Location Dependent Key Management Schemes Supported By Random Selected Cell Reporters In Wireless Sensor Network

Harith Fakhrey Tahir Al-Shwaily

Newcastle University

Newcastle upon Tyne, UK

A thesis submitted for the degree of

Doctor of Philosophy

May 2018

It is my genuine gratefulness that I dedicate this work to:

My life-coach, my two late mothers: because I owe it all to you.

My lovely wife **Banafsaj** and my son **Ali**.

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This thesis is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and acknowledgements.

Signature:

Student: Harith Al-Shwaily

Date:

Certificate of Approval

I confirm that, to the best of my knowledge, this thesis is from the student's own work and effort, and all other sources of information used have been acknowledged. This thesis has been submitted with my approval.

Signature:

Supervisor name: Dr. Martin Johnston

Date:

Acknowledgements

I would like to express my genuine appreciation and gratitude to my supervisors Dr. Martin Johnston and Dr Rajesh Tiwari for their guidance, assistance and support during my PhD project. They have been a source of motivation and inspiration and their participation in transferring research skills to help me being a researcher.

I would like to show my gratefulness for all martyrs fallen during the holy Iraqi war against terrorists and to all members in Iraqi army and all supporter troops. Their sacrifice protect my family in Iraq and contribute to maintain a peaceful studying atmosphere during my research.

I am also grateful to my lovely wife Banafsaj for her emotional support, encouragement and moral assistance. I am also grateful to my father, brothers, sisters, and all my friends in Iraq and UK for their support and encouragement to finish my study successfully.

In addition, I would like to thank all colleagues and staff within the School of Electrical and Electronic Engineering at Newcastle University for their help and support to make my times here wonderful both socially and educationally. A very special gratitude goes out to Wael, Yasir, Sinan, Bilal, Zaid, Ahmed and Israa.

I also would like to show my gratitude to my colleague Dr. Yaarob Al-Nidawi and Federico Angelini for their advices and supports in this project.

Last but not least, I would like to thank the Ministry of Higher Education and Scientific Research in Iraq and the Iraqi Cultural Attaché in London for providing the opportunity to complete my PhD degree and their continuous support and encouragement.

To all I say, thank you very much.

Abstract

In order to secure vital and critical information inside Wireless Sensor Networks (WSNs), a security requirement of data confidentiality, authenticity and availability should be guaranteed. The leading key management schemes are those that employ location information to generate security credentials. Therefore, this thesis proposes three novel location-dependent key management schemes.

First, a novel Location-Dependent Key Management Protocol for a Single Base Station (LKMP-SBS) is presented. As a location-dependent scheme, the WSN zone is divided virtually into cells. Then, any event report generated by each particular cell is signed by a new type of endorsement called a cell-reporter signature, where cell-reporters are defined as a set of nodes selected randomly by the BS out of the nodes located within the particular cell. This system is analysed and proved to outperform other schemes in terms of data security requirements. Regarding the data confidentiality, for three values of z (1,2,3) the improvement is 95%, 90% and 85% respectively when 1000 nodes are compromised. Furthermore, in terms of data authenticity an enhancement of 49%, 24%, 12.5% is gained using our approach with $z = 1, 2, 3$ respectively when half of all nodes are compromised. Finally, the optimum number of cell reporters is extensively investigated related to the security requirements, it is proven to be $z = \frac{n}{2}$.

The second contribution is the design of a novel Location-Dependent Key Management Protocol for Multiple Base Stations (LKMP-MBS). In this scheme, different strategies of handling the WSN by multiple BSs is investigated. Accordingly, the optimality of the scheme is analysed in terms of the number of cell reporters. Both data confidentiality and authenticity have been proven to be $\propto e \propto \frac{1}{N}$. The optimum number of cell reporters had been calculated as

$z_{opt} = \frac{n}{2M}$, $\sum_{\ell=1}^{M} |z_{opt}^{(\ell)}| = \dfrac{n}{2M}$. Moreover, the security robustness of this scheme is analysed and proved to outperform relevant schemes in terms of data confidentiality and authenticity. Furthermore, in comparison with LKMP-SBS, the adoption of multiple base stations is shown to be significantly important in improving the overall system security.

The third contribution is the design of the novel Mobility- Enabled, Location-dependant Key Managment Protocol for Multiple BSs (MELKMP-MBS). This scheme presents a key management scheme, which is capable of serving a WSN with mobile nodes. Several types of handover are presented in order to maintain the mobile node service availability during its movement between two zones in the network. Accordingly, the communication overhead of MELKMP-MBS is analysed, simulated and compared with the overhead of other schemes. Results show a significant improvement over other schemes in terms of handover efficiency and communication over head. Furthermore, the optimality of WSN design such as the value of N, n is investigated in terms of communication overhead in all protocols and it is shown that the optimum number of nodes in each cell, which cause the minimum communication overhead in the network , is $n = \sqrt[3]{2N}$.

Contents

List of Figures **xi**

List of Tables **xviii**

List of Acronyms **xix**

1 Introduction **1**

1.1 Emergence of Large Scale WSN 2

1.2 WSN Security Challenges 3

1.3 Cell Reporters 4

1.4 Motivation and Challenges 4

1.5 Thesis Contribution 5

1.6 Thesis Outline 6

1.7 Research Publication 7

2 Background Theory and Literature Review **8**

2.1 WSN Background 8

2.2 En-Route Filtering 9

2.3 Security Primitives 11

2.4 Key Management System 13

2.4.1 KMS Evaluation Metrics: 13

2.4.2 KMS Literature Review 15

2.4.3 Distributed KMS 18

2.4.4 Centralised KMS 20

2.4.5 Hybrid KMS 23

2.4.6 KMS for Multiple BSs 24

2.4.7 Location Dependent KMS 25

2.5 WSN integration with The Internet 29

2.5.1 Introduction . . . 29
2.5.2 Integration Schemes . . . 30
2.6 Challenges and solutions . . . 31
2.7 Routing attacks . . . 32

