Green and Secure Medium Access Control for Wireless Sensor Network

Pawar, Pranav M.

DOI (link to publication from Publisher):
10.5278/vbn.phd.engsci.00087

Publication date:
2016

Document Version
Publisher's PDF, also known as Version of record

GREEN AND SECURE MEDIUM ACCESS CONTROL FOR WIRELESS SENSOR NETWORK

BY
PRANAV MOTHABHAU PAWAR

DISSERTATION SUBMITTED 2016

AALBORG UNIVERSITY
DENMARK

Green and Secure Medium Access Control for Wireless Sensor Network

Pranav Mothabhau Pawar

A thesis submitted in partial fulfillment for the
degree of Doctor of Philosophy

in the

Department of Electronic Systems
Aalborg University

January 2016

Dissertation submitted: January 2016

PhD supervisors: Associate Professor Neeli Rashmi Prasad
Aalborg University, Denmark

Assistant Professor Rasmus Hjorth Nielsen
Aalborg University, Denmark

PhD committee: Associate Professor Rasmus Løvenstein Olsen (chairman)
Department of Electronic Systems
Aalborg University

Associate Professor Periklis Chatzimisios
Department of Informatics
Alexander TEI of Thessaloniki

Senior Researcher Dr. Dilip Krishnaswamy
IBM Research Labs
Manyata Business Park

PhD Series: Faculty of Engineering and Science, Aalborg University

ISSN (online): 2246-1248
ISBN (online): 978-87-7112-500-9

Published by:
Aalborg University Press
Skjernvej 4A, 2nd floor
DK – 9220 Aalborg Ø
Phone: +45 99407140
aauf@forlag.aau.dk
forlag.aau.dk

Printed in Denmark by Rosendahls, 2016

Abstract

Wireless sensor networks (WSNs) have great application, but, as of today, energy consumption in sensor nodes is a major constraint when considering the lifetime of the network. Energy is consumed in all layers of the network protocol, but the medium access control (MAC) layer consumes a significant share of the energy. This thesis examines the design of MAC layer mechanisms that are energy efficient and secure to support mission-critical applications.

Based on an analysis of application requirements, hybrid MAC mechanisms are found to be efficient solutions for WSNs through significant energy savings with good throughput. A survey of state-of-the-art concludes that there are no similar benchmarks for performance testing of MAC layer mechanisms and the thesis therefore proposes a framework for this.

Scheduling is a major building block of any hybrid MAC layer mechanism and the research proposes the cluster-based scheduling algorithms Green Conflict Free (GCF) and Multicolor GCF (M-GCF) to improve the scheduling delay by increasing the reuse of slots and scalability by stabilizing the topology evaluated in static and mobile scenarios. Further, the hybrid-scheduling algorithm Hybrid GCF (H-GCF) is proposed and it shifts the mode from GCF to M-GCF and vice-versa based on mobility in the network showing improved performance compared with existing state-of-the-art solutions.

The thesis also examines the need of synchronization algorithms for WSNs and proposes a cluster-based hybrid-synchronization algorithm using both tight and loose synchronization making it efficient for time division multiple access (TDMA) scheduling. A MAC mode control mechanism is proposed based on collisions in the network to shift the mode of transmission from carrier sense multiple access (CSMA) to TDMA and vice versa.

Green and Hybrid MAC (GHMAC) is proposed as a full hybrid MAC layer mechanism combining all the proposed mechanisms (scheduling, synchronization, and MAC mode control) and the results show that it outperforms existing state-of-the-art solutions.

As part of this thesis, security on the MAC layer has also been examined including sequential and activity modeling approaches for different attacks. Further, the research outlines new attacks on hybrid MAC mechanisms and, as a result, a modified GHMAC is proposed to countermeasure the effects from denial of sleep attacks - Green and Secure Hybrid MAC (GSHMAC).

Dansk Resume

Trådlœse sensornetværk har stor anvendelighed, men for nuværende er energiforbruget i sensorknuder en væsentlig hindring i forhold til levetid af netværket. Energi forbruges i alle lag af netværksprotokollen, men mediumsadgangskontrol laget forbruger en væsentlig del af energien. Denne afhandling undersœger design af ??mediumsadgangskontrol mekanismer, der er energieffektive og sikre nok til at understœtte kritiske applikationer.

Baseret påen analyse af applikationskrav, er hybride mediumsadgangskontrol mekanismer effektive lœsninger for trådlœse sensornetværk til WSNs gennem betydelige energibesparelser med god data hastighed. En undersœgelse af den nyeste relaterede forskning konkluderer, at der ikke er nogen tilsvarende benchmarks for test af mediumsadgangskontrol mekanismer og afhandlingen foreslår derfor en ramme for dette.

Planlægning er en vigtig byggesten i enhver hybrid mediumsadgangskontrol mekanisme og forskningen foreslår to klynge-baserede planlægning algoritmer (GCF og M-GCF) for at forbedre planlægningsforsinkelse ved at œge genbrug af perioder og skalerbarhed ved at stabilisere topologien evalueret i statiske og mobile scenarier. Endvidere er hybrid-planlægning algoritmen (H-GCF) foreslået, der skifter tilstand fra GCF til M-GCF og omvendt baseret påmobiliteten i netværket og viser forbedret ydeevne i forhold til eksisterende lœsninger.

Afhandlingen undersœger ogsåbehovet for synkronisering algoritmer og foreslår en klynge-baserede hybrid-synkronisering algoritme, der anvender både stram og lœs synkronisering, der gœr den effektiv for tidsmæssig planlægning. En kontrolmekanisme er foreslået baseret påkollisioner i netværket til at ændre måden hvorpåen transmission foregår.

En grœn, hybrid mediumsadgangskontrol mekanisme (GHMAC) foreslås som en fuld lœsning, der kombinerer alle de foreslåede mekanismer (planlægning, synkronisering og kontrol), og resultaterne viser, at den er bedre end eksisterende lœsninger.

Som en del af denne afhandling, er sikkerheden påmediumsadgangskontrol laget ogsåblevet undersœgt, herunder sekventielle og aktivitet modelleringstilgange til forskellige angreb. Endvidere har forskningen skitseret nye angreb påhybrid mediumsadgangskontrol mekanisme og som et resultat, er en modificeret mekanisme (GSHMAC) foreslået for modforanstaltninger effekterne af visse angreb.

Acknowledgements

This thesis represents the fascinating and thrilling journey of research. Needless to say, there are many individuals who have had crucial roles during the journey. This is only a modest effort to thank them. The way of research is long and there are many high peaks, deep valleys and steep inclines. To complete all the stages successfully, we require correct directions, great inspiration and encouragement from our supervisor. That is why I want to express my profound gratitude to my supervisor, Associate Professor Dr. Neeli R. Prasad. She always provided a perspective when approached, readily and with amazing grace. I am very thankful to her for thoughtful and logical guidance, insightful vision, continuing support and frank nature that have led me to grow immensely over the years.

This journey of research could not have been so interesting and full of knowledge without the kind support of Professor Dr. Ramjee Prasad. He has been a great mentor throughout my year of PhD study. I am very thankful to him for opening my eye to the research world.

I also want to express my deep gratitude to Dr. Rasmus H. Nielsen for guiding, collaborating and helping me to successfully complete my research. This thesis could not be accomplished within this time frame if it was not for his review. He taught me, both consciously and unconsciously, how good research is done. Dr. Rasmus has been a source of friendships as well as good advice and collaboration.

Furthermore, I am thankful to all my GISFI and CTIF colleagues from the department for their continuous support and cooperations during these years of PhD study. I am very thankful to all of them for making my stay in Aalborg memorable and comfortable.

My special thanks to Mrs. Jyoti Prasad, Dr. Anand Prasad, and Mr. Rajiv Prasad for making my stay much comfortable with their love care, and support. I am very obliged to all of them for not letting me feel away from home and making stay in Aalborg a lifetime memories.

My PhD program at Aalborg University has been funded by Sinhgad Technical Education Society (STES), Pune, India with a great thought of research in information and communication technology, which will beneficial to the society and student community in India. I am indebted to the honorable founder and president of STES, Prof. M. N. Navale, founder secretary of STES, Dr. Mrs. S. M. Navale, Vice President (HR), Mr. Rohit M. Navale, Vice President (Admin), Mrs. Rachana Ashtekar Navale, Dr. A.V. Deshpande, Dr. S. D. Markande, and Dr. M. S. Gaikwad for their trust on me and inexplicable support. I am very much thankful to Dr. S. S. Inamdar and Dr. Mrs. J. S Inamdar for motivating and supporting in the whole PhD process and for their work in changing the thought process of the engineering faculty.

I am also very thankful to all my department colleagues at SKNCOE, Pune especially Nandkumar Kulkarni, Lalit Patil, Ravindra Borhade, Yogita Wagh, Gauri Konde, Nivedita Deshmukh, Varsha Khan-

dekar, Sheetal Raina, Sayali, Sonali for their kind support and help. They make me smile and relax during all my tensions and worries.

I would like to give my biggest thank to my family, my parents (Ujwala and Mothabhau) for having given great support during every decision of life and my brother Nikhil for encouraging me with his best wishes. I am thankful to all my relatives especially my aunty Dr. Ashalata Sonawane and uncle Dr. Arun Bachhav for their best wishes for my PhD study. I am deeply indebted to my wife Dr. Harshada for being with me during my research time and having stood with me in all good and bad times. She has contributed countless hours in direct support from her busy schedule of her hospital for my work. I am very thankful to my in-laws (Arun and Nanda Borse) for raising love of my life with such values and care. A word goes for my baby boy Ayansh who enter in our life with ray of happiness.

Finally, yet important, I want to thank all my teachers from childhood for giving me the spark of knowledge and thanks to everyone who supported knowingly or unknowingly this research work. The memorable journey with all during this PhD study is going to last forever in my mind.

Contents

List of Figures **XIII**

List of Tables **XV**

List of Acronyms **XVII**

1 Introduction **1**
- 1.1 Motivation . . . 2
- 1.2 Background . . . 2
  - 1.2.1 Layers . . . 2
  - 1.2.2 Classification . . . 3
  - 1.2.3 Requirements . . . 4
- 1.3 Building Blocks of MAC Mechanisms . . . 5
- 1.4 Research Methodology . . . 7
  - 1.4.1 Research Hypotheses . . . 7
  - 1.4.2 Methodology Overview . . . 7
- 1.5 Contributions . . . 9
- 1.6 Publications . . . 12
- 1.7 Thesis Outline . . . 14
- 1.8 References . . . 16

2 Benchmarks and Comparative Evaluation of WSN MAC Mechanisms **19**
- 2.1 Introduction . . . 20
- 2.2 Related Work . . . 21
  - 2.2.1 Benchmarking Survey of WSN MAC Mechanisms . . . 21
  - 2.2.2 Available Implementation Environments . . . 24
- 2.3 Proposed Benchmarks for MAC Mechanism Testing . . . 25
  - 2.3.1 Physical Parameters . . . 25
  - 2.3.2 Performance Measurement Parameters . . . 26
  - 2.3.3 Implementation Environment . . . 26
  - 2.3.4 Testing Scenario . . . 27
  - 2.3.5 Variables for Measuring Performance . . . 28

2.4 Comparative Evaluation of Hybrid MAC Mechanisms . . . 28
2.4.1 Simulation Details . . . 28
2.4.2 Simulation Results and Analysis . . . 29
2.5 Summary . . . 30
2.6 References . . . 31

3 Conflict Free TDMA Scheduling 35
3.1 Introduction . . . 36
3.2 Related Work . . . 37
3.2.1 Classification of TDMA Scheduling Algorithms . . . 37
3.2.2 TDMA Scheduling for Flat Network . . . 39
3.2.3 TDMA Scheduling for Clustered Network . . . 41
3.3 Assumptions, System Model, and Methodology . . . 42
3.3.1 Assumptions . . . 42
3.3.2 Basic Notations . . . 42
3.3.3 System and Communication Model . . . 43
3.3.4 Methodology . . . 43
3.4 Conflict Free TDMA Scheduling . . . 44
3.4.1 GCF: Green Conflict Free TDMA Scheduling Algorithm . . . 44
3.4.2 M-GCF: Multicolor Green Conflict Free TDMA Scheduling Algorithm . . . 46
3.4.3 Simulation Results for GCF and M-GCF . . . 48
3.5 Hybrid Conflict Free TDMA Scheduling . . . 52
3.5.1 Mobility Threshold Decision . . . 52
3.5.2 Requirement of Hybrid TDMA Scheduling . . . 52
3.5.3 H-GCF: Hybrid Green Conflict Free Algorithm . . . 53
3.5.4 Simulation of H-GCF . . . 55
3.6 Summary . . . 58
3.7 References . . . 59

4 Synchronization Control 61
4.1 Introduction . . . 62
4.2 Related Work . . . 63
4.3 Cluster-based Hybrid Synchronization for WSNs . . . 65
4.3.1 Assumptions and System Model . . . 65
4.3.2 Hybrid Synchronization Mechanism . . . 65
4.4 Simulation Results . . . 67
4.4.1 Performance in Terms of Synchronization Overheads . . . 67
4.4.2 Performance Comparison under Static Scenarios . . . 69
4.4.3 Performance Comparison under Mobile Scenarios . . . 69
4.5 Summary . . . 70
4.6 References . . . 71

5 GHMAC: Green and Hybrid Medium Access Control 73

5.1 Introduction . . . 74
5.2 Related Work . . . 75
5.3 Building Blocks . . . 78
5.3.1 MAC Mode Control in GHMAC . . . 78
5.4 Simulation Results . . . 80
5.4.1 Simulation Methodology . . . 80
5.4.2 Varying Collision Threshold . . . 81
5.4.3 Varying Number of Nodes and Area of Network . . . 82
5.4.4 Mobility Scenarios . . . 83
5.4.5 Denial of Sleep Attacks . . . 84
5.5 Summary . . . 85
5.6 References . . . 86

6 MAC Security Attacks and Countermeasures 89
6.1 Introduction . . . 90
6.2 Modeling of MAC Layer Security Attacks . . . 91
6.2.1 UML Modeling . . . 91
6.2.2 Sequential Modeling of WSN MAC Security Attacks . . . 92
6.2.3 Activity Modeling of WSN MAC Security Attacks . . . 96
6.3 Comparative Evaluation of WSN MAC Security Attacks on Hybrid MAC Mechanisms . 99
6.3.1 Simulation Details . . . 99
6.3.2 Results and Discussion . . . 101
6.4 New Attacks on Hybrid MAC Mechanisms . . . 105
6.4.1 ECN Attack . . . 105
6.4.2 CH Attack . . . 106
6.5 GSHMAC: Green and Secure Hybrid Medium Access Control . . . 107
6.5.1 Introduction . . . 107
6.5.2 Related Work . . . 109
6.5.3 GSHMAC Mechanism . . . 111
6.5.4 Simulation Results and Discussions . . . 114
6.6 Summary . . . 116
6.7 References . . . 117

7 Conclusions and Future Work 119
7.1 Summary of Contributions . . . 120
7.2 Future Work . . . 121

List of Figures

1.1 Layered architecture of WSN 2
1.2 Classification of WSN MAC mechanisms based on the comparative evaluation in Chapter 2. 3
1.3 Categories of WSN 4
1.4 Building blocks for a hybrid MAC mechanism. 5
1.5 Identified and addressed challenges for WSN hybrid MAC. 6
1.6 Evolution of the problem statement 8
1.7 Structure of green and secure hybrid MAC mechanism 9
1.8 Modules of research and contributions 10
1.9 Organization of the thesis [19, 24, 25, 28, 29, 30, 31, 32, 36] 14

2.1 Blocks of testing benchmarks. 20
2.2 Chapter 2 contributions. 21
2.3 Energy consumption. 30
2.4 Throughput. 30
2.5 Delay. 31

3.1 Chapter 3 contributions. 38
3.2 Classifications of TDMA scheduling algorithms. 38
3.3 System and communication model. 44
3.4 Phase 1 of the GCF algorithm for intra-cluster communication. 45
3.5 Phase 1 of the M-GCF algorithm for intra-cluster communication. 47
3.6 Results for number of nodes. 50
3.7 Results for single-color (GCF) and multi-color (M-GCF) algorithms. 51
3.8 X-Y view of single-color (GCF) and multi-color (M-GCF) algorithms. 52
3.9 Sequence of activities in H-GCF. 54
3.10 Comparative results for fixed mobility speed - all measures are averages. 56
3.11 Comparative results for random mobility speed - all measures are averages. 57
3.12 Comparative results for varying mobility thresholds - all measures are averages. 58
3.13 Comparative results under local and global mode shift - all measures are averages. 58

4.1 Chapter 4 contributions. 63
4.2 Clock synchronization. 65

4.3 Synchronization flow diagrams. 66
4.4 Synchronization errors during network synchronization. 68
4.5 Average energy consumption during network synchronization. 68
4.6 Results for synchronization algorithms under static scenarios. 69
4.7 Results for synchronization algorithms under mobile scenarios. 70

5.1 Pillars of hybrid MAC mechanism. 74
5.2 Chapter 5 contributions. 75
5.3 MAC mode control for intra-cluster communication. 79
5.4 Results for varying collision threshold. 82
5.5 Results as a function of number of nodes. 83
5.6 Results as a function of the area of the network. 83
5.7 Results with varying percentage of mobility and speed. 84
5.8 Results under different denial of sleep attackss. 85

6.1 Chapter 6 contributions. 91
6.2 Sequence diagram of collision attack. 93
6.3 Sequence diagram of unintelligent replay attack. 93
6.4 Sequence diagram of unauthenticated broadcast attack. 94
6.5 Sequence diagram of full domination attack. 94
6.6 Sequence diagram of exhaustion attack. 95
6.7 Sequence diagram of intelligent jamming attack. 96
6.8 Activity diagram of the collision attack. 97
6.9 Activity diagram of unintelligent replay attack. 98
6.10 Activity diagram of unauthenticated broadcast attack. 99
6.11 Activity diagram of full domination attack. 100
6.12 Activity diagram of exhaustion attack. 101
6.13 Activity diagram of intelligent jamming attack. 102
6.14 Results for energy consumption. 104
6.15 Results for throughput. 104
6.16 Results for delay. 104
6.17 (a) Collision at the intermediate node, (b) Intermediate node sends an ECN message to all nodes for collision information, (c) Attack in which malicious node will unnecessarily transmit the ECN message. 105
6.18 Sequential diagram of ECN attack. 106
6.19 Activity modeling of ECN attack. 107
6.20 Activity modeling of CH attack. 108
6.21 Countermeasure for collision attack. 112
6.22 Countermeasure for replay attack. 114
6.23 Comparative results for interference on same slot - all measures are averages. 115
6.24 Comparative results for interference on random slot - all measures are averages. 116

List of Tables

2.1 Benchmarking survey of MAC mechanisms 24
2.2 Different implementation environments for WSNs 25
2.3 Simulation parameters for MAC mechanism simulation. 29

3.1 Simulation parameters for simulating TDMA scheduling algorithms. 49

4.1 Parameters for synchronization algorithm simulation 67

5.1 Parameters for GHMAC simulation. 81

6.1 Simulation and node parameters for simulating attacks on ZMAC. 103
6.2 Simulation parameters for simulating GSHMAC. 115

List of Acronyms

ADCA Asynchronous Duty Cycle Adjustment MAC

A-DRAND Adaptive Distributed Randomized

AI-LMAC Adaptive, Information Centric and Lightweight MAC

Alert Adaptive Low-Latency Event-Driven MAC

AODV Ad-Hoc On-Demand Distance Vector Routing

AP Access Point

AVR Automatic Voltage Regulator

BAN Body Area Network

Bin-MAC Binary MAC

BMAC Berkeley MAC

Box-MAC Boundary MAC

BS Base Station

CA-MAC Channel Access MAC

CARL Cluster Adaptive Rate Limiting

CBH-FTS Cluster-Based Hierarchical Flooding Time Synchronization

CBR Constant Bit Rate

CDMA Code Division Multiple Access

C-MAC Classifier-MAC

CC-MAC Correlation Based Cooperative MAC

CDMA Code Division Multiple Access

CH Cluster Head

COSMIC Cooperative Medium Access Control with Minimal Control Messages

CRN Cognitive Radio Network

CRMAC Contention Reserve MAC

CSE Collision Experience

CSMA Carrier Sense Multiple Access

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance

ct Collision Threshold

CTS Clear to Send

CWS-MAC Cooperative Wireless Sensor Network MACl

DD-TDMA Deterministic Distributed Time Division Multiplae Access

DFS Depth-First Search

Diff-MAC Differentiated Services MAC

DMAC Data Gathering MAC

DMNC Decrement Mobile Node Count

DNIB Distributed Neighborhood Information Based

DRAND Distributed Randomized Scheduling

DSMAC Dynamic Sensor MAC

DWMAC Demand Wakeup MAC

E2RMAC Energy-Efficient Reliable MAC

EBMAC Event Based MAC

ECN Explicit Contention Notification

eL-MAC Enhanced Lightweight MAC

EMCA Enhanced Multihop Clustering Algorithm

EQ-MAC Energy efficient Quality MAC

ERMAC Emergency Response MAC

FDMA Frequency Division Multiple Access

FED Full Function Device

FPRP Five-Phase Reservation Protocol

FTSP Flooding Time Synchronization Protocol

GCF Green Conflict Free

GeRaF Geographic Random Forwarding

GHMAC Green and Hybrid MAC

GLASS Grid-based Latin Squares Scheduling Access

GMAC Gateway MAC

GPS Global Positioning System

GSHMAC Green and Secure Hybrid MAC

GUI Graphical User Interface

GTIM Gateway's Traffic Indication Message

H-GCF Hybrid-GCF

HCL High Contention Level

HEATS Hybrid Energy Aware Time Synchronization

HyMAC Hybrid MAC

ID Identification

IEEE Institute of Electrical and Electronics Engineers

IDE Integrated Development Environment

ict Initial Collision Threshold

IHMAC Intelligent Hybrid MAC

IMNC Increment Mobile Node Count

IoT Internet of Things

J-Sim Java Simulator

LASA Low-energy Adaptive Slot Allocation

LCL Low Contention Level

LLC Logical Link Control

LMAC Lightweight MAC

LE-MAC Latency and Energy Aware MAC

LN Leaf Node

LPL Low Power Listening

LS Latin Square

M-GCF Multi-color-GCF

M-WSN Mobile-WSN

MAC Medium Access Control

MC Mode Change

MC-LMAC Multi-channel MAC

MD-5 Message Digest 5

MHMAC Multimode Hybrid MAC

MH-MAC Mobility Adaptive Hybrid MAC

ML-MAC Multi-layer MAC

MMSN Multi-frequency MAC

MSSS Multiple Sources, Single Sink

MANET Mobile Ad-Hoc Network

NED Network Description

nesC Nested C

NS-2 Network Simulator-2

OTCL Object Tool Command Language

OS Operating System

PDR Packet Delivery Ratio

PEDAMACS Power Efficient and Delay Aware MAC for Sensor Network

PRIMA Priority-based MAC

QMAC Query MAC

QoS Quality of Service

RBS Reference Broadcast Synchronization

RFD Reduced Function Device

RL-MAC Reinforcement Learning MAC

RMAC Randomized MAC

RMC Reverse Mode Change

RTS Request to Send

RTSync Round Trip Synchronization

RTP/RTCP Real-Time Transport Protocol

RSSI Received Signal Strength Indication

S-ALOHA Slotted ALOHA

SG Sink Gateway

SHA-1 Secure Hash Algorithm 1

SIC Sector In-charge

SM Sector Monitor

SMAC Sensor-MAC

SSSS Single Source, Single Sink

STEM Sparse Topology and Energy Management

S-WSN Static-WSN

TDMA Time Division Multiple Access

TDMA-ASAP TDMA Scheduling with Adaptive Slot-stealing and Parallelism

TDP Time Diffusion Protocol

TE2S Two-tier Receiver-initiated Secure

TMAC Timeout-MAC

TMCP Tree-based Multichannel Protocol

TPSN Timing-sync Protocol for Sensor Network

TRAMA Traffic Adaptive Medium Access Protocol

UDP User Datagram Protocol

UML Unified Modeling Language

Wise-MAC Wireless Sensor MAC

WSN Wireless Sensor Network

ZMAC Zebra MAC

Chapter 1

Introduction

The goal of this chapter is to explain the motivation, background and challenges leading up to the research work on a Wireless Sensor Network (WSN) Green and Secure Medium Access Control (MAC) mechanism. Critical issues and building blocks for hybrid MAC mechanisms are described to reach the synopsis of the thesis. The chapter identifies the research questions and explains the methodology adopted to solve them. The goals and objectives of the research work are also explained in this chapter together with the scientific contributions and the contributing publications are provided. Finally, the outline of the thesis is provided to give an overview of the individual chapters.

1.1 Motivation

The future is moving towards the Internet of Things (IoT) and it is expected that, by 2020, IoT will drive the deployment of 50 billion connected devices and a value-at-stake of $19 trillion [1]. In facilitating and realizing the vision of IoT, WSNs are becoming increasingly relevant [2, 3, 4] with great application value and broad vision in the fields of military [5], transportation and vehicle monitoring [6], agricultural [7], environmental and animal monitoring [8], healthcare applications [9], industrial and business application [10], building-, home-, weather-, and city- monitoring [11], space exploration [12], and so on.

Many IoT verticals and use cases have strict network and application layer requirements. Such use cases include telehealth, vehicular networks, industrial automation, and defense [1, 2, 3] that all require reliability, security and long network lifetime. The challenge of utilizing a WSN for these use cases is the resource constrained nature of the WSN with limited battery resources, communication bandwidth, computing power, and memory [2, 3]. Energy is being consumed across all layers of the communication stack in WSN nodes during send-, receive-, sleep-, and idle-mode and is thus a major constraint as it affects the network lifetime.

1.2 Background

A WSN consists of a large number of WSN nodes deployed over a geographical area that actively cooperate to accomplish one or more jobs such as sensing by communicating the information.

1.2.1 Layers

The individual layers of the WSN communication stack is shown in Figure 1.1 with each layer attributing to energy consumption in the node.

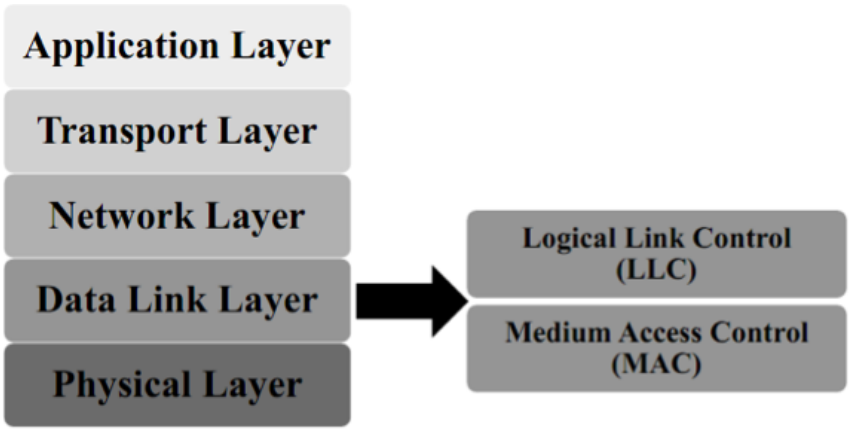


Figure 1.1: Layered architecture of WSN

The physical layer mainly consumes energy for operating the radio circuitry, performing modulation and for the actual transmission of bit streams [13]. Moving up, the data link layer is responsible for data transfer between nodes via shared links/channels. The data link layer is divided into the Logical Link Control (LLC) and MAC respectively and consumes energy for error-detection and correction, multiplexing of data streams and managing/accessing a link for data transfer. The network layer is responsible for routing the sensed information to the consigned destination node [14, 15] and the WSN

node consumes energy during route establishment, transmission of routing packets and aggregation of information [16]. The transport layer is accountable for maintaining the reliability and quality of information in the network and, hence, consumes energy during packet recovery, monitoring and detection of congestion in the network [17]. The application layer is responsible for managing different application specific functionalities such as query processing and various network management functionalities where heavy application specific functionalities can be very energy consuming [18].

Of the different layers, the MAC layer's energy requirement stands out due to the features and responsibilities undertaken to fulfill its tasks [14, 15]. The primary reason for the higher energy consumption is the decision on availability and proficient use of resources and transmission of information over the wireless medium. These processes get complex as the number of nodes or users in the network increases, which lead to more interference. The MAC layer also plays a major role in the design of WSNs as it controls the active and sleep state of each node. Major sources of energy wasted at the MAC layer are collision of frames when two or more nodes are transmitting at the same time, overhearing irrelevant transmissions, overheads due to control packets and idle listening when the node does not know when it will be a receiver [15].

1.2.2 Classification

In general, MAC mechanisms are designed either as contention- or schedule-based [15]. The classification of MAC mechanisms is shown in Figure 1.2. A contention-based MAC mechanism is simpler, more flexible and requires less infrastructure support as these mechanisms allocate resources on-demand, making it adaptable to traffic conditions and changes in topology, density of nodes, etc. The main challenges for contention-based MAC protocols are reducing energy consumption, improving throughput and guaranteeing the fairness encountered due to lack of communication coordination [15]. A schedule-based MAC mechanism differs from a contention-based by assigning time slots to each node and thereby avoiding interference in the transmission i.e. guaranteeing collision-free transmission, which reduces the energy consumption. It also guarantees good throughput and fairness because the protocol coordinates the access to the channel at any time for all nodes. Some challenges with schedule-based approaches are determining collision-free slots, assigning slots to nodes, providing tight synchronization in the network and also the adaptability to support topology and density changes.

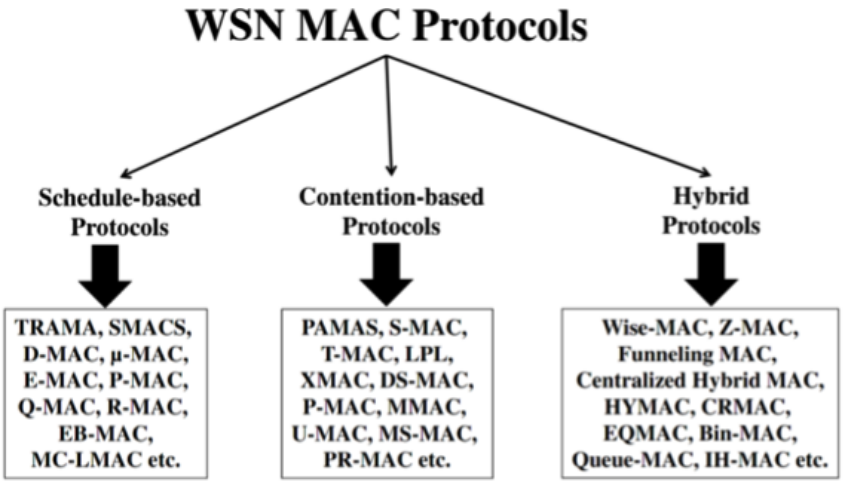


Figure 1.2: Classification of WSN MAC mechanisms based on the comparative evaluation in Chapter 2.

Many MAC mechanisms have been proposed using the above-mentioned traditional mechanisms [15]. However, each of these mechanisms have limitations and recent research has proposed hybrid mechanisms for MAC comprising characteristics of both contention- and schedule-based mechanisms. These hybrid techniques are aimed at achieving equilibrium conditions for WSN MAC by rapidly switching between Carrier Sense Multiple Access (CSMA) and Time Division Multiple Access (TDMA) based on the traffic conditions in the network, which can save significant amounts of energy. The main problem with hybrid mechanisms is their complexity that makes them applicable to only a limited set of applications [15, 19]. Existing work has analyzed current WSN applications such as vehicle monitoring on a highway, where vehicles are continuously entering and exiting, but their frequency is not same during a day. In such cases, the data-traffic is suddenly going from high to low and vice versa and, therefore, the WSN needs a MAC mechanism that is adaptable to the changes. Here, hybrid MAC mechanisms provide better and more efficient solutions that are able adapt and, thus, lead to improved performance.

Based on the discussed applications, WSNs can be categorize in two ways according to the management of the network [20] as shown in Figure 1.3; flat and cluster-based or hierarchical. A flat WSN considers the network as complete, where each node plays the same role except the sink node. In a cluster-based WSN, the nodes are divided into a number of clusters where different roles are assigned to nodes with each cluster having a Cluster Head (CH). The CH has the same energy and processing power as the other nodes, but it has an extra task as it collects the information from the other nodes in the cluster, aggregates it and sends it to other CHs or to the sink node. Cluster-based WSNs have advantages over flat WSNs as they can improve energy efficiency and enhance scalability and adaptivity. Another classification is done based on the mobility of nodes required in some applications and can be categorized as Static-WSN (S-WSN) and Mobile-WSN (M-WSN) with nodes moving with a certain speed [21] e.g. in transportation.

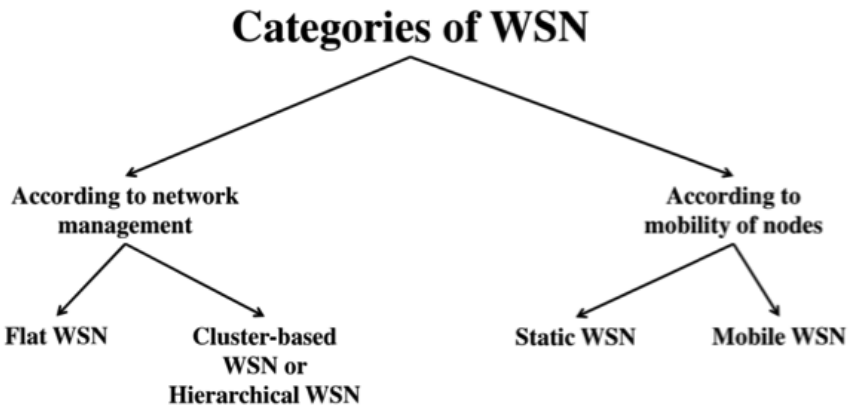


Figure 1.3: Categories of WSN

1.2.3 Requirements

In most current and emerging WSN applications, mobility is an important requirement as M-WSNs offer significant advantages in such use cases including energy efficiency, increasing the coverage area of the network and improving the channel capacity. Therefore, MAC mechanisms for WSNs should support both static and mobile scenarios and be able to perform well in both. To support the large, varied applications of S-WSNs and M-WSNs, requirements include energy efficiency, low delays, long network lifetime,

effective use of bandwidth, and scalability and adaption to changes in the network in terms of varying number of nodes and movement of nodes from one position to another. These requirements are applicable to all layers of a WSN, but are influenced more by the activities of the MAC layer. Therefore, it is necessary to design a MAC mechanism that takes mobility into consideration [19, 21].

Many WSN applications carry sensitive information e.g. about enemy targets in case of the military application, so to protect the transmitted information is also a prime concern. Comparing with traditional network security, WSN security is more complex and should also consider the constrained based nature of the nodes [22] and a security mechanism should not lead to no or very limited additional energy consumption. A WSN is susceptible to many different security attacks at all layers of the communication, the MAC layer plays a central part in the case of WSN as it accounts for substantial energy consumption by governing channel capacity utilization. The responsibilities of the MAC layer make it vulnerable to many different attacks such as collision attacks, denial of sleep attacks, exhaustion attacks, etc. [23, 24] that can introduce a significant amount of delays and also increase the energy drain in the network. Current research in WSN security has given little attention to internal MAC mechanism security, which can be fruitful to enhance MAC mechanisms performance in attack situations [25].

Based on this, the research work leading up to this thesis concentrates on the development of WSN MAC mechanisms that reduce the energy consumption, are adaptable to changing traffic conditions, are scalable, support mobility, and can countermeasure the effects of security attacks by improving performance in the presence of an attack.

1.3 Building Blocks of MAC Mechanisms

Three major blocks of a hybrid MAC mechanism have been as illustrated in Figure 1.4 and the blocks are further detailed below.

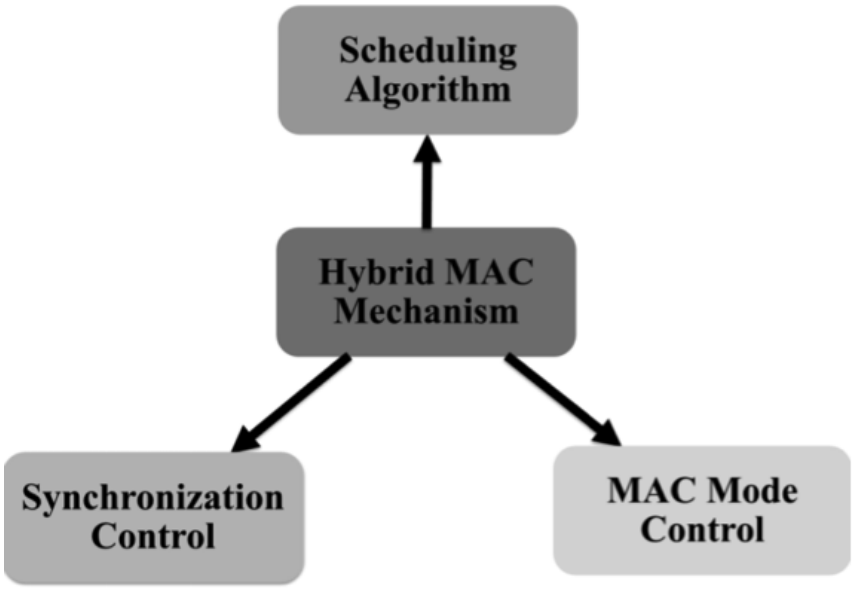


Figure 1.4: Building blocks for a hybrid MAC mechanism.

Scheduling Algorithm: This is a basic block of any hybrid MAC mechanism as scheduling algorithms are required to find conflict-free schedules for nodes to communicate. The algorithm assigns one or

more slot/schedule per frame with the objective to reduce collisions, overhearing, and idle listening, which directly improves the energy efficiency.

Synchronization Control: To provide a common notion of time across the network, synchronization control is an essential component of a hybrid MAC mechanism for an efficient TDMA scheduling algorithm.

MAC Mode Control: Hybrid MAC mechanisms use both schedule- and contention-based mechanisms according to the requirement and conditions and the mode control shifts the network from schedule- to contention-based scheduling and vice-versa. The MAC mode control algorithm continuously monitors the traffic inside the network and decides the mode shift.

Current hybrid MAC mechanisms such as Wireless Sensor MAC (Wise-MAC), ZMAC, Funneling MAC, Centralized Hybrid MAC, HYMAC, CRMAC, EQMAC, Bin-MAC, Queue-MAC, IHMAC, etc. are efficient solutions for WSNs as they save significant amount of energy with good throughput. However, these hybrid MAC mechanisms does still not fulfill the requirements for supporting real-time applications such as tele-health monitoring, intelligent transportation, smart grid [26], industry and building monitoring, etc. To satisfy the requirements of such applications, the following challenges are identified and addressed in the thesis as outlined below (also shown in Figure 1.5).

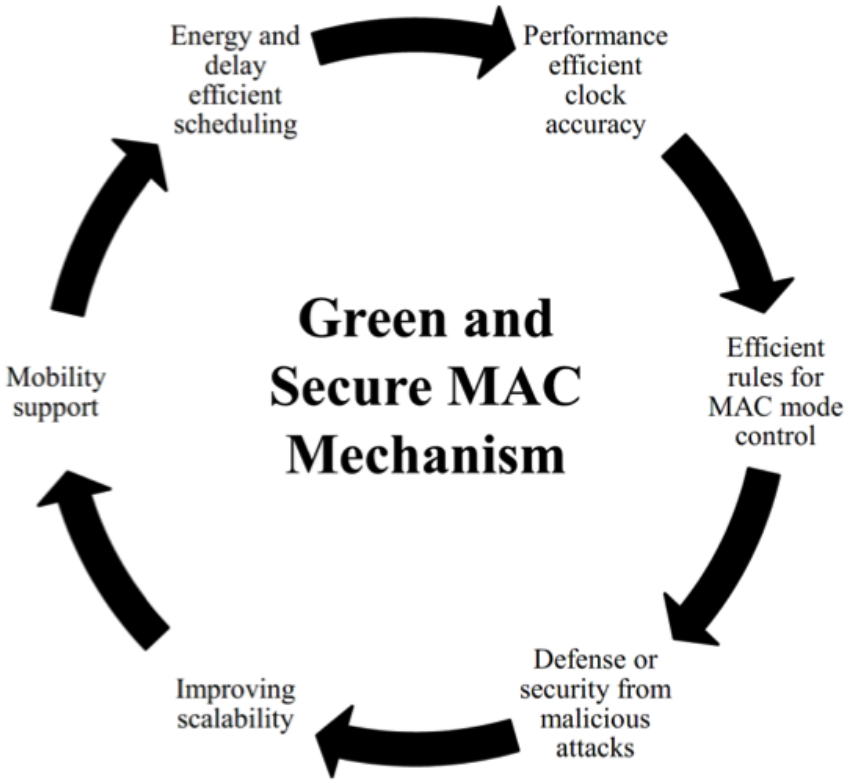


Figure 1.5: Identified and addressed challenges for WSN hybrid MAC.

Energy- and delay-efficient TDMA scheduling: TDMA scheduling algorithms used in hybrid MAC mechanisms introduce a significant amount of processing delay mostly due to neighbor discovery and slot assignment tasks performed by the particular mechanism. These algorithms must be improved to decrease the delay while maintaining energy efficiency.

Performance efficient clock accuracy: The synchronization algorithm used in a hybrid MAC mechanism introduces significant overheads in the maintenance of the global and local synchronization, according to the requirements. A synchronization algorithm is needed that reduces overhead and synchronization errors while being energy and delay efficient also as the size of the network increases.

Efficient rules for MAC mode control: Accurate and early decisions for MAC mode changes lead to performance enhancements for hybrid MAC mechanism and should be designed according to behavior patterns of traffic and collisions in the network.

Security in case of malicious attacks: Security as a requirement is addressed in very few WSN MAC mechanism, but attacks such as collision and denial of sleep attacks can disturb the processing by introducing excessive traffic, which incurs extra overheads. Understanding the attack behavior will be helpful to design secure and energy efficient hybrid MAC mechanisms.

Improving scalability and reducing topology maintenance overheads: Improved scalability and reduced topology maintenance overheads can be achieved by considering cluster-based WSNs, which in turn can improve the scheduling algorithm, the synchronization control and the mode control of the MAC mechanism.

Mobility support: Adding support for mobility can solve various connectivity issues as when a network considered being dense by design turn to being sparse after actual deployment and mobility support can also improve the energy efficiency.

1.4 Research Methodology

1.4.1 Research Hypotheses

Based on the previous overview of WSNs focussing on MAC including the key requirement, the research hypotheses have been identified as developing a green and secure hybrid MAC mechanism for WSN leading to the following research questions addressed in this thesis:

- Hybrid MAC mechanisms are advantageous for resource constrained WSNs.
- Mix-mode scheduling can improve the performance of a hybrid MAC mechanism for WSNs also in the case of mobile scenarios.
- Synchronization is a key criterium for efficient hybrid MAC mechanisms.
- MAC mode changes can improve the performance of the network - especially in the case of mix static and mobile scenarios.
- It is possible to countermeasure MAC security attacks through an efficiently designed hybrid MAC mechanism.

1.4.2 Methodology Overview

The purpose of this research work is to develop a hybrid MAC mechanism, which improves energy efficiency and security performance of WSNs. The principal contributions of the work are the design and

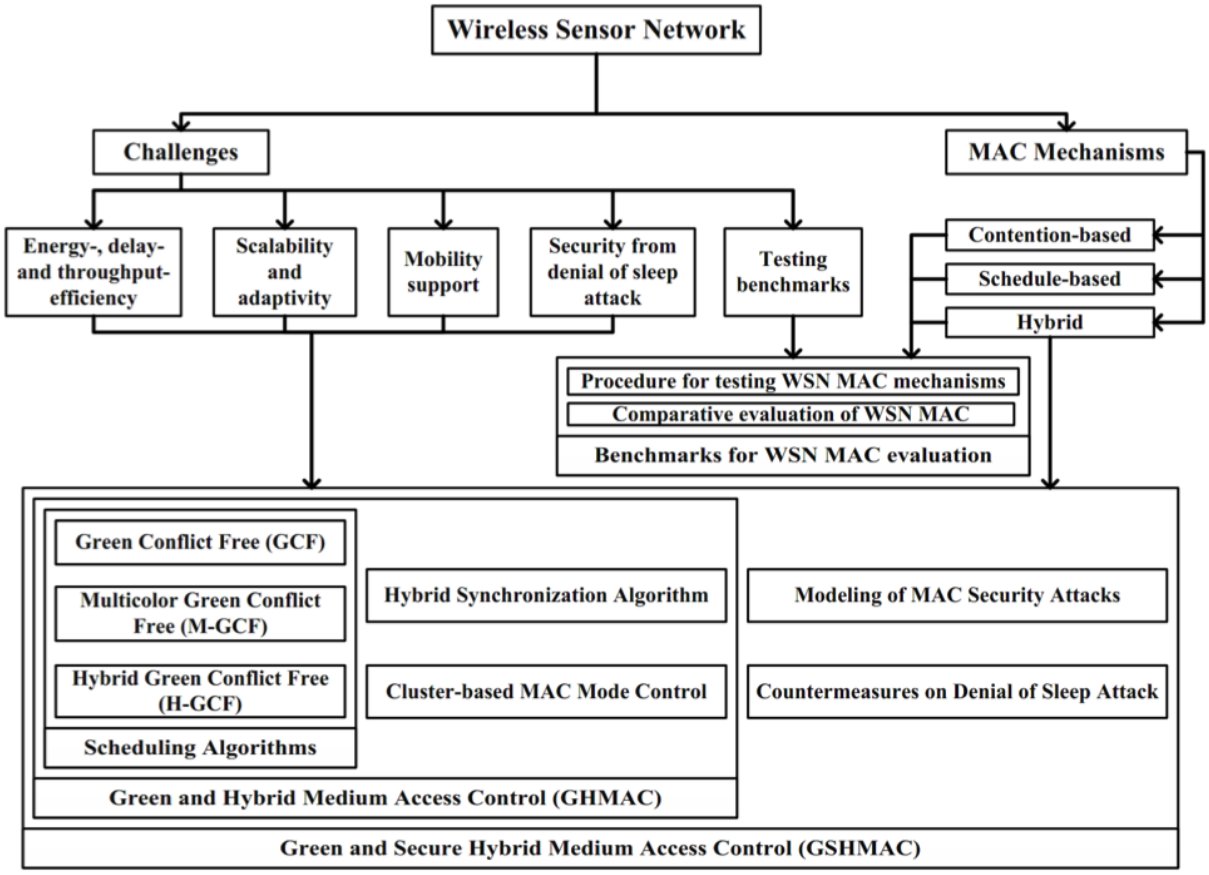


Figure 1.6: Evolution of the problem statement

implementation of Green and Hybrid MAC (GHMAC) and Green and Secure Hybrid MAC (GSHMAC) along with the individual building blocks as outlined above. The work also includes the benchmarking process to test and analyze the effectiveness of the WSN MAC mechanisms.

Selection of proper and proven methodology is a critical step of all research and research in the design of hybrid WSN MAC mechanisms requires thorough knowledge and understanding of the factors that influence the specific kind of network for which the protocol is to be designed. Therefore, the research applies a mixed of qualitative and quantitative research methodology [27].

A thorough study of different types of WSN MAC mechanisms has been done identifying to the techniques used, advantages and disadvantages, metrics used for measurement along with tools and/or test-beds used for simulation or implementation. The study drew the first conclusion that, there is no particular procedure for testing WSN MAC mechanisms in an efficient manner. Hence, the work developed a benchmark procedure for analyzing WSN MAC mechanisms in an efficient and consistent manner. The study gave an understanding of how MAC mechanisms are divided into different categories and a baseline was also established as part of the study with comparative evaluation of three types of state-of-the-art MAC mechanisms using an Network Simulator-2 (NS-2) simulator that confirmed the advantages of hybrid MAC mechanisms for WSNs. The major challenges identified in hybrid MAC mechanisms were energy-, delay-, and throughput-efficiency along with scalability and adaptivity including mobility support and security.

This first step of the detailed analysis of MAC mechanisms has given an understanding that for developing energy efficient and secure hybrid MAC mechanism, it is necessary to have a) a conflict free,

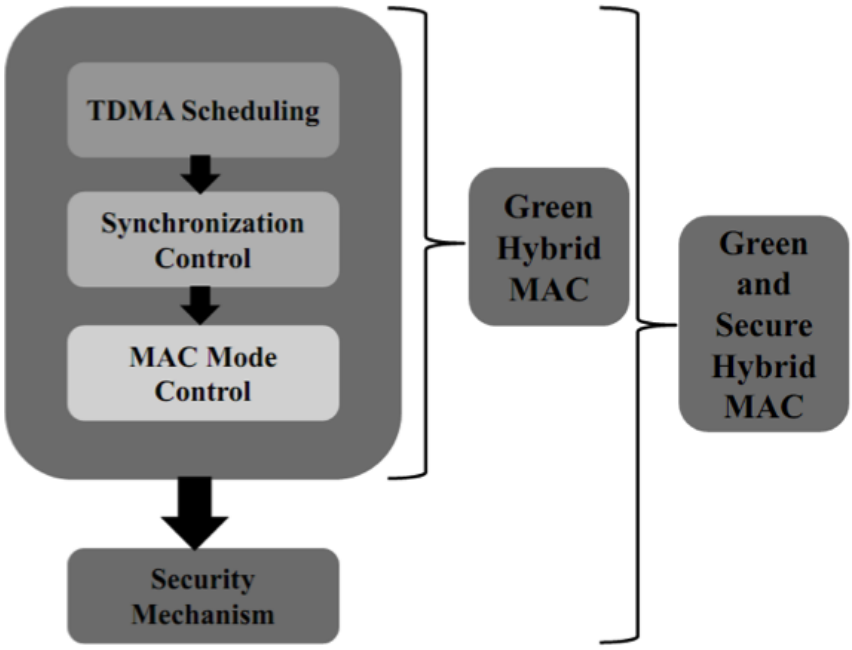


Figure 1.7: Structure of green and secure hybrid MAC mechanism

scalable, and delay efficient scheduling mechanism, b) a synchronization mechanism which reduces errors and time, c) a MAC mode control for mode shift, and d) an internal MAC mechanism to countermeasure security attacks. The work considered these four requirements as the major blocks of research and thorough review of the state-of-the-art was carried out to understand the internal working and limitation of each. Based on this, the framework was developed for designing cluster-based scheduling algorithms for static and mobile scenarios, a hybrid synchronization algorithm, a decision criteria for MAC mode shifting and countermeasure for denial of sleep attacks. Lastly, the blocks were assembled for the development of the GSHMAC mechanism and throughout the work the efficiency of the individual blocks and the designed MAC mechanism was evaluated using Matlab and NS-2 based simulations. The evaluation measured the energy-, delay-, and throughput-efficiency by considering static and mobile scenarios also with respect to security comparing the results with state-of-the-art mechanisms.

