Kemp.

B) Details of the work contained within these publications which is directly attributable to Yaarob Al-Nidawi:

With the exceptions detailed in section C, the published work is entirely attributable to Yaarob Al-Nidawi: the literature review necessary to construct and originate the ideas behind the published manuscripts, the novel ideas presented in the papers, the implementation of scheduling, clustering, TSCH, LLDN and security protocols used in the Contiki OS for analysis and all the work necessary in the editing process of the manuscripts.

C) Details of the contributions of other authors to the work:

Dr Andrew H. Kemp is the co-author for all the publications listed above. These publications have been written under his supervision, benefiting from excellent technical advice and editorial, patient guidance and valuable feedback.

Naveed Salman contributed with recommendations about how to efficiently structure a conference paper and how to emphasize the originality of the work and to make it more accessible to the reader.

Harith Yahya performed proofreading to the final drafts of the papers to ensure the solidity of the papers.

Acknowledgement

Firstly, I would like to express my sincere appreciation and thanks to my supervisor Dr Andrew H. Kemp for his guidance, patience, motivation, continues support and immense knowledge. Your guidance helped me in all the time of research and writing of this thesis. I would like to thank you for encouraging my research and for allowing me to grow as a researcher. I could not have imagined having a better mentor and supervisor like you dear Dr Kemp.

A special thanks to my caring father and loving mother. Words cannot express how grateful I am to you. Your pray for me was what sustained me this far. It was really difficult for me to be away from you all these years but you were always beating inside my heart. Whatever I am now is because of you. Thank you from the heart.

I am thankful to my wife for her love, patience and support that have always been my strength. You were always be here with me. Also I am thankful for my son, you brought the joy to my life and I have found my smile with you in all difficult times throughout this PhD. Also I would like to express my deepest gratitude for my sisters for their love and pray. Thank you all for being part of my life.

I also thank the Iraqi Ministry of Higher Education and Scientific Research and the Iraqi Cultural Attaché-London for their valuable support. Without their precious help it would not be possible to conduct this research.

Thank you Lord for always being there for me. I will keep on trusting You for my future.

For all my friends in the group of Wireless Sensor Network and friends in the school, thank you all for your valuable support and I was really lucky to work with wonderful friends like you.

Abstract

Ubiquitous object networking has sparked the concept of the Internet of Things (IoT) which defines a new era in the world of networking. The IoT principle can be addressed as one of the important strategic technologies that will positively influence the humans' life. All the gadgets, appliances and sensors around the world will be connected together to form a smart environment, where all the entities that connected to the Internet can seamlessly share data and resources. The IoT vision allows the embedded devices, e.g. sensor nodes, to be IP-enabled nodes and interconnect with the Internet. The demand for such technique is to make these embedded nodes act as IP-based devices that communicate directly with other IP networks without unnecessary overhead and to feasibly utilize the existing infrastructure built for the Internet. In addition, controlling and monitoring these nodes is maintainable through exploiting the existed tools that already have been developed for the Internet. Exchanging the sensory measurements through the Internet with several end points in the world facilitates achieving the concept of smart environment.

Realization of IoT concept needs to be addressed by standardization efforts that will shape the infrastructure of the networks. This has been achieved through the IEEE 802.15.4, 6LoWPAN and IPv6 standards.

The bright side of this new technology is faced by several implications since the IoT introduces a new class of security issues, such as each node within the network is considered as a point of vulnerability where an attacker can utilize to add malicious code via accessing the nodes through the Internet or by compromising a node. On the other hand, several IoT applications comprise mobile nodes that is in turn brings new challenges to the research community due to the effect of the node mobility on the network management and performance. Another defect that degrades the network performance is the initialization stage after the node deployment step by which the nodes will be organized into the network. The recent IEEE 802.15.4 has several structural drawbacks that need to be optimized in order to efficiently fulfil the requirements of low power mobile IoT devices.

This thesis addresses the aforementioned three issues, network initialization, node mobility and security management. In addition, the related literature is examined to define the set of current issues and to define the set of objectives based upon this. The first contribution is defining a new strategy to initialize the nodes into the network based on the IEEE 802.15.4 standard. A novel mesh-under cluster-based approach is proposed and implemented that efficiently initializes the nodes into clusters and achieves three objectives: low initialization cost, shortest path to the sink node, low operational cost (data forwarding). The second contribution is investigating the mobility issue within the IoT media access control (MAC) infrastructure and determining the related problems and requirements. Based on this, a novel mobility scheme is presented that facilitates node movement inside the network under the IEEE 802.15.4e time slotted channel hopping (TSCH) mode. The proposed model mitigates the problem of frequency channel hopping and slotframe issue in the TSCH mode. The next contribution in this thesis is determining the mobility impact on low latency deterministic (LLDN) network. One of the significant issues of mobility is increasing the latency and degrading packet delivery ratio (PDR). Accordingly, a novel mobility protocol is presented to tackle the mobility issue in LLDN mode and to improve network performance and lessen impact of node movement. The final contribution in this thesis is devising a new key bootstrapping scheme that fits both IEEE 8021.5.4 and 6LoWPAN neighbour discovery architectures. The proposed scheme permits a group of nodes to establish the required link keys without excessive communication/computational overhead. Additionally, the scheme supports the mobile node association process by ensuring secure access control to the network and validates mobile node authenticity in order to eliminate any malicious node association. The purposed key management scheme facilitates the replacement of outdated master network keys and release the required master key in a secure manner. Finally, a modified IEEE 802.15.4 link-layer security structure is presented. The modified architecture minimizes both energy consumption and latency incurred through providing authentication/confidentiality services via the IEEE 802.15.4.

Table of Contents

List of Figures

List of Tables

List of IEEE 802.15.4 Attributes

Attribute	Description
aBaseSuperFrameDuration	Time constant and corresponds to 15.36ms
aMaxLostBeacons	The maximum value of missed beacons to announce the node is orphan
aMaxPHYPacketSize	The maximum PSDU size
aTurnaroundTime	Required time for a device to change from transmit to receive state and vice versa
aUnitBackoffPeroid	Number of symbols to backoff in CSMA
LIFS	Long interframe space
macMinLIFSPeriod	Defined value of *LIFS* in the standard
macMinSIFSPeriod	Defined value of *SIFS* in the standard
macMaxFrameRetries	Maximum number of retries after transmission failure
macLLDNmgmTS	Indicate the existence of management timeslots (Boolean value)
macLLDNnumBid-irectionalTS	Number of bidirectional timeslots
macLLDNnumUp-linkTS	Number of uplink timeslots
macLLDNnumRet-ransmitTS	Number of retransmission timeslots
macLLDNdiscove-ryModeTimeout	Time threshold to change form discovery to configuration state

macMaxCSMABa-ckoffs	Maximum number of backoffs the CSMA can attempt
macSuperframeOrder	Active slot superframe duration
macTsMaxAck	ACK transmission time
macTsRxOffset	Beginning of the timeslot
macTsTxAckDelay	End of frame to start ACK
macAckWaitDuration	Required waiting time for an Acknowledgment message
SIFS	Short interframe space

List of Abbreviations

ACK	Acknowledgement
ASN	Absolute slot number
BI	Beacon interval
BO	Beacon order
CBC	Cipher block chaining
CCA	Clear channel assessment
CH	Cluster head
CIP	Cipher
CTR	Counter
CN	Correspondent node
CSL	Coordinated sampled listening
DEP	Decipher
DSME	Deterministic and synchronous multi-channel extension
EB	Enhanced beacon
FFD	Full-function device
FCS	Frame check sequence
GTS	Guaranteed time slot
IE	Information element
IoT	Internet of things
K_A	Key of node A
LLDN	Low latency deterministic network
LoWPAN	Low power wireless personal area network
MAC	Media access control
MAK	Master key

MAuC	Message authentication code
MN	Mobile node
MMP	Mobility management protocol
MWSN	Mobile wireless sensor network
PAN	Personal area network
POS	Personal operating space
RDC	Radio duty cycle
RFD	Reduced-function device
SD	Superframe duration
SO	Superframe order
TSCH	Timeslotted channel hopping
WSN	Wireless sensor network

List of Symbols

Chapters three and six

Symbol	Description
nSF	Number of slotframes
nTS	Number of timeslots in each slotframe
ebP	EB announcement duration
T	Timeslot duration
TS	Timeslot index
nS_O	Number of online superframes
nS_D	Number of discovery superframes
nS_C	Number of configuration superframes

Chapter four

Symbol	Description
T_RA	Time reference for node A
T_f	Required time to transmit a frame
C_p	Collision point
R_received	Received rank
R_current	Current rank
W_recived	Received weight
W_current	Current weight
T_P	Time period interval (resembles beacon interval)
D_{pos}	Density of sensor nodes within a POS
K_A	Key of node A

L_P	length of payload
h	number of hops
F_R	mean forwarding rate
R_R	mean rate of the received frames
U	Utilization of a relay node
B_F	number of buffered frames

Chapter five

Symbol	Description
F_{ch}	number of frequency channels
T_s	settle time
$P_{eb}(sf)$	probability of receiving at least one EB
$P_{(ts_n)}$	probability of receiving an EB in a given slot index
$Peb(sfi)$	probability of receiving an EB on a slotframe
σ	probability of leaving a POS
D_{RSSI}	distance of the mobile node from a FFD
R_{dBm}	maximum transmission range of a FFD
β	Probability of gaining a free SHARED TX link
sh	number of shared links
E_m	expected number of mobile nodes entering a POS
A_n	number of existed nodes
L_D	number of dedicated links
φ	probability of receiving an acknowledgement
η	probability of a FFD accepts an association request
ε	number of available time slots
$\overline{E_m}$	Number of mobile nodes that migrated out the POS
Re	number of association requests

θ	channel error rate
mn	number of contending mobile nodes
sf	given slotframe
W_{LM}	time window (listening to mobile nodes requests)
W_{ACK}	time window (sending ACK messages)
L_t	time between listening to an ACK to sending association
T	single timeslot duration
ts	given timeslot index (position in slotframe)
sf_D	slotframe duration
T_{LM}	random time to listen for mobile nodes
T_{ACK}	random time to send an ACK message
tp	time required to receive a response after requesting
w	maximum waiting time to join a network

Chapter six

Symbol	**Description**
AST_{req}	Requesting association
AST	Associated to the network
Ad_i	i^{th} adjacent POS
B_P	Beacon period
BE	Backoff exponent
CW	Contention window length
Dis	Indicating dissociated
D_m	Density metric
D	Distance
D_Mgts	Downlink management timeslot
E_{thr}	effective throughput

h	Hop index
i-Mgts	Image of a management timeslot
K	Possible number of movements inside a POS
L_h	latency in a given hop
L_D	Expected latency during discovery state
L_C	Expected latency during configuration state
L_{CA}	Expected latency during acknowledging configuration state
Los_D	number of lost data frames
M_m	Mobility metric
Mgts	Management timeslots
N_m	number of mobile nodes seek to associate the coordinator
N_{crt}	Set of existed nodes in a POS
N_A	Set of active nodes
$N_a(i)$	Number of nodes get associated at a given time t_i
N_w	Number of nodes waiting to associate
nP_h	Number of mobile nodes attached to a given proxy
O_c	Preferred number of online superframes
P_A	Interval time between two beacons
P_{th}	Maximum number of online superframes
R	Transmission range
Req_s	Maximum configuration request size
R_S	Symbol rate
R_t	Total running time
S	Superframe in general (any superframe type)
S_D	discovery superframe interval
S_C	configuration superframe interval
S_O	online superframe interval

SC_B	Scanning for beacon phase
S_{Bmgts}	Size of a single slot in Mgts
TS	Timeslot index
T_{SZ}	Timeslot size (excluding interframing space)
T_{ack}	Turnaround time
T_{Mgts}	Time counter after what the proxy node accepts association request
ts	Settle time in a POS
U_Mgts	Uplink management timeslot
$V_x(t)$	velocity of node x at time t
x_D	number of mobile nodes successfully transmitted discovery response frame
γ_D	Probability of the first CCA returns free (during discovery state)
α	Probability of receiving a beacon
β	probability of a received beacon determines discovery state
δ_D	Probability of the second CCA returns free (during discovery state)
θ_t	Probability to complete association within ts

Chapter seven

Symbol	**Description**
MAK-X	Master key with index X
SHA2-256(X)	Applying hash function to input X
Ran_A	Random number generated by node A
$CIP_{MAK\text{-}0}(X)$	Ciphering an input block X with key (MAK-0)
$DEP_{MAK\text{-}0}(X)$	Deciphering an input block X with key (MAK-0)
MAuC	Obtaining message authentication code of input block X
TS	Required time to exchange shared keys within a single POS
C	Ciphered text

M	Message (plain text)

Chapter 1. Introduction

The evolution of the IoT concept is determined by multiple standardization tools that have shaped the infrastructure of the IoT paradigm. Regarding limited memory and low power devices as required for wireless sensor network (WSN), three basic components have formed the communication stack which will smoothly integrate these limited power devices with the Internet. These three elements are the IPv6 protocol, the 6LoWPAN adaptation layer and the IEEE 802.15.4 standard. The IEEE 802.15.4 [4] standard defines the dominant physical and MAC layers of the IoT infrastructure. In addition, multiple industrial technologies that reside under the IoT umbrella have incorporated the IEEE 802.15.4 as the default physical and MAC components, e.g. WirelessHART, ISA 100.11a and WIA-PA. Hence, several contributions are made to optimize the performance of this standard and achieve a more coherent system. As a result, the first MAC amendment IEEE 802.15.4e [1] has been introduced that presents two important modes of operation, low-latency deterministic network (LLDN) and timeslotted channel hopping (TSCH). The LLDN is designed to support applications that emphasize high cyclic determinism and low latency reading aggregation. In the meantime, TSCH aims to provide network robustness and minimizes the impact of collision while increases network throughput and extends the effective range of communication.

The emergence of such IoT networks led them to be utilized into further, different sorts of application that each has different requirements with various challenges. Applications like health (wearable sensors) [5], cargos containers [6], automotive industry and airport logistics all share the aspect of also including mobile nodes. Therefore, the current standards and technologies must consider the overhead of node movement and its impact on the functionality of the network.

1.1 IoT Paradigm

Realizing the IoT concept is basically depended on three important standards, which are the IEEE 802.15.4, the 6LoWPAN and the IPv6 [7] protocol. The core of the IoT is the 6LoWPAN adaptation layer [8], [9] which allows IPv6 packets to be transferred through IEEE 802.15.4 standard, so it will facilitate the interoperability of the mobile IP-based wireless sensor networks (MWSNs) with the Internet. Fig. 1.1 shows the basic layout of the IoT paradigm. The 6LoWPAN layer provides two services for the sensor nodes, which are: Fragmentation / defragmentation, compression / decompression in order to transmit the IPv6 packets over IEEE 802.15.4 frames.

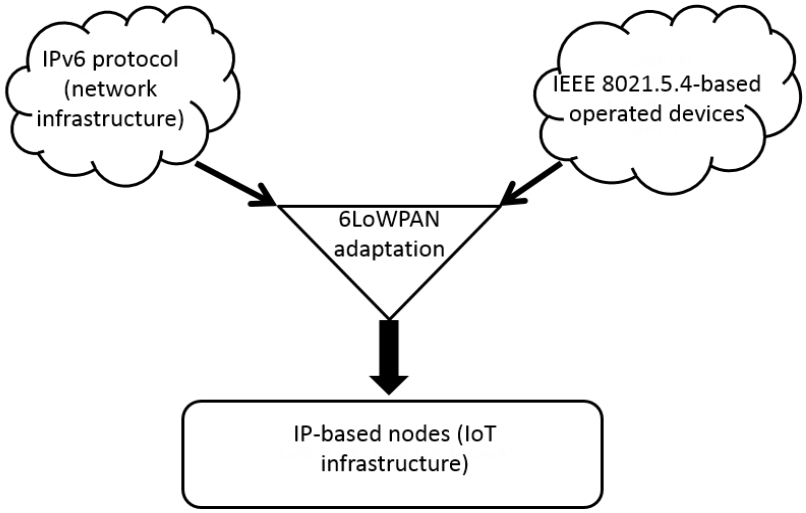


Fig. 1.1: 6LoWPAN-based network

The 6LoWPAN layer works basically by tagging the IPv6 packets with special header types to define the fragmentation process or to support multi-hop mesh networking [8]. Fig. 1.2 shows the 6LoWPAN layer stack compared to the TCP/IP and the OSI model. Such a standard led to the IP-based Wireless Sensor Network, that a sensor network can communicate and exchange information with the Internet cloud.

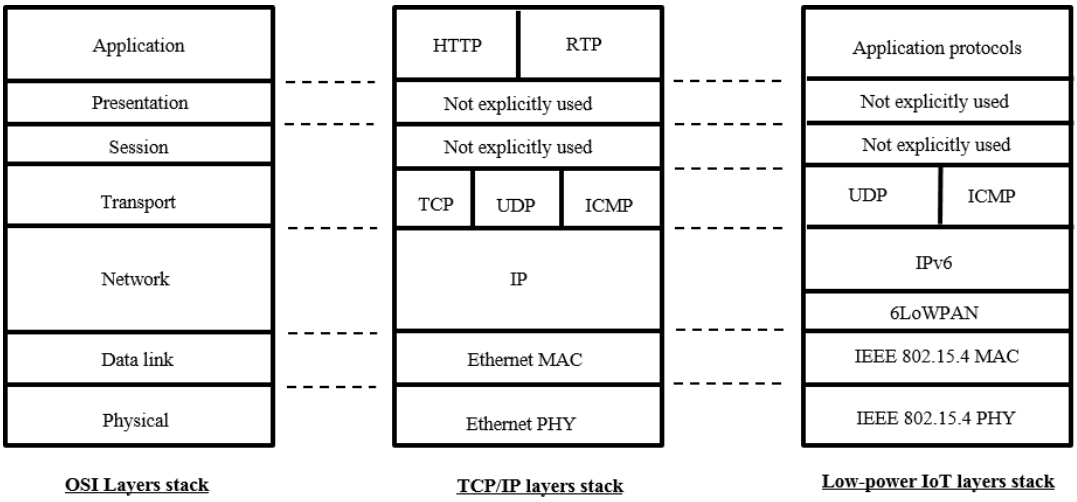


Fig. 1.2: Communication layers stack

The second important component that forms the IoT is the IEEE 802.15.4 standard which is targeted for low-rate wireless personal area networks (LR-WPANs) with devices that are low-power, low-data-rate and short-range radio frequency (RF) transmissions in a wireless personal area network (WPAN) [4], such as the wireless sensor networks.

Basically, this standard defines two types of network topology, star and peer-to-peer. In addition, the standard defines two types of devices, reduced-function device (RFD) and full-function device (FFD). The 802.15.4 MAC protocol exploits two communication modes, beacon-enabled and non-beacon (beacon-less) mode. While in the beacon-enabled mode the PAN coordinator transmits a periodic beacon to synchronize the communications between the devices and the coordinator, with the non-beacon enabled mode beacons are not broadcast and the devices contend with each other to transmit to the coordinator using the unslotted CSMA/CA [10].

1.2 Problem Statement

The IoT is becoming a reality with the existence of several standardized protocols that construct the IoT paradigm. Unfortunately, till now there are several issues that need to be addressed and are affecting the solidity of the current IoT standards.

The first issue is related to the IEEE 802.15.4 MAC structure by which there is no valid mechanism to organize the nodes in the network during the network initialization phase. In addition, the current approaches do not manage to provide an efficient multihop network topology that can relay the traffic from nodes to the sink in an energy efficient manner (during network steady state). Recent approaches rely mainly on the standardized routing protocol (RPL) which incorporate excessive overhead since the routing process is handled through the network layer. In addition, current IoT operating systems, i.e. Contiki OS [11] and TinyOS [12], are considering asynchronous media access mechanism and not the synchronous due to high energy overhead associated with the latest scheme.

The second issue is the node mobility which associated with different kinds of IoT applications. Unfortunately, recent approaches are relying on standardized protocols such as MIPv6 [13] and NEMO [14] that are not applicable for constrained devices as they require high number of exchanged messages in order to accommodate a node movement. Moreover, for IEEE 802.15.4, the only mode which the mobility has been addressed for is the beacon enabled mode while the two recent important modes (TSCH and LLDN) haven't been considered. The infrastructure of TSCH considers a frequency channel hopping strategy which complicates the mechanism of handling node movement and in turn maximizes node dissociation time. In the meantime, the LLDN mode has been designed to meet the criticality and time limitations in low latency applications. With the existence of mobile nodes in the network, the LLDN fails to meet the time constraints that have been set by the standard and this issue affects its applicability in real-time and time-sensitive applications.

The third problem is the key distributing process. Until now, there is no defined standardized key management scheme while the majority of the proposed key management protocols are adapting asymmetric key technique which is impractical for low power constrained devices. In addition, the current link-layer security structure which is adapted by the IEEE 802.15.4 to provide authentication and confidentiality services, has a high energy overhead and maximizes the latency via including a bulky cipher mode of operation. Moreover, all the approaches of handling mobility and providing key management are standalone techniques by

which these mechanisms are separated. Integrating the key bootstrapping phase with the node joining process (utilizing the same exchanged messages) can dramatically reduce the impact of energy consumption to half.

1.3 Research Contribution

The contributions of this thesis are as follows:

- Presenting a mesh-under cluster based routing (MUCBR) protocol that initializes the IEEE 802.15.4-based nodes in clusters and determines the shortest route to the sink via a chain of connected cluster heads (CH). The proposed MUCBR presents a novel initialization mechanism that mitigates the high network setup cost issue which associated with all scheduling schemes. MUCBR manages to disprove the assumption that network scheduling comes always with a high cost and thus, avoiding its adaption in the recent IoT operating systems. The clustered architecture of the proposed MUCBR produces a chain of cluster heads that eliminates the need of bridge nodes to connect two clusters and facilitates the proposed key bootstrapping/management scheme in this thesis (chapter 7).
- Investigating recent literature regarding mobility management techniques to identify the possible challenges that affect the IoT paradigm. In addition, study the impact of node mobility for both IEEE 802.15.4e TSCH and LLDN modes through implementing these modes within the Contiki OS.
- Proposing a mobility aware protocol (MTSCH) that mitigates the issue of frequency channel hopping in TSCH mode. The MTSCH presents a novel scheme to facilitate a mobile node association and reduces the dissociation time. The MTSCH introduces solid approaches to mitigate the TSCH problems of undefined beaconing, undefined slot allocation technique and undefined mechanism to organize shared slots. A passive beacon mechanism is proposed which utilizes the acknowledgement (ACK) messages, sent by FFD devices, to announce the existence of FFDs. These passive beacons will be transmitted based on a randomized fashion on a fixed channel. Thereby, each FFD selects a random time reference, picked up from a predefined time

window in order to mitigate the probability of collision with other ACK messages. Both TSCH and MTSCH have been implemented within Contiki OS to investigate the node mobility overhead for the two models. MTSCH shows improved node connectivity and a reduction of nodes' radio duty cycle (RDC) which in turn led to minimized energy consumption.

- Proposing a mobility management approach MA-LLDN that considers the defect of LLDN mode with the presence of mobile nodes. MA-LLDN manages to minimize encountered latency caused by multiple and long dissociations periods. Related technical problems such as: (i) transmission phases issue, (ii) association restriction to only discovery and configuration phases, (iii) low packet delivery ratio as changing transmission phase to accommodate new mobile nodes, (iv) low scalability as relying on a star topology network. The impact of mobility on the LLDN mode has been considered via presenting a Markov chain model which addresses the possible states a mobile node might encounter through the association process. The proposed MA-LLDN supports a multihop topology to extend the coverage of the coordinator while omitting the need for deploying further coordinators in the network. In turn, this minimizes the deployment cost and the probability of beacon collision between adjacent coordinators. The proposed approach has low latency since it delivers the readings within the same superframe. The relay nodes also act as a proxy to the coordinator where they can passively indicate the existence of the coordinator with low overhead and less association delay.
- Presenting a novel energy efficient key bootstrapping scheme (EESKB) that efficiently establishes required link-keys in clustered/non-clustered network. EESKB preserves required level of security while minimizing the energy overhead of the key management process and avoids the dependency on a public key methodology. Proposed EESKB facilitates new mobile node association process and ensures low computation/communication overhead. Moreover, the current IEEE 802.15.4 cipher modes of operation have been modified to provide authentication/confidentiality services with low energy cost. The modified link layer security preserves the same security level and

minimizes latency associated with the processes of ciphering and authenticating traffic.

Fig. 1.3 depicts the major contributions of this thesis and the main outcomes of each one with regards to the IoT context.

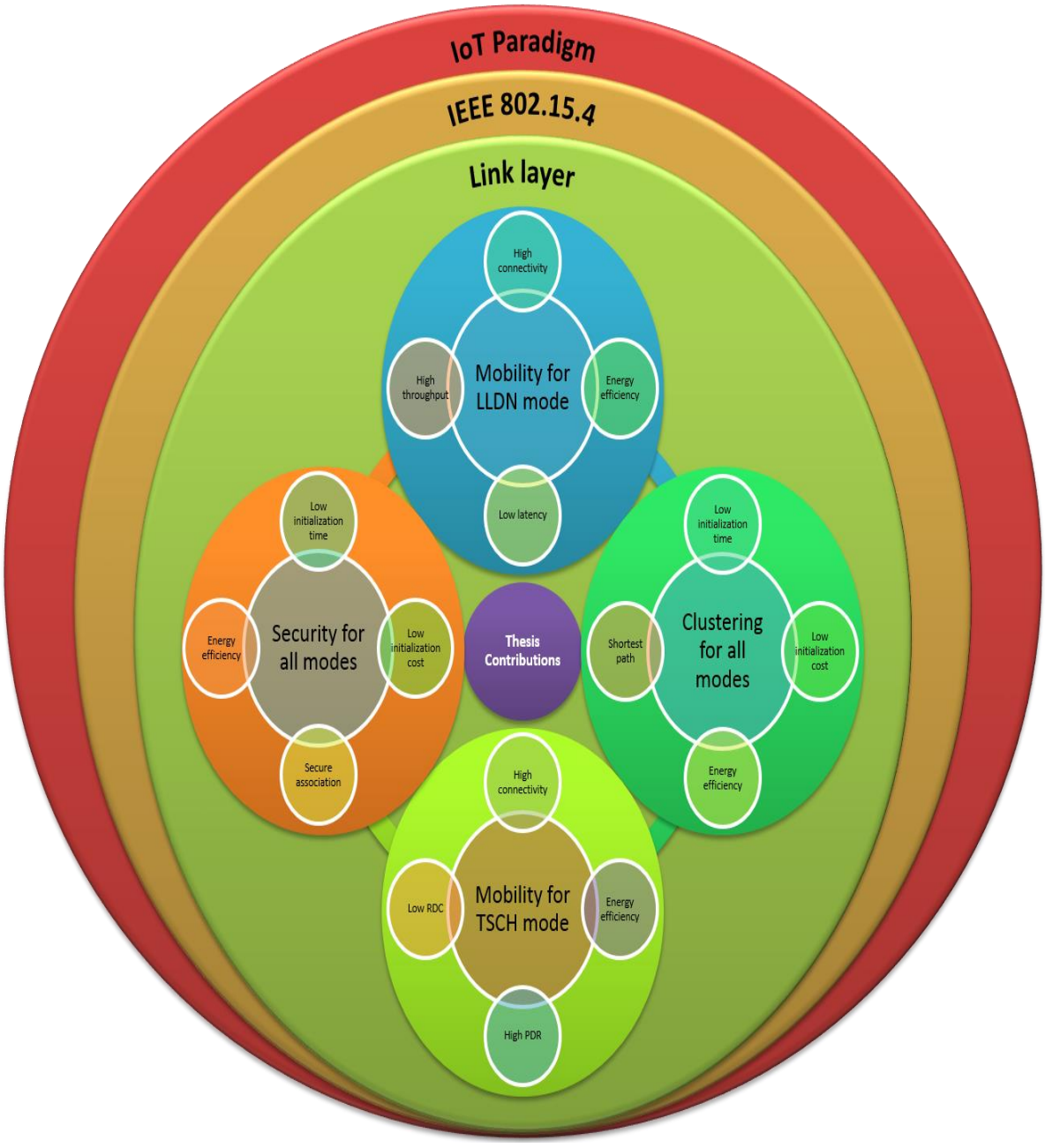


Fig. 1.3: Research contributions

1.4 Thesis outline

Following the introduction chapter that highlights the paradigm of the IoT, the next chapters are organized as follows:

Chapter 2 presents an overview on the world of IoT and explains briefly different mobility terminologies. In addition, a brief snapshot on the principle of RDC is demonstrated while defining the recent sampling/scheduling techniques used in the context of low power devices. Finally, this chapter discusses the basics of security tools and structures utilized in the field of constrained IoT devices.

Part of this chapter is presented in "Mobility of Low Power Devices: The State of The Art", IEEE Internet of Things Journal, Under Review (Revised version submitted).

Chapter 3 investigates the literature to define the current approaches and their related issues while identifying the current drawbacks that need to be addressed. An overview is presented regarding the possible approaches under each IoT communication stack layer to handle mobility. Accordingly, both IEEE 802.15.4e TSCH and LLDN modes are analysed and implemented within the Contiki OS to study the performance of these two modes with the presence of node mobility in the network. The chapter summarizes the issues in each mode and define the possible solutions for each problem individually. Simulation results are presented and consider the energy cost of handling mobility besides the total connectivity ratio to the network (as it is related to the amount dissociations caused by node movement). A comparison between LLDN and TSCH is presented to describe the drawbacks and advantages of each mode with regards to different network parameters.

The first part of this chapter has been presented in "Impact of mobility on the IoT MAC infrastructure: IEEE 802.15.4e TSCH and LLDN platform," in the proceeding of *IEEE 2nd World Forum on Internet of Things (WF-IoT),* pp.478-483, Milan, 14-16 Dec. 2015.

The second part is presented in “Mobility of Low Power Devices: The State of The Art”, IEEE Internet of Things Journal, Under Review (Revised version submitted).

Chapter 4 introduces a proposed mesh-under cluster-based routing (MUCBR) protocol that provides a network initialization approach for IEEE 802.15.4 standard. Firstly, the related work under this topic is examined and secondly the principles of mesh-under and route-over are explained. The next section of this chapter introduces the possible attributes and assumptions of the proposed MUCBR protocol and is followed by a full description of this model. Finally, the analysis section discusses related results and compares the proposed MUCBR with RIME and RPL protocols.

This chapter has been presented in "Mesh-Under Cluster-Based Routing Protocol for IEEE 802.15.4 Sensor Network," in *Proceedings of 20th European Wireless Conference;* Barcelona, 14-16 May 2014.

Chapter 5 presents a proposed novel mobility management approach that efficiently handles node mobility under the IEEE 802.15.4e TSCH mode. The chapter introduces related literature in this area followed by examining the impact of mobility on TSCH mode. A Markov chain model is presented to analyse the parameters that influence node association process. Accordingly, a novel mobility-aware MTSCH model is proposed that tackles the overhead of node movement within a TSCH network. A detailed discussion is then provided to examine the proposed MTSCH protocol and the mechanism by which to tackle the issue of frequency channel hopping. This section also examines the mechanism that will organize the enhanced beacon broadcast process and demonstrates the proposed principle of passive beaconing. The MTSCH section is followed by the implementation and analysis section which highlights the performance of both default TSCH and MTSCH. The analysis is focused on the RDC behaviour and its related energy consumption and ended by determining the connectivity ratio of each model. Finally, this chapter has been summarized to simplify the main outcomes of this chapter.

This chapter has been published in "Mobility Aware Framework for Timeslotted Channel Hopping IEEE 802.15.4e Sensor Networks," in *IEEE Sensors Journal*, vol.15, no.12, pp.7112-7125, Dec. 2015.

Chapter 6 introduces a study of the overhead of node mobility under IEEE 802.15.4e LLDN mode and proposes a mobility management protocol for LLDN mode. This chapter starts by examining the related work to this topic and then followed by presenting a Markov chain model which depicts the possible states a mobile node may encounter while operating under this mode. Next in this chapter, a novel mobility-aware MA-LLDN protocol is demonstrated and the proposed methodology to tackle the increased latency is presented. In addition, the proposed backoff mechanism and the technique to maximize the coordinator coverage for mitigating the issues of LLDN-star based topology are explained. Additionally, both default LLDN and proposed MA-LLDN schemes were evaluated and the most crucial metrics have been examined, i.e. energy consumption, PDR and latency. The chapter at the end has been summarized to conclude the possible outcomes.

This chapter has been published in "Tackling Mobility in Low Latency Deterministic Multihop IEEE 802.15.4e Sensor Network," in *IEEE Sensors Journal*, vol. 16, no. 5, pp. 1412-1427, March, 2016.

Chapter 7 deals with the security issue and specifically the key management problem for the IoT backbone. A related work section is introduced to examine the current approaches within this field. The next section addresses the proposed key bootstrapping scheme (EESKB) that manages the key initialization procedure during network deployment phase. Additionally, the methodology section shows how the proposed EESKB model can handle node mobility and ensures only authorized mobile node association. This section is followed by presenting the modified authentication/confidentiality scheme for IEEE 802.15.4 link-layer security. The modified scheme is demonstrated to address how the overhead of these two services can be minimized through adopting the hashing technique. Later in this chapter, the impact of the EESKB is compared with other related methodologies focusing on the

energy consumption factor. Moreover, the achievement of the modified IEEE 802.15.4 link-layer security has been considered and followed by the security analysis section which explains the security strength metric in this work. Finally, a summary is presented to brief out the whole chapter and its contribution.

This chapter will be presented in "Energy Efficient Key Bootstrapping Scheme for Constrained Mobile IoT Devices", To Be Submitted to the *IEEE Internet of Things Journal*.

Chapter 8 concludes the outcome of the research contributions in this thesis and how the proposed schemes managed to enhance the current IoT paradigm. In addition, a set of future directions have been discussed to provide a group of research trends that can efficiently present a solid IoT framework for mobile low power devices.

1.5 List of Publications

The following publications have emanated from the work of this research:

Journal Papers:

1- Al-Nidawi, Y.; Kemp, A.H., "Mobility Aware Framework for Timeslotted Channel Hopping IEEE 802.15.4e Sensor Networks," in *IEEE Sensors Journal,* , vol.15, no.12, pp.7112-7125, Dec. 2015.

2- Al-Nidawi, H. Yahya and A. H. Kemp, "Tackling Mobility in Low Latency Deterministic Multihop IEEE 802.15.4e Sensor Network," in *IEEE Sensors Journal*, vol. 16, no. 5, pp. 1412-1427, March, 2016.

3- Al-Nidawi, Y.; Kemp, A.H., "Mobility of Low Power Devices: The State of The Art", IEEE Internet of Things Journal, Under Review (Revised version submitted).

4- Al-Nidawi, Y.; Kemp, A.H., “Energy Efficient Key Bootstrapping Scheme for Constrained Mobile IoT Devices”, To Be Submitted to the IEEE Internet of Things Journal.

Conference Papers:

5- Al-Nidawi, Yaarob; Yahya, Harith; Kemp, Andrew H., "Impact of mobility on the IoT MAC infrastructure: IEEE 802.15.4e TSCH and LLDN platform," in *Proceedings of IEEE 2nd World Forum on Internet of Things (WF-IoT),* pp.478-483, Milan, 14-16 Dec. 2015.

6- Al-Nidawi, Yaarob; Naveed Salman, ; Kemp, Andrew H., "Mesh-Under Cluster-Based Routing Protocol for IEEE 802.15.4 Sensor Network," in *Proceedings of 20th European Wireless Conference;*, pp.1-7, Barcelona, 14-16 May 2014.

Co-Authored Publications:

7- H. Yahya, Y. Al-Nidawi and A. H. Kemp, "A dynamic cluster head election protocol for mobile wireless sensor networks," in *Proceedings of International Symposium on Wireless Communication Systems (ISWCS)*, Brussels, 2015, pp. 356-360.

8- H. A. A. Al-Kashoash, Y. Al-Nidawi, and A. H. Kemp, “Congestion Analysis for Low Power and Lossy Networks,” Accepted in *Proceedings of Wireless Telecommunications Symposium (WTS)*, 2016.

9- H. A. A. Al-Kashoash, Y. Al-Nidawi, and A. H. Kemp, “Congestion-Aware RPL for 6LoWPAN Networks,” in Accepted in *Proceedings of Wireless Telecommunications Symposium (WTS)*, 2016.

Chapter 2. Background

Node mobility is an emerging, unresolved challenge for IoT infrastructure. Under the IoT umbrella, realization of fully connected heterogeneous networks that composed of different technologies and standardized elements will be determined by how these elements tackle node mobility. The IoT infrastructure must be enabled with efficient mobility management protocols (MMPs) that handle node mobility and guarantee reliable handover and low dissociation time.

Three crucial aspects must be tackled while handling node mobility; these are the association process, routing and security. With each node movement, there must be a mechanism that ensures a smooth handoff process and minimizes the dissociation time. This association process would typically be divided into two steps within the IoT paradigm. The first step is a fast link-based handoff facility that guarantees the node is connected to its closest homogenous network attachment point. The second step is a network-based association by which the node will be assigned an IPv6 address making it globally identifiable. The routing process on the other hand is required to provide a reliable and shortest path to the sink or a correspondent destination point. The security aspect is considered as pivotal since it must ensure secure access control and eliminate malicious node association.

2.1 Mobility Overview

The impact of node mobility is an important factor influencing network functionality and sustainability. The mobility of nodes introduces several overheads that are caused by a continuous change in the network topology. The phenomena of the IoT has opened the gate to a new era of communication by which different kinds of devices, technologies and standardizations elements are diffused into a single coherent system. Wearable devices, RFIDs and sensors will form the fabric of information feeding into the IoT. These devises share that they are low-power,

memory and computationally constrained devices. Meanwhile, due to the diversity of applications within the IoT, the majority of these constrained nodes are likely to be mobile (or at least have a dynamic propagation environment) in order to perform their intended tasks. Accordingly, regardless of the network heterogeneity, these devices have to be self-configurable and service-cooperative in order to tackle the issue of mobility. Based on this point, a solid mobility management protocol has to fulfil this objective by seamlessly handling node mobility while ensuring low dissociation time and a high packet delivery ratio.

Before tackling mobility, the appropriate approach to handle node movement has to be defined which is fundamentally based on several parameters. Hence, the best MMP can be identified through defining both the IoT communication stack layer (to manage mobility) and the pattern of mobility.

The recent trend is to present a standardized framework for the IoT and this is exemplified in the current work of IEEE P2413 "Standard for an Architectural framework for the Internet of Things". Alternatively, there is a de facto communication stack that can be dedicated for constrained devices and is composed from three basic standardized protocols, IEEE 802.15.4, 6LoWPAN and IPv6[15]. The IEEE 802.15.4 forms the physical and the MAC layers inside the network stack. In addition, not to forget the application layer which can be realized by such protocols as CoAP [16] and MQTT [17]. Hence, based on this classification, the MMPs can be categorized into different layers based on which one handles the mobility.

2.1.1 Mobility Terminology and Attributes

In this section, the basic attributes and specifications of mobility inside the IoT are explored. It's mandatory to highlight the different aspects and terminologies used in the mobility context prior to discussing the recent approaches and their challenges in the IoT.

Mobility can be classified into several classes based on the aspect by which it has been categorized. The classification can be made based on device type, mobility model, node speed, movement pattern, movement detection scheme and the layer

which handles the task of controlling mobility. For more details on available models, [18] presents a comprehensive evaluation on different mobility models used for ad hoc networks. For example, Fig. 2.1 demonstrates possible classes by which mobility can be addressed.

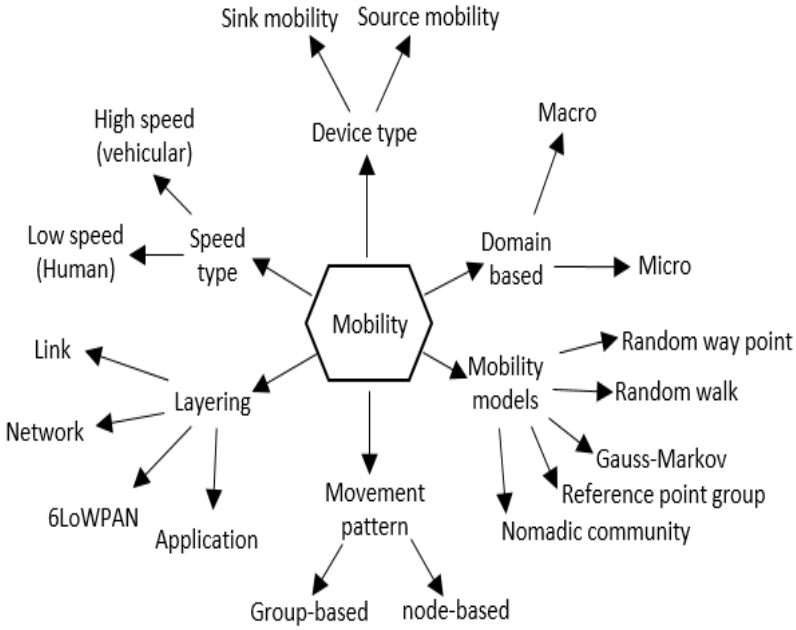


Fig. 2.1: Possible mobility classifications

2.1.2 Patterns of Mobility

The mobility can be classified into two types, micro and macro mobility [3, 19]. Micro mobility refers to node movement inside a single network domain while macro mobility is a movement between different domains. In order to allow a mobile node (MN) to join a network, there will be required two basic steps to finalize the association and this is based on the mobility type. The first step is the 'link association' and the second is the 'network association'. Any node must first performs the link association process by which to associate with the closest node in its perimeter and then consider the network association to obtain the IPv6 address. Link mobility (which is sometimes referred to as access mobility [20]) is determined by the wireless technology and must guarantee uninterrupted communication while the node changes its point of attachment. Meanwhile, other different terminologies can define the link association as handover while the network association can be

called roaming. The macro mobility requires both the process of handover and roaming while micro mobility needs only the handover step [3]. Fig. 2.2 shows an example on the difference between macro and micro mobility.

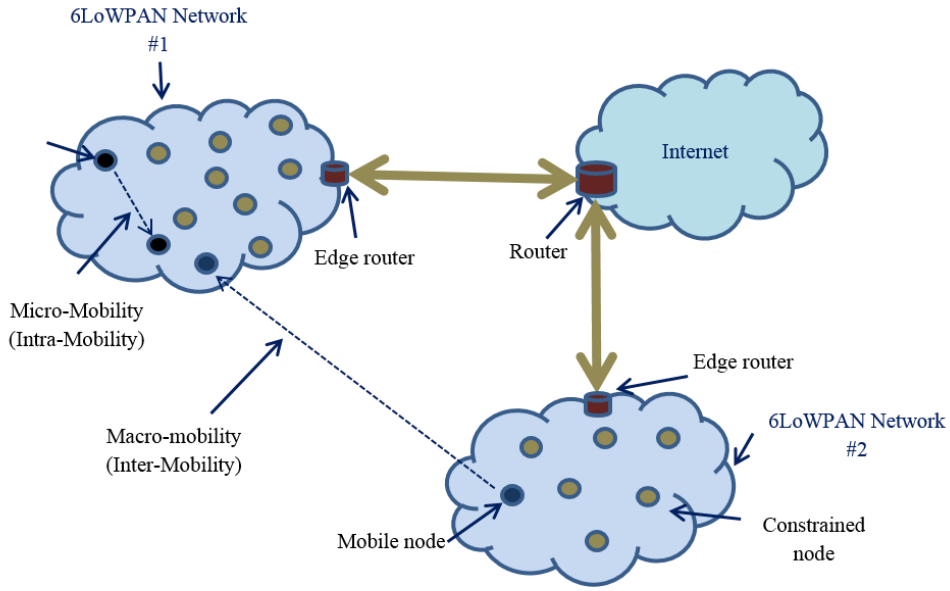


Fig. 2.2: Macro versus micro mobility [3]

Link association is based on different steps as channel scanning, association, short address allocation, authentication and any other mode-related services (presuming the IEEE 802.15.4 is the link layer). The steps are all determined by the modes of operation in the IEEE 802.15.4e (beacon-enabled, TSCH, LLDN or DSME) or the radio duty cycling used while operating on the beaconless mode (i.e. sampled listening technique).

Moreover, the mobility of nodes can be derived into two classes, node and group mobility. The node mobility refers to the movement of an individual node inside the network while the group mobility is the movement of multiple nodes together.

There is another mobility class which is called ‘network mobility’ which corresponds to the movement of an edge router that connects a network to the Internet [3].

The final attribute for mobility is determined by the role of a node in the network. This can be either sink mobility or node mobility. Several approaches rely on moving the sink node to expedite the process of data aggregation and to reduce the

overhead of data forwarding for the regular nodes in the network. In some cases, both nodes and sinks are mobile and this depends on the application type.

2.1.3 Mobility Handling Process

The principle by which the mobility is handled can be categorized into two sectors. The first one is the node-based MMPs that an MN is responsible for determining how to re-initialize a connection after a dissociation occurs. The second one is network-based MMP where the network is responsible for handling the process of associating an MN to the network. The network-based approach has less overhead over the MN as compared to the node-based scheme.

Although there is some literature indicating that with network-based mobility the nodes need no additional installation to handle mobility and there is no additional overhead, but there is still the problem of link association by which the nodes are still moving between different coordinators within the same network (domain). Thus, the only advantage of network-based MMP is when the node is communicating other terminals on other different domains.

2.1.4 Layer Based Classification

One of the important factors in the MMP design is defining which layer within the communion stack will manage mobility. Under the IoT umbrella, ideally there will be four layers that can manage mobility; MAC, 6LoWPAN, network and application. It’s advisable to think of the type of mobility prior to selecting the layer that will handle it. As an example, since the mesh-under techniques are appropriate for handling micro mobility [3], then either MAC-based or 6LoWPAN-based MMPs are suitable to manage micro mobility. Conversely, the macro mobility can be tackled through either network-based or application-based MMPs.

2.1.5 Mobility Management Initiation Process

One of the important concepts for tackling node mobility is the node movement detection scheme. Movement detection sparks the process of considering a new

association and the required steps to realize a fast handover. Based on this, the MMPs are utilizing two approaches which are either ‘reactive’ or ‘proactive’ schemes. For reactive scenarios, an MN initiates the process of association once it detects that it has lost a connection with the network. Regarding proactive approaches, the MN or the network coordinators are always monitoring the MN movement to predict the time that an MN will lose connection and the next possible attachment point based on the MN movement trajectory. The reactive technique has less energy overhead but increases the latency of the handover process. On the other hand, the proactive technique has higher energy overhead due to the process of monitoring both link quality and node movement direction, in turn it has less handover latency as compared to reactive protocols.

2.2 MAC Scheduling and Listening Techniques

The radio duty cycle (RDC) of constrained nodes can be considered as a crucial factor that determines the low power IoT network lifetime and its service availability. Two listening techniques are utilized to reduce the RDC of the nodes, sample and schedule listening technique. Alternative definitions to these two techniques are, synchronous (scheduled) and asynchronous (sampling) [21].

Other definitions as in [22] go further and classify the synchronous listening technique to two types depending on the strategy by which the nodes are synchronized, *Instantaneous synchronization* (the nodes swap control messages to achieve synchronization) and *pre-defined synchronization* (the network has predefined time division multiple access TDMA structure).

Regarding the first and the most common type of listening techniques, sampling, this technique has been utilized by the most well-known constrained nodes operating systems, Contiki OS through the ContikiMAC [23] RDC technique and the TinyOS OS through the LPL [24] RDC technique. The sampling technique is basically depends on a mechanism by which the sender has to continuously transmits the packet until the receiver turns on its radio and receives the packet [25].

On the other hand, schedule listening technique is based on a tight synchronization between adjacent nodes to synchronize the transmission and permit the receiver node to switch on the radio only on a pre-defined time slots to reduce the RDC. According to [21], unlike the sampling technique, the initialization process cost of the schedule listening approach is too high and adds complexity to the network. This overhead caused by the control messages required to synchronize the nodes. Thus, the nodes within the asynchronous techniques have gained an improved energy consumption over synchronous approaches since they do not rely on the control messages [26]. Later, the contribution of chapter four will indicate that the synchronous approach can have low energy consumption as compared to asynchronous listening technique and disproves this assumption. Fig. 2.3 demonstrates the basic structure of each listening technique. With the asynchronous (sampling) scheme, there are two methodologies. The first one is based on transmitting preamble bytes and once the receiver detects these transmissions it will open its radio to receive the actual frame (which is transmitted directly after a specific amount of preamble bytes and determined by the network settings). The second methodology is consisting on sending the actual frame multiple times to ensure that the number of transmissions cover the check interval period. The check interval period is the interval between two successive radio scanning processes that a receiver performs to detect if there is any activity on the media. Maximizing the check interval period will increase data latency and decreasing this interval will maximize the energy consumption.

Besides the ContikiMAC and LPL, other asynchronous listening techniques exist like B-MAC [27], WiseMAC [28] and X-MAC [29]. Moreover, there are two common synchronous (*Instantaneous synchronization*) listening techniques, which are T-MAC [30] and S-MAC [31]. In addition, two synchronous (*pre-defined synchronization*) techniques exist: LMAC [32] and DMAC [33]. [22] presents FLAMA [34] as TRAMA technique and consider it as *pre-defined synchronization* while [34] introduces the FLAMA listening technique and not TRAMA. The TRAMA actually is presented in [35] and FLAMA is the successor of TRAMA. In addition, Corbllini *et al*. [22] define both of TRAMA and FLAMA as *pre-defined synchronization* techniques, while they must be considered as *Instantaneous*

synchronization techniques due to the dependency on exchanged control messages during the network initialization to achieve synchronization.

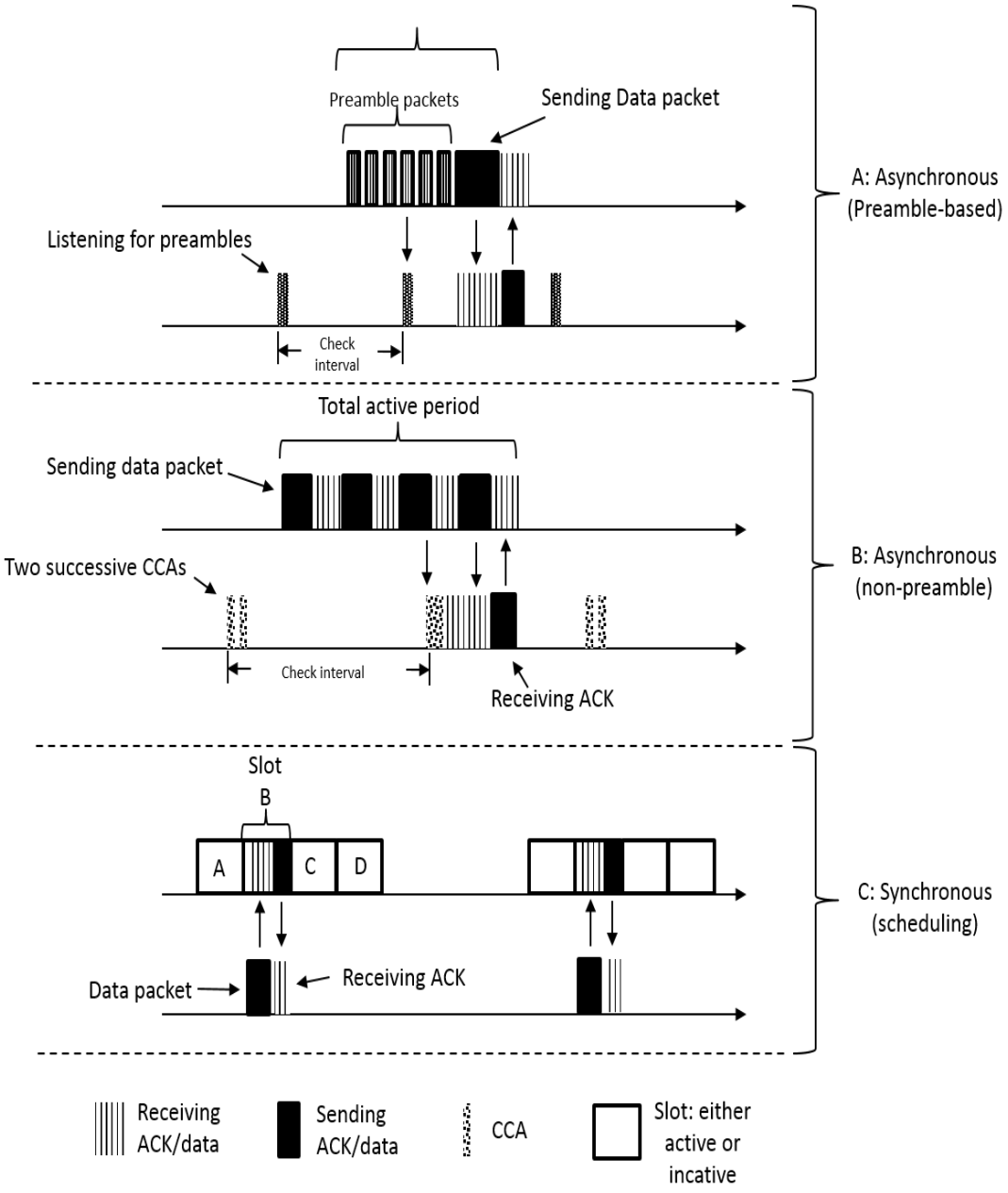


Fig. 2.3: Asynchronous and synchronous listening techniques

2.3 Security Concept Under the IoT Context

The security aspect is a wide field that composes several terminologies and different design methodologies. This section highlights the main principles and modelling techniques that are concerned with the trend of this research.

2.3.1 Security Requirements and Challenges

In order to provide authentic and reliable services and to ensure the availability of the IoT nodes, there are multiple crucial security requirements that need to be addressed prior network deployment. These requirements vary from network to network based on the type of application and the required level for security. In general, the common required security services are confidentiality, authentication, integrity and non-repudiation [36]. In the meantime, there are specific obstacles that withstand the adaptation of powerful security techniques and prevent the dependency on standardized security protocols. The main challenge here is the nature of these low power devices in term of computation and communication constrains that complicates the inheritance of any existed solid security technique. Accordingly, there must be a tradeoff between the desired security level and the overhead of achieving such security demands.

2.3.2 Security Design principles

This section presents a brief definition of the related cipher algorithms and key management approaches.

2.3.2.1 Block and Stream Ciphers

The cipher algorithms are classified into two sets, the block cipher techniques by which the cipher algorithm handles a block of data (i.e. 64,128, 256-bit) at a time. On the other side, stream ciphers process either one bit or a byte at a time. The common block cipher algorithms are AES, RC5, Skipjack and DES while the stream ciphers are like RC4, Salsa20 and its variant ChaCha.

2.3.2.2 Symmetric and Asymmetric Cipher Techniques

The cipher algorithms are categorized according the type of key used in encryption and decryption processes. The symmetric algorithms use the same key for encrypting and decrypting (ciphering and deciphering) while the asymmetric techniques use different keys for each process. The asymmetric techniques also called public key cipher algorithms since the key used for encryption is always public while the key used for decryption must be secret and private. Example on the asymmetric techniques are RSA, ElGamal and ECDSA while for the symmetric there are AES, DES and RC5.

2.3.2.3 Ciphering Versus Hashing Techniques

Another sort of algorithms used in the context of security are called the hash functions. These algorithms have the property of being one-way functions by which from the output of these functions there will be no way to obtain the input data. Unlike the hash algorithms, the cipher techniques (as AES, DES, RC4) take the plain text and encrypt it to generate the ciphered text and this resultant output can be fed into a deciphering algorithm to regenerate the original plain text. In addition to the one-way property, the hash functions have a strong collision resistance such that for any pair of blocks X and Y, it will be computationally infeasible to obtain hash(X)=hash(Y) [2]. Examples on hash algorithms are SHA (and its derivatives SHA-1, SHA-2 and SHA-3), MD5 and BLAKE.

2.3.3 Key Management Approaches

One of the important issues that delimit the reliability of the cipher techniques is how to securely distribute the keys between the nodes in the network. The common approach is relying on the asymmetric cipher algorithms which impose no security threats to the key distribution process. The public key system is the simplest scheme by which each node announces its public key that will be used to encrypt any traffic destined to it. In the meantime, each node keeps securely its private key which is used to decipher any incoming traffic.

The issue with symmetric cipher techniques is the need for secure channels to share the keys between the participants. One of the possible methods is based on a public key protocol called Diffie-Hellman key exchange that allows two nodes to set a shared key over an insecure link. This process is based on the assumption that both nodes have to share (publically) a prime number and an integer number that is a primitive root of the first prime number. Fig. 2.4 simplifies the mechanism of setting a shared key between two nodes. It shows the process of generating a shared key between two nodes A and B. The issue with Diffie-Hellman is the high computation overhead required for each key generation process and this escalates as the nodes are mobile and need to perform several association procedures with their correspondent key establishment.