3 Location-Dependent Key Management Protocol for a Single BS WSN 34
3.1 Introduction . . . 34
3.2 System Consideration . . . 35
3.3 Threat Model . . . 35
3.4 Notation and Terms . . . 35
3.5 Setup Phase . . . 37
3.6 Report Generation . . . 43
3.6.1 The first endorsement: similar report is received from different nodes 44
3.6.2 The second endorsement: MAC of authentication nodes . . . 44
3.6.3 The third endorsement: signature of cell reporters . . . 45
3.7 Key Revocation . . . 45
3.7.1 Key revocation in case of detecting a suspicious node . . . 46
3.7.2 Key revocation in case of detecting a suspicious node . . . 46
3.8 Security Analysis of LKMP-SBS . . . 48
3.8.1 System Robustness Against Routing Attacks . . . 48
3.8.2 The impact of z value on the security of each particular cell . . . 49
3.8.3 Security Strength Regarding Data Confidentiality . . . 51
3.8.3.1 The effect of N on the value of $P_{C\{\varepsilon|z\}}$ . . . 58
3.8.3.2 The effect of ε on the value of $P_{C\{\varepsilon|z\}}$ . . . 59
3.8.4 Security Strength for Data Authenticity . . . 60
3.8.4.1 The effect of N on the value of $P_{auth\{\varepsilon|z\}}$ . . . 70
3.8.4.2 The effect of ε on the value of $P_{auth\{\varepsilon|z\}}$ . . . 71
3.9 Optimum number of Cell Reporters . . . 72
3.9.1 Mathematical Analysis of optimum z based on $P_{C\{\varepsilon|z\}}$ and $P_{auth\{\varepsilon|z\}}$ 72
3.9.2 Mathematical Analysis of optimum z based on P_{zcomp} . . . 74
3.10 Conclusion . . . 76

4 Location-Dependent Key Management Protocol for a Multiple BSs WSN 79
4.1 Introduction . . . 79

4.2 WSN Control Scheme by Multiple BSs 80
4.3 System Consideration 81
4.4 Notation and Terms 82
4.5 Setup Phase 84
4.6 Report Generation 88
4.7 Key Revocation 89
4.8 Security Analysis of LKMP-MBS 91
4.8.1 Security Strength in Terms of Data Confidentiality 92
4.8.2 Security Strength in Terms of Data Authenticity 101
4.9 The Optimum Number of Cell Reporters 113
4.9.1 IndCon: Cell reporter sets having no mutual elements 114
4.9.2 ColCon: Some elements are mutual between different cell reporter sets 117
4.10 Conclusion 119

5 MELKMP-MBS: Protocol Description and Communication Overhead Analysis 122

5.1 Introduction 122
5.2 Nodes Mobility between different BS coverage regions 123
5.3 Setup Phase 124
5.3.1 Handover Phase 126
5.3.1.1 Local handover 126
5.3.1.2 Global handover 128
5.4 Communication overhead 130
5.4.1 MELKMP-MBS 133
5.4.1.1 Communication Overhead of Setup Phase and Report Generation Phase 134
5.4.1.2 Communication Overhead of Node Mobility 136
5.4.2 LKMP-SBS 142
5.4.2.1 Optimum value of n 150
5.4.3 LKMP-MBS 153
5.5 Computational cost 155
5.6 Conclusion 159

6 Conclusions and Future Work **160**

6.1 Conclusion 160

6.2 Future Work 162

References **165**

List of Figures

2.1 WSN structure. 10
2.2 A taxonomy of En-route filtering techniques [1]. 10
2.3 Symmetric-based techniques. 11
2.4 Classification of the schemes studied by [2] with references. 17
2.5 Categorisation of integration approaches [3]. 29
2.6 a) Hybrid approach; b) Gateway approach [4]. 31

3.1 Illustration of system construction shows report forward route and authentication cells for a WSN with $n \simeq 3$ and $t = 2$. 38
3.2 Event Report R structure. 43
3.3 Adjacent cells of a suspicious cell (sc). 47
3.4 Data confidentiality of LKMP-SBS and MKMP under random capture attack in a WSN consist of $N = 5,000$ for different values of ε and z. 53
3.5 Data confidentiality of LKMP-SBS and MKMP under random capture attack in a WSN consist of $N = 10,000$ for different values of ε and z. 54
3.6 Data confidentiality of LKMP-SBS and MKMP under random capture attack in a WSN consist of $N = 20,000$ for different values of ε and z. 55
3.7 Data confidentiality of LKMP-SBS and MKMP under random capture attack in a WSN consist of $N = 30,000$ for different values of ε and z. 56
3.8 The effect of changing the number of whole nodes in the network N on the Probability of compromising all cells in terms of data confidentiality due to RNCA, $\varepsilon = 10$, $z = 5$. 57
3.9 The effect of changing the number of endorsement nodes in the network ε on the Probability of compromising all cells in terms of data confidentiality due to RNCA, $N = 10,000$, $z = \frac{\varepsilon}{2}$. 58

3.10 Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 10,000$, $\varepsilon = 4$ and $z = 1, 2, 3, 4$. 62
3.11 Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 10,000$, $\varepsilon = 6$ and $z = 1, 2, 3, 4$. 62
3.12 Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 10,000$, $\varepsilon = 8$ and $z = 1, 2, 3, 4$. 63
3.13 Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 10,000$, $\varepsilon = 10$ and $z = 1, 2, 3, 4$. 63
3.14 Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 20,000$, $\varepsilon = 4$ and $z = 1, 2, 3, 4$. 64
3.15 Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 20,000$, $\varepsilon = 6$ and $z = 1, 2, 3, 4$. 64
3.16 Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 20,000$, $\varepsilon = 8$ and $z = 1, 2, 3, 4$. 65
3.17 Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 20,000$, $\varepsilon = 10$ and $z = 1, 2, 3, 4$. 65
3.18 Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 30,000$, $\varepsilon = 4$ and $z = 1, 2, 3, 4$. 66
3.19 Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 30,000$, $\varepsilon = 6$ and $z = 1, 2, 3, 4$. 66
3.20 Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 30,000$, $\varepsilon = 8$ and $z = 1, 2, 3, 4$. 67

3.21 Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 30,000$, $\varepsilon = 10$ and $z = 1, 2, 3, 4$. 67
3.22 The effect of changing the number of whole nodes in the network N on the Probability of compromising all cells in terms of data authenticity due to RNCA, $\varepsilon = 10$, $z = 5$. 69
3.23 The effect of changing the number of endorsement nodes in the network ε on the Probability of compromising all cells in terms of data authenticity due to RNCA, $N = 10,000$, $z = \frac{\varepsilon}{2}$. 69
3.24 The relationship between number of cell reporters (z) and the probability of compromising all cell reporters inside a cell of 10, 20 and 30 nodes. . . . 77

