

Enhancing Network Performance and Security of Limited-Resource Cyber-Physical Networks over Railway Systems and Other Emerging Systems

by

Novia Nurain

DOCTOR OF PHILOSOPHY



Department of Computer Science and Engineering

BANGLADESH UNIVERSITY OF ENGINEERING AND TECHNOLOGY

DHAKA-1000 BANGLADESH

July 2019

PhD Thesis

Enhancing Network Performance and Security of
Limited-Resource Cyber-Physical Networks over Railway
Systems and Other Emerging Systems

A thesis submitted to the Department of Computer Science
and Engineering in partial fulfillment of the requirement for the degree of

DOCTOR OF PHILOSOPHY
IN
COMPUTER SCIENCE AND ENGINEERING


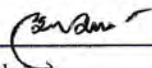
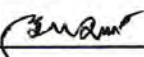
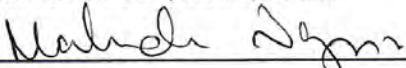

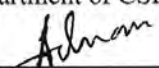
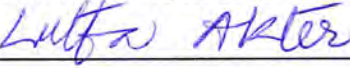

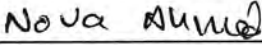
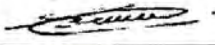
by
Novia Nurain
Student ID 1014054004 P

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
BANGLADESH UNIVERSITY OF ENGINEERING AND TECHNOLOGY
DHAKA 1000, BANGLADESH

July 2019

The thesis titled “Enhancing Network Performance and Security of Limited-Resource Cyber-Physical Networks over Railway Systems and Other Emerging Systems” submitted by Novia Nurain, Roll No. 1014054004P, Session October 2014, to the Department of Computer Science and Engineering, Bangladesh University of Engineering and Technology, has been accepted as satisfactory in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Science and Engineering and approved as to its style and contents on July 23, 2019.

Board of Examiners

1. 
Dr. A. B. M. Alim Al Islam
Associate Professor
Department of CSE, BUET, Dhaka. Chairman
(Supervisor)
2. 
Head
Department of CSE, BUET, Dhaka. (Ex-officio)
3. 
Dr. Md. Mostofa Akbar
Professor
Department of CSE, BUET, Dhaka. Member
4. 
Dr. Mahmuda Naznin
Professor
Department of CSE, BUET, Dhaka. Member
5. 
Dr. S. M. Farhad
Associate Professor
Department of CSE, BUET, Dhaka. Member
6. 
Dr. Muhammad Abdullah Adnan
Assistant Professor
Department of CSE, BUET, Dhaka. Member
7. 
Dr. Lutfu Akter
Associate Professor
Department of EEE, BUET, Dhaka. Member
8. 
Dr. Md. Abdur Razzaque
Professor
Department of CSE, Dhaka University, Dhaka. Member (External)
9. 
Dr. Nova Ahmed
Associate Professor
Department of ECE, North South University, Dhaka. Member (External)
10. 
Dr. Sriram Chellappan
Associate Professor
Department of CSE, University of South Florida,
Tampa, FL 33620, USA. Member (External)

Candidate's Declaration

This is to certify that the work entitled “Enhancing Network Performance and Security of Limited-Resource Cyber-Physical Networks over Railway Systems and Other Emerging Systems” is the outcome of the research carried out by me under the supervision of Prof. Dr. A. B. M. Alim Al Islam in the Department of Computer Science and Engineering, Bangladesh University of Engineering and Technology, Dhaka-1000. It is also declared that this thesis or any part of it has not been submitted elsewhere for the award of any degree or diploma.

Novia Nurain

Novia Nurain
Candidate

Dedication

To my Parents and my brother

Contents

<i>Candidate's Declaration</i>	ii
<i>Candidate's Dedication</i>	iii
Acknowledgments	xix
Abstract	xx
1 Introduction	3
1.1 Research Focus 1: Real-Time Limited-Resource Cyber-Physical Networks over Railway Systems	8
1.2 Research Focus 2: Miniature Versions of Limited-Resource Cyber-Physical Networks	12
1.3 Research Focus 3: Smarter Versions of Limited-Resource Cyber-Physical Networks	17
1.4 Our Contributions	20
1.5 Organization of the Thesis	23
1.6 Conclusion	23
I Real-Time Limited-Resource Cyber-Physical Networks	24
2 Integrated Networking Solution for Real-Time Detection of Missing Rail Blocks	25
2.1 Introduction	25
2.2 Related Work	27
2.3 Problem Formulation and System Model	29
2.3.1 Research Context	29
2.3.2 Proposed System Model	30

2.3.3	Node Deployment Topology and Network Architecture	33
2.4	Protocols in Our Proposed Paradigm	36
2.4.1	Cross-layer Protocol Stack	36
2.4.2	Operational Overview of the Protocols	38
2.4.3	Communication Overhead	40
2.4.4	Application Layer Protocol	41
2.4.4.1	Application layer in the inspector node	41
2.4.4.2	Application layer in the sensor node	42
2.4.5	Transport Layer Protocol	42
2.4.5.1	Transport layer in the inspector node	43
2.4.5.2	Transport layer in the sensor node	44
2.4.5.3	Responses towards packet loss	44
2.4.6	Network Layer Protocol	46
2.4.7	Data Link Layer and Physical Layer Protocols	46
2.5	Adjustment of the Operational Parameters	46
2.5.1	Bound of Timers and Thresholds	47
2.5.2	Impacts of Parameters on Network Performance	48
2.5.2.1	Simulation settings	48
2.5.2.2	Simulation results	50
2.6	Performance Evaluation	53
2.6.1	Performance Comparison against Different Alternatives	53
2.6.2	Justifications behind Adopting Different Alternatives	56
2.7	Performance Evaluation through Real Deployment on a Railline	57
2.7.1	Settings of Real Deployment	57
2.7.2	Results from Real Deployment	58
2.8	Implementation Aspects of Our Proposed Network Paradigm	60
2.8.1	Robustness against Real-world Communication Problems	60
2.8.2	Robustness of Reporting	60
2.8.3	Failure of Sensors	61
2.8.4	Commercialization Requirement	61
2.8.5	Cost Analysis	62

2.9	Conclusion	63
3	Exploring Imminent Vulnerabilities, Attacks, and Countermeasures in Real-Time System for Detecting Missing Rail Blocks	64
3.1	Introduction	64
3.2	Related Work	67
3.3	Different Security Attacks in Real-Time System for Detecting Missing rail blocks	68
3.3.1	Power Attack	69
3.3.2	Attack Models for Power Attack	69
3.3.3	Mathematical Model for Energy Consumption of Sensor Nodes	71
3.3.4	Man-in-the-middle (MITM) Attack	74
3.3.5	Replay Attack	76
3.4	Countermeasures	76
3.4.1	Mitigating Power Attack	76
3.4.2	Preventing Man-in-the-middle (MITM) Attack	79
3.4.3	Defeating Replay Attack	79
3.5	Experimental Evaluation of Power Attack	83
3.5.1	ns-2 Simulation	83
3.5.1.1	Simulation settings	85
3.5.1.2	Impacts of power attack	86
3.5.1.3	Verification of mathematical modelling of power attack	88
3.5.1.4	Performance evaluation of countermeasures	93
3.5.2	Real Deployment on Rail Lines	96
3.5.2.1	Experimental settings	96
3.5.2.2	Performance evaluation of power attack and countermeasures	97
3.6	Conclusion	101

II Miniature Versions of Limited-Resource Cyber-Physical Networks

4	Exploring Network-Level Performances of Wireless Nanonetworks Utilizing Gains of Different Types of Nano-Antennas with Different Materials	104
4.1	Introduction	104
4.2	Motivation and Related Work	107
4.3	Methodology of Our Work	113
4.4	Analytical Models of Nano-Antennas	113
4.4.1	Gain of Patch Nano-Antenna	114
4.4.2	Gain of Dipole Nano-Antenna	115
4.4.3	Gain of Loop Nano-Antenna	116
4.5	Numerical Simulation of Gain for Different Types of Nano-Antennas	117
4.5.1	Simulation Settings	117
4.5.2	Simulation Results	118
4.6	Network Model	121
4.7	Experimental Results and Analysis	123
4.7.1	Customization in $ns-2$	123
4.7.2	Experimental Settings	124
4.7.3	The Impact of Network Size	126
4.7.4	The Impact of the Traffic Rate	127
4.7.5	The Impact of the Node Speed	128
4.8	Summary of Findings	129
4.9	Conclusion	131
5	Power Attack: An Emerging Threat in Health-care Applications Using Medical Body Area Networks	134
5.1	Introduction	134
5.2	Background on MBANs	137
5.3	Power Attack and Attack Models	138
5.4	Viability Analysis of Power Attack	140
5.4.1	Mannasim Simulator	141
5.4.2	Simulation Setup	141
5.4.3	Impacts of Diverse Types of Data on Energy Consumption	142

5.4.4	Impact of Variation in Number of Sensor Nodes on Energy Consumption	144
5.4.5	Impact of Variation in Simulation Time on Energy Consumption	144
5.4.6	Simulation Findings	145
5.5	Countermeasure of Power Attack	145
5.6	Experimental Evaluation	146
5.6.1	Simulation Setup	146
5.6.2	Simulation Results	147
5.7	Conclusion	148

III Smarter Versions of Limited-Resource Cyber-Physical Networks **149**

6	General-Purpose Multi-Objective Vertical Hand-off Mechanism Exploiting Network Dynamics for mobile devices	150
6.1	Introduction	150
6.2	Related Work	153
6.3	System Model	156
6.4	Vertical Hand-Off Mechanism Using MOVH	156
6.4.1	Decision Parameters	157
6.4.2	Multi-Objective Optimization in MOVH	157
6.4.3	MOGA Description	158
6.4.3.1	Chromosome representation	159
6.4.3.2	Initial population	159
6.4.3.3	Parent selection	160
6.4.3.4	Crossover, mutation, and feasibility check	161
6.4.3.5	Population replacement	161
6.4.3.6	Termination	161
6.4.4	Settings of Operational Parameters of MOVH	162
6.4.5	Key Features of MOVH	162
6.5	Stability & Scalability of MOVH	162
6.6	Performance Evaluation	164

6.6.1	Test-bed Evaluation	165
6.6.1.1	Test-bed settings	165
6.6.1.2	Parameter selection	166
6.6.1.3	Experimental results	167
6.6.1.4	Resource overhead	168
6.6.2	Simulation Evaluation	169
6.6.2.1	Simulation settings	169
6.6.2.2	Simulation results with the variation in speed	170
6.6.2.3	Simulation results with the variation in packet rate	172
6.6.2.4	Simulation results with the variation in network size	172
6.6.2.5	Simulation results for illustration of stability	172
6.6.2.6	Justification of simulation results	174
6.7	Other Aspects of MOVH	175
6.7.1	Variations in Weights	175
6.7.2	Consideration of Constraints in Objective Function	176
6.7.3	Normalization of Decision Parameters	176
6.8	Conclusion	176
7	An Empirical Study Based Feasibility Analysis on Mathematical Modeling for MANETs	177
7.1	Introduction	177
7.2	Related Work	179
7.3	Empirical Study	179
7.3.1	Simulation Results	180
7.3.1.1	UDP with AODV	181
7.3.1.2	UDP with DSDV	184
7.3.1.3	TCP Vegas with AODV	186
7.3.1.4	TCP Vegas with DSDV	188
7.3.1.5	TCP Westwood with AODV	189
7.3.1.6	TCP Westwood with DSDV	191
7.4	Discussion	193
7.4.1	Analysis of Feasibility	197
7.5	Conclusion	200

8 Conclusions	203
8.1 Future Work	207
List of Publications	211
References	213

List of Figures

1.1	Diversified applications of infrastructure networks [1]	3
1.2	Interconnection between cyber and physical objects [2]	4
1.3	Applications of cyber-physical networks	5
1.4	An overview of different research studies done under this thesis	7
1.5	Different occurrences of derailments	9
1.6	Reasons behind occurrences of derailments	9
1.7	System diagram of WSN-based real-time missing rail block detection system [3]	11
1.8	Comparison of size of nano device	12
1.9	A typical nano-machines	13
1.10	Classical applications of nanonetworks	14
1.11	Basic framework of a medical body area network [4]	15
1.12	Different sensors in a MBAN [4]	16
1.13	Multi-radio smartphone [5]	17
1.14	Diversified applications of MANETs	19
2.1	Railway track	30
2.2	Simplified block diagram of the system model	30
2.3	Our sensor node with its real deployment	31
2.4	Outputs generated by our sensor node	31
2.5	Node deployment and communication scenarios	33
2.6	Communication scenarios in reverse direction	35
2.7	Cross-layer protocol stack	36
2.8	Packet format in our proposed communication paradigm	37
2.9	Time-sequence diagram of operations of our protocols	38

2.10	Transmission of packets from a sensor node to the train and to other sensor node	40
2.11	State diagrams of operation in the Application layer	41
2.12	Transport layer protocol in the Inspector node	42
2.13	Transport layer protocol in the sensor node	43
2.14	Topology for 10km long rail track	52
2.15	Snapshot of our real deployment	57
3.1	Attack models of power attack	70
3.2	Transfer of the packets between an adversary node (an) and an sensor node (sn) under attack	72
3.3	Man-in-the-middle (MITM) attack in real-time system for detecting missing rail blocks	75
3.4	Replay attack in missing rail block detection system	75
3.5	Timing diagram for sensors on the rail track	77
3.6	Working principle of the countermeasure deployed into the sensor node on the rail track	82
3.7	Attack-defense-practical vulnerabilities tree for real-time missing rail block detection system	84
3.8	Attack scenarios of MITM attack and jamming attack	87
3.9	Impacts of different attacks on the energy consumption of sensor devices . .	87
3.10	Impact of varying interval between attacks on the energy consumption by the sensor node under attack for static attack model	89
3.11	Impact of varying interval between attacks on the energy consumption by the very next sensor node under attack for static attack model	90
3.12	Impact of varying total attack time on the energy consumption by the sensor node under attack for static attack model	91
3.13	Impact of varying total attack time on the energy consumption by the very next sensor node under attack for static attack model	92
3.14	Impact of varying speed of the train on the energy consumption by the sensor node under attack for mobile attack model	93
3.15	Impact of varying speed of the train on the energy consumption by the very next sensor node under attack for mobile attack model	94

3.16	Impact of varying interval between attacks on the energy consumption by the sensor node under attack for mobile attack model	95
3.17	Impact of varying interval between attacks on the energy consumption by the very next sensor node under attack for mobile attack model	96
3.18	Impact of varying total attack time on the energy consumption by the sensor node under attack for mobile attack model	97
3.19	Impact of varying total attack time on the energy consumption by the very next sensor node under attack for mobile attack model	98
3.20	Performance comparison of countermeasures for varying interval between attacks on the energy consumption by the sensor node under attack	98
3.21	Performance comparison of countermeasures for varying interval between attacks on the energy consumption by the very next sensor node under attack	99
3.22	Performance comparison of countermeasures for varying total attack time on the energy consumption by the sensor node under attack	100
3.23	Performance comparison of countermeasures for varying total attack time on the energy consumption by the very next sensor node under attack	101
3.24	Real deployment	101
3.25	Power consumption during real deployment of the power attack and countermeasures for (a) sensor node under attack and (b) the very next sensor node under attack	102
4.1	Impact on gains for varying frequencies over different types of nano-antennas	118
4.2	Impact on gain for varying heights and lengths of patch nano-antennas using different types of materials	119
4.3	Impact on gains for varying height and widths of patch nano-antennas using different types of materials	120
4.4	Impact on gains for varying length of dipole nano-antennas using different types of materials	121
4.5	Impact on gains for varying radius of loop nano-antennas using different types of materials	122
4.6	Network model	122
4.7	Impacts of variation in network size of nanonetworks using patch nano-antennas	125

4.8	Impacts of variation in network size of nanonetworks using dipole nano-antennas	126
4.9	Impacts of variation in network size of nanonetworks using loop nano-antennas	127
4.10	Impact of variation in the traffic rate of nanonetworks using patch nano-antennas	128
4.11	Impact of variation in traffic rate of nanonetworks using dipole nano-antennas	129
4.12	Impact of variation in the traffic rate of nanonetworks using loop nano-antennas	130
4.13	Impact of variation in speed of nodes in nanonetworks using patch nano-antennas	131
4.14	Impact of variation in speed of nodes in nanonetworks using dipole nano-antennas	132
4.15	Impact of variation in speed of nodes in nanonetworks using loop nano-antennas	133
5.1	Architecture of a medical body area network [6]	136
5.2	Architecture of Tier-1-Comm: a) wired; b) wireless; c) cluster and wired; and d) cluster and wireless	138
5.3	Attack models of power attack for different architectures	139
5.4	Impact of data types on energy consumption of MBANs	142
5.5	Impact of different types of data on energy consumption of personal server .	143
5.6	Impact of variation in number of sensor nodes on energy consumption of MBANs	144
5.7	Impact of variation in simulation time on energy consumption of MBANs .	145
5.8	Energy consumption of ECG sensor at different query interval	147
6.1	Relative signal strengths of different wireless networks available in nearby public places of a university premise	151
6.2	Vertical hand-off over heterogeneous networks	156
6.3	Flow diagram of MOGA	159
6.4	Crossover and mutation processes of MOVH	160
6.5	Convergence of GA and MOVH	163
6.6	Test-bed deployments for both indoor and outdoor experiments (red circles denote destination devices	166

6.7	Performance evaluation and operational overhead for GRA, TOPSIS, and MOVH	167
6.8	Impact of variation in speed of nodes on different performance metrics using GRA, TOPSIS, and MOVH	170
6.9	Impact of variation in the packet rate on different performance metrics using GRA, TOPSIS, and MOVH	171
6.10	Impact of variation in network size on different performance metrics using GRA, TOPSIS, and MOVH	173
6.11	Network setting for evaluation of stability	173
7.1	Impact of variation in network size on different performance metrics while using UDP with AODV	181
7.2	Impact of variation in speed of the nodes on different performance metrics while using UDP with AODV	182
7.3	Impact of variation in packet rate on different performance metrics while using UDP with AODV	183
7.4	Impact of variation in the number of maximum allowed connections among the nodes on different performance metrics while using UDP with AODV	184
7.5	Impact of variation in network size on different performance metrics while using UDP with DSDV	185
7.6	Impact of variation in speed of the nodes on different performance metrics while using UDP with DSDV	186
7.7	Impact of variation in packet rate on different performance metrics while using UDP with DSDV	187
7.8	Impact of variation in the number of maximum allowed connections among the nodes on different performance metrics while using UDP with DSDV	188
7.9	Impact of variation in network size on different performance metrics while using TCP Vegas with AODV	189
7.10	Impact of variation in speed of the nodes on different performance metrics while using TCP Vegas with AODV	190
7.11	Impact of variation in packet rate on different performance metrics while using TCP Vegas with AODV	191

7.12	Impact of variation in the number of maximum allowed connections among the nodes on different performance metrics while using TCP Vegas with AODV	192
7.13	Impact of variation in network size on different performance metrics while using TCP Vegas with DSDV	193
7.14	Impact of variation in speed of the nodes on different performance metrics while using TCP Vegas with DSDV	194
7.15	Impact of variation in packet rate on different performance metrics while using TCP Vegas with DSDV	194
7.16	Impact of variation in the number of maximum allowed connections among the nodes on different performance metrics while using TCP Vegas with DSDV	195
7.17	Impact of variation in network size on different performance metrics while using TCP Westwood with AODV	195
7.18	Impact of variation in speed of the nodes on different performance metrics while using TCP Westwood with AODV	196
7.19	Impact of variation in packet rate on different performance metrics while using TCP Westwood with AODV	196
7.20	Impact of variation in the number of maximum allowed connections among the nodes on different performance metrics while using TCP Westwood with AODV	197
7.21	Impact of variation in network size on different performance metrics while using TCP Westwood with DSDV	198
7.22	Impact of variation in speed of the nodes on different performance metrics while using TCP Westwood with DSDV	199
7.23	Impact of variation in packet rate on different performance metrics while using TCP Westwood with DSDV	199
7.24	Impact of variation in the number of maximum allowed connections among the nodes on different performance metrics while using TCP Westwood with DSDV	200

List of Tables

2.1	Simulation parameters	48
2.2	Impacts on distance and different performance metrics for varying values of timers and thresholds	49
2.3	Impact of variation in number of sensor nodes on performance metrics . . .	51
2.4	Impact of speed variation on performance metrics	51
2.5	Impact of direction of train’s route on performance metrics	51
2.6	Impact of varying packet error rate on performance metrics	51
2.7	Performance of our proposed protocol for parallel rail tracks	52
2.8	Performance evaluation of our protocol with respect to different alternative protocols	54
2.9	Percentages of improvement using our protocol with respect to different alternative protocols	54
2.10	Network lifetime using our protocol with respect to different alternative protocols for different intervals between arrivals of two successive trains	56
2.11	Experimental results from real deployments	58
2.12	Effect of speed variation on end-to-end delay (ms)	59
2.13	Comparison with well-known protocols	59
2.14	Breakdown of cost of different hardware components of our system	62
3.1	Simulation parameters	85
3.2	Response time for different types of security attacks	88
3.3	Response time of the train for different events	100
4.1	Simulation parameters	125
5.1	Data rates of different bio-sensors	142

6.1	Globally-accepted ranges for values of different parameters in various wire- less networks	164
6.2	% improvement in different metrics using MOVH	168
6.3	Selection of different networks	174
6.4	Percentages of improvement in energy consumption using MOVH	175
6.5	Percentages of improvement in average throughput, delay, and service cost using MOVH	175
7.1	Network parameters	180
7.2	Simulation parameters	180
7.3	Summary of all simulation results	201
7.4	Co-efficients for varying packet rate for UDP with AODV	201
7.5	Summery of all co-efficients of higher order functions for average delay for variation in network size	202
7.6	Summery of all co-efficients of higher order functions for delivery ratio for variation in network size	202

Acknowledgments

All praises due to Allah, the most benevolent and merciful.

At first, I thank almighty Allah for all His mercy throughout my journey in pursuit of PhD degree. He has bestowed his blessings on me and my parents so that I could move forward with my studies and research and my parents could bear with me with patience during this time. Allah made it easy when the pressure of PhD becomes unbearable.

Next, I express my deepest gratitude to my supervisor Professor Dr. A. B. M. Alim Al Islam for his guidance on this long journey of Ph.D. and showing me the path of conducting a successful research. He shared his wisdom with me in analyzing subject matters and at the same time valued my thoughts to synthesize those topics. He taught me how to write academic papers. His support gave me strength at the time of my disappointment. Without his continuous motivation and encouragement, I could not have finished this writing.

Finally, I want to express my deepest gratitude to my parents and my brother for always believing in me even at the moment when I am losing my confidence.

Abstract

The rapid development of diversified applications of infrastructure networks (e.g., transportation and health-care systems) facilitate the emergence of a new engineering network called cyber-physical networks. These networks face challenges in road to enhancing network performance and security of cyber-physical networks owing to limited resource issues. These limited resource issues include limited amount of available energy to feed the system, low processing capability, limited amount of storage space, and low bandwidth for network communication. Therefore, in this thesis, first, a low-cost lightweight integrated networking solution is proposed for a limited-resource cyber-physical network, which is aimed for real-time detection of missing rail blocks on a railway track. Existing research studies pertinent to railway transportation systems mainly focus on wireless network based solutions for precise localization of trains and non-real-time monitoring of rails for cracks, small breakage, and corrugation. To the best our knowledge, these solutions are not developed through focusing on real-time missing rail block detection as the predominant concern and are not amenable to address the concern. Furthermore, some of these solutions exploit a technique of using high-voltage signal over rail tracks in developed countries. However, in developing countries such as Bangladesh, India, Kenya, etc., where the rail tracks are publicly open, using this sort of technology poses a significant threat to living bodies that are in proximity or even come in contact with the rail lines. Therefore, in this thesis, we introduce a new low-cost lightweight networking paradigm for detecting missing rail blocks.

The proposed networking paradigm is exposed to different security vulnerabilities associated with the inclusion of cyber-physical networks. Existing studies in this regard mainly focus on developing attacks covering replay attack, displacement attack, jamming attack, etc., and their corresponding countermeasures for a Balise-based train control system, which are

not directly applicable to the proposed paradigm intended for detecting missing rail blocks. Therefore, in this regard, we introduce a new security threat entitled as power attack exploiting vulnerability pertinent to the low energy source adopted in the proposed paradigm. Consequently, we develop and thoroughly analyzed potential countermeasures for the power attack. Combining all the countermeasures, an integrated networking solution for the purpose of detecting missing rail blocks will be developed. We perform extensive experimentation using both `ns-2` simulator and real deployment to investigate the applicability and the effectiveness of our proposed networking solution as well as countermeasures the real-time system for detecting missing rail blocks.

Next part of this research, we focus on network-level performance and security of miniature versions of limited-resource cyber-physical networks, i.e., nanonetworks and body area networks. Existing studies in this regard focus on performance enhancement of nanonetworks via designing new channel models and routing protocols. However, the impacts of different types of nano-antennas having different materials on the network-level performances of the wireless nanonetworks remain still unexplored in the literature. Therefore, in this research, we explore the impacts of using different well-known types of antennas such as dipole, patch, and loop (having different alternative materials available to date, i.e., copper, graphene, and carbon nanotubes) on the network-level performance of wireless nanonetworks from various perspectives such as network throughput, end-to-end delay, delivery ratio, and drop ratio. We perform rigorous simulation using our customized `ns-2`. Our evaluation demonstrates that a dipole nano-antenna using copper material exhibits around 51% better throughput and about 33% better end-to-end delay compared to other alternatives. Besides, a new security attack entitled power attack, as well as a countermeasure, is also introduced in this research for body area networks, which is a special type of limited-resource cyber-physical networks composed of low-power wearable or implanted wireless medical sensor devices. We analyze the viability of performing power attack in medical body area networks in reality and effectiveness of proposed countermeasure using `Mannasim`.

Finally, in this thesis, we focus on the other extreme of the limited-resource cyber-physical networks, i.e., smarter version comprising of multi-radio smart devices such as smartphones and tablets. Security aspects of such networks have already been widely ex-

plored from different perspectives in the literature. Therefore, in this work, we propose a multi-objective vertical hand-off mechanism to enhance the network-level performance from various perspectives of both network and device-level metrics such as energy consumption, throughput, delay, etc. which yields better scalability and stability. We conduct evaluation comprising both test-bed experiments and ns-2 simulation. The results from both test-bed experiments and ns-2 simulation demonstrate that our proposed mechanism has significant performance improvement over existing state-of-the-art approaches such as GRA and TOPSIS. Furthermore, we endeavor to formulate mathematical models for the different performance metrics of mobile wireless networks. We perform rigorous simulation utilizing ns-2 to capture the performance of mobile wireless networks under diversified settings and develop a lemma as follows: mathematical modeling of mobile wireless networks considering variation in all parameters is not feasible.

Acronyms

ns-2	Network simulator 2. 11
AODV	Ad hoc On-Demand Distance Vector. 53
BANs	Body area networks. 6
BS	Base Station. 15
CPNs	Cyber-physical networks. 3
CTS	Clear to send. 48
DD	Directed Diffusion. 53
DSDV	Destination-Sequenced Distance-Vector. 55
DSR	Dynamic Source Routing. 55
GRA	Grey Relational Analysis. 18
GSM-R	Global System for Mobile Communications Railway. 10
LTE	Long-Term Evolution. 17
MANETs	Mobile ad-hoc networks. 18
MBANs	Medical body area networks. 15
MITM	Man-in-the-middle. 20
MOVH	Multi-objective vertical hand-off mechanism. 18
MU	Mobile Unit. 15
RMST	Reliable Multi-Segment Transport. 53
RTS	Request to send. 48

- SAW** Simple Additive Weighting. 18
- SINR** Signal to interference ratio. 18
- TOPSIS** Technique for Order Preference by Similarity to Ideal Solution. 18
- UMTS** Universal Mobile Telecommunications Service. 17
- WSNs** Wireless sensor networks. 10

Chapter 1

Introduction

The recent proliferation of technological progression in semiconductor design, material sciences, and networking paves ways for diversified applications of infrastructure networks, e.g., transportation, smart spaces, health-care systems, industrial, and sensors networks (exhibited in Fig. 1.1). Such applications facilitate the emergence of a new engineering network called Cyber-physical networks (CPNs).

Cyber-physical networks comprise two components: one is *cyber* and other is *physical*. Here, cyber implies integration of 3 Cs, i.e., computation, communication, and control.



(a) Transportation Systems



(b) Health-care Systems



(c) Smart spaces



(d) Industrial systems

Figure 1.1: Diversified applications of infrastructure networks [1]

Physical implies natural and human-made networks governed by the laws of physics and operating in real-time. Hence, cyber-physical network resembles a network in which both the cyber and physical systems are tightly integrated at all scales and levels [2]. Cyber-physical networks integrate computation and physical processes using embedded computers and networks to compute, communicate, and control the physical processes to receive feedback on how the physical processes affect computations and vice-versa. Fig. 1.2 delineates the interconnection between cyber and physical objects towards the road of CPNs.

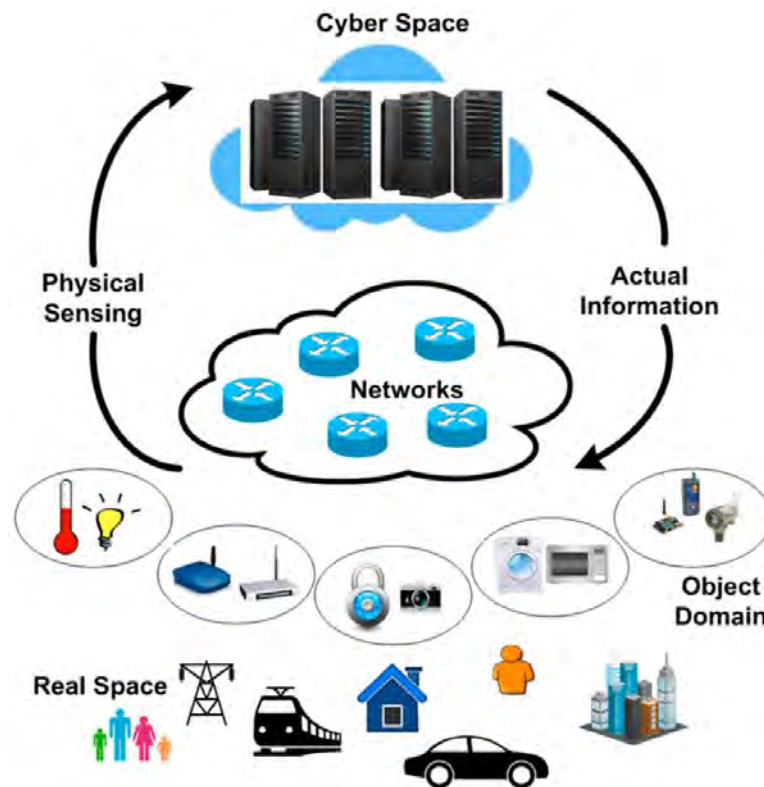


Figure 1.2: Interconnection between cyber and physical objects [2]

Cyber-physical networks (CPNs) come from the transformation of the existing networks and integration of the traditional embedded system networks. There exist several features such as dynamically reconfigurable, fully automated, auto-assembly, integration, etc., which make CPNs different from other system networks. The following two quotes from [7, 8] signifies the uniqueness of CPNs.

“A cyber-physical network integrates computing, communication and storage capabilities with monitoring and/or control of entities in the physical world, and must do so dependably, safely, securely, efficiently and real-time.” [7]

“Cyber-physical networks will transform how we interact with the physical world just like the Internet transformed how we interact with one another.” [8]



(a) Automated driving [9]



(b) Air traffic control [10]



(c) Surgical robots [11]



(d) Automated farming [12]



(e) Human-robot collaboration [13]



(f) Smart grid [14]

Figure 1.3: Applications of cyber-physical networks

With the myriad gleaming applications, CPNs have the potential to dwarf the IT revolution of the 20-th century. The applications of CPNs expand from small systems (i.e, aircraft) to very large systems (i.e, power grid). These applications include but not limited to confidence medical devices and systems, assisted living [11], agriculture [12], traffic control and safety, advanced automotive systems [9], process control, energy conservation, environmental control, avionics [10], instrumentation, critical infrastructure control (i.e., electric power, water resources, and communications systems) [14], distributed robotics [13], de-

fense systems, manufacturing, and smart structures. Fig. 1.3 illustrates different applications of CPNs. These applications need specialization to ensure fault tolerance, security, safety, and decentralized control of CPNs.

The complexity of these applications poses many challenges in enhancing network performance and security of cyber-physical networks (CPNs) owing to their limited resource issues. Cyber-physical networks are inherently known to be limited resource. However, recently evolved applications of CPNs in diversified fields such as aviation, defense [15], and critical infrastructure (i.e., power grid, water resource management, etc.) [15] have realized high-end resources such as high power computing, precise controlling, etc. In this thesis, we mainly focus on applications of CPNs that do have resource constraints. Therefore, we coined the term limited-resource cyber-physical networks for this study. These limited resource issues include limited amount of available energy to feed the system, low processing capability, limited amount of storage space, and low bandwidth for network communication. Some devices of CPNs may be deployed in remote locations where no stable power sources are accessible. Furthermore, some CPNs utilize devices with very limited capabilities and functionalities owing to the availability of current limited-capability devices and cost limitation. Such devices generally have limited computing, processing, communication, and storage capabilities. Therefore, the communication and security protocols of CPNs should be modeled considering these constraints owing to limited resource issues.

We envision to address these issues pertinent to network-level performance and security of limited-resource cyber-physical networks in this thesis work. Towards that road, first, we focus on real-time limited-resource cyber-physical networks. More specifically, we focus on real-time limited-resource cyber-physical networks for railway systems to detect missing rail blocks on railway tracks. Here, we provide a low-cost lightweight integrated networking solution for real-time detection of missing rail blocks on a railway track. Consequently, we focus on digging potential security threats to eventually coming up with necessary countermeasures beyond enhancing network-level performance for such networking solution.

In this thesis, we focus on two opposite extremes of limited-resource cyber-physical networks, i.e., miniature versions (e.g., nanonetworks and Body area networks (BANs)) and smarter versions (e.g., multi-radio smart devices networks and mobile wireless networks).

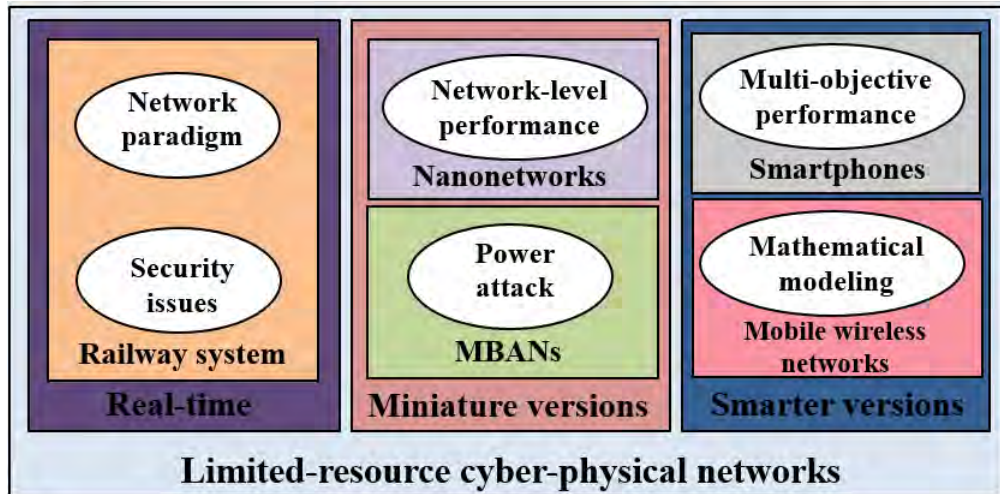


Figure 1.4: An overview of different research studies done under this thesis

Here, for the miniature versions of limited-resource cyber-physical networks, we aim to investigate the impacts of different types of nano-antennas having different materials on the network-level performances of the wireless nanonetworks. Consequently, we endeavor to explore the security of another example of the miniature versions of the limited-resource cyber-physical networks, i.e., body area networks. In this work, first, we introduce a new attack entitled *Power Attack* exploiting power constraint of the sensor devices along with countermeasure.

Besides, the thesis envisions to focus on smarter versions of limited-resource cyber-physical networks. Security aspects of such networks have already been widely explored from different perspectives in the literature. Therefore, in this thesis, first, we aim to provide a multi-objective vertical hand-off mechanism to enhance the network-level performance of multi-radio smart devices such as smartphones, tablets, walkie-talkie, etc. We also focus on the formulation of mathematical models for the different performance metrics of mobile wireless networks.

Fig. 1.4 demonstrates an overview of the studies, which are performed under the umbrella of this thesis work. We briefly elaborate on these parts of the thesis.

1.1 Research Focus 1: Real-Time Limited-Resource Cyber-Physical Networks over Railway Systems

We start this thesis by exploring real-time limited-resource cyber-physical networks. More specifically, we narrow down our focus on railway transportation systems as a representative of real-time systems. From decades railway transportation systems play a vital role in the socio-economic development of both developed and developing countries. Furthermore, the emergence of digitization technology has created new opportunities for the future of the rail industry and railway networks. Digital development of railway transportation systems from the traditional systems exposes diversified challenges, which attracts the attention of the researcher community [16–20].

The process of transformation from the traditional railway transportation system to the digitized railway transportation system has been successfully accomplished in many developed countries. However, low-income developing countries such as Bangladesh, India, Kenya, etc., raise crucial concerns in the way of devising intelligent railway transportation systems. The concerns circle around the widespread availability of publicly-exposed rail tracks, limited capability for escalating safety standard of the rail tracks owing to resource constraint, limited availability of electricity in rural areas, the paucity of long-range communication network infrastructure along the rail tracks, etc.

Furthermore, developing countries encounter frequent train accidents in comparison to developed countries. Derailment of trains is one of the major causes of the occurrences of train accidents in most cases. Developing countries such as Bangladesh, India, Kenya, etc., experience frequent occurrences of derailments in almost every year [21–27]. Fig. 1.5 depicts occurrences of derailments in developing countries.

These derailment events occur for both passenger trains and freight trains. In both cases, such derailments cost a huge amount of economic loss. Moreover, many people die and suffer from injuries, ranging from minor to severe due to derailments of passenger trains. In most of the cases, derailments happen due to losing continuity of rail track or faults in rail track (e.g., failed joint, rail end break, head worn rail). The reasons behind this discontinuity and faults in rail track can be both human-created and natural. natural calamities such as



(a) Derailment of train in India [22]



(b) Derailment of train in Gazipur, Bangladesh [27]



(c) Derailment of train in Chittagong, Bangladesh [26]



(d) Derailment of train in Kalaura, Bangladesh [25]

Figure 1.5: Different occurrences of derailments



(a) Publicly open rail tracks



(b) Miscreants uproot blocks due to political unrest

Figure 1.6: Reasons behind occurrences of derailments

cyclone, tornado, flood, etc., may result in uprooted rail tracks. However, most of the cases uprooted rail tracks occur due to actions of humans. Since in developing countries most of the rail tracks are publicly open, the tracks become more vulnerable for people to uproot rail tracks (Fig. 1.6a).

Besides, during the time of political unrest and mass protest in developing countries, miscreants used to uproot rail blocks to hinder the rail communication as a symbol of protest [21, 23, 26–28] (Fig. 1.6b).

A potential solution to this problem is to develop a real-time detection of missing rail

blocks leveraging Wireless sensor networks (WSNs). Through the years, researchers have shown a profound interest in developing WSN-based solutions for precise localization of trains and monitoring of rails for cracks, small breakage, and corrugation [29–34]. To the best of our knowledge, none of the above-mentioned solutions consider real-time detection of missing rail blocks as their prime concern. Moreover, most of these solutions demand well-established cellular network for long-range communication, Global System for Mobile Communications Railway (GSM-R) based specialized infrastructure, or WiMax connectivity, which are often very difficult to ensure in many developing countries. Furthermore, some of these solutions exploit a technique of using high-voltage signal over rail tracks in developed countries. However, in developing countries such as Bangladesh, India, Kenya, etc., where the rail tracks are publicly open, using this sort of technique poses a significant threat to living bodies that are in proximity or even come in contact with the rail lines. Therefore, in this thesis, we envision to address the issue of real-time detection of missing rail blocks to avoid derailments considering the challenges pertinent to developing countries.

Towards that road, we develop an integrated networking solution. Fig. 1.7 illustrates the system model of our proposed networking solution. As illustrated in Fig. 1.7, the real-time missing rail block detection system consists of two different modules: 1) Sensor module in the train and 2) Sensor module on the rail track. The former module consists of a control unit and a network module. The later module subsumes of a sensing unit, a control unit, and a network module. Here, the sensor module on the rail track senses vibration created by the approaching train from a substantial distance. Any discontinuity on rail track such as missing rail block hinders or changes the nature of propagation of vibration created by the approaching train. Next, the sensor module on the rail track sends a report about the condition of the rail track leveraging signal processing methods over the received vibration data to the sensor module in the train. After receiving the report from the sensor module on the track, the sensor module in the train initiates necessary alarms such as “stop” or “slow down” alarms to the driver.

Next, we present a novel ad-hoc network architecture, node deployment topology, and light-weight network protocols for enabling the real-time communication between trains and sensors on the rail tracks. Our proposed paradigm offers a low-cost and lightweight solu-

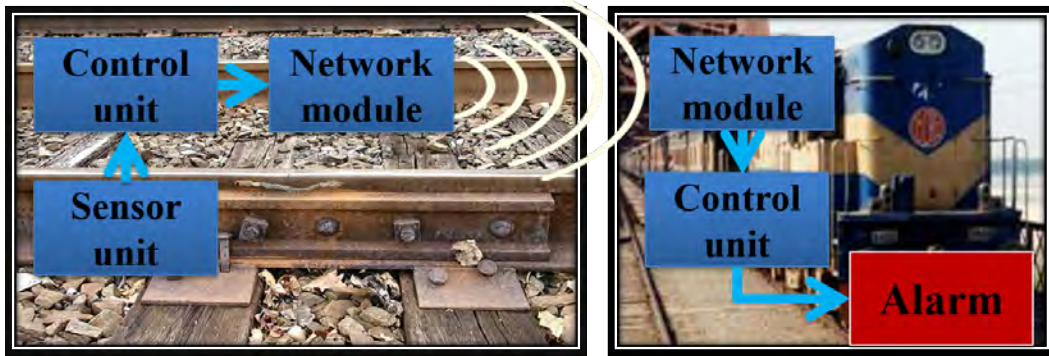


Figure 1.7: System diagram of WSN-based real-time missing rail block detection system [3]

tion, which exhibits a near-to-perfect performance in comparison to other state-of-the-art approaches.

However, deployment of wireless sensor-based solution exposes different security vulnerabilities [35]. Hence, analysis of potential vulnerabilities, attacks, and countermeasures grab our interests. Existing studies contain only a bunch of studies pertinent to the security of railway transportation system. Besides, the number of studies which take into consideration the concerns of developing countries pertinent to the security analysis of the railway system is even petty. Studies presented in [36–40] mainly focus on traditional attacks such as replay attack, displacement attack, jamming attack, etc., and their corresponding countermeasures [36–38]. However, to the best of our knowledge, exploration of security vulnerabilities and countermeasures of a real-time system for detecting missing rail blocks concerning developing countries is yet to be explored in the literature. Therefore, in this thesis, we endeavor to explore potential security threats exploiting vulnerabilities of our proposed real-time system for detection of missing rail blocks on the rail tracks.

In this thesis, first, we introduce a new threat entitled as power attack through exploiting vulnerability pertinent to the energy source of the real-time system for detecting missing rail blocks. Consequently, we present both theoretical and mathematical modeling of attack models to effectively launch the power attack. Furthermore, we perform extensive experimentation using both Network simulator 2 (*ns-2*) and real deployment to investigate the applicability and the effectiveness of our exposed attack models for the real-time system for detecting missing rail blocks. Consecutively, we explore the effects of traditional attacks such as man-in-the-middle attack and replay attack on the real-time system. Afterward, to mitigate these attacks, we propose a set of countermeasures. We perform extensive experi-

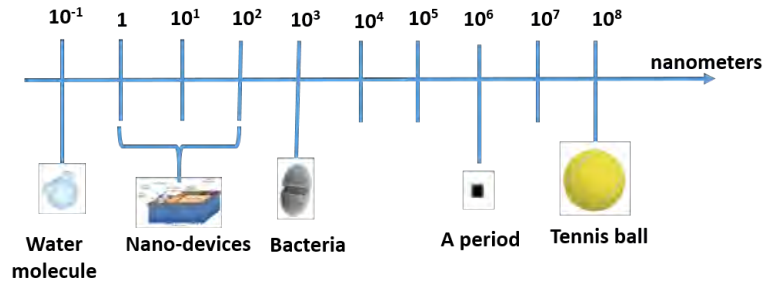


Figure 1.8: Comparison of size of nano device

mentation using both ns-2 simulator and real deployment to demonstrate applicability and effectiveness of our exposed attacks along with our proposed countermeasures.

1.2 Research Focus 2: Miniature Versions of Limited-Resource Cyber-Physical Networks

As mentioned at the beginning of this chapter, the next focus of the thesis is the miniature versions of the limited-resource cyber-physical networks. Here, we take into account two types of networks: one is wireless nanonetworks and the other is medical body area networks.

The recent emergence of nano-technology paves the path towards the development of nano-machines having a size of one to few hundred nanometers (Fig. 1.8). These nano-machines are equipped with nano-antenna, memory, CPU, and power supply. Fig. 1.9 demonstrates general structure of a nano-machine. These nano-machines are able to perform very simple and specific tasks at nano-level such as computing, data storing, sensing and actuation [41, 42] for diversified applications in biomedical, environmental science, industrial development, food science, military, etc., [43, 44]. The nano-machines can be developed for performing highly-sophisticated tasks such as recognizing and destroying tumors cells via penetration of sensitive body sites, for example, the spinal cord, gastrointestinal, etc., [45]. Such delicate health care applications promote nano-machines to have communication capabilities between each other to make decisions efficiently to treat complex diseases [46]. The communication among the nano-machines for such applications introduces a new paradigm called wireless nanonetworks.

Nanonetworks are not a simple extension of traditional communication networks at the

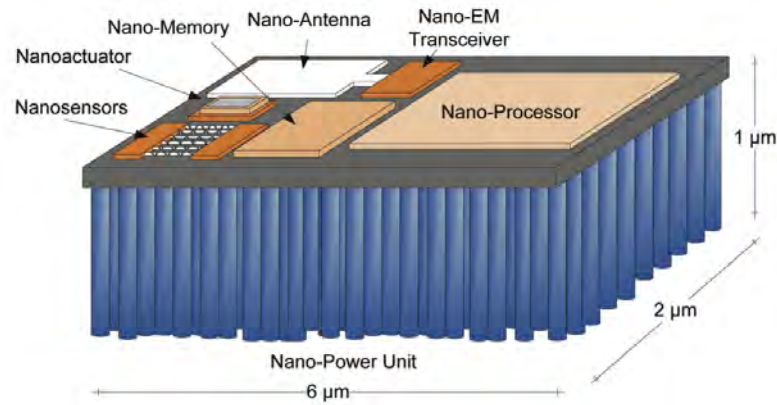
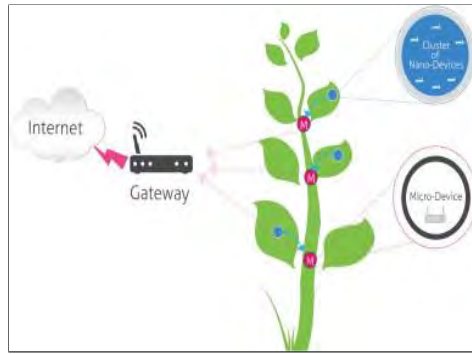


Figure 1.9: A typical nano-machines

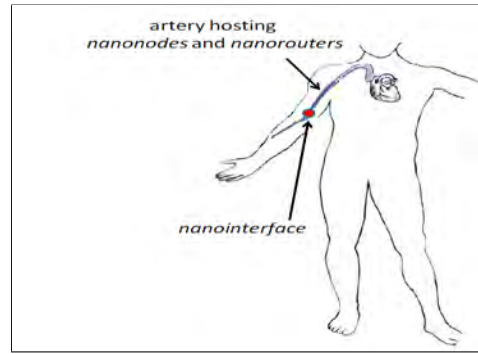
nano-scale. In the literature, there exist some classical applications of wireless nanonetworks. Fig. 1.10 demonstrates some promising applications that have been proposed in the existing studies. Nanonetworks can be utilized for environmental monitoring such as observing the condition of leaves in trees (Fig. 1.10a). Besides, the use of nanonetworks in health-care applications has been investigated in [47, 48] which is demonstrated in Fig. 1.10b, 1.10c, and 1.10d. In health-care applications, nanodevices can be used for blood pressure monitoring, measurement of heart bit rate (Fig. 1.10c), drug delivery, (Fig. 1.10b) pulse oximetry etc. Fig. 1.10d depicts that nanonetworks can also be used for monitoring of human lung cells. Owing to being a completely new communication paradigm having the potential of the above-mentioned promising applications, existing research in this field is still at an embryonic stage and requires further exploration in this field.

However, the limited capabilities of nano-machines such as short transmission range, small processing power, limited memory, scarcity of energy, etc., pose various challenges in the research of nanonetworks. Most of the existing studies on nanonetworks mainly focus on the exploration of the protocol stack, network architectures, and channel access procedure. These studies endeavor on designing protocols for the lower layers of the protocol stack, i.e., Physical and MAC layers [51–53]. The research on developing protocols for the upper layer, i.e., Network layer, still remains in a rudimentary stage [54, 55]. Here, the main focus remains limited to node-level energy efficiency [56].

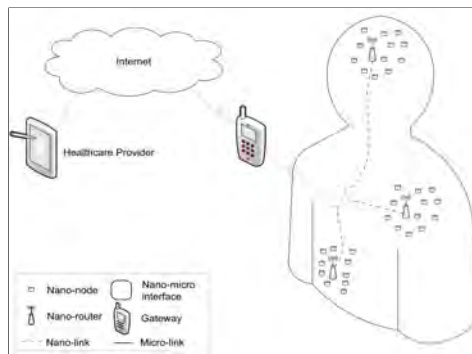
Furthermore, recent studies [57], [58] focus on analyzing wireless communication between a pair of nanodevices. Such studies facilitate deciding on efficient nano-antennas from the perspective of point-to-point communication. However, network-level communication in



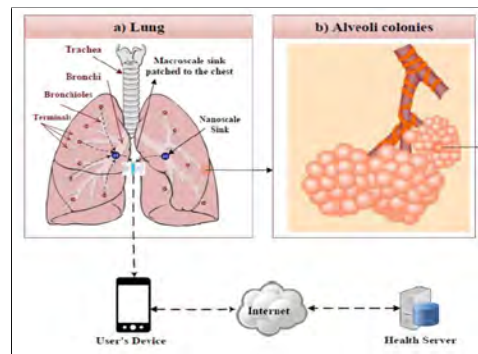
(a) Environmental monitoring [49]



(b) Drug delivery [50]



(c) Health status monitoring [49]



(d) Monitoring of an organ [48]

Figure 1.10: Classical applications of nanonetworks

a nanonetwork remains beyond the scope of all the above-mentioned studies, which is utmost important for deciding on a suitable nano-antenna from its several alternatives. Therefore, in this thesis, we investigate network-level performances of diversified nanonetworks while using different nano-antennas having different materials. Here, we consider three different types of nano-antennas (i.e., patch, dipole, and loop nano-antenna) along with three different materials (i.e., copper, carbon nanotubes, graphene). Our network-level investigation covers various perspectives such as network throughput, end-to-end delay, delivery ratio, and drop ratio. We report varying impacts of nano-antennas, which might be counter-intuitive in some cases, and network behavior from different environments including varying network size, data transmission rate, and speed of nodes.

Our evaluation reveals that a dipole nano-antenna using copper material exhibits around 51% better throughput and about 33% better end-to-end delay compared to other alternatives. Furthermore, our results are expected to exhibit high impacts on the future design of wireless nanonetworks through facilitating the process of finding the suitable type of nano-antenna

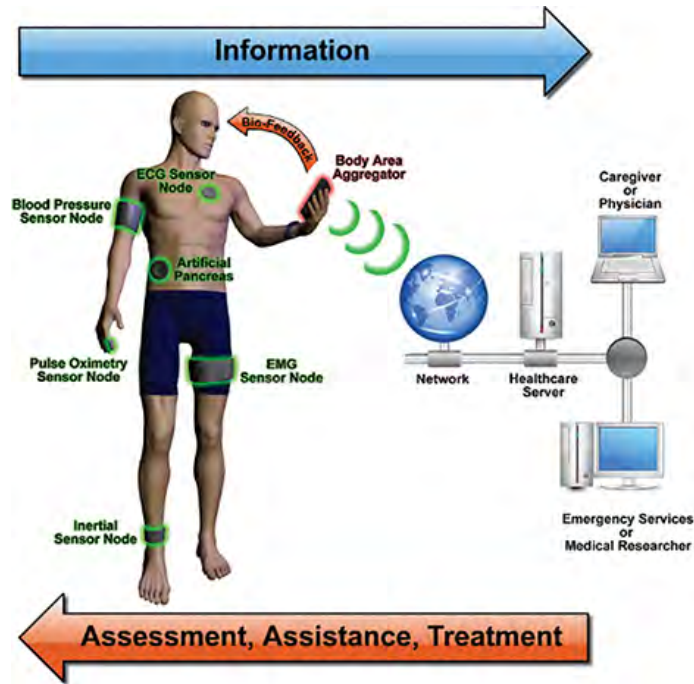


Figure 1.11: Basic framework of a medical body area network [4]

and suitable material for the nano-antennas. Next, in the thesis, we focus on medical body area networks, which is another example of miniature versions of limited-resource cyber-physical networks.

The recent rise in aged population and chronic diseases is placing increasing pressure on health care expenditure. Ubiquitous health care is regarded as a potential driver in reducing such health expenditure. Advancement in wireless communication and sensor technologies permits real-time acquisition, transmission, and processing of critical medical information for ubiquitous health-care applications. Hence, Medical body area networks (MBANs) emerge as a key technology to facilitate ubiquitous health-care services.

A basic framework of a medical body area network is illustrated in Fig. 1.11. It demonstrates that a MBAN is a kind of communications network having a human as a center and components are network elements related with the human body. In MABN, several sensor nodes such as ECG, EEG, blood pressure, motion sensor, and hearing sensor reside on a human body (Fig. 1.12). These sensors sense and collect important physical parameters such as body temperature, blood pressure, heart rate, blood oxygen concentration, etc. and send the parameters to the Base Station (BS) or the Mobile Unit (MU) near the human body in a wireless way. Finally, the Base Station (BS) or the Mobile Unit (MU) uploads the parame-

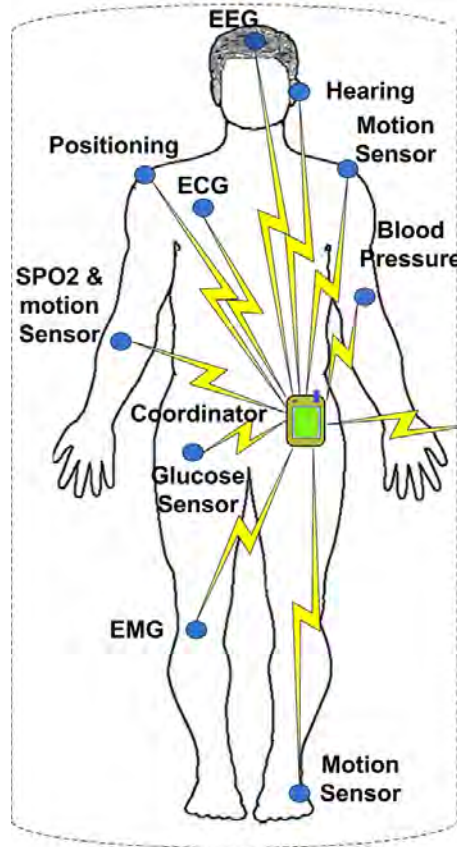


Figure 1.12: Different sensors in a MBAN [4]

ters to the terminal server through the Internet to have them analyzed and processed by the remote medical service providers.

Unfortunately, the development of MBANs is hindered by various security threats due to the vulnerable nature of the wireless channel. Eavesdropping [59], data modification, impersonation attack [60], and denial of service attack [61] are some of the current popular security threats of MBANs. Most of the existing research studies [62–65] mainly focus on finding effective countermeasures of these attacks.

Therefore, in this thesis, we introduce a new attack entitled as power attack via exploitation of vulnerabilities of the energy resources of sensor nodes in MBANs. Power attack forces a sensor to die off due to lack of power. We propose attack models to launch power attack effectively. Besides, we also propose a lightweight countermeasure for the power attack. Finally, we exhibit the efficacy of our proposed countermeasure using experimental evaluation.



Figure 1.13: Multi-radio smartphone [5]

1.3 Research Focus 3: Smarter Versions of Limited-Resource Cyber-Physical Networks

Next, we focus on the smarter versions of limited-resource cyber-physical networks. Here, we consider multi-radio smart devices and wireless mobile networks. Security aspects of such networks have already been widely explored from different perspectives in the literature [66–68]. However, enhancement of networking performance exploiting available multi-radios is little explored in the literature. Therefore, in this part of the thesis, we confine our work to the enhancement of network-level performance of such networks.

The pervasiveness of different wireless network technologies such as WiFi, WiMAX, Universal Mobile Telecommunications Service (UMTS), Long-Term Evolution (LTE), and Bluetooth facilitates the idea of having a wireless connection to the Internet always and everywhere. Nowadays such connectivity has become a real need for both work and personal life. People feel quite lost if they are not able to check their e-mails frequently, chat online with their friends, look for the fastest route to reach a place at any moment and in every place with their mobile phones or wireless devices.

This aspect becomes more prevalent with the rapid advancement of multi-radio technology in wireless networks, for example, multi-radio smartphones (Fig. 1.13) [5], tablets, multi-radio walkie-talkie [69], multi-radio routers [70]. These devices offer wireless connectivity and ability to surf on the Internet in every situation.

In such a scenario, the question arises that *which network should the mobile device select and connect to ensure the continuous connectivity along with the best experience to the end user?* To maintain network connectivity over multiple diverse networks the mobile devices

have to switch off from one network and to switch on to another network, i.e., to perform vertical hand-off. However, diverse network technologies also exhibit highly dynamic behavior in the presence of the others, i.e., in their co-deployment. Moreover, multi-radio devices often face resource constraints. For these reasons, maintaining network connectivity over multiple diverse networks from a multi-radio device is a real challenge. It demands the device capability to support multi-objective vertical hand-off, to deal with the network dynamics that exhibits in any co-deployment of heterogeneous wireless networks, and to deal with the resource constraint of the device itself.

Existing studies on multi-objective decision-making mechanisms such as Grey Relational Analysis (GRA) [71], Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) [72], and Simple Additive Weighting (SAW) [73] have been proposed for selecting the best network during vertical hand-off. These mechanisms use different network parameters, such as data rate, delay, Signal to interference ratio (SINR), etc., together to choose the best network. However, these approaches fail to capture the impacts of network dynamics. In addition, only a few of the above-mentioned hand-off mechanisms take into account energy consumption, which is an important device-level parameter for many multi-radio devices.

Therefore, in this thesis, we provide a Multi-objective vertical hand-off mechanism (MOVH) considering both network-level and device-level parameters leveraging the multi-objective genetic algorithm. We evaluate the performance of our MOVH mechanism against the two most popular alternatives: GRA and TOPSIS. This evaluation comprises both test-bed experiments and $ns-2$ simulation. The results from both test-bed experiments and $ns-2$ simulation demonstrate that our MOVH mechanism has significant performance improvement over both GRA and TOPSIS.

Next, we focus on mobile wireless networks, i.e., Mobile ad-hoc networks (MANETs). Owing to features such as intrinsic flexibility, lack of infrastructure, ease of deployment, auto configuration, and low cost, MANETs have emerged as a widely known communication paradigm for the last few years.

MANETs foreshadow its gleaming prospects in diversified applications such as battle-field communication [74], emergency relief scenarios [75], law enforcement [76], public meeting [74], virtual classroom [77], and security-sensitive computing environments [74].



(a) Battlefield communication [74]



(b) Emergency relief scenarios [75]



(c) Law enforcement [76]



(d) virtual classroom [77]

Figure 1.14: Diversified applications of MANETs

Fig. 1.14 demonstrates diversified applications of MANETs. Diverse applications of MANETs emphasize the need for network-performance improvements of MANETs. To evaluate the performance improvements of MANETs, there exist two approaches: one is test-bed experiments and the other is mathematical modeling. In this thesis, we focus on mathematical modeling as it is the fastest and cost-effective tool for evaluating the performance of mobile wireless networks.

Existing research studies [78], [79], [80] have attempted to formulate mathematical models for MANETs focusing on a few performance metrics such as average end-to-end delay and average throughput leaving formulation of mathematical models for average energy consumption, delivery ratio, and drop ratio unexplored. Moreover, these studies consider the

impact of lower layers, i.e., Physical layer and MAC layer of the protocol stack, leaving the impact of upper layers, i.e., Network layer and Transport layer yet to be explored. Therefore, in this thesis, we attempt to analyze the feasibility of developing mathematical models for MANETs considering the impact of all layers in the protocol stack in addition to that of different parameters using rigorous ns-2 simulation under diversified settings. Our rigorous empirical study reveals a key finding that mathematical modeling of MANETs considering variation in all parameters is not feasible.

Next, we delineate our contributions.

1.4 Our Contributions

Part I of this thesis focuses on real-time limited-resource cyber-physical network. Here, we make the following contributions:

- We devise a new integrated networking solution for detecting missing rail blocks on publicly-open rail tracks of developing countries. We introduce a novel ad-hoc network architecture along with node deployment topology for communication between an approaching train and sensor nodes embedded on rail tracks. In addition, we develop and implement a new lightweight cross-layer protocol for communication between an approaching train and sensor nodes ahead on the rail track. To evaluate the performance of the proposed cross-layer protocol, rigorous experiments is performed through both ns-2 simulation and real-testbed implementation. Performance of the proposed cross-layer protocol is compared to that of well-known state-of-the-art protocols used for rail monitoring (i.e., IEEE 802.11 and IEEE 802.15.4) [81, 82]. Here, the base of the comparison is different performance metrics such as delivery ratio, end-to-end delay, and average energy consumption. The paradigm exhibits a near-to-perfect performance for both simulation and real experimental evaluation.
- Subsequently, we explore the security vulnerabilities of the proposed network paradigm. Here, we introduce a new security attack called power attack exploiting the limited energy availability of the network paradigm. Consequently, we also explore the possibilities of other well-known security attacks such as Man-in-the-middle (MITM)

attack and replay attack of the proposed network paradigm for real-time detection of missing rail blocks. We present attack models to effectively launch these attacks. To demonstrate the viability and efficacy of the proposed attack models, mathematical modeling, numerical simulation, ns-2 simulation, and real testbed implementation are performed. Besides, effective lightweight countermeasures are introduced to mitigate these attacks. Rigorous experimentation is carried out to exhibit the effectiveness of the proposed countermeasures using both ns-2 simulation and real deployment on rail lines. In the experimentation, network-level performance is thoroughly analyzed in terms of delivery ratio, energy consumption, and delay even after applying the countermeasures.

Part II focuses on the miniature versions of the limited-resource cyber-physical networks, we make the following contributions:

- We perform innate exploration of the impacts of using different well-known nano-antennas and materials available to date on the network-level performance of nanonetworks. Here, we perform rigorous simulation using a customized ns-2 simulator. Three different types of nano-antennas (i.e., patch, dipole, and loop nano-antenna) along with three different materials (i.e., copper, carbon nanotubes, graphene) are explored in the analysis and simulation. Adoption of the antenna alternatives and materials are based on their acceptability in existing studies [83–85]. However, to the best of our knowledge, this work is the first to perform analysis on the impacts of these antennas and materials on the network-level performance. Our evaluation reveals a number of novel findings pertinent to finding an efficient nano-antenna from its several available alternatives for enhancing network-level performances of nanonetworks. Our evaluation depicts that a dipole nano-antenna using copper material exhibits around 51% better throughput and about 33% better end-to-end delay compared to other alternatives. Our results are expected to exhibit high impacts on the future design of wireless nanonetworks through facilitating the process of finding the suitable type of nano-antenna and suitable material for the nano-antennas.
- We focus on developing a new security attack called power attack for another miniature version of the limited-resource cyber-physical networks, i.e., body area networks.

Here, first, we devise attack models followed by developing a lightweight countermeasure. To demonstrate the viability and the efficacy of the proposed power attack and its countermeasure in body area networks Mannasim simulator [86] is used. Our evaluation exhibits the efficacy of our proposed countermeasure.

Finally, Part III of this thesis focuses on the smarter versions of the limited-resource cyber-physical networks, we make the following contributions:

- We propose a multi-objective vertical hand-off mechanism leveraging customized multi-objective genetic algorithm for the smarter versions (i.e., smart devices having heterogeneous multi-radios) of limited-resource cyber-physical networks to enhance networking performance. Our proposed mechanism yields better scalability and stability for the vertical hand-off. To demonstrate the superior network and device-level performances of the proposed mechanism, the performance of the proposed mechanism is evaluated using both ns-2 simulation and real testbed experiments against that of two other state-of-the-art approaches of multi-objective decision-making mechanisms namely GRA [87] and TOPSIS [88]. These approaches are extensively focused in recent research studies [89–92]. Here, we consider different metrics such as total energy consumption, energy consumption per transmitted bit, throughput, delay, etc.
- As existing studies on enhancing network performance often adopt mathematical modeling, therefore, we envision to develop mathematical modeling for mobile wireless networks. We perform rigorous simulation utilizing ns-2 to assess the viability of mathematical modeling for different performance metrics such as energy consumption, throughput, delay, etc., of mobile wireless networks under diversified settings. Our rigorous empirical study reveals that we need to develop cross-layer mathematical models to represent the performance of the mobile networks and such mathematical models need to resolve higher-order polynomial equations. Consequently, our study uncovers a key finding as lemma: *mathematical modeling of mobile wireless networks considering variation in all parameters is not feasible.*

1.5 Organization of the Thesis

The rest of the chapters are organized as follows:

Part I of this thesis comprises of Chapter 2 and 3. Here, we focus on real-time limited resource cyber-physical system for detecting missing rail blocks on the rail tracks. Chapter 2 provides an integrated networking solution to detect missing rail blocks of railway tracks for developing countries comprising a network architecture, node deployment topology, and cross-layer communication protocol.

Chapter 3 explores potential security vulnerabilities, attacks, and countermeasures of the proposed networking solution. Here, we introduce attack models and countermeasures for a new security attack entitled power attack along with other traditional attacks such as man-in-the-middle attack and replay attack.

Part II of the thesis illustrates the miniature versions of the limited-resource cyber-physical networks. This part of the thesis comprises of Chapter 4 and 5. Here, Chapter 4 explores the impacts of different nano-antennas on the network-level performance of the nanonetworks. Chapter 5 exploits security vulnerabilities of the body area networks to introduce a new attack i.e., power attack.

Finally, Part III of the thesis comprises of Chapter 6 and 7. Here, we focus on the smarter versions of the limited-resource cyber-physical networks. Chapter 6 provides a multi-objective vertical hand-off mechanism to improve the network-level performance of smart devices such as smartphones, tablets, etc. Consequently, Chapter 7 focuses on developing mathematical models considering diverse parameters for mobile wireless networks. Finally, we offer concluding remarks in Chapter 8.

1.6 Conclusion

In this introductory chapter, we introduce the background and motivation of the works that we take up in this thesis. Consecutively, we clearly outline the contributions of this research work. In the next chapter, we will begin with Part I of the thesis that deals with real-time limited-resource cyber-physical networks for railway systems.

Part I

Real-Time Limited-Resource Cyber-Physical Networks

Chapter 2

Integrated Networking Solution for Real-Time Detection of Missing Rail Blocks

2.1 Introduction

Developing countries such as Bangladesh, India, Kenya, etc., experience frequent occurrences of derailments in almost every year [21–27]. These derailment events include both passenger trains and freight trains. In both cases, derailments cost a huge amount of economic loss. Moreover, many people die and suffer from injuries, ranging from minor to severe due to derailments of passenger trains. In most of the cases, derailments happen due to losing continuity of rail track or faults in rail track (e.g., failed joint, rail end break, head worn rail). The reasons behind these discontinuity and faults in rail track can be both human-created and natural. Besides, during the time of political unrest and mass protest in developing countries, miscreants used to uproot rail blocks to hinder the rail communication as a symbol of protest [21, 23, 26, 27]. As the railway tracks in developing countries are publicly open, it is very easy for miscreants to have access on the railway track. Moreover, natural calamities such as cyclone, tornado, flood, etc., also result in uprooted rail tracks. Such missing rail occurrences due to uprooting rail blocks are mainly accountable for derailments in developing regions [23].

Furthermore, due to high speed and momentum, it is not possible to stop a train within a short distance from a missing or faulty rail occurrence. Now, if it was possible to detect the missing or faulty rail from a sufficiently long distance, the train could avoid the derailment. In this context, our endeavor is to provide an automated real-time solution that detects the discontinuity in railway track from a sufficiently long distance, thus the train can avoid the derailment. If we could develop such an automated real-time solution, then we can save valuable lives and protect the economy from suffering losses caused by derailments owing to missing rail blocks.

An intuitive solution to detect discontinuity and fault in rail track is exploitation of Wireless Sensor Networks (WSNs). Through the years, researchers have shown a profound interest in developing WSN-based solutions for monitoring rail tracks and their infrastructures [29–31, 33]. To the best of our knowledge, none of these solutions are built through focusing on real-time missing rail block detection as the predominant concern, rather they mostly focus on expensive micro-level monitoring. Moreover, from the networking perspective, most of these solutions demand well-established cellular network for long-range communication, GSM-R based base station framework, or WiMax connectivity [93].

However, as a research context, low-income countries raise some crucial concerns in the way of devising specialized WSN-based solutions for the purpose of derailment detection. First concern circles around the paucity of long-range network infrastructure, limited cellular network connectivity, and limited availability of electricity in rural rail areas [94–97]. Second and the most important concern is limited affordability due to low-resource settings. It is less likely for a developing country to adopt even a WSN-based solution that will demand expensive networking infrastructures.

Therefore, our study encompasses to address above-specified concerns by devising a low-cost and lightweight WSN-based automated real-time system leveraging a novel concept of communication between train and rail track. Our proposed system exploits a new networking paradigm that does not demand any expensive infrastructure or framework, which enables it to be a potential solution for low-resource settings.

Our proposed low-cost and lightweight WSN-based solution consists of two different modules: (1) Sensor node on rail track and (2) Inspector node in train. Inspector node in

the train sends a query to a sensor node to know about the condition of the rail track ahead. Upon receiving the query the sensor node residing on the rail track senses the condition of the track and sends a reply to the inspector node along with the sensing results. Then, the inspector node takes necessary steps on the basis of reply about the condition of the rail track. We ensure the robustness of the whole sensing scheme through an evaluation of false positive and false negatives. However, in this chapter, our main endeavor is to devise a suitable network architecture, node deployment topology, and network protocol considering low-resource context.