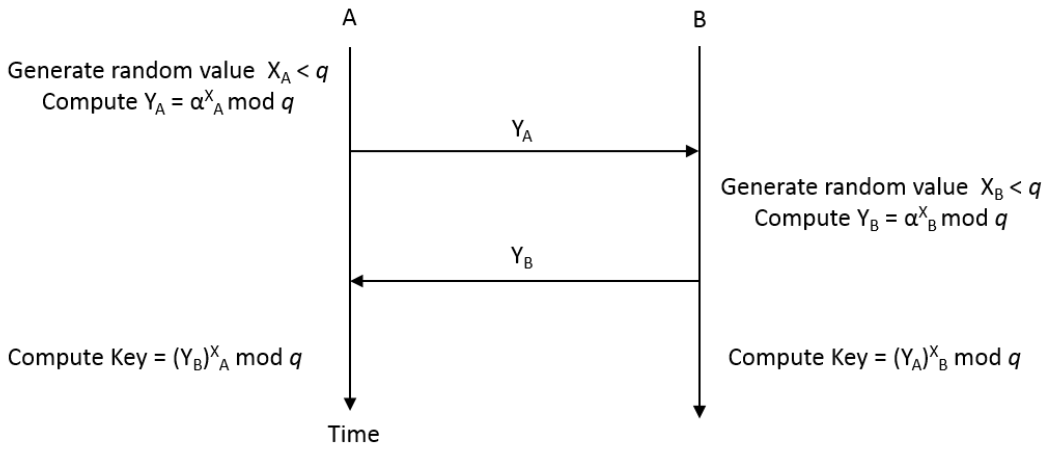


Fig. 2.4: Diffie-Hellman key exchange protocol

2.3.4 Block Cipher Operations Modes

There are multiple modes of operation that easily integrate the cipher algorithms with different kind of applications and used to increase the security of these cipher techniques. The stream of data that needs to be encrypted will not always fit the block size of the cipher algorithm. Hence, the block cipher operation mode technique can handle this incompatibility and manages the blocks of data that are larger than the block size of algorithm. Moreover, these modes of operation are designed to add security to the generated ciphered data and are used to compute the

message authentication code (MAuC). MAuC values are utilized to validate the authenticity of transmitted data. There are several operation modes as ECB, CBC, CFB, OFB and CTR. Fig. 2.5 shows the infrastructure of the two main modes, CBC and CTR. The modes are taking a block of plain text P and partition it into fixed block sizes [P1, P2, …, Pn] that matches the correspondent block cipher input size. The output cipher text is the concatenation of resulted ciphered blocks [C1, C2, …, Cn].

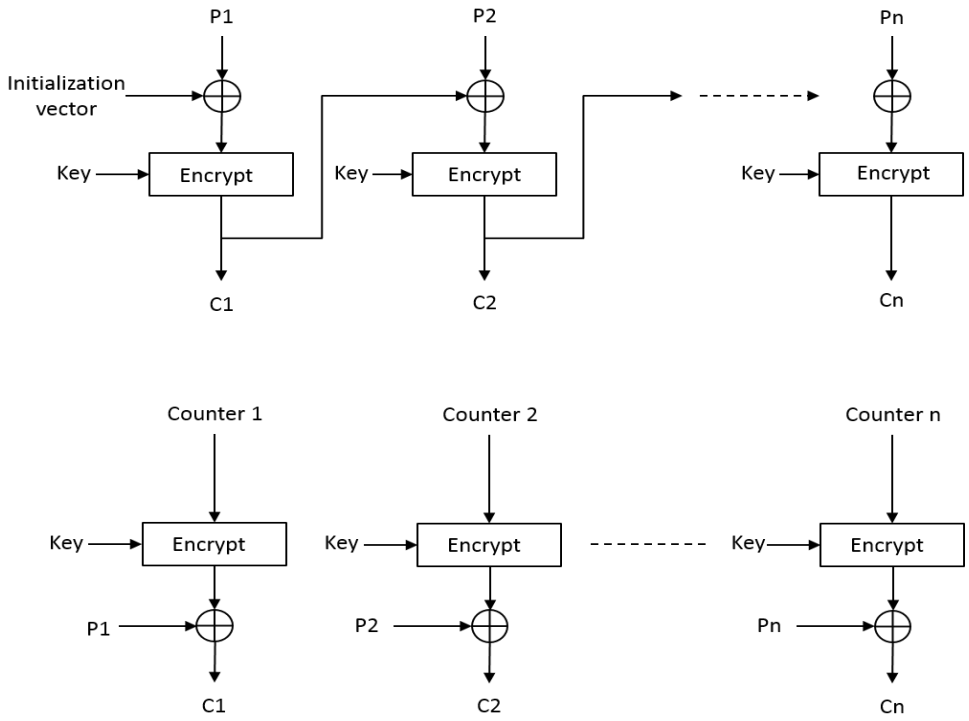


Fig. 2.5: CBC and CTR block cipher operation modes [2]

2.4 Summary

This chapter briefly introduced the basic attributes of node mobility and the differences between synchronous and asynchronous listening techniques. In addition, the types of cipher algorithms and their functionalities have been presented to provide an overview over the basic security components under the IoT context. The next chapter will address recent mobility issues and the impact of node movement regarding both TSCH and LLDN modes.

Chapter 3. Mobility of Low Power IoT Devices: State of The Art and Issues

Realizing the target of high reliability and availability is a crucial concept in the IoT context. Different types of IoT applications introduce several requirements and obstacles. One of the important aspects degrading network performance is the node mobility inside the network. Without a solid and adaptive mechanism, node mobility can disrupt the network performance due to dissociations from the network. Hence, reliable techniques must be incorporated to tackle the overhead of node movement.

This chapter has two folds, the first one examines the current aspects and scenarios of handling node mobility. The second one is concerned with implementing and studying the overhead of node mobility under both IEEE 802.15.4 TSCH and LLDN modes.

3.1 Mobility of Constrained IoT Devices

The current approaches to handle node mobility within the IoT paradigm have been addressed in this section. The recent state of art is categorized based on several layer-based MMP scenarios and mobility patterns. In addition, both detailed classification and visualization scenes have been presented to shape the attributes and limitations of the current MMPs. Security in relation to node mobility is also considered to highlight the overlap of mobility and security within the scope of the IoT. Finally, this section is concluded with the possible future trends that need to be addressed in order to tackle the IoT mobility issue.

3.1.1 Related Work

Several surveys have been conducted to address mobility with each focusing on a dedicated layer and missing the IEEE 802.15.4 MAC approaches. The mobility with respect to the entire communication stack layers has never been introduced. The previous surveys address either some proprietary protocols that are not related to the

IoT context or handle some of the IPv6- based (or 6LoWPAN-based approaches). This chapter considers all the up-to-date approaches with the inclusion of one of the most important elements, which is the link layer-based MMPs (IEEE 802.15.4). Moreover, this chapter addresses some recent approaches with regards to the upcoming industrial technologies and operating systems that provide an influential core infrastructure for the IoT paradigm.

In order to efficiently cover the mobility issue within the IoT, the MMPs designated for each layer must be evaluated to provide a general visualization of the real impact of mobility. Based on [3] and [19], the standardized contributions to manage macro mobility can be visualized and it has been depicted in Fig. 3.1 Although some of these protocols can be utilized to handle node micro mobility, it will incur high overhead if handled through link layer approaches.

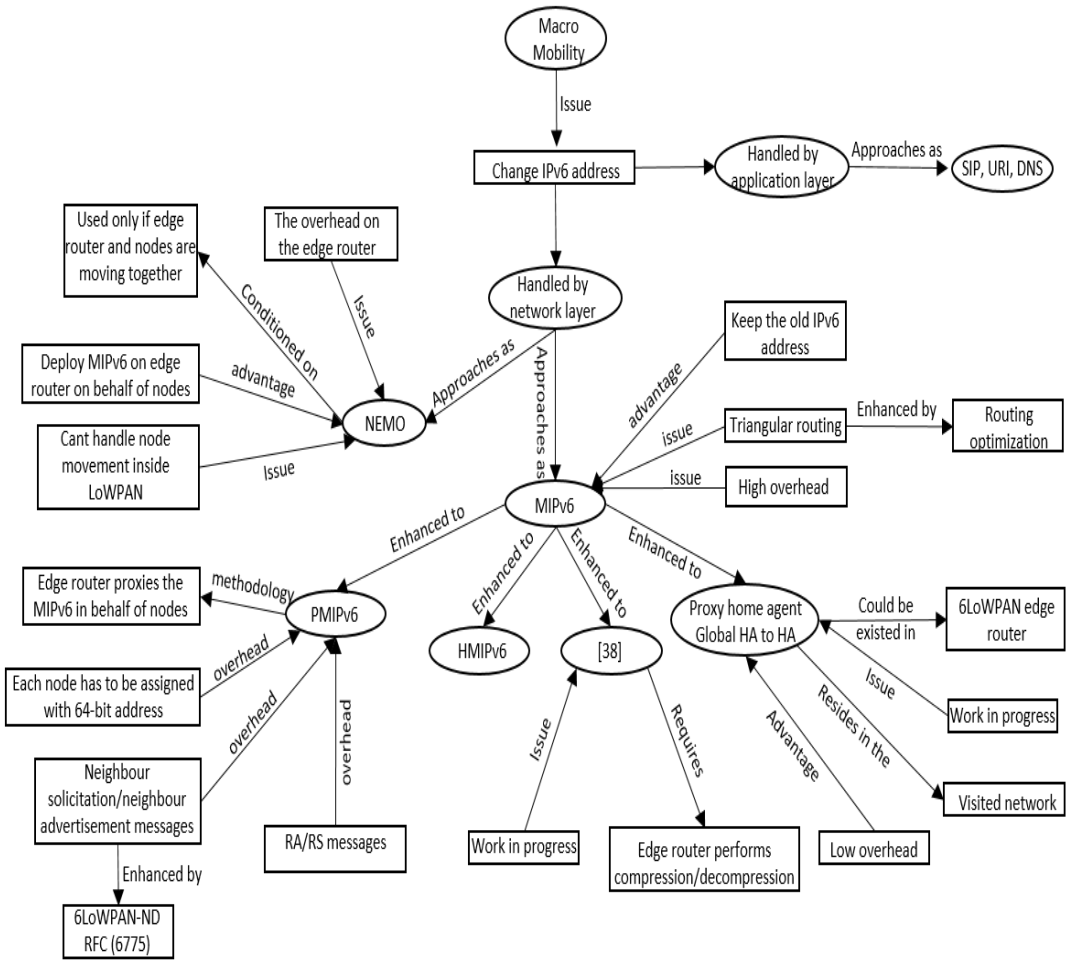


Fig. 3.1: Standardized macro MMPs

3.1.2 Mobility Under IEEE 802.15.4

Mobility can be considered as an issue for the IEEE 802.15.4 since the standard is designed for static LoWPAN networks. Thus, cooperating mobile nodes with IEEE 802.15.14 networks must be studied while identifying the existing drawbacks that complicate the adaptability of this standard to node movement. The association process, which must be carried by each orphan mobile node seeking to join a new coordinator, is a key problem of mobility management [38]. This is also contributed by the CSMA/CA mechanism, since it tends to maximize the required time prior to transmission [39]. Hence, the core problem of IEEE 802.15.4 is the inability of nodes to manage contentions and is affected by CSMA/CA mechanism. So, any new design must either resolve this issue or has to define a new approach to address node contention inside the network.

In order to handle node mobility efficiently through the IEEE 802.15.4 link layer, there are several important elements that all of the proposed approaches are utilizing. Such parameters are:

- Beacon interval (BI): corresponds to the time duration between each two successive broadcasted beacons. Increasing BI period will maximize the mobile waiting time to associate since only through beacons a mobile node can determine the existence of a coordinator.
- *aMaxLostBeacon* value*:* this parameter is set by the network to indicate the maximum number of lost beacons before announcing the node is disconnected and has lost connection with the coordinator.
- Superframe duration (SD) corresponds to the active period duration in a superframe by which the coordinator is active and can accept the association requests through any free time slot in this SD.
- Number of frequency channels: increasing the number of available frequency channels will burden the association process through maximizing the required time to indicate at which channel a given coordinator is broadcasting beacons.

Recent approaches mainly focus on optimizing the response of the standard in order to provide fast mobile node association. This can be obtained by manipulating the

aforementioned parameters that influence association response time, like BI and SD, fixing beacons broadcast to a single frequency channel or by reducing *aMaxLostBeacon* waiting time. This will in turn lead to raise other problems like collision, low packet delivery ratio and latency. So, recent solutions make a trade-off between fast node association, high collision and high latency.

Involving the IEEE 802.15.4 in mobility, opens the gate to the MAC layer mobility problem since it is considered as a network-based issue rather than MAC-based issue. Authors in [40] and [41] present surveys regarding recent MAC protocols which are designed to support nodes mobility. The studies mainly focus on proprietary MAC-aware protocols like MS-MAC [42], MMAC [43], M-TDMA [44], MA-MAC [45], MobiSense [46], MCMAC [47], MHMAC [48], MOBMAC [49] and MLMAC [50].

Similarly, the research community contributes via several approaches to mitigate the mobility issue in IEEE 802.15.4 due to the increased demands for a standardized IoT MAC protocol that can support mobility, especially with the existence of several applications that require mobility as a crucial service in IoT infrastructure. Table 3.1 concludes the current mobility approaches regarding the IEEE 802.15.4 beacon-enabled and beacon-less modes while identifying the possible issues and advantages of each one. It’s clear that two important IEEE 802.15.4 modes (TSCH and LLDN) have not been considered before while they are gaining an increased interests in different upcoming IoT applications. Accordingly, section 3.2 concerns with these two modes and studies the impact of node movement with regards to them.

3.1.3 MMPs for 6LoWPAN-Based Networks

This section addresses recent methodologies that are dedicated for 6LoWPAN-based networks. For the majority of approaches in this topic, 6LoWPAN adaptation layer is acting as a passive element that does not take any role in the process of handling mobility but only performing its allocated task as a linchpin between IPv6 and IEEE 802.15.4 standards. Table 3.2 concludes and classifies the recent 6LoWPAN mobility-based protocols.

Table 3.1: IEEE 802.15.4-based MMPs

Approach	Methodology	Pros	Cons
Zen *et al*. [51]	- Based on link quality indicator (LQI) to estimate the dissociation and predicting any lost LQI value	- Minimizing the inaccessibility time by interrupting *amaxLostBeacon* waiting time value to initiate association quickly. - Predicting LQI value of lost beacon	- False predicted LQI value that will lead to initiate association even the node still connected. - Beacon interval (BI) still has the impact on dissociation time
Chaabane *et al*. [52]	- Hierarchical infrastructure which is a centralized approach to handle mobility with LQI indicator. - The coordinators decide the next point of attachment and based on super coordinator	- Network-based approach by which the network decides the next attachment which minimizer he overhead on the MN. - Minimizing the dissociation time caused by the proactivity feature the tis based on the LQI	- Centralized process that is based on what is called the super coordinator (SC) to manage mobility. - The SC can be considered as single of point of failure. - Excessive communication overhead.
Bashir *et al*. [53]	- Reduced BI interval to expedite the association - Coordinators are exchanging mobility-related information to manage MN movement between two coordinators.	- Low association time by minimizing the beacon interval - Proactive, based on LQI indicator	- Excessive coordinator-to-coordinator communication overhead - Requires every two adjacent coordinators to be within the coverage of each other which increases the interference and the probability of collision
Sthapit *et al*. [54]	- Broadcasting beacons on affixed frequency channel	- Minimizing the scanning time sic the MN will scan only single frequency channel	- BI interval issue is still existed. - *amaxLostBeacon* waiting time issue is still existed.
Yu *et al. [55]*	- Weighted LQI scheme to initiate a new re-association process. - increasing the threshold value of initiating a re-association	- Mitigating the ping-pong issue caused by low threshold value - Predicting the LQI value of a lost beacon	- BI is still an issue - Faulty re-association caused by LQI value - Maximizing the association time since the threshold of re-association has been increased
Li *et al*. [56]	- Providing what is called access routers (AR) to handle mobility - Presenting an addressing scheme to assist mobility management - Introducing a table that will trace a MN route	- Keeping a route to a MN when moving between ARs	- Increasing the communication overhead that are between ARs to manage mobility - Gateways, if utilized as points to connect AR, will be considered as single point of failure. - Else, the ARs overlapped coverage will increase interference and collision probability

Table 3.2: 6LoWPAN-based MMPs

Approach	Mobili-ty type	Addressing technique	Initiation process	Handling process	Device mobility	layer	approach	Security feature	Base protocol
Kim *et al*. [57]	macro/ micro	devised (called GDID)	proactive	network-based	group mobility	network	ID/LOC separation technique	CGA to provide authentication	IPv6
Wang *et al*. [58]	micro	devised (based on prefix and location info.)	proactive	network-based	node mobility	MAC and network	location-based IPv6 address structure	none	IPv6 and 6LoWPAN
Teo *et al*. [59]	micro		reactive	network-based	node mobility	network		none	PMIPv6
Shahamabadi *et al*. [60]	macro	N/A	reactive	network-based	group-based	network	reduction of control messages	none	NEMO
Koster *et al*. [61]	micro/m acro	two routing tables, one for MIPv6 and one for MANET	reactive	node-based	node mobility	network	combine MIPv6 and MANET (OLSR)	based on IEEE 802.15.4 security metrics (AES)	MIPv6 and MANET (OLSR)
Kim *et al*. [62]	macro	default addressing (IPv6 and 6LoWPAN)	reactive	network-based	node mobility	network	PAN attachment detection and utilize RA/RS messages	none	PMIPv6
Bag *et al*. [63]	micro/m acro	16-bit address for MNs and static 6LoWPAN nodes	proactive	network-based	node mobility	6LoWP AN and network	deploying static 6LoWPAN nodes to relay messages and track MN	none / but add later the LEAP as secure key management in updated work	partially PMIPv6 and HMIPv6
Rong *et al*. [64]	macro	default NEMO	reactive	network-based	group mobility	network	cluster network and the coordinator performs NEMP	none	NEMO

Approach	Mobili-ty type	Addressing technique	Initiation process	Handling process	Device mobility	layer	approach	Security feature	Base protocol
Jara *et al*. [65]	macro	IPv6 addressing	reactive	network-based	node and group mobility	network	using fixed IPv6 addressing and reduce mobility-related signalling message	security based on a challenge scheme	partially on MIPv6
Ha *et al*. [66]	macro	default MIPv6 addressing	proactive	network-based	node mobility	network	dedicated static node that track MNs and send related info. To visited PAN	none	MIPv6
Zininos *et al*. [67]	macro and micro	IPv6 network prefix and link layer addressing	proactive	network-based	node-mobility	network	dedicated static node that track MNs	using secured keyed association (no info. on how to generate the keys)	MIPv6
Montavont *et al*. [68]	macro/ micro	default MIPv6	proactive	host-based	node mobility	network	overhearing neighbour transmission to detect whether it has moved	none	MIPv6 and ND (RFC 6775)
Fotouhi *et al*. [69]	micro	not considered	proactive	host-based	node mobility	network	modifying trickle timer and assess link quality	none	RPL
Jara *et al*. [70]	macro	fixed IPv6 addressing and short addressing for inside a PAN	reactive	host-based	node mobility	network	simplified MIPv6 through eliding addressing stages	challenge scheme and cryptographic SIM card	MIPv6

3.1.4 IoT Purpose-Based MMP

In this section, different types of MMPs will be addressed that are nominated for specific sorts of platforms or services and can be considered as good candidates in the IoT context. These MMPs are not suited in the default communication IoT stack layer but are presented to tackle the mobility issue for proprietary platforms, OSs, RPL-based approaches, industrial technologies and SDN-based protocol. For each technique, the related approach has been identified and discussed

3.1.4.1 Multiple Gateway

A new mobility approach is presented in [71] which proposes a soft handover scheme (SH-WSN6) for 6LoWPAN-based WSN. This scheme reduces both the connection loss factor and the number of unnecessary handovers associated with multiple gateways (gateways can be mobile). This work is based on a network architecture designed in SENSEI project. According to SH-WSN6, instead of deleting a connection with a recent gateway (GW) upon receiving router advertisements (RA) messages from different one, the sensor node adds the new GW to its list. Following this technique, the sensor node will have a new route-to-resource directory (RD) in a SENSEI network which in turn enhances connectivity by realizing route diversity. The sensor node can delete any of registered GWs in the case of unreliable link problems occurring with a given GW. The conducted analysis shows that the SH-WSN6 has lower handover latency as compared with PMIPv6 [72] and MIH-PMIPv6 [73].

3.1.4.2 RPL-Based Protocol

Instead of handling mobility from inside the link layer, another approach has devised the possibility of handling node movement through the network layer and specifically the RPL protocol. mRPL in [69] has been introduced which supports a smart-hop handoff mechanism and provides fast mobility service for the RPL protocol [74]. The proposed work considers health monitoring applications and provides an efficient handoff mechanism in RPL while avoiding collision during the handoff period. The smart-hop mechanism consists of two phases, the discovery

phase and data transmission phase. During the data transmission phase, MN checks the quality of the link with its access point (AP) based on the reply packets from the AP. For each *n* packets, the average RSSI (ARSSI) value is computed and once ARSSI starts degrading, MN initiates the discovery stage. Four additional timers in RPL are included to support and control the monitoring process of link quality. In addition, in the case of existing multiple APs, the MN can prioritize the selection process based on ARSSI that can be gained through forcing MN to broadcast DIS message and each AP replies with its ARSSI.

3.1.4.3 IoT Middleware MMP Approach

Moving away from standardized techniques, a new methodology is based on a proprietary middleware element of the IoT. An IoT middleware is presented in [75] which operates on user handled devices and dedicated for post-emergency networks. The proposed approach is based on analyzing user's context data that can be collected from surrounding devices as RFID tags and mobile devices. Acquiring context-related information helps to determine the best evacuation route that optimizes both traffic congestion and delay. The IoT middleware monitors two contexts, static object locations and user's physical context in order to decide the evacuation route without user's supervision. Two objectives have been considered for optimization, minimizing the evacuation delay and maximizing the number of access points to ensure high service coverage. Based on this model, with a conflicting nature, the Pareto principle has been utilized to determine the Pareto optimal point.

3.1.4.4 Software Defined Network SDN-Based MMP

Recently, there is a focus towards the concept of SDN-based network and their advantages to tackle existed issues as security, scheduling and mobility. In [76], a software defined IoT MMP called (UbiFlow) is presented that can effectively manages node mobility in an urban multi network. UbiFlow divides an urban network into different geographical partitions that are controlled by multiple controllers. Mobility management tasks as access point (AP) selection, handover

optimization and flow scheduling are performed by controller coordinators. To maintain network stability and consistency, an overlay structure that is based on distributed hashing is proposed. The UbiFlow categorizes the SDN controllers into two types, associated (the controller that an MN is currently connected to) and a supervisory controller (the first one an MN associated to it and maintains a record of MN's mobility-related information). Each controller has what is called a finger table which is considered while forwarding any mobility-related information (via the closest controller) to a supervisory controller and based on a hashing address. Based on the proposed scheme, a newly associated controller can identify the supervisory controller of an MN and forwards lookup information via the overlay structure and through the closest controller to the destination. Accordingly, the associated controller can fetch the previous session between MN and its previous controller to reroute traffic to its current partition.

3.1.4.5 OS-Based MMP

The emergence of IoT has been incorporated with the development of multiple operating systems (OSs) that are dedicated for constrained devices. OSs such as Contiki OS [11], TinyOS [12] and RIOT [77] can be considered as preferable OSs for IoT applications. A comprehensive survey in [78] provides a review on the current operating systems that are devoted to IoT. Contribution in [79] enhances Contiki collection protocol [80] by supporting it with a light mechanism to manage mobility. The proposed modifications allow MN to quickly allocate new parents after dissociation. In addition, the scheme overcomes the loop problem while combining the receiver initiated MAC layer with routing beacons. The proposed approach, which is called mobility collect, is shown to have less energy consumption and high reliability as compared with the default Contiki MAC in a full mobility scenario (both sink and source nodes are mobile) .

3.1.4.6 Industrial MMP

There are several industrial technologies that can contribute to the IoT paradigm like WirelessHART, ZigBee and ISA100.11a. These technologies can provide efficient

platforms for low power devices and maintain the required reliability and availability for IoT applications. [81] has evaluated the impact of node mobility on Wireless HART technology [82]. The analysis has considered several network topologies and the impact of multihop communications and shows that default Wireless HART can't efficiently handle node mobility. Accordingly, listen, advertise, network neighbor discovery (LAN-ND) scheme proposed in [83] that reduces the required time needed by an MN to detect neighbor devices. Instead of listening to transmitted data link protocol data units (DLPDU) on a discovery link (required to associate with a network), the nodes can also listen on the advertised link to facilitate and expedite association. The existed nodes are preconfigured by network manager (NM) to transmit information regarding when and how MNs can access the network and finalize association.

Moving to the ZigBee infrastructure, authors in [84] address the impact of mobility on ZigBee networks for both ZigBee devices and ZigBee routers. Under different mobility scenarios, the end devices suffer from high data loss rate in several mobility models while ZigBee routers shown to have less data loss. According to the authors, this performance is traced back to the routing capability of router nodes that end devices could not maintain. Dhaka *et al*. [85] have evaluated the impact of sink mobility on ZigBee networks. The analysis shows that for different types of sinks movement trajectories, the performance of static sink is better. This is caused by the time overhead required by nodes to establish a new route after each sink movement. Moreover, [86] addresses the mobility issue in ZigBee networks and proposed an enhancement to maximize delivery ratio in real-world scenarios. The proposed approach is based on managing a router deployment strategy that can be constructed in a tree topology and matches with the highest probabilities of the MNs movement trajectories. Hence, this technique maximizes the settle time of MNs in the router coverage areas and minimizes number of dissociations to increase PDR. The approach provides a low-complexity heuristic algorithm that positions the routers along the possible MN movement's routes. Based on MN's historical movement information, the possible router positions can be determined and the reliability can be increased as long as MNs move with regularity. Finally, authors in [87] address the mobility regarding ZigBee-based health inpatient monitoring applications. The authors present a mobility manger (ZiM2) which handles node mobility. The

proposed ZiM2 provides handoff management, location management and paging service. ZiM2 design concept is based on two parts, ZiM2 mobile (provides mobility management) and ZiM2 frontier (provides location database to support both paging and location management).

3.1.5 Application Layer-Based MMP

One of the approaches to handle node mobility is through the application layer by which MMP ensures a continuous session with the server or any destined application provider. There are several contributions in this field but majority can't be considered appropriate for low power devices due to excessive signaling overhead. SAMP [88] is presented as an application MMP which shows low session setup latency and is more scalable as compared to MIPv6, but it doesn't consider the energy overhead. Chun *et al*. [89] present CoMP MMP that is based on CoAP protocol [16]. The authors address several limitations of the default CoAP protocol in case of mobility. CoMP follows the concept of sustained tracking of IPv6 address for a node that changes network domains instead of a tunneling technique as in MIPv6. The network architecture is composed of three basic components, web of things mobility management system (WMMS) which contains a mobility management table (MMT), CoAP client and CoAP server node. The MMT keeps track of MN CoAP location to ensure that WMMS is always updated with MN's location information. CoAP has two basic layers, request/response layer and message layer. The message layer controls message communication between two end points over UDP. In addition, at the request/response layer, the CoAP utilizes PUT, POST, GET, DELETE messages to support mobility management process. The CoMP keeps track of the IPv6 address through defining permanent address P-Addr and temporary T-Addr fields in MMT. The T-Addr changes with each access point change. Moreover, the CoAP node also maintains a similar table called local binding cache (LBC) that also holds P-Addr and T-Addr. Through analytical and simulation analysis, CoMP shows lower packet loss as compared with MIPv6 and HMIPv6 beside lower handover latency as compared with MIPv6.

3.1.6 Secured-Based MMPs

The security issue within the IoT is closely related to node mobility due to the high number of link and network changes accompanied with each node movement. Hence, it will be preferable to consider the security challenge with regards to MMP design phase. Hopefully, this will reduce the overhead of deploying a standalone security protocol that might be incompatible with the node mobility pattern. There are several security requirements for IoT applications and authors in [36] present a list of the possible challenges and approaches for security within IoT context. One of the approaches in this topic is presented by [90] which demonstrates the infeasibility of both MIPv6 and IPsec protocols deployment on constrained devices. Accordingly, authors present light versions of both MIPv6 and IPsec protocols and show that realizing an integrated MIPv6 and IPsec is still achievable in low power devices. The presented approach is a node-based technique and proposes modifications to both binding update (BU) and binding acknowledgement (BA) messages in order to minimize overhead of the default MIPv6. Regarding the security aspect, authors addressed the incompatibility of IPsec ESP with MIPv6 regarding route optimization due to the lack of security association (SA) establishment with all correspondent nodes (CNs). In the meantime, the proposed scheme preserves protection for traffic due to dependency on the route optimization scheme as in default MIPv6. Authors suggested to utilize the AES-CCM mode with IPsec instead of AES-CBC in order to minimize the overhead of security. In this thesis, chapter 7, a new modified scheme is presented that will show even AES-CCM has a high energy consumption. In [91], the security threats and the possible vulnerabilities associated with ID/LOC mobility management scheme have been analyzed (this technique can be seen in [70] and [57]). This work indicates the possible security drawbacks concerning such technique as theft of device ID, spoofing location update and denial of service (that could be either basic denial of service (DoS) (diverting traffic to a random node) or flooding (directing traffic to a victim node)). Moreover, the authors indicate that route routability RR (in MIPv6) can be considered as a part of solution since the communications between HA and MN are authenticated through tunneling but it only provides authenticity for MN and not CN. Accordingly, authors have proposed the deployment of ECC Diffie-Hellman key exchange protocol between CN and HA in order to provide

authenticity and overcome the aforementioned vulnerabilities. Finally, the presented scheme provides three generated keys that are dedicated for MN to Home gateway (GW), Home GW to Foreign GW and MN to Foreign GW. Finally, the CoAP protocol also involved in this area via [92] which presents an external authorization service called (IoT-OAS) under the IoT paradigm which is based on OAuth protocol [93]. The objective of IoT-OAS is to minimize overhead on constrained smart objects caused by processing incoming requests while mitigating the burden of authorization-related information. Additionally, service providers that run HTTP or CoAP will be efficiently integrated with the authorization layer regardless the burden of any implementation. Accordingly, HTTP or CoAP providers can disseminate their services without the overhead of implementing OAuth logic. The proposed IoT-OAS shows less memory footprint overhead as compared with OAuth protocol. In addition, the presented external authorization mechanism shows better dynamicity to remotely configure access control policies without requiring direct intervention to devices that are already deployed. Although the proposed protocol did not consider the mobility, but it can provide an efficient secure architecture for mobile constrained devices.

3.1.7 Research Questions and Suggestions

Mobility has become an essential factor that needs to be managed efficiently through dedicated protocols in the IoT stack or merged into one of the existing elements (CoAP, IPv6, 6LoWPAN or IEEE 802.15.4). The issue here is which layer will passively handle node mobility. In this section, the factors that influence mobility and affect the association and dissociation process have been summarized. Fig. 3.2 illustrates the parameters that influence and increase the complexity of mobility and the factors which mobility, in turn, influences. Based on the observed contributions in the field of mobility and the addressed challenges with their possible approaches in the literature, the possible obstacles which complicate the process of managing mobility in the IoT paradigm can be concluded.

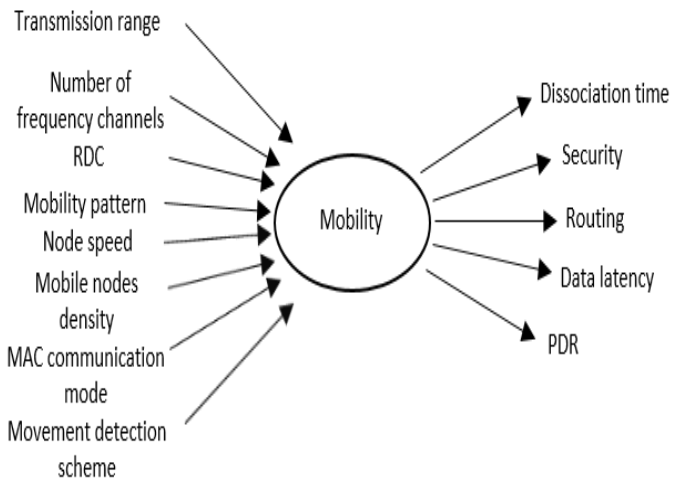


Fig. 3.2: Possible elements that have an impact on or impacted by mobility

A. *IoT MAC layer*: The IEEE 802.15.4 standard and its amendments can be considered as the de facto MAC layer within the IoT infrastructure. Thus, this standard must have the capability to efficiently handle node mobility (micro mobility). Unfortunately, until now there is no defined standardized scheme to tackle mobility from inside the IEEE 802.15.4 while the current association mechanisms (default association and FastA) are seen to show low response time to node dissociation and have a maximized association latency. In addition, for the provided three modes of operations in amendment [1], TSCH, LLDN and DSME, there is a real problem with the existence of node mobility and especially with the case of TSCH and LLDN as described in [94, 95] respectively. In turn, regarding the IoT MAC layer, IEEE 802.15.4, there must be a standardized tool within this standard that can provide: (i) fast coordinator discovery mechanism to ensure low scanning time and to allocate the required coordinator and associate, (ii) fast and reliable handover service for nodes moving inside a single LoWPAN (consisting of multiple coordinators), (iii) fast link association for nodes that have migrated from a different LoWPAN and hand it to the network layer to finalize the association address (i.e. assign IPv6 address and enforce any required security measures).

B. *6LoWPAN Adaptation Layer*: Although there are several approaches that are considered for 6LoWPAN networks, these are not implemented in the 6LoWPAN layer except in [63] which integrates the 6LoWPAN layer in the mobility handling process. This can be traced back to the actual functionality of 6LoWPAN which composes compression/ decompression and fragmentation/defragmentation only. Therefore, it can be incorporated only in the case where the mesh header structure is changed through this layer. Accordingly, majority of contributions that are designed for 6LoWPAN-based networks are not modifying the 6LoWPAN infrastructure for the sake of handling mobility

C. *Network layer*: The network layer in the IoT structure is presented by the IPv6 protocol and the possible MMPs that are dedicated for this protocol. It's clear in previous sections that there are significant contributions aimed to minimize the overhead of the two important protocols MIPv6 and NEMO. But all the proposed models lack the ability to handle the micro mobility or even if they can, then they incur a huge overhead caused by the default mechanisms that are based on either MIPv6 or NEMO. Thus, here must be an inclusive protocol that can operate in two modes of operation (simple link handover in the 2^{nd} layer or both link and network handover in the 2^{nd} and 3^{rd} layers) to efficiently support both micro and macro mobility respectively. Hence, the amount of overhead is reduced since the MMP here is calling only the required functionality based on the type of mobility.

D. *Application layer*: inside the IoT paradigm and till now, CoAP can be considered as the de facto application protocol. An MMP inside this layer must ensure a continuous application session or at least having low disruption time. This is a crucial concept especially in applications that impose real time services and presume the existence of an uninterrupted session with the destined application. Examining the outcome of an analysis conducted in [96] led us to conclude that there is a good potential of

achieving better utilization of handoff application layer protocols (e.g. SIP [97]) to handle mobility. Thus, this area needs to be addressed since there is interest in designing MMPs that can utilize an application-based handoff protocol or any other application layer based protocols for the IoT such as CoAP.

3.2 Mobility Impact on the IoT MAC Infrastructure

In this section, the overhead of mobility on both IEEE 802.15.4e timeslotted channel hopping (TSCH) and low latency deterministic (LLDN) modes is investigated. These two modes can be considered as the MAC layer of the IoT paradigm because of their importance and resilience to different network obstacles. In addition, the set of metrics and limitations that influence the network survivability will be identified to ensure efficient mobile node handling process. Both TSCH and LLDN have been implemented via the Contiki OS to determine their functionality.

3.2.1 LLDN and TSCH Description

The IEEE 802.15.4e standard has introduced several techniques and enhancements in this amendment as the coordinated sampled listening technique (CSL), deterministic and synchronous multi-channel extension (DSME), LLDN and TSCH modes. This section will focus on both LLDN and TSCH modes for their importance and crucial services that can influence positively the rise of the IoT concept.

3.2.1.1 IEEE 802.15.4e TSCH Mode

This mode has gained a lot of interest in the research community due its robustness that achieved through a hybrid technique which based on both time and frequency channel diversity. Due to its importance and robustness, the IETF has formed a dedicated group (6TiSCH) [98] to integrate the IPv6 and the TSCH mode. The default routing protocol has been set to the RPL routing protocol.

The coordinator in the TSCH network assigns a dedicated timeslot for each node and when each timeslot elapses the frequency channel will be changed. The mechanism by which the nodes and the coordinator determine the recent frequency channel for the current timeslot is based on the channel offset and the number of frequency channels and the number of timeslot. Each timeslot has a unique number called the absolute slot number (ASN). Hence, the nodes can indicate the frequency channel of the current timeslot via:

$$PH_{channel} = Frequency_{List}\,[\mathrm{ASN} + CH_{Offset}\ \%\ N_{ch}]$$

Where $PH_{channel}$ is the physical channel, $Frequency_{List}$ is the list of the available frequency channels, CH_{Offset} is the channel offset and N_{ch} is the number of channels in $Frequency_{List}$.

Accordingly, the coordinator assigns each node a link, which is a combination of time and frequency to facilitate transmitting readings without any collision. In the meantime, the coordinators periodically broadcast the enhanced beacons (EB) to indicate the existence of a coordinator and to determine the ASN value. This will inform the nodes that seek to join the network on the current sequence of channels for the upcoming timeslots. The TSCH network has defined what is called a slotframe (as depicted in Fig. 3.3) that contains a number of timeslots, corresponds to the number of nodes, and this slotframe will be repeated (but with different ASN and channels) in each time based on the period of transmission.

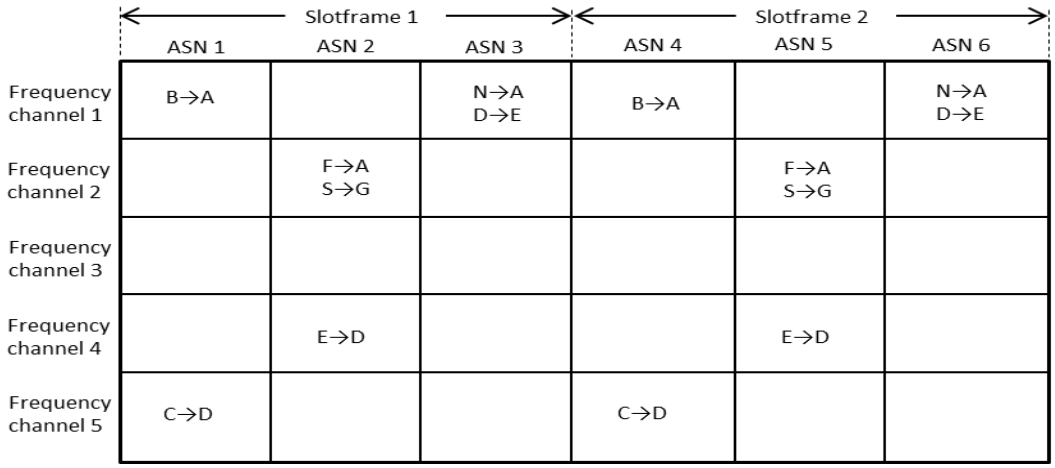


Fig. 3.3: TSCH slotframe architecture

The timeslots in the slotframe structure is categorized into three types; TX (which is allocated for a specific node to transmit reading), RX (for sending information from the coordinator to the nodes and SHARED TX (that is the nodes are contending on to send requests or readings). The type of each timeslot will be defined through EB.

The mobile node that announces it status as 'orphan' will initiate the association process by scanning the available number of frequency channels in $Frequency_{List}$ for a valid EB. Once it detects an EB, it sends an association request to request a link with the coordinator. Although the standard has identified the association process in the TSCH mode as optional, this will introduce several issues since the standard assumes that an orphan node can be synchronized with a network through only listening to the EBs and hence, deduce the structure of the slotframe. However, the coordinator has also to be identified about the new node wishing to join the network and to allocate a dedicate TX slot or increase the number of SHARED TX. Thus, the TSCH can preserve its targeted functionality by providing reliable and collision-free communication. In the meantime, the mechanism of the association process can be carried out either through the default association process defined in [4] or through the fast association technique FastA (expressed in Fig. 3.4) which is described in [1].

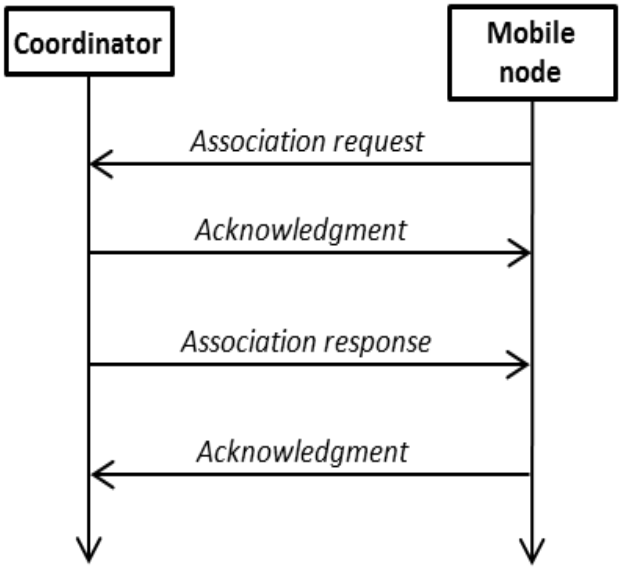


Fig. 3.4: FastA association scheme [1]

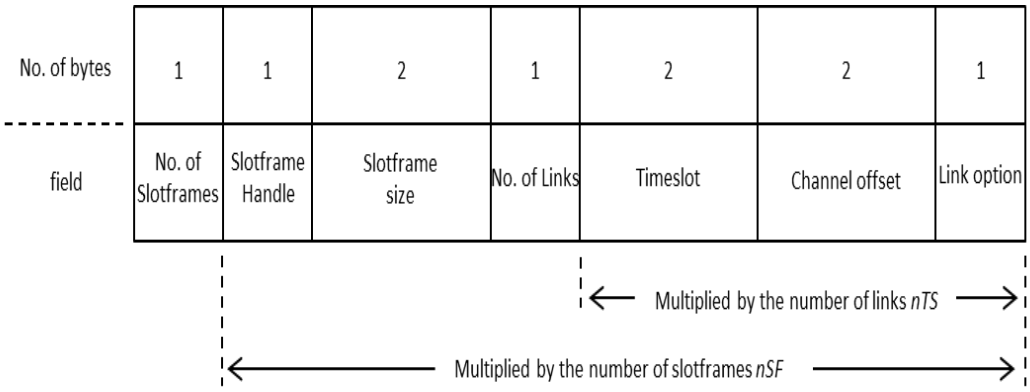


Fig. 3.5: Information element (IE) structure

The IEEE 802.15.4e defines the information element (IE) that will be included in the EB which includes the required information for a node seeking to join the network. The IE can define the number of slotframes and the number of links per slotframe in addition to the channel offset as in Fig. 3.5 and is preceded by five bytes ASN value and a one byte join priority field. Moreover, the above fields are followed by a *macTimeslotTemplate* which describes the format of a single timeslot and is up to 25bytes. This can be omitted to ensure not exceeding the *aMaxPHYPacketSize*, but must be presented in the network initialization and for each reply to an association request. Finally, the IE defines the hoping sequence information that also can be omitted to prevent exceeding the *aMaxPHYPacketSize.* The value *nSF* corresponds to the number of slotframes while *nTS* is the number of timeslots in each slotframe. Hence the FFD can advertise EB in every *ebP* time (since the next slotframes are defined in IE). *ebP* can be expressed as in (1) where *T* corresponds to the timeslot duration (approximated to 10µs [99]):

$$ebP = \sum_{i=1}^{nSF} \sum_{j=1}^{nTS} T_{ij} \tag{3.1}$$

Hence, in order to reduce the waiting time for a mobile node wishing to join a network, the number of defined slotframes (*nSF*) must be reduced, since reducing *nTS* can negatively affect the association. Decreasing *nTS* leads to reduce the number of available shared slots that are required to accommodate the mobile nodes and permit communication with a FFD.

3.2.1.2 IEEE 802.15.4e LLDN Mode

Several applications in the industry require deterministic systems to ensure low delay data aggregation services. Based on this, the IEEE 802.15.4e has presented the LLDN mode that according to the standard, within less than 10ms the coordinator must be able to collect data from 20 devices.

The LLDN mode is considered as a preferable solution among the industrial applications due to its low latency (LL) advantage. LLDN achieved LL utility through employing two strategies; (i) assigning what is called the slot owner timeslot that is dedicated for each node inside the personal operating space (POS) of a coordinator, (ii) reducing the data frame MAC header to a single byte for data frames (excluding two frame check sequence (FCS) bytes). This is achieved by omitting the address fields and relying on the timeslot (*TS*) index inside the superframe to determine the sender node identity. Hence, this eliminates CSMA-CA delay (caused by the contention process during each *TS*) and reduces transmitting/receiving time delay.

The LLDN mode has three distinct transmission states and each has predefined superframe structure and purpose. The first transmission state is the 'discovery state' which is initiated either during the network setup or to handle new node associations to the network. The second phase is the 'configuration state', by which the nodes that managed to communicate with the coordinator during the discovery state shall receive network configurations during this state. The last state is the 'online state', where the nodes can transmit their readings to the coordinator within allocated timeslots assigned during the configuration state. The coordinator specifies the state of transmission through the periodically transmitted beacons. Each one of the discovery, configuration and online states has a defined number of superframes during its period that will be defined by the network administrator; nS_D, nS_C and nS_O respectively as in Fig. 3.6.

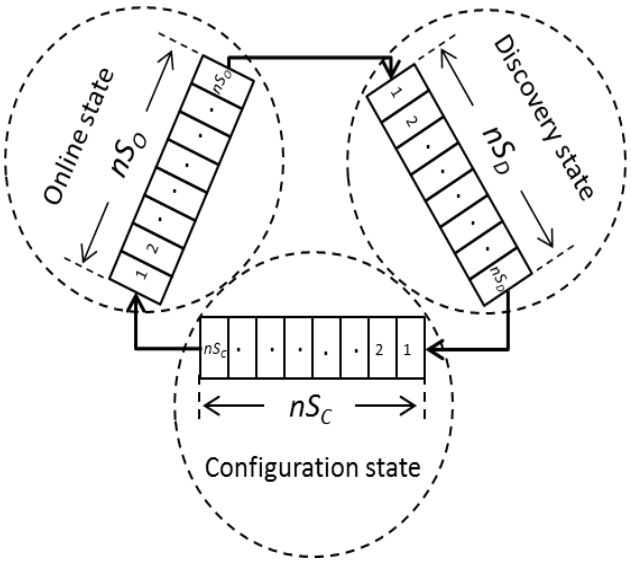


Fig. 3.6: LLDN transmission states

The discovery and configuration states share the same superframe structure but with different network purposes. The discovery and configuration superframes contain only one beacon slot and two management *TS*s (uplink and downlink). Although the online superframe has beacon, management, uplink and bidirectional slots, the default setting has omitted both management and bidirectional slots (as *macLLDNmgmTS* is set to FALSE and *macLLDNnumBidirectionalTS* is set to zero). Beacons are broadcast periodically and used to synchronize the nodes, identify the present transmission state and contain an acknowledgment bitmap of the received readings in the previous superframe. The uplink management *TS* is utilized by dissociated nodes during discovery and configuration transmission states to transmit discovery response frames and configuration status frames respectively. During the downlink management slot, the coordinator responds to nodes' requests by either replying with ACK messages (within discovery state) or a configuration request frame (within configuration state).

Uplink timeslots are unidirectional (from nodes to coordinator) and the default number of *TS*s in the uplink is set to 20 (based on the *macLLDNnumUplinkTS* value) and its maximum value is 255. Transmission failure can be refreshed by permitting the nodes to retransmit within the next superframe and is defined by the *macLLDNnumRetransmitTS* value, which specifies the number of retransmission timeslots within an uplink section. The bidirectional section has

macLLDNnumBidirectionalTS timeslots and the direction of transmission is indicated within the beacon fields. Fig. 3.7 indicates the basic layout of a general LLDN superframe structure.

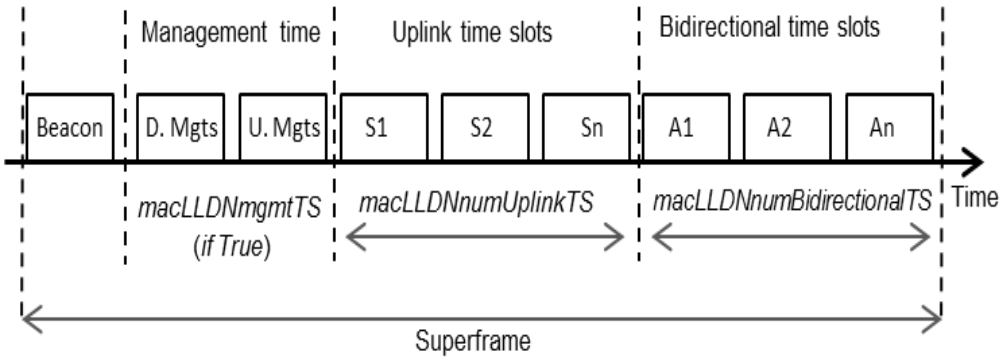


Fig. 3.7: Superframe structure in LLDN mode [1]

Nodes seeking to join the network must follow a sequence of association steps determined by the transmission state of the upcoming superframes. Each node wishing to associate with the network must scan for beacons to determine both the existence of a coordinator and the transmission state of the current superframe. Once it has received a valid beacon that indicates a discovery state, the node sends a discovery response frame to indicate its willingness to join the intended coordinator.

A node can transmit its request only during the uplink management slot (its time is defined through the beacon). The management *TS*s are treated as shared group *TS*s and the nodes commence transmission based on a simplified CSMA-CA. If the coordinator receives the request correctly, it will reply with an ACK message during the downlink *TS* of the next superframe. Each coordinator waits for *macLLDNdiscoveryModeTimeout* seconds until changing to the configuration state if no discovery response frames are received. The association process will transfer to the second phase if the coordinator indicates the configuration transmission state through an announced beacon. Once a node indicates this state, it sends a configuration status frame (during the uplink management *TS*) to request network configuration parameters. The correspondent coordinator will reply with a configuration request frame that contains the assigned timeslot, its duration, transmission channel and any related information based on the network settings. Finally, a node receiving the configuration request frame replies with an ACK

message to confirm successful configuration. Fig. 3.8 depicts the mechanism of association in the LLDN mode based on the predefined three transmission states.

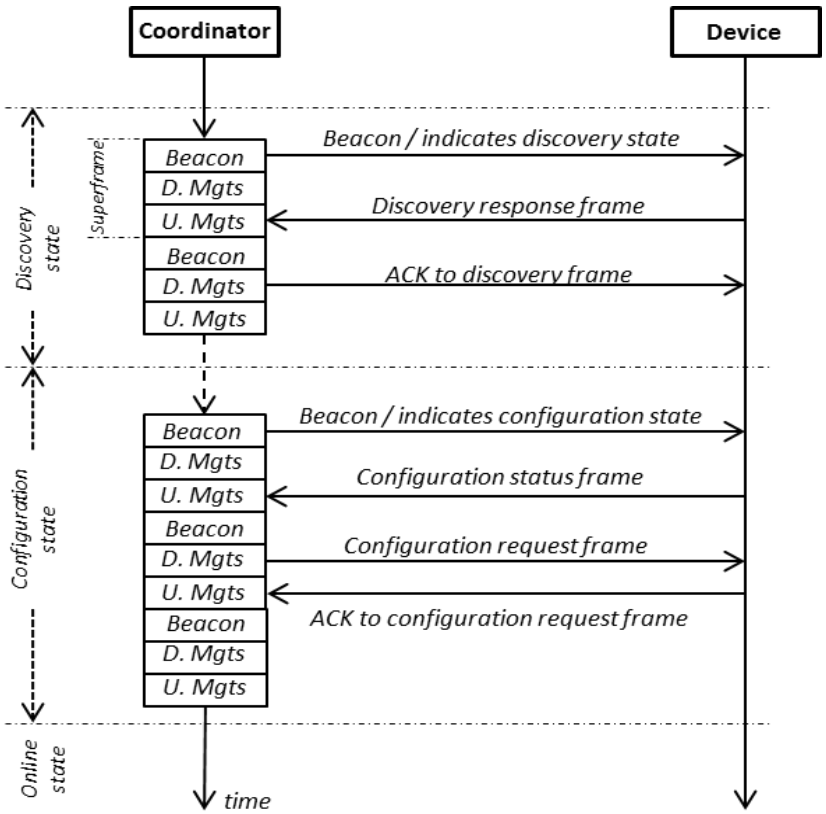


Fig. 3.8: Association procedure in LLDN mode

3.2.2 Mobility-Related Issues of Both TSCH and LLDN Modes

This section addresses the possible challenges that affect the network performance with regards to nodes movement. In addition, it will set the possible approaches that mitigate the overhead of node mobility in order to realize better network connectivity and functionality. Table 3.3 simplifies the potential issues that are caused by node mobility and degrade network availability. Later, the possible issues related to each mode will be individually addressed and tackled in chapters five and six.

Table 3.3: Challenges and approaches for TSCH and LLDN modes

TSCH			LLDN		
Issue	**Impact**	**Approach**	**Issue**	**Impact**	**Approach**
Multiple frequency channels	Increase the scanning time	Fixing beaconing transmission to a single channel	The mobile nodes are limited to associate only during the discovery state	The mobile nodes will be disconnected during the whole online state period	Facilitate the association process by forcing the coordinator to accepts association requests during the online state
Undefined beaconing mechanism	Mobile nodes can't detect the existence of coordinator	Provide beaconing strategy as in LLDN or beacon enabled mode	The LLDN has no defined approach to change between the states	The nodes will stay in a single defined state	Setting the duration of each state based on the mobility metric of the nodes
Undefined timeslots management scheme	Mobile nodes added/deleted will change the number of timeslot; means changing ASN value and desynchronization	Systematic approach that inform the nodes about any changes in the slotframe structure to keep ASN value consistent	The nodes are obligated to transmit only during the online state	During the discovery and configuration states, the node can't send readings which will increase the latency of data	Omit the discovery and configuration states while modifying the online state to accept association requests and configure nodes
Undefined mechanism that defines the existence of SHARED TX slots	Mobile nodes association; lack of these slots will prevent mobile nodes from associating to the network	Ensures the existence of SHARED TX slots in each slotframe while determining the number of slots based on the mobility metric	Star topology network and single hop communication	Needs for high number of coordinators to cover the entire deployment area	Facilitate the network infrastructure to include multihop tree network where even the leaf nodes can accept associations

3.2.3 Simulation Results and Analyses

Determining the impact of node mobility is achieved through testing the functionality of both modes of operation within a real test platform. This is carried out via implementing the TSCH and LLDN modes within the Contiki OS. Two important parameters are evaluated, which are the RDC of the nodes (that contribute the energy consumption) and nodes connectivity. In addition, two factors that affect the mobile node association process are considered in the analysis. These are the number of mobile nodes and the superframe /slotframe size (LLDN/TSCH). Table 3.4 demonstrates the utilized simulation parameters. LLDN online superframe to discovery and configuration superframes ratio is 5 to 1. One of the drawbacks that degrades LLDN operation is the interference between the nodes (either coordinators or mobile nodes). This issue has no impact on the TSCH operation due to the principle of channel hopping. Therefore, in this analysis, two cases of the LLDN deployment have been provided, one with interference and one where the interference range has been set to be coincide with the active range of the nodes.

Table 3.4: Simulation parameters

Parameter	Value
OS	Contiki 2.6.1
Scattering area size	240m×240m
Microcontroller	MSP430
Transceiver	CC2420
Mobility model	Random waypoint
Nodes' speed range	1-4 m/s
Payload size	20 Bytes

Fig. 3.9 presents the RDC performance of the three scenarios, LLDN with interference (LLDN,In), LLDN without interference (LLDN,NoIn) and TSCH. The RDC here corresponds to the total operation time of the transceiver (for the two states, transmitting and receiving) over total node's running time since deployment. For slotframe/superframe size of 0.5s, the TSCH has lower RDC than the default LLDN (with interference) for both cases of 6 mobile nodes (6n) and 15 mobile nodes (15n) as in Fig. 3.10.

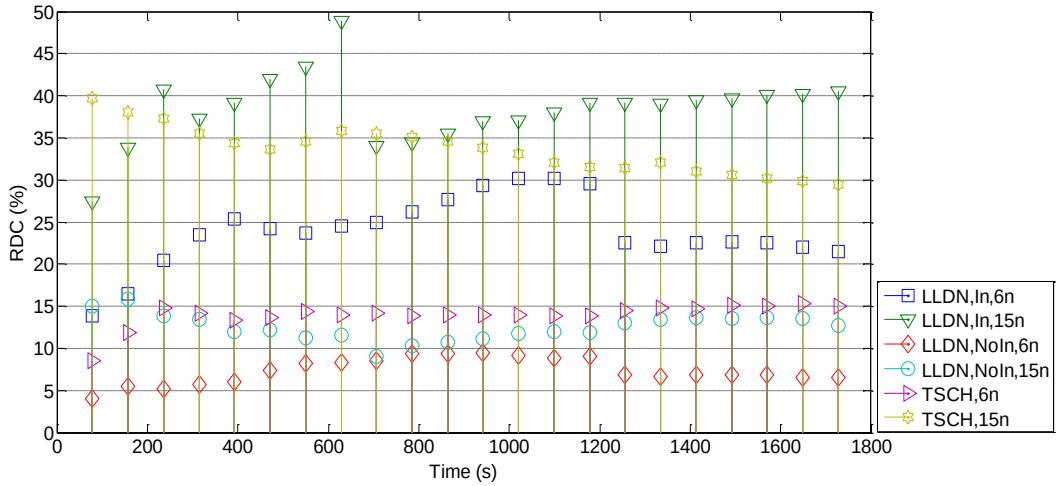


Fig. 3.9: RDC comparison between LLDN and TSCH, slotframe/superframe size =0.5s, transmission range=50m, no. of coordinators=9

However, by increasing the number of nodes to 15n, the TSCH has an RDC that is slightly higher than the LLDN.