4.1 A WSN controlled individually by two BSs BS_1 and BS_2 81
4.2 A WSN controlled collaboratively by two BSs BS_1 and BS_2 82
4.3 Illustration of system construction showing report forward route and authentication cells for a WSN with $M = 3$,$n \simeq 3$ and $t = 2$ 85
4.4 Data confidentiality of LKMP-MBS and MKMP under random node capture attack in a WSN consist of $N = 5,000$, $z = 3$ and for different values of ε. 94
4.5 Data confidentiality of LKMP-MBS and MKMP under random node capture attack in a WSN consist of $N = 10,000$, $z = 3$ and for different values of ε. 95
4.6 Data confidentiality of LKMP-MBS and MKMP under random node capture attack in a WSN consist of $N = 20,000$, $z = 3$ and for different values of ε. 96
4.7 Data confidentiality of LKMP-MBS and MKMP under random node capture attack in a WSN consist of $N = 30,000$, $z = 3$ and for different values of ε. 97
4.8 The effect of changing the number of nodes in the network N on the probability of compromising all cells in terms of data confidentiality due to RNCA, $M = 4$,$\varepsilon = 10$ and $z = 5$. 98
4.9 The effect of changing the number of endorsement nodes in the network ε on the probability of compromising all cells in terms of data confidentiality due to RNCA, $N = 10,000$, $M = 4$ and $z = \frac{\varepsilon}{2}$. 99

4.10 Comparison between LKMP-MBS and LKMP-SBS for different values of M in terms of $P_{C\{\varepsilon|z\}}$ due to a RNCA in a WSN consisting of $N = 5,000$, $z = 1, 3, 5, 7$ and $n = Mz + 3$. 102
4.11 Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 10,000$, $\varepsilon = 4$ and $z = 3$. 104
4.12 Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 10,000$, $\varepsilon = 6$ and $z = 3$. 104
4.13 Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 10,000$, $\varepsilon = 8$ and $z = 3$. 105
4.14 Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 10,000$, $\varepsilon = 10$ and $z = 3$. 105
4.15 Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 20,000$, $\varepsilon = 4$ and $z = 3$. 106
4.16 Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 20,000$, $\varepsilon = 6$ and $z = 3$. 106
4.17 Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 20,000$, $\varepsilon = 8$ and $z = 3$. 107
4.18 Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 20,000$, $\varepsilon = 10$ and $z = 3$. 107
4.19 Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 30,000$, $\varepsilon = 4$ and $z = 3$. 108
4.20 Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 30,000$, $\varepsilon = 6$ and $z = 3$. 108

4.21 Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 30,000$, $\varepsilon = 8$ and $z = 3$. 109
4.22 Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 30,000$, $\varepsilon = 10$ and $z = 3$. 109
4.23 The effect of changing the number of nodes in the network N on the probability of compromising all cells in terms of data authenticity due to RNCA, $\varepsilon = 10$, $z = 3$. 111
4.24 The effect of changing the number of endorsement nodes in the network ε on the Probability of compromising all cells in terms of data authenticity due to RNCA, $N = 10,000$, $z = \frac{\varepsilon}{2}$. 111
4.25 The relationship between the number of cell reporters (z) and the probability of compromising all cell reporters (P_{z_comp}) for a WSN with four BSs ($M = 4$) when the number of sensor nodes inside each cell $n = 20, 30$ and 40.116
4.26 The relationship between the number of cell reporters (z) and the probability of compromising all cell reporters (P_{z_comp}) inside a a particular cell for different numbers of BS ($M = 1, 2, 3$). 120

5.1 A 16 cell WSN controlled collaboratively by two BSs, i.e., BS_1 and BS_2. . 124
5.2 Message sequence chart of the intended mobility local handover. 131
5.3 Message sequence chart of the Non-intended mobility local handover. . . . 131
5.4 Message sequence chart of the intended mobility global handover followed when a node a is moved from BS_{old} coverage area to BS_{new} coverage area . 132
5.5 Message sequence chart of the Non-intended mobility global handover followed when a node a is moved from BS_{old} coverage area to BS_{new} coverage area. 132
5.6 A square terrain of size A divided into 100 cells and covered by a WSN consists of $N = 300$ where each side contains $\backsimeq \sqrt{300}$. 134
5.7 Node mobility in a square terrain consist of N nodes, $N' = \frac{N}{n}$ cells and covered by 4 BS each one has a square coverage. 138
5.8 Node mobility in a square terrain consist of N nodes, $N' = \frac{N}{n}$ cells and covered by 4 BS each one has a circular coverage. 139

5.9 Node mobility in a square terrain consist of N nodes, $N' = \frac{N}{n}$ cells and covered by 4 BS each one has a hexagonal coverage. 140
5.10 Comparison between communication cost of ELKMP-MBS for different values of n, N. 142
5.11 Communication overhead vs. N for MELKMP-MBS, SODD and TTDD (Circular BS coverage, intended mobility, $d = 100$ packet, $\lambda = 1$ packet). . 143
5.12 Communication overhead vs. N for MELKMP-MBS, SODD and TTDD (Hexagonal BS coverage, intended mobility, $d = 100$ packet, $\lambda = 1$ packet). 144
5.13 Communication overhead vs. N for MELKMP-MBS, SODD and TTDD (Square BS coverage, intended mobility, $d = 100$ packet, $\lambda = 1$ packet). . . 145
5.14 Communication cost of LKMP-SBS, LEDS/MKMP, TODD and SODD ($n = 2$, $d = 100$ packet, $\lambda = 1$ packet). 146
5.15 Communication cost of LKMP-SBS, LEDS/MKMP, TODD and SODD ($n = 5$, $d = 100$ packet, $\lambda = 1$ packet). 146
5.16 Communication cost of LKMP-SBS, LEDS/MKMP, TODD and SODD ($n = 10$, $d = 100$ packet, $\lambda = 1$ packet). 147
5.17 Communication cost of LKMP-SBS, LEDS/MKMP, TODD and SODD ($n = 20$, $d = 100$ packet, $\lambda = 1$ packet). 147
5.18 Communication cost of LKMP-SBS, LEDS/MKMP, TODD and SODD ($n = 40$, $d = 100$ packet, $\lambda = 1$ packet). 148
5.19 Communication cost of LKMP-SBS, LEDS/MKMP, TODD and SODD ($n = 60$, $d = 100$ packet, $\lambda = 1$ packet). 148
5.20 Communication cost of LKMP-SBS, LEDS/MKMP, TODD and SODD ($n = 80$, $d = 100$ packet, $\lambda = 1$ packet). 149
5.21 Communication cost of LKMP-SBS, LEDS/MKMP, TODD and SODD ($n = 100$, $d = 100$ packet, $\lambda = 1$ packet). 149
5.22 Communication cost of LKMP-SBS versus the number of total nodes in the network (N) for different number of nodes inside each cell ($n = (100, 60, 40, 10, 2)$). 150
5.23 Communication cost of LKMP-SBS vs. the number of nodes inside each cell n for $N = 10,000, 30,000, 50,000, 70,000, 90,000$. 151
5.24 Communication overhead vs. N for LKMP-MBS, MKMP, SODD and TTDD ($M = 2$, $d = 100$ packet, $\lambda = 1$ packet). 154
5.25 Communication overhead vs. N for LKMP-MBS, MKMP, SODD and TTDD ($M = 4$, $d = 100$ packet, $\lambda = 1$ packet). 156