The outline of the research methodology is given in Figure 1.6 that shows the steps from challenges for WSNs to the different building blocks considered.

1.5 Contributions

The objective of this thesis is to develop an energy efficient (green) and secure hybrid MAC mechanism for WSNs. The primary factors that influence the performance of a MAC mechanism are the resource constrained nature of WSNs subject to changing conditions of the network, mobility of nodes and different security attacks. The research contributes to improving energy efficiency, throughput, delay, scalability and security performance of the MAC mechanism in case of both S-WSN and M-WSN.

The research contributes with the novel hybrid MAC mechanisms GHMAC [28] and GSHMAC [29] to address the different challenges mentioned in Section 1.2. GHMAC comprises of a scheduling algorithm for finding efficient conflict-free slots under S-WSN and M-WSN, a hybrid synchronization algorithm for synchronizing timeframes among the nodes to communicate and a cluster-based MAC mode control to

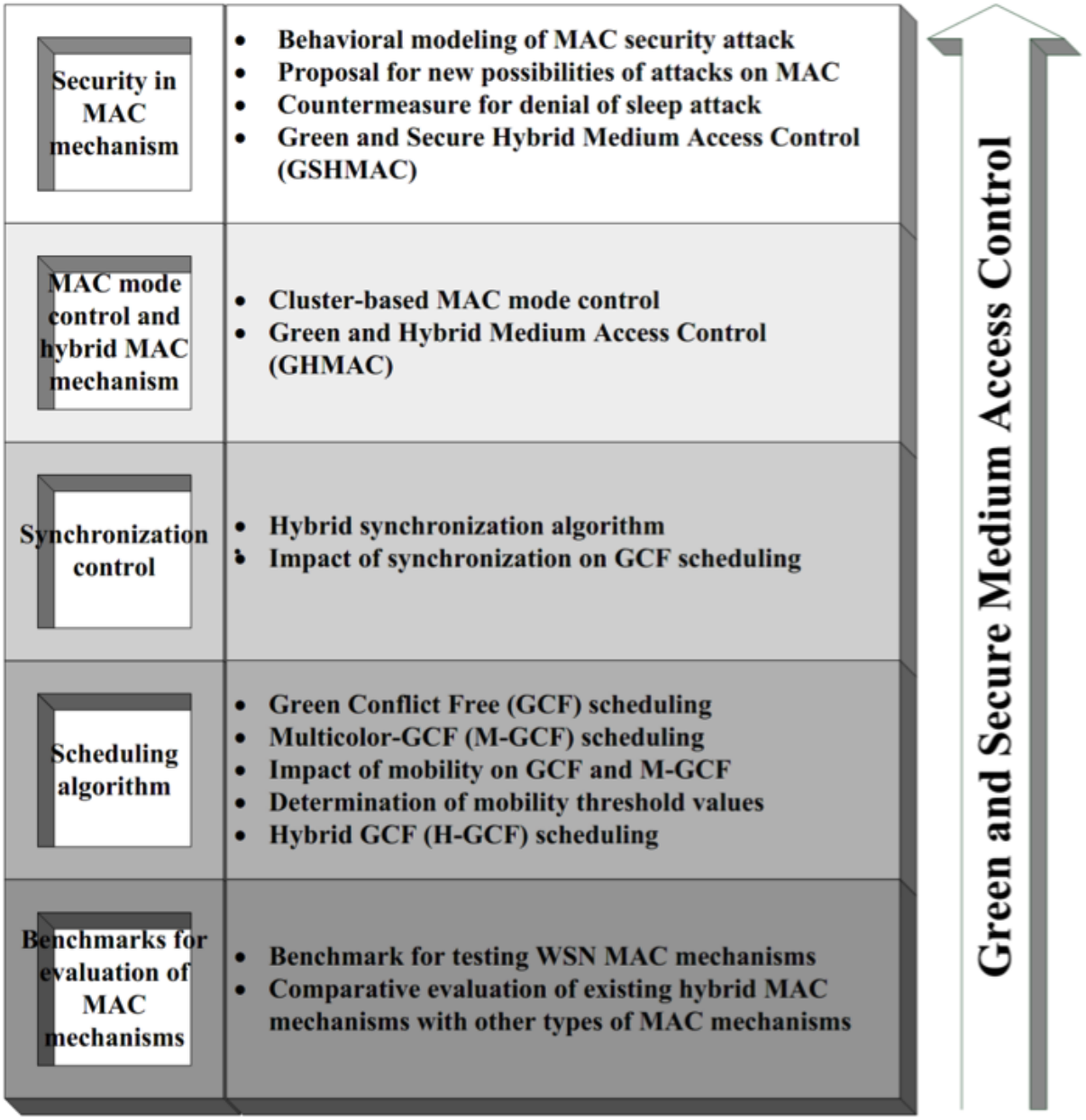


Figure 1.8: Modules of research and contributions

shift the mode from CSMA to TDMA and vice versa according to the requirement of nodes. GHMAC is further extended into GSHMAC by making the addition of security countermeasures against denial of sleep attacks. The contributing building blocks and proposed hybrid MAC mechanisms are outline in Figure 1.7.

The contributions of research are divided into five different modules as shown in Figure 1.8 and described in greater details below.

1. Benchmark for Evaluation

Many different MAC mechanisms have been proposed and evaluated and this research work has surveyed and analyzed the ones proposed in the last few decades. Analyses show that there are major variations in these works in terms of observed parameters and, hence, the research contributed to the analysis of MAC

mechanisms. Simulation and implementation environments have been defined to get consistent results, identifying metrics to be used and verified, scenarios to be tested and validated, and appropriate physical parameters to be used according to a specific transceiver. The contribution also gives the comparative evaluation of state-of-the-art and widely used contention-, schedule-, and hybrid-MAC mechanisms and the results show that hybrid MAC mechanisms can reduce energy consumption and throughput as compared with contention-, and schedule-based MAC mechanisms.

2. Scheduling

The performance of a hybrid MAC mechanism mainly depends upon the scheduling algorithm used. This thesis surveyed different scheduling algorithms available in the literature, and defined a new classification method: single- and multi-coloring scheduling, and flat-network-based- and cluster-based-scheduling. The thesis contributes with three cluster-based scheduling mechanisms, Green Conflict Free (GCF) [30], Multi-color-GCF (M-GCF) [31] and Hybrid-GCF (H-GCF) [32]. Cluster-based scheduling improves the scalability by stabilizing the topology, and it improves the delay by increasing the reuse of slots. GCF is a single-color scheduling algorithm, which finds conflict-free schedules among three-hop neighbors for efficient inter- and intra-cluster communication. M-GCF is multi-color scheduling algorithm, which also finds conflict-free schedules among three-hop neighbor view. GCF and M-GCF both are applied to a conflict-free graph, and they consider multi-hop clusters and both show good energy efficiency, delay, throughput, scalability, and reuse of slots in static WSN scenarios as compared with state-of-the-art algorithms. GCF and M-GCF are further evaluated in mobile scenarios by varying the percentage and speed of mobile nodes for checking their applicability in a M-WSN. The evaluation shows that M-GCF has satisfactory performance under static and low mobility conditions while GCF shows better performance with high mobility conditions [33]. The thesis contributes to the mobility threshold values based on the GCF and M-GCF evaluations and proposes a new hybrid-scheduling algorithm H-GCF. H-GCF works in two modes and shifts the modes according to the mobility threshold value. The H-GCF algorithm shows reduced energy consumption, delay, and increased throughput under both fixed and random mobile conditions. The algorithm is also evaluated for local mode shift for clusters and global mode shift of the network.

3. Synchronization

A hybrid MAC mechanism requires a synchronization algorithm for TDMA scheduling mechanism to allow nodes to communicate in the specified slot or timeframe. To harmonize the overall scheduling of the hybrid MAC mechanisms, this thesis proposes a cluster-based hybrid synchronization algorithm combining the features of two synchronization techniques using strict (tight) sender-receiver synchronization for inter-cluster communication and approximate (loose) diffusion synchronization for intra-cluster communication [34, 35, 33]. The tight synchronization for inter-cluster communication is advantageous for sensitive information but is also resource consuming and sensitive to clock drift compared to loose diffusion synchronization. The hybrid synchronization algorithm [36] shows reduced synchronization errors and energy consumption over varying time and number of nodes, as compared with both sender-receiver and diffusion synchronization algorithms. The research verified the applicability of the hybrid synchronization mechanism with the TDMA scheduling algorithm GCF under static and mobile conditions and shows significant performance improvement in both scenarios.

4. MAC Mode Control and GHMAC

The hybrid MAC mechanism works in two modes, CSMA and TDMA, according to the requirement and shifting between the two is done using the proposed cluster-based MAC mode control mechanism. The developed MAC mode control mechanism supports inter-cluster communication using TDMA and two modes and mode shift for intra-cluster communication. The work assumes that all nodes in the cluster except the CH are initially working in CSMA mode and mode shift from CSMA to TDMA and vice-versa is based on a collision threshold value that triggers a shift as the number of collisions increases thereby improving the energy efficiency. The next part of the research combines the proposed scheduling algorithm, synchronization mechanism, and MAC mode control into a complete hybrid MAC mechanism, GHMAC. The GHMAC mechanism is validated under different collision threshold values for both static-, and mobile-scenarios, and also under the presence of different kinds of denial of sleep attacks. It outperforms state-of-the-art algorithms and shows good performance improvements in energy-efficiency, throughput, delay, and scalability in the presence of mobility and security attacks.

5. Security and GSHMAC

MAC mechanisms play a significant role in the transmission of data, and it is prone to different security attacks including those affecting the resource access mechanism of a WSN and lead to waste of useful resources, which affects the lifetime of the WSN. A major class of attacks on WSN MAC is denial of sleep, which does not allow the WSN node to sleep for saving energy. The first contribution of the thesis in concern with security is behavioral modeling of different denial of sleep attacks, using sequential and activity modeling approaches of the Unified Modeling Language (UML) [37] that are useful tools to understand the list of activities and their sequence in a WSN. The next contribution of the thesis is the evaluation of the hybrid MAC mechanism in the presence of different denial of sleep attacks and shows that the current state-of-the-art mechanisms lack security related to these attacks, while the proposed GHMAC approach shows good performance in the presence of it. The behavioral modeling of the denial of sleep attack and the analysis of hybrid MAC mechanisms in the presence of it motivates the research into definitions of new attacks on the WSN MAC and, hence, the research contributes with two new WSN MAC security attacks; Explicit Contention Notification (ECN) attack and CH attack. Both of these attacks target the decision-making system of a hybrid MAC mechanism, and disturb the overall processing, which leads to degradation of performance. The subsequent contributions of the thesis are on proposals for reducing the effect of the attack on the performance of a WSN leading up to the proposal of GSHMAC, which is a cluster-based secure hybrid MAC mechanism. GSHMAC countermeasures collision-, replay- and full domination attack using internal MAC mechanisms instead of cryptographic mechanisms. GSHMAC shows good energy efficiency, throughput, delay and scalability in the presence of denial of sleep attacks.

1.6 Publications

The contributions have been peer-reviewed and published in journal and conference proceedings or are in the process for being so. The relevant publications are listed below:

A. Journal Publication

1. Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Shingo Ohmori, Ramjee Prasad, "Behavioral Modeling of WSN MAC Layer Security Attacks: A Sequential UML Approach", Journal of Cyber Security and Mobility, River Publishers, Vol. 1, Issue 1, 2012, 65-82.

2. Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Shingo Ohmori, Ramjee Prasad, "Activity Modeling and Comparative Evaluation of WSN MAC Security Attacks", Journal of Cyber Security and Mobility, River Publishers, Vol. 1, Issue 2 & 3, 2012, 205-225.

3. Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Ramjee Prasad, "Mobility Impact on Cluster Based MAC Layer Protocols in Wireless Sensor Networks", Springer Wireless Personal Communication, Special Issue on Wireless Personal Multimedia Communication 2012 (WPMC-2012), Vol. 74, No. 4, 2014, 1213-1229.

4. Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Ramjee Prasad, "GHMAC: Green and Hybrid Medium Access Control for Wireless Sensor Networks" Submitted to Springer Wireless Personal Communication.

B. Conference Publications

B.1 As First Author

1. Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Shingo Ohmori, Ramjee Prasad, "Hybrid Mechanisms: Towards an Efficient Wireless Sensor Network Medium Access Control", 14th International Symposium on Wireless Personal Multimedia Communication (WPMC), Brest, France, October 3-6, 2011, 1-5.

2. Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Shingo Ohmori, Ramjee Prasad, "GCF: Green Conflict Free Scheduling Algorithm for WSN", IEEE - International Conference on Communication - Energy Efficiency in Wireless Networks and Wireless Networks for Energy Efficiency (ICC-E2NETS) Workshop, Ottawa, Canada, June 10-15 2012, 5726 -5730.

3. Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Shingo Ohmori, Ramjee Prasad, "M-GCF: Multicolor Green Conflict Free Scheduling Algorithm for WSN", 15th International Symposium on Wireless Personal Multimedia Communication (WPMC), Taipei, Taiwan, September 24-27 2012, 143 - 147.

4. Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Ramjee Prasad, "H-GCF: Hybrid Green Conflict Free Scheduling Algorithm for Wireless Sensor Network", 16th International Symposium on Wireless Personal Multimedia Communications (WPMC), Atlanta City - NJ USA, June 24-27, 2013, 1-5.

5. Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Ramjee Prasad, "A Hybrid Algorithm for Efficient Wireless Sensor Network Time Synchronization", 4th International Conference Wireless Communication, Vehicular Technology, Information Theory, Aerospace and Electronics Systems Technology, Aalborg, Denmark, May 11-14, 2014, 1-5.

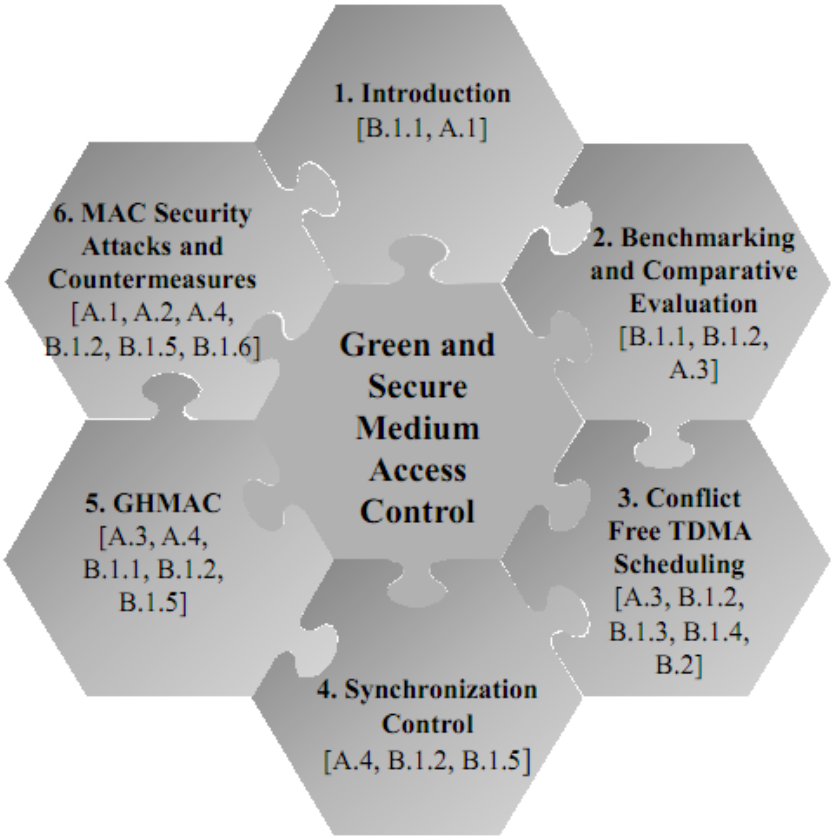


Figure 1.9: Organization of the thesis [19, 24, 25, 28, 29, 30, 31, 32, 36]

6. Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Ramjee Prasad, "GSHMAC: Green and Secure Hybrid Medium Access Control for WSN", International Conference in Wireless Communication, Vehicular Technology, Information Theory, Aerospace and Electronics Systems Technology, Hyderabad, India,December 13-16, 2015, 1-5.

B.2 As Co-Author

1. Dnyaneshwar Mantri, Pranav M Pawar, Neeli R. Prasad, Ramjee Prasad, "Cluster-based Myopic and Non-myopic Scheduling for Wireless Sensor Network", Students' Technology Symposium (TechSym), Kharagpur, India, February 28 - March 2, 2014, 116-120.

2. Dnyaneshwar Mantri, Pranav M Pawar, Neeli R. Prasad, Ramjee Prasad, "An Efficient Schedule based Data Aggregation using Node Mobility for Wireless Sensor Network", 4th International Conference Wireless Communication, Vehicular Technology, Information Theory, Aerospace and Electronics Systems Technology, Aalborg, Denmark, May 11-14, 2014, 1-5.

1.7 Thesis Outline

The thesis is organized into six chapters as shown in Figure 1.9. A brief description of each chapter is given below.

Chapter 2: Benchmarks and Comparative Evaluation of WSN MAC mechanisms

Chapter 2 describes the need for benchmarks and proposes benchmarks for WSN MAC mechanism evaluation by first surveying different WSN MAC layer mechanisms providing a detailed discussion of the individual benchmarks used. An evaluation methodology for benchmarking of WSN-MAC layer mechanisms is given. The next part of Chapter 2 provides a comparative evaluation of a hybrid MAC mechanism with other MAC mechanisms and provides a clear understanding of the different kinds of MAC mechanisms by measuring performance metrics such as energy consumption, delay and throughput with varying traffic interval and area of the network.

Chapter 3: Conflict Free TDMA Scheduling

Chapter 3 discusses the concept of TDMA scheduling and different ways to classify TDMA scheduling algorithms including the related work in TDMA scheduling for flat and clustered networks. The chapter proposes the three novel conflict-free scheduling algorithms; GCF, M-GCF, and H-GCF including the assumptions, system model, notation and problem statement considered in developing the three scheduling algorithms. The algorithms are simulated considering both static and mobile scenarios and the results show that the proposed novel algorithms have enhanced performance as compared with state-of-the-art solutions.

Chapter 4: Synchronization Control

Chapter 4 introduces the concept of synchronization algorithms, its importance in WSN MAC mechanism, classification, and open issues. The chapter gives a proposal for an enhanced cluster-based hybrid synchronization algorithm, which combines the characteristics of two synchronization algorithms for improved performance. Simulation results show that the proposed algorithm leads to reduced overheads, energy consumption and delay and enhances throughput as compared with other synchronization mechanisms.

Chapter 5: GHMAC: Green and Hybrid Medium Access Control

Chapter 5 first discusses the detailed related work in hybrid MAC mechanisms and then proposes the MAC mode control mechanism for a hybrid MAC mechanism to shift the mode. The chapter also discusses the different modules of GHMAC with its features. The simulations and results given in the chapter illustrates the performance measurement of GHMAC by considering varying collision threshold values, static-, and mobile-network scenarios, and the performance in presence of denial of sleep attacks. The results show that GHMAC has reduced energy consumption and delay, and increased throughput as compared to state-of-the-art solutions.

Chapter 6: MAC Security Attacks and Countermeasures

Chapter 6 provides a detailed related work in the security of MAC mechanisms from denial of sleep attacks and presents a detailed discussion of WSN MAC layer security attacks and model these using an UML approach. The chapter illustrates the UML modeling of WSN MAC layer security attack using sequential and activity modeling approach and evaluates WSN MAC layer security attacks in different scenarios. The modeling and evaluation of WSN MAC layer security lead to a proposal for reducing the effects of security attacks. Chapter 6 also introduces new MAC layer attacks and proposes a novel

secure MAC mechanism, GSHMAC, which shows good performance in the presence of WSN MAC layer security attacks.

Chapter 7: Summary and Future Work

The chapter concludes the thesis and provides a summary of the research and recommendations to develop energy efficient and secure MAC mechanism for WSN. The chapter also gives the future work.

1.8 References

[1] Kirk Bloede, Greg Mischou, Amar Senan, and Ryan Koontz. The internet of things, smart products demand a smart strategy using m&a for a competitive edge. Technical report, Woodside Capital Partners, London, March 2015.

[2] Giuseppe Anastasi, Marco Conti, Mario Di Francesco, and Andrea Passarella. Energy conservation in wireless sensor networks: A survey. *Ad Hoc Netw.*, 7(3):537–568, May 2009.

[3] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer Networks*, 52(12):2292 – 2330, 2008.

[4] Shuai Li, Congduc Pham, Arunita Jaekel, Mohammad Abdul Matin, Anang Hudaya Muhamad Amin, and Yangming Li. Perception, reaction, and cognition in wireless sensor networks. *IJDSN*, 2013, 2013.

[5] M.P. Durisic, Z. Tafa, G. Dimic, and V. Milutinovic. A survey of military applications of wireless sensor networks. In *Embedded Computing (MECO), 2012 Mediterranean Conference on*, pages 196–199, June 2012.

[6] Wenjie Chen, Lifeng Chen, Zhanglong Chen, and Shiliang Tu. Wits: A wireless sensor network for intelligent transportation system. In *Computer and Computational Sciences, 2006. IMSCCS '06. First International Multi-Symposiums on*, volume 2, pages 635–641, June 2006.

[7] A. Paventhan, S. Krishna, H. Krishna, R. Kesavan, and N.M. Ram. Wsn monitoring for agriculture: Comparing snmp and emerging coap approaches. In *India Educators' Conference (TIIEC), 2013 Texas Instruments*, pages 353–358, April 2013.

[8] Fadi M. Al-Turjman, Hossam S. Hassanein, and Mohamed A. Ibnkahla. Efficient deployment of wireless sensor networks targeting environment monitoring applications. *Comput. Commun.*, 36(2):135–148, January 2013.

[9] Wen-Dien Chang, Tzu-Shiang Lin, Joe-Air Jiang, Chang-Wang Liu, Chia-Pang Chen, Da-Wei Lai, Hsu-Cheng Lu, Chung-Wei Yen, and Ping-Lang Yen. An implementation of a wsn-based medical monitoring system: A pilot study of the blood pressure monitoring of hemodialysis patients. *Engineering in Agriculture, Environment and Food*, 5(3):83 – 89, 2012.

[10] K. Islam, Weiming Shen, and Xianbin Wang. Wireless sensor network reliability and security in factory automation: A survey. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 42(6):1243–1256, Nov 2012.

[11] T. Torfs, T. Sterken, S. Brebels, J. Santana, R. van den Hoven, V. Spiering, N. Bertsch, D. Trapani, and D. Zonta. Low power wireless sensor network for building monitoring. *Sensors Journal, IEEE*, 13(3):909–915, March 2013.

[12] Ivan Minakov and Roberto Passerone. Pases: An energy-aware design space exploration framework for wireless sensor networks. *J. Syst. Archit.*, 59(8):626–642, September 2013.

[13] F.M. Costa and H Ochiai. Energy-efficient physical layer design for wireless sensor network links. In *Communications (ICC), 2011 IEEE International Conference on*, pages 1–5, June 2011.

[14] A. Bachir, M. Dohler, T. Watteyne, and K.K. Leung. Mac essentials for wireless sensor networks. *Communications Surveys Tutorials, IEEE*, 12(2):222–248, Second 2010.

[15] Pei Huang, Li Xiao, S. Soltani, M.W. Mutka, and Ning Xi. The evolution of mac protocols in wireless sensor networks: A survey. *Communications Surveys Tutorials, IEEE*, 15(1):101–120, First 2013.

[16] N.A. Pantazis, S.A. Nikolidakis, and D.D. Vergados. Energy-efficient routing protocols in wireless sensor networks: A survey. *Communications Surveys Tutorials, IEEE*, 15(2):551–591, Second 2013.

[17] A.J.Dinusha Rathnayaka and Vidyasagar M. Potdar. Wireless sensor network transport protocol: A critical review. *Journal of Network and Computer Applications*, 36(1):134 – 146, 2013.

[18] Ian F. Akyildiz and Mehmet Can Vuran. *Application Layer*, pages 191–219. John Wiley & Sons, Ltd, 2010.

[19] P. Pawar, R. Nielsen, N. Prasad, S. Ohmori, and R. Prasad. Hybrid mechanisms: Towards an efficient wireless sensor network medium access control. In *Wireless Personal Multimedia Communications (WPMC), 2011 14th International Symposium on*, pages 1–5, Oct 2011.

[20] Ameer Ahmed Abbasi and Mohamed Younis. A survey on clustering algorithms for wireless sensor networks. *Computer Communications*, 30(14 - 15):2826 – 2841, 2007. Network Coverage and Routing Schemes for Wireless Sensor Networks.

[21] Qian Dong and W. Dargie. A survey on mobility and mobility-aware mac protocols in wireless sensor networks. *Communications Surveys Tutorials, IEEE*, 15(1):88–100, First 2013.

[22] Xiangqian Chen, Kia Makki, Kang Yen, and N. Pissinou. Sensor network security: a survey. *Communications Surveys Tutorials, IEEE*, 11(2):52–73, Second 2009.

[23] David R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff. Effects of denial-of-sleep attacks on wireless sensor network mac protocols. *Vehicular Technology, IEEE Transactions on*, 58(1):367–380, Jan 2009.

[24] Pranav M. Pawar, Rasmus Hjorth Nielsen, Neeli R. Prasad, Shingo Ohmori, and Ramjee Prasad. Behavioral modeling of wsn mac layer security attacks: A sequential uml approach. *Journal of Cyber Security and Mobility*, 1(1):65–82, 2012.

[25] Pranav M. Pawar, Rasmus Hjorth Nielsen, Neeli R. Prasad, Shingo Ohmori, and Ramjee Prasad. Activity modelling and comparative evaluation of wsn mac security attacks. *Journal of Cyber Security and Mobility*, 1(2):1–20, 2012.

[26] V.C. Gungor, Bin Lu, and G.P. Hancke. Opportunities and challenges of wireless sensor networks in smart grid. *Industrial Electronics, IEEE Transactions on*, 57(10):3557–3564, Oct 2010.

[27] Maura Borrego, Elliot P. Douglas, and Catherine T. Amelink. Quantitative, qualitative, and mixed research methods in engineering education. *Journal of Engineering Education*, 98(1):53–66, 2009.

[28] Pranav M. Pawar, Rasmus Hjorth Nielsen, Neeli R. Prasad, and Ramjee Prasad. GHMAC: Green and Hybrid Medium Access Control for Wireless Sensor Networks (submitted). *Springer Wireless Personal Communication*, 2015.

[29] Pranav M. Pawar, Rasmus Hjorth Nielsen, Neeli R. Prasad, and Ramjee Prasad. Gshmac: Green and secure medium access control for wsn. International Conference in Wireless Communication, Vehicular Technology, Information Theory, Aerospace and Electronics Systems Technology, Hyderabad, India, 2015, 1-5.

[30] P.M. Pawar, R.H. Nielsen, N.R. Prasad, S. Ohmori, and R. Prasad. Gcf: Green conflict free tdma scheduling for wireless sensor network. In *Communications (ICC), 2012 IEEE International Conference on*, pages 5726–5730, June 2012.

[31] P.M. Pawar, R.H. Nielsen, N.R. Prasad, S. Ohmori, and R. Prasad. M-gcf: Multicolor-green conflict free scheduling algorithm for wsn. In *Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on*, pages 143–147, Sept 2012.

[32] P.M. Pawar, R.H. Nielsen, N.R. Prasad, and R. Prasad. H-gcf: A hybrid green conflict free scheduling algorithm for mobile wireless sensor networks. In *Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on*, pages 1–5, June 2013.

[33] Bharath Sundararaman, Ugo Buy, and Ajay D. Kshemkalyani. Clock synchronization for wireless sensor networks: A survey. *Ad Hoc Networks (Elsevier*, 3:281–323, 2005.

[34] Saurabh Ganeriwal, Ram Kumar, and Mani B. Srivastava. Timing-sync protocol for sensor networks. In *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems*, SenSys '03, pages 138–149, New York, NY, USA, 2003. ACM.

[35] Weilian Su and I.F. Akyildiz. Time-diffusion synchronization protocol for wireless sensor networks. *Networking, IEEE/ACM Transactions on*, 13(2):384–397, April 2005.

[36] P.M. Pawar, R.H. Nielsen, N.R. Prasad, and R. Prasad. A hybrid algorithm for efficient wireless sensor network time synchronization. In *Wireless Communications, Vehicular Technology, Information Theory and Aerospace Electronic Systems (VITAE), 2014 4th International Conference on*, pages 1–5, May 2014.

[37] Tom Pender. *UML Bible*. John Wiley & Sons, Inc., New York, NY, USA, 1 edition, 2003.

Chapter 2

Benchmarks and Comparative Evaluation of WSN MAC Mechanisms

This chapter focuses on benchmarks for design and comparative evaluation of Wireless Sensor Network (WSN) Medium Access Control (MAC) mechanisms. In this chapter, the requirements for testing benchmarks for WSN MAC are discussed and new benchmarks proposed. The benchmarks define physical and performance measurements, implementation environments and testing scenarios to be used for efficient testing of WSN MAC mechanisms. The chapter also gives comparative evaluation of hybrid MAC mechanisms with contention- and schedule-based MAC mechanisms. The comparative evaluation gives a better understanding of MAC mechanism performance and is also helpful to understand the requirements to design of new hybrid MAC mechanisms.

2.1 Introduction

Research in WSN has grown enormously in the last few decades and has given a drive to the application of WSNs in many different domains as discussed previously. The research prospect of WSN is spread widely in MAC mechanisms, deployment strategies, routing mechanisms, data aggregation, energy-efficient mechanisms, security, coding techniques, synchronization algorithms, cloud, and many more [1, 2]. New research is verified using a particular evaluation method, and evaluation is further supported by comparison with results from state-of-the-art research. However, there are no specific rules and regulation to test the research in an efficient manner. This chapter presents testing procedures for WSN MAC mechanisms.

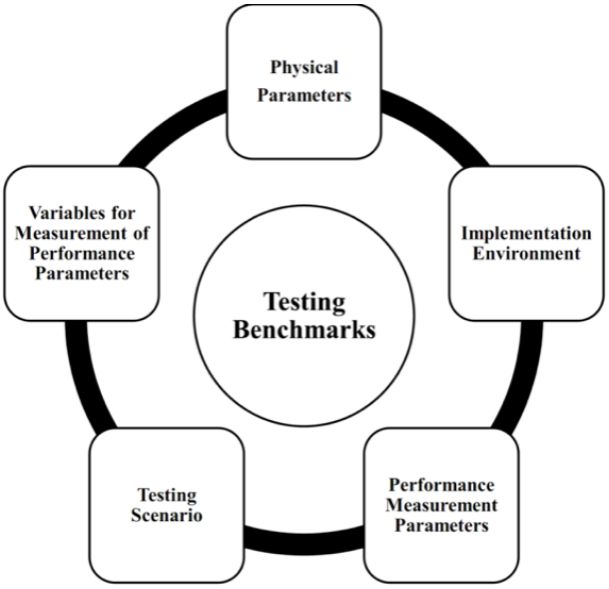


Figure 2.1: Blocks of testing benchmarks.

The research in MAC mechanisms has been of significant impact to the application growth because the MAC layer plays a major role in resource allocation and energy efficiency in WSNs [3]. The development of new MAC mechanisms is currently hindered by the absence of a common benchmarking standard to decide the appropriateness of a particular MAC mechanism [4]. Currently, every researcher has his/her own way of testing and this variation in evaluation criteria leads to challenges in comparison with existing mechanisms and also makes it difficult to check a mechanism's applicability to a standard set of applications. To understand the need for benchmarks, a detailed review of MAC mechanism has been done by considering different parameters such as implementation, measurements, scenarios, comparisons and physical parameters. Currently, most of the MAC mechanisms are implemented using open source tools, which provide a developer with the opportunity to release the code to a large audience of designers who will be able to conduct research using it. This chapter presents the testing procedure for evaluating MAC mechanisms efficiently based on a MAC mechanism survey. The blocks of the testing benchmark procedure are as shown in Figure 2.1. These procedures will make cross-comparison of protocols easier, and will provide proper direction for MAC mechanism testing.

The next part of this chapter shows the comparative evaluation of state-of-the-art and widely used hybrid (contention- and schedule-based) MAC mechanisms. The comparative evaluation is performed to understand the behavior of different MAC mechanisms. Firstly, this analysis is a useful tool for realizing the challenges of hybrid MAC mechanisms. Secondly, it gives valuable guidelines for addressing

the challenges in a better manner. The evaluation is performed using the open source tool Network Simulator-2 (NS-2) [5] and measures the energy consumption, delay and throughput of three different MAC mechanisms by varying packet interval, area of the network and number of nodes. The results show that hybrid MAC mechanisms are energy efficient and scalable solutions, but incur significant delays during processing [6].

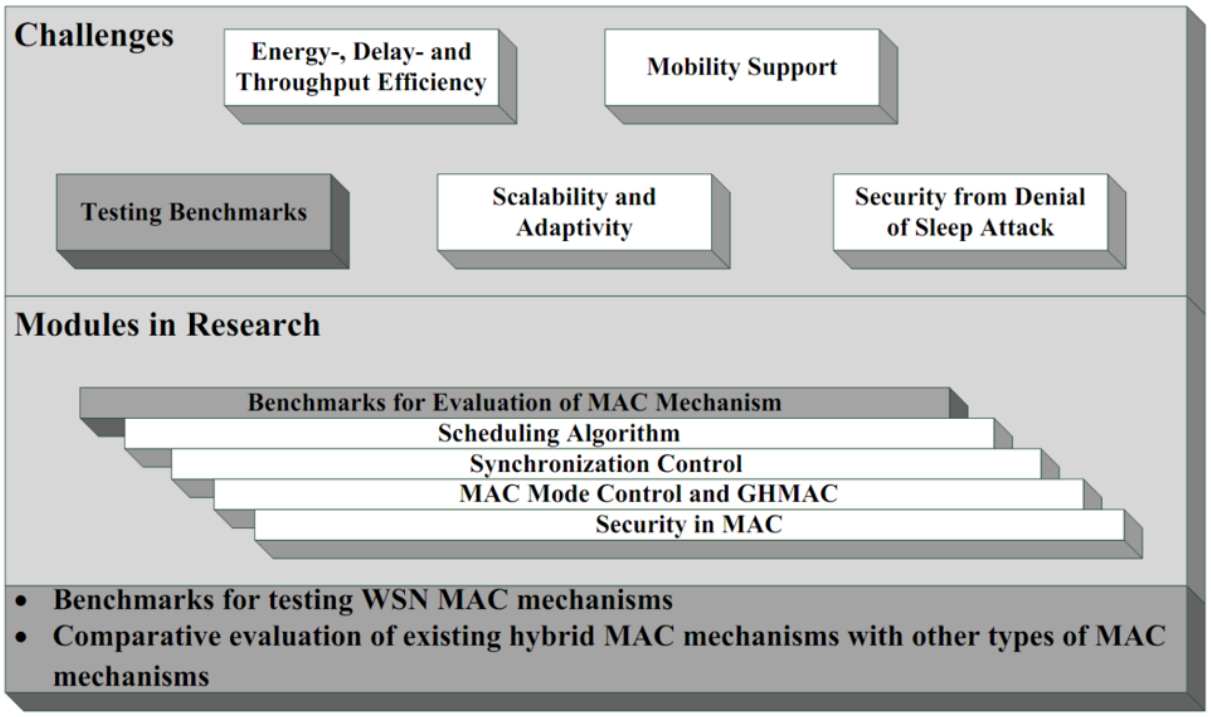


Figure 2.2: Chapter 2 contributions.

Figure 2.2 shows the contribution of this chapter addressing the testing benchmarks challenge of MAC mechanisms and presenting the benchmarks for testing MAC mechanisms efficiently. The other contribution of the chapter is a comparative evaluation of existing state-of-the-art hybrid MAC mechanisms with other types of MAC mechanisms. The remaining four sections are organized as follow: Section 2.2 discusses two topics in the related work, first a benchmarking survey for MAC mechanisms, and then an available implementation environment for MAC mechanisms. Section 2.3 discusses the proposed benchmarking procedure for MAC mechanisms. Section 2.4 focuses on a comparative evaluation of different types of MAC mechanisms and, lastly, Section 2.5 provides a summary.

2.2 Related Work

2.2.1 Benchmarking Survey of WSN MAC Mechanisms

Table 2.1 shows the benchmarking survey of state-of-the-art MAC mechanisms. The survey is performed considering the used implementation environment or tool, measurements performed, scenario, physical parameters and a comparison with existing MAC mechanisms. The benchmarking survey shows that testing is performed considering diverse parameters. The surveyed mechanisms have not used any standardized procedure for uniform testing or performance evaluation and the disparity in the evaluation method makes it difficult to test the comparative performance.

No.	Mechanism	Implementation	Measurements	Scenario(s)	Comparison(s)	Physical Parameters
1	Asynchronous Duty Cycle Adjustment MAC (ADCA) [7]	NS-2	Energy consumption vs. traffic, throughput and delay vs. traffic	One-hop, Multi-hop random	TMAC	Transmission rate = 250kbps, transmission range = 25m, sleep power = 20 mA, receiving power = 4 mA, transmitting power =10mA
2	Adaptive, Information Centric and Lightweight MAC (AI-LMAC) [8]	OMNet++	Average latency vs. number of hops	Multi-hop random	Lightweight MAC (LMAC)	Not specified
3	Adaptive Low-Latency Event-Driven MAC (Alert) [9]	Matlab based simulator	Time required to read messages (Time vs. number of messages)	Multi-hop random topology	Sift, Slotted ALOHA (S-ALOHA)	Transmission rate = 250kbps, transmission range= 75-100m, transmitting power= 17.4mA, receiving power=19.7mA, idle power = 20μA and sleep power = 1μA
4	Boundary MAC (Box-MAC) [10]	Tmote sky mote, CC2420-based platforms under Tiny OS 2.X	Energy consumption vs. receive check interval (in low and high traffic conditions), total transmitters (Channel contention) vs. packet sent/received, maximum throughput for single node to node communication, receive check interval vs. radio on-time per day	Multi-hop random topology	X-MAC, BMAC	Transmission rate = 250kbps, transmission range= 75m, transmitting power= 17.4mA, receiving power=19.7mA, idle power = 20μA and sleep power = 1μA
5	Correlation Based Cooperative MAC (CC-MAC) [11]	NS-2	Average energy consumption vs. reporting period, distortion vs. reporting period, medium Access delay vs. reporting period, good-put vs. reporting period, packet drop rate vs. reporting period	Multi-hop random deployment with single sink and multiple sources	Timeout-MAC (TMAC), Sensor-MAC (SMAC), Traffic Adaptive Medium Access Protocol (TRAMA), IEEE 802.11	Transmission range =100m, transmission rate = 250kbps, transmitting power = 24.75 mW, receiving power = 13.5 mW and sleep power = 15mW
6	Classifier-MAC (C-MAC) [12]	Tiny Operating System (OS), NS-2	Data rate vs. throughput, data rate vs. latency, data rate vs. normalized energy consumption, event moving speed vs. throughput, event moving speed vs. latency, event moving speed vs. normalized energy consumption, latency/hop vs. transmission range, hop count ratio vs. transmission range, initial duty cycle vs. throughput, initial duty cycle vs. latency, initial duty cycle vs. normal energy consumption, throughput vs. number of nodes (density), latency vs. number of nodes (density), normalized energy vs. number of nodes	Multi-hop random topology	SMAC, BMAC, Geographic Random Forwarding (GeRaF)	Transmission range = 250m, transmission rate= 250kbps, transmitting power= 27mA, receiving power=10mA, idle power=10mA
7	Converge-cast MAC [13]	OPNET	Throughput vs. traffic load per sources, throughput vs. traffic load per sources, throughput vs. density, delay vs. density, fairness vs. offered load, measurements with varying number of channels	Grid with sink at the center, random circular topologies	CMAC, 802.11	Transmission range = 250m, transmission rate= 250kbps, transmitting power= 27mA, receiving power=10mA, idle power=10mA
8	Cooperative Medium Access Control with Minimal Control Messages (COSMIC) [14]	OPNET	Delivery ratio vs. number of nodes, network lifetime vs. number of nodes, outage ratio vs. number of nodes	Uniform random	CSMA/CA	Radio range = 30m, transmission rate= 250kbps, transmitting power= 27mA, receiving power=10mA, idle power=20μA
9	Differentiated Services MAC (Diff-MAC) [15]	OPNET	Latency vs. traffic load, average traffic received at sink vs. traffic load, traffic load vs. energy consumption, number of hops vs. latency, number of hops vs. packet delivery ratio	Uniform random, mobility mode: random waypoint	SMAC, Saxena MAC	Transmission range= 80m, transmission rate = 250kbps, transmitting power= 24.75mA, receiving power =13.5mA, idle power=15mA

10	Data Gathering MAC (DMAC) [16]	NS-2	Energy vs. number of hops, delay vs. number of hops, interval vs. delay, interval vs. energy, interval vs. delivery ratio, delay vs. number of sources, energy vs. number of sources, delivery ratio vs. number of sources	Multi-hop chain, multi-hop random	SMAC	Transmission range= 250m, transmission rate = 100kbps, transmitting power= 0.66mA, receiving power =0.395mA, idle power=0.35mA
11	Dynamic Sensor MAC (DSMAC) [17]	NS-2	Average packet latency vs. interval, power consumption vs. interval, average power consumption/packet vs. interval	One-hop, multi-hop chain	SMAC	Transmission range= 80m, transmission rate = 20kbps, transmitting power= 24.75mA, receiving power =13.5mA, idle power=15mA
12	Demand Wakeup MAC (DWMAC) [18]	NS-2	Sensing range vs. average and maximum end-to-end delay, sensing range vs. delivery ratio, sensing range vs. average energy consumption, end-to-end delay vs. number of nodes along the edge of the grid, delivery ratio vs. number of nodes along the edge of the grid, average energy consumption vs. number of nodes along the edge of the grid	Multi-hop grid, multi-hop random	SMAC, Randomized MAC (RMAC)	Transmission rate =20kbps, transmitting power =31.2mW, receiving power =22.2mW, idle power=22.2mW, sleep power=3μW, transmission range =250m
13	Energy-Efficient Reliable MAC (E2RMAC) [19]	PARSEC	Number of hops vs. packet delivery ratio, number of hops vs. latency per hop,number of hops vs. energy consumption, arrival rate vs. packet delivery ratio, arrival rate (packets/sec/node) vs. latency per hop, route energy consumption vs. arrival rate	Multi-hop chain	Sparse Topology and Energy Management (STEM), SMAC, Institute of Electrical and Electronics Engineers (IEEE) 802.11, RMAC, CSMA	Transmission rate =250kbps, transmitting power =35mW, receiving power =41mW, idle power=22.2mW, sleep power=0.015mW, transmission range = 250m
14	Event Based MAC (EBMAC) [20]	Tiny OS	Time vs. power consumed, throughput vs. number of nodes, latency vs. number of nodes	Multi-hop chain	BMAC	Transmission rate = 250kbps, transmitting power =17mA, receiving power = 23 mA, idle power =1mA, sleep power=1mA, transmission range = 250m
15	Enhanced Lightweight MAC (eL-MAC) [21]	Tiny OS	Throughput vs. number of contended node, packet generation per minute vs. packet received ratio, packet generation per minute vs. average power consumed per node, packet generation per minute vs. average energy consumption per bit received	One-hop topology, multi-hop grid	LMAC	Transmission rate = 19.2kbps, transmitting power = 24.75mW, receiving power = 13.5mW, sleep power =15mW, transmission range = 250m
16	Energy efficient Quality MAC (EQ-MAC) [22]	OMNet++	Load (bytes/node/second) vs. average energy consumed, mean inter-arrival time vs. average delay	Multi-hop grid (sink at the bottom corner)	SMAC, Query MAC (QMAC)	Transmission rate = 20 kbps, transmitting power = 13.5mW,receiving power = 24.75mW, sleep power =15mW, transmission range = 250m
17	Emergency Response MAC (ERMAC) [23]	NS-2	Load vs. energy consumption, load vs. delivery ratio, hop count from the base station vs. completeness, load vs. delivery ratio, time vs. energy consumption, load vs. average per packet latency, time vs. delivery ratio, average per packet latency vs. time	Multi-hop grid	ZMAC	Transmission rate = 19.2kbps, transmitting power = 52.2mW, receiving power = 59.1 mW, sleep power = 59.1 mW, transmission range = 10m
18	Latency and Energy Aware MAC (LE-MAC) [24]	NS-2	Network size vs. end-to-end delay, network size vs. total energy consumption, duty cycle vs. end-to-end latency, duty cycle vs. total energy consumption, number of traffic sessions vs. end-to-end latency and total energy consumption	Multi-hop grid	SMAC	Transmission rate = 19.2kbps, transmitting power =13.5mW, receiving power = 24.75mW, sleep power = 15mW, transmission range =55m
19	Multi-channel MAC (MC-LMAC) [25]	Glomosim	Number of channels vs. throughput, delivery rate vs. number of channels, latency vs. number of channels, energy efficiency vs. number of channels, number of source nodes vs. aggregate throughput, density vs. aggregate throughput, density vs. delivery ratio, aggregate throughput vs. number of sink nodes	Multi-hop random, single sink and multi sink topologies	MMSN, CSMA	Transmission rate = 250kbps, transmission range = 40m

20	Multi-layer MAC (ML-MAC) [26]	Matlab	Energy consumption, delay, throughput vs. inter-arrival time	Multi-hop random	SMAC	Transmission rate = 19.2kbps, transmitting power = 13.5mW, receiving power = 24.75mW, sleep power = 15mW, transmission range =55m
21	Multi-frequency MAC (MMSN) [27]	Glomosim	Packet delivery ratio, aggregate MAC throughput, channel access delay, and energy consumption per byte vs. channel frequency, delivery ratio, aggregate throughput and channel access delay vs. node density, CBR streams vs. aggregate throughput and channel access delay	Multi-hop uniform random	CSMA	Transmission rate = 250kbps, transmission range = 40m
22	Reinforcement Learning MAC (RL-MAC) [28]	NS-2	Message inter-arrival time vs. % of active time, latency, data throughput, energy efficiency	One-hop, multi-hop chain, multi-hop grid	SMAC, TMAC	Transmission rate = 20 kbps, transmitting power = 13.5mW, receiving power = 24.75mW, sleep power = 15mW, transmission range = 250m
23	Berkeley MAC (BMAC) [29]	Tiny OS	Number of nodes vs. throughput, throughput vs. power consumed, fragment size vs. energy per byte, number of hops vs. latency, energy vs. latency, number of hops vs. duty cycle	One-hop, multi-hop chain, multi-hop random	SMAC, TMAC	Transmission rate = 20 kbps, transmitting power = 13.5mW, receiving power = 24.75mW, sleep power = 15mW, transmission range = 250m
24	SMAC [30]	NS-2, Tiny OS	Energy consumption vs. message inter-arrival time, latency vs. number of hops, throughput vs. number of hops, throughput vs. inter-arrival period, energy-time cost per byte vs. message inter-arrival period	One-hop, two-hop, multi-hop chain	IEEE 802.11	Transmission rate = 20 kbps, transmitting power = 13.5mW, receiving power = 24.75mW, sleep power =15mW, transmission range = 250m
25	Tree-based Multichannel Protocol (TMCP) [31]	Glomosim	Number of neighbors vs. throughput, number of neighbors vs. delivery ratio, number of neighbors vs. latency, number of channels, delivery ratio, latency vs. throughput, number of sources vs. delivery ratio, packet/second vs. delivery ratio	Multi-hop random	MMSN	Transmission rate =19.2kbps, transmitting power = 52.2mW, receiving power = 59.1mW, sleep power = 59.1mW, transmission range = 10m
26	Zebra MAC (ZMAC) [32]	NS-2, Tiny OS	Number of sources vs. throughput, number of sources vs. throughput, packet per second vs. average throughput, packet per second vs. fairness, packet per second vs. throughput / energy, average per node throughput vs. power consumption, packet per second vs. average number of transmission per second	One-hop, two-hop, multi-hop random	BMAC,SMAC, Sift	Transmission rate = 19.2kbps, transmitting power = 52.2mW, receiving power = 59.1mW, sleep power = 59.1mW, transmission range = 250m
27	Funneling MAC [33]	Tiny OS	Beacon transmission power vs. throughput, data rate vs. throughput, number of hops vs. loss rate, running time vs. throughput, number of sources vs. throughput, energy tax vs. number of sources, energy tax vs. data rate	Multi-hop grid	ZMAC, BMAC	Transmission rate = 19.2kbps, transmitting power = 52.2mW, receiving power = 59.1mW, sleep power = 59.1mW, transmission range =250m
28	TMAC [34]	OMNet++	Load (byte/node/s) vs. energy used, average energy consumption vs. load	Multi-hop grid, one-hop	SMAC, CSMA	Transmission rate = 20 kbps, transmitting power = 10mA, receiving power = 4mA, sleep power = 20 mA, transmission range = 250m

Table 2.1: Benchmarking survey of MAC mechanisms

2.2.2 Available Implementation Environments

WSNs are still an active area of research, and new protocols and components are being proposed and tested. Table 2.2 lists different implementation environments. A large numbers of the implementation environments are open source projects that have become widely used simulation platforms as they can be used and extended without concern of licensing expenses. Another added advantage is that an open source protocol developed by researchers can be added back into the simulation projects and evaluated by other researchers. The open source tools are useful for researchers who want to compare their protocol with other protocols or test cross-layer interactions.