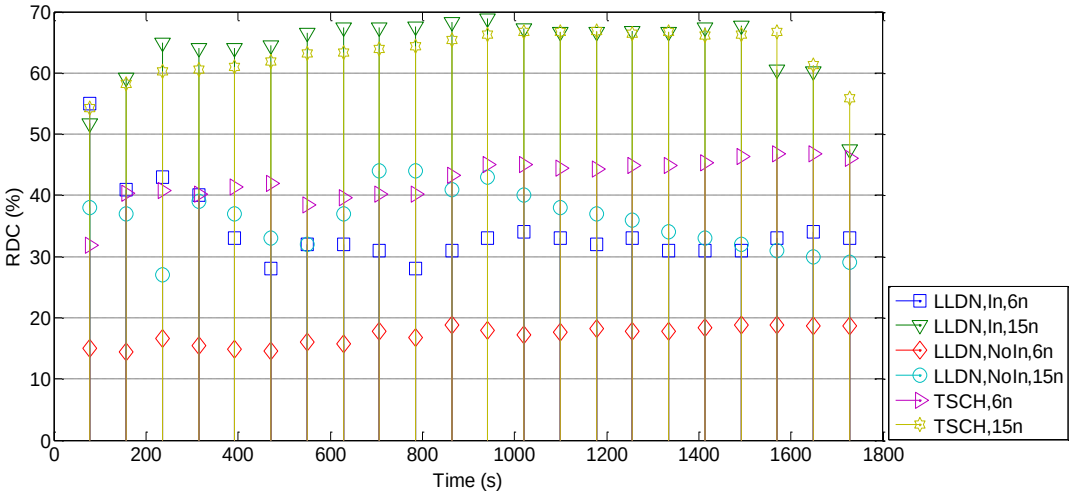


Fig. 3.10: RDC comparison between LLDN and TSCH, slotframe/superframe size =2s, transmission range=50m, no. of coordinators=9

The issue in TSCH is influenced by the problem of contention between the mobile nodes and once a node fails to associate, it has to scan again and wait until it receives a valid EB on the channel which it scanning on. This waiting time is mainly influenced by the number of channels N_{ch} in the $Frequency_{List}$, which has been set to 16 (number of defined channels in the IEEE 802.15.4, 2.4 GHz). In the meantime, LLDN,NoIn shows better performance than TSCH and LLDN,In. Neglecting the

impact of interference has minimized the probability of collision and the need again for retransmission of data or association requests. Finalizing the association process from the first attempt will cancel extra waiting time for the next EB on the fixed scanning channel (in the case of TSCH) or waiting till the discovery state (as in LLDN). Consequently, this minimizes the scanning time and in turn realizes lower RDC activity. The mobile nodes incur lower RDC while increasing the transmission range to 100m as in Fig. 3.11 since the nodes reside longer time in the coordinator perimeter and hence, lower number of dissociations.

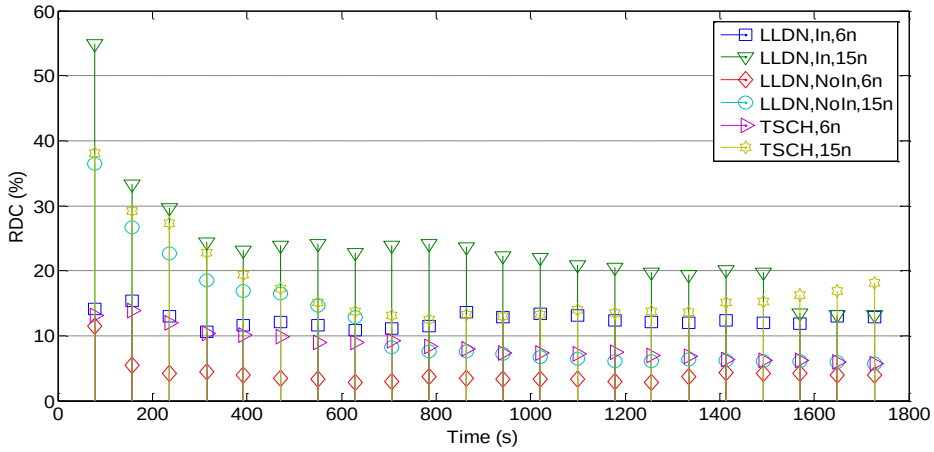


Fig. 3.11: RDC comparison between LLDN and TSCH, slotframe/superframe size =0.5s, transmission range=100m, no. of coordinators=4

Increasing the slotframe/superframe duration to 2s has resulted high RDC behaviour due the impact of lengthy periods of waiting between each consecutive beacons as shown in Fig. 3.12.

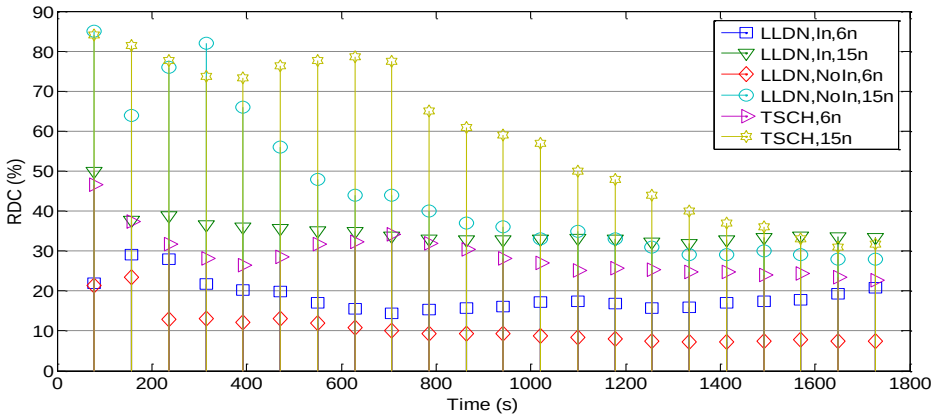


Fig. 3.12: RDC comparison between LLDN and TSCH, slotframe/superframe size =2s, transmission range=100m, no. of coordinators=4

By maximizing the transmission range of the sensor nodes, the network gains the advantage of reducing the number of coordinators and thus, minimizing the impact of collisions. The only drawback will be during the network initialization phase where all the mobile nodes contend on the same time to associate and this can get worse especially when more nodes are located in the same coordinator perimeter. Hence, the RDC is at its peak through the initialization phase and then decreases as time passes. As the nodes running into the steady state of operation, the RDC declines since the nodes have already associated. In addition, even if the mobile nodes disconnected from the network, the nodes will easily associate again without the overhead of contention as during the initialization phase of the network deployment (since not all the nodes will be disconnected as the same time).

According to the RDC performance, the ratio of connectivity can be visualized, since lower RDC for mobile nodes, means better node stability and less association attempts and thus, high node connectivity. This can be indicated through investigating the relation between the RDC behaviour of both LLDN,In and LLDN,NoIn with the connectivity metric. Nevertheless, the TSCH has different aspect, since although it has higher RDC than LLDN,In for case slotframe size 2s, it has demonstrated better connectivity in several cases as compared to LLDN,In. This is caused by the LLDN association procedure where the nodes manage transceiver activity during discovery and configuration states by relying on the schedule that is indicated in the announced EBs of each state. Hence, LLDN realizes efficient radio utilization by determining when exactly to switch on or off radio. On the second hand, the TSCH has no specific association schedule and has no defined beaconing structure. In turn, although the TSCH shows higher RDC in some cases, but the RDC activity can’t be used to deduce the connectivity. Therefore, TSCH shows to have better connectivity than LLDN,In (as in case 50m range 6n, 2s and 15n, 2s; case 100m range 6n, 2s).

Fig 3.13 shows the percentage of time that a mobile node was connected to the network since deployment for transmission range of 50m while Fig. 3.14 corresponds to the connectivity with 100m range. As indicated earlier, TSCH demonstrates higher connectivity ratio in almost all scenarios as LLDN,In, but the LLDN,NoIn has the leading connectivity among them. This is traced back to the impact of collision caused by the inter-cluster interference (interference between adjacent clusters). Intra-cluster interference is negligible since the coordinator ensures that there is no overlapping between the assigned slots to the nodes in the cluster.

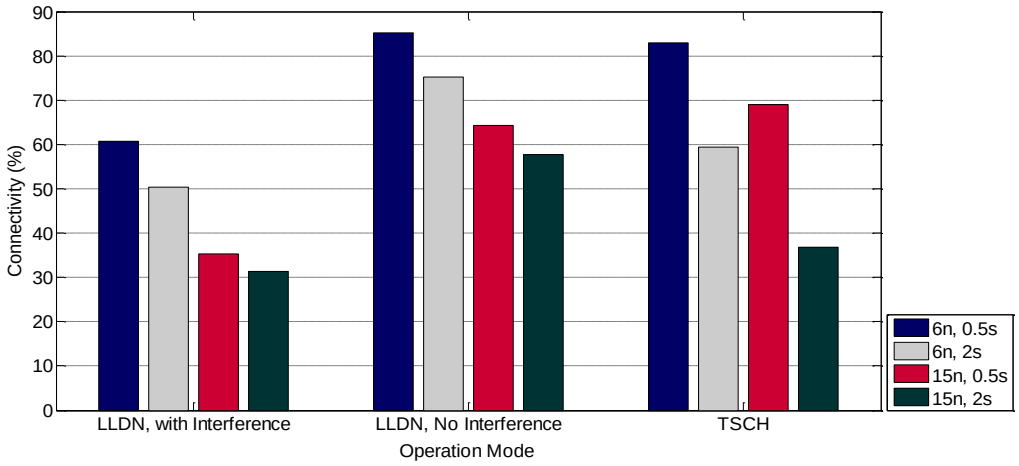


Fig. 3.13: Ratio of connectivity to the network, transmission range=50m, no. of coordinators=9

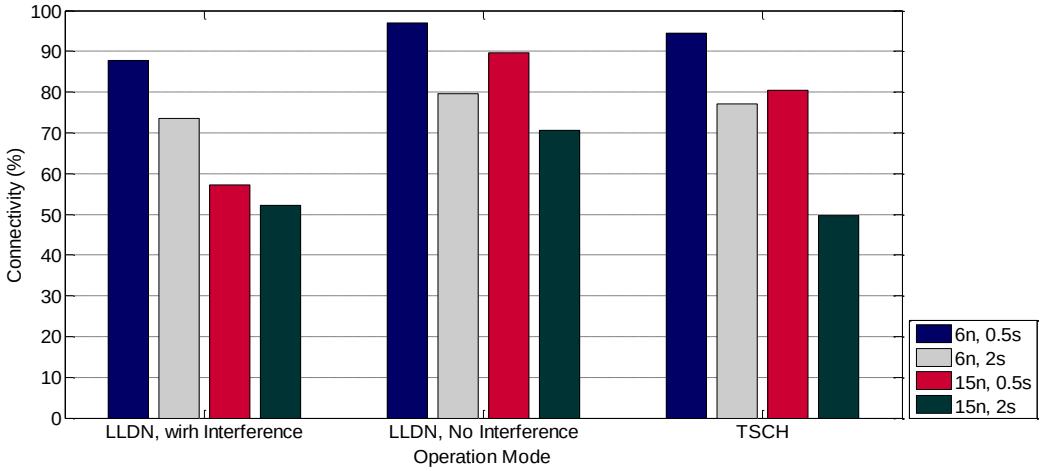


Fig. 3.14: Ratio of connectivity to the network, transmission range=100m, no. of coordinators=4

3.3 Summary

Node mobility is an upcoming challenge in the IoT context due to the lack of a defined and standardized protocol that manages mobile node associations and dissociations dedicated to low power devices. In this chapter, a study that highlights the challenges which arise as a consequence of node movement has been presented. Two of the important IEEE 802.15.4e modes of operation have been implemented in an IoT-based OS and tested against node mobility. The obstacles of each mode have been identified and the possible approaches to tackle these issues have been indicated. Simulations show that TSCH has better connectivity but higher RDC than the default implementation of the LLDN. After neglecting the impact of interference, the LLDN shows better RDC and highest connectivity ratio than TSCH. The drawback with LLDN is operation on a single channel which incurred several collisions and in turn this complicates the association process and successful data transmission. Conversely, the defect with TSCH operating on multiple channels is that this complicates the association process caused by waiting a longer time to receive a beacon. The coordinator in TSCH announces the beacon on a different channel at each time and thus, the mobile node has to scan for a longer time until it receives the beacon on the relevant channel (or searching the whole available list of channels which means extra scanning time). Hence, the best approach for the LLDN mode is to combine the concept of channel hopping and only to the uplink slots while fixing the beaconing to a single channel, where all the nodes adjust the scanning channel to it. In addition, the management timeslots in the LLDN have also to be set to a fixed channel that is known for all nodes prior to deployment. Moreover, facilitating the association process during the online state through activating the management slots will mitigate the overhead of waiting to associate until the discovery state. Regarding the TSCH mode, the appropriate practice for tackling node mobility is by defining a beaconing strategy that sets the beacon structure which facilitates the association process. In addition, the beaconing has to be fixed to a single frequency channel that is predetermined by all the nodes prior to deployment and thus, leads to a low scanning time.

The following chapter will address the issue of IEEE 802.15.4-based network initialization prior considering the problem of node mobility in chapters 5 and 6.

Chapter 4. Network Initialization Phase: Mesh-under Cluster-based Approach

This chapter investigates the initialization phase of the IEEE 802.15.4 network via determining the best strategy to organize the nodes into the network. Two important metrics are considered in this stage, the RDC and the shortest path to the coordinator (data aggregator node). The RDC of low power nodes can be considered as a crucial factor that determines the constrained-based IoT network lifetime and its service availability. Clustering would be a preferable solution to minimize node radio duty cycle by electing multiple cluster heads around the network to schedule node transmissions and collect readings. This chapter presents a mesh-under cluster-based routing (MUCBR) protocol that will divide the network into multiple clusters and perform the routing function within the IEEE 802.15.4 platform. MUCBR is implemented via the Contiki operating system. It reschedules the structure of the 802.15.4 standard in order to reduce the RDC of the sensor nodes and minimizes the number of collisions. The election of the CHs is density-aware and determined by the routing direction inside the network which in turn reduces the number of hops and minimizes the number of collisions caused by the existence of multiple CHs in a single area.

4.1 Mesh-Under Routing Philosophy

The rise of the 6LoWPAN layer has inspired the research community to bring a new term of classification to the routing world in the field of IoT, this classification is based on which layer will make the routing decision and accordingly there will be two types of routing: mesh-under and route-over [100]. This classification is simplified in Fig. 4.1. Unfortunately, neither IEEE 802.15.4 nor 6LoWPAN define how mesh topology will be achieved [101] to route towards the coordinator, which is considered the sink.

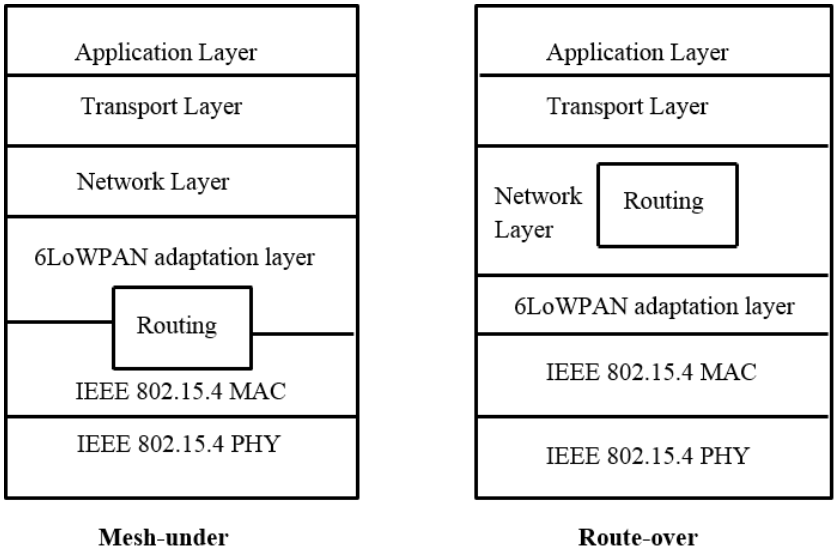


Fig. 4.1: Mesh-under versus route-over

Comparing to other network topologies, the cluster-based networks have: better performance and scalability [102], lower communication overhead which in turn reduces the energy consumption [103] and can be considered as an energy efficient solution for low power nodes data routing [104].

All these facts led the research here to propose a mesh-under cluster-based routing (MUCBR) protocol that provides the following services: clustering technique under the IEEE 802.15.4, reduced RDC schedule listening technique, routing to the sink through the shortest path and transmissions with low collisions as compared to IEEE 802.15.4 standard.

The clustering process will take into account the density of the nodes within a specific area. The dependency on the density factor is necessary to reduce the number of CHs, since increasing the number of CHs inside a single personal operating space can increase the number of collisions due to the fact that multiple coordinators within a POS increases the risk of assigning matched time slots and leads to transmission collisions. In addition, the node with the least depth to the sink and the highest weight (according to the MUCBR weighting mechanism) will be elected as CH. This will ensure the election of a CH on the upward edge of each cluster and in turn minimizes the number of hops to the sink as depicted in Fig. 4.2.

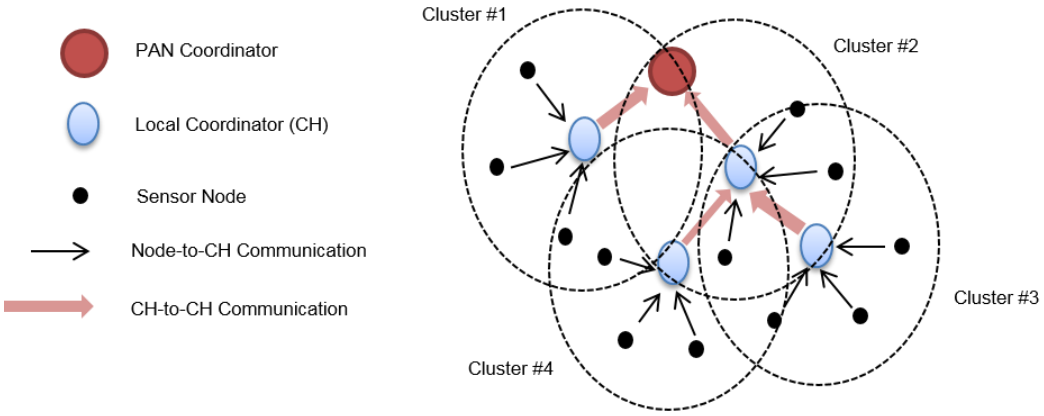


Fig. 4.2: MUCBR cluster network

The CH in each cluster (corresponding to the coordinator) will assign a random time reference for each node within its cluster to reduce the inter-cluster interference. This time reference is used by each node to start transmitting or receiving. The idea behind randomizing and spreading nodes access is to reduce collisions encountered in IEEE 802.15.4. The proposed algorithm has been implemented within the Contiki OS based on the IEEE 802.15.4 platform. The simulations show low RDC and in turn an improved energy efficient routing technique while achieving a shortest path to the sink. Moreover, the collision parameter has been reduced by a factor of 40% as compared to the default 802.15.4.

4.2 Related Work

Several works have been presented regarding WSN clustering techniques, one of the pioneers within this field is the LEACH [105] protocol. Due to its simplicity and effectiveness it has inspired other contributions that optimized its performance and led to new clustering approaches. Here we will commit ourselves to work that considered the 802.15.4 standard as the underlying infrastructure. Regarding cluster-tree utilization and analysis, authors in [106] present directed acyclic graph structure within the beacon-enabled mode to form a cluster-tree WSN. The authors minimize delay and improve the robustness of the network by permitting every node to have more than one parent in order to mitigate the parent/CH failure or sleeping. The paper also indicates that the synchronization process within the beacon-enabled mode can lead to a collision between the superframes with the same depth. With

respect to clustering techniques and impact on network performance, authors in [107] indicate that clustering can reduce the number of collisions in the beacon enabled mode. Hence, the authors suggest allocating different frequency channels to each cluster which can be assigned by the base station.

In terms of inter-cluster interference, both [108] and [109] have tackled this issue but both presented techniques incur high overhead and do not fit the infrastructure of the IEEE 802.15.4.

4.3 MUCBR Design Principles

The basic feature of the proposed MUCBR is to provide a routing service within the link layer (mesh-under). This will add an advantage to the network in terms of reduced energy consumption.

Operating with the IEEE 8021.5.4, there is a possibility of inter-cluster interference due to the synchronization process of the beacon-enabled mode [106]. In addition, the node's radio has to stay ON within the contention period of the slotted CSMA/CA period until a free slot is located. This will increase the energy consumption. On the other hand, for the non-beacon enabled mode, the nodes have to always be awake to avoid deafness [108] which in turn leads to 100% radio duty cycle.

Accordingly, since the IEEE 802.15.4 standard did not indicate how the clustering will be achieved [108], the MUCBR approach is based on clustering the IEEE 802.15.4 standard to reduce nodes RDC. The proposed MUCBR resembles the beacon-enabled mode by which the coordinator is assigning the timeslots to the nodes but in with the MUCBR, the CHs allocate a random *time-reference* to each node instead of sequential slots. This *time-reference* represents a solid time by which the node will either starts sending or receiving (not a time slot) and simulates the guaranteed time slot (GTS) that no other nodes will contend on this timing. During these *time-references*, nodes will transmit to their CHs while the CHs must listen during these reference times.

This will gain a significant reduction in the duty cycle for both the non-CH and CH nodes. Fig. 4.3 shows the basic differences between the patterns of communication carried out by three nodes for the IEEE 802.15.4 and MUCBR. T_RA, T_RB and T_RC are time references assigned randomly, for nodes A, B and C respectively by a CH in order to identify the transmission initiation time. Thus, the CH and any member within the cluster will only be required to open radio through T_f intervals.

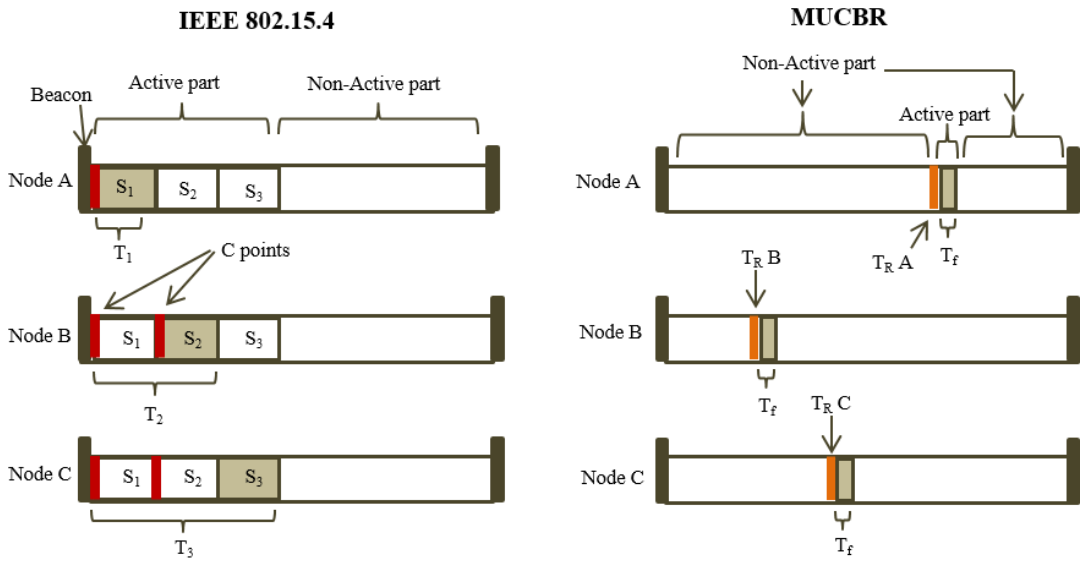


Fig. 4.3: Patterns of slot/time reference allocation in IEEE 802.15.4 and MUCBR

According to the conducted simulation tests through Contiki OS, the value of T_f ranges between (0.54ms for 12-byte) and (4.2ms for 128-byte) while the default slot duration within the 802.15.4 is 15.36ms. This mechanism managed to reduce the RDC. On the other side, if node C in the IEEE 802.15.4 standard tries to transmit, then it must contend with nodes A and B and if it was not able to utilize slots S_1 and S_2, then it has to open the radio for time duration T_3. Moreover, there is a probability of collision that might occur at a collision point (C points) due to the contention. Thus, retransmission is required while a time slot has been lost due to the contention of two nodes.

The dependency of MUCBR on randomly distributed time references over the beacon interval minimizes the probability of collisions that might occur at C_p points and eliminates the needs for retransmission, hence saving energy.

4.4 MUCBR Protocol Description

The proposed algorithm is based on the IEEE 802.15.4 infrastructure and appends four types of frames to the defined frame type list in this standard. These frames are: *Establish_Cluster, Broadcast_Weight, CH_Elect* and *CH_Request* as depicted in Table 4.1. The frame type values are reserved for future use within [110]. The amendment 1 MAC sublayer, IEEE std. 802.15.4e [1] has not yet been implemented within the Contiki OS environment, so the reserved frame type values of the earlier standard version [110] have been considered.

Table 4.1: Appended frames indexes

Frame type value b2b1b0	Frame_type
100	*Establish_Cluster*
101	*Broadcast_Weight*
110	*CH_Elect*
111	*CH_Request*

Seeking to reduce the size of the packets required to initialize the nodes into clusters, the PAN ID compression bit within the frame control field is set to one due to the existence of the source and destination addresses. Hence, the source PAN identifier field in the IEEE 802.15.4 frames will be omitted which gains a reduction of two bytes (utilized feature based on the 802.15.4 specifications).

Analyses in [111] indicate how the CCA within CSMA/CA can increase the delay, so the MUCBR (during clusters initialization) does not utilize the CSMA/CA technique to access the medium but another technique has been devised that will omit the RDC time required for checking medium prior to transmission. Therein, each node will generate a random number that represents a time indicator for transmission called *(rand_tick*) and chosen within the *phase_state* time duration. The *phase_state* represents one of the clustering process stages: *phase_ranking*, *phase_weighting*, *phase_election*, *phase_requesting* and *phase_scheduling*.

These phases are separated by a guard time (GT). The time duration of any phase is equal to the summation of the GT and preceding timing indicator, subtracted from the current timing indicator, i.e.:

$$phase\_election = election\_timing - (weigting\_timing + GT)$$

The values of *ranking_timing*, *weighting_timing*, *electing_timing*, *requesting_timing*, *scheduling_timing* are adjusted with regards to the number of nodes in the network (the user must adjust these values prior to initialization), high number of nodes leads to choose high timing values in order to decrease the probability of collision. These timing intervals are set fixed for all the nodes and ensure all the nodes to be synchronized and committed to the clustering phases. The timing alignments are demonstrated in Fig. 4.4.

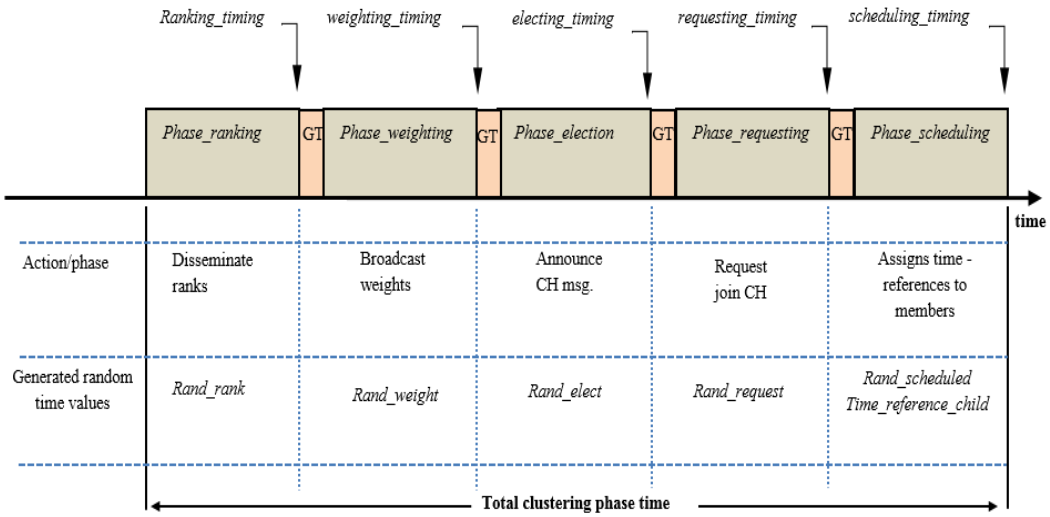


Fig. 4.4: MUCBR clustering phases timing

The mechanism of MUCBR is as follows. The initialization of the cluster network is basically started by the PAN coordinator (sink) via broadcasting an *Establish_Cluster* message. The message will embed a rank field (1-Byte) which is set to one as an indication to the coordinator, and will be incremented by one as passing each hop across the network. Each node within the PAN will first act as FFD device and enter the passive scan mode waiting for the *Establish_Cluster* message. Each node which receives this message has to increment the rank field in the message and store the value as its rank in the network. Once a node has its own rank, it will update the rank field within the message to its rank (*R_current*) and the

source address to its short address. Thereafter the node has to retransmit the message to its neighbors at a time tick, called *rand_rank*, which is randomly generated and lies within the *phase_ranking* period. Fig. 4.5 presents the message sequence chart carried out by the nodes to initialize the 802.15.4 network into clusters.

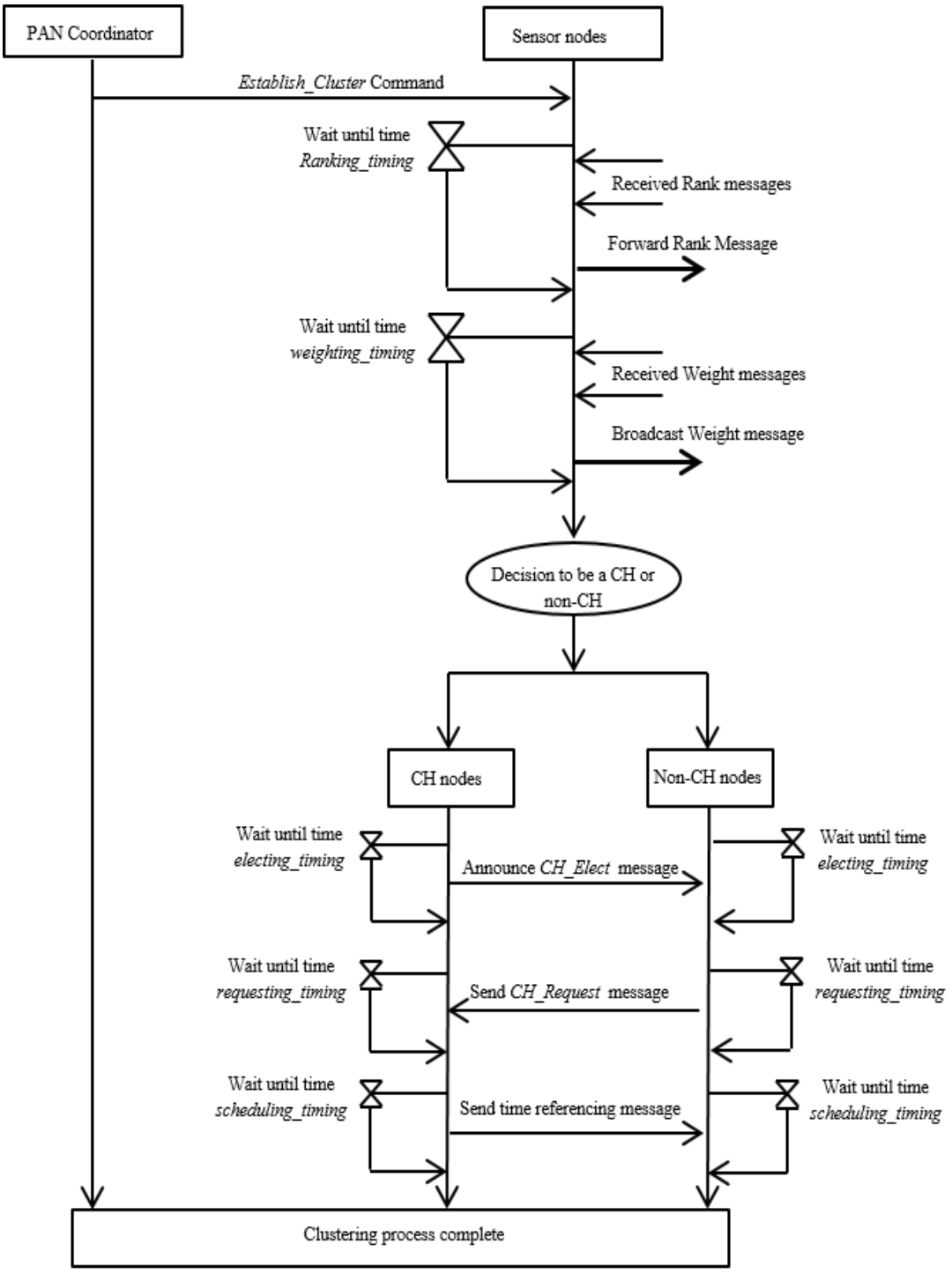


Fig. 4.5: MUCBR clustering process (message sequence chart)

In order to avoid the count-to-infinity routing problem [112], the nodes will not forward any message that carries the same rank or higher while recording these messages. The *phase_ranking* period will ensure that the *Establish_Cluster* message has been forwarded down to all nodes within the network. After the *phase_ranking* time has finished, each node computes its weight and generates a time tick, *rand_weight*, within the *phase_weighting* period to announce its weight at this time. The weight of a node (*W_current*) is equal to the number of *D* (Downward) nodes within the POS.

The *D* value corresponds to the number of received announcements (*Establish_Cluster* messages) that have a rank value (*R_received*) larger or equal to the rank of the current node *R_current*. In accordance with the computed weight *W_current*, the node will announce its weight at *rand_weight* time using the *Broadcast_Weight* frame and waits for *phase_weighting* period to finish while recording the received nodes weights (*W_recived*) for *F* (Forward) nodes. *F* nodes are those where $R\_received \leq R\_current$. Considering only *F* nodes is necessary to select a node with a highest weight on the upward direction of a cluster to achieve the shortest path to the sink.

Regarding the received announced weights from *F* nodes, each node will check if $W\_current \geq W\_recived$. If the current node has a higher weight than *F* nodes, then it will announce itself as CH (because it's the only node with highest weight and shortest path for the *D* nodes) and broadcasts the *CH_Elect* message at time *rand_election*, randomly generated within the *phase_election* interval. For nodes which have the highest weight within their POS, they have to broadcast the *CH_Elect* message and act as CHs to wait for the association request messages *CH_request* from adjacent nodes. Thus only one CH within each POS will be elected. When nodes receive *CH_Elect* announcement they will decide to which CH to connect, based on the rank value indicated by each *CH_Elect* announcement and send a *CH_Request* message at *rand_request*, randomly generated within the *phase_requesting* time duration. The destination address in the *phase_requesting* is set to the source address of selected CH. Any node that has not received a *CH_Elect* announcement (deserted node) will send CH_*Request* to one of the neighbour nodes,

the intended node then acts as CH to this unconnected node and proceed to the next step.

The last step is determined by the CH, which will generate a random time reference (*time_ reference_child*) for each member in the cluster, where 0 < *time_ reference_child* < T_P. T_P is the period that nodes are programmed to transmit and resemble the beacon interval value. This randomness with an adequate T_P value will reduce the inter-cluster interference. Subsequently, the probability of a collision-free clustered network is:

$$P_{collisionFree} = 1 - \left(\frac{D_{pos} \times T_f}{T_P}\right) \quad (4.1)$$

D_{pos} indicates the density of sensor nodes within a POS and T_f is the required time to transmit a single frame.

The T_P is limited by the interval of the adjusted period timing to transmit readings and matches the BI impact in IEEE 802.15.4 beacon-enabled mode. A low value of BI will increase collisions while a high value increases the delay. The CH (during the sensing phase) switches its radio ON only during time references that are generated for its members.

Meanwhile, the CH transmits the collected readings of the members along with its reading within a specified time reference (*time_ reference_self)* allocated by a CH which it has been connected to.

During the remaining time the radio is OFF. Each member node upon the received *time_reference_child*, will transmit strictly at this time and next at (*time_ reference _child* + T_P). After each transmission, the nodes will increment this value by the transmission period time (T_P). The issue of rotating the CH task around the nodes, which utilizes the residual energy of each node as factor for CH election, has not been addressed by this work. Prior to the initialization process all nodes were assumed to have fixed residual energy.

Fig. 4.6 shows a flow chart that represents the process carried out by each node in the network in order to determine clustering.

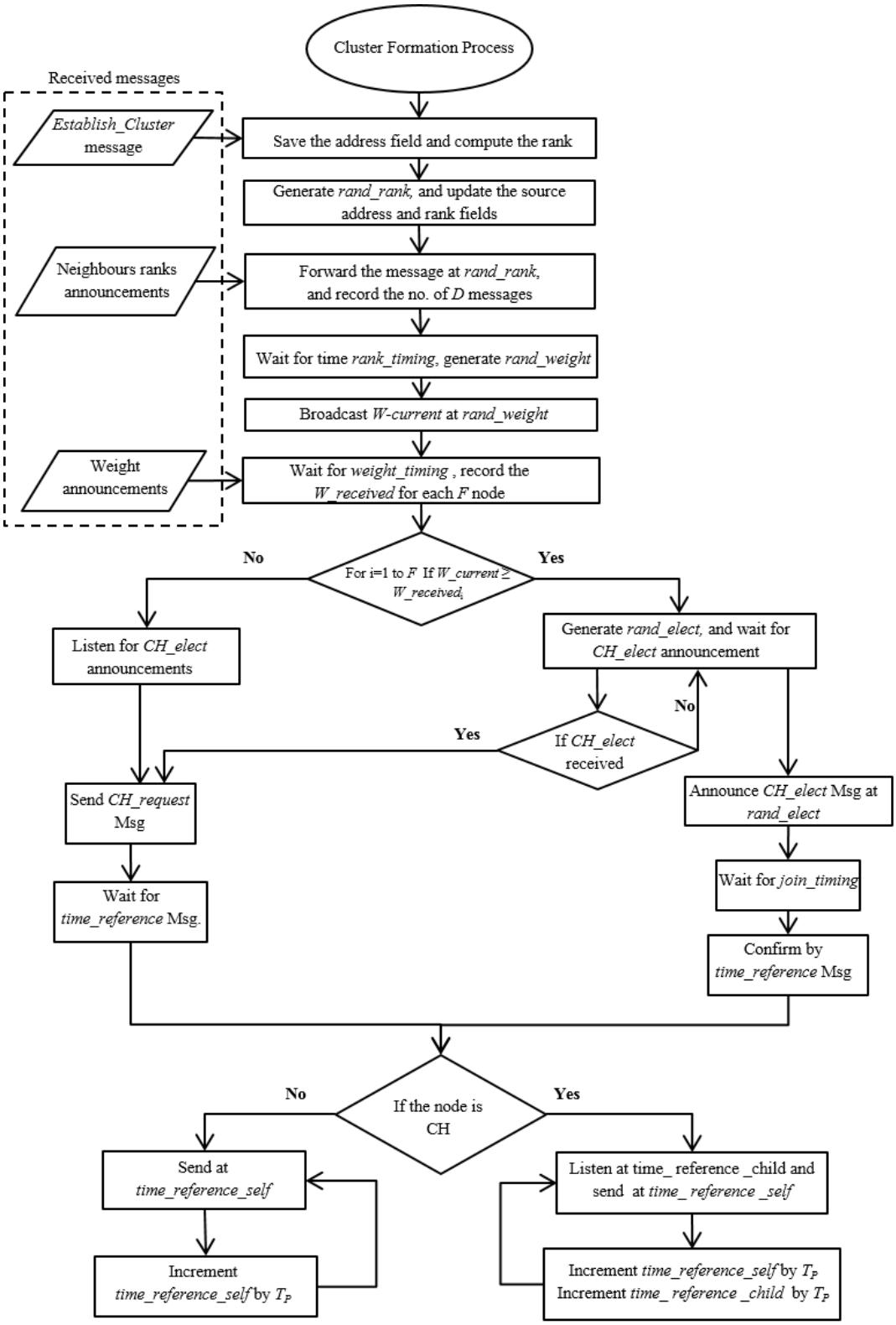
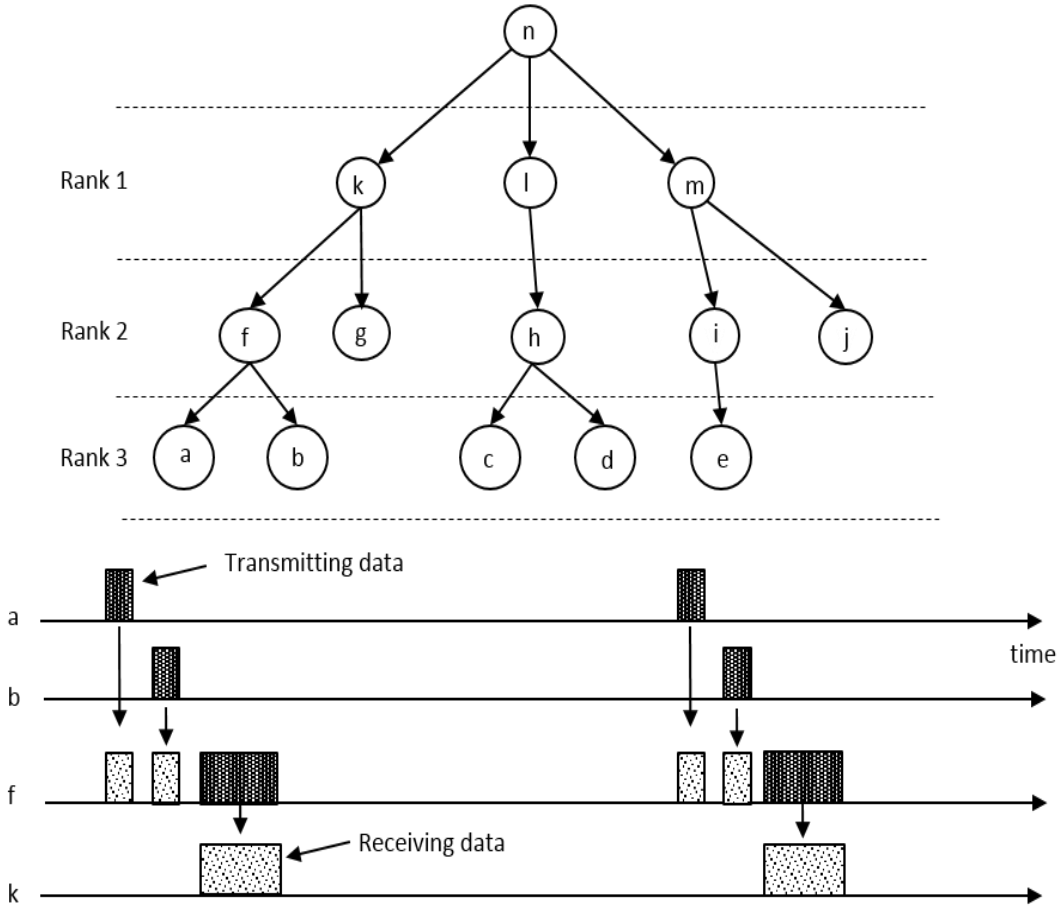


Fig. 4.6: MUCBR clustering process (node-based activity)

In order to accurately adjust the radio operation, the MUCBR relies on the *rtimer* time library within the Contiki OS. *rtimer* always gives feedback on the number of ticks, called *clock_tick*, which corresponds to the MCU clock frequency, Thus achieving high time resolution. The MUCBR handles the radio states through this time library to achieve the required light RDC. Through simulations, multiple payload size has been fed to the network in order to get the exact radio time required to transmit IEEE 802.15.4 frame. Since the sky sensor node, used as the node test platform, utilizes the MCU MSP430 with a clock frequency 32768. Then, the radio has been adjusted with a timer that counts to 165 *clock_tick* which corresponds to approximately 5ms, the time required to receive IEEE 802.15.4 frame. Only during these timer counts the radio will be active, else, the radio goes to sleep to save energy. The problem with the *rtimer* is a 2-byte register that will overflow after every two seconds. Thus, an extra 32-bit time variable in the Contiki has been defined in order to overcome this problem.

4.5 Low Latency Data Forwarding Scheme

In order to realize low end-to-end data aggregation process, the MUCBR utilizes the principle of ranking-based priority slots allocation. This scheme consists of allocating the first slots of the superframe structure to the nodes with the highest ranking values (bottom of the network) as nodes a, b, c, d and e in Fig. 4.7. As example, slot assigned to node f in the superframe schedule is after the slots of nodes a and b. This will let node f to collect the readings from both node a and b prior sending its data and thus, avoiding the defer of data forwarding (readings from nodes a and b) to the next superframe. The same procedure applies with node k, where its slot in the superframe schedule is commencing after the slot of node f to give the opportunity of collecting required readings from nodes a,b and f. Hence, minimizing the incurred data latency caused by buffering data on the relay nodes (k and f) and waiting for the next superframes. The MUCBR varies the slots duration sizes as regards to the size of transmitted data. Since node f is relaying data from nodes a and b, then its slot size will be triple the slot size of node a. Fig. 4.7 simplifies the sequence of relaying readings based on the above strategy.



		Cluster K and descendent nodes	Cluster l and descendent nodes	Cluster m and descendent nodes
Slot 1	t_1 t_2	a → f b → f	c → h d → h	e → i
Slot 2	t_1 t_2 t_3 t_4	f(a) → k f(b) → k f → k g → k	h(c) → l h(d) → l h → l	i(e) → m i → m
Slot 2	t_1 t_2 t_3 t_4 t_5	k(f(a)) → n k(f(b)) → n k(f) →n k(g) → n k → n	l(h(c)) → n l(h(d)) → n l(h) → n l → n	m(i(e)) → n m(i) → n m(j) → n m → n

Fig. 4.7: MUCBR ranking-based scheduled data forwarding

4.6 Latency Overhead of Sampling and Scheduling Listening Techniques

This section determines the impact of latency for both scheduling and sampling techniques. For both schemes, the number of hops has the main influential impact on increasing data latency. Regarding scheduling technique (utilized by MUCBR), the number of hops and the number of intermediate nodes (attached to CHs through the route to the sink) are the main factors that maximize end-o-end delay. The latency in this case is determined by the amount of time to forward a frame by each node and can be based on the length of payload (L_P), long interframe space *LIFS* and *aTurnaroundTime* values (both set by IEEE 802.15.4), number of hops (h) and number of nodes attached to a CH in the route for each hop (n (h)):

$$Latency_{scheduling} = \sum_{i=1}^{h} \sum_{j=1}^{n(h)} \left(\left(LIFS + \frac{8 \times L_P}{baud} \right)_j + aTurnaroundTime \right)_i \quad (4.2)$$

The *aTurnaroundTime* is the required time to change the state of transceiver from receiving to transmitting and vice versa. The baud rate value for IEEE 802.15.4 (2.4Ghz) is 250Kbps.

In the meantime, for the sampling technique, since there is no synchronizations in the network and the nodes can transmit readings at any given time, the latency is influenced by the mean forwarding rate of each relay node (F_R) and the mean rate of the received frames (R_R) for any relay node. Therefore, the utilization (U) of each relay node can be expressed as $U = R_R / F_R$.

The mean forwarding rate in the sampling technique is determined by the impact of CSMA/CA technique and can be expressed by:

$$F_R = \frac{1}{\left(\frac{2^{BE}-1}{2} \times aUnitBackoffPeriod\right) + \left(\frac{8 \times L_P}{baud}\right) + macAckWaitDuration + CCA_{duration} + aTurnarroundTime + \frac{8 \times Ack\_Size}{baud}} \quad (4.3)$$

aUnitBackoffPeriod is the backoff time prior transmitting and corresponds to 20 symbols in the IEEE 802.15.4 standard while *macAckWaitDuration* is the required waiting time for an Acknowledgment message and according to the standard is 54 symbols.

The delay overhead here can be considered as an *M*/*M*/1 queuing problem and the resulted buffering delay can be estimated accordingly. The number of frames that are buffered (B_F) and are waiting to be forward is:

$$B_F = \frac{U^2}{1-U} \tag{4.4}$$

Meanwhile, the delay time at each relay node in the route can be expressed as:

$$delay_{relay} = \frac{B_F}{R_R} + \frac{1}{F_R} \tag{4.5}$$

Accordingly, the total buffering latency for a route with *h* hops in the sampling scheme is:

$$Buffering\ Lattency_{sampling} = \sum_{i=1}^{h} \left(\frac{B_F}{R_F} + \frac{1}{F_R}\right)_i \tag{4.6}$$

4.7 Hosting Security

The MUCBR process produces a chain of connected CHs by which any CH is acting as a leaf node to another CH (lowest ranking) and as a CH to other nodes attached to it (higher ranking). Accordingly, after the key bootstrapping scheme (discussed later in chapter 7), all the adjacent CHs can share their CH node-base key. The strategy here is to enforce each CH for distributing the node-base key of all the CHs attached to it (sending only to its leaf nodes that are acting as CH). The *CH_Elect* message transmitted by each CH will contains the required key credentials for above parent

CH (hop 1) while the response message to *CH_Request* frame contains the related non-CH nodes' keys of members of the same cluster (hop 2). This technique will be exploited later in chapter 7 to facilitate the key establishment procedure and is following every association process.

Although during the initialization stage all the nodes are keeping radio ON which will increase the energy cost, this action is mandatory to force the CH nodes for listening and recording all security credentials of neighbour CHs. The process by which the key management scheme will utilize the designed cluster network here is demonstrated later in chapter 7.

As example, suppose that CH node F as in Fig. 4.8 (this example assumes all the leaf nodes have become CH nodes only to simplify this procedure) has its own node-base key K_F. Then during deployment, this node obtains adjacent CH keys K_E, K_B and K_C via its parent CH node B while receives K_G through listening to transmitted key credentials by node G. In some cases, node F and G are not within the range of each other, for that reason the CH nodes have been obliged to forward the keys of their child CH nodes to the lowest two hop nodes.

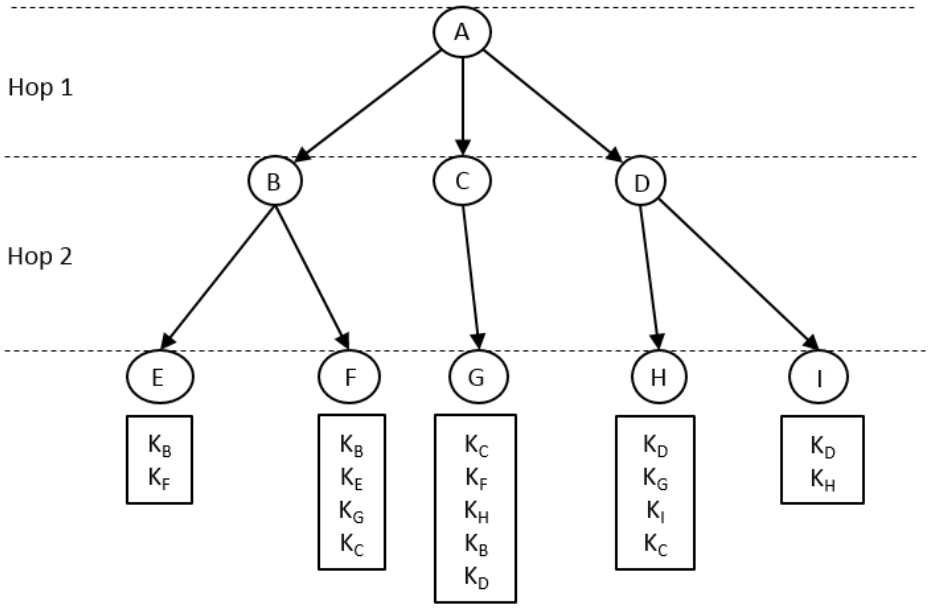


Fig. 4.8: Lists of acquired keys of neighbour CHs

4.8 Results and Analysis

The RPL and RIME implementation within the Contiki OS are based on the ContikiMAC RDC technique, which is a sampled RDC listening technique and considered as low power RDC MAC protocol [113]. The analysis highlights the importance of the scheduled RDC listening technique (utilized by MUCBR) over the sampled RDC listening technique (utilized by RPL and RIME).

The analyses are based on three classifications: Route-over/sampled-listening (RPL), Mesh-under/sampled-listening (RIME) and Mesh-under/scheduled-listening (MUCBR). The implementation of the RPL within Contiki is said to be route-over since it utilizes the IPv6 protocol. The derivation of this classification will state the differences between two basic important design aspects (mesh-under over route-over) and (scheduled over sampled-listening).

The analyses differentiate between the basic two types of nodes in the network: leaf/non-CH (RFD nodes) and router/CH (FFD nodes). Furthermore, these analyses will address two life-time phases of a network, initialization (clusters formation) and steady (basic readings forwarding).

In order to provide more realistic analysis, the Powertrace tool [114] has been utilized which is believed, according to the developers, to assure 96% accuracy comparing to power measurements obtained through the hardware-based tool. This tool is based on assigning timestamps to the transceiver states, receiving and transmitting. Hence, a timings profile will be formed to indicate the exact time activity of each radio state.

4.8.1 Simulation Parameters

All the nodes within the network are running the Contiki OS 2.6 and 100 nodes are deployed randomly utilizing the Contiki OS Cooja simulator [115] while only one sink exists at the edge of the network. Table 4.2 presents the basic network parameters utilized in the MUCBR simulations.

Table 4.2: MUCBR simulation parameters

Parameter name	Value
OS	Coniki 2.6
MAC Protocol	NullMAC
Radio duty cycling algorithm	MUCBR Scheduling
No. of nodes	100
Scattering area size meter	400m*400m
Ave, no. of nodes within a POS	6
Transmission range	50m
Interference range	100m
Microcontroller	MSP430
Transceiver	CC2420

4.8.2 Performance Analysis

The nodes for the three protocols were adjusted to transmit a fixed payload size every 2 seconds. Periodic packet generation has been utilized since it is more realistic to conduct reporting on the network performance [39]. On average, the number of runs (simulation) are 24 for each scenario and the mean output of the nodes' performance is considered. Increasing the number of runs has no impact since the variation of the collected results after this value is relatively small. Fig. 4.9 demonstrates the energy consumption of the two radio states of operations (transmitting and receiving) regarding CH nodes (in MUCBR) and router nodes (in RIME and RPL), all having on average three child/members. Fig. 4.10 considers the non-CH and leaf nodes. During the clustering initialization time (first 7 seconds), MUCBR consumes more power than RIME and RPL because of the 100% radio activity required to initialize the nodes into clusters. Then subsequently the nodes will act either as CH or non-CH nodes which will reduce RDC power. After running the nodes for 1000 seconds, the required radio energy of MUCBR (CH/ router) is only 43% of the required energy by RIME and 21% of the consumed energy by RPL. Moreover, the radio energy of MUCBR (non-CH/leaf) is only 38% of the consumed energy by RIME and 29% of the required energy by RPL.

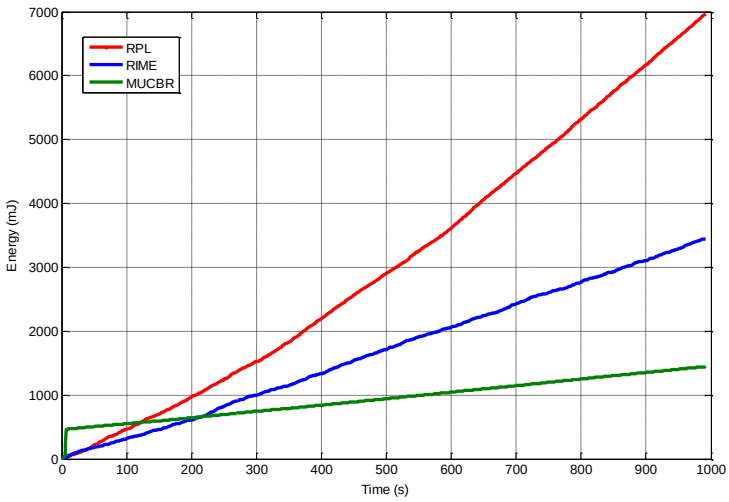


Fig. 4.9: CH/Parent energy consumption

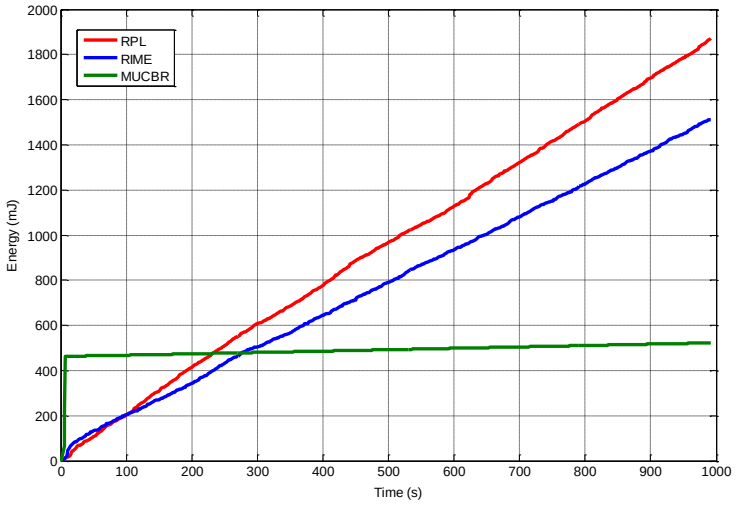


Fig. 4.10: Non-CH/leaf energy consumption

Fig. 4.11 and 4.12 depict the radio duty cycle through the initialization phase of the three protocols for both CH/router and non-CH/leaf nodes respectively. MUCBR requires 100% RDC through the first 7 seconds to initialize the network and lead to maximize the total radio energy consumption.