5.26 Communication overhead vs. N for LKMP-MBS, MKMP, SODD and TTDD ($M = 6$, $d = 100$ packet, $\lambda = 1$ packet). 157
5.27 Communication overhead vs. N for LKMP-MBS, MKMP, SODD and TTDD ($M = 8$, $d = 100$ packet, $\lambda = 1$ packet). 158
5.28 Communication cost of LKMP-MBS for different values of $M = 2, 4, 6, 8$. . 159

6.1 BS performance monitoring system 164

List of Tables

1.1 Feature comparison of the main RTLS market players [5]. 2
1.2 Popular Security Threats in WSNs [6, 7]. 4

3.1 Approximate value of x_t for different values of N, ε and z. 68

4.1 Comparison between LKMP-MBS and LKMP-SBS in terms of X_t. 110
4.2 Status matrix of the Markov module 120

5.1 Communication cost analysis for LEDS/MKMP and LKMP-SBS 135
5.2 Simulation vs. Mathematical results of the optimum n in terms of communication overhead 152
5.3 Reduction in computational overhead ΔP vs. N, t 155

List of Acronyms

Acronyms/Abbreviations

AES	Advanced Encryption Standard
AN	Anchor Node
ASCBKE	Asymmetric Cryptography Based Key Exchange
B-PCGR	Basic PCGR
BS	Base Station
C-PCGR	Cascaded PCGR
CH	Cluster Head
DoS	Denial of Service
DSEDA	Digital Signature assisted End-to-end Data Authentication
EBS	Exclusion Basis System
ECC	Elliptic Curve Cryptography
EDDK	Energey-eficient Distributed Deterministic Key management
EEKM	Energey-eficient Key Management protocol
FPWK	Full Pairwise Keys
IoT	Internet of Things
IP	Internet Protocol
KMS	Key Management System
LBRS	Location-Based Resilient Secrecy

LDK	Location Dependent Keying
LEDS	Location-dependent End-to-end Data Security
LKMP-MBS	Location-Dependent Key Management Protocol for MBS
LKMP-SBS	Location-Dependent Key Management Protocol for a SBS
Lock	LOcalized Combinatorial Keying
MAC	Message Authentication Codes
MBS	Multiple Base Station
MELKMP-MBS	Mobility Enabled LKMP-MBS
MKMP	Multi-BS Key Management Protocol
PCGR	Pre-distribution and local Collaboration-based Group Re-keying
PCREF	Polynomial-based Compromise-Resilient En-route Filtering scheme
PGK	Plain Global Key
PKC	Public Key Cryptography
PUF	Physical Uncloneable Function
RSDTMK	Random Seed Distribution with Transitory Master Key
SBS	Single Base Station
SCBKE	Symmetric Cryptography Based Key Exchange
SCBKE	Symmetric Key Cryptography
SHELL	Scalable, Hierarchical, Efficient, Location-aware and Lightweight
SKC	Symmetric Key Cryptography
SN	Sensor Node
STKM	Spanning Tree Key Management
TCP/IP	Transmission Control Protocol Internet Protocol (TCP/IP)
WLAN	Wireless Local Area Network
WSN	Wireless Sensor Network

Chapter 1

Introduction

Wireless sensor networks (WSNs) came into prominence in the last decade, inspired by the ubiquitous scenario of communicating sensors that have a limited power and relatively small size, typically deployed in great numbers over a large area and employed to monitor various phenomenon. WSNs have been reported as one of the most significant technologies of the recent century. As a result, this type of network has gathered much interests in optimising the architecture depending on different aspects. The construction of any network and its resource limitations decide whether it is sufficient to be used in a specific application or not. According to [7, 8] a WSN probably contains hundreds or thousands of sensor nodes with some or all of following characteristics: Self-organization, low-power and low cost (storage, communication and processing). All of these nodes are employed in various applications such as military intuition and tracking, environmental monitoring and disaster prediction. Thus, WSN is a rather large network, widespread and might be used in critical applications. As a result, the building of a rigid security scheme is significantly crucial to protect the communicated data.

Moreover, WSNs can be integrated with Internet of things (IoT), which is a connection of real world physical objects with the Internet [9]. There are some topologies that have been adopted to maintain this integration [10, 11]. However, many security issues need to be taken into account when each integration scheme is applied [4]. One limitation of most used schemes is the consideration of the Base station (BS) as a single point of failure. According to [10], a possible solution is the use of multiple BSs which can offer an improvement to the network availability in addition to load balance. However, such a system might have some challenges such as those related to data consistency.

1.1 Emergence of Large Scale WSN

One of the main areas of research within the smart city context is smart health, which engages novel IoT initiatives to improve both quality and access to health care and smart services in general. Smart health is a hot topic targeted by many researches, as an instance, the study implemented by Adame, Toni, et al. in [5]. This study presents an IoT hybrid monitoring system for health care environments which integrates RFID and WSN technologies in a single platform providing location, status, and tracking of patients and assets. According to literature review presented in [5], WSNs deployed in Real time locating system (RTLS) used in health care services are a large scale networks consists of up to thousands of nodes as shown in table 1.1.

Table 1.1: Feature comparison of the main RTLS market players [5].

RTLS	Technology Support	Number of Nodes
RFID global solutions [12]	Barcode UWB Active, passive, and semi-passive RFID (900 MHz)	Tens of thousands
Stanley Healthcare [13]	WiFi Ultrasound (40 kHz) Active RFID (125 kHz, 434 MHz)	Tens of thousands
Ekahau [14]	WiFi Active RFID (2.4 GHz) Infrared	50,000
Awarepoint [15]	WiFi BLE	Thousands
Centrak [16]	WiFi Gen2IR BLE Active RFID (900 MHz)	Thousands
TeleTracking [17]	Infrared Active RFID (900 MHz)	Thousands
Zebra [18]	WiFi IEEE 802.15.4f UWB (6.35–6.75 GHz) Active RFID (900 MHz)	Thousands
Radianse [19]	WiFi Active RFID (433 MHz)	Thousands

1.2 WSN Security Challenges

As explained previously, securing communicated data inside WSNs is significantly crucial due to data criticality and WSN employment in vulnerable places. However, providing data security in a WSN has a number of challenges as described below [7]:

- The enormous number of nodes deployed usually in WSNs in comparison with traditional Ad Hoc networks which lead to the necessity of designing a security protocol with very good scalability.
- The resources of sensor nodes deployed within any WSN are extremely limited. Therefore, the proposed security protocol has to be energy efficient.
- WSN topology is usually dynamic where there are frequent changes for different reasons such as: node addition/removal, node revocation and node relocation. One key factor of any security protocol performance is measured by how it copes with the possible changes in network topology.
- WSN sensor nodes are lacking of a global identifications in contrast to conventional networks that consist of Internet protocol (IP) based entities. Therefore, a proposed security protocol must not require any global identification.