No.	Implementation Environment(s)	License	Programming Language	WSN Support
1	NS-2 [5]	General public license	C++, Object Tool Command Language (OTCL)	Large amount of protocols available contributed by NS-2 users, complex configuration
2	QualNet [35]	Free for academic research/ commercial	C and Parsec	Basic mobility and radio propagation models, 802.11, possible to add additional battery and energy model, more updated but commercial
3	OPNET Modeler Wireless Suite [36]	Commercial	Configuration by Graphical User Interface (GUI) and implementation by C++	Different propagation models, 802.11, ZigBee, some Mobile Ad-Hoc Network (MANET) protocols, commercial and expensive
4	Tiny OS Test bed [37]	Berkeley software distribution	Nested C (nesC)	Supports large number of protocols. Give more clear results.
5	OMNet++ [38]	Academic public license	Network Description (NED), C++	MiXiM, Castalia for WSN support, active project with a massive user base, eclipse-based Integrated Development Environment (IDE) for development
6	Avrora [39]	Berkeley software distribution	Automatic Voltage Regulator (AVR) micro controller Binaries	Particularly for programs which are written for AVR micro controller with support for Mica2 and MicaZ, not fully mature.
7	Java Simulator (J-Sim) [40]	Berkeley software distribution	Java, Tool Command Language (TCL)	Includes sensor network packages, containing models such as propagation, battery, radio model and sensor protocol stack.
8	ATEMU [41]	Berkeley software distribution	AVR micro controller Binaries	Complete emulation of the AVR instruction set with partial Mica2 support, TinyOS based code can be run, slow simulation speed, not fully mature
9	SENSE [42]	Berkeley software distribution	C++	Includes battery and power models, MAC layers, as well as network protocols, not much development happen using it.
10	Shawn [43]	Berkeley software distribution	C++	Not much WSN support, currently working on active WSN support.

Table 2.2: Different implementation environments for WSNs

2.3 Proposed Benchmarks for MAC Mechanism Testing

2.3.1 Physical Parameters

The physical layer plays an important role in determining the performance of a particular MAC mechanism. For doing the implementation of a MAC mechanisms, researchers need to consider three important parameters of the physical layer; transmission rate, transmission range, and energy model. Changes in these parameters affect the performance of the MAC layer. The survey of MAC mechanisms in Table 2.1 shows the disparity in use of the physical layer parameters in different MAC mechanisms. These disparities make comparison and evaluation difficult. Another more observed disparity is a discrepancy between the parameters that the manufacturer estimates and the parameters that are used in implementation and analysis.

Variations in the bandwidth considered at the physical layer have drastic effects on the observed performance of the upper layer protocols. It is possible to mask the latency a MAC mechanism introduces to a network by increasing the physical layer bandwidth. The survey shows that there are vast discrepancies in the bandwidth used in the evaluation.

Another physical layer parameter that effects the evaluation is the power profile of the physical layer. The power profile consists of transmit, receive, sleep, and idle powers. Tuning the simulated power profile can dramatically change the results and changing the radio between sleep, receive, transmit, and idle powers affects the observed energy efficiency.

The most important recommendation to make for physical parameters is the use of accurate parameters for the chosen physical layer model. Presently, the commonly used radio transceivers in WSN experimentation are CC1000, CC1010, TR3000, TR1000, and CC2420. However, as the physical layer technology continues to progress and evolve at a fast rate, these are likely to be superseded. Therefore, so as not to bias the benchmark towards one particular chip or chip manufacturer, it is necessary to use accurate

physical layer parameters. The most commonly used sensor motes for implementation are Atemel, Imote 2, BTnode, Iris Mote, Mica 2, Micaz, TelosB, T-mote Sky, and, Sun Spot.

2.3.2 Performance Measurement Parameters

The performance of MAC mechanisms should be measured by considering the parameters described below.

Energy consumption: Energy consumption of a WSN is a critical parameter for measuring its performance and is considered a key measurement parameter for analyzing the efficiency. The lifetime of a WSN depends on the energy of the sensor nodes. The energy consumption of a WSN node is defined as the amount of energy required for performing one particular activity. The most common activities performed by WSN nodes are transmission, receiving, sleep, idle, sensing and processing.

Delay: The delay in a WSN is defined as the time required for a packet to reach its destination by traversing a number of hops. Many different factors affect the total end-to-end delay, such as sleep time, queuing time, and distance between the nodes (number of hops).

Throughput: Throughput is an important performance parameter to measure the utilization of the channel. It is the amount of data transmitted from the sender towards the receiver at a given time. Many implementations measure the throughput in terms of packet delivery ratio. The packet delivery ratio is the ratio of packets received at the receiver and the packets sent by the sender in a given period of time. Throughput is affected by control overheads, collisions, and delay in the channel.

Fairness: This is the ability of different nodes or users to share the channel equally. In the case of MAC mechanisms, fairness means that one node is not preferred over others when multiple nodes are trying to access the channel.

Scalability: Scalability points towards the adaptivity of the MAC mechanism in changing number nodes, area of network, and topology. Scalability is the ability to perform well with increasing number of nodes and traffic. A MAC mechanism should be scalable and adaptive to such situations.

Mobility Support: Currently, most MAC mechanisms do not consider mobility support as an important metric. However, it is necessary to consider it, as WSNs are moving towards mobile WSNs. Mobility support can be evaluated by changing the mobility models, varying the percentage of mobility, and velocity of nodes.

Security: Security performance is an important parameter as the number of security attacks are increasing on WSNs, and can degrade the performance of a WSN. Therefore, all the above-mentioned parameters should be measured by considering security as an essential part.

2.3.3 Implementation Environment

Table 2.2 shows the different implementation environments used in MAC mechanism simulations. Two good available options for implementation are NS-2 and the Tiny OS based test bed. NS-2 is an open source tool, and it has a wide library to support WSNs. It allows the developer to independently examine

other developer's code and determine the cross-layer performance. Another option for implementation is to develop a new simulator for the proposed and validate it according to the given benchmark.

2.3.4 Testing Scenario

Testing scenarios describe the deployment strategies used for the arrangement of nodes i.e. topology and connection pattern used in the network. The topology of the network is an important factor to consider for implementation because the performance of the network can vary according to topology changes. Most of the surveyed MAC mechanisms have analyzed the performance of a multi-hop random topology. However, to understand the overall behavior of the MAC mechanism, it is necessary to test the MAC mechanism in the below mentioned scenarios.

One-hop: The scenario to be considered for one-hop includes Multiple Sources, Single Sink (MSSS). In this scenario, nodes are placed equidistant from the sink and the sink is placed at the center and all other nodes, i.e. sources are placed around the sink node at one-hop distance. The scenario is useful to check the performance of the protocol for local communication in the absence of routing.

Multi-hop Chain: This scenario is considered as a Single Source, Single Sink (SSSS) scenario. Nodes are placed in a chain in such a way that each node is within broadcast radius of the neighboring node. The first node in the chain is the source node, the last node is the sink, and all in between nodes are doing the work of packet forwarding i.e. act as hops. This multi-hop scenario is useful to exploit the effect of hidden terminals and also to determine the expected upper-level performance from a particular path.

Multi-hop Grid: The grid scenario represents the most complex scenario with multiple chains and this scenario is used to check the performance of the protocol with interfering traffic flows. In a grid, nodes are equidistant from each other in the horizontal and vertical plane.

Multi-hop Random: Multi-hop random scenarios are widely used for testing the performance of MAC mechanisms and provide the most realistic behavior of a WSN. The randomness in the network introduces more inconsistencies and makes the behavior more realistic with increasing traffic, increasing collisions, interference, and synchronization errors, which degrade the performance of the protocol. The work discussed in this thesis considers the multi-hop random scenario.

Mobility: Mobility scenarios are useful in case of a Mobile-WSN (M-WSN). In this case, the nodes are mobile according to a particular mobility model. The work presented in this thesis considers mobility scenarios by using the random waypoint mobility model. Different mobility models include [44],

- Random Waypoint Model
- Manhattan Grid Model
- Gauss-Markov Model
- Reference Point Group Mobility Model
- Disaster Area Model
- Random Street

- Random Direction Model, etc.

Security: Security is a primary concern in WSNs and, therefore, it is necessary to check the behavior of the protocol in the presence of security attacks. The ideal protocol should work even in the presence of an attack and be able to mitigate the attack. A security attack can introduce a significant amount of power consumption and delays and can reduce the utilization of the channel.

2.3.5 Variables for Measuring Performance

The different variables used for measuring the performance of new WSN MAC mechanism are as follows,

Number of nodes: As the number of nodes is increasing so does the numbers of contenders to access the channel. This increase causes more interference, which results in a reduction of throughput of the network. An ideal mechanism should show constant throughput with increasing number of nodes.

Traffic rate: This variable is useful to show the behavior of a MAC mechanism with varying traffic rate. Most of the experimentation of MAC mechanism is done by varying the rate of traffic. An increasing traffic rate results in the production of more packets per node that increases the load on the channel, which results in network congestion. The increased congestion reduces throughput, which directly affects the fairness of the protocol and induces more delay because of the overload on to the channel.

Area of network: This variable is useful to check the scalability of the protocol with varying area of the network and distance between nodes. The variation in area shows the variation in energy consumption, throughput, and delay of the protocol as increasing distances increase the bit error rate (with fixed number of nodes).

Number of channels: This variable is useful for multi-channel MAC mechanisms as with number of channels increasing so do the interference and number of synchronization errors. The increment in interference leads to more collisions, which reduces the total throughput of the channels and the synchronization errors affect the delay and energy consumption of the system.

Mobility models: Mobility of the nodes affects the throughput of the network because the bandwidth reservation made or the control information exchanged may not be utilized if the node mobility is very high. Measurements with varying mobility models can show the applicability of mobility model to a particular protocol. Not all mobility models are working efficiently in all cases.

Number of malicious nodes: An increase in the number of malicious nodes leads to fast penetration of attacks inside the network and the higher amount of maliciousness disturbs the normal functioning of the network. In case of a denial of sleep attack, the higher the number of nodes denied to sleep, the more the energy consumption and the less network lifetime.

2.4 Comparative Evaluation of Hybrid MAC Mechanisms

2.4.1 Simulation Details

To evaluate the performance of contention, schedule and hybrid MAC mechanisms, a multi-hop random topology is considered to show how the network is expected to behave in realistic scenarios. Varying

traffic interval, area of the network and number of nodes are used for measuring the energy consumption, delay and throughput. The mechanisms used for simulation are SMAC (contention-based), DMAC (schedule-based) and ZMAC (hybrid). All simulations are performed using the discrete event simulator NS-2. The parameters used in the simulations are as shown in Table 2.3.

Table 2.3: Simulation parameters for MAC mechanism simulation.

Parameters	**Setting used**
Wireless Physical	
Network interface type	Wireless Physical
Radio propagation model	Two-Ray Ground
Antenna type	Omni-directional Antenna
Channel type	Wireless Channel
Link Layer	
Interface queue	Priority Queue
Buffer size of IFq	50
MAC	SMAC, DMAC and ZMAC
Routing protocol	Ad-hoc Routing
Transport layer protocol	User Datagram Protocol (UDP)
Traffic model	Constant Bit Rate (CBR)
Energy Model	
Initial energy (Joule)	100
Idle power (mW)	14.4
Receiving power (mW)	14.4
Transmission power (mW)	36.0
Sleep power (μW)	15.0
Node Placement and Other Parameters	
Number of nodes	50
Number of sources	49
Number of BS	1
Node placement	Random
Placement of nodes and Base Station (BS)	Nodes are placed randomly in a given area, and the BS is placed at the center of the area.
Number of simulation runs	50
Number of packets transmitted by each source node	100

2.4.2 Simulation Results and Analysis

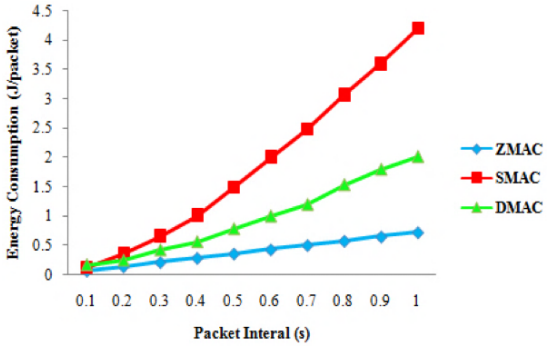
The comparative energy consumption of the three different MAC mechanisms is as shown in Figure 2.3a and 2.3b. The energy consumption is calculated by using the following formula,

$$E_{total} = \sum_{k=o}^{n} E_{ik} - E_{fk} \tag{2.1}$$

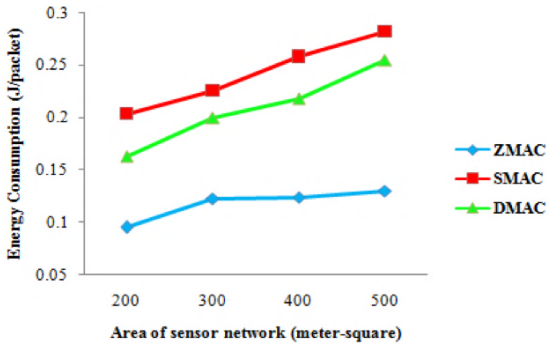
where E_{total} is the total energy consumption of all nodes, E_{ik} is the initial energy of node k and E_{fk} is the final energy of node k. The average energy consumption is calculated over number of packets.

Figure 2.3a shows the measurement of energy consumption with varying packet intervals and it is observed that the hybrid MAC mechanism outperforms both the contention- and the schedule-based MAC mechanism. Hybrid MAC mechanisms adapt better to increases in traffic, resulting in less energy consumed compared to the other two MAC mechanisms. Higher energy efficiency under high traffic rates is the main feature of the hybrid MAC mechanism.

Figure 2.3b shows the energy consumption as a function of the area of the WSN, which is varied from 200m^2 to 500m^2, and as the area of the WSN increases, the nodes move further away from each other. In addition, here, the hybrid MAC mechanism shows better energy consumption in scenarios with both high and low density of nodes. The results point to the scalability of hybrid MAC mechanisms in varying density of nodes.

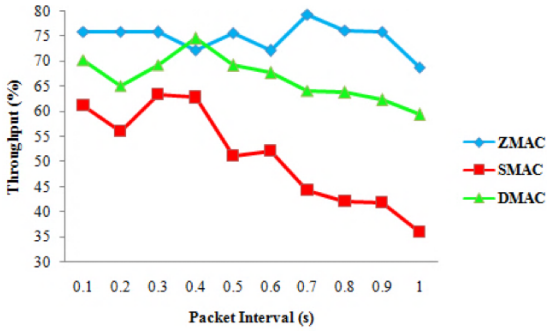


(a) As a function of packet interval.

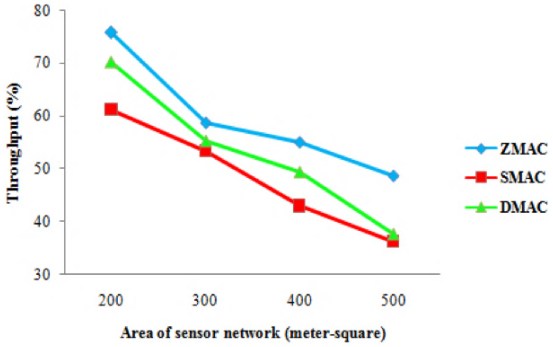


(b) As a function of the area of the sensor network.

Figure 2.3: Energy consumption.



(a) As a function of packet interval.



(b) As a function of the area of the sensor network.

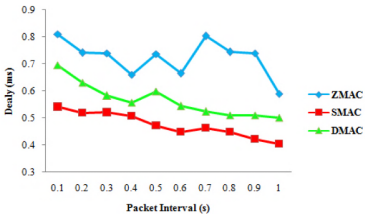
Figure 2.4: Throughput.

Figure 2.4a and Figure 2.4b show the throughput of the three MAC mechanisms by varying packet interval and area of the network, respectively. Again, the hybrid MAC mechanism outperforms the two other MAC mechanisms because of its adaptability to traffic conditions. Figure 2.4b shows the measurement of throughput by varying the network area, and it is observed that the throughput of all three MAC mechanisms is going down with increases in the area and distance between nodes. As the distance between two nodes increases, so does the bit error rate, which results in an increased number of dropped packets reducing the overall throughput.

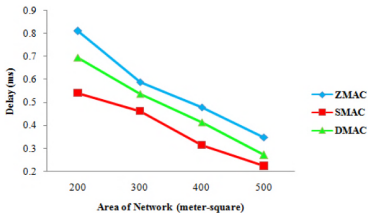
Figure 2.5a, Figure 2.5b and Figure 2.5c show the average packet delay of all three MAC mechanisms under varying traffic conditions, area of the network and number of nodes respectively. It is observed that the average delay of the contention-based protocol is less than the other two. The hybrid MAC mechanism has a higher delay because higher overheads are incurred at the beginning of the neighbor discovery and slot assignment. However, this could eventually be compensated for through improvements in energy efficiency and throughput.

2.5 Summary

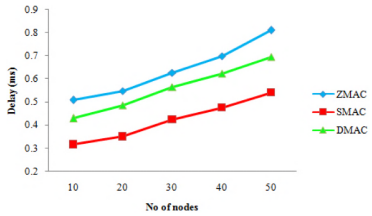
The presented benchmarks for testing of MAC mechanisms are useful in efficiently evaluating and comparing MAC mechanisms. The benchmark defines the physical parameters, implementation environments, testing scenarios, performance measurement parameters, and variables for performance measurements. These benchmarks are derived from the extensive survey of MAC mechanisms and different implementa-



(a) As a function of packet interval.



(b) As a function of the area of the sensor network.



(c) As a function of number of nodes.

Figure 2.5: Delay.

tion environments. The chapter also presented a comparative evaluation of a hybrid MAC mechanism with other types of MAC mechanisms. The evaluation indicates that hybrid MAC mechanisms are viable solutions for real-time applications, which have a mix of traffic rates. The comparative results of the MAC mechanisms show that the hybrid MAC mechanism has reduced energy consumption and improved throughput, but induces a delay in processing. Therefore, it is necessary to reduce the induced delay to improve the real-time performance of hybrid MAC mechanisms. The conclusion from the result gives important guidelines to develop enhanced hybrid MAC mechanisms.

2.6 References

[1] Tifenn Rault, Abdelmadjid Bouabdallah, and Yacine Challal. Energy efficiency in wireless sensor networks: A top-down survey. *Computer Networks*, 67:104 – 122, 2014.

[2] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer Networks*, 52(12):2292 – 2330, 2008.

[3] Pei Huang, Li Xiao, S. Soltani, M.W. Mutka, and Ning Xi. The evolution of mac protocols in wireless sensor networks: A survey. *Communications Surveys Tutorials, IEEE*, 15(1):101–120, First 2013.

[4] Derek J Corbett andAntonio G Ruzzelli, David Everitt, and Gregory O'hare. Technical Report 593: A Procedure for Benchmarking MAC Protocols used in Wireless Sensor Networks. Technical report, University of Sydney, 2006.

[5] Network simulator-2 (ns-2).

[6] P. Pawar, R. Nielsen, N. Prasad, S. Ohmori, and R. Prasad. Hybrid mechanisms: Towards an efficient wireless sensor network medium access control. In *Wireless Personal Multimedia Communications (WPMC), 2011 14th International Symposium on*, pages 1–5, Oct 2011.

[7] Yu-Chia Chang, Jehn-Ruey Jiang, Jang-Ping Sheu, and Hsin-Yi Shih. Adca: An asynchronous duty cycle adjustment mac protocol for wireless sensor networks. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1–5, Nov 2008.

[8] S. Chatterjea, L.F.W. van Hoesel, and P.J.M. Havinga. Ai-lmac: an adaptive, information-centric and lightweight mac protocol for wireless sensor networks. In *Intelligent Sensors, Sensor Networks and Information Processing Conference, 2004. Proceedings of the 2004*, pages 381–388, Dec 2004.

[9] V. Namboodiri and A. Keshavarzian. Alert: An adaptive low-latency event-driven mac protocol for wireless sensor networks. In *Information Processing in Sensor Networks, 2008. IPSN '08. International Conference on*, pages 159–170, April 2008.

[10] David Moss and Philip Levis. BoX-MACs: Exploiting Physical and Link Layer Boundaries in Low-Power Networking. Technical report, Stanford, 2008.

[11] Mehmet C. Vuran and I.F. Akyildiz. Spatial correlation-based collaborative medium access control in wireless sensor networks. *Networking, IEEE/ACM Transactions on*, 14(2):316–329, April 2006.

[12] Sha Liu, Kai-Wei Fan, and P. Sinha. Cmac: An energy efficient mac layer protocol using convergent packet forwarding for wireless sensor networks. In *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON '07. 4th Annual IEEE Communications Society Conference on*, pages 11–20, June 2007.

[13] Fabrice Theoleyre. A route-aware {MAC} for wireless multihop networks with a convergecast traffic pattern. *Computer Networks*, 55(3):822 – 837, 2011.

[14] A.B. Nacef, S. Senouci, Y. Ghamri-Doudane, and A.-L. Beylot. Cosmic: A cooperative mac protocol for wsn with minimal control messages. In *New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on*, pages 1–5, Feb 2011.

[15] M. Aykut Yigitel, Ozlem Durmaz Incel, and Cem Ersoy. Diff-mac: A qos-aware mac protocol with differentiated services and hybrid prioritization for wireless multimedia sensor networks. In *Proceedings of the 6th ACM Workshop on QoS and Security for Wireless and Mobile Networks*, Q2SWinet '10, pages 62–69, New York, NY, USA, 2010. ACM.

[16] G. Lu, B. Krishnamachari, and C.S. Raghavendra. An adaptive energy-efficient and low-latency mac for data gathering in wireless sensor networks. In *Parallel and Distributed Processing Symposium, 2004. Proceedings. 18th International*, pages 224–, April 2004.

[17] Hui Cao, Kenneth Parker, and Anish Arora. O-mac: A receiver centric power management protocol. *2012 20th IEEE International Conference on Network Protocols (ICNP)*, 0:311–320, 2006.

[18] Yanjun Sun, Shu Du, Omer Gurewitz, and David B. Johnson. Dw-mac: A low latency, energy efficient demand-wakeup mac protocol for wireless sensor networks. In *Proceedings of the 9th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '08, pages 53–62, New York, NY, USA, 2008. ACM.

[19] Jain, Vivek and Biswas, Ratnabali and Agrawal, D.P. Energy-Efficient and Reliable Medium Access in Sensor Networks. In *World of Wireless, Mobile and Multimedia Networks, 2007. PIMRC 2007. IEEE International Symposium on*, pages 1–8, June 2007.

[20] Z. Merhi, M. Elgamel, and M. Bayoumi. Eb-mac: An event based medium access control for wireless sensor networks. In *Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on*, pages 1–6, March 2009.

[21] L.A. Latiff, R.A. Rashid, S.H. Syed Ariffin, W.M.A. Wan Embong, N. Fisal, and A. Lo. Implementation of enhanced lightweight medium access (el-mac) protocol for wireless sensor network. In *Communications (APCC), 2010 16th Asia-Pacific Conference on*, pages 267–272, Oct 2010.

[22] B. Yahya and J. Ben-othman. An energy efficient hybrid medium access control scheme for wireless sensor networks with quality of service guarantees. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1–5, Nov 2008.

[23] L. Sitanayah, C.J. Sreenan, and K.N. Brown. Er-mac: A hybrid mac protocol for emergency response wireless sensor networks. In *Sensor Technologies and Applications (SENSORCOMM), 2010 Fourth International Conference on*, pages 244–249, July 2010.

[24] Changsu Suh, DeepeshMan Shrestha, and Young-Bae Ko. An energy-efficient mac protocol for delay-sensitive wireless sensor networks. In Xiaobo Zhou, Oleg Sokolsky, Lu Yan, Eun-Sun Jung, Zili Shao, Yi Mu, DongChun Lee, DaeYoung Kim, Young-Sik Jeong, and Cheng-Zhong Xu, editors, *Emerging Directions in Embedded and Ubiquitous Computing*, volume 4097 of *Lecture Notes in Computer Science*, pages 445–454. Springer Berlin Heidelberg, 2006.

[25] Ozlem Durmaz Incel, Lodewijk van Hoesel, Pierre Jansen, and Paul Havinga. Mc-lmac: A multi-channel {MAC} protocol for wireless sensor networks. *Ad Hoc Networks*, 9(1):73 – 94, 2011.

[26] Manish Kumar Jha, Atul Kumar Pandey, Dipankar Pal, and Anand Mohan. An energy-efficient multi-layer {MAC} (ml-mac) protocol for wireless sensor networks. *{AEU} - International Journal of Electronics and Communications*, 65(3):209 – 216, 2011.

[27] Gang Zhou, Chengdu Huang, Ting Yan, Tian He, J.A. Stankovic, and T.F. Abdelzaher. Mmsn: Multi-frequency media access control for wireless sensor networks. In *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, pages 1–13, April 2006.

[28] Zhenzhen Liu and I. Elhanany. Rl-mac: A qos-aware reinforcement learning based mac protocol for wireless sensor networks. In *Networking, Sensing and Control, 2006. ICNSC '06. Proceedings of the 2006 IEEE International Conference on*, pages 768–773, 2006.

[29] Joseph Polastre, Jason Hill, and David Culler. Versatile low power media access for wireless sensor networks. In *Proceedings of the 2Nd International Conference on Embedded Networked Sensor Systems*, SenSys '04, pages 95–107, New York, NY, USA, 2004. ACM.

[30] Wei Ye, J. Heidemann, and D. Estrin. An energy-efficient mac protocol for wireless sensor networks. In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 3, pages 1567–1576 vol.3, 2002.

[31] Yafeng Wu, J.A. Stankovic, Tian He, and Shan Lin. Realistic and efficient multi-channel communications in wireless sensor networks. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, April 2008.

[32] Injong Rhee, A. Warrier, M. Aia, Jeongki Min, and M.L. Sichitiu. Z-mac: A hybrid mac for wireless sensor networks. *Networking, IEEE/ACM Transactions on*, 16(3):511–524, June 2008.

[33] Gahng-Seop Ahn, Se Gi Hong, Emiliano Miluzzo, Andrew T. Campbell, and Francesca Cuomo. Funneling-mac: A localized, sink-oriented mac for boosting fidelity in sensor networks. In *Proceedings of the 4th International Conference on Embedded Networked Sensor Systems*, SenSys '06, pages 293–306, New York, NY, USA, 2006. ACM.

[34] Tijs van Dam and Koen Langendoen. An adaptive energy-efficient mac protocol for wireless sensor networks. In *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems*, SenSys '03, pages 171–180, New York, NY, USA, 2003. ACM.

[35] Qualnet.

[36] Opnet.

[37] Tinyos.

[38] Omnet++.

[39] Avrora.

[40] A. Sobeih, Wei-Peng Chen, J.C. Hou, Lu-Chuan Kung, N. Li, Hyuk Lim, Hung ying Tyan, and Honghai Zhang. J-sim: a simulation environment for wireless sensor networks. In *Simulation Symposium, 2005. Proceedings. 38th Annual*, pages 175–187, April 2005.

[41] D. Blazakis, J. McGee, D. Rusk, and J.S. Baras. Atemu: a fine-grained sensor network simulator. In *Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on*, pages 145–152, Oct 2004.

[42] Gilbert Chen, Joel Branch, Michael Pflug, Lijuan Zhu, and Boleslaw Szymanski. Sense: A wireless sensor network simulator. In BoleslawK. Szymanski and Bülent Yener, editors, *Advances in Pervasive Computing and Networking*, pages 249–267. Springer US, 2005.

[43] S.P. Fekete, A. Kroller, S. Fischer, and D. Pfisterer. Shawn: The fast, highly customizable sensor network simulator. In *Networked Sensing Systems, 2007. INSS '07. Fourth International Conference on*, pages 299–299, June 2007.

[44] Tracy Camp, Jeff Boleng, and Vanessa Davies. A survey of mobility models for ad hoc network research. *Wireless Communications and Mobile Computing*, 2(5):483–502, 2002.

Chapter 3

Conflict Free TDMA Scheduling

This chapter discusses Time Division Multiple Access (TDMA) scheduling algorithms, which are one of the building blocks of a hybrid Medium Access Control (MAC) mechanism. The chapter gives the related work in TDMA scheduling algorithms and provides three different classification methods for TDMA scheduling algorithms. Assumptions, basic notations, and the system- and communication model used in the thesis are discussed. The chapter describes the three proposals for a TDMA scheduling algorithm i.e. Green Conflict Free (GCF), Multi-color-GCF (M-GCF), and Hybrid-GCF (H-GCF). The comparative evaluation of GCF, M-GCF, and H-GCF by considering static and mobile scenarios is presented and simulation results of energy consumption, delay, and throughput are discussed. The proposed TDMA scheduling algorithms are compared with state-of-the-art TDMA scheduling algorithms.

3.1 Introduction

Nodes in a Wireless Sensor Network (WSN) are working under severe resource constraints of energy, bandwidth, processing and memory [1, 2]. This resource constrained nature of WSNs can be addressed to a large extent through the MAC layer mechanism. If the MAC mechanism allows all resources to be utilized at one time, it will not have an efficient use of resources [3, 4]. Therefore, resources should be allocated to a WSN according to traffic and load in the network. It is proficiently achieved by using a hybrid-MAC mechanism, which shifts its mode from contention-MAC to schedule-MAC and vice-versa based on the traffic in the network [3, 4, 5].

TDMA scheduling is a significant block of any hybrid MAC mechanism as the performance is affected by it. A hybrid MAC mechanism uses TDMA scheduling, when it experiences high contention or higher traffic in the network. Consider an application of a WSN in a pollution sensing environment, where pollution sensors are set up on each traffic signal. This application requires continuous monitoring, but the traffic is varying at different times of days. The traffic in such kinds of WSN applications is suddenly moving from high to low and vice-versa. Hybrid MAC mechanisms are a good solution for such applications. When traffic is high in the network, more sensing events are coming to the sensor, which leads to more contention, but such situations are likely to be important to make the correct decision. In our considered pollution-sensing application, when the hybrid MAC mechanism is used with an efficient TDMA scheduling algorithm, it leads to more accurate decisions at peak times when traffic on the road is higher and larger sensing event are coming to sensor nodes.

The primary task of a TDMA scheduling algorithm is to decide conflict free schedules depending on the network topology. A good TDMA scheduling algorithm should assign optimal schedules by reducing the contention in the network. The other significant challenges in TDMA scheduling are assigning the optimal schedules with maximum reuse of the slots, scaling to changes in the network and supporting mobility. A TDMA scheduling algorithm is also helpful to use bandwidth efficiently. This chapter discusses the different proposals of TDMA scheduling algorithms for addressing the above-stated challenges.

TDMA scheduling mechanisms are divided according to usage and network management as flat or clustered WSNs. Many algorithms have been proposed to perform TDMA scheduling in flat WSNs. The problem with the proposed mechanisms for TDMA scheduling in flat WSNs is that they are not sufficiently energy efficient and they lack performance in delay and scalability. The current research trend is to achieve TDMA scheduling using clustering, which has proven to be an efficient approach for achieving improved energy efficiency with decreased delays and increased scalability [6]. The clustering improves the scalability by stabilizing the network at the level of sensor nodes and thus lowers the topology maintenance overhead. Clustering also reduces the number of slots required by increasing the reuse of slots that, in turn, reduce the amount of delay in the communication. Especially applications of sensors in healthcare, industry, and vehicular networks set up new requirements for mobility support in WSNs and, therefore, this becomes a prime challenge in the design of TDMA scheduling algorithms [5, 7].

This chapter addresses the challenges of TDMA scheduling through three proposals of cluster-based TDMA scheduling algorithms: GCF, M-GCF and H-GCF [8, 9, 10]. The GCF- and M-GCF algorithms are proposed to address the optimal assignment of schedules and to improve the reuse of slots and scalability. The GCF algorithm finds a single conflict free schedule across three-hop neighbors for inter- and intra-cluster communication, while the M-GCF algorithm finds multiple conflict free schedules. The

algorithms are applied to a multi-hop cluster and use a conflict graph to find a conflict free schedule. By reducing the number of conflicts, the algorithms show better energy efficiency, average delay, scalability and slot sharing when compared with state-of-the-art solutions.

The challenge in TDMA scheduling is mobility support and to address this requirement, the hybrid TDMA scheduling algorithm, H-GCF, has been proposed by combining GCF and M-GCF. Mobility threshold values for H-GCF are found performing simulations of GCF and M-GCF under different mobility conditions. The comparative evaluation shows that the multi-color algorithm, M-GCF, shows better slot sharing and less conflicts with reduced energy consumption, delay, and good throughput in static and low mobility conditions while the single-color algorithm, GCF, shows better performance in high mobility conditions. H-GCF shifts from M-GCF to GCF and vice-versa based on mobility threshold value and shows reduced energy consumption, delay, and increased throughput under both fixed and random mobile conditions. The H-GCF algorithm is also analyzed by considering local mode changes, which considers the mode shift of individual cluster, instead of the global mode shift of the whole network.

Figure 3.1 shows the Chapter 3 contributions with challenges addressed, modules in the research and contributions to it. The remainder of the chapter is organized as follows. Section 3.2 focuses on ways of classification of TDMA scheduling algorithms and details the different kinds of flat- and cluster-based TDMA scheduling algorithms with their limitations. Section 3.3 describes the assumptions, the system- and communication model, notations, problem definition and methodology used. Section 3.4 gives the details of the GCF- and M-GCF algorithms with flowcharts and slot assignment algorithms used. The section also presents the comparative results of GCF and M-GCF under static and mobile scenarios. Section 3.5 defines the mobility threshold value, which is used in H-GCF to shift the mode from GCF to M-GCF and vice-versa. It also provides the requirements for and present the proposed hybrid TDMA scheduling algorithm, H-GCF. The last part of Section 3.5 discusses the simulation results of GCF, M-GCF, and H-GCF under different scenarios. Lastly, Section 3.6 gives the summary of the TDMA scheduling work discussed in the chapter.

3.2 Related Work

3.2.1 Classification of TDMA Scheduling Algorithms

TDMA scheduling algorithms for WSNs are classified in different ways according to the technique, mechanism and network management used to apply or to find the conflict free schedules or slots for doing the efficient communication as shown in Figure 3.2 and described below.

Centralized vs. distributed TDMA scheduling [11]: TDMA scheduling algorithms are classified into centralized and distributed based on where the schedules are created and assigned. Centralized TDMA scheduling gathers the information about the network and assigns a time slot according to associated global information. Mostly WSNs utilize distributed TDMA scheduling algorithms they are more suited for large number of nodes and not need full comprehensive knowledge.

Single-color vs. multi-color TDMA scheduling [8, 9]: Most TDMA scheduling algorithms use graph coloring based mechanisms to find conflict free schedule across a number of hops. Single coloring algorithms assign a single conflict free schedule to nodes across the number of hops while multi coloring algorithms allocate multiple conflict free schedules. Most of the research in WSN TDMA

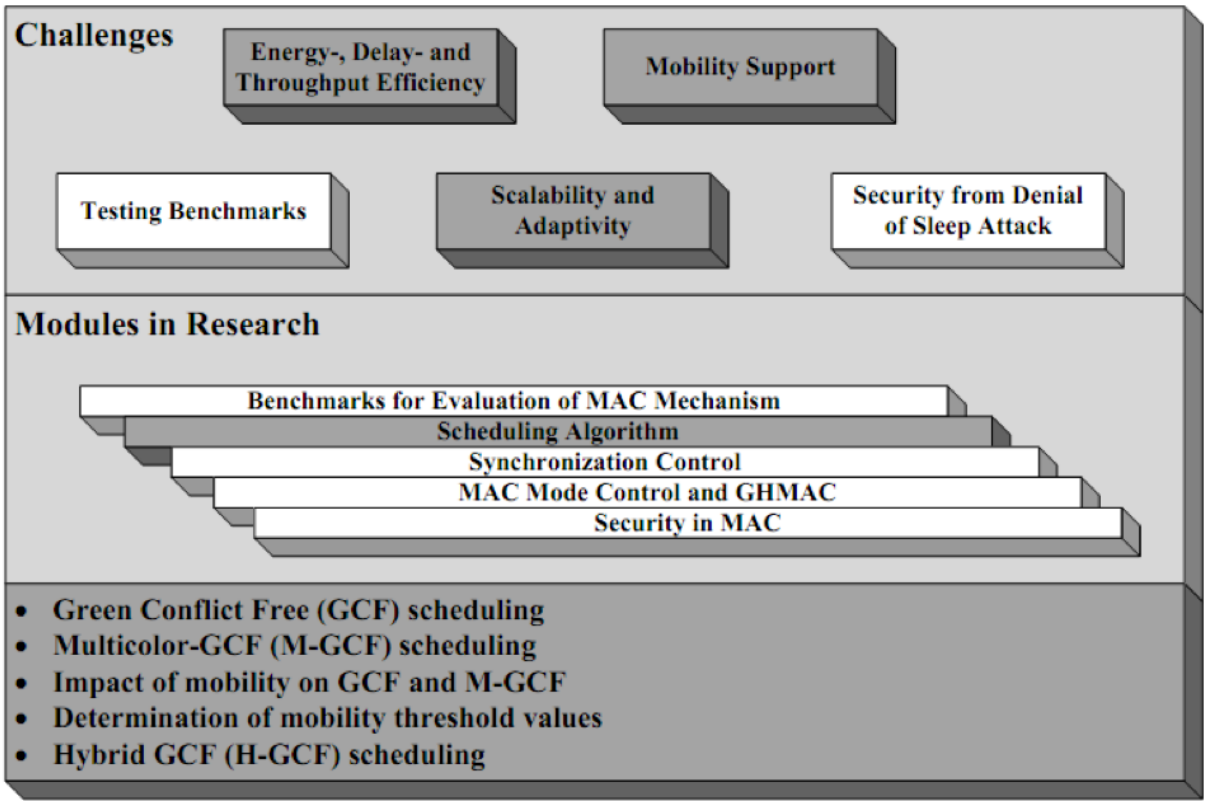


Figure 3.1: Chapter 3 contributions.

scheduling is concentrated on single-color TDMA scheduling, but multi-color TDMA scheduling is an important approach for certain intelligent applications.

Flat-network-based vs. cluster-based TDMA scheduling [8, 9]: This classification is centered on the network management or system model used to develop the TDMA scheduling algorithm. Many flat-network-based TDMA scheduling algorithms are available but to improve scalability and application in large WSNs cluster-based TDMA scheduling algorithms are more viable solutions. The following explains this classification in detail and the limitations of each of one with the primary motivation on graph coloring based clustered TDMA scheduling.

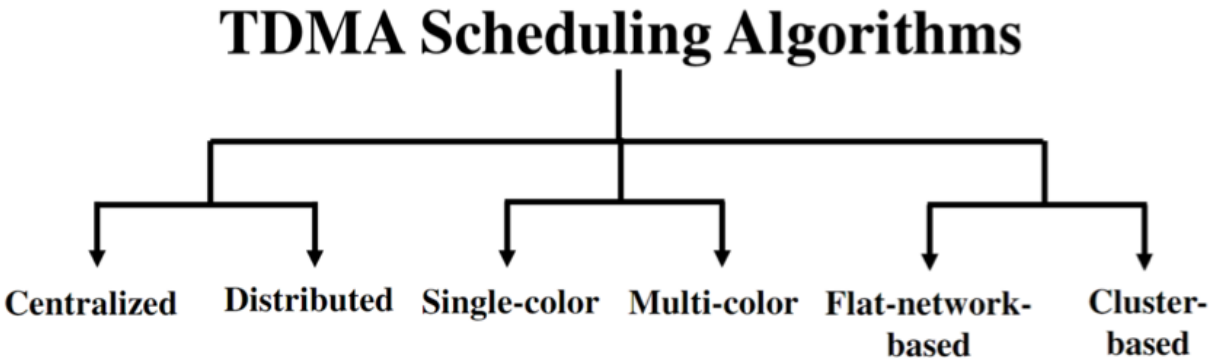


Figure 3.2: Classifications of TDMA scheduling algorithms.

3.2.2 TDMA Scheduling for Flat Network

Grid-based Latin Squares Scheduling Access (GLASS) [12] maintains grateful performance degradation in delay intensive WSNs as the data load increases. It is lightweight, overhead efficient, highly scalable, and robust in the presence of mobility. GLASS provides a decentralized scheme for creating a conflict free schedule and exploits the opportunities for minimizing overhead cost. GLASS uses Latin Square (LS) characteristics to ease the assignment of time slots for transmissions among nodes within the grid cell, thus reducing the number of colliding transmissions. GLASS assumes that each node in the WSN is location-aware and it can be modified further using clustering.

Distributed Randomized Scheduling (DRAND) [13] provides reliable data transmission and reduces collisions, but increases the control overhead and scalability with network size and mobility. DRAND maps a solution to the dining philosopher's problem to the time slot assignment. Nodes can be either philosopher (transmitters) or forks (receivers), where philosophers must contend to win access to forks. In DRAND and most of the slot assignment algorithms, whenever there is a slot requirement, the lowest possible non-conflicting slot number is picked. This causes the number of nodes mapped to a slot to decrease with the slot number, which consequently increase the interference.

Five-Phase Reservation Protocol (FPRP) [14] is a distributed TDMA slot assignment algorithm designed for dynamic slot assignment in which the real time is divided into a series of pairs of reservation and data transmission phases. During the reservation phase, the protocol assigns a slot of the next data transmission phase to the node that has data to send. Thus, the actual data transmission occurs using the slot assigned in the previous reservation phase. For each time slot of the data transmission phase, FPRP runs a five-phase protocol a number of times to pick a winner of each slot and the algorithm improves its assignments as it runs for more cycles.

In SEEDEX [15], at the beginning of each slot, if a node has a packet ready for transmission, it draws a "lottery" and, if it wins, it becomes eligible to transmit. A node knows the seeds of the random number generators of its two-hop neighbors, and hence it knows the number of nodes, within two hops, who are also eligible to transmit. The basic idea of Deterministic Distributed Time Division Multiplae Access (DD-TDMA) [16] is to let each node choose its particular slot according to the information collected from neighbor nodes. Mainly, in the algorithm this information refers to whether node's two-hop neighbors are scheduled. As a deterministic collision-free algorithm is used in TDMA scheduling, there is no need to wait for an acknowledgment from neighbors to avoid a possible collision. The scheduled node broadcasts its slot assignment to its one-hop neighbors and these one-hop neighbors broadcast this information to update their two-hop neighbors. This is repeated for every frame until finally all nodes are scheduled. The algorithm shows good running time, but has larger message complexity as compared with DRAND.

The distributed multiple slot assignment algorithm [17] works in three phases; neighborhood discovery, slot assignment and compaction. In the first phase, nodes find the one- and two-hop neighborhoods and from that, they form the initial schedule matrix. In the second phase, every node tries to reserve additional undecided slots for conflict free transmission in a fair way. The last phase consists of three steps where each node first determines its distance from a sink node in terms of hop count, transmits its slot preference towards the sink and finally receives a mapping between the old and new frames from the sink, and forwards it. The message overheads and frame length of the algorithm are much less than DRAND.

Distributed Neighborhood Information Based (DNIB) [18] algorithm decides its particular slot ac-

cording to the information collected from its one- and two-hop neighbor nodes. The algorithm (running in parallel on each node) is composed of the slot assignment process, update procedure and recovery procedure. During the slot assignment process, each non-scheduled node calculates contender ranks for itself and for its non-scheduled neighbors according to the IDs and two-hop distances to the sink. In the update procedure, once a node is assigned a slot, it sends a "one-hop broadcast" message to update its one-hop neighbors. These one-hop neighbors in turn send a "two-hop broadcast" message to update their two-hop neighbors. The recovery procedure is activated when a node does not succeed to schedule for a predetermined period. This may occur because it misses information about some of its one- and/or two-hop neighbors. DNIB shows better running time, but higher message complexity than DRAND.

The node-based TDMA scheduling algorithm [7] has been adopted from a classical multi-hop TDMA scheduling algorithm developed for general ad-hoc networks with the idea of TDMA scheduling as many non-conflicting sets of nodes are possible in each time slot. The algorithm has two parts. In the first part, it colors the conflict graph, $GC_c = (V_c, EC_c)$, where $V_c = V \setminus \{1\}$, $EC_c = EC \setminus N_1$ and $N_1 = \{(i,j)|i = 1\}$. In the second part, it schedules the links in the original network, $(u, v) \in E$ based on this coloring. The complexity of the algorithm depends on the maximum degree of the node in the conflict graph.

The level-based TDMA scheduling algorithm [7] has three parts. In the first part, it obtains a linear network $GL = (VL, EL)$. The linear network has nodes $VL = (v_1, \ldots, v_n)$ with node v_l corresponding to all nodes at level l in the original network and edges $(v_i, v_i + 1) \in EL$ for $1 <= i < N$. The interference graph $CL = (VL, IL)$ includes edge (v_j, v_l), if there is an interference edge between a node at level j and any node at level l in the original network for $j, l >= 1$. The resulting conflict graph $GCL = (VL, ECL)$ thus includes edge (vj, vl), if the transmissions of a node at level j and a node at level l conflict in the original network. In the second part, this linear network colors with M colors. In the third part, it schedules the links in the original network, $(u, v) \in E$, based on the coloring of the linear network. The complexity of the algorithm depends on time required to form a linear network and the maximum degree of the node in a graph.

The distributed slot assignment in Power Efficient and Delay Aware MAC for Sensor Network (PEDAMACS) [19] works in two stages. During the first stage of the algorithm, each node picks one slot for transmission in the order of the traversal of a Depth-First Search (DFS) of the graph. In the second stage, the DFS is repeated, and now each node picks as many of the remaining colors as it can for transmission. At both stages, the nodes send this information to their one-hop and two-hop neighbors so that all their interferers in the conflict graph, GC, learn about the assignment. The DFS traversal starts with a TOKEN message generated at the Access Point (AP). Here, the complexity of the algorithm depends on the number of token transmissions at each stage and total number of transmission for distributing the color assignments.

The distributed link-based algorithm [20] consists of two phases. The first phase involves edge coloring - an assignment of a color to each edge in the network such that no two edges incident on the same node are assigned the same color. The second phase uses the edge coloring solution for link. It maps each color to a unique time slot and attempts to assign a direction of transmission along each edge such that the hidden terminal problem is avoided.

Flat-network-based TDMA scheduling has many limitations whenever there is a need to scale the network due to maintaining a global view of the network for which this scheduling also shows less slot

sharing and slot reuse. This type of scheduling incurs considerable energy consumption and average delay because of the large amount of message exchanges during slot determination at initial stages of the network and the reassignment of slots under mobility conditions is also difficult because of consideration of the total network instead of part of the network.

3.2.3 TDMA Scheduling for Clustered Network

The authors [21] propose a self-reorganizing slot allocation protocol for multi-cluster sensor network that uses an adaptive slot allocation based on feedback derived from the collision experienced by the local nodes to reduce inter-cluster TDMA interference under low load conditions. It reduces the inter-cluster interference using feedback-based adaptive allocation, reorganization without relying on any global synchronization and shows good performance with moderate cluster overlapping. As a disadvantage, it focuses only on inter-cluster communication and does not cosnider variable node density across the cluster. It is useful for sensor applications, which can tolerate relatively large delivery latency, but not frequent packet drops.

The Low-energy Adaptive Slot Allocation (LASA) [22] TDMA scheduling algorithm for WSNs uses a variable slot size instead of a fixed slot size and it eliminates slot idle time when nodes remain unnecessarily active with no data to transmit or receive. It uses Code Division Multiple Access (CDMA) codes for avoiding inter-cluster interference, which makes it complicated to implement. The technique is suitable for applications where there are high traffic fluctuation and a significant variance in sensor data length.

Multi-cluster, multi-parent, wake-up TDMA scheduling [23] is proposed for delay-sensitive WSN where it provides bi-directional latency guarantee while optimizing the node battery lifetime. The algorithm gives a distributed solution to finding the schedule with each Cluster Head (CH) responsible for assigning slots in its smaller area. The algorithm can be improved if more CHs can be used but the adverse effect on slot assignment will be observed if cluster overlapping increases. The scheduling shows exquisite performance for applications where both forward and backward traffic is high.

The algorithm for reducing inter-cluster TDMA interference by adaptive MAC allocation in sensor networks [24], reduces interference by pre-allocating slots for dome edge nodes. It uses slot pre-allocation algorithm, which does not need the synchronization of the whole network, but the only information on individual cluster. The major disadvantage of the algorithm is; it does not support intra-cluster communication, which reduces its efficiency. The algorithm is suitable for sensor application, which can tolerate relatively large delivery latency but not frequent packet drops.

The Adaptive Distributed Randomized (A-DRAND) [25] TDMA scheduling for clustered WSNs is the cluster-based version of the popular flat TDMA scheduling algorithm DRAND. Here, the CH needs more slots and will be alternated afterwards by other cluster members for energy balance. It adapts very quickly to changes in CHs but induces overheads in slot reassignment. The algorithm is useful for environmental monitoring and industrial process control.

TDMA Scheduling with Adaptive Slot-stealing and Parallelism (TDMA-ASAP) [26] is a WSN TDMA scheduling algorithm with adaptive slot-stealing and effective parallelism. The transmission parallelism based on a level-by-level localized graph coloring and support appropriate sleeping between transmissions. It supports judicious and controlled TDMA slot stealing to avoid empty slots to be unused. TDMA-ASAP

is not exactly a clustering approach as it divides the network according to the transmission range of nodes. The algorithm is suitable for applications, which require quick response time in higher traffic.

The algorithm in [27] shows improvements in energy efficiency with respect to interfering cluster TDMA scheduling, intra-cluster node TDMA scheduling, and transmission powers and time control for individual nodes. It finds the best solution iteratively, which reduces the energy consumption. The use of group-based TDMA scheduling is the advantage of the algorithm, but it is not adaptable to variable traffic conditions and applicable only if CDMA will be used.

The above survey points out some significant disadvantages of currently available cluster-based TDMA scheduling techniques. A key disadvantage is that most of them are limited to inter- or intra-cluster TDMA scheduling and, thus, are not suitable for finding network-wide i.e. inter- and intra-cluster conflict free schedules.