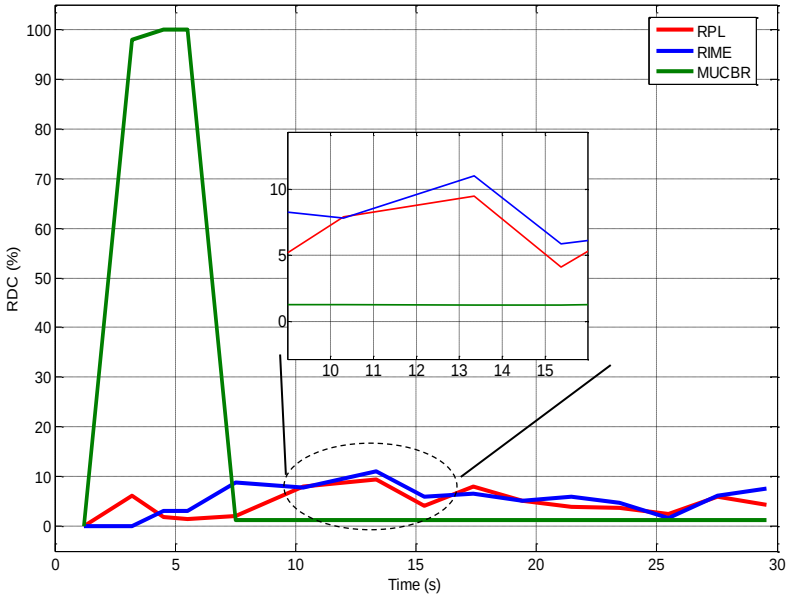


Fig. 4.11: RDC-initialization phase (CH/Parent)

The MUCBR enters the steady state operation of the RDC in the 8th second where the scheduled radio operation took place; therein the CH nodes will transmit and receive only during defined time indicators and the non-CH nodes will transmit to their CHs also within a defined time reference.

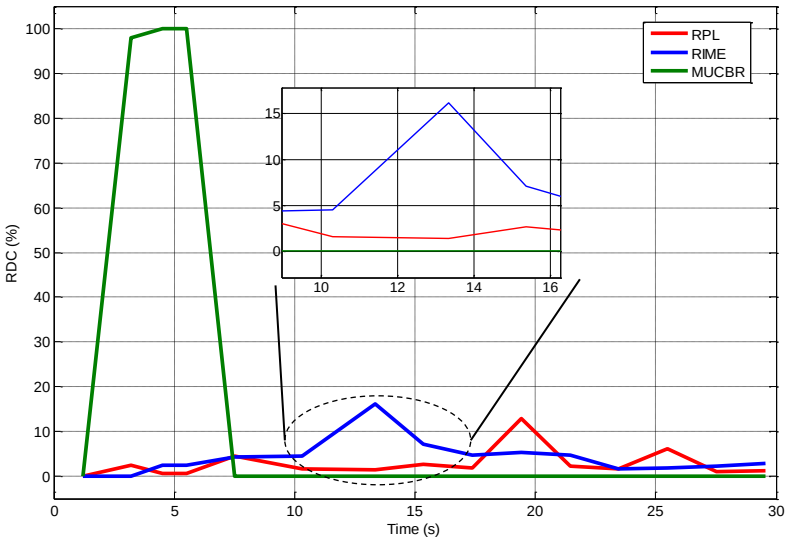


Fig. 4.12: RDC-initialization phase (Non-CH/leaf)

Fig. 4.13 and 4.14 show the RDC through steady state (steady period) time of the three protocols for both CH and non-CH nodes. The CHs nodes within MUCBR achieved 1.3% RDC while the router nodes in RIME have an average 5.7% RDC and 7.5% RDC in RPL.

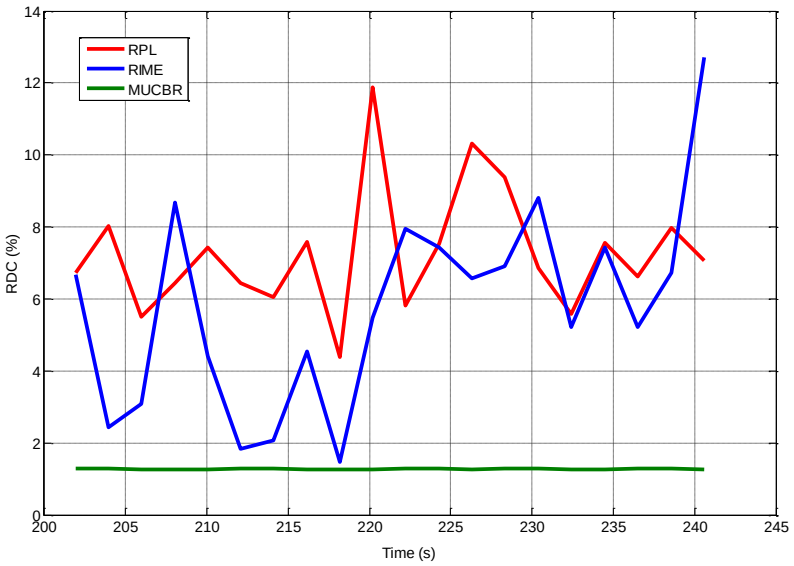


Fig. 4.13: RDC-steady phase (CH/Parent)

Similarly, the non-CH nodes in MUCBR achieved 0.08% RDC while the leaf nodes in RIME have an average 2.2% RDC and 2.8% RDC in RPL.

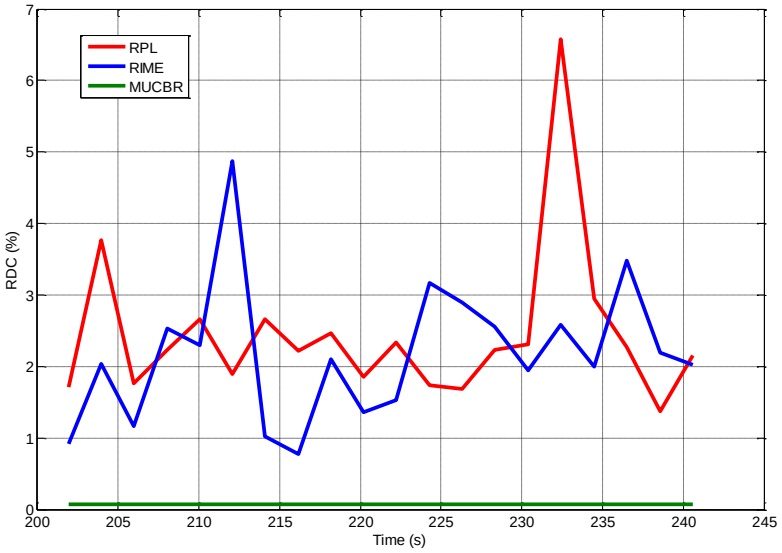


Fig. 4.14: RDC-steady phase (Non-CH/leaf)

The analyses indicate the advantage of the scheduled-listening considered by the MUCBR over the sampling-listening technique. The excessive energy consumption of transmission for RIME and ContikiRPL is due to the sampling-listening technique which requires the sender to continuously transmit readings in order to permit correct message reception.

In term of collision, Fig. 4.15 presents the probability of collision-free for the 802.15.4 standard while increasing both *macSuperframeOrder* (SO) and the number of nodes in POS.

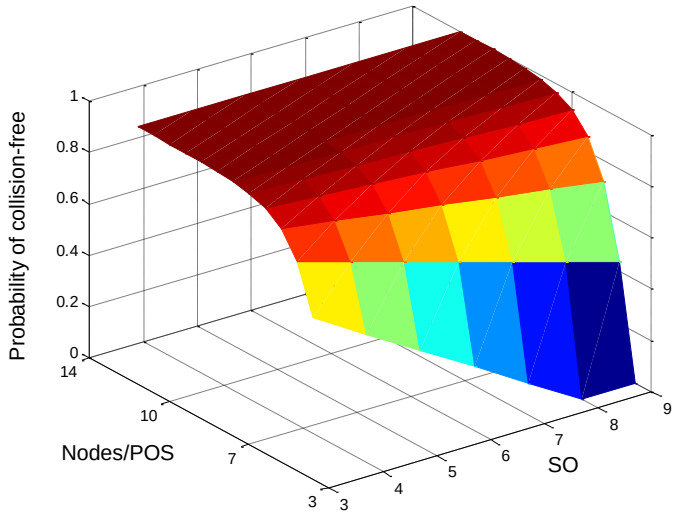


Fig. 4.15: Probability of collision-free (IEEE 802.15.4)

The SO value determines the active slot superframe duration (SD) while the *Beacon Order* (BO) determines the beacon interval (BI) duration, and obtained as follow:

$$BI = aBaseSuperFrameDuration * 2^{BO}$$

and

$$SD = aBaseSuperFrameDuration * 2^{SO}$$

Where *aBaseSuperFrameDuration* is a time constant and corresponds to 15.36ms while SO and BO must satisfy: $0 \leq SO \leq BO \leq 14$.

Increasing the value of SO will reduce the collision but maximizes the RDC. Thus, increasing SO to mitigate the collision is not preferred due to the excessive rise in the energy consumption.

On the other side, Fig. 4.16 demonstrates the probability of collision-free regarding MUCBR. The MUCBR is dependant only on the BO value (BI duration). So, the SO value has no influence on the MUCBR which is only affected by nodes density, thus the collision has been reduced. Even with the worst case of 9 nodes in each POS, the probability of collision-free does not fall below 0.99. For fairness in comparing with 802.15.4, since the T_f in MUCBR is dedicated for only single frame while the time slot in 802.15.4 can convey three frames, the number of nodes in the POS regarding MUCBR is multiplied by 3. Thus, there will be the same number of frames for the MUCBR and 802.15.4.

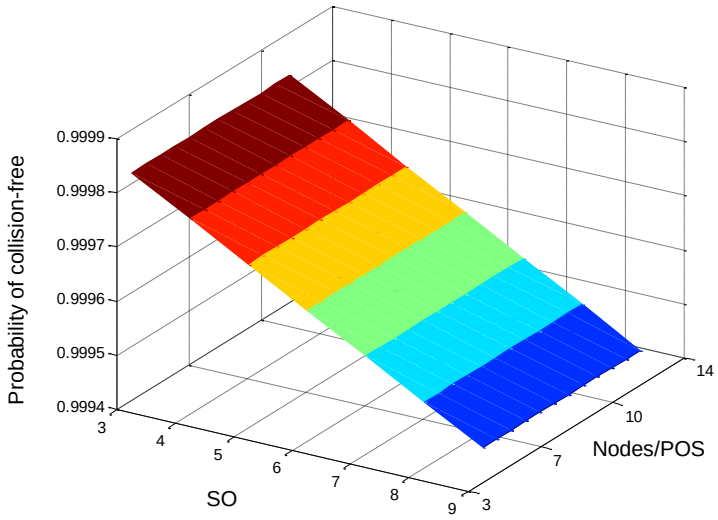


Fig. 4.16: Probability of collision-free (MUCBR)

Regarding the required time to initialize the nodes into the correspondent architecture (clusters, tree, etc.), Fig. 4.17 demonstrates the actual required time to setup the nodes into the designated structure. The RIME has the highest initialization time as compared with MUCBR and RPL while the RPL manages to show less setup time as the number of nodes increased.

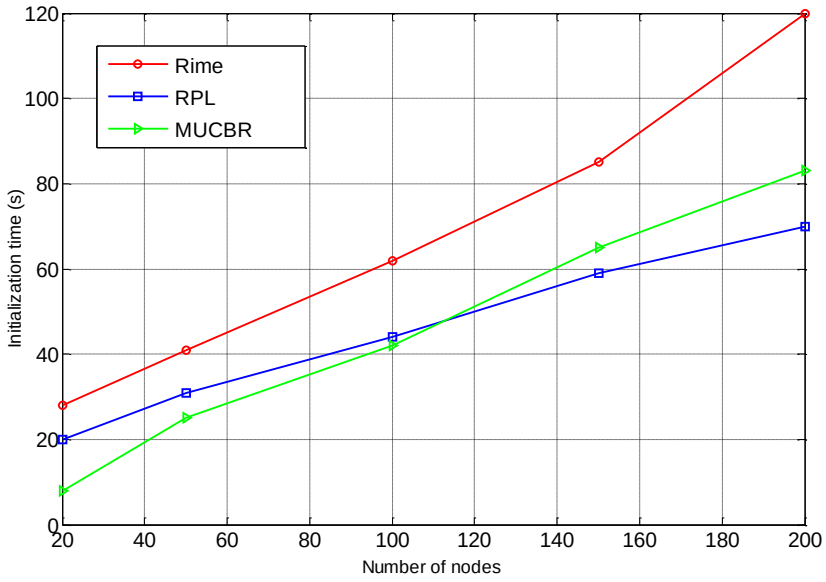


Fig. 4.17: Cost in terms of initialization latency

The RPL mechanism, which is based on building the DODAG tree, shows better network initialization process by which it requires less energy consumption (little communication overhead) and a minimal routes setup time. However, eventually this has an insignificant impact on reducing the total energy overhead of the RPL that is mainly caused by routing through the network layer as depicted earlier. In the meantime, the MUCBR has the lowest initialization time but increasing the number of nodes above 120 will lead to degrade the initialization process as the time windows (Fig. 4.4) need to be enlarged to ensure efficient frame commands forwarding to the deepest node in the network.

Regarding the latency issue and the difference between the MUCBR and both RIME and RPL, the following analyses will show the variations between both sampling and scheduling methodologies. The sampling technique is basically determined by the check interval period (section 2.2 and Fig. 2.3) and the probability of collision caused by undefined synchronization strategy between the nodes. As discussed in chapter two, the check interval rate has an impact on the latency since by increasing this interval (to reduce the RDC), data latency will be maximized.

Fig. 4.18 shows how the latency increases with the RIME as the check interval is maximized to 500ms. By increasing the number of transmitted frames (to 100) and check interval to 500ms, the latency has reached 1.21s.

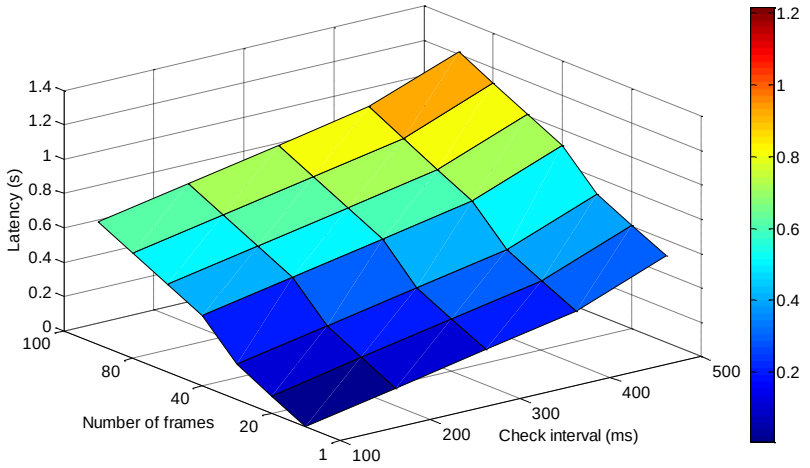


Fig. 4.18: Impact of check interval rate on RIME

In the meantime, for the RPL protocol, since the routing is determined by the network layer and the header has increased to accommodate the IPv6 packet information, the latency has slightly increased and reached 1.36s for the same previous check interval rate and number of frames, depicted in Fig. 4.19.

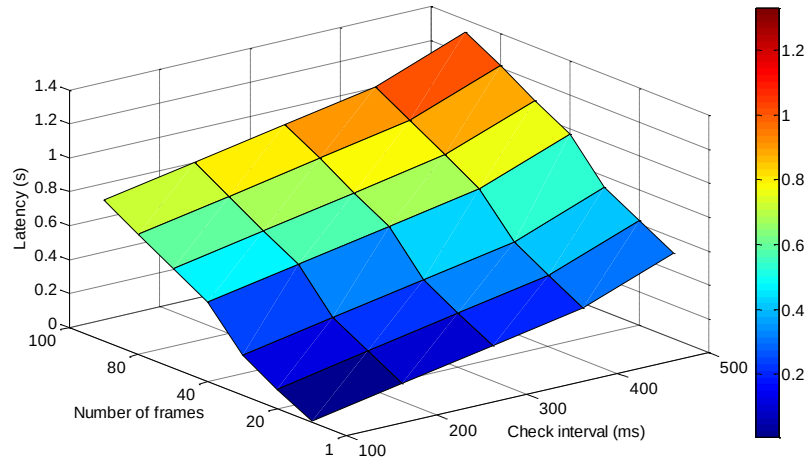


Fig. 4.19: Impact of check interval rate on RPL

The analytical results have showed a close outcome to the simulation results as shown in Fig. 4.20. For the MUCBR, the difference between the results is influenced by the mismatching between the nodes' clock timings. Although the implementation of the MUCBR within the Contiki OS has utilized the *rtimer* ticking rather than the Clock_time() library (to ensure a tight synchronizations), for several occasions there has been a small clock drifting that led to vary the latency.

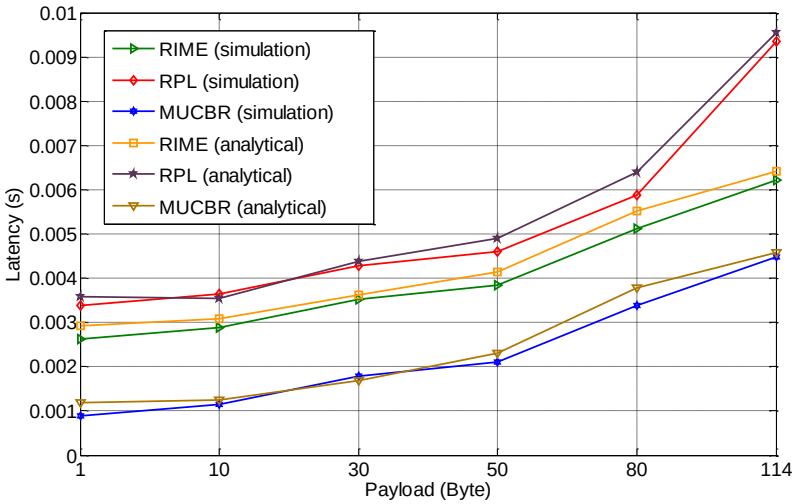


Fig. 4.20: RIME, RPL and MUCBR latency impact

On the other hand, for both RIME and RPL, the probability of successful transmission is varying for each hop as the number of contending nodes is changing which has produced multiple margins of differences between both analytical and simulation results.

Comparing the performance of MUCBR with RIME and RPL, the data latency has dramatically been reduced especially with the case of one-hop network. This traced to the independency on parameters that degrade latency as CSMA/CA, check interval rate or probability of successful transmission. For both RIME and RPL, three successful transmission probability scenarios have been considered, 1, 0.8 and 0.5 as seen in Fig. 4.21.

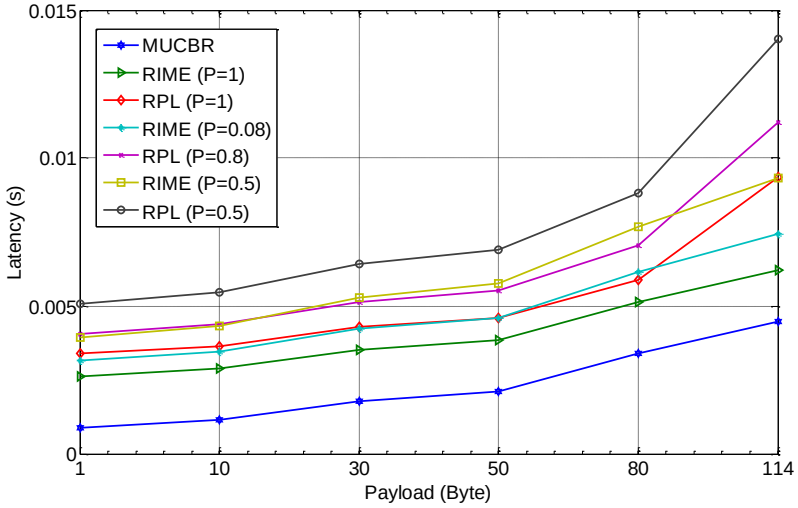


Fig. 4.21: Latency overhead for one-hop network

Meanwhile, MUCBR performance starts degrading once the number of hops is increased as indicated in Fig. 4.22.

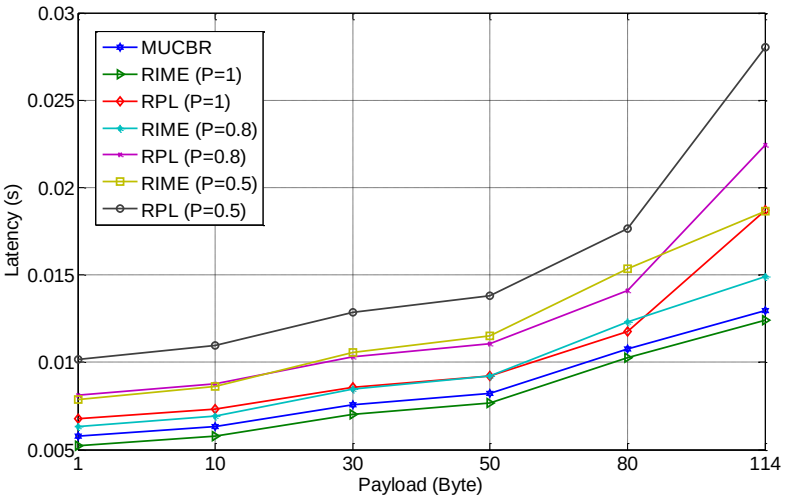


Fig. 4.22: Latency overhead for two-hop network

This is caused by the delay, encountered in the relay node, to collect the readings from all child nodes prior forwarding data to the sink node. By increasing the number of hops to three (as in Fig. 4.23), the RIME (with both cases of successful transmission probabilities, for 1 and 0.8) has showed to have less latency as compared to MUCBR. Even the RPL (probability of 1) shows better performance for payloads with 80 bytes and below.

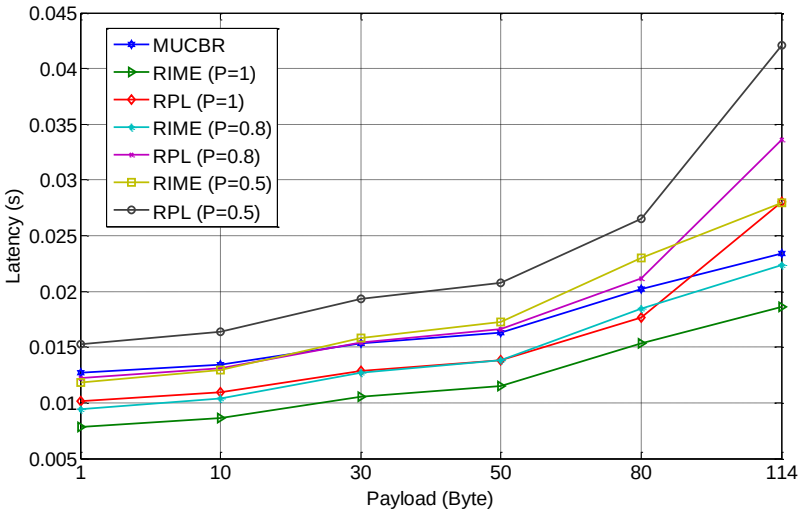


Fig. 4.23: Latency overhead for three-hop network

The same performance is realized as increasing the number of hops to four (presented in Fig. 4.24).

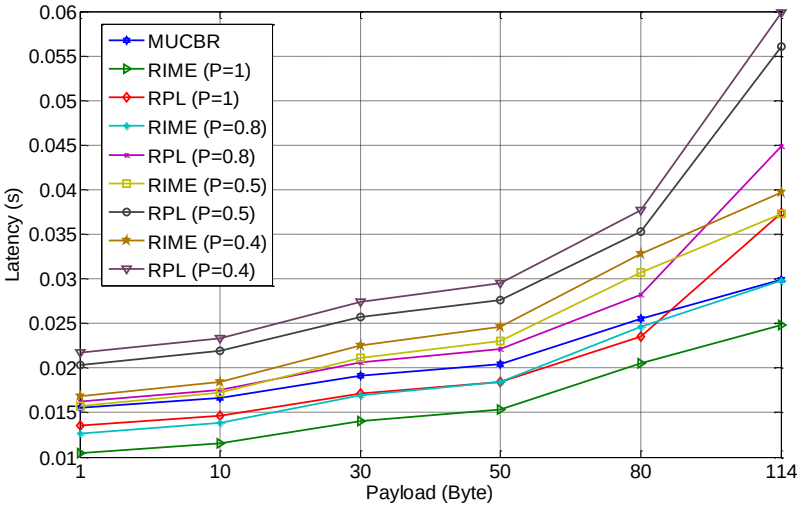


Fig. 4.24: Latency overhead for four-hop network

For this scenario, majority of transmissions will encounter a cumulated collision probability of more than 0.6, especially with the case of having a successful transmission probability of less than 0.74 at each hop.

Basically, for three hops and more, it will be difficult to realize a network with a cumulated probability of successful transmission of 0.8 or more. On the other hand,

due to both tight synchronization and slot randomness of the MUCBR, there was no collision encountered during the steady state of the network.

4.9 Summary

The proposed MUCBR protocol presents a mush-under routing technique that utilizes the clustering topology principle in order to divide the network into CH nodes and non-CH nodes. Therefore, the RDC has been minimized by allocating the nodes in each cluster with random time references instead of time slots to communicate with the CH and in turn route the data to the sink (utilizing the shortest path through CHs). In addition, routing within the link layer has a real advantage in terms of energy consumption that could be utilized for applications that require a timely-event based data aggregation within a single LoWPAN. The proposed MUCBR manages to provide 0.08% RDC for non-CH nodes and 1.3% RDC for CH nodes with timely-based transmissions of one message every two seconds and CHs with an average of three members.

Furthermore, the randomness of the time references which are allocated to the members in each cluster reduces both the inter-cluster and intra-cluster interference with an appropriate value of T_P and with respect to node density. Thus, the collision impact has been reduced by 40% as compared to IEEE 802.15.4. Finally, the MUCBR CH election scheme provides a chain of connected CHs via a single-hop link and eliminates the need for a bridge node to connect two adjacent clusters and ensure connectivity to the sink through the shortest path.

The MUCBR provided a reliable network initialization scheme that efficiently arranges the nodes into clusters and facilitates the adaptation of operating modes as TSCH and LLDN. Accordingly, the next chapter focuses on the issue of mobility under the TSCH mode which can be easily deployed based on the network topology that constructed through MUCBR.

Chapter 5. Mobility Aware Scheme for IEEE 802.15.4e Timeslotted Channel Hopping Mode

Realization of the IoT concept needs to be addressed by standardization efforts that will shape the infrastructure of the networks. Although these standards provide a coherent and diffused system, several implications challenge these standards to achieve optimal performance and reliability. Node mobility can be considered as the delimited factor for realizing a fully connected network, especially with the inclusion of TSCH mode that will complicate the association process of the mobile nodes, as a result of the frequency hopping mechanism. In this chapter, the impact of mobility over the TSCH sensor network has been investigated and a Markov chain model is presented to determine the parameters that affect mobile node association process. Secondly, a proposed mobility-aware MTSCH protocol is introduced which facilitates the mobile nodes association and minimizes the latency incurred by leaving the nodes dissociated from the network.

5.1 Mobility Issue in TSCH mode

With all mobility-related issues discussed earlier in chapter three and with the lack of a defined approach that can be standardized for the IoT cloud, TSCH complicates the case of mobility by introducing the concept of channel hopping. The diversity of frequency channels will let the EBs be advertised on several channels and thus, the mobile nodes have to deduce on which channel the EB is being broadcast.

This research has identified several issues in the TSCH mode and in order to support mobility, the IEEE 802.15.4 TSCH mode must provide the following services:

1) The mobile nodes must be able to determine the frequency channel that EBs are being advertised on. Thus, minimizing the waiting time for association and reducing the packet loss rate.
2) Since the standard does not indicate how the TSCH network should be

constructed [98, 116], the TSCH must provide an approach that defines how the EBs will be broadcast; which nodes broadcast and when to broadcast (period of transmission).

3) The TSCH has to define an allocation scheme by which the nodes will have dedicated links. For two adjacent FFDs' personal operating space (or clusters) that have the same channel offset, the absolute slot number (ASN) sequence values will be the same and thus, the links will collide. This issue has to be considered by the allocation scheme.

4) The IE must indicate any alteration that might occur in the slotframe structure which is caused by deletion/ addition of new nodes that leave/join the FFD.

5) Define the periodicity of EBs broadcasting to ensure fast scanning process while not compromising the energy consumption. The mobile nodes rely on the EBs to identify the existence of a coordinator and start association process to reconnect to the network. By increasing the number of advertised EBs, the mobile nodes will easily identify the existence of coordinator and then associate and synchronize with the network smoothly. In accordance, the coordinator will suffer from high energy consumption due to excessive EBs transmissions that required to facilitate nodes association. In the meantime, the coordinators must ensure that increasing the number of advertised beacons has less impact on energy consumption or collisions with other overlapped advertised EBs from adjacent coordinators. Therefore, a tradeoff mechanism must be existed to differentiate between either achieving better mobile nodes connectivity and high energy consumption, or low connectivity with less energy consumption.

5.2 Related work

The related work can be classified into two fields, the mobility within IEEE 802.15.4 and the TSCH structure. There is a lack of effort towards investigating the mobility issue for TSCH. Regarding the mobility, a work by the IETF [117], is considering the existence of mobile nodes and is targeting the RPL routing protocol,

but there is no valid mobility management approach presented that can tackle the channel hopping issue. In the meantime, the architecture of the IPv6 over the TSCH [118] assumes the existence of mobile nodes, but left this issue to the RPL, where there is no clear mobility management protocol presented as mentioned earlier. Similarly, several contributions are presented towards the mobility within IEEE 802.15.4 beacon-enabled and beaconless modes such as [51-55] or introducing cross layer approaches as in [119]. Hence, there is no mobility management protocol dedicated for the IEEE 802.15.4e TSCH.

In this section, the current contributions that are dedicated solely for optimizing the TSCH infrastructure are examined.

Duglielmo *et al.* [120] investigate the problem of not defining an advertising algorithm by the IEEE 802.15.4e standard, hence the authors present a random-based advertisement algorithm. Accordingly, they investigate the impact of the number of channels used by advertisers over the joining time for a node seeking to associate a TSCH network. The random-based advertisement model is, according to the authors, derived from [121]. The presented model aims to reduce the impact of collisions caused by advertising two or more EBs on the same link and thus, each advertiser will commence broadcasting EBs based on a probability (P_{eb}) that is derived locally according to specific network conditions (i.e., the number of neighbors). In turn, this technique will minimize the probability of collision since each advertiser has different P_{eb}. Vilajosana *et al.* [122] model the energy consumption of the TSCH network and provide an experimental validation based on nodes running the OpenWSN [121]. The paper provides analyses of the overhead for both the scheduling process and control signal on energy consumption. The analyses are based on classifying the source of energy consumption for each slot type: Rx, Tx, off and idle listening slots. The experimental validations are performed on two types of hardware, GINA and OpenMote-STM32 platforms.

Stanislowski *et al.* [99] emphasize the problem of clock-drift and its impact on the TSCH network that requires tight synchronization between communicating nodes. The authors present an adaptive synchronization technique that permits each node to calculate with neighbors its clock drift and based on the information, each node will periodically performs internal rectification to track its neighbor's drift. This

mitigates the desynchronization problem effect on the communicating nodes. The analyses were based on the GINA mote platform and running OpenWSN stack.

Jianwei *et al.* [123] investigate the performance of both the TSCH and CSL techniques and compared between them regarding the energy consumption and latency. The analyses, were based on nodes running the Contiki OS utilizing the MSP-EXP430 microcontroller and CC2520 transceiver. The results show that while the TSCH has less energy consumption than the SCL, the CSL has much less latency than TSCH.

Barcelo *et al.* [124] provide an extension to the 6TiSCH stack RPL routing in order to support node mobility utilizing a position-aware routing approach. The routing process is divided into two parts, default RPL routing among the static nodes and the proposed position-aware routing technique between mobile and static nodes. The static nodes, which are considered as the anchor points in this work, are location-aware nodes while the mobile nodes with unknown positions. The technique shows an improvement, over some of existed geographic routing algorithm, and robustness to positioning inaccuracies. In the meantime, the presented work did not alter the TSCH mode and keeps the issue of mobility unresolved.

Palattella *et al.* [125] present a traffic aware scheduling algorithm (TASA) that manages the distribution process of slots and channels to the nodes within the TSCH network. The TASA is a centralized approach and dedicated for static multihop network and targeting to achieve high parallel transmissions with a reduced number of channels. The process by which TASA allocates links is determined by two important factors, the network topology and data-traffic load. Hence, the objective is maximizing the throughput and minimizing latency. The presented work, which is an amendment to previous work for the authors in [126], shows how the TASA could be incorporated into the IoT stack.

XU *et al.* [127] introduce a delay-aware resource allocation (DARA) model which carry out a resource allocation service for multi-camera TSCH networks. The concept of resources in the TSCH network is interpreted in term of links. Unlike the previous works, which require cross-layer information to allocate resources, DARA requires only limited statistical information as a packet delay-deadline. The presented work ensures not to exceed the delay-deadline limit for transferring a

video while preserving video quality. This is achieved through providing a slot weighting mechanism which is dependent on the video coding technique, video content and specific application requirements. Moreover, it assigns each sensor node an index that follows some parameters. Based on the indexing, the sensor with the largest index will get the current timeslot. Hence, minimizing the delay and preserving video quality.

Peng *et al.* [128] present an adaptive TSCH (A-TSCH) that provides a blacklisting technique which selects the best channel with less interference to hop over. Hence, the channels with high noise will be eliminated from the channels hopping list. The A-TSCH has been analyzed and shows an improvement over the default TSCH.

5.3 Evaluation of the Mobility Impact on the TSCH Network

The association process in the TSCH network starts by scanning the available channels for advertised EBs. Although the channel hopping can be seen as an advantage by letting the EB be broadcast on a different channel in every period [129], but this will maximize the mobile waiting time to receive a valid EB. Once a node has received an EB, it will synchronize to the network based on the IE parameters. Then, the node should commence the association process, which is either the default association process depicted in [4] or the FastA approach presented in [1].

In this research, the terms CH, parent and coordinator will always have the same meaning and refer to FFD device. In a similar manner, the terms non-CH, mobile node and child are referring to RFD devices.

According to IEEE 802.15.4e, sending an association request is optional in the case of TSCH mode. Hence, to maintain synchronization, a mobile node can rely only on an advertised EB. Based on this approach, the FFD will be unaware of any mobile node seeking to join the network (cluster). On the other hand, to achieve full connectivity, FFD device has to be alerted (through association request) regarding a node wishes to join the network. The FFD task here is to provide the required resources for handling the new mobile node through allocating a dedicated link or

adding new SHARED TX link. To sum up, the association request can't be optional in TSCH mode.

The timeslots (links) in TSCH are classified into three types (identified via the link option field), TX link, RX link and SHARED TX link. For a node wishing to join FFD, it has to send its association request during a SHARED TX link and then receives the association information during the RX link or SHARED link. Hence, the association process is completely dependent on the existence of a SHARED TX link in a slotframe and whether this link is free or busy (occupied by an already exited member or accessed by another mobile node). In the presence of a SHARED TX link (linkoptions bitmap set shared transmission), the node performs a clear channel assessment to check whether the link is idle. In the case of CCA failure (or did not receive a valid acknowledgment), the node has to invoke the TSCH-CA backoff mechanism seeking to reduce the number of collisions that may occur. Unlike the CSMA-CA, the TSCH backoff [1] (presented in Fig. 5.1) waiting is determined in terms of shared links rather than the *aUnitBackoffPeroid*.

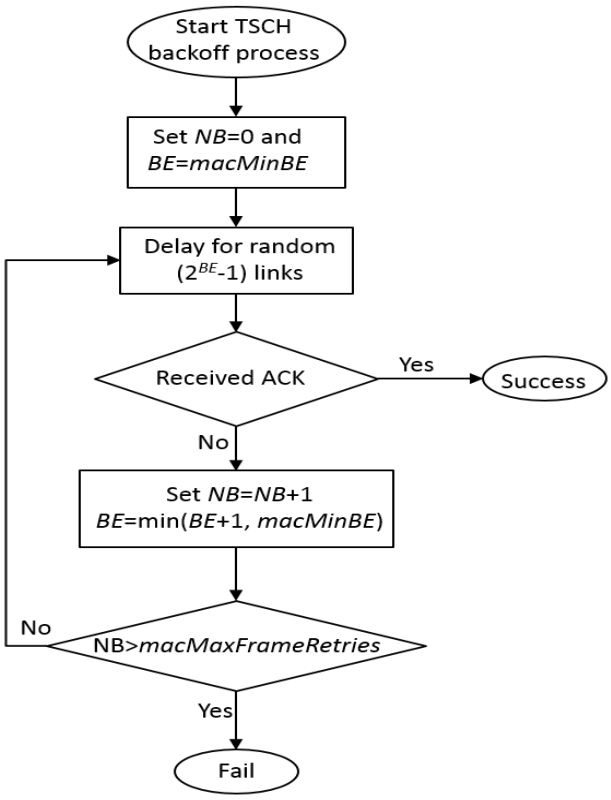


Fig. 5.1: TSCH CSMA-CA backoff process

So, each FFD must maintain an adequate number of shared slots that simulate the number of mobile nodes entering the POS of an FFD in a given slotframe period. Hence, the mobile nodes join the network immediately without any given delay. In order to determine whether a node will join a network or not, there must be an estimation to the time that a node will settle in a given POS and the required time to associate with an FFD. Fig 5.2 presents the possible trajectories that a mobile node may follow when entering a POS at a given point x.

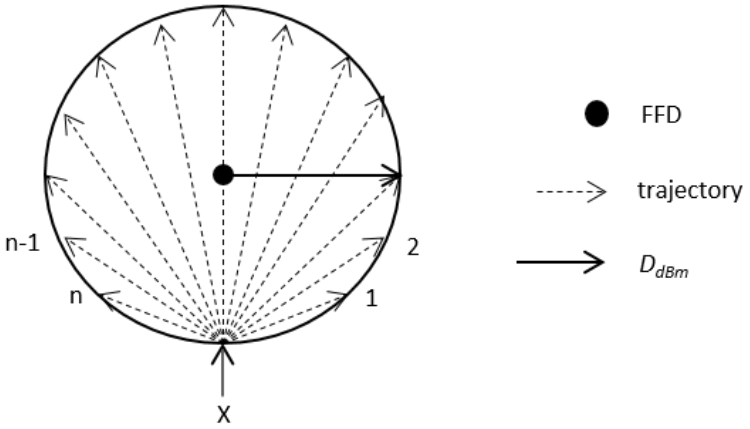


Fig. 5.2: Possible trajectories of a mobile node in a POS

The assumption here is that in each POS, a mobile node will move at a constant speed and direction. The probability of traveling in a given trajectory is 1/*n* and is uniformly distributed. Thus, the expected settle time T_s elapsed in a POS of a FFD that has a transmission range *R* at a given dBm is approximately given by (based on assuming straight line of movement):

$$T_s = \frac{\sum_n t_n}{n} \tag{5.1}$$

Where, *t* is the settle time of a given trajectory and *n* is the number of possible trajectories in a POS. ln the meantime, the analysis in this research does not depend on the expected settle time since the random waypoint model is incorporated as the default pattern of node movement in the network. In all simulation scenarios of this research, the trajectories are changing in a single POS and do not follow a straight line.

Expected settle time cannot be defined as the connectivity time to an FFD, since this time will be divided into two parts, the requesting association time (time required to associate with the FFD) and join time or associated time (time by which the nodes are connected and can transmit readings to the FFD).

The behavior of the TSCH can be modeled via a Markov chain that depicts the possible states a mobile node can encounter to join a TSCH network. The modeling is based on three fundamental stochastic processes {$sf(t)$, $tl(t)$, $s(t)$} which are the slotframe index $sf(t)$ (by which a node receives a valid beacon), the status of the timeslot $tl(t)$ and the status of the node $s(t)$. *sf* states ranges between [sf_i ,sf_{i_f}], where sf_i indicates the i^{th} slotframe that a mobile node receives a valid beacon and sf_{i_f} represents a slotframe that a mobile node fails to capture a beacon. sf_x denotes an arbitrary slotframe. The *tl* states varies between *AC, B,* nAc_1 (received an ACK message to the association request, timeslot is busy and no ACK message received). Invalid ACK message to an association request will trigger the TSCH backoff process and thus, the possible *tl* states may vary in the range [nAc_2, nAC_j], where *j* corresponds to *macMaxFrameRetries* value. Finally the *s* process has four possible states {*Or*, *A*, *R*, *J*} which are orphan (dissociated from the network), Accepted (association request has been accepted), Reject (association request has been rejected) and joined (mobile node has joined and synchronized with the network). Fig. 5.3 depicts the transition probabilities of the Markov chain model for the possible states within a TSCH network. The probability $P_{eb}(sf)$ of receiving at least one EB within a slotframe *sf* composed of *nTS* will follow a binomial distribution and is given by:

$$P_{eb}(sf) = \sum_{j=1}^{nTS} \binom{nTS}{j} \left(\frac{1}{F_{ch}}\right)^{j} \left(1 - \frac{1}{F_{ch}}\right)^{F_{ch}-j} \tag{5.2}$$

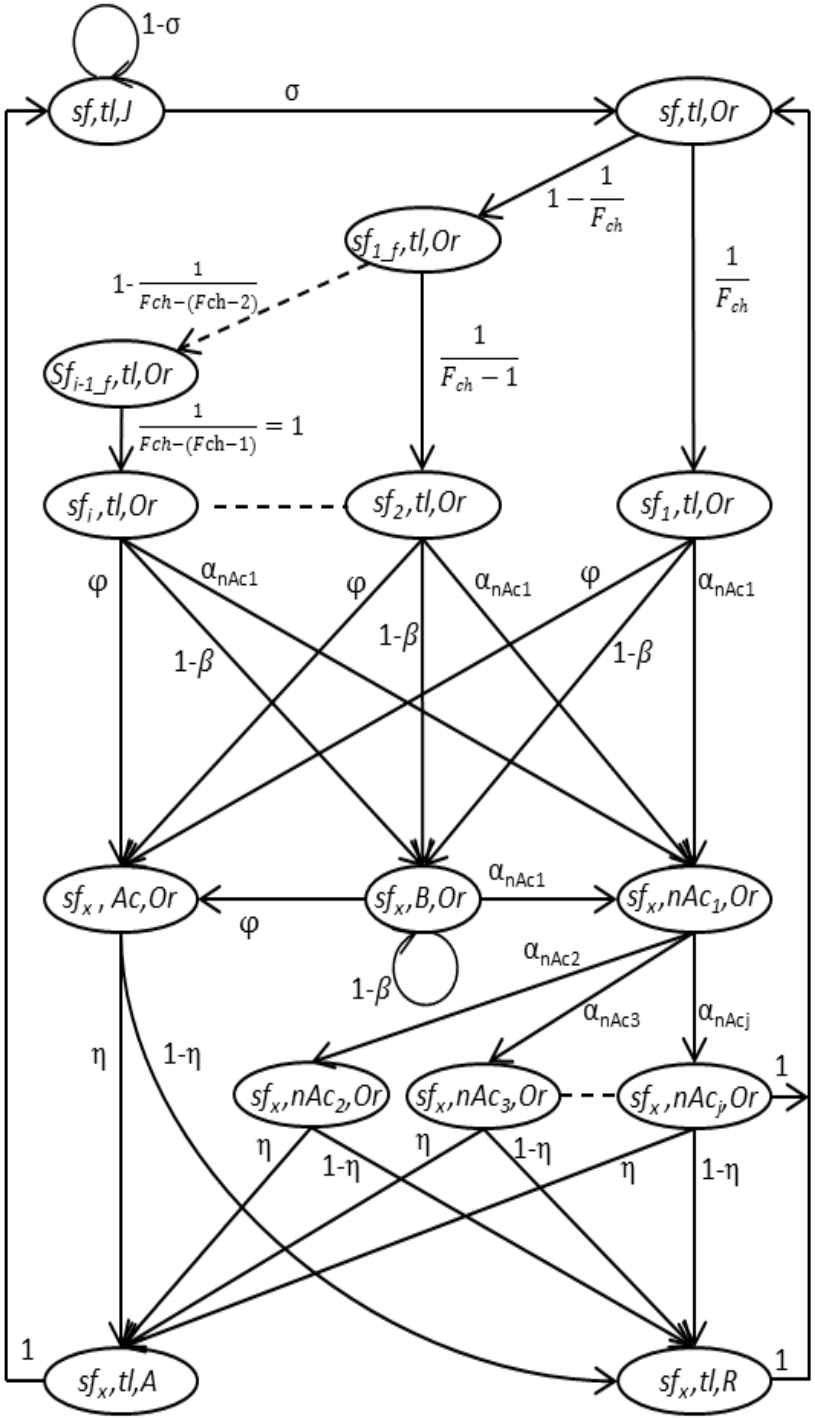


Fig. 5.3: Markov chain model for a mobile node in TSCH network

Where F_{ch} , is the number of available frequency channels that the TSCH hopped over. Moreover, with the case of a network where the mobile nodes require an association time larger than the settle time in a POS, the probability (P_{eb}) that a mobile node receives an EB in a given slot index (ts_n) is described in (5.3). Note

here, the difference between ts_n and ts_{n+1} is always dependent on the period of EB transmissions and the slotframe size (in links) where their maximum trial is i that correspond to the number of available frequency channels.

$$P_{(ts_n)} = \frac{\left(1 - \frac{1}{F_{ch}}\right)^{ts_n - 1}}{F_{ch}} \quad ts_n = 1,2,3, \ldots. \tag{5.3}$$

The sequence of which timeslot a mobile nodes receives an EB is not only contributing the delay by which a node can join a network, but also maximizes the RDC and hence, increase the energy consumption.

However, conducted simulations here verify that the mean settle time may always be larger than the required time for association.

$$T_s > T_{as} + T_{con} + T_{ma}$$

where T_{as} is the required time for a mobile node to associate with a coordinator once it receives an EB. T_{con} is the time where the status of the node is connected and T_{ma} is the time to indicate the node is disconnected due to missing ACK messages (which depends on the number of missed ACK messages to announce the node as orphan and start scanning for EBs).

Thus, the coordinator or CH may always complete its period of channel hopping while the node is in its POS. In turn, the transmitted EB may always be advertised on all the available frequency channels while a mobile node is in POS. Hence, the probability $P_{eb}(sf_i)$ that a mobile receives an EB on a specific frequency channel in a given slotframe i is:

$$P_{eb}(sf_i) = \frac{1}{F_{ch} - (i-1)} \cdot \prod_{z=0}^{i-2} \left(1 - \frac{1}{F_{ch} - z}\right), for\ i \neq 1 \tag{5.4}$$

The probability (σ) of leaving a POS is based on the position of a node regarding FFD position and whether it is moving inside or outside the POS:

$$\sigma = \begin{cases} \frac{R_{dBm} - D_{RSSI}}{2R_{dBm}}, & RSSI_{t+1} < RSSI_t \\ \frac{R_{dBm} + D_{RSSI}}{2R_{dBm}}, & RSSI_{t+1} > RSSI_t \end{cases} \quad (5.5)$$

Where, D_{RSSI} is the distance of the mobile node from an FFD based on the RSSI of the received ACK messages from the FFD. R_{dBm} is the maximum transmission range of FFD at a given dBm transmission power.

In order to address the probability (β) that a mobile node will gain a free SHARED TX link, there is a need to identify the relevant parameters that an FFD can provide, as: number of shared links *sh*, expected number of mobile nodes (E_m) entering a POS at a given *sf*, number of attached nodes (A_n) to the FFD (children, non-CH) and number of dedicated links (L_D).

$$\beta = \frac{sh}{E_m + (A_n - L_D)}, \quad \text{for } L_D \leq A_n \quad (5.6)$$

Moreover, the probability (φ) that a mobile node receives back an acknowledgement is:

$$\varphi = 1 - (\alpha_{nAc1} + (1 - \beta)) \quad (5.7)$$

In addition, the probability (η) that an FFD accepts an association request is dependent on the number of available time slots (ε) that an FFD can additionally allocate without compromising the node lifetime, $\overline{E_m}$ the mobile nodes that migrated out of the POS within the same *sf*, *Re* is the number of association requests and the channel error-free rate (θ).

$$\eta = \left(1 - \frac{Re}{\overline{E_m} + \varepsilon}\right) \theta \quad (5.8)$$

The transition probabilities of the possible states that a mobile node can encounter during the association process now can be easily derived. The probability of a SHARED TX slot being blocked is presented in (5.9) while the probability of a SHRED TX slot is free and the request has been sent correctly is indicated in (5.10).

$$P(sf_x, B, Or|sf, tl, Or) = \left[1 - \frac{sh}{E_m + (A_n - L_D)}\right] \left(\sum_{n=1}^{x} \frac{1}{F_{ch} - (n-1)} \cdot \prod_{z=0}^{n-2}\left(1 - \frac{1}{F_{ch} - z}\right) + 1\right) \quad (5.9)$$

$$P(sf_x, Ac, Or|sf, tl, Or) = \left(1 - \left(\alpha_{nAc1} + (1 - \beta)\right)\right) \left[\sum_{n=1}^{x} \frac{1}{F_{ch} - (n-1)} \cdot \prod_{z=0}^{n-2}\left(1 - \frac{1}{F_{ch} - z}\right) + 1\right] + P(sf_x, B, Or|sf, tl, Or) \quad (5.10)$$

In accordance, the probability of transmission failure within a SHARED TX slot is:

$$P(sf_x, nAc_1, Or|sf, tl, Or) = \alpha_{nAc1} \left(\sum_{n=1}^{x} \frac{1}{F_{ch} - (n-1)} \cdot \prod_{z=0}^{n-2}\left(1 - \frac{1}{F_{ch} - z}\right) + P(sf_x, B, Or|sf, tl, Or)\right) \quad (5.11)$$

Hence, the probability of failure to join after several backoff SHARED TX slots is:

$$P(sf_x, tl, R) \,|\, sf, tl, Or) = \left(1 - \left(1 - \frac{Re}{\overline{E_m} + \varepsilon}\right)\theta\right) \left[\sum_{l=1}^{j} P(sf_x, nAc_1, Or).\alpha_{nAcl} + P(sf_x, Ac, Or)\right] \quad (5.12)$$

Finally, the probability that a mobile node will join a network is indicated in (5.13):

$$P(sf_x, tl, J) = \eta \left(P(sf_x, Ac, Or) + \sum_{l=1}^{j} P(sf_x, nAc_1, Or).\alpha_{nAcl} \right) \quad (5.13)$$

Once a node gets into the *nAc* state, it will not return to *B* state since the FFD has a sufficient shared links. Thus, from states nAc_i, the node will either be directed to *j* or to *Or* states.

5.4 MTSCH Protocol for Mobile IoT Constrained Devices

The concept of the proposed MTSCH is basically dependent on embodying the practice of beaconing that is adapted in the default IEEE 802.15.4 beacon-enabled mode. Here, a novel passive beacons principle is presented by which the nodes can determine whether they have left a POS and to identify the presence of an FFD in a new area they have moved to. Therefore, the MTSCH relies on the ACK messages that an FFD replies to a node in order to validate a successful transmission. Hence, the ACK messages are acting as passive beacons which announce the presence of an FFD. Instead of obligating FFD nodes to reply for each transmission individually and to utilize the ACK message in the sake of acting as beacons, the ACK message of the TSCH is to be modified. Each FFD has to respond, at the end of each slotframe, only once to verify a successful transmission for all the members. This concept resembles the concept of group ACK used in LLDN mode. In addition, each ACK will indicate:

1. The time that a FFD will listen for any mobile node (radio is ON for receiving association requests).
2. The nodes that whose transmissions were correctly received.
3. Whether a modification has occurred in the cluster or not (due to join/leave a mobile node).

All the ACK messages will be transmitted on a fixed frequency channel (F_{ACK}) while omitting this channel from the *Frequency_List* that the TCSH network hopping over.

Hence, the mobile nodes that seek to join a network have to scan only one channel which will save time and energy. Moreover, the FFD has to reply only one ACK for all the members which will save energy by (*Et*):

$$Et = V \times I_{tra} \times \sum_{m=1}^{A_n - 1} (macTsMaxAck)_m \tag{5.14}$$

macTsMaxAck denotes the maximum transmission time of a single ACK message, *V* is transceiver supply voltage and I_{tra} is the transmission state current consumption.

Each slotframe gains extra free time g_t that contributes the additional resources which are affecting the number of mobile nodes that can be handled as in (5.6). g_t can be expressed as:

$$g_t = \sum_{m=1}^{A_n} (macTsRxOffset + macTsTxAckDelay + macTsMaxAck)_m \tag{5.15}$$

Where *macTsRxOffset* and *macTsTxAckDelay* are guarding times within a single timeslot and are defined by [1].

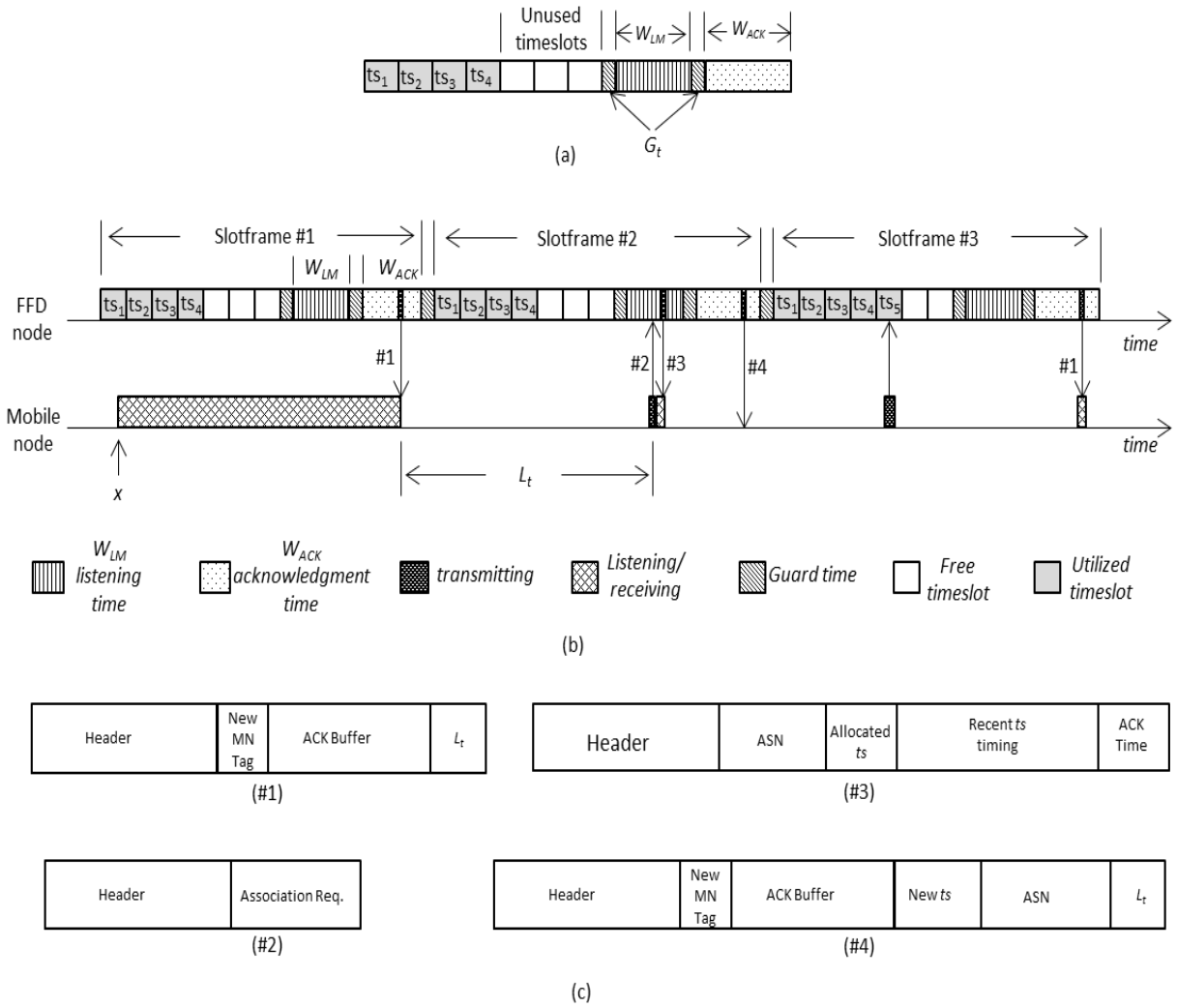


Fig. 5.4: MTSCH mechanism to accommodate mobile nodes

For a mobile node that determines it has been disconnected from the network (invalid ACK) at time *x* in Fig. 5.4, the node shall switch its radio ON and starts a passive scan for ACK messages on frequency channel F_{ACK} (message #1 in Fig. 5.4). Once the mobile node detected an ACK message, it will determine the L_t time that is presented in the last field of the ACK frame and corresponds to the time by which an FFD will switch its radio ON to listen for any association request from a mobile node. For MTSCH, the waiting time (w) of a mobile node seeking to join an FFD will be $0 < w \leq 2\ sf_D$. (sf_D denotes a single slotframe duration). Thus, with MTSCH, the mobile node can join an FFD with only two successive slotframes and commence sending readings within the third slotframe.

After time L_t, the mobile node transmits its association request and waits for time *tp* (time required by a device to respond to a request) and then receives the association reply (message #3) that identifies the synchronization parameters required for a mobile node to join a network. This message contains the ASN, allocated *ts* (by which the node can transmit its readings within a slotframe schedule), recent timing slots (in order to let the mobile node knows exactly when to increment the ASN and keeps its schedule synchronized with the network) and finally the ACK time which depicts the time by which the FFD will transmit its ACK message to the nodes.