In this chapter, our contributions are as follows -

- We present a novel network paradigm consisting an ad-hoc network architecture, node deployment topology, and lightweight network protocols, which facilitate devising an automated system to detect missing and faulty rail blocks.
- We evaluate performance of our proposed network paradigm through both `ns-2` simulation and experiments with real deployment considering diversified settings.
- We also present a quantitative comparison between our proposed networking protocols and other well-known alternative protocols used in existing rail monitoring solutions, in terms of different performance metrics.

2.2 Related Work

Up to now, several studies in the literature [30–33, 98–106] focus on micro-level monitoring of railway systems through detecting cracks, small breakages, stress, and inclination in the rails. These studies do not deal with missing rails in a railway track. Most of these studies exploit expensive acoustic emission and long range ultrasound techniques to monitor rail crack and breakage. Some other studies [107] exploit a technique of using voltage signal over rail tracks for such detection. However, in developing countries such as Bangladesh, where the rail tracks are publicly open, using this sort of technique poses significant threat to living bodies in contact of the rail lines.

On the other hand, several methods have been proposed for monitoring overall railway infrastructure [29, 81, 104, 106, 108]. These methods focus on macro-level monitoring of the

overall railway system. However, such methods require continuous monitoring of the rail tracks, and therefore these methods are energy-hungry. Now, the task of detecting missing rails in a railway track falls in between these two extremes, i.e., micro-level and macro-level monitoring, and thus appeals to be investigated in a specialized manner.

Besides, the most prominent hole in the literature in this regard is that the already-proposed mechanisms are mostly non real-time. However, in case of developing countries, which frequently experience sudden effects on tracks due to various reasons such as political protest, real-time solutions on the rail track are of the utmost importance. However, there is a paucity of such mechanisms in the literature [109]. Chakraborty et al., [3] proposed a solution for detecting missing rail. However, no network design was discussed in the proposal. In this paper, we address this issue and plan to devise a real-time solution in this regard.

Now, from the networking perspective, researchers have shown profound interest in investigating a suitable network architecture, deployment topology, and network protocol considering the harshness of outdoor longterm condition monitoring, power usage, and the complex geometry railway track.

Determining the optimum node deployment often requires a trade-off. The network configuration can be optimized considering different constraints - minimum level of redundancy, minimum power consumption, maximum level of reliability, etc. Pascale et al., [29] proposed a WSN for signaling and control in railway stations to calculate the minimum number of nodes required for deploying a network topology. The natural topology choices available for WSN in rail applications are star, tree, and mesh topologies. In most of the topologies, there is a single base station that can send and/or receive messages to/from a number of remote sensor nodes. The remote nodes can communicate directly with the base station but or with each other. The base station communicates with the remote monitoring server through cellular network communication. As we have mentioned earlier, in developing, a large amount of rural rail area is yet to be covered by cellular network service. Nevertheless, a node deployment topology for missing or faulty rail detection considering the low-resource settings and open access in railway track is yet to be proposed in the literature.

A number of communication techniques for WSN in railway have been suggested in state-of-the-art literature [81, 82]. Inter-sensor node communication and sensor node to base

station transmission are usually short range. Bluetooth, IEEE 802.15.4, WiFi are used for these short range transmissions. The base station transmits gathered data back to the control center, and this requires long-range communication. GSM, GPRS, and UMTS are generally used for this purpose. Another recent communication advancement is GSM-R (Global System for Mobile Communications-Railway), which is an adaptation of GSM telephony for railway applications. It is designed for information exchange between trains and control centers. These base station based framework demands for expensive and heavy networking infrastructure with reliable power supply.

The most power consuming part for a wireless sensor node is data communication. The sensor nodes need to transmit data reliably via the network despite the paucity of power supply. Hence, energy efficiency and reliability are both crucial here. Several protocols [31, 110, 111] have been proposed in the literature considering these two aspects. However, these studies consider the transmission in railway tunnels or multihop (daisy chain) networks mounted in train carriages.

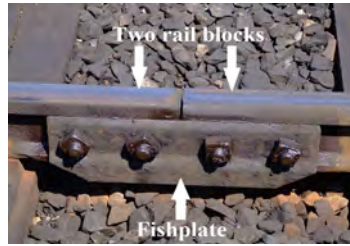
Considering the low-resource context of developing countries, we should focus on cost-effectiveness and paucity of cellular network infrastructure in rural rail areas, with utmost importance while developing a detection systems for missing and faulty rails. To the best of our knowledge, no work in the literature has focused on these issues.

2.3 Problem Formulation and System Model

In this section, first, we give a brief description of our research context. After that, we delineate our proposed system model and topology.

2.3.1 Research Context

We consider the busiest railway station and its nearby railway tracks of a developing country (anonymized) in our study to realize different pragmatic aspects in devising our solution. Accordingly, real deployments of our study for adjusting operational parameters as well as performing performance evaluation were conducted at the railway station. Throughout the whole chapter, we consider values of the parameters obtained from the rail track and train



(a) A railway track with continuous rail blocks



(b) A discontinuity

Figure 2.1: Railway track

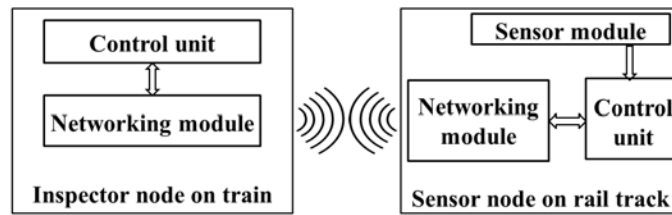


Figure 2.2: Simplified block diagram of the system model

operating in the same context. However, it is worth mentioning that the adopted values of operational parameters are analogous to the contexts of different developing countries such as Bangladesh, India, Kenya, etc. In the country under our consideration, the average speed of a passenger train varies from 40kmph to 60kmph, and the maximum attainable speed is ~ 80 kmph. During our field study and as per comments from domain experts such as train's engine operator, we found that a train with 80kmph speed can be safely stopped within ~ 200 m distance, after activating its break.

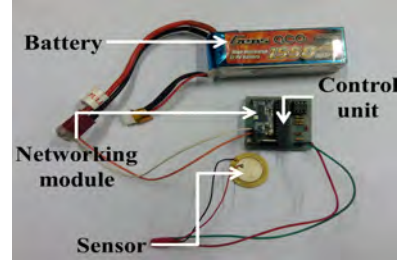
The railway track under consideration consists of metal rail blocks connected by fishplates as shown in Figure 2.1a. Each metal railway block is ~ 120 m in length. A discontinuity of railway track can be created through uprooting these metal rail blocks or similar events (Figure 2.1b). Here, in this chapter, our endeavor is to make a solution that notifies an approaching train from at least ~ 1 km distance upon detection of such a discontinuity in the rail track ahead in order to stop the train safely.

2.3.2 Proposed System Model

Our proposed system consists of two different modules: (1) Sensor node on rail track and (2) Inspector node on train. In Figure 2.2, we represent the simplified block diagram of our proposed system model.

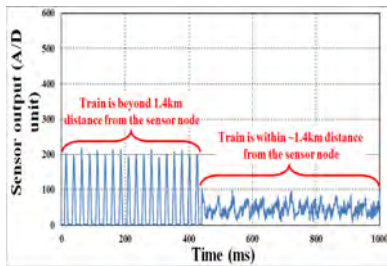


(a) Our sensor node on track

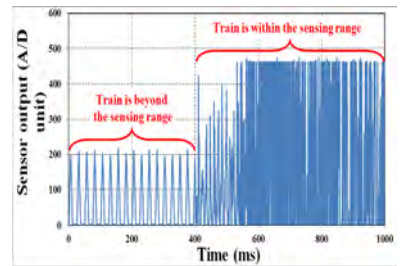


(b) Components of our node

Figure 2.3: Our sensor node with its real deployment



(a) Continuous and fit rail track



(b) Discontinuous rail track

Figure 2.4: Outputs generated by our sensor node

Sensor node on rail track: The sensor node is placed on a rail track as shown in Figure 2.3a. It consists of a sensor module, a networking module, a control unit, and a battery (Figure 2.3b). The sensor module senses vibration on the rail track created by an approaching train. We use a low-cost piezoelectric sensor for this purpose. Alongside, we incorporate an amplifier circuit that enables detection of vibration from more than 1km distance. The vibration created by an approaching train follows a distinct pattern for a continuous and fit rail track as shown in Figure 2.4a. Any discontinuity on the railway track hinders natural propagation of this vibration, created by the train, to the sensor node. Figure 2.4b depicts outputs generated by the sensor module in presence of a discontinuity ($\sim 16\text{cm}$ long gap in this case) in the rail track. Outputs of the sensor module in the two scenarios are different enough to make the distinction even through visual perception. In our case, a control unit analyzes the outputs generated by the sensor module using signal processing and detects continuity or discontinuity of railway track. The control unit notifies the condition of rail track to the approaching train through a networking module. We ensure the robustness of the whole sensing scheme through an evaluation of false positives and false negatives. The evaluation of the sensing scheme is not our main focus in this chapter, hence, we exclude those results. Nonetheless, it is worth mentioning that a sensor node does the sensing only

after receiving a query from the train instead of sensing continuously to ensure an improved battery life.

Here, as the network module, we use HC-12 (working frequency is 433MHz) RF module [112] having an omni-directional antenna with communication range of $\sim 750\text{m}$. Besides, for enabling simple communication and to avoid interference, the sensor nodes utilize two different communication channels for two different real-time communications (one with the train and another with the next node as described later). Furthermore, in order to keep a simple packet format, we use 2-bit binary counter addressing for the sensor nodes. For example, the addresses of the sensor nodes are denoted as 00, 01, 10, 11, 00, and so on.

It is to be noted, for the time being, in this thesis, we consider single linear rail track while developing 2-bit addressing mechanism. We need to consider distinct addressing of sensor nodes for two parallel rail tracks. However, while exploring the security issues of our proposed paradigm, we incorporate two new information, i.e., train id and trip number to tackle different security attacks (mentioned in Section 3.4). Incorporation of these two information ensures that 2-bit addressing scheme can also be used for parallel rail tracks. However, addressing mechanism for parallel rail tracks still needs further exploration. Hence, it could be a potential avenue for our future research.

Inspector node in the train: This node is placed in the train. It consists of a networking module and a control unit. The control unit sends queries to the immediate sensor node placed on the rail track ahead via the networking module and fetches a monitoring report about condition of the rail track from the sensor node. Subsequently, the control unit interprets the report and notifies the driver accordingly.

Note that we delineate our proposed real-time missing rail block detection system as an example of a cyber-physical networks (CPNs) instead of Internet of Things (IoT). We have done so as, according to the definition of CPNs, it mainly focuses on sensing, computation, and communication to build a relation between cyber and physical world [7]. In a similar manner, for our proposed system, we collect vibration (which is created by the approaching train) from the physical environment and pass the information to the cyber world for decision making. We can also define our system as network of things. On the other hand, IoT generally focuses on networking, i.e., connecting different types of devices through the Internet

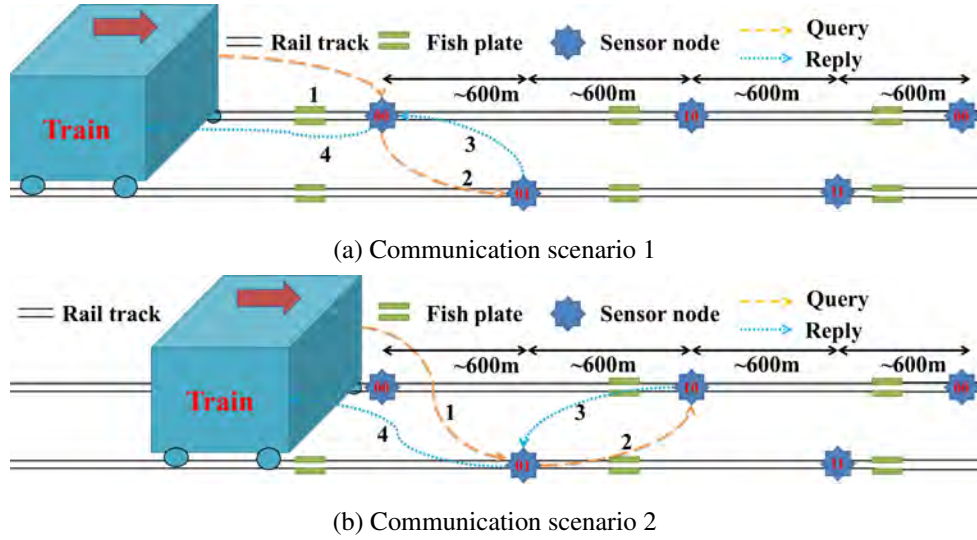


Figure 2.5: Node deployment and communication scenarios

to exchange data [113]. Hence, we consider our proposed system as an example of real-time cyber-physical networks (CPNs) instead of IoT.

Next, we elaborate the node deployment topology along with network architecture.

2.3.3 Node Deployment Topology and Network Architecture

Figure 2.5 presents a conceptual overview (not drawn at scale) of our proposed node deployment topology and ad-hoc network architecture. Our proposed network architecture subsumes a single mobile node (i.e., the Inspector node in train) and multiple static nodes (i.e., the sensor nodes on rail track).

Here, we place the sensor nodes on the rail track in a zigzag pattern so that we can monitor both railway lines. We place two consecutive sensor nodes $\sim 600\text{m}$ apart, as the network module of our sensor node has a communication range of $\sim 750\text{m}$. Our addressing of the sensor nodes follows a 2-bit binary counter scheme. Since the sensor nodes use two different communication channels, to keep the communication simple, all sensor nodes placed on the same rail line communicate with the train over the same communication channel. For example, in Figure 2.5, the sensor nodes addressed as 00 and 10 communicate with the Inspector node on train through the same channel (Channel 1), while sensor nodes addressed as 01 and 11 communicate with the inspector node using a different channel (Channel 2). As the sensor nodes 00 and 10 are placed $\sim 1.2\text{km}$ apart, the communication ranges of these two

nodes do not overlap, inhibiting any potential interference or overhearing.

Communication from a train is performed over two hops. Here, the train always needs to know the address along with the communication channel of the immediate sensor node ahead that is needed to be queried next. To resolve the aforementioned issue, for a certain trip, a pre-specified ordered list of the sensor nodes' addresses along with their communication channels is stored in a memory of the Inspector node in train. It is worth mentioning that the memory of the Inspector node is 256KB and it is sufficient enough to store the pre-specified ordered list for the longest rail track of Bangladesh, i.e., 507km from Dhaka to Panchagarh [114]. We have to store addresses and corresponding communication channel for about 845 sensors in the pre-defined list to cover the longest rail track.

To elaborate our proposed communication paradigm, we consider a scenario, where a train is moving to a forward direction as shown in Figure 2.5a. Here, first, the Inspector node in train initiates a communication by sending a query packet to the very next sensor node 00. This query packet contains the address of the second sensor next sensor node, i.e., 01 as destination. Inspector node uses the pre-defined ordered list to know the address of the very next sensor node and the second next sensor node. After receiving the query packet from the inspector node the sensor node 00 forwards this query to the sensor node 01. As we mentioned earlier, we intend to notify the approaching train about the condition of the rail track ahead from at least ~ 1 km distance. As a result, it is sufficient to fetch the monitoring report from two-hop distance that covers ~ 1.2 km. After that, the sensor node 01 replies back to the sensor node 00 with its monitoring report. Then, the sensor node 00 replies back to the Inspector node in train combining the monitoring reports of nodes 00 and 01. Here, when the sensor node 00 communicates with the sensor node 01, the sensor node 00 switches its communication channel from its current one (Channel 1) to the communication channel of sensor node 01 (Channel 2). After that, when the sensor node 00 again communicates with the train, it again switches its channel to the previous one (Channel 1).

Next, as shown in Figure 2.5b, the Inspector node in train directly sends a query packet to the sensor node 01 (over Channel 2) having sensor node 10 as destination. After receiving the query packet from the inspector, sensor node 01 switches to Channel 1 and forward the received query packet. Now, due to our proposed zigzag pattern topology, there are only

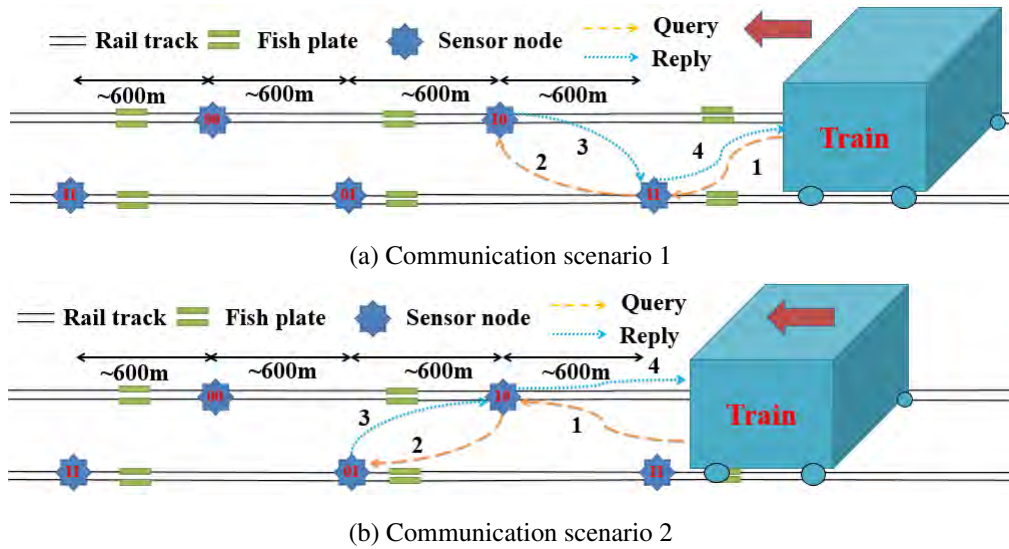


Figure 2.6: Communication scenarios in reverse direction

2 sensor nodes (i.e., 00 and 10), which are also listening to the very same channel, i.e., Channel 1 and are in the communication range of sensor node 01. Hence, when sensor node 01 forwards the query packet, both sensor node 00 and 10 will receive this query packet. However, this query packet will be discarded by sensor node 00 as the destination address of the query packet is set as 10. Accordingly, the monitoring report is again fetched from two-hop distance ($\sim 1.2\text{km}$).

Next, we explore the communication scenarios when the train is traveling from reverse direction (Fig. 2.6). As shown in Fig. 2.6a, the inspector node in the train sends a query packet to sensor node 11 over Channel 2. The inspector node sets the destination address by the address of the second next sensor node to which the sensor node 11 will forward the query packet, i.e., sensor node 10. As mentioned earlier, the inspector node gets the addresses from a pre-defined ordered list, which will be provided at the beginning of the journey. After receiving the query packet from the inspector node, sensor node 11 switches its communication channel from Channel 2 to Channel 1 and forwards the query packet to sensor node 10. Then, sensor node 10 replies back to sensor node 11 about the condition of the rail track ahead as report packet. Sensor node 11 replies back to the train with a combined monitoring report from sensor node 10 and itself. Channel switching occurs in a similar manner as mentioned in forward communication scenarios.

Fig. 2.6b exhibits that the inspector node in train now sends a query packet to sensor node 10 with a destination address of the next hop, i.e., 01 over Channel 1. Sensor node 10

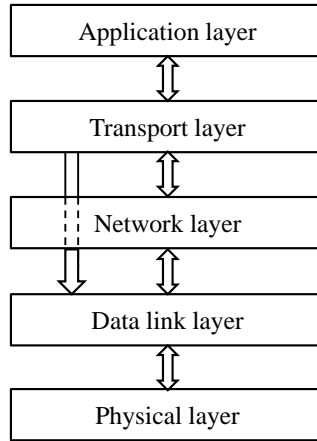


Figure 2.7: Cross-layer protocol stack

forwards this query packet to sensor node 01 over Channel 2. Note that, when the sensor node 10 communicates to the sensor node 01 with a query packet over a certain channel, the sensor node 11 listens over the very same channel and both 01 and 11 reside in the communication range of sensor node 10. However, in this case, the sensor node 11 discards such query packets from 10, as the query packets contain the address of the sensor node 01 as the destination address.

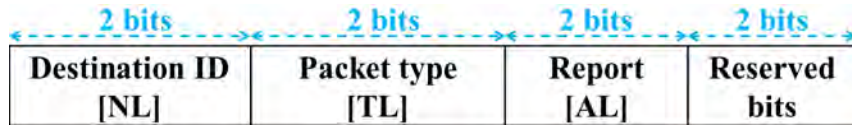
It is evident that our proposed communication paradigm works for both forward and reverse direction, as simply changing the list of sensor addresses to be queried ahead can realize the rail track to be traveled (and queried) ahead. Next, we will delineate details of our proposed protocols enabled in our communication paradigm.

2.4 Protocols in Our Proposed Paradigm

In this section, first, we present a new cross-layer protocol stack adopted in our paradigm. After that, we elaborate our lightweight protocols with a time-sequence diagram, state diagram, and flow-charts.

2.4.1 Cross-layer Protocol Stack

We adopt a cross-layer protocol stack based on the underlying notion of classical OSI model (Figure 2.7). Here, we introduce a common flag variable (named “Channel Switching Indicator”) between Transport layer and Data Link layer of the OSI model. This cross-layer



(a) Basic packet



(b) Query packet



(c) Acknowledgement packet



(d) Reply packet

Figure 2.8: Packet format in our proposed communication paradigm

alliance handles channel switching procedure presented in the previous section.

Figure 2.8 illustrates the packet¹ format for our proposed protocol. The total size of the packet is only one byte including two reserved bits. Besides, the report block of the packet is created by the Application layer. In case of a Reply packet, this report block contains the condition of the rail track sensed by the current sensor node and the very next sensor node if available. In case of Query and Acknowledgment packets, the report block does not contain any useful information and thus remains blank. Additionally, the Transport layer adds the packet type information, which can be either of query from the train, query from the sensor node, acknowledgment, and reply. Fig. 2.8b, Fig. 2.8c, and Fig. 2.8d demonstrate format of query, reply, and acknowledgement packet respectively. In addition, the Network layer of the Inspector node in train adds the destination ID, i.e., address of the final sensor node needed to be reached in two-hop communication. For example, in case of the communication scenario depicted in Figure 2.5a, the destination ID for the query packet released from the train is 01, which is first intercepted and taken care of by the sensor node 00. It is worth mentioning

¹Here, by mentioning 'packet', we refer to the data unit comprising information from all layers

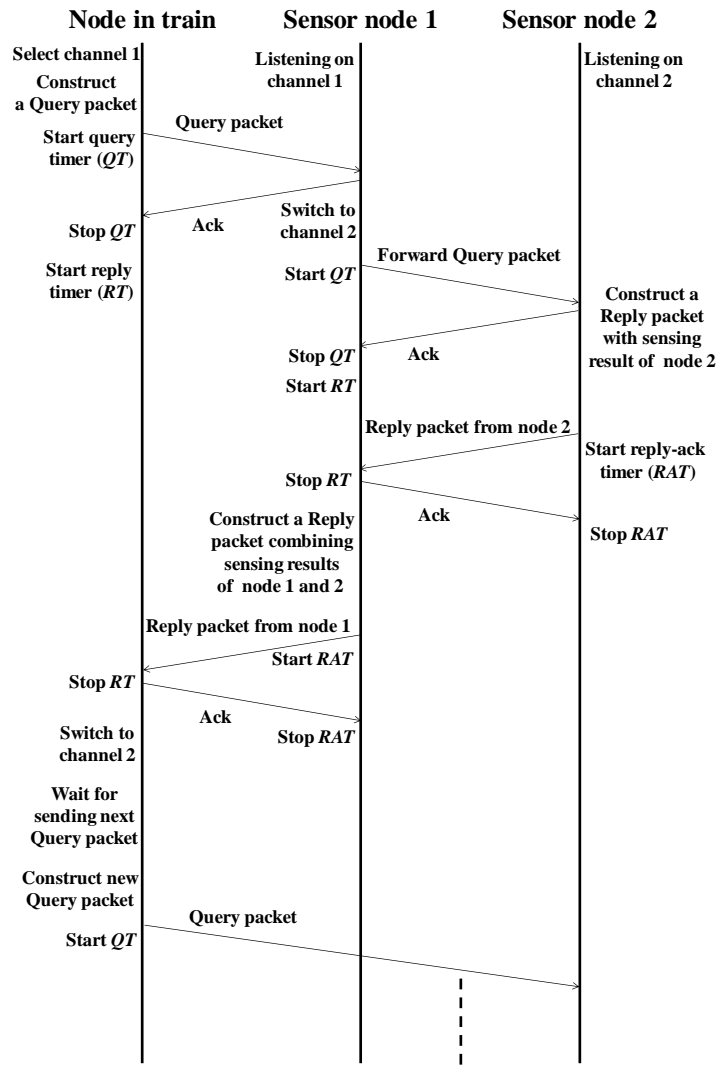


Figure 2.9: Time-sequence diagram of operations of our protocols

that the Data Link layer simply works with the packet got from the Network layer making no further change to it. Here, the only task of the Data Link layer is to perform necessary channel switching.

2.4.2 Operational Overview of the Protocols

Figure 2.9 presents a high-level operational overview of our proposed protocol with a time-sequence diagram. The overview pertains to the scenario presented in Figure 2.5a. We elaborate steps in Figure 2.9 below.

Step 1: In the very first step, the Inspector node in train sends a Query packet to the sensor node 00 (having a destination ID 01) using the default Channel 1. After sending the Query packet, the Inspector node starts a timer called query timer (QT) for this packet

to wait for corresponding Acknowledgment (Ack). Upon receiving the Query packet, the sensor node 00 sends an Ack back to the Inspector node. After receiving this Ack, the Inspector node stops the QT and starts a new timer called reply timer (RT) to wait for receiving corresponding Reply packet from the sensor node 00.

Step 2: In this step, the sensor node 00 sends a Query packet to sensor node 01 after switching to Channel 2 from Channel 1. After sending the Query packet, the sensor node 00 starts a QT for this packet to wait for corresponding Ack. After receiving the Query packet, the sensor node 01 sends an Ack back. Upon receiving this Ack, the sensor node 00 stops the QT and starts a RT for the Reply packet from sensor node 01. The reason behind starting a new timer (RT) rather than continuing the ongoing timer (QT) is that the Ack is generally sent immediately, whereas the Reply is sent after sensing the track over a period of time.

Step 3: Next, the sensor node 01 sends a Reply packet to the sensor node 00. After sending the Reply packet, the sensor node 01 starts a reply-ack timer (RAT) for this Reply packet to wait for its Ack. Upon receiving the Reply packet, the sensor node 00 sends an Ack back to the sender node 01. After receiving this Ack, the sensor node 01 stops the RAT .

Step 4: Afterwards, the sensor node 00 sends a Reply packet incorporating its own sensing result, sensing result from the sensor node 01 (if any), and the condition of the sensor node 01 (whether the sensor node 01 is responding or not) to the Inspector node after switching its channel to Channel 1 from Channel 2. Sensor node 00 starts a RAT after sending the Reply packet. Upon receiving the Reply packet, the Inspector node sends an Ack back to the sensor node 00. After receiving this Ack, the sensor node 00 stops its RAT .

Step 5: Finally, the Inspector node sends a Query packet to the sensor node 01. To do so, it waits for a certain time duration for the entrance of train in the communication range of sensor node 01. The waiting time duration is iteratively updated measuring the speed of the train and the distance covered by the train. When the waiting time expires, the Inspector node switches its channel from Channel 1 to Channel 2 and sends a Query packet to the sensor node 01. Then, the similar process, as presented above, continues involving the sensor nodes 01 and 10 (Figure 2.5b).

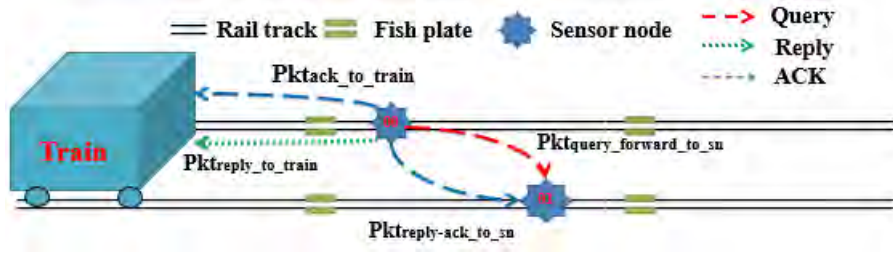


Figure 2.10: Transmission of packets from a sensor node to the train and to other sensor node

2.4.3 Communication Overhead

In general, communication overhead is defined as the total number of packets to be transmitted from one node to another. It also includes the overhead of the routing process, routing table and packet preparation in a sensor node. Our proposed network topology is very simplistic in nature, resembling a linear topology. Hence, the communication overhead of our proposed paradigm depends on the number of sensor nodes on the route of a train and the total number of the packet transmitted by a sensor node.

In our proposed protocol, communication from train is performed over two hops. Fig. 2.10 exhibits the transmission of the packet from one sensor node (i.e., 00) to the train and to immediate next sensor node (i.e., 01) for a communication. The sensor node 00 performs transmission in four cases:

- Case I: upon receiving an initial query message from the train, the sensor node 00 forwards the query to the very next sensor node 01. The transmitted packet is delineated as $Pkt_{query_forward_to_sn}$ in Fig. 2.10.
- Case II: sensor node transmits an acknowledgment to the train after receiving a query message from it ($Pkt_{ack_to_an}$).
- Case III: next, after receiving a reply message from the very next node comprising the monitoring report about the condition of the rail track ahead, the sensor node transmits the reply to the train incorporating its own report ($Pkt_{reply_to_an}$).
- Case IV: finally, after receiving a reply from the very next sensor node 01, the sensor node 00 sends a reply-ack message to the very next sensor node ($Pkt_{reply-ack_to_sn}$).

Our proposed protocol use three types of thresholds, i.e., Th_Q , Th_R , Th_{RA} for re-transmission of packets (specified in 2.4.5). The total number of transmitted packet per



Figure 2.11: State diagrams of operation in the Application layer

communication is computed as follows:

$$\begin{aligned}
 & Pkt_{query_forward_to_sn} \times Th_Q + Pkt_{ack_to_train} \times Th_Q + \\
 & Pkt_{reply_to_train} \times Th_R + Pkt_{reply_ack_to_sn} \times Th_{RA}
 \end{aligned} \tag{2.1}$$

Eq. 2.1 provides an estimation of the communication overhead per communication. The occurrences of communication depend on the number of sensor nodes on the rail track.

2.4.4 Application Layer Protocol

The role of our Application layer is to ensure overall control of node functionalities. Figure 2.11 presents Application layer state diagrams for both Inspector and the sensor node.

2.4.4.1 Application layer in the inspector node

As shown in Figure 2.11a, operation in Application layer in the Inspector node can be in one of the two states. In the Idle state, the Application layer waits for a certain amount of time following an idle timer before starting a new communication. This idle timer is iteratively updated based on speed of train (can be measured by an onboard sensor) and the distance by the train (which can be iteratively calculated from the speed). When the idle timer expires, operation in the Application layer switches to the Communication state. The inspector node performs all required communication with the sensor nodes in this state. Here, after receiving a Reply packet from the immediate next sensor node, the Inspector node again switches to the Idle state detecting an end of communication.

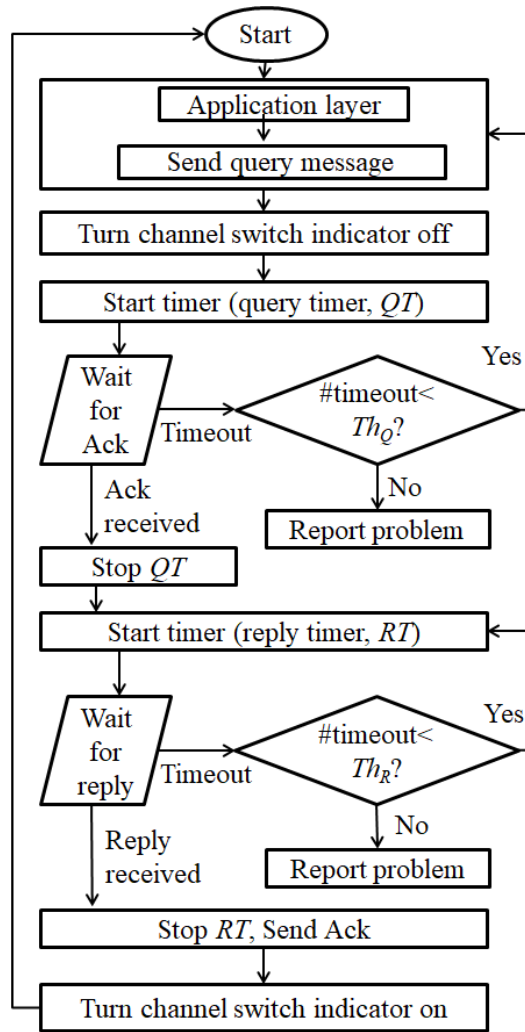


Figure 2.12: Transport layer protocol in the Inspector node

2.4.4.2 Application layer in the sensor node

When a Query packet is received, operation in the Application layer switches from the Idle state to Communication state. In this case, an incoming Query packet either from a train or from an immediate previous sensor node initiates the communication session. This communication session of the sensor node terminates after receiving an Ack in response to the Reply packet sent earlier from the sensor node.

2.4.5 Transport Layer Protocol

Now, we present the Transport layer protocol of our proposed paradigm. The protocols differ for the two types of nodes.

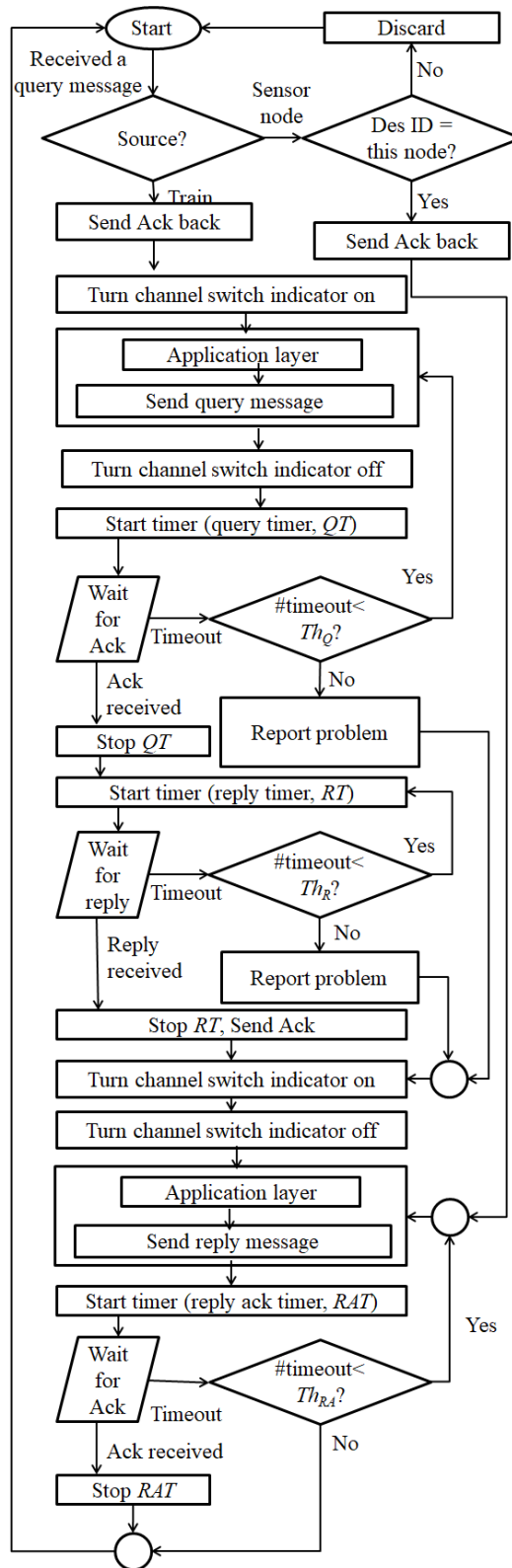


Figure 2.13: Transport layer protocol in the sensor node

2.4.5.1 Transport layer in the inspector node

Figure 2.12 presents a flow chart of operation in Transport layer for the Inspector node. Here, first, the Transport layer sends a query message to the very next sensor node and starts

a query timer (QT) for corresponding Ack. In case of expiration of the QT , a new query message is sent to the same sensor node based on the query-timeout threshold (Th_Q). In case of exceeding the number of such attempts beyond Th_Q , a dead link pertinent to the sensor node is reported. In case of receiving corresponding Ack, QT is stopped and a reply timer (RT) is started. Upon receiving the reply message, the Transport layer sends an Ack back to the sensor node and stops RT . In case of not receiving the reply message an approach similar to QT expiration handling occurs for the RT expiration based on the reply threshold (Th_R). Finally, the Transport layer sets *channel switching indicator* flag, which is shared with the Data Link layer, for initiating the next transmission.

Simplistic modeling, a small number of control messages, the absence of congestion window and buffering are key features of our proposed Transport layer protocol. These features make our protocol more lightweight compared to many other existing alternatives.

2.4.5.2 Transport layer in the sensor node

Figure 2.12 presents a flow chart of operation in the Transport layer processing in a sensor node. When a query message is received from a train, the Transport layer sends a newly-generated query message to its very next sensor node using a different communication channel. Next, after receiving a reply message from that very next sensor node, the Transport layer sends a reply message to the Inspector node on the train using the other communication channel. Acknowledgments for these query and reply messages are handled in a process similar to that performed by the Inspector node. Besides, if a sensor node receives a query message and its ID is same as the destination ID of the query message, the sensor node sends back a reply message to the source sensor node of the query message and the query message is not forwarded further. If the IDs do not match, the query message is simply discarded without sending the reply message.

2.4.5.3 Responses towards packet loss

In our proposed protocol, we envision to handle occurrences of packet loss. Here, we delineate different responses of our proposed protocol against packet loss.

- Case I: According to Fig. 2.9, sensor node 1 sends an acknowledgment packet back

to the train node after receiving a query packet from the train node. If this acknowledgment packet gets lost, then the train waits for the expiration of query timer QT . After the expiration of QT timer, the train retransmits the query packet to sensor node 1 based on the value of query-timeout threshold (Th_Q). If the number of retransmits exceed beyond Th_Q , then, a dead link is reported pertinent to sensor node 1.

- Case II: After receiving a query packet from the train node, sensor node 1 forwards this query packet to sensor node 2 (Fig. 2.9) starting QT timer. Now, if this query packet gets lost, corresponding Ack will not be sent by the sensor node 2. Then, the sensor node 1 waits for the expiration of QT timer and resends the query packet based on the value of Th_Q . If the number of timeouts exceeds the value of Th_Q , then, a dead link is reported pertinent to sensor node 2. For such a case, sensor node 1 will generate a report packet based on its sensing result and forward it back to the train node.

If the Ack packet from the sensor node 2 gets lost on the way to sensor node 1, it resembles the same scenario as Case II and handled in a similar manner by the sensor node 1.

- Case III: Let us consider another case, where the reply packet from sensor node 2 fails to reach sensor node 1. For such a case, sensor node 2 will wait for reply-ack time (RAT) before retransmitting the reply packet based on reply-ack threshold (Th_{RA}). If the number of timeouts of reply-ack timer is beyond Th_{RA} , then, the corresponding link is reported as dead link. As a response, now, sensor node 1 constructs a reply packet with its sensing result and transmits the packet back to the train node.
- Case IV: Now, let us consider another scenario, where the reply packet sent by sensor node 1 gets lost on the way to the train node. Here, sensor node 1 waits again for the expiration of reply-ack timer, i.e., RAT and retransmits the reply packet. The number of retransmission of reply packet is restricted by threshold Th_{RAT} . On the other hand, the train node restarts the reply timer (RT) for Th_R times before reporting a problem.

2.4.6 Network Layer Protocol

Network layer of the Inspector node only adds ID of the destination sensor node as per the pre-specified address list of ordered sensor nodes to form a packet as shown in Figure 2.8. In our case, we need to communicate the packet over a linear topology having previously-known orderly addressed nodes. This can be done with fixed-address routing eliminating the need of route finding. Consequently, our Network layer protocol becomes ultra simplistic and lightweight.

2.4.7 Data Link Layer and Physical Layer Protocols

The Data Link layer only takes decision for channel switching based on the channel switch indicator flag set by the Transport layer. Owing to simplistic linear topology of our proposed protocol, there will be only two nodes within the communication range of a sensor node. Furthermore, no external node will interfere from outside during communication. Hence, our MAC protocol does not require any carrier sensing control packets to avoid collision. In our proposed protocol, we have not considered duty cycling as this can result in low delivery ratios [115, 116] even though it can lower energy consumption. Such a lowered delivery ratio is critical to our time-sensitive application as explored in this study. Accordingly, the Data link layer simply passes the decision along with a frame (same as the packet) to the Physical layer. The Physical layer broadcasts the frame as per the decision through RF communications using Gaussian frequency shift keying (GFSK) modulation schemes.

2.5 Adjustment of the Operational Parameters

We use three types of timers (QT , RT , and RAT) and three types of thresholds (Th_Q , Th_R , and Th_{RA}) in our protocol. We need to set values of these parameters to achieve high delivery ratio, low end-to-end delay, and low energy consumption. To do so, in this section, we first determine upper bounds for these parameters. Towards that road, queuing theory is considered as a potential mathematical model [117–120]. In general, queuing theory is suitable to model or analyze networks in which multiple flows are injected with different rates and served with different policies. Such networks with irregular demands or traffic bursts re-

sult in queues. However, in our proposed paradigm for missing rail block detection system, we consider a very simplistic linear topology with fully deterministic demands and services, hence, eliminating the queuing effect. Besides, our requirements are very simple and no other external devices will interfere from outside. We deploy the sensor devices in such a way that there lie only two sensor nodes within the communication range of a sensor node. Hence, our proposed paradigm eliminates MAC delays due to collision during data transmission. Therefore, we utilize a simplistic numerical analysis considering retransmission to determine upper bounds for different parameters in our proposed protocol.

2.5.1 Bound of Timers and Thresholds

As we mentioned earlier, we intend to notify a running train about the condition of 1km rail track ahead. This implies that the train should receive the reply message when it is at least 1km apart from the sensor node 01 in Figure 2.5a. As discussed in Section 2.3, we safely consider a transmission range of 600m based on the capability of our adopted networking module [112]. Hence, as per the scenario of Figure 2.5a, the train should receive the reply message from the sensor node 01 before running 200m distance or less after entering into the transmission range of the sensor node 00 and sending it (node 00) a query message. This confirms the distance covered ahead to be at least 600m+600m-200m =1000m. Now, the maximum distance d covered by a train through running at a speed v m/s, during an ongoing communication with the sensor node 00, can be approximated as follows:

$$d = v \times (2 \times QT \times Th_Q + 2 \times RAT \times Th_{RA} + RT \times Th_R) \quad (2.2)$$

Here, for the similarity in packet size and communication link, we infer that QT is equal to RAT and Th_Q is equal to Th_{RA} . Thus, Eq. 2.2 can be reduced as follows:

$$d = v \times (4 \times QT \times Th_Q + RT \times Th_R) \quad (2.3)$$

As d must be less than 200m, we deduce the following -

$$v \times (4 \times QT \times Th_Q + RT \times Th_R) < 200 \quad (2.4)$$

Now, we intend to determine upper bounds of the variables in Eq. 2.4. As we mentioned earlier, the maximum speed of train in the country under our focus is 80kmph. Hence, the

Parameter	Value	Parameter	Value
Transmission range (m)	600	Tx power (dBm)	20
Frequency (MHz)	433	Rx power (dBm)	-117
Bandwidth (Kbps)	5	Idle power (dBm)	12.5
Radio propagation model	Two-ray ground	Sensing power (dBm)	16.02
Type of traffic	CBR	Train speed (km/hr)	80
Packet size (byte)	1	Simulation time (s)	20

Table 2.1: Simulation parameters

upper bound of the train speed v is set to 22.22m/s. Note that, after getting a query message, a sensor node takes less than 2 seconds in preparing the sensing results which we confirm by our experimentation. Preparation of the sensing results runs simultaneously in two sensor nodes under query of the Inspector node. In addition, we experimentally found that a node takes less than 50ms time to switch a channel. As a result, we consider the minimum value for RT to be 2150ms including a safety margin of at least 100ms. Accordingly, from a numerical simulation of Eq. 2.4 using different values of operational parameters, we find upper bounds of QT , Th_Q , RT , and Th_R as 50ms, 20, 2200ms, and 2 respectively.

Next, we investigate impacts of variations in these parameters on performance metrics namely end-to-end delay, energy consumption, and delivery ratio using a network simulator `ns-2`.

2.5.2 Impacts of Parameters on Network Performance

In order to investigate changes in performance owing to variations of different timers and thresholds, we implement our proposed protocol in `ns-2`. In this subsection, we first provide a brief description of our real experimentation based simulation settings followed by simulation results and findings.

2.5.2.1 Simulation settings

For the integration of our proposed cross-layer protocol, we need to make certain changes in the existing protocol stack of `ns-2`. We deploy a lightweight MAC protocol omitting the Request to send (RTS) and Clear to send (CTS) packets. Our customized MAC protocol takes its decision of channel switching based on an indicator flag shared with the Transport layer

QT , RAT (ms)	RT (ms)	Th_Q , Th_{RA}	Th_R	Distance (m)	Delivery ratio (%)	E2E delay (ms)	Avg. energy consump. (J)
1	2151	1 - 9	1, 2	0	0	-	0.118
5	2155	1	1, 2	90.7	100	2206.19	0.2819
		3	1, 2	108.2	100	2250.20	0.3671
		5	1, 2	128.0	100	2272.23	0.4882
		7	1, 2	156.3	100	2296.25	0.6018
		9	1, 2	197.9	100	2316.29	0.8304
10	2160	1	1, 2	90.7	100	2206.19	0.2819
		3	1, 2	108.2	100	2250.20	0.3671
		5	1, 2	128.0	100	2272.23	0.4882
		7	1, 2	156.3	100	2296.25	0.6018
		9	1, 2	197.9	100	2316.29	0.8304
20	2170	1	1, 2	90.7	100	2206.19	0.2819
		3	1, 2	108.2	100	2250.20	0.3671
		5	1, 2	128.0	100	2272.23	0.4882
		7	1, 2	156.3	100	2296.25	0.6018
		9	1, 2	197.9	100	2316.29	0.8304
50	2200	1	1, 2	90.7	100	2206.19	0.2819
		3	1, 2	108.2	100	2250.20	0.3671
		5	1, 2	128.0	100	2272.23	0.4882
		7	1, 2	156.3	100	2296.25	0.6018
		9	1, 2	197.9	100	2316.29	0.8304

Table 2.2: Impacts on distance and different performance metrics for varying values of timers and thresholds

and passes the decision to the wireless Physical layer. For the Network layer, we emulate the notion of broadcasting. Besides, we deploy our proposed Transport layer protocols in ns-2. We provide an average result of twenty simulation runs each having a simulation time of 20s.

In our simulation, we construct a linear scenario based on Figure 2.5 comprising four nodes. Here, we have one Inspector node and three sensor nodes. The Inspector node moves towards the sensor node, emulating the movement of a train, at a uniform speed of 80kmph. Additionally, we exploit the built-in power models of ns-2 to calculate energy consumption in our simulation. In the calculation of energy consumption, we use our experimentally-obtained values and measurements provided in [112] to resemble our adopted HC-12 module. Table 2.1 presents the values and measurements used in our simulation.

2.5.2.2 Simulation results

Table 7.2 delineates the impacts of variation in different timers and thresholds on traveled distance and different performance metrics. Here, the distance resembles the total distance passed by a train before the train receives a Reply packet from the sensor node after sending a query. Consequently, we explore variations in different performance metrics for different values of timers and thresholds considering the above mentioned upper bound values. Here, we use three performance metrics namely delivery ratio, end-to-end delay, and average energy consumption. In our simulation, end-to-end delay represents the total time passed between sending a Query packet from the Inspector node and receiving a Reply packet back from the sensor node in response to the query.

We evaluate values of traveled distance and performance metrics starting from 1ms as the value of QT . Table 7.2 shows that, for this value, no packet gets successfully transmitted irrespective of values of Th_Q and Th_R . Therefore, we increase the value of QT up to 50ms (the upper bound derived from our numerical analysis). Here, for a fixed value of Th_Q and Th_{RA} , the values of distance, end-to-end delay, and energy consumption remain same for the different values of QT . However, for a specific value of QT , the distance, end-to-end delay, and energy consumption increase with an increase in Th_Q and Th_{RA} . Note that, since we have adopted the upper bound of our distance as 200m, we do not increase the values of Th_Q and Th_{RA} beyond 9 to remain within the 200m distance. Here, the delivery ratio remains 100% irrespective of all variations. Moreover, Table 7.2 demonstrates that values of distance and performance metrics remain same irrespective of variation in Th_R . Consequently, we vary the values of RT using the equation. $RT = 2150 + QT$ (based on our numerical analysis). Our results reveal that for any value of QT , the distance increases with an increase in the values of both Th_Q and Th_{RA} .

Next, to exhibit the generalization of our proposed protocol, we aim to extend our simulations with different parameter values, such as different number of sensor nodes and speed of the train. We vary the number of sensor nodes on the rail track from 2 to 5. Table 2.3 exhibits the results for the variation in the number of sensor nodes on the rail track. Our simulation reveals that the delivery ratio remains 100% for all variations. The average end-to-end delay does not exhibit any significant changes for an increase in the number of sensor nodes.

# sensor nodes	Delivery ratio	Avg. end-to-end delay (ms)	Avg. energy consumption (J)
2	100	2316.294	0.8304
3	100	2316.284	1.173
4	100	2316.274	1.468
5	100	2316.277	1.748

Table 2.3: Impact of variation in number of sensor nodes on performance metrics

Speed (km/h)	Delivery ratio	End-to-end delay (ms)	Avg. energy consumption (J)
20	100	2316.302	0.8304
40	100	2316.300	0.8304
60	100	2316.297	0.8304
80	100	2316.294	0.8304

Table 2.4: Impact of speed variation on performance metrics

Direction of train	Distance (m)	Delivery ratio	Avg. end-to-end delay (ms)	Avg. energy consumption (J)
Forward	125.7	99.93	2547.30	2.734
Reverse	123.8	99.34	2536.23	2.732

Table 2.5: Impact of direction of train's route on performance metrics

Packet error rate (%)	Delivery ratio	End-to-end delay (ms)	Avg. energy consumption (J)
20	99.812	2552.30	2.773
40	99.45	2571.45	2.782
60	97.19	2601.36	2.786
80	89.69	2753.14	2.820

Table 2.6: Impact of varying packet error rate on performance metrics

However, the average energy consumption exhibits an increasing trend with an increase in the number to sensor nodes.

Consequently, we also vary the speed of the train on the performance of our proposed protocol. Table 2.4 demonstrates the results for this variation. We vary the train speed from 20kmph to 80kmph with a granularity of 20kmph. Our simulation reveals that the delivery ratio remains 100% for all these variations in speed. Consequently, the average energy consumption remains the same with an increase in the speed of the train. Moreover, the end-to-end delay does not exhibit any significant change for higher speed of the train. In addition to explore the robustness of our proposed protocol in real-world rail track, we

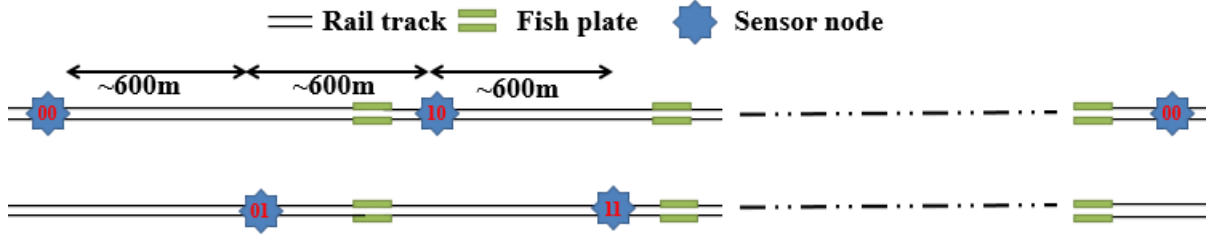


Figure 2.14: Topology for 10km long rail track

Delivery ratio	End-to-end delay (ms)	Avg. energy consumption (J)
91.6	2753.45	2.734

Table 2.7: Performance of our proposed protocol for parallel rail tracks

conduct simulation with a 10km rail track having around 16 sensor nodes are deployed on the rail track following our proposed zigzag topology (Fig. 2.14). Consequently, we conduct simulation for scenarios when the train is coming from opposite direction as per Fig. 2.6a. Table 2.5 delineates the impact of train’s route direction on different performance metrics for rail track of about 10km long. The simulation results exhibit that our proposed protocol is also applicable for reverse direction of travel route of the train.

Furthermore, to explore the robustness of the proposed system against real-world communication problems such as lossy links, we introduce packet losses into our simulation for a scenario of 10km long rail track with 16 sensor nodes deployed on the rail track. Here, we vary the packet error rate of 20%, 40%, 60%, and 80%. Table 2.6 illustrates the results for this variation. Our simulation result exhibits that our protocol still exhibits a decline in delivery ratio for different packet error rate. However, the end-to-end delay and average energy consumption do not exhibit any significant change for different packet error rate.

So far, we consider single track for our above mentioned simulation scenarios. Next, we want to explore the performance of our proposed paradigm for parallel rail lines. For this simulation, we consider 10km long two parallel rail tracks. Here, about 16 sensor nodes are deployed on the rail track for each of the parallel rail lines. Two trains are simultaneously travelling over the two parallel rail tracks. Table 2.7 demonstrates that the delivery ratio of our proposed protocol decreases significantly for parallel rail tracks. To improve the performance for parallel rail track further modifications are necessary for our proposed protocol, which we envision to explore in near future.

2.6 Performance Evaluation

In this section, we demonstrate the performance of our proposed protocol compared to different alternatives.

2.6.1 Performance Comparison against Different Alternatives

Here, we first compare our protocol with that of well-known state-of-the-art protocols used for railway monitoring [81,82]. These protocols mainly use IEEE 802.11 and IEEE 802.15.4 MAC protocols with corresponding radios. Traditional 802.11 radios are suitable for long-range data transmission and have high bandwidth. Consequently, they utilize RTS and CTS to avoid collisions. However, usage of these control messages consumes a significant amount of energy making IEEE 802.11 an energy-hungry protocol. On the other hand, 802.15.4 radios have low bandwidth and suitable for short-range communication. Consequently, IEEE 802.15.4 does not utilize any RTS and CTS for avoiding collisions. Hence, it offers an energy-efficient alternative. For simulating both 802.11 and 802.15.4 MAC protocols, we use Ad hoc On-Demand Distance Vector (AODV) and TCP Tahoe as Network and Transport layer protocol. Besides, we focus on using protocols specifically designed for wireless sensor networks. Here, we utilize well-known Reliable Multi-Segment Transport (RMST) [121] protocol in the Transport layer and Directed Diffusion (DD) [122] as the routing protocol. For this variation, we use IEEE 802.15.4 as MAC protocol. Next, use SMAC as MAC layer protocol. Consequently, we explore different variants of TCP such as TCP Reno, SACK, and Westwood. For these variants we consider SMAC and AODV as MAC and Network layer protocol. Furthermore, we also explore two Transport layer protocols specifically designed for embedded sensor networks, i.e., iTCP [123] and MABCC [124]. Table 2.8 exhibits performance of our protocol with respect to different alternative protocols. Table 2.9 depicts the percentages of improvement using our proposed protocols with respect to all these alternatives. The table exhibits superiority of our proposed protocol over all the alternatives.

Next, in order to investigate impacts of operations of our proposed cross-layer protocols at different layers, we compare the performance of our protocols against that of existing alternatives of MAC, Network, and Transport layers. Here, we first replace MAC

Protocol under comparison	Delivery ratio (%)	End-to-end delay (s)	Avg. energy consumption (J)
802.11, AODV, TCP Tahoe	92	3.66	63.48
802.15.4, AODV, TCP Tahoe	80	3.06	3.40
802.15.4, Directed Diffusion, RMST	97	4.36	1.48
SMAC, AODV, TCP Tahoe	79	4.897	1.795
SMAC, AODV, TCP Reno	79	4.8923	1.80
SMAC, AODV, TCP SACK	78	4.895	1.793
SMAC, AODV, TCP Westwood	78	4.925	1.801
SMAC, AODV, iTCP	78	6.18	1.766
SMAC, AODV, MABCC	97	2.59	1.765
802.11, Proposed NL, Proposed TL	100	5.08	5.79
802.15.4, Proposed NL, Proposed TL	100	8.04	1.02
Proposed MAC, DSDV, Proposed TL	27	5.09	1.88
Proposed MAC, DSR, Proposed TL	100	4.69	0.88
Proposed MAC, Static routing, Proposed TL	30	4.40	0.363
Proposed MAC, Proposed NL, TCP NewReno	62	4.73	1.79
Proposed MAC, Proposed NL, TCP Vegas	95	4.80	1.80

Table 2.8: Performance evaluation of our protocol with respect to different alternative protocols

Protocols under comparison	% improvement with respect to		
	Delivery ratio	End-to-end delay	Avg. energy consump.
802.11, AODV, TCP Tahoe	8	27	98
802.15.4, AODV, TCP Tahoe	24	34	75
802.15.4, Directed Diffusion, RMST	3	47	44
SMAC, AODV, TCP Tahoe	27	46	54
SMAC, AODV, TCP Reno	27	46	54
SMAC, AODV, TCP SACK	28	46	54
SMAC, AODV, TCP Westwood	28	46	54
SMAC, AODV, iTCP	28	57	53
SMAC, AODV, MABCC	4	-2	53
802.11, Proposed NL, Proposed TL	0	54	85
802.15.4, Proposed NL, Proposed TL	0	71	18
Proposed MAC, DSDV, Proposed TL	270	53	56
Proposed MAC, DSR, Proposed TL	0	53	5
Proposed MAC, Static routing, Proposed TL	233	47	-1
Proposed MAC, Proposed NL, TCP NewReno	60	50	53
Proposed MAC, Proposed NL, TCP Vegas	5	51	54

Table 2.9: Percentages of improvement using our protocol with respect to different alternative protocols

layer of our proposed protocol by two MAC alternatives namely 802.11 and 802.15.4 keeping our protocols in rest of the layers intact. Next, we replace our Network layer protocol by Destination-Sequenced Distance-Vector (DSDV), Dynamic Source Routing (DSR), and static routing protocol. Finally, we replace our proposed Transport layer protocol by popular TCP variants namely TCP NewReno [125] and TCP Vegas [125]. Table 2.8 exhibits performance of our protocol with respect to different alternative protocols. Consequently, Table 2.9 demonstrates percentages of improvement compared to all these alternative. We perform our performance comparison to analyze contributions of each of the components we have designed. As we analyze the individual contribution of all our developed components, we present all the variants in a row in the table. Here, all the reported values of % improvement are achieved through the combination of all our proposed protocols against the combination we have mentioned in the corresponding rows. The results reveal that our proposed protocol outperforms all the existing alternatives with respect to the different performance metrics covering delivery ratio, end-to-end delay, and average energy consumption.

Additionally, we focus on another performance metric namely network lifetime. To compute average network lifetime (t), we utilize the following equation.

$$t = \frac{E_i}{P} \quad (2.5)$$

Here, E_i is the initial energy of the batteries used in all sensor modules and P is the average power consumed by the sensor modules. We consider most commonly used LiPo battery with capacity 12000mAh. Next, to compute power consumed by sensor devices we use the following equation.

$$P = \frac{E_a + (t_i \times P_i)}{t_a + t_i} \quad (2.6)$$

Here, E_a denotes the energy consumption of the sensor devices during active communication, t_i is the interval between arrival of next train where the sensors remain idle, and P_i is the idle power of the sensors. Finally, t_a refers the time needed to perform active communication by sensor devices and t_i refers the time sensor devices remain idle for arrival of the next train.

Table 2.10 illustrates the results on network lifetime using our protocol with respect to different other alternatives. Here, we vary the arrival interval of trains as 10mins, 20mins,

Protocols under comparison	Network lifetime in days for different arrival intervals of trains		
	10 mins	20 mins	30 mins
802.11, AODV, TCP Tahoe	4	7	9
802.15.4, AODV, TCP Tahoe	21	24	25
802.15.4, Directed Diffusion, RMST	24	26	27
SMAC, AODV, TCP Tahoe	18	22	24
SMAC, AODV, TCP Reno	26	27	27
SMAC, AODV, TCP SACK	26	27	27
SMAC, AODV, TCP Westwood	26	27	27
SMAC, AODV, iTCP	27	28	28
SMAC, AODV, MABCC	24	26	27
802.11, Proposed NL, Proposed TL	18	22	24
802.15.4, Proposed NL, Proposed TL	26	27	27
Proposed MAC, DSDV, Proposed TL	26	27	27
Proposed MAC, DSR, Proposed TL	26	27	27
Proposed MAC, Static routing, Proposed TL	27	27	28
Proposed MAC, Proposed NL, TCP NewReno	24	26	27
Proposed MAC, Proposed NL, TCP Vegas	24	26	27
Proposed MAC, Proposed NL, Proposed TL	27	28	28

Table 2.10: Network lifetime using our protocol with respect to different alternative protocols for different intervals between arrivals of two successive trains

and 30mins. The results reveal that our proposed protocol outperforms all the existing alternatives in terms of network lifetime in addition to other performance metrics (delivery ratio, end-to-end delay, and average energy consumption) as presented earlier in Table 2.4.

2.6.2 Justifications behind Adopting Different Alternatives

Exploration of the existing studies on real-time MAC protocols for wireless sensor networks [126] reveal that SMAC is used for real-time communication. Consequently, studies pertinent to railway monitoring [81, 82] mainly use IEEE 802.11 and IEEE 802.15.4. Therefore, we use these alternatives of MAC layer protocol for comparison. Besides, the studies in [127] [122] specifies that AODV, DSR, and Directed Diffusion (DD) are intended for real-time communication in WSNs. Therefore, we use these routing protocols along with static routing in our performance comparison to evaluate the performance of our proposed protocols against these Network layer alternatives. Furthermore, studies presented



Figure 2.15: Snapshot of our real deployment

in [128, 129] specify that TCP variants such as TCP Tahoe, TCP Reno, NewReno, Vegas, SACK, and Westwood can be options for real-time communication in WSNs. Hence, we have adopted these alternatives in our performance comparison to evaluate the performance of our proposed protocols against these Transport layer alternatives. Moreover, we also adopt iTCP [123] and MABCC [124] as other Transport layer alternatives in our performance comparison, as these two alternatives have been specifically explored for embedded sensor networks for enhanced performance. Nonetheless, we have adopted different combinations of the alternatives in our performance comparison to show efficacy of the combination of our proposed protocols in the three different layers.

Next, we present outcomes of our real deployment using the proposed protocols.

2.7 Performance Evaluation through Real Deployment on a Railline

We perform a set of experiments to evaluate the performance of our proposed network paradigm in a real scenario. In this section, first, we delineate the real deployment settings followed by the experimental results. Next, we present a comparison between our proposed protocol and other well-known protocols in the real scenario.

2.7.1 Settings of Real Deployment

In our experimental setup, we adopt communication scenario as shown in Figure 2.5, i.e., three sensor nodes on the rail track and one Inspector node on the train. During the ex-

Combination	QT , RAT (ms)	Th_Q , Th_{RA}	RT (ms)	Th_R	Delivery ratio (%)	End- to- end- de- lay (ms)	Avg. power con- sumption per node (mW)
C1	1	7	2151	2	0	-	48.23
C2	3	3	2153	2	31.2	2224	74.3
C3	3	5	2153	2	34.3	2251	74.4
C4	3	7	2153	2	36.5	2276	74.4
C5	5	3	2155	2	100	2173	73.2
C6	5	5	2155	2	100	2197	73.7
C7	5	7	2155	2	100	2213	74.1
C8	10	3	2160	2	100	2177	73.2
C9	10	5	2160	2	100	2195	73.8
C10	10	7	2160	2	100	2219	74.1
C11	20	3	2170	2	100	2175	73.3
C12	20	5	2170	2	100	2201	73.7
C13	20	7	2170	2	100	2223	74.2

Table 2.11: Experimental results from real deployments

perimentation, the maximum speed of the train was ~ 50 kmph and the average speed was ~ 30 kmph. Such speeds are frequently observed in the country under our focus. Besides, Figure 2.15 delineates a snapshot of our real deployment of a sensor node on the rail track. The Inspector node subsumes the same set of components except having no vibration sensor module. Similar to simulation, in our real experiment, we measured three performance metrics namely delivery ratio, end-to-end delay, and average power consumption per node for different combinations of timers and thresholds. These combinations of variables are emanated from our simulation results.

2.7.2 Results from Real Deployment

Table 2.11 summarizes results found in real experimentation. The notable fact is that the delivery ratio remains 100% for different valued combinations of variables with $QT, RAT \geq 5$ ms. Besides, in these cases, end-to-end delay and the average power consumption per node do not exhibit much variation. However, for the combinations with $QT, RAT < 5$ ms, the delivery ratio degrades significantly mimicking the results of the simulation. Besides, in these

Train speed (kmph)	End-to-end delay (ms)				
	C2	C5	C7	C10	C13
10	2230	2169	2216	2218	2221
20	2226	2175	2214	2223	2220
30	2217	2172	2215	2219	2228
40	2221	2176	2208	2224	2224
50	2226	2174	2212	2217	2211

Table 2.12: Effect of speed variation on end-to-end delay (ms)

Protocol	Coverage (m)	Avg. power consumption per node (mW)
IEEE 802.11	~ 120	214.5
IEEE 802.15	~ 75	126.4
Our protocol	~ 1200	73.7

Table 2.13: Comparison with well-known protocols

cases, the average power consumption per node remains higher than that for combinations with $QT, RAT \geq 5$ ms.

To investigate the effect of speed on the performance of our proposed protocol, we independently measured the aforementioned performance metrics at different train speeds of the train. For all combinations of parameters with $QT, RAT \geq 5$ ms, the delivery ratio remains same (i.e., 100%) for different train speeds. Table 2.12 shows the effect of train speed on end-to-end delay (in ms) for five different combinations - C2, C5, C7, C10, and C13 (as presented in Table 2.11). The table suggests that the end-to-end delay always remains close to 2.2 seconds and does not vary significantly with train speed.

Next, we compare the performance of our protocol with two well-known protocols used in wireless sensor network for rail track monitoring - IEEE 802.11 and IEEE 802.15.4 - in terms of energy consumption and coverage. Here, we define coverage as the maximum distance between the Inspector node and the sensor node 01 in Figure 2.5a, at which they can communicate reliably via the sensor node 00. To do so, we deployed two different settings involving ESP8266 (IEEE 802.11) and XBee (IEEE 802.15.4) following our proposed deployment topology (Figure 2.5). Table 2.13 summarizes the obtained results, which suggest substantially better performance of our protocol compared to the alternative approaches.

2.8 Implementation Aspects of Our Proposed Network Paradigm

In addition to performance evaluation, we analyze important implementation aspects of our proposed paradigm. The aspects are robustness, sensor failure, commercialization, and cost analysis.

2.8.1 Robustness against Real-world Communication Problems

In our proposed system, we envision to handle diverse real-world communication problems such as lossy links, interference, and collisions. To cope with lossy links, in our proposed protocol, we leverage the notion of Acknowledgment packets. Consequently, the Transport layer protocol performs re-transmission of different types of packets based on different timers such as query timer (QT), reply timer (RT), and reply-ack timer (RAT). However, since the train requires to receive the reply packet from about $\sim 1\text{km}$ ahead for a safe stoppage in case of sensing a discontinuity, the re-transmission of packets cannot continue for a long period of time. Hence, the protocol introduces different thresholds such as query threshold (Th_Q), reply threshold (Th_R), and reply-ack threshold (Th_{RA}) to restrict the number of re-transmissions of different packets. Next, to avoid interference and collisions, the sensor nodes utilize two different communication channels for two different real-time communications (one with the train and another with the next node) as described in Section 3.3.2.

2.8.2 Robustness of Reporting

In our proposed system, the Reply packet received by an Inspector node from the very next sensor node contains a report about the rail track ahead. The report can be of six types: (1) both of the next two sensor nodes are reporting continuity in rail track, (2) both of the next two sensor nodes are reporting discontinuity in rail track, (3) the very next sensor node is reporting discontinuity in rail track, (4) the second next node is reporting discontinuity, (5) the very next node is not responding, and (6) the second next node is not responding. However, among these reports, the fifth one can be assessed by absence of report message. Hence, we use 3 bits for report block of the packet format of our proposed paradigm. We convention-

ally interpret the first message as a green signal; second, third, and fourth messages as a red signal; and fifth and sixth messages as a yellow signal. Here, the trickiest task is interpreting the yellow signal, and we will explain this later in this section.

2.8.3 Failure of Sensors

In most of the cases, a group of miscreants uproots a long metal rail block to hinder rail communication. Here, miscreants can uproot a rail block along with its sensor nodes. In any case, i.e., uprooted rail block with or without its sensor nodes, the sensor module will sense a discontinuity in the rail track as shown in Figure 2.4b. Consequently, the Inspector node will interpret a red signal from the Reply packet sent by this sensor node. Now, the question is what will happen if the uprooted sensor node loses its power connection. In this case, this sensor node will not respond to any query from the train or another sensor node. As a result, the Inspector node will interpret this scenario as a yellow signal. In case of a yellow signal, it is not recommended to stop the train in the first place, because, some other issues (for example natural battery outage) can also result in a yellow signal. Therefore, in case of a yellow signal, drivers are recommended to slow down the train to a certain speed level so that they can observe the condition of rail track ahead from a reasonable distance at a slow speed and stop the train if any fault in the rail track is observed [130]. If no fault is observed, drivers can speed up the train again marking the sensor node for maintenance in the pre-specified ordered list of sensors as mentioned in Section 2.3.2. Now, another question remains as what will happen if only the sensor module is removed keeping the rest of the device working. Note that, it is nearly impossible to remove the sensor module in such a way. Even if the miscreants can do it, the sensor node will send a Reply packet including the default discontinuity report. Consequently, the Inspector node will interpret this occurrence as a red signal. This is the only case where a false alarm can be generated by our proposed system, and occurring such a case is very unlikely in reality.

2.8.4 Commercialization Requirement

We have presented a prototype of our system and its real deployment in Figure 2.3. The commercial version of it will subsume a mechanical cage, which will enable firm attachment

Hardware components	Cost
Piezoelectric sensor	\$1.5
Networking module	\$4
Microcontroller	\$.5
PCB	\$1
Total cost	\$7

Table 2.14: Breakdown of cost of different hardware components of our system

of the sensor node with the rail track and make the device waterproof. Note that, deployment of the commercial version will not result in any modification of the current rail track infrastructure, rather than incorporating the cage as an add-on. Although the cage makes the whole device less prone to vulnerabilities, scope still remains for the miscreants to create adverse situations.