3.3 Assumptions, System Model, and Methodology

3.3.1 Assumptions

Node Assumptions

- All nodes have similar capabilities and equal significance.
- Nodes are location unaware without any Global Positioning System (GPS) capabilities.
- Every node has a unique Identification (ID) and all the nodes in the network are synchronized.
- All nodes get their slot from one pool of slots.
- Nodes use one slot / set of slots for multi-hop communication.
- The Base Station (BS), CHs, and nodes are assumed static or mobile according to the requirement.

Network Assumptions

- There is a single BS in the network.
- The network is divided into clusters; every cluster has a CH and cluster members.
- The clusters are considered as multi-hop clusters to achieve better energy efficiency and scalability in the clustered environment.
- There are mixed uni- and bi-directional links.

3.3.2 Basic Notations

- $G = (V, E)$ is a graph representing the network with V as the set of all vertices ($BS + CH + NormalNodes(NN)$) and E is the set of edges (links).
- The graph, G, is divided into n cliques and $G = \{G_1, G_2, \ldots, G_n\}$.
- $GC = (V_c, E_C)$ is the conflict graph of G with V_c vertices and E_C edges.

- N is the number of nodes (vertices) in the conflict graph GC.
- v is a node which slot is to be determined.
- N_{1v}, N_{2v} and N_{3v} are the sets of one-, two-, and three hop neighbors of node v respectively.
- (x_v, Γ_{v_1}) is the one-hop view of node v.
- $(x_v, \Gamma_{v_1}, \Gamma_{v_2})$ is the two-hop view of node v.
- $(x_v, \Gamma_{v_1}, \Gamma_{v_2}, \Gamma_{v_3})$ is the three-hop view of node v.
- I is the list of slots; $I = \{1, 2, 3, \ldots, n\}$.
- $H(I)$ is the set of slots assigned to a node.
- i is the number of slots in the set.
- d_v is the degree of node v.
- $D[N]$ is the list of degrees of each node in GC.
- M is the set of CH and NN in a network, $M \in (V - BS)$.
- th is the mobility threshold value.
- mn is the mobility node count.
- T is the network runtime.

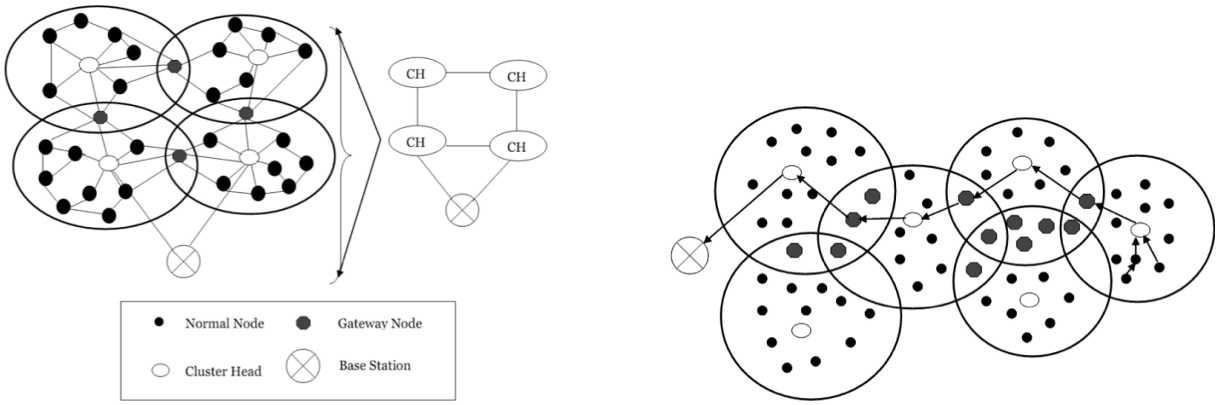
3.3.3 System and Communication Model

Each clique is considered a cluster and is formed using a multi-hop clustering algorithm [6]. Each cluster has a CH that acts as a BS for that particular cluster and which gathers data from all other normal nodes in the cluster and then forward towards the BS. Two clusters are connected using gateway nodes which are nodes common between two or more clusters where the interference range of the clusters overlaps with each other. Figure 3.3a and 3.3b show the system and communication model considered for the proposed algorithms respectively. The system model gives the architectural view, which explains the skeleton and full body of the considered network. The communication model shows how packets generated from normal nodes will be destined to the CH and from there to the BS. Here, both the communication between normal nodes and the CH (intra-cluster communication) and communication between the CH and the BS (inter-cluster communication) are multi-hop.

3.3.4 Methodology

The TDMA scheduling problem considered here will determine,

- The non-conflicting schedules within the cluster to communicate between the normal nodes and CH (intra-cluster communication).
- The network-wide, non-conflicting schedules to communicate between the CHs and the BS (inter-cluster communication).



(a) Proposed system model.

(b) Proposed communication model.

Figure 3.3: System and communication model.

The problem of finding non-conflicting schedule for intra and inter-cluster communication will be solved using the following TDMA scheduling algorithms for intra- and inter-cluster communication,

- Single-color - GCF: Single non-conflicting schedule.
- Multi-color - M-GCF: A set of non-conflicting schedules.
- Hybrid-color - H-GCF: An adaptable schedule according to mobility conditions of nodes.

3.4 Conflict Free TDMA Scheduling

3.4.1 GCF: Green Conflict Free TDMA Scheduling Algorithm

Flow of Algorithm

The GCF algorithm for assigning the slot/color is divided into two phases,

- Phase 1: Intra-cluster communication
- Phase 2: Inter-cluster communication

Figure 3.4 shows the flow of activities for Phase 1 of the GCF algorithm with the purpose of finding a single conflict free slot for intra-cluster communication across three-hop neighbors. Phase 1 takes the total network, $G = (V, E)$, as an input that is divided into C clusters, and it starts by taking the first cluster for processing as the first step. In the second step, the algorithm calculates the conflict graph [7], $GC_{CP} = (V_{CP}, EC_{CP})$, where V_{CP} is the set of nodes/vertices in the processed cluster and EC_{CP} is the set of conflicting edges/links between the nodes/vertices. The next step assigns a slot to each node in GC_{CP} using Algorithm 1. The algorithm runs iteratively for each cluster until all clusters in the network has been processed, and each node has been assigned a slot.

Phase 2 of the GCF algorithm works through the same steps as Phase 1 except for the following: The task of this phase is to find conflict free slots for inter-cluster communication and the inputs are the network $G_{CH} = (V_{CH}, E_{CH})$, where V_{CH} is the set of all CHs and the BS i.e. $V_{CH} \in (CHs + BS)$ and E_{CH}, as the set of edges connecting them. The next step in the algorithm calculates the conflict graph $GC_{CH} = (V_{CH}, EC_{CH})$ where EC_{CH} is the set of conflicting edges or links. The input to the next step

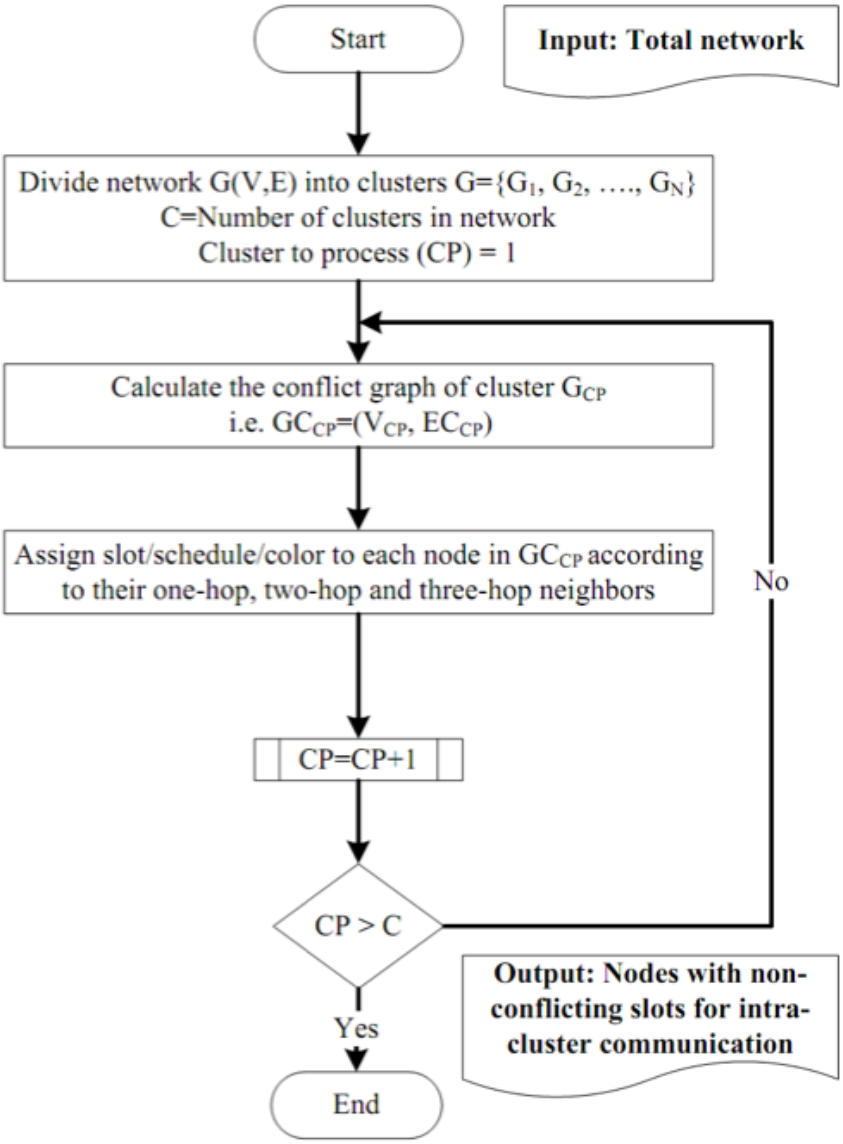


Figure 3.4: Phase 1 of the GCF algorithm for intra-cluster communication.

is the conflict graph, GC_{CH}, the value of $N_{GC_{CH}}$ and the initial value of the node to process (NP) for assigning the slot. The third step assigns the slot to each node in GC_{CH} using Algorithm 1, according to their one-, two-, and three-hop neighbors. The sub-process from the third step increments the value of NP by one and the fourth step checks if NP is greater than $N_{GC_{CH}}$ or not. If greater, it ends the algorithm and otherwise, it repeats the algorithm until all nodes in GC_{CH} have been allocated a communication slot for inter-cluster communication. At the end of the two phases, each node in the network will have a non-conflicting slot across their three-hop boundaries for intra- and inter-cluster communication.

Algorithm for Assigning Slot

The conflict free slot for intra-cluster communication is found using Algorithm 1. The algorithm requires a conflict free graph, $GC = (V_c, EC)$, of each cluster as an input and finds non-conflicting slot for each node across a three-hop boundary.

Algorithm 1 is also used to find a conflict free slot for inter-cluster communication, but with modified

input. The input is the conflict graph, $GC = (V_c, EC)$, of graph $G = (V, E)$ with $V \in (CHs + BS)$ and E as the edges connecting the CH to each other and to the BS.

Algorithm 1: GCF algorithm for finding conflict free slot for intra-cluster communication.

input : The conflict graph $GC = (V_c, EC)$ of each sub graph ($G = G_1, G_2, \ldots, G_n$)

output : The nodes with non-conflicting slots

for *each node* $v \in V_c$ **do**
    Calculate degree d;
    $D[N] = d$;
    Calculate degree N_{1_v}, N_{2_v} and N_{3_v};
Sort($D[N]$);
for *each node* $v \in D[N]$ **do**
    if v *is the first element in the list* **then**
        Assign slot from set I to node v;
        $N = N + 1$;
        $I = I + 1$;
    else
        if $v \notin N_{1_v} \&\& v \notin N_{2_v} \&\& v \notin N_{3_v}$ **then**
            //Assigns a slot other than its one-, two-, and three- hop neighbors;
            Assign slot I to node v;
            $N = N + 1$;
            $I = I + 1$;

3.4.2 M-GCF: Multicolor Green Conflict Free TDMA Scheduling Algorithm

Flow of Algorithm

The multi-coloring based M-GCF algorithm for assigning sets of slots/colors are organized into two phases,

- Phase 1: Intra-cluster communication
- Phase 2: Inter-cluster communication

Figure 3.5 elaborates the course of events in Phase 1 of the M-GCF algorithm. The intra-cluster slot assignment phase finds the conflict free set of slots for intra-cluster communication across the three-hop view. It takes the total network, $G = (V, E)$, as an input that is divided into C clusters and starts processing with the first cluster; CP gives the value of the current cluster to be processed. In the succeeding step, the algorithm calculates the conflict graph, $GC_{CP} = (V_{CP}, EC_{CP})$, for cluster number CP, where V_{CP} is the set of nodes/vertices and EC_{CP} is the set of conflicting edges/links between the nodes/vertices. The next step is the core of the M-GCF algorithm, which assigns the conflict free set of slots to each node in GC_{CP} using Algorithm 2. Here, it assigns the slots according to one-, two- and three-hop views. The sub-process of this step increments the value of CP by one and compares its value with N and if it is greater than CP then the algorithm terminates and otherwise it will be repeated N times. Finally, the algorithm ends with assigning sets of non-conflicting slots to each node in the cluster.

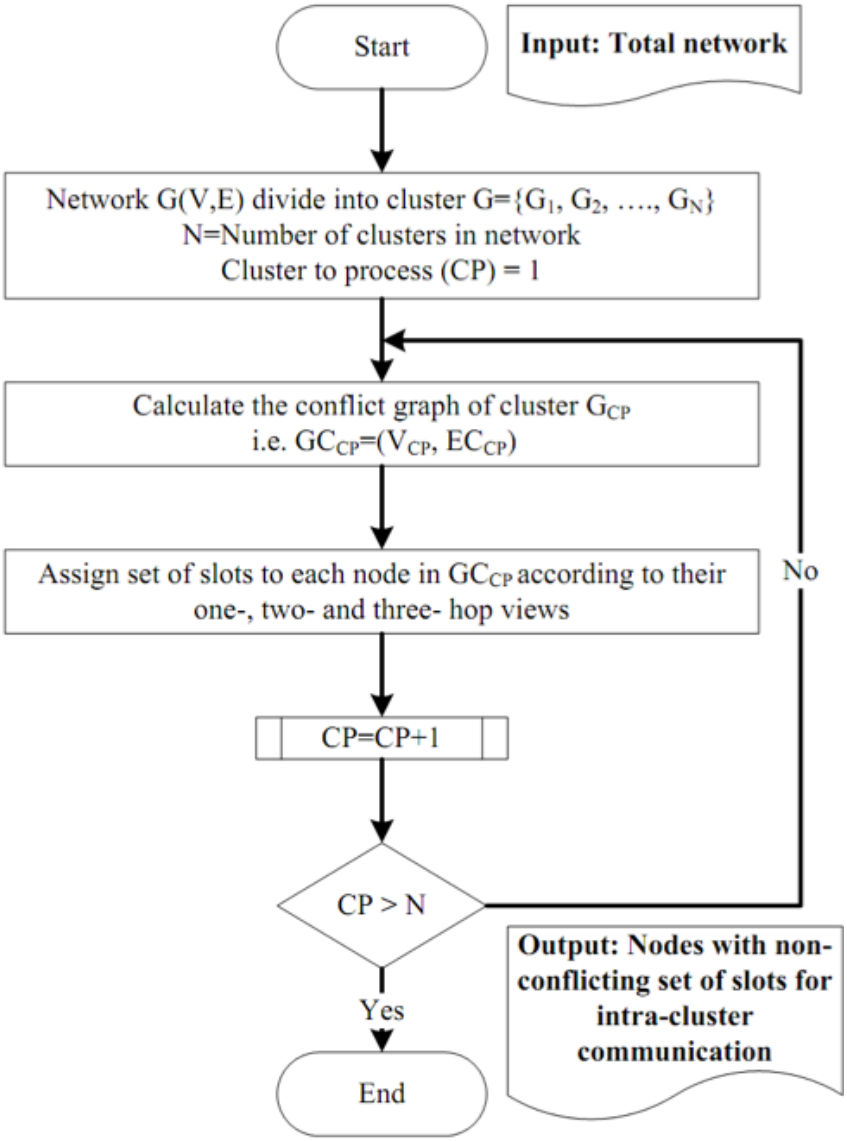


Figure 3.5: Phase 1 of the M-GCF algorithm for intra-cluster communication.

The steps of getting sets of slots for inter-cluster communication using the M-GCF algorithm is working like Phase 1 under the following consideration. It takes the same input as Phase 2 of the GCF algorithm i.e. the network graph, $G_{CH} = (V_{CH}, E_{CH})$. The second step calculates the conflict graph, $GC_{CH} = (V_{CH}, EC_{CH})$. The input to the next step is the conflict graph, GC_{CH}, the value of $N_{GC_{CH}}$ and the initial value of NP for assigning the slot. The third step assigns a set of slots to each node in GC_{CH} using Algorithm 2, according to their one-, two-, and three-hop views. Later on, the algorithm increments the value of NP and checks if it is greater than $N_{GC_{CH}}$ then the algorithm terminates with output as a non-conflicting set of slots for inter-cluster communication and otherwise it repeats the steps to achieve the final output. The execution of the two phases ends with a non-conflicting set of slots for doing efficient communication inside and outside the cluster across their three-hop view.

Algorithm for Assigning Multiple Slots

Algorithm 2 assigns the conflict free set of slots for intra-cluster communication. This algorithm also requires a conflict free graph, $GC = (V_c, EC)$, of each cluster as input and finds a non-conflicting set of slots for each node across their three-hop views. Here, the algorithm calculate the degree, d_v, of each node, v, and copy it into an array, $D[N]$, and succeeding with this it finds the one-, two- and three-hop view of each node, v, i.e. (x_v, Γ_{v_1}), $(x_v, \Gamma_{v_1}, \Gamma_{v_2})$ and $(x_v, \Gamma_{v_1}, \Gamma_{v_2}, \Gamma_{v_3})$. The collected information of each node is arranged in the form of node ID, degree of node, one-, two-, and three-hop views, and then, like in Algorithm 1, it sorts the entries in a list in decreasing order of degrees. The next part of the algorithm assigns the set of $H(i)$ conflict free slots to each node, v, from the slot pool, I, according to its one-, two- and three-hop views [28], if it is not the first element in the list. Similarly, Algorithm 2 is applied to assign the conflict free slots for inter-cluster communication with input being the conflict graph, $GC = (V_c, EC)$, of graph $G = (V, E)$ with $V \in (CHs + BS)$ and E are the edges connecting the CH to each other and to the BS.

Algorithm 2: M-GCF algorithm for finding conflict free set of slots for intra-cluster communication.

input : The conflict graph $GC = (V_c, EC)$ of each sub graph $(G = G_1, G_2, \ldots, G_n)$
output : The nodes with non-conflicting slots

for *each node* $v \in V_c$ **do**
    Calculate degree d;
    $D[N] = d$;
    Calculate degree (x_v, Γ_{v_1}), $(x_v, \Gamma_{v_1}, \Gamma_{v_2})$ and $(x_v, \Gamma_{v_1}, \Gamma_{v_2}, \Gamma_{v_3})$;
Sort($D[N]$);
for *each node* $v \in D[N]$ **do**
    if v *is the first element in the list* **then**
        Assign set of $H(I)$ to node v;
        $N = N + 1$;
        $I = I + 1$;
    else
        if $(v \in x_v, \Gamma_{v_1})\&\&(v \in x_v, \Gamma_{v_1}, \Gamma_{v_2})\&\&(v \in x_v, \Gamma_{v_1}, \Gamma_{v_2}, \Gamma_{v_3})$ **then**
            Assign set of $H(i)$ colors to node v;
            $N = N + 1$;
            $I = I + 1$;

3.4.3 Simulation Results for GCF and M-GCF

Simulation Parameters

The simulations of the algorithms are performed using Matlab and Network Simulator-2 (NS-2) and the parameters considered are shown in Table 3.1.

GCF and M-GCF are compared with DRAND, which is an efficient and widely used slot assignment algorithm for flat WSNs and A-DRAND, the cluster-based version of DRAND in a static scenario. The clustering used for implementation of GCF and M-GCF is Enhanced Multihop Clustering Algorithm

Table 3.1: Simulation parameters for simulating TDMA scheduling algorithms.

Parameters	Setting used
Wireless Physical	
Network interface type	Wireless Physical
Radio propagation model	Two-Ray Ground
Antenna type	Omni-directional Antenna
Channel type	Wireless Channel
Link Layer	
Interface queue	Priority Queue
Buffer size of IFq	50
TDMA scheduling	DRAND, A-DRAND, M-GCF, GCF, H-GCF
Routing protocol	Ad-hoc Routing
Transport layer protocol	UDP
Traffic model	CBR
Energy Model	
Initial energy (Joule)	100
Idle power (mW)	14.4
Receiving power (mW)	21.0
Transmission power (mW)	14.4
Node Placement and Other Parameters	
Number of nodes	25, 50, 75, and 100
Number of sources	24, 49, 74, and 99
Number of BS	1
Node placement	Random
Placement of nodes and BS	Nodes are placed randomly in a given area, and the BS is positioned in the middle of a given area.
Number of simulation runs	50

(EMCA) [29] which is highly scalable multi-hop clustering algorithm. The mobility model considered is a random waypoint mobility model [30].

The performance of GCF and M-GCF is measured by considering the following two scenarios,

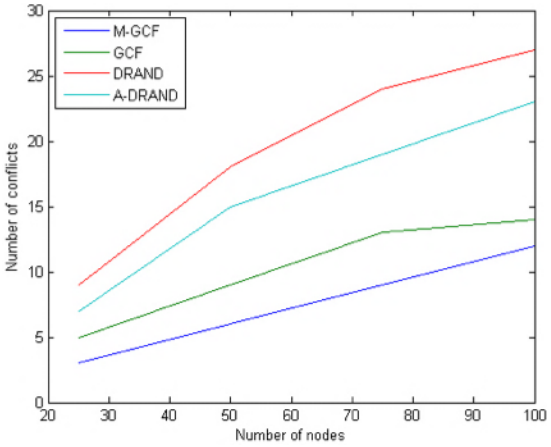
- Static scenarios: The performance is measured by varying the number of nodes and traffic rate where the measurements are averages for energy, delay and throughput.

- Mobile scenarios: The performance is measured by varying the percentage of mobile nodes and the mobility speed of nodes.

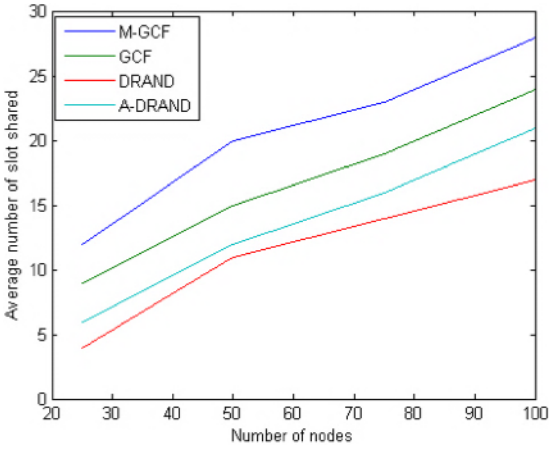
Simulation Results under Static Scenario

Figure 3.6a shows the trend of the number of nodes vs. number of conflicts in case of M-GCF, GCF, DRAND and A-DRAND. The number of conflicts in case of M-GCF is less compared to the other three due to the multi-coloring that assigns multiple slots to each node, which increases the total number of required slots but reduces the conflicts. Another reason for the reduction in conflicts is that M-GCF is applied to the conflict graph as also done for GCF. GCF shows better results than DRAND and A-DRAND because it finds the conflict free schedule across three-hop neighbors while the other two assign the conflict free schedule across two-hop neighbors only.

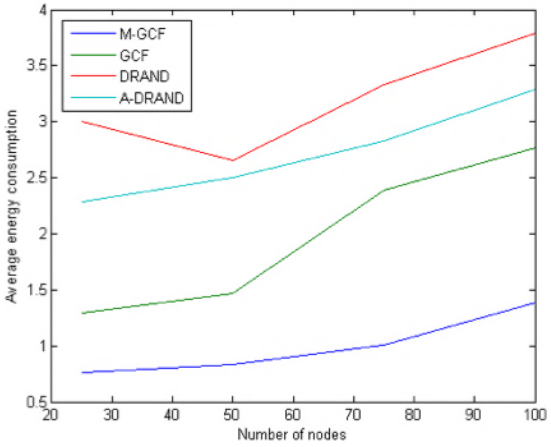
Figure 3.6b shows the trend in the average number of slots shared as a function of the number of nodes. The graph shows that as the number of nodes increases, the number of slots required increases, which results in an upsurge in the number of slots shared. Here, M-GCF shows better slot sharing than the other algorithms as the multi-coloring approach used in M-GCF improves the slot sharing by allocating a set of slots to each node compared to assigning a single slot to each node. Another reason for the increased slot



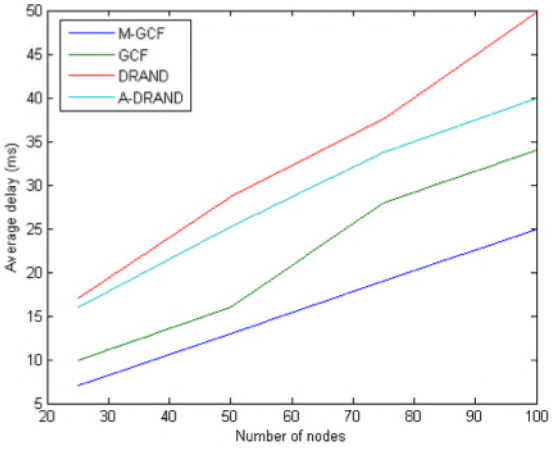
(a) Number of conflicts.



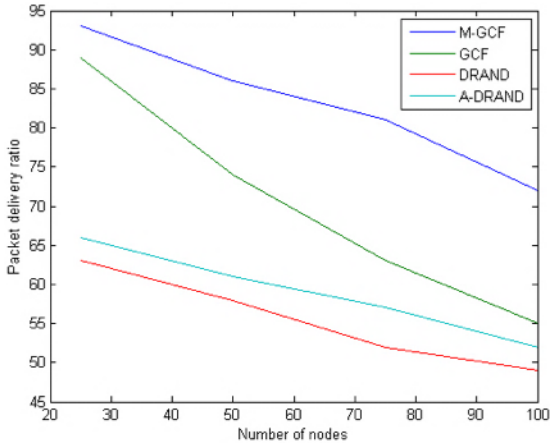
(b) Average number of slots shared.



(c) Average energy consumption.



(d) Average delay.

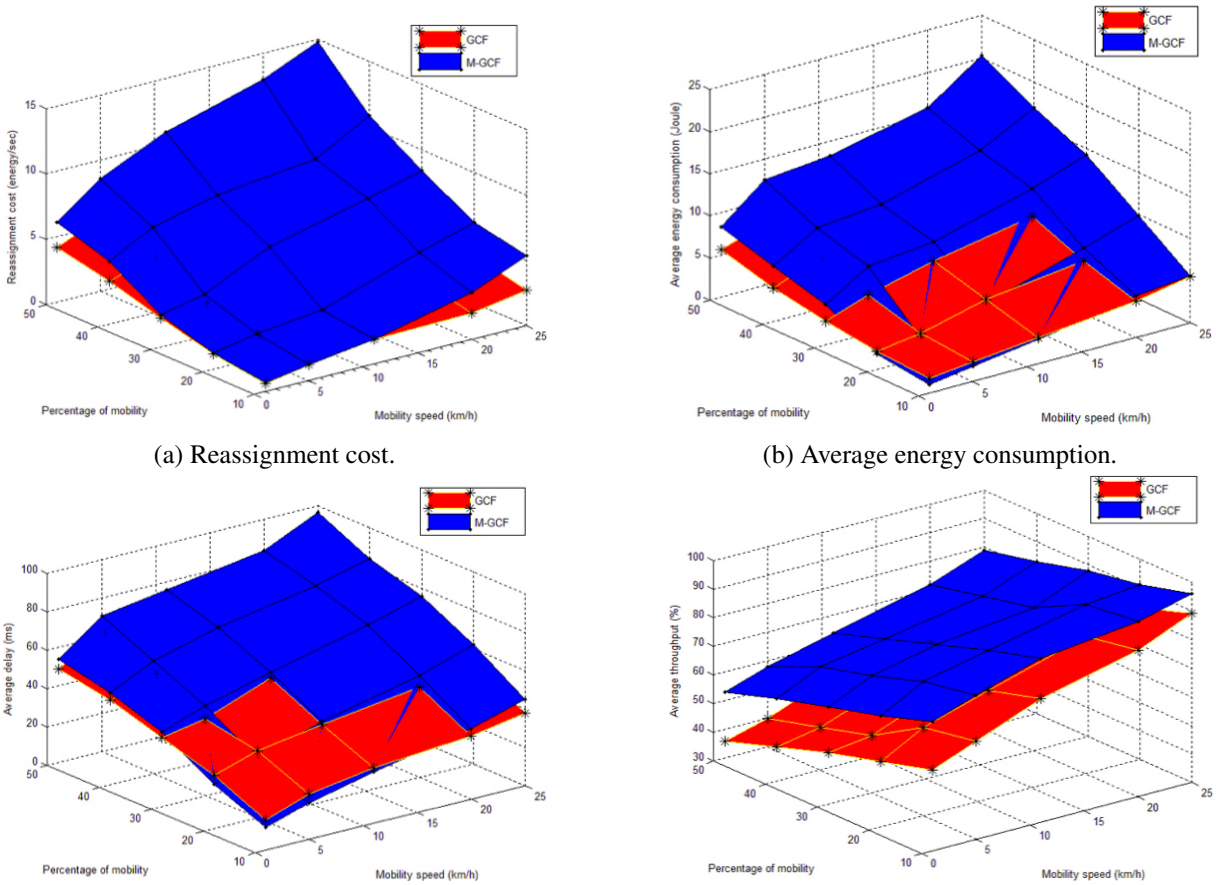


(e) Packet delivery ratio.

Figure 3.6: Results for number of nodes.

sharing in M-GCF (and GCF) is the multi-hop cluster-based approach used, which allows the same slots to be used in another cluster without conflicts.

Figure 3.6c, 3.6d and 3.6e show the trend as a function of number of nodes for average energy consumption, delay and packet delivery ratio respectively. In all three cases, M-GCF shows better performance. The reason for the better performance is the technique used in M-GCF where the conflict free graph and the assignment of multiple slots to each node are utilized. Another important reason for the



(a) Reassignment cost.

(b) Average energy consumption.

(c) Average delay.

(d) Average throughput.

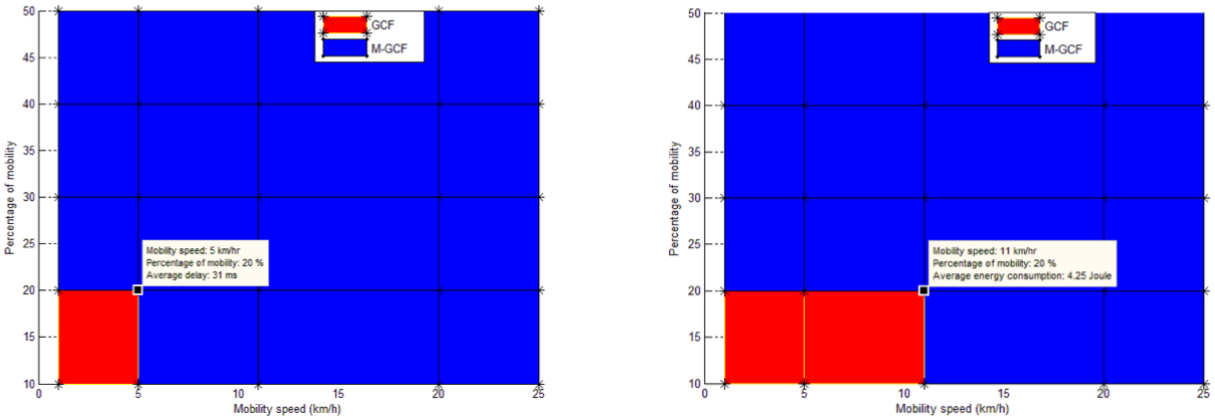
Figure 3.7: Results for single-color (GCF) and multi-color (M-GCF) algorithms.

improved performance of M-GCF over the other algorithms is the smaller number of conflicts with more slots sharing as shown in Figure 3.6a and 3.6b. GCF also shows better performance as compared with DRAND and A-DRAND, as it also uses the conflict free graph for assigning the slots and shows good slot sharing as compared with the other algorithms.

Simulation Results under Mobile Scenario

Figure 3.7a shows the mesh graph for the reassignment cost of GCF and M-GCF under different mobility speed and a varying number of mobile nodes. In the case of mobile scenarios, whenever a node moves, the neighbor nodes are likely to change. Therefore, it is necessary to update the slot assignment, i.e. reassignment of slots to continue conflict free communication. Reassignment of slots consumes energy and requires time to complete where the reassignment cost is defined as the energy per second required to reassign the slots to the node. The mesh graph shows that the reassignment cost of M-GCF is higher than for GCF because M-GCF is a multi-coloring based algorithm and GCF is a single-coloring algorithm. M-GCF assigns a set of slots to each node and, therefore, whenever reassignment is required a set of slots is needed while GCF has to reassign a single slot only. Hence, the energy and time required for reassigning a set of slot are higher than reassigning a single slot.

Figure 3.7b and 3.7c show the mesh graphs of the average energy consumption and delay in case of GCF and M-GCF under different mobility speed and varying number of mobile nodes. The results show



(a) Average delay.

(b) Average energy consumption.

Figure 3.8: X-Y view of single-color (GCF) and multi-color (M-GCF) algorithms.

that the M-GCF algorithm perform worse than the GCF algorithm because of the higher reassignment cost. The average delay and energy consumption of the M-GCF algorithm are slightly better than the GCF algorithm in case of low mobility conditions i.e. less mobile nodes and lower speed. The reason for the better performance during low mobility conditions is the reduced need for reassignment and thus consumption of energy.

Figure 3.7d shows the mesh graph of average throughput in case of GCF and M-GCF where the packet delivery ratio of M-GCF is 10% to 20% better than GCF in both low and high mobility conditions. The reason for the better throughput in case of M-GCF is the assignment of multiple slots to each node that increases the chance of a packet to reach the destination.

3.5 Hybrid Conflict Free TDMA Scheduling

3.5.1 Mobility Threshold Decision

The mobility threshold is the combined value of mobility percentage and mobility speed under which both single- and multi-coloring algorithms show approximately the same performance and the value can be used to decide upon a particular algorithm according to the mobility requirements of the application.

Figure 3.8a shows the X-Y view of the average delay of the single-color (GCF) and multi-color (M-GCF) algorithms with varying percentage of mobile nodes and the speed of these. It shows that the average delay of M-GCF is lower than GCF up to a mobility percentage 20% and mobility speed of 5 km/h after which M-GCF delays start to increase.

Figure 3.8b shows the X-Y view of the average energy consumption of GCF and M-GCF where the energy consumption of M-GCF is reduced compared to GCF up to a mobility percentage of 20% and a mobility speed of 11 km/h. The intersection of Figures 3.8a and 3.8b gives the equilibrium mobility threshold value as 20% for the mobility percentage and 5 km/h for the mobility speed.

3.5.2 Requirement of Hybrid TDMA Scheduling

The performance of GCF and M-GCF under static scenario shows that these two algorithms reduce energy consumption, delay and increase the total throughput of a WSN as compared with state-of-the-art

algorithms. The improvements are due to both algorithms (1) find a conflict free schedule across a three-hop boundary, (2) find slots by applying the slot assignment algorithm on the conflict graph and (3) use multi-hop clustering. These three unique improvements increase the amount of slot sharing and the number of conflicts in the network that provide better results for energy consumption, delay and throughput.

As seen from the previous results, the two proposed algorithms, GCF and M-GCF, perform differently depending on the mobility conditions and as such a hybrid algorithm can be advantageous, if it is able to operate in one of the two modes depending on these conditions. The primary requirements of the hybrid algorithm are,

- When to shift the mode?
- Moreover, by using what threshold value?

Two values can be used to determine the shift in mode: The mobility threshold value as the equilibrium value of a number of mobile nodes and the mobility threshold value that will be decided by doing multiple runs of the experiment with varying percentage of mobility and speed of mobility. The values used (based on Figure 3.8b) are percentage of mobility of 20% and speed of mobility of 11 km/h. Below these values, the average energy consumption of M-GCF is less than the GCF and above this value its performance start to degrade and GCF is showing reduced energy consumption over M-GCF.

3.5.3 H-GCF: Hybrid Green Conflict Free Algorithm

For H-GCF to be able to shift between M-GCF (multi-color TDMA scheduling) and GCF (single-color TDMA scheduling) and vice versa, intelligent sensor nodes with some required capabilities are assumed (GCF, M-GCF and transition between these according to the mobility threshold value).

Figure 3.9 shows the sequence of activities for the H-GCF algorithm summarized as,

- Initially, all nodes in the network are using M-GCF with good performance under static and low mobile conditions as assumed for the start of the network i.e. 0% mobility in the network.
- The BS maintains two values:
  - Mobility threshold, th, is the equilibrium value of a number of mobile nodes above or below which the network can change the mode from GCF to M-GCF and vice-versa.
  - Mobile node count, mn, is the number of mobile nodes.
- If a node becomes mobile (detected if there is churn in the neighbors), it sends the Increment Mobile Node Count (IMNC) message towards the BS that increments the value of mn.
- If the value of mn crosses the value of th, then the network will generate an MC message and broadcast it. When receiving the MC message, the node will change the mode from M-GCF to GCF.
- If a node becomes static (no mobility detected for 1 to 2 seconds), it sends the Decrement Mobile Node Count (DMNC) message towards the BS that decrements the value of mn.

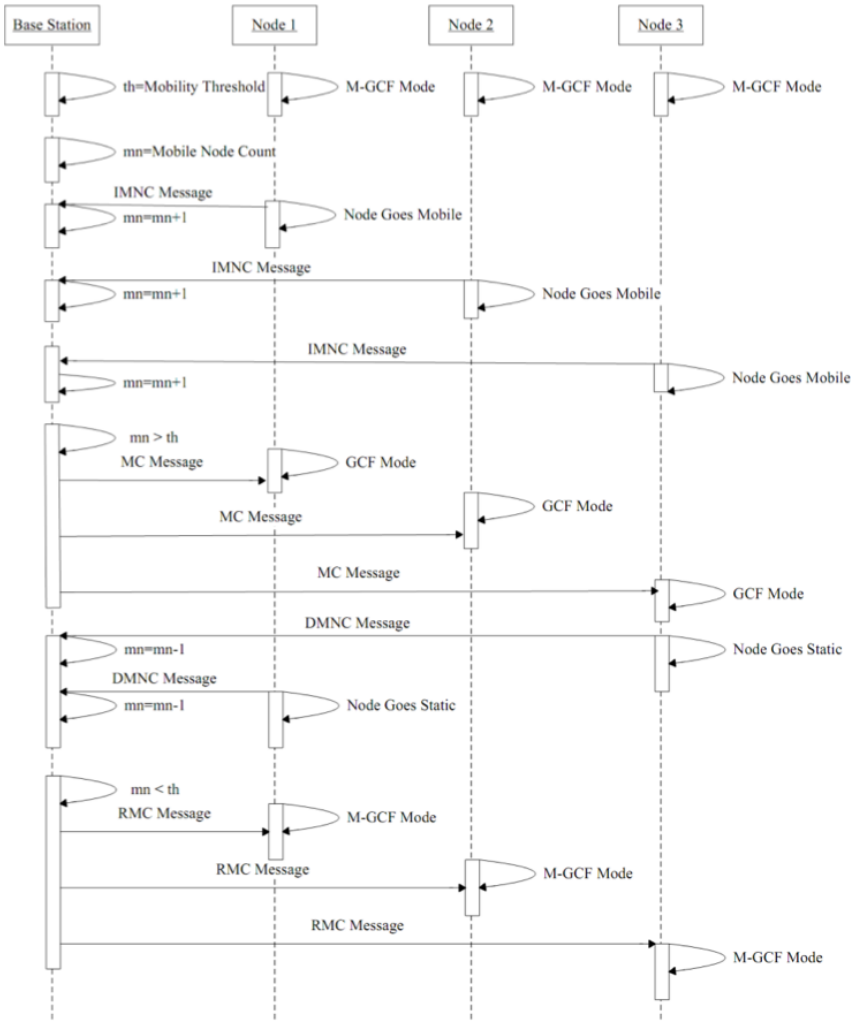


Figure 3.9: Sequence of activities in H-GCF.

- If the value of mn crosses the value of th, the network will generate a Reverse Mode Change (RMC) message and broadcast it for the node to shift mode from GCF to M-GCF.

The H-GCF algorithm assigns a single or set of conflict free single slot(s) to the nodes according to the mobility requirement of the network by considering the node functionality, the mobility threshold value and the initial mobile node count. The algorithm is divided into three phases,

- Phase 1: Set all nodes in M-GCF mode.
- Phase 2: If the node goes mobile.
- Phase 3: If the node goes static.

As illustrated in Figure 3.9 and presented in Algorithm 3, Phase 1 sets all non-BS nodes, M, in M-GCF mode, which assigns a set of slots to each node (multi-coloring). The task of Phase 2 is to check the movement status of nodes. If a node, n, becomes mobile, it sends an IMNC message to the BS, which, according to the threshold, changes the mode to GCF. Phase 3 of the algorithm is initiated, if a mobile

node, n, goes static and sends a DMNC message to the BS that considers the threshold for change of mode to M-GCF.

Algorithm 3: H-GCF algorithm to find a conflict free slot or set of slots according to the requirement of a network.

input : The graph $G(V, E)$ with $BS \in V$, $M \in (V - BS)$. th = Mobility threshold, mn = Mobile node count.

output : The nodes with non-conflicting slot or set of slots according to the requirement.

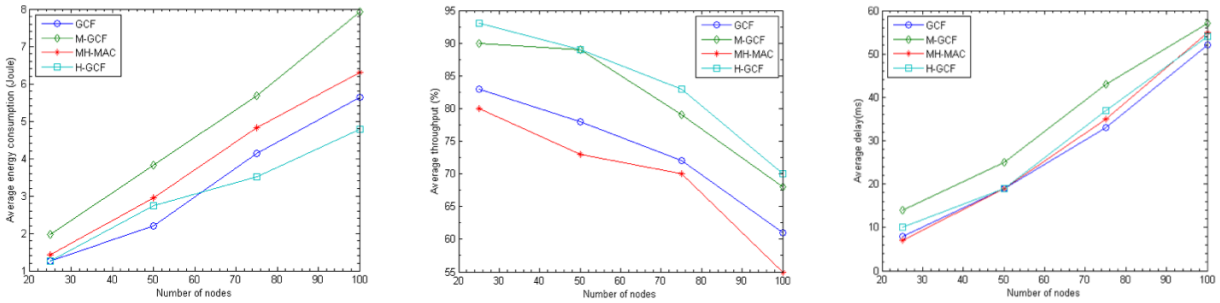
```
for the whole network running time up to T do
    for M ∈ (V − BS) do
        Assign the non-conflicting set of slots using M-GCF;
    if the node goes mobile then
        Send IMNC message to BS;
        if BS receive IMNC message then
            mn = mn + 1;
            if mn > th then
                BS will send MC message;
    for M ∈ (V − BS) receives the MC message do
        Shift the node mode to GCF and reassign the slots using GCF ;
    if the node goes static then
        Send DMNC message to BS;
        if BS receive DMNC message then
            mn = mn − 1;
            if mn < th then
                BS will send RMC message;
    for M ∈ (V − BS) receives the RMC message do
        Shift the node mode to M-GCF and reassign the slots using M-GCF;
```

3.5.4 Simulation of H-GCF

Simulation Details

To measure their performance, the single-, multi- and hybrid-color TDMA scheduling algorithms (GCF, M-GCF and H-GCF) as well as the state-of-the-art mobile MAC mechanism Mobility Adaptive Hybrid MAC (MH-MAC) are implemented in Matlab R2011b and NS-2. The parameters used for simulation are shown in Table 3.1 with the varying number of nodes in the network for checking the adaptability of the algorithms in changing network conditions. The common characteristic of the proposed algorithms is the use of multi-hop clustering in the form of EMCA [29], which is a highly scalable multi-hop clustering algorithm. The simulation considers a random waypoint mobility model [30] for generating mobility as commonly used for ad-hoc networks.

Simulations are performed under four different environments for measuring the correct performance of the algorithms to satisfy all the probable conditions of a WSN,



(a) Energy consumption. (b) Throughput. (c) Delay.

Figure 3.10: Comparative results for fixed mobility speed - all measures are averages.

1. Simulations with fixed mobility speed: This idealistic condition considers a mobility threshold of 20%, and speed of mobility as fixed at 11 km/h.

2. Simulations with random mobility speed: This more realistic or random condition considers a mobility threshold of 20% and random mobility speeds varying from 1 to 20 km/h.

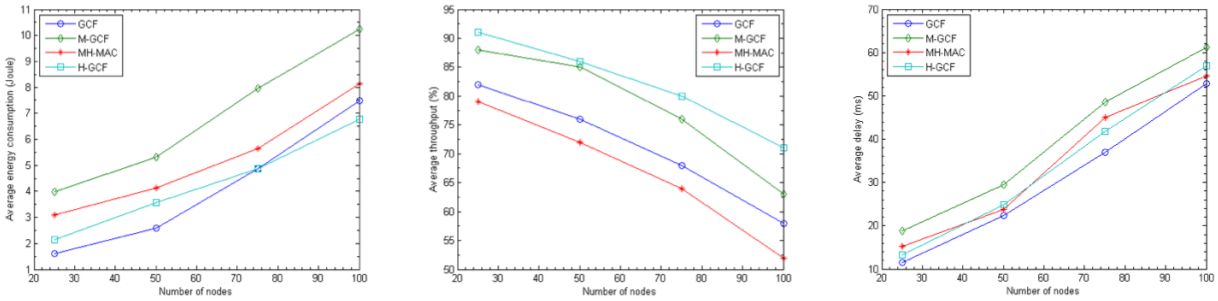
3. Simulations of H-GCF with varying mobility thresholds: To measure the performance of H-GCF under changing mobility threshold values - low as 10%, ideal as 20% and high as 50%.

4. Simulations of H-GCF by considering local mode shifts: The above three cases consider global mode shifts of the network according to mobility in the network but this case considers local mode shifts where the mode can be shifted in individual clusters. In this case, some clusters are working in GCF and some clusters are working in M-GCF. Here, mode shift decisions are transferred from the BS to the CHs and each CH maintains the mobility threshold value and shifts its mode accordingly.

Simulation Results with Fixed Mobility Speed

Figure 3.10a shows the average energy consumption of GCF, M-GCF, MH-MAC and H-GCF under varying number of nodes. The trend shows that the energy consumption of M-GCF is higher than GCF, MH-MAC and H-GCF because of the higher cost of reassignments of the multiple slots when nodes are mobile. The graph shows various patterns for GCF and H-GCF; initially the energy consumption of the two algorithms is almost identical after which GCF has lower energy consumption, but as the number of node increases, the energy consumption of H-GCF becomes lower. The reason for this is that H-GCF, as a hybrid mechanism, shifts from M-GCF mode to GCF mode according to the network requirements. However, H-GCF incurs slightly higher energy consumption compared to GCF as energy is required to transfer IMNC and DMNC messages as well as Mode Change (MC) and RMC messages used for changing the mobility status of nodes and changing the mode. MH-MAC has higher energy consumption than GCF and H-GCF due to its use of contention-based TDMA scheduling in mobile scenarios.

Figure 3.10b illustrates the trend in the average throughput and shows that the throughput of GCF is less than the other three because of the lower number of slots assigned and the increased number of conflicts. The graph shows an almost identical trend for M-GCF and H-GCF due to the increased number of slots where the performance of H-GCF is similar to or higher than M-GCF because of the shift between GCF and M-GCF mode according to the node mobility. MH-MAC shows lower throughput than the other three mechanisms because of the use of the contention-based TDMA scheduling.



(a) Energy consumption. (b) Throughput. (c) Delay.

Figure 3.11: Comparative results for random mobility speed - all measures are averages.

Figure 3.10c shows the average delay that for GCF is less than for M-GCF and H-GCF because of reduced reassignment cost (energy/sec) when nodes become mobile. M-GCF incurs greater delays compared to both GCF and H-GCF due to the increased number of slots that must be reassigned resulting in a higher energy overhead. MH-MAC shows a delay similar to GCF and H-GCF.

Simulation Results with Random Mobility

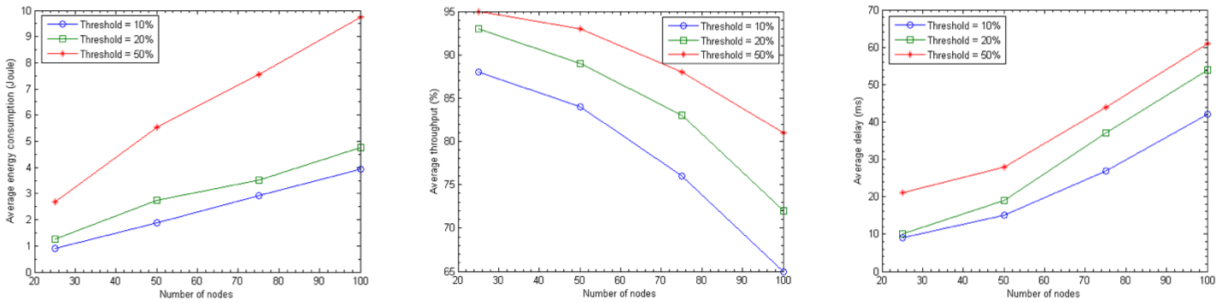
Applications of WSNs such as a Body Area Network (BAN) [31] as well as sensors in vehicles [32] and habitat monitoring call for scenarios with varying speed. The results in this subsection present a discussion for such random mobility scenarios.