The FFD node has to identify any change to the cluster by transmitting as usual the ACK, but this time alternative ACK format is proposed that comprises the new *ts* field and identifies *ts* timing of the new mobile node that joined the network. This will let the existed nodes in the POS (or cluster) to know exactly when to increment the ASN and prevent possible desynchronization.

The slotframe structure within TSCH is slightly altered by dividing the sf_D period into three parts. The first part is the usual timeslots part that composes dedicated links and SHARED TX links. The second part is called W_{LM} section which the FFD listens for association requests. The third piece is W_{ACK} part where the FFD sends an ACK message (passive beacon) by which the existing members (connected to FFD) determine whether their transmissions were successfully received. Each FFD will pick up a random time (T_{LM}) within W_{LM} to open its radio ON for small duration of time and listen to any association request. In the same way, each FFD selects a random time (T_{ACK}) within W_{ACK} period to transmit the ACK message. The last field of each broadcast ACK message is always containing L_t, that is:

$$L_t = (sf_D - T_{ACK}) + T_{LM} \tag{5.16}$$

Dependency on randomization within a predefined time window shows improved performance by reducing the probability of collision and this has been demonstrated in [130].

The mobile node can also keep its radio ON within L_t to determine if there is any other FFD beaconing with higher RSSI to ensure more settle time.

Fig. 5.5 shows the flow chart that demonstrates the tasks for both of an FFD device and a mobile node in the TSCH network. Finally, the mobile node is able to start transmitting readings at the allocated timeslot. Including the timings in message #3 and #4 rather than the number of nodes can be seen here as an obligatory task, since there is a case that an FFD has to assign a *ts* which has been released by a node that migrated the cluster, like *ts* 1 or 2 or 3 as in Fig. 5.4. Hence, the nodes here in the cluster (POS) will increment the ASN each time new *ts* is started.

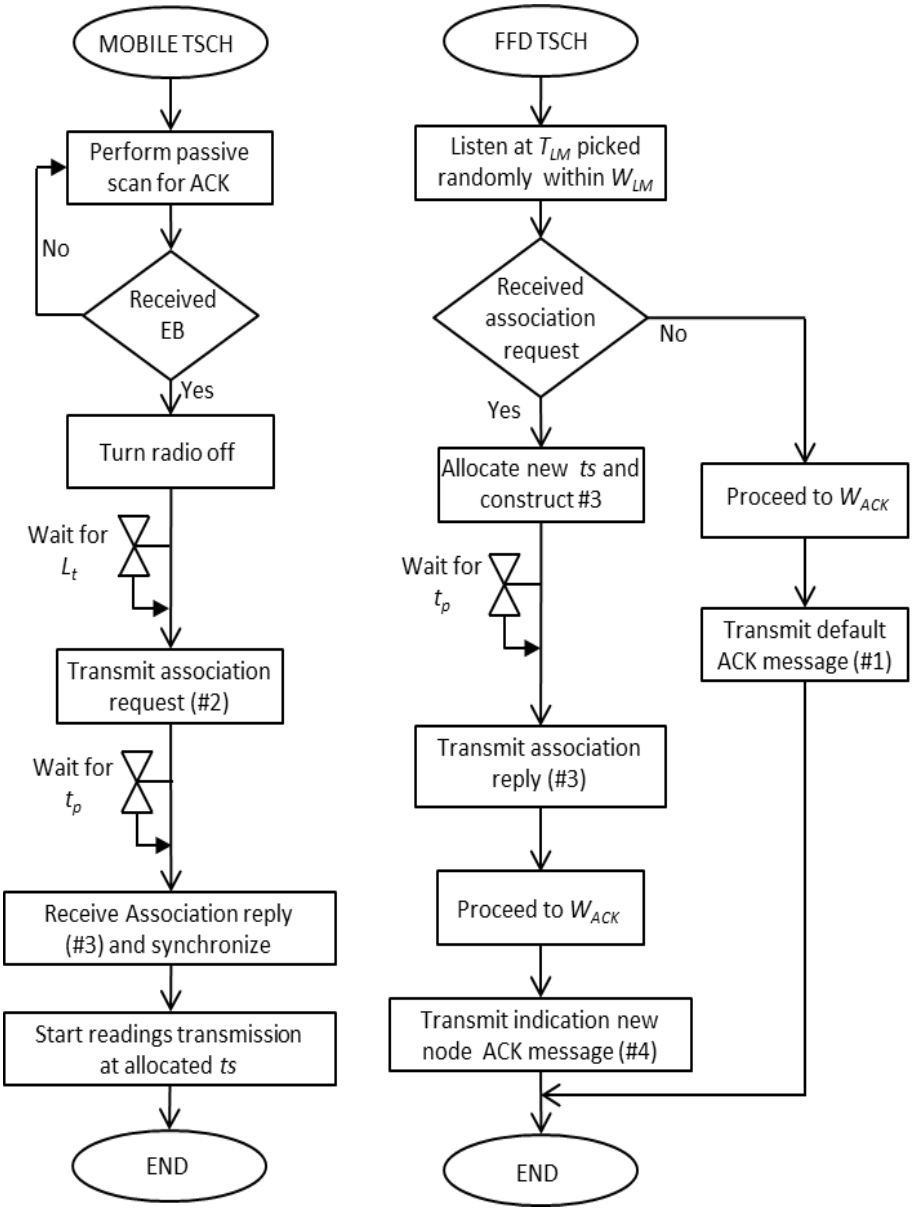


Fig. 5.5: Handling association flowchart for FFD and RFD

5.5 Implementation and Analysis

The analysis will emphasize three important aspects that determine the network lifetime and availability, these are: RDC, energy and association time (the total time that a mobile was connected to the network).

In order to observe the real performance for both TSCH mode and the proposed MTSCH scheme, the two models are implemented within the Contiki OS and simulated through Cooja network simulator [131].

The test-bed platform for each sensor node is composed of the MSP430 microcontroller and CC2420 transceiver. Different scenarios have been adapted in the simulation process to investigate the impact for each number of mobile nodes, slotframe interval (EB period) and transmission range. Powertrace tool [114] has been utilized to assess the performance of the two models. In addition, since the periodic transmission is considered to be more substantial for determining applications [39], the nodes are programmed to transmit periodically based on the slotframe duration.

Several deployments are considered within the Contiki OS implementation. These deployments are changing each time by varying the number of mobile nodes (*mn*), transmission range of the nodes (for both of CH and Non-CH) and slotframe duration sf_D. Moreover, in order to handle mobility, both TSCH and MTSCH are configured to accommodate only a single association request in each slotframe. Hence, the TSCH has a single SHARED TX slot in each slotframe while the MTSCH will respond only to a single request per slotframe.

In order to assure that advertised EBs are hopping over the entire frequency channels sequence. Either the number of timeslots within a slotframe should set to be prime [129], or the number of frequency channels F_{ch} should also set to be prime [126]. Therefore, seeking to guarantee that EBs are broadcast over the whole channels sequence and since the number of links within a slotframe can't be adjusted due to mobility, the number of utilized frequency channels in the available frequency hopping list F_{ch} is set to 13.

The simulation of node movements is based on the random waypoint mobility that resembles the random walk mobility model while including pauses time metric to the model. Other different mobility models as Exponential Correlated Random Mobility model, Nomadic Community Mobility Model, Reference Point Group Mobility Model and Pursue Mobility Model also can be exploited but are dedicated for group mobility scenarios where the decision of node movement is based according to other nodes in the group [18], which is not related to the designated applications addressed in this research. Accordingly, the random waypoint has been adapted in this research and implemented within the Contiki OS to mimic the movements of mobile nodes.

Before investigating the overhead of mobility over the TSCH network, the performance of TSCH regarding static nodes have to be evaluated to show how clearly the mobility can degrade nodes' performance. Fig. 5.6 presents a simple example of the real outstanding performance of a TSCH network regarding static nodes.

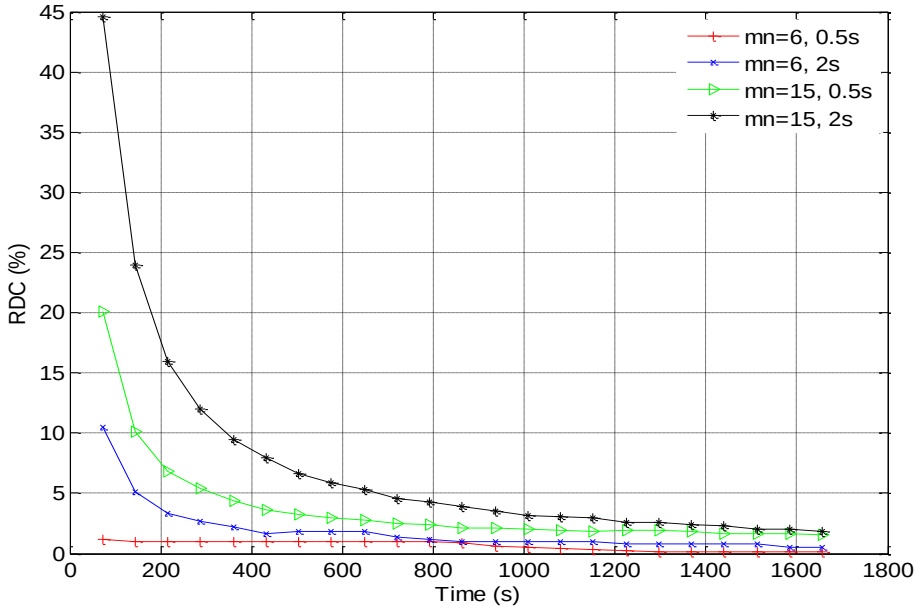


Fig. 5.6: RDC of static TSCH network

The average RDC for *mn*=6 and sf_D =0.5s is 0.56% and for sf_D =2s is 1.15%. Here, the RDC is representing the average radio operating time over the node running

time. Increasing the number of mobile nodes maximizes the RDC during the initialization of the network. This incurred delay is caused by the contention activity of the CSMA process.

In the meantime, for long *sf* durations (less number of transmissions) there will be high RDC only during the initialization of the network that is caused by maximizing the waiting time for a valid EB (long intervals between consecutive EBs). Meanwhile, the accumulative RDC drops down after a period of operation to achieve less RDC values for long *sf* periods. Fig. 5.7 depicts the RDC for both of MTSCH (labeled M) and TSCH (labeled T) regarding six mobile nodes and at a transmission range of 50m. On average, the RDC of TSCH is 13% for slotframe duration sf_D of 0.5s and increasing while maximizing sf_D to reach 44% for 2s. This due to the impact of maximizing the sf_D duration that increases the waiting time for the mobile node to receive an EB, whereas the RDC is supposed to be decreased due to maximizing the transmissions interval.

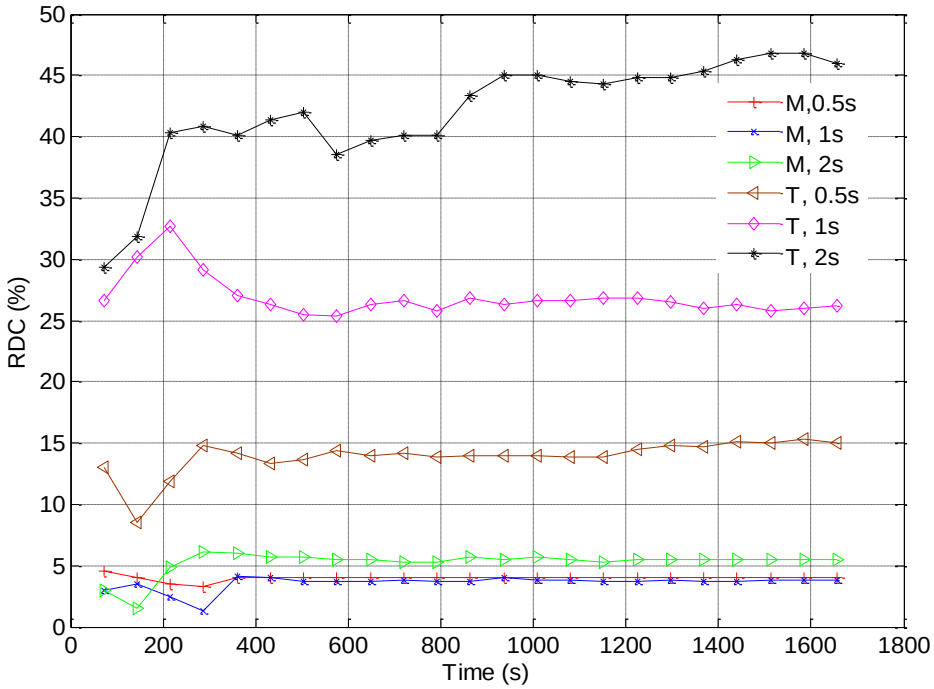
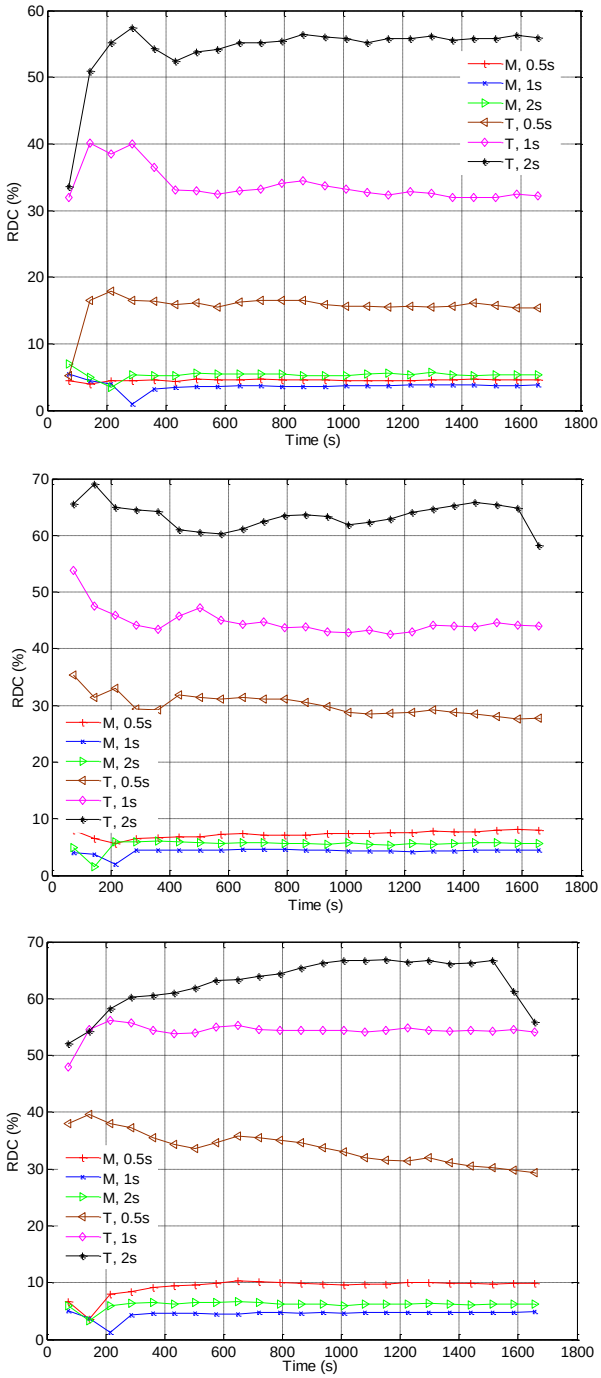


Fig. 5.7: RDC for non-CH nodes with range=50m, *mn*=6

On the other side, the MTSCH has an RDC of 4% for sf_D of 0.5s and 3.6% for sf_D =1s. In case of sf_D is 2s, although the RDC must be reduced, the RDC has raised to 5.5% since the waiting time for a valid EB has a greater impact on the RDC than the

effect of increasing the transmission intervals. This case has been repeated with other scenarios as in Fig 5.8 (a), (b) and (c). Accordingly with TSCH, the RDC is increasing each time the sf_D or *mn* is increasing. While with MTSCH case, the RDC is decreased when maximizing sf_D to 1s and raised when sf_D is increased to 2s whenever the *mn* is maximized.



(a)

mn= 9

(b)

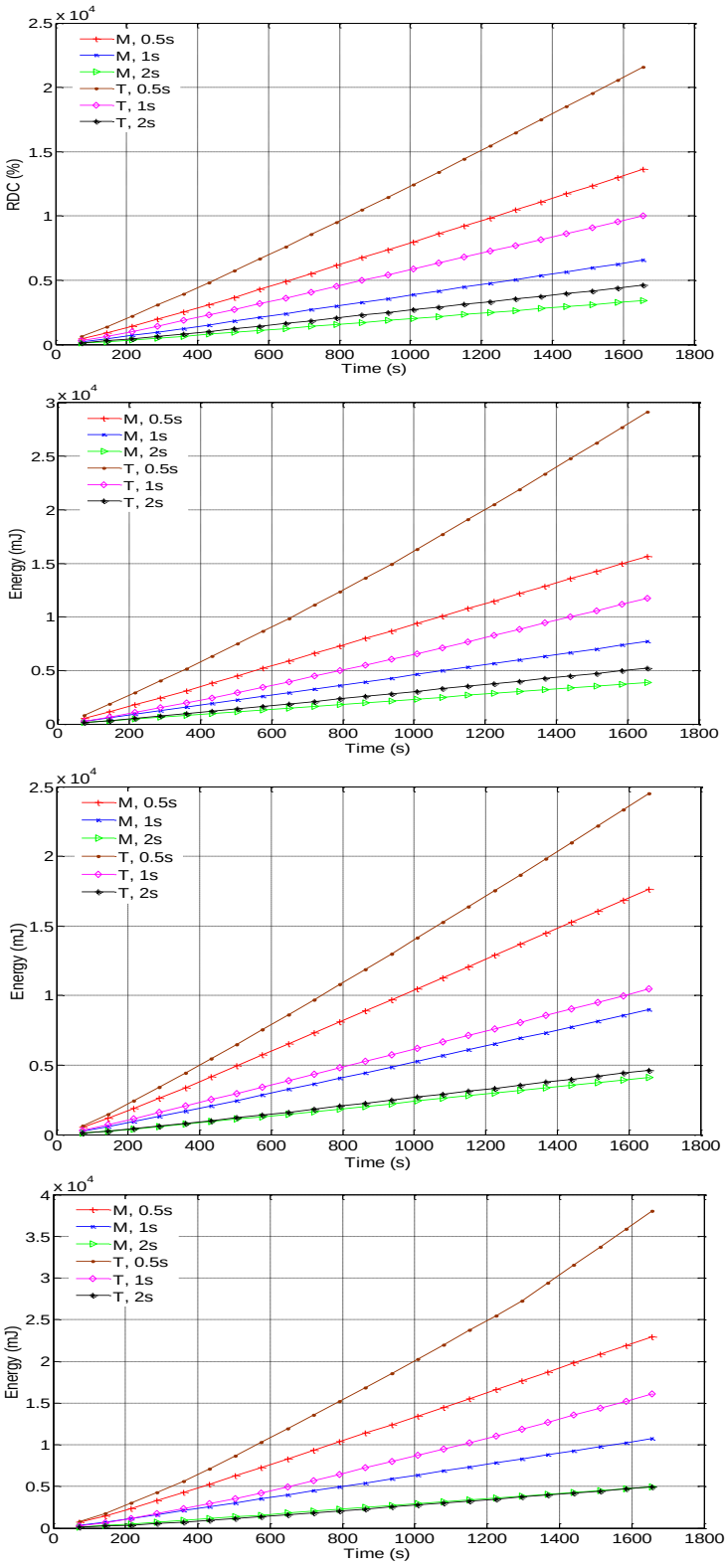
mn= 12

(c)

mn=15

Fig. 5.8: RDC for non-CH nodes with range=50m

Looking to the FFD (CH) side, the MTSCH also managed to reduce the RDC of FFD devices due to relying on a single ACK for all the nodes within the POS rather than individual ACK for each member. The FFD within MTSCH spent 13,620 mJ after running for 1,700s, sf_D =0.5s and mn=9 and range 50m (Fig. 5.9 (a)). In accordance, the FFD within TSCH consumed 21,594 mJ for the same period of running time and simulation parameters. By increasing the number of mobile nodes, the MTSCH performed slightly better than TSCH, where it consumes 49,199mJ against 49,257mJ for TSCH regarding 15 nodes, sf_D =1s and range 100m (Fig. 5.9 (d)). Thus, the greater impact of the MTSCH, regarding FFD, will be achieved when increasing the number of EB announcements (shortening sf_D). The MTSCH manages to gain this advantage due to the utilization of the ACK messages as passive beacons. This in turn has omitted the EBs and their overhead, which is also can be deduced through (5.14).



(a) *mn*= 9, range=50

(b) *mn*= 9, range=100

(c) *mn*= 15, range=50m

(d) *mn*= 15, range=100m

Fig. 5.9: Energy consumption of CH nodes

Referring to the total energy consumption of all transceivers' states, the non-CH nodes of TSCH have consumed 26,578mJ for *mn*=6, sf_D =1s and at a transmission range of 50m (Fig. 5.10 (a)). Similarly the MTSCH has depleted 4,207mJ when increasing the sf_D to 2s (Fig. 5.10 (b)), the TSCH has a total of 46,423mJ while MTSCH has spent 6,105mJ. The next step is to increase the transmission range and determine the impact, which is set to 70m, the TSCH incurred 12,612mJ for sf_D =1s while MTSCH is 2,998mJ. Maximizing sf_D to 2s, led to increase the energy consumption for both of the models, where the TSCH consumed 25,936mJ and MTSCH 4,120mJ. The final selected range of transmission is 100m, where the energy consumption is dramatically reduced as compared to 50m transmission range.

The energy consumption of TSCH has been reduced to 12,306mJ in the case of sf_D =1 and to 23,201 for sf_D =2 (Fig. 5.10 (c)). In addition, MTSCH minimized it consumption to 2,355mJ for sf_D =1s and to 2,624mJ for sf_D =2s (Fig. 5.10 (d)). Its notable here that by increasing the transmission range the energy consumption is reduced. Extending the coverage area POS of FFD devices will increase the connectivity and thus, less dissociations form the network. The energy consumption of TSCH is gradually increased by extending sf_D while MTSCH has a similar behaviour as in Fig.5.7 and Fig. 5.8. Here the energy consumption of scanning for EBs has a higher impact than increasing the periodicity of transmitting readings.

It's clear how the mobility has a great overhead upon the TSCH network and how it increases the RDC and energy consumption. Back to Fig. 5.6, the average RDC for *mn*=6 and sf_D =0.5s is 0.56% and for sf_D =2s is 1.15%. Hence, the RDC has jumped from 0.56% and 1.15% to 13% and 44% for sf_D =0.5s and sf_D =2s respectively.

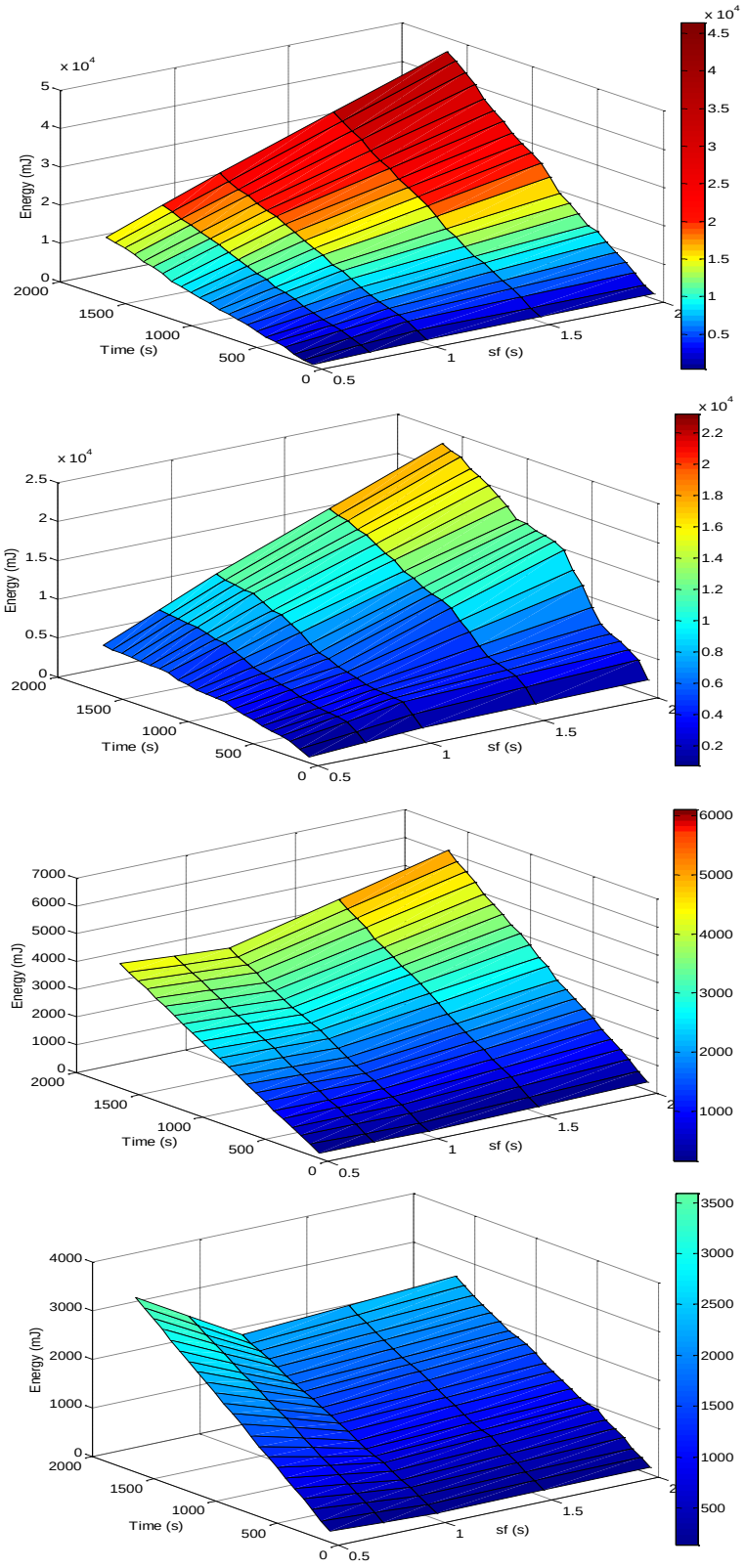


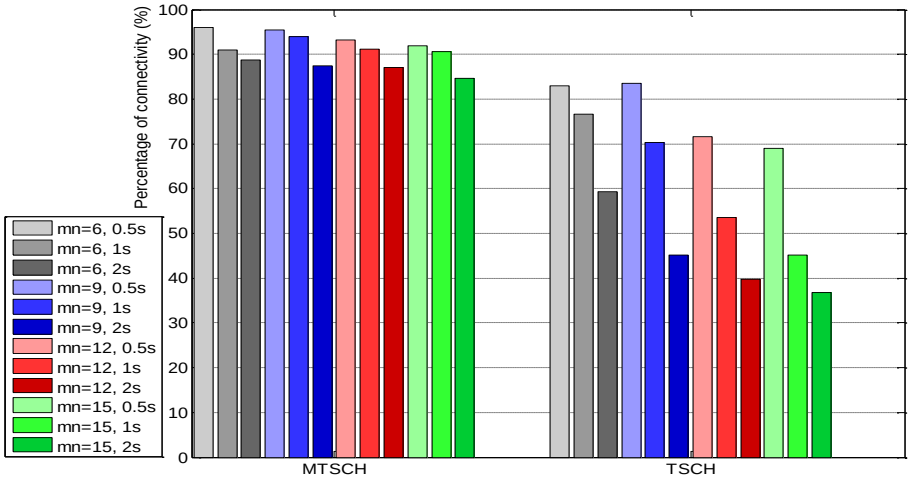
Fig. 5.10: Energy consumption of non-CH nodes, *mn*=6

The third important part that has been evaluated is the associated time (connected time), by which the total amount of time that a mobile node was connected since deployment. By maximizing the associated time, both the availability and packet delivery ratio will be increased.

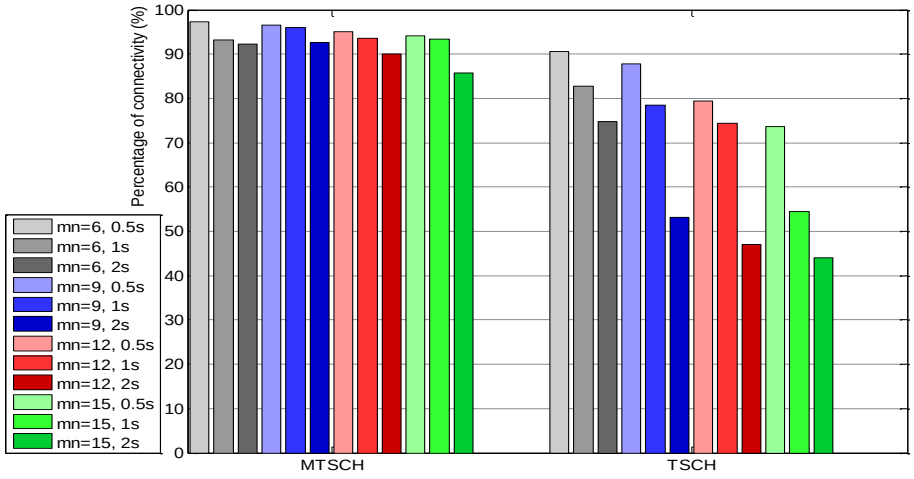
To shed light on this part, Fig. 5.11 indicates the percentage of associated time for each network scenario. It can be seen that the MTSCH improved the connectivity from 82.9% to 95.9% for *mn*=6 and sf_D =0.5s and at range of 50m. Fixing to the same range, MTSCH raises the connectivity from 69% to 91.9% and from 36.7% to 84.7% for sf_D =0.5s and sf_D =2s respectively, each with *mn*=15 nodes.

Meanwhile, by shifting the transmission range to 70m, the TSCH has a percentage of connectivity equal to 90.6% and MTSCH lifts it up to 97.3% for *mn*=6 and *sf*=0.5s. Similarly, increasing *mn* to 15 with *sf*=2s, TSCH has 43.9% connectivity while MTSCH managed to achieves 85.7% of connectivity.

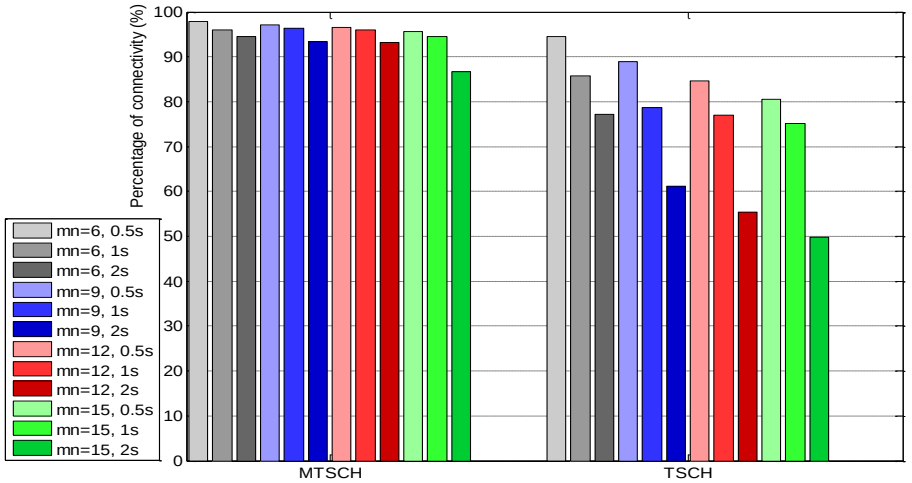
The association time faces a severe degradation in the default TSCH which is originally affected by the amount of time that a node is spending on scanning. A mobile node first is waiting for amount of time to indicate whether it has left a POS and this process is based on either missed beacons or receives no ACK messages. Then, a mobile node consumes time to allocate a beacon on one of the available 16 frequency channels. Lastly, contending with other mobile nodes seeking to join the same coordinator which in turn can force the node to wait for extra time until it determines a free SHARED TX slot.



(a) Range=50m



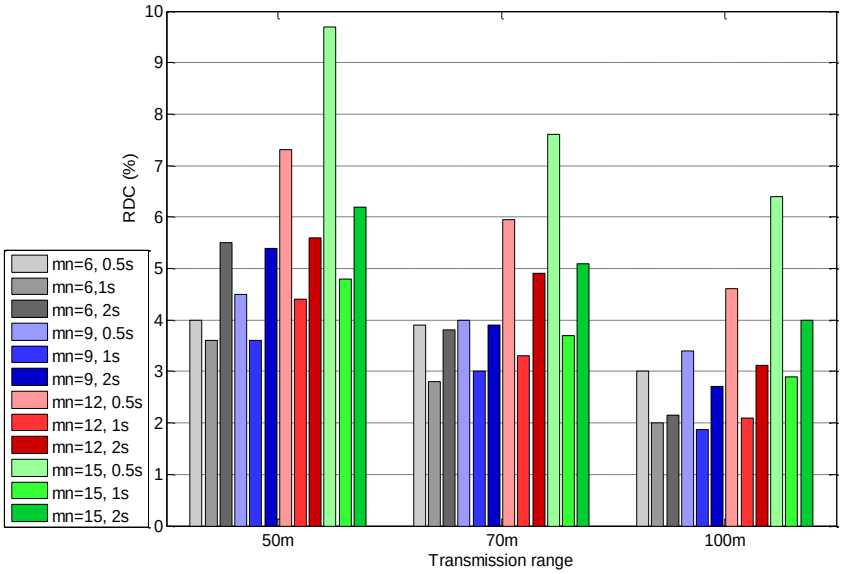
(b) Range=70m



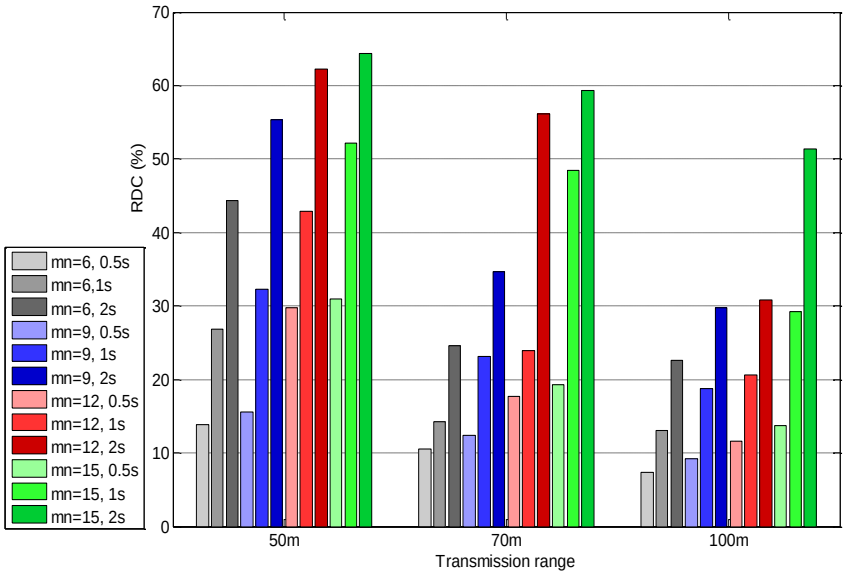
(c) Range=100m

Fig. 5.11: Percentage of time associated to the network

Furthermore, setting transmission range to 100m, both TSCH and MTSCH show there best performance as compared to previous ranges. At *mn*=15 and sf_D =2s, MTSCH boosts node connectivity from 49.7% to 86.7%. Finally, Fig. 5.12 (a) and (b) present the whole picture of the RDC performance for mobile nodes with respect to different transmission ranges, sf_D and *mn*.



(a) MTSCH



(b) TSCH

Fig. 5.12: Average RDC of non-CH nodes

The MTSCH managed to reduce the RDC of TSCH from 7% to 3% in the case of *mn*=6, sf_D =0.5s and transmission range of 50m. Similarly, for the worst application scenarios, the MTSCH has RDC of 9.4% and the TSCH is 31% regarding *mn*=15, sf_D =0.5s and transmission range=50m. In addition, the RDC has been reduced form 50% to 4% for *mn*=15, sf_D =2s and at a transmission range of 100m.

For both Fig 5.11 and Fig. 5.12, in addition to the impact of *sf*, boosting the number of mobile nodes complicates the contention process (that is required to associate), in turn long waiting times are introduced. Accordingly, the dissociation periods are extended while degrading the connectivity.

Finally, the simulation results show a relative behavior as the analytical results by which the margin of error for determining the probability of finding a blocked FFD, during an association process, did not exceed 0.06. This is indicated in Fig. 5.13 that compares the simulation with the analytical outcome for A_n values of 2 and 5, L_D values of 1 and 2, and E_m ranges [1, 4].

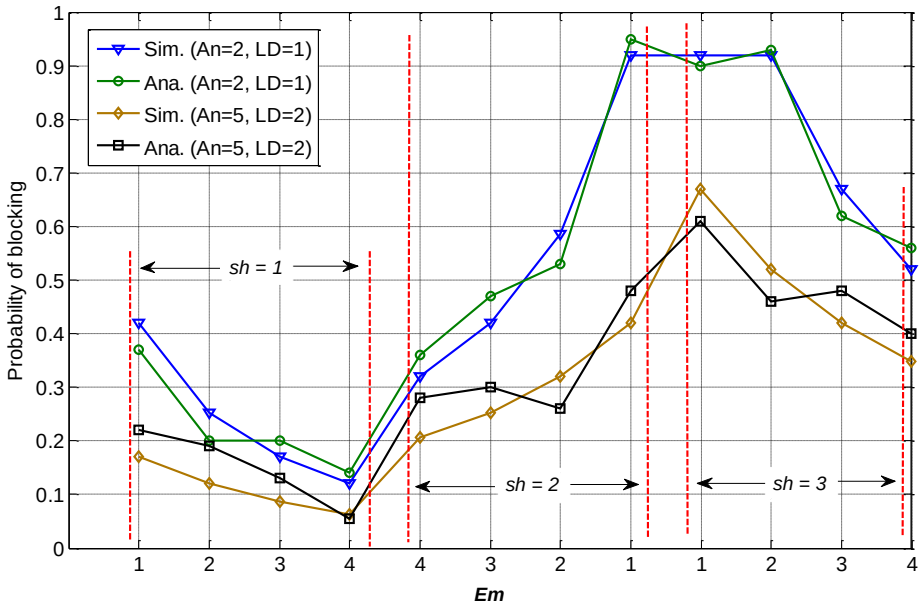


Fig. 5.13: Probability of blocking a mobile node, sf_D =0.5, *mn*= 6, α_{nAc1}=1

In the meantime, the probability of joining an FFD device during the association process shows similar results for both analytical and simulation analysis as described in Fig. 5.14. The ε (epsilon) takes two values (2 and 4) while R_e ranges between [1, 3] and $\overline{E_m}$ ranges from [1, 4].

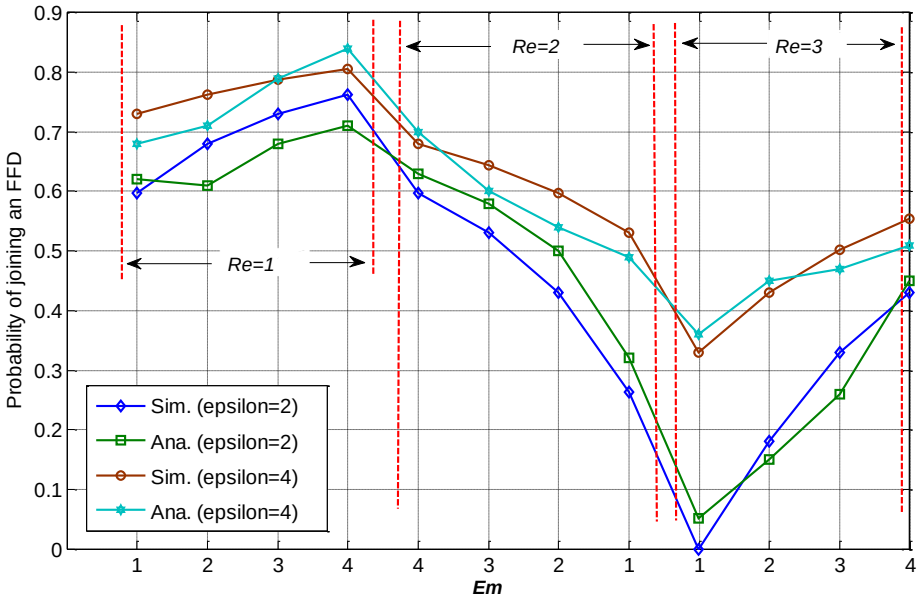


Fig. 5.14: Probability of joining an FFD, sf_D =0.5, mn= 6, φ =0.9, θ=1

The simulation analysis shows slight variations form the analytical results due to the randomness of mobile node movement by which the number of nodes in a POS can't be determined correctly. This is traced to the impact of changing trajectories inside a POS and in turn, mobile nodes have no steady settle time. In order to accurately determine the exact mobile node behavior, the stochastic properties for the utilized mobility model must be considered.

5.6 Summary

The proposed MTSCH framework is shown to provide a mobility service with low overhead on both of FFD and RFD nodes. Different implementation scenarios show the gain by reducing RDC of the mobile nodes and ranges between, on average, 7% to 50% for 6 to 15 mobile nodes respectively. MTSCH enhanced the connectivity metric (percentage of time the node is associated to the network) of the nodes by

reducing the listening time or waiting for a valid EB. MTSCH increased mobile nodes connectivity time by a ratio of 10% (*mn*=6) to 50% (*mn*=15) for 50m transmission range while it improves the connectivity by a ratio of 3% (*mn*=6) and 36% (*mn*=15) for 100m range. On the other hand, after running the nodes for 1,700s, MTSCH reduces FFD energy consumption (for *mn*=9 and range=50m) by 7,000mJ and 1,200mJ for 0.5s and 2s sf_D durations respectively. In addition, MTSCH achieves a saving in energy (for *mn*=15 and range 50m) averaged to 18,000mJ (sf_D =0.5s) and 600mJ (sf_D =1s). Hence, the advantage of implementing MTSCH to support node mobility has influenced the performance of all the nodes within the network, FFD and RFD. Furthermore, the proposed MTSCH overcomes the problem of advertising EBs and the impact of collision by defining a randomized period W_{ACK}. The FFD nodes can listen and deduce T_{ACK} of the adjacent FFD devices and thus, selecting a different T_{ACK} time within this window. This ensures that the closet one hop devices will avoid collisions. Finally, two issues exist in the implementation of TSCH and have been identified through the implementation within the Contiki OS. The first one is the handling process of the dedicated links in the presence of mobile nodes that imposes the dynamic nature on the allocations process. Hence, the abandoned links have to be utilized and reallocated again to new mobile nodes entering the POS. the second problem is the variations in the number of slots that lead to change the sequence of the ASN, which in turn existing nodes must be informed of to maintain synchronization with the network. Therefore, after each join process, if the new mobile node has not utilized an abandoned link, the FFD must inform the existed nodes regarding the addition of new timeslot which will affect the ASN sequence. Thereby, the existed nodes within each cluster shall maintain synchronization with the FFD.

The next chapter considers the second IEEE 802.15.4e operation mode, LLDN, and studies the overhead of node mobility while providing a set of approaches to enhance this mode.

Chapter 6. Mobility under IEEE 802.15.4e Low Latency Deterministic IoT Network

Providing reliable services for low latency (LL) applications within the Internet of things context is a challenging issue. Several IoT applications require deterministic systems that ensure a reliable and low latency aggregation service. The IEEE 802.15.4e standard has presented the low-latency deterministic network mode (LLDN) that can fulfil the major requirements of low latency applications. Meanwhile, several LL applications, for example in the automotive industry, demand the support of node mobility which in turn affects network performance. Node mobility triggers several dissociations from the network that will increase latency and degrade node throughput. In this chapter, the impact of node mobility over the LLDN mode is investigated while defining the key factors that maximize latency and degrade throughput. In addition, an enhanced version of the LLDN mode is presented and evaluated that supports node mobility while maintaining the targeted limits of LL application requirements.

6.1 Mobility Issues Under IEEE 802.15.4e LLDN Mode

Studying the infrastructure of the LLDN can conclude several issues that rose by the association process and are escalated with the presence of mobile nodes. These issues can be summarized into the following:

- There is no mechanism to change from transmission state to another after the network initialization phase.
- During the online state (which is the dominant state through the network lifetime) any node seeking to join the network has no feasible procedure to communicate with a coordinator, especially with the *macLLDNmgmTS* is set to FALSE during the online state.
- The size of the management *TS* and the contention mechanism must be reconfigured to accommodate multiple orphan nodes (or mobile nodes seeking

to join the network) and minimize the dissociation time to reduce latency.

- In order to commence the association process, the network must transit to the discovery state and drop the online state. This means preventing the connected nodes from transmitting regular readings and wait till completion of both discovery and configuration states. This can get worse in the case of high mobility, where the network has several transitions from the online state to other states.
- The LLDN is based on a simplified CSMA-CA where the *macMaxCSMABackoffs* value has been set to zero. This complicates the association process due to the announcement of a channel access failure after only a single unsuccessful clear channel assessment scan. Hence, the node has to scan for another beacon and superframe, which will maximize the dissociation interval.

The default assumption of the LLDN is based on a star topology that considers single-hop scenarios, whereas in reality and for multiple application types a multihop infrastructure is required. Considering a single hop infrastructure for dense network, with mobile nodes and short range transmission can cause a flaw in the design phase. First, due to the increased required numbers of coordinators in order to assure single hop transmission, this will in turn increase deployment cost and complexity. Second, this will maximize the number of dissociations due to short range transmissions and high number of mobile nodes

6.2 Related Work

Other literature addressed the issue of latency in sensor network but do not address the mobility nor are dedicated for the IEEE 802.15.4 standard [132-135]. Similarly, the recent contributions that concern LLDN do not consider mobility. Therefore, a significant part of the IoT paradigm, which is the IEEE 802.15.4e LLDN mode, has not been addressed before and need to be evaluated comprehensively to optimize performance with regards to node mobility.

Here the current enhancements to the default LLDN structure are introduced. A. Berger *et al*. [136] improve data collection reliability of the default LLDN star topology by amending the structure with relay nodes. The objectives behind the relay nodes are to increase the transmission reliability via retransmitting unsuccessfully delivered packets and to extend the topology to two-hop networks. The authors indicate that the coordinator is stationary while the nodes might be mobile but did not address the issue of association since the target of the paper is realizing reliable transmission and 2-hop communication. The authors amended this work and improve its reliability in [137] through utilizing the combinatorial testing approach (CT) which is described in [138].

G. Patti *et al*. [139] introduce the multi-channel approach to reduce operational cycle times (superframe size). Maximizing the number of nodes increases the cycle time linearly, and hence the authors have divided the network into clusters (called subnetworks). Each cluster will have a different frequency channel to simultaneously operate without any interference with other clusters. Although this approach will minimize the cycle time for the individual subnetwork, but still the head coordinator operates for a full cycle related to the number of nodes in the total subnetworks that are connected to it.

L. Dariz *et al*. [140] improve LLDN performance via optimizing the LLDN superframe duration. This is achieved through turning the timeslot allocation procedure into a flexible and efficient allocation process. Instead of fixing the number of base timeslots in the uplink and downlink slots to a fixed size in the superframe, the number of base slots will be variable based on each node's requirement. In addition, the authors amended the superframe structure to accommodate more slots types as high-priority uplink and high-priority downlink slots to fulfil the requirements of some nodes with high priority data.

M. Anwar *et al*. [141] provide an analysis for different LLDN configuration parameters during network control design. The analysis takes into account different LLDN configuration parameters such as base timeslot size, superframe size, enabled security or not and payload size. The target is to provide a tradeoff between LLDN configuration parameters that will aid the LLDN network control design phase.

H. Kapil *et al*. [142] incorporate node relay placement strategy and error correction

technique to minimize the number of retransmissions and hence, a reduced number of relays and better energy efficiency. The objective of the proposed approach is an adaptive retransmission technique by integrating a Reed Solomon error correction scheme with a relay placement mechanism (that is based on the rainbow ranking algorithm [143]). The advantage is less nodes and less energy consumption while high LLDN reliability is achieved.

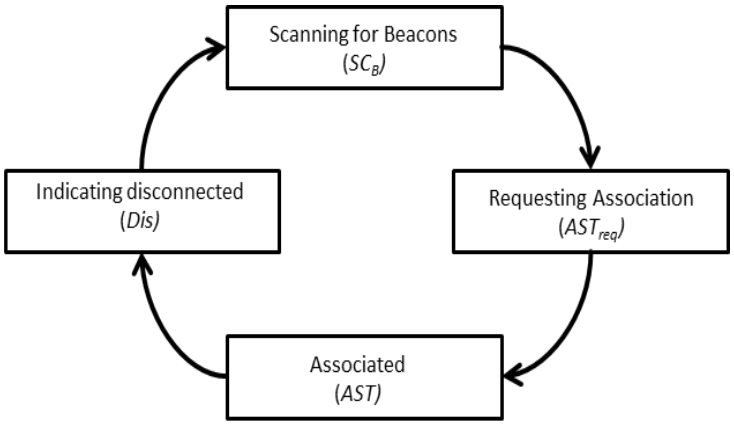


Fig. 6.1: LLDN-based mobile node lifecycle

6.3 Mobility Overhead Over IEEE 802.15.4e LLDN

The impact of node movement and the overhead upon the network performance needs to consider the lifecycle of a mobile node. The possible life stages that an LLDN-based mobile node encounters since deployment can be categorized into four basic steps as explained in Fig. 6.1. Based on this classification, the elapsed time in each state can be estimated. From this point, the possible time duration of each superframe type in LLDN can be defined, as for each transmission state there will be a different superframe duration. Discovery and configuration superframe intervals are closely related where the discovery superframe interval (S_D) can be defined as:

$$S_D = \frac{\left(B_p + (T_{sz} \times 2) + (3 \times SIFS) + P_A\right)}{R_s} \qquad (6.1)$$

B_P is the beacon period in symbols and corresponds to physical header plus MAC

header lengths (in bytes) and is multiplied by the number of symbols per byte (for the 2.4 GHz band both physical and MAC are 2). T_{SZ} is the real slot size (excluding interframe spacing) of a slot and the short interframe space (*SIFS*) corresponds to *macMinSIFSPeriod* while R_S is the symbol rate. P_A is the interval time between each beacon announcement, since the network administrator may extend the period between each superframe (in this research, P_A is set to zero) to utilize energy (where P_A is the inactive period). The B_P can be estimated to be (6+7) ×2 symbols and T_{SZ} is equal to (6+4+14) ×2 symbols, where the maximum payload (in the discovery stage messages) is 14 bytes. In addition, configuration superframe duration (S_C) can be estimated as in (6.2). Where T_{SZ} here is equal to (6+4+14+ *additional_payload*) × 2 and long interframe space (*LIFS*) corresponds to *macMinLIFSPeriod*. *additional_payload* depends on the application and could be the frequency channel, assigned timeslot, etc.

$$S_C = \frac{\left(B_p + (T_{sz} \times 2) + (2 \times SIFS) + LIFS + P_A\right)}{R_s} \qquad (6.2)$$

Finally, online superframe (S_O) can be estimated as indicated in [1] while identifying the MAC payload size:

$$S_O = \frac{\left(B_p + SIFS + (N_{TS} \times T_{SZ}) + (N_{TS} \times LIFS) + P_A\right)}{R_s} \qquad (6.3)$$

Where N_{TS} represents the possible number of timeslots in the uplink unidirectional field and can be either set to *macLLDNnumUplinkTS* value or can be varied based on the number of nodes in a POS. Here T_{SZ} is the actual slot size of a single base timeslot (excluding interframe spacing) in the uplink and equal to (6 + 3 + payload_size) × 2.

As in Fig. 6.1, there are four states that a mobile node may encounter, scanning for beacon interval (SC_B), requesting association (AST_{req}), fully Associated to network (*AST*) and indicating disconnect (*Dis*) (or orphan). The first phase of the mobile

lifecycle that will be estimated is *Dis*, where it can have two values based on the methodology followed to indicate the dissociation (announce the node is orphan), which is either based on the number of lost beacons or missed ACK messages.

$$Dis = \begin{cases} aMaxLostBeacons \times S_o & (\text{beacon} - \text{dependent}) \\ nmACK \times S_o & (\text{Ack message} - \text{dependent}) \end{cases} \quad (6.4)$$

where *nmACK* represents the number of missed ACK messages. Regarding the second phase, scanning for beacon interval (SC_B) can be expressed as:

$$SC_B \cong \begin{cases} \dfrac{S_D}{2} & \text{(discovery state)} \quad (6.5) \\ \left(\dfrac{S_O}{2}\right) + \left(\sum_{j=1}^{\left\lfloor \frac{O_c}{(M_m + D_m)/2} \right\rfloor} S_{D(j)} \right) mod\ P_{th} & \text{(online state)} \quad (6.6) \\ \dfrac{(t_2 - t_1)^2}{T} + \dfrac{\left((T - t_1) - t_2\right)^2}{T} & \text{(two coordinators exist)} \quad (6.7) \\ \dfrac{S_O + (nS_O \times S_O) + (nS_C \times S_C)}{2} & \text{(defined transmission states)} \quad (6.8) \end{cases}$$

In these four scenarios, (6.5) is the case where the coordinator is in the discovery transmission state. The analysis here is assuming perfectly scheduled timeslots, but in the case of different superframes durations, it will follow the random incidence paradox [144, 145] and expressed as:

$$\frac{\sigma^2 + \mathbb{E}[S]^2}{2\ \mathbb{E}[S]} \quad (6.9)$$

However, since the LLDN deals with tightly synchronized nodes, perfectly scheduled and fixed superframes duration are assumed, so $SC_B = (S/2)$, where S is any superframe (S_D, S_C or S_O).

In the case of the coordinator in the online state, the scanning and waiting time is

dependent on the interval that is adjusted to transfer from the online to discovery state as in (6.6). The approximated scenario is to harness both the mobility metric (M_m) and density (D_m), which can both be derived based on [146, 147] and [148] respectively, to determine the duration between each transfer. (O_c) in (6.6) represents the preferred number of online superframes in each period before flipping to a discovery state while P_{th} is the maximum number of online superframes after which there must be a discovery state. Based on these parameters it will be easy to efficiently provide a tradeoff between latency and dissociation time. Increasing mobility and density metric will increase the number of discovery superframes per online superframe in order to accommodate more mobile nodes and reduce the scanning waiting time. This will ensure that whenever either of the mobility or density metric increases, the number of online superframes will be reduced to minimize the scanning time and hence, realizing fast association. According to [147], the mobility metric can be considered as the average relative speed of nodes over the possible number of node pairs and running time. Hence, for a given graph $G = (N, P)$, where N is a set of nodes and P is a set of links between the nodes and $\in N$, the mobility metric M_m can be expressed as [146, 147]:

$$M_m = \frac{1}{|P|} \sum_{x_1=1}^{|N|} \sum_{x_2=1}^{|N|} \frac{1}{R_t} \int_0^{R_t} |V_{x1}(t) - V_{x2}(t)| \, dt \qquad (6.10)$$

Where R_t is the total running time, $V_x(t)$ is velocity of node x at time t. In addition, according to [148] the density metric D_m can be expressed as:

$$D_m = \frac{|N| \, \pi \, R^2}{A} \qquad (6.11)$$

Here A is the scattered area and R is the transmission range. Returning to (6.7) which holds the condition that two coordinators exist. For a given period of time T, if the first coordinator announces at t_1 and the second announces at t_2 and t_1, $t_2 \in T$, then there are two inter-arrival times, (t_2-t_1) and ((T-t_1)-t_2). Thus, the expected

waiting time can be expressed as in (6.7).

The fourth scenario, as in (6.8), is applied when there is a defined structure of the network transmission states. The scanning time in this condition is based on the number of online superframes (nS_O) and the number of configuration superframes (nS_C) that are both defined prior to network deployment.

The third phase of the mobile node lifecycle is the AST_{req}, which will be completely dependent on the ratio of the number of both discovery and configuration superframes to the online superframes. In addition, it will follow the impact of the number of mobile nodes entering the same POS at the same time besides the nodes speed and transmission range. Accordingly, Fig. 6.2 presents a Markov chain that models the possible states for a mobile node during the association process. A mobile node's condition can be described in three stochastic processes; node status, backoff condition and CCA outcome ($s(t)$, $b(t)$ and $c(t)$ respectively). The possible states of $s(t)$ are orphan, received beacon, discovering, configuring, configuring_ACKing and associated, which will be presented as $s = \{s_o, s_d, s_{cr}, s_{ca}, s_a\}$. Meanwhile, b will be varied in the range $[0, 2^{BE}-1]$ and presented as $b = \{b_0, b_1, \ldots, b_n\}$.

The backoff exponent, *BE*, will be set to *macMinBE* value. Finally, c represents the possible states of the two CCA processes as CCA_{1_free}, CCA_{1_busy}, CCA_{2_free} and CCA_{2_busy} and presented as $c = \{c_{11}, c_{12}, c_{21}, c_{22}\}$. The probability ($\alpha$) of receiving a valid beacon depends on the amount of coverage percentage within the scattered area (there is an adequate number of coordinators to cover the whole area of deployment). The analysis here always assumes having a well scattered deployment, $\alpha = 1$. The probability (β) of the received beacon determines a discovery state is based on the adjusted ratio of discovery state to other transmission states. During the network initialization period, $\beta = 1$ for at least a period of *macLLDNdiscoveryModeTimeout* if no node requests association.