2.8.5 Cost Analysis

The cost of hardware components required for our complete sensor node prototype is below \$7 considering the retail price of the piezoelectric sensor, networking module, microcontroller, PCB, battery, etc., as available in the country under focus. A breakdown of the cost is illustrated in Table 2.14. In commercial production, materials are purchased in bulk amount, which generally reduces the cost per item by at least 2 to 3 times than the retail price [131]. Besides, a typical breakdown shows that the material cost is 72% of the total product cost, which considers labor cost within the rest 28% [132]. Hence, the product cost including all other costs will still be less than \$7 in commercial production. Besides, according to the networking topology depicted in Figure 2.5, our system incorporates two sensor nodes per $\sim 1.2\text{km}$. Hence, the device cost per kilometer will be less than \$12 excluding packaging, deployment, and maintenance costs.

2.9 Conclusion

Derailments due to uprooting rails is a frequent and noteworthy problem in developing countries considering their economic losses and lethal consequences. Existing solutions to detect uprooted or faulty rails do not contemplate the context of developing regions that generally present limited network connectivity in rural rail areas along with low-resource settings. As a remedy, in this chapter, we propose a WSN-based automated real-time solution leveraging a new communication paradigm between an approaching train and rail track. For this purpose, we design low-cost and lightweight networking architecture and protocol, which are worth of adopting in developing regions. We evaluate the performance of our proposed network paradigm through both ns-2 simulation and real experimentation, which demonstrate its effectiveness and worthiness for our intended purpose.

However, our proposed protocol does not contain any security measures to ensure secure transmission of information about the rail track ahead. Till now, our main endeavor is to develop a new paradigm, which focus on transmitting information about a discontinuity in the rail track ahead to an approaching train for taking necessary initiatives to avoid a looming derailment. However, if the information about the track ahead can be falsified or can be delayed accidentally or maliciously, disasters such as train derailment and failures in the train wagons can be an ultimate consequence. Hence, ensuring the security of such a real-time system for detecting missing rail blocks is highly important. Therefore, in the next chapter, we endeavor to explore different vulnerabilities of the real-time system for detecting missing rail blocks. Towards that road, we aim to investigate applicability of different traditional attacks such as man-in-the-middle attack, reply attack, eavesdropping, etc. Consequently, we aim to explore the possibility of new security threats exploiting the vulnerability of energy sources of the real-time system for detecting missing rail blocks. Alongside, we envision to investigate the necessary countermeasures to overcome the security attacks. Towards the road to develop a countermeasure, we could add additional information such as train id and trip number to our existing packets and encrypt the packets using a shared crypto-key between the train and sensor node. Therefore, detail analysis on the attacks and countermeasures are the focus of our next chapter.

Chapter 3

Exploring Imminent Vulnerabilities, Attacks, and Countermeasures in Real-Time System for Detecting Missing Rail Blocks

3.1 Introduction

Railway system plays a crucial role in economic and social progress over many years in both developed and developing countries. However, derailments of trains have turned into a common phenomenon in developing countries such as Bangladesh, India, Kenya, etc., [21–27]. Such occurrences of derailments often result in huge amount of economic losses along with injuries of people, ranging from minor to severe, or even lethal consequences. In most of the cases, derailments occur due to missing rail blocks, which often become possible owing to the reality of having widespread availability of publicly-open rail tracks mostly in developing countries [21, 23, 26, 27]. Therefore, development of a real-time system for detecting missing rail blocks sustaining the reality and concerns paves the way for intelligent railway transportation system.

The process of transformation from the traditional railway transportation system to the intelligent railway transportation system has been successfully accomplished in many de-

veloped countries. However, low-income developing countries such as Bangladesh, India, Kenya, etc., raise crucial concerns in the way of devising specialized intelligent railway transportation systems to tackle derailments without introducing any major changes in the existing architecture. The concerns circle around widespread availability of publicly-exposed rail tracks, limited capability for escalating safety standard of the rail tracks owing to resource constraint, limited availability of electricity in rural areas, paucity of long-range communication network infrastructure along the rail tracks, etc. Hence, the railway transportation systems of developing countries often experience difficulties substantially different from that of the developed countries. Derailments of trains owing to missing rail blocks is a notable consequence of experiencing such difficulties.

Existing research studies pertinent to railway transportation systems mainly focus on wireless network based solutions for precise localization of trains and monitoring of rails for cracks, small breakage, and corrugation [29–34]. Most of these solutions demand well-established cellular network for long-range communication, GSM-R based specialized infrastructure, or WiMax connectivity, which are often difficult to ensure in many developing countries. Besides, the inclusion of wireless-based systems often expose different vulnerabilities associated with the networks [35]. Hence, the rails become potential targets for different security attacks in many developing countries. Therefore, analysis of potential vulnerabilities, attacks, and countermeasures grab interests of the research community. Studies presented in [36–40] focus on developing traditional attacks such as replay attack, displacement attack, jamming attack, etc., and their corresponding countermeasures for the balise-based train control system. However, the balise-based system usually used for knowing the accurate locations of the moving trains incurring a considerable cost, which is often difficult to bear by low-income developing countries. Thus, such existing studies mostly focus on expensive micro-level monitoring of rail way systems rather than focusing the perspective of real-time detection of missing rail blocks while being consistent with the context of low-income developing countries.

To the best of our knowledge, the study in [3] first presents a real-time system for detecting missing rail blocks taking into account the concerns pertinent to the developing countries. However, here, no network design has been discussed. Therefore, in Chapter 2, we propose

a network design along with node deployment topology (3.3.2) and a cross-layer protocol (3.4.1) for communication between an approaching train and sensor nodes embedded on rail track. In our proposed solution, the sensors on the rail tracks exploit vibration from an approaching train to detect discontinuity over a rail track. Then, the information about a discontinuity in the rail track ahead is sent to an approaching train for taking necessary initiatives to avoid a looming derailment. However, if the information about the track ahead can be falsified or can be delayed accidentally or maliciously, disasters such as train derailments and failures in the train wagons can become an ultimate consequence. Hence, ensuring security of such real-time system for detecting missing rail blocks is highly important. Therefore, in this chapter, we endeavor to explore different vulnerabilities of the real-time system for detecting missing rail blocks. Towards that road, we introduce a new security threat entitled as power attack exploiting the vulnerability of energy sources of the real-time system for detecting missing rail blocks. Consequently, we investigate two very well known attacks, i.e., man-in-the-middle attack and replay attack. The reason behind is: these attacks cause serious harms in comparison to other traditional attacks such as eavesdropping, masquerade attack, and black hole attack. Alongside, we also investigate the necessary countermeasures to overcome these attacks revealed through our study.

Based on our study, in this Chapter, we make the following set of contributions:

- We present a new security threat entitled as power attack through enabling quick depletion of energy resources of the sensor nodes employed for the purpose of real-time detection of missing rail blocks.
- We delineate attack models and formulate mathematical models to facilitate effective launching of the power attack.
- Alongside, we provide attack models for man-in-the-middle attack and replay attack, as these attacks cause more deleterious effects in real-time system for detecting missing rail blocks in comparison to other traditional attacks of sensor networks such as eavesdropping, black hole attack, and masquerading attack.
- Next, we sequentially propose countermeasures to mitigate all the exposed attacks.

- Finally, we perform rigorous experimentation to exhibit applicability and effectiveness of our proposed attack and threat models using both ns-2 simulation and real deployment on rail line.

3.2 Related Work

Researchers have exhibited profound interest in designing the components and systems involved in modern railway operation. Most of the existing studies mainly focus on inspection of railway system via detecting cracks, small breakages, stress, inclination in the rails [30–33, 98–106]. Besides, several methods are proposed to monitor overall railway system [29, 81, 104, 108]. Most of these studies exploit expensive acoustic emission and long-range ultrasound techniques to monitor rail crack and breakage. However, recently, the emergence of machine vision systems fosters design of on-board track monitoring systems [34, 133]. Such track monitoring systems capture high-resolution images of the rail track and then perform pattern recognition algorithm on the images to detect defects on the rail track.

Besides, there exists a few studies focus on designing suitable network paradigm considering outdoor long-term conditions of railway tracks [29, 81, 82, 111]. The authors in [29] proposed a WSN-based solution for signaling and control in railway stations using cellular networks. Besides, studies in [81, 82] utilize Bluetooth, IEEE 802.15.4, and WiFi for communication among sensor nodes. On the other hand, GSM, GPRS, UMTS, and GSM-R are also explored for similar communications. The above-specified solutions demand expensive deployment of expensive network structure.

However, the above-mentioned solutions are not applicable for developing countries such as Bangladesh, India, Kenya, etc., where the rail tracks are publicly open and have resource constraints. Furthermore, developing countries very frequently experience derailment owing to missing rail block for various reasons such as political protest, natural calamity, etc., hence, a real-time solution to detect missing rail block is of the utmost importance.

Consequently, existing studies also focus on investigation of security protocol for rail communication [36–40]. These studies mainly focus on the security aspects such as ex-

ploration of vulnerabilities, attack design, and countermeasure of the balise-based system used mainly in European Train Control System (ETCS) to retrieve the location of a moving train. However, the balise-based system is not deployed in the developed countries, hence, the proposed security measures of the balise-based system are not applicable for the developing countries. Moreover, the balise-based system do not address the detection of missing rail block. Hence, a low-cost real-time solution is needed to detect missing rail block for developing countries.

The study in [3] propose a real-time solution for detecting missing rail block pertinent to the context of developing countries. However, here, no security issues are addressed. Therefore, in this work, we envision to propose a new security attack entitled as power attack exploiting the vulnerability of energy resources. Furthermore, we analyze possibility of other well-known attacks such as MITM attack and replay attack.

3.3 Different Security Attacks in Real-Time System for Detecting Missing rail blocks

In our proposed real-time system for detecting missing rail blocks, accurate reply messages containing monitoring reports are crucial for the trains. The reception of maliciously wrong report messages or the absence of report messages could lead to disasters such as derailment, infrastructure damage, and monetary loss. Furthermore, the real-time system uses batteries as energy sources of the sensors to maintain the low-cost property responsible for making the system suitable for developed countries. An adversary could able to exploit these vulnerabilities to launch attacks on the system. Therefore, in this work, we envision to explore a new attack entitled as power attack exploiting the vulnerability pertinent to energy sources. This attack leads to the disruption of reception of messages about the condition of the track ahead.

Consequently, we explore two popular attacks such as man-in-the-middle attack and replay attack as these attacks cause serious vandalism in comparison to other traditional attacks of wireless sensor networks such as eavesdropping, masquerade attack, and black hole attack.

3.3.1 Power Attack

In general, the term power attack is defined as simultaneous occurrences of power peaks that produce overloading of electrical circuits of a device and then trigger the trip of circuit breakers (CBs) of power facilities, leading to undesired power outages [134]. However, this definition is not directly applicable for the real-time system for detecting missing rail blocks. Hence, we need to redefine the term power attack for such system. Since the sensors on the rail track of the missing rail block detection system are powered by batteries, there are no circuit breakers that can be tripped off due to power overload. Therefore, to launch a power attack, an adversary node forces a sensor device to deplete energy more drastically, which eventually causes the sensor node to die off due to draining out of stored energy.

It is to be noted that the damages of power attack are twofold. First, the power attack forces the sensors to die off much early than usual lifetime leading to frequent change/maintenance of energy sources, which eventually causes monetary loss. Secondly, since the sensors on the rail track die off due to battery outage, the sensors will not respond to any query from the train or from other sensor nodes. This causes disruption of communication owing to the absence of report messages. Such absence of report messages leads to frequent slow-down of the train during trip causing delay of the train schedule.

Next, we endeavor to develop attack models to launch effective power attack.

3.3.2 Attack Models for Power Attack

In case of the real-time system for detecting missing rail blocks presented in Chapter 2, the sensors on the rail track consume energy during transmissions and receptions of packets while performing communication between the train and the sensor nodes. Hence, an adversary node forces sensors on the rail track to deplete more energy by accepting and responding to frequent incoming packets. Based on this idea, we develop two attack models of power attack specifically for the network architecture of real-time system for detecting missing rail blocks.

Fig. 3.1 delineates two attack models: 1) Static attack model and 2) Mobile attack model for power attack. Here, we assume that the adversary is a compromised sensor, which is able to perform communication similar to the train.

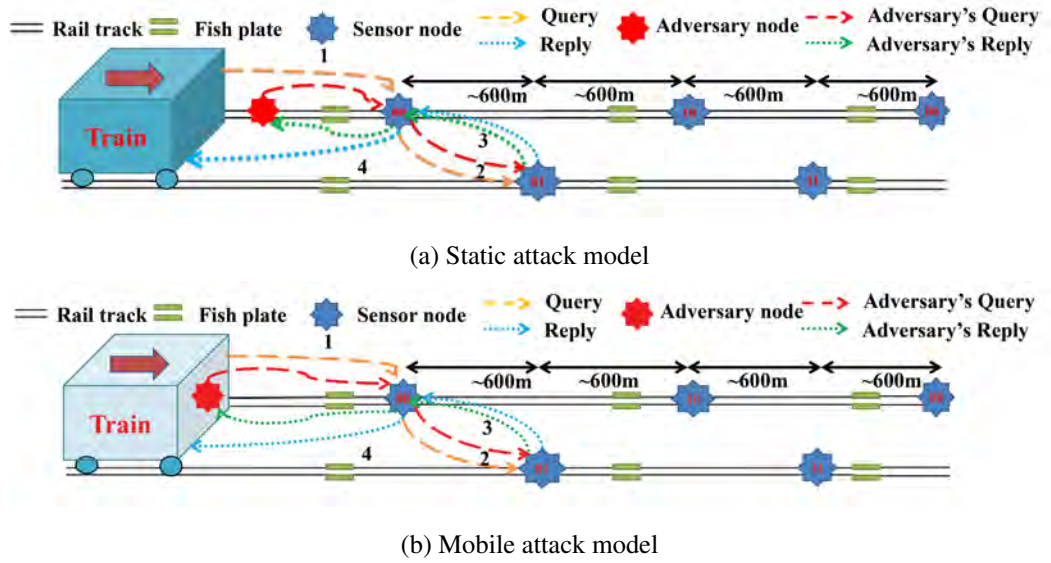


Figure 3.1: Attack models of power attack

In the static attack model, an adversary is placed on the rail track (Fig. 3.1a). The adversary launches the power attack by sending a query packet to sensor node addressed as 00. Since no authentication is performed in the real-time system for detecting missing rail blocks, the sensor node 00 fails to distinguish the query packet of the adversary from the query packet of the train. Hence, sensor node 00 performs communication similar to the train’s query (as described in Section) for adversary’s query packet. The adversary continues the attack by sending query packets at frequent intervals. It is evident from Fig. 3.1a that even though the adversary is static it eventually launches attacks on two sensor nodes (i.e., sensor node 00 and 01) at the same time.

Fig. 3.1b demonstrates the mobile attack model. In mobile attack model, the adversary is placed inside the train and it is moving along with the train. Similar to the static attack model, the adversary sends frequent query packets to the sensor nodes on the rail track. Then, the sensor nodes perform the entire communication for the adversary’s queries. Here, the adversary attacks all the sensor nodes on the rail track owing to mobility.

For our proposed power attack, an adversary needs to quantify the lifetime of the batteries of the sensor nodes under attack. Hence, to facilitate effective launching of the power attack the adversary requires to estimate the amount of energy consumed by the sensor nodes under attack. Therefore, we endeavor to devise a mathematical model to estimate the total energy consumption of the sensor devices under power attack.

3.3.3 Mathematical Model for Energy Consumption of Sensor Nodes

In this section, we focus on devising a mathematical model for the energy consumption of the sensor nodes under the power attack. Here, we first consider the static attack model delineated in Fig. 3.1a. We perform mathematical modeling of the energy consumption based on the number of transmitted and received packets.

First, we estimate the transmission energy consumption of the sensor node under attack denoted as 00 (Fig. 3.1a).

$$E_{tx_attack} = P_{tx} \times T_{tx_attack} \quad (3.1)$$

Here, P_{tx} is the transmission power of the sensor node 00 and T_{tx_attack} represents the total transmission time during power attack. Next, T_{tx_attack} is computed as follows:

$$T_{tx_attack} = \frac{L_p \times N_{tx_attack}}{BW} \quad (3.2)$$

Here, L_p denotes the number of bits in a packet and BW represents the bandwidth. N_{tx_attack} represents the total number of packets transmitted by the sensor node under attack by an adversary node (an). N_{tx_attack} is computed as follows:

$$N_{tx_attack} = F_{attack} \times T_{total_time} \times \text{Total number of transmitted packets per communication} \quad (3.3)$$

Here, F_{attack} and T_{total_time} denotes the frequency of attack and the total time respectively.

Fig. 3.2a exhibits the transmission of the packet between the adversary node and the sensor node under attack. The sensor node 00 under attack performs transmission in four cases:

- Case I: upon receiving an initial query message from the adversary node the sensor node 00 forwards the query to the very next sensor node 01. The transmitted packet is delineated as $Pkt_{query_forward_to_sn}$ in Fig. 3.2a.
- Case II: sensor node transmits an acknowledgment to the adversary node after receiving a query message from the adversary node ($Pkt_{ack_to_an}$).

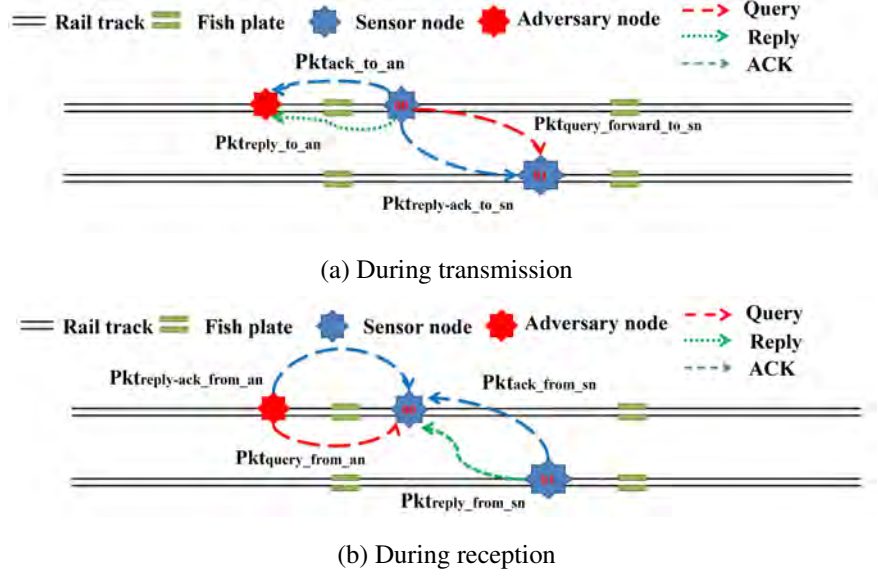


Figure 3.2: Transfer of the packets between an adversary node (an) and an sensor node (sn) under attack

- Case III: next, after receiving a reply message from the very next node comprising the monitoring report about the condition of the rail track ahead, the sensor node transmits the reply to the adversary node incorporating its own report ($Pkt_{reply_to_an}$).
- Case IV: finally, after receiving a reply from the very next sensor node 01, the sensor node 00 sends a reply-ack message to the very next sensor node ($Pkt_{reply-ack_to_sn}$).

Hence, the total number of transmitted packet is computed as follows:

Total number of transmitted packets per communication =

$$Pkt_{query_forward_to_sn} \times Th_Q + Pkt_{ack_to_an} \times Th_Q + Pkt_{reply_to_an} \times Th_R + Pkt_{reply-ack_to_sn} \times Th_{RA} \quad (3.4)$$

In Eq. 3.4, Th_Q , Th_R , and Th_{RA} are three types of threshold used for re-transmission of packets (as specified in Chapter 3.4.1).

Next, we compute the reception energy consumption of the sensor node under attack by the adversary node.

$$E_{rx_attack} = P_{rx} \times T_{rx_attack} \quad (3.5)$$

Here, P_{rx} is the reception power of a sensor node and T_{rx_attack} represents the total reception time during attack. Similar to Eq. 3.2, T_{rx_attack} is computed using the following equation:

$$T_{rx_attack} = \frac{L_p \times N_{rx_attack}}{BW} \quad (3.6)$$

Here, N_{rx_attack} represents total number of packets received by the sensor node under attack. We estimate the value of N_{rx_attack} as follows:

$$N_{rx_attack} = F_{attack} \times T_{total_time} \times \text{Total number of received packets per communication} \quad (3.7)$$

Fig. 3.2b demonstrates four different cases when packets are received by the sensor node 00 under the attack of adversary node.

- Case I: sensor node receives a query from the adversary node ($Pkt_{Query_from_an}$).
- Case II: sensor node receives an acknowledgment from the very next sensor node after forwarding the query message from the attacker node ($Pkt_{Ack_from_sn}$).
- Case III: sensor node receives a reply packet from the very next node containing information about the condition of the rail track ahead ($Pkt_{Reply_from_sn}$).
- Case IV: sensor node receives a reply-ack packet from the adversary node owing to the transmission of reply packet to adversary node ($Pkt_{reply-ack_from_an}$).

Hence, the total number of received packets is computed as follows:

Total number of received packets per communication =

$$Pkt_{query_from_an} \times Th_Q + Pkt_{ack_from_sn} \times Th_Q + Pkt_{reply_from_sn} \times Th_{RA} + Pkt_{reply-ack_from_an} \times Th_{RA} \quad (3.8)$$

Now, combining the above mentioned energy components, we deduce energy consumption by a sensor node under attack as follows:

$$E_{attack} = E_{tx_attack} + E_{rx_attack} \quad (3.9)$$

Furthermore, the sensor node under attack also performs normal communication with the train, hence, the total energy consumption by the sensor node is devised as follows:

$$E_{total} = E_{attack} + E_{tx} + E_{rx} + E_{sl} \quad (3.10)$$

Here, E_{tx} , E_{rx} , and E_{sl} represents the transmission, reception, and sleep energy consumption by a sensor node during communication with train. Similar to E_{tx_attack} and E_{rx_attack} , E_{tx} and E_{rx} are also calculated using equations specified above. However, E_{sl} is computed as follows:

$$E_{sl} = P_{sl} \times T_{sl} \quad (3.11)$$

Here, P_{sl} is the sleep power. Next, T_{sl} is devised as follows:

$$T_{sl} = T_{total_time} - T_{tx_attack} - T_{rx_attack} - T_{tx} - T_{rx} \quad (3.12)$$

After putting all the values in Eq. 3.10, we finally compute the total energy consumption of the sensor node under attack.

As mentioned earlier that the static attack model allows an adversary to launch power attack on two sensor node simultaneously (Fig. 3.1a). Hence, we also need to device mathematical model for energy consumption of the very next sensor node denoted as 01 as exhibited in Fig. 3.1a. We could devise a mathematical model for the total energy consumption of the very next sensor node leveraging the above-specified equations. Furthermore, our empirical evaluation (described in Section 3.5.1.3) reveals that the same mathematical model resembles the energy consumption of the sensor node under attack for mobile attack model.

Next, we explore another potential attack i.e., man-in-the-middle attack for the system for detecting missing rail blocks.

3.3.4 Man-in-the-middle (MITM) Attack

In the real-time system for detecting missing rail blocks, there are no cryptographic primitives used to defeat malicious adversaries. Therefore, the missing rail block detection system is prone to well-known man-in-the-middle (MITM) attack [135]. Fig. 3.8a demonstrates the attack of the real-time system for detecting missing rail blocks. During this attack, the adversary intercepts packets during communication between the train and the sensor nodes on the rail track. Next, the adversary customizes the contents of the packets and then re-sends the packets to the sensor node. Since the packets do not contain any information pertinent to

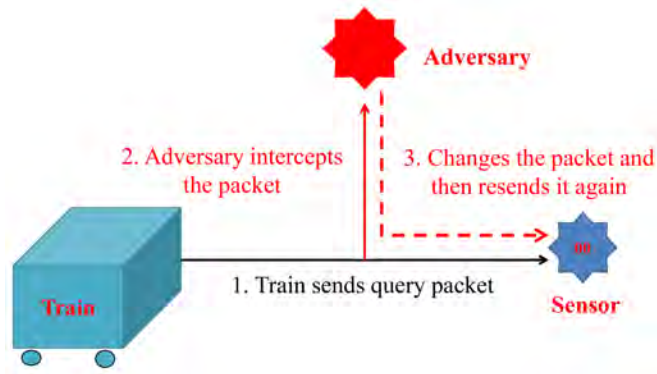


Figure 3.3: Man-in-the-middle (MITM) attack in real-time system for detecting missing rail blocks

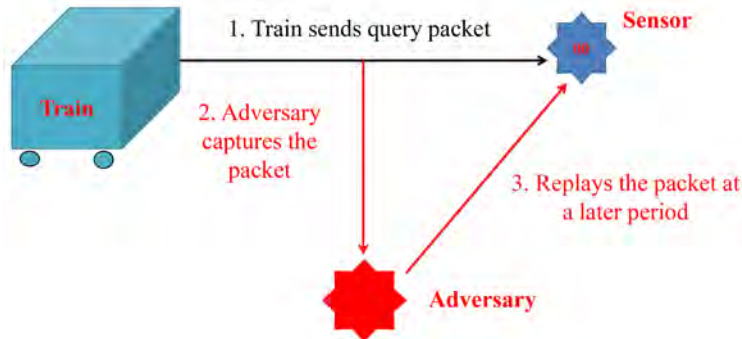


Figure 3.4: Replay attack in missing rail block detection system

the identification of the source, the sensor nodes on the rail track fail to distinguish between train's packets and adversary's packets.

It is to be noted that the adversary launching the MITM attack not only able to disrupt the communication between the train and the sensor nodes, but also able to cause accidents owing to derailment of trains. For instance, if the adversary changes the information of the destination ID block or packet type block in the packet, then such changes could cause disruption of the valid communication. Furthermore, if the adversary generates fake monitoring reports by changing the report block of the packet, then disasters such as derailments and infrastructure damage could happen.

Next, we explore another potential attack, i.e., replay attack for the real-time system for detecting missing rail blocks.

3.3.5 Replay Attack

In the real-time system, the absence of mechanism for detection of stale packets makes the system vulnerable to replay attack [135, 136]. During a replay attack the adversary captures packets from on-going communication, stores the packets, and then replays the packets at later period. Fig. 3.4 depicts the steps of replay attack by the adversary. If the adversary continues to replay query packets to the sensor node on the rail track at frequent intervals, then the sensor node will deplete energy more rapidly than usual. This will cause frequent changes or maintenance of the energy sources of the sensor devices.

So far we explore three different types of attacks possible in real-time system for detecting missing rail blocks. Next, we envision to develop efficient countermeasures to mitigate above-mentioned attacks.

3.4 Countermeasures

Our proposed real-time system for detecting missing rail blocks is developed focusing low-resource settings of the developed countries such as Kenya, India, Bangladesh, etc. Hence, upgrading the existing railway infrastructure to defend against the malicious adversary will increase costs. Therefore, we envision to design countermeasures against the security attacks of missing rail block detection system without any additional investment on hardware.

3.4.1 Mitigating Power Attack

The power attack presented in Section 3.3.1 exploits the vulnerability that the sensor nodes on the rail track are allowed to accept any packets at any time. Hence, during power attack the adversary forces the sensor to consume more energy by accepting and responding to the query packets send at frequent interval.

An instinctive countermeasure to this power attack is to allow the sensor nodes to be active for accepting packets from the train during a specific time interval and to force the sensor nodes to reject any incoming packets for another specific time interval before the arrival of the next train. Fig. 3.5 delineates the timing diagram of the sensor nodes on the rail track deployed for the above mentioned naive countermeasure.

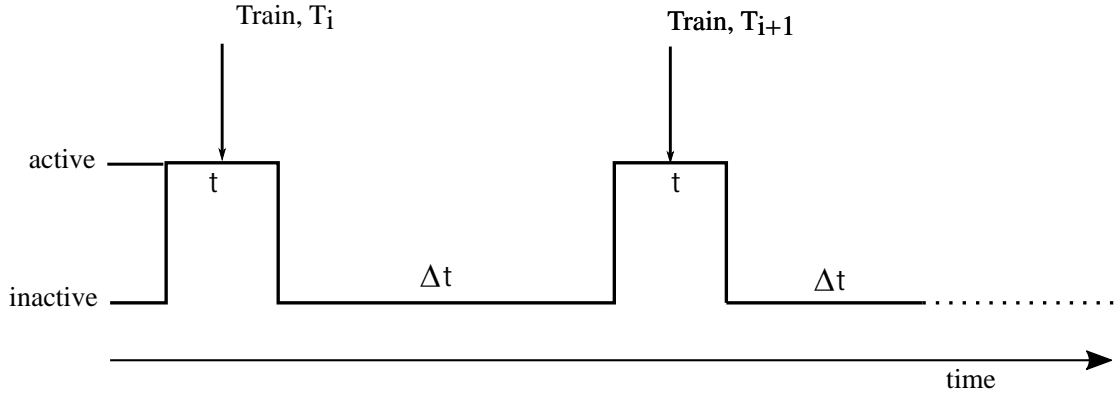


Figure 3.5: Timing diagram for sensors on the rail track

Here, the sensor node on the rail track remains active for t interval for train T_i and remains inactive for Δt interval before the arrival of the next train (T_{i+1}). At the end of Δt interval the sensor node becomes active again for the t period of time for train T_{i+1} . It is to be noted that the terms active and inactive denote acceptance and rejection of packets by the sensor node respectively. Next, we have to determine the values of t and Δt . We experimentally found that in the real-time system for detecting missing blocks, it requires around 2.3s to perform a complete communication as per our proposed communication paradigm in Chapter . Here, the sensors take around 2s to prepare the sensing results after receiving a query packet and about 50ms to perform channel switching operation. Therefore, the sensor on the rail track needs to be active for about 2.3s after receiving the query packet from the train. Hence, we set the value of t to be 2.5s including a safety margin of 200ms.

Next, we need to determine the value of Δt effectively. The reason behind is: if a sensor receives a valid query packet from the train during this Δt period then the sensor will discard the packet and the train will not have any information about the condition of the rail track ahead. Therefore, the sensor on the rail track needs to reject query packets until it receives a valid query packet from the next train on the schedule. Hence, Δt should be set by the interval of the arrival time of the next train. However, the system for detecting missing rail blocks presented in Chapter 2, the sensor node on the rail track does not have any measures to know the schedule of the next incoming train. Therefore, we include the schedule, i.e., the arrival interval of the next train to the query packet by extending the size of the query packet from 1 byte to 2 bytes. now, after receiving the query packet the sensor node on the rail track sets the value of Δt equal to the value of the interval specified in the query packet. For

example, let the next train of the schedule will start 10 minutes after the first train. The first train inserts the value of 10 minutes in the query packet and sends the query packet to the sensor node. Then, the sensor node becomes inactive for the next 10 minutes by setting the value $\Delta t = 10$ minutes. Next, the sensor node becomes active once again after 10 minutes and remains active for $t = 2.5s$ for the next train. It is to be noted that the sensor node on the track will update the value of Δt based on the query packet only if the query packet is received from the train. As according to the communication paradigm of the real-time missing rail block detection system when the sensor node receives a query packet from the train and it forwards the query packet to the very next sensor node (Fig. 2.5a). However, now the very next sensor node will not update the value of its Δt as the query packet is received from the sensor node.

However, developing countries such as India, Bangladesh, Kenya, etc., experience frequent late arrivals of the trains beyond schedule owing to diversified reasons [137–139]. Hence, we introduce a safety margin, δ with Δt to address the delay of the train schedule. Now, the sensor node will remain active to accept query packets of the next train from $(\Delta t - \delta)$ to $(t + \Delta t + \delta)$.

Moreover, if the schedule of the arrival of a train is cancelled, then the sensor nodes on the rail track will fail to update the value of Δt for the next train. Hence, indefinite rejection of query packets of subsequent trains will take place. Furthermore, since the transmitted packets are in plaintext, a malicious adversary is able to change the contents of the packet. Hence, if the adversary changes the interval of arrival of the next train that is incorporated in the query packet and forces the sensor node on the track to reject packets during the arrival of the next train. Thus, a door opens for another threat, i.e., man-in-the-middle (MITM) attack. Besides, if the adversary captures a query packet from an on-going communication and then replays the packet at later time. It causes the sensor to be inactive during that time leading to the replay attack. Therefore, next, we need to find countermeasures for the MITM and the replay attack.

3.4.2 Preventing Man-in-the-middle (MITM) Attack

MITM attack exploits the vulnerability that the packets in real-time missing rail block detection system are transmitted in plaintext. Hence, if the packets are protected with encryption (i.e., one-time pad (OTP)), then this attack will be defeated. Here, a crypto-key is shared between the train and the sensor node on the rail track. The train has different shared crypto-key for different sensors on the rail track. This shared crypto-key is stored into the sensors on the rail track during installation of the system and a list of shared key for each sensor is stored in the memory of the sensor node in the train. The size of the shared key is the same size as the packet. Now, when a train sends a query packet to a sensor node on the rail track, it performs XOR operation of each bit of the packet with the corresponding bit in the shared crypto-key stored specifically for that sensor node. Owing to the feature of OTP the resulting ciphertext is impossible to decrypt or break [140, 141]. Upon receiving the encrypted query packet the sensor node the rail track performs a similar XOR operation using its stored shared key to decrypt the packet.

However, rarely seldom the shared crypto-key can be compromised. Then, we will need to reset the shared keys. To do so, a special control packet is used. To separate the control packets from the normal packets, the reserved bits of the packet (as specified in Chapter 3.4.1) are used. Although the packets of missing rail block detection system are encrypted to prevent an adversary from changing the contents, the adversary can still capture the packets and replay the packets. Therefore, next, we endeavor to find a countermeasure for the replay attack.

3.4.3 Defeating Replay Attack

In the replay attack, the adversary replays old packets. Therefore, to defeat the replay attack, we need to ensure the freshness of the packets. In general, addition of nonce (random number) or timestamps information to the packets ensures the freshness of the packets [142, 143]. These approaches are not directly applicable to defeat the replay attack of the real-time system for detecting missing rail block.

Usage of the timestamps technique requires synchronization among different clocks of different sensors via a secure protocol. However, constraints of wireless sensor networks

make it infeasible to use traditional synchronization techniques to these networks [144, 145]. Hence, new synchronization protocols are introduced in the literature specifically for wireless sensor networks [146]. However, deployment of these protocols will strip the lightweight feature of the real-time missing rail block detection system. Moreover, these synchronization techniques require message passing among sensor nodes, which procrastinates the reception of report messages. Such delay leaves less time to stop the train within the safety margin in case of the occurrences of missing rail blocks on the track.

Next, nonces (i.e., randomly generated numbers) are also used to ensure freshness of data to resolve the replay attack. Such values should only be used a single time for each transmission of packets. Hence, the size of a nonce needs to be large enough to avoid reuse [147]. Therefore, the incorporation of nonces in real-time system for detecting missing rail blocks will increase the size of the packets. Furthermore, the sensors on the rail track have to store all the used nonces to avoid exploitation of expired nonces by the adversary to mitigate the replay attack. However, owing to limited storage capabilities of sensor nodes on the rail track (EPROM of the microcontroller only has 1024bytes [148]) the sensor nodes will fail to store all the nonces used by all the trains travelling on that track. Hence, if the adversary captures a packet and replays the packet at later time (i.e., after 2 or more days), then the sensor nodes on the rail track will fail to detect the stale packets even after using nonces. Therefore, nonces can not be used to defeat replay attack in the real-time system for detecting missing rail block. Hence, we need to focus on developing a new countermeasure to defeat the replay attack.

Now, as a new countermeasure, instead to transmitting the arrival time of the next train in the query packet (as described in Section 3.3.1) we incorporate the train id and the trip number for the corresponding train. As same train makes several trips the train id would remain same for all the trips and the trip number would change for each trip. The incorporation of train id authenticates the packets from the trains. We increase the packet size to 3 bytes to incorporate 1 byte for train id and 1 byte for trip number. 1 byte for train id and 1 for byte trip number will be enough to resemble all the trips made by the trains for a specific track of the developing countries [149].

According to this new countermeasure, when a train sends a query packet to the sensor

node on the rail track it incorporates the corresponding train id and the trip number within the query packet. Upon reception of the query packet, the sensor node on the rail track searches its memory for the corresponding train id. If the train id is found then the sensor node checks whether the received trip number is equal to the stored trip number for the corresponding train id. If the received trip number is equal to the stored trip number then the sensor node accepts the packet and updates the stored trip number. Otherwise, the sensor node discards the received packet. If the train id is not stored into the memory of the sensor node on the rail track, then the sensor node stores the received train id along with the trip number. Fig. 3.6 represents the working principle of the above-mentioned countermeasure that is deployed into the sensor node on the rail track.

In this countermeasure, as both the train id and trip number are stored in the memory, the sensor node easily detects a stale packet which is sent by the adversary (as the trip number of the replayed packet would be smaller than the stored trip number). It is to be noted that the train ids and the trip numbers of the trains that use the same rail track can easily be stored into the memory of the sensor node on the rail track as not all the available trains travel using the same track. Consequently, since the packets are encrypted using a shared crypto-key, the man-in-the-middle attack is also defeated. Furthermore, this countermeasure resolves the power attack as now the sensor node on the rail track does not accept any frequent query packets from the adversary.

However, in developing countries, cancellation of schedule of trains owing to different reasons is a common phenomenon [150–152]. The occurrence of such cancellation of schedule of trains leads to indefinite denial of query packets of subsequent trains. Therefore, to handle the schedule missing problem we modify the above-mentioned countermeasure by introducing a safety margin Δ . Now, upon receiving a query packet from the train, the sensor node on the track accepts the packets for a specific train only if the corresponding received trip number satisfies the following condition:

$$\text{stored_trip_number} \leq \text{received_trip_number} \leq \text{stored_trip_number} + \Delta \quad (3.13)$$

According to this modification, the sensor node on the track accepts trip numbers within a range instead of a fixed value. Similarly, a centralized system generates the next trip number

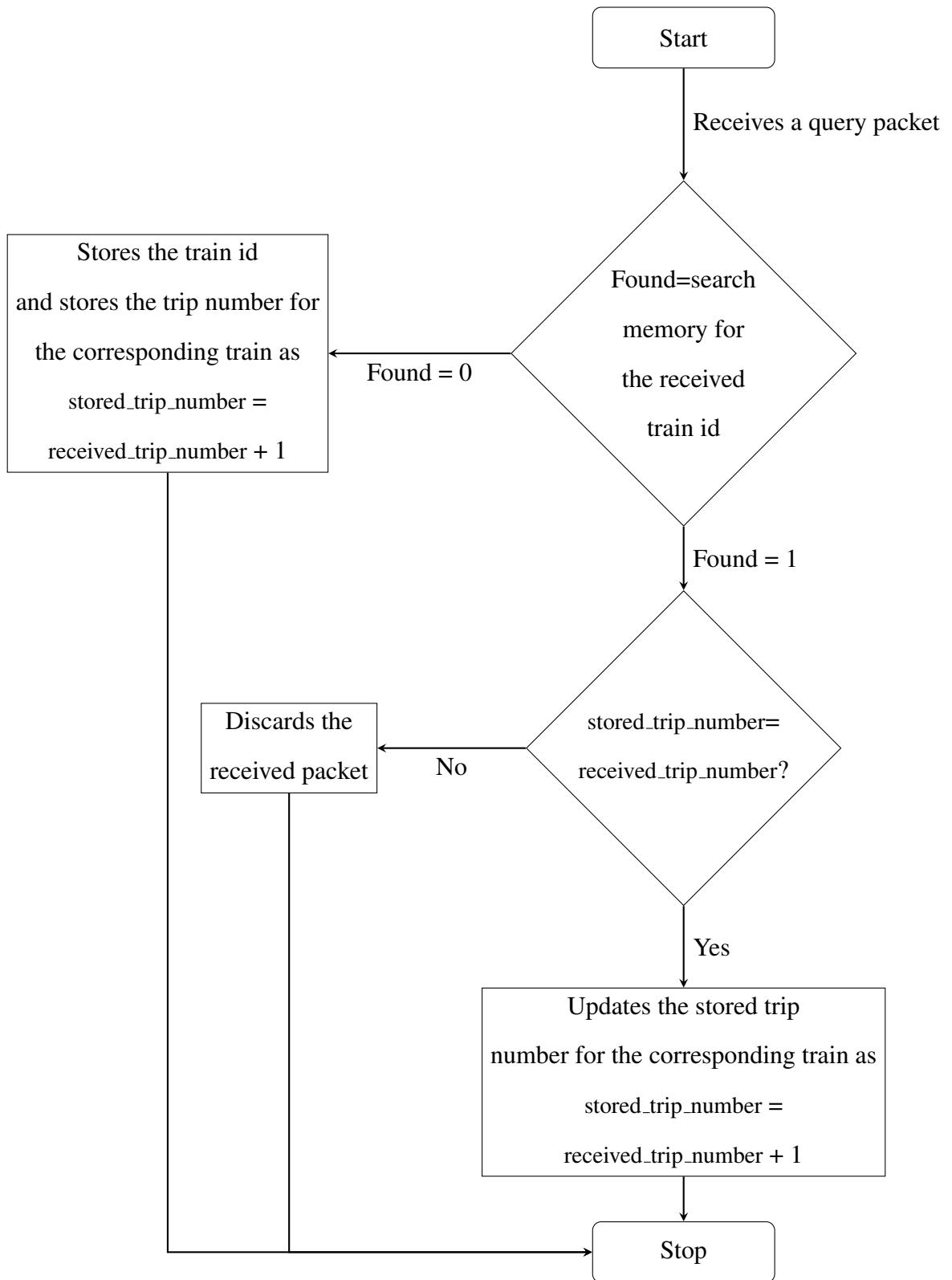


Figure 3.6: Working principle of the countermeasure deployed into the sensor node on the rail track

for the train from a similar range after the disruption of schedule of the previous trip of that train.

It is evident from the above discussion that the proposed countermeasure resolves power attack, man-in-the-middle attack, and replay attack.

Consequently, it is also evident from the above discussion that these attacks i.e., power attack, man-in-the-middle attack, and replay attack are related to each others. To capture the interaction among different attacks carried out on the real-time system for detecting missing rail blocks and the defenses that could be put in place to fend off the attacks, we use attack-defense tree [153, 154]. Here, we extend the notion of attack-defense tree by incorporation of a node to denote practical vulnerabilities. Fig. 3.7 delineates the attack-defense-practical vulnerabilities tree for real-time system for detecting missing rail blocks.

Next, we endeavor to represents simulation results to exhibit the effectiveness of the attacks and the performance analysis of the proposed countermeasures.

3.5 Experimental Evaluation of Power Attack

In this section, we envision to perform robust simulations for the exposed security attacks and countermeasures. However, since the simulation of the man-in-the-middle (MITM) attack and the replay attack is trivial, we will eschew it. Hence, we focus our attention only on the power attack. We perform rigorous simulations of the power attack using both `ns-2` simulation and real deployment on rail lines. In this section, first, we elaborate results from `ns-2` simulation, next, we delineate findings from our real deployment.

3.5.1 ns-2 Simulation

Here, we first delineate simulation settings for the simulation of the power attack using our proposed attack models. Next, we exhibit the impact of power attack on the real-time system for detecting missing rail blocks. Then, we verify the mathematical modelling of the power attack. Finally, we demonstrate the performance of our proposed countermeasures of he power attack.

In order to launch the power attack on the real-time system for detecting missing rail

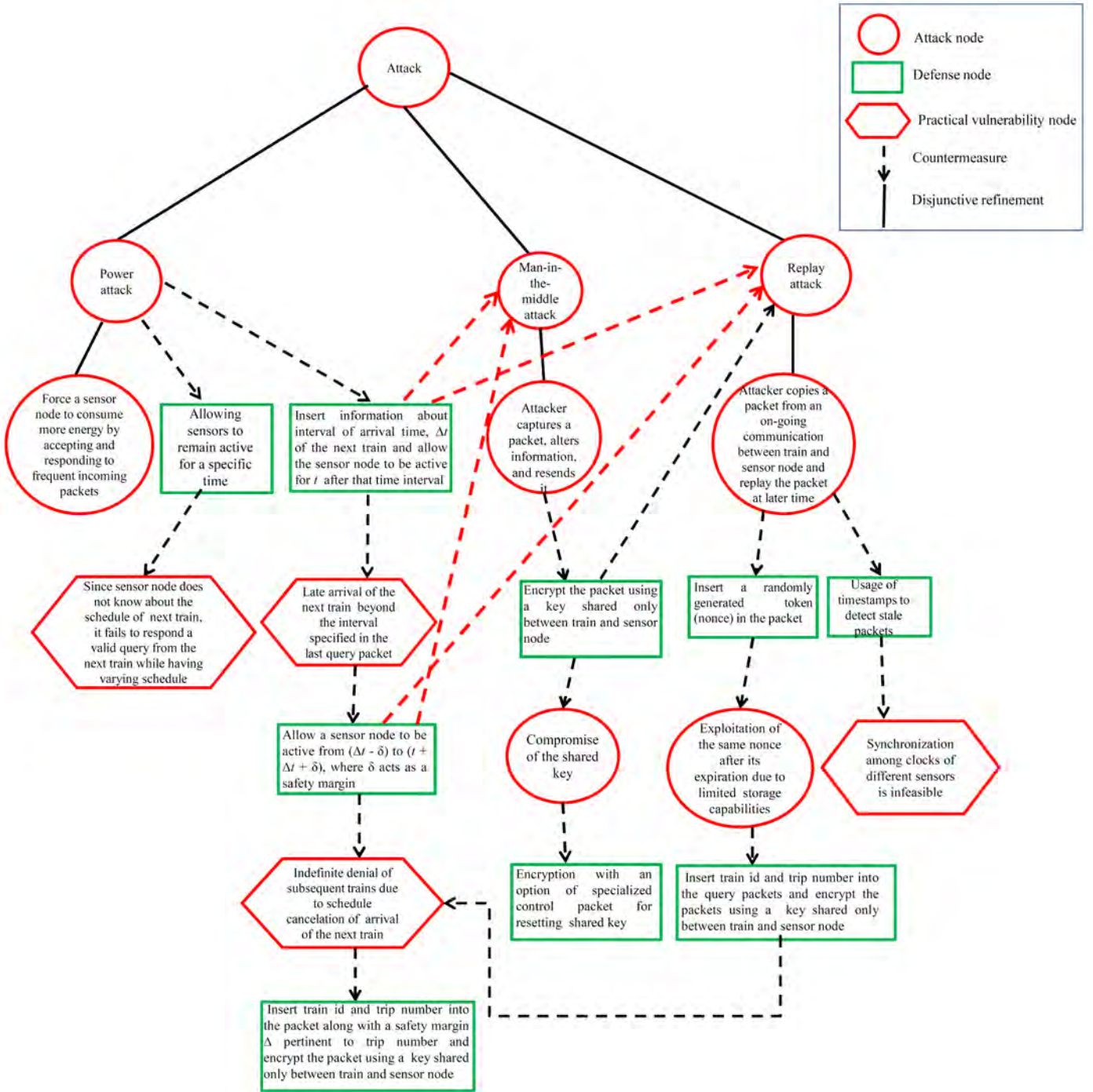


Figure 3.7: Attack-defense-practical vulnerabilities tree for real-time missing rail block detection system

blocks, at first, we integrate the cross-layer protocol of the system (described in Section 3.4.1) in $ns-2$. In order to do so, we need to make certain changes in the existing protocol stack of $ns-2$. At the Application layer, we model the customized packet format of the missing rail blocks detection system. Then, at the Transport layer, we deploy the data trans-

Parameter	Value	Parameter	Value
Transmission range (m)	600	Tx power (W)	0.1
Frequency (MHz)	433	Rx power (W)	0.065
Bandwidth (Kbps)	5	Train speed (km/hr)	80
Packet size (byte)	1	Simulation time (s)	50

Table 3.1: Simulation parameters

mission protocol as specified in Section 3.4.1. Besides, an indicator flag is introduced to store the decision pertinent to channel switching and is shared with MAC layer to resemble the cross-layer design. For the Network layer, we emulate the notion of static routing using the existing packet forwarding module of AODV in *ns-2* eliminating its route request and route reply mechanisms. Finally, for MAC layer, we deploy a lightweight MAC protocol by omitting the RTS and CTS packets. The customized MAC layer protocol takes its decision of channel switching based on the indicator flag that is shared by the Transport layer and passes the decision to the Physical layer.

3.5.1.1 Simulation settings

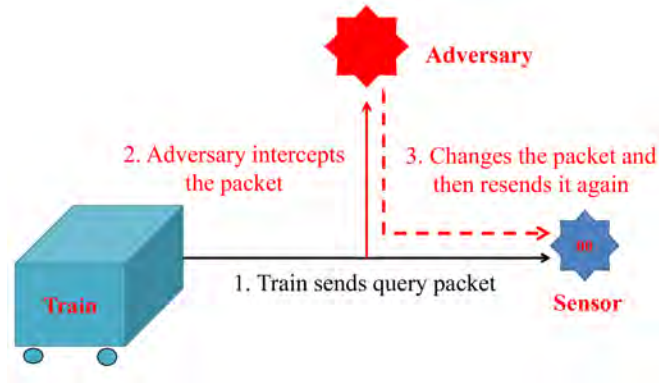
To deploy the power attack, we construct a linear scenario based on Fig. 3.1 comprising four nodes. Here, we have one mobile node to represent the train, two static nodes to resemble the sensors on the rail track. We have one node to represent the adversary. The adversary node is static for the static attack model (Fig. 3.1a) and mobile during the mobile attack model (Fig. 3.1b). In general, the passenger trains of the developing country under consideration travel at a average speed varying from $\sim 40\text{kmph}$ to $\sim 60\text{kmph}$. However, the maximum attainable speed of the train is $\sim 80\text{kmph}$. Hence, for our simulation, we set the speed of the mobile node resembling the train to 80kmph . Since to exhibit the power attack, we need to demonstrate the rise of energy consumption, hence, we exploit the built-in power models of *ns-2* to calculate the total energy consumption in our simulation. For the calculation of energy consumption, we utilize the measurements provided in [112, 155] to resemble the adopted HC-12 module. Furthermore, we compute the average of 20 simulation runs each having a duration of 50s. Table 3.1 presents the values and measurements used in our simulation for the power attack. Next, we demonstrate the impact of the power attack on the

real-time system for detecting missing rail blocks.

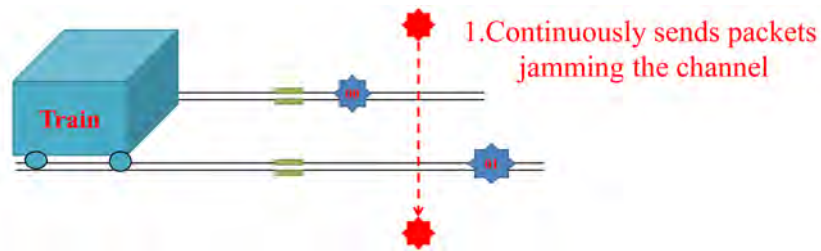
3.5.1.2 Impacts of power attack

The aim of the adversary launching the power attack is to force the sensors under attack to consume more energy by accepting query packets more frequently. Hence, to illustrate the impact of power attack, we use the total energy consumption as the performance metric. Furthermore, to justify the change in total energy consumption during the power attack, we analyze three components of the energy consumption, i.e., transmission, reception, and sleep energy consumption. Furthermore, according to the attack model of the power attack presented in Fig. 3.1, the adversary affects two sensor nodes at a time. Therefore, we demonstrate the energy consumption for the sensor node under attack (sensor node 00 of Fig. 3.1) as well as the energy consumption of the very next sensor node under attack (sensor node 01 of Fig. 3.1). Fig. 3.9 exhibits the impact of the power attack. Here, the adversary sends the query message to the sensor node under attack at 4s interval for about 50s. The sensor node under attack performs a full communication for each query packets. hence, both the transmission and the reception energy increase for the sensor node under attack and the very next sensor node under attack in comparison to the scenario without the attack (Fig. 3.9b and Fig. 3.9c respectively). However, the sensor nodes under attack remain more active, hence, the sleep energy consumption decreases in comparison to without attack (Fig. 3.9d). Thus, our simulation establishes a successful launch of the attack.

Consequently, to evaluate efficacy of our proposed power attack, we perform comparison with two other popular attacks such as man-in-the-middle (MITM) attack and jamming attack. Fig. 3.8 depicts conceptual scenarios showing how we enable these attacks in our simulation using $ns-2$. Fig. 3.8a demonstrates the attack model for man-in-the-middle attack. Here, the attacker node intercepts a packet and resend the packet to the designated destination changing the content of the packet. However, $ns-2$ does not has any provision to change the payload of a packet during an ongoing communication. Therefore, in our simulation, we do not change the content of the packet while emulating the man-in-the-middle attack. To simulate the jamming attack in $ns-2$, we place two sensor nodes orthogonal to the rail track as depicted in Fig. 3.8b. These sensor nodes act as jammers by sending contin-

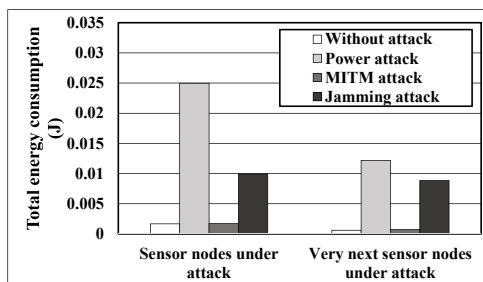


(a) Man-in-the-middle (MITM) attack

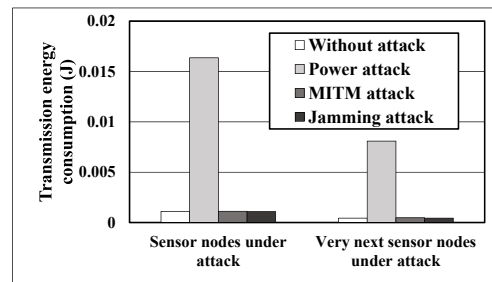


(b) Jamming attack

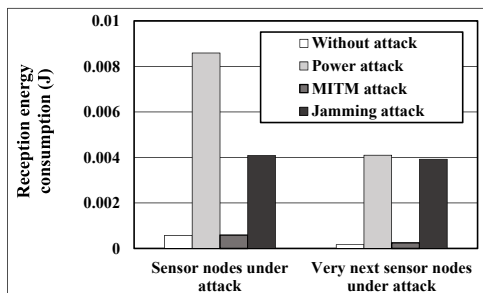
Figure 3.8: Attack scenarios of MITM attack and jamming attack



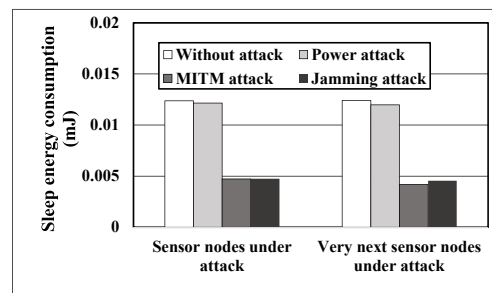
(a) Total energy consumption



(b) Transmission energy consumption



(c) Reception energy consumption



(d) Sleep energy consumption

Figure 3.9: Impacts of different attacks on the energy consumption of sensor devices

uous packets, which interferes with legitimate wireless communication. Fig. 3.9 illustrates different components of energy consumption for man-in-the-middle attack and jamming at-

Attacks	Response time (s)
Man-in-the-middle attack	3.90
Jamming attack	3.92
Power attack	4.37

Table 3.2: Response time for different types of security attacks

tack in comparison to the power attack. Fig. 3.9b, Fig. 3.9c, Fig. 3.9d, and Fig. 3.9a exhibit that transmission, reception, sleep, and total energy consumption during the power attack is higher in comparison to that of the other security attacks, i.e., jamming attack and MITM attack for both the sensor nodes on the rail track.

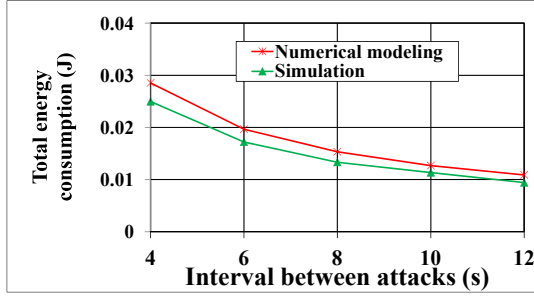
Besides the evaluation of power consumption for different types of attack, we also explore the response time of the query packet that is sent by the train for different attacks. Here, response time indicates the time that is needed to perform a full communication, i.e., from the transmission of the query packet to the reception of the report packets by the train. Table 3.2 delineates the response time different types of attacks. Here, our evaluation reveals that the response time of power attack is greater than the jamming attack and MITM attack.

After the successful launch of the power attack, next, we need to verify our proposed mathematical models for the energy consumption.

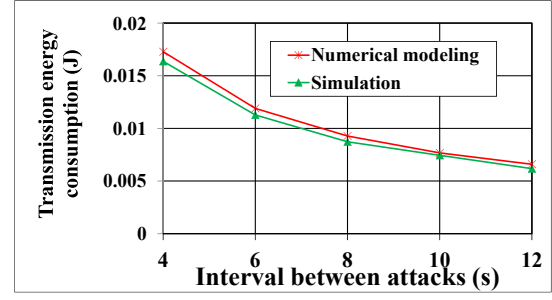
3.5.1.3 Verification of mathematical modelling of power attack

In this section, we envision to verify our proposed mathematical model for the energy consumption of the sensor node under power attack by comparing it with the results obtained from $ns-2$ simulation. We verify the accuracy of our proposed model from two perspectives: 1) with the varying interval between attacks and 2) with the varying attack time. First, we represent the accuracy of our proposed mathematical model of energy consumption for static attack model.

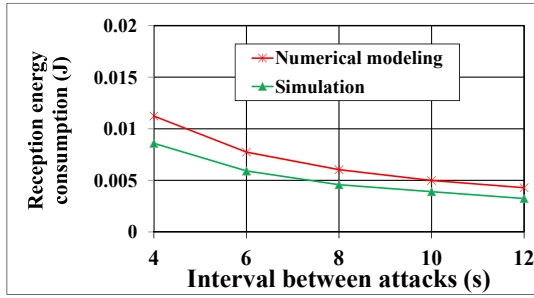
Varying interval between attacks for static attack model: Fig. 3.10 depicts the impact of variation of the interval between attacks for our proposed numerical modeling and for $ns-2$ simulation during power attack. Here, the adversary performs attack at the interval from 4s to 12 for 50s. The Fig. 3.10a reveals that with an increase of the interval between attacks the total energy consumption exhibit a decreasing pattern. We analyze the decrease of the energy consumption by focusing on three components of energy consumption. With



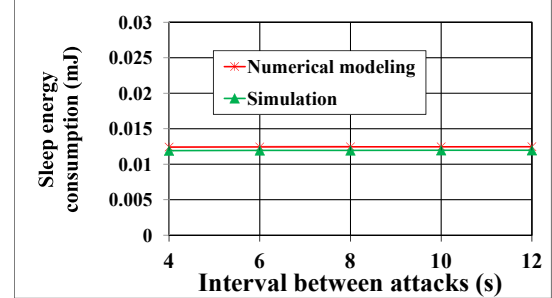
(a) Total energy consumption



(b) Transmission energy consumption



(c) Reception energy consumption

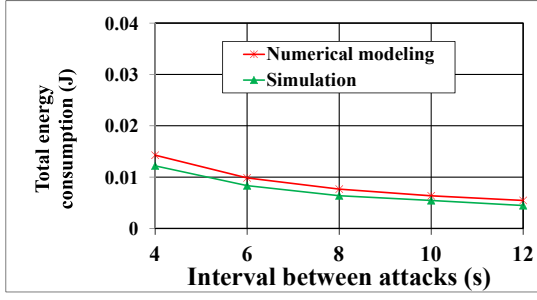


(d) Sleep energy consumption

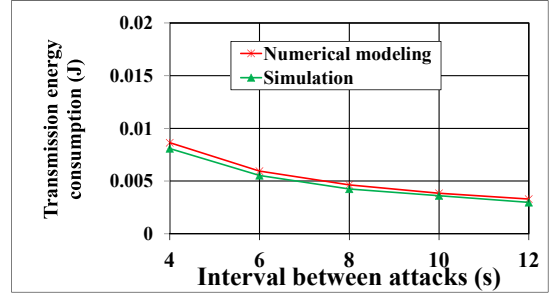
Figure 3.10: Impact of varying interval between attacks on the energy consumption by the sensor node under attack for static attack model

an increase in the interval between attacks the occurrences of attack decreases for a fixed amount of time. Hence, the number of transmitted and received packets decrease leading to decrease to the transmission and reception energy (Fig. 3.10b and Fig. 3.10c). On the contrary, the sleep energy increases (Fig. 3.10d). However, as the sleep power is very low, an increase in the sleep energy consumption does not have a significant impact on the total energy consumption. Furthermore, Fig. 3.10 clearly reveals that our proposed numerical model closely estimates the total energy consumption along with its three components of the sensor node under attack for static attack model. Our mathematical model estimates the total energy consumption, transmission, reception and sleep energy consumption of the sensor node under attack with about $\sim 88\%$, $\sim 94\%$, $\sim 81\%$, and $\sim 95\%$ accuracy respectively.

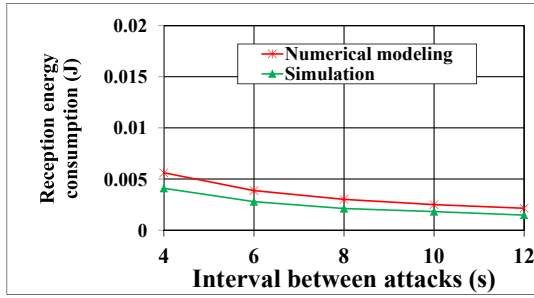
Consequently, Fig. 3.11 exhibits similar patterns for different energy consumption for the very next sensor node under attack. Furthermore, Fig. 3.11a, Fig. 3.11b, Fig. 3.11c, and Fig. 3.11d exhibit the efficacy of our proposed mathematical model for the very next sensor node under attack. Our model estimates the total energy consumption, transmission, reception



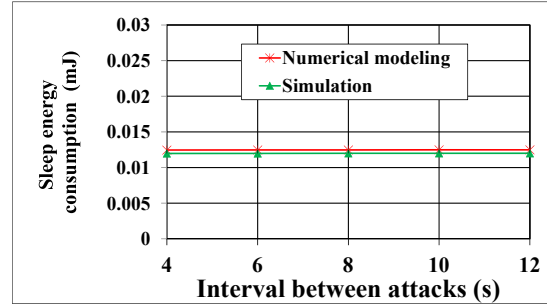
(a) Total energy consumption



(b) Transmission energy consumption



(c) Reception energy consumption



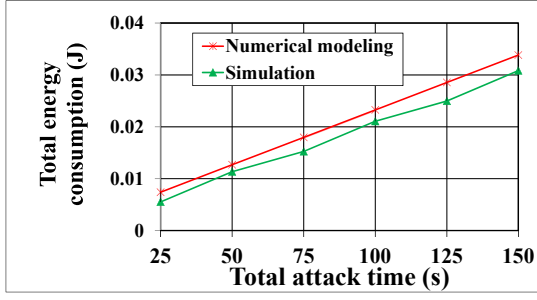
(d) Sleep energy consumption

Figure 3.11: Impact of varying interval between attacks on the energy consumption by the very next sensor node under attack for static attack model

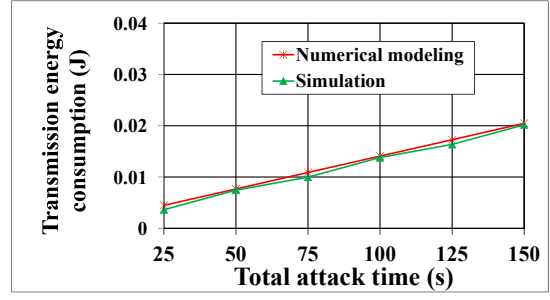
and sleep energy consumption of the very next sensor node under attack with about $\sim 85\%$, $\sim 91\%$, $\sim 80\%$, and $\sim 95\%$ accuracy respectively. Next, focus on our second perspective i.e., total attack time.

Impacts of varying total attack time for static attack model: Fig. 3.12 delineates the impacts of total attack time on the sensor node under attack. Here, we vary the total attack time from 25s to 150s and the interval between attacks is 10s. Fig. 3.12a depicts an increasing trend for total energy consumption of the sensor node under attack with an increase in the total attack time. The number of occurrences of attack increases with an increase in the total attack time. Hence, the transmission and reception energy consumption increase (Fig. 3.12b and Fig. 3.12c). Consequently, as the overall sleep time increases with an increase of total attack time, the sleep energy consumption also increases (Fig. 3.12d). The efficacy of our proposed numerical model also holds for the variation of total attack time. The very next sensor node under attack also exhibits similar outcomes (Fig. 3.13).

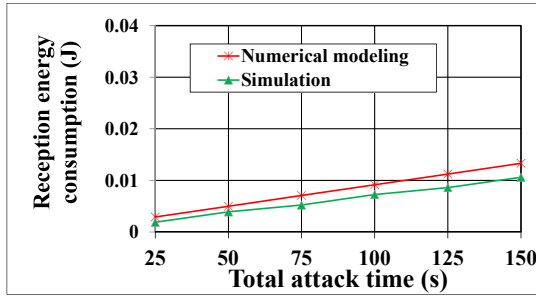
Next, we endeavor to investigate the applicability of our proposed mathematical model



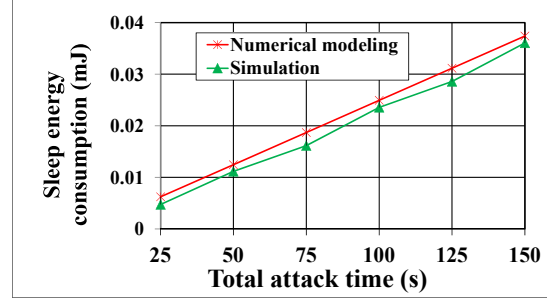
(a) Total energy consumption



(b) Transmission energy consumption



(c) Reception energy consumption



(d) Sleep energy consumption

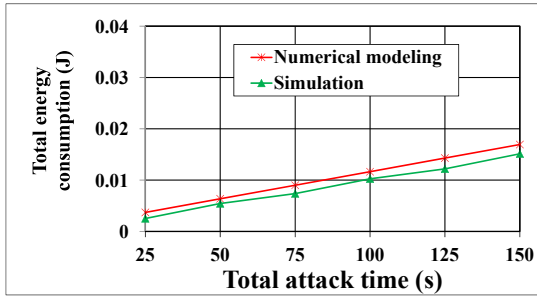
Figure 3.12: Impact of varying total attack time on the energy consumption by the sensor node under attack for static attack model

for mobile attack model. To do so, we first explore possible changes in the total energy consumption along with its three components owing to any change in the speed of the train.

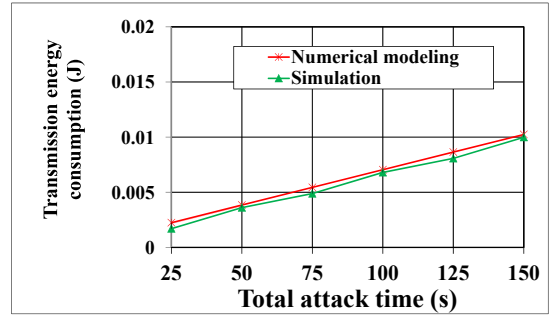
Impacts of varying speed of the train:

Fig. 3.14 and Fig. 3.15 represents the impact of varying speed of the train on the energy consumption for the sensor nodes under attack using different attack interval between attacks by the adversary.

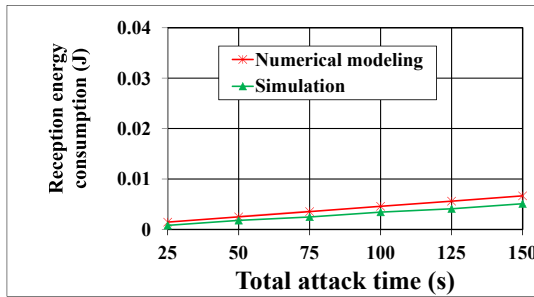
Here, we vary the speed of the train from 10kmph to 80kmph. Fig. 3.14a depicts that the total energy consumption for the sensor node under attack does not exhibit any significant change with an increase in the speed of the train. The different components of energy consumption also reveal similar results (Fig. 3.14b, Fig. 3.14c, and Fig. 3.14d). Similar outcomes are also exhibited for the very next sensor node under attack in Fig. 3.15a. The reason behind: the size of the transmitted packets in the real-time system for detecting missing rail blocks is very small, i.e., only one byte and instead of a stream of packets only one packet is transmitted for each transmission, hence, any change in the speed does not have



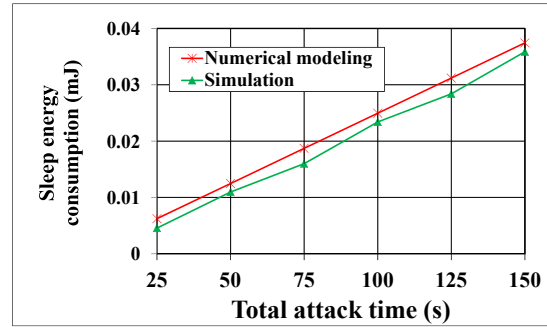
(a) Total energy consumption



(b) Transmission energy consumption



(c) Reception energy consumption



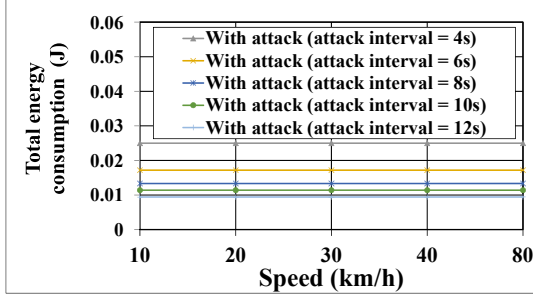
(d) Sleep energy consumption

Figure 3.13: Impact of varying total attack time on the energy consumption by the very next sensor node under attack for static attack model

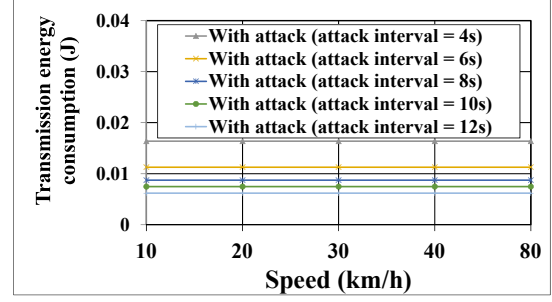
any significant impact on the energy consumption. Therefore, it is evident that our proposed mathematical model for the energy consumption of the sensor nodes under attack is also applicable for the mobile attack model.

Next, to verify the accuracy of our proposed mathematical model for the mobile attack model, we perform simulations varying the interval between attacks and varying the total attack time for both sensor nodes under attack. Fig. 3.16 and Fig. 3.18 demonstrate the results of these two variations for the sensor node under attack. The results of these variations also exhibit similar outcomes as to the results for the static model. Furthermore, Fig. 3.16 and Fig. 3.18 delineate efficacy of our proposed model for the energy consumption of the sensor node under attack for the mobile attack model. Besides, the very next sensor node under attack also exhibit similar outcomes for varying the interval between attacks (presented in Fig. 3.17) and varying the total attack time (presented in Fig. 3.19).