Figure 3.11a, 3.11b and 3.11c show the comparative performance of H-GCF with random mobility speed. The result shows that the average energy consumption and average delays of all four algorithms are increased compared with the fixed mobility results. The energy consumption and delay of H-GCF are increased because of random mobility that adds disparity in achieving the mobility threshold value at the BS and, therefore, affects the shift of mode. The delayed shift of mode from M-GCF to GCF incurs extra energy consumption and delay. The results show a significant difference in the performance of MH-MAC in random mobility conditions because of the increased contention. The results for the average throughput show a decrease due to the randomness in the packet transmission, which leads to packet loss.

Simulation Results with varying Mobility Threshold

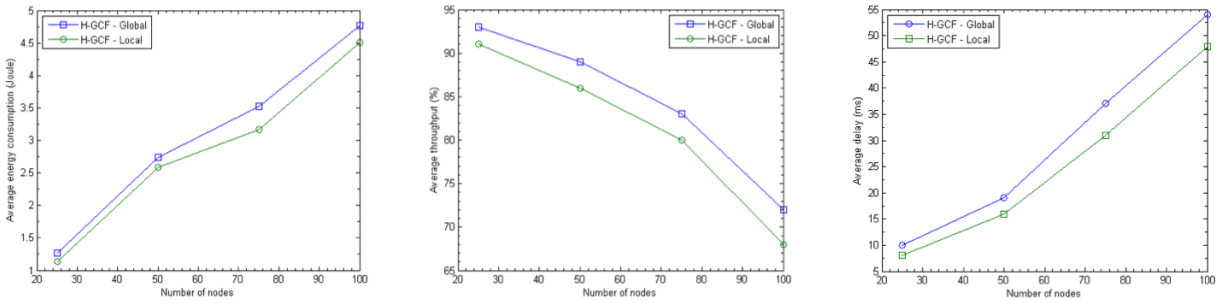
Figure 3.12a, 3.12b and 3.12c show the average energy consumption, throughput and delay of the H-GCF algorithm under three different threshold values (10%, 20% and 50%) with varying number of nodes. Figure 3.12a and 3.12c show that average energy consumption and delay are increasing with an increasing number of nodes and threshold values. The reason for the increased average energy consumption and delay is that as the number of node increases, so does the resource (energy and time) requirements, which result in an increased average energy consumption and delay. Another reason is the threshold value used, there the higher the threshold, the more the time the network will be in M-GCF mode, which leads to a higher required number of slots, and more reassignment cost (energy/sec) to assign and reassign the slots when nodes go mobile.

Figure 3.12b shows that the average throughput is reduced with an increased number of nodes because more nodes lead to more conflicts and that reduce the total utilization of the channel. The graph shows that with higher threshold values, the average throughput increases because more time is spent in M-GCF



(a) Energy consumption. (b) Throughput. (c) Delay.

Figure 3.12: Comparative results for varying mobility thresholds - all measures are averages.



(a) Energy consumption. (b) Throughput. (c) Delay.

Figure 3.13: Comparative results under local and global mode shift - all measures are averages.

mode where a more slots per node can be utilized for the transmission instead of a single slot in GCF mode. The availability of more slots to node leads to reliable transmission of packets towards the destination.

Simulation with Local Mode Shift

Figure 3.13a, 3.13b and 3.13c show the average energy consumption, delay, and throughput in case of H-GCF with both global and local mode shifts. The average energy consumption and delay of the H-GCF local shift is less than the H-GCF global mode shift, but the average throughput of H-GCF with global mode shift is more than the H-GCF local mode shift. The reason for the better energy consumption and delay in case of H-GCF local mode shift is the mixed distribution of GCF and M-GCF in one single network. Another reason for less energy consumption and delay is the distribution of mode shift responsibility among the individual CHs in the network. The mixed use of GCF and M-GCF in the network affects the average throughput of the network by distributing slots non-uniformly in the network.

3.6 Summary

TDMA scheduling is one of the principal components of any hybrid MAC mechanism for WSNs to find an efficient and conflict free schedule. The common TDMA scheduling challenges are to determine optimal conflict free schedule, improve reuse of slots and, as WSN nodes go mobile, support mobility conditions. The work of this chapter addressed these issues by analyzing the gap between the previous work and proposed three different approaches for TDMA scheduling based on graph coloring.

The first two TDMA scheduling algorithms (GCF and M-GCF) find the conflict free schedule across three-hop neighbors and show better slot sharing and reduced number of conflicts by using multi-hop

clustering and a conflict graph as input to the slot assignment. The algorithms also show better energy consumption delay, and packet delivery with varying the number of nodes in a Static-WSN (S-WSN). The research also analyzed the performance of GCF and M-GCF under mobile scenarios. Here, the single-color algorithm, GCF, is the best solution in case of high mobile scenarios and the multi-color algorithm, M-GCF, is the better solution in static and low mobile scenarios because of the high reassignment cost. In understanding the disadvantages of the previous two algorithms, the research sets the requirements for a hybrid TDMA scheduling mechanism and proposes H-GCF as a hybrid cluster-based TDMA scheduling algorithm.

H-GCF uses both the single- and multi-color algorithms and offsets their disadvantages by shifting mode from M-GCF to GCF and vice-versa according to the mobility conditions in the network. The research also determined the correct mobility threshold value for mode shift of the H-GCF algorithm. The H-GCF algorithm shows reduced energy consumption delay, and increased throughput with good scalability and adaptivity to changes in network conditions such as increase or decrease in number of nodes, percentage of mobile nodes and speed of mobile nodes. The research proved this through simulations with fixed and random mobility, and different mobility threshold by varying number of nodes in the network. The simulations of H-GCF is also performed by considering local mode shift of the network where some parts of the network is working according to single-color and the other parts in a multi-color mode. The local mode shift shows good energy consumption and lower delays compared to global mode shift.

3.7 References

[1] Giuseppe Anastasi, Marco Conti, Mario Di Francesco, and Andrea Passarella. Energy conservation in wireless sensor networks: A survey. *Ad Hoc Netw.*, 7(3):537–568, May 2009.

[2] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer Networks*, 52(12):2292 – 2330, 2008.

[3] A. Bachir, M. Dohler, T. Watteyne, and K.K. Leung. Mac essentials for wireless sensor networks. *Communications Surveys Tutorials, IEEE*, 12(2):222–248, Second 2010.

[4] Pei Huang, Li Xiao, S. Soltani, M.W. Mutka, and Ning Xi. The evolution of mac protocols in wireless sensor networks: A survey. *Communications Surveys Tutorials, IEEE*, 15(1):101–120, First 2013.

[5] P. Pawar, R. Nielsen, N. Prasad, S. Ohmori, and R. Prasad. Hybrid mechanisms: Towards an efficient wireless sensor network medium access control. In *Wireless Personal Multimedia Communications (WPMC), 2011 14th International Symposium on*, pages 1–5, Oct 2011.

[6] Ameer Ahmed Abbasi and Mohamed Younis. A survey on clustering algorithms for wireless sensor networks. *Computer Communications*, 30(14 - 15):2826 – 2841, 2007. Network Coverage and Routing Schemes for Wireless Sensor Networks.

[7] Qian Dong and W. Dargie. A survey on mobility and mobility-aware mac protocols in wireless sensor networks. *Communications Surveys Tutorials, IEEE*, 15(1):88–100, First 2013.

[8] P.M. Pawar, R.H. Nielsen, N.R. Prasad, S. Ohmori, and R. Prasad. Gcf: Green conflict free tdma scheduling for wireless sensor network. In *Communications (ICC), 2012 IEEE International Conference on*, pages 5726–5730, June 2012.

[9] P.M. Pawar, R.H. Nielsen, N.R. Prasad, S. Ohmori, and R. Prasad. M-gcf: Multicolor-green conflict free scheduling algorithm for wsn. In *Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on*, pages 143–147, Sept 2012.

[10] P.M. Pawar, R.H. Nielsen, N.R. Prasad, and R. Prasad. H-gcf: A hybrid green conflict free scheduling algorithm for mobile wireless sensor networks. In *Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on*, pages 1–5, June 2013.

[11] Sinem Coleri Ergen and Pravin Varaiya. Tdma scheduling algorithms for wireless sensor networks. *Wirel. Netw.*, 16(4):985–997, May 2010.

[12] Chih-Kuang Lin, V. Zadorozhny, P. Krishnamurthy, Ho-Hyun Park, and Chan-Gun Lee. A distributed and scalable time slot allocation protocol for wireless sensor networks. *Mobile Computing, IEEE Transactions on*, 10(4):505–518, April 2011.

[13] Injong Rhee, A. Warrier, Jeongki Min, and Lisong Xu. Drand: Distributed randomized tdma scheduling for wireless ad hoc networks. *Mobile Computing, IEEE Transactions on*, 8(10):1384–1396, Oct 2009.

[14] Chenxi Zhu and M.S. Corson. A five-phase reservation protocol (fprp) for mobile ad hoc networks. In *INFOCOM '98. Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 1, pages 322–331 vol.1, Mar 1998.

[15] R. Rozovsky and P. R. Kumar. Seedex: A mac protocol for ad hoc networks. In *Proceedings of the 2Nd ACM International Symposium on Mobile Ad Hoc Networking &Amp; Computing*, MobiHoc '01, pages 67–75, New York, NY, USA, 2001. ACM.

[16] Yu Wang and I. Henning. A deterministic distributed tdma scheduling algorithm for wireless sensor networks. In *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on*, pages 2759–2762, Sept 2007.

[17] A. Sinha and N. Das. A distributed multiple-slot assignment algorithm for wireless sensor networks. In *Computers and Devices for Communication, 2009. CODEC 2009. 4th International Conference on*, pages 1–4, Dec 2009.

[18] I. Slama, B. Shrestha, B. Jouaber, D. Zeghlache, and T.J. Erke. Dnib: Distributed neighborhood information based tdma scheduling for wireless sensor networks. In *Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th*, pages 1–5, Sept 2008.

[19] S.C. Ergen and P. Varaiya. Pedamacs: power efficient and delay aware medium access protocol for sensor networks. *Mobile Computing, IEEE Transactions on*, 5(7):920–930, July 2006.

[20] Shashidhar Gandham, Milind Dawande, and Ravi Prakash. Link scheduling in wireless sensor networks: Distributed edge-coloring revisited. *Journal of Parallel and Distributed Computing*, 68(8):1122 – 1134, 2008.

[21] Tao Wu and S. Biswas. A self-reorganizing slot allocation protocol for multi-cluster sensor networks. In *Information Processing in Sensor Networks, 2005. IPSN 2005. Fourth International Symposium on*, pages 309–316, April 2005.

[22] S. Hussain, A.S. Zahmati, and X. Fernando. Lasa: Low-energy adaptive slot allocation scheduling algorithm for wireless sensor networks. In *Sarnoff Symposium, 2009. SARNOFF '09. IEEE*, pages 1–6, March 2009.

[23] Huang Lee, A. Keshavarzian, and H. Aghajan. Multi-cluster multi-parent wake-up scheduling in delay-sensitive wireless sensor networks. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1–6, Nov 2008.

[24] Tao Wu and S. Biswas. Reducing inter-cluster tdma interference by adaptive mac allocation in sensor networks. In *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a*, pages 507–511, June 2005.

[25] Shihan Li, Depei Qian, Yi Liu, and Jie Tong. Adaptive distributed randomized tdma scheduling for clustered wireless sensor networks. In *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on*, pages 2688–2691, Sept 2007.

[26] S. Gobriel, D. Mosse, and R. Cleric. Tdma-asap: Sensor network tdma scheduling with adaptive slot-stealing and parallelism. In *Distributed Computing Systems, 2009. ICDCS '09. 29th IEEE International Conference on*, pages 458–465, June 2009.

[27] Tao Shu and Marwan Krunz. Energy-efficient power/rate control and scheduling in hybrid tdma/cdma wireless sensor networks. *Computer Networks*, 53(9):1395 – 1408, 2009.

[28] Fabian Kuhn. Local multicoloring algorithms: Computing a nearly-optimal tdma schedule in constant time. In Susanne Albers and Jean-Yves Marion, editors, *STACS*, volume 3 of *LIPIcs*, pages 613–624. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany, 2009.

[29] Ying Qian, Jinfang Zhou, Liping Qian, and Kangsheng Chen. Highly scalable multihop clustering algorithm for wireless sensor networks. In *Communications, Circuits and Systems Proceedings, 2006 International Conference on*, volume 3, pages 1527–1531, June 2006.

[30] C. Bettstetter, G. Resta, and P. Santi. The node distribution of the random waypoint mobility model for wireless ad hoc networks. *Mobile Computing, IEEE Transactions on*, 2(3):257–269, July 2003.

[31] Jiang Xing and Yunru Zhu. A survey on body area network. In *Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference on*, pages 1–4, Sept 2009.

[32] Uichin Lee, Biao Zhou, M. Gerla, E. Magistretti, P. Bellavista, and A. Corradi. Mobeyes: smart mobs for urban monitoring with a vehicular sensor network. *Wireless Communications, IEEE*, 13(5):52–57, October 2006.

Chapter 4

Synchronization Control

This chapter explains the importance of synchronization for hybrid Medium Access Control (MAC) mechanisms and proposes a cluster-based hybrid synchronization mechanism. The chapter surveys the related work in synchronization to determine the effects of synchronization on Time Division Multiple Access (TDMA) scheduling algorithm and the overall influence on hybrid MAC mechanisms. The presented proposal for cluster-based hybrid synchronization is a hybridization of tight- and loose-synchronization mechanism that is compared with state-of-the-art synchronization mechanism in static- and mobile-scenarios. The evaluation also considers the applicability of the cluster-based hybrid synchronization to Green Conflict Free (GCF), the scheduling algorithm. The evaluation results consist of measurements of synchronization overheads, energy consumption, delay, and throughput.

4.1 Introduction

Technological advancements are happening in low-cost sensors capable of performing wireless communication and data processing, but having limited processing power and computation resources. The use of these to form a Wireless Sensor Network (WSN) has increased considerably in the last few years, but the real-time requirements of certain applications stimulate different areas of research, where the resource constrained nature of WSNs is a major challenge [1].

The basic procedure in all WSN applications is to collect data from each sensor node and to form relevant information and as such time is a fundamental notion. Here, the clock of each sensor node should be synchronize with the clock of other nodes to establish a global state of information and synchronization also essential to achieve good efficiency in terms of energy and delay with reduced packet loss. Many of the crucial functions of a WSN require synchronized timescales in the network including data fusion, power management mechanisms, TDMA scheduling algorithms, and tasks in localization, security and tracking. TDMA scheduling is one of the most important schemes for hybrid MAC mechanisms and the performance of TDMA scheduling is majorly affected by the synchronization mechanism as nodes communicate within their consigned slot. Accurate operations of TDMA scheduling algorithms require all participants or nodes to have the same or at least a similar notion of time [2, 3, 4].

Existing time synchronization algorithms have the ability to estimate the time uncertainties accurately and synchronize the local clocks [2]. Even so, existing protocols are developed considering flat networks and do not sufficiently address the issues of scalability and mobility in the network, which become a major barrier to deployment as the number of nodes increases, and mobility becomes widespread transforming a WSN into a Mobile-WSN (M-WSN) [5]. The objective of the research is to develop a hybrid synchronization algorithm for cluster-based M-WSN [6]. The proposed algorithm combines sender-receiver [7] and diffusion-based [8] synchronization algorithms to achieve proficient and effective time synchronization among the nodes. It uses tight sender-receiver synchronization for inter-cluster communication and approximate (loose) diffusion synchronization for intra-cluster communication. The tight synchronization is maintained between Cluster Head (CH) and Base Station (BS) by considering the communication between them as more resource constrained [9]. The proposed algorithm shows fewer synchronization errors and improved energy efficiency with an increased number of nodes as well as reduced runtime of the algorithm. It also shows significant throughput, and reduced delays when used with a TDMA scheduling algorithm such GCF under a varying number of nodes in a static scenario, and varying speeds and percentage of mobile nodes in a mobile scenario.

Figure 4.1 shows the challenges addressed in this chapter and modules of research explored specific to synchronization control including energy-, delay-, and throughput-efficiency, scalability, and mobility support. The remainder of the chapter is structured as follows. Section 4.2 describes the related work in synchronization with advantages and disadvantages of tight and loose synchronization algorithms with future requirements. Section 4.3 proposes the hybrid synchronization algorithm with assumptions, system model, problem statement, methodology and details of the mechanism. Section 4.4 presents the simulation results of the proposed algorithm compared with the state-of-the-art solutions and, lastly, Section 4.5 summarizes the contributions of the chapter.

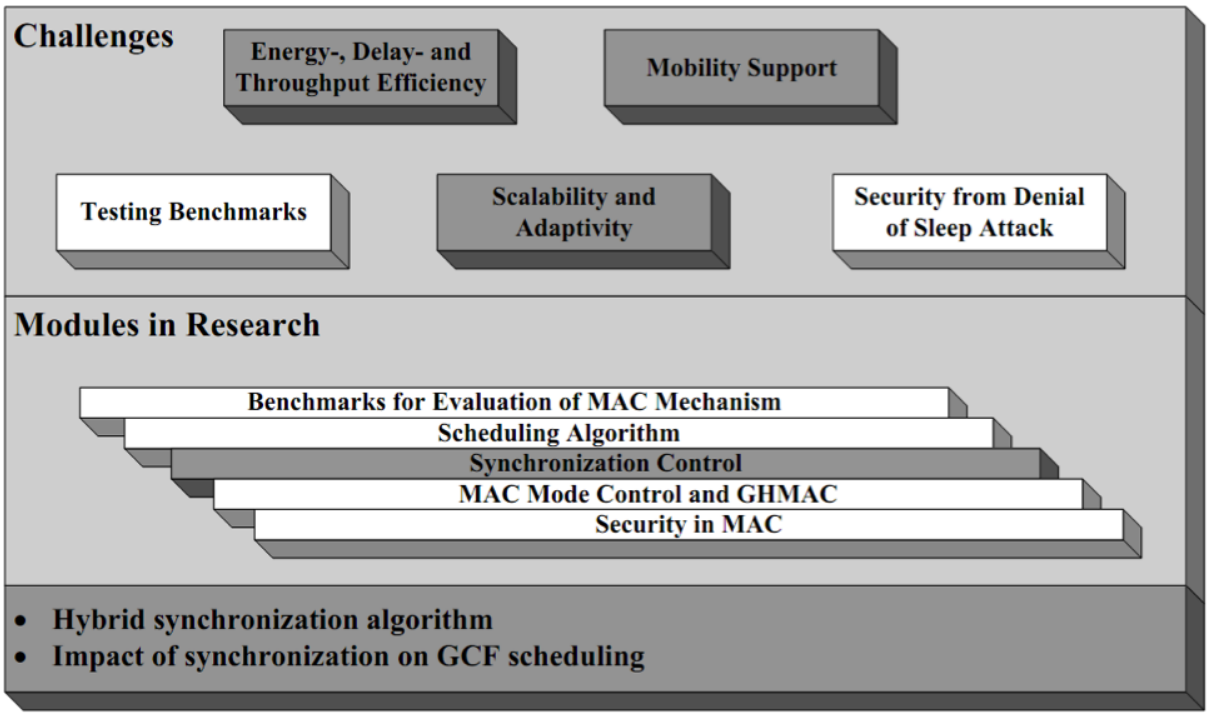


Figure 4.1: Chapter 4 contributions.

4.2 Related Work

The synchronization of clocks is a major issue in WSNs, to cope with unreliable network transmission and unbounded message latencies. The degradation or errors in synchronization accuracy result in degradation of system performance and, hence, the synchronization is considered as a crucial constraint to support different real-time applications.

This issue is addressed by using master-slave-, peer-to-peer-, deterministic-, probabilistic-, sender-receiver-, receiver-receiver-, internal-, external-, and diffusion-based synchronization approaches [2]. The master-slave synchronization protocol considers one node as a master and other nodes in the network as slaves. Here, a slave's clock is synchronized according to master clocks. These protocols are simple, non-redundant, and scalable, but require centralized control and introduce a significant amount of processing overheads [10]. The peer-to-peer mechanisms synchronize the clock by communicating with each node in the network. They remove the risk of master node failure by offering peer-to-peer configuration flexibility. The weakness of peer-to-peer synchronization is difficulty in control, increased overheads due to peer-to-peer message exchange for synchronization decisions, and less adaptability to network changes [11, 12].

Most of the approaches in synchronization are deterministic as they guarantee an upper bound on the clock offset with some diffusion [13]. These methods involve additional processing and forces more data transfers for synchronization decisions. The advantages of deterministic methods are that they are controlled by probabilistic approaches reducing the extra message overheads and guarantee a maximum clock offset with a failure probability [14].

In sender-to-receiver synchronization, the sender sends a local timestamp to the receiver after a certain interval and the receiver synchronizes its clock with the received timestamp. The variation in the received message delays leads to the imperfection of clocks [15]. The receiver-to-receiver synchronization reduces

the message delay variance. Here, receivers' exchange messages at the same time and calculate the time offsets based on the difference in reception times. These mechanisms are vulnerable to propagation delay differences at the receiver side.

Internal synchronization mechanisms do not support global time-based synchronization with nodes from within the system, but each node synchronizes itself by minimizing the maximum difference between local clocks of the sensors [16]. External synchronization references real-world time externally where the local clocks of the system are synchronized according to a real-world reference time. These protocols are not suitable for WSNs as they consume a significant amount of energy to synchronize the clocks [17]. The majority of these approaches are tight synchronization approaches, which are expected to have perfect synchronization among the nodes.

The advantages of tight synchronization algorithms are protocol scalability and the synchronization accuracy, which do not degrade significantly as the size of the network increases. They are not particularly effective in terms of energy conservation, as they require physical clock correction. They are also disadvantageous in terms of multi-hop and mobility support [2, 5]. Loose synchronization algorithms, on the other hand, are advantageous in terms of tolerant message losses and maintains system-wide equilibrium time between all nodes. These algorithms are also beneficial in terms of mobility support, but lead to high complexity because multiple masters initiate diffusion broadcast. The convergence time becomes high when no external precise timeservers are used. Here, it is possible that the clock run backward to adjust the lower value to equilibrium time [2, 5].

Recent research in synchronization algorithms has been focused on hybrid synchronization mechanism combining two or more approaches. Hybrid Energy Aware Time Synchronization (HEATS) [17] combines Reference Broadcast Synchronization (RBS) and Timing-sync Protocol for Sensor Network (TPSN) to minimize the amount of transmissions required to synchronize an entire network. HEATS allows nodes to synchronize among themselves within a few microseconds of each other to save a significant amount of energy. This synchronization method works better for smaller number of nodes; its performance falls as the number of nodes in the network increases. Cluster-Based Hierarchical Flooding Time Synchronization (CBH-FTS) [18] is a hybrid synchronization algorithm, which combines Flooding Time Synchronization Protocol (FTSP) and TPSN. Here, the root node multicasts the time-sync message to selected CHs instead of flooding the synchronization messages to neighbor nodes. The protocol mechanism is concerned with a specific context driven semantics for synchronization, which increases the overheads during the synchronization decisions. The scheme is developed by considering only one hierarchy of clustered networks. Thus, it is not suitable for large-scale network hierarchies. The cluster-based hybrid synchronization scheme uses RBS for CHs synchronization using actor node and intra-cluster synchronization using the Round Trip Synchronization (RTSync) technique [19]. The scheme reduces the energy consumption and delay. The scheme uses piggybacking and an event ordering mechanism for achieving the synchronization, which increases the overheads of the synchronization system. The scheme is suited for the resource scarceness of WSN in contrast to schemes that use global time scales.

The advantages and disadvantages of the above stated synchronization algorithms show that there is a requirement for more scalable, accurate, message tolerant, energy efficient and mobility supported synchronization algorithms. In addition, the study of the hybrid synchronization algorithms shows that the currently available hybrid synchronization algorithms are usually a combination of different tight synchronization mechanisms. These hybrid mechanisms are not suitable for WSN where there are

requirements for network scalability and nodes in the network are mobile with varying speed. The above objectives are difficult to achieve efficiently solely using a tight synchronization mechanism. Hence, to address this problem, this research works proposes a hybrid synchronization approach which combines the features of both tight synchronization i.e. TPSN and loose synchronization i.e. Time Diffusion Protocol (TDP).

4.3 Cluster-based Hybrid Synchronization for WSNs

4.3.1 Assumptions and System Model

It is assumed that all nodes have similar capabilities and equal importance. Each sensor node has a unique identifier and all sensor nodes are deployed densely. There exists a single BS in the network that is considered static and the network is divided into a cluster; every cluster has CH and cluster members. CHs and nodes are assumed either static or mobile according to the requirement. Every sensor node has its own clock triggered by a crystal oscillator that gives the node the only notion of time. Clusters are considered multi-hop to achieve better energy efficiency and scalability. There are mixed links, unidirectional and bidirectional links and the network has a burst of activities.

The network is represented by the graph $G(V, E)$ where V is the set of nodes and E is the set of links. G is divided into different subgraphs or cliques, $G = G_1, G_2, \ldots, Gn$ and each clique is considered a cluster; formed using a multi-hop clustering algorithm. Performing clustering on a WSN deployment prior to synchronization has two advantages. First, it creates a regular pattern from which synchronization information is extracted. Second, it reduces the amount of communication overheads [20]. The system model considers that the nodes in the cluster synchronize with the timing of CHs and all CHs are to be synchronized with the timing of the BS. The application considered in developing the system model considers certain tolerances throughout the lifetime of the network. The model assumes that a certain tolerance of time is allowed in between cluster members and CHs.

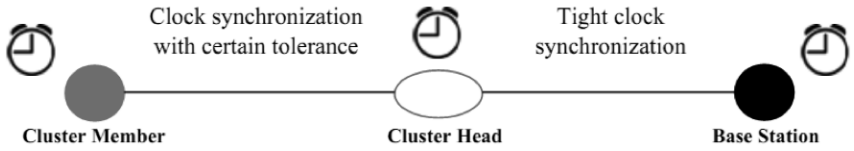


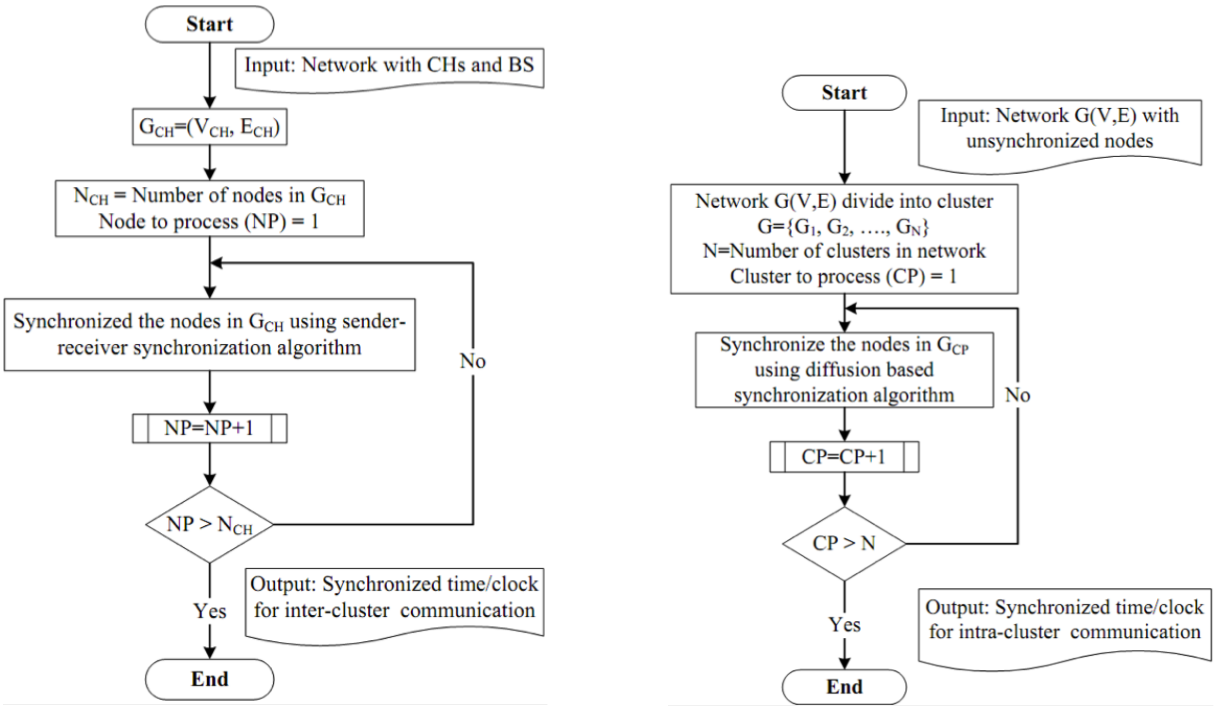
Figure 4.2: Clock synchronization.

4.3.2 Hybrid Synchronization Mechanism

The proposed synchronization mechanism is a hybrid approach as a combination of the following two approaches (Figure 4.2 shows the clock synchronization in the proposed algorithm):

- Sender-receiver synchronization [1, 5] between BS and CHs provides higher accuracy and better scalability.

- Diffusion-based synchronization [1, 6] between CHs and cluster members reduces energy consumption and improves message tolerance.



(a) Inter-cluster.

(b) Intra-cluster.

Figure 4.3: Synchronization flow diagrams.

Figure 4.3a shows a flow diagram of the inter-cluster synchronization phase. The inter-cluster synchronization phase takes the graph $G_{CH} = (V_{CH}, E_{CH})$ as input where V_{CH} is the set of CHs and the BS in the network and E_{CH} is the set of edges connecting the CHs and the BS. The next steps synchronize each CH with the BS and collect the correct timing information from the BS to synchronize the clock with that of the BS. The two phases of the synchronization are level discovery and the actual synchronization. During the level discovery phase, the root node, BS, is assigned level 0 and broadcasts the $level\_discovery$ packet where it incorporates the identity and level of the sender. The neighboring CHs receive this packet and assign a level incremented of 1 compared to the received level. Once they have their level assigned, the CHs broadcast a new $level\_discovery$ packet containing their own level. The process continues until all CHs in the network have their level assigned. Any received level higher than the already assigned level is ignored.

In the synchronization phase, the CHs are synchronized with the BS using a two-way message exchange performed along each edge of the hierarchical structure established in the level discovery phase. CHs which are neighboring tthe BS send a $synchronization\_pulse$ packet to the BS. The packet contains the level of the CH and a value of time, T_1. The BS receives this packet at a time, T_2, where $T_2 = T_1 + \Delta + d$ and Δ and d represent the clock drift between the two nodes and the propagation delay respectively. At time T_3, the BS sends an acknowledgment packet to the CH along with the values of T_1, T_2 and T_3. The CH receives the packet at T_4 and, by knowing the clock drift, the CH corrects its clock accordingly so that it is synchronized with the BS. CHs that are not neighboring to the BS synchronize with their neighboring CHs, which are already synchronized.

Figure 4.3b shows the intra-cluster synchronization phase. The intra-cluster synchronization phase assumes that the network $G(V, E)$ is divided into the number of clusters, G_{CP}. In addition, it assumes that the CHs in each cluster, G_{CP}, are already synchronized with the inter-cluster synchronization phase. The

individual cluster members in each cluster, G_{CP} synchronize using the diffusion-based synchronization algorithm. The diffusion-based synchronization algorithm diffuses the clocks of the cluster members in the cluster, G_{CP}, to the clock value of the CH_{CP} by allowing a certain tolerance ranging randomly from 10s to 60s from the ideal time. Here, CH_{CP} is considered the leader of the cluster, CP, and the cluster members synchronize with it. Therefore, no particular election/re-election procedure for choosing a leader is required.

4.4 Simulation Results

The simulation of the algorithm is performed using Network Simulator-2. The parameters considered for the simulation are as shown in Table 4.1 and the simulation considers the WSN nodes to be deployed uniformly randomly in an area of 100m by 100m.

Table 4.1: Parameters for synchronization algorithm simulation

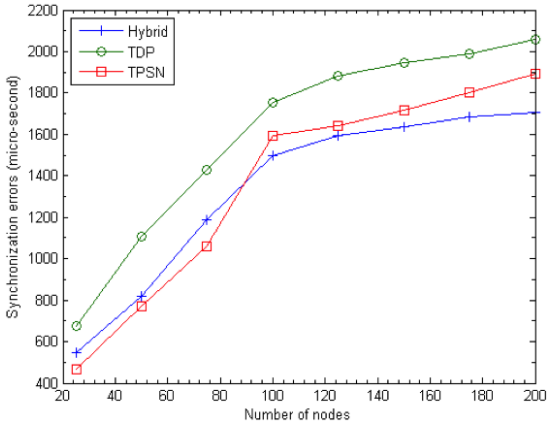
Parameters	**Setting used**
Number of nodes	25, 50, 75, 100, 125, 150, 175, and 200
Number of sources	24, 49, 74, 99, 124, 149, 174, and 199
Number of BS	1
Placement of nodes and BS	Nodes are placed randomly in a given area, and the BS is positioned in the middle of a given area.
Initial energy (Joule)	100
Propagation model	Two-ray Ground
Traffic model	Constant Bit Rate
Idle power (mW)	14.4
Receiving power (mW)	21.0
Transmission power (mW)	14.4
Number of simulation runs	50
Mobility model	Random waypoint [21]
Clustering algorithm	Enhanced Multihop Clustering Algorithm (EMCA) [22]

The proposed hybrid synchronization algorithm is compared with sender-receiver synchronization algorithm TPSN [5] that is widely used and efficient sender-receiver time synchronization algorithm and with time diffusion synchronization algorithm TDP [6] that allows some level of tolerance within the network synchronization. The performance of the hybrid synchronization algorithm is measured in the following three ways,

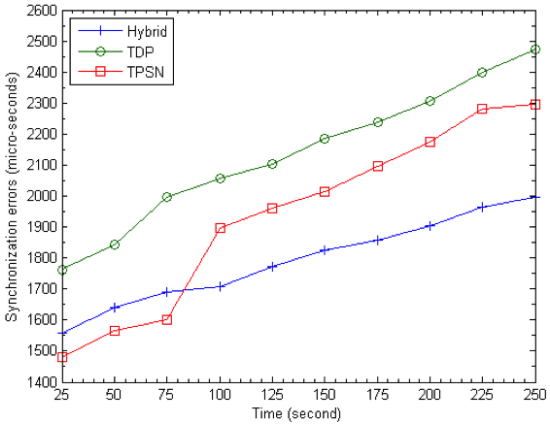
- Measurement in terms of synchronization overheads where the performance measure is used to determine the synchronization overheads, synchronization errors and energy needed for synchronization.
- Performance evaluation under static scenarios using GCF in terms of measurement for average energy efficiency, average delay, and throughput by varying number of nodes in the network.
- Performance evaluation under mobile scenarios using GCF with varying mobility percentage and mobility speed.

4.4.1 Performance in Terms of Synchronization Overheads

Figure 4.4a shows the synchronization errors with varying number of nodes in case of the three different synchronization algorithms TPSN, TDP and the proposed hybrid algorithm. The synchronization errors in

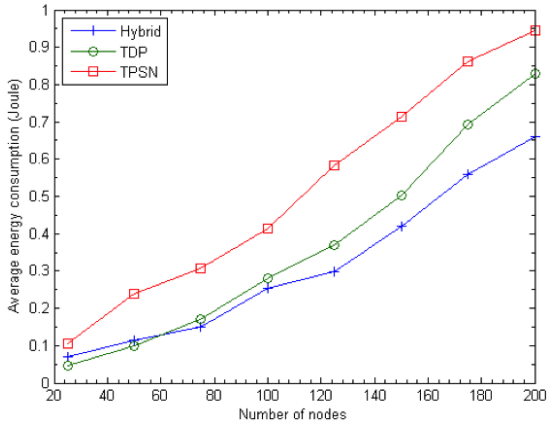


(a) As a function of number of nodes.

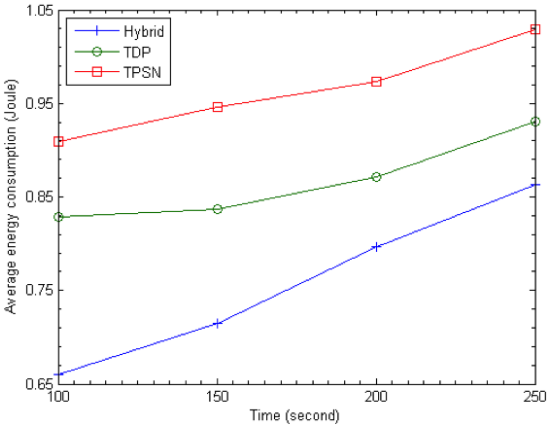


(b) As a function of time.

Figure 4.4: Synchronization errors during network synchronization.



(a) As a function of number of nodes.

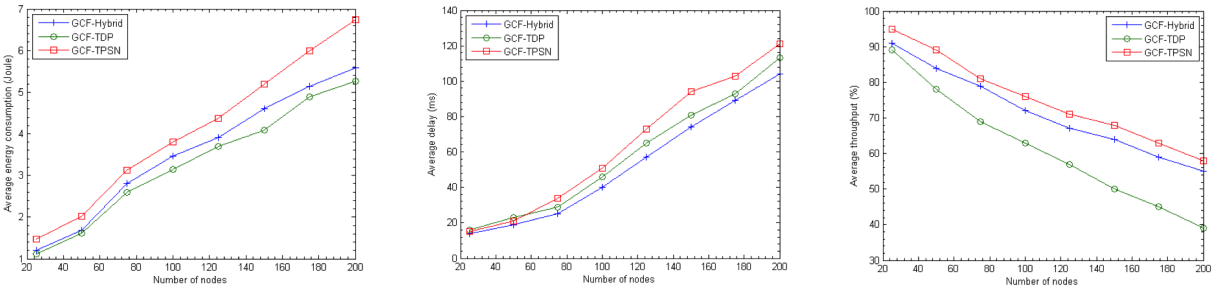


(b) As a function of time.

Figure 4.5: Average energy consumption during network synchronization.

case of the hybrid synchronization algorithm are in-between the errors of TDP and TPSN. This situation changes as the number of nodes increases and it becomes difficult to maintain the perfect synchronization in the network with 90 nodes being the value the proposed algorithm outperforms the two others in terms of synchronization errors. Here, TDP has more synchronization errors than TPSN because it does not synchronize the clock perfectly; it synchronizes the clock by keeping some tolerance. The reason for the proposed algorithm's reduced synchronization error is the use of diffusion-based synchronization inside the cluster and the use of sender-receiver synchronization in between the CHs and BS, and not for the whole network, which helps to reduce the synchronization errors. Figure 4.4b shows the synchronization errors with varying time for 200 nodes. The trends are similar to the ones for varying number of nodes showing the proposed hybrid algorithm to outperform TDP and TPSN over time as these have difficulties in maintaining the synchronization. The hybrid synchronization algorithm shows balanced synchronization errors both with varying number of nodes and varying time.

Figure 4.5a and 4.5b show the average energy consumption for the three synchronization algorithms with varying number of nodes and time (for 200 nodes) respectively. The result indicates that the performance of TPSN is worse than the other two algorithms the main reason being the amount of messages it generates to maintain the tight time synchronization across the network. TDP shows lower



(a) Average energy consumption. (b) Average delay. (c) Average throughput.

Figure 4.6: Results for synchronization algorithms under static scenarios.

energy consumption than TPSN and also gives lower energy consumption than the hybrid synchronization algorithm up till 50 nodes. The reason for the improved energy consumption in case of TDP is that it does not rely upon individual sensor nodes to be a master node; it enables the network time to attain an equilibrium value by entirely a diffusion process. The hybrid synchronization algorithm optimizes the average energy consumption by balancing the role of sender-receiver- and time diffusion-synchronization. The sender-receiver synchronization is used only for a small number of nodes, i.e. in between CHs and BS (CH+BS < Number of nodes in all clusters) while the time diffusion algorithm is used for synchronizing cluster members. Another reason for showing lower energy consumption is that the hybrid algorithm allows the sensor nodes to maintain a similar time within a certain tolerance throughout the network.

4.4.2 Performance Comparison under Static Scenarios

Figure 4.6a, 4.6b and 4.6c show the performance of GCF under the three different synchronization algorithms.

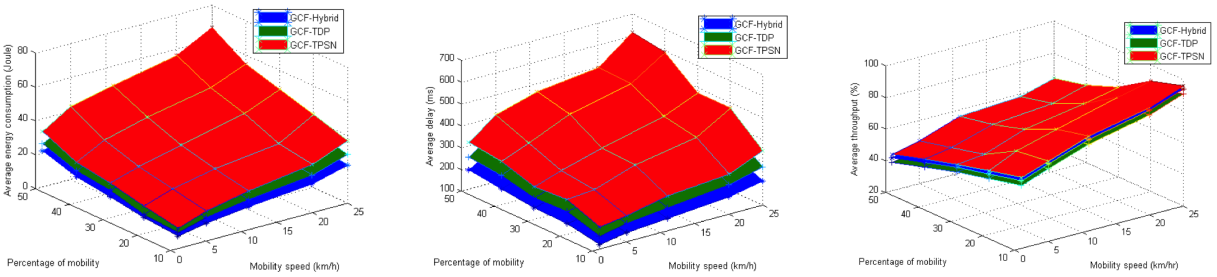
Figure 4.6a shows that the average energy consumption of the hybrid synchronization algorithm is in between the average energy consumption of TDP and TPSN. The average energy consumption of the hybrid synchronization algorithm is lower with a reduced number of nodes, but it increases with number of nodes due to the hybrid mechanism used.

Figure 4.6b shows that the average delays of the hybrid synchronization algorithm and TDP are lower than for TPSN as TPSN is not utilizing any approximate synchronization. Here, the average delay of TDP is better than the hybrid synchronization algorithm because the hybrid synchronization algorithm combines both perfect and approximate synchronization to minimize delays at synchronization and communication which results in a combined reduction of average delays.

Figure 4.1 shows the average throughput where TPSN is better than other two with the hybrid synchronization algorithm being in between TPSN and TDP. TPSN is better performing as it uses tight synchronization which helps to keep the uniform throughput while in the case of the hybrid algorithm some nodes are keeping tolerance in synchronization of nodes and in TDP all nodes are keeping tolerance in synchronization, which affects the total throughput of the network.

4.4.3 Performance Comparison under Mobile Scenarios

Figure 4.7a and Figure 4.7b show mesh graphs of average energy consumption and delay respectively, with varying percentage of mobile nodes and mobility speed. The meshes illustrate that the energy consumption and delays in case of GCF with TPSN are more than the other two algorithms due to its strict



(a) Average energy consumption. (b) Average delay. (c) Average throughput.

Figure 4.7: Results for synchronization algorithms under mobile scenarios.

synchronization. It is difficult to maintain a strict synchronization among all nodes in a mobile network and energy will be wasted for performing synchronization among the nodes and significant amount of delay occur when re-running the synchronization algorithm due to changes in the network. In the case of TPSN, it is observed that the number of conflicts is increased because of un-synchronized nodes due to mobility, which leads to increase in energy consumption and delay. TDP performs better due to its approximate synchronization. However, the performance of the hybrid algorithm is outperforming the other two because it allows keeping strict synchronization among the clusters and loose or approximate synchronization inside the cluster. It maintains proper synchronization between CHs, which reduces energy consumption and delay. The entirely loose synchronization of TDP leads to communication overheads in terms of loss of packets and retransmission of lost packets that increase energy consumption and delay.

Figure 4.7c shows the throughput of the the three algorithms where TPSN shows good throughput because of its perfect synchronization while TDP shows lowest throughput because of its loose synchronization and the the hybrid algorithm gives an equilibrium throughput as expected.

4.5 Summary

Synchronization of time is a significant block of any hybrid MAC mechanism, as nodes have to synchronize with the same time during the TDMA scheduling phase. The synchronization is also an important parameter to apply hybrid MAC mechanisms in real time applications of WSNs. An efficient synchronization algorithm should be lightweight, less error prone, and energy efficient. It should also be scalable and adaptable to changes in conditions of the network, such as an increase in number of nodes and mobility in WSN.

The chapter has given a detailed survey of related work in synchronization algorithms for WSN showing that synchronization mechanisms are majorly classified into tight- and loose-synchronization algorithms. Each of which has problems in terms of timing error, energy efficiency, scalability, and adaptivity. Hence, the chapter presents a hybrid synchronization algorithm for cluster-based M-WSN.

The hybrid synchronization algorithm combines the tight- and loose-synchronization algorithms to enhance the efficiency of the synchronization algorithm. It uses tight sender-receiver synchronization for inter-cluster communication and loose diffusion synchronization for intra-cluster communication. The proposed scheme is useful for scalability, energy efficiency, fault-tolerance, and mobility support.

The chapter also presented a comparative evaluation of the proposed hybrid synchronization algorithm showing fewer synchronization errors and better energy efficiency with varying number of nodes and

time. The algorithm's efficiency is compared with state-of-the-art and widely used sender-receiver- and diffusion-synchronization algorithms. The presented hybrid synchronization algorithm is also verified for its applicability to the TDMA scheduling algorithm using GCF. The applicability of the hybrid synchronization with TDMA scheduling is evaluated in both static and mobile scenarios and the results show that the performance of TDMA scheduling is enhanced in the presence of the hybrid synchronization algorithm, as compared with other synchronization algorithms. The hybrid synchronization mechanism has good energy efficiency, decreased delay and better throughput in a Static-WSN (S-WSN) scenario and is able to adapt when changing the percentage of node mobility and speed of a node in a M-WSN scenario.

4.6 References

[1] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer Networks*, 52(12):2292 – 2330, 2008.

[2] Bharath Sundararaman, Ugo Buy, and Ajay D. Kshemkalyani. Clock synchronization for wireless sensor networks: A survey. *Ad Hoc Networks (Elsevier*, 3:281–323, 2005.

[3] Erchin Serpedin and Qasim M. Chaudhari. *Synchronization in Wireless Sensor Networks: Parameter Estimation, Peformance Benchmarks, and Protocols*. Cambridge University Press, New York, NY, USA, 1st edition, 2009.

[4] P.M. Pawar, R.H. Nielsen, N.R. Prasad, S. Ohmori, and R. Prasad. Gcf: Green conflict free tdma scheduling for wireless sensor network. In *Communications (ICC), 2012 IEEE International Conference on*, pages 5726–5730, June 2012.

[5] Isaac Amundson and Xenofon D. Koutsoukos. A survey on localization for mobile wireless sensor networks. In *Proceedings of the 2Nd International Conference on Mobile Entity Localization and Tracking in GPS-less Environments*, MELT'09, pages 235–254, Berlin, Heidelberg, 2009. Springer-Verlag.

[6] Ameer Ahmed Abbasi and Mohamed Younis. A survey on clustering algorithms for wireless sensor networks. *Computer Communications*, 30(14 - 15):2826 – 2841, 2007. Network Coverage and Routing Schemes for Wireless Sensor Networks.

[7] Saurabh Ganeriwal, Ram Kumar, and Mani B. Srivastava. Timing-sync protocol for sensor networks. In *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems*, SenSys '03, pages 138–149, New York, NY, USA, 2003. ACM.

[8] Weilian Su and I.F. Akyildiz. Time-diffusion synchronization protocol for wireless sensor networks. *Networking, IEEE/ACM Transactions on*, 13(2):384–397, April 2005.

[9] P.M. Pawar, R.H. Nielsen, N.R. Prasad, and R. Prasad. A hybrid algorithm for efficient wireless sensor network time synchronization. In *Wireless Communications, Vehicular Technology, Information Theory and Aerospace Electronic Systems (VITAE), 2014 4th International Conference on*, pages 1–5, May 2014.

[10] S. Ping. IRB TR-03-013: Delay Measurement Time Synchronization for Wireless Sensor Networks. Technical report, Intel Research, June 2003.

[11] Kay Römer. Time synchronization in ad hoc networks. In *Proceedings of the 2Nd ACM International Symposium on Mobile Ad Hoc Networking &Amp; Computing*, MobiHoc '01, pages 173–182, New York, NY, USA, 2001. ACM.

[12] Qun Li and Daniela Rus. Global clock synchronization in sensor networks. In *IEEE Transactions on Computers*, pages 214–226, 2004.

[13] M.L. Sichitiu and C. Veerarittiphan. Simple, accurate time synchronization for wireless sensor networks. In *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE*, volume 2, pages 1266–1273 vol.2, March 2003.

[14] G. J. Pottie and W. J. Kaiser. Wireless integrated network sensors. *Commun. ACM*, 43(5):51–58, May 2000.

[15] Jeremy Elson, Lewis Girod, and Deborah Estrin. Fine-grained network time synchronization using reference broadcasts. *SIGOPS Oper. Syst. Rev.*, 36(SI):147–163, December 2002.

[16] M. Mock, R. Frings, E. Nett, and S. Trikaliotis. Continuous clock synchronization in wireless real-time applications. In *Reliable Distributed Systems, 2000. SRDS-2000. Proceedings The 19th IEEE Symposium on*, pages 125–132, 2000.

[17] D.L. Mills. Internet time synchronization: the network time protocol. *Communications, IEEE Transactions on*, 39(10):1482–1493, Oct 1991.

[18] Yanjing Sun, Jiansheng Qian, and Jinlei Wu. Hybrid energy-aware time synchronization protocol for wsns in coal mine. In *Information Acquisition, 2007. ICIA '07. International Conference on*, pages 436–441, July 2007.

[19] P. Yadav, N. Yadav, and S. Varma. Cluster based hierarchical wireless sensor networks (chwsn) and time synchronization in chwsn. In *Communications and Information Technologies, 2007. ISCIT '07. International Symposium on*, pages 1149–1154, Oct 2007.

[20] Dong Shao-Long and Xing Tao. Cluster-based power efficient time synchronization in wireless sensor networks. In *Electro/information Technology, 2006 IEEE International Conference on*, pages 147–151, May 2006.

[21] C. Bettstetter, G. Resta, and P. Santi. The node distribution of the random waypoint mobility model for wireless ad hoc networks. *Mobile Computing, IEEE Transactions on*, 2(3):257–269, July 2003.

[22] Ying Qian, Jinfang Zhou, Liping Qian, and Kangsheng Chen. Highly scalable multihop clustering algorithm for wireless sensor networks. In *Communications, Circuits and Systems Proceedings, 2006 International Conference on*, volume 3, pages 1527–1531, June 2006.