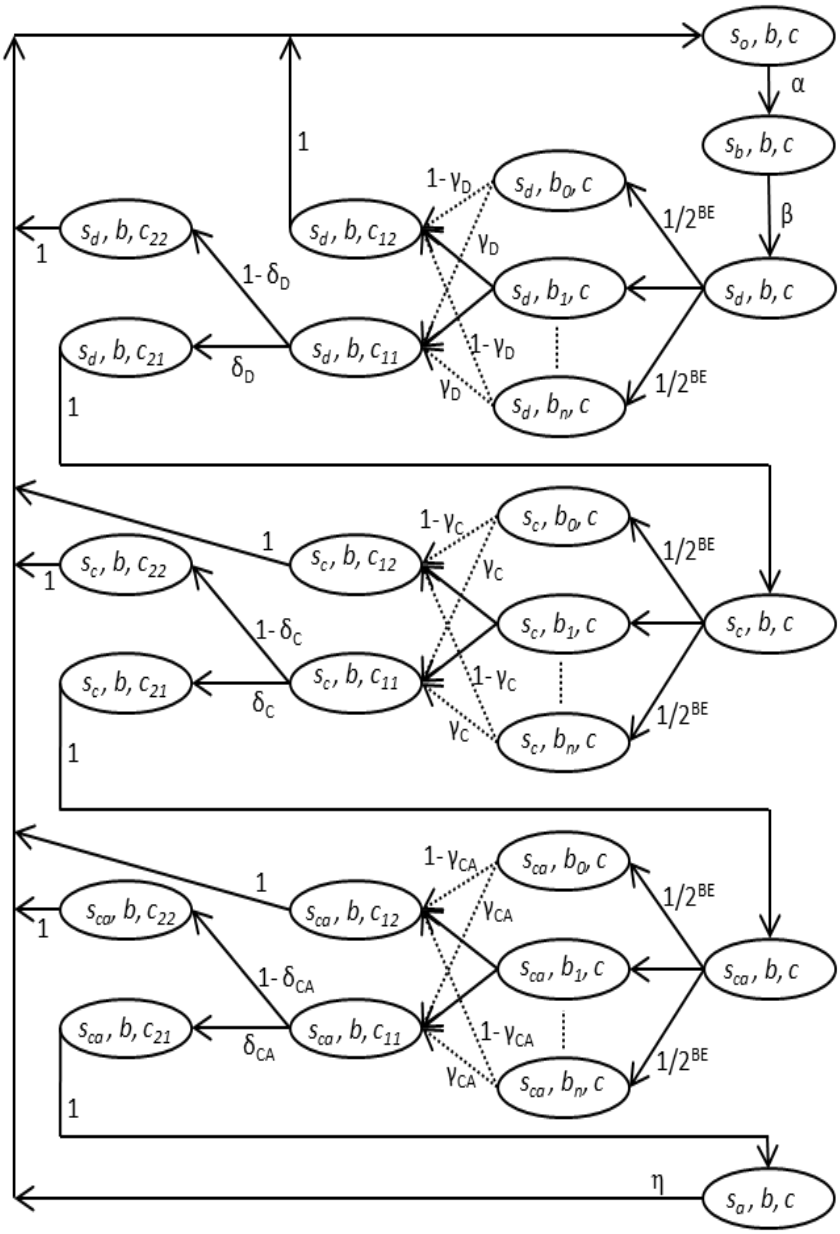


Fig. 6.2: Markov chain for mobile node transitions in LLDN

Meanwhile, within the network steady state period, β can be expressed as in (6.12). Where, x_D is the number of mobile nodes that have successfully transmitted discovery response frames and received ACK messages.

$$\beta = \frac{macLLDNdiscoveryModeTimeout}{\left(\sum_{j=1}^{\left\lceil \frac{O_c}{(M_m+D_m)/2} \right\rceil} S_{D(j)}\right) mod\ P_{th} + (S_C \times x_D)} \qquad (6.12)$$

The probability that the first CCA (during discovery state) γ_D returns a free channel within a given *BE* value (b_i) depends on whether the node has selected a given *bi* and whether the previous *bi* backoff slots have not been utilized by the other remaining nodes and can be expressed as in (6.13).

$$\gamma_{D(bi)} = \frac{1}{2^{BE}} \left[\left(1 - \frac{1}{2^{BE}} \right)^{N_m - 1} \right]^{bi-1} \tag{6.13}$$

Similarly, transmitting the request successfully depends on the probability (δ_D) that the node has selected a given *bi* and no other remaining nodes have already selected the same *bi* backoff slot:

$$\delta_D = \frac{1}{2^{BE}} \left(1 - \frac{1}{2^{BE}} \right)^{N_m - 1} \tag{6.14}$$

Where N_m corresponds to the number of mobile nodes seeking to associate with the coordinator within the same superframe and can be derived as:

$$N_m = \mathbb{E}[\![|N_{crt}| - |N_A|]\!] + \sum_{j=1}^{ne} Ad_{(j)} + |N_w| \tag{6.15}$$

N_{crt} is a set of existed nodes in the POS and N_A is a set of active nodes, where $N_A \in N_{crt}$. $Ad_{(j)}$ represents the number of mobile nodes entering from the j^{th} adjacent POS and (*ne*) is the total number of adjacent POSs. N_w is a set of nodes already in the POS and waiting for the discovery state.

Moreover, during the configuration state, the probabilities of the first and second CCA return free channel states and the node transmits successfully (γ_C, δ_C) are expressed in (6.16) and (6.17) respectively.

$$\gamma_{C(bi)} = \frac{1}{2^{BE}} \left[\left(1 - \frac{1}{2^{BE}}\right)^{(X_D \times nS_D)-1} \right]^{bi-1} \quad (6.16)$$

$$\delta_C = \frac{1}{2^{BE}} \left(1 - \frac{1}{2^{BE}}\right)^{(X_D \times nS_D)-1} \quad (6.17)$$

X_D denotes the number of nodes managed to receive ACK for the discovery response frame. Finally, the probabilities (γ_{CA}, δ_{CA}) during the acknowledgement phase of the configuration state are obtained as:

$$\gamma_{CA(bi)} = \frac{1}{2^{BE}} \left[\left(1 - \frac{1}{2^{BE}}\right)^{(X_C \times nS_C)-1} \right]^{bi-1} \quad (6.18)$$

$$\delta_{CA} = \frac{1}{2^{BE}} \left(1 - \frac{1}{2^{BE}}\right)^{(X_C \times nS_C)-1} \quad (6.19)$$

X_C denotes the number of nodes which managed to receive a configuration request frame.

Accordingly, the relevant probabilities of each transmission mode can be calculated to conclude the probability of associating to a coordinator. The probability of receiving an ACK message during the discovery state is:

$$p(s_{cr}, b, c | s_o, b, c) = \alpha\, \beta\, \delta_D \sum_{bi=0}^{2^{BE}-1} \frac{1}{2^{BE}}\, \gamma_{D_{(bi)}} \quad (6.20)$$

And the probability of receiving the required synchronization information during the configuration state is described in (6.21):

$$p(s_{ca}, b, c|s_{cr}, b, c) = p(s_{cr}, b, c|s_o, b, c)\ \delta_c \sum_{bi=0}^{2^{BE}-1} \frac{1}{2^{BE}}\ \gamma_{DC_{(bi)}} \quad (6.21)$$

Finally, the probability of associating to the coordinator is:

$$p(s_a, b, c|s_{ca}, b, c) = p(s_{ca}, b, c|s_o, b, c)\ \delta_{CA} \sum_{bi=0}^{2^{BE}-1} \frac{1}{2^{BE}}\ \gamma_{CA_{(bi)}} \quad (6.22)$$

The latency during either discovery or configuration state is determined by the number of mobile nodes, since (as defined in the standard) the assumption is that the coordinator shall stay at each state until responding to all requested nodes within POS. Therefore, AST_{req} can be derived based on the incurred expected latency at each state. The latencies (L_D), (L_C), (L_{CA}) during the discovery, configuration and acknowledging configuration states respectively can be estimated as:

$$\mathbb{E}(L_D) = \sum_{j=1}^{nS_D} \left(1 - p(s_{cr}, b, c|s_o, b, c)\right)^{j-1} p(s_{cr}, b, c|s_o, b, c)\ (S_D \times j) \quad (6.23)$$

$$\mathbb{E}(L_C) = \sum_{j=1}^{nS_C} \left(1 - p(s_{ca}, b, c|s_{cr}, b, c)\right)^{j-1} p(s_{ca}, b, c|s_{cr}, b, c)\ (S_C \times j) \quad (6.24)$$

$$\mathbb{E}(L_{CA}) = \sum_{j=1}^{nS_C} \left(1 - p(s_a, b, c|s_{ca}, b, c)\right)^{j-1} p(s_a, b, c|s_{ca}, b, c)\ (S_C \times j) \quad (6.25)$$

Hence, the expected waiting time during the association request phase AST_{req} is:

$$AST_{req} = \mathbb{E}(L_D) + \mathbb{E}(L_C) + \mathbb{E}(L_{CA}) \tag{6.26}$$

In order to determine a successful association, the required time to associate must be less than a settle time (*ts*) in a POS. Thus, the probability (θ_t) to complete association is basically dependent on the expected amount of time to associate with a coordinator to the expected settle time in a POS. In other words, this will match the time where the node status is considered as associated since according to the four phases, *Dis*, SC_B and AST_{req} are representing the total dissociation period in a POS and *AST* is where the node is considered as connected.

$$\theta_t = 1 - \frac{Dis + SC_B + AST_{req}}{ts} \tag{6.27}$$

The *ts* parameter is dependent on several elements as node speed, possible trajectories inside a POS and coordinator coverage. Therefore, for a mobile node under the random waypoint mobility scenario, there will be three basic elements; node speed, possible moving distance and pause time. For a node speed *sp* in the range [sp_1, sp_n], distance *D* in the range [d_1, d_n] and pause time *p* in the range [p_1, p_n], the expected settle time can be defined as:

$$ts = \frac{\sum_{i=1}^{k} \mathbb{E}[d]_i}{\mathbb{E}[sp]} + \sum_{i=1}^{k} \mathbb{E}[p]_i$$

$$= \frac{\sum_{i=1}^{k} \left(\int_{d_1}^{d_n} D \, \frac{1}{d_n - d_1} \, dD \right)_i}{\int_{sp_1}^{sp_n} sp \, \frac{1}{sp_n - sp_1} \, dsp} + \sum_{i=1}^{k} \left(\int_{p_1}^{p_n} p \, \frac{1}{p_n - p_1} dp \right)_i$$

Hence, settle time is:

$$ts = \frac{\sum_{i=1}^{k}\left(\frac{d_n + d_1}{2}\right)_i}{\frac{sp_n + sp_1}{2}} + \sum_{i=1}^{k}\left(\frac{p_n + p_1}{2}\right)_i \quad (6.28)$$

Where *k* is the possible number of movements (or the possible epochs before leaving POS) and is affected by the transmission range of the coordinator and *D*. (*i*) represents a specific epoch in a POS and varies from 1 to *k*. The focus of this research here is not interested in investigating the stochastic features of the random waypoint mobility model while a comprehensive analysis can be found in [149, 150].

The probability of leaving the POS (η) will be dependent on the transmission range (*R*) of the nodes and the total number of movements inside a given POS (assuming a straight line trajectory in a POS), expressed in (6.29).

$$\eta = \frac{1}{2\,R_{dBm}} \sum_{i=1}^{k} d_i \quad (6.29)$$

For a better network performance in a mobile IoT network environment, a dissociation function must be introduced, which is a measure of the number of nodes that are dissociated. Thus, the target of a mobile network must always seek for low dissociation function (low number of dissociated nodes) to gain high network connectivity and availability. This measure can be derived based on the Kaplan-Meier estimator [151]. Thus, for *n* distinct event times $t_1 < t_i < \ldots < t_n$, the dissociation function ($\hat{S}(t)$) for a total time *t*, that $t_1, t_i, \ldots, t_n \in t$, can be expressed as in (6.30). Where, $N_a(i)$ represents the number of dissociated nodes at a given time t_i and $N_m(i)$ is the total number of mobile nodes at time t_i,

$$\hat{S}(t) = \prod_{i=1}^{n}\left[1 - \frac{N_{m(i)} - N_{a(i)}}{N_{m(i)}}\right] \quad (6.30)$$

One of the issues that need to be highlighted is the node throughput that is crucial for several LL network applications, especially that requires streaming [152, 153]. The throughput of LLDN network is related to the amount of time that the coordinator is within the online state. Therefore, the number of lost data frames (Los_D) after each transfer from the online to other states must be computed, which can be expressed as:

$$Los_D = \left\lceil \frac{nS_D \times S_D + nS_C \times S_C}{S_O} \right\rceil \quad (6.31)$$

In the meantime, the effective throughput (E_{thr}) in (bps) of the network can be defined as:

$$E_{thr} = \left(\frac{MSDU \times 8}{S_o}\right)\left(1 - \frac{nS_D \times S_D + nS_C \times S_C}{nS_o \times S_O}\right) \quad (6.32)$$

Where nS_O is the number of online superframes and the data payload (MAC service data unit, MSDU) is the actual payload data size in octets as defined by the standard.

Furthermore, the packet delivery ratio, which is related to the impact of dissociation, during a given *ts* time can be expressed as:

$$PDR_{dissociation} = \frac{ts - \left(Dis + SC_B + AST_{req}\right)}{ts} \quad (6.33)$$

The impact of transferring each time from the online state can lead to PDR degradation and can be calculated as:

$$PDR_{transfer} = 1 - \frac{Los_D}{nS_o} \quad (6.34)$$

6.4 Proposed Enhanced and Mobile-Aware LLDN Scheme

From the previous sections, two main requirements to achieve better network performance can be concluded, which are low latency and multihop infrastructure. Since the LLDN is designated for a star topology, then there must be a mechanism to facilitate the multihop feature which supports both node mobility and LL. Comparing the star topology to other different topologies for the case of IEEE 802.15.4 infrastructure, it has less latency but unfortunately has less success probability [154]. Conversely, if the application is looking for low dissociations, then the network has to be assisted with multiple coordinators to guarantee low waiting time prior to achieve association. This leads the research here to the strategy of increasing the number of coordinators, but this will unfortunately open the gate to another issue, which is beacon collision. Beacons of adjacent coordinators collide due to overlapped communication range and this issue has been addressed in several works [155-157]. Therefore, the objective of the proposed approach here is:

- To minimize the dissociation time and increase the mobile node connectivity.
- Determining how the latency and collision can be minimized.
- To support a multihop paradigm while omitting extra coordinators.
- Combining the advantages of both tree and star topologies.

A comprehensive analysis in [154] shows that the tree topology outperforms the star topology in terms of transmission success probability, but the problem with a tree strategy is significant latency. Thus, the trend here is to figure out an approach that provides multihop (tree infrastructure) while minimizing the encountered delay. One of the approaches that could be utilized is clustering [158], this technique is suitable to minimize the impact of collisions and maximizes transmission success rate but in turn increases the latency in the tree infrastructure. Hence this problem must be tackled through modifying the existed LLDN superframe infrastructure. Accordingly, the proposed approach is based on two principles; first, defining the concepts of proxy coordinator and passive beacon and second, modifying the LLDN superframe.

The concept of passive beacons can be realized by forcing each node to add an extra two bytes to the MAC header of data frames, one byte preamble (*preamble_1*) and two bytes for the time that the proxy node can receive an association request. The nodes need not include the extra three bytes in each data frame, but this can be performed in every interval of time and this interval is influenced by the mobility metric. This concept has been called the passive beacon since the nodes are not beaconing but are indicating passively (through data frames) the minimum relevant information regarding node association and thus, the data frames are acting as beacons. Therefore, the nodes are acting as a proxy to the original coordinator within the LLDN. Any node that acts as a coordinator will be denoted as a proxy.

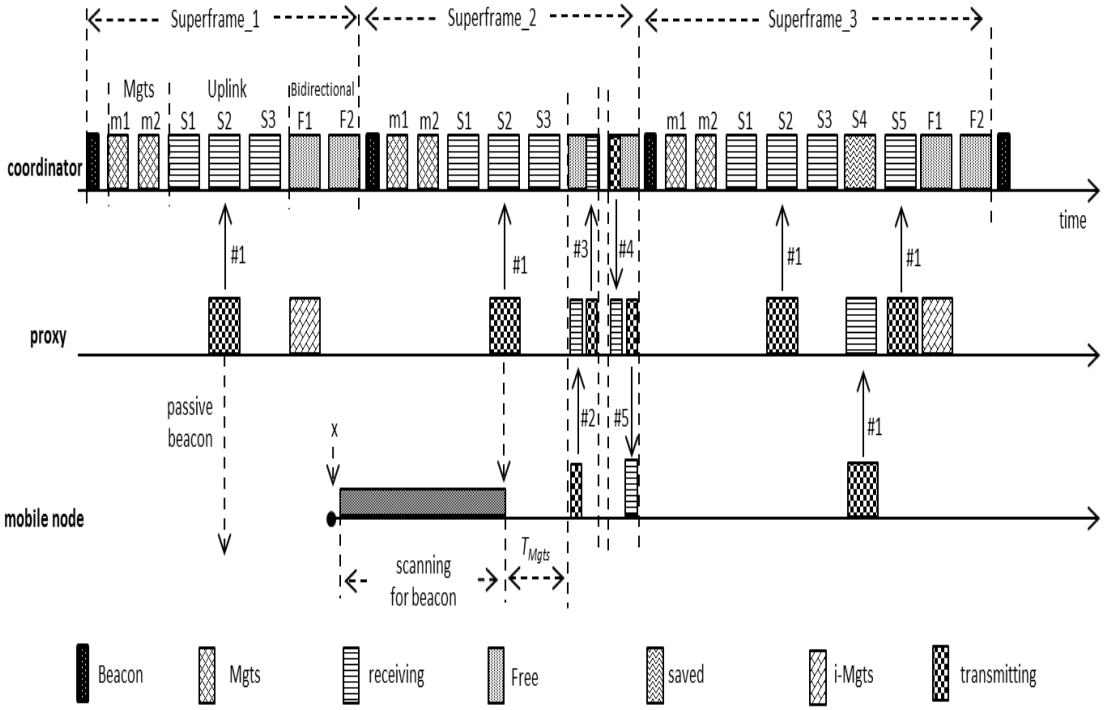


Fig. 6.3: 2-hops mobile node association in MA-LLDN

A mobile node that can't detect any beacons can listen for existing data frames and scan the header for the preamble byte. If *preamble_1* exists, then the next two bytes is the time (T_{Mgts}) by which the proxy node is accepting association requests (as in Fig. 6.3). T_{Mgts} is the time interval between the transmitted data frame and the time a proxy switches the radio on to receive a request. In order to mitigate any chance of collision with the coordinator, the proxy utilizes the F slots (additional free slots the

coordinator allocates for the purpose of permitting proxy node to accept association requests freely). Each proxy adjusts the time to accept association requests within defined slot boundaries (called image timeslot (*i-Mgts*)) that coincide with the first bidirectional (F1) slot in the superframe. The duty of the coordinator in this case is to ensure that there are always at least two free F timeslots in the bidirectional field of the superframe to be used by the proxy nodes. This will ensure that the management timeslots *i-Mgts* (of proxies) are not overlapping with the current utilized (transmitting data) slots in the superframe. The coordinator will always utilize the first n/2 bidirectional slots as uplink and the second n/2 slots as downlink, for slots [F1-Fn], where n here is the number of slots in the bidirectional field.

Once a proxy receives an association request (message #2 in Fig. 6.3) during the *i-Mgts*, it will relay the request to the coordinator within the same slot (message #3), since this slot has been freed within the superframe for the purpose of this task. During the next timeslot, the coordinator responds with the required information (message #4) in order to synchronize the mobile node (allocated timeslot, transmission channel, etc.). The proxy has to relay the information back to the mobile node (message #5) and finalize the association process. Hence, the entire process is accomplished within only two consecutive timeslots (in the case of two hops).

The coordinator upon the addition of a new mobile node will add four additional timeslots to the uplink and bidirectional fields for each upcoming superframe. This will be one for transferring data from mobile node to proxy (slot S4), one for transferring data from proxy to coordinator (slot S5) and two (slots F1 and F2) for the purpose of *i-Mgts* slots. The *i-Mgts* slots are harnessed by the proxy nodes to permit more mobile nodes in the future to join the network.

The modified superframe has reduced the latency by instructing the proxies to relay the data frames of the nodes, which are not within the first hop, within the same superframe. Hence, the latency L_h for a node in a given hop (h) is:

$$L_{h[min]} \leq L_h \leq L_{h[max]}$$

$L_{h[\min]}$ and $L_{h[\max]}$ can be calculated as:

$$L_{h[min]} = \left[\sum_{i=2}^{h}\left(\frac{i(i+1)}{2}-1\right)nP_i + (h-1) + L_{h-1}\right](T_{SZ} + IFS) \quad (6.35)$$

$$L_{h[max]} = \begin{cases} \left[\left(\frac{h(h+1)}{2}-1\right) + \sum_{i=2}^{h}\left(\frac{i(i+1)}{2}-1\right)nP_i\right] \\ \times (T_{SZ} + IFS)\ ;\ for\ h > 1 \\ (T_{SZ} + IFS); \qquad otherwise \end{cases} \quad (6.36)$$

Where the *IFS* corresponds to the interframe spacing that could be either *macMinSIFSPeriod* or *macMinLIFSPeriod*. nP_h refers to the number of mobile nodes attached to a given proxy (within the route) at hop *h*. Since the maximum configuration request size (Req_s) is 48 symbols (physical and MAC header plus configuration status payload), then the required time to commence transmission of two messages is always less than timeslot size (T_{SZ}). Hence, a single timeslot T_{SZ} in the uplink field of a superframe can accommodate two transmissions, sending an association request and replying with an ACK message. Thus, this property will be always true:

$$Req_s + T_{ack} + ACK_s + SIFS < T_{SZ} \quad (6.37)$$

ACK_s is the ACK message size which can't exceed 48 symbols (physical and MAC header plus configuration request payload) and T_{ack} is the turnaround time and corresponds to *aTurnaroundTime* value, which is 12 symbols. According to the standard, the required time for a node to switch from receive to transmission mode and vice versa is equal to *aTurnaroundTime* symbols. Thus, it has been included in this analysis.

Considering more than two hops is also still feasible, but the coordinator must provide at least four F slots in the bidirectional field to accomplish an association. This is caused by the T_{SZ} size limitation, where it is impossible to handle three transmissions in a single T_{SZ}. The required time is larger than the size of individual T_{SZ}:

$$3 \times Req_s + 2 \times T_{ack} + 3 \times ACK_s + SIFS > T_{Sz} \qquad (6.38)$$

Therefore, for 3-hops and 4-hops mobile nodes, the coordinator has to allocate at least four slots to complete the association process as in Fig. 6.4. The coordinator must be adjusted based on the number of permitted hops in the network. Hence, for a network that allows three hops, the coordinator is forced to allocate four slots [F1-F4] in order to guarantee smooth mobile node association.

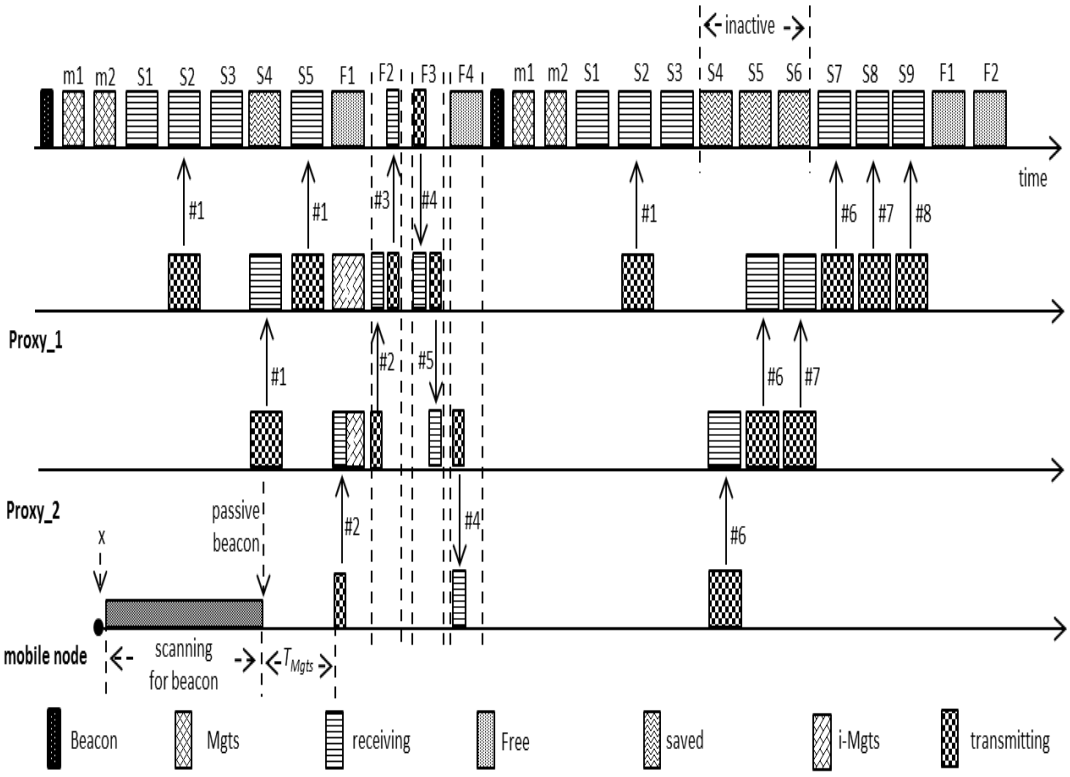


Fig. 6.4: 3-hops mobile node association in MA-LLDN

Seeking to avoid the hidden-node problem [159, 160] in multi hop networks, transmitting regular readings to the coordinator must be accompanied with the allocation of extra slots to the superframe. These slots will be called "*saved*" and the coordinator may stay inactive during these slots to save energy. The saved slots are required for the purpose of transferring data between mobile nodes and proxies as in {S4} in Fig. 6.3 and {S4, S5, S6} in Fig. 6.4.

For a given network, if at hop h=2 the set of proxy nodes $Prox_2=[R_1^2 - R_n^2]$ and at h=3 the set of proxies $Prox_3=[R_1^3 - R_m^3]$ are existed. The negotiations between a given mobile node M_x, proxy and coordinator C during the association phase at h=2 and h=3 described as in Table 6.1.

Table 6.1: Multihop communication messages

h=2	h=3
F1: $M_x \rightarrow R_x^1$	F1: $M_x \rightarrow R_x^2$
F1: $R \rightarrow C$	F2: $R_x^2 \rightarrow R_x^1$
F2: $C \rightarrow R_x^1$	F2: $R_x^1 \rightarrow C$
F2: $R_x^1 \rightarrow M_x$	F3: $C \rightarrow R_x^1$
	F3: $R_x^1 \rightarrow R_x^2$
	F4: $R_x^2 \rightarrow M_x$

Regarding the case of h=4, it will still be feasible to conduct the association within four slots [F1-F4] due the property of (6.37) and (6.38).

On the other hand, there are two important drawbacks in the structure of the LLDN. The first one is its dependency on three transmission states and the second is the sequence of the *Mgts* in the superframe. The first issue is caused by the types of transmission states which influence two crucial aspects in the network, throughput and association. The throughput is affected due to the transfer from the online state to other states, which will make the nodes refrain transmitting data until the coordinator switches again to the online state.

The association issue has already been indicated previously. Accordingly, the first enhancement can be achieved through swapping the *D_Mgts* with the *U_Mgts* (Fig. 3.7). Therefore, the coordinator can reply within the same superframe to the requested node instead of waiting to the next superframe. Thus, during *U_Mgts*, the mobile node requests association and the coordinator responds immediately at *D_Mgts.*

The second enhancement can be realized through modifying the structure of the two *Mgts*s. These two slots must be existed in each superframe and not optional as indicated by the standard, at least the superframe includes the *Mgts* in every period of time that corresponds to the mobility metric. In addition, in order to preserve network throughput and to minimize the dissociation time, the structure of the transmission states must be altered.

According to the LLDN, the nodes can only associate through the sequence of discovery then configuration states. These two states can be observed during the initialization phase of the network while during the steady state and since the coordinators is forced to keep *Mgts* in each superframe, these states can be omitted. Hence, the network keeps operating inside the online state without switching to other states and considers the *Mgts* to accomplish the required association process, as indicated in Fig. 6.3 and 6.4.

For limited power coordinators and multihop network, there will be some limitations regarding beaconing. This affects the period of beaconing and then maximizes the superframe duration S_O. This issue also can be caused by increasing the number of LLDN devices within the POS that in turn maximizes S_O. In this case, N_m and S_O influence the number of nodes N_w waiting to associate and this value could be increased as the coordinator increases S_O. Thus, there must be a mechanism to facilitate multiple mobile nodes associations within the same superframe.

In addition, restructuring the *Mgts* to accommodate multiple nodes and maintain these slots properly will preserve the functionality of the *Mgts* as dedicated by the standard which can be utilized for other purposes instead of association. Therefore, a backoff mechanism is proposed in this chapter to manage mobile node access during *Mgts*.

The proposed backoff technique relies on amending the *Mgts* size that can be achieved through utilizing the timeslot size field in the beacon. In addition, bits 5-7 in the flag fields of the beacon are utilized to define the number of base time slot in each *Mgts*. Hence, the *Mgts* can be constructed as a slotted access field by which it can resemble the contention access period (CAP) in the beacon enabled mode. The size of each slot (S_{Bmgts}) inside the *Mgts* can be estimated to be (in symbols):

$$S_{Bmgts} = Max\_Backoff\_Time + Total\_CCA\_duration + Maximim\_transmission\_time + SIFS$$

$$S_{Bmgts} = [(2^{BE} - 1) \times 20] + (2 \times 8) + 48 + 12$$

Hence, the maximum S_{Bmgts} size can be 216 symbols. The maximum transmission time has been set to 48 symbols with the assumption that the association request payload contains (full address, short address and 4-Byte for application-specific purposes). The proposed backoff mechanism is an amended version of the simplified CSMA-CA and the number of contentions is limited by the number of slots in a single *Mgts* (nS_{Bmgts}). Regarding the proposed backoff algorithm, *CW* and *BE* are set to 2 and 3 respectively as indicated by the standard for LLDN mode.

Fig. 6.5 simplifies the proposed backoff scheme by which to handle multiple mobile nodes access during the management time slots.

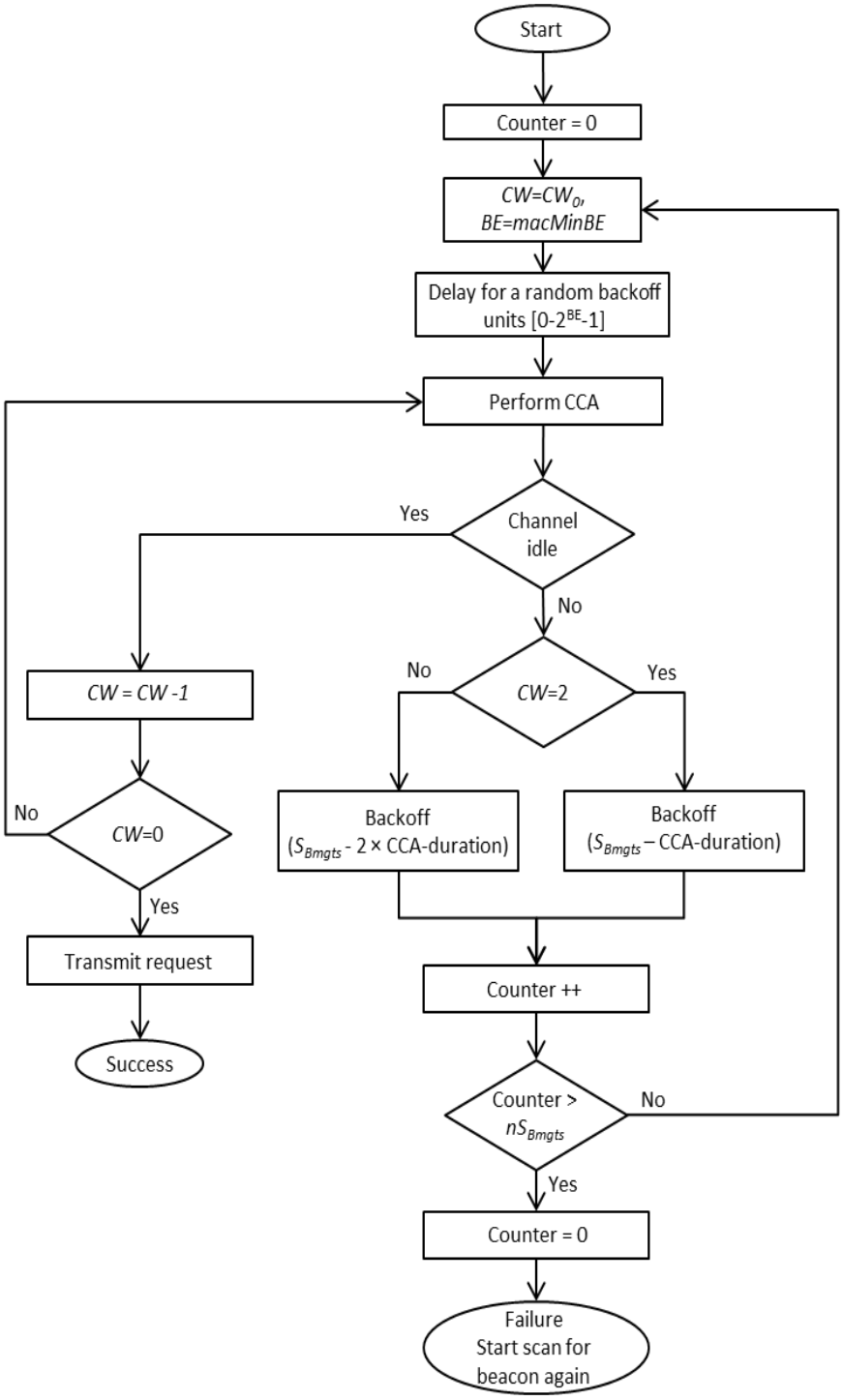


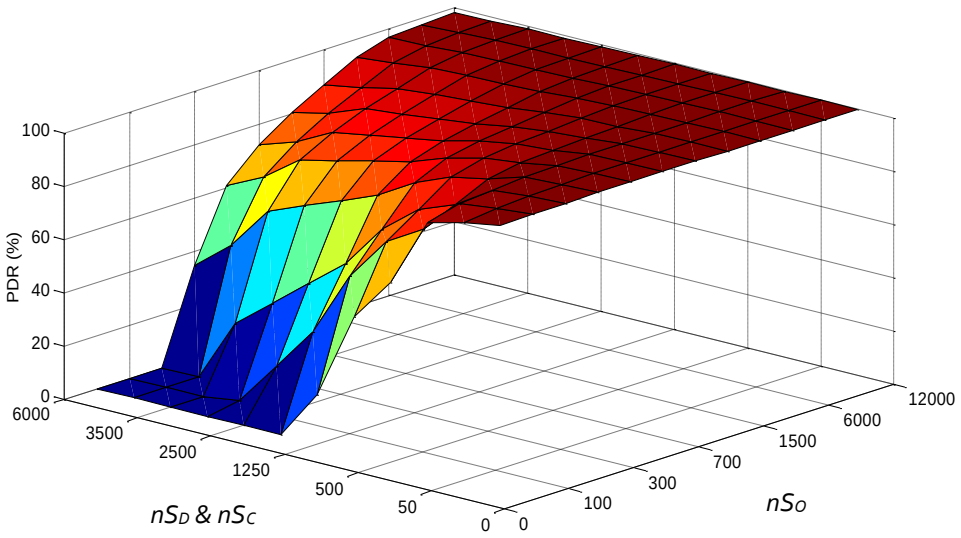
Fig. 6.5: Proposed MA-LLDN backoff scheme

6.5 Results and Analyses

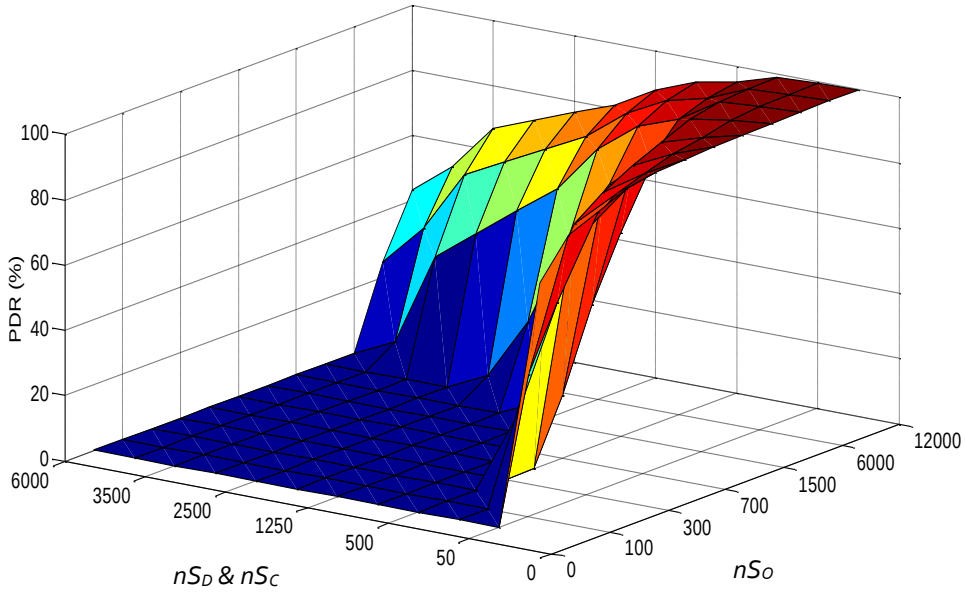
This section highlights three important aspects that are influenced by node mobility in LLDN network. PDR in static networks can be affected primarily by the number of collisions and interference within a network, but for mobile nodes new factors are included that degrade network PDR. Moreover, in LLDN networks there are two additional factors that reduce PDR. These are the excessive dissociations (due to changing POS) and the regular transfers from online state to other states. Thus, the first part of this section presents two factors related to PDR, one concerns the overhead of dissociation (named $PDR_{dissociation}$, for dissociated nodes) and the second considers the impact of transferring away from the online state (named $PDR_{transfer}$, for nodes already connected) that prevent the node from sending readings until the end of both discovery and configuration states. The $PDR_{transfer}$ is depending here on seven parameters that are S_O, S_C, S_D, nS_D, nS_C, nS_O and the number of slots in the superframe (corresponds to *macLLDNnumUplinkTS*). Increasing the number of slots maximizes the S_O value. S_C and S_D values are always fixed to 2.976ms and 2.528ms respectively since the structure of the superframe in these two states rarely changes (fixed number of fields in the superframe).

In addition, the values of nS_C and nS_D will always be equal since there must be an equivalent number of configuration superframes to accommodate the possible number of mobile nodes that have been considered in the discovery stage. In order to tackle the node mobility and achieve better network connectivity, the network administrator must increase the number of discovery and configuration superframes, nS_D and nS_C. Accordingly, this approach will minimize network $PDR_{transfer}$ due to the maximization of the period that the nodes are obliged to refrain transmitting readings prior the completion of discovery and configuration states.

The S_O duration (influenced by the number of slots) can worsen the case for low durations as indicated in Fig. 6.6 (a) and (b) that show a varying number of slots. The important feedback here is determining the ratio of discovery and configuration to online superframes ((nS_C+ nS_D)/nS_O).



(a): Slots=1, S_C=2.976ms, S_D=2.528ms, S_O=1.004ms



(b): Slots=40, S_C=2.976ms, S_D=2.528ms, S_O=168.48ms

Fig. 6.6: PDR (case of the impact of transfer from the online state)

Accordingly, to achieve a PDR no less than 98%, for slots (*macLLDNnumUplinkTS*) =1, 8, 20 and 40, then the ratio of the number of discovery and configuration to online superframes must be no larger than 0.08, 0.2, 0.33 and 1 respectively (nS_C&nS_D fixed to 50). Here the ratio corresponds to the number of online

superframe to one discovery and one configuration superframe.

The second parameter is $PDR_{dissociation}$ which is affected by the number and interval of dissociations periods from the network. The $PDR_{dissociation}$ is basically dependent on the transmission range and node mobility metric. Fig. 6.7 shows the impact of increasing the transmission range from 50m to 150m on the PDR. In this scenario, the impact of nS_O has the inverse effect to its impact on the $PDR_{transfer}$ in the case of transfer. Here, by increasing the nS_O, the value of SC_B is also maximized and hence, increasing the dissociation time which will reduce the $PDR_{dissociation}$. Unlike in $PDR_{transfer}$ case, here the target is looking for low nS_O to ensure high $PDR_{dissociation}$. In addition to the nS_O value, the number of slots per superframe influences the $PDR_{dissociation}$, where for few slots, better $PDR_{dissociation}$ can be achieved. This is traced to the impact of S_O on both SC_B and *Dis* that also maximizes dissociation time and in turn minimizes $PDR_{dissociation}$. Although the associated *AST* phase is deterministic, the remaining mobile node's lifecycle phases (SC_B, AST_{req} and *Dis*) are stochastic and thus, the impact will vary depending on the node's mobility metric.

Comparing Fig. 6.6 to Fig 6.7, it will be deduced that both nS_O and S_O have a contradictory role in both $PDR_{dissociation}$ and $PDR_{transfer}$. Fig. 6.7 (a) shows that for a transmission range of 50m, in order to achieve a PDR no less than 90%, the maximum number of nS_O has to be no more than 150. Meanwhile, for the case of 150m, the maximum nS_O value to gain no less than 91% PDR is 500. In summary, maximizing nS_O will increase the PDR for the connected nodes while reducing the PDR for the dissociated nodes. The dissociated nodes have to wait longer time until connecting due to long SC_B time that caused by large nS_O value.

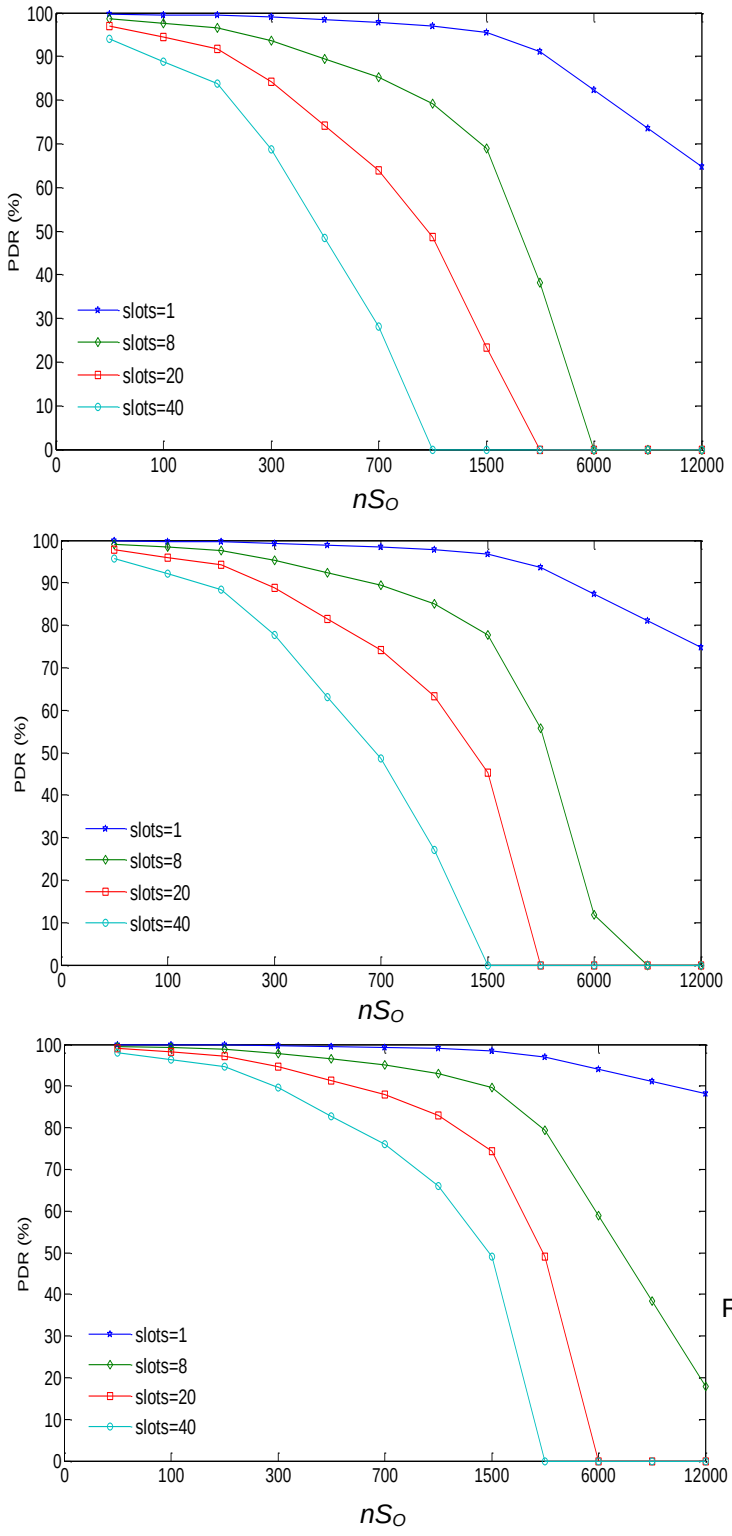
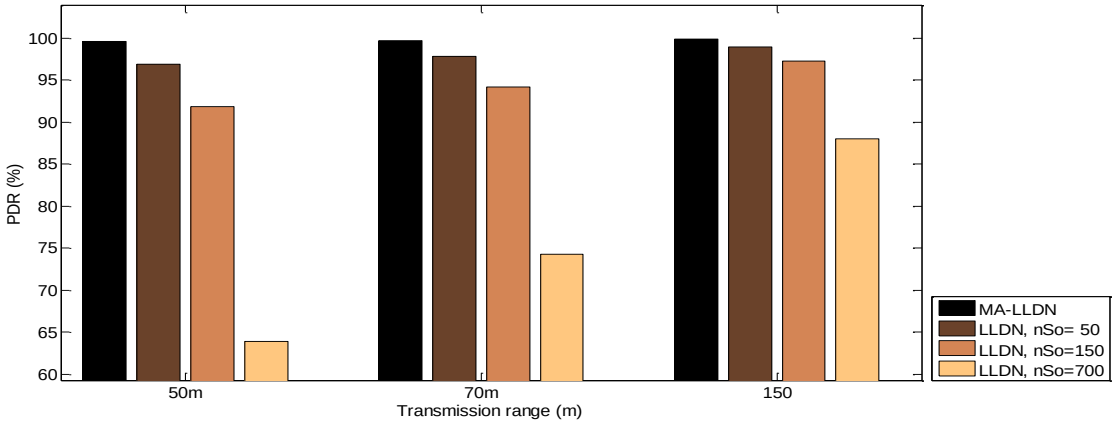
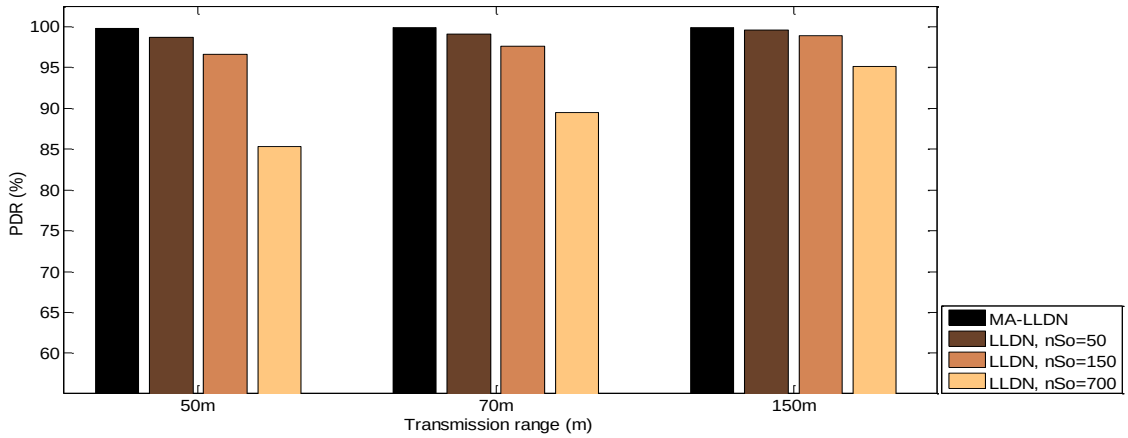


Fig. 6.7: PDR (dissociation), 𝔼[s]=6m/s, 𝔼[d]=9m, 𝔼[P]=6s, nS_C & nS_D=50 S_C=2.976ms, S_D=2.528ms,

In order to comprehend the advantage of the proposed MA-LLDN over LLDN, Fig. 6.8 (a) and (b) show how the MA-LLDN gains higher PDR than LLDN with regards to nS_C & nS_D =50, which is considered the best scenario for LLDN. By increasing *nSO* value, the default LLDN realizes lower PDR as indicated earlier in Fig 6.7.



(a): slots=8, S_O=34.208ms, S_C=2.976ms, S_D=2.528ms, nS_C =50

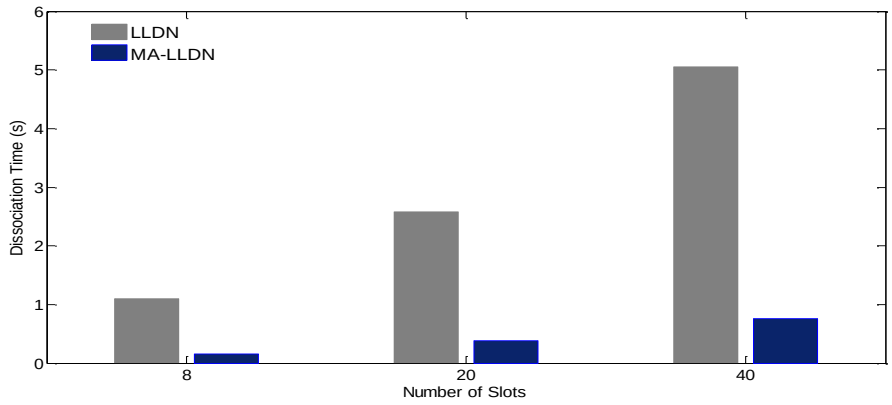


(b): slots=20, S_O= 84.576ms, S_C=2.976ms, S_D=2.528ms, nS_C =50

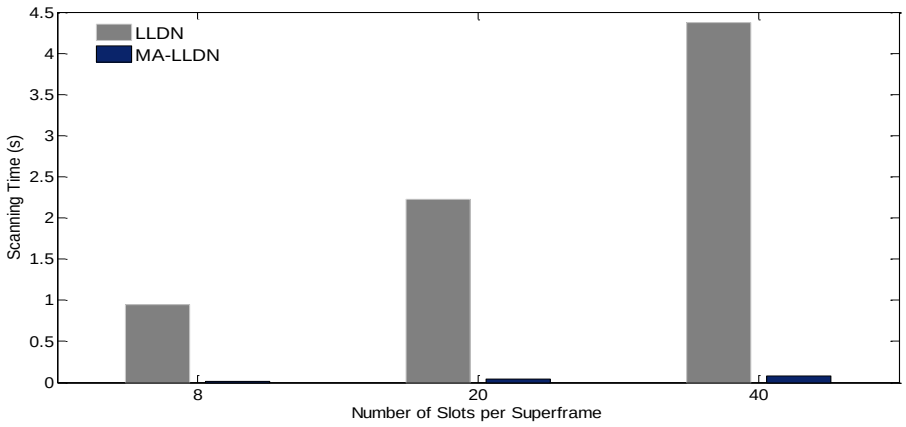
Fig. 6.8: Comparison between the PDR of both LLDN and MA-LLDN

Even while varying the number of slots or transmission range, MA-LLDN exhibits slightly different variations not as LLDN where maximizing number of slots has a significant drawback on the PDR. This is contributed by the dependency of MA-LLDN on the *Mgts* inside online state to accommodate mobile node association rather than flipping to discovery and configuration states (as is the default structure of LLDN). Moreover, the flexibility of MA-LLDN to make the online state accepts associations, led to ignore the impact of nS_C & nS_D on the dissociation issue.

In the meantime, in order to highlight the differences between MA-LLDN and LLDN in term of dissociation time, Fig. 6.9 (a) depicts how the MA-LLDN manages to obtain low dissociation time while nS_C & nS_D & nS_O =50. At these settings, the LLDN has its low dissociation time (increasing these parameters will maximize the dissociation time). The most influential factor to the dissociating time is the SC_B time which is depicted in Fig. 6.9 (b). The SC_B is mainly affected by S_O value which is raised by increasing the number of slots in each superframe. The demonstrated dissociation time in Fig. 6 (a) represents the expected time that a node will be disconnected from a network once it has left a POS.



(a): S_C=2.976ms, S_D=2.528ms, nS_C & nS_D & nS_O =50.



(b): S_D=2.528ms, nS_C & nS_D & nS_O =50

Fig. 6.9: Comparison between LLDN and MA-LLDN dissociation time

Fig. 6.10 describes the expected dissociated time with respect to the number of slots and nS_O. It identifies a real problem with LLDN that violates the target of low data latency caused by dissociation. It's clear that for large nS_O values the dissociation can be over 800s. Hence, for each dissociation, the node has to buffer data until it establishes again a connection with the network. Therefore, reducing the dissociation time will reduce dramatically the data latency of the buffered data.

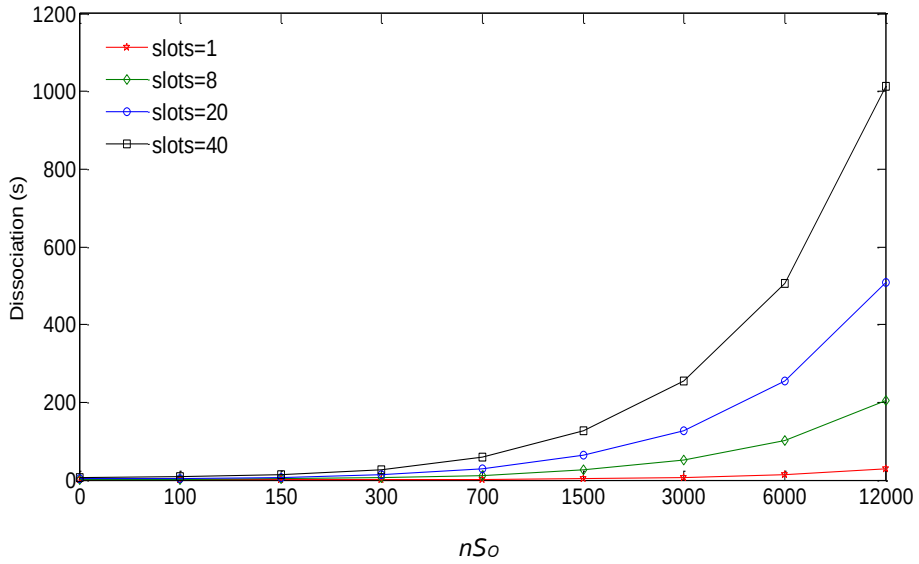


Fig. 6.10: Total dissociation time of LLDN, SC=2.976ms, S_D=2.528ms, nS_C & nS_D =50.

Accordingly, to meet the required target of LLDN for *macLLDNnumUplinkTS*=20 and a latency less than 10s, the maximum nS_O can be no greater than 200 as in Fig. 6.11. The realized $PDR_{dissociation}$ (regarding nS_O=200) could be about 87% for 50m range and 95% for 150m range. In addition, the maximum $PDR_{transfer}$ that can be ascertained based on these settings is 74%.

Fig. 6.11 shows the impact of latency incurred by dissociation versus throughput. The disadvantage at this point is that increasing nS_O here will rapidly raise the latency due to increasing the dissociation time, but in turn it has a slight advantage on the achieved throughput.

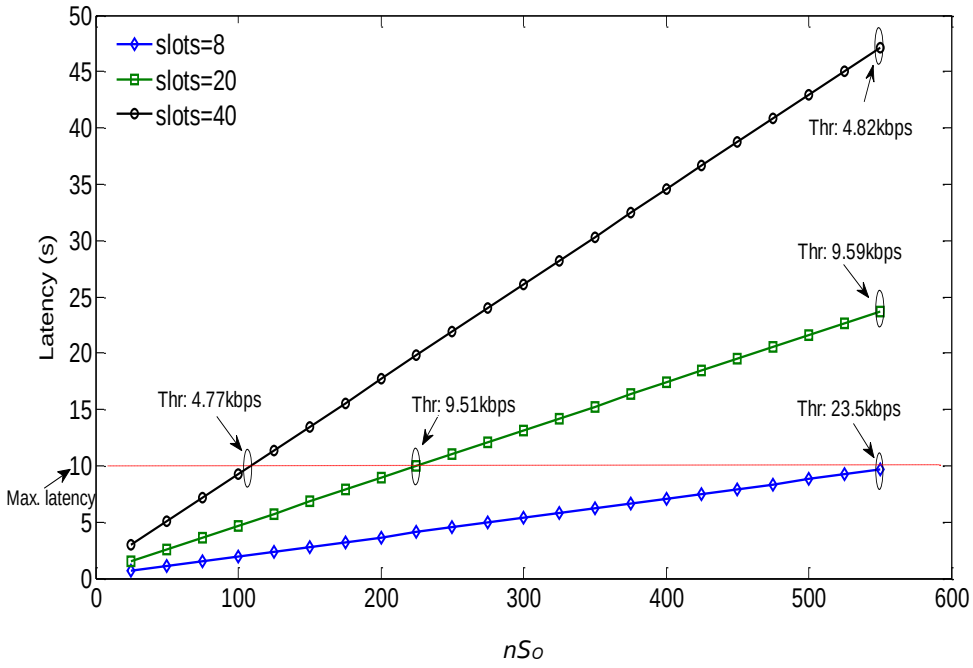


Fig. 6.11: Data latency caused by dissociating from the network in LLDN S_C=2.976ms, S_D=2.528ms, nS_C & nS_D =50.