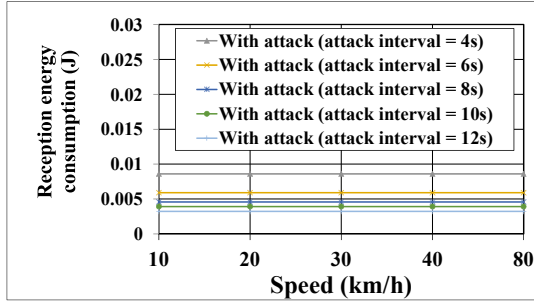
Next, we evaluate the performance of countermeasures.



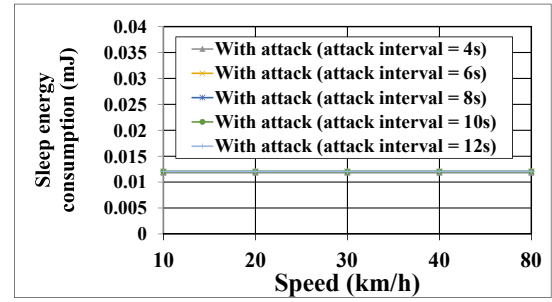
(a) Total energy consumption



(b) Transmission energy consumption



(c) Reception energy consumption

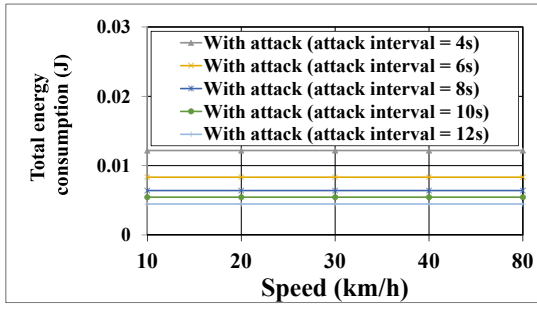


(d) Sleep energy consumption

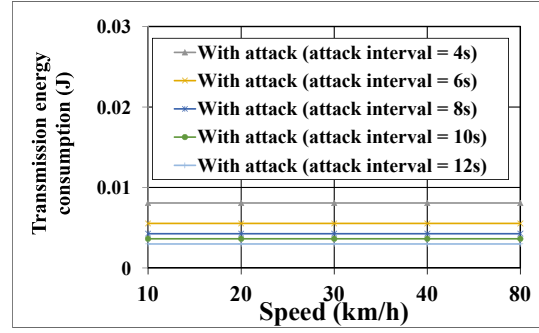
Figure 3.14: Impact of varying speed of the train on the energy consumption by the sensor node under attack for mobile attack model

3.5.1.4 Performance evaluation of countermeasures

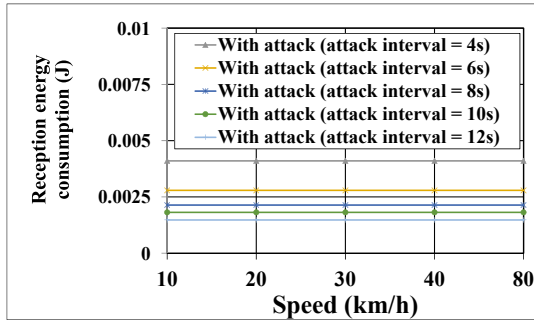
In this paper, we present two countermeasures to mitigate power attack. The first countermeasure utilizes the interval of the arrival of the next train, Δt along with a safety margin δ (described in Section 3.4.1). Next, the second countermeasure utilizes train id and trip number (Section 3.4.3). We mark the former countermeasure as **countermeasure 1** and the later countermeasure as **countermeasure 2** during the performance evaluation of the countermeasures. Simulations of both countermeasures for MITM attack and replay attack are trivial, hence, we focus on evaluating the performance of the countermeasures on the power attack. We evaluate the performance of our proposed countermeasures from two perspectives: 1) varying the interval between attacks and 2) varying the total attack time. It is to be noted, the mobility of the adversary does not have any significant impact on the energy consumption of the sensor node under attack, hence, the proposed countermeasures work effectively for both static and mobile attack model. We first represent the outcomes of variation of the interval between attacks.



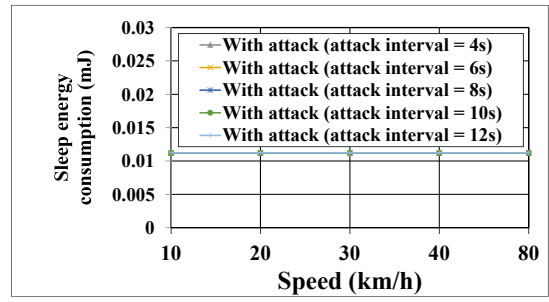
(a) Total energy consumption



(b) Transmission energy consumption



(c) Reception energy consumption



(d) Sleep energy consumption

Figure 3.15: Impact of varying speed of the train on the energy consumption by the very next sensor node under attack for mobile attack model

Fig. 3.20 depicts the performance of our proposed countermeasures in comparison to that power attack for varying interval between attacks for the sensor node under attack. Here, the attacks are performed by the adversary at different intervals (i.e., 4s, 6s, 8s, 10s, and 12s) for 50s. Fig. 3.20a, Fig. 3.20b, and Fig. 3.20c demonstrate reduction of energy consumption for total, transmission and reception energy consumption respectively for both countermeasures. However, both the countermeasures increase the energy consumption of the sleep energy as owing to incorporation of the countermeasures the sensors under attack are performing less number of communication in comparison to that the number of communication performed during the power attack. These outcomes exhibit mitigation of power attack. Furthermore, the simulation reveals that countermeasure 2 outperforms countermeasure 1. The safety margin δ of countermeasure 1 (introduces to handle delays of regular schedule of train) allows the sensor node to be active for interval longer than that the time is required to satisfy a query from the train. Hence, the sensor becomes vulnerable for the adversary to perform power attack during that period. Consequently, if the value of δ increases the vulnerability of the

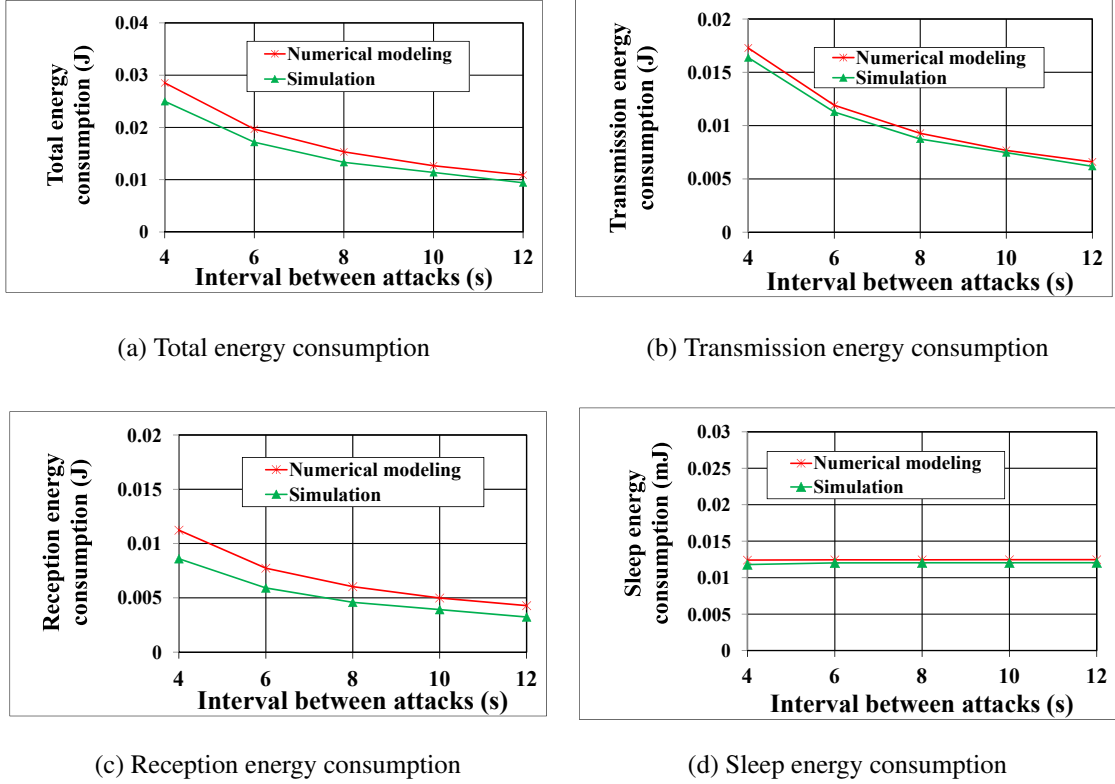


Figure 3.16: Impact of varying interval between attacks on the energy consumption by the sensor node under attack for mobile attack model

sensor also increases, which eventually will increase the energy consumption (owing to this straight forward relation between the value of δ and energy consumption we omit the graphs exhibiting variation of δ). For performance evaluation of our proposed countermeasures, we consider, $\delta = 4s$. However, for countermeasure 2, no such vulnerability is created. Therefore, countermeasure 2 performs better in comparison to countermeasure 1. Consequently, Fig. 3.21 depicts similar outcomes for the very next sensor node under attack.

Fig. 3.22 demonstrates performance evaluation of countermeasures for varying the total attack time for the sensor node under attack. Here, the total attack time is varied from 25s to 150s with a granularity of 25s. Similar to previous results, countermeasure 2 outperforms countermeasure 1 for varying the total attack time. We demonstrate results of the sensor node under attack for both countermeasure. The proposed countermeasures also exhibit similar performance for the very next sensor node under power attack (Fig. 3.23).

Next, we illustrate the outcomes of our real deployment.

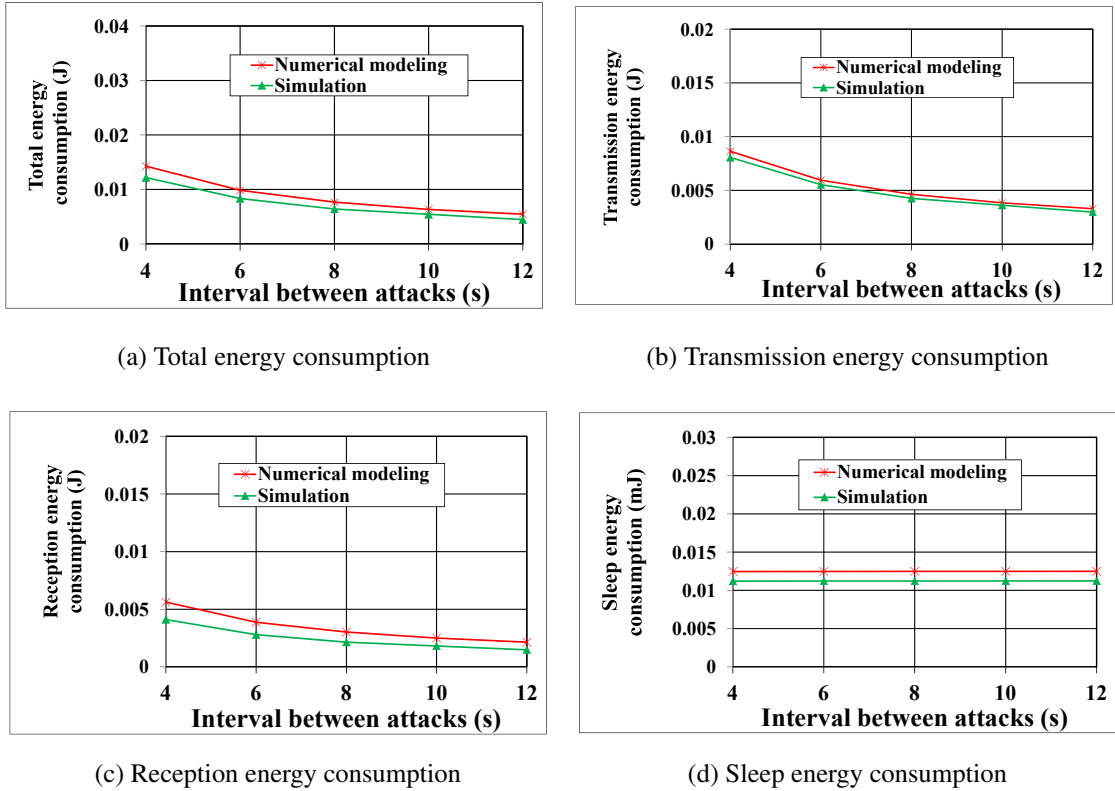


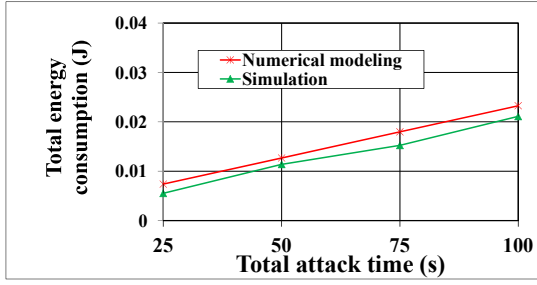
Figure 3.17: Impact of varying interval between attacks on the energy consumption by the very next sensor node under attack for mobile attack model

3.5.2 Real Deployment on Rail Lines

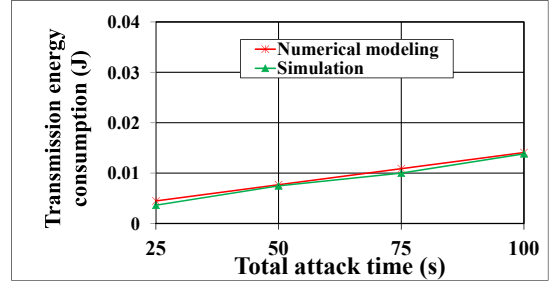
We perform a set of experiments to launch the power attack in the real-time system for detecting missing rail blocks and to evaluate the performance of the proposed countermeasures in a real scenario on the rail track. It is to be noted that since the simulations of MITM attack and replay attack are trivial, we focus mainly on the simulations of the power attack. In this section, we first present the settings of the real deployment followed by the results.

3.5.2.1 Experimental settings

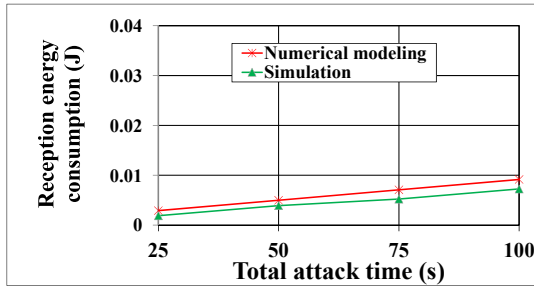
In our experimental setup for the attack, we adopt a scenario presented in Fig. 3.1a. We deploy the attack on the track of Kamalapur railway station, which is one of the busiest railway stations of Bangladesh. Here, we place two sensor nodes on the rail track (Fig. 3.24a). The components of the sensor node are depicted in Fig. 3.24b. Both the sensor node in the train and the adversary node contain similar components expect having no vibration sensor module. Fig. 3.24c exhibits a snapshot of the adversary node placed on the rail track.



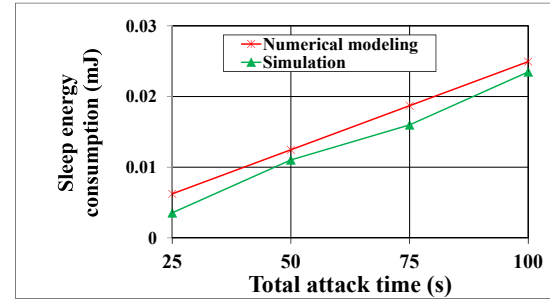
(a) Total energy consumption



(b) Transmission energy consumption



(c) Reception energy consumption



(d) Sleep energy consumption

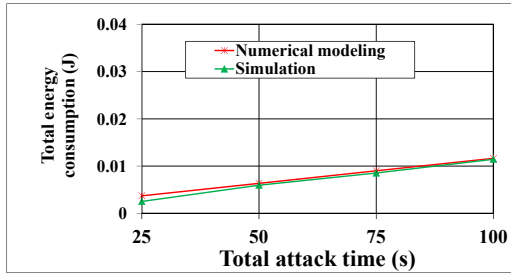
Figure 3.18: Impact of varying total attack time on the energy consumption by the sensor node under attack for mobile attack model

Our endeavor is to simulate the power attack along with its countermeasures and to analyze the power consumption during transmission and reception of packets. Hence, we perform the simulation without the vibration sensing module for the sensor node on the rail track (Fig. 3.24a). To generate power attack the adversary sensor node sends query packet at 4s interval for 120s. We measured power consumption for the sensor node under attack and for the very next sensor node under attack.

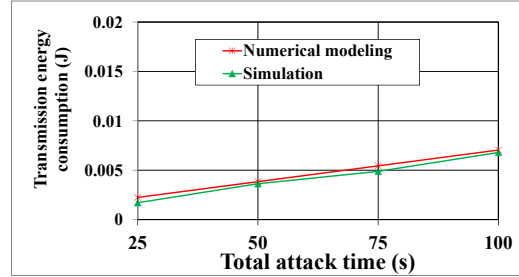
Next, we illustrate the results of the real deployment.

3.5.2.2 Performance evaluation of power attack and countermeasures

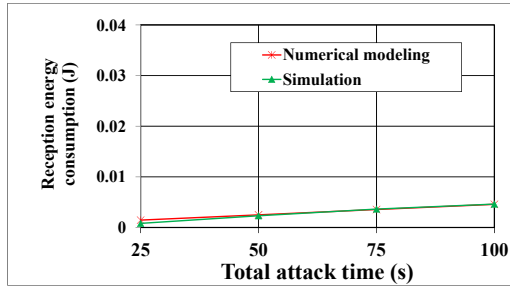
Fig. 3.25 demonstrates the results of the power attack and proposed countermeasures for sensors on the rail track. Fig. 3.25a shows that power attack increases the power consumption by the sensor node under attack in comparison to that of power consumption without attack. Fig. 3.25b exhibits similar outcomes for the very next sensor node under attack. Here, for the real deployment we perform power attack only for about 120s. If the attack continues



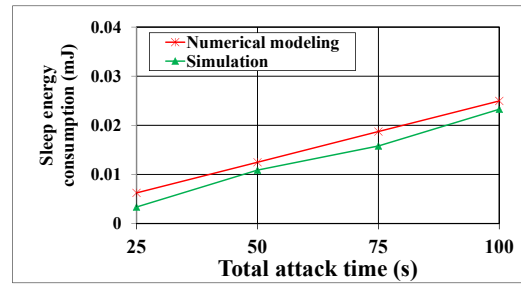
(a) Total energy consumption



(b) Transmission energy consumption

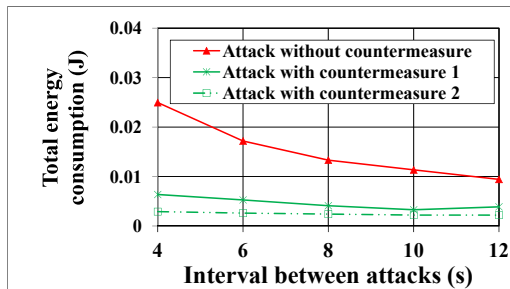


(c) Reception energy consumption

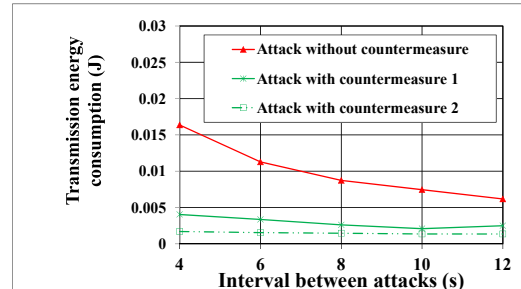


(d) Sleep energy consumption

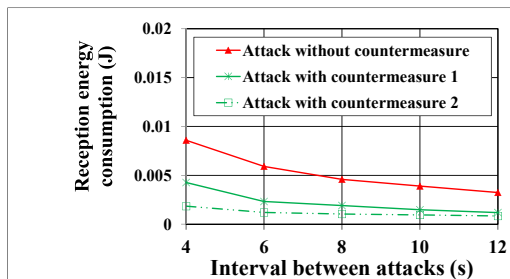
Figure 3.19: Impact of varying total attack time on the energy consumption by the very next sensor node under attack for mobile attack model



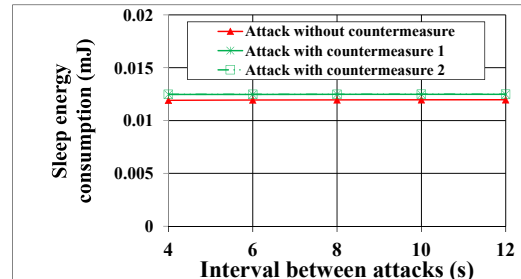
(a) Total energy consumption



(b) Transmission energy consumption

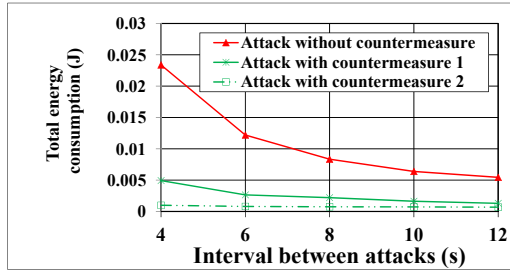


(c) Reception energy consumption

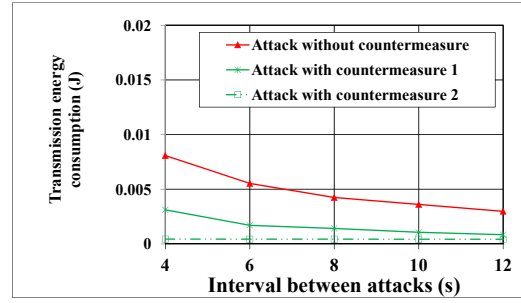


(d) Sleep energy consumption

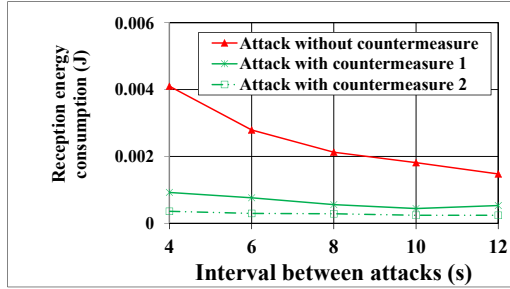
Figure 3.20: Performance comparison of countermeasures for varying interval between attacks on the energy consumption by the sensor node under attack



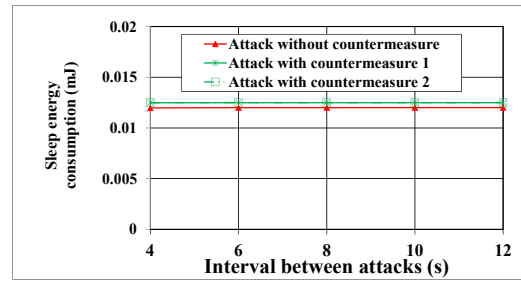
(a) Total energy consumption



(b) Transmission energy consumption



(c) Reception energy consumption



(d) Sleep energy consumption

Figure 3.21: Performance comparison of countermeasures for varying interval between attacks on the energy consumption by the very next sensor node under attack

to persist for long period of time, it will eventually force the energy resource of the sensor node, i.e., battery, to die off due to draining out of stored energy. This will result disruption of communication.

Consecutively, we evaluate the performance of our proposed countermeasures. Our simulation reveals that the proposed countermeasures reduce power consumption compared to the power consumption during the attack. Furthermore, similar to $ns-2$ simulation results, in the real deployment, countermeasure 2 outperforms countermeasure 1. Fig. 3.25b exhibits similar outcomes for the very next sensor node under attack. Thus, our real deployment proves the efficacy of our proposed countermeasures.

However, it is to be noted that for our real deployment, we do not take into account the sensing. Furthermore, in real deployment the microcontroller also consumes power for performing operation. However, for our $ns-2$ simulation we do not consider the power consumption of microcontroller.

Besides the evaluation of power consumption, we also explore the response time of the query packet that is sent by the train for different events. Here, response time indicates the

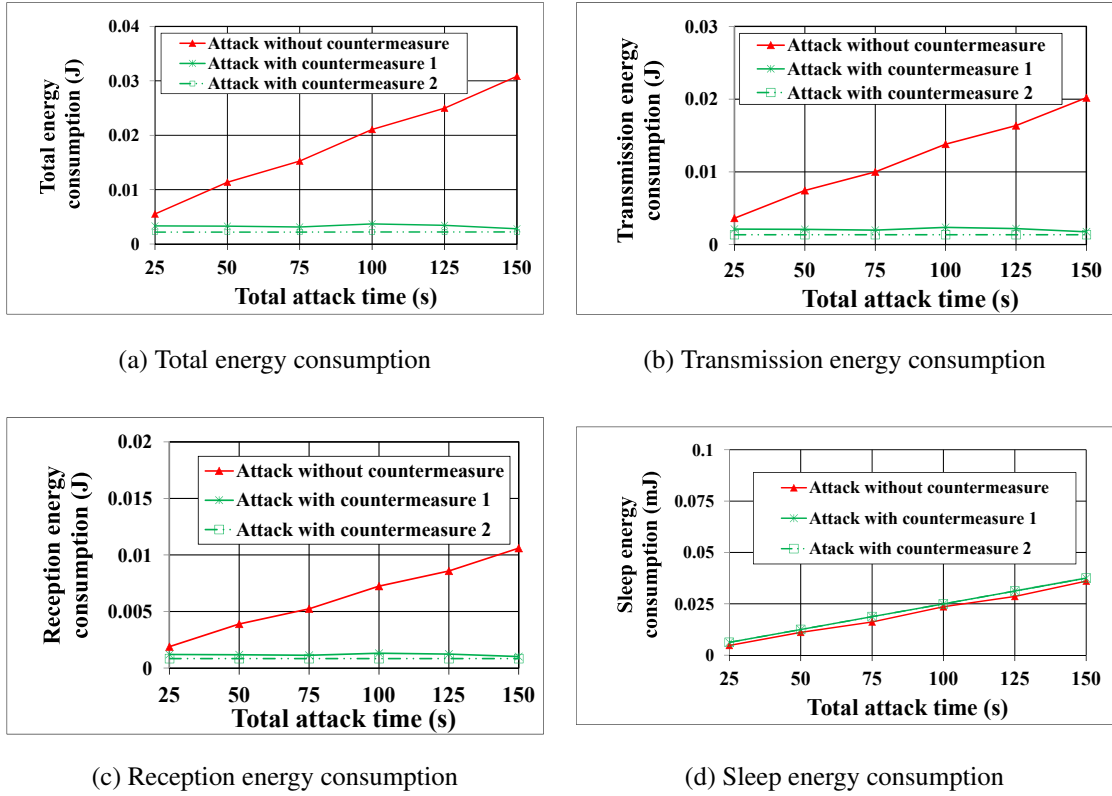
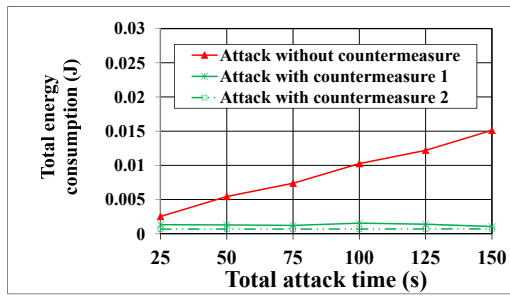


Figure 3.22: Performance comparison of countermeasures for varying total attack time on the energy consumption by the sensor node under attack

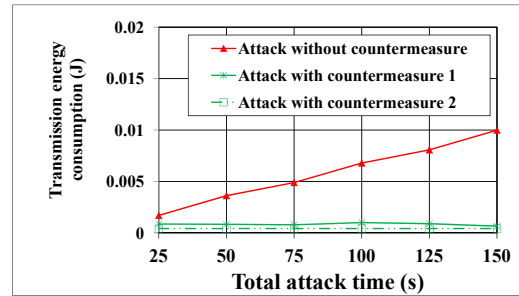
Events	Response time (ms)
Without attack	1244
With attack	1245
Attack with countermeasure 1	1259
Attack with countermeasure 2	1269

Table 3.3: Response time of the train for different events time that is needed to perform a full communication, i.e., from the transmission of the query packet to the reception of the report packets by the train.

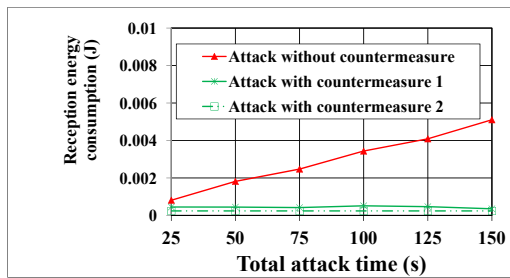
Table. 3.3 demonstrates the response time of the train for different events. It is to be noted that our focus for the real deployment is confined to the network-level delay of the query packet, hence, we do not take into account the time needed for sensing while computing the response time. Table. 3.3 exhibits that the response time for without attack event is similar to the response time for the attack. However, the response time increases during the countermeasures as the size of the packets are increased. Consequently, countermeasure 2 takes more time to respond to the query packets. However, the changes in the response time for different events are not of that significant. Furthermore, our simulation reveals that the delivery ratio remains 100% for different events.



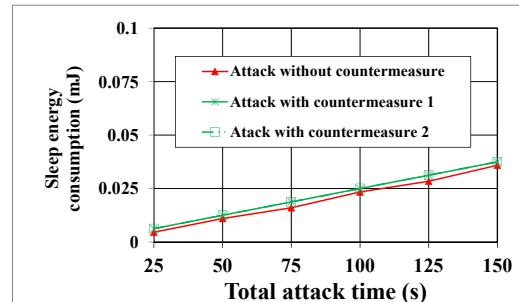
(a) Total energy consumption



(b) Transmission energy consumption



(c) Reception energy consumption

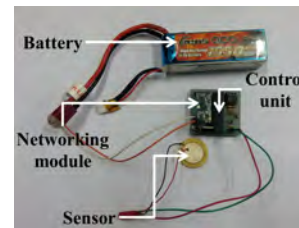


(d) Sleep energy consumption

Figure 3.23: Performance comparison of countermeasures for varying total attack time on the energy consumption by the very next sensor node under attack



(a) Sensor node on the rail track



(b) Components of sensor node



(c) Adversary sensor node

Figure 3.24: Real deployment

3.6 Conclusion

Derailments owing to missing rail blocks frequently occur in developing countries such as Bangladesh, India, Kenya, etc. Hence, development of a real-time system for detecting miss-

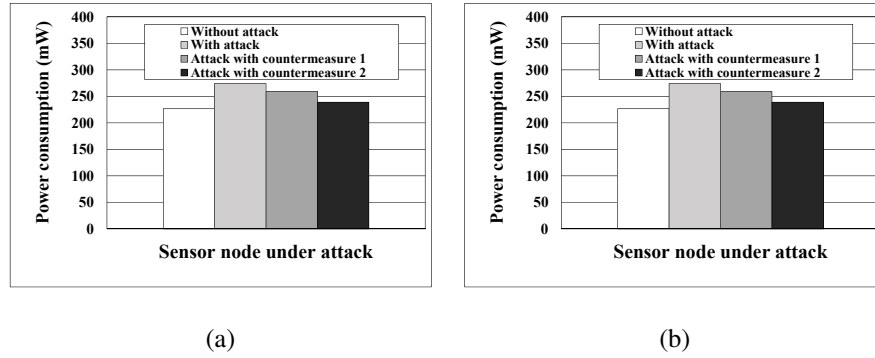


Figure 3.25: Power consumption during real deployment of the power attack and countermeasures for (a) sensor node under attack and (b) the very next sensor node under attack

ing rail blocks considering diverse constraints of developing countries grabs attention to the researchers. In Chapter 2 we represent a real-time system for detecting missing rail blocks in developing countries. However, the work does not address any issue related to security of the system even though security of such a system is of utmost significance considering its vulnerabilities from diversified perspectives.

Therefore, in this chapter, we endeavor to analyze potential security threats pertinent to the real-time system for detecting missing rail blocks. Hence, we propose a new security threat entitled as power attack along with its attack models. In our attack model, an adversary node forces the sensors, which are placed on the rail track to deplete more energy by accepting and responding to frequent request about the condition of the track ahead. Consequently, we perform experimentation using both $ns-2$ simulation and real deployment to exhibit applicability and effectiveness of our proposed attack and attack models. Consequently, we explore popular security threats such as MITM attack and replay attack. Afterward, we propose effective countermeasures to mitigate the damages of different attacks exposed through our study. We demonstrate the efficacy of our proposed countermeasures via $ns-2$ simulation and real deployment in the rail lines.

In the next part of the thesis, we move on to explore the miniature versions of limited-resource cyber-physical networks.

Part II

Miniature Versions of Limited-Resource Cyber-Physical Networks

Chapter 4

Exploring Network-Level Performances of Wireless Nanonetworks Utilizing Gains of Different Types of Nano-Antennas with Different Materials

4.1 Introduction

The recent proliferation of nanotechnology fosters development of nano machines or nano devices having a size of one to few hundred nanometers. Such nano machines are envisioned to have promising applications in diversified fields such as bio-medical, environment science, industrial development, food science, etc., [156]. Such applications inspire investigation of the nano devices to organize themselves in wireless nanonetworks and perform complex tasks in a distributed way through exploiting communication capabilities [157].

However, communication in nanonetworks poses challenges owing to limitations in capabilities of the nanosensors such as limited transmission range, less processing power, small memory, scarcity of energy, etc. Besides, nano devices radiate over terahertz (THz) band using nano-antennas, which have a short communication range. Short communication range in the THz band and accompanied signal absorption render the direct communication between nano devices often infeasible in real applications. Additionally, nano devices have

very low power and limited operating capabilities owing to their tiny sizes. These limitations of nano devices introduce mammoth challenges during communication in the wireless nanonetworks. Furthermore, communication in the wireless nanonetworks is also influenced by the basic communication units of nano devices, i.e., nano-antennas.

From the electromagnetic perspective, miniaturization of traditional metallic antennas to nano-antennas would theoretically result in very high resonance frequencies. Moreover, metals could fail to behave in its conventional way for such high frequencies [157]. Therefore, metallic nano-antennas might face some difficulties as pointed out in the study presented in [158]. Consequently, the use of different nanomaterials such as carbon nanotubes (CNT) [159] and graphene [160] in fabricating miniature nano-antennas comes into play to overcome the difficulties faced by metallic antennas. However, the impact of different materials on network-level performances of wireless nanonetworks is yet to be explored in the literature.

Several research studies [161] advocate that the resonance frequency of an antenna can be tuned by changing the length, width, height, and material of the antenna. As a result, careful selection of these parameters for a nano-antenna can enhance frequency range from UV to near-IR spectrum. Even in case of such careful selection being made, it still remains unclear how good the network-level performances of different nano-antennas would be. To clarify this, gains of different types of nano-antennas need to be analyzed and compared, which is yet to be done in the literature to the best of our knowledge. Exploration of existing literature on nano-antennas delineate the usage of patch, dipole, and loop nano-antennas in diversified real-life applications [83–85]. Furthermore, it also influences our choices of materials, i.e., graphene, CNT, and copper. Therefore, in this paper, we perform investigation on gains of customized nano-antennas (i.e., different types of well-known nano-antennas such as patch, dipole, and loop for various materials such as copper, CNT, and graphene) leveraging analytical models.

Furthermore, several real-life applications of wireless nano devices such as nuclear, biological and chemical defenses, damage detection systems, and health monitoring systems foster transmission of sensed information over large-size wireless nanonetworks. However, communication in wireless nanonetworks is expected to experience different hurdles, owing

to limitations of nano devices such as limited transmission range, less computation power, small memory, scarcity of energy, etc. Therefore, traditional approaches for wireless communication suffer from performance loss in nanonetworks [58]. To overcome such loss existing studies attempt to enhance efficiency at the Physical and MAC layers, where the main focus remains limited to node-level energy efficiency [162]. However, a network-level performance exploration for large-size wireless nanonetworks exploiting different types of nano-antennas is envisioned as a potential research study which is yet to be explored in the literature to the best of our knowledge. Therefore, in this paper, we perform a study to evaluate the impacts of using different types of nano-antennas having different materials on enhancing the network-level performances of large-size wireless nanonetworks. This study also leads us towards the road to finding efficient nano-antennas for wireless nanonetworks. Here, our primary focus in this paper is to present theoretical foundations of future real implementations. The real implementation of customized nano-antennas (i.e., dipole, patch, and loop nano-antennas with different types of materials such as copper, CNT, and graphene) is expected to be quite expensive demanding prolonged work. Moreover, additional concerns need to be addressed for such implementation to avoid different health hazards. Therefore, presenting a theoretical foundation is of utmost importance before attempting for the real implementation. Hence, we perform our analysis from a theoretical point of view with experimentation using simulation. Later, we use the results of our analysis in our customized network simulator $ns-2$ for the evaluation of network-level performance of nanonetworks. In general, the network-level performance of nanonetworks mainly depends on the propagation of the transmitted signal over communication channel. This propagation, in turn, vastly depends on gain of nano-antennas. Nonetheless, other factors that affect the propagation of the transmitted signal include path-loss, molecular absorption noise, interference, shadowing, scattering, transmission frequency, composition of the medium, and levels of energy of each nano device [163]. This research study by Jornet et al., along with another research study presented in [164] have already presented analyses on these aspects. However, these studies are yet to explore the aspect of gain of nano-antennas, which is perhaps the most important player that controls the network-level performance and offers a flexibility to be controlled at the design level. To the best of our knowledge, such an exploration on the im-

fact of gain of nano-antennas over the network-level performance is yet to be done in the literature too. Therefore, in this paper, we specifically consider the impacts of gains on the network-level performance of nanonetworks. Higher gain of an antenna resembles higher coverage and communication range. This phenomenon is expected to improve network-level performance in terms of providing reduced end-to-end delay, higher throughput, and higher delivery ratio. Therefore, in our study, we first focus on analyzing antenna gains for different types of nano-antennas using different materials. Subsequently, exploiting outcomes of the analysis, we investigate network-level performances of diversified nanonetworks while using different nano-antennas. Our network-level investigation covers various perspectives such as network throughput, end-to-end delay, delivery ratio, and drop ratio.

Based on our study, we make the following set of contributions in this work:

- We present analytical models for antenna gains of different types of nano-antennas such as patch, dipole, and loop nano-antennas.
- Next, we perform numerical simulation for antenna gains based on the analytical models to investigate impacts of different types of materials such as copper, CNT, and graphene for different types of nano-antennas. Our numerical simulation results reveal that the gain of dipole nano-antenna using copper material exhibits the highest antenna gain compared to other alternatives.
- Finally, we evaluate network-level performances of large-size wireless nanonetworks exploiting different types of nano-antennas, having different materials, using rigorous ns-2 simulation. Our evaluation reveals a number of novel findings pertinent to network-level performance of wireless nanonetworks.

4.2 Motivation and Related Work

According to the literature, nanonetworks have four types of communication paradigms i.e., nanomechanical, acoustic, electromagnetic, and molecular communication. However, owing to diverse potential applications molecular communication and wireless electromagnetic (EM) communication recently grabbed the interest of research community.

The molecular or bio-inspired communication exploits biological molecules as information carriers. For example, the information is encoded on several biological molecules (e.g. RNA), which are diffused to the environment [165, 166]. Existing studies pertinent to molecular communication mostly focused on issues related to Physical layer, MAC layer, and Network layer. One of the most common issues in the Physical layer is the propagation of signals in various media and environments. Hence, existing studies focus on designing different propagation models such as random walk model [167], random walk models with drift [168, 169], diffusion-based models [170], diffusion-reaction based models [171], active transport models [172], and collision-based model [173] for molecular communication. Furthermore, existing studies using molecular communication focus on other issues of the physical layer such as signal modulation [174], signal amplification [175], and channel capacity [176]. Moreover, there exist some research studies in the literature focusing on diverse issues of link layer such as error handling [177, 178], addressing [179], and synchronization [180]. The authors in [181, 182] explore the development of routing protocol for molecular communication.

On the other hand, wireless communication in nanonetworks is based on electromagnetic (EM) waves. However, the research in this field is still in the embryonic stage. Hence, existing studies [164], [162], [183] in the literature focused on properties of nano-materials and corresponding modeling of wireless communication in THz band. However, the real implementation of a nano-antenna for enabling such communication is still an ongoing research area. For example, the study presented in [161] computes decay rates of transmitters for nano-antennas while using gold, copper, silver, and aluminum. Its results emphasize on careful selection of size, shape, and material for enhancing transmitter frequency over EM spectrum in nano-scale.

Operating over EM spectrum using conventional metallic antennas seems to be apparently not suitable for nano-communication [158]. Graphene, a novel material implicitly lying in the nano-scale along with having distinctive quantum mechanical properties, appears as a potential solution to the problem of adopting the metallic antennas [158]. Consequently, graphene has attracted tremendous interests in various research areas due to its exceptional electrical and mechanical properties [184]. Alongside, other materials such as CNT [159]

also offer an alternative to the problem. However, choosing the efficient one among the alternatives through analyzing their gains is yet to be investigated in the literature. Another unexplored part is to perform analysis based on different types of nano-antennas that could be built using the different materials.

Besides, recent studies also focus on the exploration of the protocol stack, network architectures, and channel access procedure pertinent to diversified applications of wireless nanonetworks. More specifically, most of the existing research efforts focus on deployment of Physical and MAC layer protocol, where the main intention confined to ensuring energy efficiency.

Existing studies at Physical layer of wireless nanonetworks mainly focus on channel models and designing of nano-antenna imposing the capability to operate in terahertz band or in VHF band [167, 185–190]. In [187], neuro-spike communication of molecular communications has been considered. Here, an interference model for synaptic channels with particular focus on InterSymbol Interference (ISI) and Single-Input Single-Output (SISO) channel is proposed. The authors here have investigated the overlapping between the two consecutively signals which are sent from a presynaptic terminal to a postsynaptic terminal and their interferences. Additionally, important metrics of synaptic communication channel pertaining the ISI are also analyzed. The relationship between channel rate region and ISI is also explored.

Next, the study presented in [188] investigates the state of the art in molecular electronics considering Terahertz Band (0.1-10.0 THz) for electromagnetic (EM) communication among nano-devices. Here, a new propagation model for EM communications in the Terahertz Band has been developed based on radiative transfer theory and in light of molecular absorption. This model considers the total path loss and the molecular absorption noise that a wave in the Terahertz Band suffers when propagating over very short distances. Besides, the channel capacity of the Terahertz Band has been analyzed by using this model for different power allocation schemes, including a scheme based on the transmission of femtosecond-long pulses. Besides, in [189], the authors introduce the equivalent discrete-time channel model (EDTCM) to the area of diffusion-based molecular communication (DBMC). Here, the main focus is on an absorbing receiver, which is based on the first passage time concept. The EDTCM improves the accessibility of DBMC and supports the adaptation of

classical wireless communication algorithms to the area of DBMC. Moreover, for the exact EDTCM, three approximations based on binomial, Gaussian, and Poisson approximation are proposed and analyzed in order to reduce computational complexity. In addition, the Bahl-Cocke-Jelinek-Raviv (BCJR) algorithm is utilized for studying all four channel models.

The study presented in [191] proposes a new Physical layer Aware MAC protocol for nanonetworks using EM communication in the Terahertz Band. This protocol utilizes a pulse-based communication scheme and a low-weight channel coding schemes for nanonetworks. In PHLAME, the transmitting and receiving nano devices jointly select the optimal communication scheme parameters and the channel coding scheme with a view to maximizing the probability of successfully decoding the received information while minimizing the generated multi-user interference. The authors in [192] propose a hierarchical network architecture, which integrates body area nanonetworks and macro-scale health-care monitoring system. They also propose two different energy-harvesting protocol stacks that regulate the communication among nano-devices during the execution of advanced nano-medical applications.

Moreover, the authors in [186] explore modulation and encoding schemes for nanosensor networks. Here, they propose the utilization of low-weight channel codes to mitigate the interference in pulse-based electromagnetic nanonetworks in the Terahertz band. Besides, the impulsive interference has been statistically modeled which is generated by a Poisson field of nanomachines that operate under a new pulse-based communication scheme named TSOOK (Time Spread On-Off Keying), and provide a closed-loop expression for the probability density function of the interference. The impact of the code weight on the total interference power and the information rate is analytically and numerically evaluated. Finally, this paper reveals that using low-weight channel codes, the overall interference can be reduced while keeping constant or even increasing the achievable information rate in an interference limited scenario.

At MAC layer, a Receiver Initiated Harvesting-aware MAC protocol is introduced in [193]. In RIH-MAC, receiver-initiated protocol has been proposed which takes into account the energy harvesting properties of nano nodes, where they may form a centralized or distributed network. The scalability with the increase in the number of nanonodes is also

considered. This protocol is suitable to be deployed in a large number of nanonetwork applications, where delay and packet loss are not mandatory QoS requirements. Moreover, here, a cluster-based communication is considered among the nanosensors. Another harvesting-aware MAC protocol is introduced in [194] which utilizes a hierarchical cluster-based architecture where all nanonodes communicate directly with the more powerful nanocontroller in one hop. Here, energy and spectrum-aware MAC protocols for wireless nanonetworks have been proposed which consider throughput and lifetime optimal channel access by jointly optimizing the energy harvesting and consumption processes. A system design parameter, namely, the critical packet transmission ratio (CTR) has been formulated, which is the maximum allowable ratio between the transmission time and the energy harvesting time, below which the nanosensor node can harvest more energy than the consumed one. Based on the CTR, a novel symbol compression scheduling algorithm is introduced using pulse-based physical layer technique. The symbol-compression algorithm uses the flexibility of the inter-symbol spacing of the pulse-based physical layer. This enables multiple nano sensors to transmit their packets concurrently without inducing any collisions. Besides, a packet-level timeline scheduling algorithm is proposed, which relies on a theoretical bandwidth adaptive capacity-optimal physical layer with a goal of achieving the balanced single-user throughput with the infinite network lifetime.

Next, studies presented in [195] introduce a flood-based lightweight routing protocol at Network layer. Here, an analytical model for the energy harvesting process of a nano-device is developed which is powered by a piezoelectric nano-generator. This model takes into account the energy consumption processes for communication among nano devices in the Terahertz Band. The variation in nano device energy and their correlation with the whole network traffic is modeled here. A mathematical framework to analyze the impact of several network metrics such as end-to-end packet delivery probability, the end-to-end delay, and the throughput is developed. However, this protocol suffers from redundancy and collisions, which degrades the performance of WSNs with respect to energy consumption.

Besides, in [196], a joint coordinate and routing system (CORONA) for nanonetworks has been proposed. The joint coordinate and routing system here is considered to be deployed on a two-dimensional ad hoc nanonetwork. At setup phase, user-selected nodes are used

as anchor-points. Then, all nodes compute their distances in number of hops from these anchors by utilizing geo-location. At operation phase, the routing is enabled by selecting the appropriate subset of anchors which are selected by the sender of a packet. Here, the rate of packet re-transmission and packet loss rate are reduced. However, routing through fixed coordinate-based anchor nodes faces difficulty when any of the anchor nodes does not work properly.

In [50], the authors introduce an open source tool modeling WSNs within the NS-3 simulator namely Nano-Sim. Here, they analyze and evaluate complete performance of nanonetworks operating in a health-monitoring system. A new flooding routing algorithm and a more efficient MAC protocol are proposed focusing on a nanonetworks operating in a health monitoring scenario. The network behavior of nanonetworks is investigated to analyze the impact of the density of nodes, the transmission range of nanomachines, and the adoption of specific combinations of routing and MAC strategies.

Another approach namely Dynamic Infrastructure (DIF) [197, 198] has been introduced to reduce transmissions without compromising the high network coverage. The key idea in DIF is that only nodes with good reception quality can act as re-transmitters, while the remaining nodes revert to receiving-only mode. While the DIF approach ensures energy efficiency, as in the flood approach, every single node in the topology overhears transmitted packets in the network even when it is not necessary. Here, overall packet transmission is also diminished.

Consequently, recent studies [57], [58] focus on analyzing wireless communication between a pair of nano devices. Such studies facilitate deciding on efficient nano-antennas from the perspective of point-to-point communication. However, network-level communication in a nanonetwork remains beyond the scope of all the above-mentioned studies, which is utmost important for deciding on a suitable nano-antenna from its several alternatives. Therefore, in this chapter, we attempt to investigate the network-level communication in nanonetworks. To do so, first, we present analytical models for gains of different types of nano-antennas.

4.3 Methodology of Our Work

In this chapter, we aim to facilitate selection of suitable nano-antennas and materials while enhancing the network-level performance of nanonetworks. To do so, first, we derive analytical models of gains for different types of nano-antennas. Here, our primary focus in this work is to present theoretical foundations of future real implementations. The real implementation of customized nano-antennas (i.e., dipole, patch, and loop nano-antennas with different types of materials such as copper, CNT, and graphene) is expected to be quite expensive demanding prolonged work. Moreover, additional concerns need to be addressed for such implementation to avoid different health hazards. Therefore, presenting a theoretical foundation is of utmost importance before attempting for the real implementation. Hence, we perform our analysis from a theoretical point of view with experimentation using simulation. Later, we use the results of our analysis in our customized ns-2 for the evaluation of network-level performance of nanonetworks utilizing different nano-antennas with different materials.

4.4 Analytical Models of Nano-Antennas

In this section, we formulate analytical models of gains of different types of nano-antennas [199]. In order to formulate analytical models, first, we consider that the gain of a nano-antenna is generally expressed as follows [199]:

$$G = \eta \times D \quad (4.1)$$

Where, G denotes the expected gain of a nano-antenna, η denotes the antenna radiation efficiency, and D denotes the directivity of the nano-antenna. *Directivity* is the ratio between radiation intensity in a certain direction from the antenna and the radiation intensity averaged over all directions. If the direction is not specified, the ratio considers the direction of the maximum radiation intensity. Eq. 4.1 suggests that we need to deduce η and D to find gains of different types of nano-antennas. Therefore, next, we focus on developing analytical models of D and η for different types of nano-antennas.

4.4.1 Gain of Patch Nano-Antenna

The antenna radiation efficiency η of a patch nano-antenna depends on the total quality factor Q_t of the antenna and the quality factor due to the radiation losses Q_{rad} [199]. Therefore, the radiation efficiency for the patch nano-antenna is formulated as follows:

$$\eta = \frac{Q_t}{Q_{rad}} \quad (4.2)$$

The quality factor is a figure-of-merit that represents the antenna losses. There are several losses such as radiation, conduction (ohmic), dielectric and surface wave losses. The total quality factor Q_t of a patch nano-antenna is influenced by all of these losses [199]. Therefore, the total quality factor of a patch nano-antenna is defined as follows:

$$\frac{1}{Q_t} = \frac{1}{Q_{rad}} + \frac{1}{Q_c} + \frac{1}{Q_d} + \frac{1}{Q_{sw}} \quad (4.3)$$

where, Q_c , Q_d , and Q_{sw} are the quality factors due to conduction, dielectric, and surface wave losses respectively. Therefore, we need to calculate these quality factors individually for determining the total quality factor. The quality factor due to radiation losses is calculated as [199]:

$$Q_{rad} = \frac{2\omega\epsilon_r}{h\frac{G_t}{l}} K \quad (4.4)$$

where, $\frac{G_t}{l}$ is the total conductance per unit length of the radiating aperture, ϵ_r is the dielectric constant of the substrate material, and h is the height of the patch nano-antenna. K can be computed using the following equation,

$$K = \frac{L_p}{4} \quad (4.5)$$

Here, L_p is the patch length of the non-radiation edge of the patch nano-antenna.

For dominant Transverse Magnetic Mode (TM) of a patch nano-antenna $\frac{G_t}{l}$ is calculated as $\frac{G_t}{l} = \frac{G_r}{W_p}$ where, W_p is the patch width of the radiation edge of the patch nano-antenna, and G_r is the conductance of the patch nano-antenna. Here, G_r is determined as $G_r = 2G_s$ [200]. G_s can be computed using the following equation,

$$G_s = \begin{cases} \frac{W_p}{90\lambda}, & W_p < 0.35\lambda \\ \frac{W_p}{120\lambda} - \frac{1}{60\pi^2}, & 0.35\lambda \leq W_p < 2\lambda \\ \frac{W_p}{120\lambda}, & 2\lambda \leq W_p \end{cases} \quad (4.6)$$

Where, λ is the wavelength. Using the above mentioned equations, we can compute Q_{rad} . Next, we need to compute Q_c , Q_d and Q_{sw} . Since the height of the patch nano-antenna remains in nano-scale ($h_p \ll \lambda$) the losses due to surface waves Q_{sw} become very small. Therefore, we neglect the impact of Q_{sw} on the total quality factor. Next, the quality factor due to conduction losses is calculated as $Q_c = h_p \sqrt{\pi f \mu \sigma}$ [199]. Here, f is the operating frequency, σ is the conductivity and μ is the permeability of conductor associated with patch and ground plane.

It is to be notated that to mimic effect of different materials on gains of patch nano-antennas the values of σ and μ are set based on the the choice of materials. In our study, we consider three types of materials, i.e., copper, carbon nanotubes (CNT), and graphene and the values of σ and μ are selected based on studies presented in [201–204].

Besides, the quality factor due to electric losses is computed as follows.

$$Q_d = \frac{1}{\tan \delta} \quad (4.7)$$

Where, $\tan \delta$ is loss tangent of the substrate material. Here, δ refers skin depth [205]. The value of δ depends on the materials used in the nano-antennas. Thus, it changes due to variation in the material of a patch nano-antenna.

After the determination of Q_t and Q_{rad} , we compute the value of η using Eq. 4.2. Finally, to compute the gain as per Eq. 4.1 the directivity of the patch nano-antenna is computed as follows [200]:

$$D = \frac{1}{15G_s} \frac{W_p^2}{\lambda} \quad (4.8)$$

4.4.2 Gain of Dipole Nano-Antenna

A traditional antenna can also be modeled with a series combination of radiation resistance R_r , loss resistance (ohmic) R_L and an antenna reactant component X_A . However, the antenna reactance component X_A does not dissipate any real power. Hence, only R_L is responsible for antenna radiation loss. Therefore, we formulate the antenna radiation efficiency η for a dipole nano-antenna as follows:

$$\eta = \frac{R_r}{R_r + R_L} \quad (4.9)$$

For the dipole nano-antenna, the radiation resistance R_r is modeled as:

$$R_r = 20\pi^2 \left(\frac{L_d}{\lambda} \right)^2 \quad (4.10)$$

Furthermore, the loss resistance R_L for the dipole nano-antenna is determined as follows [206]:

$$R_L = \frac{L_d}{6\pi r_d} \sqrt{\frac{\pi f \mu}{2\sigma}} \quad (4.11)$$

Here, L_d is the length and r_d is the radius of the dipole nano-antenna. μ is the permeability of dipole, and σ is the conductivity of dipole. The values of permeability and conductivity of a dipole nano-antenna depend on different materials used in nano-antenna. Here, we set the values based on [201–204] to reflect the impact of three different materials, i.e., copper, CNT, and graphene. For dipole nano-antennas, the length of a nano-antenna is very small ($L_d \ll \lambda$). Therefore, we can approximate the value of directivity D to 1.5 [199].

4.4.3 Gain of Loop Nano-Antenna

For a loop nano-antenna, Eq. 4.9 also retains. However, the radiation resistance R_r is modeled as follows [199]:

$$R_r = Z \left(\frac{2\pi}{3} \right) \left(\frac{kS}{\lambda} \right)^2 N^2 \quad (4.12)$$

Where, Z is the intrinsic impedance of the medium, which is computed through multiplying permeability by the speed of light [207]. Besides, k is the wave number, S is the surface area of the loop, and N is the number of turn in the loop. Here, the surface area S can be calculated as $S = \pi a^2$, where a is the radius of the loop. Besides, the loss resistance R_L for the loop nano-antenna is computed as [199]:

$$R_L = \frac{Na}{b} R_s \left(\frac{R_p}{R_0} + 1 \right) \quad (4.13)$$

Where, b is the radius of the wire used to create loop, R_s is the surface impedance of the conductor, R_0 is ohmic skin effect resistance per unit length, and R_p is ohmic resistance per unit length due to proximity effect. The value of R_s is calculated as $\sqrt{\frac{\pi f \mu}{\sigma}}$. Here, the values of μ and σ are selected based on materials used in loop nano-antennas.

The reduction in the ratio between R_p and R_0 reduces R_L . Such reduction will decrease losses for nano-antennas. We can reduce this ratio to approximately zero through increasing

separation between two successive loops [199]. Such reduction of losses increases the gains remarkably for loop nano-antennas. Similar to the dipole nano-antenna the directivity of the loop nano-antenna is considered to be approximately 1.5 [199].

It is worth mentioning that individual baseline equations utilized above have been mentioned either in [199] or [200]. However, the studies presented in [199, 200] utilized the equations for only general metallic antennas. On the other hand, in this chapter, we have adopted them in a coherent way that paves the path to analytically explore impacts of different nano-antennas.

Next, we conduct experiments using numerical simulations to investigate gains of different types of nano-antennas while using different types of materials such as copper, CNT, and graphene. In this experiment, we exploit the aforementioned analytical models.

4.5 Numerical Simulation of Gain for Different Types of Nano-Antennas

We conduct numerical simulation for gain based on analytical models presented in Section 4.4. In our simulation, we intend to explore the impact of different materials such as copper, CNT, and graphene on the gain of nano-antenna. We also explore the impact of variation of different metrics such as length, width, radius and the number of loops on the gains. For simplicity we consider an ideal signal generator. Hence, the input impedance and return loss for the antenna will be equal to zero. Before analyzing and presenting our simulation results, we briefly illustrate our simulation settings.

4.5.1 Simulation Settings

First, we analyze the impacts of operating frequency on gains for different types of nano-antennas using different types of materials. We also explore the impact of different types of material on the gain of a nano-antenna with a variation in frequency. We compute the gains of different nano-antennas using Eq. 4.1. We utilize Eq. 4.2 for the computation of radiation efficiency η for a patch nano-antenna and Eq. 4.9 for a dipole and a loop nano-antenna. We utilize Eq. 4.8 for directivity of the patch nano-antenna.

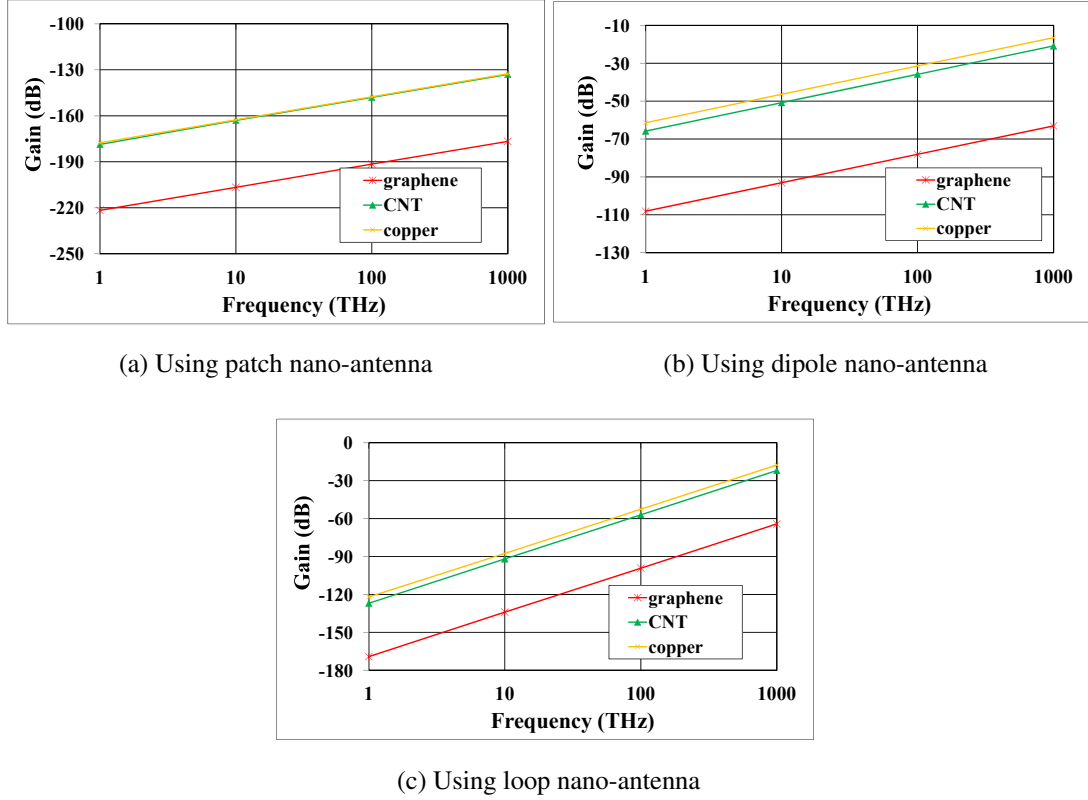


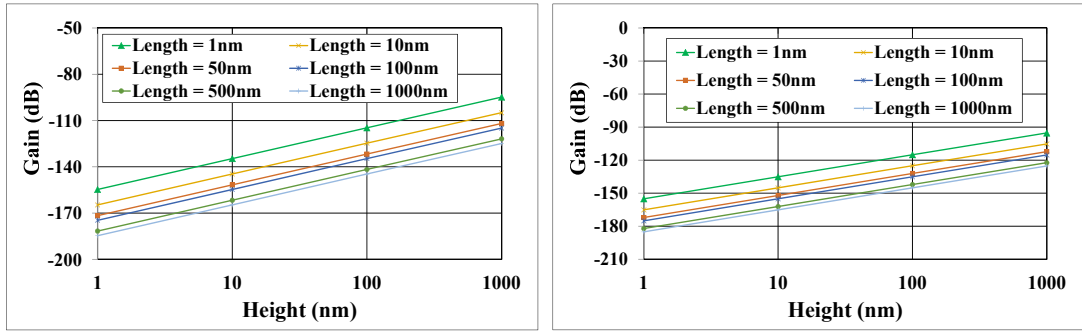
Figure 4.1: Impact on gains for varying frequencies over different types of nano-antennas

The operating frequency of a nano-antenna is in THz range [208]. Therefore, we consider the operating frequency range of the nano-antenna between 1 THz to 1000 THz for our numerical simulation. In our simulation, we consider the fact that both the available transmission bandwidth and the propagation loss increase with an increase in the antenna resonant frequency owing to very limited power in nano devices [209]. Therefore, we limit the frequency range within 1000 THz in our numerical simulation.

Consequently, we set several other parameters in our simulation. For example, to exhibit the impacts of different materials on the gain of a specific type of nano-antenna, we set the conductivity of copper, CNT, and graphene based on [201], [202]. Besides, we set the permeability of copper, CNT, and graphene based on [203] and [204]. In addition, we set the values of height, length, width, and radius of a nano-antenna ranging from 1nm to 1000nm.

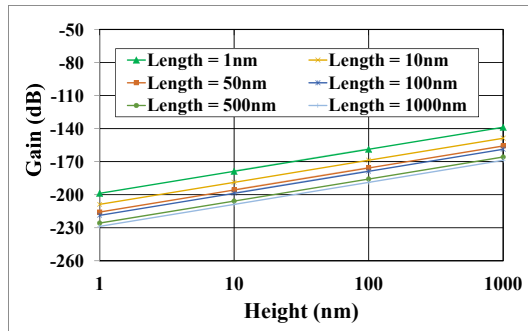
4.5.2 Simulation Results

We present the simulation results found with our simulation settings. First, we analyze the the impact on antenna gain for varying in frequency. Fig.4.1 depicts the impact. The figure



(a) Using copper as material

(b) Using CNT as material

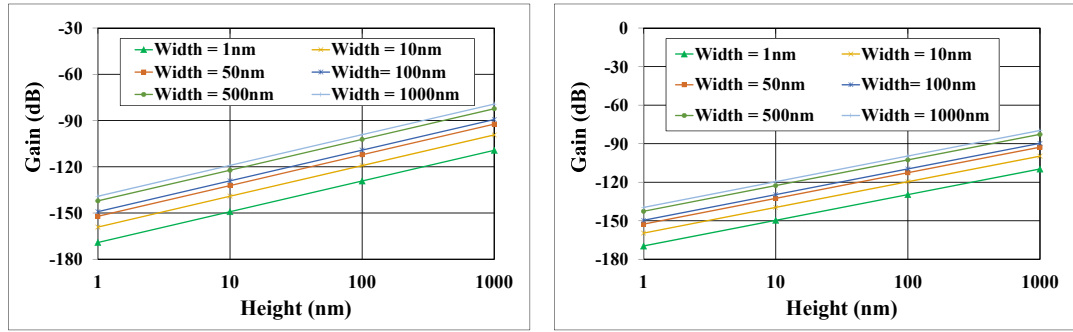


(c) Using graphene as material

Figure 4.2: Impact on gain for varying heights and lengths of patch nano-antennas using different types of materials

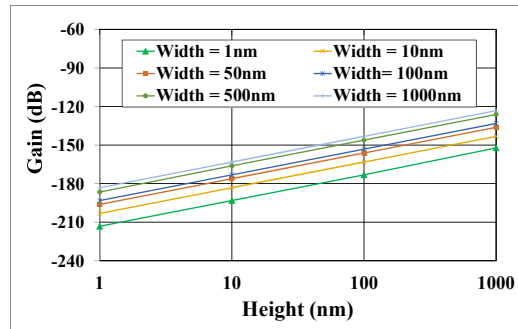
demonstrates an increasing trend in gain with an increase in frequency for different types of nano-antennas. Here, as per Fig. 4.1a the gain of a patch nano-antenna while using graphene is less compared to that while using copper and CNT. Besides, gains of dipole nano-antennas using copper are high compared to that using CNT and graphene (Fig. 4.1b). Additionally, loop nano-antennas demonstrates the same pattern as dipole and patch nano-antenna (Fig. 4.1c). Furthermore, the gains of dipole nano-antennas using different materials remain higher compared to that to patch and loop nano-antennas.

Next, we analyze the impact of variation in length, width, height, radius, and the number of loop on gains of different nano-antennas. Fig. 4.2 demonstrates the impacts on gain for varying in the height with in a range from 1 nm to 1000 nm for a rectangular patch nano-antenna. Here, the gain increases with an increase in the height. Besides, Fig. 4.2 depicts that the gain increases with a decrease in the length of non radiation edge of a rectangular patch nano-antenna for having specific height. Additionally, the figure demonstrates low gains while using graphene (Fig. 4.2c) compared to that while using copper (Fig. 4.2a) and



(a) Using copper as material

(b) Using CNT as material



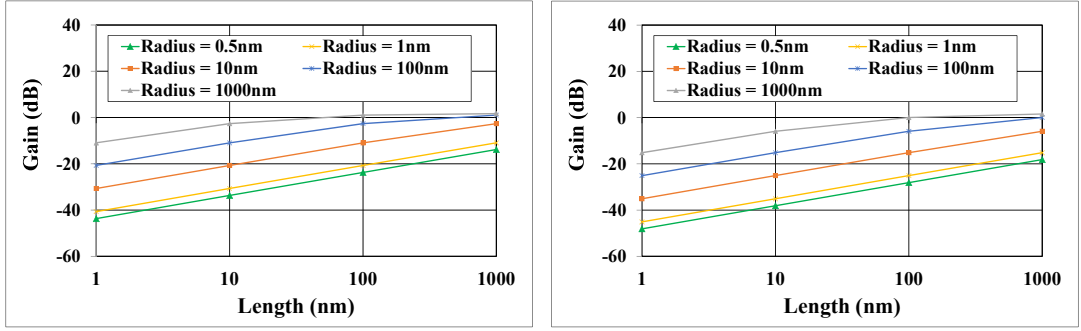
(c) Using graphene as material

Figure 4.3: Impact on gains for varying height and widths of patch nano-antennas using different types of materials

CNT (4.2b).

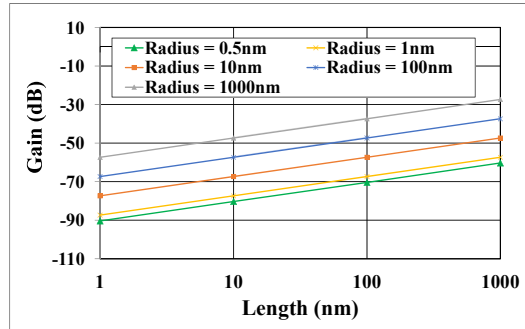
Fig. 4.3 shows the impact of variation in width of a radiation edge of patch antenna for different values of height. The gain for a specific height increases with an increase in the width. Here, we again find that the antenna gains while using graphene are low compared to that while using the others. Fig. 4.4 demonstrates the impact on gain with a variation in length and radius of dipole nano-antennas. The gain exhibits an increasing trend with an increase in length and radius. Here, the gains while using copper and CNT get saturated for large radius of the antennas. Again, we find that the gain using graphene is less compared to others.

Next, Fig. 4.5 illustrates the impact on gain for varying of the radius of loop and the number of loops for loop nano-antennas. The results exhibit an increase in antenna gain with an increase in radius and the number of loops. Besides, similar to the previous variations the antenna gains while using graphene remain lower compared to that while using copper and CNT.



(a) Using copper as material

(b) Using CNT as material



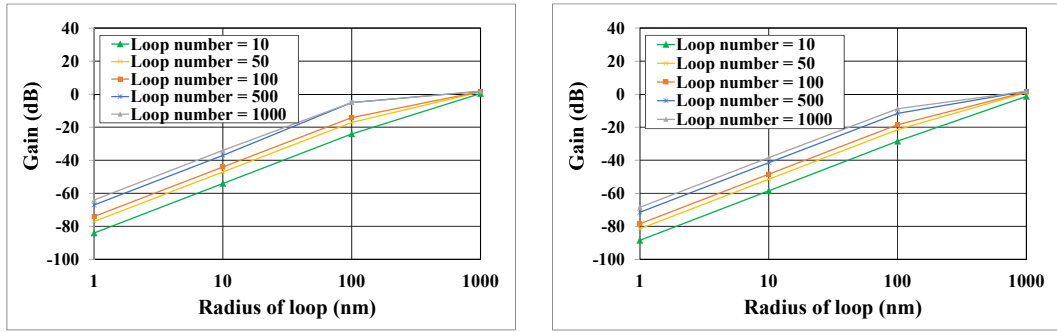
(c) Using graphene as material

Figure 4.4: Impact on gains for varying length of dipole nano-antennas using different types of materials

From our numerical simulation we find that the gain of the antennas is extremely small (-50 to $-170dB$) for THz band frequency. Such gain is suitable for various application such as AN/SPS- 40 surface search radar [210]. Up to now, we perform numerical simulation for analyzing the gain of a single nano-antenna. Next, we focus on analyzing the performance of a nanonetwork comprising nano-nodes, where nano-nodes are equipped with the already analyzed nano-antennas. Here, we perform experimental analysis of nanonetworks for different types of nano-antennas using customized NS-2 simulator. Before presenting our simulation settings and results, we first briefly elaborate our considered network model in the next section.