According to [6], security attacks on WSNs are classified into:

- Outsider attackers: The adversary is not an element of the WSN, e.g. a jamming attack carried out by a node that does not belong to the network and is applied on the physical layer of sensor nodes belonging to this network.
- Insider Attacker: The adversary compromises one of the WSN nodes by using node tampering or by making use of a software bug in the system.

In addition to conventional security threats such as replay attack, Denial of service (DoS) and information disclosure, there are some specific attacks targeting WSNs such as: Sybil attack, sink node attack, sinkhole attack, node replication attack, and wormhole attack [6, 7]. The most common threats are illustrated in Table. 1.2.

Table 1.2: Popular Security Threats in WSNs [6, 7].

Threat	Layer	Insider	Outsider
Jamming Attack, Node Tampering Attack	Physical		✓
Collision Attack, Exhaustion Attack, Unfair Competition Attack	Data Link	✓	✓
Traffic Analysis, False Routing Information Attack, Selective Forwarding Attack,Sinkhole Attack, Sybil Attack, Wormhole Attack, HELLO Flood Attack, Acknowledgment Spoof Attack, Passive Wiretapping Attack	Network	✓	
Flooding Attack, Desynchronization Attack	Transport	✓	

1.3 Cell Reporters

The core paradigm in this thesis is the consideration of the availability of a hidden agent inside each group of nodes in a particular region. This agent is an ordinary node selected randomly by BS or a group of BSs and called a "Cell Reporter". The selected reporter has neither a privilege nor any extra credentials and does not informed about its new role as a "cell reporter" in order to prevent its identity. The main idea behind this paradigm is to prevent any adversary from compromising a threshold number of nodes inside a region that allow him/her to generate a fake report, launch a malicious revocation to any node, drop packets or to participate in any type of attack. Employing cell reporters allows the BS(s) to reveal any type of collusion between different compromised nodes in a particular region and facilitate the process of detecting a malicious region containing one or more compromised nodes. In order to prevent them from being compromised, the selected set of cell reporters is changed periodically where the change frequency depends on different aspects such as security level, application and network complexity.

1.4 Motivation and Challenges

As explained previously, a WSN is vulnerable to different types of internal and external attacks that make use of resource limitations of sensor nodes. In addition, IoT connected WSNs can be thwarted by a single point of failure if a single BS is used. Therefore, a promising solution to this problem is the adoption of multiple BSs to control the network, report requesting and report generating. Finally, plenty of recent research has focussed on a WSN that supports mobile nodes such as those used in smart cities, urban monitoring, border surveillance and military applications where sensor nodes are subjected to intended

or non-intended mobility. Therefore, The motivation of this thesis is to propose and analyse a key management scheme which tackles four important problems in the recent key management schemes to the best of our knowledge:

1. Poor confidentiality and authenticity in the available location dependent key management schemes and their vulnerability to severe attacks [20,21]. This is addressed in Chapter 3. **Challenges**: Increase these two securiy requirements without affecting end-to-end security, increasing hierarchy complexity, computation and communication cost.

2. Unsuitability of schemes to be used in multiple BS WSNs and the superficiality of tackling this problem by some recent schemes [21]. This is addressed in Chapter 4. **Challenges**: Propose an approach of controlling a WSN by multiple BS, the affect of this approach on the mehanism of selecting cell reporters and the impact of the number of BSs on both the the system security and the optimum number of cell reporters.

3. Lack of an affective revocation scheme for malicious nodes and cells. This is addressed in both Chapter 3 and Chapter 4

4. Inability to handle node mobility in a single or multiple BS environment. Chapter 5 **Challenges**: Handover processes, potential increase of network overhead, the impact of changing BS coverage's shape and the mobile node speed.

1.5 Thesis Contribution

This thesis presents three novel contributions:

- A novel location dependent key management protocol for single BS (LKMP-SBS) presented in Chapter 3. In this scheme, the WSN terrain is assumed to be virtually divided into square cells. Then, event reports generated by each particular cell are signed by that cell's reporter signature. This system is analysed and shown to outperform other schemes in terms of data security requirements. Moreover, the optimization of this scheme is thoroughly investigated in terms of different factors.

- Design of a novel location dependent key management protocol for multiple BSs (LKMP-MBS). In this scheme, different strategies of handling WSN controlled by multiple BSs is investigated. Accordingly, the optimality of the scheme is analysed in terms of the number of cell reporters. Moreover, the security robustness of this scheme is analysed and shown to be outperforming other relevant schemes in terms of data confidentiality and authenticity. Furthermore, in comparison with LKMP-SBS, the adoption of multiple BSs is shown to be significantly important in improving the overall system security.

- Design of a novel Mobility Enabled Location-dependant Key Managment Protocol for Multiple BS MELKMP-MBS. This scheme presents a key management scheme which is capable of serving a WSN with mobile nodes. Several types of handover are presented in order to maintain the mobile node service availability during its movement between two zones in the network. In addition, several shapes of virtual cells, square, circular and hexagonal, are discussed. Accordingly, the communication overhead of MELKMP-MBS is analysed, simulated and compared with the overhead of other schemes. Moreover, the design optimality in terms of communication overhead is investigated regarding the number of nodes inside each particular cell.

1.6 Thesis Outline

The organisation of this thesis is as follows: Chapter 2 presents the technical background of WSNs, En-route filtering process, WSN connectivity with the Internet and the importance of employing multiple BSs in WSNs. Moreover, this Chapter also reviews related work on Key Management Schemes and En-route Filtering. In Chapters 3,4 and 5 three novel key management schemes are proposed, analysed and evaluated. Particularly, Chapter 3 presents a location-dependent key management scheme for a single BS WSNs. In this Chapter, the cell reporters paradigm is introduced as a novel contribution to improve the security of location-dependent key management schemes. Chapter 4 presents the impact of using the same paradigm to build a location-dependent key management scheme for multiple BS WSNs. Chapter 5 presents a mobility enabled key management scheme from multiple BSs WSN. Moreover, this Chapter introduces a methodology of measuring communication overhead which is dependent to measure communication overhead of all

presented key management schemes. Finally, Chapter 6 concludes the outcome of this thesis and proposes ideas for future work.