Chapter 5

GHMAC: Green and Hybrid Medium Access Control

This chapter discusses state-of-the-art related work in hybrid Medium Access Control (MAC) mechanisms and design blocks of Green and Hybrid MAC (GHMAC) with the key contribution of MAC mode control, which is useful to shift MAC mode from Carrier Sense Multiple Access (CSMA) to Time Division Multiple Access (TDMA) and vice versa. GHMAC uses TDMA scheduling utilizing Green Conflict Free (GCF), synchronization using the proposed cluster-based hybrid synchronization, and the proposed MAC mode control. GHMAC is evaluated under static and mobile scenarios including security and its performance is compared with state-of-the-art hybrid MAC mechanisms. The security scenarios consider the evaluation of GHAMC under different types of denial of sleep attack. The performance evaluation shows improved energy-, throughput-, and delay-efficiency with increased scalability.

5.1 Introduction

A hybrid MAC mechanism has three important pillars; scheduling algorithm, synchronizations, and MAC mode control mechanism, as shown in Figure 5.1 [1], and a good hybrid MAC mechanism should be energy- and delay-efficient, have good channel utilization, and be scalable and adaptive to changing conditions in the network. Currently available hybrid MAC mechanisms are not sufficiently adaptable and scalable when considering the network environment during mobility and an increase in number of nodes [1, 2, 3, 4].

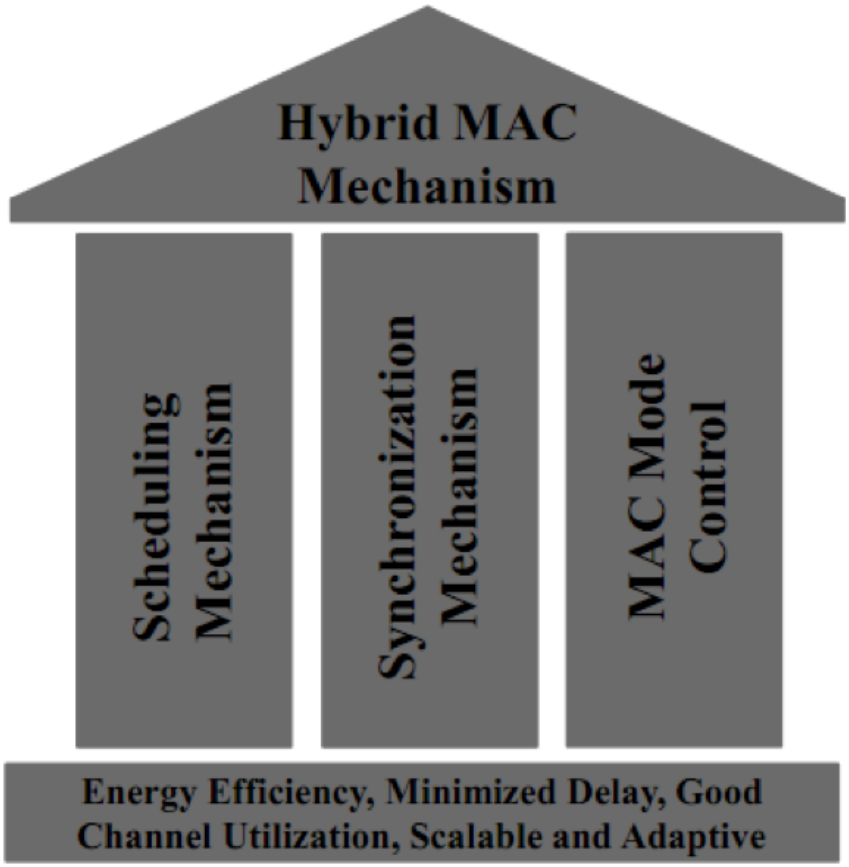


Figure 5.1: Pillars of hybrid MAC mechanism.

The chapter presents a novel hybrid MAC mechanism, GHMAC [5], based on the advantages and disadvantages of currently available hybrid MAC mechanisms. GHMAC is a cluster-based hybrid MAC mechanism as it uses a schedule-based MAC mechanism for inter-cluster communication and a mix of contention- and schedule-based MAC mechanisms for intra-cluster communication based on the level of collisions in the cluster. As such, the algorithm improves the overall efficiency of a Wireless Sensor Network (WSN). GHMAC uses GCF [6] as scheduling algorithm as presented in Chapter 3, which efficiently finds three-hop conflict free schedules in a multi-hop cluster-based network [7]. The synchronization used in GHMAC considers a hybrid synchronization [8], which is presented in Chapter 4, using tight synchronization for inter-cluster communication (sender-receiver synchronization) [9] and approximate synchronization for intra-cluster communication (diffusion-based synchronization) [10]. This reduces the synchronization overheads through fewer synchronization errors, which leads to improved energy efficiency. The last important pillar of a hybrid MAC mechanism is MAC mode control and here

GHMAC applies collision threshold-based MAC mode control for changing the mode from contention-based to schedule-based and vice-versa based on the collisions in the network.

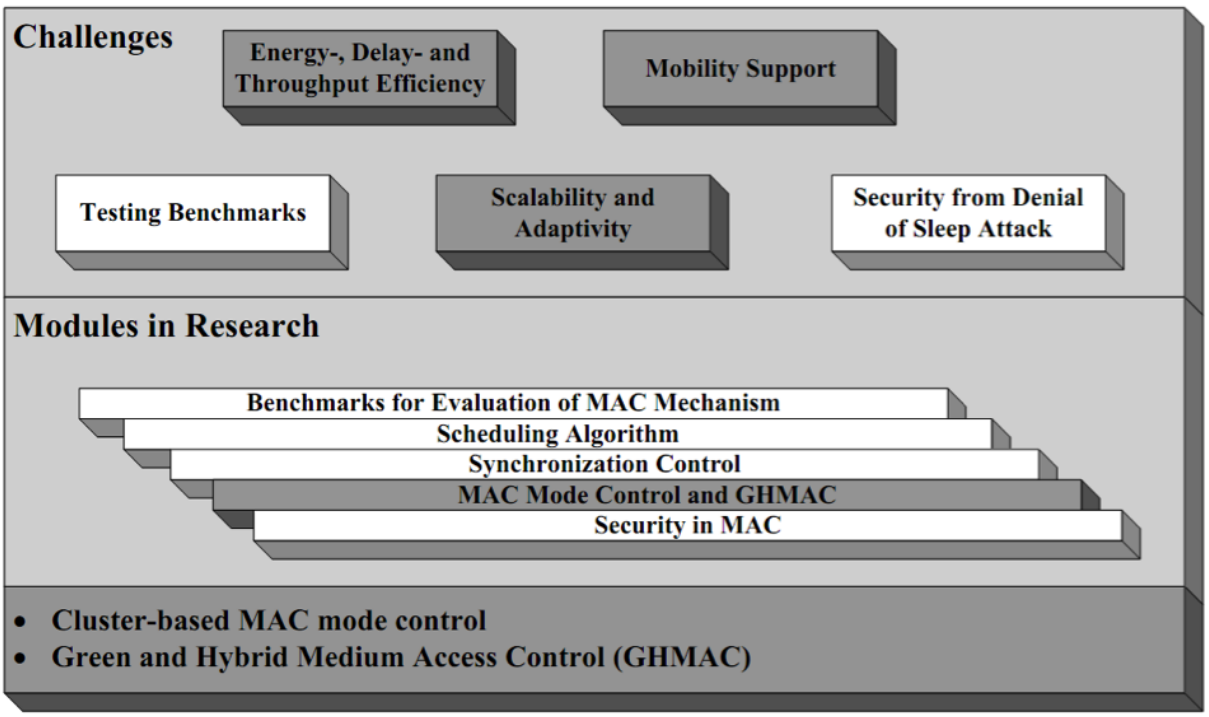


Figure 5.2: Chapter 5 contributions.

GHMAC is evaluated in different scenarios including static and mobile scenarios and also scenarios with security. In the static scenarios, the evaluation is done with varying collision thresholds, number of nodes and area of the network. The mobile scenarios include varying percentage of mobile nodes and mobility speed in the network. The security scenarios consider performance under various denials of sleep attacks. The result shows that GHMAC has better energy efficiency, higher throughput, and lower delays and that it is scalable and adaptable to changing network conditions, as compared with the state-of-the-art hybrid MAC mechanisms.

Figure 5.2 shows the contributions described in Chapter 5. The first contribution of the chapter is a cluster-based MAC mode control, and the next part is assembling all blocks of the hybrid MAC mechanism and forming the new hybrid MAC mechanism: GHMAC. GHMAC addresses the WSN MAC mechanism challenges identified in the thesis.

The remainder of the chapter is organized as follows. Section 5.2 presents the related work in hybrid MAC mechanisms with the scheduling and synchronization used, the MAC mode control and the advantages and disadvantages of. Section 5.3 describes the different blocks of the GHMAC mechanism in short, and discusses the MAC mode control mechanism in detail. Section 5.4 presents the simulation results of GHMAC under the different scenarios. Section 5.5 provides a summary of the chapter.

5.2 Related Work

Zebra MAC (ZMAC) [11] is a widely used hybrid MAC mechanism for WSNs, which dynamically adjust the behavior of the MAC mechanism to utilize either CSMA or TDMA depending on the level of contention in the network. ZMAC starts with a setup phase consisting of neighbor discovery, slot assignment, local

frame exchange and global time synchronization. It uses the distributed implementation of the RAND algorithm, Distributed RAND (DRAND) [11], as a two-hop conflict free scheduling algorithm for assigning conflict free slots. ZMAC uses the Timing-sync Protocol for Sensor Network (TPSN) [9] for global synchronization and the Real-Time Transport Protocol (RTP/RTCP) [11] for local synchronization and has two modes, High Contention Level (HCL) and Low Contention Level (LCL). ZMAC is energy efficient with exceptional throughput, but it is not scalable as the network grows because of the used tight synchronization and complex time-frame rules used for transmission control.

Gateway MAC [12] is as cluster-based MAC mechanism, which uses advantages of both contention, and contention-free mechanisms. Here, gateway node gathers requirements for transmission during contention period and contention-free period is used for distribution of data using specific slots. Gateway MAC (GMAC) offers active network control mechanisms to maximize sleep durations, and minimizing idle listening. The mechanism shows increased computational and communication overheads because of continuous transfer of gateway responsibilities.

Funneling MAC [13] uses network-wide Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) and an overlaid TDMA mechanism in funneling regions. It uses sink-oriented scheduling, where the burden of managing the TDMA scheduling in the funneling region falls on the sink node. It requires TDMA only in the intensity region and not in the total sensor field. Funneling MAC uses lightweight beacon-based clock synchronization and super frames contain the combination of both CSMA and TDMA frames. It avoids scalability issues by reducing the TDMA overheads, but it incurs extra overheads to avoid MAC interference.

Centralized hybrid MAC [14] provides reliable services by using a priority-based hybrid time-coordinated contention and contention-free MAC mechanism. Full Function Device (FED) and Reduced Function Device (RFD) are both considered device types and the time coordinated contention-based mechanism is managed by priority-based centralized scheduling. It relies on beacon messages for network-wide synchronization and the centralized hybrid MAC mechanism guarantees reliable throughput to selected priority users, but it is not suitable for a dense network as it is difficult to manage priorities for a high number of nodes.

Hybrid MAC (HyMAC) [15] combines the strength of TDMA and Frequency Division Multiple Access (FDMA) schemes inside constrained WSNs. It is suitable for applications where data gathered by sensor nodes has to be sent to at least one Base Station (BS). HyMAC's communication period is a fixed length TDMA cycle with a collection of a number of frames. It uses a breadth-first search-scheduling algorithm for assigning time slots and FireFly-based hardware synchronization to synchronize the communication. It shows high throughput with small end-to-end delay, but use of a hardware-based synchronization increases the overheads of the HyMAC.

Contention Reserve MAC (CRMAC) [16] is a hybrid MAC mechanism inspired by IEEE 802.15.4, and it is suitable for intra-cluster communication in cluster-based WSNs. The mechanism works in two phases: the setup phase, where it forms the cluster and an operational phase that reserves the slots according to the requirements and performs the data transmission. It relies on cluster-based scheduling for assigning efficient conflict free slots and operates in rounds with beacon-based synchronization. The mechanism is suitable for short packet transmissions under low load conditions.

Energy efficient Quality MAC (EQ-MAC) [17] is the combination of two sub-protocols Classifier-MAC (C-MAC) and Channel Access MAC (CA-MAC), and uses a hybrid approach of both TDMA and

CSMA mechanisms where it differentiates between long- and short-messages with TDMA scheduling used for long messages and CSMA for short messages. EQ-MAC uses cluster-based random scheduling for message differentiation, and this differentiation of control and data messages improves the energy efficiency, but also introduces a large amount of delays for low priority traffic. Priority-based MAC (PRIMA) [18] is an extended cluster-based version of EQ-MAC and consists of two phases; the clustering phase and the channel access phase. It shows improved scalability over EQ-MAC in large-scale WSNs. The maintenance of multiple priority queues increases the overhead of both EQ-MAC and PRIMA.

Emergency Response MAC (ERMAC) [19] is a hybrid MAC mechanism for emergency response services, which allows contention in TDMA slots to achieve a high delivery ratio and low latency. It maintains two separate queues; one for high priority packets and another for low priority packets. The mechanism maintains a synchronized and loose slot structure for local modification of a schedule and it uses separate slots for uni- and broadcast traffic, and the synchronization is based on Flooding Time Synchronization Protocol (FTSP) [20]. ERMAC shows considerable flexibility to adapt to traffic and topology changes, but it is not scalable for a high density of nodes because of maintenance of two separate queues for high- and low-priority packets.

Cooperative Wireless Sensor Network MACl (CWS-MAC) [21] is a traffic adaptive flow specific hybrid MAC mechanism, which utilizes flow-specific queue size statistics to select between medium accesses for nodes. Here, the contention-based mechanism is superimposed on top of a TDMA framing where CWS-MAC uses an interframe space and a contention beacon for deciding the priority in-between contention and non-contention flows. The approach shows substantial improvement in average delay, but leads to increases in energy consumption due to overheads incurred during priority decisions.

Multimode Hybrid MAC (MHMAC) [22] works in both synchronous and asynchronous modes - with or without contention, and it is developed to support cross-layering applications for packetizing radio. MHMAC considers three states; synchronous-, asynchronous- and full-one. The states are changed using Hello packets, which consist of a MHMAC state field and a slot reserve-bit. The protocol shows significant improvements in energy consumption, throughput, and latency but introduces overheads during a state change.

Binary MAC (Bin-MAC) [23] is a lightweight hybrid MAC mechanism for delay-sensitive applications. It provides a deterministic contention resolution mechanism, which achieves a bounded latency on data transmissions and it changes the mode according to the query message from the BS. The mechanism consists of four steps: contention resolution, binary tree collision resolution, slot consolidation, and duty-cycle adjustment. It does not use any clock synchronization for synchronizing the node. The algorithm shows considerable enhancements in energy efficiency, throughput, and delay, but increases overheads because of a four-step mechanism and synchronization of time is difficult if the density of nodes increases.

Queue-MAC [24] is a hybrid CSMA/TDMA MAC mechanism, which dynamically adapts the duty-cycle according to network traffic. The network traffic is analyzed using the queue length of nodes. Queue-MAC's super-frame structure contains fixed length CSMA and dynamic TDMA periods, and it implements the queue indicator inside the MAC packet. The algorithm shows considerable efficiency on specific hardware.

Intelligent Hybrid MAC (IHMAC) [25] is a low power Quality of Service (QoS) guaranteed MAC mechanism. IHMAC uses both broadcast and link scheduling and adapts the scheduling according to the network load. It uses virtual clustering for frame synchronization and a decentralized scheduling

approach where a node locally uses the clock arithmetic to find a slot. The mechanism shows satisfactory performance for delay-sensitive applications, but introduces overhead during schedule decision.

The study of related work illustrates that hybrid MAC mechanisms have exemplary performance efficiency, but that it is necessary to improve the mechanisms in order to support real-time applications. There is also a need to improve upon the mechanisms in terms of energy, delay, and throughput under the requirement of scalability. The proposed work improves the efficiency by utilizing more efficient scheduling and synchronization with an effective MAC mode control mechanism.

5.3 Building Blocks

GHMAC is a hybrid medium access mechanism, which uses both TDMA and CSMA modes of communication according to the demand and the condition of the network. GHMAC has the following different blocks to improve the efficiency beyond existing MAC mechanisms:

Cluster-based Topology: The cluster-based topology improves the scalability, energy efficiency, and reduces the effect of security attacks compared to a flat network. GHMAC uses Enhanced Multihop Clustering Algorithm (EMCA) [26] for forming the cluster-based topology. Enhanced Multihop Clustering Algorithm (EMCA) is proved as highly scalable when network scale grows. It uses multihop links for both inter- and intra- cluster communication. It also helps to reduce the uneven size of clusters and consumes approximately uniform amount energy during each rounds of clustering.

GCF Scheduling Algorithm: The scheduling algorithm is the core part of the hybrid MAC mechanism, which decides the specific conflict free slot for communication. The hybrid MAC mechanism proposed here uses GCF as a scheduling algorithm. GCF is a three-hop conflict free scheduling algorithm for WSNs. It shows significant improvements in energy efficiency, delay, and throughput with a large number of nodes and varying traffic rates.

Hybrid Synchronization Algorithm: Synchronization is necessary to achieve the timing accuracy during the slot assignment and node communication. GHMAC uses a hybrid synchronization for achieving this using approximate diffusion-based synchronization for intra-cluster communication and tight sender-receiver synchronization for inter-cluster communication. The hybrid synchronization used here achieves better energy efficiency and less synchronization errors at the synchronization level and it also improves the total energy efficiency, throughput, and delay.

MAC Mode Control Mechanism: TDMA mode is used for inter-cluster communication and TDMA or CSMA mode for intra-cluster communication.

5.3.1 MAC Mode Control in GHMAC

The MAC mode control for GHMAC consists of the following activities,

- The communications between CHs and between CHs and the BS i.e. inter-cluster communication use TDMA mode. The CH will always communicate using TDMA mode because information gathered at the CH is aggregated information from all nodes in a particular cluster, and it should have guaranteed transmission to the concerned CH or BS without conflicts. The TDMA-based

communication guarantees that during the given time schedule only one particular node can communicate and that no other nodes will disturb or communicate during that time slot.

- The communication between the cluster members and the CH (intra-cluster communication) takes place by using either TDMA or CSMA mode. Initially, all nodes are using CSMA, but the network can decide to shift to TDMA whenever the traffic and/or the number of collisions increases.

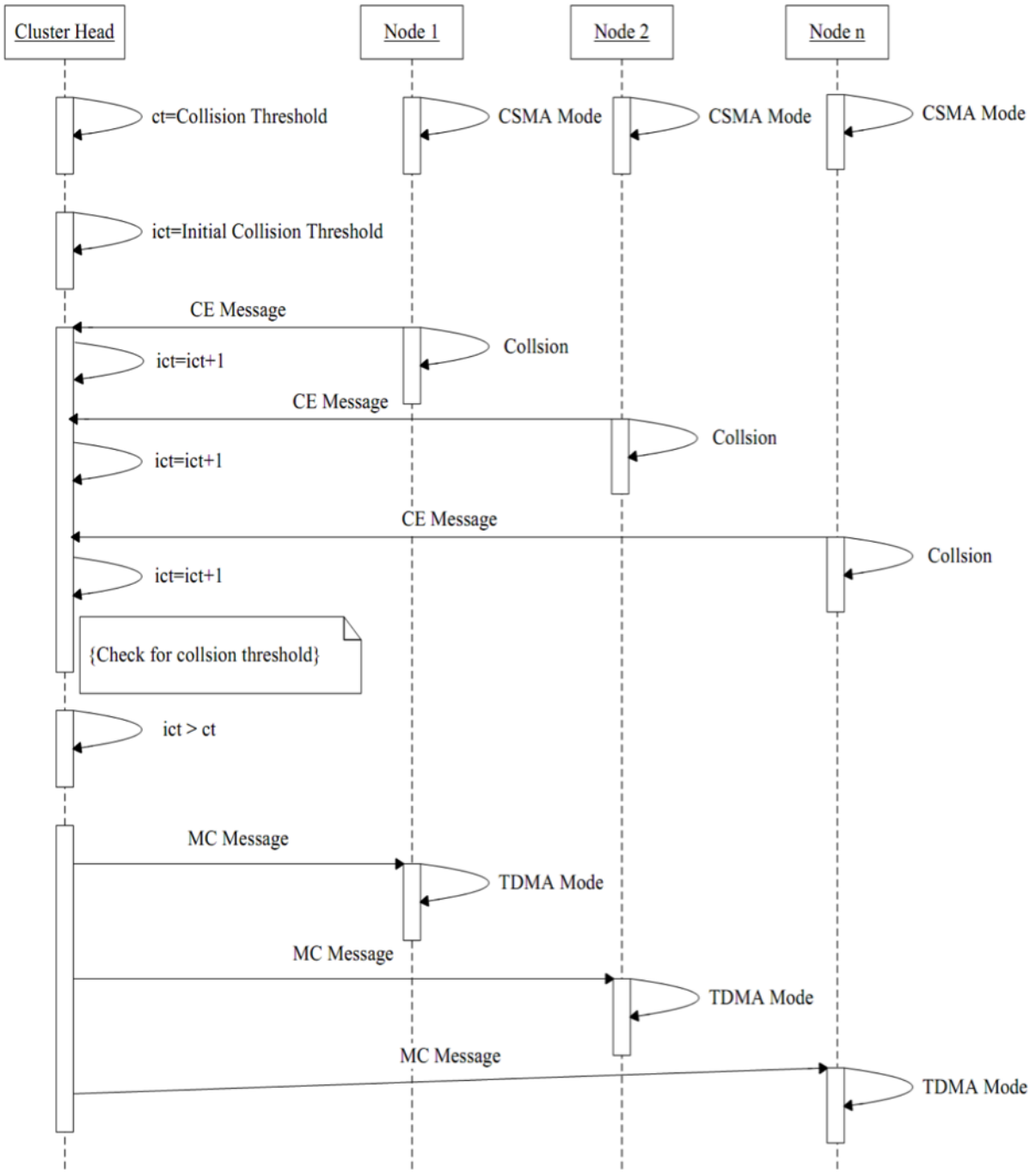


Figure 5.3: MAC mode control for intra-cluster communication.

The mode change mechanism for intra-cluster communication is as shown in Figure 5.3. Here, the CH maintains the Collision Threshold (*ct*) value and Initial Collision Threshold (*ict*). Initially, all nodes in the cluster are working in CSMA mode as, whenever a network operation starts, there is very low traffic in

the network and less competition to do communication activities. As the traffic grows, the conflicts will increase. Whenever a node experiences a collision, it transmits the Collision Experience (CSE) message to the CH and, after receiving the CSE message, the CH increments the *ict* count by one. If the *ict* count is greater than the *ct* count, the CH sends a Mode Change (MC) message to all nodes in the cluster. This MC message allows nodes to change their mode to TDMA that can reduce the number of collisions.

5.4 Simulation Results

5.4.1 Simulation Methodology

The simulation of the GHMAC algorithm is performed using Network Simulator-2 (NS-2) and the parameters considered for the simulation are as shown in Table 5.1. The simulation considers the WSN nodes deployed uniform randomly in an area of 100m by 100m. The number of slots used and number of resulting clusters in the network will be different for each simulation run because of random deployment of source nodes changes during each simulation run. The GHMAC is compared with the state-of-the-art hybrid MAC mechanisms; ZMAC, GMAC, ERMAC, and IHMAC. ZMAC is a widely used hybrid MAC mechanism, ERMAC is a priority-based hybrid MAC mechanism, GMAC is cluster-based hybrid MAC mechanism and IHMAC is one of the recent state-of-the-art work in hybrid MAC mechanisms. The implementation considers the random waypoint [27] mobility model and the clustering algorithm used is EMCA. The performance measurement of proposed algorithm consider the following three metrics,

- Average energy consumption: The work considers energy consumption of node as difference between initial energy of node and final energy of the node at the end of simulation. The average energy consumption is calculated as sum of energy consumption of all nodes divided by total number of nodes.
- Average delay: The work considers the average end-to-end delay from all the sources to the BS. It is calculated as above. The delay of one packet is time difference between packets receive time at BS and packet send time from source node. The total delay in the network is considered as sum of delays of all received packets. The average end-to-end delay is sum of delays of all received packets divided by total number of received packets.
- Average throughput: Throughput is computed in terms of packet delivery ratio (PDR). Packet Delivery Ratio (PDR) is the ratio of number of packets received by sink node divided by number of packets sent by source nodes. It is considered in percentage. The packets are transmitted with constant bit rate (CBR). The work uses user datagram protocol (UDP) as a transport layer protocol. Each node sends 100 packets with time interval of 1 second

The performance of GHMAC is measured in the following four ways,

- Measurement of GHMAC performance with varying collision threshold: The performance of GHMAC is measured by considering different collision threshold values and determining the equilibrium threshold value for performing the next performance evaluation.
- Performance measurement of GHMAC under static scenario: The performance of GHMAC is measured by varying the number of nodes and area of the network. The performance metrics used for measurement are average energy consumption, average delay, and average throughput.

- Performance measurement of GHMAC under mobile scenario: The GHMAC performance is measured by varying the percentage of mobile nodes and mobility speed of nodes.
- Performance of GHMAC under different denial of sleep attacks: The GHMAC performance is evaluated under different denial sleep attacks [28].

Table 5.1: Parameters for GHMAC simulation.

Parameters	**Setting used**
Wireless Physical	
Network interface type	Wireless Physical
Radio propagation model	Two-Ray Ground
Antenna type	Omni-directional Antenna
Channel type	Wireless Channel
Link Layer	
Interface queue	Priority Queue
Buffer size of IFq	50
MAC	GHMAC, ZMAC, GMAC, ERMAC and IHMAC
Routing protocol	Ad-hoc Routing - Ad-Hoc On-Demand Distance Vector Routing (AODV) [29]
Transport layer protocol	UDP
Traffic model	CBR
Energy Model	
Initial energy (Joule)	100
Idle power (mW)	14.4
Receiving power (mW)	14.4
Transmission power (mW)	36.0
Node Placement and Other Parameters	
Number of nodes	20, 40, 60, 80 and 100
Number of sources	19, 39, 59, 79 and 99
Number of BS	1
Node placement	Random
Placement of nodes and BS	Nodes are placed randomly in a given area, and the BS is placed at the center of the area.
Number of simulation runs	50
Number of packets transmitted by each source node	100
Packet time interval (second)	1

5.4.2 Varying Collision Threshold

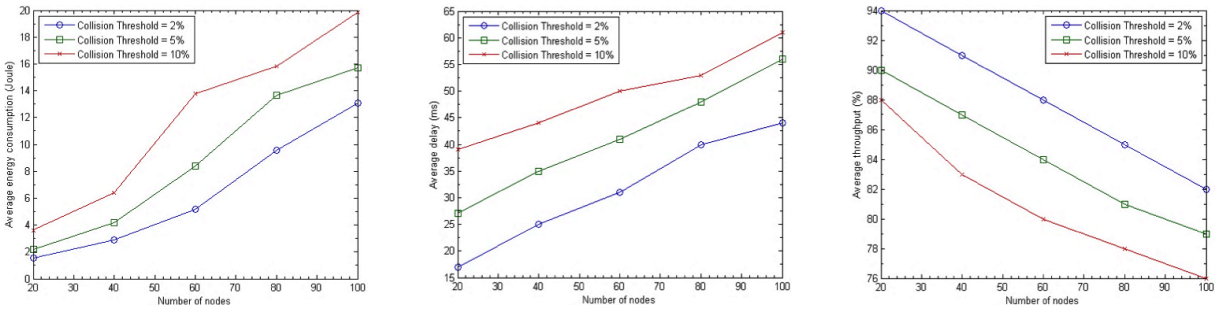
The *ct* value is the value below which the network should work in CSMA, and above which the network should shift from CSMA to TDMA. Here, the *ct* value of the network is determined by using the concept of collision rate. The collision rate for a node is the number of collisions seen by the node divided by the number of packets sent.

$$\text{Collision rate on a single node} = \frac{\text{Number of collisions seen}}{\text{Number of packets sent}} \tag{5.1}$$

$$\text{Collision rate in the network} = \frac{\text{Total number of collisions seen across all nodes}}{\text{Total number of packets sent across all nodes}} \tag{5.2}$$

In equation (5.2), the total number of packets sent across the network includes the packets that are relayed by the gateways and the CHs. The above calculation of average collision rate in the network provides a measure of the maximum number of collisions in the network to be observed before changing the mode. The average collision rate considered in the network is 5%, beyond which the network can be considered congested [30, Chapter 17].

Figure 5.4a, 5.4b and 5.4c show the average energy consumption, delay, and throughput respectively, by varying the number of nodes under three different *ct* values (2%, 5% and 10%). Here, the *ct* is measured as a function of a number of nodes. The number of nodes is varying as 20, 40, 60, 80, and 100. The



(a) Average energy consumption. (b) Average delay. (c) Average throughput.

Figure 5.4: Results for varying collision threshold.

trends of energy consumption and delay show that, as the *ct* increases, average energy consumption and delay also increase. The average throughput graph shows the reverse trend, where, as the *ct* increases, the algorithm shows a decrease in the average throughput of the network. The reason for this is the *ct* value; if the *ct* value is small, the network will quickly shift from CSMA to TDMA, which saves energy and increases throughput with reduced delays. The GHMAC performance is reduced with a higher threshold value such as 10%.

The simulations in the next subsections use 5% as the *ct* value.

5.4.3 Varying Number of Nodes and Area of Network

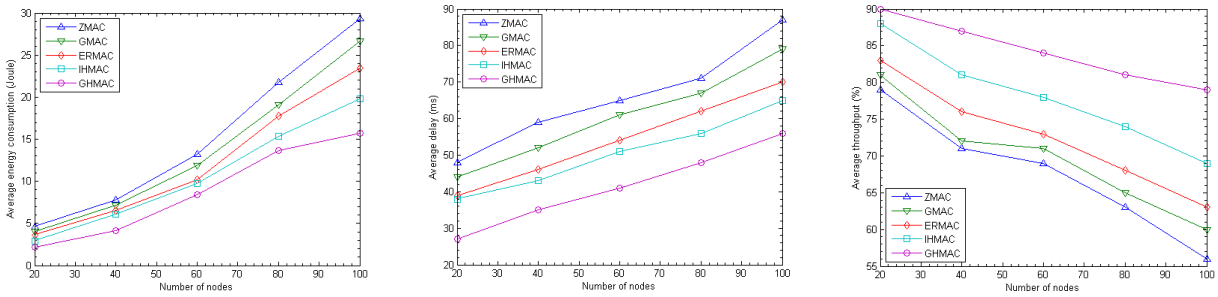
Figure 5.5a, 5.5b and 5.5c show the comparative average energy consumption, delay, and throughput of GHMAC, IHMAC, ERMAC, G-MAC, and ZMAC with varying number of nodes. The trends of all three graphs show that the performance of GHMAC is better than the performance of IHMAC, ERMAC, G-MAC, and ZMAC; the reasons being:

- GHMAC uses GCF scheduling while ZMAC uses the DRAND scheduling mechanism; ERMAC uses a tree-based scheduling, and IHMAC uses combined broadcast-and link scheduling. The GCF algorithm finds a conflict free schedule across three hops while DRAND finds a conflict free schedule across two hops only. The energy consumption, throughput, and delay performance of GCF is better than DRAND and the tree-based scheduling as GCF increases the reuse of slots.

- The hybrid synchronization algorithm used in GHMAC results in less overhead to the system and it consumes less energy for synchronization compared to the TPSN algorithm used in ZMAC, the loose synchronization used in ERMAC and virtual clustering based synchronization in IHMAC.

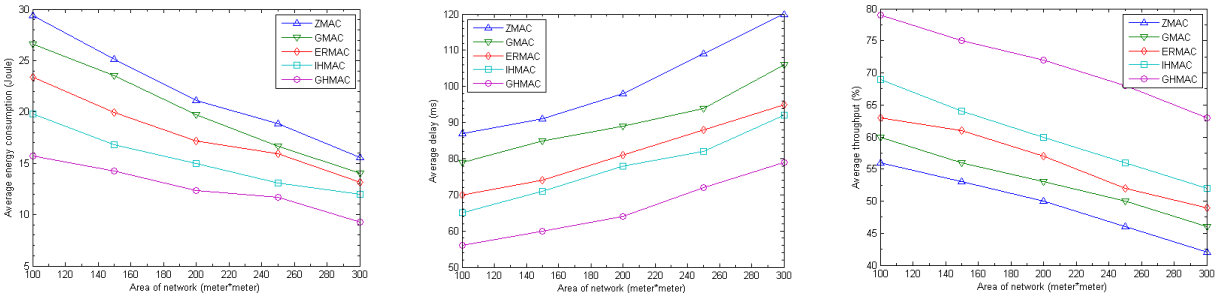
- Figures also show the performance comparison of GHMAC with GMAC. The reason for lower performance of GMAC than GHMAC is continuous transfer of gateway responsibilities. Here, the centralized gateway node requires more resources to collect all transmission requirements during a contention period and then schedules their distributions during a reservation-based.

- Another reason for GHMAC's better performance with an increasing number of nodes is its scalability and adaptivity to a larger number of nodes in the network. It achieves the scalability by using a cluster-based topology for its deployment. The cluster-based topology helps to achieve scalability by improving the total performance of the protocol.



(a) Average energy consumption. (b) Average delay. (c) Average throughput.

Figure 5.5: Results as a function of number of nodes.



(a) Average energy consumption. (b) Average delay. (c) Average throughput.

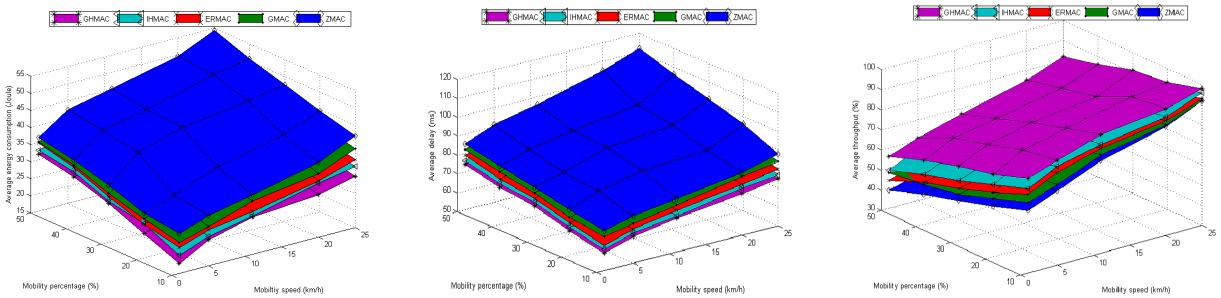
Figure 5.6: Results as a function of the area of the network.

Figure 5.6a, 5.6b and 5.6c show the average energy consumption, delay, and throughput in case of GHMAC, IHMAC, ERMAC, GMAC, and ZMAC with varying area of the network. The number of nodes considered for the simulation is 100, with different areas of node distribution: 100m x 100m, 150m x 150m, 200m x 200m, 250m x 250m, and 300m x 300m. The trends of the graphs show that average energy consumption and throughput are decreasing, and delays are increasing with the area of the network in case of all three hybrid MAC mechanisms. Here, GHMAC also outperforms IHMAC, ERMAC, GMAC, and ZMAC in dense and sparse networks. The important reason for GHMAC superior performance is its scalability to adapt to changing network conditions. Here, the change in area of the network effects on density of nodes. The network is dense with area as 100m*100m and it is spars with area 300m*300m.

5.4.4 Mobility Scenarios

Figure 5.7a, 5.7b and 5.7c show the average energy consumption, delay, and throughput under different mobility scenarios by varying the mobility speed and percentage of mobile nodes in the network. The simulation speeds considered are 1 km/h, 5 km/h, 11 km/h, 20 km/h, and 25 km/h. The simulation also considers different percentage of mobile nodes as 10%, 20%, 30%, 40%, and 50%. The total number of nodes considered in the simulation is 100 with an area of the network of 100m x 100m. The results show that GHMAC outperforms ZMAC, GMAC, ERMAC, and IHMAC in a mobile scenario as:

- GHMAC uses the cluster-based GCF scheduling algorithm, which supports, while ZMAC uses the DRAND scheduling algorithm that selects a schedule randomly, ERMAC forms the schedule by employing a data-gathering tree, and IHMAC uses combined link plus broadcast scheduling, which increases the overheads during node mobility. DRAND is not developed considering mobility



(a) Average energy consumption. (b) Average delay. (c) Average throughput.

Figure 5.7: Results with varying percentage of mobility and speed.

situations; it consumes more energy for rescheduling when a node goes mobile. The tree-based scheduling also incurs high overhead during node mobility for preserving the tree structure.

- GHMAC uses a hybrid synchronization algorithm, which is a combination of a tight synchronization algorithm, TPSN, and loose synchronization algorithm, Time Diffusion Protocol (TDP), which maintains synchronization when a node goes mobile. ZMAC uses tight synchronization, which increases the overheads when a node goes mobile, and there is a need of resynchronization. ERMAC uses loose synchronization in the whole network, which incurs less energy consumption than ZMAC, but increases overheads when nodes go mobile. IHMAC uses virtual clustering for frame synchronization, which increases the performance cost by increasing the synchronization packets during node mobility.

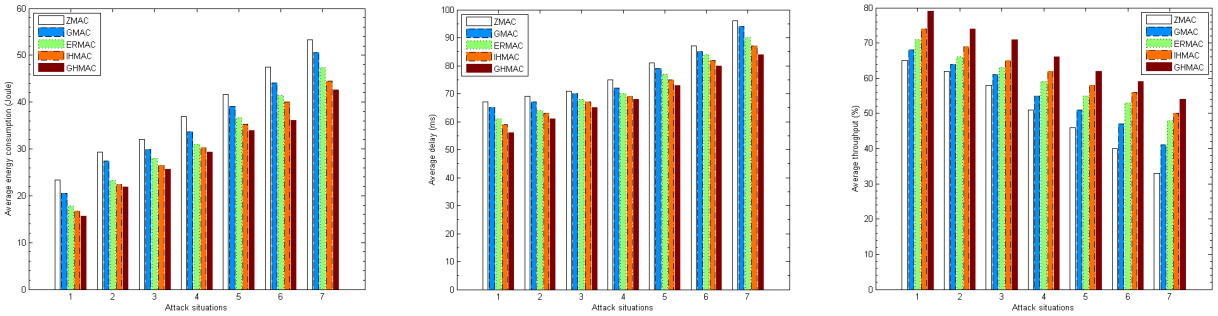
- Here, GMAC, a cluster-based hybrid mechanism also shows more degraded performance than GHMAC because of increase in transfer of gateway responsibilities during the mobility of nodes, which leads to increase in overheads in the network.

5.4.5 Denial of Sleep Attacks

The different scenarios considered for attacks analysis are as follows:

- Without attacks
- Under unintelligent replay attack
- Under unintelligent broadcast attack
- Under exhaustion attack
- Under collision attack
- Under full domination attack
- Under intelligent jamming attack

The simulations are carried out under the assumption that an attacker can initiate the attack from multiple nodes - randomly from 1 to 20 malicious nodes in the network. Figure 5.8a, 5.8b and 5.8c show that the performance of GHMAC is better than the other hybrid MAC mechanisms under the considered



(a) Average energy consumption. (b) Average delay. (c) Average throughput.

Figure 5.8: Results under different denial of sleep attackss.

scenarios. The performance of GHMAC, IHMAC, ERMAC, GMAC and ZMAC are degraded in case of an intelligent jamming attack as this considers that an intelligent attacker has full knowledge of the MAC mechanism used in the network. The major reasons for GHMAC performance improvements over ZMAC, GMAC, ERMAC, and IHMAC in different attack situations are the use of a cluster-based topology, scheduling and hybrid synchronization, which adjusts the synchronization according to the requirements of inter- or intra-cluster communication. The cluster-based approach reduces the penetration of attacks by maintaining a hierarchy of nodes for communication compared to flat networks, which are more prone to attack. In case of flat networks, malicious nodes can spread the attack quickly as each node has access to all other nodes in the network, while in a cluster-based network, a malicious node is constrained to a single cluster unless the CH is compromised, which makes the penetration of the attack slower than in a flat network.

5.5 Summary

A hybrid MAC mechanism is a viable solution for WSN applications considering variable traffic conditions and resource constraints, where one kind of mechanism is not a feasible solution. The chapter surveys the various state-of-the-art hybrid MAC mechanisms according to the working mechanism and presents the cluster-based hybrid MAC mechanism GHMAC. GHMAC is a hybrid MAC mechanism, which achieves conflict free scheduling using GCF algorithm, time-frame synchronization using a hybrid synchronization algorithm, and shifting of MAC mode using collision-threshold-based MAC mode control. The MAC mode control presented in the chapter shift the mode of intra-cluster communication by analyzing the amount of collisions in the specified cluster.

The chapter also presents an evaluation of the hybrid MAC mechanisms in three different scenarios: static, mobile and security. In the static scenario, the evaluation is performed by varying the collision-threshold, number of nodes and area of the network. The results of varying collision-threshold are used to analyze the accurate collision-threshold value for mode shift. The GHMAC results with varying number of nodes and area of network show good energy-, delay-, and throughput-efficiency and scalability as compared to state-of-the-art hybrid MAC mechanisms. The result in the mobile scenario shows the adaptivity of GHMAC in the mobile environment with varying the amount of mobile nodes and their speed. GHMAC's and the other hybrid MAC mechanisms' performance are also measured in the presence of denial of sleep attacks. The measurement shows that GHMAC gives an exemplary performance in different attack situations in comparison with other state-of-the-art mechanism. The analysis of GHMAC

in the security scenario also provides the motivation to enhance its performance further by introducing an internal attack defense mechanism.

5.6 References

[1] A. Bachir, M. Dohler, T. Watteyne, and K.K. Leung. Mac essentials for wireless sensor networks. *Communications Surveys Tutorials, IEEE*, 12(2):222–248, Second 2010.

[2] Giuseppe Anastasi, Marco Conti, Mario Di Francesco, and Andrea Passarella. Energy conservation in wireless sensor networks: A survey. *Ad Hoc Netw.*, 7(3):537–568, May 2009.

[3] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer Networks*, 52(12):2292 – 2330, 2008.

[4] Isaac Amundson and Xenofon D. Koutsoukos. A survey on localization for mobile wireless sensor networks. In *Proceedings of the 2Nd International Conference on Mobile Entity Localization and Tracking in GPS-less Environments*, MELT'09, pages 235–254, Berlin, Heidelberg, 2009. Springer-Verlag.

[5] Pranav M. Pawar, Rasmus Hjorth Nielsen, Neeli R. Prasad, and Ramjee Prasad. GHMAC: Green and Hybrid Medium Access Control for Wireless Sensor Networks (submitted). *Springer Wireless Personal Communication*, 2015.

[6] P.M. Pawar, R.H. Nielsen, N.R. Prasad, S. Ohmori, and R. Prasad. Gcf: Green conflict free tdma scheduling for wireless sensor network. In *Communications (ICC), 2012 IEEE International Conference on*, pages 5726–5730, June 2012.

[7] Ameer Ahmed Abbasi and Mohamed Younis. A survey on clustering algorithms for wireless sensor networks. *Computer Communications*, 30(14 - 15):2826 – 2841, 2007. Network Coverage and Routing Schemes for Wireless Sensor Networks.

[8] P.M. Pawar, R.H. Nielsen, N.R. Prasad, and R. Prasad. A hybrid algorithm for efficient wireless sensor network time synchronization. In *Wireless Communications, Vehicular Technology, Information Theory and Aerospace Electronic Systems (VITAE), 2014 4th International Conference on*, pages 1–5, May 2014.

[9] Saurabh Ganeriwal, Ram Kumar, and Mani B. Srivastava. Timing-sync protocol for sensor networks. In *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems*, SenSys '03, pages 138–149, New York, NY, USA, 2003. ACM.

[10] Weilian Su and I.F. Akyildiz. Time-diffusion synchronization protocol for wireless sensor networks. *Networking, IEEE/ACM Transactions on*, 13(2):384–397, April 2005.

[11] Injong Rhee, A. Warrier, M. Aia, Jeongki Min, and M.L. Sichitiu. Z-mac: A hybrid mac for wireless sensor networks. *Networking, IEEE/ACM Transactions on*, 16(3):511–524, June 2008.

[12] Brownfield, M.I. and Mehrjoo, K. and Fayez, A.S. and Davis, N.J., IV. Wireless sensor network energy-adaptive mac protocol. In *Proceedings of the 3rd Consumer Communications and Networking Conference*, CCNC '06, pages 778-782, Las Vegas, NV, USA, 2006. IEEE.

[13] Gahng-Seop Ahn, Se Gi Hong, Emiliano Miluzzo, Andrew T. Campbell, and Francesca Cuomo. Funneling-mac: A localized, sink-oriented mac for boosting fidelity in sensor networks. In *Proceedings of the 4th International Conference on Embedded Networked Sensor Systems*, SenSys '06, pages 293–306, New York, NY, USA, 2006. ACM.

[14] Hyung-Won Cho, Min-Hee Cho, Jong-Moon Chung, and Wun-Cheol Jeong. A centralized hybrid mac protocol for wireless sensor networks. In *Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on*, pages 455–460, Dec 2007.

[15] M. Salajegheh, H. Soroush, and A. Kalis. Hymac: Hybrid tdma/fdma medium access control protocol for wireless sensor networks. In *Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on*, pages 1–5, Sept 2007.

[16] Ge Ma and Dongyu Qiu. An efficient mac protocol based on hybrid superframe for wireless sensor networks. In *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on*, pages 1–4, Oct 2008.

[17] B. Yahya and J. Ben-othman. An energy efficient hybrid medium access control scheme for wireless sensor networks with quality of service guarantees. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1–5, Nov 2008.

[18] J. Ben-othman, L. Mokdad, and B. Yahya. An energy efficient priority-based qos mac protocol for wireless sensor networks. In *Communications (ICC), 2011 IEEE International Conference on*, pages 1–6, June 2011.

[19] L. Sitanayah, C.J. Sreenan, and K.N. Brown. Er-mac: A hybrid mac protocol for emergency response wireless sensor networks. In *Sensor Technologies and Applications (SENSORCOMM), 2010 Fourth International Conference on*, pages 244–249, July 2010.

[20] Miklós Maróti, Branislav Kusy, Gyula Simon, and Ákos Lédeczi. The flooding time synchronization protocol. In *Proceedings of the 2Nd International Conference on Embedded Networked Sensor Systems*, SenSys '04, pages 39–49, New York, NY, USA, 2004. ACM.

[21] T.O. Walker, M. Tummala, and J. McEachen. Distributed medium access control with flow-based priority for cooperative multi-hop wireless sensor networks. In *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, pages 493–493, Jan 2008.

[22] L. Bernardo, R. Oliveira, M. Pereira, M. Macedo, and P. Pinto. A wireless sensor mac protocol for bursty data traffic. In *Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on*, pages 1–5, Sept 2007.

[23] V. Salmani and P.H. Chou. Bin-mac: A hybrid mac for ultra-compact wireless sensor nodes. In *Distributed Computing in Sensor Systems (DCOSS), 2012 IEEE 8th International Conference on*, pages 158–165, May 2012.

[24] Shuguo Zhuo, Ye-Qiong Song, Zhi Wang, and Zhibo Wang. Queue-mac: A queue-length aware hybrid csma/tdma mac protocol for providing dynamic adaptation to traffic and duty-cycle variation in wireless sensor networks. In *Factory Communication Systems (WFCS), 2012 9th IEEE International Workshop on*, pages 105–114, May 2012.

[25] M. Arifuzzaman, M. Matsumoto, and T. Sato. An intelligent hybrid mac with traffic-differentiation-based qos for wireless sensor networks. *Sensors Journal, IEEE*, 13(6):2391–2399, June 2013.

[26] Ying Qian, Jinfang Zhou, Liping Qian, and Kangsheng Chen. Highly scalable multihop clustering algorithm for wireless sensor networks. In *Communications, Circuits and Systems Proceedings, 2006 International Conference on*, volume 3, pages 1527–1531, June 2006.

[27] C. Bettstetter, G. Resta, and P. Santi. The node distribution of the random waypoint mobility model for wireless ad hoc networks. *Mobile Computing, IEEE Transactions on*, 2(3):257–269, July 2003.

[28] Pranav M. Pawar, Rasmus Hjorth Nielsen, Neeli R. Prasad, Shingo Ohmori, and Ramjee Prasad. Behavioral modeling of wsn mac layer security attacks: A sequential uml approach. *Journal of Cyber Security and Mobility*, 1(1):65–82, 2012.

[29] Perkins, C. and Belding-Royer, E. and Das, S. Ad Hoc On-Demand Distance Vector (AODV) Routing. In *Workshop on Mobile Computing Systems and Applications*, pages 1-11, New Orleans, LA, USA, 2003.

[30] Hal Stern. *Managing NFS and NIS.* O'Reilly & Associates, Inc., Sebastopol, CA, USA, 2nd edition, 2001.

Chapter 6

MAC Security Attacks and Countermeasures

The objective of this chapter is to understand the mechanisms of Medium Access Control (MAC) security attacks and propose countermeasures. The chapter achieves the first objective by modeling MAC security attacks using activity and sequential modeling approaches of Unified Modeling Language (UML) and evaluations of the attacks. The understanding of the effects of attacks on hybrid MAC mechanisms leads to the proposal of new attacks i.e. Explicit Contention Notification (ECN) and Cluster Head (CH) attacks. The chapter reviews state-of-the-art countermeasures for MAC security attacks. This review together with the understanding of MAC security attacks provide the motivation to achieve the second objective i.e. the Green and Secure Hybrid MAC (GSHMAC) mechanism that countermeasures MAC security attacks. The comparative evaluation of GSHMAC with state-of-the-art solutions shows that this is an efficient solution in terms of energy, throughput and delay.