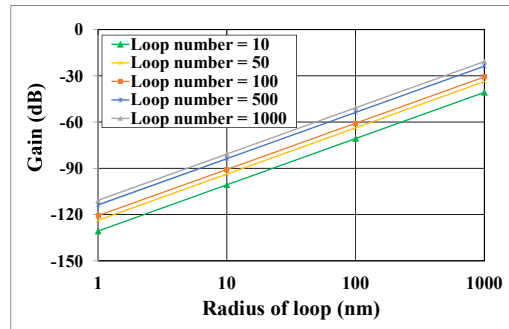
4.6 Network Model

In this section, we present a network model of a nano-network. Fig. 4.6 demonstrates an example network model intended for health-monitoring system, which is one of the promis-



(a) Using copper as material

(b) Using CNT as material



(c) Using graphene as material

Figure 4.5: Impact on gains for varying radius of loop nano-antennas using different types of materials

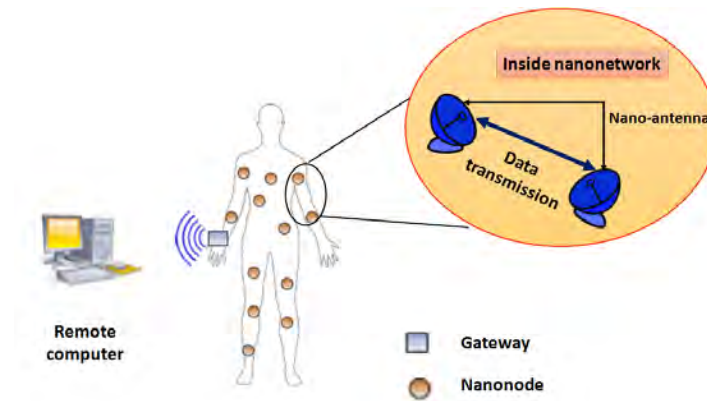


Figure 4.6: Network model

ing applications of nano-networks. The model comprises several nano-nodes of an example nanonetwork. Each nano-node is equipped with a nano-antenna. The nano-nodes periodically communicate with each other through transmission of data packets. The nano-network is generally connected with a remote node via a gateway as shown in Fig. 4.6. In this chapter, we focus on the data transmission only among the nano-nodes of the nanonetwork.

4.7 Experimental Results and Analysis

In this section, we provide the results and analysis of our experiments. We support our research findings with experimental data. For this, we evaluate the network-level performances of nanonetworks using different nano-antennas by implementing network model using the widely used network simulator `ns-2`. The aim of the evaluation is to demonstrate the practical utility of antenna-centric data transmission in nanonetworks for diversified fields, more specifically in the bio-medical field. We analyze four performance metrics i.e., end-to-end delay, throughput, packet delivery ratio, and drop ratio for our simulation.

4.7.1 Customization in `ns-2`

A well-known classical network simulator `ns-2` does not natively support nano-scale communications which is representative of nanonetworks. Moreover, `ns-2` is not designed for such a PHY-level and high frequency simulations. Therefore, we have to customize `ns-2` for our simulation pertaining to nanonetworks. Note that the classical propagation model, such as Two Ray propagation model mostly operates based on the heights of the conventional antennas. Hence, such classical models can not be applied for nano-antennas. We utilize the far-field equation to model the radio propagation model of nanonetworks [199]. The far-field equation is: $P_R = \left(\frac{\lambda}{4\pi \times R}\right)^2 \times G_T \times G_R \times P_T$. Here, P_T and P_R are the transmitted and received power respectively, G_T and G_R are the gain of the transmitter's and receiver's nano-antenna respectively, and R is the distance between the two nano devices. In general, a near-field is bounded within the region of $2D^2/\lambda$. Now, if we consider the highest possible frequency to be 750 THz (beyond this, the wave will be UV ray which is not safe for most of the applications, i.e., health-care applications), the wavelength to be 4×10^{-7} , and the antenna size to be 100 nm, then the near-field region will be bounded by 5×10^{-8} m. The region bounded by 5×10^{-8} m actually vanishes inside the nano-antenna leaving it impossible to operate in the near-field. In addition, existing studies [85] also advocate for usage of far-field equation for nano-antennas. Therefore, we are using the far-field equation for nano-antennas.

4.7.2 Experimental Settings

We consider a homogeneous nanonetwork i.e., all nodes use the same type of nano-antennas. The coverage area of the network is $0.3 \times 0.001 \text{ m}^2$ in our simulation. At the beginning of the simulation, the nano nodes are distributed randomly over the area in a uniform manner. The nano nodes move at a speed of 0.2 m/s [57]. We randomly select a sender and a receiver among the nano nodes. The sender sends a packet of size 128 bytes, which is transferred to the receiver using Adhoc On-Demand Distance Vector (AODV) routing protocol. Note that, in this chapter, we focus on the network-level performance of nanonetworks for diversified applications such as nuclear, biological and chemical (NBC) defenses, damage detection systems, health monitoring systems, etc., rather than on the link-level performance over a pair of nodes as already studied in [57, 211]. Hence, we consider multi-hop routing (i.e., AODV) instead of one-hop case. Next, we use TCP as Transport layer protocol. The reason behind such choice: we consider THz Band communication among nanonodes and several real-life applications in diversified fields such as environment science [212], industrial development [212], and food science [156] of such communication introduce burst traffic into the network. These will introduce many challenges at the transport layer such as congestion control and end-to-end reliable transport. Therefore, we use TCP as a transport protocol to cope with the traffic dynamics utilizing its congestion control window mechanism. With these parameters, we compute the average of ten simulation runs each having a duration of 20 seconds operation. We consider three types of nano-antennas such as patch, dipole, and loop nano-antenna. Therefore, we need to set the parameters pertinent to these nano-antennas in our simulation. Besides, we know that nanonetworks generally operate over the THz band, hence, we set the frequency of nano-antennas to 1 THz. The values of antenna gains are set using the values generated from our numerical simulation for 1 THz for different nano-antennas using different materials. A successful data transmission in a nanonetwork happens if the received power by a receiving antenna is above a certain threshold. We consider the value of this threshold as 10% of the transmission power following the study presented in [57]. Furthermore, we use the equation of far-field [199] to compute the power received by the receiving nano-antenna. The values of different simulation parameters are described in Table 4.1. The values of different parameters are set based on the study

Parameter	Value	Parameter	Value
Simulation time (s)	20	Type of traffic	CBR
Area (m ²)	0.3 × 0.001	Tx power (dBnW)	2
Frequency (THz)	1	Rx power threshold (dBnW)	0.02
Packet size (bytes)	128	Bandwidth (MBps)	11

Table 4.1: Simulation parameters

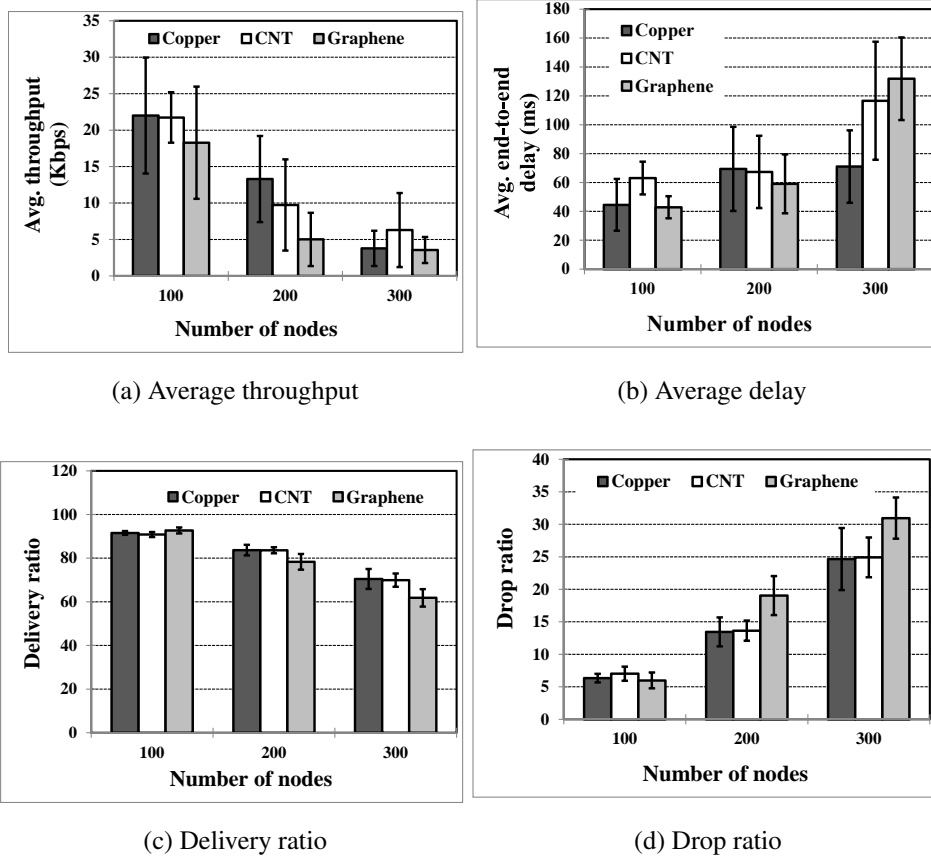


Figure 4.7: Impacts of variation in network size of nanonetworks using patch nano-antennas

presented in [213], [57]. Diversified real-life applications of nano-sensors such as nuclear, biological and chemical (NBC) defenses, damage detection systems, and health monitoring systems requires having a nanonetwork with a very large number of nano-sensor nodes. In order to evaluate the network-level performances of such nanonetworks using different nano-antennas in diverse settings, we vary network size i.e., the number of nano nodes. Next, we present experimental findings for the impacts of variation to the parameters.

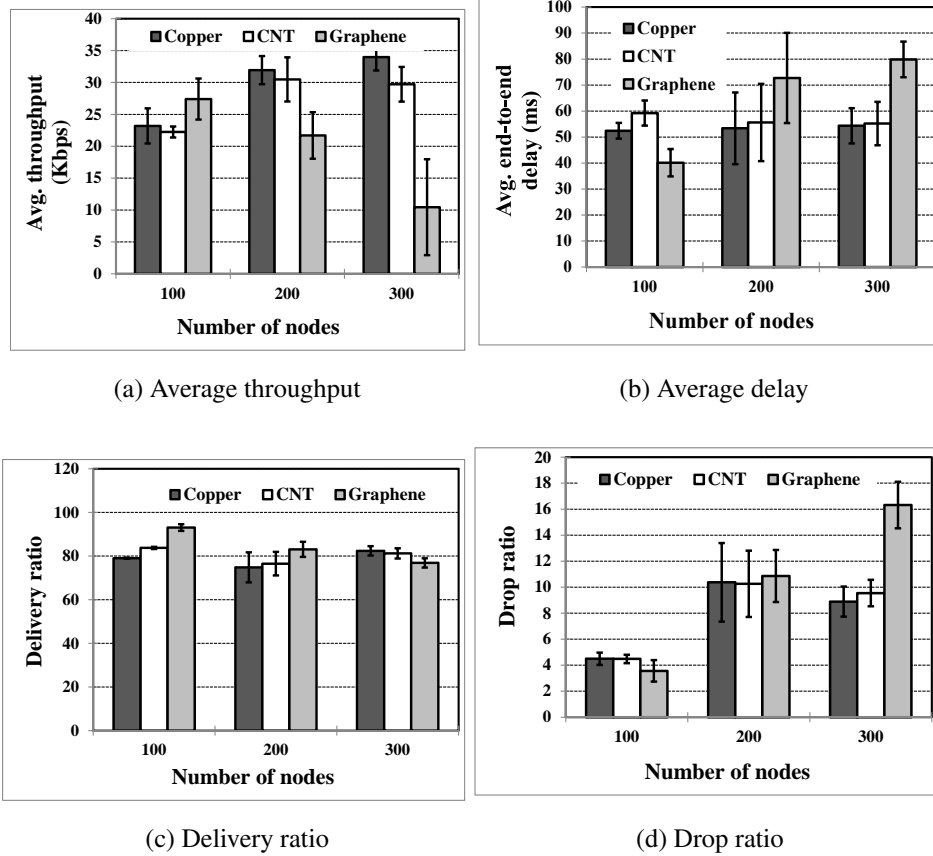


Figure 4.8: Impacts of variation in network size of nanonetworks using dipole nano-antennas

4.7.3 The Impact of Network Size

First, we perform network-level performances evaluation of nanonetworks in response to varying network sizes (i.e., the number of nano nodes). Fig. 4.7, Fig. 4.8, and Fig. 4.9 illustrate the impacts of variation in network size on different performance metrics while using patch, dipole, and loop nano-antennas respectively having different materials, i.e., copper, CNT, and graphene. Here, Fig. 4.8a demonstrates that the average throughput of a nanonetwork using dipole nano-antennas increases with an increase in the network size. However, the average throughput of the nanonetwork using patch and loop nano-antennas exhibit a decreasing trend with an increase in the number of nodes (Fig. 4.7a and Fig. 4.9a). Besides, the average throughput is higher for nanonetworks using copper as the antenna material compared to that using CNT and graphene.

Fig. 4.7b, Fig. 4.8b, and Fig. 4.9b present average end-to-end delay for patch, dipole and loop nano-antennas. These figures depict that the average delay increases with an increase in the network size. Besides, the superiority of dipole antennas using copper material is evident

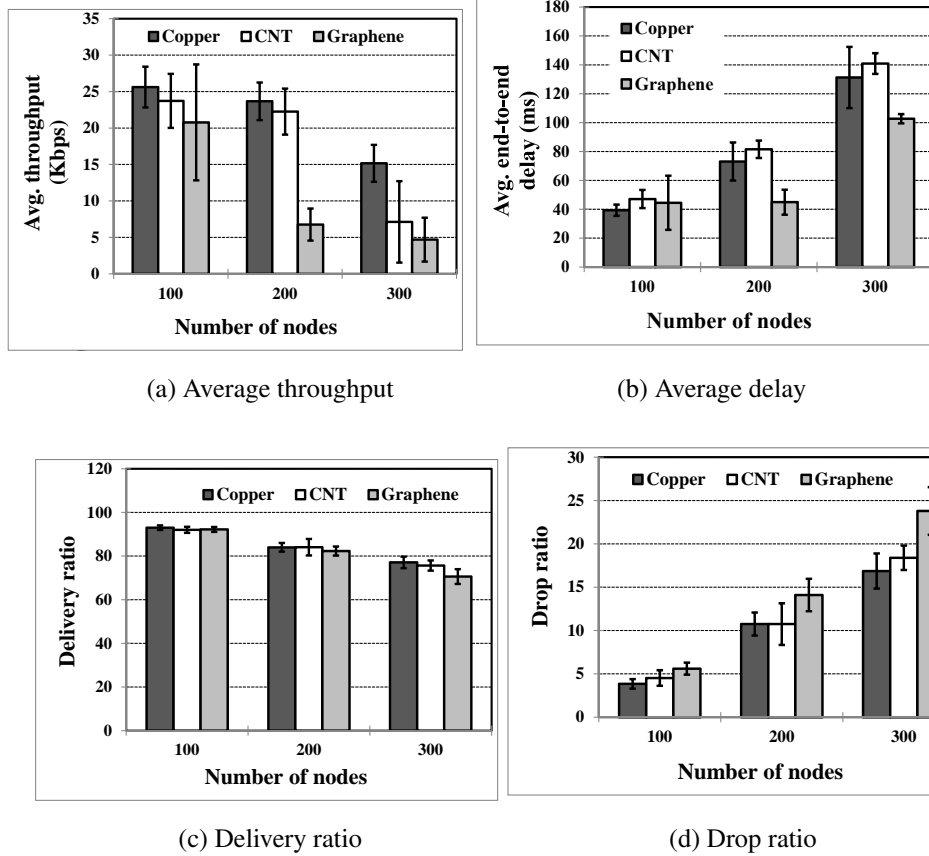


Figure 4.9: Impacts of variation in network size of nanonetworks using loop nano-antennas

compared to other nano-antennas from these figures.

Fig. 4.7c, Fig. 4.8c, and Fig. 4.9c show the delivery ratio for different types of nano-antennas. Here, all types of nano-antennas using different materials exhibit similar outcomes. Finally, Fig. 4.7d, Fig. 4.8d, and Fig. 4.9d delineate the drop ratio for patch, dipole, and loop nano-antennas. The drop ratio exhibits an increasing trend with an increase in the network size. Here, once again we find that dipole nano-antennas using copper material outperform other variations.

4.7.4 The Impact of the Traffic Rate

Fig. 4.10, Fig. 4.11, and Fig. 4.12 show the impact of variation in traffic rate in terms of packet injection rate over nanonetworks using patch, dipole, and loop nano-antennas. However, the performance metrics do not exhibit any particular trend with an increase in the packet rate. In response to the increase in packet rate, the average throughput, average delay, delivery ratio, and drop ratio for dipole antennas mostly degrade more compared to

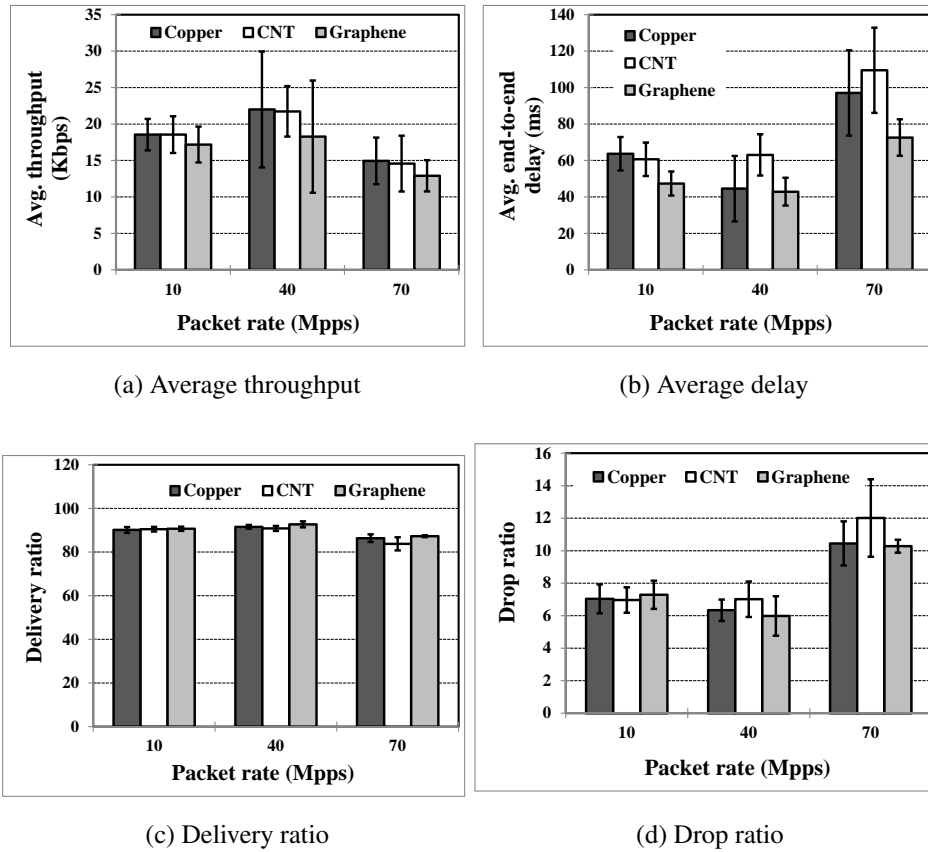


Figure 4.10: Impact of variation in the traffic rate of nanonetworks using patch nano-antennas

patch and loop nano-antennas. Moreover, graphene performs better than copper for dipole nano-antennas in case of having high packet rates. On the other hand, copper outperforms CNT and graphene for patch and loop nano-antenna.

4.7.5 The Impact of the Node Speed

Fig. 4.13, Fig. 4.14, and Fig. 4.15 present impacts of variation in speed of nano nodes. It is evident from these figures that for high speed of nano nodes the throughput for dipole antenna remains higher compared to that for patch and loop antenna. Furthermore, copper outperforms CNT and graphene for the high speeds. However, Fig. 4.13b, Fig. 4.13c, and Fig. 4.13d demonstrate better performance for patch nano-antenna compared to that for dipole antenna in terms of average delay, delivery ratio, and drop ratio respectively for high speed of nodes. Here, the performance using loop nano-antenna is quite similar to that using patch nano-antenna. Besides, copper exhibits better outcomes compared to that with CNT and graphene for all of the different types of antennas in response to a variation in the speed.

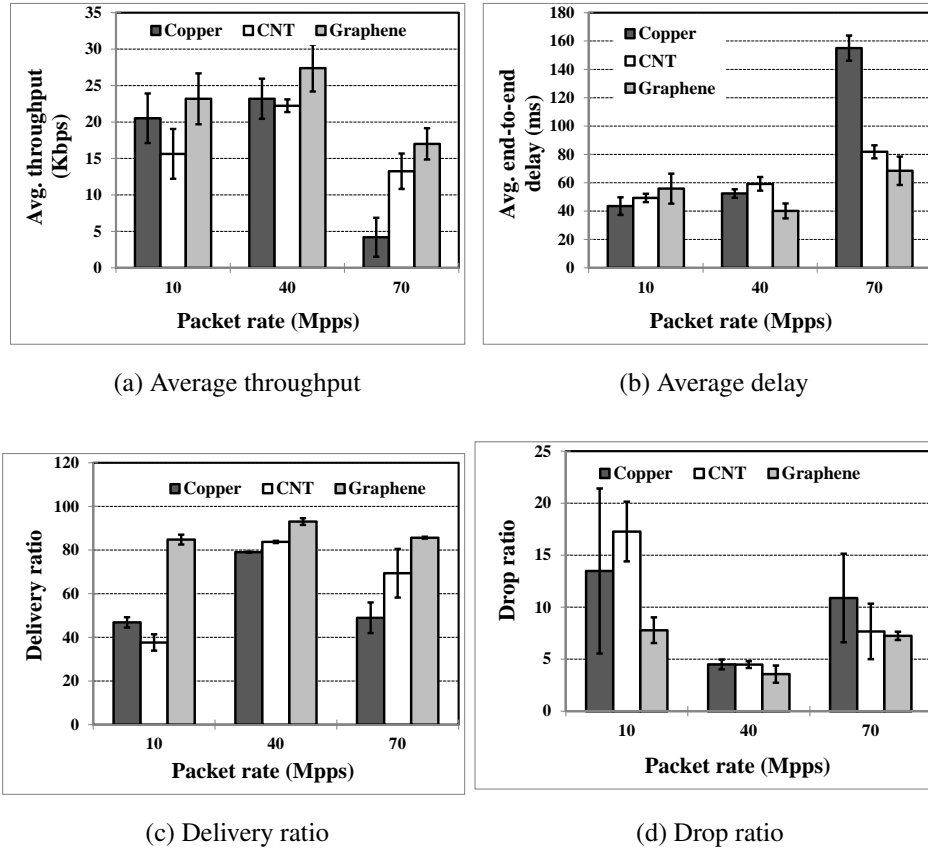


Figure 4.11: Impact of variation in traffic rate of nanonetworks using dipole nano-antennas

4.8 Summary of Findings

First, we perform the numerical simulation to analyze the gains of different types of nano-antennas using different types of materials. Later, we perform $ns-2$ simulation to evaluate the network-level performances of nanonetworks using different nano-antennas. The experiments clearly reveal the following findings:

- The numerical simulation confirms that the dipole nano-antenna exhibits better gain compared to that of patch and loop nano-antennas. In addition, numerical simulation demonstrates higher gains while using copper compared to that while using CNT and graphene.
- $ns-2$ simulation reveals that a nanonetwork comprising dipole antenna performs around 60% better for large-size nanonetworks.
- Consequently, $ns-2$ simulation reveals another finding that the average throughput for a nanonetwork using dipole nano-antennas increases with an increase in the network

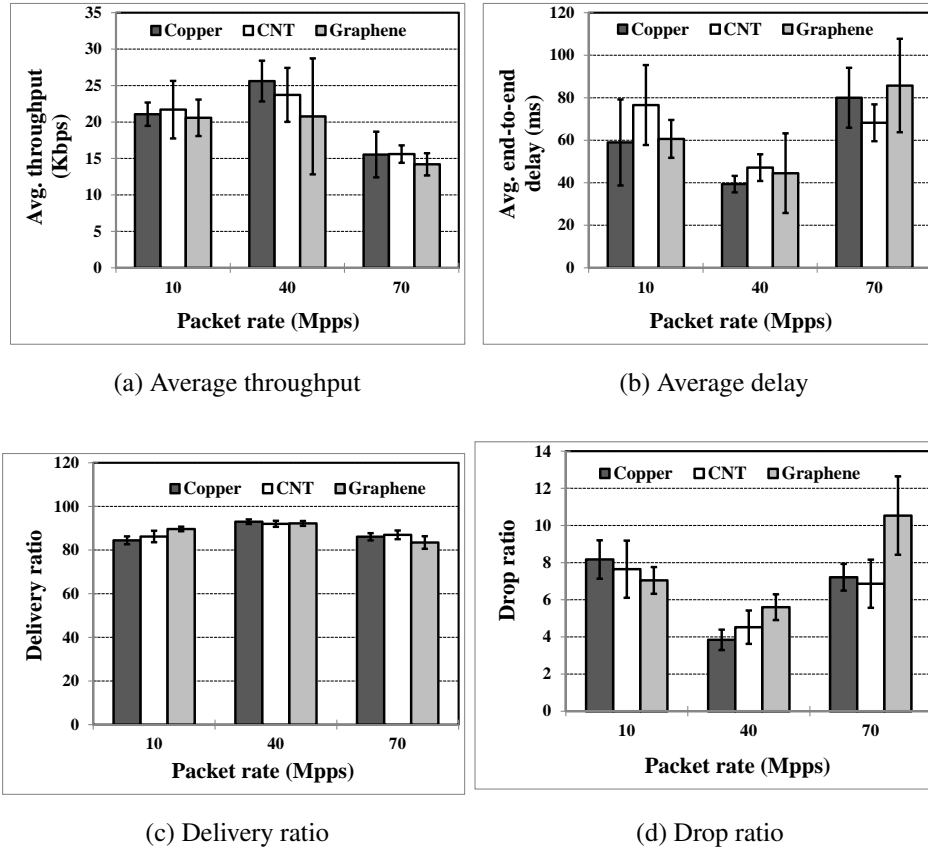


Figure 4.12: Impact of variation in the traffic rate of nanonetworks using loop nano-antennas

size. However, for patch and loop nano-antennas, the average throughput decreases with an increase in the size of the network. In case of large-size networks, dipole nano-antennas having higher gains can operate over longer range, and thus provide better performance. Nonetheless, patch nano-antennas outperform both dipole and loop nano-antennas for high traffic rate and high speed of nano nodes. These two contradictory outcomes can be explained through considering the transmission range as well as the extent of interference. In case of large-size networks, dipole nano-antennas having higher gains can operate over longer range, and thus provide better performance. However, the longer range backfires in case of high traffic rate or high mobility through increasing the extent of interference. Therefore, in such cases, the lowest gain option, i.e., the patch antennas perform the best.

- Furthermore, $ns-2$ simulation reveals that copper performs around 47% better compared to CNT and graphene irrespective of any type of nano-antennas. However, it is worth mentioning that copper might not be a feasible option to use for several

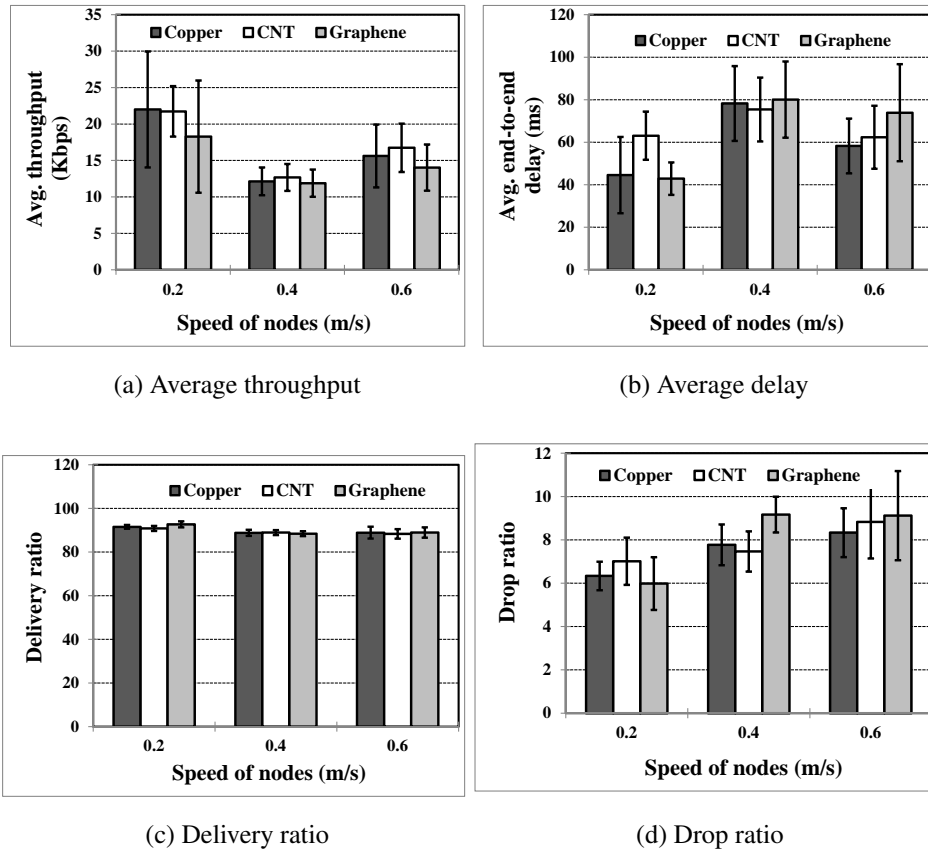


Figure 4.13: Impact of variation in speed of nodes in nanonetworks using patch nano-antennas

bio-medical applications such as immune support systems [214], drug delivery systems [215], health monitoring systems [216], etc., which generally demand implantation of nano devices within a living body. This happens as copper is generally known to be reactive while implanted within a living body [217]. Nonetheless, copper could be used for other applications such as bio-weapons [218], water quality control [219], etc., due to not having any such reactive impact for these cases.

- Finally, a dipole nano-antenna using copper material exhibits around 51% better throughput and about 33% better end to end delay compared to other alternatives.

4.9 Conclusion

Wireless nanonetworks are expected to be used in a myriad of diversified contemporary and future applications. Successful exploitation of wireless nanonetworks in the applications demands a careful investigation on components of nano nodes and architectures of nanonet-

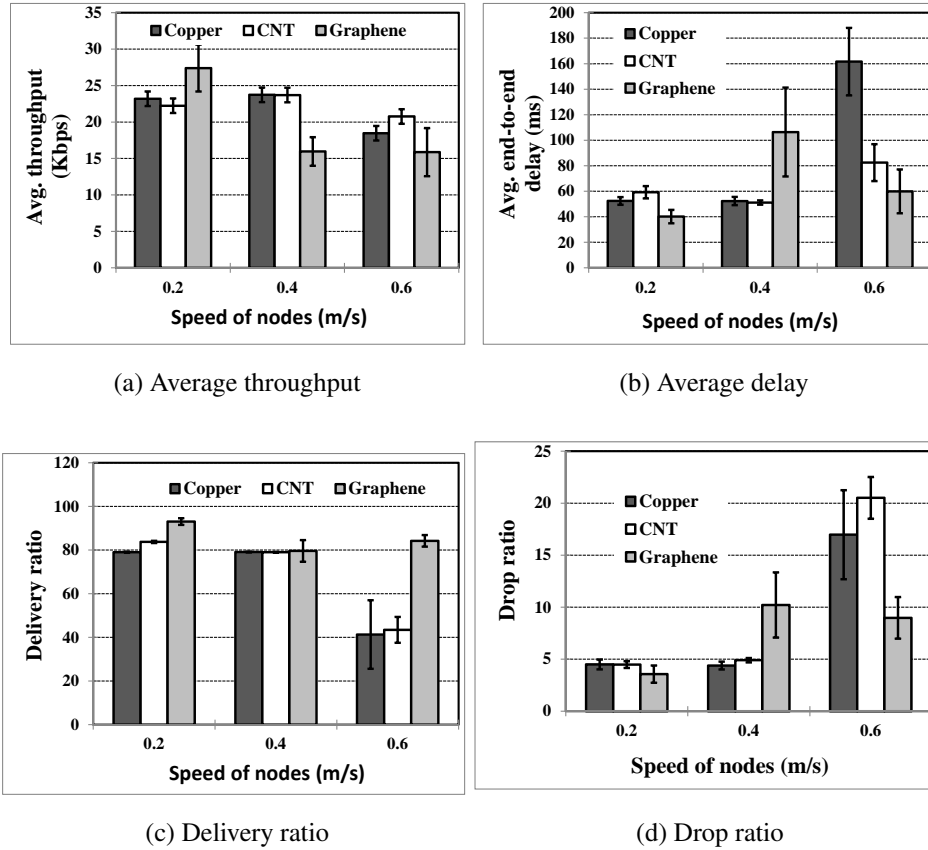
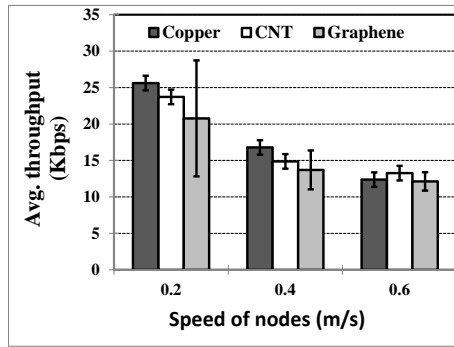


Figure 4.14: Impact of variation in speed of nodes in nanonetworks using dipole nano-antennas

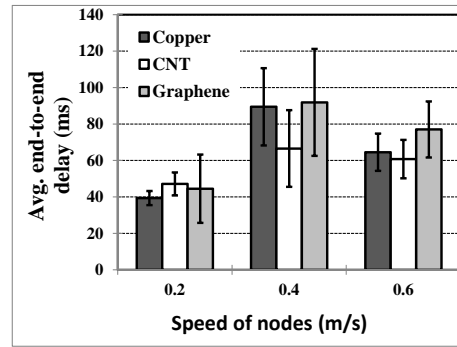
works. However, it is a very challenging and unexplored research field since there remain vacancies in the literature in findings suitable components of nano nodes. One of the key components of a wireless nano node is gain-efficient nano-antenna. Therefore, in this work, we perform an antenna-centric network-level performance analysis for the wireless nanonetworks. Our analysis offers a basis for finding a suitable nano-antenna from its several alternatives. Here, we find that the dipole nano-antennas perform better for large-size wireless nanonetworks. However, for high data transmission rate and for high speed of nano nodes, patch nano-antennas outperform the dipole and loop nano-antennas.

Moreover, we also find that antenna gains vary with the change in material used in nano-antennas. The numerical simulation using our analytical models validate this claim. Furthermore, we implement our models in a widely-used network simulator ns-2. Our simulation results demonstrate that the nano-antennas using copper perform better compared to other alternative materials such as CNT and graphene.

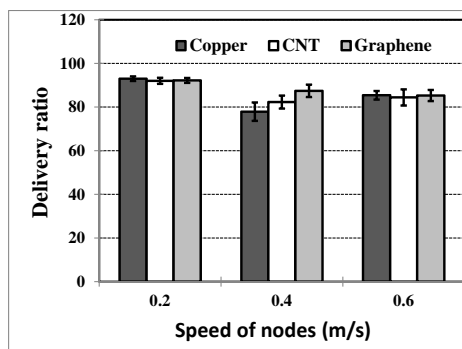
In the next chapter, we focus on another example of miniature versions of limited-



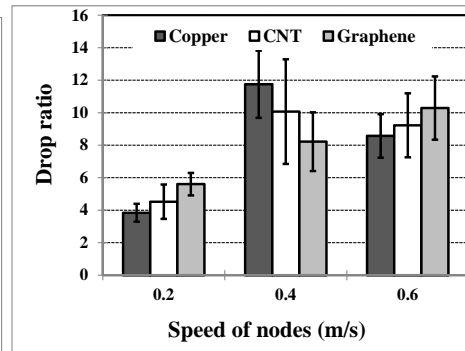
(a) Average throughput



(b) Average delay



(c) Delivery ratio



(d) Drop ratio

Figure 4.15: Impact of variation in speed of nodes in nanonetworks using loop nano-antennas

resource cyber-physical networks, i.e., medical body area networks.

Chapter 5

Power Attack: An Emerging Threat in Health-care Applications Using Medical Body Area Networks

5.1 Introduction

Aging population is one of the most monumental demographic facts that has come to the foreground in the 21st century. The world aging population is increasing rigorously with an increase in life expectancy of people. For example, the number of world aged people was about 200 millions in 1950, which is projected to be increased to about 1.8 billions (20% of the total world population) within 2050 [220]. Even in developing countries such as Bangladesh, the number of aged people is projected to increase from about 9.77 millions in 2011 to 44.10 millions by 2050 [221]. Older populations are more likely to be affected by chronic diseases. Therefore, the aging population and the rise of chronic diseases are placing increasing pressure on the cost of providing health care. For example, expenditure on health and aged care is expected to rise from 9% to 12.4% of GDP [222] in developed countries and this expenditure is about 3.8% of GDP [223] in developing countries. A full-fledged medical body area network health monitoring system is considered to be a potential solution for this upcoming challenges in health-care system.

Medical Body Area Networks (MBAN) is a special type of networks composed of low-

power wearable or implanted wireless medical sensor devices. Such a network facilitates ubiquitous health-care services for patient management such as remote patient monitoring, disability management, emergency medical response system (EMRS), and even promoting healthy living styles. MBANs can be used to monitor vital body signs such as heart rate, temperature, blood pressure, electrocardiogram (ECG), electroencephalogram (EEG) and pH level of patients. Furthermore, MBANs provide more comfortable ways to monitor a patient, both in and outside the hospital environment.

The implementations of MBANs are still in embryonic state. Unfortunately, the development of MBANs even in this state is being hindered by various security threats. Eavesdropping [59], data modification, impersonation attack [60], and denial of service attack [61] are some of the current popular security threats of MBANs. Most of the existing research studies [62–65] mainly focus on finding effective countermeasures of these attacks. However, a new attack can easily be introduced via exploitation of vulnerabilities of the system pertinent to power constraint of sensor nodes in MBANs.

Most of the sensor nodes of MBANs are powered by micro batteries that limit system energy resources. Furthermore, not all the sensor nodes are equally power hungry. Therefore, when sensor nodes in MBANs perform data forwarding too frequently, these nodes generate power spikes at different levels leading to energy depletion of batteries of those nodes. These characteristics make MBANs vulnerable to battery drain attacks. Exploiting this vulnerability, we introduce a new attack named Power Attack, where a malicious node forces a sensor device to deplete energy more drastically and eventually causes the sensor node to die off due to lack of power. The ultimate goal of a power attack is to interrupt or terminate ongoing communication among sensor nodes inside a victim body as well as communication with the remote service provider. Furthermore, an attacker can perform power attack without being noticed by the victim. However, note that, it will not be possible to induce a power attack for a few sensors such as ICD (implantable cardiac defibrillator) without being noticed by the victim as such sensor nodes generate shock in the body of the victim while performing sensing and data transmission.

The outcome of power attack in MBANs is twofold: the victim fails to transmit necessary real-time data and the remote service provider generates false alarm service. Such damage

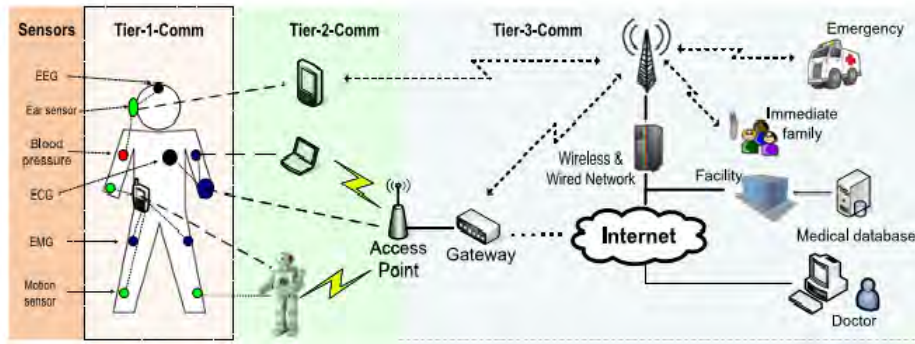


Figure 5.1: Architecture of a medical body area network [6]

leads to health hazards, which could be even life threatening. The power attack also forces the sensor device to die off which may damage the sensor nodes leading to monetary loss.

The term Power Attack was actually first introduced in [224] for cloud environment. Here, the feasibility of launching power attacks in three main-stream cloud service business models, namely platform as a service (PaaS), infrastructure as a service (IaaS), and software as a service (SaaS), were investigated. However, we will not be able use these existing attack models directly in MBANs due to the divergence of hardware implementation of sensor nodes compared to cloud environment. Hence, we need to design our own attack model for power attack in MBANs, which remain still unexplored in the literature to the best of our knowledge.

The contributions of this chapter are follows:

- We introduce attack models for an emerging security threat i.e., power attack in health-care applications using MBANs.
- Next, we analyze the viability of launching a power attack in reality using `Mannasim` simulator which extends popular `ns-2` simulator.
- Then, we devise a lightweight counter measure for the power attack.
- Finally, we demonstrate the efficacy of our proposed counter measure using empirical evaluation by `Mannasim`.

5.2 Background on MBANs

MBANs enable networks over low-power wearable or implanted wireless medical sensor devices. ECG, EEG, EMG, motion sensors, and blood pressure sensors are few examples of well known wearable medical sensor devices. On the other hand, implanted devices are sensors that are swallowed for short-term monitoring or placed in the body during surgery to monitor physical parameters during and after the healing process. Fig. 5.1 demonstrates a general architecture of a MBAN. The architecture is divided into three components: Tier-1-Comm, Tier-2-Comm, and Tier-3-Comm. Tier-1-Comm consists of several sensor devices such as ECG, EEG, EMG, blood pressure sensor, and motion sensor along with a personal server. The sensors transmit patient data to the personal device. Then, through a Bluetooth/WLAN connection, these data are sent to nearby access points (Tier-2-Comm). Finally, in Tier-3-Comm, these data are streamed remotely (can be over Internet) to a medical doctor site for ubiquitous health monitoring, to a medical database for record keeping, or to the corresponding equipment that issues an emergency alert.

In this chapter, we mainly focus on Tier-1-Comm. There are four different architectures available for Tier-1-Comm. Fig. 5.2 illustrates the four different architectures namely wired, wireless, cluster and wired, and cluster and wireless. In wired architecture, all the sensor nodes are connected with a personal server via cables (Fig. 5.2a). Existing health-care applications such as SMART [225] and MITHril [226] deploy this architecture. Fig. 5.2b depicts a typical wireless architecture utilizing a star topology. Here, multiple sensors forward body signals to a personal server, and then the accumulated data is forwarded to an access point. WiMoCa [227] deploys this architecture.

Finally, Fig. 5.2c and Fig. 5.2d illustrate advance architectures. In these architectures, multiple wired or wireless sensors are connected to a single central processor and the central processor transmits the accumulated data to the personal server. Such introduction of the central processor reduces the amount of raw data that needs to be transmitted to the personal server and saves the overall power of lowpowered sensor devices. Irrespective of the choice of architecture, the sensor nodes are generally equipped with a small amount of power. Next, we introduce a new attack entitled power attack exploiting the scarcity of power in sensors.

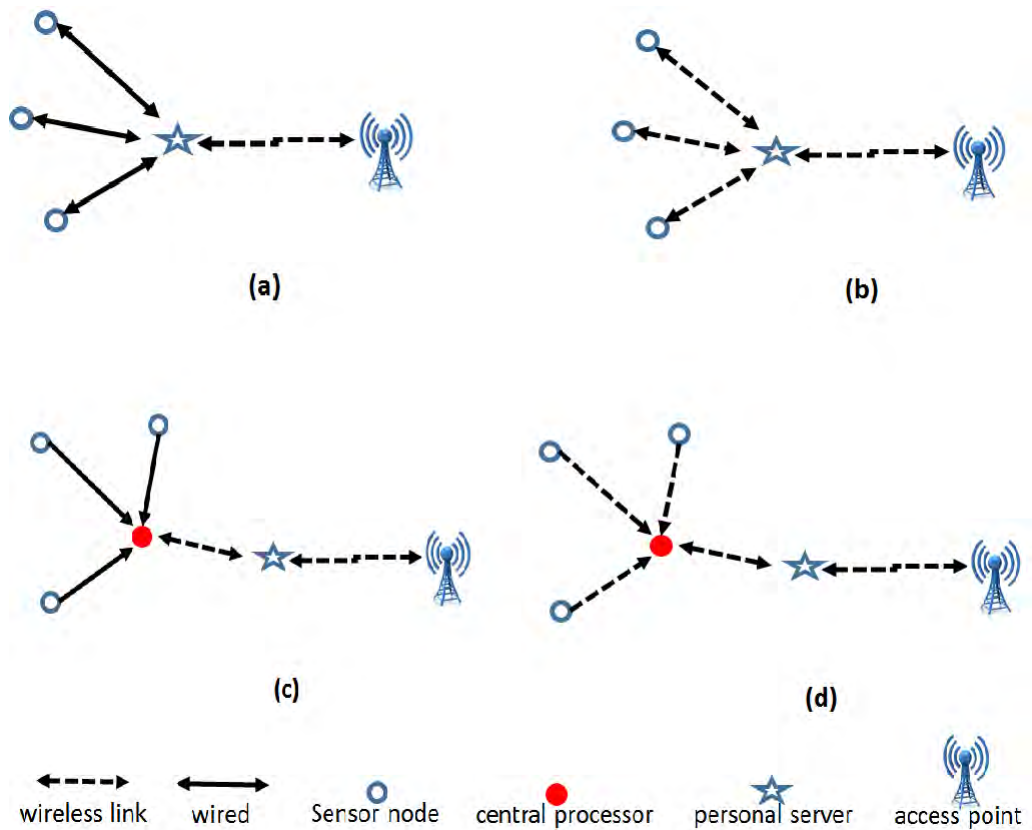


Figure 5.2: Architecture of Tier-1-Comm: a) wired; b) wireless; c) cluster and wired; and d) cluster and wireless

5.3 Power Attack and Attack Models

In this section, we introduce our proposed security threat (power attack) in health-care applications such as ubiquitous health monitoring, computer-assisted rehabilitation for elderly people, emergency medical response system, and promoting healthy living styles for disabled people. These health-care applications are generally deployed using MBANs. Most of MBAN devices are powered by micro-batteries, which limit the storage of system energy resources. Such batteries may not even be replaceable in cases where the devices are implanted in a living body. Exploiting this vulnerability, we can introduce an attack named power attack that causes a sensor device to reduce power more drastically. However, in order to guarantee better life-times of micro-batteries, a sensor node can perform one-way communication. In such cases, power attack cannot be performed. Therefore, we mainly focus on MBANs where both-way communication is permitted.

In general, the term power attack is defined as simultaneous occurrence of power peaks

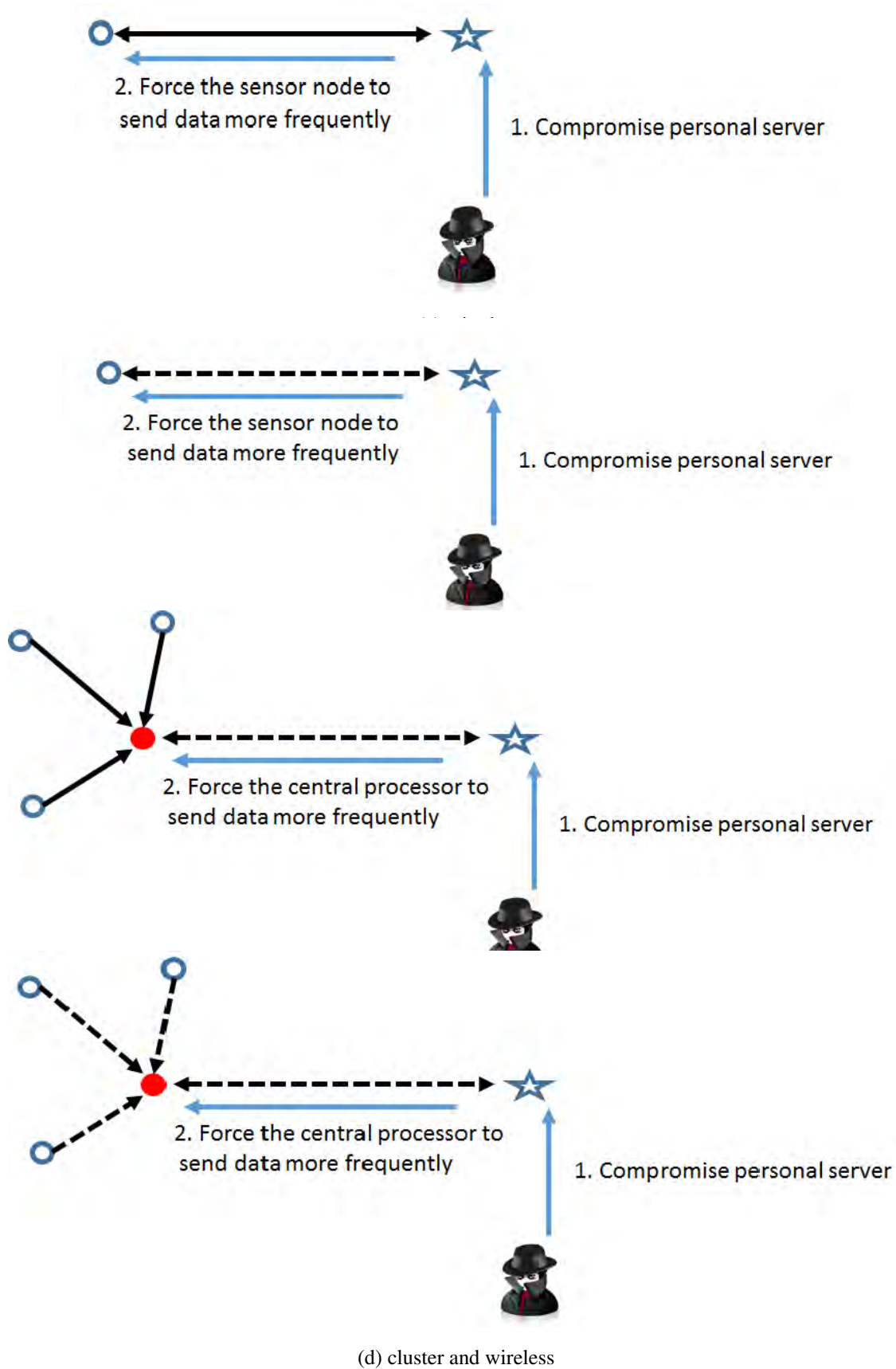


Figure 5.3: Attack models of power attack for different architectures

that produce overloading of electrical circuits of a device and then trigger the trip of circuit breakers (CBs) of power facilities, leading to undesired power outages [224]. However, in case of MBANs, this definition is not directly applicable. Since, most of the sensors of MBANs are powered by micro-batteries, there are no circuit breakers that can be tripped off due to power overload. Therefore, to generate a power attack, we have to drain out the energy of batteries, which will in turn force a sensor device to die off due having shortage of power. Sensor devices require energy for data collection, processing, and transmission. Hence, if we force a sensor device to disseminate data more frequently than usual, then the batteries will consume more energy, which will eventually force the batteries to drain out quickly. Based on this idea, we develop attack models for different architectures of MBANs as presented in Fig. 5.6.

Fig. 5.3 illustrates attack models of power attack for different architectures. In our attack model, an attacker compromises the personal server of an MBAN. An attacker can compromise the personal server via Internet. Personal server envisions remote software updates. An attacker can manage to manipulate this software update. Moreover, an attacker can simply go to the room where a patient is and wait for the chance to physically compromise a local server. Then, after compromising the personal server, an attacker forces either the sensor devices (Fig. 5.3a and Fig. 5.3b) or the central processor (Fig. 5.3c and Fig. 5.3d) to disseminate sensed or processed data more frequently than usual. Such frequent dissemination of data will consume more energy and eventually will cause a sensor node to die off owing to its scarcity of power.

Next, we assess the viability of launching a power attack using simulator.

5.4 Viability Analysis of Power Attack

In this section we assess the viability of launching a power attack in the medical body area networks using empirical evaluation. In order to do so, we need to examine the type of the sensor node consumes more energy while sensing and processing, which will eventually increase the overall energy consumption. Besides, we also need to explore the impacts of the number of sensor nodes on the consumption of overall energy. These knowledge will help us

to launch the power attack effectively. Therefore, we perform extensive empirical simulation resembling real deployment to examine the viability of power attack.

In order to perform empirical evaluation we use `Mannasim`, a simulator for wireless sensor network that extends `ns-2` simulator. Since most of the sensor nodes in MBANs are powered by battery the existing energy mode `EnergyModel` in `ns-2` failed to resemble sophisticated models for energy depletion in the real world. Moreover, for sensor nodes, we need to know the energy consumption for sensing and processing the data instead of transmission and reception energy. `Mannasim` contains a battery model resembling real deployment of sensor nodes.

5.4.1 Mannasim Simulator

`Mannasim` provides couple of classes that extends the classes of `ns-2`. A `Battery` class extends the `EnergyModel` of `ns-2`. It can be used to implement different existing battery models. It provides methods like turning sensor node on and off, it can put it into a sleep mode and it can decrease energy when the sensor performs sensing, processing or disseminating. There is a class entitle `SensorBaseApp` and its children `CommonNodeApp` and `ClusterHeadApp` are classes that represent different applications for wireless sensor network.

5.4.2 Simulation Setup

We construct a scenario comprising a personal server and several types of sensor nodes such as such as ECG, EEG, blood pressure, motion sensor, and hearing sensor (Fig. 5.6a and Fig. 5.6b). Here, the sensor nodes sense and process data and communicate with the personal server. On the other hand the personal server only transmits and receives data, it does not perform any sensing and processing. We analyze the sensing, processing, transmission, and reception energy consumption for the system. Here, we use different types of bio-sensor nodes for different physiological signal such as blood flow, ECG signal, respiratory rate, nerve potential, blood pressure, and body temperature. The corresponding data rates and parameter value range are selected based on [228] shown in Table 5.1.

We run the entire simulation for 50 seconds and we take the average of 10 runs.

Bio-sensors	Data interval (s)	Sensing interval (s)	Parameter ranges
Blood flow	0.025	0.0001	1-300ml/s
ECG signal	0.002	0.001	0.5-4mV
Nerve potential	0.00005	0.0001	0.01-3mV
Respiratory rate	0.05	0.03	2-50breaths/min
Blood pressure	0.01	0.005	10-400mm/Hg
Body temperature	5	10	32-40C

Table 5.1: Data rates of different bio-sensors

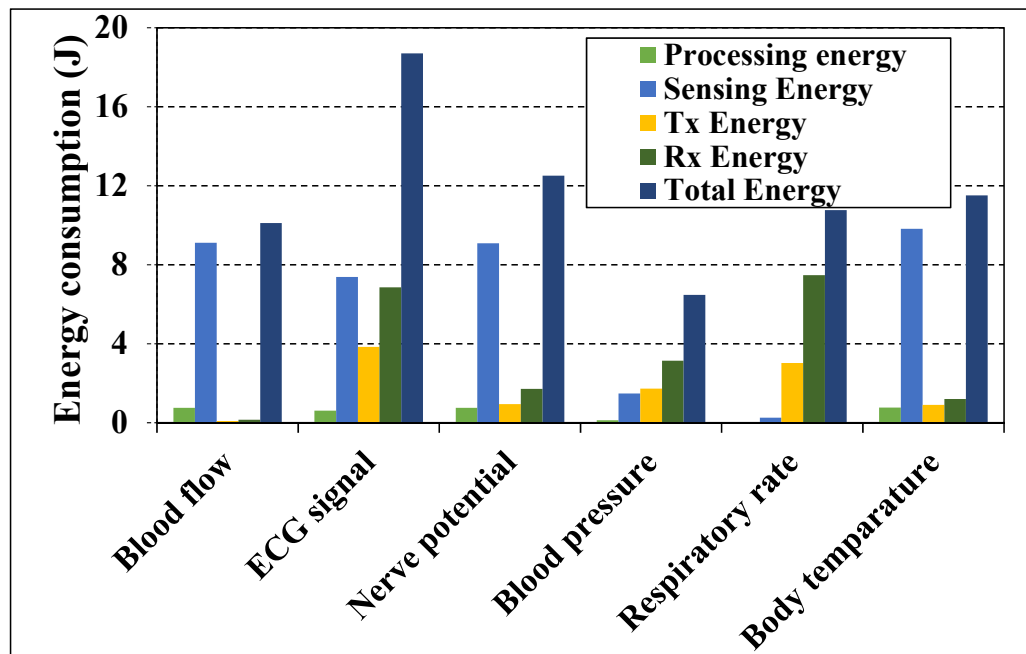


Figure 5.4: Impact of data types on energy consumption of MBANs

5.4.3 Impacts of Diverse Types of Data on Energy Consumption

We evaluate the impacts of different types of data on the energy consumption. Fig. 5.4 exhibits sensing, processing, transmission, reception, and total energy consumption for different types of data. such as blood flow, ECG signal, nerve potential, respiratory rate, blood pressure, and body temperature collected from diverse bio-sensors such as ECG, EEG, blood pressure, motion sensor, etc.

Fig. 5.4 shows that the sensors for blood flow, nerve potential, and body temperature consume more energy for sensing. However, even though ECG signal data consume less sensing energy compared to them, the over all energy consumption is high for ECG signal.

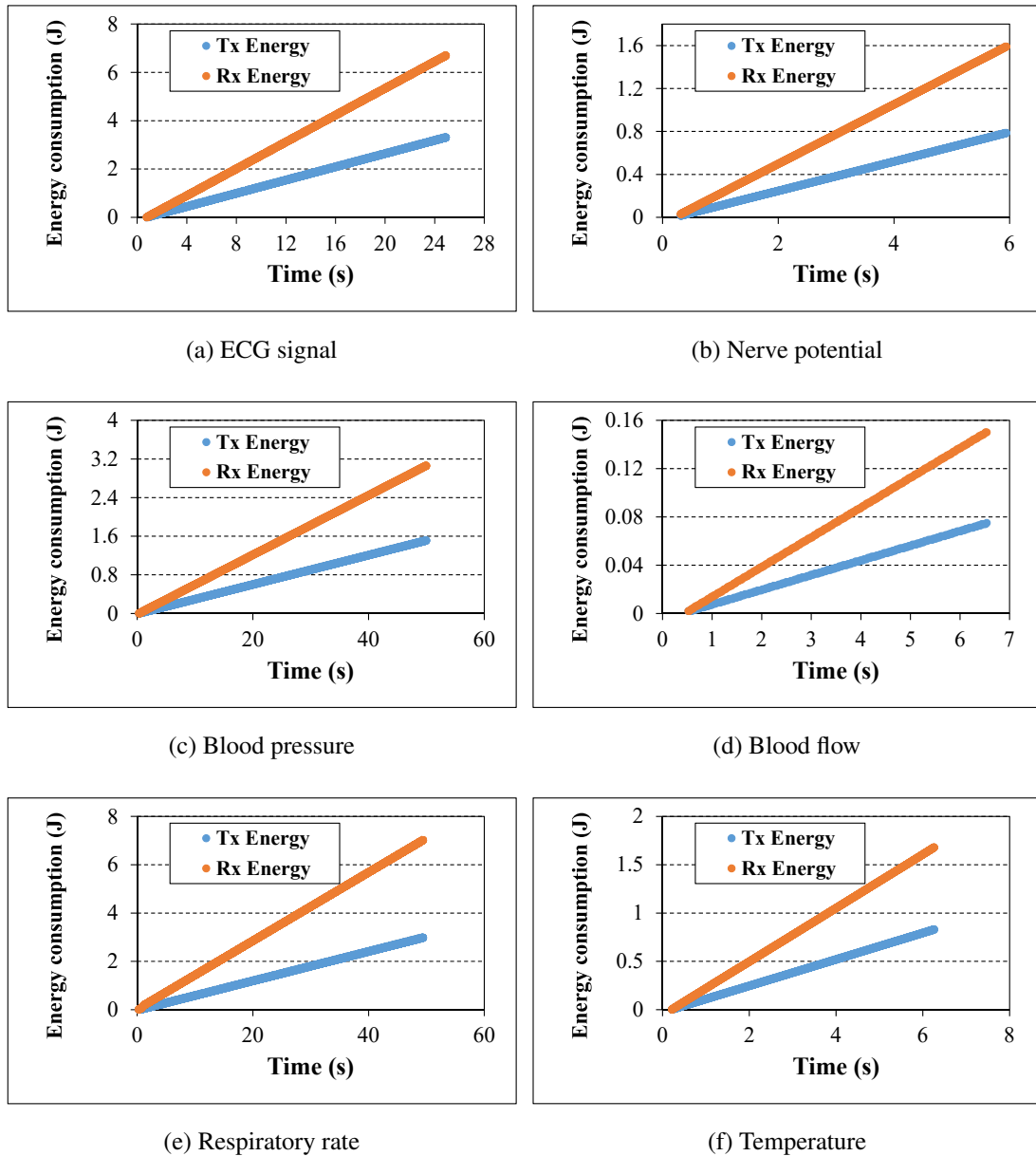


Figure 5.5: Impact of different types of data on energy consumption of personal server

ECG signal consumes more energy while transmitting and receiving data, the over all energy consumption increases in case of ECG signal.

Next, we explore instantaneous energy consumption of the personal server for different data types. Fig. 5.5 reveals that the personal server consumes more energy for data of ECG signal and respiratory rate.

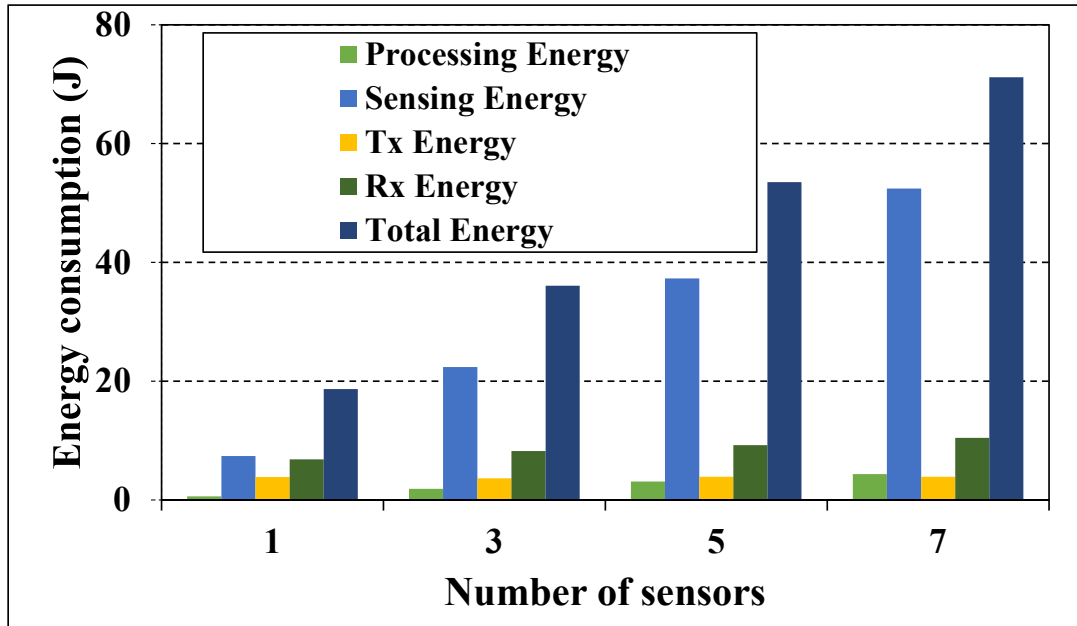


Figure 5.6: Impact of variation in number of sensor nodes on energy consumption of MBANs

5.4.4 Impact of Variation in Number of Sensor Nodes on Energy Consumption

Here, we evaluate the impact of different number of sensor nodes on the energy consumption of MBANs. Since from our previous evaluation, we found that ECG signal consumes more energy, now we vary the number of ECG signal generator sensor nodes to illustrate the impact of number of sensor nodes on energy consumption. We vary the number of sensor nodes 1, 3, 5, and 7 (Fig. 5.6). Fig. 5.6 exhibits that the over all energy consumption increases with an increase in the number of nodes.

5.4.5 Impact of Variation in Simulation Time on Energy Consumption

We demonstrate the impacts of different simulation time on the energy consumption of MBANS in Fig. 5.7 for 10s, 30s, 50s, and 70s. Fig. 5.7 depicts that the sensing energy increases with an increase in the simulation time. Therefore, the overall energy consumption increases with an increase in simulation time.

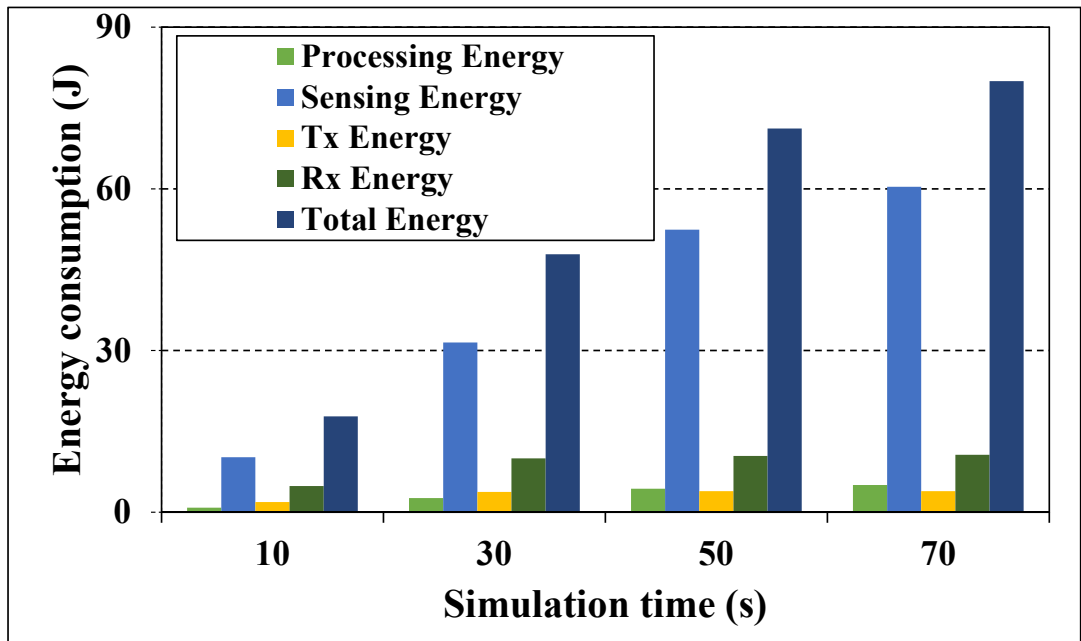


Figure 5.7: Impact of variation in simulation time on energy consumption of MBANs

5.4.6 Simulation Findings

We could summarize the findings of our simulation as follows: 1) sensors used for sensing ECG signal consume more energy compared to other types of bio-sensors. Moreover, the energy consumption of the personal server also increases during the communication with ECG sensor, 2) the over all energy consumption increases noticeably with the increase in the number of sensor nodes, and 3) finally, the over all energy consumption of sensor nodes increase if we continue sensing for longer period.

From the simulation results, we could conclude that to perform a power attack more effectively, an attacker needs to force the sensor to sense and process ECG signal for a longer period of time. These will eventually increase the over all energy consumption of the system and cause either the sensor node or the server point to die off more frequently.

Since our evaluation reveals that ECG sensor is a potential attack vector for power attack. Therefore, next, we envision to devise a lightweight countermeasure for ECG sensor device.

5.5 Countermeasure of Power Attack

Being highly resource constrained, complex, and resource intensive countermeasures cannot be implemented in MBANs. Therefore, in this section, we propose a simple countermeasure

specifically focusing on ECG sensor device of MBANs.

In general, to detect an anomaly in heart rate a minimum number of heart cycles are required for analysis. More specifically, at least 3 cycles are required for analysis of heart diseases [229,230]. The average heart cycle is typically 0.7 - 8 seconds, therefore, we need a recording time of 2.56 seconds for at least 3 cardiac cycles [229]. We utilize this information to develop our counter measure for power attack.

For our attack, a compromised personal server will make request to either a sensor node or a central processor to disseminate data more frequently having shorter time as interval. Hence, if the time interval between two consecutive requests of compromised personal server is less than the minimum recording time (i.e., 2.56 seconds), a ECG sensor prohibits sending data to the personal server. Since the ECG sensor is not responding to the requests that are made within the specified time interval, the overall energy consumption will be reduced. Thus, we can avoid power attack. In order to illustrate efficacy of this proposed countermeasure, we perform simulation resembling a real deployment.

Next, to illustrate the efficacy of our proposed countermeasure, we perform extensive empirical simulation resembling real deployment using *Mannasim* simulator.

5.6 Experimental Evaluation

In this section, we demonstrate the efficacy of our proposed counter measure using empirical evaluation. In order to perform empirical evaluation we use *Mannasim*.

5.6.1 Simulation Setup

We construct a simulation scenario based on the scenario presented in the study [231]. Here, an attacker compromises the personal server for sending malicious data extraction commands to ECG sensor node. These commands are intended to trigger ECG sensor node to unnecessarily transmit sensed data resulting in depletion of its battery. The values of different parameters for ECG sensor such as sensing interval and the ranges of ECG data are set based on values presented in [228]. We consider an ECG sensor that uses one 130 mAh AA battery as its power source. Besides, we set the initial energy, sensing, processing, and disseminating

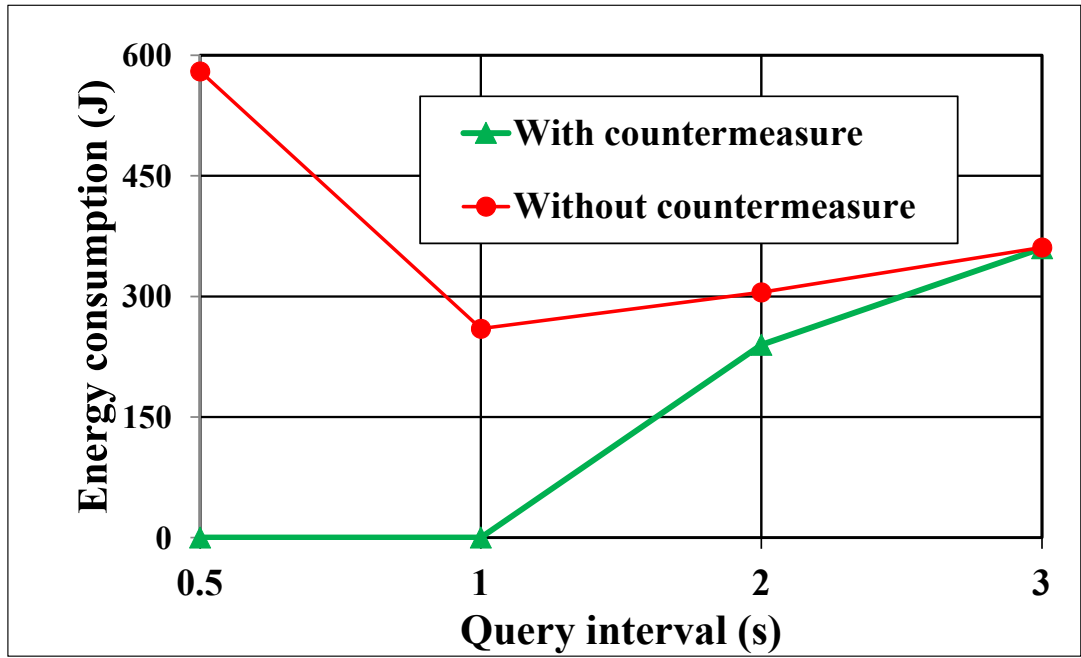


Figure 5.8: Energy consumption of ECG sensor at different query interval

power of the ECG sensor based on values presented in [232,233]. As per our proposed attack model, a compromised personal server unnecessarily injects query to ECG sensor and then ECG sensor sends data to the personal server forming a two-way communication. Hence, the energy consumption of ECG sensor is under our consideration as it is powered by in-built battery. Therefore, in our simulation, we evaluate the impact of different query intervals on the energy consumption of ECG sensor.