1.7 Research Publication

The outcomes of this thesis contribution are shown in following publications:

- Fakhrey, H., Boussakta, S., Tiwari, R., Al-Mathehaji, Y. and Bystrov, A., 2015, June. Location-dependent key management protocol for a WSN with a random selected cell reporter. In *IEEE International Conference on Communications (ICC)*, 2015 (pp. 6300-6305). IEEE.

- Fakhrey, H., Tiwari, R., Johnston, M. and Al-Mathehaji, Y.A., 2016. The optimum design of location-dependent key management protocol for a WSN with a random selected cell reporter. *IEEE Sensors Journal*, 16(19), pp.7217-7226.

- Fakhrey, H., Johnston, M.,Tiwari, R and Angelini, F. The Optimum Design of Location-Dependent Key Management Protocol for Multiple Sink WSN using a Random Selected Cell Reporter. Submitted for *IEEE Sensors Journal*, 2017.

- Fakhrey, H., Johnston, M. and Tiwari, R. Mobility-Enabled Key management Scheme for Multiple Sink WSN. Submitted for *IEEE Transaction on Wireless Communication*, 2017.

- Fakhrey, H., Johnston, M. and Tiwari, R. How to control a WSN by multiple BSs?. Submitted for *IEEE Sensors Letter*, 2017.

- Fakhrey, H., Johnston, M. and Tiwari, R. Node Mobility Model in Wireless Sensor Network. Submitted for *IEEE Sensors Letter*, 2017.

Chapter 2

Background Theory and Literature Review

This chapter presents a brief description of the related theory and gives an overview of the related literature. This thesis focuses on key management protocols, but some other related protocols are also presented. In addition, the challenges facing WSN integration with the Internet is presented with appropriate solutions. Finally, routing attacks threatening WSNs area briefly described.

2.1 WSN Background

The structure of the WSN can consist of two sub-networks, a data collection network and data distribution network as shown in Fig. 2.1. The former network elements are classified into sensor nodes and the BS(s). The sensor nodes are limited resource devices that have a function of measuring physical data and communicating with others nodes in the vicinity via wireless channels [22]. On the other hand, the BS is a powerful device whose function is the aggregation and forwarding of sensors' data. The role of the data distribution network is the dissemination of detected data to be available for all users. Thus, a WSN structure has limitations in most of its components and the main communication media is the wireless channel, but both of these specifications might be considered as weak points.

Regarding to mentioned weaknesses and other reasons, WSN may have a vulnerability to different types of security threats. Firstly, WSN deployment in a hostile terrain causes them to be prone to several kinds of malicious attacks .As an instance, [22] pointed out that a WSN is vulnerable to traditional wireless network attacks such as DoS, impersonation

and common attack but the potential resources limitation leads to the unsuitability of the inherited network security techniques. Moreover, [23] pointed out that even the modified schemes for another types of Ad hoc networks are not suitable for WSN. That increases the demands on crucial schemes which might fulfil the WSN security requirement in spite of their resource limitations.

2.2 En-Route Filtering

En-Route filtering can be defined as the process of checking, investigating then filtering of a generated report in its route from the origin zone to the BS. This process is implemented by the intermediate nodes or entities in order remove false reports within few nodes after the generation zone. Hence, this participate in decreasing the processing overhead, energy consumption and bandwidth exhaust. In en-route filtering, each generated report is enclosed by signatures or Message Authentication Codes (MAC)s which are used to authenticate the report by intermediate nodes and accordingly drop the report contains any fault. According to [1], all en-route filtering schemes are consisting of three phases:

1. Key exchange phase: whole nodes are exchanging specific keys with relevant intermediate nodes on the path between origin zone and the sink.

2. En-route filtering phase: The intermediate nodes are checking, filtering and forwarding the reports toward the sink.

3. Sink validation phase: The BS acts as the last line of defence for the entire WSN by collecting and filtering all reports.

According to [1], almost techniques [24–31] proposed to achieve the key exchange phase can be classified into:

1. Symmetric Cryptography Based Key Exchange (SCBKE).

2. Asymmetric Cryptography Based Key Exchange (ASCBKE).

In most SCBKE techniques, MACs, which are derived by using symmetric keys shared between several nodes, are used to legitimise the generated reports where each report has to include the minimum number of valid MACs. In contrast, signatures are used by the majority of ASCBKE techniques to verify the generated report by the BS and the intermediate nodes. In these techniques, pre-shared credentials do not required while

the used signatures are generated mainly by Shamir's threshold threshold secret sharing scheme [32] and Elliptic Curve Cryptography (ECC) [33].

However, the use of en route filtering might be threatened by adversaries targeting the legitimate report by using a DoS [34], report disruption attacks [35] and selective forwarding attack [36].

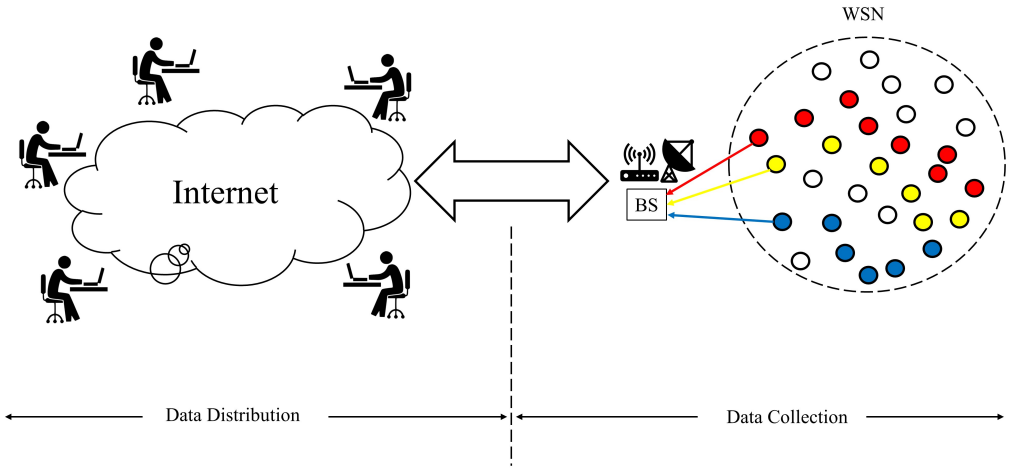


Figure 2.1: WSN structure.