Fig. 6.12 demonstrates the relation between the $PDR_{transfer}$ and the encountered average latency plus the ratio S_D, S_C over S_O. Seeking to reduce the latency (caused by dissociation) and to achieve higher connectivity intervals, the nS_O value must be reduced against nS_C and nS_D (increasing the S_O to S_D & S_C ratio). In turn, the $PDR_{transfer}$ is unfortunately dropping to its lowest rates of 20% and 68% for 0.81 and 0.32 ratios respectively (while fixing nS_O at 100). For low nS_C value as 50, the $PDR_{transfer}$ is rarely impacted and keeps a steady low degradation against decreasing nS_O. In summary, Fig. 6.12 shows the overhead of maintaining low latency (caused by data buffering for the dissociated nodes) on the $PDR_{transfer}$ of the associated nodes to the network.

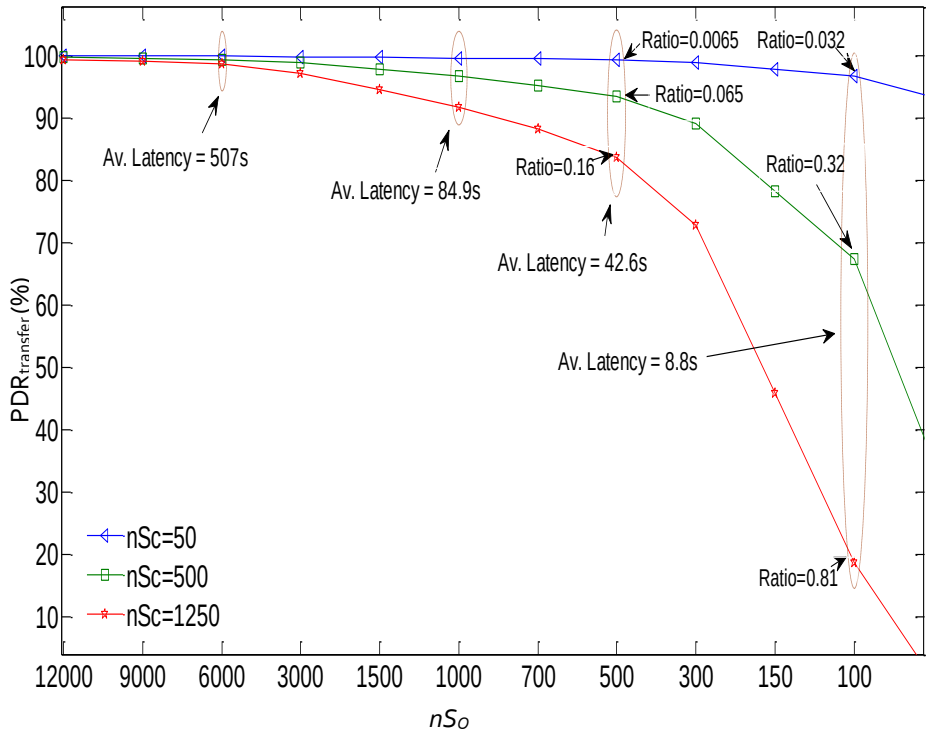
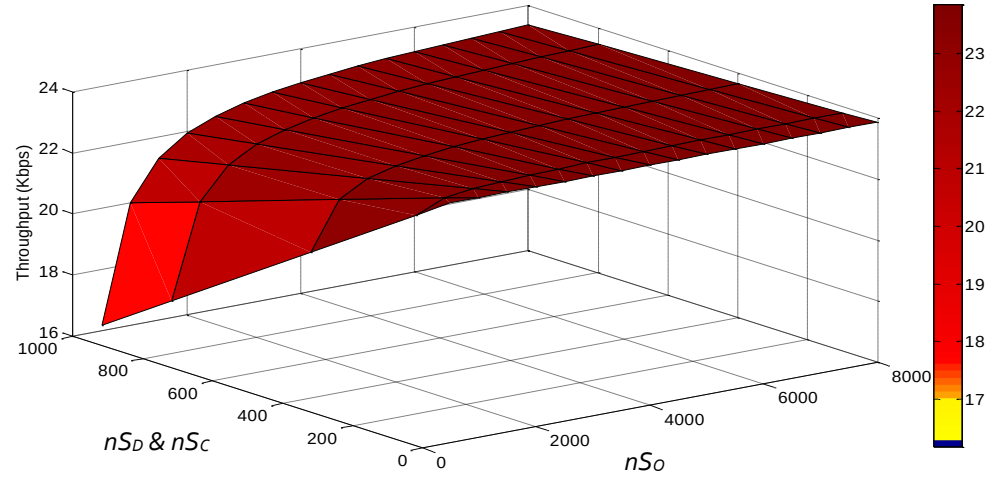
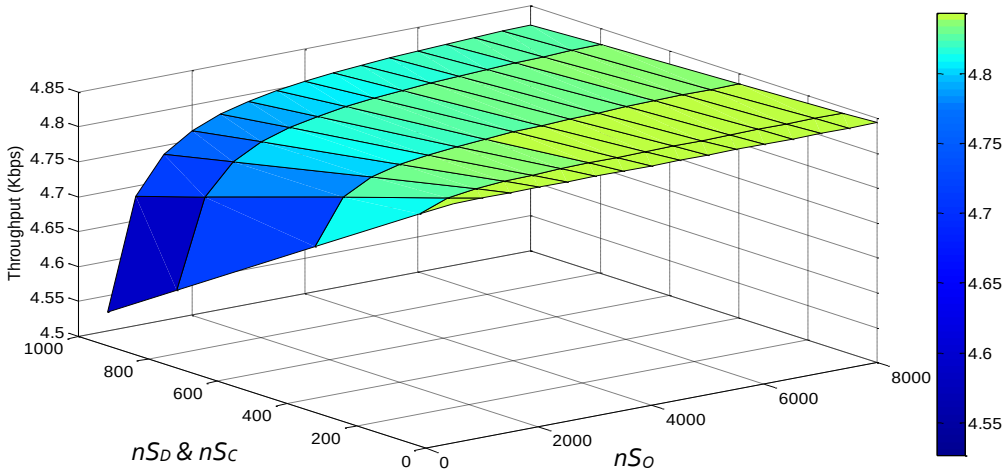


Fig. 6.12: Impact of (S_C & S_D/S_O) ratio on $PDR_{transfer}$, S_C=2.976ms, S_D=2.528ms, slots=20

Finally, Fig. 6.13 (a) and (b) give a snapshot regarding the LLDN node's throughput. The case of slots=1 (i.e. just a single node exists in the POS, *macLLDNnumUplinkTS*=1) has not included here, but in general the average throughput to meet a dissociation of no more than 10ms is 165kbps. Fig. 6.13 (a) (for slots=8) clearly shows an advantage over slots= 40 since the S_O size is being maximized with each slot number increase. In order to gain a dissociation less than 10ms, for the case of slots=8 and nS_C & nS_D=50, the average throughput is 23.5kbps. Regarding *macLLDNnumUplinkTS*=40 nodes and nS_C & nS_D=50, the throughput has declined to 4.7kbs which is caused by increasing the size of the superframe which means less transmission data rate. Hence, the throughput metric must be carefully considered in order to meet the target constrains of LL applications. Regarding this analysis, the transmission failure impact, caused by packet collisions, has been ignored due to the fact of assuming the nodes are running with a tight synchronization that can cancel any probability of collision.



(a): slots=8, S_O= 34.208ms, B_P=30symbols, MSDU=102B, S_C=2.976ms, S_D=2.528ms



(b): slots=40, S_O= 168.48ms, B_P=80symbols, MSDU=102B, S_C=2.976ms, S_D=2.528ms

Fig. 6.13: LLDN nodes throughput

Similarly, Fig. 6.14 demonstrates clearly the throughput of LLDN mode with regards to both analytical and simulation analyses with an LLDN superframe structure of 10 slots.

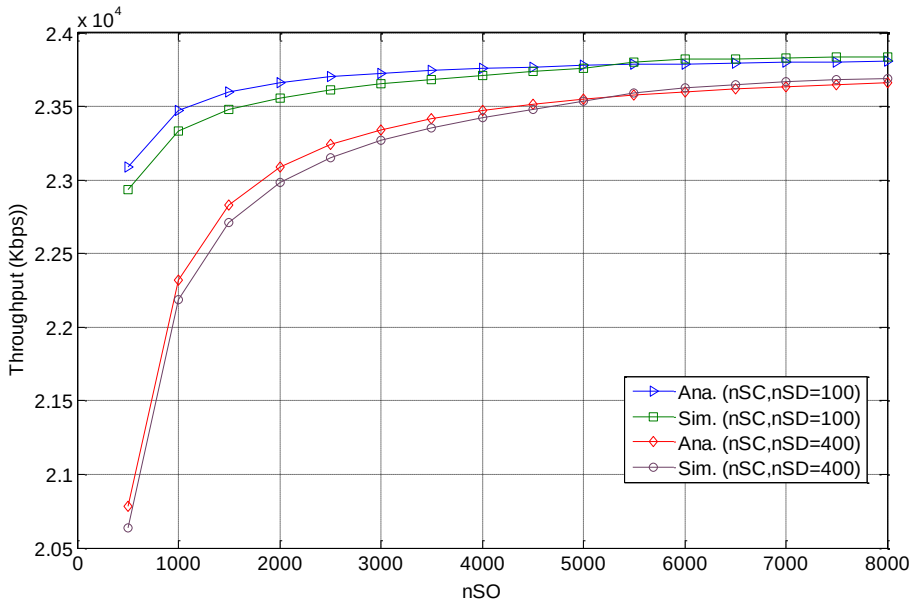


Fig. 6.14: Throughput of LLDN mode, MSDU=102B, S_C=2.976ms, S_D=2.528ms, slots=10

In the meantime, in order to determine the reliability of the network in term of handling node mobility, the dissociation function can be utilized to analyse this metric. Fig. 6.15 describes the dissociation function of both default LLDN mode and the proposed MA-LLDN scheme.

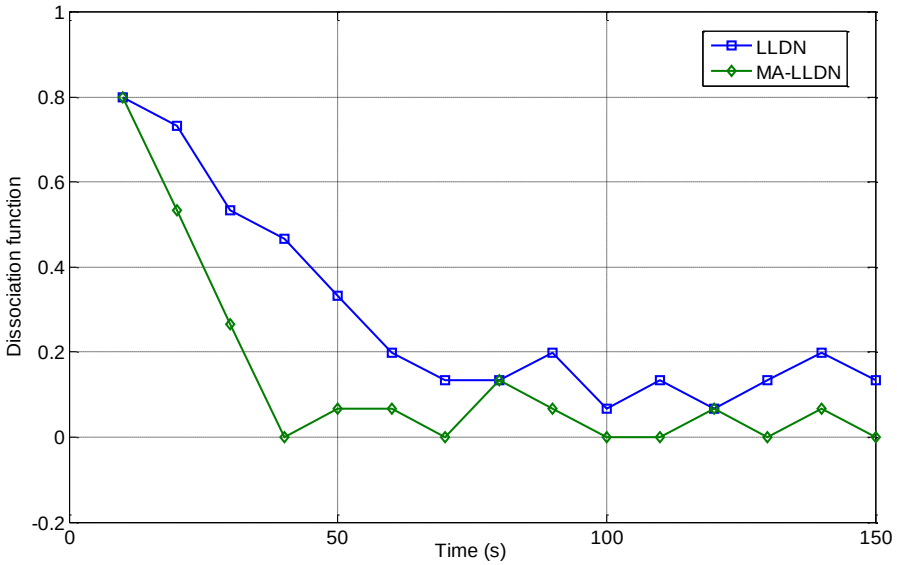


Fig. 6.15: Dissociation function, S_C=2.976ms, S_D=2.528ms, nS_C & nS_D =50.

During the initialization phase, the LLDN suffers from high dissociation factor due to the discussed mobility-related issues earlier in this chapter. Meanwhile, the MA-LLDN manages to push forward the network towards the steady state with less required time as in the case of LLDN. The new backoff mechanism (Fig. 6.5) manages to expedite the process of associating the mobile nodes with the network. In addition, eliminating both discovery and configuration states led to introduce low dissociation metric as compared with LLDN after network initialization phase.

Finally, the connectivity ratio of the LLDN mode is impacted mainly by three factors, transmission range, superframe duration and number of contending mobile nodes as presented in Fig. 6.16.

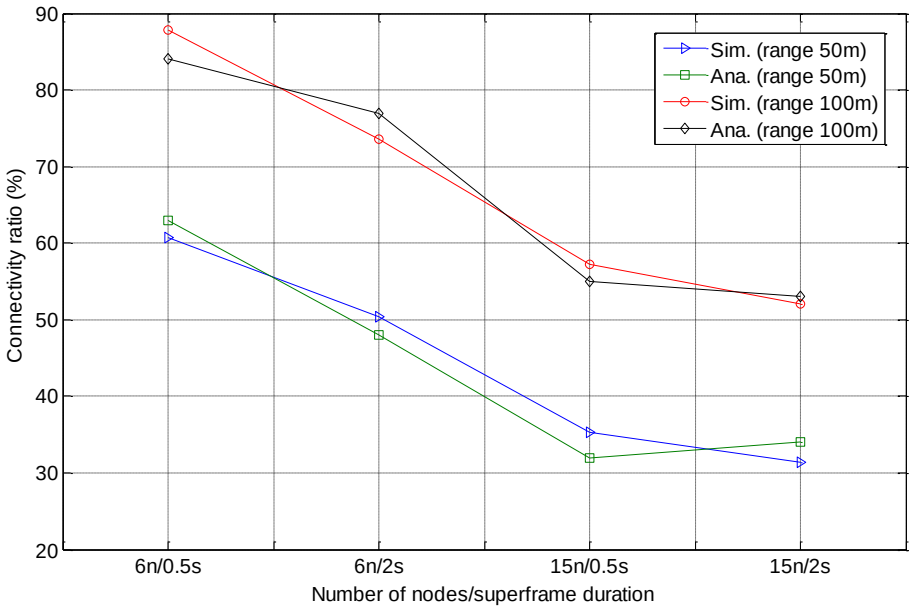


Fig. 6.16: LLDN connectivity ratio, nS_C & nS_D=50 S_C=2.976ms, S_D=2.528ms, number of coordinators: 4 (range 100m) & 9 (range 50m).

Maximizing the superframe interval from 0.5s to 2s has a significant impact for low transmission ranges and causes a mild overhead for high ranges (i.e. 100m). Moreover increasing the number of nodes has increased the dissociation time due to the impact of the nodes' contending process that reduces the probability of associating from the first attempt.

6.6 Summary

The objective of the IEEE 802.15.4e LLDN operation mode is to provide a deterministic network behaviour for several application types, especially industrial ones that require low latency. Unfortunately, the default IEEE 802.15.4e LLDN infrastructure suffers with the existence of mobile nodes. Accordingly, the objective of providing deterministic and LL services has been violated. This chapter has provided a comprehensive analysis to the impact of node mobility upon the LLDN while presenting a feasible approach to tackle the overhead of node movement. Even with a static scenario, the assumption of collecting sensor readings of 20 sensor nodes in less than 10ms is not valid unless the frame payload is only one byte as in (6.3). The proposed MA-LLDN model manages to reduce the dissociation time to be less than the interval of two online superframe durations. MA-LLDN reduces the dissociation delay in different scenarios by a factor of 75%. In addition, the MA-LLDN enhances the PDR in several cases by more than 30%. In addition, MA-LLDN provides a low latency multihop structure for the LLDN mode where the readings (of nodes that are more than one hop distance) can be delivered within the same superframe. Similarly, the relay nodes can advertise passively the existence of coordinator and act accordingly as proxies to the default coordinator. Hence, MA-LLDN manages to reduce the deployment cost and the probability of overlapped beacon collisions (due to reducing the required number of coordinators). The proposed cooperative beaconing strategy between regular nodes and the coordinators has maximized the coverage area and ensures low scanning and association time and in turn, high network connectivity achieved.

After providing a clustered IEEE 802.15.4 network through MUCBR and tackling the mobility via MTSCH and MA-LLDN protocols, the following chapter investigates the mobility-based security problem of the IoT MAC layer. Chapter seven highlights the main issues of mobile node security and presents a proposed key management scheme that supports the node movement under IEEE 802.15.4 standard.

Chapter 7. Secure Key Bootstrapping Scheme for Mobile IoT Devices

The security element is an upcoming crucial challenge within the IoT context. Its importance is traced to the way by which the security issue is affecting the availability of the network services and survivability. Several factors degrade the security of a network, specifically under the IoT paradigm, as node mobility, constrained resources, accessibility to the Internet and diversity of both IoT applications and requirements.

In order to provide security, there are multiple steps need to be considered that will ensure a solid secure network. These steps can be:

- Addressing which type of services to provide like confidentiality, authentication, integrity and access control.
- Determining the security techniques that will support the aforementioned services as symmetric cipher or asymmetric cipher techniques.
- Regarding selected ciphering technique, a key management scheme need to be established in order to support a secure key distributing mechanism.

These steps will form the general paradigm of the network security system and define what elements are needed to realize the required security level.

Under the IoT context, there are different approaches to provide security that are based on which layer handles network security. This can be either link-security, network security or application security.

For mobile low power devices and within the IoT case, the security must be enforced through either IPv6 or IEEE 802.15.4. Regarding the IEEE 802.15.4, this standard provides both confidentiality and authentication via eight security levels as below:

1) No security.
2) Authentication: through AES-CBC (32-bit).
3) Authentication: through AES-CBC (64-bit).
4) Authentication: through AES-CBC (128-bit).
5) Confidentiality: though AES-CTR.
6) Confidentiality and authentication: through AES-CCM (32-bit).

7) Confidentiality and authentication: through AES-CCM (64-bit).
8) Confidentiality and authentication: through AES-CCM (128-bit).

The security information that are provided through this standard can be indicated though setting the security enabled bit in the frame control to one which will add accordingly the auxiliary security header (up to 21-byte) to the default IEEE 802.15.4 frame (which is maximum 127-byte).

Although the standard provides data authenticity and confidentiality, it doesn't define a valid key management scheme to allocate the nodes in the network with the required set of keys that ensure the deployment of such security services.

Meanwhile, regarding the network stack layers, the 6LoWPAN adaptation layer has no security approach [36] which can be resulted by the functionality of this layer that is only existed to provide fragmentation/defragmentation and compression/decompression. The IPv6 protocol relies on the IPsec protocol which is considered to have high overhead over the constrained devices [66, 161]. In the meantime, the SSL [162] can also be a good candidate for the IoT stack but it doesn't match the constrained devices limitations since the SSL relies on the X.509 certificate [163] public key system to distribute the required keys. Moreover, there is another solution represented by the S-HTTP security protocol [164] but it isn't applicable for low power devices since the HTTP itself is not in use and the CoAP is utilized instead.

The CoAP in [165] has been enforced with a light version of the DTLS protocol [166] by which the headers in the default DTLS have been compressed to minimize the communication overhead. However, the proposed work doesn't support any key handling scheme.

Based on the discussion earlier, it is clear that there is a lack to an energy efficient and secure keying scheme that will be integrated into the IoT structure of the low power mobile IoT devices. There are few contributions in this field that are completely employing the public key system to distribute the required network keys, which in turn maximize the computation burden on the nodes. Hence, any proposed architecture must bare in mind the exclusion of any sort of public key system while ensuring both security and scalability/flexibility that can be inherited through public key approaches.

7.1 Related Work:

This section highlights recent approaches that address the security issue within the IoT context. Majority of contributions in this field have considered the impact of providing both data confidentiality and authenticity in order to reduce the impact of utilizing some of the current security approaches. Meanwhile, there is a little effort to tackle the issue of key management while others have just assumed deploying asymmetric key approaches due to their simplicity and security strength.

j. Ramos *et al*. [167] have addressed the issue of providing both authorization and authentication services for constrained smart objects. For the bootstrapping phase, the authors suggest to utilize the extensible authentication protocols over LAN (WAPOL) [168] but in its lightweight version with integration of two protocols (EAP) [169] and (RADIUS) [170]. In addition, to provide authentication and authorization, the structure of the network has to provide four terminal points which are non-constrained devices, EAP authenticator, EAP server and Authorization server. The existence of such servers will maximize the network security but on the other hand will tend to maximize the communication cost and increase the network deployment cost.

D. Altolini *et al* [171] study the impact of the link layer IoT security overhead and provide both software and hardware implementations. The link layer structure that has been considered is based on the AES cipher algorithm with multiple modes of operation (i.e. CTR, CBC and CCM). The authors have examined the energy overhead, memory footprint and latency. The analysis has showed that providing link-layer security hardware implementation has saved the energy consumption for up to six times as compared to SW implementation. In addition, the authors have introduced two types of code implementations, optimized code (minimizing memory usage through reducing code size) and the default un-optimized code.

P. kumar *et al*. [172] have presented a secure key establishment scheme for constrained devices in a smart home environment. The proposed model relies only on the hash function and AES-based MAuC schemes instead of any asymmetric technique to preserve energy. The authors show that the proposed approach has less energy consumption as compared with literature. In addition, the authors manage to minimize the number of required messages to establish secure pair-wise keys to tackle the issue of security-based communication overhead.

G. Piro *et al*. [173] present a security framework for the IEEE 802.15.4 standard that provide multiple security levels besides a key distribution scheme. The authors relies

on either RSA or Diffie-Hellman approaches to provide a key management services. The authors managed to fill the gap of the required security architecture for the IEEE 802.15.4 but did not provide any analysis over the impact of the proposed protocol as regards to energy consumption.

S. Sciancalepore *et al*. [174] provide a full analysis over the impact of security over IEEE 802.15.4 standard in terms of the required time to encrypt a full MAC frame, communication-based latencies caused by deploying security mechanisms and overhead of the key establishment phase. The authors propose a key management approach for the IEEE 802.15.4 that utilizes the Diffie-Hellman methodology. Relying on the Diffie-Hellman has a major drawback on the network since it tends to maximize communication overhead due to the number of required messages to exchange the relative prime numbers to establish the link key. This is traced to the limitation of the IEEE 802.15.4 frame size while the minimum prime number sizes should not be less than 512-byte.

Other previous approaches like [175], [176] and [177] are mainly focusing on how to adapt the public key system schemes into the IoT system and thus, the overhead of these public ley systems will be inherited and degrades network performance.

7.2 Energy Efficient Key Bootstrapping Scheme for Mobile Low Power Devices

The initializing process of the nodes with the required link-keys must ensure two important criteria, providing secure key distribution scheme and minimizing the energy cost of generating the required shared keys for the nodes in the network. One of the key strategical decisions here is to avoid the dependency on any sort of public key methodologies to overcome any resulted overhead. Hence, the devised approach must completely rely on both symmetric cipher techniques and hash functions.

The proposed work here presents energy efficient secure key bootstrapping (EESKB) scheme that provides the nodes with the required keys for secure communication. The proposed scheme is utilizing the IEEE 802.15.4 communication infrastructure and the proposed work (MUCBR) which has been presented in chapter 4. The approach here is to utilize the messages that have been used to initialize the nodes into clusters for distributing the required keys to activate the security service of the IEEE 802.15.4. Therefore, instead of dedicating different security-based communication phase during the network initialization lifetime, the

network initialization period will be shortened while the energy cost of deploying the nodes and engaging them into the field will be minimized. This traced to the fact that the same command frames, which are required for arranging the nodes into clusters, are exploited to manage the link-keys within each cluster in the network.

The proposed EESKB provides two modes of operation, the first one is invoked during the network initialization phase by which the nodes will establish shared keys with the nearest CHs in the network based on the MUCBR (and can be with each adjacent node according to how the nodes will be structured in the network). The second mode is dealing with the mobile nodes that have already joined the network during the initialization phase but have been disconnect from the default CH (due to movement) and need to re-associate with a new CH (in the new visited perimeter). The proposed EESKB also matches the message sequence charts for both default association and FastA schemes of the IEEE 802.15.4. In addition, it can be exploited during the 6LoWPAN neighbour discovery protocol since it has the same required number of messages.

7.2.1 Methodology:

The proposed EESKB protocol is basically resembling the default Kerberos [2] technique (in term of ticketing) and handles mobile nodes while authenticating them in the network as they change CHs after each movement. The presented technique is relying on the previous shared CH-pairwise key to authenticate the identity of a MN with a new CH. In addition, it only utilizes a single a message in order to finalize the authentication/association process (by limiting the security-based information to the maximum payload limit of the IEEE 802.15.4). Moreover, the EESKB utilizes the multipath-routing feature of the MUCBR that suggests the familiarity of any coordinator with all surrounding coordinators to provide efficient routing and realize redundancy. Hence, all the coordinators/CHs have a list of pair-wised keys of all neighbour CHs. Thus, any mobile node that migrates form its own default cluster to a neighbour cluster, it will exploit the old CH pairwise-link key with the new CH in order to authenticate itself. The old key here is acting as a ticket to facilitate mobile node authentication and accomplish association.

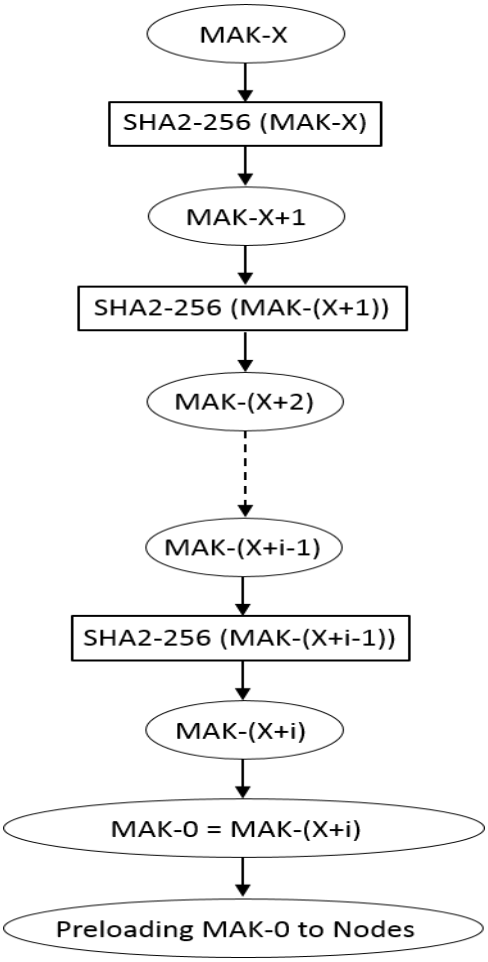


Fig. 7.1: MAK generation procedure

7.2.1.1 Initialization phase:

The first action, after the nodes are deployed in the field, is to arrange the nodes into clusters (can be trees or any sort of network structure based on the network scheduling scheme) and establishes the shortest roots to the network aggregation points through CHs. The EESKB exploits the IEEE 802.15.4 frames used by the MUCBR to initialize the required link-keys without affecting either MUCBR or the mechanism of the IEEE 802.15.4. As stated earlier, the EESKB also can be adapted to either IEEE 802.15.4 or 6LoWPAN messages sequence charts and not only restricted to the MUCBR.

Each node in the network will be preloaded initially with a key called the master key (MAK) that will be generated (as described in Fig. 7.1) by the network coordinator and has a sequence in the hash chain. The network coordinator generates the

required number of keys through a hash function (i.e. SHA2) and export the last generated key (MAK-0) to the nodes prior deployment. Fig. 7.1 states the derivation process of the first preloaded key (MAK-0) that has been generated, through several hash (i.e i^{th} iterations) function iterations, originally from MAK-X. Hence, MAK-0 = $[SHA2\text{-}256]^i$ (MAK-X). Note that keys in the range MAK-X to MAK-(X+i-1) are stored and will be released later whenever the network administrator seeks to update the recent key.

After node deployment, the first step of the key establishment phase is generating the node-base key that is formed through hashing MAK-0, node ID (represented by the short address or EUI unique node address) and a random number generated by each node. As example, for node called A, the node-base key of node A is:

$$K_A = SHA2\text{-}256\ (Ran\_A \parallel MAK\text{-}0 \parallel A)$$

A is the node ID and Ran_A is a random number generated by node A. (||) symbol denotes the concatenation process. The second step will be determined by the neighbouring discovery scheme (as 6LoWPAN discovery protocol [178]) since the proposed EESKB will utilize the advertising messages without any extra overhead. In this work, the MUCBR is the current platform to establish the network and the EESKB is embedding its key- related information into broadcasted frames. Each node will announce its generated node-base and encrypted/authenticated using MAK-0 (the ciphering is based on the AES-128 algorithm and the frames are authenticated using AES-CBC-128).

$$MAuC\ [CIP_{MAK\text{-}0}(K_A), MAK\text{-}0]$$

Each node during this period will also listen for all neighbour nodes' announcements and record received node-base keys. After a specific time (TS) that corresponds to a duration by which all the nodes within a single POS can exchange all the node-base keys without any issue, each node starts to generate all the related link-keys with the adjacent nodes (can be with only the CH if it's a clustering structure).

Fig. 7.2 presents the pseudocode of the establishment process and will be executed by each node in the network (except the coordinator).

```
Begin
    Set A = node_ID;
    Ran_A = random_rand();
    K_A = SHA2-256 (Ran_A || MAK-0 || A);
    Start_Broadcasting…// based on the scheduling or sampling technique
        MAuC [CIP_MAK-0 (K_A), MAK-0];
    End_Broadcasting
    Start_Listening…
        WHILE (current_time < current_time + TS)
            IF (received key announcement) && Authenticated
                NGH_ID[i] = source_address; // i.e. node B
                K_B = DEP_MAK-0 (payload);
                IF (A_ID > B_ID)
                    K_A,B = SHA2-256 (K_A || K_B || MAK-0);
                ELSE
                    K_A,B = SHA2-256 (K_B || K_A || MAK-0);
                End_IF
                i++;
            End_IF
        End_WHILE
    End_Listening
    MAK-1 = SHA2-26 (MAK-0);
    Delete (MAK-0);
End
```

Fig. 7.2: Pseudocode of establishing shared link keys (EESKB)

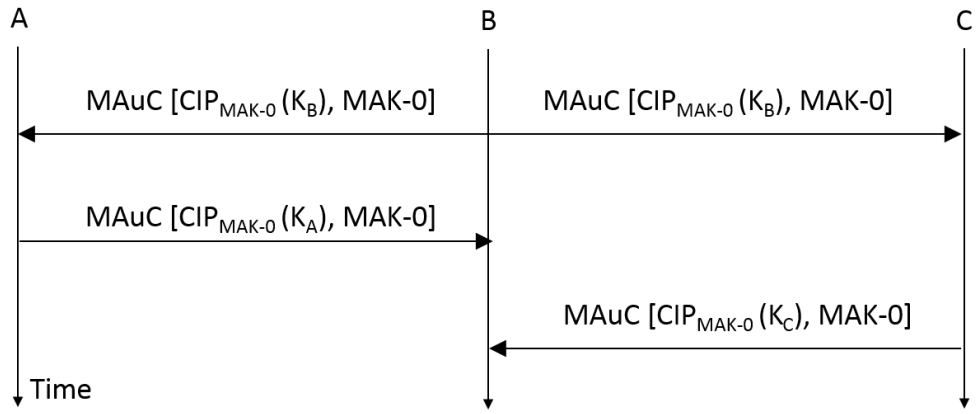


Fig. 7.3: Message sequence chart of the proposed EESKB establishment process

Fig. 7.3 indicates how the nodes communicate with each other to establish the required pair-wise keys. The nodes can decrypt all the received frames utilizing the AES technique to extract the neighbour node-base key, if node B is an adjacent node:

$$K_B = DEP_{MAK-0} \text{ (payload)}$$

Accordingly, both nodes can generate the pair-wise key which is shared between these two nodes and will be unique in the network. In order to mitigate the issue of generating false keys caused by different blocks sequence of the hashing input data, the nodes will determine the correct sequence based on the node ID value. Hence, in this case, if node A address is higher than node B, then:

$$K_{A,B} = \text{SHA2-256 } (K_A \parallel K_B \parallel \text{MAK-0})$$

Otherwise:

$$K_{A,B} = \text{SHA2-256 } (K_B \parallel K_A \parallel \text{MAK-0})$$

This process will continue until each node generates its pair-wise key with all adjacent nodes based on their received node-base keys (in the case of clustering, this process will be conducted only with the CH).

The final step is deleting the master key (MAK-0) to tackle the issue of node compromise and eliminate any chance for the attacker to generate more link keys with other nodes in the network.

Fig. 7.4 shows the possible keys lists for each node after the establishment phase in a sample of network. Each node must first have the second generated MAK which is MAK-1, since MAK-0 has been deleted after the initialization process. In addition, the list of key has to include the node-base keys with the link-keys of each adjacent node.

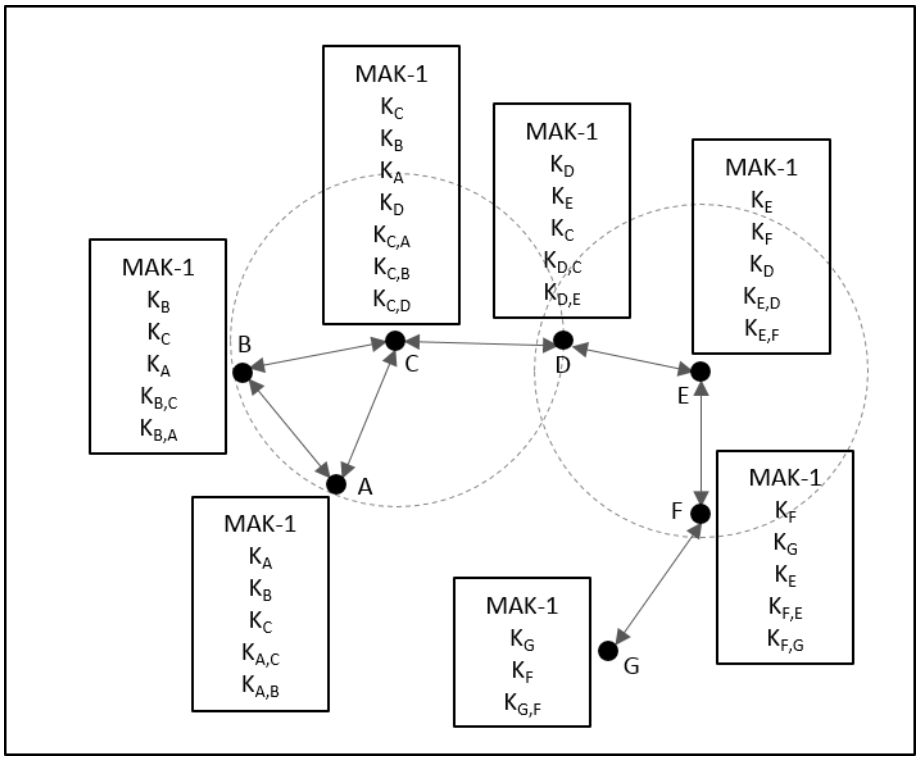


Fig. 7.4: Shared keys lists (EESKB)

7.2.1.2 Secure Mobile Node Association:

During the network steady state, after nodes deployment, and due to node movement, the mobile nodes tend to leave the current cluster associated with and need to join a new cluster. In order to ensure that there are no malicious nodes will have the ability to access and join the network, security measures have to be considered to mitigate this issue. Accordingly, besides providing mobility management schemes to handle movement and minimize the mobile node dissociation time as described in both chapters three, five and six, there must be a secure scheme to ensure only legitimate mobile nodes can join the network. Meanwhile, for any scheme that has to enforce secure association, it must ensure low overhead (both computation and communication) on the mobile nodes.

Accordingly, the proposed EESKB has to guarantee two aspects, energy efficiency and secure mobile node association.

EESKB is considering the same messages, association requests, utilized in the process of associating to a new CH (or coordinator). This will reduce the cost of applying the security scheme since validating new mobile node authenticity is integrated into the communication infrastructure of the association process (examples on these processes can be seen in chapters three, five and six).

A mobile node that has lost a connection with the network will start a new association process to join the network. Within the association request, the node embeds any security-related information in order to validate its authenticity and accordingly receive the permission to join the network. The EESKB utilizes the principle of "Ticket" from the Kerberos protocol by which the ticket here corresponds to the key with the old CH. Since every CH has a list of all adjacent node-base keys, then all CHs can prove whether the new mobile node was originally associated with the network through one of the neighbour CHs or not.

Fig. 7.5 demonstrates the algorithm by which a mobile executes in order to authenticate itself with a new CH. The mobile node generates a random number (Ran_M) and sends it with the ID of the old CH as plain text (not ciphered) to the new CH. This information must be in plain to permit the new CH from fetching the required security credentials of the old CH.

In addition, the node sends its base key encrypted by the old CH's base key with the hash value of old CH base key, random number and a time information stamp (TIS) that's is required to tackle any chance of commencing a replay attack.

$$\text{Old\_CH\_ID, Ran\_M, SHA2-256 } (K_{old\_CH} \,||\, \text{Ran\_M} \,||\, \text{TIS}), \text{CIP}_{K\_old\_CH}\,(K_M)$$

After successful request transmission, the mobile node listens for a response from the CH that is also embedded within the confirmation reply message for the request of association (also can be one of the association mechanisms depicted in chapters three, five and six). The CH upon receiving the mobile node base key, random value and TIS, will examine if this message is a replay attack by validating the TIS value. Based on a correct validation, the CH can decrypt the mobile node base key K_M since it is aware of its neighbour CHs base key which the mobile node was previously connected with before. Accordingly, the CH encrypts its base key K_{new_CH} with also K_{old_CH} and send it back with the association reply.

```
Begin
        Ran_M = random_rand();
        Scan_for_Beacons… // scan for any network indicators
        IF (received_beacon)
                New_CH = source_address;
                Fetch (association_configurations);//based on mode of operation
        End_IF
        Send… // based on the specified access scheme of the network
                Old_CH_ID, Ran_M, SHA2-256(K_old_CH || Ran_M || TIS), CIP_K_old_CH (K_M);
        End // if transmission was successful
        Listen… // receive association and security-based information
                Knew_CH = DEP_K_old_CH (payload);
        End
        IF (M_ID > New_CH_ID)
                K_M,New_CH = SHA2-256 (K_M || K_new_CH || MAK-j);
        ELSE
                K_M,New_CH = SHA2-256 (K_new_CH || K_M || MAK-j);
        ENF_IF
        Delete (K_old_CH);
END
```

Fig. 7.5: Pseudocode of mobile node association procedure (EESKB)

Finally, both mobile node and CH can generate their new link key based on the same methodology during the initialization, with respect to the highest ID value:

$$K_{M,New\_CH} = SHA2\text{-}256\ (K_M \parallel K_{new\_CH} \parallel MAK\text{-}j)$$

The pervious forma is assuming the ID of mobile node is higher than the ID of new CH. The required messages and their contents of this association scheme are defined in Fig. 7.6.

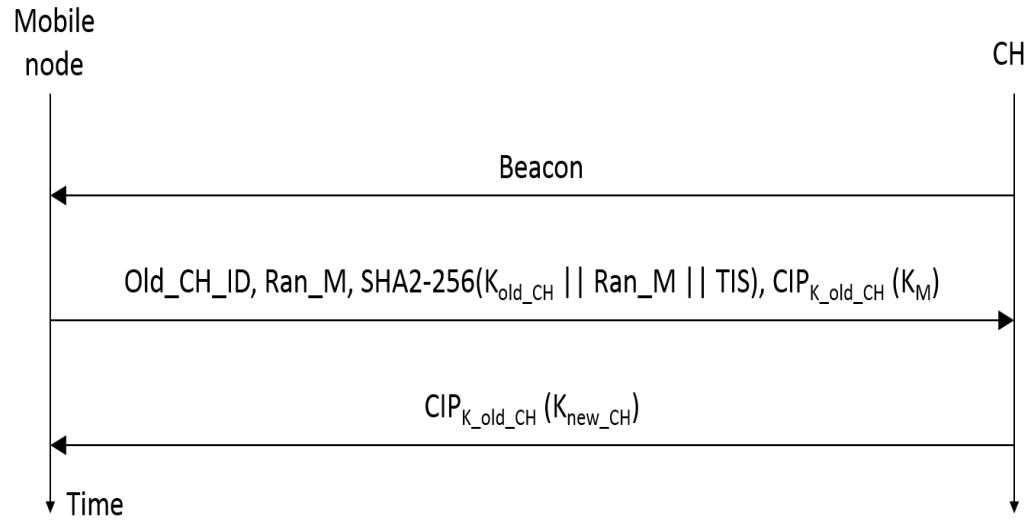


Fig. 7.6: EESKB mobile node association message sequence chart

The final step for the mobile node is deleting the link key and the base key of the old CH besides synchronizing with the new CH, based on the new CH configurations.

7.3 Confidentiality and Authentication Services for IEEE 802.15.4

The default structure of the IEEE 802.15.4 standard is exploiting the AES-CBC and AES-CCM modes to provide authentication and confidentiality services respectively. The AES-CBC mode is depicted in Fig.7.7 that utilizes the AES cipher algorithm to generate the MAuC value which will be transmitted by the sender with each outgoing frame. The receiver verifies the authenticity of the received message through re-generating the same value and compares it with the received incoming MAuC to validate the identity of the sender and data integrity.

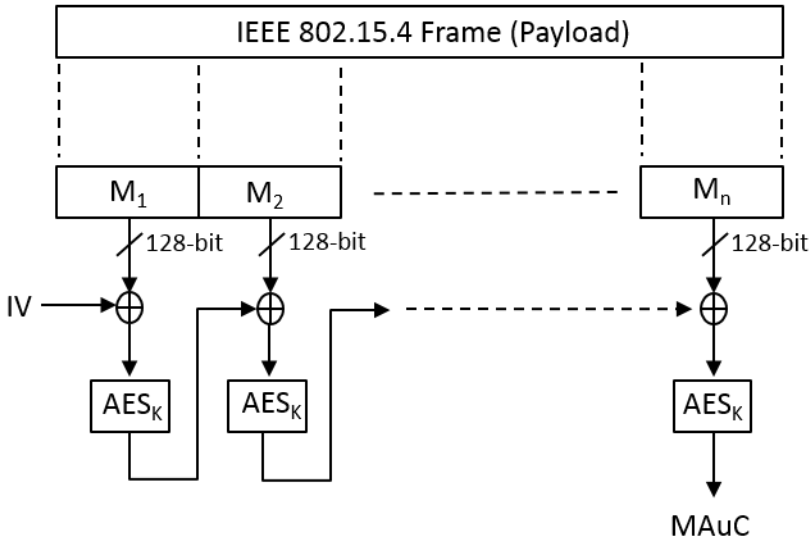


Fig. 7.7: AES-CBC MAuC generation diagram

Similarly, the standard depends on the AES-CCM mode that is a hybrid technique between both CBC and counter mode to provide data encryption and authentication. The AES-CCM mode is described in Fig. 7.8 (visualised according to CCM scheme [2]) which explains how the CCM mode performs first the CBC mode (to obtain MAuC) and then the counter mode to encrypt the IEEE 802.15.4's payload. C_0 represents the MAuC value while $C=\{C_1,C_2,\ldots C_n\}$ correspond to the output cipher text.

The IEEE 802.15.4 standard utilizes the AES cipher algorithm to provide the related link-layer security services. Hence, all the simulations in this research have adapted this algorithm in order to examine the advantage of the modified IEEE 802.15.4 structure over the default one.

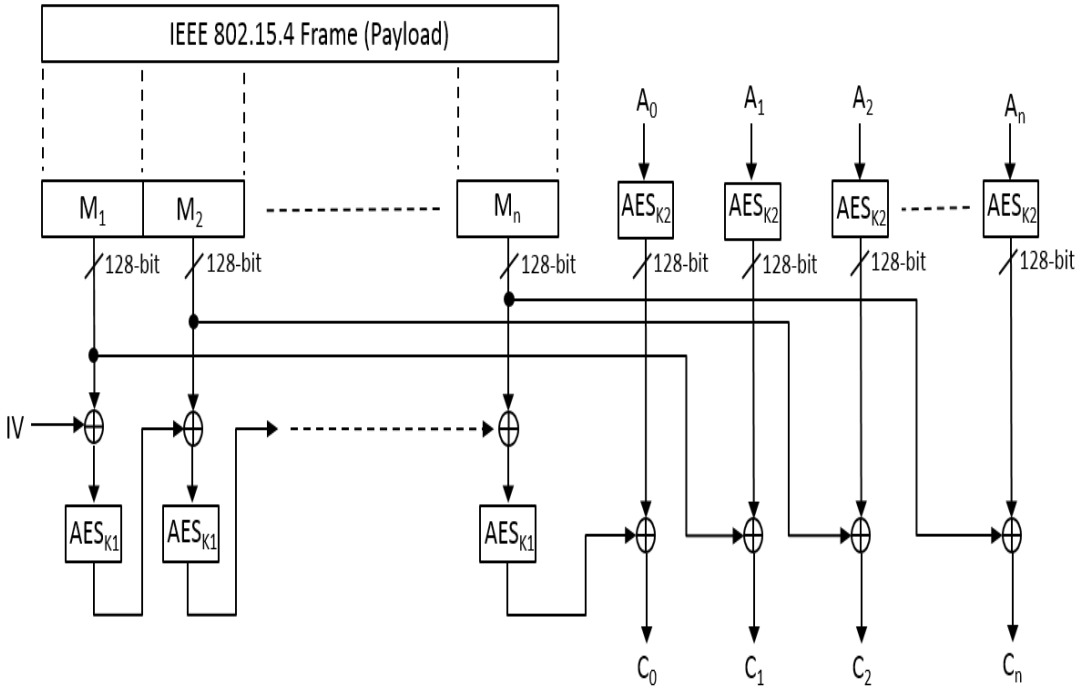


Fig. 7.8: AES-CCM mode diagram

Few contributions in this area address the impact of modes of operations on the constrained nodes. [171] shows how these modes can be optimized through an alternative hardware implementation that can reduce the software-based energy cost. [179] indicates the overhead of IEEE 802.15.4-related modes of operation with different payload sizes and their incurred latencies. The study utilizes the TelosB hardware to investigate the impact of providing link security services through the IEEE 802.15.4 but did not provide any suggestions on how to minimize the energy cost.

Accordingly, in this work, an alternative design is presented that minimizes the cost of providing both confidentiality and authentication services via the IEEE 802.15.4 standard. The proposed approach here is relying on the hash MAuC (HMAuC) principle rather than the CBC mode to support authentication. In addition, data confidentiality is still achieved through the AES algorithm but integrated with the HMAuC rather than the AES-CCM mode.

There are two main optimization points in the proposed alternative method. First, the hash technique here (i.e. SHA2-256) has less execution time and then less energy consumption. Second, the SHA2-256 takes an input block size of 512-bit as compared to the AES, which is 128-bit. Accordingly, this reduces the latency of

authenticating data to four times as the original mode. Fig. 7.9 shows an example on how to generate a HMAuC value via the hash functions. The (ipad) and (opad) values are used interchangeably to produce two different keys from a single key as indicated in [2].

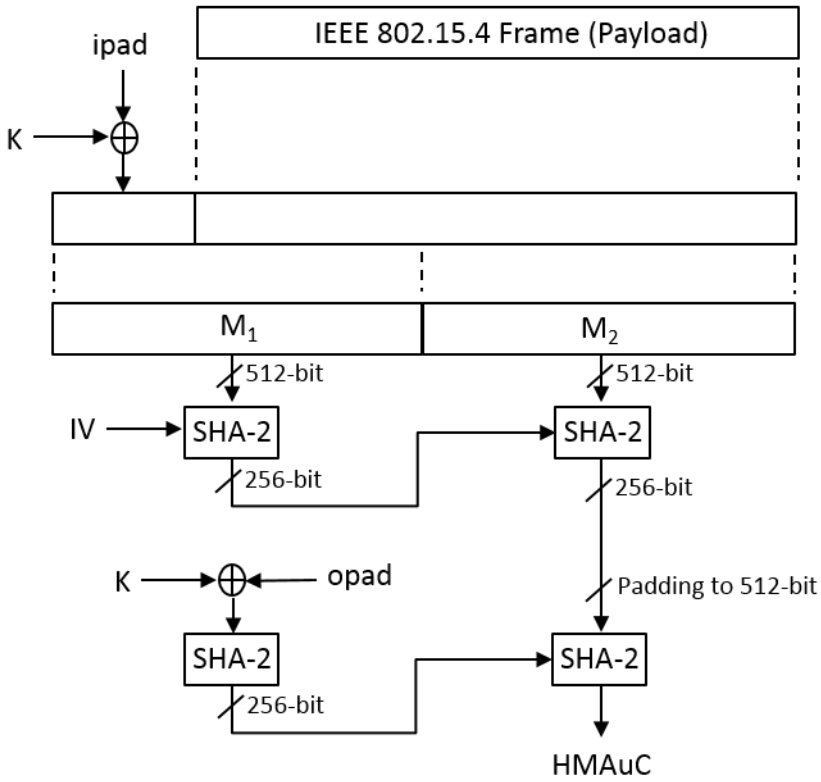


Fig. 7.9: Modified IEEE 802.15.4 MAuC generation process

7.4 Results and Analyses:

In order to study the performance of the proposed key management scheme, the EESKB model has been implemented within the Contiki OS while its performance is compared to relevant approaches in the literature. This means that two algorithms have to be considered, which are AES and SHA2-256. Unlike the analyses conducted in pervious chapters, here with regards to the impact of security, the computation cost will be brought to light since the real impact of the cipher algorithms is based on the burden of these algorithms upon the node microcontroller. Accordingly, the analysis is based on the MSP430F169

microcontroller that its current consumption at 2.2V is 330uA. One of the important points to notice is the impact of microcontroller frequency operation value, where in this research the analysis is based on MSP430 8 MHz while in the literature is varied to reach 206MHz as for StrongArm as in [180].

Fig. 7.10 shows the overhead of the EESKB for both initialization and association processes. The initialization cost is only encountered one time which is during the network deployment. The association cost is associated with each join process while the node is changing cluster heads (or coordinators).

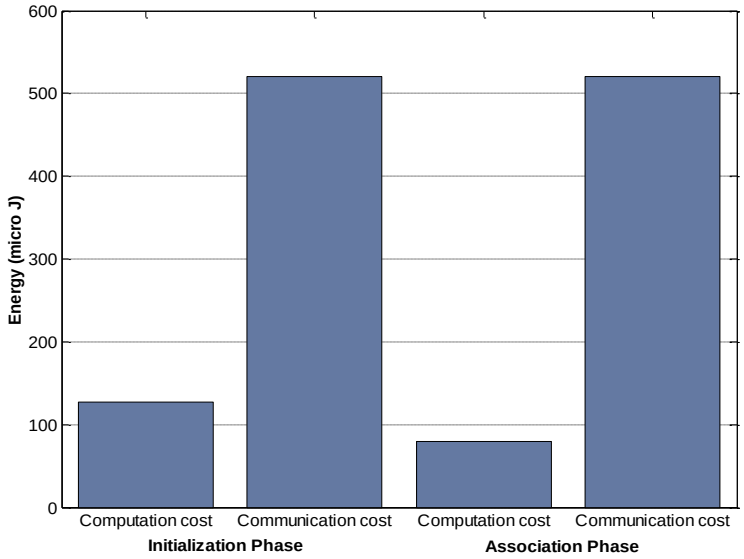


Fig. 7.10: EESKB energy cost of both initialization and association phases

In the meantime, the overhead over the coordinators (CHs) nodes has not been considered since the computation/communication cost for the methods (proposed and literature) can't exceed the cost over the mobile node.

There are three related approaches in the literature that the EESKB has been compared with. These protocols are presented in [172], [174] and [173].

The fist analysis examines the impact of the proposed EESKB on both computation and communication cost based on deployment with Contiki OS. Fig.7.11 shows that the EESKB association phase has the lowest energy consumption while Kumar et al. approach has less energy cost than EESKB initialization phase. As stated earlier, the association phase is the dominant process during the network lifetime since its related with the mobility of nodes while the initialization phase is occurred only one time during node lifetime.

Both Sciacalepero *et al*. and Piro *et al*. have the maximum computation cost since the two processes rely on RSA and Diffie-Hellman approaches. The key issue with the RSA public key system is the overhead of generating both public and private keys and the process of encrypting and decrypting using these generated keys. The same issue exists with Diffie-Hellman method by which there is a high overhead that is caused by the process of generating the mutual keys between any pair of nodes.

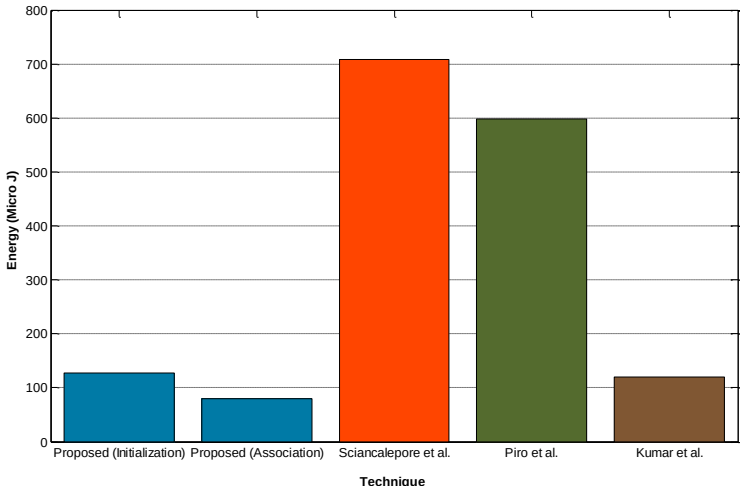


Fig. 7.11: Comparison of the computation cost (overhead of microcontroller)

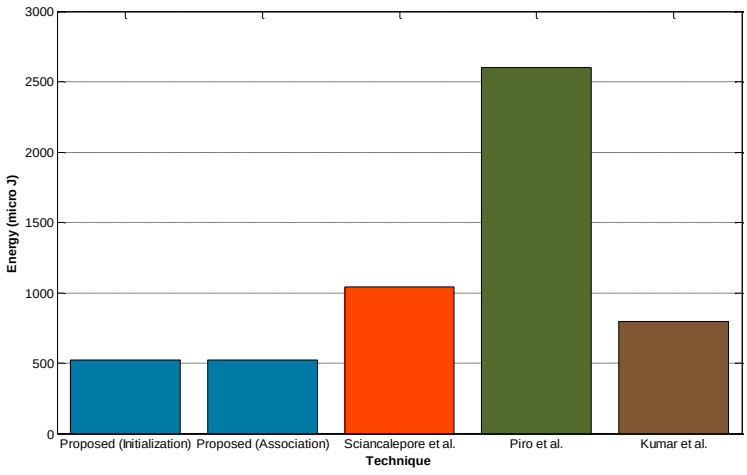


Fig. 7.12: Comparison of the communication cost (overhead of transceiver)

The communication cost is influenced by the required number of messages to distribute the keys. Hence, minimizing the number of messages must be the target of any keying scheme. Fig. 7.12 indicates the advantage of EESKB over other techniques. EESKB has the lowest number of exchanged messages and thus, has low energy consumption. Although Sciacalepero *et al*. has exploited the Diffie-Hellman which requires only two messages as the proposed EESKB, it has included the process of verifying mutual authentication which is as compared to the default Diffie-Hellman mechanism is not required. This process is not mandatory since the Diffie-Hellman itself can guarantee the mutual authentication. Fig. 7.13 demonstrates the total cost of both communication and computation cost. EESKB

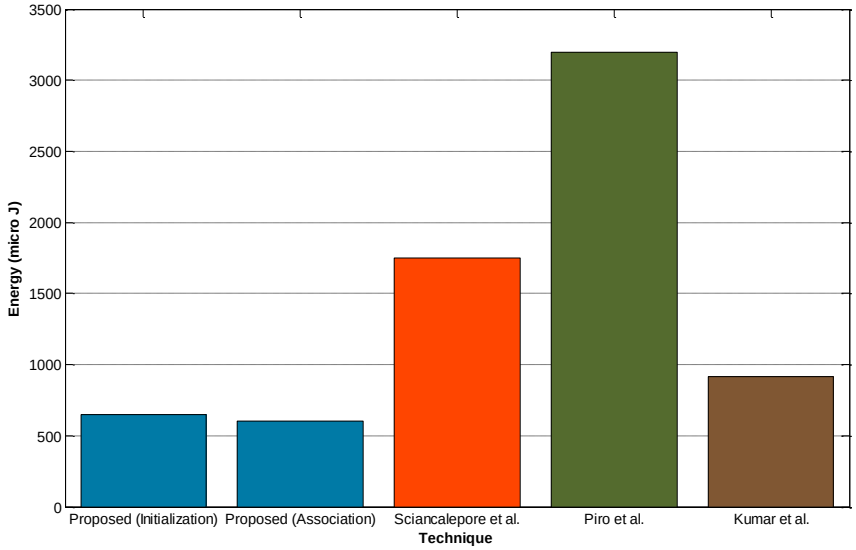


Fig. 7.13: Total security-related energy cost

and Kumar *et al*. tend to have the lowest energy overhead due their dependency on only symmetric techniques and hash functions.

In term of the impact of mobility, the analysis is based on the LLDN mode since the standard-based TSCH mode has no defined association scheme and thus, the study is based on the LLDN default scheme to examine the impact of mobility on the proposed and relevant security models.

Figures 7.14 and 7.15 present how the energy cost is increasing with time as 6 mobile nodes are moving and changing their points of attachment accordingly.