5.6.2 Simulation Results

Fig. 5.8 demonstrates the energy consumption of a ECG sensor at different query intervals with and without our proposed countermeasure. Since, our countermeasure prohibits ECG sensor to disseminate data for the query interval less than 2.5 seconds, the energy consumption of the ECG sensor with a countermeasure is very low at query interval 0.5, 1, and 2 seconds compared to the energy consumption without any countermeasure. These results delineate the efficacy of our proposed countermeasure.

5.7 Conclusion

Recent advancement in diverse health-care applications owing to the proliferation of sensor devices opens a door for different security threats in MBANs. In this chapter, we introduce power attack that presents a security threat exploiting power constraint of sensor devices. We develop attack models of power attack for different architectures of MBANs. Then, we assess the viability of launching the power attack. Next, we devise a lightweight countermeasure for power attack. Finally, we demonstrate the efficacy of our proposed countermeasure using experimental evaluation. Next, we shift our focus to the final part of our thesis, which comprises the smarter versions of limited-resource cyber-physical networks.

Part III

Smarter Versions of Limited-Resource Cyber-Physical Networks

Chapter 6

General-Purpose Multi-Objective

Vertical Hand-off Mechanism Exploiting

Network Dynamics for mobile devices

6.1 Introduction

The recent boost in simultaneous use of multiple networking interfaces in diversified mobile devices, such as smartphone, tablet, etc., accelerates the rapid adoption of various types of wireless network technologies such as WiFi, WiMAX, UMTS, LTE, and Bluetooth. This adoption in turns yields the pervasiveness of wireless signals all over the world. Fig. 6.1 shows a sample of various types of wireless network signals with different relative signal strengths present in our university premises. The figure reveals that several networks are available in nearby places, exhibiting varying signal strengths.

The pervasiveness of various wireless networks with varying signal strengths and network-level parameters, makes it difficult to use these networks in a dynamic and integrated way from a single device. This is because no single wireless network technology performs better in all the criteria. Each technology performs better in one or more criteria while worse in the other criteria. For example, UMTS has a larger coverage area but lower bandwidth. On the other hand, WiFi has limited coverage area but higher bandwidth. Each of these network technologies also exhibit highly dynamic behaviour in the presence of the

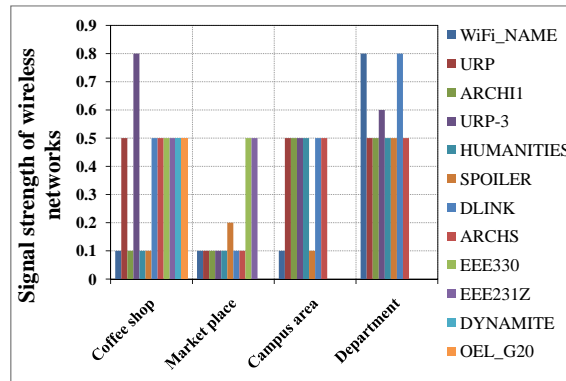


Figure 6.1: Relative signal strengths of different wireless networks available in nearby public places of a university premise

others, i.e., in their co-deployment. Moreover, multi-interface devices often face resource constraints. For these reasons, maintaining network connectivity over multiple diverse networks from a multi-interface device is a real challenge. It demands the device capability to support multi-objective vertical handoff, to deal with the network dynamics that exhibits in any co-deployment of heterogenous wireless networks, and to deal with the resource constraint of the device itself.

The mechanism of maintaining connectivity over diverse networks through switching off from one network and switching on to another network is called hand-off (HO). Hand-off that is performed over heterogeneous wireless networks (i.e., networks having different physical and link layer technologies) is known as vertical hand-off. Fig. 6.2 exhibits an example scenario of a vertical hand-off. The vertical hand-off mechanism has three consecutive phases: initiation phase, decision phase, and execution phase. The first phase selects the decision parameters. The second phase chooses the best network based on the selected parameters. The last phase establishes a connection with the chosen network.

In this chapter, we mainly focus on the second phase, i.e., on the task of choosing the best network, of vertical hand-off, which is known to be an NP-Hard problem [234]. Several research studies [71–73, 235–237] have proposed solutions to this problem. Most of these

studies have chosen the best network using different network parameters in isolation. They have mainly uses received signal strength (RSS) [235, 236]. Bandwidth and monetary cost are also used along with RSS in a few studies [238, 239].

Statistical data [240] exhibits that around two billion people are currently using mobile devices and different Internet services through their devices. Therefore, it is difficult to make all of them satisfied by choosing the network using a single criterion for all of their Internet services. Hence, the need to develop a general-purpose multi-objective best-network selection mechanism for vertical handoff has emerged.

Recently, a few multi-objective decision making mechanisms such as Grey Relational Analysis (GRA) [71], Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) [72], and Simple Additive Weighting (SAW) [73] have been proposed for selecting a best network during vertical hand-off. These mechanisms although uses different network parameters, such as data rate, delay, SINR, etc., together to choose the best network, they use a fixed value for each of these parameters. The values of these parameters, however, do not remain fixed in the presence of different environmental factors, other users, and other wireless networks and the variation depends on the number of co-users, on the number of co-networks, and on the environmental factors. We refer this phenomenon as the *Network dynamics* of wireless networks.

Fixed value usage of network parameters lacks the resemblance of the real deployments of the heterogenous wireless networks. The use of network dynamicity in all network parameters, however, increases the number of dimensions in the search space, i.e., execution time. Again, a slight change in the real-time value of a parameter may result in unnecessary switching between different wireless networks. Such unnecessary switching may result in instability in the hand-off mechanism. None of the above-mentioned handoff mechanisms has dealt with these issues diligently. They also face rank abnormality problem [241, 242]. Rank abnormality happens due to switching between different alternate networks as a response to the change in the priorities of the network-level parameters. Such abnormality in the ranks leads frequent network hand-offs. Frequent network hand-offs is the most undesirable property of any network selection mechanisms. A mechanism [243] based on fuzzy logic and Genetic Algorithm (GA) overcomes this rank abnormality problem at the cost of

limited scalability.

In addition, only a few of the above-mentioned hand-off mechanisms take into account energy consumption, which is an important device-level parameter for many multi-interface devices such as smart-phones. However, the ultimate improvement is yet to be achieved.

In order to address the above mentioned issues, we formulate the network selection problem as a multi-objective optimization problem (MOP) and solve it using a customized Multi-Objective Genetic Algorithm (MOGA). The customized MOGA utilizes artificial intelligence to reduce execution time in multi-dimensional search space. Our goal is to improve the network performance with respect to combined network and device-level parameters. We name our solution as Multi-Objective Vertical Hand-off (MOVH). It takes into account network dynamics. It is free from rank abnormality problem. It is energy efficient and highly stable and scalable.

Our contributions in this chapter are as follows:

- We propose an improved vertical hand-off mechanism, more specifically we focus on the network selection process namely MOVH using a customized MOGA.
- We delineate higher scalability and stability of MOVH through numerical simulation.
- We illustrate better performance of MOVH in indoor and outdoor test-bed settings than that of GRA and TOPSIS.
- Finally, we demonstrate better performance of MOVH using `ns-2` simulation for larger networks.

6.2 Related Work

The traditional vertical hand-off decisions (VHD) methods over heterogeneous networks mainly compare received signal strength (RSS) in making hand-off decisions [235, 236, 244, 245]. Other network-level parameters, such as bandwidth, are also compared along with RSS in several vertical hand-off mechanisms [237, 246, 247]. The hand-off mechanism in [237] compares RSS and estimated lifetime or available bandwidth. The hand-off mechanisms in [238, 239] also consider the monetary cost and bandwidth along with RSS.

Other well known hand-off decision making parameters are residual bandwidth and user service requirements [248]. Lee et al., [248] develop an QoS based VHD algorithm which takes into consideration the residual bandwidth and user service requirements for making decision whether to hand-off from a WLAN to Wireless Wide Area Network (WWAN) and vice versa. Another bandwidth based VHD method between WLANs and a Wideband Code Division Multiple Access (WCDMA) network using Signal to Interference and Noise Ratio (SINR) is presented in [249]. In addition, since users prefer the cheapest available access network in order to reduce incurred service cost, there are several studies in the literature, which introduce the cost function to select the best available network in the hand-off. Wang et al., [250] introduce first policy enabled hand-off strategy, that use an optimized cost function to select the target network by introducing trade-off between user satisfaction and network efficiency. In [251], the authors select the network having the lowest cost value, where the cost function depends on the bandwidth, delay, and power requirement. Moreover, in [252] the authors formulate the VHD problem as a Markov Decision Process (MDP). Here, they focus mainly on user's monetary budget along with the velocity and location information. Although these mechanisms consider a diverse set of parameters, they mostly consider these parameters in isolation. Consequently, these mechanisms attempt to optimize only a single objective while performing vertical hand-off decisions over heterogeneous networks.

In the recent times, some research studies formulate the vertical hand-off mechanism as a multi-objective optimization problem (MOP). In [253], the authors utilize multiple attribute decision-making (MADM) method for VHD in heterogeneous wireless networks. TOPSIS (Techniques for Order Preference by Similarity to Ideal Solution) [72], GRA (Grey Relational Analysis) [71], SAW (Simple Additive Weighting) [73], and AHP (Analytic Hierarchy Process) [254] are names of the most popular classical MADM method. TOPSIS [72] selects the candidate network which is the closet to the ideal solution and farthest from the worst case solution. Next, GRA [71] ranks the candidate networks and then selects the one with the highest rank. On the other hand, SAW [73] utilizes an overall score (i.e. the weighted sum of all the attributes) of a candidate network to select a target network. Finally, AHP [254] decomposes the network selection problem into several sub-problem and assigns a weight value to for each one. Moreover, [255] introduces an intelligent network selection strategy

based on combining two MADM methods (i.e., analytical network process (ANP) and TOPSIS). The ANP method is applied to find the weights of each parameter and TOPSIS method is used to rank the alternative networks.

Therefore, in this work, we focus on energy consumption, considering the battery power of the user's device, as a parameter in addition to other parameters to select the best network during vertical hand-off over heterogeneous networks.

Several studies, deploy fuzzy logic (FL) and neural network (NN) to choose the best network in VHD. FL and NN are combined in multiple criteria hand-off mechanisms in [243], [256], and [257]. In [256] fuzzy neural network (FNN) combined with Particle Swarm Optimization (PSO) algorithm with global optimization capability is discussed. In [257] fuzzy logic control based hand-off mechanism is discussed to decide best target network. Fuzzy logic systems allow human experts' qualitative thinking to be encoded as algorithms to improve the overall efficiency.

VHD mechanisms in [72], [71], [73], [254], [253], [255], [243], [256], and [257], however, did not consider the energy consumption of the user device while performing VHD. Higher energy consumption seriously affects user experience and should not be ignored while choosing the best network.

Multiple objective based selection of the best network in vertical hand-off mechanisms require the use of relative weights for decision parameters. Existing studies [71,72] use fixed weight for each decision parameter. This fixed weight for decision parameter is assigned based on either user satisfaction levels or application requirements. Such usage makes these mechanisms special purpose. For devising a general-purpose vertical hand-off mechanism, we must avoid the use of fixed weight for each decision parameter.

Most of the VHD mechanisms mentioned in this section also experience frequent unwanted switching between the networks, which limits their stability. The study in [243] overcomes this limitation by using fuzzy logic and GA. [243], however, solves the stability problem at the cost of scalability. It takes much higher time to execute.

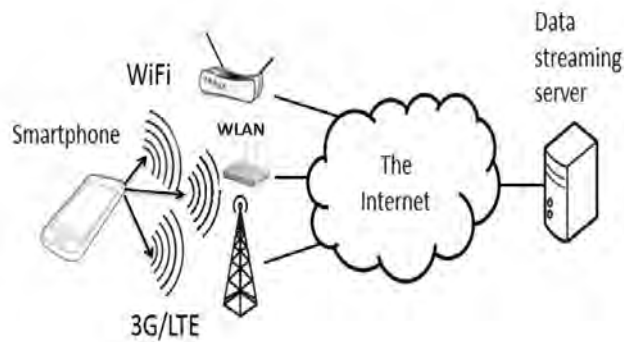


Figure 6.2: Vertical hand-off over heterogeneous networks

6.3 System Model

In this section, we present a system model of vertical hand-off in the context of mobile networks. Fig. 6.2 exhibits an example scenario where a vertical hand-off is expected to be performed.

We have already mentioned that a vertical hand-off comprises of three consecutive phases: initiation phase (i.e., hand-off information gathering), hand-off decision phase, and hand-off execution phase. The initiation phase deals with selecting different decision parameters such as data rate, delay, received signal strength, service cost, remaining battery power, etc., and gathering data on these parameters. The decision phase focuses on choosing the best network based on the selected parameters. Finally, the execution phase establishes a connection with the chosen network. In this chapter, we mainly focus on the second phase (i.e., choosing the best network) of vertical hand-off taking into account the impacts of different decision parameters along with the presence of network dynamics.

6.4 Vertical Hand-Off Mechanism Using MOVH

In this section, we propose a new multi-objective vertical hand-off (MOVH) mechanism. In our MOVH, we propose a general-purpose network selection mechanism for vertical hand-off. We take into account the impact of important decision parameters. We incorporate network dynamics. We ensure energy efficacy. We also ensure higher stability and scalability.

We use a customized Multi-Objective Genetic Algorithm (MOGA).

6.4.1 Decision Parameters

In order to choose the best network from a set of heterogeneous networks, we need to evaluate the performance of the networks on some useful metrics. We use several performance metrics as our decision parameters to make our selection process a general-purpose. We classify these decision parameters into three groups. The first group comprises of network-level parameters, such as data rate, end-to-end delay, received signal strength (RSS), and jitter. The second group comprises of device-level parameters, such as battery power, both remaining and ongoing energy levels. The last group comprises of business parameters such as service cost of a network.

A network with a high data rate, low battery power, low end-to-end delay, low service cost, high signal strength and low jitter is always desired as the best network while making vertical hand-off decisions over heterogeneous networks. However, none of these parameters are in coherence with the others. Therefore, we need to focus on multi-objective optimization in order to obtain the best-possible combination of the parameters. The following subsection illustrates the multi-objective optimization problem for our MOVH.

6.4.2 Multi-Objective Optimization in MOVH

In order to find the best network, we perform multi-objective optimization process considering many decision parameters. We maximize following equation:

$$\arg \max_i f(x) = \sum_{j=1}^M w_j \times f_i(x_j); \forall i \in N \quad (6.1)$$

Here, x_j corresponds to a decision parameter, M is the total number of decision parameters, and N is the total number of alternative networks. $f_i(x)$ is the value of overall fitness function for i^{th} network, which we get through taking a weighted sum of the individual objective functions (w_j signifies the weighting factor of j^{th} individual objective function pertinent to j^{th} parameter). Individual objective function i.e., $f_i(x_j)$ for $j \in M$ is a normalized value of j^{th} decision parameter. We perform normalization operation to compare decision parameters that have different measurement units into a uniform scale. We need to maximize the

values of some parameters such as data rate, remaining battery power, and received signal strength (RSS) while we need to minimize the values of several other parameters such as consumed battery power, delay, service cost, and jitter. Therefore, we follow different normalization processes for different decision parameters as: $f_i(x_j) = \frac{x_j}{X_{max}}$, for maximization, and $f_i(x_j) = \frac{X_{min}}{x_j}$, for minimization. We randomly set the weight for each parameter as:

$$w_i = \frac{r_i}{\sum_{j=1}^M r_j}$$

Here, r refers to random value, which is generated using a uniform distribution. The index of r denotes the index of associated parameter. Such randomized adjustment of weights ensures that our hand-off mechanism remains free from rank abnormality problem and results in better stability. The introduction of this simple randomization does not demand any heavy processing time. Consequently, our approach ensures more stability and scalability compared to that of GA [243]. We will demonstrate the effectiveness of our random adjustment of weights in Section 6.5.

6.4.3 MOGA Description

In this section, we first provide a brief description of genetic algorithms and then elaborate the selection process of a best-possible network using customized MOGA.

Genetic algorithms are well known as population-based search methods resembling the natural phenomena of biological evolution. These algorithms are mainly useful for optimization problems. In general a genetic algorithm starts with an initial population. A population is known to be a set of solutions. Each component of the population is encoded by a set of attributes indicating the diversity of the population which are called chromosome. Genetic algorithm then follows an iterative process. Each iteration is referred as generation. In each generation, different genetic operators i.e., crossover, mutation, replacement are applied to the population. A fitness function is evaluated to ensure the survival of the fittest individual. The fitness is the value of the optimization function which is considered to resolve. Based on the fitness function, the fitter individuals are usually selected as parent to breed and generate new fitter individuals in the population for the next generation. This process of evolution is allowed to continue until either a satisfactory level of fitness value has been attained or a sufficient number of generations have been produced. Fig. 6.3 delineates

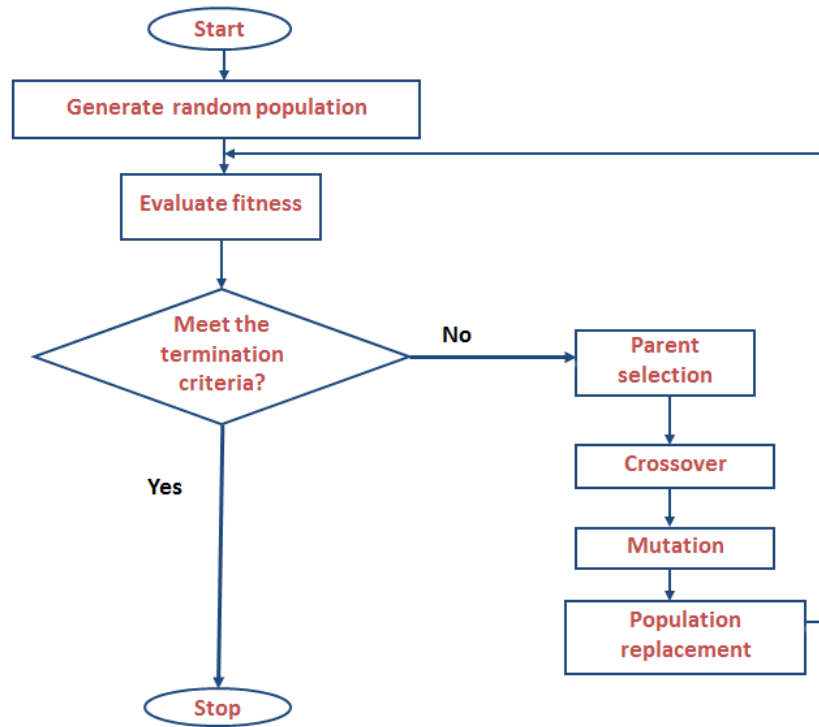


Figure 6.3: Flow diagram of MOGA

the flow diagram of MOGA. Next, we elaborate different steps of MOGA.

6.4.3.1 Chromosome representation

Performance of GA-based approaches significantly depends on the successful representation of chromosomes. We encode each chromosome using a string of genes that represents the dynamic status (i.e., the value of each parameter) of each network. Each chromosome contains $(M + 1)$ tuples, where M tuples correspond to M different decision parameters and the other tuple associates the identifier of the corresponding network. In contrast to conventional chromosome representation, our representation does not refer to a potential solution. It rather refers to the dynamic status of a network and the identifier of a corresponding network, i.e., $(M + 1)^{th}$ tuple, of a chromosome refers to a potential solution.

6.4.3.2 Initial population

We create a random initial population. In the initial population, we randomly generate values of the tuples, i.e., t_j , for each chromosome maintaining the constraint:

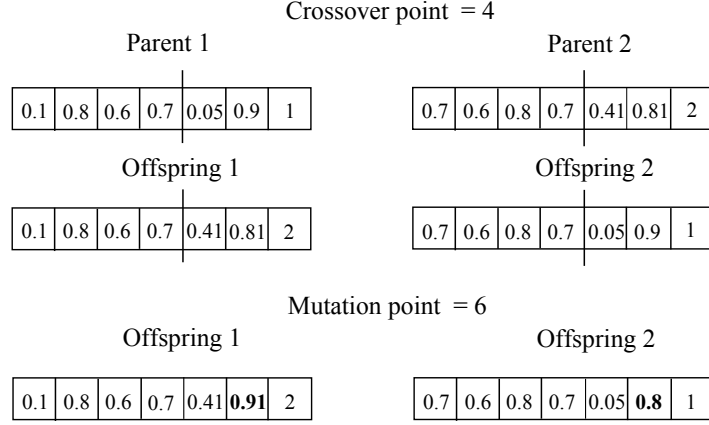


Figure 6.4: Crossover and mutation processes of MOVH

$$Z_{i,j}^{min} \leq t_j \leq Z_{i,j}^{max}; \forall j \in M, \forall i \in N;$$

Here, $Z_{i,j}^{min}$ and $Z_{i,j}^{max}$ are normalized minimum and maximum values of j^{th} parameter for i^{th} network. We accommodate network dynamics by using a parameter value randomly picked from a predefined range instead of a fixed value.

6.4.3.3 Parent selection

For parent selection procedure, we use the Tournament Selection Method [258], which is one of the most popular selection methods in Genetic Algorithms. In this method, to select each candidate solution, i.e., parent to generate new population, we select a random subset of size $k = 3 \times N$ from the current population pool. Then, we select the best solution by evaluating the fitness function from the subset. To calculate the fitness function, we take the weighted sum of the normalized value of each parameter as shown in Eq.6.1. While performing the weighted sum, we also use randomly picked weights. The usage of such random weights ensures the assignment of dynamic priorities to the parameters in each population, which enables fast exploration in a multi-dimensional search space pertinent to a multi-objective optimization problem. Comparing the fitness function with the random weights, we take the best half of the current population as the survivors for the next generation.

6.4.3.4 Crossover, mutation, and feasibility check

We apply one point crossover operation on the survivors. We take a random crossover point between 1 and M (excluding 1 and M). Subsequently, we generate two new offsprings through exchanging parts from two parents' tuples from the crossover point. Then, with the mutation probability 0.01, a tuple is selected randomly to change its value to a new one. Here, Fig. 6.4 shows the crossover and mutation processes of our MOVH.

After generating the offsprings, we perform feasibility check on each of them for correcting their network ids i.e. $(M + 1)^{th}$ tuple of that chromosome. If the parameter values of an offspring do not correspond to its associated network's range, then it is discarded as an infeasible solution. The process of parent selection, crossover, mutation, and feasibility check are repeated until we find a desired number of feasible offsprings.

6.4.3.5 Population replacement

Different strategies exist for replacing a population in GA. Two of the most popular strategies are to completely replace parents by the offsprings [259], and taking the best individuals from both parents and offsprings [260]. The first strategy is called "Replace All" and the second strategy is called "Elitism". The Replace All strategy possesses higher potential to escape from the local optima, whereas the Elitism strategy possesses higher capability for fast convergence.

In MOVH, we adopt a new population replacement strategy combining both Replace All and Elitism. We replace the worst half of the parents by the better half of the offsprings. As a result, the new population contains the individuals with good fitness values retaining the representatives from both parents and offsprings. Such combination achieves a good capability of fast convergence while retaining a good potential of escaping from local optima. We achieve higher scalability, which we prove in Section 6.5.

6.4.3.6 Termination

MOVH terminates whenever any of the following two criteria is met. The first criteria is- if the newly generated population converges to only one network, then that is the best network. The second criteria is- if the number of generation exceeds a maximum threshold value, then

we consider the solution with the maximum fitness value as the best network.

6.4.4 Settings of Operational Parameters of MOVH

We have several operational parameters of MOVH such as the number of tuples in a chromosome, population size, crossover rate, mutation rate, and population selection strategy. The values of some of these parameters (i.e., the number of tuples and population size) are set from decision parameters and available networks. Crossover rate and mutation rate are chosen as 0.8 and 0.01 respectively following the study presented in [261] as these values provide significant improvement in the performance of genetic algorithm. These choices also confirm that no user involvement is required for setting different operational parameters to use our MOVH mechanism.

6.4.5 Key Features of MOVH

MOVH possesses three key features which are as follows:

- Randomized adjustment of weights corresponding to each decision parameter, which ensures high stability in accordance with the nature of being general-purpose.
- Utilization of customized Multi-Objective Genetic Algorithm (MOGA), which performs efficient searching in a multi-dimensional search space, resulting in higher scalability while ensuring the nature of being multi-objective.
- Incorporation of network dynamics utilizing the ranges of values for the decision parameters instead of picking the fixed values for the decision parameters, which again ensures high stability.

These three key features combined ensure better network performance in multiple objective aspects.

6.5 Stability & Scalability of MOVH

The term stability refers to network dynamics impact on the selection of the best network while performing vertical hand-off over heterogeneous networks. Decision parameter values

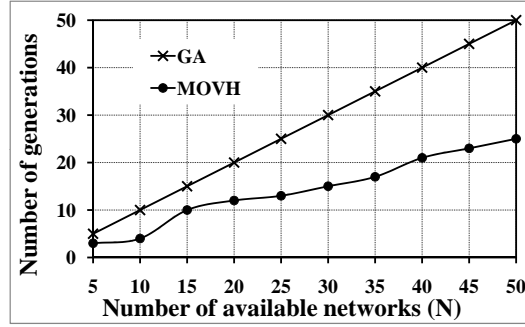


Figure 6.5: Convergence of GA and MOVH

can change dynamically owing to network dynamics. If a slight change in a network parameter forces a vertical hand-off solution to switch from one network to another network, then the solution is referred to as not stable. If a vertical hand-off solution provides a unique selection in multiple runs having slight changes in diverse parameters then the solution is accepted as stable. On the other hand, scalability indicates the capability to converge quickly towards a decision irrespective of the size of the network. In this section, we investigate stability and scalability of our MOVH. We adopt a customized multi-objective GA (MOGA) and consider the traditional GA (specifically the fuzzy based GA [243]) as our benchmark solution since it is known to be the most stable among the existing mechanisms such as TOPSIS, GRA. Creating a large number of wireless networks in an area for a test-bed experiment is really cumbersome and performing an ns-2 simulation with a large number of networks demands significant amount of time and memory. For this reason, we perform scalability evaluation through numerical simulation.

To illustrate the stability and scalability, we consider an example of heterogeneous wireless scenario consisting of UMTS, WiMAX, WLAN, and GSM/EDGE. Fig. 6.1 illustrates the existence of several different wireless networks in our university premises. This number tends to increase in near future. Therefore, we construct an example scenario consisting of 8 different networks such as one UMTS network (UMTS_1), two WiMAX networks (WiMAX_1, WiMAX_2), four WLAN networks (WLAN_1, WLAN_2, WLAN_3, and WLAN_4), and one EDGE network (EDGE_1). For each networks, we randomly select its parameter values following globally-accepted ranges as shown in Table 6.1. We also consider variations in the same network parameter for a certain type of network, for example, WiMAX_1, WiMAX_2 of WiMAX network. The reason behind such consideration is to

mimic variations in hardware solutions provided by different vendors.

We run MOVH mechanism multiple times with the slight changes in the decision parameters. Each run ends up with the same selection, WLAN_4. On the other hand, fuzzy based GA gives different selections with a slight change either in parameter values or in priorities. These results prove better stability of our MOVH mechanism than that of fuzzy based GA mechanism. Our MOVH mechanism eliminates the well-known rank inconsistency problem [241] ensuring better stability. The better stability yields from the randomized adjustments of the weights in the fitness function and from the accommodation of network dynamics by using random values from some predefined ranges for different decision parameters instead of fixed values. We further confirm the stability of MOVH using ns-2 simulation later in this chapter.

We also evaluate the scalability of our MOVH mechanism against that of fuzzy based GA mechanism and present our results in Fig. 6.5. The fuzzy based GA optimizes each network separately, and thus the number of generations is at least equal to the number of alternative networks. Our MOVH converges to a single network solution approximately 2 times faster than that of fuzzy based GA. This result indicates that MOVH is more scalable than that of fuzzy based GA.

Table 6.1: Globally-accepted ranges for values of different parameters in various wireless networks

Network	Data rate (Mb/s)	Battery power consumption (J)	Remaining battery power (J)	Service cost (USD)	End-to-end delay (ms)	Jitter (ms)
UMTS_1	37.00-39.00	23.00-25.00	45.00-49.00	16.21-18.02	49.00-51.00	1.00-2.00
WiMAX_1	65.00-69.00	23.00-26.00	54.00-59.00	14.21-15.14	74.00-76.00	10.00-12.00
WiMAX_2	66.00-70.00	24.00-25.00	35.00-39.00	13.75-15.36	72.00-76.00	9.00-14.00
WLAN_1	50.00-52.00	14.00-16.00	37.00-42.00	0.19-0.20	35.00-36.00	11.00-13.00
WLAN_2	46.00-49.00	12.00-15.00	50.00-54.00	0.20-0.21	34.00-36.00	12.00-13.00
WLAN_3	45.00-47.00	14.00-17.00	45.00-60.00	0.20-0.21	32.00-35.00	10.00-12.00
WLAN_4	49.00-53.00	13.00-18.00	29.00-31.00	0.19-0.21	35.00-48.00	11.00-12.00
EDGE_1	0.19-0.19	5.00-7.00	46.00-51.00	0.004-0.006	159.00-163.00	9.00-11.00

6.6 Performance Evaluation

In order to prove the superior performance of MOVH, we evaluate its performance against that of other state-of-the-art approaches of multi-objective decision making mechanisms such

as GRA [71] and TOPSIS [72]. We implement GRA and TOPSIS according to [71] and [72] respectively. We choose these two alternatives as they are possibly the best alternatives so far found in the literature [262].

6.6.1 Test-bed Evaluation

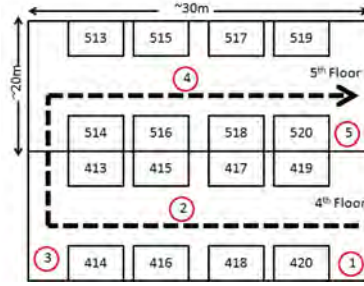
For the test-bed experiments, we build up our own network with COTS mobile devices. We elaborate the network settings in the next subsection, and then, present the experimental results.

6.6.1.1 Test-bed settings

We accomplished test-bed experiments in two different phases: indoor and outdoor. Our indoor experiment consisted of six android devices of NTTdocomo model of Samsung galaxy (model# *SC-03D*). We placed the devices on the 4th and the 5th floors of the ECE building at BUET campus in Dhaka, Bangladesh. The placement of the devices at two different floors addresses the mobility in three dimensional space. We also performed outdoor experiment with the same number of devices placed on the open field outside the ECE building.

In both indoor and outdoor settings, we used five of the devices as the destinations and one as the source. Fig. 6.6a shows device placements in our indoor network. The indoor area is approximately 30 m long and 20 m wide. Fig. 6.6b shows the outdoor placements of the devices. The outdoor area is approximately 25 m long and 20 m wide. The red circles in Fig. 6.6a and Fig. 6.6b denote the placements of the destination devices. Fig. 6.6c shows a snapshot of the device we used for our experiment. Four of the destination devices were WiFi enabled, which were connected to the Internet through 3G cellular networks. The other destination device was connected through Bluetooth. We used the cellular 3G network infrastructure of GrameenPhone [263]. In our experiment, we placed the destination devices at approximately 15 m distant from each other.

We roamed with the source device from one destination device to another one following the trajectory shown in Fig. 6.6a and Fig. 6.6b respectively. We ran the experiments periodically and observed the results. We experimented our proposed mechanism MOVH along with the other popular mechanisms, such as GRA and TOPSIS, and got connected to the



(a) Indoor settings



(b) Outdoor setting



(c) Device used for test-bed

Figure 6.6: Test-bed deployments for both indoor and outdoor experiments (red circles denote destination devices)

best-possible network. We transmitted data via the selected network from the source to the selected destination device and computed different metrics. We performed this experiment nine times and present the results by averaging the values.

6.6.1.2 Parameter selection

In our test-bed experiment, we used real-time values for some decision parameters, such as data rate, RSS, end-to-end delay, and battery level. The real-time values are extracted from the devices. We used a range of $\pm 2.5\%$ of the device values in order to incorporate network dynamics and to make it similar to the case that considered the ranges in Table 6.1. The data rate of the destination devices varied from 26 to 65 Mbps. In order to get the end-to-end delay, we periodically connected the source node with each destination node and transmitted the data over them to get a feedback from the destination devices. We computed the end-to-end delay once the feedback had been available.

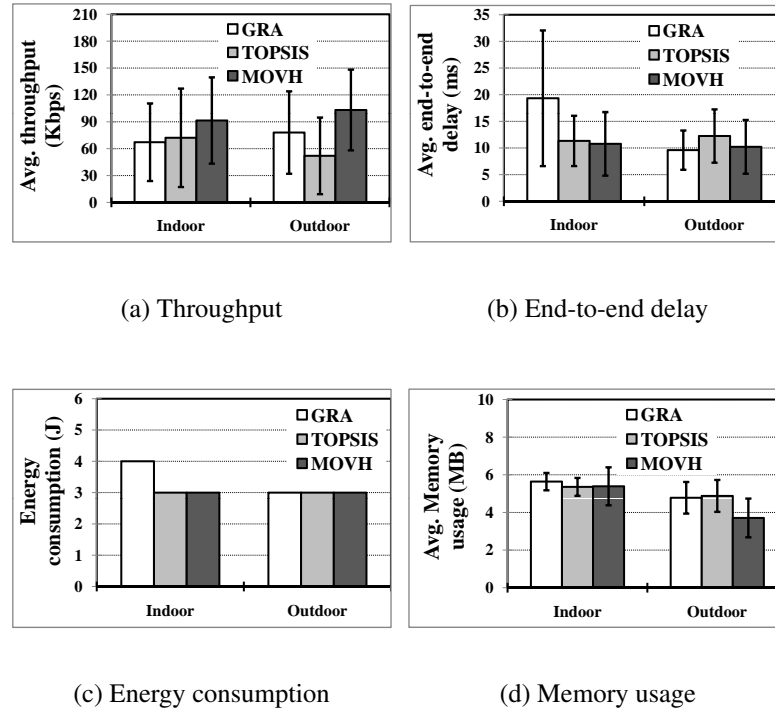


Figure 6.7: Performance evaluation and operational overhead for GRA, TOPSIS, and MOVH

6.6.1.3 Experimental results

In this subsection, we analyze the performance of MOVH in test-bed in terms of throughput, end-to-end delay, and battery consumption.

Throughput Analysis We compare the performance of MOVH with that of GRA and TOPSIS. We transmit different number of packets from the source node to the destination nodes and compute the average throughput. We present the average network throughput for different mechanisms both in indoor and in outdoor setting in Fig. 6.7a. The figure reveals a significant improvement in network throughput using MOVH over that of using GRA and TOPSIS.

End-to-End Delay Analysis We present the end-to-end delay in Fig. 6.7b. The figure reveals that MOVH almost always results in smaller end-to-end delay.

Energy Consumption Analysis We analyze energy efficiency of different mechanisms in terms of total energy consumption. Here, we consider energy consumption of the source device. We run each mechanism nine times within the trajectory and compute the total energy

Table 6.2: % improvement in different metrics using MOVH

Performance metric	Setting	% improvement w.r.t.	
		GRA	TOPSIS
Throughput	Indoor	26	21
	Outdoor	24	49
End-to-end delay	Indoor	44	5
	Outdoor	-6	16
Energy consumption	Indoor	0	0
	Outdoor	25	0
Memory usage	Indoor	6	0
	Outdoor	22	23

consumption. Fig. 6.7c shows the energy consumption of MOVH, GRA, and TOPSIS. The figure indicates that MOVH either consumes similar or less energy compared to that of GRA and TOPSIS.

6.6.1.4 Resource overhead

In addition to throughput, end-to-end delay, and energy consumption, another key performance indicator of a hand-off mechanism is its resource overhead, such as memory usage and CPU usage. In our experiment, CPU usage is very negligible and same for all other mechanisms. Therefore, we mainly focus on memory usage. In order to calculate memory usage, we use Proportionate Set Size (PSS) [264] which is a statistic that the Android system computes to determine whether it needs to kill a process or not. Measuring only how much memory an App is consuming is not enough since an App maybe using some shared memory with other processes. For this reason, Android uses the notion of PSS statistic. Fig. 6.7d shows memory usage for all three mechanisms under consideration. MOVH uses significantly less memory compared to that of the other two mechanisms in both indoor and outdoor settings.

We summarize the percentages of performance improvement of MOVH over GRA and TOPSIS on various performance metrics in Table 6.2. It demonstrates that MOVH provides significant improvement in most of the cases.

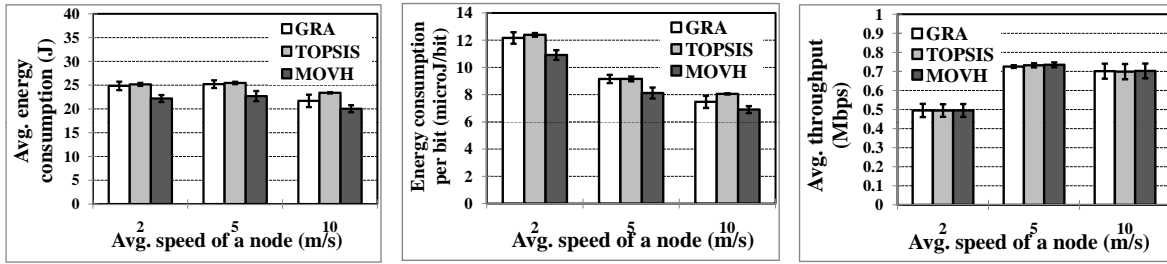
6.6.2 Simulation Evaluation

In addition to our test-bed experiments, we further evaluated the performance of our MOVH mechanism through ns-2 simulation. Here, we focused on five different performance metrics. These metrics are end-to-end delay, throughput, energy consumption, energy consumption per transmitted bit, and service cost. We describe our simulation parameter settings first, then the simulation results.

6.6.2.1 Simulation settings

We considered a heterogeneous network over a coverage area of 1000×1000 m² in our simulation. Each mobile node in the network was equipped with four different radios- 802.11b, 802.11g, 802.11n, and 802.15.4 having a data rate of 11 Mbps, 54 Mbps, 108 Mbps, and 0.25 Mbps respectively. The radios used an omni-directional antenna with varied transmission ranges: 140m, 140m, 250m, and 125m for 802.11b, 802.11g, 802.11n, and 802.15.4 respectively. The carrier sensing ranges were set twice as the transmission range. We placed eight stationary single-radio nodes over the coverage area resembling access points that act as destinations of data flows. We also considered 20 multi-radio mobile nodes as source nodes of the flows. We used the Two-Ray-Ground reflection model [265] as the underlying radio propagation model. We exploited the built-in power models of ns-2 to compute energy consumption for all radios. In order to compute the energy consumption by each radio, we used the measurements provided in [266] for 802.11b, [267] for 802.11g, [268] for 802.11n, and [269] for 802.15.4. Each mobile node consisted of a drop-tail priority queue having a maximum capacity of 40 packets under the transmission. We set the multi-radio nodes to use Ad hoc On-Demand Distance Vector (AODV) as the network layer protocol in our simulation. We enabled constant bit rate data flow over the nodes. We used TCP traffic flow in our simulation. Here, we transmitted 60M packets per second each packet carrying a payload of 512 bytes.

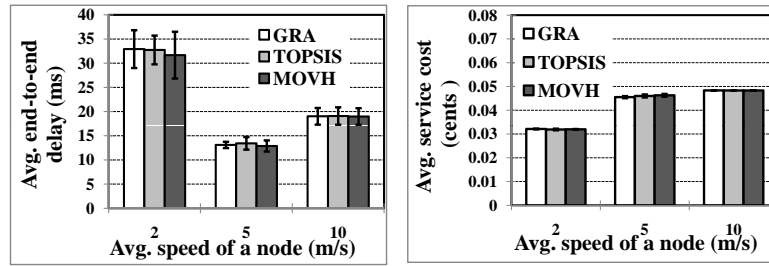
In addition to simulation parameters, we needed to select the decision parameters for vertical hand-off mechanisms. We considered data rate, consumed battery power, remaining battery power, delay, and service cost as the decision parameters. We used round trip time of the packets as the delay. We compute the service cost following traditionally used monetary



(a) Energy consumption

(b) Energy per bit

(c) Avg. throughput



(d) Avg. delay

(e) Avg. service cost

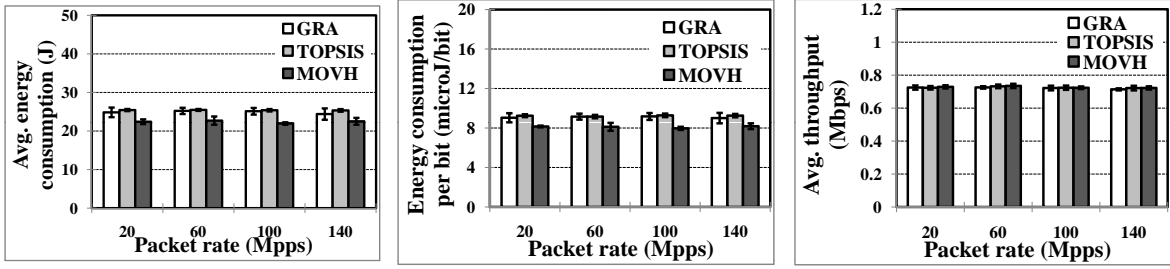
Figure 6.8: Impact of variation in speed of nodes on different performance metrics using GRA, TOPSIS, and MOVH

amount (for example, 75 cents for 512 Mb data transfer over 802.11b) for each radio. With these settings, we compute the average of seven simulation runs, each run had a duration of 50 seconds of operation and an initial interval of 20 seconds. 20 seconds interval helps all the nodes to become stable to operate. In each simulation run, we executed vertical hand-off mechanisms at every 10 second and transmitted data packets over the selected network.

In order to evaluate the performance of MOVH in diverse settings, we varied different network parameters such as speed of the nodes, packet rate, and network size.

6.6.2.2 Simulation results with the variation in speed

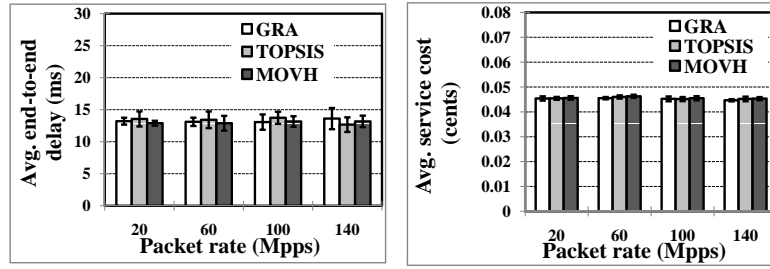
We compared the performance of MOVH, GRA [71], and TOPSIS [72] in response to varying speed of source nodes. Fig. 6.8 illustrates the impact of the variation in speed of the nodes on different performance metrics for MOVH along with GRA and TOPSIS. Here, we select the average energy consumption and the energy consumption per bit as two of our evaluation metrics. We choose the metric energy consumption per transmitted bit due to its operational significance along with its wide acceptability for evaluating energy efficiency.



(a) Energy consumption

(b) Energy per bit

(c) Avg. throughput



(d) Avg. delay

(e) Avg. service cost

Figure 6.9: Impact of variation in the packet rate on different performance metrics using GRA, TOPSIS, and MOVH

Fig. 6.8a depicts that MOVH consumes less energy compared to the energy consumed by either GRA or TOPSIS. MOVH achieves 9% and 12% energy consumption reduction compared to GRA and TOPSIS respectively. Fig. 6.8b also shows less energy consumption per bit by MOVH compared to that of the other two mechanisms. MOVH achieves 10% and 13% improvements in this respect over GRA and TOPSIS respectively. The improvement of these two metrics confirms the energy efficacy of MOVH.

We present network throughput for MOVH comparing that of two approaches, i.e., GRA and TOPSIS in Fig. 6.8c, which indicates a small increase in the throughput of the network.

We compare the average end-to-end delay incurred in MOVH against that of in GRA and TOPSIS (Fig. 6.8d). Here, we find that the use of MOVH results in decreased end-to-end delay compared to that of GRA and TOPSIS. Finally, Fig. 6.8e depicts the performance of MOVH in terms of service cost, which remains almost the same as those of other two mechanisms i.e., TOPSIS, and GRA.

6.6.2.3 Simulation results with the variation in packet rate

We evaluated the performance of MOVH in response to a variation in the packet rate. In our evaluation, we considered four different packet rates, such as 20 Mpps, 60 Mpps, 100 Mpps, and 140 Mpps, where pps refers to packets per second. Fig. 6.9a depicts the average energy consumption for different packet rates. MOVH consumes significantly less energy compared to that of GRA and TOPSIS. The percentage of improvement is 10% and 12% compared to that of GRA and TOPSIS respectively. Fig. 6.8b also depicts a similar trend of improvement in case of energy per bit. Here, we find that MOVH consumes 11%, and 12% less energy per bit compared to that of GRA and TOPSIS.

Fig. 6.9c presents the network throughput of different VHDs. The average throughput is higher in MOVH compared to GRA and TOPSIS. Fig. 6.9d depicts the impact of packet rate variation on the average end-to-end delay. The average delay is less in MOVH compared to that in GRA and TOPSIS. Finally, Fig. 6.9e depicts that the service cost in MOVH remains the same as in GRA and TOPSIS with an increase in packet rate.

6.6.2.4 Simulation results with the variation in network size

We present simulation results with the variation in network size (i.e., the number of nodes) in Fig. 6.10. Fig. 6.10a depicts that MOVH consumes either less or same energy as GRA and TOPSIS do. Again, Fig. 6.10b reveals that MOVH consumes less or same energy per bit as in other two alternatives i.e., GRA and TOPSIS.

Fig. 6.10c illustrates the average throughput in MOVH, GRA, and TOPSIS. Here, we find that the network throughput using MOVH has higher values in large networks compared to that of using GRA and TOPSIS. Fig. 6.10d shows that the average end-to-end delay in MOVH has the same values as in GRA and TOPSIS. Finally, Fig. 6.10e shows the results in terms of service cost. MOVH has little higher service cost compared to that of GRA and TOPSIS.

6.6.2.5 Simulation results for illustration of stability

We evaluated the stability of MOVH through n_S-2 simulation. We considered a network setting comprising of eight access points of different network types, such as 802.11g, 802.11b,

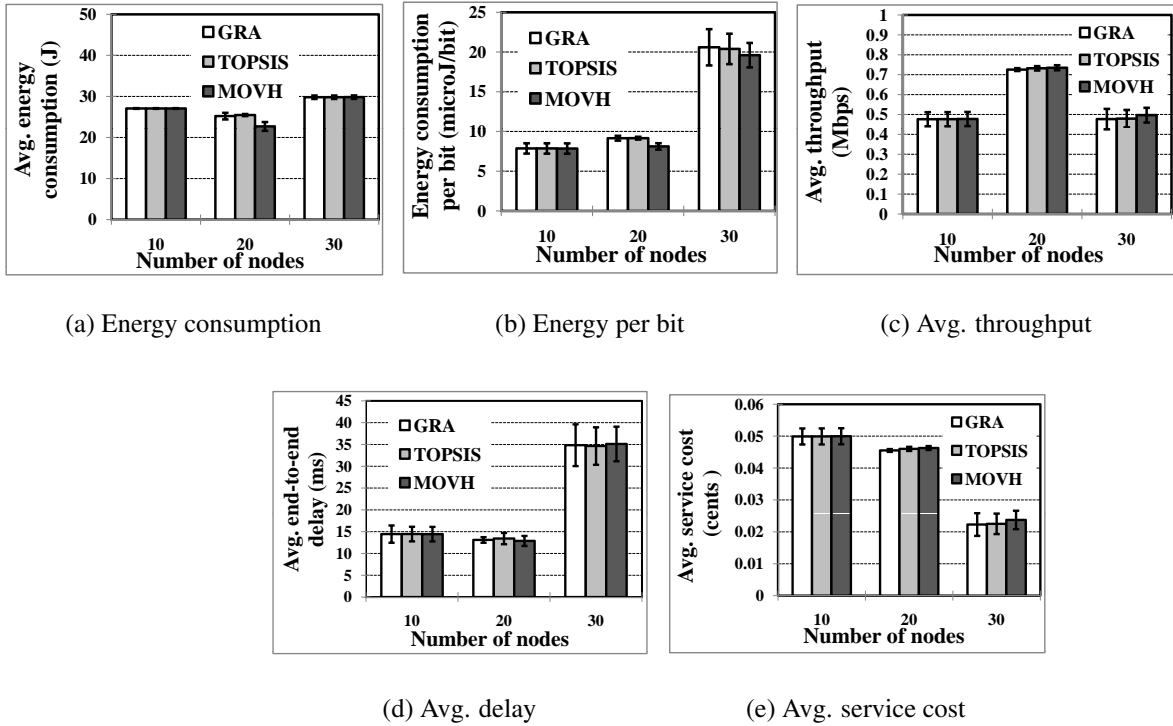


Figure 6.10: Impact of variation in network size on different performance metrics using GRA, TOPSIS, and MOVH

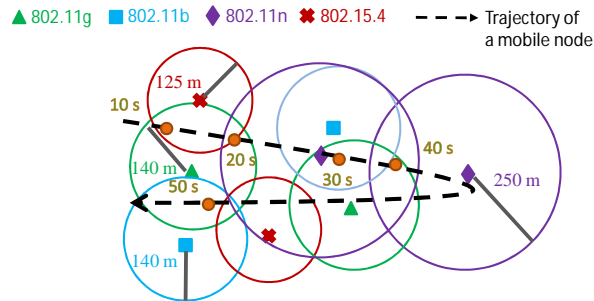


Figure 6.11: Network setting for evaluation of stability

802.11n, and 802.15.4.

Fig. 6.11 presents the network settings along with the trajectory of a mobile node having high speed. We log network connectivities of the mobile node while moving along the trajectory. Table 6.3 demonstrates connectivities with different networks at different points of time starting from 10 seconds to 50 seconds with a granularity of 10 seconds. Fig. 6.11 shows the positions of the mobile node at the time of logging network connectivities.

Table 6.3 exhibits that MOVH selects the same network, i.e., 802.11g, whereas the other

Algorithm	Selected networks at					change in network
	10 (s)	20 (s)	30 (s)	40 (s)	50 (s)	
GRA	802.15.4	802.11n	802.11n	802.11g	802.11g	2
TOPSIS	802.11g	802.11n	802.11n	802.11n	802.11g	2
MOVH	802.11g	802.11g	802.11g	802.11g	802.11g	0

Table 6.3: Selection of different networks

two approaches exhibit variation in network connectivities. Since our MOVH mechanism ignores transient changes (owing to network dynamics, which is very natural for wireless networks) in the decision parameters it selects the same network at different logging period. This result also confirms better stability of MOVH in selecting networks compared to that of the other two mechanisms i.e., TOPSIS, and GRA.

6.6.2.6 Justification of simulation results

Throughout this subsection, we have evaluated MOVH using ns-2 simulation software with different network settings. We consider four decision parameters (i.e., RSS, data rate, battery level, and delay) in our test-bed experiments. However, we consider five decision parameters, i.e., data rate, consumed battery power, remaining battery power, end-to-end delay, and service cost for ns-2 simulation. The increase in the number of decision parameters makes the individual optimization of decision parameters very difficult. Hence we focus on an overall optimization in terms of all the decision parameters instead of optimizing each parameter individually. The % of improvement in different network metrics are summarized in Table 6.4 and in Table 6.5.

Table 6.4 and Table 6.5 presents that the performances have improved in most of the cases. The extents of improvement are, however, lower than that of test-bed experiments. This is because the test-bed experiments took the advantage of more network dynamics in the decision parameters than that was done in the simulation environment. Besides, the test-bed experiments consider less number of decision parameters compared to that of the simulation environment. These two factors combined resulted in lower extents of improvement in simulation compared to that in the test-bed experiments.

Network parameters under variation	Different values of parameter	% improvement in avg. energy consumption w.r.t.		% improvement in avg. energy consumption/ bit w.r.t.	
		GRA	TOPSIS	GRA	TOPSIS
		Average speed of nodes (m/s)	2	11	12
	5	10	11	11	11
	10	8	14	8	14
Packet rate (Mpps)	20	10	12	10	12
	60	10	11	11	11
	100	13	14	13	14
	140	8	11	9	12
Network size (Number of nodes)	10	0	0	0	0
	20	10	11	11	11
	30	0	0	9	4

Table 6.4: Percentages of improvement in energy consumption using MOVH

Network parameters under variation	Different values of parameter	% improvement in avg. network throughput w.r.t.		% improvement in avg. end-to-end delay w.r.t.		% improvement in avg. service cost w.r.t.	
		GRA	TOPSIS	GRA	TOPSIS	GRA	TOPSIS
		Average speed of nodes (m/s)	2	0	0	4	3
	5	1	0	2	4	-2	-1
	10	0	1	0	1	0	0
Packet rate (Mpps)	20	1	1	2	5	0	0
	60	1	0	2	4	-2	-1
	100	0	0	0	4	-1	-1
	140	1	0	3	-4	-2	0
Network size (Number of nodes)	10	0	0	0	0	0	0
	20	1	0	2	4	-2	-1
	30	4	4	-1	-1	-6	-5

Table 6.5: Percentages of improvement in average throughput, delay, and service cost using MOVH

6.7 Other Aspects of MOVH

6.7.1 Variations in Weights

In our proposed algorithm, we perform randomized adjustments of weights in the fitness function for different decision parameters. Such randomization of weights ensures that our proposed MOVH mechanism results in better stability and makes MOVH free from rank abnormality problem [241]. Randomization of weights allows the protocol to be general-purpose as no priorities are assigned to particular network-level parameters.

6.7.2 Consideration of Constraints in Objective Function

Our proposed objective function (in Eq. 6.1) currently does not have any constraints associated with it. However, constraints can be added on decision parameters such as service cost, delay, battery power. However, such constraints are scenario specific. Hence, incorporation of such constraints will make our proposed mechanism special-purpose instead of being general purpose.

6.7.3 Normalization of Decision Parameters

In our proposed mechanism, we perform normalization to compare decision parameters that have different measurement units into a uniform scale. For our proposed mechanism, we follow the normalization approach presented in section 6.4.2. However, other processes of normalization such as (1 – minimizing parameters) could also be used. We envision to explore the performance of such a normalization process in our future work.

6.8 Conclusion

In this work, we propose a general-purpose multi-objective vertical hand-off mechanism named MOVH, exploiting a customized MOGA. MOVH addresses network dynamics while making hand-off decisions. We presented details of MOVH operations and algorithm. MOVH exhibits higher stability and scalability. We evaluated the performance of MOVH in terms of different performance metrics through both test-bed experiments and `ns-2` simulation. Our evaluation results reveal that our proposed mechanism outperforms the state-of-the-art approaches by some significant margins.

Next, we focus on performance enhancement of mobile wireless networks, which is another representative of smarter versions of limited-resource cyber-physical networks.

Chapter 7

An Empirical Study Based Feasibility Analysis on Mathematical Modeling for MANETs

7.1 Introduction

Mobile Ad hoc Networks (MANETs) have become a widely renowned communication paradigm now-a-days due to their intrinsic flexibility, lack of infrastructure, ease of deployment, auto configuration, and low cost. MANETs foreshadow its gleaming prospects in diversified applications such as battlefield communication [74], emergency relief scenarios [75], law enforcement [76], public meeting [74], virtual classroom [77], and security-sensitive computing environments [74]. Several real deployments of MANETs have already started to operate with tremendous success in some of these applications. Besides, vehicular (V2V) [270] and airborne communication networks [271] appear to be two prominent upcoming commercial applications of MANETs.

The extensive flourish in applications and real deployments of MANETs emphasizes performance improvement and efficient maintenance of the deployed networks as well as network planning for future applications. Therefore, many research studies focus on investigating such activities throughout the last decade. Most of the studies focus on improving the performance of MANETs. In order to synthesize and evaluate the performance improvement

of MANETs we can utilize different techniques. Examples include mathematical modeling and empirical study exploiting different methodologies such as simulation and testbed experiment. Here, mathematical modeling is considered as the fastest and the most cost-effective one among the techniques. However, precise mathematical modeling for MANETs is yet to be explored in the literature.

Several research studies [78], [79], [80] have attempted to formulate mathematical models for MANETs focusing on a few performance metrics such as average end-to-end delay and average throughput. These models mainly emphasize on distinct levels of functionality of one of the lower layers in protocol stack (physical layer and medium access control (MAC) layer) in their formulation leaving the crucial influences of upper layers such as network and transport layer and intricate interaction between different layers unexplored. Moreover, these models mainly consider the impact of only a few network parameters such as the number of nodes [79] and packet rate [78] ignoring that of some important operational parameters such as velocity of node and maximum number of allowed connections among nodes.

To the best of our knowledge, a precise mathematical model for MANETs simultaneously considering the impact of all layers in the protocol stack and diversified parameters, is yet to be formulated in the literature. Therefore, in this chapter, we study the impact of the different layers and parameters on different performance metrics such as average end-to-end delay, average throughput, average energy consumption, delivery ratio, and drop ratio through rigorous simulation using *ns-2* to facilitate the task of modeling for MANETs. Subsequently, we assess the feasibility of such modeling through studying the simulation results. Our study reveals that such modeling needs to resolve higher order equations.

Based on our study, we make the following contributions in this chapter:

- We perform extensive simulation of MANETs using *ns-2* through varying different parameters and considering diversified deployment scenarios.
- Subsequently, we analyze the results of our simulation to reveal trends in network performance for developing mathematical models on different performance metrics such as average end-to-end delay, average throughput, average energy consumption, delivery ratio, and drop ratio for MANETs.

- Finally, we analyze the feasibility of such mathematical modeling. Our analysis reveals that such mathematical models need to resolve higher-order equations. Consequently, our study uncovers a key finding that *mathematical modeling of MANETs considering variation of all parameters is not feasible..*

7.2 Related Work

A number of mathematical models have been explored for wireless networks in the literature. Gupta and Kumar propose the most widely accepted model in this regard [272]. However, they consider a static model where all nodes are fixed, which fails to adapt the mobile environment of MANETs. Subsequently, Rizvi et al., present an analytical model for the capacity of MANETs considering the impact of a few network parameters [273]. Besides, Jun et al., propose an analytical model for average end-to-end delay [80]. Sharma et al., introduce a mathematical model on average end-to-end delay and maximum achievable per node throughput for in vehicle Ad hoc multimedia network [274]. Besides, some other studies [78] propose simplified analytical models for end-to-end delay in MANETs. However, the prior approaches mostly focus on the functionality of MAC layer. Consequently, these approaches lack in taking account the influence of network layer and transport layer and intricate interactions between different layers. Moreover, these approaches consider only a few network parameters such as the number of nodes and packet rate, and thus ignore the other important parameters such as velocity of nodes and the number of maximum connections. Besides, the prior approaches focus on formulating analytical models for end-to-end delay and throughput, ignoring other performance metrics such as average energy consumption, delivery ratio, and drop ratio. Therefore, in this work, we perform a rigorous empirical study to analyze the feasibility for MANETs considering all these factors.

7.3 Empirical Study

In this section, we simulate on the performance of MANETs from different point of view using ns-2 to expose trends in the performance. The simulation results facilitate to asses the feasibility of mathematical modeling for performance considering variation in different pa-

Parameter	Values
Network size	5, 10, 20, 40, 50, 80, and 100 nodes
Node speed	2, 8, 16, 20, 25, 40, and 50 m/s
Packet rate	1000, 5000, 20000, 50000, 80000, and 100000 packets/s
Max. connections	5, 10, 20, 25, 40, and 50

Table 7.1: Network parameters

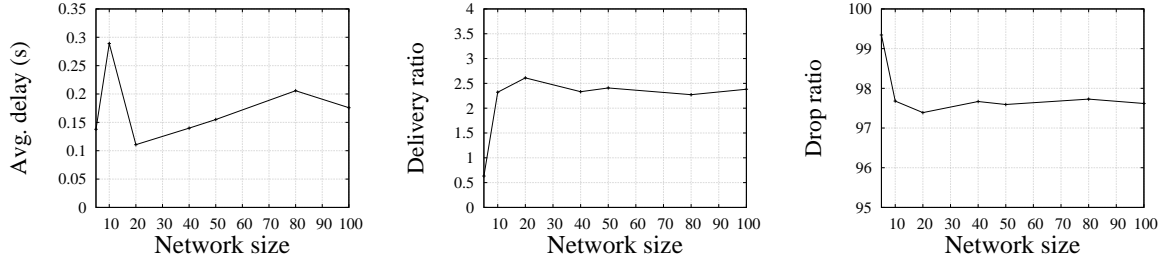
Parameter	Value	Parameter	Value
Simulation time	200 sec	Coverage area	$1000 \times 500 \text{ m}^2$
Traffic source	CBR	Mobility model	Random waypoint
Propagation model	Two-ray ground	Energy model	EnergyModel
Packet size	512 bytes	Pause time	2 s
Initial energy	100 J	Minimum speed	1 m/s
Transmission range	250 m	Radio bandwidth	54 Mbps
Transmission power	3132 e-3 W	Reception power	3528 e-3
Idle power	712 e-6 W	Sleep power	144 e-9 W

Table 7.2: Simulation parameters

rameters. While carrying out the simulation, we consider four network parameters: network size in terms of the number of nodes, speed of the nodes, packet transmission rate and the maximum number of connections allowed among the nodes. All these parameters impose significant impact on the performance of MANETs. We create different scenarios varying these parameters to resemble pragmatic deployments. We present the network parameters in Table 7.1 along with their values. Besides, we separately enable AODV and DSDV in network layer to investigate the impact of operations in network layer. We also separately enable UDP and TCP in the transport layer to investigate the impact of operations in transport layer on the performance of MANETs. For all the scenarios, we use a fixed coverage area of $1000 \times 500 \text{ m}^2$. Besides, we use the realistic Two-Ray Ground reflection model [275] as the radio propagation model. Additionally, we use EnergyModel as the energy model. Here, the initial energy level and other energy values are set accordingly to investigate the energy consumption of different mobile nodes [276]. The name and corresponding values of other simulation parameters are summarized in Table 7.2.

7.3.1 Simulation Results

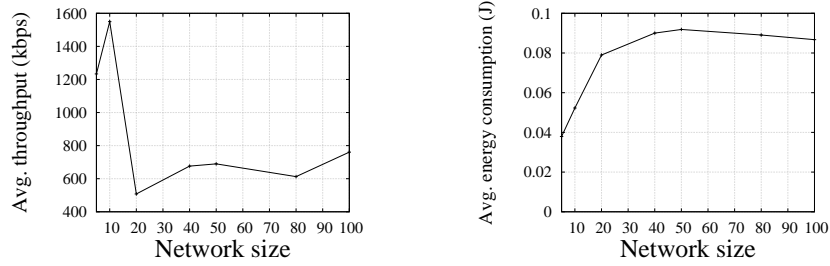
There are several metrics that can be used in evaluating the performance of MANETs. However, in this chapter, we focus on five metrics and utilize them in analyzing the performance of MANETs. These performance metrics are: average throughput, average end-to-end delay,



(a) Impact on average delay

(b) Impact on delivery ratio

(c) Impact on drop ratio



(d) Impact on average throughput

(e) Impact on average energy consumption

Figure 7.1: Impact of variation in network size on different performance metrics while using UDP with AODV

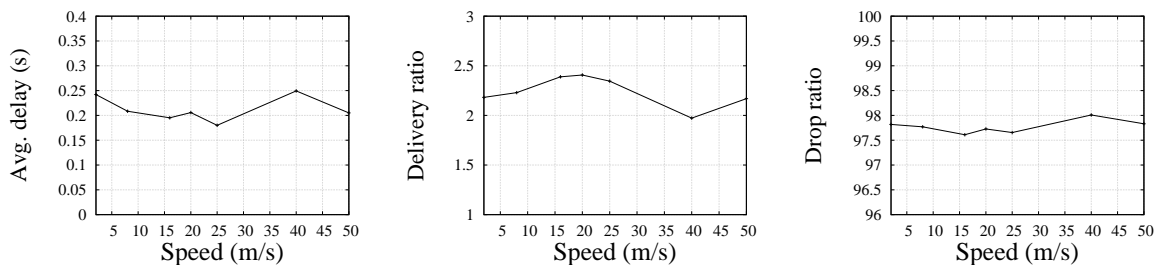
average energy consumption, delivery ratio, and drop ratio. Here, delivery ratio represents the number of packets successfully delivered to destinations over total number of packets sent [277]. This metric can specify the packet loss rate, which limits the maximum throughput of the network. In addition, drop ratio represents the number of packets dropped because of mobility or full queues over total number of packets sent [277]. This performance metric helps in quantifying the amount of transmitted data packets are dropped by routers in the path to destinations due to errors occurred in the physical or upper layers. We analyze the impact of variation in parameters on these performance metrics through simulation. Here, we perform 30 independent simulation runs and take average over them for achieving near-stable results. Now, we present these results over different scenarios.

7.3.1.1 UDP with AODV

We first enable AODV at network layer and UDP at transport layer. Here, Fig. 7.1 demonstrates the impact of variation in network size, in terms of the number of nodes on different performance metrics.

Fig. 7.1a illustrates that average end-to-end delay exhibits no specific trend in response to the variation in network size. However, Fig. 7.1b and Fig. 7.1c exhibit two different trends for delivery ratio and drop ratio respectively. These graphs show that the delivery ratio increases with an increase in the number of nodes, whereas drop ratio decreases with an increase in the number of nodes. Besides, in both the cases, the rate of change decreases as the size of the network increases. In addition, Fig. 7.1d demonstrates that throughput exhibits fluctuation rather than presenting any trend. On the other hand, Fig. 7.1e shows that average energy consumption increases with an increase in network size, however, the rate of increase diminishes as the size of the network increases.

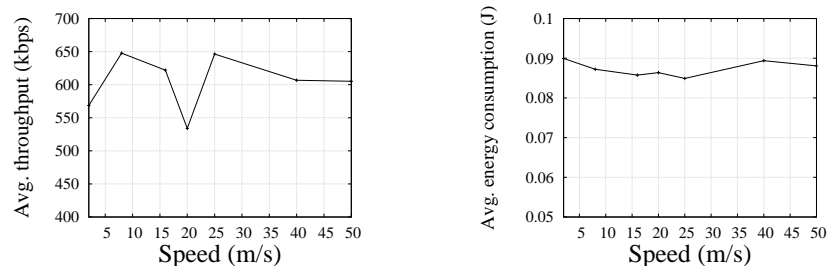
The impact of variation in speed of nodes on different performance metrics is demonstrated in Fig. 7.2. Here, Fig. 7.2a, Fig. 7.2c, and Fig. 7.2e show that average delay, drop ratio and average energy consumption decrease at lower speeds. However, they exhibit fluctuation at higher speed. On the other hand, delivery ratio increases for low speed and decreases for high speed (Fig. 7.2b). However, in the case of average throughput, once again we find no specific trend (Fig. 7.2d).



(a) Impact on average delay

(b) Impact on delivery ratio

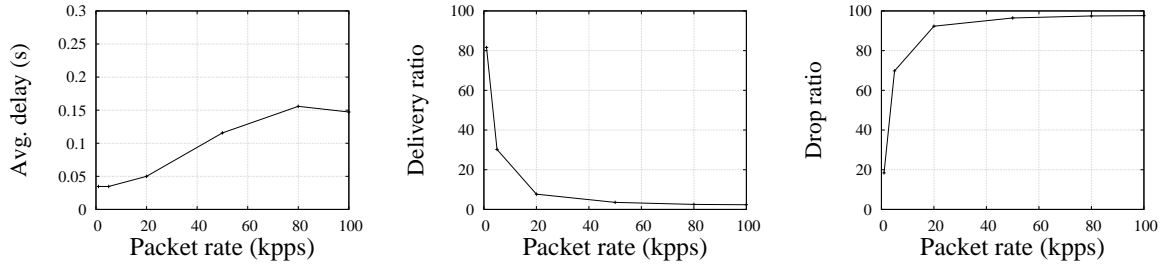
(c) Impact on drop ratio



(d) Impact on average throughput

(e) Impact on average energy consumption

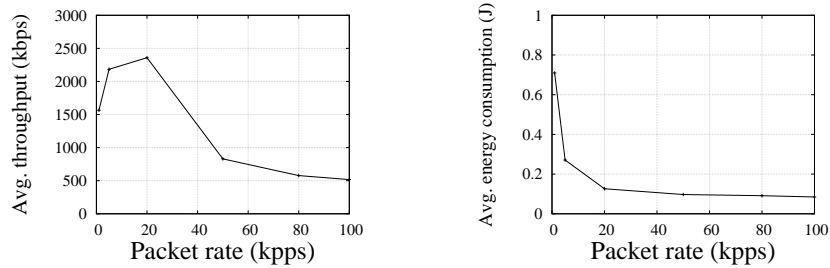
Figure 7.2: Impact of variation in speed of the nodes on different performance metrics while using UDP with AODV



(a) Impact on average delay

(b) Impact on delivery ratio

(c) Impact on drop ratio



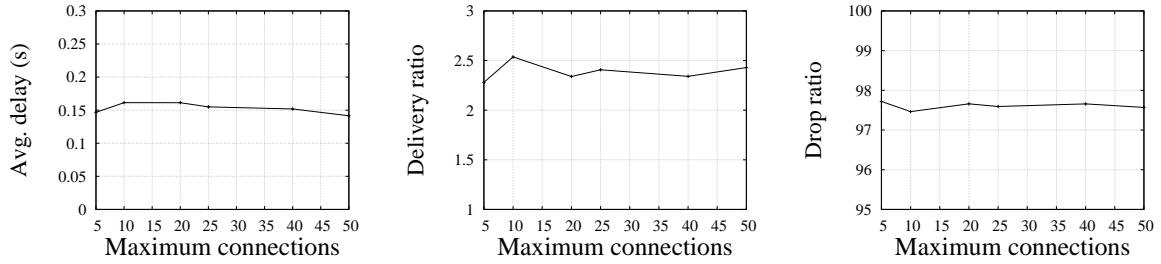
(d) Impact on average throughput

(e) Impact on average energy consumption

Figure 7.3: Impact of variation in packet rate on different performance metrics while using UDP with AODV

The impact of different packet transmission rates on different performance metrics is illustrated in Fig. 7.3. Here, Fig. 7.3a and Fig. 7.3c exhibit similar increasing trend for average delay and drop ratio respectively. On the contrary, delivery ratio (Fig. 7.3b) and average energy consumption (Fig. 7.3e) decrease with an increase in data rate. Besides, average throughput (Fig. 7.3d) increases at lower data rates. However, decreases at a diminishing rate for high data rates.