Recent En-routing techniques are classified as shown in Fig. 2.2. Furthermore, Symmetric-Based Techniques are further classified as shown in Fig. 2.3 which is an updated taxonomy for that shown in [1]-Fig. 3

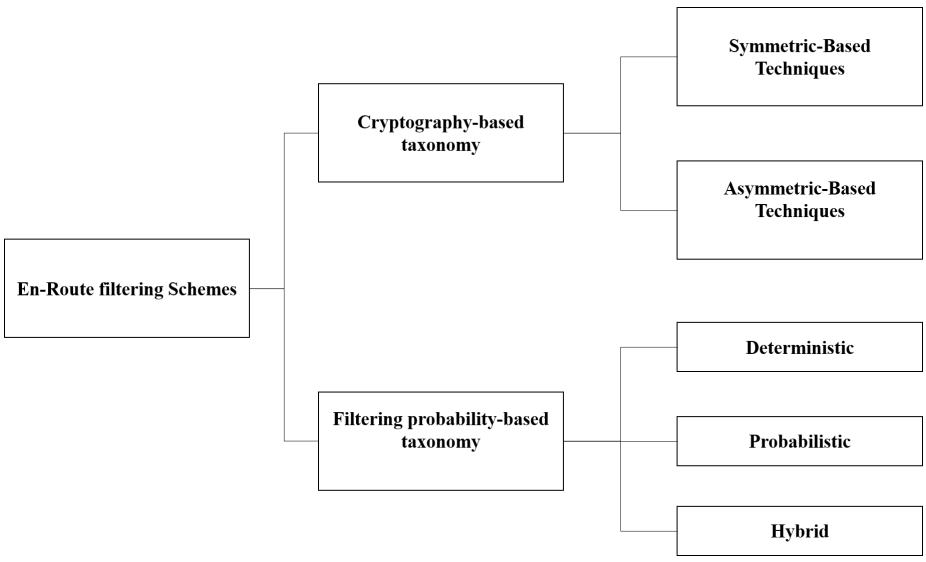


Figure 2.2: A taxonomy of En-route filtering techniques [1].

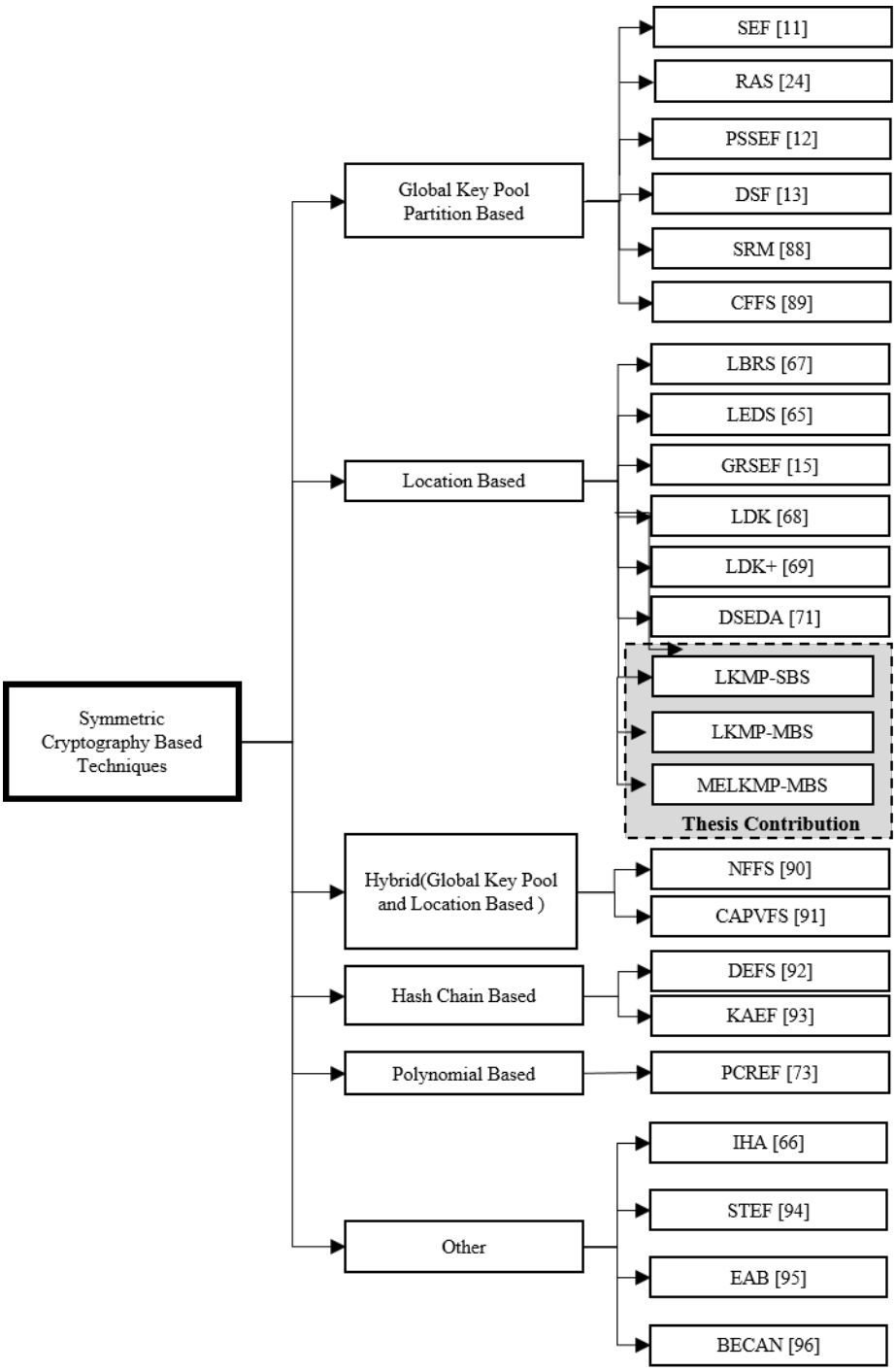


Figure 2.3: Symmetric-based techniques.