6.1 Introduction

Wireless Sensor Network (WSN) applications in areas related to everyday life are increasing and at the same time the use of WSNs in industrial use cases is becoming still more widespread. Applications include home security and automation, vehicular communication to monitor and control a vehicle, industrial applications to control, monitor, and record activities, sensors in the human body for medical purposes, weather monitoring to increase the accuracy of weather predictions and agricultural applications to increase the crop yield. Every application of sensors can significantly improve aspects of living and help to increase productivity and efficiency in the domains in which they are deployed [1, 2].

However, as applications of WSNs are becoming still more widespread and broad, and their demands are increasing, the chances of the network being attacked or compromised by malicious users are also increasing. Malicious users attack a network by disrupting the normal functionality in order to gain unauthorized access to operations or information for various purposes. This, in turn, results in stalled or reduced productivity. Proper security measures while deploying WSNs are, therefore, a necessity to take full advantage of the deployment of new applications [3].

Due to the rise of many mission critical WSN applications, the range and number of security attacks on WSNs have increased significantly over the last decade [3] and it is, therefore, necessary to design WSNs and related mechanisms also considering constraints with respect to security. Attacks can happen at all layers of a WSN but are more harmful when they are in the form of resource consumption attacks. Resource consumption attacks mainly take place at the MAC layer because this is the layer that controls the access to the resources in the network [4].

Related to the contributions in the previous chapters, this chapter is specifically concerned with contributions to security for WSN MAC. The significant contributions and challenges addressed in this chapter are as shown in Figure 6.1. The research focuses on denial of sleep MAC layer attacks on WSNs that primarily affect the sleep mode of WSN nodes. During sleep mode, nodes save energy by keeping the radio off, and denial of sleep attacks prevent nodes from going into this mode, which increases the energy consumption and reduces the total network lifetime. However, understanding the behavior of MAC security attacks is important in order to develop secure mechanisms for the MAC layer.

The first contribution of this chapter is to understand and model the behavior of WSN MAC security attacks for development of efficient MAC mechanisms. The chapter models the behavior of MAC security attacks using sequential and activity modeling approach of the UML methodology. The UML-based approach has been chosen for better analysis of security attack behavior [5, 6, 7, 8]. UML is a well-known modeling methodology and is a standard notation for real world objects as a first step in developing an object-oriented design methodology. The important benefit of UML is that it provides security developers a standardized methodology for visualizing security attacks that are present in WSNs.

Modeling the behavior of WSN MAC security attacks gives an understanding of the working of an attack inside the network, which is useful to implement the attack mechanism and check its effects on the performance of the WSN. The second contribution of the chapter is a comparative evaluation of WSN MAC security attacks on hybrid MAC mechanisms using the tool Network Simulator-2 (NS-2). The implementation uses the hybrid MAC mechanism ZMAC [9]. The results show the actual performance degradation due to security attacks on energy consumption, delay and throughput in varied conditions of traffic and number of malicious nodes in the network. The implementation results show that the MAC security attacks degrade the performance of a WSN by 50% or more. These results also act as a valuable

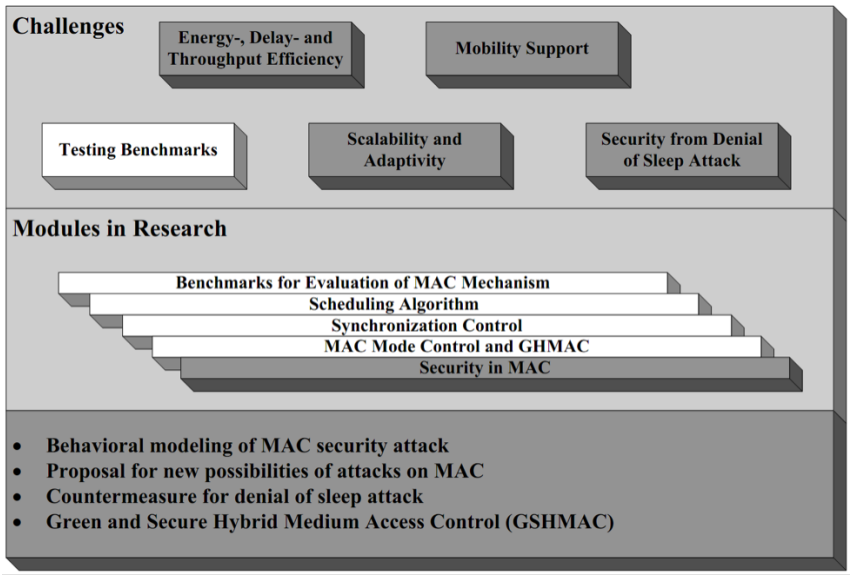


Figure 6.1: Chapter 6 contributions.

motivational tool to develop a secure and efficient hybrid MAC mechanism for WSN. The detailed study of hybrid MAC mechanisms under different attack situations gives two possibilities of security attacks specifically on hybrid MAC mechanisms i.e. ECN attack and CH attack.

The modeling and evaluation of WSN MAC security attack also give motivation to develop a secure MAC mechanism for WSNs that is proposed as the secure hybrid MAC mechanism GSHMAC. GSHMAC is a cluster-based [11] secure hybrid MAC mechanism [12] and is a secure extension of the Green and Hybrid MAC (GHMAC) proposal made in Chapter 5. It uses the internal mechanisms provided in hybrid MAC for counter measuring collision, replay and full domination attack and shows improved energy efficiency, delay and throughput in malicious attack situations as compared with state-of-the-art solutions.

Section 6.2 provides the details on the UML modeling approach, and the sequential and activity modeling of the WSN MAC security attacks. Section 6.3 provides the comparative evaluation of WSN MAC security attacks and discusses the effect of different kinds of WSN MAC security attacks on a hybrid MAC mechanism. Section 6.4 presents the possible new ways of the attack penetration specifically for hybrid MAC mechanisms. Section 6.5 provides the contribution towards a secure MAC mechanism for WSNs through the proposal of GSHMAC with simulation results and discussions. Lastly, Section 6.6 summarizes the chapter.

6.2 Modeling of MAC Layer Security Attacks

6.2.1 UML Modeling

UML [7] is a language for specifying, visualizing, constructing and documenting artifacts and is used to evolve and derive a system. It presents a standard way to show interactions/behavior within the system that provides a conceptual understanding of system functionality. UML provides a large set of diagrams such as use case diagram, sequence diagram, activity diagram, state machine diagram, deployment diagrams and many more to model the system behavior.

The research focuses on the use of UML to model security attacks using sequence diagrams [7]. A

sequence diagram is used primarily to show the interactions between objects in sequential order in which they occur also known as message sequence charts. A sequence diagram shows, as parallel vertical lines, different processes or objects that live simultaneously, and, as horizontal arrows, the messages exchanged between them, in the order in which they occur. Activity diagrams [7] are often used to give a functional view of a system as it describes logical processes, or functions, where each process represents a sequence of tasks and the decisions that govern when and how they are performed. An activity diagram is designed to support the description of behaviors that depend upon the results of internal processes, as opposed to external events as in interaction diagrams. The flow in an activity diagram is driven by the completion of an action. Activity diagrams are useful tools to understand the basic flow of security attacks and will be utilized in the following to do so.

6.2.2 Sequential Modeling of WSN MAC Security Attacks

Collision Attack

Figure 6.2 explains the flow of events in case of collision attacks [13, 14]. The details of each event are as follows,

- An external attacker initiates the collision attack through the malicious *node 3*.
- Once the attack is initiated by *node 3*, it will start to send noise packets to all nodes in the network. It will increase the traffic in the network causing the channel to become busy doing this activity.
- *node 1* detects an event and sends an RTS packet to *node 2*. At the same time, the malicious *node 3* also generates a noise packet and forwards it towards *node 2*. Both packets will reach *node 2* simultaneously and cause a collision.
- Again, *node 1* detects the event and checks channel availability by exchanging RTS and Clear to Send (CTS) with *node 2*. Once *node 1* receives the CTS from *node 2*, *node 1* starts to send data packets towards *node 2*. If, at the same time, the malicious *node 3* also sends noise packets toward *node 2*, collisions will happen in the network.
- The malicious *node 3* is continuously generating noise packets that make the channel always busy. During this, if any other node tries to use the channel, a collision will take place. This collision of packets leads to retransmission of the packets that in turn leads to increasing energy consumption.

Unintelligent Replay Attack

Figure 6.3 explains the flow of events in case of an unintelligent replay attack [15]. The details of each event are as follows,

- An external attacker initiates the unintelligent replay attack through the malicious *node 4*.
- The malicious *node 4* detects the event and sends an unauthenticated data/control packet towards the sink hop-by-hop, *node 4* $\rightarrow$ *node 3* $\rightarrow$ *node 2* $\rightarrow$ *node 1*.
- After some time, the malicious *node 4* will replay the event and will forward it through the network. Here, the malicious node does not differentiate between control and data packets.

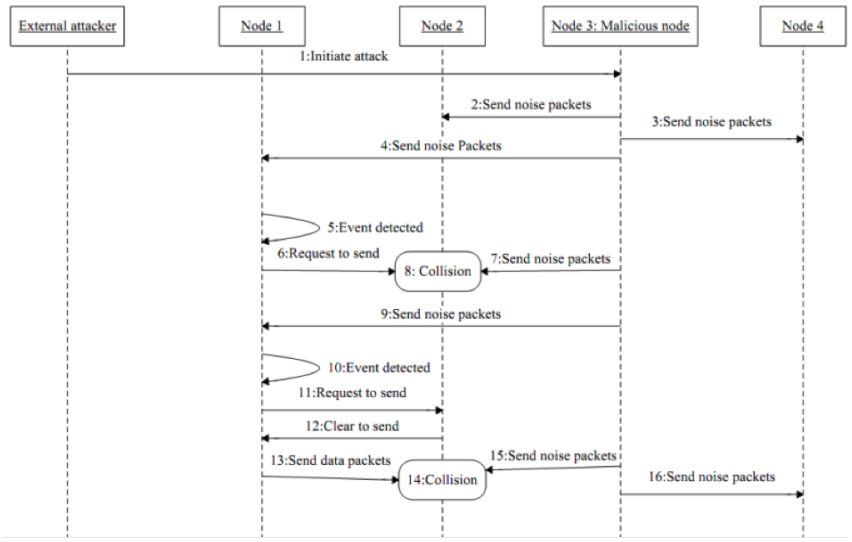


Figure 6.2: Sequence diagram of collision attack.

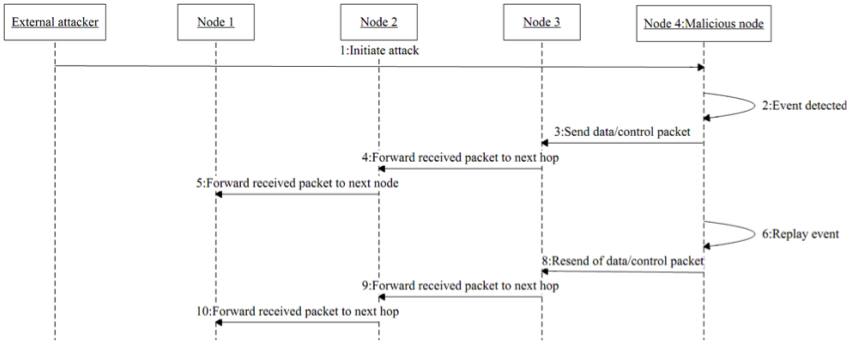


Figure 6.3: Sequence diagram of unintelligent replay attack.

Unauthenticated Broadcast Attack

Figure 6.4 explains the flow of events in case of the unauthenticated broadcast attack [15]. The details of each event are as follows,

- An external attacker initiates an unauthenticated broadcast attack through the malicious *node 3*.
- The malicious *node 3* detects the event and broadcasts the packet to the whole network.
- Whenever the packet reaches a node, the node will try to authenticate it but authentication will fail because, even though, in this attack, the attacker has full protocol knowledge, it does not have the ability to penetrate the network.
- Every time the malicious *node 3* detects the event and broadcasts the packet to the whole network. This unnecessary broadcasting of packets will waste energy in all nodes in the network because nodes will have to wake up to listen due to the event.
- *node 4* detects the event and sends the message towards *node 3*. If, at the same time, the malicious *node 3* detects and broadcasts the event, it leads to a collision on the channel between *node 3* and *node 4*.

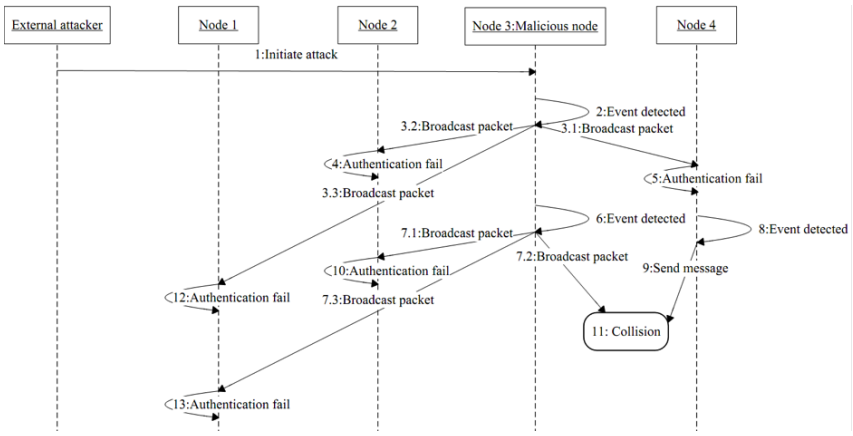


Figure 6.4: Sequence diagram of unauthenticated broadcast attack.

Full Domination Attack

Figure 6.5 explains the flow of events in case of full domination attack [15]. The details of each event are as follow,

- An external attacker initiates the full domination attack through the malicious *node 2* and *node 4*.
- The malicious *node 4* detects the event and broadcasts the message to the network. Here, the message is accepted by all nodes because, in this attack, the attacker has full knowledge of the MAC mechanism and the ability to penetrate the network.
- The malicious *node 2* detects the event and broadcasts the message to the network.
- The malicious *node 2* replays the event again after some time and broadcasts it to the whole network. The repeated broadcasting of the event will prevent nodes from going into sleep mode, thus increasing the overall power consumption.
- *node 3* detects an event and sends the data, and this collides with the broadcast message sent by the malicious *node 2*.

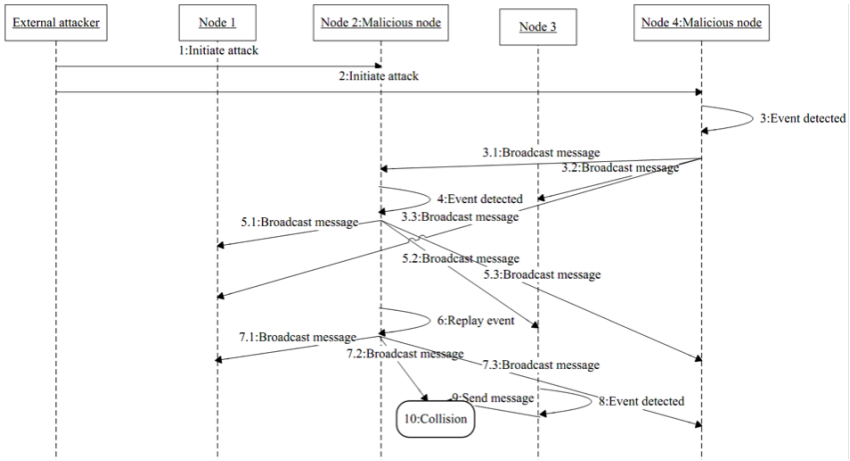


Figure 6.5: Sequence diagram of full domination attack.

Exhaustion Attack

Figure 6.6 explains the flow of events in case of the exhaustion attack [15]. The details of each event are as follows,

- An external attacker initiates an exhaustion attack through the malicious *node 4*.
- *node 1* detects the event and exchanges RTS and CTS and finally sends the data to *node 2*.
- The malicious *node 4* detects an event and sends RTS to *node 2*.
- *node 2* will reply by CTS. After that, the malicious node will repeatedly generate an RTS packet and transmit it towards *node 2* until the total energy of *node 2* is exhausted.

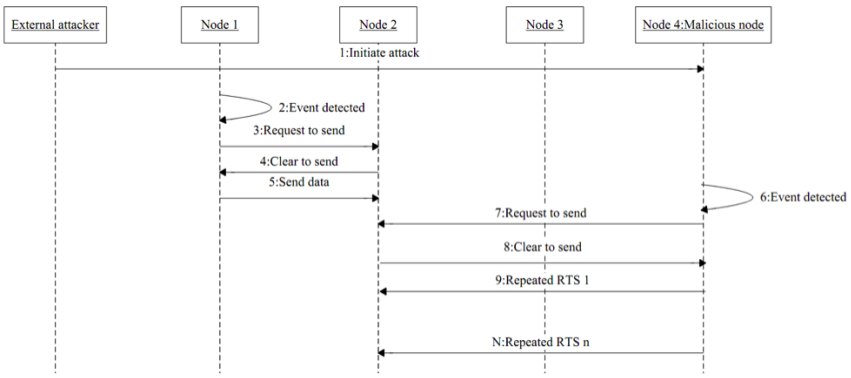


Figure 6.6: Sequence diagram of exhaustion attack.

Intelligent Jamming Attack

Figure 6.7 explains the flow of events in case of intelligent jamming attack [15, 16]. The details of each event are as follows,

- An external attacker initiates an intelligent jamming attack through the malicious *node 4*.
- The malicious *node 4* detects the control event and transmits the unauthenticated unicast message to *node 3*.
- *node 3* detects an event and forwards the message towards *node 1*; this message collides with the message broadcasted by the malicious *node 4*.
- The malicious *node 4* detects an event and broadcasts the unauthenticated broadcast message in the network.
- The malicious *node 4* uses the knowledge of the MAC layer mechanism for selective replay of data or control events. *node 4* replays the previously detected data event and transmits the unauthenticated unicast message to *node 2*.
- The malicious *node 4* selectively replays the control event and broadcasts the unauthenticated control message in the network.

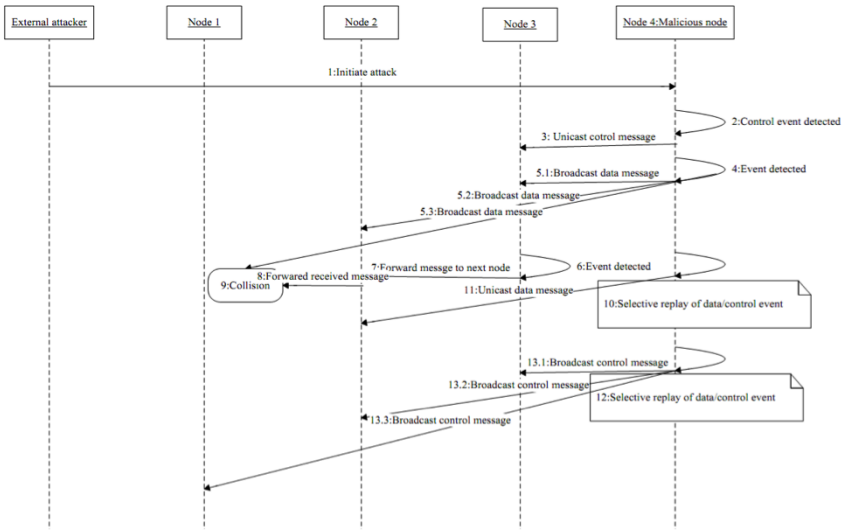


Figure 6.7: Sequence diagram of intelligent jamming attack.

6.2.3 Activity Modeling of WSN MAC Security Attacks

Collision Attack

Figure 6.8 shows the activity diagram for the collision attack and the different activities are as follows,

- The malicious node randomly creates noise packets and transmits them over the network.
- A normal node starts a transmission to the sink either by direct communication or through relays using multi-hop communication.
- A collision happens between the control or data packet from the normal node and the noise packet from the malicious node. Repeatedly collisions will reduce the performance of the network.

Unintelligent Replay Attack

The sequence of activities in case of an unintelligent replay attack is shown in Figure 6.9 and are as follows,

- The normal node has data to send and checks if the channel is available and, if it is, the node starts the transmission.
- The malicious node records the transmission as if in normal node mode, which it keeps replaying unintelligently, i.e. without making differentiation between data and control packets; it will replay any transmission the normal node would have generated.
- The malicious node checks the remain energy on each replay, and once the energy is exhausted, the attack will be terminated, and the external attacker will try to initiate the attack on another node.

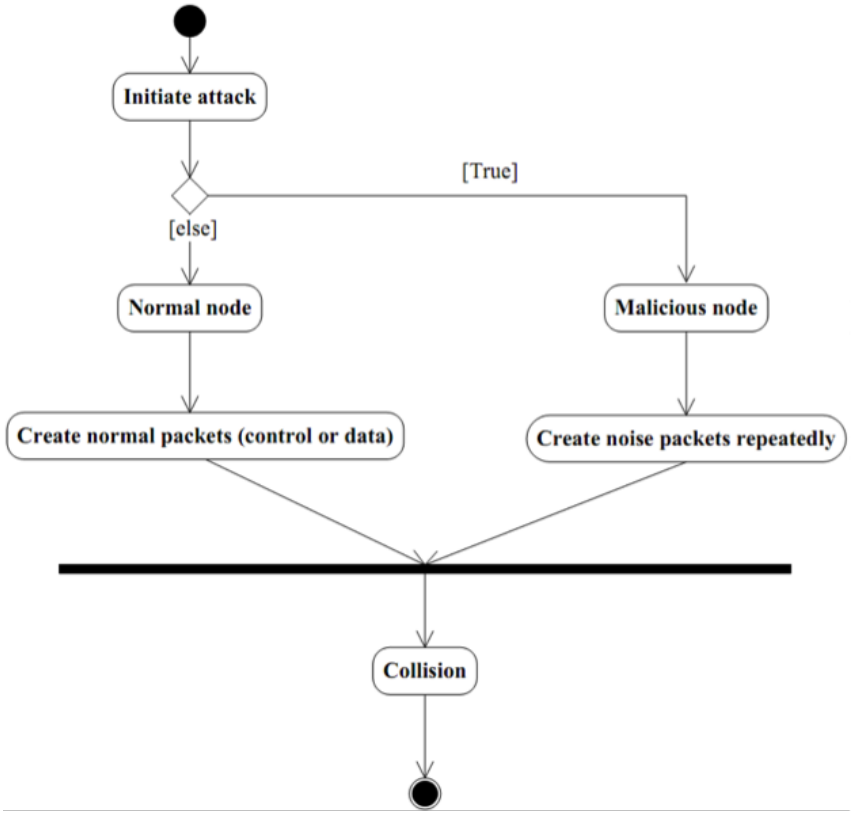


Figure 6.8: Activity diagram of the collision attack.

Unauthenticated Broadcast Attack

Figure 6.10 shows the activity modeling of the unauthenticated broadcast attack. The sequence of activities performed by the normal and malicious node is as follows,

- The normal node does communication as in the previous attack.
- The malicious node uses similar transmissions, but broadcasts the packet to all nodes in the network and, further, tries to authenticate itself, which fails.
- If the broadcast takes place during transmission of a normal node, a collision will take place. These collisions and the failed attempt to authenticate lead to performance degradation and thereby excessive energy consumption.

Full Domination Attack

The modeling of the sequence of activities for the full domination attack can be seen from Figure 6.11 and activities are as follows,

- The normal node broadcasts a packet to the network if the channel is available.
- The malicious node does the same and tries for authentication. As the attacker has full network knowledge, the authentication is successful, and the malicious packet is transmitted while the malicious node attempts to introduce collisions during normal traffic.

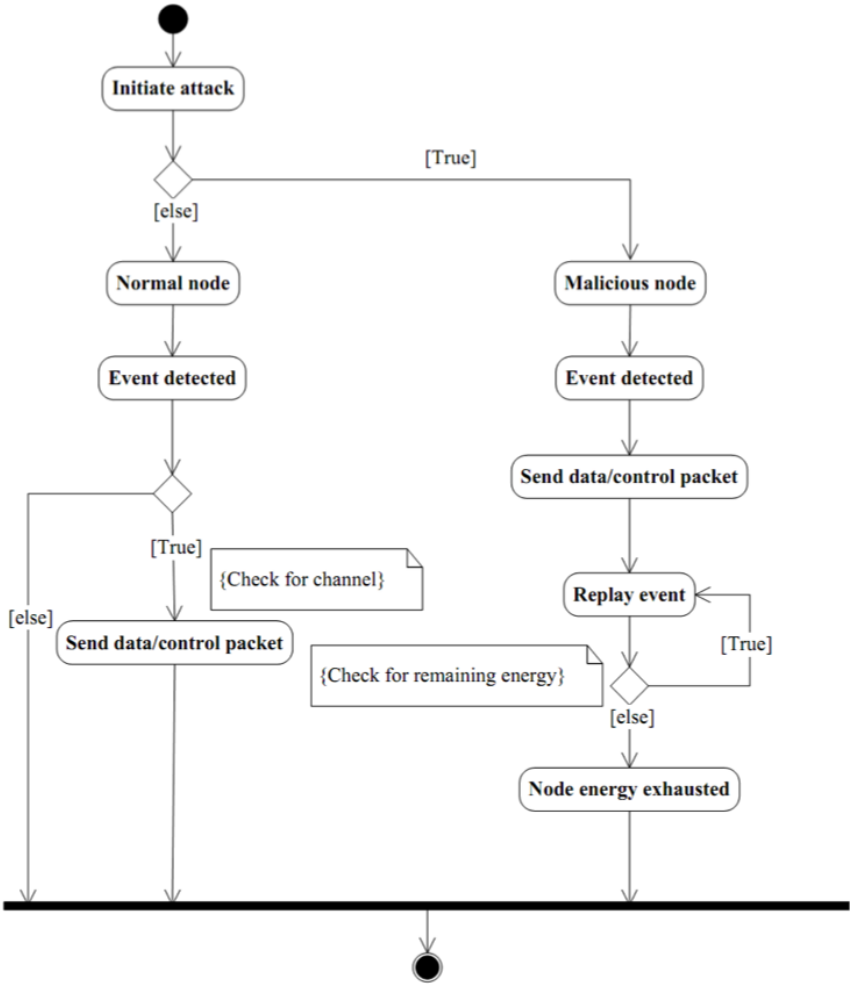


Figure 6.9: Activity diagram of unintelligent replay attack.

- The malicious node can also replay the communication unintelligently and broadcast it until the node's energy is exhausted. The full domination attack reduces the efficiency of the network by introducing authenticated broadcast and by replaying transmissions.

Exhaustion Attack

Figure 6.12 explains the sequence of activities during an exhaustion attack and the sequence of activities are described as follows,

- The normal node can send RTS, receive CTS from destination, and send data towards the target node.
- In the case of the malicious node, it sends RTS and waits for CTS from the target node. If it receives the CTS, it will send the RTS repeatedly towards the destination node until its energy is exhausted.

Intelligent Jamming Attack

Figure 6.13 shows the sequence of activities that happen during an intelligent jamming attack and the activities are as follows,

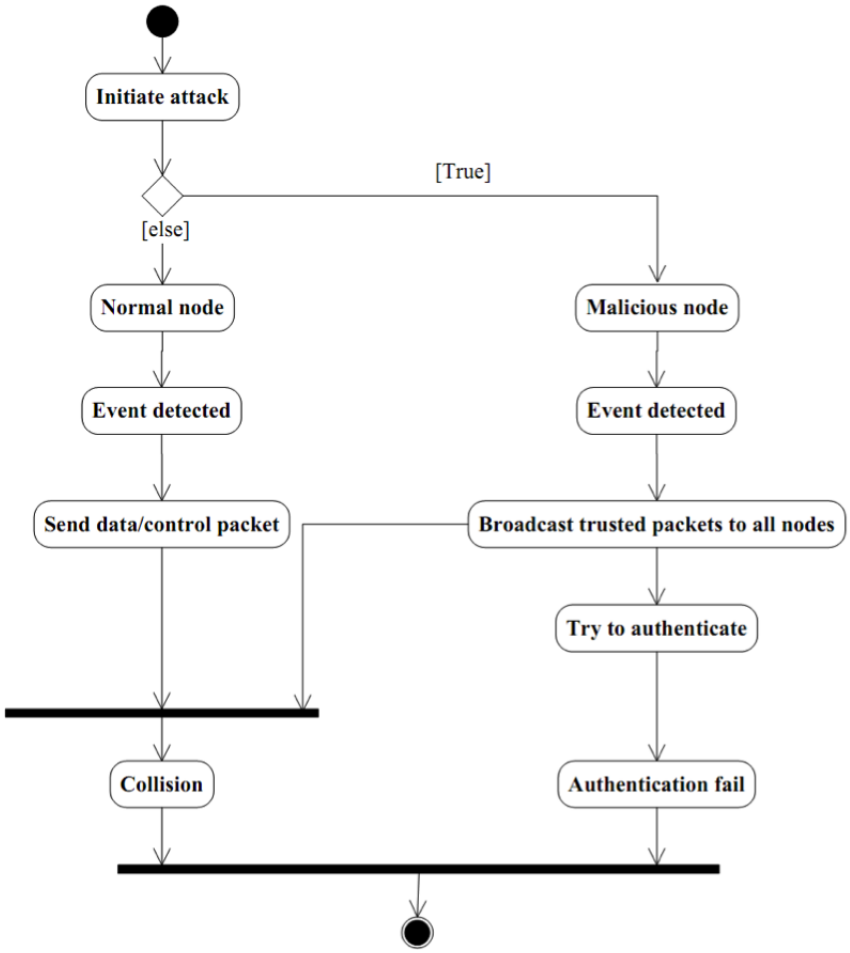


Figure 6.10: Activity diagram of unauthenticated broadcast attack.

- The normal node has data to send and broadcasts it if the channel is available.
- The malicious node does the same, authenticates to the node, and broadcasts the packet, in the same way, as for the full domination attack.
- The most important feature of the intelligent jamming attack is its intelligent behavior. It can differentiate between data and control packets, and will selectively replay the events until the node energy is exhausted.
- The replaying of event and broadcast of authenticated packets lead to collisions during normal transmissions.

6.3 Comparative Evaluation of WSN MAC Security Attacks on Hybrid MAC Mechanisms

6.3.1 Simulation Details

All simulations are carried out using the discrete event simulator NS-2 and the simulation parameters are shown in Table 6.1.

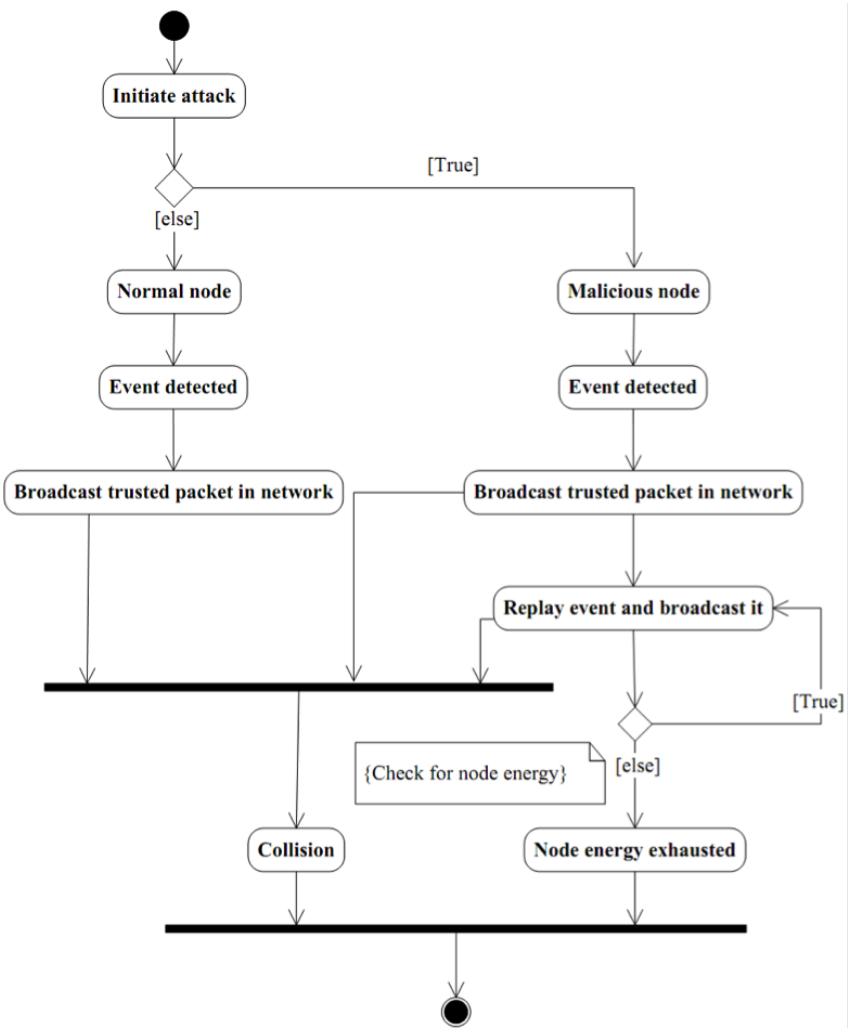


Figure 6.11: Activity diagram of full domination attack.

The simulations are performed using the hybrid MAC mechanism Zebra MAC (ZMAC) and the simulated scenarios are:

- ZMAC without any attacks
- ZMAC under unintelligent replay attack
- ZMAC under unintelligent broadcast attack
- ZMAC under exhaustion attack.
- ZMAC under collision attack.
- ZMAC under full domination attack.
- ZMAC under intelligent jamming attack.

The simulations are carried out under the assumption that the attacker can initiate the attack from multiple nodes. The initial simulation is done using four malicious nodes, but the impact of varying malicious nodes (from 2 to 32) is also investigated.

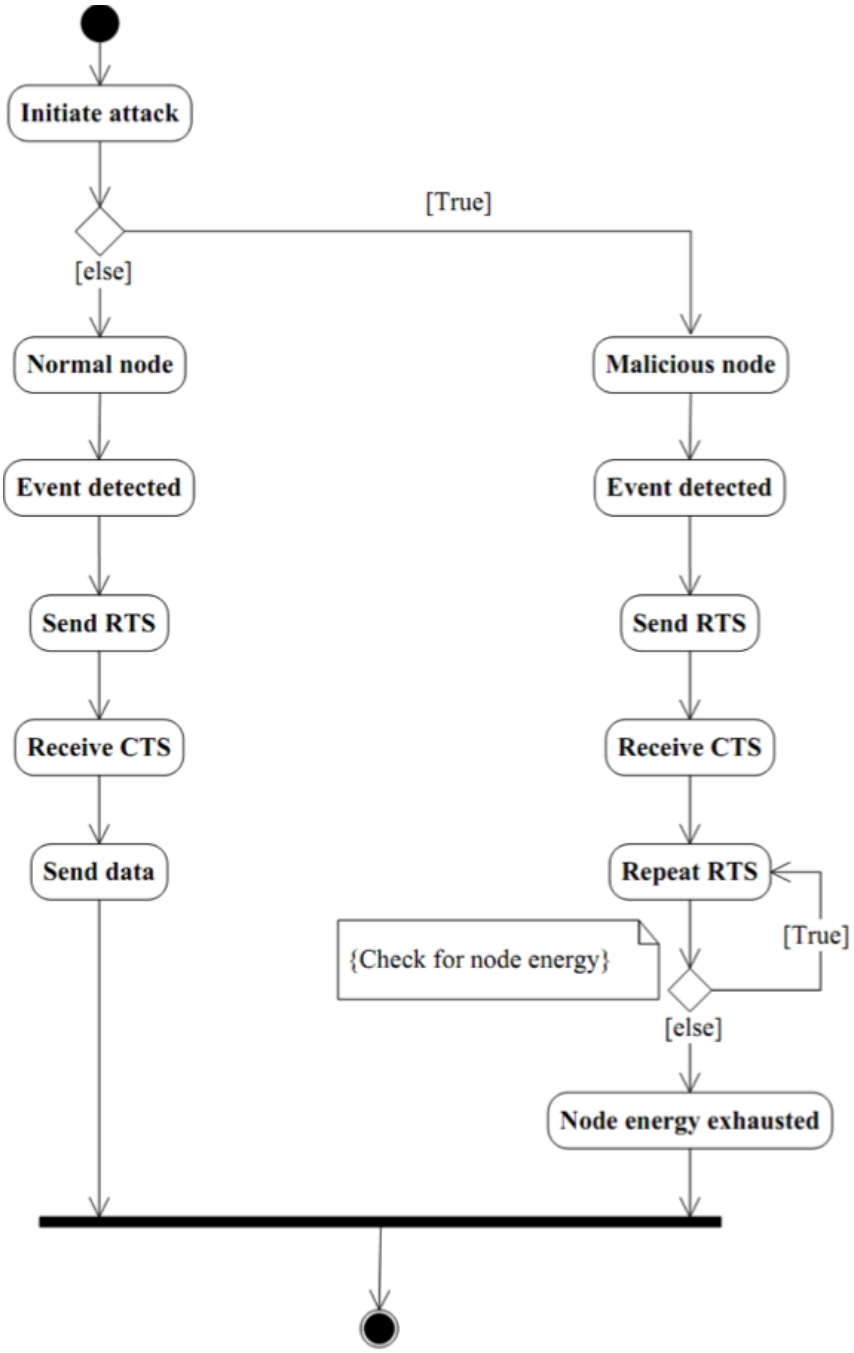


Figure 6.12: Activity diagram of exhaustion attack.

6.3.2 Results and Discussion

Figure 6.14a, 6.14b, 6.15a, 6.15b, 6.16a and 6.16b show the performance, i.e. energy consumption, throughput and delay of ZMAC under normal conditions and attacks. The figures show that the performance of the WSN degrades with the attacks and the reasons for the performance degradations under the individual attacks are as follows,

Unauthenticated Broadcast Attack: The performance degradation due to this attack is less compared to the other attacks because this attack utilizes more energy and requires extra time for authentication of the broadcast packets coming from the malicious nodes. The attack results in degradation

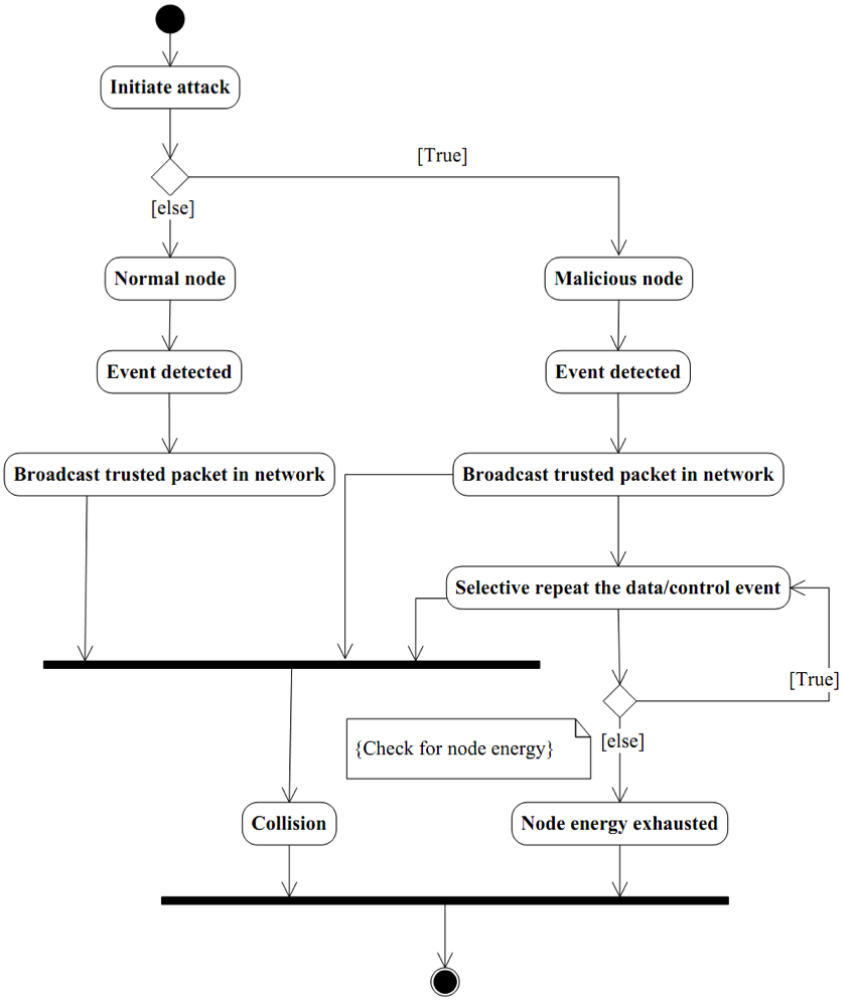


Figure 6.13: Activity diagram of intelligent jamming attack.

of the total throughput of the network due to an increased number of collisions caused by the unauthenticated packets and the following retransmission of packets from trusted nodes.

Unintelligent Replay Attack: The performance degradation due to this attack is more severe than for the unauthenticated broadcast attack because this attack increases the energy consumption by replaying data or control packets and thereby wastes energy. A significant increase in delay can be observed because the node checks for energy at each replay and also requires additional time to carry out the replay. This unnecessary replay keeps the channel busy, which may introduce collisions and prevent transmission of other packets, which result in degradation of the total throughput of the network. The attack has more severe performance degradation than the unintelligent replay attack because it can take place in any situations, i.e. (i) no protocol knowledge, no ability to penetrate, (ii) full protocol knowledge, no ability to penetrate, and (iii) full protocol knowledge, network penetrated.

Exhaustion Attack: The most adverse effect of this attack is that it totally blocks the transmission towards one particular node and blocks this node until its energy is depleted, or the network becomes partitioned.

Collision Attack: The noise packets introduced by this attack result in significant performance degradation due to the increased number of collisions in the network. The collisions lead to performance

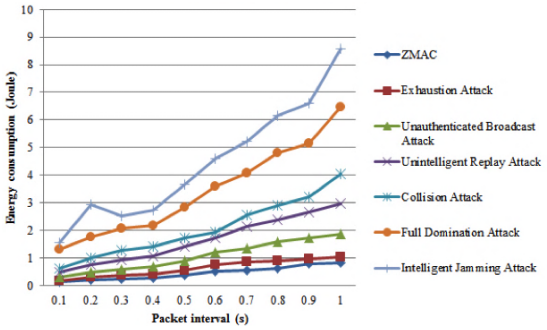
Table 6.1: Simulation and node parameters for simulating attacks on ZMAC.

Parameters	**Setting used**
Wireless Physical	
Network interface type	Wireless Physical
Radio propagation model	Two-Ray Ground
Antenna type	Omni-directional Antenna
Channel type	Wireless Channel
Link Layer	
Interface queue	Priority Queue
Buffer size of IFq	50
MAC	ZMAC
Routing protocol	Ad-hoc Routing
Transport layer protocol	UDP
Traffic model	CBR
Energy Model	
Initial energy (Joule)	100
Idle power (mW)	14.4
Receiving power (mW)	14.4
Transmission power (mW)	36.0
Node Placement and Other Parameters	
Number of nodes	20, 40, 60, 80, 100
Number of sources	19, 39, 59, 79 and 99
Node placement	Random
Placement of nodes and BS	Nodes are placed randomly in a given area, and the BS is placed at the center of the area.
Number of simulation runs	50

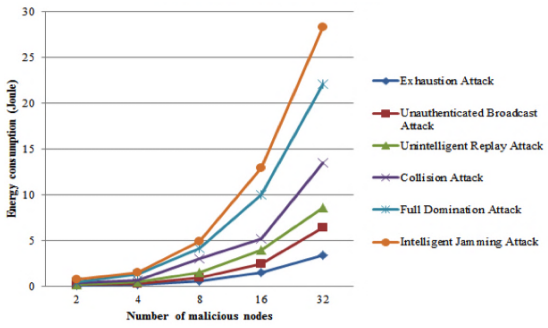
degradation by (i) blocking the channel, (ii) increasing the retransmission of packets, (iii) introducing delays, and (iv) reducing the chances of packets to reach their destination. The effect of collisions is adverse as the traffic load increases.

Full Domination Attack: This attack is a combination of the previously two attacks and, therefore, has more effects that are adverse. The results show that energy, throughput, and delay degradations are much increased compared to the previous attacks as this attack increases the delay and energy consumption by repeatedly broadcasting packets. The repeated broadcast makes the channel always busy, so it will not be available to other nodes to transmit, and it reduces the throughput by not giving the chance to new packets to be transmitted through the network. As for the exhaustion attack, it also partition the network but much faster than the previous attacks.

Intelligent Jamming Attack: This is the most disastrous of the considered attacks because it works intelligently by selectively retransmitting data and control packets. It requires in-depth knowledge of the protocols used in the network. The results show that the performance degradation of this attack is slightly more severe than the full domination attack as this attack intelligently retransmit.

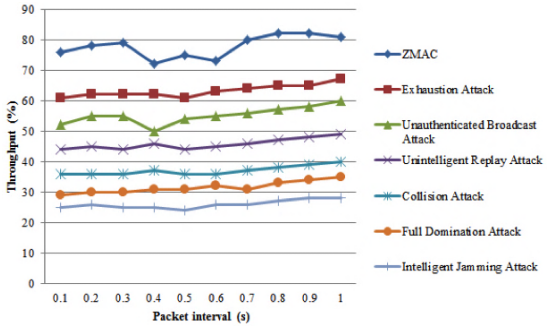


(a) As a function of packet interval.

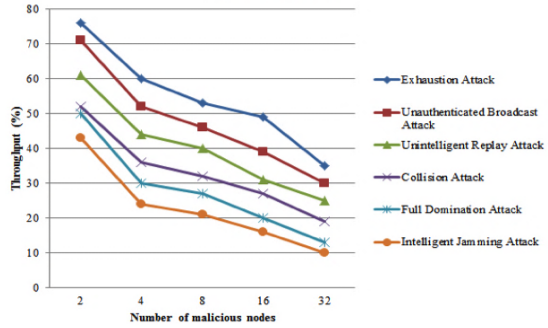


(b) As a function of number of malicious nodes.

Figure 6.14: Results for energy consumption.

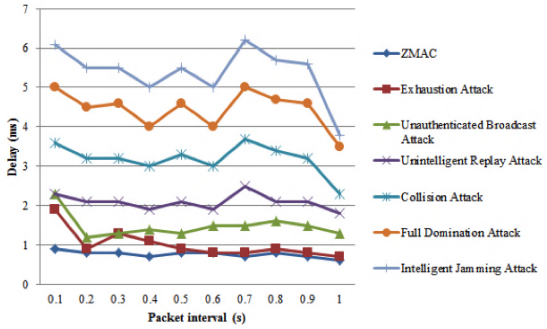


(a) As a function of packet interval.

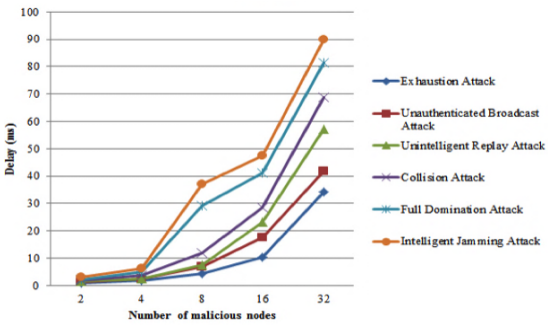


(b) As a function of number of malicious nodes.

Figure 6.15: Results for throughput.



(a) As a function of packet interval.



(b) As a function of number of malicious nodes.

Figure 6.16: Results for delay.

6.4 New Attacks on Hybrid MAC Mechanisms

6.4.1 ECN Attack

Working Mechanism of ECN Attack

In the case of a hybrid MAC mechanism such as ZMAC, an ECN message is used to notify all nodes in the network about a collision. The nodes will get the understanding of the contention using ECN messages, and they will act accordingly using this information. Figure 6.17 shows the normal processing along with the ECN attack. Figure 6.17.a shows the three different paths from the intermediate node that may lead to contention at the intermediate node. The intermediate node experiences the contention and transmits the ECN message to all nodes in the network as shown in Figure 6.17.b. Figure 6.17.c shows the ECN attack in which the malicious node, which has full knowledge of the MAC layer mechanism used, will generate the ECN message and try to confuse the nodes, which disturbs the normal communication of the nodes and also incurs increased consumption of energy.

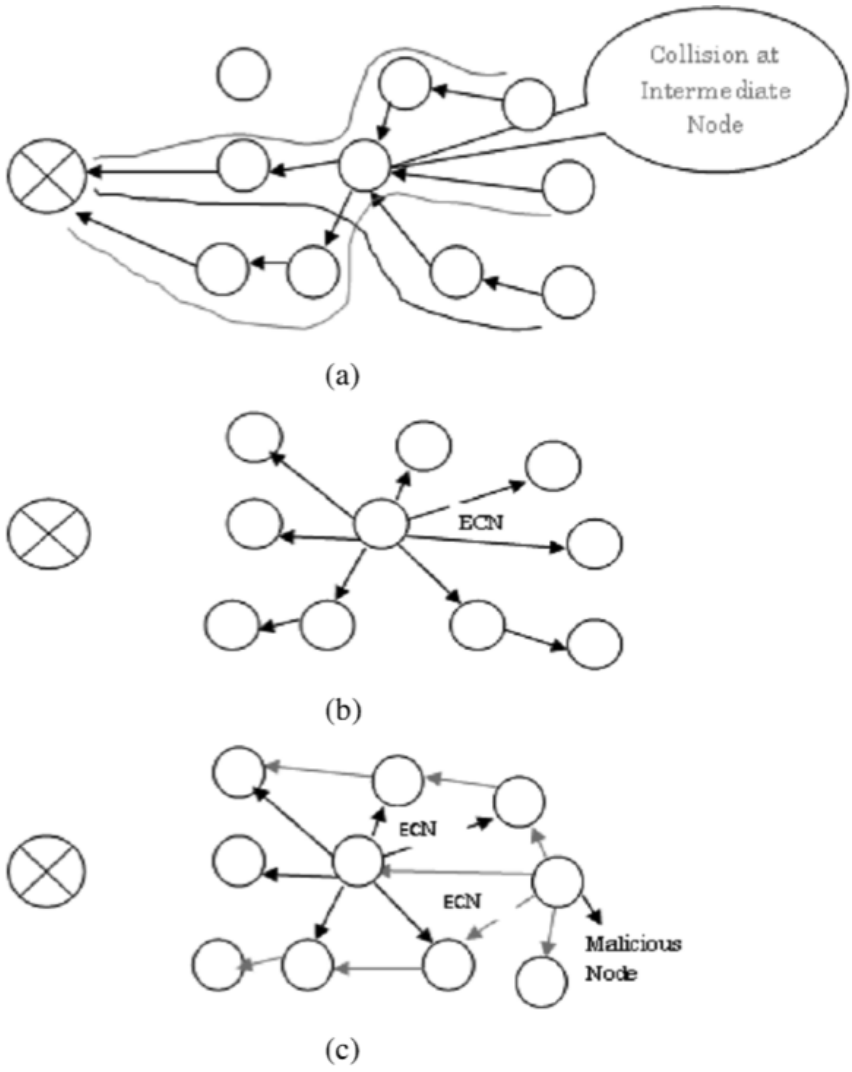


Figure 6.17: (a) Collision at the intermediate node, (b) Intermediate node sends an ECN message to all nodes for collision information, (c) Attack in which malicious node will unnecessarily transmit the ECN message.