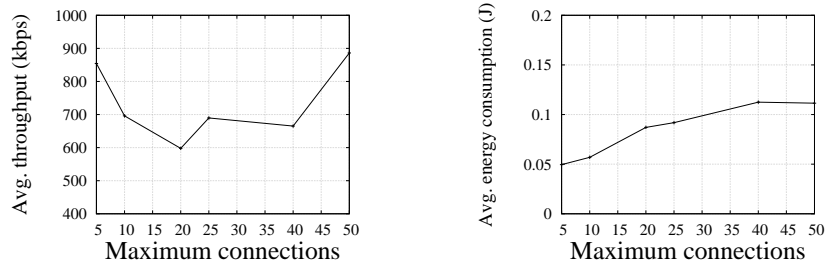
The impact of variation in the number of maximum allowed connections among the nodes on different performance metrics is demonstrated in Fig. 7.4. Here, Fig. 7.4a, Fig. 7.4b, and Fig. 7.4c exhibit almost similar trend of having similar values irrespective of variation in the number of maximum connections for average delay, delivery ratio, and drop ratio respectively. However, average throughput (Fig. 7.4d) again exhibits fluctuation rather presenting a trend. Besides, we see that average energy consumption increases with an increase in the number of maximum connections (Fig. 7.4e).



(a) Impact on average delay

(b) Impact on delivery ratio

(c) Impact on drop ratio



(d) Impact on average throughput

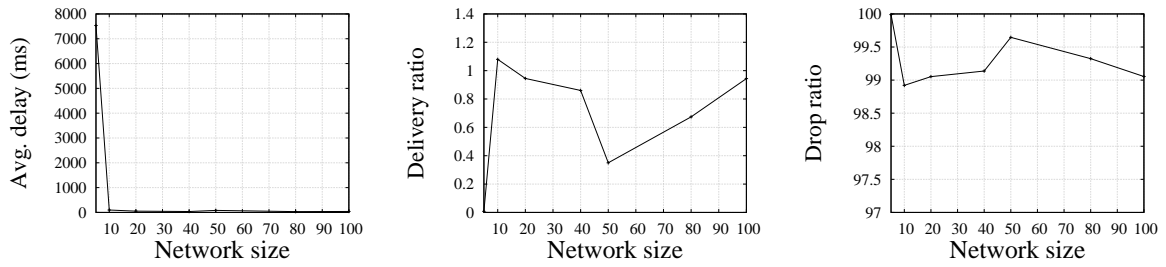
(e) Impact on average energy consumption

Figure 7.4: Impact of variation in the number of maximum allowed connections among the nodes on different performance metrics while using UDP with AODV

7.3.1.2 UDP with DSDV

Now, we enable DSDV, in place of AODV as done in previous case in the network layer, to investigate the impact of network layer operation on the metrics. Here, Fig. 7.5 demonstrates the impact of variation in network size on different performance metrics. Fig. 7.5a shows that the value of average end-to-end delay is very high for small number of nodes, however, it depicts no significant difference for higher number of nodes. This happens due to periodic updates in DSDV, which requires more time to find a routing path over a small number of mobile nodes in comparison to that incurred in on-demand update of AODV. Besides, delivery ratio (Fig. 7.5b) and average throughput (Fig. 7.5d) exhibit fluctuating values with the variation in network size. However, in Fig. 7.5c and Fig. 7.5e drop ratio and average energy consumption depict two visible trends respectively. Average energy consumption increases with the increment in network size, however, the rate of increment diminishes for larger networks.

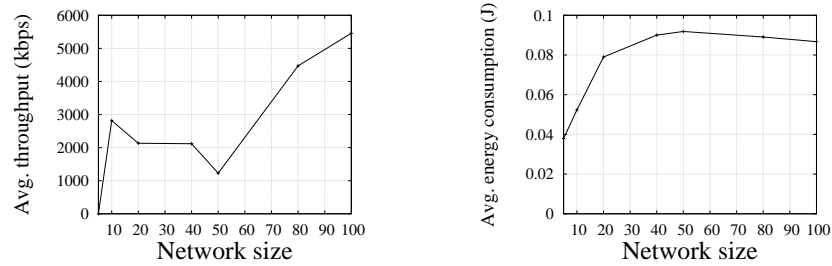
The impact of variation in speed of the nodes in MANET on different performance met-



(a) Impact on average delay

(b) Impact on delivery ratio

(c) Impact on drop ratio



(d) Impact on average throughput

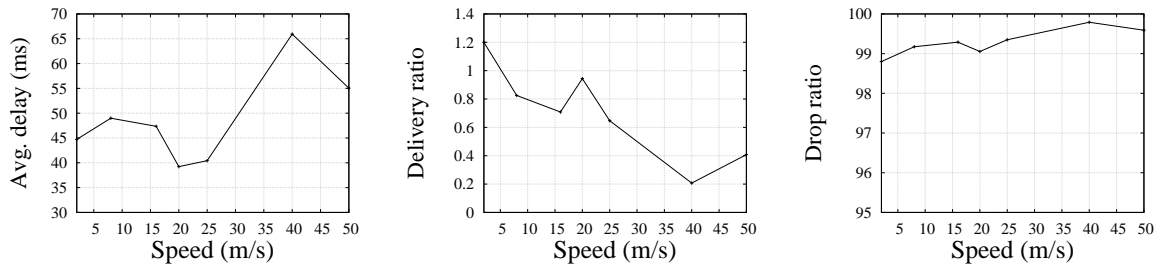
(e) Impact on average energy consumption

Figure 7.5: Impact of variation in network size on different performance metrics while using UDP with DSDV

rics is demonstrated in Fig. 7.6. Here, from Fig. 7.6a, Fig. 7.6b, and Fig. 7.6d it is clearly evident that average delay, delivery ratio, and average throughput exhibit no specific pattern in response to variation in the speed of nodes. However, drop ratio in Fig. 7.6c and average energy consumption in Fig. 7.6e exhibit an increasing and a decreasing trend respectively.

The impact of variation in packet transmission rate on different performance metrics is demonstrated in Fig. 7.7. Here, average delay exhibits a visible trend (Fig. 7.7a). Besides, delivery ratio and average energy consumption depict a decreasing trend where the rate of decrease diminishes with an increase in packet rate. Fig. 7.7b and Fig. 7.7e portray the trend. In addition, drop ratio represents an increasing trend as shown in Fig. 7.7c. The average throughput increases up to a certain packet rate, and then starts to decrease (Fig. 7.7d).

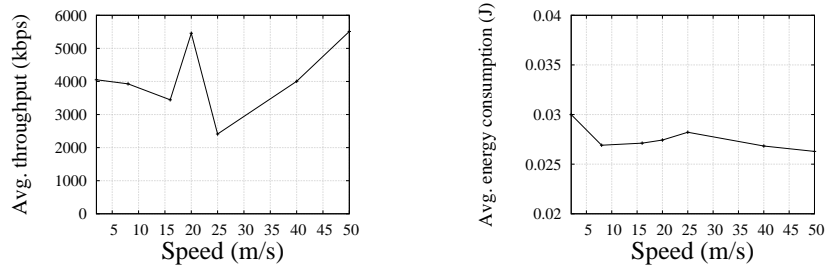
The impact of variation in the number of maximum allowed connections among nodes on different metrics is exhibited in Fig. 7.8. Here, average delay (Fig. 7.8a), drop ratio (Fig. 7.8c), and average energy consumption (Fig. 7.8e) exhibit some visible trends. However, we fail to determine any significant pattern for delivery ratio (Fig. 7.8b) and average throughput



(a) Impact on average delay

(b) Impact on delivery ratio

(c) Impact on drop ratio



(d) Impact on average throughput

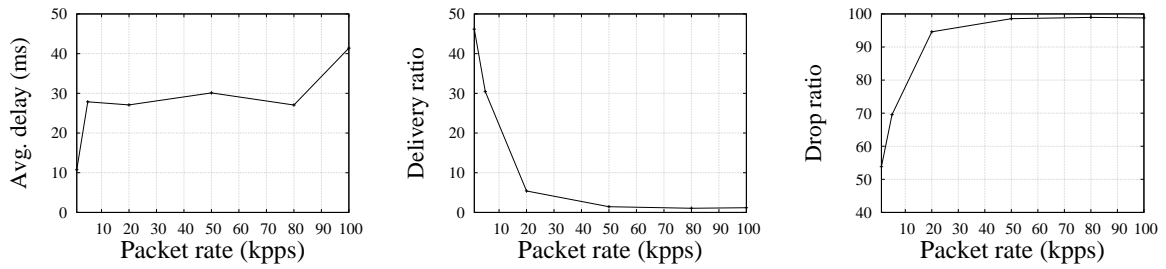
(e) Impact on average energy consumption

Figure 7.6: Impact of variation in speed of the nodes on different performance metrics while using UDP with DSDV

(Fig. 7.8d).

7.3.1.3 TCP Vegas with AODV

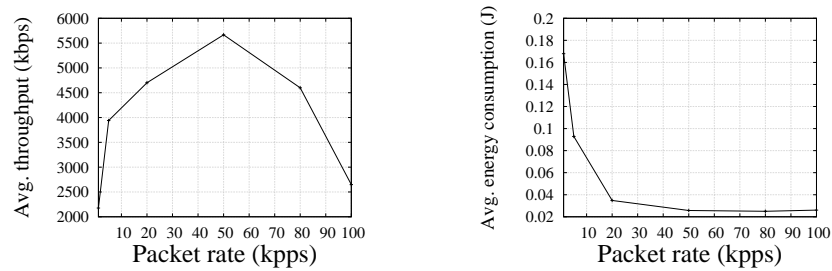
Next, we enable different variants of TCP in transport layer (with AODV in network layer) to investigate the impact of transport layer operations. Fig. 7.9 demonstrates the impact of variation in network size on different performance metrics with TCP Vegas in the transport layer and AODV in the network layer. Here, average delay (Fig. 7.9a) and delivery ratio (Fig. 7.9b) exhibit fluctuations. Besides, Fig. 7.9c and Fig. 7.9e exhibit fluctuations for drop ratio and average energy consumption. Nonetheless, average throughput also exhibits a bit fluctuation as shown in Fig. 7.9d. These outcomes reveal that the performance of MANETs significantly vary based on the operation of transport layer as the trends in Fig. 7.1 and Fig. 7.9 differ significantly. The impact of variation in speed of the nodes in MANET on different performance metrics is illustrated in Fig. 7.10. In response to a variation in speed, average delay (Fig. 7.10a), drop ratio (Fig. 7.10c), average throughput (Fig. 7.10d), and average energy consumption (Fig. 7.10e) exhibit no specific trends. However, delivery ratio



(a) Impact on average delay

(b) Impact on delivery ratio

(c) Impact on drop ratio



(d) Impact on average throughput

(e) Impact on average energy consumption

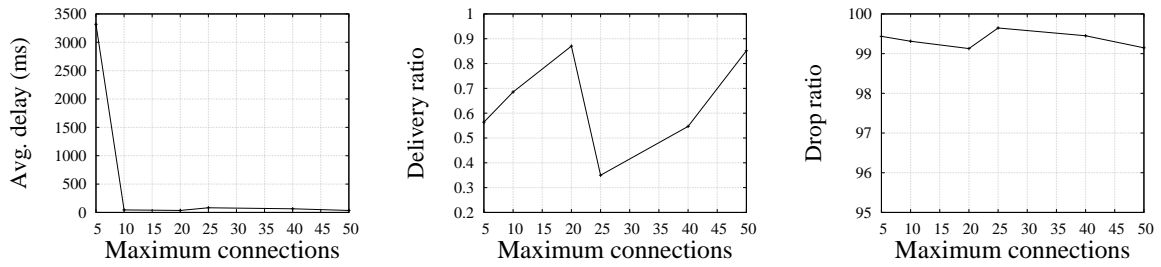
Figure 7.7: Impact of variation in packet rate on different performance metrics while using UDP with DSDV

decreases with an increase in speed as shown in Fig. 7.10b.

The impact of variation in packet transmission rate on different performance metrics is illustrated in Fig. 7.11. Here, average delay depicts no specific trend (Fig. 7.11a). In addition, delivery ratio increases with an increase in packet rate and the rate of increase diminishes at higher packet rates (Fig. 7.11b). Besides, drop ratio decreases with a diminishing rate of decrease (Fig. 7.11c). Additionally, average throughput (Fig. 7.11d) and average energy consumption (Fig. 7.11e) exhibit a linear increase with an increase in packet rate.

The influence of variation in the maximum number of allowed connections on difference performance metrics is illustrated in Fig. 7.12. Here, Fig. 7.12a, Fig. 7.12b, and Fig. 7.12c shows that average delay, delivery ratio and drop ratio exhibit fluctuations with a variation in the number of maximum connections.

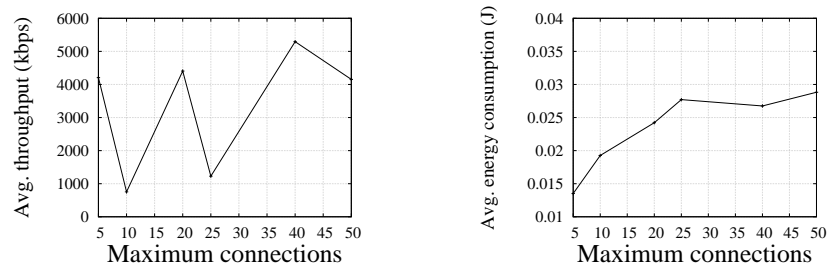
However, average throughput and average energy consumption exhibit a decreasing trend with an increase in the maximum number of connections after a certain value of it (Fig. 7.12d and Fig. 7.12e).



(a) Impact on average delay

(b) Impact on delivery ratio

(c) Impact on drop ratio



(d) Impact on average throughput

(e) Impact on average energy consumption

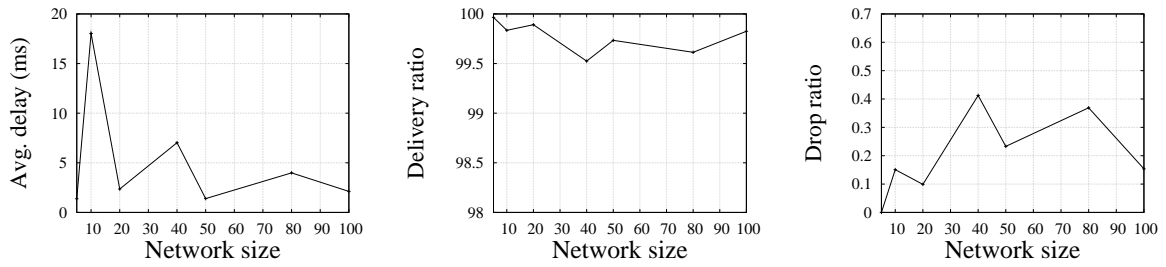
Figure 7.8: Impact of variation in the number of maximum allowed connections among the nodes on different performance metrics while using UDP with DSDV

7.3.1.4 TCP Vegas with DSDV

Now, we enable DSDV, in place of AODV in the network layer. Here, Fig. 7.13 illustrates the impact of variation in network size on different performance metrics while using DSDV in the network layer with TCP Vegas in the transport layer. Here, none of the metrics exhibit any visible trend. Fig. 7.13 portrays the metrics in this case.

The influence of different speed of nodes on different performance metrics is demonstrated in Fig. 7.14. Similar to the outcome of network size, the behavior of different metrics also do not follow any trend in response to a variation in speed. Fig. 7.14 depicts the values of different metrics.

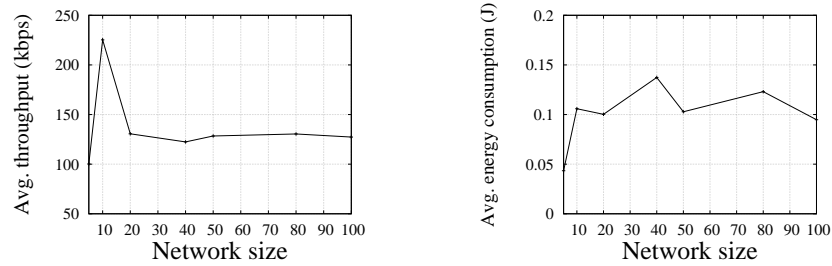
The impact of variation in packet rate on different metrics is illustrated in Fig. 7.15. Here, Fig. 7.15a and Fig. 7.15c show that average delay and drop ratio decrease with an increase in packet rate. However, the rate of change diminishes with an increase in packet rate. Besides, the values of delivery ratio and average energy consumption increase with an increase in packet rate. These results are illustrated in Fig. 7.15b and Fig. 7.15e respec-



(a) Impact on average delay

(b) Impact on delivery ratio

(c) Impact on drop ratio



(d) Impact on average throughput

(e) Impact on average energy consumption

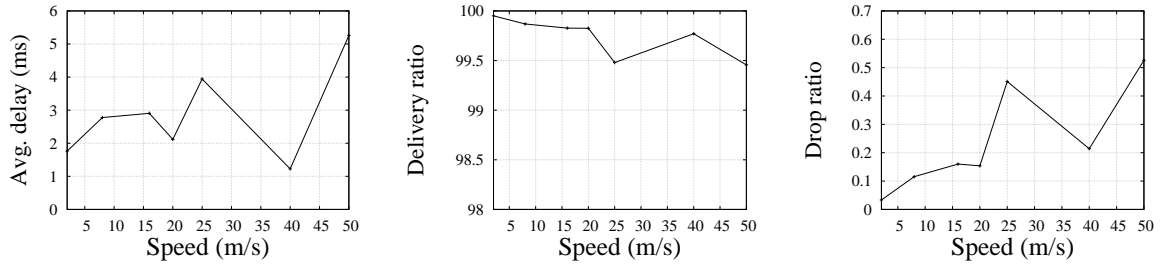
Figure 7.9: Impact of variation in network size on different performance metrics while using TCP Vegas with AODV

tively. Additionally, average throughput does not follow any specific pattern, as shown in Fig. 7.15d.

The impact of variation in the maximum number of allowed connections on different performance metrics is illustrated in Fig. 7.16. Here, Fig. 7.16a and Fig. 7.16c show that average delay and drop ratio decrease with an increase in the maximum number of connections. However, the rate of change diminishes for higher number of connections. Besides, the value of delivery ratio (Fig. 7.16b) increases with an increase in the maximum number of connections, where the rate of increase diminishes with an increase in the number of maximum connections. However, average throughput and energy consumption do not exhibit any specific trend (Fig. 7.16d and Fig. 7.16e).

7.3.1.5 TCP Westwood with AODV

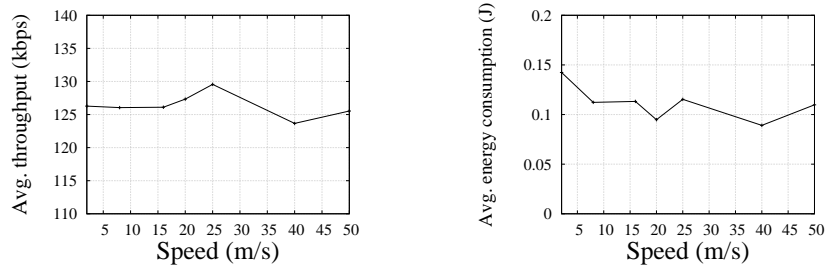
Next, we enable another TCP variant, TCP Westwood in the transport layer with AODV in the network layer. Here, Fig. 7.17 illustrates the impact of variation in network size on different performance metrics. Fig. 7.17a depicts no specific pattern for average delay with



(a) Impact on average delay

(b) Impact on delivery ratio

(c) Impact on drop ratio



(d) Impact on average throughput

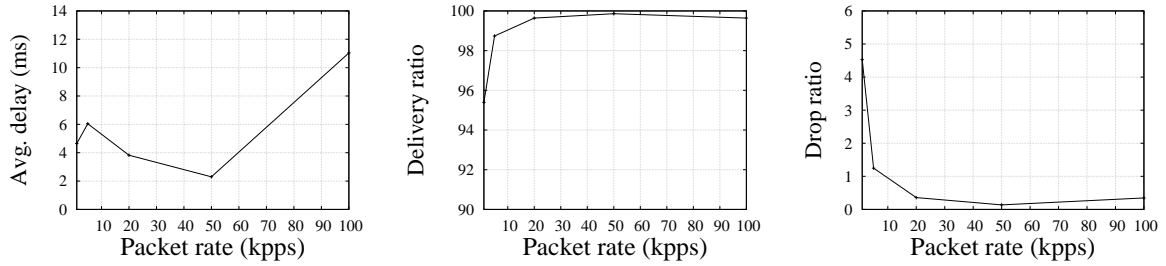
(e) Impact on average energy consumption

Figure 7.10: Impact of variation in speed of the nodes on different performance metrics while using TCP Vegas with AODV

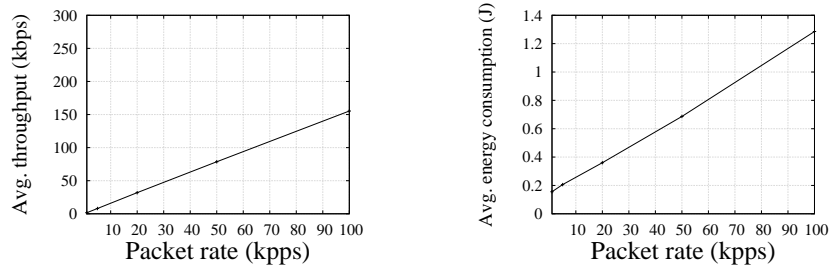
the variation in the number of nodes. However, delivery ratio increases for higher number of nodes (Fig. 7.17b). Nonetheless, drop ratio in Fig. 7.17c and average throughput in Fig. 7.17d show fluctuations rather than any visible trend. Besides, average energy consumption in Fig. 7.17e increases with an increase in network size.

The impact of variation in the speed of mobile nodes on different metrics is shown in Fig. 7.18. Here, Fig. 7.18a shows that average delay fails to show any pattern when the speed is changing. However, delivery ratio mostly decreases with an increase in speed, as demonstrated in Fig. 7.18b. Additionally, drop ratio in Fig. 7.18c, average throughput in Fig. 7.18d, and average energy consumption in Fig. 7.18e exhibit fluctuations with the variation in speed.

The impact of variation in packet transmission rate is illustrated in Fig. 7.19. Here, Fig. 7.19a shows that average delay fails to present any trend with the change in packet rate. However, delivery ratio (Fig. 7.19b), average throughput (Fig. 7.19d), and average energy consumption (Fig. 7.19e) increase with an increase in packet rate and the rate of increase diminishes for higher packet rates. Besides, drop ratio in Fig. 7.19c decreases for higher



(a) Impact on average delay (b) Impact on delivery ratio (c) Impact on drop ratio



(d) Impact on average throughput (e) Impact on average energy consumption

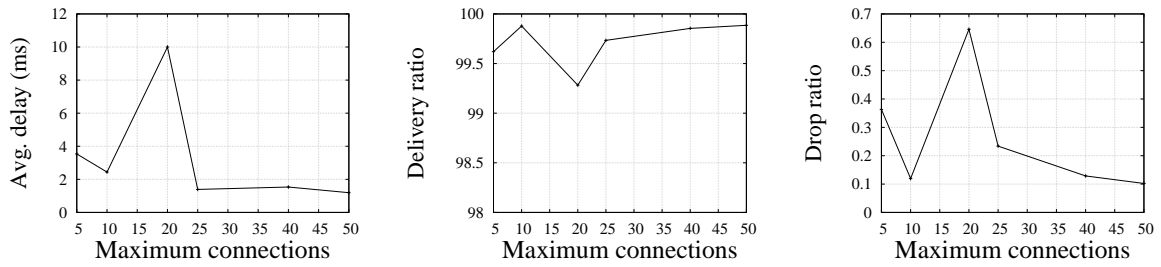
Figure 7.11: Impact of variation in packet rate on different performance metrics while using TCP Vegas with AODV

packet rates.

The impact of variation in the number of maximum allowed connections on different performance metrics is illustrated in Fig. 7.20. Here, Fig. 7.20a shows that average delay exhibit no specific trend with the change in the maximum number of connections. However, delivery ratio (Fig. 7.20b) mostly remains same with an increase in the maximum number of connections. Besides, drop ratio (Fig. 7.20c) and average throughput (Fig. 7.20d) exhibit fluctuations. In addition, average energy consumption in Fig. 7.20e mostly exhibit an increasing trend with an increase in the number of maximum connections.

7.3.1.6 TCP Westwood with DSDV

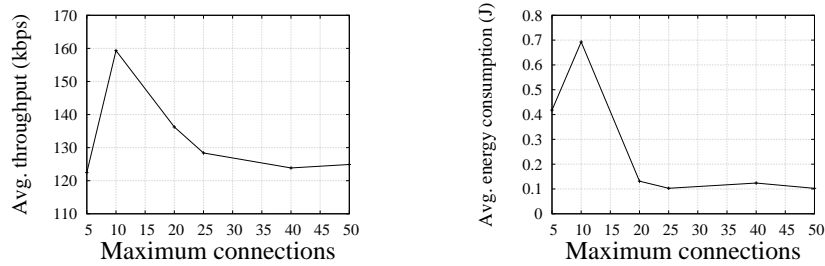
Next, we enable DSDV in place of AODV with TCP Westwood. Here, Fig. 7.21 demonstrates the impact of variation in network size on different metrics while using TCP Westwood in the transport layer with DSDV in the network layer. Here, average delay increases for lower number of nodes, however, for higher number of nodes it exposes much stable pattern (in Fig. 7.21a). In addition, delivery ratio in Fig. 7.21b exhibits an increasing pattern, in



(a) Impact on average delay

(b) Impact on delivery ratio

(c) Impact on drop ratio



(d) Impact on average throughput

(e) Impact on average energy consumption

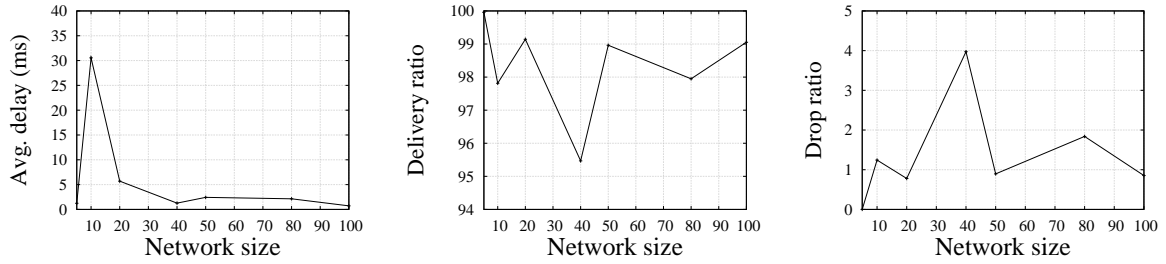
Figure 7.12: Impact of variation in the number of maximum allowed connections among the nodes on different performance metrics while using TCP Vegas with AODV

contrast, drop ratio (Fig. 7.21c) depicts a decreasing trend with the increase of network size for higher number of nodes. However, average throughput (Fig. 7.21d) shows considerable fluctuation over diverse network size. Besides, average energy consumption in Fig 7.21e mostly exhibits an increasing trend with the increase in network size.

Fig. 7.22 illustrates the impact of variation in speed of nodes on different performance metrics. Here, average delay (Fig. 7.22a), drop ratio (Fig. 7.22c), and average throughput (Fig. 7.22d) exhibit no specific trend in this case. However, delivery ratio (Fig. 7.22b) and average energy consumption (Fig. 7.22e) decrease with an increase in speed.

Fig. 7.23 exhibits the impact of variation in packet transmission rate on different metrics. Here, average delay in Fig. 7.23a decreases for higher packet rates. Besides, delivery ratio (Fig. 7.23b) increases with packet rate. In addition, drop ratio in Fig. 7.23c decreases with an increase in packet rate. However, average throughput marginally increases for higher packet rates (Fig. 7.23d). Additionally, average energy consumption (Fig. 7.23e) significantly increases with an increase in packet rate.

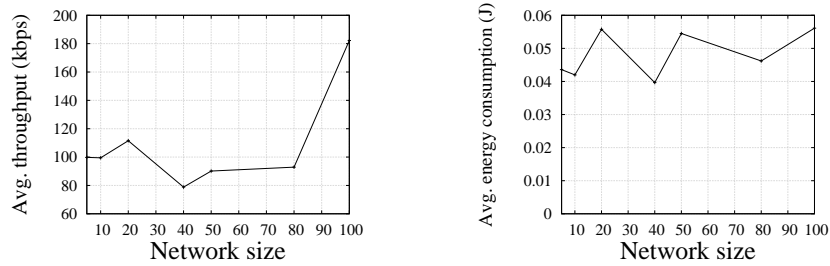
Now, the impact of maximum number of allowed connections on different metrics is



(a) Impact on average delay

(b) Impact on delivery ratio

(c) Impact on drop ratio



(d) Impact on average throughput

(e) Impact on average energy consumption

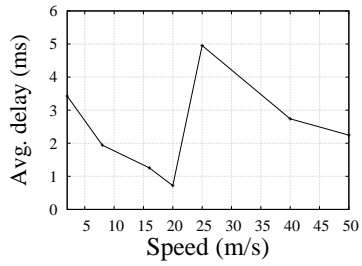
Figure 7.13: Impact of variation in network size on different performance metrics while using TCP Vegas with DSDV

illustrated in Fig. 7.24. Here, average delay decreases up to a certain number of connections, and then starts to increase afterward (Fig. 7.24a). Besides, delivery ratio in Fig. 7.24b and average energy consumption in Fig. 7.24e increase with an increase in the number of maximum connections. However, drop ratio (in Fig. 7.24c) and average throughput (in Fig. 7.24d) decrease with an increase in the number of allowed maximum connections.

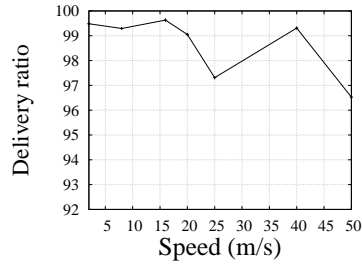
7.4 Discussion

We perform rigorous simulation considering diversified settings in order to investigate the performance of MANETs. Here, our investigation is based on analyzing the trends of five different performance metrics. We summarize the outcome of our simulation in Table 7.3. Analyzing the summary, we can highlight the following findings:

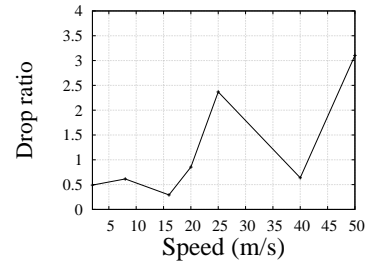
- The performance of MANETs not only depends on the variation of different network parameters such as network size, speed, packet rate, and maximum connections, but also on the change in network layer and transport layer protocol.



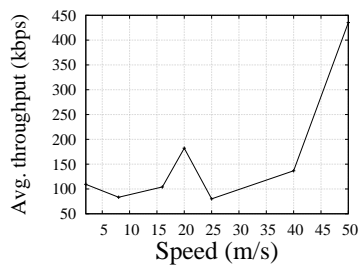
(a) Impact on average delay



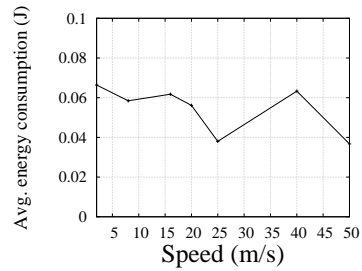
(b) Impact on delivery ratio



(c) Impact on drop ratio

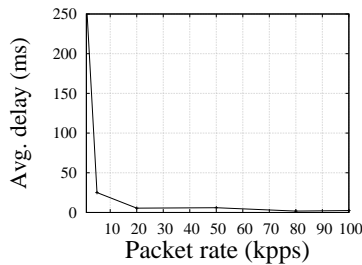


(d) Impact on average throughput

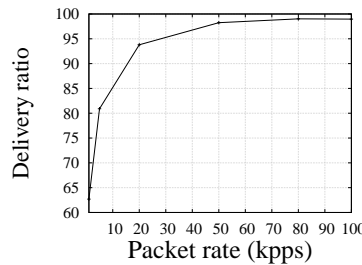


(e) Impact on average energy consumption

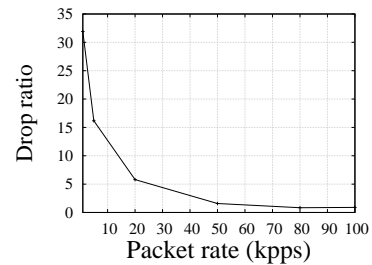
Figure 7.14: Impact of variation in speed of the nodes on different performance metrics while using TCP Vegas with DSDV



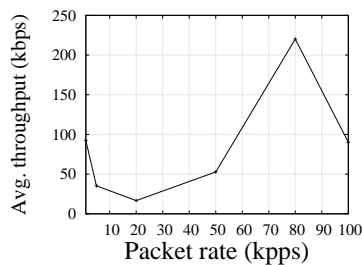
(a) Impact on average delay



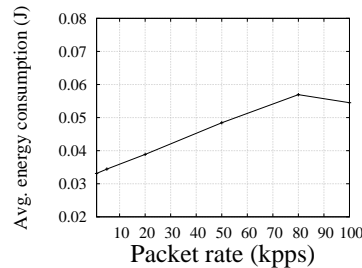
(b) Impact on delivery ratio



(c) Impact on drop ratio

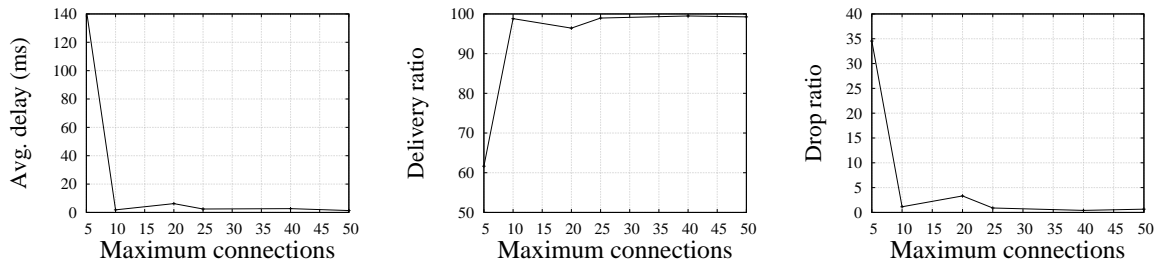


(d) Impact on average throughput



(e) Impact on average energy consumption

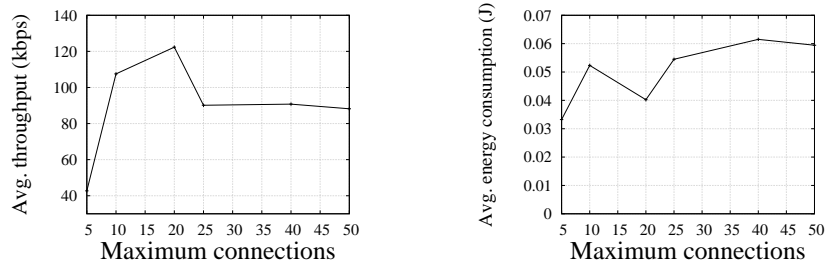
Figure 7.15: Impact of variation in packet rate on different performance metrics while using TCP Vegas with DSDV



(a) Impact on average delay

(b) Impact on delivery ratio

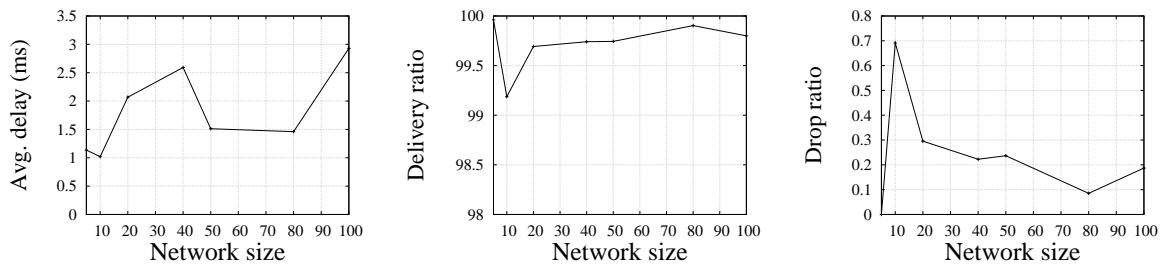
(c) Impact on drop ratio



(d) Impact on average throughput

(e) Impact on average energy consumption

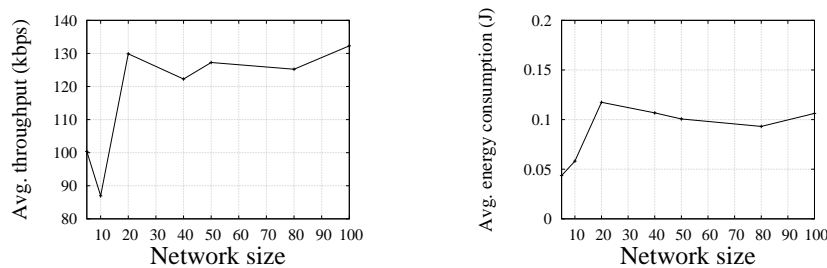
Figure 7.16: Impact of variation in the number of maximum allowed connections among the nodes on different performance metrics while using TCP Vegas with DSDV



(a) Impact on average delay

(b) Impact on delivery ratio

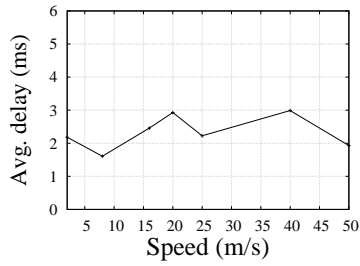
(c) Impact on drop ratio



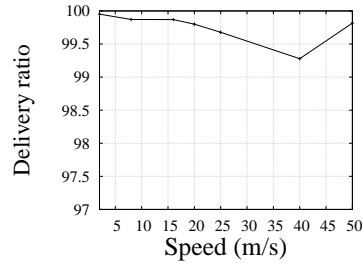
(d) Impact on average throughput

(e) Impact on average energy consumption

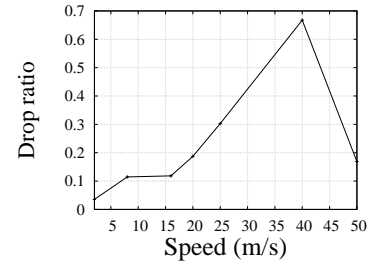
Figure 7.17: Impact of variation in network size on different performance metrics while using TCP Westwood with AODV



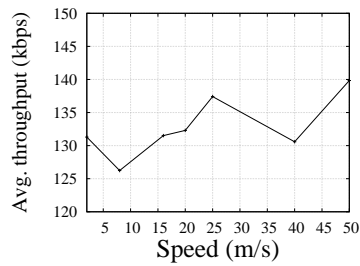
(a) Impact on average delay



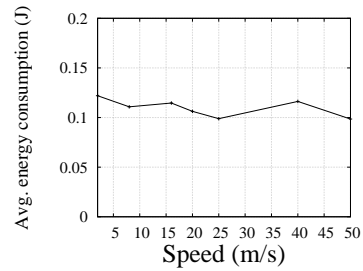
(b) Impact on delivery ratio



(c) Impact on drop ratio

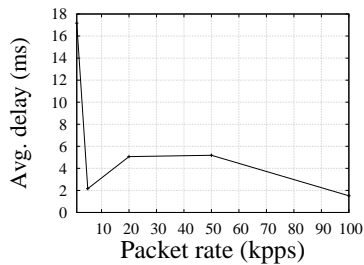


(d) Impact on average throughput

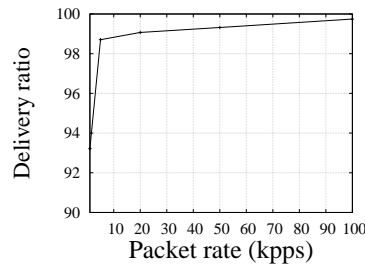


(e) Impact on average energy consumption

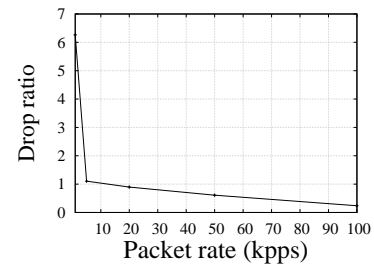
Figure 7.18: Impact of variation in speed of the nodes on different performance metrics while using TCP Westwood with AODV



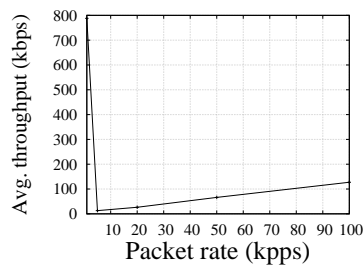
(a) Impact on average delay



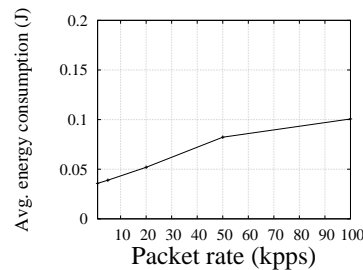
(b) Impact on delivery ratio



(c) Impact on drop ratio

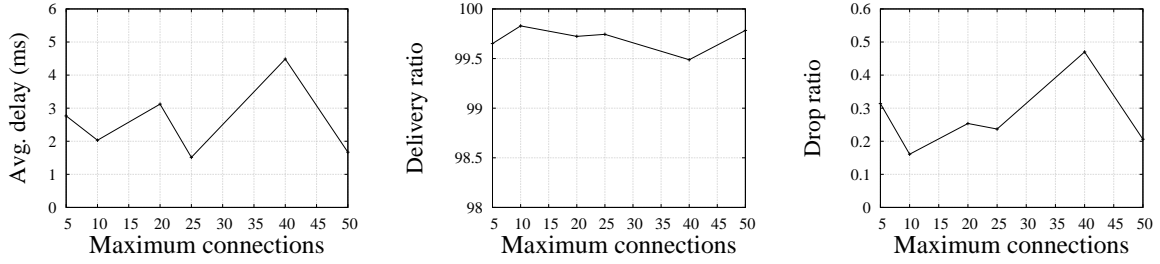


(d) Impact on average throughput



(e) Impact on average energy consumption

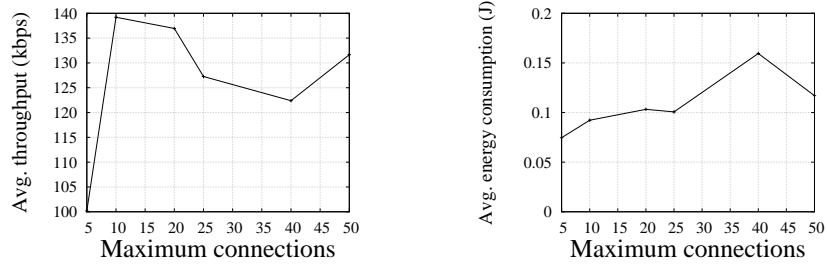
Figure 7.19: Impact of variation in packet rate on different performance metrics while using TCP Westwood with AODV



(a) Impact on average delay

(b) Impact on delivery ratio

(c) Impact on drop ratio



(d) Impact on average throughput

(e) Impact on average energy consumption

Figure 7.20: Impact of variation in the number of maximum allowed connections among the nodes on different performance metrics while using TCP Westwood with AODV

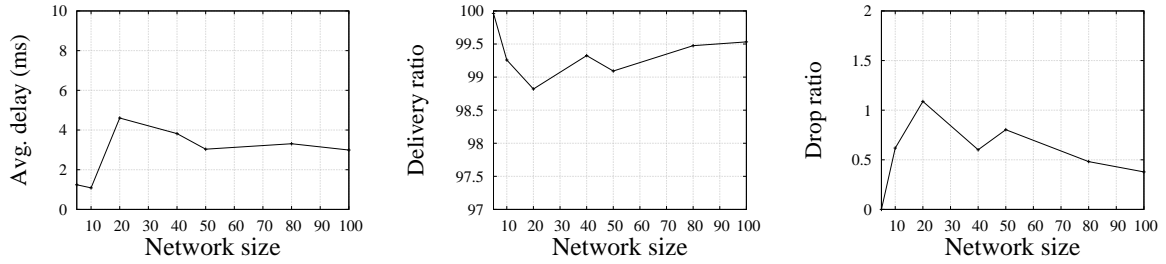
- Consequently, we need to develop cross-layer mathematical models for modeling the performance of MANETs.
- Besides, all the performance metrics do not exhibit visible trends with a variation in network and operational parameters. Now, we assess the feasibility of such mathematical models for MANETs.

7.4.1 Analysis of Feasibility

To assess viability of such diverse mathematical model, we first develop polynomial functions using MATLAB for all the outcomes corresponding to each metrics. A general form of the equation is shown in Equation 7.1.

$$f(x) = p_1 \times x^6 + p_2 \times x^5 + p_3 \times x^4 + p_4 \times x^3 + p_5 \times x^2 + p_6 \times x + p_7 \quad (7.1)$$

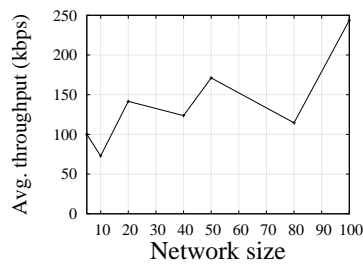
Here, we find that all the metrics exhibit graphs following polynomial equations having degrees five or higher. In this chapter, we attempt to represent some of the equations pertinent for the metrics.



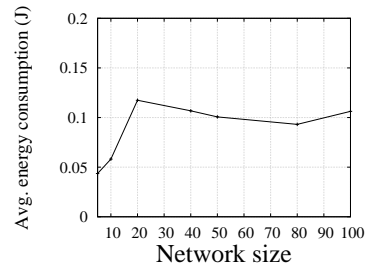
(a) Impact on average delay

(b) Impact on delivery ratio

(c) Impact on drop ratio



(d) Impact on average throughput

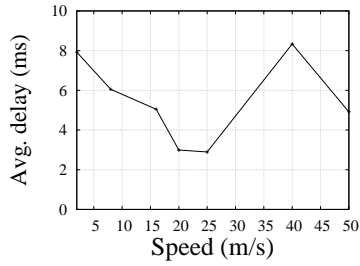


(e) Impact on average energy consumption

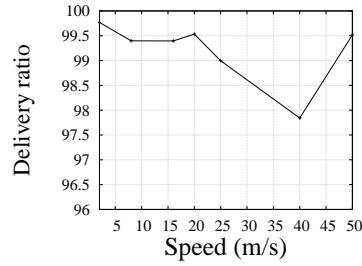
Figure 7.21: Impact of variation in network size on different performance metrics while using TCP Westwood with DSDV

We find from Table 7.3 that variation in packet transmission rate exhibits good trends. Therefore, we derive polynomial representations for all the metrics in case of variation in packet rate. Such representations exhibit higher order polynomial functions as shown in Table 7.4 with corresponding co-efficients. We present a few more results for average delay and delivery ratio in case of variation in network size in Table 7.5 and Table 7.6 respectively. These results reveal that we need to solve equations with higher-order in order to develop mathematical models. Now equations having order of five or greater than five are algebraically unsolvable according to *Abel-Ruffini theorem* [278]. Therefore, we can conclude that cross layer modeling of MANETs and deriving their closed forms are simply not feasible. Hence, we propose a lemma as follows:

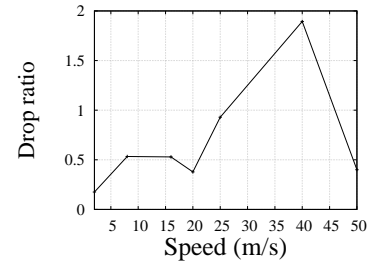
Lemma 1 *Mathematical modeling of mobile wireless networks considering variations in all parameters is not feasible.*



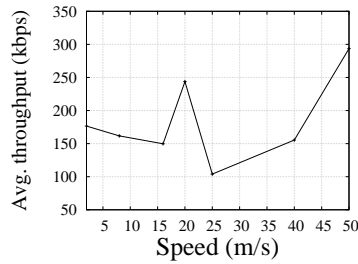
(a) Impact on average delay



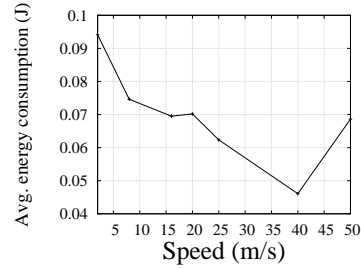
(b) Impact on delivery ratio



(c) Impact on drop ratio

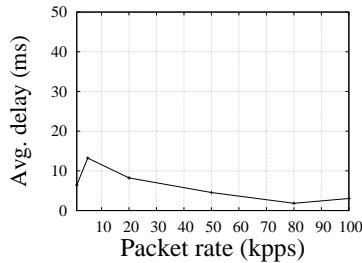


(d) Impact on average throughput

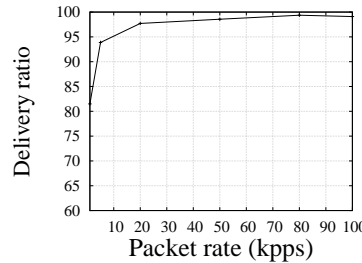


(e) Impact on average energy consumption

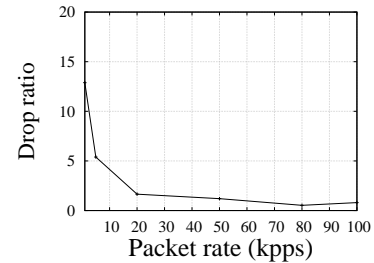
Figure 7.22: Impact of variation in speed of the nodes on different performance metrics while using TCP Westwood with DSDV



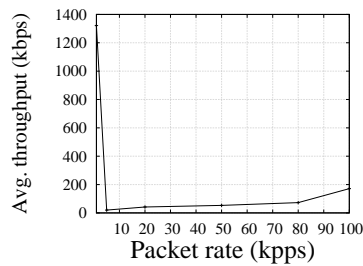
(a) Impact on average delay



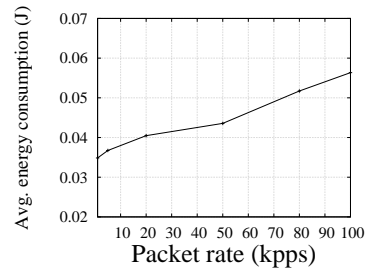
(b) Impact on delivery ratio



(c) Impact on drop ratio

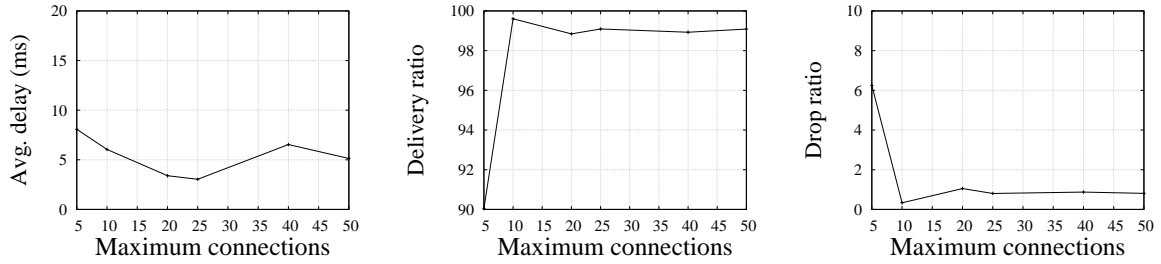


(d) Impact on average throughput



(e) Impact on average energy consumption

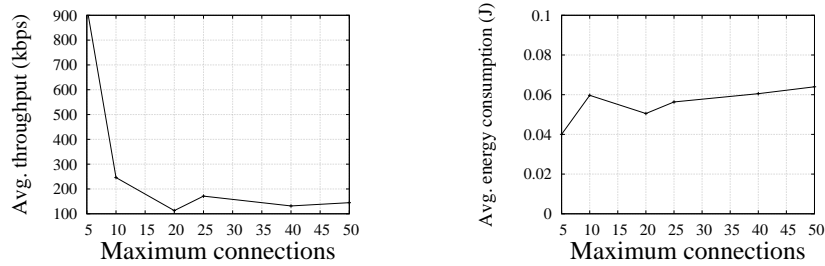
Figure 7.23: Impact of variation in packet rate on different performance metrics while using TCP Westwood with DSDV



(a) Impact on average delay

(b) Impact on delivery ratio

(c) Impact on drop ratio



(d) Impact on average throughput

(e) Impact on average energy consumption

Figure 7.24: Impact of variation in the number of maximum allowed connections among the nodes on different performance metrics while using TCP Westwood with DSDV

7.5 Conclusion

The recent flourish in diversified applications of MANETs necessitates the evaluation of performance of MANETs. Mathematical models serve as the fastest and the most cost-effective means to perform the evaluation task comparing to other alternatives such as simulation and testbed experiment. However, earlier studies on mathematical modeling fail to simultaneously consider the impact of variation in different parameters and also ignore the crucial influence of the operation of upper layers such as network and transport layers.

Moreover, the studies develop mathematical model only for average end-to-end delay and average throughput. However, other matrices such as average energy consumption, delivery ratio, and drop ratio remain yet to be explored. Therefore, in this work, we analyze the feasibility of developing mathematical models considering the impact of parameters and upper layers in the protocol stack. In our analysis, we perform rigorous simulation utilizing *ns-2* to capture the performance of MANETs in diversified environment. Afterwards, we asses the feasibility of mathematical modeling through studying the simulation results.

Metrics	Transport & Network layer protocols	Network parameter under variation			
		Network Size	Speed	Packet rate	Max. connections
Average delay	UDP wth AODV	No	Yes	Yes	Yes
	TCP Vegas with AODV	No	No	No	No
	TCP Westwood with AODV	No	No	No	No
	UDP with DSDV	Yes	No	Yes	Yes
	TCP Vegas with DSDV	No	No	Yes	Yes
	TCP Westwood with DSDV	Yes	No	Yes	Yes
Delivery ratio	UDP wth AODV	Yes	Yes	Yes	Yes
	TCP Vegas with AODV	No	Yes	Yes	No
	TCP Westwood with AODV	Yes	Yes	Yes	Yes
	UDP with DSDV	No	No	Yes	No
	TCP Vegas with DSDV	No	No	Yes	Yes
	TCP Westwood with DSDV	Yes	Yes	Yes	Yes
Drop ratio	UDP wth AODV	Yes	Yes	Yes	Yes
	TCP Vegas with AODV	No	No	Yes	No
	TCP Westwood with AODV	No	No	Yes	No
	UDP with DSDV	Yes	Yes	Yes	Yes
	TCP Vegas with DSDV	No	No	Yes	Yes
	TCP Westwood with DSDV	Yes	No	Yes	Yes
Average throughput	UDP wth AODV	No	No	Yes	No
	TCP Vegas with AODV	No	No	Yes	Yes
	TCP Westwood with AODV	No	No	Yes	No
	UDP with DSDV	No	No	Yes	No
	TCP Vegas with DSDV	No	No	No	No
	TCP Westwood with DSDV	No	No	Yes	Yes
Average energy consumption	UDP wth AODV	Yes	Yes	Yes	Yes
	TCP Vegas with AODV	No	No	Yes	Yes
	TCP Westwood with AODV	Yes	No	Yes	Yes
	UDP with DSDV	Yes	Yes	Yes	Yes
	TCP Vegas with DSDV	No	No	Yes	No
	TCP Westwood with DSDV	Yes	Yes	Yes	Yes

Table 7.3: Summary of all simulation results

Metrics	p_1	p_2	p_3	p_4	p_5	p_6
Average delay	$2.492e - 26$	$-3.499e - 21$	$-4.08e - 21$	$6.60e - 11$	$-3.85e - 11$	0.03503
Average energy consumption	$-1.27e - 23$	$3.26e - 16$	$-2.96e - 13$	$1.13e - 8$	-0.00017	0.8675
Average throughput	$8.7e - 21$	$-2.59e - 15$	$2.84e - 10$	$-1.36e - 5$	0.2281	1349
Delivery ratio	$-1.39 - 21$	$3.58e - 16$	$-3.27e - 11$	$1.26e - 6$	-0.01949	99.86
Drop ratio	$1.39e - 21$	$-3.58e - 16$	$3.27e - 11$	$-1.26e - 11$	0.01949	0.1356

Table 7.4: Co-efficients for varying packet rate for UDP with AODV

Consequently, we find that we need to develop cross-layer mathematical models to represent the performance of MANETs. Besides, such models need to resolve higher-order polynomial equations, which is algebraically unsolvable. Therefore, mathematical modeling of

Metrics	Transport & Network layer	Varying network size						
		p_1	p_2	p_3	p_4	p_5	p_6	p_7
Average delay	UDP wth AODV	$-4.53e - 10$	$1.3e - 007$	$1.4e - 5$	0.00078	-0.020	0.2201	-0.5488
	TCP Vegas with AODV	$-5.332e - 8$	$1.53e - 5$	-0.0016	0.08655	-2.164	23.51	-71.86
	TCP Westwood with AODV	$7.25e - 11$	$-2.09e - 8$	$2.26e - 6$	-0.00011	0.0025	-0.0196	0.09028
	UDP with DSDV	$8.83e - 6$	-0.00264	0.3044	-16.93	472.6	-6136	$2.83e4$
	TCP Vegas with DSDV	$-6.59e - 8$	$1.96e - 5$	-0.0022	0.12	-3.168	36.18	-114.1
	TCP Westwood with DSDV	$5.07e - 9$	$-1.498e - 6$	0.00016	-0.0087	0.2111	-1.959	6.751

Table 7.5: Summery of all co-efficients of higher order functions for average delay for variation in network size

Metrics	Transport & Network layer	Varying network size						
		p_1	p_2	p_3	p_4	p_5	p_6	p_7
Delivery ratio	UDP wth AODV	$-1,22e - 9$	$3.88e - 7$	$-4.68e - 5$	0.00277	-0.083	1.189	-3.537
	TCP Vegas with AODV	$8.05e - 10$	$-2.21e - 7$	$2.257e - 5$	-0.00105	0.02336	-0.2296	100.6
	TCP Westwood with AODV	$1.599e - 9$	$-4.75e - 7$	$5.38e - 5$	-0.00291	0.07698	-0.892	102.8
	UDP with DSDV	$3.84e - 7$	-1.50 e8	2.30e8	-1.70 e8	6.09e7	-8.43e6	$6.11e4$
	TCP Vegas with DSDV	$1.171e - 8$	$-3.238e - 6$	0.00033	-0.0158	0.3575	-3.59	110.7
	TCP Westwood with DSDV	$-5.389e - 10$	$1.311e - 7$	$-1.047e - 5$	0.00025	0.0044	-0.2347	101

Table 7.6: Summery of all co-efficients of higher order functions for delivery ratio for variation in network size

MANETs considering variation in all parameters is simply *not* feasible. Accordingly, future effort on developing such cross-layer mathematical models for MANETs, considering all the diversity, need to proceed with specific assumptions to achieve a solvable outcome.

Next, in the final chapter, we draw the conclusion of our thesis by describing the major contributions of this research work.

Chapter 8

Conclusions

The gleaming prospect of cyber-physical networks results in the recent growth of diversified applications of infrastructure networks, e.g., transportation, smart spaces, health-care systems, industrial, and sensors networks. However, cyber-physical networks encounter various challenges towards the road to enhancing the network-level performance and security owing to limited resource issues. These limited resource issues include, but are not limited to, limited amount of available energy to feed the system, low processing capability, limited amount of storage space, and low bandwidth for network communication. Therefore, in this thesis, we attempt to explore the network-level performance and security issues of limited-resource cyber-physical networks.

In Part I, we focus on developing an integrated networking solution along with security issues for a real-time limited-resource cyber-physical network over railway systems of developing countries to prevent occurrences of derailments.

Derailment due to uprooted or faulty rail blocks is an epoch-making problem in many developing countries such as Bangladesh, India, Kenya, etc. Such derailments result in both death tolls and loss of property. Low-resource settings and the paucity of networking infrastructure in remote rail areas of developing countries pose a challenge in devising an automated real-time system for detecting uprooted or faulty rail blocks to stop such derailments. Therefore, as a remedy, in this thesis, we propose a new networking paradigm to facilitate devising an automated system leveraging a real-time communication between train and rail track, considering the aforementioned concerns. Here, we present a novel ad-hoc network

architecture, node deployment topology, and light-weight network protocols for enabling the communication. Our proposed paradigm offers a low-cost and lightweight solution for the intended purpose worth of adopting in developing countries. Nonetheless, the paradigm exhibits a near-to-perfect performance, which we evaluate through both $ns-2$ simulation and real experimental evaluation, yet maintaining the low-cost and lightweight status.

Such a system needs to be shielded from looming security threats posed by potential malicious adversaries. A rigorous study on the exploration of potential security threats and vulnerabilities of a real-time system specifically designed for detecting missing rail blocks in the context of developing countries is yet to be explored in the literature. Therefore, next, in this thesis, we focus on the security issues pertinent to our proposed networking solution for the real-time system of detecting missing rail blocks of the rail tracks. Towards that road, in this thesis, first, we introduce a new threat entitled as power attack through exploiting vulnerability pertinent to the energy source of the real-time system for detecting missing rail blocks. Consequently, we present both theoretical and mathematical modeling of attack models to effectively launch the power attack. Furthermore, we perform extensive experimentation using both $ns-2$ simulator and real deployment to investigate the applicability and the effectiveness of our exposed attack models for the real-time system for detecting missing rail blocks. Next, we present different attack models to effectively launch other traditional attacks such as man-in-the-middle attack and replay attack. Afterward, to mitigate these attacks, we propose a set of countermeasures. Consequently, we perform extensive experimentation using both $ns-2$ simulator and real deployment to demonstrate the effectiveness of our proposed countermeasures.

Next, in Part II of the thesis, we focus on the miniature versions of limited-resource cyber-physical networks. Here, we first investigate the network-level performance of nanonetworks. Since existing studies in the field of nanonetworks are still in the embryonic stage, we envision to investigate the enhancement of performance of such networks.

Recent advancement in nanotechnology fosters the emergence wireless nanonetworks. Researchers consider wireless nanonetworks as a revolutionary emerging network paradigm from the point of its diversified applications and contributions to the humanity. Nanonetworks are not just a simple extension of traditional communication networks at the nano-

scale. Owing to being a completely new communication paradigm, existing research in this field is still at a rudimentary stage. Furthermore, most of the existing studies focus on performance enhancement of nanonetworks via designing new channel models and routing protocols. However, the impacts of different types of nano-antennas on the network-level performances of the wireless nanonetworks remain still unexplored in the literature. Therefore, in this thesis, we explore the impacts of different well-known types of antennas such as patch, dipole, and loop nano-antennas on the network-level performances of wireless nanonetworks. We also investigate the performances of nanonetworks for different types of traditional materials (e.g., copper) and for nanomaterials (e.g., carbon nanotubes and graphene). We perform rigorous simulation using our customized ns-2 simulation to evaluate the network-level performances of nanonetworks exploiting different types of nano-antennas using different materials. Our evaluation reveals a number of novel findings pertinent to finding an efficient nano-antenna from its several alternatives for enhancing network-level performances of nanonetworks. Our evaluation demonstrates that a dipole nano-antenna using copper material exhibits around 51% better throughput and about 33% better end-to-end delay compared to other alternatives. Furthermore, our results are expected to exhibit high impacts on the future design of wireless nanonetworks through facilitating the process of finding the suitable type of nano-antenna and suitable material for the nano-antennas.

Next, we focus on another example of miniature versions, which is medical body area networks. The recent rise in aged population and chronic diseases is placing increasing pressure on health care expenditure. Ubiquitous health care is regarded as a potential driver in reducing such health expenditure. Advancement in wireless communication and sensor technologies permits real-time acquisition, transmission, and processing of critical medical information for ubiquitous health-care applications. Hence, medical body area networks (MBANs) emerge as a key technology to facilitate ubiquitous health-care services. However, energy restriction of micro-battery of a sensor device holds back the development of MBANs and also makes MBANs vulnerable to different malicious attacks. In this thesis, we focus on security issues for such networks. Here, first, we introduce a new attack entitled *Power Attack* exploiting power constraint of the sensor devices. Power attack forces a sensor

to die off due to lack of power supply. We propose attack models to launch power attack effectively. Consecutively, we analyze the viability of performing power attack in medical body area networks in reality using *Mannasim* simulator. Besides, we also propose countermeasure for the presented power attack. Finally, we exhibit an efficacy of our proposed countermeasure using experimental evaluation.

Finally, in Part III, we explore smarter versions of limited-resource cyber-physical networks. Security aspects of such networks have already been widely explored from different perspectives in the literature [66–68]. However, enhancement of networking performance exploiting available multi-radios is little explored in the literature. Therefore, in this thesis, first, we explore multi-radio smart devices such as smartphones, tablet, routers, walkie-talkie, etc. The pervasiveness of different wireless network technologies such as WiFi, WiMAX, UMTS, LTE, and Bluetooth facilitates the idea of having a wireless connection to the Internet always and everywhere. This aspect becomes more prevalent with the rapid advancement of multi-radio devices. To ensure a continuous connectivity to such ubiquitous heterogeneous wireless networks demands a general-purpose multi-objective vertical hand-off mechanism taking into account network dynamics as one of its decision attributes. However, to the best of our knowledge, such a mechanism is yet to be devised. Therefore, in this thesis, we propose a new multi-objective vertical hand-off (MOVH) mechanism taking into account network dynamics as one of its decision attributes. We customize Multi-Objective Genetic Algorithm (MOGA) in this regard. The results obtained from our numerical simulation demonstrate that the new mechanism yields better scalability and stability. We also evaluate the performance of our MOVH mechanism against two most popular alternatives: GRA and TOPSIS. This evaluation comprises of both test-bed experiments and *ns-2* simulation. The results from both test-bed experiments and *ns-2* simulation demonstrate that our MOVH mechanism has significant performance improvement over both GRA and TOPSIS.

Next, we focus on exploring the network-level performance of mobile adhoc networks (MANETs). The recent flourish of countless diversified applications of MANETs has emphasized the need to evaluate and enhance the network-level performance of such networks. Towards that road, derivation of mathematical models is considered as the fastest and the most cost-effective tool. However, feasibility analysis of mathematical modeling

for MANETs considering the impact of all layers in the protocol stack in addition to that of different parameters remains unexplored till now. Therefore, in this thesis, we attempt to analyze the feasibility of developing mathematical models for MANETs considering both of the aspects. In our analysis, we perform rigorous simulation utilizing ns-2 to capture the performance of MANETs under diversified settings. Our rigorous empirical study reveals that we need to develop cross-layer mathematical models to represent the performance of MANETs and such mathematical models need to resolve higher-order polynomial equations. Consequently, our study uncovers a key finding that *mathematical modeling of MANETs considering variation in all parameters is not feasible*.

8.1 Future Work

There are many avenues to extend the work presented in this dissertation.

In Part I, we have investigated real-time limited-resource cyber-physical networks over railway systems considering the constraints of developing countries. In this work, we have focused on providing a networking solution for real-time detection of missing rail blocks on the rail tracks (in Chapter 2). Consecutively, we also explored different security issues pertinent to such system (in Chapter 3). There are many aspects of this work that was beyond the scope of this dissertation. Some of the most immediate research opportunities can be summarized as follows:

- **Cross-junction addressing:** In this work, we consider a linear railway track while developing a network solution. However, in real-life there exist railways with cross-junctions. In railway cross-junctions, multiple rail tracks (maximum three) converge in or diverge from a common track. For such case, we have to consider distinct addressing of sensor nodes on different rail tracks and even for two parallel rail tracks. Incorporation of this addressing feature utilizing the reserved bits, which are introduced in our proposed communication paradigm (Fig. 2.9), could be a potential research direction in the future.
- **Fault tolerance:** According to our proposed communication paradigm for detection of missing rail blocks, if a sensor node does not respond to a query message, this can

imply two occurrences: (1) the sensor node is uprooted with rail block and (2) the wireless communication link with the sensor node is broken, though the rail track is maintaining its standard condition. In this thesis, in our proposed networking system, we only consider the first occurrence. In the future, fault tolerance feature could be incorporated into our system to make the system more robust against these issues. Besides, in the current work, we conduct real testbed deployment implanting the sensing module beside a rail block (Fig. 2.15). In future, we could conduct experiment with missing rail blocks by attaching the sensor module with a broken rail block.

- **Energy harvesting:** In our current system, we have used batteries as the energy sources of the sensor devices. However, Harnessing of solar energy may not adequate and reliable for our system on cloudy or foggy days. On the contrary, vibration and sound created by the train can be alternative energy sources in such cases. We have experimented in our lab with energy harvesting from vibration and obtained promising results. We want to further dig into it in the near future.
- **Feasibility of Incorporation of Long-Range Radio:** Our proposed protocol utilizes two-hop based solution to cover a distance of about 1000m as the train requires to receive the reply packet from about 1000m ahead for a safe stoppage in case of sensing a discontinuity. Here, this distance coverage can be extended using a high-gain antenna on the train. Besides, low-power long-range modules such as LoRa could be a potential choice to cover a longer distance. However, LoRa does not perform well in a dynamic scenario having a mobile node (the train in our case) [279]. Additionally, other long-range alternatives such as WiMAX generally incurs high energy consumption, hence, making it infeasible for our case. Therefore, the feasibility of adaptation a long-range radio demands detail analysis and exploration, which were beyond the scope of this dissertation could be another potential research problem for the future.
- **Planning Node Deployment Topology in Real Cases:** Our proposed protocol performs well for linear railway tracks, however, for curved track, the protocol may suffer from poor transmission quality owing to the presence of obstacles. To handle issues pertinent to curved tracks, we need to determine a suitable node deployment topology.

Such determination also gets influenced by other factors such as highway crossing, nearby power stations, etc. Performance analysis on the determination of suitable node deployment topology in real cases could be another potential research problem for the future.

- **Incorporation of GPS:** In future, incorporation of GPS module to provide precise locations of trains for transmission of query packets could be considered another potential future avenue of our current work. Consequently, we could explore the usage of GPS to handle addressing mechanism for parallel rail tracks in near future.
- **Investigation of Security issues pertinent to communication channel:** In this thesis, we have confined our work to the exploration of different network attacks such as man-in-the-middle attack and replay attack of the real-time system for detecting missing rail blocks. This work could be extended via investigation of potential security flaws pertinent to the communication channel for attacks such as jamming. Furthermore, exploration of the applicability of our exposed attacks and corresponding countermeasures for the systems adopted in the rail tracks of developed countries could be an interesting research avenue.