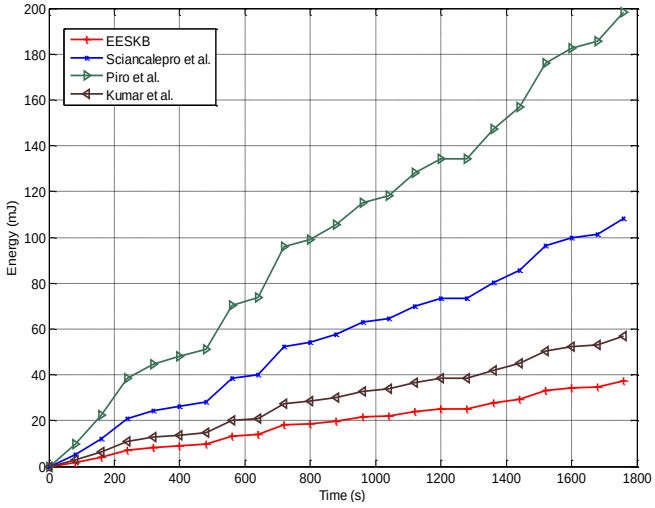


Fig. 7.14: Energy consumption, range:50m, superframe:0.5s

Although maximizing the superframe duration has to increase the energy overhead as it has been seen in chapter six, but here the mobility impact is caused by the number of association processes (i.e. increased energy overhead as maximizing the number of required associations to maintain full connectivity). Therefore, since increasing the superframe duration will minimize the number of attempts that a mobile node can perform, the security overhead has been reduced.

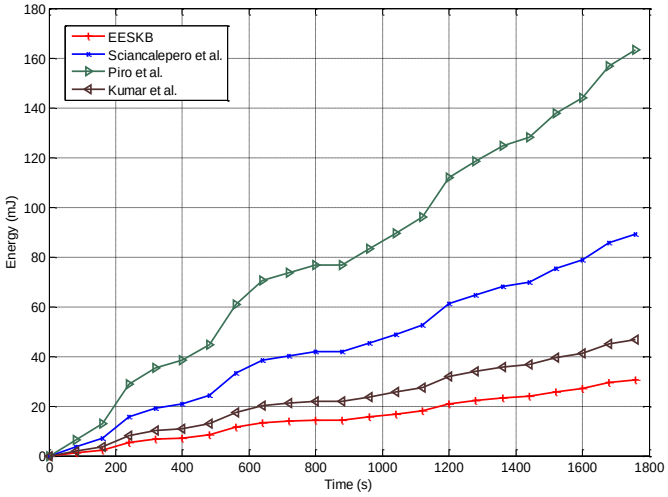


Fig. 7.15: Energy consumption, range: 50m, superframe: 2s

Changing the transmission rage to 100m shows less energy cost as compared to 50m range due to the increase of the settle time for the mobile nodes. This means less dissociations and accordingly, minimal association processes and less energy consumption. Both Figures 7.16 and 7.17 show a comparison between EESKB and related techniques for 100m range regarding both 0.5s and 2s superframe durations.

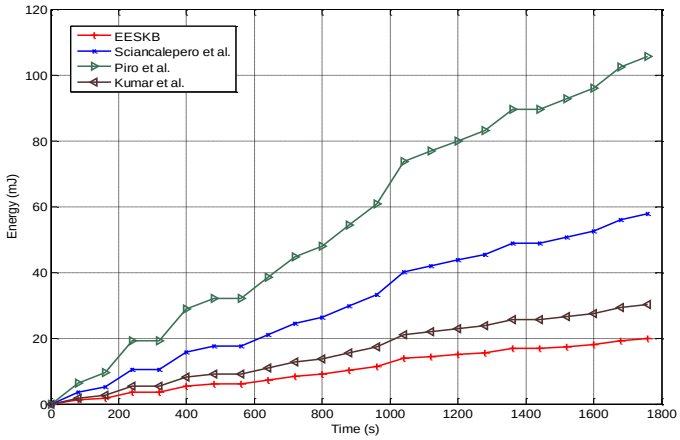


Fig. 7.17: Energy consumption, range: 100m, superframe: 0.5s

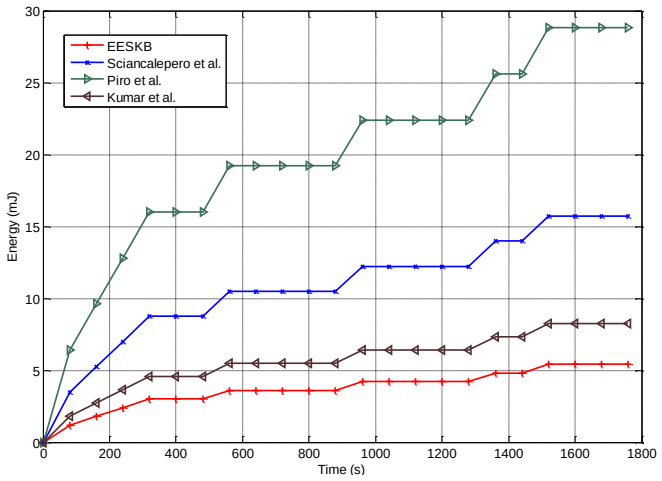


Fig. 7.16: Energy consumption, range: 100m, superframe: 2s

Fig. 7.18 demonstrates how the proposed approach for realizing authentication and confidentiality has a great energy utilization over the default IEEE 802.15.4 modes of operation. The confidentiality through the modified approach (HMAuC+AES) has realized a reduction of about 40% of the default AES-CCM mode. Similarly, the modified authentication (HMAuC) approach has achieved a reduction of 60% over the original AES-CBC mode. Hence, the proposed authentication/confidentiality scheme has manged to reduce the energy cost while still preserves the required security measure as long as the SHA2-256 is still actively a secure hashing function.

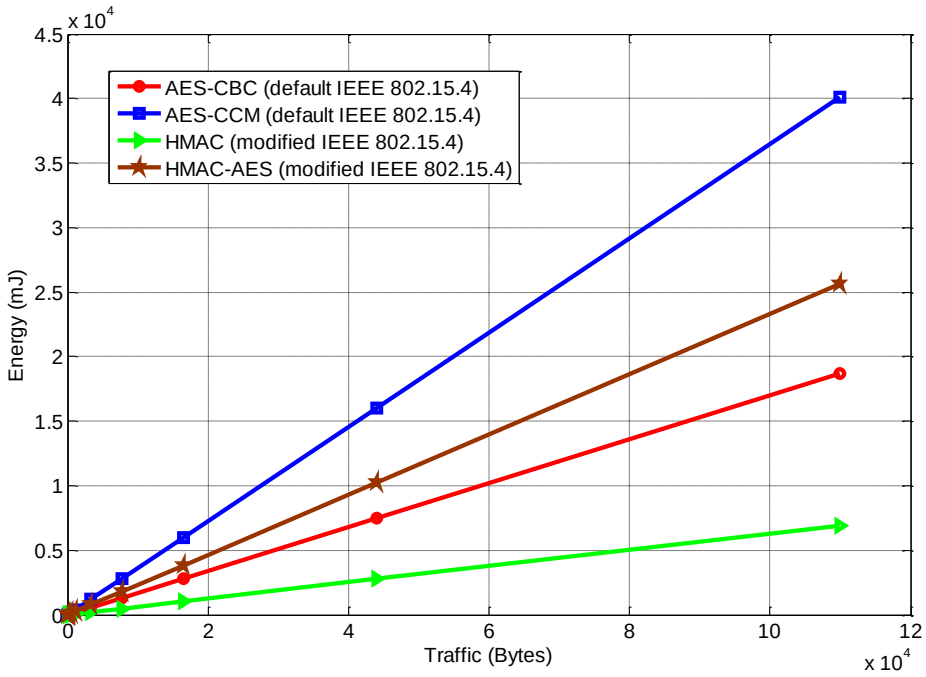


Fig. 7.18: Energy consumption utilization of the modified IEEE 802.15.4 operation modes

Finally, the modified structure of the IEEE 802.15.4 structure has reduced the latency which is caused by authenticating/ciphering outgoing frames. The dependency on the SHA hash function has led to minimize the required time of providing authentication/confidentiality services and is incurred through two factors. The hash function firsts deal with 512-bit as compared with 128-bit in AES. Secondly, the execution time of SHA-256 is less than the required time for the AES.

Fig. 7.19 depicts the impact of the modified structure on latency as compared with the default IEEE 802.15.4 model.

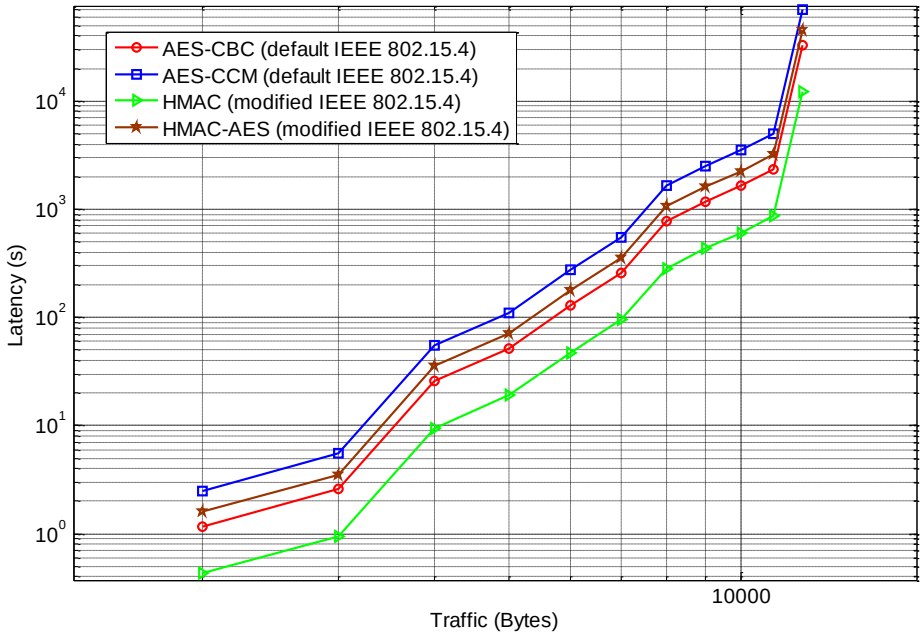


Fig. 7.19: Impact of the default and modified IEEE 802.15.4 structures on latency

7.5 Security Analysis:

One of the important threats to the IoT networks is the node compromise attack. The only reliable approach is through providing a tamper resistant hardware. Although other approaches can be exploited to tackle this issue by which to examine the node behaviour, but these approaches can't guarantee the elimination of such attacks and incur high computational overhead. In the meantime, the proposed EESKB follows a mechanism by which generates the required pair-wise keys with regards on a preloaded master key that will eventually deleted after the network initialization phase. Thus, if any node is captured by an adversary, the revealed keys form the compromised node can't be exploited in other network parts to generate the relevant shared keys.

On the other hand, the security strength of the proposed key management protocol is basically relies on both AES and SHA2-256 algorithms and whenever these techniques preserve security, the prosed approach is still secure and valid for application.

7.6 Summary:

This chapter addresses the importance of security service for low power mobile IoT devices. The mobile nodes need regularly to change their points of attachment to the network and thus, need an authorization scheme that can tackle this issue. One of the obstacles here is how to facilitate the application of efficient cipher techniques without the existence of solid secure key distribution schemes. In this chapter, a proposed key bootstrapping scheme EESKB has been proposed to provide secure and energy efficient key management approach. The proposed EESKB manged to have the lowest energy cost as compared with other relevant methodologies in the literature. In addition, the integration of the EESKB with the association mechanisms (either in IEEE 802.15.4 or 6LoWPAN neighbour discovery) will expedite the join process to the network and minimize the energy consumption since the same messages are utilized for both securing and configuring the mobile node with the network.

Chapter 8. Conclusion and Future Work

8.1 Conclusion

It is clear that even with significant contributions regarding mobility, managing node movement still incurs a high overhead. Regarding the handoff process of mobile nodes inside a single LoWPAN, there is no standardized effort to address this issue especially with the problems related to IEEE 802.15.4 association techniques. The upcoming mobility pattern within the IoT context will significantly comprise of both micro and macro mobility. Hence, there must be standardized approaches that can handle simultaneously both mobility types while separating the scenarios of addressing both types with a single mechanism to omit the overhead of handling inter-domain mobility from intra-domain mobility. Accordingly, a given MMP can provide two callings processes dedicated to either micro or macro mobility.

On the other hand, security arises as a crucial aspect in IoT applications using mobile nodes. The problem is how to ensure secure access control for the mobile nodes that are either moving within a single domain or between different domains. Due to the limited power and computation capabilities, it will be difficult to deploy strong security protocols on the mobile nodes. Hence, these mobile nodes will be seen here as a potential source of security breaches to the network. The possible research issues and questions that can be concluded are as follows:

- How to provide a secure key management scheme that supports three services: (i) key bootstrapping, (ii) key update scheme, (iii) new node insertion scheme that can verify the authenticity of any new node seeking to join the network which has moved from either the same LoWPAN or a different one.
- How to provide a light and efficient node anonymity service that keeps the node identification information private.
- How the default security protocols for *unconstrained* devices i.e. IPsec and SSL and others, can be adapted for *constrained* devices to minimize the gap of heterogeneity caused by using multiple types of protocols.

Overall, the field of mobility for low power IoT devices is still in its infancy, and especially when considering security, there is much work still to be done.

Regarding the clustering and managing the RDC for IEEE 802.15.4, the analysis in this thesis points to the superiority of the mesh-under technique (utilized by MUCBR and RIME) over the route-over technique (utilized by RPL) in terms of energy consumption. The basic reason behind the high energy consumption is the packet size. Routing within the IPv6 network layer (route-over) will add extra packet header load to the IEEE 802.15.4 frames which dramatically increase energy consumption. Moreover, the probability of collision will increase due to maximizing required transmission time and hence, more MAC occupancy. In addition, the analyses show how the clustering technique can minimize the energy consumption by reducing the nodes RDC. The results in chapter 4 clearly show that the scheduling listening techniques provide a better power efficiency. It also disproves the assumptions that the power requirements of the network setup in scheduling techniques are always higher than the power savings achieved by it. This achieved through proposing the MUCBR which relies on a light mechanism to initialize the nodes into clusters and provides synchronization.

Turning to the issue of mobility under TSCH mode, the analysis in chapter 5 shows the real impact of node mobility upon a TSCH network. The overhead is incurred by the impact of increased listening time while scanning for a valid EB that is required to conduct an association. According to the implemented TSCH within the Contiki OS and the observed performance, the possible factors that affect the overall network services with the presence of mobile nodes can be classified as:

- Mobility patterns of the sensor nodes.
- Nodes movement speed.
- Number of FFD devices in a given mobile node POS.
- Transmission range for both FFD and RFD devices.
- Settle time that is determined by the possible trajectory of the mobile node within a given FFD POS and the transmission range.
- Number of SHARED TX slots in each slotframe that can accommodate

mobile node association requests.

- Number of mobile nodes in a single FFD POS.
- Number of frequency channels available for hopping.
- FFD deployment pattern in the scattered area of mobile nodes.

Similarly, regarding the mobility problem under LLDN mode and based on the study in chapter 6, dividing the transmission states into three events (discovery, configuration and online) affects negatively both dissociated and associated nodes. The orphan nodes that seek to join the network are relying on both discovery and configuration transmission states to determine the network and synchronize with the coordinator. Hence, the node connectivity factor is dependent on the occurrence ratio of these two states to the duration of online states during a network lifetime. In the meantime, the throughput of the connected nodes is dependent on the interval of the online states since during the discovery and configuration states the nodes are forbidden from sending readings. Accordingly, there must be a tradeoff between the nS_O value and the values of nS_D and nS_C to realize an acceptable amount of throughput versus dissociation time. Increasing nS_O to the values of nS_D and nS_C will maximize node throughput, but in turn increase the dissociation time.

Finally, looking at the security challenge for mobile IoT devices, the proposed EESKB managed to overcome the dependency on public key system methodologies (i.e. RSA and Diffie-Hellman) and has eliminated their encountered burden on the mobile nodes. Although the Diffie-Hellman and the RSA techniques can support macro mobility, but they can't be applied since without any secure access control mechanism that can prevent any arbitrary node from contacting a foreign network, these two public keying schemes can't be deployed. Hence, until now the macro mobility is still unachievable with the recent network standards. (i.e. invalid node identity).

8.2 Future Work

This research has concluded multiple future study directions and these research trends can be summarized as follow:

- Considering the issue of macro mobility with regards to a cross layer approach that performs a link-layer handoff followed by a network layer association.
- Determining a hybrid technique that facilitates the integration of the mobile node with two different standards (i.e. IEEE 802.11 and IEEE 802.15.4). The movement of a node from one network to another (different standards) requires an efficient handoff scheme that preserves the connectivity for the node with less overhead.
- Investigating different mobility patterns and their stochastic processes based on the application type to predict the mobile nodes' speed, next position, estimated upcoming pauses time and direction of movement. This will optimize the mobility management process via determining the next point of attachment to the network. Accordingly, expecting the next CH that a mobile node will be attached to.
- Providing a secure access control mechanism under macro mobility scenarios to facilitate the node movement into different network domain while omitting the dependency on protocols as IPsec or SSL.
- Studying the type of macro/vehicular mobility of constrained devices that can be the next node mobility class. The focus here is on adapting the current mobility/security protocols with this type of node movement. The study has to investigate a new methodology by which to utilize the next 5G network for providing future-based IoT backbone and examines its applicability for low power devices.

REFERENCES

[1] "IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer," *IEEE Std 802.15.4e-2012 (Amendment to IEEE Std 802.15.4-2011)*, pp. 1-225, 2012.

[2] W. Stallings, *Cryptography and Network Security, 4/E*: Pearson Education India, 2006.

[3] Z. Shelby and C. Bormann, *6LoWPAN: The wireless embedded Internet* vol. 43: John Wiley & Sons, 2011.

[4] "IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)*, pp. 1-314, 2011.

[5] S. C. Mukhopadhyay, "Wearable Sensors for Human Activity Monitoring: A Review," *IEEE Sensors Journal,*, vol. 15, pp. 1321-1330, 2015.

[6] M. Becker, B.-L. Wenning, C. Görg, R. Jedermann, and A. Timm-Giel, "Logistic applications with wireless sensor networks," in *Proceedings of the 6th Workshop on Hot Topics in Embedded Networked Sensors*, 2010, p. 6.

[7] S. Deering and a. R. Hinden, "Internet protocol, version 6 (IPv6) specification," *RFC 2460, IETF*, 1998.

[8] G. MONTENEGRO, N. KUSHALNAGAR, and J. HUI, "IETF RFC 4944," *Transmission of IPv6 packets over IEEE*, vol. 802.

[9] G. Mulligan, "The 6LoWPAN architecture," in *Proceedings of the 4th workshop on Embedded networked sensors*, 2007, pp. 78-82.

[10] N. Salman, I. Rasool, and A. Kemp, "Overview of the IEEE 802.15. 4 standards family for low rate wireless personal area networks," in *Wireless Communication Systems (ISWCS), 2010 7th International Symposium on*, 2010, pp. 701-705.

[11] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki - a lightweight and flexible operating system for tiny networked sensors," in *Proceeding of the 29th Annual IEEE International Conference on Local Computer Networks*, , 2004, pp. 455-462.

[12] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo, *et al.*, "TinyOS: An Operating System for Sensor Networks," in *Ambient Intelligence*, W. Weber, J. Rabaey, and E. Aarts, Eds., ed: Springer Berlin Heidelberg, 2005, pp. 115-148.

[13] C. Perkins, D. Johnson, and J. Arkko, "Mobility support in IPv6," RFC 6275, IETF 2070-1721, 2011.

[14] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network mobility (NEMO) basic support protocol," RFC 3963, IETF 2070-1721, 2005.

[15] S. Deering and R. Hinden, "Internet protocol, version 6 (IPv6) specification," *IETF, RFC 2469*, 1998.

[16] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (CoAP)," in *IETF, RFC 7252*, ed, 2014.

[17] "MQ Telemetry Transport (MQTT), *http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4554519*.

[18] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless communications and mobile computing*, vol. 2, pp. 483-502, 2002.

[19] I. F. Akyildiz, X. Jiang, and S. Mohanty, "A survey of mobility management in next-generation all-IP-based wireless systems," *IEEE Wireless Communications*, , vol. 11, pp. 16-28, 2004.

[20] F. M. Chiussi, D. A. Khotimsky, and S. Krishnan, "Mobility management in third-generation all-IP networks," *IEEE Communications Magazine*, , vol. 40, pp. 124-135, 2002.

[21] J.-P. Vasseur and A. Dunkels, *Interconnecting smart objects with ip: The next internet*: Morgan Kaufmann, 2010.

[22] G. Corbellini, E. C. Strinati, and A. Duda, "LA-MAC: Low-latency asynchronous MAC for wireless sensor networks," in *Proceeding of the IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC),* , 2012, pp. 380-386.

[23] A. Dunkels, "The contikimac radio duty cycling protocol," *Technical Report T2011:13, Swedish Institute of Computer Science,*, 2011.

[24] D. Moss, J. Hui, and K. Klues, "Low power listening," *TinyOS Core Working Group, TEP*, vol. 105, 2007.

[25] J. G. Ko, N. Tsiftes, A. Dunkels, and A. Terzis, "Pragmatic low-power interoperability: ContikiMAC vs TinyOS LPL," in *Proceeding of the 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012*, 2012, pp. 94-96.

[26] J. Kim, J. On, S. Kim, and J. Lee, "Performance evaluation of synchronous and asynchronous MAC protocols for wireless sensor networks," in *Proceeding of the Sensor Technologies and Applications, 2008. SENSORCOMM'08. Second International Conference on*, 2008, pp. 500-506.

[27] J. Polastre, J. Hill, and D. Culler, "Versatile low power media access for wireless sensor networks," in *Proceedings of the 2nd international conference on Embedded networked sensor systems*, 2004, pp. 95-107.

[28] A. El-Hoiydi and J.-D. Decotignie, "Low power downlink MAC protocols for infrastructure wireless sensor networks," *Mobile Networks and Applications*, vol. 10, pp. 675-690, 2005.

[29] M. Buettner, G. V. Yee, E. Anderson, and R. Han, "X-MAC: a short preamble MAC protocol for duty-cycled wireless sensor networks," in *Proceedings of the 4th international conference on Embedded networked sensor systems*, 2006, pp. 307-320.

[30] T. Van Dam and K. Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks," in *Proceedings of the 1st international conference on Embedded networked sensor systems*, 2003, pp. 171-180.

[31] W. Ye, J. Heidemann, and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks," *IEEE/ACM Transactions on Networking, ,* vol. 12, pp. 493-506, 2004.

[32] L. F. van Hoesel and P. Havinga, "A lightweight medium access protocol (LMAC) for wireless sensor networks: Reducing preamble transmissions and transceiver state switches," in *Proceedings of the 1st international Worksop on Networked Sensor Systems (INSS),* 2004.

[33] G. Lu, B. Krishnamachari, and C. S. Raghavendra, "An adaptive energy-efficient and low-latency MAC for data gathering in wireless sensor networks," in *Proceedings of the 18th International Parallel and Distributed Processing Symposium,* 2004, p. 224.

[34] V. Rajendran, J. J. Garcia-Luna-Aveces, and K. Obraczka, "Energy-efficient, application-aware medium access for sensor networks," in *Proceeedings of the IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, ,* 2005, pp. 8 pp.-630.

[35] V. Rajendran, K. Obraczka, and J. J. Garcia-Luna-Aceves, "Energy-efficient, collision-free medium access control for wireless sensor networks," *Wireless Networks,* vol. 12, pp. 63-78, 2006.

[36] J. Granjal, E. Monteiro, and S. S. J, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," *IEEE Communications Surveys & Tutorials,* vol. 17, pp. 1294-1312, 2015.

[37] R. Silva and J. S. Silva, "An Adaptation Model for Mobile IPv6 support in lowPANs," *IETF, Internet Draft, Work in Progress, draft-silva-6lowpan-mipv6-00,* 2009.

[38] C. Chaabane, A. Pegatoquet, M. Auguin, and M. Ben Jemaa, "Energy optimization for mobile nodes in a cluster tree IEEE 802.15.4/ZigBee network," in *Proceeedings of the Computing, Communications and Applications Conference (ComComAp), ,* 2012, pp. 328-333.

[39] G. Anastasi, M. Conti, and M. D. Francesco, "A Comprehensive Analysis of the MAC Unreliability Problem in IEEE 802.15.4 Wireless Sensor

Networks," *IEEE Transactions on Industrial Informatics,* vol. 7, pp. 52-65, 2011.

[40] D. Qian and W. Dargie, "A Survey on Mobility and Mobility-Aware MAC Protocols in Wireless Sensor Networks," *IEEE Communications Surveys & Tutorials,,* vol. 15, pp. 88-100, 2013.

[41] Z. Ping, C. Huihuang, S. Jianghong, and P. N. Green, "Research on Medium Access Control protocols for mobile sensor networks," in *Proceeding of the IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS),,* 2010, pp. 223-227.

[42] P. Huan and J. Sanjay, "An adaptive mobility-aware MAC protocol for sensor networks (MS-MAC)," in *proceeding of the IEEE International Conference on Mobile Ad-hoc and Sensor Systems,,* 2004, pp. 558-560.

[43] M. Ali, T. Suleman, and Z. A. Uzmi, "MMAC: a mobility-adaptive, collision-free MAC protocol for wireless sensor networks," in *proceeding of the 24th IEEE International Performance, Computing, and Communications Conference, . IPCCC.* , 2005, pp. 401-407.

[44] A. Jhumka and S. Kulkarni, "On the design of mobility-tolerant TDMA-based media access control (MAC) protocol for mobile sensor networks," in *Distributed Computing and Internet Technology*, ed: Springer, 2007, pp. 42-53.

[45] Z. Tang and W. Dargie, "A mobility-aware medium access control protocol for wireless sensor networks," in *Proceedings of the IEEE GLOBECOM Workshops (GC Wkshps),,* 2010, pp. 109-114.

[46] A. Gonga, O. Landsiedel, and M. Johansson, "MobiSense: Power-efficient micro-mobility in wireless sensor networks," in *proceedings of the International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS),,* 2011, pp. 1-8.

[47] M. Nabi, M. Blagojevic, M. Geilen, T. Basten, and T. Hendriks, "MCMAC: An Optimized Medium Access Control Protocol for Mobile Clusters in Wireless Sensor Networks," in *Proceedings of the 7th Annual IEEE*

Communications Society Conference on Sensor Mesh and Ad Hoc Communications and Networks (SECON),, 2010, pp. 1-9.

[48] A. Raja and S. Xiao, "A Mobility Adaptive Hybrid Protocol for Wireless Sensor Networks," in *Proceedings of the 5th IEEE Consumer Communications and Networking Conference, CCNC*, 2008, pp. 692-696.

[49] P. Raviraj, H. Sharif, M. Hempel, and C. Song, "MOBMAC - an energy efficient and low latency MAC for mobile wireless sensor networks," in *Proceedings of Systems Communications, ,* 2005, pp. 370-375.

[50] S. Mank, R. Karnapke, and J. Nolte, "An Adaptive TDMA based MAC Protocol for Mobile Wireless Sensor Networks," in *Proceedings of the International Conference on Sensor Technologies and Applications, SensorComm,,* 2007, pp. 62-69.

[51] K. Zen, D. Habibi, and I. Ahmad, "A new algorithm to improve mobile sensor node connectivity based on link quality indicator," in *Proceedings of the IEEE Region 10 Conference (TENCON)*, 2009, pp. 1-6.

[52] C. Chaabane, A. Pegatoquet, M. Auguin, and M. Ben Jemaa, "Energy optimization for mobile nodes in a cluster tree IEEE 802.15.4/ZigBee network," in *Proceedings of the Computing, Communications and Applications Conference (ComComAp),*, 2012, pp. 328-333.

[53] F. Bashir, Woon-Sung, Baek Sthapit, P. Pandey, D. Jae-Young, and a. Pyun, "Coordinator assisted passive discovery for mobile end devices in IEEE 802.15.4," in *Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC),*, 2013, pp. 601-604.

[54] P. Sthapit, Y.-S. Choi, G.-R. Kwon, J.-Y. Pyun, and S.-s. Hwang, "Fast Association Scheme over IEEE 802.15. 4 based Mobile Sensor Network," in *Proceedings of the Ninth International Conference on Wireless and Mobile Communications ICWMC* 2013, pp. 179-184.

[55] Y. Min-Chieh and L. Jenq-Shiou, "Adaptive weighted scheme for improving mobile sensor node connectivity in IEEE 802.15.4 networks," in

Proceedings of the IEEE Network Operations and Management Symposium (NOMS),, 2012, pp. 968-973.

[56] L. Yong, P. Yong, and W. Ping, "Research and implementation of a mobility management mechanism for Wireless Sensor Networks based on IEEE 802.15.4," in *Proceedings of the IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER),* , 2011, pp. 260-264.

[57] K. Jinho, L. Jun, K. Hyoeng Kyu, L. Dae Sun, H. Choong Seon, and L. Sungwon, "An ID/Locator Separation-Based Mobility Management Architecture for WSNs," *IEEE Transactions on Mobile Computing,*, vol. 13, pp. 2240-2254, 2014.

[58] X. Wang, D. Le, Y. Yao, and C. Xie, "Location-based mobility support for 6LoWPAN wireless sensor networks," *Journal of Network and Computer Applications,* vol. 49, pp. 68-77, 2015.

[59] K. H. Teo, S. Subramaniam, and G. R. Sinniah, "Node Mobility Support Between Multi-hop 6LoWPAN Networks Based on Proxy Mobile IPv6," *Wireless Personal Communications,* vol. 85, pp. 959-986.

[60] M. S. Shahamabadi, B. Bin Mohd Ali, P. Varahram, and A. J. Jara, "A Network Mobility Solution Based on 6LoWPAN Hospital Wireless Sensor Network (NEMO-HWSN)," in *Proceedings of the Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS),* , 2013, pp. 433-438.

[61] V. Koster, D. Dorn, A. Lewandowski, and C. Wietfeld, "A Novel Approach for Combining Micro and Macro Mobility in 6LoWPAN Enabled Networks," in *Proceedings of the IEEE Vehicular Technology Conference (VTC Fall),* , 2011, pp. 1-5.

[62] J. H. Kim, R. Haw, and C. S. Hong, "Development of a framework to support network-based mobility of 6LoWPAN sensor device for mobile healthcare system," in *Proceeedings of the International Conference on Consumer Electronics Digest of Technical Papers* ,2010.

[63] G. Bag, M. T. Raza, H. Mukhtar, A. H. Akbar, S. M. S. Shams, K. Ki-Hyung, *et al.*, "Energy-aware and bandwidth-efficient mobility architecture for 6LoWPAN," in *Proceedings of the IEEE Military Communications Conference, MILCOM.* , 2008, pp. 1-7.

[64] C. Rong, Z. Ya-Lai, C. Qian-bin, D. Tao, and Z. Wei-Guang, "Group mobility in 6LoWPAN-based WSN," in *Proceedings of the International Conference on Wireless Communications and Signal Processing (WCSP),*, 2010, pp. 1-5.

[65] A. J. Jara, M. A. Zamora, and A. F. G. Skarmeta, "HWSN6: Hospital Wireless Sensor Networks Based on 6LoWPAN Technology: Mobility and Fault Tolerance Management," in *Proceedings of the International Conference on Computational Science and Engineering, CSE '09.* , 2009, pp. 879-884.

[66] M. Ha, D. Kim, S. H. Kim, and S. Hong, "Inter-MARIO: A Fast and Seamless Mobility Protocol to Support Inter-Pan Handover in 6LoWPAN," in *Proceedings of the Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE,* 2010, pp. 1-6.

[67] Z. Zinonos and V. Vassiliou, "Inter-mobility support in controlled 6LoWPAN networks," in *Proceedings of the IEEE GLOBECOM Workshops (GC Wkshps),* , 2010, pp. 1718-1723.

[68] J. Montavont, D. Roth, and T. Noël, "Mobile ipv6 in internet of things: Analysis, experimentations and optimizations," *Ad Hoc Networks,* vol. 14, pp. 15-25, 2014.

[69] H. Fotouhi, D. Moreira, and M. Alves, "mRPL: Boosting mobility in the Internet of Things," *Ad Hoc Networks,* vol. 26, pp. 17-35, 2015.

[70] V. P. Kafle, H. Otsuki, and M. Inoue, "An ID/locator split architecture for future networks," *IEEE Communications Magazine,,* vol. 48, pp. 138-144, 2010.

[71] J. Petajajarvi and H. Karvonen, "Soft handover method for mobile wireless sensor networks based on 6LoWPAN," in *Proceedings of the International*

Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS),, 2011, pp. 1-6.

[72] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy mobile ipv6," RFC 5213, IETF 2070-1721, 2008.

[73] L. Jun and F. Xiaoming, "Evaluating the Benefits of Introducing PMIPv6 for Localized Mobility Management," in *Proceedings of the IWCMC '08. International Wireless Communications and Mobile Computing Conference,*, 2008, pp. 74-80.

[74] T. Winter, "RPL: IPv6 routing protocol for low-power and lossy networks," *IETF, RFC 6550*, 2012.

[75] N. A. Surobhi and A. Jamalipour, "An IoT-based middleware for mobility management in post-emergency networks," in *Proceedings of the 21st International Conference on Telecommunications (ICT), ,* 2014, pp. 283-287.

[76] W. Di, D. I. Arkhipov, E. Asmare, Q. Zhijing, and J. A. McCann, "UbiFlow: Mobility management in urban-scale software defined IoT," in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM),*, 2015, pp. 208-216.

[77] E. Baccelli, O. Hahm, Gu, x, M. nes, Wa*, et al.*, "RIOT OS: Towards an OS for the Internet of Things," in *Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), ,* 2013, pp. 79-80.

[78] O. Hahm, E. Baccelli, H. Petersen, and N. Tsiftes, "Operating Systems for Low-End Devices in the Internet of Things: a Survey," *IEEE Internet of Things Journal, ,* vol. PP, pp. 1-1, 2015.

[79] N. Hassanzadeh, O. Landsiedel, F. Hermans, O. Rensfelt, and T. Voigt, "Revisiting the need for mobile MAC protocols in wireless sensor networks," *SIGBED Rev.,* vol. 9, pp. 7-10, 2012.

[80] J. Ko, J. Eriksson, N. Tsiftes, S. Dawson-Haggerty, M. Durvy, A. Terzis*, et al.*, "Beyond interoperability: Pushing the performance of sensornet IP

stacks," in *Proceedings of the International Conference on Embedded Networked Sensor Systems (ACM SenSys)*, 2011.

[81] S. Montero, J. Gozalvez, M. Sepulcre, and G. Prieto, "Impact of mobility on the management and performance of WirelessHART industrial communications," in *Proceedings of the IEEE 17th Conference on Emerging Technologies & Factory Automation (ETFA), ,* 2012, pp. 1-4.

[82] I. E. 1.0, "Industrial communication networks – Wireless communication network and communication profiles – WirelessHART™," International Electrotechnical Commission, IEC2010.

[83] S. Montero and J. Gozalvez, "LAN-ND, a new neighbour discovery protocol for mobile WirelessHART industrial networks," in *Proceedings of the IEEE 18th Conference on Emerging Technologies & Factory Automation (ETFA),,* 2013, pp. 1-8.

[84] T. Sun, N.-C. Liang, L.-J. Chen, P.-C. Chen, and M. Gerla, "Evaluating mobility support in zigbee networks," in *Embedded and Ubiquitous Computing*, ed: Springer, 2007, pp. 87-100.

[85] H. Dhaka, A. Jain, and K. Verma, "Impact of coordinator mobility on the throughput in a ZigBee mesh networks," in *Proceedings of the IEEE 2nd International Advance Computing Conference (IACC), ,* 2010, pp. 279-284.

[86] S. Yuan-Yao, C. Wei-Ho, H. Pi-Cheng, and P. Ai-Chun, "A Mobility-Aware Node Deployment and Tree Construction Framework for ZigBee Wireless Networks," *IEEE Transactions on Vehicular Technology, ,* vol. 62, pp. 2763-2779, 2013.

[87] H. C. Tung, K. F. Tsang, K. L. Lam, H. Y. Tung, B. Y. S. Li, L. F. Yeung, *et al.*, "A mobility enabled inpatient monitoring system using a ZigBee medical sensor network," *Sensors*, vol. 14, pp. 2397-2416, 2014.

[88] P. Sangheon, P. Kunwoo, K. Taekyoung, and C. Yanghee, "SAMP: scalable application-layer mobility protocol," *IEEE Communications Magazine,*, vol. 44, pp. 86-92, 2006.

[89] S.-M. Chun, H.-S. Kim, and J.-T. Park, "CoAP-Based Mobility Management for the Internet of Things," *Sensors,* vol. 15, pp. 16060-16082, 2015.

[90] A. J. Jara, D. Fernandez, P. Lopez, M. A. Zamora, and A. F. Skarmeta, "Lightweight Mobile IPv6: A mobility protocol for enabling transparent IPv6 mobility in the Internet of Things," in *Proceeedings of the IEEE Global Communications Conference (GLOBECOM),*, 2013, pp. 2791-2797.

[91] A. J. Jara, L. Marin, A. F. G. Skarmeta, D. Singh, G. Bakul, and K. Daeyeoul, "Secure Mobility Management Scheme for 6LoWPAN ID/Locator Split Architecture," in *Proceedings of the Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS),*, 2011, pp. 310-315.

[92] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios," *IEEE Sensors Journal, ,* vol. 15, pp. 1224-1234, 2015.

[93] E. Hammer-Lahav, "The oauth 1.0 protocol," *IETF, RFC 5849,* 2010.

[94] Y. Al-Nidawi and A. H. Kemp, "Mobility Aware Framework for Timeslotted Channel Hopping IEEE 802.15.4e Sensor Networks," *IEEE Sensors Journal,,* vol. 15, pp. 7112-7125, 2015.

[95] Y. Al-Nidawi, H. Yahya, and A. Kemp, "Tackling Mobility in Low Latency Deterministic Multihop IEEE 802.15.4e Sensor Network," *IEEE Sensors Journal, ,* vol. 16, pp. 1412-1427, 2015.

[96] S. Mohanty and I. F. Akyildiz, "Performance Analysis of Handoff Techniques Based on Mobile IP, TCP-Migrate, and SIP," *IEEE Transactions on Mobile Computing,,* vol. 6, pp. 731-747, 2007.

[97] E. Wedlund and H. Schulzrinne, "Mobility support using SIP," in *Proceedings of the 2nd ACM international workshop on Wireless mobile multimedia,* 1999, pp. 76-82.

[98] D. Dujovne, T. Watteyne, X. Vilajosana, and P. Thubert, "6TiSCH: deterministic IP-enabled industrial internet (of things)," *IEEE Communications Magazine, ,* vol. 52, pp. 36-41, 2014.

[99] D. Stanislowski, X. Vilajosana, Q. Wang, T. Watteyne, and K. S. Pister, "Adaptive synchronization in IEEE802. 15.4 e networks," *IEEE Transactions on Industrial Informatics,*, vol. 10, pp. 795-802, 2014.

[100] A. H. Chowdhury, M. Ikram, H.-S. Cha, H. Redwan, S. Shams, K.-H. Kim, *et al.*, "Route-over vs Mesh-under Routing in 6LoWPAN," in *Proceedings of the international conference on wireless communications and mobile computing: Connecting the world wirelessly*, 2009, pp. 1208-1212.

[101] C. Gomez, E. Kim, D. Kaspar, and C. Bormann, "Problem statement and requirements for IPv6 over low-power wireless personal area network (6LoWPAN) routing," *IETF, RFC 6606*, 2012.

[102] X. Wang and H. Qian, "Constructing a 6LoWPAN Wireless Sensor Network Based on a Cluster Tree," *IEEE Transactions on Vehicular Technology,* vol. 61, pp. 1398-1405, 2012.

[103] A. Bachir, M. Dohler, T. Watteyne, and K. K. Leung, "MAC Essentials for Wireless Sensor Networks," *IEEE Communications Surveys & Tutorials,* vol. 12, pp. 222-248, 2010.

[104] L. Karim and N. Nasser, "Energy Efficient and Fault Tolerant Routing Protocol for Mobile Sensor Network," in *Proceedings of the IEEE International Conference on Communications (ICC)*, 2011, pp. 1-5.

[105] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd annual Hawaii international conference on System sciences, ,* 2000, p. 10 pp. vol. 2.

[106] B. Pavkovic, W. J. Hwang, and F. Theoleyre, "Cluster-Directed Acyclic Graph Formation for IEEE 802.15.4 in Multihop Topologies," in *Proceedings of the 5th International Conference on New Technologies, Mobility and Security (NTMS)*, 2012, pp. 1-6.

[107] H. Tavakoli, J. Mi, x, x, M. Naderi, V. B. Mi, *et al.*, "Interaction of clustering period and event sensing reliability in IEEE 802.15.4 based

WSNs," in *Proceedings of the 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2013, pp. 774-779.

[108] N. Abdeddaim, F. Theoleyre, F. Rousseau, and A. Duda, "Multi-Channel Cluster Tree for 802.15.4 Wireless Sensor Networks," in *Proceedings of the IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)*, 2012, pp. 590-595.

[109] L. Li and Z. Jing, "Reducing inter-cluster TDMA interference by slot-pre-allocation-protocol in sensor networks," in *Proceedings of the 2nd International Conference on Industrial and Information Systems (IIS)*, , 2010, pp. 230-233.

[110] "IEEE Draft Standard for Local and Metropolitan Area Networks Part 15.4: Low Rate Wireless Personal Area Networks (LR-WPANs) Amendment: Active Radio Frequency Identification (RFID) System Physical Layer (PHY)," *IEEE P802.15.4f/D05, June 2011 (Revision of IEEE Std 802.15.4-2006)*, pp. 1-63, 2011.

[111] M. O. Farooq and T. Kunz, "Contiki-based IEEE 802.15.4 node's throughput and wireless channel utilization analysis," in *Proceedings of the Wireless Days (WD), IFIP*, 2012, pp. 1-3.

[112] J. W. Hui and D. E. Culler, "IPv6 in Low-Power Wireless Networks," *Proceedings of the IEEE*, vol. 98, pp. 1865-1878, 2010.

[113] J. G. Ko, N. Tsiftes, A. Dunkels, and A. Terzis, "Pragmatic low-power interoperability: ContikiMAC vs TinyOS LPL," in *Proceedings of the 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON),*, 2012, pp. 94-96.

[114] A. Dunkels, J. Eriksson, N. Finne, and N. Tsiftes, "Powertrace: Network-level power profiling for low-power wireless networks," *Technical reoprt T2011:05, SICS*, 2011.

[115] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-Level Sensor Network Simulation with COOJA," in *Proceedings 31st IEEE Conference on Local Computer Networks*, 2006, pp. 641-648.

[116] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, *et al.*, "Standardized Protocol Stack for the Internet of (Important) Things," *IEEE Communications Surveys & Tutorials,*, vol. 15, pp. 1389-1406, 2013.

[117] R. Assimiti, T. Phinney, and P. Thubert, "RPL applicability in industrial networks," *Informational Draft, IETF*, 2013.

[118] E. P. Thubert, " An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4, ," *draft-ietf-6tisch-architecture-08, 6TiSCH, IETF*, May 2015.

[119] M. Al-Jemeli and F. A. Hussin, "An Energy Efficient Cross-Layer Network Operation Model for IEEE 802.15.4-Based Mobile Wireless Sensor Networks," *IEEE Sensors Journal, ,* vol. 15, pp. 684-692, 2015.

[120] D. De Guglielmo, A. Seghetti, G. Anastasi, and M. Conti, "A performance analysis of the network formation process in IEEE 802.15. 4e TSCH wireless sensor/actuator networks," in *Proceeding of the IEEE Symposium on Computers and Communication (ISCC), ,* 2014, pp. 1-6.

[121] T. Watteyne, X. Vilajosana, B. Kerkez, F. Chraim, K. Weekly, Q. Wang, *et al.*, "OpenWSN: a standards-based low-power wireless development environment," *Transactions on Emerging Telecommunications Technologies*, vol. 23, pp. 480-493, 2012.

[122] X. Vilajosana, W. Qin, F. Chraim, T. Watteyne, C. Tengfei, and K. S. J. Pister, "A Realistic Energy Consumption Model for TSCH Networks," *IEEE Sensors Journal,*, vol. 14, pp. 482-489, 2014.

[123] Z. Jianwei, A. E. Xhafa, R. Vedantham, R. Nuzzaci, A. Kandhalu, and L. Xiaolin, "Comparison of IEEE 802.15.4e MAC features," in *Proceedings of the IEEE World Forum on Internet of Things (WF-IoT),*, 2014, pp. 203-207.

[124] M. Barcelo, A. Correa, X. Vilajosana, J. Lopez Vicario, and A. Morell, "Novel Routing Approach for the TSCH Mode of IEEE 802.15.14e in Wireless Sensor Networks with Mobile Nodes," in *Proceedings of the IEEE 80th Conference Vehicular Technology (VTC Fall), ,* 2014, pp. 1-5.

[125] M. R. Palattella, N. Accettura, L. A. Grieco, G. Boggia, M. Dohler, and T. Engel, "On optimal scheduling in duty-cycled industrial iot applications using ieee802. 15.4 e tsch," *IEEE Sensors Journal, ,* vol. 13, pp. 3655-3666, 2013.

[126] M. R. Palattella, N. Accettura, M. Dohler, L. A. Grieco, and G. Boggia, "Traffic Aware Scheduling Algorithm for reliable low-power multi-hop IEEE 802.15.4e networks," in *Proceedings of the IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC),*, 2012, pp. 327-332.

[127] J. Xu, Y. Andrepoulos, Y. Xiao, and M. van der Schaar, "Non-Stationary Resource Allocation Policies for Delay-Constrained Video Streaming: Application to Video over Internet-of-Things-Enabled Networks," *IEEE Journal on Selected Areas in Communications,*, vol. 32, pp. 782-794, 2014.

[128] D. Peng and G. Roussos, "Adaptive time slotted channel hopping for wireless sensor networks," in *Proceeding of the 4th Computer Science and Electronic Engineering Conference (CEEC),* , 2012, pp. 29-34.

[129] T. Watteyne, M. Palattella, and a. L. Grieco, " Using IEEE802.15.4e TSCH in an IoT context: Overview, Problem Statement and Goals," *IETF Draft, draft-ietf-6tisch-tsch-06*, 2015.

[130] Y. Al-Nidawi, S. Naveed, and A. H. Kemp, "Mesh-Under Cluster-Based Routing Protocol for IEEE 802.15.4 SensorNetwork," in *Proceedings of 20th European Wireless Conference EW;* , 2014, pp. 1-7.

[131] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-Level Sensor Network Simulation with COOJA," in *Proceedings of 31st IEEE Conference on Local Computer Networks,* , 2006, pp. 641-648.

[132] P. Ieryung, K. Dohyun, and H. Dongsoo, "MAC Achieving Low Latency and Energy Efficiency in Hierarchical M2M Networks With Clustered Nodes," *IEEE Sensors Journal, ,* vol. 15, pp. 1657-1661, 2015.

[133] M. Arifuzzaman, M. Matsumoto, and T. Sato, "An Intelligent Hybrid MAC With Traffic-Differentiation-Based QoS for Wireless Sensor Networks," *IEEE Sensors Journal, ,* vol. 13, pp. 2391-2399, 2013.

[134] M. Bagaa, M. Younis, D. Djenouri, A. Derhab, and N. Badache, "Distributed Low-Latency Data Aggregation Scheduling in Wireless Sensor Networks," *ACM Transactions on Sensor Networks (TOSN),* vol. 11, p. 49, 2015.

[135] N. Duc-Long, T. Le Quang Vinh, O. Berder, and O. Sentieys, "A low-latency and energy-efficient MAC protocol for cooperative wireless sensor networks," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM), ,* 2013, pp. 3826-3831.

[136] A. Berger, M. Pichler, W. Haslmayr, and A. Springer, "Energy Efficient and Reliable Wireless Sensor Networks-An Extension to IEEE 802.15. 4e," *EURASIP Journal on Wireless Communications and Networking 2014, 2014:126 doi:10.1186/1687-1499-2014-126,* 2014.

[137] A. Berger, A. Entinger, A. Potsch, and A. Springer, "Improving IEEE 802.15.4e LLDN performance by relaying and extension of combinatorial testing," in *Proceedings of the IEEE Emerging Technology and Factory Automation (ETFA),*, 2014, pp. 1-4.

[138] E. Uhlemann and A. Willig, "Joint Design of Relay and Packet Combining Schemes for Wireless Industrial Networks," in *Proceedings of the IEEE Vehicular Technology Conference, VTC Spring*, 2008, pp. 2441-2445.

[139] G. Patti, G. Alderisi, and L. L. Bello, "Introducing multi-level communication in the IEEE 802.15.4e protocol: The MultiChannel-LLDN," in *Proceedings of the IEEE Emerging Technology and Factory Automation (ETFA), ,* 2014, pp. 1-8.

[140] L. Dariz, G. Malaguti, and M. Ruggeri, "Performance analysis of IEEE 802.15.4 real-time enhancement," in *Proceedings of the IEEE 23rd International Symposium on Industrial Electronics (ISIE),*, 2014, pp. 1475-1480.

[141] M. Anwar and Y. Xia, "IEEE 802.15.4e LLDN: Superframe configuration for networked control systems," in *Proceedings of the 33rd Chinese Control Conference (CCC), ,* 2014, pp. 5568-5573.

[142] H. Kapil and C. S. R. Murthy, "Rainbow product ranking based relay placement and adaptive retransmission scheme for a reliable 802.15.4e LLDN," in *Proceedings of the IEEE International Conference on Industrial Technology (ICIT), ,* 2015, pp. 1914-1919.

[143] F. Qinyuan, H. Kai, and D. Yafei, "Rainbow Product Ranking for Upgrading E-Commerce," *IEEE Internet Computing, ,* vol. 13, pp. 72-80, 2009.

[144] R. C. Larson and A. R. Odoni, *Urban operations research*: Prentice Hall, Englewood Cliffs, NJ, 1981.

[145] D. P. Bertsekas and J. N. Tsitsiklis, *Introduction to Probability*: Athena Scientific, Second Edition, 2008.

[146] F. Bai and A. Helmy, "A survey of mobility models," *Wireless Adhoc Networks. University of Southern California, USA,* vol. 206, 2004.

[147] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, and M. Degermark, "Scenario-based performance analysis of routing protocols for mobile ad-hoc networks," in *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, 1999, pp. 195-206.

[148] N. Bulusu, D. Estrin, L. Girod, and J. Heidemann, "Scalable coordination for wireless sensor networks: self-configuring localization systems," in *Proceedings of the International Symposium on Communication Theory and Applications (ISCTA 2001), Ambleside, UK*, 2001.

[149] C. Bettstetter, H. Hartenstein, and X. Pérez-Costa, "Stochastic properties of the random waypoint mobility model," *Wireless Networks,* vol. 10, pp. 555-567, 2004.

[150] S. Bandyopadhyay, E. J. Coyle, and T. Falck, "Stochastic Properties of Mobility Models in Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing,,* vol. 6, pp. 1218-1229, 2007.

[151] E. L. Kaplan and P. Meier, "Nonparametric estimation from incomplete observations," *Journal of the American statistical association,* vol. 53, pp. 457-481, 1958.

[152] W. Dalei, C. Song, W. Haohong, and A. K. Katsaggelos, "Application-Centric Routing for Video Streaming Over MultiHop Wireless Networks," *IEEE Transactions on Circuits and Systems for Video Technology,,* vol. 20, pp. 1721-1734, 2010.

[153] I. F. Akyildiz, T. Melodia, and K. R. Chowdury, "Wireless multimedia sensor networks: A survey," *IEEE Wireless Communications, ,* vol. 14, pp. 32-39, 2007.

[154] C. Buratti, "Performance Analysis of IEEE 802.15.4 Beacon-Enabled Mode," *IEEE Transactions on Vehicular Technology, ,* vol. 59, pp. 2031-2045, 2010.

[155] K. Jin-Woo, K. Jihoon, and E. Doo-Seop, "Multi-dimensional channel management scheme to avoid beacon collision in LR-WPAN," *IEEE Transactions on Consumer Electronics, ,* vol. 54, pp. 396-404, 2008.

[156] N. Nordin and F. Dressler, "Effects and Implications of Beacon Collisions in Co-Located IEEE 802.15.4 Networks," in *Proceedings of the IEEE Vehicular Technology Conference (VTC Fall),*, 2012, pp. 1-5.

[157] E. Toscano and L. Lo Bello, "A multichannel approach to avoid beacon collisions in IEEE 802.15.4 cluster-tree industrial networks," in *Proceedings of the IEEE Conference on Emerging Technologies & Factory Automation, ETFA*, 2009, pp. 1-9.

[158] Z. Hanzalek and P. Jurcik, "Energy Efficient Scheduling for Cluster-Tree Wireless Sensor Networks With Time-Bounded Data Flows: Application to IEEE 802.15.4/ZigBee," *IEEE Transactions on Industrial Informatics, ,* vol. 6, pp. 438-450, 2010.

[159] A. Koubaa, R. Severino, M. Alves, and E. Tovar, "Improving Quality-of-Service in Wireless Sensor Networks by Mitigating Hidden-Node

Collisions," *IEEE Transactions on Industrial Informatics, ,* vol. 5, pp. 299-313, 2009.

[160] S. Shiann-Tsong, S. Yun-Yen, and L. Wei-Tsong, "CSMA/CF Protocol for IEEE 802.15.4 WPANs," *IEEE Transactions on Vehicular Technology,,* vol. 58, pp. 1501-1516, 2009.

[161] A. J. Jara, D. Fernandez, P. Lopez, M. A. Zamora, and A. F. Skarmeta, "Lightweight Mobile IPv6: A mobility protocol for enabling transparent IPv6 mobility in the Internet of Things," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*, 2013, pp. 2791-2797.

[162] E. Rescorla, *SSL and TLS: designing and building secure systems* vol. 1: Addison-Wesley Reading, 2001.

[163] R. Housley, W. Polk, W. Ford, and D. Solo, "RFC 3280-Internet X. 509 Public Key Infra-structure Certificate and Certificate Revocation List (CRL) Profile. 2002," *Network Working Group-Request for Comments, The Internet Society*.

[164] E. Rescorla and A. Schiffman, "The secure hypertext transfer protocol," *IETF, RFC (2660),* 1999.

[165] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight Secure CoAP for the Internet of Things," *IEEE Sensors Journal,* vol. 13, pp. 3711-3720, 2013.

[166] E. Rescorla and N. Modadugu, "Datagram transport layer security version 1.2," *IETF, RFC (6347),* 2012.

[167] J. L. Hern, R. ndez, M. P. Pawlowski, A. J. Jara, A. F. Skarmeta, and L. Ladid, "Toward a Lightweight Authentication and Authorization Framework for Smart Objects," *IEEE Journal on Selected Areas in Communications,* vol. 33, pp. 690-702, 2015.

[168] L. M. S. Committee, "Part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE Std 802.11 i-2004," *IEEE Comput Soc,* 2004.

[169] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible authentication protocol (EAP)," ed. IETF, RFC 3748: RFC 3748, June, 2004.

[170] S. Willens, A. C. Rubens, C. Rigney, and W. A. Simpson, "Remote authentication dial in user service (RADIUS)," *IETF, RFC 2865*, 2000.

[171] D. Altolini, V. Lakkundi, N. Bui, C. Tapparello, and M. Rossi, "Low power link layer security for IoT: Implementation and performance analysis," in *Proceedings of the 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2013, pp. 919-925.

[172] P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttila, and M. Sain, "Lightweight and Secure Session-Key Establishment Scheme in Smart Home Environments," *IEEE Sensors Journal*, vol. 16, pp. 254-264, 2016.

[173] G. Piro, G. Boggia, and L. A. Grieco, "A standard compliant security framework for IEEE 802.15.4 networks," in *Proceedings of the IEEE World Forum on Internet of Things (WF-IoT), ,* 2014, pp. 27-30.

[174] S. Sciancalepore, G. Piro, E. Vogli, G. Boggia, and L. A. Grieco, "On securing IEEE 802.15.4 networks through a standard compliant framework," in *Proceedings of the Euro Med Telco Conference (EMTC), 2014*, 2014, pp. 1-6.

[175] S. N. Premnath and Z. J. Haas, "Security and Privacy in the Internet-of-Things Under Time-and-Budget-Limited Adversary Model," *IEEE Wireless Communications Letters*, vol. 4, pp. 277-280, 2015.

[176] S. Misra, S. Goswami, C. Taneja, A. Mukherjee, and M. S. Obaidat, "A PKI Adapted Model for Secure Information Dissemination in Industrial Control and Automation 6LoWPANs," *IEEE Access*, vol. 3, pp. 875-889, 2015.

[177] I. Nikolaevskiy, D. Korzun, and A. Gurtov, "Security for medical sensor networks in mobile health systems," in *Proceedings of the IEEE 15th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM),*, 2014, pp. 1-6.

[178] S. Chakrabarti, Z. Shelby, and E. Nordmark, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)," *IETF, RFC 6775*, 2012.

[179] S. Sciancalepore, G. Piro, G. Boggia, and L. Grieco, "Application of IEEE 802.15. 4 security procedures in OpenWSN protocol stack," *IEEE Standards Education e-Magazine*, vol. 4, 2014.

[180] G. S. Quirino, E. D. Moreno, and L. B. Matos, "Performance Evaluation of Asymmetric Encryption Algorithms in embedded platforms used in WSN," in *Proceedings of the International Conference on Security and Management (SAM)*, 2013, p. 1.