Behavioral Modeling of ECN Attack

Figure 6.18 and 6.19 explain the flow of events in case of an ECN attack. The details of each event are as follows,

- *node 4* detects the event and transmits the message towards the sink node via *node 4* $\rightarrow$ *node 3* $\rightarrow$ *node 2* $\rightarrow$ *node 1* to the sink node. During this transmission, *node 3* will detect some event and tries to transmit towards the sink node and experiences the collision at the intermediate *node 2*. *node 2* measures the level of contention and transmits the ECN message to all one-hop and two-hop neighbors in the network.

- The same situation can be observed when *node 3* and *node 2* sense the event and experience the collision at *node 1* after some time. *node 1* transmits the ECN message to the nodes in the network.

- The external attacker compromises the malicious *node 4* by initiating an ECN attack. Once the attack is launched the malicious node transmits the unnecessary ECN messages in the network and confuses the normal communication.

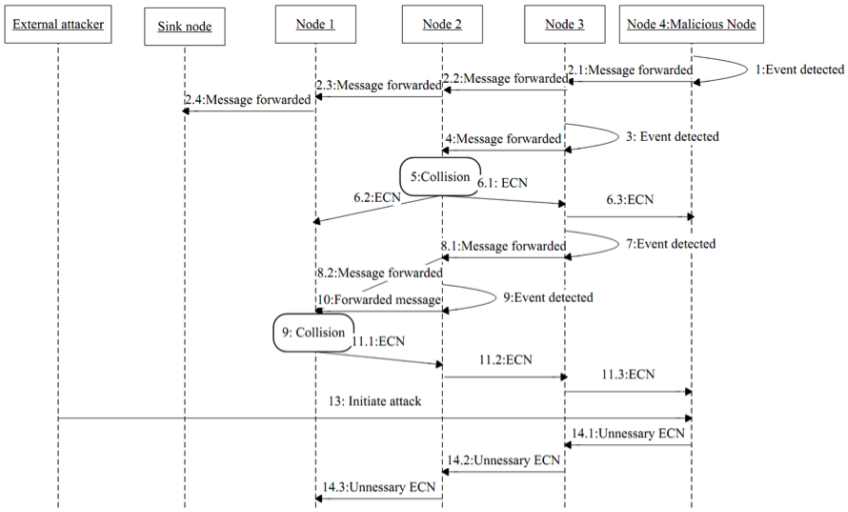


Figure 6.18: Sequential diagram of ECN attack.

6.4.2 CH Attack

Figure 6.20 shows the sequence of activities that happens during the proposed security attack on a cluster-based MAC mechanism [4, 15]. The CH attack considers that intelligent attackers have full knowledge about the WSN and that a cluster-based MAC mechanism is used. Here, the attacker is said to be an intelligent attacker because he can differentiate between a normal node and a CH node, and initiates the attack only if the node is a CH.

A CH is responsible for collecting information from other nodes in the cluster i.e. intra-cluster communication and transmitting the aggregated information to other CHs or the BS i.e. inter-cluster communication. Therefore, an attack on a CH is more harmful than an attack on a normal node. Here, the malicious CH performs the following illegitimate activities,

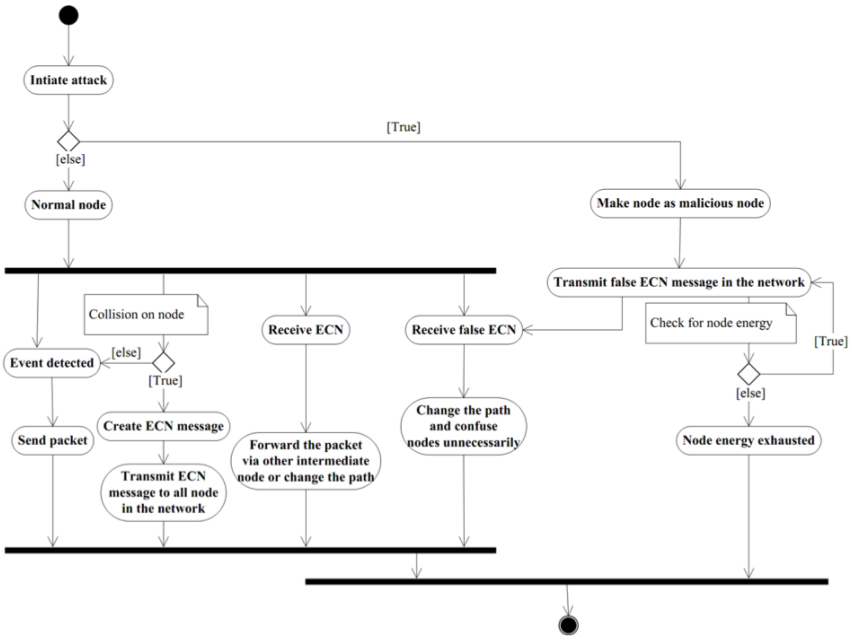


Figure 6.19: Activity modeling of ECN attack.

- The malicious CH will repeatedly retransmit aggregated data towards the BS and other CHs. This repeated retransmission of data towards the BS increases the redundancy of information at the BS, and also leads to incorrect decisions at the BS. The repeated retransmission from the malicious to other CHs increases the energy consumption of both CHs and leads to wrong decisions. The significant impact of this retransmission is that CH energy will deplete and the CH election algorithm needs to run more frequently, which affect the total energy consumption, the lifetime of the network and the throughput of the network.

- The repeated information transmitted from the malicious CH may collide with aggregated information coming from normal CHs and lead to inter-cluster collision. The repeated transmissions also increase inter-cluster collisions, which reduce the performance of overall network.

- The malicious CH has the capability to generate reverse traffic towards normal nodes as links between any normal node and a CH are considered bi-directional. The reverse traffic from the malicious CH may collide with normal traffic coming from the normal node and lead to intra-cluster collision. The increase in intra-cluster collision evades the events detected and affects the overall behavior of the WSN.

- The energy consumption because of inter- and intra-cluster collision depletes the energy of nodes earlier and leads to an earlier partition of the total network and/or cluster.

6.5 GSHMAC: Green and Secure Hybrid Medium Access Control

6.5.1 Introduction

A WSN is subject to different attacks at different layers, but attacks on the MAC layer attacks affect the system more as the MAC layer allocates resources to the system and inefficient allocation of resources

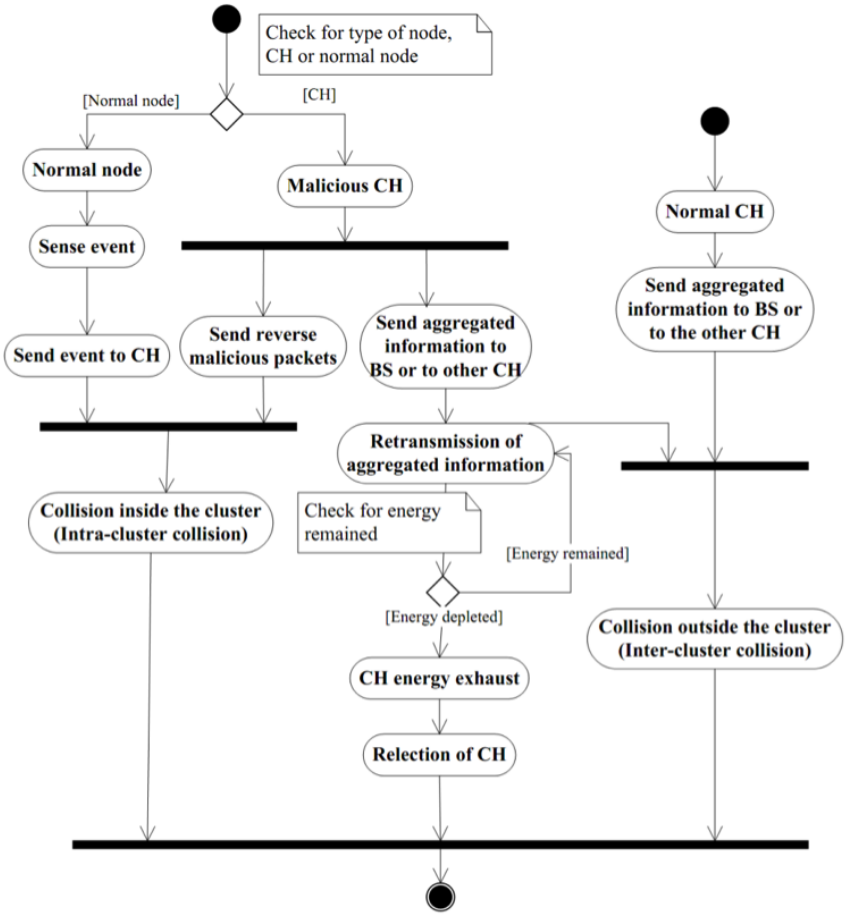


Figure 6.20: Activity modeling of CH attack.

leads to early depletion of energy and increases the resource scarcity in the network. Therefore, it is important to find countermeasures to protect the MAC layer from security attacks. The literature proposes different security solution for MAC layer attacks, but the majority of these solutions are cryptographic and the computational complexity when it comes to WSNs is a concern. Lighter weight solutions for WSNs can be achieved through the internal MAC mechanisms.

This section proposes a novel MAC layer mechanism, GSHMAC, to countermeasure the collision attack, replay attack and full domination attack [10]. It is an extension to GHMAC proposed in Chapter 5. The solution uses the internal MAC mechanisms to enhance the performance in the presence of security attacks. GSHMAC is a cluster-based hybrid MAC mechanism, which uses mixed Time Division Multiple Access (TDMA) and Carrier Sense Multiple Access (CSMA) mode for intra-cluster communication and TDMA mode only for inter-cluster communication. During intra-cluster communication, it shifts the mode according to the collision threshold value. The GSHMAC is already secure to some extent, as it uses cluster-based network for implementation, where an attack in one cluster will not easily penetrate into another cluster. The other security perspective in GSHMAC is the TDMA mode used for inter-cluster communication where, if a node shifts to TDMA mode, it will communicate only during consigned slots. Therefore, the attack will have effects only when malicious nodes steal those slots.

GSHMAC is made more secure by modifying some of the internal mechanisms where it is possible to detect a collision attack using the collision threshold value [17], detect replay attack by maintaining and analyzing the replay counter and detect full domination attack by combining both countermeasures.

The collision attack can be detected in case of collisions introduced after shifting the mode to TDMA and it mitigates the attack by declaring the malicious node by analyzing a Collision Experience (CSE) message. The replay attack is detected by analyzing the replay counter and the node that produces a large amount of reply packets is declared as a malicious node. The full domination attack is detected using both countermeasures as the attack is carried out introducing both collision and replay attacks. The work mainly concentrates on the detection mechanisms, but also includes simple mitigation mechanisms where a node will be removed from the network, once the node is detected and declared as malicious. The proposed secure MAC mechanism, GSHMAC, shows better performance in the presence of different kinds of denial of sleep attacks as compared with state-of-the-art secure MAC mechanisms where it shows improved energy efficiency, delay and throughput. The solution is evaluated for interference on both the same slot and on a random slot.

6.5.2 Related Work

Qingchun Ren et al. [14] presented a secure MAC mechanism using a soft decision theory approach that is developed considering a Request to Send (RTS)/CTS based MAC mechanism. The intrusion detection mechanism proposed for this mechanism uses a collision ratio, probability of successful data packet transmission, data packets waiting time, and RTS packet arrival ratio for making a decision on attacks. It countermeasures the attack by switching a node to sleep mode. The proposed mechanism works for defending against collision, unfairness and exhaustion attacks. A disadvantage of the proposed work is that it considers too many parameters for attack decision that leads to increased computational complexity. The authors. [18] also proposed another optimized secure MAC mechanism based on fuzzy logic. It uses RTS arrival rate, average waiting time, and collision rate as an indicator for attack decision. This mechanism also puts the node in sleep mode once the attack is detected. The work considers collision, unfairness and exhaustion attacks. The complexity of the algorithm increases because of the complex operations performed during fuzzy decisions.

Brownfield et al. [19] studied energy resource vulnerabilities of WSN MAC mechanisms and proposed a new MAC mechanism, Gateway MAC (GMAC), for alleviating the effect of a denial of sleep attack. GMAC uses centralized cluster management to defend against denial of sleep attacks, and the gateway node is responsible for relaying all inter- and intra-network traffic. If the gateway node cannot properly authenticate a packet, it will not forward it to the next node. The responsibilities of the gateway node are alternating based on the reduction of battery level. Here, if the attacker cannot encrypt the Gateway's Traffic Indication Message (GTIM), the other nodes will not accept the attacker's schedule. Therefore, the attack can affect only one node at a time as gateway responsibilities are continually updated. GMAC shows good energy savings in the presence of a denial of sleep attack as compared to other MAC mechanisms. The mechanism shows increased computational and communication overheads because of continuous transfer of gateway responsibilities and authentication of the packet at gateway.

David R. Raymond et al. [20] developed a Cluster Adaptive Rate Limiting (CARL) approach to defend against denial of sleep attacks. It considers the denial of sleep attack involving unauthenticated and replay packets. The rate limiting approach sets the limits on the active period of radio. It improves the defense against attacks by limiting active periods of the high rate malicious traffic. This increases the sleep time of a node and significantly lower the energy usage in the presence of an attack. The authors evaluated the impact of CARL on BMAC protocols, which showed improved energy efficiency. The disadvantages of

CARL are that the network designer has to set the various threshold values to control the rate-limiting behavior and an increase in control traffic.

David R. Raymond et al. [15] made a significant contribution in the area of denial of sleep attacks for WSN MAC mechanisms. They proposed the denial of sleep attacks classification method according to the attacker's knowledge of the MAC mechanism and the capabilities to evade authentication and encryption mechanisms. The paper proposed three different classes of denial of sleep attacks and measured the performance of SMAC, TMAC, BMAC, and GMAC under these. A framework for defense against denial of sleep attacks is also proposed, which consists of active link-layer authentication, anti-replay protection, jamming identification and mitigation, and broadcast attack defense.

Raghavendra V. Kulkarni et al. [21] proposed a secure MAC mechanism based on generalized neurons. The proposed solution is applicable to denial of service attacks on CSMA-based MAC mechanism. The mechanism uses generalized neurons to monitor multiple parameters, which reflect the possibilities of an attack. The critical parameters considered here are collision rate, packet request rate and average packet waiting time. Here, the neurons are trained using a particle swarm optimization mechanism. The algorithm shows improved network lifetime in the presence of an attack. The algorithm is complex and requires extensive training of neurons for attack detection.

Chen Chen et al. [22] proposed a defense mechanism for SMAC. It mainly considers defense against attacks, which have information of the victims such as collision attack, unfairness attack, exhaustion attack, and broadcast attack. The mechanism uses a fake schedule switch scheme with Received Signal Strength Indication (RSSI) measurement, for counter measuring the attack. The mechanism shows decreased packet drops in an attack situation. The disadvantage is that the solution increases the energy consumption and transmission delay because of the fake schedule switch scheme.

P. Sankara Rao et al. [23] presented a multi-layer perception based mechanism for securing CSMA-based MAC mechanism. It increases the security of the MAC mechanism by continuously monitoring for attack situations. The monitoring mechanism uses collision rate, average waiting time and RTS arrival rate as decision parameters. The perception system is trained using back propagation and a radial basis function. The mechanism assures improved performance in the presence of an attack, but does not given any experimental proofs for it.

Ching-Tsung Hsueh et al. [24] proposed the Two-tier Receiver-initiated Secure (TE2S) for WSN denial of sleep attacks. It presents a simplified authenticating process for improving the performance of MAC countermeasures. The proposed scheme is considered as a cross-layer receiver-initiated secure scheme and generates dynamic session keys using a hash chain. These keys are useful for mutual authentication and symmetric encryption keys. It uses a simple and fast Message Digest 5 (MD-5) or Secure Hash Algorithm 1 (SHA-1) for getting the hash-based dynamic session keys. The proposed scheme shows improved defense against attacks and reduced energy consumption. The mechanism increases the computation overheads because of the used cryptographic solutions.

Tapalina Bhattasali et al. [25] presented a distributed collaborative mechanism for detecting sleep deprivation torture in WSNs. The proposed solution uses a hierarchical network framework for a heterogeneous sensor field. Here, the sensor nodes are given various roles based on their battery capacity, such as Sink Gateway (SG), Sector Monitor (SM), Sector In-charge (SIC) and Leaf Node (LN). SICs are used to gather the data sensed by LNs, and the SM is used to detect valid and invalid data. The mechanism promises improved energy efficiency but has not provided any experimental evidences for it.

The above review of related work illustrates that currently available secure MAC mechanisms are based on neural networks, fuzzy and cryptographic approaches. These approaches countermeasure denial of sleep attacks but increase the computational complexity, which raises the overheads on resource constrained WSNs. The proposed solutions are also not tested by considering multiple malicious nodes in the network. Therefore, the motivation of the proposed work is to develop a less computational intensive, energy, delay, and throughput efficient, secure MAC mechanism by considering internal features of hybrid MAC mechanisms.

6.5.3 GSHMAC Mechanism

GSHMAC is a green and secure hybrid MAC mechanism, which uses both TDMA and CSMA mode of communication according to the requirement of the network. It is designed using a cluster-based system model and the assumptions and detailed explanation is given in Chapter 3. To improve the efficiency of the hybrid MAC mechanism, GSHMAC has the following blocks,

Cluster-based topology: This improves the scalability, energy efficiency and contributes to reducing the effect of a security attack because of its inherent security. GSHMAC uses Enhanced Multihop Clustering Algorithm (EMCA) [26] for forming the cluster-based topology.

GCF scheduling algorithm: This is the essential part of the hybrid MAC mechanism, which decides the particular conflict free slot for communication. The hybrid MAC mechanism proposed here uses GCF [27] as a scheduling algorithm, which is explained in the Chapter 3.

Hybrid synchronization mechanism: This is necessary to achieve timing accuracy during node communication and slot assignment. GSHMAC uses a hybrid synchronization for achieving it efficiently [28] where the algorithm uses approximate diffusion based synchronization for intra-cluster communication and tight sender-receiver synchronization for inter-cluster communication.

MAC mode control: GSHMAC uses TDMA mode for inter-cluster communication and TDMA or CSMA mode for intra-cluster communication. The detailed explanation of MAC mode control can be found in Chapter 5.

Countermeasures for WSN MAC attack: The proposed secure hybrid MAC layer mechanism includes countermeasures against WSN MAC layer attacks (collision, replay and full-domination attacks). The proposed solutions use the internal characteristics of the hybrid MAC mechanism such as the collision threshold value for the counter measuring the collision attack and data counter value for the counter measuring the replay attack.

Countermeasure for Collision Attack

In the case of a collision attack, the malicious user has knowledge of the MAC layer mechanism and turns one of the nodes in a network malicious. The malicious node continuously generates packets and keeps the channel busy by increasing the collisions and this increased number of collisions reduces the performance of the network.

The proposed countermeasure is developed considering the hybrid MAC layer mechanism, GHMAC, that changes its mode from CSMA to TDMA and vice-versa according to the amount of traffic in the

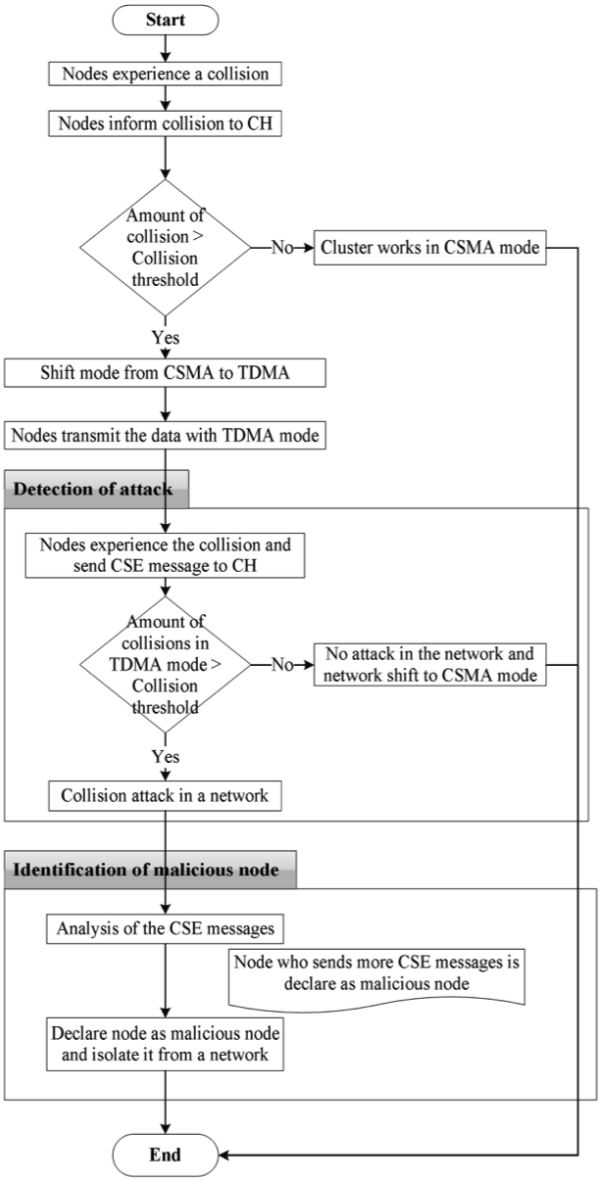


Figure 6.21: Countermeasure for collision attack.

network. The system considers that each CH maintains the collision threshold value and, if the number of collisions in the cluster goes beyond the collision threshold value, the cluster shifts the mode from CSMA to TDMA. The collision threshold considered here is 5% [17], which is the normal collision rate considered in the literature. If the collisions experienced by a node is above the collision threshold, the node shifts the mode, which will happen in case of an attack. In TDMA mode, every node will communicate only in consigning slots, and it is expected that collisions in the network should reduce. However, as the malicious users have knowledge of the MAC layer mechanism used, this user will still be able to introduce collisions into the network. Hence, if a collision is introduced in TDMA mode and it is going beyond the collision threshold value, then a collision attack is detected, and the network will take countermeasures.

Figure 6.21 shows the mechanism to countermeasure the collision attack where the proposed GSH-MAC mechanism considers that if nodes in a cluster experience a collision, it will inform the CH using a CSE message. If the amount of collisions goes beyond the collision threshold value, the cluster will shift

the mode from CSMA to TDMA, and otherwise the cluster will work in CSMA mode. Once the mode is shifted to TDMA, nodes will start to transmit in TDMA mode and, if nodes experience collisions in TDMA mode, the CHs will be informed. If the amount of collisions goes beyond the collision threshold value in TDMA mode, a collision attack is detected and otherwise the network shifts to CSMA mode. The CSE message transmitted from a node contains node ID and information about the collision. Once the collision attack in a network is detected, the system analyzes the CSE message and the node that sent the highest number of CSE messages to the CH is declared a malicious node and isolated from the network by removing all incoming and outgoing links from the node and updating the routing table of the network. The algorithm detects the node that sent the maximum number of CSE message in multi-hop scenario by doing path analysis. During path analysis, it analyses individual node on path for number of CSE message generated and node that generated maximum number of CSE messages is declared as malicious.

The other situation is when collisions are introduced due to misconfiguration of nodes or interference by some other sources. The proposed countermeasure considers such situations as malicious if the collision is caused due to crossing the collision threshold value. The same previously described mechanism will be used to detect misconfigured or interfering node. The proposed countermeasure is not using any cryptographic mechanism to detect the attack, but detects the attack using the internal MAC mechanism.

Countermeasure for Replay Attack

The countermeasure for replay attack on the WSN MAC layer is built up considering that data generated by the node has a unique Identification (ID). Every data packet considered here consist of the node ID, data ID, and information. If a node receives data the same data ID and node ID, it is not in sequence and not following the packet interval gap set in the network, the network has detected a replay attack.

The CH of each cluster maintains a data counter and the initial value of this data counter is N when the network is initialized. The data counter is incremented by one when the event is not a replay event. The system considers that a malicious node replays the same data continuously in the network, without following any packet interval gap between the node. The non-malicious replay is separated out as they are following the allotted packet interval gap.

The mechanism for detecting the replay attack is as shown in Figure 6.22. Here, the node sends a packet to the CH, and if the received packet has the same node ID and data ID as a previously received packet, it is not in expected sequence and not following the packet interval set in the network then the data counter will not be incremented. If the data counter is not incremented, it means that a replay is taking place in the cluster. Replays are one of the signs of a replay attack and, once the replay event is detected, the system analyzes the replayed packets. The node who replayed the maximum number of packets is declared malicious and is isolated from the network.

Countermeasure for Full Domination Attack

The full domination attack is detected on the network by combining the countermeasures of the collision and replay attack. This attack dominates the network by introducing collisions and replays of a large number of events in the network. The malicious collisions are detected using the proposed countermeasures for the collision attack, which uses the collision threshold value and CSE messages to limit the collisions and detect the malicious node. The malicious replay events are identified using the proposed countermeasures for the replay attack, which detect such events using the data counter value and packet interval set in

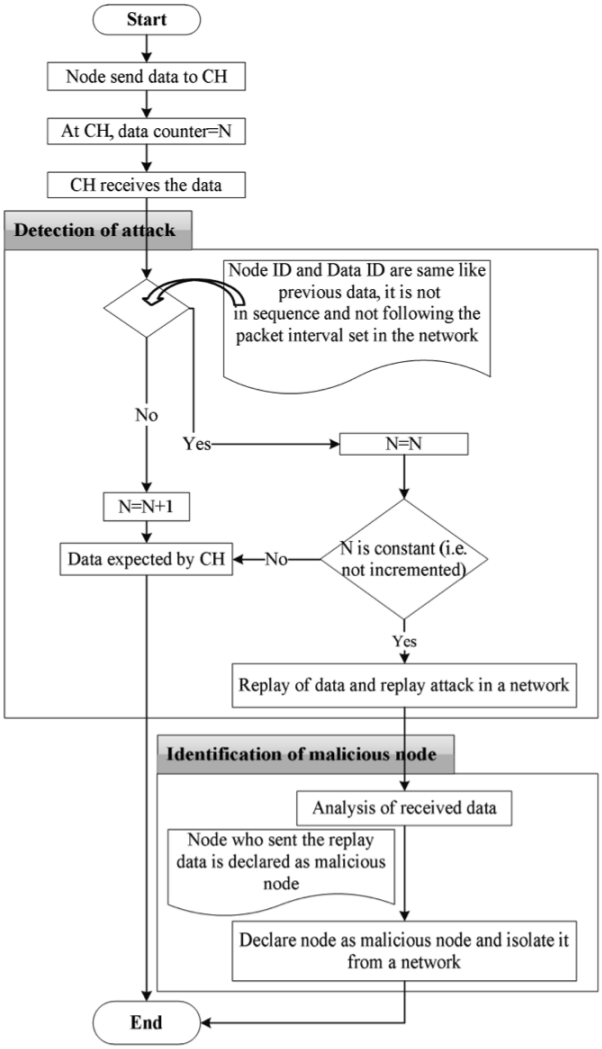


Figure 6.22: Countermeasure for replay attack.

the network. The full domination attack is detected if a collision on the network is introduced due to malicious packets and replay of unnecessary events in the network.

6.5.4 Simulation Results and Discussions

Simulation Details

The simulation of the algorithm is performed using NS-2 and the parameters considered for the simulation are presented in Table 6.2. The simulations are carried out under the assumption that the attacker can initiate an attack from multiple nodes randomly from 1 to 20 malicious nodes in the network. The simulation considers the packet interval as 0.1s.

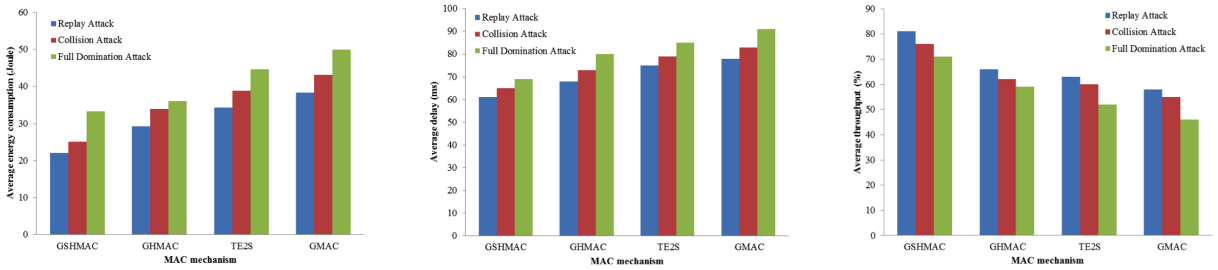
The performance is measured under different denial sleep attacks including replay, collision and full domination attack.

Results for Interference on Same Slot

Figure 6.23a, 6.23b and 6.23c show the average energy consumption, delay, and throughput of GSHMAC, GHMAC, TE2S, and GMAC under different attack situations. Here, the experimentation considers the

Table 6.2: Simulation parameters for simulating GSHMAC.

Parameters	Setting used
Wireless Physical	
Network interface type	Wireless Physical
Radio propagation model	Two-Ray Ground
Antenna type	Omni-directional Antenna
Channel type	Wireless Channel
Link Layer	
Interface queue	Priority Queue
Buffer size of IFq	50
MAC	GHMAC, GSHMAC, GMAC, TE2S
Routing protocol	Ad-hoc Routing
Transport layer protocol	UDP
Traffic model	CBR
Energy Model	
Initial energy (Joule)	100
Idle power (mW)	14.4
Receiving power (mW)	14.4
Transmission power (mW)	36.0
Node Placement and Other Parameters	
Number of nodes	100
Number of sources	99
Number of BS	1
Node placement	Random
Placement of nodes and BS	Nodes are placed randomly in a given area, and the BS is placed at the center of the area.
Clustering Algorithm	EMCA
Number of simulation runs	50

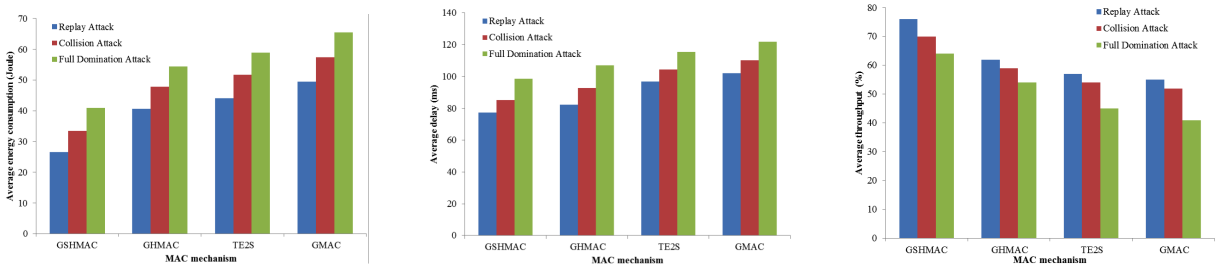


(a) Energy consumption. (b) Delay. (c) Throughput.

Figure 6.23: Comparative results for interference on same slot - all measures are averages.

interference on the same slot. The graph shows that the performance of GSHMAC is better than the other three mechanisms in attack situations because GSHMAC countermeasures the attacks using the internal MAC mechanism. GSHMAC detects the attacks using collision threshold and data counter value and mitigates the attack by isolating the malicious node. TE2S is a receiver-initiated secure MAC mechanism and it also countermeasures the different kinds of denial of sleep attacks, but its performance is worse than GSHMAC as it uses a cryptographic mechanism. The cryptographic approaches used by TE2S increases the communication and key maintenance overheads, which reduces the overall performance of the MAC mechanism. TE2S shows better performance than GMAC as TE2S is Low Power Listening (LPL), where it overcomes GMAC. GMAC is a cluster-based approach, which shows good performance in presence of attacks because of its frame architecture and cluster-based approach used.

The cluster-based approach brings down the penetration of an attack by maintaining a hierarchy of nodes for communication. The MAC mode control mechanism used in GSHMAC also helps to



(a) Energy consumption. (b) Delay. (c) Throughput.

Figure 6.24: Comparative results for interference on random slot - all measures are averages.

countermeasure a collision attack to an extent because as collisions in the network increase, it shifts to TDMA mode. Another reason for GSHMAC being better than the other two mechanisms is that GSHMAC is more accurate to detect collision and domination attack as collisions present in TDMA mode too.

Results for Interference on Random Slots

Figure 6.24a, 6.24b and 6.24c show the average energy consumption, delay, and throughput of GSHMAC, GHMAC, TE2S, and GMAC under different attack situations by considering attacks on random slots. The results from considering attacks on random slots show the increase in average energy consumption and delay, and reduction in average throughput of all four MAC mechanisms. The reason for the reduced performance is that the attack occurs on random slots, which is difficult to detect, as it increases the number of possibilities of node interference.

The effect of interference significantly affects the considered network capacity. In the considered situations, GSHMAC shows improved performance over the other MAC mechanisms because of its internal MAC mechanism for detecting the attack. It detects the attack immediately as the interference affects the number of collisions and, if the collisions go beyond the considered threshold in TDMA mode, the attack will be detected and necessary action is taken by isolating the malicious node. TE2S also shows reduced performance in this random slot scenario situation, as it is difficult to maintain the session keys in the network, which degrades the performance. In GMAC, the centralized gateway node requires more resources to collect all the transmission requirements during a contention period and then schedules their distributions during a reservation-based, contention-free period, if an attack occurs on random slots and interference increases.

6.6 Summary

Detection and prevention from MAC layer attacks is a key security concern to save energy resources in a WSN. This chapter surveyed different WSN MAC security attacks and modeled them to understand the behavior of the attacks for developing more secure MAC mechanisms. As part of the contributions, the behavior of security attacks was modeled using sequential and activity modeling approach approaches to give gives a detailed view of the activities executed during mounting of an attack and the sequence of execution of these activities. The chapter also contributed with simulation results of security attacks on a hybrid MAC mechanism and the results show the network degradation due to the attack under varying traffic and number of malicious nodes. The intelligent jamming attack poses the greatest threat to a WSN because of its intelligent nature, i.e. the attacker has full knowledge of the protocol used and it

can differentiate between control and data packets as well as penetrate the network. The modeling of security attacks and simulation results, in general, gives a high motivation and framework for further investigating efficient and secure MAC mechanisms for WSNs. The chapter proposed two new hybrid MAC mechanism attacks and modeled their behavior i.e. ECN attack and CH attack, based on discussions of hybrid MAC mechanisms and behavior of existing attacks.

In order to enhance the security performance of WSNs and to secure the WSN MAC mechanisms from attacks, the research contributed a cluster-based secure hybrid MAC mechanism, GSHMAC that considers the internal MAC mechanism to countermeasures collision, replay and full domination attacks.

6.7 References

[1] Giuseppe Anastasi, Marco Conti, Mario Di Francesco, and Andrea Passarella. Energy conservation in wireless sensor networks: A survey. *Ad Hoc Netw.*, 7(3):537–568, May 2009.

[2] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer Networks*, 52(12):2292 – 2330, 2008.

[3] Xiangqian Chen, Kia Makki, Kang Yen, and N. Pissinou. Sensor network security: a survey. *Communications Surveys Tutorials, IEEE*, 11(2):52–73, Second 2009.

[4] A. Bachir, M. Dohler, T. Watteyne, and K.K. Leung. Mac essentials for wireless sensor networks. *Communications Surveys Tutorials, IEEE*, 12(2):222–248, Second 2010.

[5] Pranav M. Pawar, Rasmus Hjorth Nielsen, Neeli R. Prasad, Shingo Ohmori, and Ramjee Prasad. Behavioral modeling of wsn mac layer security attacks: A sequential uml approach. *Journal of Cyber Security and Mobility*, 1(1):65–82, 2012.

[6] Pranav M. Pawar, Rasmus Hjorth Nielsen, Neeli R. Prasad, Shingo Ohmori, and Ramjee Prasad. Activity modelling and comparative evaluation of wsn mac security attacks. *Journal of Cyber Security and Mobility*, 1(2):1–20, 2012.

[7] Tom Pender. *UML Bible*. John Wiley & Sons, Inc., New York, NY, USA, 1 edition, 2003.

[8] Sunghyuck Hong and Sunho Lim. Analysis of attack models via unified modeling language in wireless sensor networks: A survey study. In *Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on*, pages 692–696, June 2010.

[9] Injong Rhee, A. Warrier, M. Aia, Jeongki Min, and M.L. Sichitiu. Z-mac: A hybrid mac for wireless sensor networks. *Networking, IEEE/ACM Transactions on*, 16(3):511–524, June 2008.

[10] Pranav M. Pawar, Rasmus Hjorth Nielsen, Neeli R. Prasad, and Ramjee Prasad. Gshmac: Green and secure medium access control for wsn. International Conference in Wireless Communication, Vehicular Technology, Information Theory, Aerospace and Electronics Systems Technology, Hyderabad, India, 2015, 1-5.

[11] Ameer Ahmed Abbasi and Mohamed Younis. A survey on clustering algorithms for wireless sensor networks. *Computer Communications*, 30(14 - 15):2826 – 2841, 2007. Network Coverage and Routing Schemes for Wireless Sensor Networks.

[12] P. Pawar, R. Nielsen, N. Prasad, S. Ohmori, and R. Prasad. Hybrid mechanisms: Towards an efficient wireless sensor network medium access control. In *Wireless Personal Multimedia Communications (WPMC), 2011 14th International Symposium on*, pages 1–5, Oct 2011.

[13] P. Reindl, K. Nygard, and Xiaojiang Du. Defending malicious collision attacks in wireless sensor networks. In *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*, pages 771–776, Dec 2010.

[14] Qingchun Ren and Qilian Liang. Secure media access control (mac) in wireless sensor networks: intrusion detections and countermeasures. In *Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15th IEEE International Symposium on*, volume 4, pages 3025–3029 Vol.4, Sept 2004.

[15] David R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff. Effects of denial-of-sleep attacks on wireless sensor network mac protocols. *Vehicular Technology, IEEE Transactions on*, 58(1):367–380, Jan 2009.

[16] Yee Wei Law, Marimuthu Palaniswami, Lodewijk Van Hoesel, Jeroen Doumen, Pieter Hartel, and Paul Havinga. Energy-efficient link-layer jamming attacks against wireless sensor network mac protocols. *ACM Trans. Sen. Netw.*, 5(1):6:1–6:38, February 2009.

[17] Hal Stern. Chapter 17: Network performance analysis. In Mike Loukides, editor, *Managing NFS and NIS*. O'Reilly & Associates, Inc., Sebastopol, CA, USA, 2nd edition, 2001.

[18] Qingchun Ren and Qilian Liang. Fuzzy logic-optimized secure media access control (fsmac) protocol wireless sensor networks. In *Computational Intelligence for Homeland Security and Personal Safety, 2005. CIHSPS 2005. Proceedings of the 2005 IEEE International Conference on*, pages 37–43, March 2005.

[19] M. Brownfield, Yatharth Gupta, and N. Davis. Wireless sensor network denial of sleep attack. In *Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC*, pages 356–364, June 2005.

[20] David R. Raymond and S.F. Midkiff. Clustered adaptive rate limiting: Defeating denial-of-sleep attacks in wireless sensor networks. In *Military Communications Conference, 2007. MILCOM 2007. IEEE*, pages 1–7, Oct 2007.

[21] R.V. Kulkarni, G.K. Venayagamoorthy, A.V. Thakur, and S.K. Madria. Generalized neuron based secure media access control protocol for wireless sensor networks. In *Computational intelligence in miulti-criteria decision-making, 2009. mcdm '09. ieee symposium on*, pages 16–22, March 2009.

[22] Chen Chen, Li Hui, Qingqi Pei, Lv Ning, and Peng Qingquan. An effective scheme for defending denial-of-sleep attack in wireless sensor networks. In *Information Assurance and Security, 2009. IAS '09. Fifth International Conference on*, volume 2, pages 446–449, Aug 2009.

[23] P.S. Rao, K.V.S.R.P. Varma, R.A. Satapati, and E. Vamsidhar. Multilayer perceptron based secure media access control protocol for wireless sensor networks. In *Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on*, pages 1–5, Dec 2010.

[24] Ching-Tsung Hsueh, Chih-Yu Wen, and Yen-Chieh Ouyang. Two-tier receiver-initiated secure scheme for hierarchical wireless sensor networks. In *ITS Telecommunications (ITST), 2012 12th International Conference on*, pages 254–258, Nov 2012.

[25] Tapalina Bhattasali, Rituparna Chaki, and Sugata Sanyal. Sleep deprivation attack detection in wireless sensor network. *CoRR*, abs/1203.0231, 2012.

[26] Ying Qian, Jinfang Zhou, Liping Qian, and Kangsheng Chen. Highly scalable multihop clustering algorithm for wireless sensor networks. In *Communications, Circuits and Systems Proceedings, 2006 International Conference on*, volume 3, pages 1527–1531, June 2006.

[27] P.M. Pawar, R.H. Nielsen, N.R. Prasad, S. Ohmori, and R. Prasad. Gcf: Green conflict free tdma scheduling for wireless sensor network. In *Communications (ICC), 2012 IEEE International Conference on*, pages 5726–5730, June 2012.

[28] P.M. Pawar, R.H. Nielsen, N.R. Prasad, and R. Prasad. A hybrid algorithm for efficient wireless sensor network time synchronization. In *Wireless Communications, Vehicular Technology, Information Theory and Aerospace Electronic Systems (VITAE), 2014 4th International Conference on*, pages 1–5, May 2014.

Chapter 7

Conclusions and Future Work

This chapter concludes the thesis and proposes the future work based on the research. This thesis addressed the energy consumption and security issues in Wireless Sensor Network (WSN) Medium Access Control (MAC) and proposed a both green and secure MAC mechanism. The major contributions are in the benchmarking for testing of WSN MAC mechanisms, three Time Division Multiple Access (TDMA) scheduling algorithms - Green Conflict Free (GCF), Multi-color-GCF (M-GCF) and Hybrid-GCF (H-GCF), a hybrid synchronization control mechanism, a MAC mode control mechanism, a hybrid MAC mechanism - Green and Hybrid MAC (GHMAC), modeling of WSN MAC security attacks, novel WSN MAC attacks, and countermeasures for denial of sleep attacks. The novel methods together with the implementation and simulation results have been presented in this thesis. Throughout the thesis, either the proof of concept, simulation results or the implementation results are presented to validate the findings.

7.1 Summary of Contributions

This chapter presents the summary of the research work presented in the thesis. It discusses the inference from each of the contributions and which challenges of Wireless Sensor Network (WSN) Medium Access Control (MAC) is addressed by it. The chapter also discusses the future work for each of the presented contributions. The widely growing applications of WSNs demands for energy efficient and secure MAC for efficient management of the constrained resources and, therefore, the work is mainly concentrated on developing a hybrid MAC mechanism that addresses these two requirments.

The focus of Chapter 1 is to give an introduction to and a vision for developing a green and secure hybrid MAC mechanism. It provides insight to the motivation, challenges, novelty, contributions, and research questions and methodology followed. The research identified the challenges of WSN MAC by studying different WSN applications and existing WSN-MAC mechanisms. Energy, delay and throughput efficiency, scalability, adaptivity, mobility-support and security from different denial of sleep attacks are the major challenges identified from the research. Another important challenge is a common testing benchmark framework for measuring performance of WSN MAC mechanisms. The development of a new hybrid MAC mechanism is initiated based on these identified challenges. The hybrid MAC mechanism has three major blocks: 1) Scheduling algorithm, 2) synchronization mechanism and 3) MAC mode control. The challenges are mapped with these three major blocks to develop an efficient hybrid MAC mechanism. Hence, the work is divided into five important modules: 1) Benchmarks for evaluation of WSN MAC mechanisms, 2) scheduling algorithm, 3) synchronization control, 4) MAC mode control and 5) security in MAC.

Chapter 2 proposed benchmark framework for evaluation of WSN MAC mechanisms developed by studying state-of-the-art WSN MAC mechanisms according to use of performance metrics, implementation tools, scenarios and physical parameters. The study showed that individual WSN MAC mechanisms uses a different set of parameters. Therefore, to streamline the testing process, a common set of parameters were proposed in the chapter. The second part of the chapter gave a comparative evaluation of hybrid MAC mechanisms and traditional WSN-MAC mechanisms. The evaluation provided guidelines to improve the performance of hybrid MAC mechanisms in terms of energy, delay and throughput.

Scheduling algorithms are requiring for finding efficient schedules for nodes to communicate and are an important block for effective hybrid MAC mechanisms. The research in Chapter 3proposed three different scheduling algorithms: Green Conflict Free (GCF), Multi-color-GCF (M-GCF) and Hybrid-GCF (H-GCF). These algorithms address the challenges of scheduling algorithms as outlined in Chapter 1. GCF finds a single conflict free schedule across a three-hop neighborhood, while M-GCF finds multiple conflict free schedules. GCF performs well in high mobility conditions, while M-GCF works better in static and low mobility conditions. Therefore, to overcome the challenges of both of these algorithms, H-GCF is proposed, which shifts its mode from GCF to M-GCF and vice-versa according to mobility threshold value.

The performance of the scheduling is affected by the kind of time synchronization used as considered in Chapter 4. A scheduling algorithm requires all nodes to have similar or at least approximate similar notion of time. The research achieves this by proposing a hybrid cluster-based synchronization mechanism, which uses tight synchronization for inter-cluster communication and loose synchronization for intra-cluster communication. The proposed hybrid synchronization algorithm is scalable, energy efficient, fault tolerant and support mobility. It shows improvements in number of synchronization errors and better

energy consumption as compared with sender-receiver and diffusion-based synchronization mechanisms.

MAC mode control is necessary in hybrid MAC to take mode shift decisions - Carrier Sense Multiple Access (CSMA) to Time Division Multiple Access (TDMA) and vice versa, according to traffic conditions inside the network and is addressed in Chapter 5. The chapter presented a collision threshold based MAC mode control for cluster-based hybrid MAC. The chapter also includes proposed work for combining the scheduling algorithm, synchronization mechanism and MAC mode control to form a novel hybrid MAC mechanism, Green and Hybrid MAC (GHMAC). GHMAC shows reduced energy consumption and delay with improved throughput in different static and mobile scenarios of WSNs. It also shows good performance in presence of security attacks (different types of denial of sleep attacks).

Lastly, Chapter 6 of this thesis concerns MAC security centered on WSN MAC attacks and denial of sleep attacks. The research modeled different types of denial of sleep attacks using sequential and activity modeling approaches of Unified Modeling Language (UML) to provide an understanding of the behavior of these attacks and their attack penetration mechanisms. This is a useful tool for implementing and checking the performance of security attacks on hybrid MAC mechanisms. The modeling of the WSN MAC security attacks and the comparative evaluation of the attacks led to the proposal of novel attacks on hybrid MAC mechanisms and motivated finding countermeasure for these. The research proposed a secure scheduling mechanism, which is an extension of the GCF scheduling that finds a conflict free secure slot and improves performance of GCF in presence of a Cluster Head (CH) attack. Lastly, the Green and Secure Hybrid MAC (GSHMAC) mechanism is presented that uses an internal MAC mechanism for counter measuring three different kinds of security attacks: Collision attack, replay attack and full domination attack. The simulation results of GSHMAC shows reduced energy consumption and delay with enhanced throughput, as compared with other state-of-the-art secure MAC solutions.

In conclusion, the work and proposed mechanisms laid forward in this thesis confirms the research hypothesis through the proposal of a green and secure hybrid MAC solution for WSNs that is energy, delay and throughput efficient, scalable, adaptable, secure and supports mobility.

7.2 Future Work

The research contributions in this thesis on hybrid MAC layer solutions make WSNs more energy efficient and secure and are verified under various scenarios. As part of the future work, this research offers a wider scope for improvements including,

- Testing benchmarks for WSN MAC mechanisms can be further extended by designing a standard for such consisting of standardized parameters, performance metrics and scenarios designed according to specific WSN application requirements. This work includes applicability to other wireless networks.

- The scheduling algorithms proposed in this thesis are evaluated in terms of their communication overheads, but the work can further be extended for minimizing computation cost. The M-GCF algorithm assigns multiple slots to a node, which may incur high initial computational cost to assign the slot before the actual communication. Future work can focus on reducing the initial overheads incurred by the algorithm.

- The synchronization mechanism can be further extended by considering more hybridization i.e. the nodes using loose or tight synchronization according to the sensitiveness (or real time requirements) of the traffic.
- The hybrid MAC mechanism can be enhanced further by considering aspects of a Cognitive Radio Network (CRN) where primary and secondary users are competing among themselves for getting the resources.
- Future work in hybrid MAC mechanisms can involve the design according to different mobility pattern such as pedestrian or vehicular mobility pattern.
- The accuracy of the mode shift decisions can be improved by considering multiple parameters including amount of collision or retransmission, network allocation vector, failure of carrier sense, etc.
- The security work can be extended by considering the combined effect of denial of sleep attacks on all layers of WSN protocol stack.
- The security work proposed can be further extended by considering mitigation of attacks.
- The future work in security also includes exploring solutions for other WSN layer attacks using the internal working mechanism of a particular layer protocol.

ISSN (online): 2246-1248
ISBN (online): 978-87-7112-500-9

AALBORG UNIVERSITY PRESS