Next, in Part II, we have explored network-level performance and security issues or miniature versions of limited-resource cyber-physical networks. Here, we consider nanonetworks and medical body area networks. Both of the fields are still in the rudimentary state. New research directions pertinent to these fields can be summarized as follows:

- In our current work, while exploring suitable nano-antennas for nanonetworks, we consider far-field equation for propagation, however, compared with microwave and mm-wave signals, THz signals experience more severe atmospheric attenuation owing to spreading loss and molecular absorption loss. Therefore, in future, a new path loss model could be developed to address these considerations for transmission utilizing nano-antennas. Alongside, validation of the analytical models and the network-level performances of this work for nanonetworks with different nano-antennas by performing real testbed experiments could be considered a potential avenue for further future

research. Furthermore, our work could easily be extended for several other nano-antennas such as monopole and slot nano-antennas.

- Next, we have explored security issues for medical body area networks. Here, in this work, we have devised a countermeasure for a specific sensor, i.e., ECG sensor. However, exploration of potential countermeasures for other sensor devices such as EEG, EMG, blood pressure, motion sensor, etc., for our proposed power attack could be an interesting future research avenue. Furthermore, the formulation of different analytical models resembling the energy consumption of sensor devices during power attack to further facilitate devising countermeasures can also be explored as an extension of our work.

Finally, we have focused on smarter version of limited-resource cyber-physical networks. Here, in this work, we confined to smart devices and mobile wireless networks. The work in this thesis pertinent to the smarter version has introduced further research opportunities, which are summarized as follows:

- In this thesis, we have proposed a general-purpose multi-objective vertical hand-off mechanism named MOVH, which exhibits higher stability and scalability. In the future, the sensitivity of different operational parameters (for example cross-over rate, and mutation rate) of MOVH with different network settings could be analyzed. Besides, exploration of the impacts of noisy measurements on different decision parameters during vertical hand-off remains another potential research problem that could be focused in future.

In summary, this thesis makes contributions in three parts of limited-resource cyber-physical networks to enhance network-level performance and security of the contemporary cyber-physical networks. We believe our contributions will be able to meet the current and future applications of the limited-resource cyber-physical networks. Consequently, our research incites several directions for important future research in the fields.

Publications

The research conducted as part of this thesis has resulted in the following publications.

Journal Publications

1. N. Nurain, S. Tairin, T. A. Khan, S. Ishraq, and A. B. M. A. A. Islam, *Power Attack: An Imminent Security Threat in Real-Time System for Detecting Missing Rail Blocks in Developing Countries*, Journal of Computers & Security, Elsevier, vol. 84, pp. 35-52, 2019. [280]
2. N. Nurain, B. M. S. Talukder, T. Choudhury, S. Tairin, M. Ferdousi, M. Naznin, and A. B. M. A. A. Islam, *Exploring Network-Level Performances of Wireless Nanonetworks Utilizing Gains of Different Types of Nano-Antennas with Different Materials*, Wireless Networks, Springer, pp. 1-14, 2019. [281]
3. T. Chakraborty, N. Nurain, S. Tairin, T. A. Khan, J. Noor, and A. B. M. A. A. Islam, *A new network paradigm for low-cost and lightweight real-time communication between train and rail track to detect missing and faulty rail blocks*, Journal of Network and Computer Applications, Elsevier, vol. 131, pp. 40-54, 2019. [282]
4. A. B. M. A. A. Islam, M. J. Islam, N. Nurain, and V. Raghunathan, *Channel Assignment Techniques for Multi-radio Wireless Mesh Networks: A Survey*, Communications Surveys and Tutorials, IEEE, Vol. 18, No. 2, pp 988-1017, 2016. [283]
5. N. Nurain, S. Tairin, T. A. Khan, S. Ishraq, and A. B. M. A. A. Islam, *Innate Investigation of Security Threats and Countermeasures in Real-Time System for Detecting Missing Rail Blocks in Developing Countries*, IEEE Transactions on

Computers (Under review).

Conference Publications

1. N. Nurain and A. B. M. A. A. Islam, *Poster: Power Attack in Body Area Networks: Dream or Reality?*, In Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services Companion, ACM, Singapore, 2016. [284]
2. N. Nurain and A. B. M. A. A. Islam, *Power Attack: An Emerging Threat in Health-care Applications Using Medical Body Area Networks*, In Proceedings of Seventh ACM Symposium on Computing and Development, ACM, Nairobi, Kenya, 2016. [285]
3. S. Tairin, N. Nurain and A. B. M. A. A. Islam, *Multi-layer Performance Enhancement in Wireless Nanosensor Networks*, In Proceedings of 2017 International Conference on Networking, Systems and Security (NSysS), IEEE, Dhaka, Bangladesh, 2017. [286]
4. N. Nurain, T. Akter, H. Zannat, M. Akter, A. B. M. Alim Al Islam, and Md. H. Kabir, *General-Purpose Multi-Objective Vertical Hand-off Mechanism Exploiting Network Dynamics*, International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, Abu Dhabi, UAE, 2015. [287]
5. N. Nurain, M. Mostakim, and A. B. M. A. A. Islam, *Towards Empirical Study Based Mathematical Modeling for Throughput of MANETs*, International Conference on Networking Systems and Security (NSysS) [Poster], IEEE, Dhaka, Bangladesh, 2015. [288]
6. N. Nurain, M. Mostakim, and A. B. M. A. A. Islam, *Towards Empirical Study Based Mathematical Modeling for Energy Consumption and End-to-End Delay of MANETs*, 17th International Conference on Computer and Information Technology (ICCIT), IEEE, Dhaka, Bangladesh, 2014. [289]
7. T. R. Toha, M. M. R. Lunar, A s m Rizvi, N. Nurain, and A. B. M. A. A. Islam, *GMC: Greening MapReduce Clusters Considering both Computation En-*

- ergy and Cooling Energy*. IEEE International Conference on Communications (ICC 2018), pp. 1-6, Kansas City, Kansas, USA, 2018. [290]
8. Q. M. Alam, B. Sarker, B. Biswas, K. H. Zubaer, T. R. Toha, N. Nurain, and A. B. M. A. A. Islam, *Towards Simulating Non-lane Based Heterogeneous Road Traffic of Less Developed Countries*. International Conference on Information and Communications Technology (ICT) for Sustainability (ICT4S 2018), pp. 37-48, Toronto, Canada, 2018. [291]
 9. M. Islam, MD. N. Ansary, N. Nurain, S. P. Shams, and A. B. M. A. A. Islam, *A Sweet Recipe for Consolidated Vulnerabilities: Attacking a Live Website by Harnessing a Killer Combination of Vulnerabilities for Greater Harm*. International Conference on Networking, Systems and Security (NSysS 2018), pp. 1-9, IEEE, Dhaka, Bangladesh, 2018. [292]
 10. M. Alam, N. Nurain, S. Tairin, M. Naznin, and A. B. M. A. A. Islam, *Conjugate Congestion Control Based Transport Layer Protocol for Molecular Communication in Body Area Nanonetworks (BANs)*. International Conference on Networking, Systems and Security (NSysS 2018), pp. 1-6, IEEE, Dhaka, Bangladesh, 2018. [293]
 11. M. Alam, N. Nurain, S. Tairin, and A. B. M. A. A. Islam, *Energy-efficient transport layer protocol for hybrid communication in body area nanonetworks*. Humanitarian Technology Conference (R10-HTC), 2017 IEEE Region 10, pp. 674-677, IEEE, Dhaka, Bangladesh, 2017. [294]
 12. R. A. Shetu, T. Toha, M. M. R. Lunar, N. Nurain, and A. B. M. A. A. Islam, *Workload-Based Prediction of CPU Temperature and Usage for Small-Scale Distributed Systems*. International Conference on Computer Science and Network Technology (ICCSNT), pp. 1090-1093, IEEE, Harbin, China, 2015. [295]

Bibliography

- [1] “An introduction to cyber-physical systems.” https://www.uio.no/studier/emner/matnat/ifi/nedlagte-emner/INF5910CPS/h11/undervisningsmateriale/20110830_CPS-WSN-Overview.pdf, 2017. [Last accessed: December 1, 2018].
- [2] S. Ali, S. B. Qaisar, H. Saeed, M. F. Khan, M. Naeem, and A. Anpalagan, “Network challenges for cyber physical systems with tiny wireless devices: a case study on reliable pipeline condition monitoring,” *Sensors*, vol. 15, no. 4, pp. 7172–7205, 2015.
- [3] T. Chakraborty, T. A. Khan, and A. Islam, “Poster: Railcop: Detecting missing rail on railway using wireless sensor networks,” in *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services Companion*, pp. 16–16, ACM, 2016.
- [4] Seminaronly, “Medical body area networks.” <https://www.seminaronly.com/computer/%20science/wireless-body-area-network.php>, 2015. [Last accessed: December 1, 2018].
- [5] LG, “Multi-radio smartphones.” <https://www.lg.com/us/cell-phones/lg-LS775-boost-mobile-stylo-2>, 2015. [Last accessed: December 1, 2018].
- [6] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. Leung, “Body area networks: A survey,” *Mobile networks and applications*, vol. 16, no. 2, pp. 171–193, 2011.

- [7] T. Sanislav and L. Miclea, “Cyber-physical systems-concept, challenges and research areas,” *Journal of Control Engineering and Applied Informatics*, vol. 14, no. 2, pp. 28–33, 2012.
- [8] “Nsf workshop on cyber-physical systems.” <https://cps-vo.org/node/179>, 2006. [Last accessed: December 1, 2018].
- [9] “Automated driving.” <https://www.cs.cmu.edu/afs/cs/project/alv/www/>, 2017. [Last accessed: December 1, 2018].
- [10] “Air traffic control.” <https://www.nasa.gov/simlabs/atc>, 2017. [Last accessed: December 1, 2018].
- [11] “Surgical robot.” <https://www.davincisurgery.com/da-vinci-surgery/da-vinci-surgical-system/>, 2017. [Last accessed: December 1, 2018].
- [12] “Automated farming.” <http://www.kesmac.com/pages/media>, 2017. [Last accessed: December 1, 2018].
- [13] “Human-robot collaboration.” <https://www.rethinkrobotics.com/>, 2017. [Last accessed: December 1, 2018].
- [14] “Smart grids.” <https://www.siemens.com/global/en/home/products/energy/energy-automation-and-smart-grid.html>, 2017. [Last accessed: December 1, 2018].
- [15] K. Wan, K. Man, and D. Hughes, “Specification, analyzing challenges and approaches for cyber-physical systems (cps).,” *Engineering Letters*, vol. 18, no. 3, 2010.
- [16] J. Black, *Urban transport planning: Theory and practice*. Routledge, 2018.
- [17] D. Tokody and F. Flammini, “The intelligent railway system theory,” *International Transportation*, vol. 69, no. 1, pp. 38–40, 2017.

- [18] J. Yin, T. Tang, L. Yang, J. Xun, Y. Huang, and Z. Gao, “Research and development of automatic train operation for railway transportation systems: A survey,” *Transportation Research Part C: Emerging Technologies*, vol. 85, pp. 548–572, 2017.
- [19] Y. Huang, L. Yang, T. Tang, Z. Gao, F. Cao, and K. Li, “Train speed profile optimization with on-board energy storage devices: A dynamic programming based approach,” *Computers & Industrial Engineering*, vol. 126, pp. 149–164, 2018.
- [20] Y. Huang, H. Yu, J. Yin, H. Hu, S. Bai, X. Meng, and M. Wang, “An integrated approach for the energy-efficient driving strategy optimization of multiple trains by considering regenerative braking,” *Computers & Industrial Engineering*, vol. 126, pp. 399–409, 2018.
- [21] F. Mutie, “Transforming kenya railways key to saving lives, <https://goo.gl/5jjjae8>,” 2015. [Last accessed: December 1, 2018].
- [22] Madhyamam, “Train derails in bihar, four killed, <https://goo.gl/0A2NLK>,” 2014. [Last accessed: December 1, 2018].
- [23] “Bangladesh opposition accused of fatal train derailment, <http://www.bbc.com/news/world-asia-25211962>,” December 2013. [Last accessed: December 1, 2018].
- [24] S. Report, “Rail tracks cut off, <https://goo.gl/0q0QLc>,” November 2013. [Last accessed: December 1, 2018].
- [25] “Train derails in bangladesh hartal violence, some 40 injured, <http://en.people.cn/90777/8193270.html>,” April 2013. [Last accessed: December 1, 2018].
- [26] “Dhaka- chittagong train derails; 20 hurt, <https://goo.gl/00a2lW>,” April 2013. [Last accessed: December 1, 2018].
- [27] “50 injured in gazipur train mishap, <https://goo.gl/eHpb6e>,” November 2010. [Last accessed: December 1, 2018].

- [28] bdnews24.com, “Rail tracks uprooted in rangpur , <https://bdnews24.com/bangladesh/2013/12/15/rail-tracks-uprooted-in-rangpur>,” December 2013. [Last accessed: December 1, 2018].
- [29] A. Pascale, N. Varanese, G. Maier, and U. Spagnolini, “A wireless sensor network architecture for railway signalling,” in *Proc. 9th Italian Netw. Workshop*, pp. 1–4, 2012.
- [30] K. Bollas, D. Papasalouros, D. Kourousis, and A. Anastasopoulos, “Acoustic emission inspection of rail wheels,” *J. Acoust. Emission*, vol. 28, pp. 215–228, 2010.
- [31] G. Shafiullah, A. Gyasi-Agyei, and P. Wolfs, “Survey of wireless communications applications in the railway industry,” in *Wireless Broadband and Ultra Wideband Communications*, pp. 65–65, IEEE, 2007.
- [32] A. Wilkinson, “Long range inspection and condition monitoring of rails using guided waves,” in *Proc. 12th Int. Conf. Exhib., Railway Eng., London, UK*, 2013.
- [33] P. Yilmazer, A. Amini, and M. Papaelias, “The structural health condition monitoring of rail steel using acoustic emission techniques,” in *Proc. 51st Annu. Conf. NDT*, pp. 1–12, 2012.
- [34] Q. Li, Z. Shi, H. Zhang, Y. Tan, S. Ren, P. Dai, and W. Li, “A cyber-enabled visual inspection system for rail corrugation,” *Future Generation Computer Systems*, vol. 79, pp. 374–382, 2018.
- [35] A. H. Carlson, D. Frincke, and M. J. Laude, “Railroads and the cyber terror threat,” *Technical Report CSDS-DF-TR-03-14, Center for Secure and Dependable Systems, University of Idaho*, 2003.
- [36] H. W. Lim, W. G. Temple, B. A. N. Tran, B. Chen, Z. Kalbarczyk, and J. Zhou, “Data integrity threats and countermeasures in railway spot transmission systems,” *arXiv preprint arXiv:1709.05935*, 2017.
- [37] R. Bloomfield, M. Bendele, P. Bishop, R. Stroud, and S. Tonks, “The risk assessment of ertms-based railway systems from a cyber security perspective: Methodology and

- lessons learned,” in *International Conference on Reliability, Safety and Security of Railway Systems*, pp. 3–19, Springer, 2016.
- [38] Z.-T. Teo, B. A. N. Tran, S. Lakshminarayana, W. G. Temple, B. Chen, R. Tan, and D. K. Yau, “Securerails: towards an open simulation platform for analyzing cyber-physical attacks in railways,” in *Region 10 Conference (TENCON), 2016 IEEE*, pp. 95–98, IEEE, 2016.
- [39] W. G. Temple, B. A. N. Tran, B. Chen, Z. Kalbarczyk, and W. H. Sanders, “On train automatic stop control using balises: Attacks and a software-only countermeasure,” in *Dependable Computing (PRDC), 2017 IEEE 22nd Pacific Rim International Symposium on*, pp. 274–283, IEEE, 2017.
- [40] Y. Wu, J. Weng, Z. Tang, X. Li, and R. H. Deng, “Vulnerabilities, attacks, and countermeasures in balise-based train control systems,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 4, pp. 814–823, 2017.
- [41] I. F. Akyildiz, F. Brunetti, and C. Blázquez, “Nanonetworks: A new communication paradigm,” *Computer Networks*, vol. 52, no. 12, pp. 2260–2279, 2008.
- [42] T. Suda, M. Moore, T. Nakano, R. Egashira, A. Enomoto, S. Hiyama, and Y. Moritani, “Exploratory research on molecular communication between nanomachines,” in *Genetic and Evolutionary Computation Conference (GECCO), Late Breaking Papers*, vol. 25, p. 29, 2005.
- [43] F. Afsana, S. Mamun, M. Kaiser, and M. Ahmed, “Outage capacity analysis of cluster-based forwarding scheme for body area network using nano-electromagnetic communication,” in *Electrical Information and Communication Technology (EICT), 2015 2nd International Conference on*, pp. 383–388, IEEE, 2015.
- [44] M. H. Rehmani and A.-S. K. Pathan, *Emerging Communication Technologies Based on Wireless Sensor Networks: Current Research and Future Applications*. CRC Press, 2016.
- [45] R. A. Freitas Jr, “Progress in nanomedicine and medical nanorobotics,” *Handbook of theoretical and computational nanotechnology*, vol. 6, pp. 619–672, 2005.

- [46] A. R. Botello-Méndez, E. Cruz-Silva, J. M. Romo-Herrera, F. López-Urías, M. Terrones, B. G. Sumpter, H. Terrones, J.-C. Charlier, and V. Meunier, “Quantum transport in graphene nanonetworks,” *Nano letters*, vol. 11, no. 8, pp. 3058–3064, 2011.
- [47] I. F. Akyildiz and J. M. Jornet, “The internet of nano-things,” *IEEE Wireless Communications*, vol. 17, no. 6, pp. 58–63, 2010.
- [48] E. Zarepour, N. Hassan, M. Hassan, C. T. Chou, and M. E. Warkiani, “Design and analysis of a wireless nanosensor network for monitoring human lung cells,” in *Proceedings of the 10th EAI International Conference on Body Area Networks*, pp. 139–145, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2015.
- [49] I. F. Akyildiz, J. M. Jornet, and M. Pierobon, “Nanonetworks: A new frontier in communications,” *Communications of the ACM*, vol. 54, no. 11, pp. 84–89, 2011.
- [50] G. Piro, L. A. Grieco, G. Boggia, and P. Camarda, “Nano-sim: simulating electromagnetic-based nanonetworks in the network simulator 3,” in *Proceedings of the 6th International ICST Conference on Simulation Tools and Techniques*, pp. 203–210, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2013.
- [51] G. Piro, G. Boggia, and L. A. Grieco, “On the design of an energy-harvesting protocol stack for body area nano-networks,” *Nano Communication Networks*, vol. 6, no. 2, pp. 74–84, 2015.
- [52] J. M. Jornet, J. C. Pujol, and J. S. Pareta, “Phlame: A physical layer aware mac protocol for electromagnetic nanonetworks in the terahertz band,” *Nano Communication Networks*, vol. 3, no. 1, pp. 74–81, 2012.
- [53] J. J. Lehtomäki, A. O. Bicen, and I. F. Akyildiz, “On the nanoscale electromechanical wireless communication in the vhf band,” *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 311–323, 2015.

- [54] T. Nakano, T. Suda, Y. Okaie, M. J. Moore, and A. V. Vasilakos, "Molecular communication among biological nanomachines: A layered architecture and research issues," *IEEE transactions on nanobioscience*, vol. 13, no. 3, pp. 169–197, 2014.
- [55] L. Felicetti, M. Femminella, G. Reali, T. Nakano, and A. V. Vasilakos, "Tcp-like molecular communications," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 12, pp. 2354–2367, 2014.
- [56] J. M. Jornet and I. F. Akyildiz, "Low-weight channel coding for interference mitigation in electromagnetic nanonetworks in the terahertz band," in *2011 IEEE ICC*, pp. 1–6, IEEE, 2011.
- [57] A. Tsioliaridou, C. Liaskos, S. Ioannidis, and A. Pitsillides, "Corona: A coordinate and routing system for nanonetworks," in *Proceedings of the Second Annual International Conference on Nanoscale Computing and Communication*, pp. 18:1–18:6, ACM, 2015.
- [58] C. Liaskos and A. Tsioliaridou, "A promise of realizable, ultra-scalable communications at nano-scale: A multi-modal nano-machine architecture," *IEEE Transactions on Computers*, vol. 64, no. 5, pp. 1282–1295, 2015.
- [59] J. Liu and K. S. Kwak, "Hybrid security mechanisms for wireless body area networks," in *2010 Second international conference on ubiquitous and future networks (ICUFN)*, pp. 98–103, IEEE, 2010.
- [60] N. Sharma and E. M. Bansal, "Preventing impersonate attacks using digital certificates in wban," *IJAEST-INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES*, vol. 1, no. 9, pp. 31–35, 2011.
- [61] T. Sundararajan and A. Shanmugam, "A novel intrusion detection system for wireless body area network in health care monitoring," *Journal of Computer Science*, vol. 6, no. 11, p. 1355, 2010.
- [62] S. N. Ramli and R. Ahmad, "Surveying the wireless body area network in the realm of wireless communication," in *Information Assurance and Security (IAS), 2011 7th International Conference on*, pp. 58–61, IEEE, 2011.

- [63] R. Kumar and R. Mukesh, "State of the art: Security in wireless body area networks," *International Journal of Computer Science & Engineering Technology (IJCSET) Vol.*, vol. 4, no. 5, pp. 622–630, 2013.
- [64] G. Ragesh and K. Baskaran, "An overview of applications, standards and challenges in futuristic wireless body area networks," 2012.
- [65] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 51–58, 2010.
- [66] A. Naveed and S. S. Kanhere, "Security vulnerabilities in channel assignment of multi-radio multi-channel wireless mesh networks," in *Global Telecommunications Conference*, pp. 1–5, 2006.
- [67] M. Bouabdellah, N. Kaabouch, F. El Bouanani, and H. Ben-Azza, "Network layer attacks and countermeasures in cognitive radio networks: A survey," *Journal of Information Security and Applications*, vol. 38, pp. 40–49, 2018.
- [68] H. Kim and E. K. Ryu, "Delegation based user authentication framework over cognitive radio networks," *Journal of Sensor and Actuator Networks*, vol. 6, no. 4, pp. 29–45, 2017.
- [69] "Motorola cls1110 2-way radio." https://express.google.com/express/u/0/product/Motorola-CLS1110-2-Way-Radio/8498857661897192161_15780019955733654456_6136318, 2012. [Last accessed: December 1, 2018].
- [70] "Extreme range wifi router." <http://www.techfresh.net/extreme-range-wi-fi-router/>, 2012. [Last accessed: December 1, 2018].
- [71] K. Savitha and C. Chandrasekar, "Grey relation analysis for vertical handover decision schemes in heterogeneous wireless networks," *European Journal of Scientific Research*, vol. 54, no. 4, pp. 560–568, 2011.

- [72] L. Sheng-mei, P. Su, and X. Ming-hai, "An improved topsis vertical handoff algorithm for heterogeneous wireless networks," in *Communication Technology (ICCT), 2010 12th IEEE International Conference on*, pp. 750–754, IEEE, 2010.
- [73] K. Savitha and C. Chandrasekar, "Vertical handover decision schemes using saw and wpm for network selection in heterogeneous wireless networks," *arXiv preprint arXiv:1109.4490*, 2011.
- [74] J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, "An overview of mobile ad hoc networks: applications and challenges," *Journal-Communications Network*, vol. 3, no. 3, pp. 60–66, 2004.
- [75] N. Aschenbruck, E. Gerhards-Padilla, M. Gerharz, M. Frank, and P. Martini, "Modelling mobility in disaster area scenarios," in *Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems*, pp. 4–12, ACM, 2007.
- [76] E. Huang, W. Hu, J. Crowcroft, and I. Wassell, "Towards commercial mobile ad hoc network applications: A radio dispatch system," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pp. 355–365, ACM, 2005.
- [77] B. Kalaavathi, S. Madhavi, K. Duraiswamy, *et al.*, "Virtual class room using mobile ad hoc networks," 2009.
- [78] R. Kumar, M. Misra, and A. K. Sarje, "A simplified analytical model for end-to-end delay analysis in manet," *IJCA Special Issue on Mobile Ad-hoc Networks MANETs*, pp. 195–199, 2010.
- [79] T. Jun, A. Dalton, S. Bodas, C. Julien, and S. Vishwanath, "Expressive analytical model for routing protocols in mobile ad hoc networks," in *Communications, 2008. ICC'08. IEEE International Conference on*, pp. 2134–2140, IEEE, 2008.
- [80] T. Jun and C. Julien, "Delay analysis for symmetric nodes in mobile ad hoc networks," in *Proceedings of the 4th ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks*, pp. 191–200, ACM, 2009.

- [81] V. J. Hodge, S. O’Keefe, M. Weeks, and A. Moulds, “Wireless sensor networks for condition monitoring in the railway industry: A survey,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 3, pp. 1088–1106, 2015.
- [82] B. Ai, X. Cheng, T. Kürner, Z.-D. Zhong, K. Guan, R.-S. He, L. Xiong, D. W. Matolak, D. G. Michelson, and C. Briso-Rodriguez, “Challenges toward wireless communications for high-speed railway,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 5, pp. 2143–2158, 2014.
- [83] I. Llatser, C. Kremers, A. Cabellos-Aparicio, J. M. Jornet, E. Alarcón, and D. N. Chigrin, “Graphene-based nano-patch antenna for terahertz radiation,” *Photonics and Nanostructures-Fundamentals and Applications*, vol. 10, no. 4, pp. 353–358, 2012.
- [84] A. Locatelli, “Peculiar properties of loop nanoantennas,” *IEEE Photonics Journal*, vol. 3, no. 5, pp. 845–853, 2011.
- [85] L. Razzari, A. Toma, M. Clerici, M. Shalaby, G. Das, C. Liberale, M. Chirumamilla, R. P. Zaccaria, F. De Angelis, M. Peccianti, *et al.*, “Terahertz dipole nanoantenna arrays: resonance characteristics,” *Plasmonics*, vol. 8, no. 1, pp. 133–138, 2013.
- [86] B. Musznicki and P. Zwierzykowski, “Survey of simulators for wireless sensor networks,” *International Journal of Grid and Distributed Computing*, vol. 5, no. 3, pp. 23–50, 2012.
- [87] K. Savitha and C. Chandrasekar, “Grey relation analysis for vertical handover decision schemes in heterogeneous wireless networks,” *Journal of Scientific Research*, vol. 54, no. 4, pp. 560–568, 2011.
- [88] L. Sheng-mei, P. Su, and X. Ming-hai, “An improved topsis vertical handoff algorithm for heterogeneous wireless networks,” in *IEEE 12th International Conference on Communication Technology*, pp. 750–754, 2010.
- [89] P. Goyal, D. Lobiyal, and C. Katti, “Dynamic user preference based network selection for vertical handoff in heterogeneous wireless networks,” *Wireless Personal Communications*, vol. 98, no. 1, pp. 725–742, 2018.

- [90] M. Mouad and L. Cherkaoui, “A comparison between fuzzy topsis and fuzzy gra for the vertical handover decision making,” in *Intelligent Systems and Computer Vision*, pp. 1–6, 2017.
- [91] X. Song, W. Liu, M. Zhang, and F. Liu, “A network selection algorithm based on fahp/gra in heterogeneous wireless networks,” in *2nd IEEE International Conference on Computer and Communications*, pp. 1445–1449, 2016.
- [92] A. Agrawal, A. Jeyakumar, and N. Pareek, “Comparison between vertical handoff algorithms for heterogeneous wireless networks,” in *International Conference on Communication and Signal Processing*, pp. 1370–1373, 2016.
- [93] “Gsm-r, <https://en.wikipedia.org/wiki/GSM-R>,” 2017. [Last accessed: December 1, 2018].
- [94] G. Intelligence, “Rural coverage: strategies for sustainability, <https://goo.gl/bG62BX>,” 2015. [Last accessed: December 1, 2018].
- [95] G. Intelligence, “Gsma country overview : Bangladesh, <https://goo.gl/06hmDQ>,” 2014. [Last accessed: December 1, 2018].
- [96] B. Railway, “Railway root map of bangladesh, <https://goo.gl/nzRXkr>,” 2013. [Last accessed: December 1, 2018].
- [97] T. T. Info, “Emu, memu and demu trains, <http://www.totaltraininfo.com/memu.php>,” 2016. [Last accessed: December 1, 2018].
- [98] S. Ramesh and S. Gobinathan, “Railway faults tolerance techniques using wireless sensor networks,” *IJECT*, vol. 3, no. 1, 2012.
- [99] P. Koakowski, J. Szelek, K. Sekua, A. Swiercz, K. Mizerski, and P. Gutkiewicz, “Structural health monitoring of a railway truss bridge using vibration-based and ultrasonic methods,” *Smart Materials and Structures*, vol. 20, no. 3, p. 035016, 2011.
- [100] R. Lagnebäck, *Evaluation of wayside condition monitoring technologies for condition-based maintenance of railway vehicles*. PhD thesis, Luleå tekniska universitet, 2007.

- [101] N. Nenov, E. Dirmirov, G. Mihov, T. Ruzhekov, and P. Piskulev, “A study on sensors for measuring load of railway vehicle wheels in motion,” in *31st International Spring Seminar on Electronics Technology*, pp. 550–555, IEEE, 2008.
- [102] K. Sekuła and P. Kołakowski, “Piezo-based weigh-in-motion system for the railway transport,” *Structural Control and Health Monitoring*, vol. 19, no. 2, pp. 199–215, 2012.
- [103] D. Barke and W. Chiu, “Structural health monitoring in the railway industry: a review,” *Structural Health Monitoring*, vol. 4, no. 1, pp. 81–93, 2005.
- [104] E. Berlin and K. Van Laerhoven, “Sensor networks for railway monitoring: Detecting trains from their distributed vibration footprints,” in *International Conference on Distributed Computing in Sensor Systems*, pp. 80–87, IEEE, 2013.
- [105] P. J. Bennett, K. Soga, I. Wassell, P. Fidler, K. Abe, Y. Kobayashi, and M. Vanicek, “Wireless sensor networks for underground railway applications: case studies in prague and london,” *Smart Structures and Systems*, vol. 6, no. 5-6, pp. 619–639, 2010.
- [106] E. Aboelela, W. Edberg, C. Papakonstantinou, and V. Vokkarane, “Wireless sensor network based model for secure railway operations,” in *25th International Performance, Computing, and Communications Conference*, pp. 6–11, IEEE, 2006.
- [107] E. Peek and W. Basta, “Broken rail detection system and method,” 2000. US Patent 6,102,340.
- [108] F. Flammini, A. Gaglione, F. Ottello, A. Pappalardo, C. Pragliola, and A. Tedesco, “Towards wireless sensor networks for railway infrastructure monitoring,” in *Electrical Systems for Aircraft, Railway and Ship Propulsion (ESARS)*, pp. 1–6, IEEE, 2010.
- [109] W. Bayissa and M. Dhanasekar, “High-speed detection of broken rails, rail cracks and surface faults,” *CRC for Rail Innovation, Brisbane, Australia, Project*, no. P4, p. 116, 2011.

- [110] R. Liu, Y. Wu, I. Wassell, and K. Soga, "Frequency diversity measurements at 2.4 ghz for wireless sensor networks deployed in tunnels," in *IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 2990–2994, IEEE, 2009.
- [111] G. Shafiullah, S. A. Azad, and A. S. Ali, "Energy-efficient wireless mac protocols for railway monitoring applications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 2, pp. 649–659, 2013.
- [112] S. Studio, "Hc-12, <https://goo.gl/zkYBOv>," 2010. [Last accessed: December 1, 2018].
- [113] V. K. Sehgal, A. Patrick, and L. Rajpoot, "A comparative study of cyber physical cloud, cloud of sensors and internet of things: Their ideology, similarities and differences," in *2014 IEEE International Advance Computing Conference (IACC)*, pp. 708–716, IEEE, 2014.
- [114] Newage, "Longest train service to start saturday, <http://www.newagebd.net/article/55487/longest-train-service-to-start-saturday>," 2018. [Last accessed: June 1, 2019].
- [115] J. Suhonen, T. Hämäläinen, and M. Hännikäinen, "Availability and end-to-end reliability in low duty cycle multihopwireless sensor networks," *Sensors*, vol. 9, no. 3, pp. 2088–2116, 2009.
- [116] G. Campobello, S. Serrano, A. Leonardi, and S. Palazzo, "Trade-offs between energy saving and reliability in low duty cycle wireless sensor networks using a packet splitting forwarding technique," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, no. 1, p. 932345, 2010.
- [117] M. F. Neuts, *Structured stochastic matrices of M/G/1 type and their applications*, vol. 5. Marcel Dekker New York, 1989.
- [118] "Queuing theory <https://goo.gl/zkYBOv>," 2010. [Last accessed: December 1, 2018].

- [119] A. Carrington, C. Harding, and H. Yu, “Optimising wireless network control system traffic—using queuing theory,” in *Proceedings of the 14th International Conference on Automation & Computing, Brunel University*, 2008.
- [120] S. Kafaie, M. H. Ahmed, Y. Chen, and O. A. Dobre, “Performance analysis of network coding with ieee 802.11 dcf in multi-hop wireless networks,” *IEEE Transactions on Mobile Computing*, vol. 17, no. 5, pp. 1148–1161, 2017.
- [121] M. A. Kafi, J. B. Othman, and N. Badache, “A survey on reliability protocols in wireless sensor networks,” *ACM Computing Surveys (CSUR)*, vol. 50, no. 2, p. 31, 2017.
- [122] L. Khelladi and N. Badache, “Revisiting directed diffusion in the era of iot-wsns: Power control for adaptation to high density,” in *8th International Conference on Information, Intelligence, Systems & Applications*, pp. 1–6, IEEE, 2017.
- [123] A. A. Al Islam and V. Raghunathan, “itcp: an intelligent tcp with neural network based end-to-end congestion control for ad-hoc multi-hop wireless mesh networks,” *Wireless Networks*, vol. 21, no. 2, pp. 581–610, 2015.
- [124] A. A. Al Islam, S. I. Alam, V. Raghunathan, and S. Bagchi, “Multi-armed bandit congestion control in multi-hop infrastructure wireless mesh networks,” in *2012 IEEE 20th International Symposium on Modelling, Analysis & Simulation of Computer and Telecommunication Systems (MASCOTS)*, pp. 31–40, IEEE, 2012.
- [125] L. A. Grieco and S. Mascolo, “Performance evaluation and comparison of westwood+, new reno, and vegas tcp congestion control,” *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 25–38, 2004.
- [126] Z. Teng and K.-I. Kim, “A survey on real-time mac protocols in wireless sensor networks,” *Communications and Network*, vol. 2, no. 02, p. 104, 2010.
- [127] S. Rachamalla and A. S. Kancharla, “A survey of real-time routing protocols for wireless sensor networks,” *International Journal of Computer Science and Engineering Survey*, vol. 4, no. 3, p. 35, 2013.

- [128] P. Papadimitriou and V. Tsaoussidis, “On transport layer mechanisms for real-time qos,” *J. Mobile Multimedia*, vol. 1, no. 4, pp. 342–363, 2006.
- [129] A. Sharif, V. Potdar, and A. Rathnayaka, “Performance evaluation of different transport layer protocols on the ieee 802.11 and ieee 802.15. 4 mac/phy layers for wsn,” in *Proceedings of the 7th International Conference on Advances in Mobile computing and multimedia*, pp. 300–310, ACM, 2009.
- [130] R. Safety and S. B. Limited, “Gert8000 rule book: Train driver manual, <https://goo.gl/ExPxj4>,” 2015. [Last accessed: December 1, 2018].
- [131] T. design trust, “Cost price, trade price, wholesale price?” <http://goo.gl/XmdeX8>, 2014. [Last accessed: December 1, 2018].
- [132] Dewhurst and Meeker, “The true cost of oversea manufacturing.” <http://goo.gl/nKNbuL>, 2004. [Last accessed: December 1, 2018].
- [133] Y. Dou, Y. Huang, Q. Li, and S. Luo, “A fast template matching-based algorithm for railway bolts detection,” *International Journal of Machine Learning and Cybernetics*, vol. 5, no. 6, pp. 835–844, 2014.
- [134] Z. Xu, H. Wang, Z. Xu, and X. Wang, “Power attack: An increasing threat to data centers,” in *NDSS*, 2014.
- [135] F. Shahzad, M. Pasha, and A. Ahmad, “A survey of active attacks on wireless sensor networks and their countermeasures,” *arXiv preprint arXiv:1702.07136*, 2017.
- [136] P. Syverson, “A taxonomy of replay attacks [cryptographic protocols],” in *Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings*, pp. 187–191, IEEE, 1994.
- [137] S. Mamun, “Train schedules derailed, buses delayed, <https://goo.gl/zkYBOv>,” 2016. [Last accessed: December 1, 2018].
- [138] K. Sen, “Train delays as driver takes time for sleep, <https://www.telegraphindia.com/states/west-bengal/>

- train-delays-as-drivertakes-time-for-sleep-204615,” 2018. [Last accessed: December 1, 2018].
- [139] A. Chauhan, “Rs 11 crore levied as superfast surcharge, but trains delayed up to 95% of times, <https://timesofindia.indiatimes.com/india>,” 2017. [Last accessed: December 1, 2018].
- [140] D. Rijmenants, “One-time pad, <http://users.telenet.be/d.rijmenants/en/onetimepad.html>,” 2009. [Last accessed: December 1, 2018].
- [141] W. Hammersmith, “One-time-pad encryption with keyable characters,” Jan. 23 2003. US Patent App. 10/254,743.
- [142] A. Perrig, J. Stankovic, and D. Wagner, “Security in wireless sensor networks,” *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.
- [143] G. R. Joginpally, “Replay attack & its countermeasures, <http://joginipally.blogspot.com/2009/07/replay-attack-its-countermeasures.html>,” 2009. [Last accessed: December 1, 2018].
- [144] Y.-C. Wu, Q. Chaudhari, and E. Serpedin, “Clock synchronization of wireless sensor networks,” *IEEE Signal Processing Magazine*, vol. 28, no. 1, pp. 124–138, 2011.
- [145] B. Sundararaman, U. Buy, and A. D. Kshemkalyani, “Clock synchronization for wireless sensor networks: a survey,” *Ad hoc networks*, vol. 3, no. 3, pp. 281–323, 2005.
- [146] K.-L. Noh, Q. M. Chaudhari, E. Serpedin, and B. W. Suter, “Novel clock phase offset and skew estimation using two-way timing message exchanges for wireless sensor networks,” *IEEE transactions on communications*, vol. 55, no. 4, pp. 766–777, 2007.
- [147] J. Viega and M. Messier, *Secure Programming Cookbook for C and C++: Recipes for Cryptography, Authentication, Input Validation & More.* ” O’Reilly Media, Inc.”, 2003.
- [148] T. A. forum, “Eeprom library, <https://www.arduino.cc/en/Reference/EEPROM>,” 2018. [Last accessed: December 1, 2018].

- [149] G. of Bangladesh, “Bangladesh railways, <http://railway.portal.gov.bd/site/page/e35cebe7-3b39-46be-ae6b-f267d4d1375f>,” 2018. [Last accessed: December 1, 2018].
- [150] ANI, “Delhi: 12 trains cancelled due to operational reason, <http://www.india.com/news/agencies/delhi-12-trains-cancelled-due-to-operational-reason-2888246/>,” 2018. [Last accessed: December 1, 2018].
- [151] A. Pant, “320 trains running late, 16 cancelled, 2 rescheduled due to dense fog in delhi, <https://www.ndtv.com/delhi-news/320-trains-running-late-16-cancelled-2-rescheduled-due-to-dense-> 2018. [Last accessed: December 1, 2018].
- [152] S. O. Report, “Flood: Todays train for north, south-west dists cancelled, <http://www.thedailystar.net/country/flood-snaps-dhakas-rail-link-southern-northern-districts-banglad> 2017. [Last accessed: December 1, 2018].
- [153] B. Kordy, S. Mauw, S. Radomirović, and P. Schweitzer, “Foundations of attack–defense trees,” in *International Workshop on Formal Aspects in Security and Trust*, pp. 80–95, Springer, 2010.
- [154] A. Bagnato, B. Kordy, P. H. Meland, and P. Schweitzer, “Attribute decoration of attack–defense trees,” *International Journal of Secure Software Engineering (IJSSE)*, vol. 3, no. 2, pp. 1–35, 2012.
- [155] S. Studio, “Hc-12, <https://goo.gl/zkYBOv>,” 2010. [Last accessed: December 1, 2018].
- [156] F. Afsana, S. Mamun, M. Kaiser, and M. Ahmed, “Outage capacity analysis of cluster-based forwarding scheme for body area network using nano-electromagnetic communication,” in *EICT, 2015 2nd International Conference on*, pp. 383–388, IEEE, 2015.

- [157] A. R. Botello-Mendez, E. Cruz-Silva, J. M. Romo-Herrera, F. Lopez-Urias, M. Terrones, B. G. Sumpter, H. Terrones, J.-C. Charlier, and V. Meunier, “Quantum transport in graphene nanonetworks,” *Nano letters*, vol. 11, no. 8, 2011.
- [158] J. M. Jornet and I. F. Akyildiz, “An electromagnetic and quantum theory perspective for nano-scale communication in the terahertz band,” *First NaNoNetworking Day, Spain*, July 2009.
- [159] B. Atakan and O. B. Akan, “Carbon nanotube-based nanoscale ad hoc networks,” *Communications Magazine*, vol. 48, pp. 129–135, June 2010.
- [160] J. M. Jornet and I. F. Akyildiz, “Graphene-based plasmonic nano-antenna for terahertz band communication in nanonetworks,” *IEEE JSAC*, vol. 31, pp. 685–694, December 2013.
- [161] A. Mohammadi, V. Sandoghdar, and M. Agio, “Gold, copper, silver and aluminum nanoantennas to enhance spontaneous emission,” *Journal of Computational and Theoretical Nanoscience*, vol. 6, no. 9, pp. 2024–2030, 2009.
- [162] J. M. Jornet and I. F. Akyildiz, “Low-weight channel coding for interference mitigation in electromagnetic nanonetworks in the terahertz band,” in *2011 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2011.
- [163] J. M. Jornet and I. F. Akyildiz, “Information capacity of pulse-based wireless nanosensor networks,” in *Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 8th Annual IEEE Communications Society Conference on*, (Utah, USA), pp. 80–88, IEEE, 2011.
- [164] J. M. Jornet and I. F. Akyildiz, “Channel capacity of electromagnetic nanonetworks in the terahertz band,” in *Communications (ICC), 2010 IEEE International Conference on*, pp. 1–6, IEEE, 2010.
- [165] I. F. Akyildiz and J. M. Jornet, “Electromagnetic wireless nanosensor networks,” *Nano Communication Networks*, vol. 1, no. 1, pp. 3–19, 2010.

- [166] B. D. Unluturk, D. Malak, and O. B. Akan, "Rate-delay tradeoff with network coding in molecular nanonetworks," *IEEE Transactions on Nanotechnology*, vol. 12, no. 2, pp. 120–128, 2013.
- [167] T. Nakano, Y. Okaie, and J.-Q. Liu, "Channel model and capacity analysis of molecular communication with brownian motion," *IEEE communications letters*, vol. 16, no. 6, pp. 797–800, 2012.
- [168] S. Kadloor, R. S. Adve, and A. W. Eckford, "Molecular communication using brownian motion with drift," *IEEE Transactions on NanoBioscience*, vol. 11, no. 2, pp. 89–99, 2012.
- [169] K. Srinivas, A. W. Eckford, and R. S. Adve, "Molecular communication in fluid media: The additive inverse gaussian noise channel," *IEEE Transactions on Information Theory*, vol. 58, no. 7, pp. 4678–4692, 2012.
- [170] M. Pierobon and I. F. Akyildiz, "Diffusion-based noise analysis for molecular communication in nanonetworks," *IEEE Transactions on Signal Processing*, vol. 59, no. 6, pp. 2532–2547, 2011.
- [171] T. Nakano and J.-Q. Liu, "Design and analysis of molecular relay channels: An information theoretic approach," *IEEE Transactions on NanoBioscience*, vol. 9, no. 3, pp. 213–221, 2010.
- [172] A. W. Eckford, N. Farsad, S. Hiyama, and Y. Moritani, "Microchannel molecular communication with nanoscale carriers: Brownian motion versus active transport," in *Nanotechnology (IEEE-NANO), 2010 10th IEEE Conference on*, pp. 854–858, IEEE, 2010.
- [173] A. Guney, B. Atakan, and O. B. Akan, "Mobile ad hoc nanonetworks with collision-based molecular communication," *IEEE Transactions on Mobile Computing*, vol. 11, no. 3, pp. 353–366, 2012.
- [174] C. T. Chou, "Molecular circuits for decoding frequency coded signals in nanocommunication networks," *Nano Communication Networks*, vol. 3, no. 1, pp. 46–56, 2012.

- [175] T. Nakano and J. Shuai, "Repeater design and modeling for molecular communication networks," in *Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on*, pp. 501–506, IEEE, 2011.
- [176] A. Guney, B. Atakan, and O. B. Akan, "Mobile ad hoc nanonetworks with collision-based molecular communication," *IEEE Transactions on Mobile Computing*, vol. 11, no. 3, pp. 353–366, 2012.
- [177] F. Walsh, S. Balasubramaniam, D. Botvich, T. Suda, T. Nakano, S. F. Bush, and M. Ó. Foghlú, "Hybrid dna and enzyme based computing for address encoding, link switching and error correction in molecular communication," in *International Conference on Nano-Networks*, pp. 28–38, Springer, 2008.
- [178] T. Nakano and M. Moore, "In-sequence molecule delivery over an aqueous medium," *Nano Communication Networks*, vol. 1, no. 3, pp. 181–188, 2010.
- [179] M. J. Moore and T. Nakano, "Addressing by beacon distances using molecular communication," *Nano Communication Networks*, vol. 2, no. 2, pp. 161–173, 2011.
- [180] M. J. Moore and T. Nakano, "Synchronization of inhibitory molecular spike oscillators," *Bio-Inspired Models of Networks, Information, and Computing Systems*, pp. 183–195, 2012.
- [181] S. Balasubramaniam *et al.*, "Opportunistic routing through conjugation in bacteria communication nanonetwork," *Nano Communication Networks*, vol. 3, no. 1, pp. 36–45, 2012.
- [182] L. C. Cobo and I. F. Akyildiz, "Bacteria-based communication in nanonetworks," *Nano Communication Networks*, vol. 1, no. 4, pp. 244–256, 2010.
- [183] J. M. Jornet and I. F. Akyildiz, "Graphene-based nano-antennas for electromagnetic nanocommunications in the terahertz band," in *Proceedings of the 4th European Conference on Antennas and Propagation(EuCAP),Barcelona, Spain*, pp. 1–5, IEEE, April 2010.

- [184] A. Geim and K. Novoselov, “The rise of graphene,” *Nature materials*, vol. 6, no. 3, pp. 183–191, 2007.
- [185] J. J. Lehtomäki, A. O. Bicen, and I. F. Akyildiz, “On the nanoscale electromechanical wireless communication in the vhf band,” *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 311–323, 2015.
- [186] J. M. Jornet and I. F. Akyildiz, “Low-weight channel coding for interference mitigation in electromagnetic nanonetworks in the terahertz band,” in *2011 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2011.
- [187] Q. Liu, P. He, K. Yang, and S. Leng, “Inter-symbol interference analysis of synaptic channel in molecular communications,” in *2014 IEEE International Conference on Communications (ICC)*, pp. 4424–4429, IEEE, 2014.
- [188] J. M. Jornet and I. F. Akyildiz, “Channel modeling and capacity analysis for electromagnetic wireless nanonetworks in the terahertz band,” *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3211–3221, 2011.
- [189] M. Damrath, S. Korte, and P. Hoeher, “Equivalent discrete-time channel modeling for molecular communication with emphasize on an absorbing receiver,” *IEEE Transactions on NanoBioscience*, 2017.
- [190] M. U. Mahfuz, D. Makrakis, and H. T. Mouftah, “Characterization of molecular communication channel for nanoscale networks.,” in *BIOSIGNALS*, pp. 327–332, 2010.
- [191] J. M. Jornet, J. C. Pujol, and J. S. Pareta, “Phlame: A physical layer aware mac protocol for electromagnetic nanonetworks in the terahertz band,” *Nano Communication Networks*, vol. 3, no. 1, pp. 74–81, 2012.
- [192] G. Piro, G. Boggia, and L. A. Grieco, “On the design of an energy-harvesting protocol stack for body area nano-networks,” *Nano Communication Networks*, vol. 6, no. 2, pp. 74–84, 2015.

- [193] S. Mohrehkesh and M. C. Weigle, “Rih-mac: receiver-initiated harvesting-aware mac for nanonetworks,” in *Proceedings of ACM The First Annual International Conference on Nanoscale Computing and Communication*, p. 6, ACM, 2014.
- [194] P. Wang, J. M. Jornet, M. A. Malik, N. Akkari, and I. F. Akyildiz, “Energy and spectrum-aware mac protocol for perpetual wireless nanosensor networks in the terahertz band,” *Ad Hoc Networks*, vol. 11, no. 8, pp. 2541–2555, 2013.
- [195] J. M. Jornet, “A joint energy harvesting and consumption model for self-powered nano-devices in nanonetworks,” in *2012 IEEE International Conference on Communications (ICC)*, pp. 6151–6156, IEEE, 2012.
- [196] A. Tsioliariidou, C. Liaskos, S. Ioannidis, and A. Pitsillides, “Corona: A coordinate and routing system for nanonetworks,” in *Proceedings of the Second Annual International Conference on Nanoscale Computing and Communication*, p. 18, ACM, 2015.
- [197] C. Liaskos and A. Tsioliariidou, “A promise of realizable, ultra-scalable communications at nano-scale: A multi-modal nano-machine architecture,” *IEEE Transactions on Computers*, vol. 64, no. 5, pp. 1282–1295, 2015.
- [198] Liaskos, T. Christos, X. Angeliki, A. Dimitropoulos, and Pitsillides, “Mitigating the broadcast storm in nanonetworks with 16-bits,” in *Foundation of Research and Technology - Hellas*, pp. TR–TNL–IRG–2015–1, 2015.
- [199] C. A. Balanis, *Antenna theory: analysis and design*. John Wiley & Sons, 2016.
- [200] D.-G. Fang, *Antenna theory and microstrip antennas*. CRC Press, 2009.
- [201] T. Ebbesen, H. Lezec, H. Hiura, J. Bennett, H. Ghaemi, T. Thio, *et al.*, “Electrical-conductivity of individual carbon nanotubes,” *Nature*, vol. 382, no. 6586, pp. 54–56, 1996.
- [202] J. Yu, X. Huang, C. Wu, and P. Jiang, “Permittivity, thermal conductivity and thermal stability of poly (vinylidene fluoride)/graphene nanocomposites,” *IEEE Transactions on Dielectrics and Electrical Insulation*, vol. 18, no. 2, pp. 478–484, 2011.

- [203] R. Che, L.-M. Peng, X. F. Duan, Q. Chen, and X. Liang, “Microwave absorption enhancement and complex permittivity and permeability of Fe encapsulated within carbon nanotubes,” *Advanced Materials*, vol. 16, no. 5, pp. 401–405, 2004.
- [204] H. R. Matte, K. Subrahmanyam, and C. Rao, “Novel magnetic properties of graphene: presence of both ferromagnetic and antiferromagnetic features and other aspects,” *The Journal of Physical Chemistry C*, vol. 113, no. 23, pp. 9982–9985, 2009.
- [205] “Skin effect.” <https://en.wikipedia.org/wiki/Skineffect>, 2016. Last accessed on 30-July-2016.
- [206] “Dipole antenna.” www.antenna-theory.com/antennas/shortdipole.php, 2016. Last accessed on 30-July-2016.
- [207] “Wave impedance.” en.wikipedia.org/wiki/Wave_impedance, 2016. Last accessed on 30-July-2016.
- [208] I. F. Akyildiz, J. M. Jornet, and M. Pierobon, “Nanonetworks: A new frontier in communications,” *Communications of the ACM*, vol. 54, pp. 84–89, November 2011.
- [209] Z. L. Wang, “Towards self-powered nanosystems: from nanogenerators to nanopiezotronics,” *Advanced Functional Materials*, vol. 18, no. 22, pp. 3553–3567, 2008.
- [210] “Radar tutorial.” <http://www.radartutorial.eu/19.kartei/karte517.en.htm>. Last accessed on 30-July-2016.
- [211] C. Liaskos and A. Tsioliaridou, “A promise of realizable, ultra-scalable communications at nano-scale: A multi-modal nano-machine architecture,” *IEEE Transactions on Computers*, vol. 64, no. 5, pp. 1282–1295, 2015.
- [212] E. Zarepour, M. Hassan, C. T. Chou, and A. A. Adesina, “Electromagnetic wireless nanoscale sensor networks,” *Emerging Communication Technologies Based on Wireless Sensor Networks: Current Research and Future Applications*, pp. 143–178, 2016.
- [213] G. Piro, L. A. Grieco, G. Boggia, and P. Camarda, “Nano-sim: simulating electromagnetic-based nanonetworks in the network simulator 3,” in *Proceedings of*

- the 6th International ICST Conference on Simulation Tools and Techniques*, pp. 203–210, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2013.
- [214] C.-J. Chen, Y. Haik, and J. Chatterjee, “Development of nanotechnology for biomedical applications,” in *Conference, Emerging Information Technology 2005.*, IEEE, 2005.
- [215] B. Wowk, “Cell repair technology,” *Cryonics*, vol, pp. 21–30, 1988.
- [216] R. A. Freitas, “What is nanomedicine?,” *Nanomedicine: Nanotechnology, Biology and Medicine*, vol. 1, no. 1, pp. 2–9, 2005.
- [217] D. C. Hansen, “Metal corrosion in the human body: the ultimate bio-corrosion scenario,” *The Electrochemical Society Interface*, vol. 17, no. 2, pp. 31–34, 2008.
- [218] R. E. Smalley, M. S. Dresselhaus, G. Dresselhaus, and P. Avouris, *Carbon nanotubes: synthesis, structure, properties, and applications*, vol. 80. Springer Science & Business Media, 2003.
- [219] J. W. Aylott, “Optical nanosensorsan enabling technology for intracellular measurements,” *Analyst*, vol. 128, no. 4, pp. 309–312, 2003.
- [220] “Assignment point.” <http://www.assignmentpoint.com/arts/social-science/population-ageing-bangladesh.html>, 2011. [Last accessed on 16-September-2016].
- [221] “Worldbank.org.” http://siteresources.worldbank.org/SOUTHASIAEXT/Resources/223546-1296680097256/7707437-1296680114157/NCD_BD_Policy_Feb_2011.pdf, 2011. [Last accessed on 16-September-2016].
- [222] M. for Health and Aging, “Speech opening address,” *Speech Opening Address*, 2009.
- [223] “Trading economics.” www.tradingeconomics.com/bangladesh/health-expenditure-total-percent-of-gdp-wb-data.html, 2013. [Last accessed on 16-September-2016].

- [224] Z. Xu, H. Wang, Z. Xu, and X. Wang, “Power attack: An increasing threat to data centers.,” in *NDSS*, 2014.
- [225] D. Curtis, E. Shih, J. Waterman, J. Guttag, J. Bailey, T. Stair, R. A. Greenes, and L. Ohno-Machado, “Physiological signal monitoring in the waiting areas of an emergency room,” in *Proceedings of the ICST 3rd international conference on Body area networks*, p. 5, 2008.
- [226] A. Pentland, “Healthwear: medical technology becomes wearable,” *Studies in health technology and informatics*, vol. 118, pp. 55–65, 2005.
- [227] E. Farella, A. Pieracci, L. Benini, L. Rocchi, and A. Acquaviva, “Interfacing human and computer with wireless body area sensor networks: the wimoca solution,” *Multimedia Tools and Applications*, vol. 38, no. 3, pp. 337–363, 2008.
- [228] J. Khan, M. Yuce, and F. Karami, “Performance evaluation of a wireless body area sensor network for remote patient monitoring,” in *2008 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 1266–1269, IEEE, 2008.
- [229] D. H. G. Ltd., “Ecg sensor.” www.data-harvest.co.uk/docs/uploads/3279_ds057_5_ecg.pdf, 2010. [Last accessed on 16-September-2016].
- [230] H. Med, “Cardiac cycle.” howmed.net/physiology/cardiac-cycle/, 2010. [Last accessed on 16-September-2016].
- [231] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, “They can hear your heartbeats: non-invasive security for implantable medical devices,” in *ACM SIGCOMM Computer Communication Review*, vol. 41, pp. 2–13, ACM, 2011.
- [232] D. Lucani, G. Cataldo, J. Cruz, G. Villegas, and S. Wong, “A portable ecg monitoring device with bluetooth and holter capabilities for telemedicine applications,” in *Engineering in Medicine and Biology Society, 2006. EMBS’06. 28th Annual International Conference of the IEEE*, pp. 5244–5247, IEEE, 2006.

- [233] “All about battery.” <http://www.allaboutbatteries.com/Energy-tables.html>, 2011. [Last accessed on 16-September-2016].
- [234] V. Gazis, N. Houssos, N. Alonistioti, and L. Merakos, “On the complexity of” always best connected” in 4g mobile networks,” in *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*, vol. 4, pp. 2312–2316, IEEE, 2003.
- [235] C. Eshanta, M. Ismail, K. Jumari, and P. Yahaya, “Who strategy for qos-provisioning in the wimax/vvlan interworking system,” *Asian Journal of Applied Sciences*, vol. 2, no. 6, pp. 511–20, 2009.
- [236] H. Bing, C. He, and L. Jiang, “Performance analysis of vertical handover in a umts-wlan integrated network,” in *Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003. 14th IEEE Proceedings on*, vol. 1, pp. 187–191, IEEE, 2003.
- [237] A. H. Zahran and B. Liang, “Performance evaluation framework for vertical handoff algorithms in heterogeneous networks,” in *Communications, 2005. ICC 2005. 2005 IEEE International Conference on*, vol. 1, pp. 173–178, IEEE, 2005.
- [238] A. Hasswa, N. Nasser, and H. Hassanein, “Tramcar: A context-aware cross-layer architecture for next generation heterogeneous wireless networks,” in *Communications, 2006. ICC’06. IEEE International Conference on*, vol. 1, pp. 240–245, IEEE, 2006.
- [239] N. Nasser, S. Guizani, and E. Al-Masri, “Middleware vertical handoff manager: A neural network-based solution,” in *Communications, 2007. ICC’07. IEEE International Conference on*, pp. 5671–5676, IEEE, 2007.
- [240] “World-wide user of smart phone.” <http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones>, 2014. [Last accessed on 16-September-2016].
- [241] M. Kassar, B. Kervella, and G. Pujolle, “An overview of vertical handover decision strategies in heterogeneous wireless networks,” *Computer communications*, vol. 31, no. 10, pp. 2607–2620, 2008.

- [242] P. N. Tran and N. Boukhatem, "Comparison of madm decision algorithms for interface selection in heterogeneous wireless networks," in *Software, Telecommunications and Computer Networks, 2008. SoftCOM 2008. 16th International Conference on*, pp. 119–124, IEEE, 2008.
- [243] Y. Nkansah-Gyekye and J. I. Agbinya, "Vertical handoff decision algorithm based on fuzzy logic and genetic algorithm," in *Proceedings of Southern African Telecommunication Networks & Applications Conference (SATNAC 2008), Wild Coast Sun, Eastern Cape, South Africa*, pp. 7–10, 2008.
- [244] S. Mohanty and I. F. Akyildiz, "A cross-layer (layer 2+ 3) handoff management protocol for next-generation wireless systems," *IEEE transactions on mobile computing*, vol. 5, no. 10, pp. 1347–1360, 2006.
- [245] X. Yan, N. Mani, and Y. A. Sekercioglu, "A traveling distance prediction based method to minimize unnecessary handovers from cellular networks to wlans," *IEEE communications letters*, vol. 12, no. 1, pp. 14–16, 2008.
- [246] A. F. Christopher and M. Jeyakumar, "User data rate based vertical handoff in 4g wireless networks.," *Journal of Theoretical & Applied Information Technology*, vol. 58, no. 1, 2013.
- [247] A. H. Zahran, B. Liang, and A. Saleh, "Signal threshold adaptation for vertical handoff in heterogeneous wireless networks," *Mobile Networks and Applications*, vol. 11, no. 4, pp. 625–640, 2006.
- [248] C. W. Lee, L. M. Chen, M. C. Chen, and Y. S. Sun, "A framework of handoffs in wireless overlay networks based on mobile ipv6," *IEEE journal on selected areas in communications*, vol. 23, no. 11, pp. 2118–2128, 2005.
- [249] K. Yang, I. Gondal, B. Qiu, and L. Dooley, "Combined sinr based vertical handoff algorithm for next generation heterogeneous wireless networks," 2007.
- [250] H. J. Wang, R. H. Katz, and J. Giese, "Policy-enabled handoffs across heterogeneous wireless networks," in *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on*, pp. 51–60, IEEE, 1999.

- [251] F. Zhu and J. McNair, "Optimizations for vertical handoff decision algorithms," in *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE*, vol. 2, pp. 867–872, IEEE, 2004.
- [252] C. Sun, E. Stevens-Navarro, and V. W. Wong, "A constrained mdp-based vertical handoff decision algorithm for 4g wireless networks," in *Communications, 2008. ICC'08. IEEE International Conference on*, pp. 2169–2174, IEEE, 2008.
- [253] K. Savitha and C. Chandrasekar, "An overview of vertical handoff decision based on madm for heterogeneous wireless network," *Journal of Computer Application (JCA)*, vol. 3, no. 3, pp. 12–15, 2010.
- [254] K. Radhika and A. V. Reddy, "Ahp and group decision making for access network selection in multi-homed mobile terminals," *International Journal on Computer Science and Engineering*, vol. 3, no. 10, p. 3412, 2011.
- [255] M. Lahby, L. Cherkaoui, and A. Adib, "An intelligent network selection strategy based on madm methods in heterogeneous networks," *arXiv preprint arXiv:1204.1383*, 2012.
- [256] W. Nan, S. Wenxiao, F. Shaoshuai, and L. Shuxiang, "Pso-fnn-based vertical handoff decision algorithm in heterogeneous wireless networks," *Procedia Environmental Sciences*, vol. 11, pp. 55–62, 2011.
- [257] P. T. Kene and M. S. Madankar, "Flc based handoff mechanism for heterogeneous wireless network: a design approach," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 2, pp. 653–658, 2013.
- [258] B. L. Miller, D. E. Goldberg, *et al.*, "Genetic algorithms, tournament selection, and the effects of noise," *Complex systems*, vol. 9, no. 3, pp. 193–212, 1995.
- [259] D. Whitley, "A genetic algorithm tutorial," *Statistics and computing*, vol. 4, no. 2, pp. 65–85, 1994.
- [260] C. W. Ahn and R. S. Ramakrishna, "Elitism-based compact genetic algorithms," *IEEE Transactions on Evolutionary Computation*, vol. 7, no. 4, pp. 367–385, 2003.

- [261] M. Mitchell, *An introduction to genetic algorithms*. MIT press, 1998.
- [262] E. Stevens-Navarro and V. W. Wong, “Comparison between vertical handoff decision algorithms for heterogeneous wireless networks,” in *Vehicular technology conference, 2006. VTC 2006-Spring. IEEE 63rd*, vol. 2, pp. 947–951, IEEE, 2006.
- [263] “Grameenphone.” <http://www.grameenphone.com>, 2014. [Last accessed on 16-September-2016].
- [264] “Pss calculation.” <http://developer.android.com/reference/android/os/Debug.MemoryInfo.html>, 2014. [Last accessed on 16-September-2016].
- [265] “Two ray ground reflection model.” <http://www.isi.edu/nsnam/ns/doc/node-219.html>, 2016. [Last accessed on 16-September-2016].
- [266] T. Stathopoulos, M. Lukac, D. McIntire, J. Heidemann, D. Estrin, and W. J. Kaiser, “End-to-end routing for dual-radio sensor networks,” in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pp. 2252–2260, IEEE, 2007.
- [267] Y. Xiao, P. Savolainen, A. Karppanen, M. Siekkinen, and A. Ylä-Jääski, “Practical power modeling of data transmission over 802.11 g for wireless applications,” in *Proceedings of the 1st International Conference on Energy-efficient Computing and Networking*, pp. 75–84, ACM, 2010.
- [268] D. Halperin, B. Greenstein, A. Sheth, and D. Wetherall, “Demystifying 802.11 n power consumption,” in *Proceedings of the 2010 international conference on Power aware computing and systems*, p. 1, 2010.
- [269] J. Polastre, R. Szewczyk, and D. Culler, “Telos: enabling ultra-low power wireless research,” in *Information Processing in Sensor Networks, 2005. IPSN 2005. Fourth International Symposium on*, pp. 364–369, IEEE, 2005.
- [270] “Car 2 car communication consortium, <http://www.car-to-car.org>,” 2013. [Last accessed: December 1, 2018].

- [271] “Airborne networks, <http://www.technologyreview.com>,” 2013. [Last accessed: December 1, 2018].
- [272] P. Gupta and P. R. Kumar, “The capacity of wireless networks,” *IEEE Transactions on information theory*, vol. 46, no. 2, pp. 388–404, 2000.
- [273] A. R. Syed S. Rizvi and K. M. Elleithy, “A new efficient 3-phase algorithm for performing capacity analysis of mobile ad hoc networks (manet),” 9th *INFORMS Telecommunications Conference: Telecommunications Modeling, Policy, and Technology*, vol. 12, no. 1, pp. 388–404, 2008.
- [274] K. K. Sharma, H. Sharma, and A. Ramani, “Modeling and analysis of end-to-end delay for ad hoc pervasive multimedia network,” in *Proceedings of the International MultiConference of Engineers and Computer Scientists*, vol. 1, 2010.
- [275] “Two-ray model, <http://www.isi.edu/nsnam/ns/doc/node219.html>,” 2013. [Last accessed: December 1, 2018].
- [276] A. Ghandar, E. Shabaan, and Z. T. Fayed, “Performance analysis of observation based cooperation enforcement in ad hoc networks,” *arXiv preprint arXiv:1201.3782*, 2012.
- [277] M. I. M. Saad and Z. A. Zukarnain, “Performance analysis of random-based mobility models in manet routing protocol,” *European Journal of Scientific Research*, vol. 32, no. 4, pp. 444–454, 2009.
- [278] P. Pesic, *Abel’s proof*. MIT press Cambridge, MA, 2003.
- [279] R. Sanchez-Iborra, J. Sanchez-Gomez, J. Ballesta-Viñas, M.-D. Cano, and A. F. Skarmeta, “Performance evaluation of lora considering scenario conditions,” *Sensors*, vol. 18, no. 3, p. 772, 2018.
- [280] N. Nurain, S. Tairin, T. A. Khan, S. Ishraq, and A. A. Al Islam, “Power attack: An imminent security threat in real-time system for detecting missing rail blocks in developing countries,” *Computers & Security*, vol. 84, pp. 35–52, 2019.
- [281] N. Nurain, B. M. S. B. Talukder, T. Choudhury, S. Tairin, M. Ferdousi, M. Naznin, and A. A. Al Islam, “Exploring network-level performances of wireless nanonetworks

- utilizing gains of different types of nano-antennas with different materials,” *Wireless Networks*, vol. 25, no. 5, pp. 2651–2664, 2019.
- [282] T. Chakraborty, N. Nurain, S. Tairin, T. A. Khan, J. Noor, M. R. Islam, and A. A. Al Islam, “A new network paradigm for low-cost and lightweight real-time communication between train and rail track to detect missing and faulty rail blocks,” *Journal of Network and Computer Applications*, vol. 131, pp. 40–54, 2019.
- [283] A. A. Al Islam, M. J. Islam, N. Nurain, and V. Raghunathan, “Channel assignment techniques for multi-radio wireless mesh networks: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 988–1017, 2015.
- [284] N. Nurain and A. Islam, “Power attack: An emerging threat in health-care applications using medical body area networks,” in *Proceedings of the 7th Annual Symposium on Computing for Development*, p. 33, ACM, 2016.
- [285] N. Nurain and A. Islam, “Power attack: An emerging threat in health-care applications using medical body area networks,” in *Proceedings of the 7th Annual Symposium on Computing for Development*, p. 33, ACM, 2016.
- [286] S. Tairin, N. Nurain, and A. A. Al Islam, “Network-level performance enhancement in wireless nanosensor networks through multi-layer modifications,” in *2017 International Conference on Networking, Systems and Security (NSysS)*, pp. 75–83, IEEE, 2017.
- [287] N. Nurain, T. Akter, H. Zannat, M. M. Akter, A. A. Al Islam, and M. H. Kabir, “General-purpose multi-objective vertical hand-off mechanism exploiting network dynamics,” in *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 825–832, IEEE, 2015.
- [288] N. Nurain, M. Mostakim, and A. A. Al Islam, “Towards empirical study based mathematical modeling for throughput of manets,” in *2015 International Conference on Networking Systems and Security (NSysS)*, pp. 1–6, IEEE, 2015.
- [289] N. Nurain, M. Mostakim, and A. A. Al Islam, “Towards empirical study based mathematical modeling for energy consumption and end-to-end delay of manets,” in *2014*

17th International Conference on Computer and Information Technology (ICCIT), pp. 424–429, IEEE, 2014.

- [290] T. R. Toha, M. M. Lunar, A. Rizvi, N. Nurain, and A. A. Al Islam, “Gmc: Greening mapreduce clusters considering both computational energy and cooling energy,” in *2018 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2018.
- [291] Q. M. Alam, B. Sarker, B. Biswas, K. H. Zubaer, T. R. Toha, N. Nurain, and A. A. Al Islam, “Towards simulating non-lane based heterogeneous road traffic of less developed countries.,” in *ICT4S*, pp. 37–48, 2018.
- [292] M. Islam, M. N. Ansary, N. Nurain, S. P. Shams, and A. A. Al Islam, “A sweet recipe for consolidated vulnerabilities: Attacking a live website by harnessing a killer combination of vulnerabilities for greater harm,” in *2018 5th International Conference on Networking, Systems and Security (NSysS)*, pp. 1–9, IEEE, 2018.
- [293] M. Alam, N. Nurain, S. Tairin, M. Naznin, and A. A. Al Islam, “Conjugate congestion control based transport layer protocol for molecular communication in body area nanonetworks (bans),” in *2018 5th International Conference on Networking, Systems and Security (NSysS)*, pp. 1–6, IEEE, 2018.
- [294] M. Alam, N. Nurain, S. Tairin, and A. A. Al Islam, “Energy-efficient transport layer protocol for hybrid communication in body area nanonetworks,” in *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, pp. 674–677, IEEE, 2017.
- [295] R. A. Shetu, T. Toha, M. M. R. Lunar, N. Nurain, and A. A. Al Islam, “Workload-based prediction of cpu temperature and usage for small-scale distributed systems,” in *2015 4th International Conference on Computer Science and Network Technology (ICCSNT)*, vol. 1, pp. 1090–1093, IEEE, 2015.