2.3 Security Primitives

It is indispensable to secure the data flow process by maintaining specific security services in spite of the mentioned threats. So a significant and effective tool is needed to ensure following security services: authenticity, confidentiality, availability, integrity and non-repudiation [1, 22, 39, 40]. According to [22], it is crucial for sensor nodes to contain basic security primitives in order to protect communicated data. These primitives might be used to secure protocols creation. These primitives could be classified into three groups, hash

primitives, Symmetric Key Cryptography (SKC) and asymmetric key cryptography. The main challenge in the field of WSN security is the implementation of these primitives with their full efficiency in spite of resident resource limitations. Thus, the limited resources inside the WSNs might hinder the implementation of the principal method used to secure its information. The SKC is suitable for providing both of the integrity and authentication services depending on its mode of operation. [22] pointed out that [41–43] analysed deeply the suitability of using SKC technique to secure sensors data. Through their research, they investigate the feasibility of SKC algorithms software implementation. As a result, they conclude that RC4 and Skipjack had less than 10 % overhead on all resources while Advanced Encryption Standard (AES) impose higher penalty (20 %). Based on these results, they assumed mentioned SKC primitives are suitable for practical using. On the other hand, [44] claims that some of the AES-Based hardware implementation are not secure. [22] also assume that most of AES hardware implementation does not offer all their functionalities. Thus, a special care is needed when a specific standard used with hardware implementation. Hash function is used to ensure the integrity of sent packets by adding MAC, which is unique digital fingerprint. But this primitive seems to have some limitation in comparison with the previous primitives. As an instance, [42] proves that SKC algorithms are approximately ten times faster than hash function ones. Consequently, special mode of SKC operations, CBC-MAC, is used to compute MAC instead of hash functions [22]. Asymmetric key cryptography which is also known as Public Key Cryptography (PKC) is one of the security primitives that have some disadvantages and advantages in terms of its implementation in WSN. It had been defined by [45] as a form of cryptography that requires two keys, a public one, which is known by all entities and a private key, which is kept secret by each entity. It is useful for authentication purpose because of its property that allows each operation performed by private key to be reversed by using public key and vice-versa. But one of limitation of using PKC in WSN is the significant computation cost which might hinder its application in such a limited resources network. However, one of the promising PKC primitive is the ECC. Its properties in term of key size, energy consumption, memory cost, simplicity and infrastructure are the best in comparison with other PKC primitives. Due to these specifications, [22] pointed out that ECC was implemented to maintain WSN security in software by [46, 47] and in hardware by [48] . On the other hand, PKC has been considered by [40] as a cryptography solution that require very high energy to implement its very difficult mathematical problems. Thus, PKC is one of the most powerful security

primitives and ECC is the best suitable one for WSN but it still consumes more power in comparison with SKC primitives.

2.4 Key Management System

The described primitives in the previous Section are employed to protect communication channel between any pair of devices inside WSN form any adversary. As a result of using these primitives, a security credentials are needed to be stored inside each node. A key management system (KMS) must be available to handle the tasks of generation and distribution of mentioned keys. KMS had been defined by [45] as a set of operations and mechanisms that might be used to support the construction of keys and maintain the keying relationships between authorized parties according to security policy. Hence, KMS has a major importance in the maintenance of security in WSNs by establishing, distributing and managing network keys.

The KMS in WSNs have been interested in scientific literature due to their significance. Re-keying, which is the networks' ability to update cryptographic keys of entire nodes during their operation, is one of the common aspects in these different schemes. According to [2], these schemes can be categorized depending on re-keying into: static and dynamic. In the static key management, keys are stationary during lifetime of the network, this leads to a significant increment on the mentioned keys. On the other hand, in the dynamic key management schemes, cryptographic keys are refreshed during network life, so that it is regarded as a promising key management in sensor network by [2,49,50]. They report that such kinds of schemes are useful to dramatically improve both of network survivability and flexibility.

2.4.1 KMS Evaluation Metrics:

Due to the importance of the security services listed previously, different problems are challenging the design of efficient KMS. In addition to security problems inherited from wireless networks, WSNs introduce more challenges. According to [51], these challenges are:

1. Broadcasting nature of wireless communication.

2. Resource limitation of sensor nodes.

3. Large density.

4. Dynamic network topology.

5. Hazardous physical attacks.

Thus, with the listed challenges, specific metrics might be useful to evaluate a particular KMS. According to the findings of [2, 52, 53], the evaluation metrics are security metrics, efficiency metrics and flexibility metrics. They can be illustrated as follows:

- Security terminologies

    a. Node revocation: The process of frustrating the actions of malicious nodes inside the network by revoking them. It is measured by the ratio of recoverable nodes within the network.

    b. Forward secrecy: The node prevention from using old keys to generate a new decrypted message.

    c. Backward secrecy: The prevention of update node from decryption of old messages encrypted by using former keys.

    d. Collusion resistance: The process of preventing recently joined and compromised nodes from collaboration to capture the whole sensor network.

    e. Resilience: It is an action taken from key management scheme to prevent the adversary who compromised a specific node from affecting rest nodes in the same network.

- Efficiency metrics: The key management scheme must not load heavily the constrained resources in terms of:

    a. Memory: The amount of memory required to store security credentials, user ID and trusted certificates.

    b. Bandwidth: The number and size of exchanged messages between the nodes to accomplish key generation processes, node replacement and node removal.

    c. Energy: The amount of energy consumed during the key agreement process, data transmission and reception and computational procedures required to generate and distribute new keys.

- Flexibility metrics: In order to design a key management technique that function well with wide range coverage WSNs, following metrics should be available:

  a. Mobility: Ability of distributing new keys to mobile nodes to allow them to interconnect with their adjoining nodes in the new regions.

  b. Scalability: The maintenance of security and efficiency features for large networks as optimum as small networks because of the possibility of adding or removing a plenty of nodes during network lifetime.

  c. Key connectivity: The probability of two nodes to be able to establish their keys after re-keying process. It is essential to provide security continuity.

2.4.2 KMS Literature Review

Much research is focused on analysing available key management schemes designed for WSNs. Mentioned studies have a different prospective to classifying the different studied schemes. An illustration about these studies will be illustrated in the upcoming paragraphs.

Firstly, available key management schemes have been investigated by [51]. In this survey, the mentioned schemes as of 2008 were compared and classified according to particular considerations. Considered architecture of WSNs were "hierarchical" and "distributed". The author classifies key management schemes into three categories: probabilistic, deterministic and hybrid key management. According to the set of metrics, both of security properties and resource consumption were analysed for each scheme. The major conclusion of this study was "no one-size-fits-all solution".

Secondly, Zhang, et al. in [54] define the key management as the vital scheme used to provide security in WSNs. They also present a survey of proposed key management schemes in WSNs as of 2009. Mentioned schemes were classified according to the mechanism of the encryption key into: Symmetric, asymmetric and hybrid key management schemes. They conclude that both the symmetric and asymmetric schemes have disadvantages, while hybrid schemes might combine the advantages of them.

Thirdly, many lightweight key management schemes were presented by [53] as alternatives of traditional techniques, which seem to be unsuitable in modern limited resource networks. These techniques were reviewed in this study and evaluated according to the same KMS evaluation metrics. They focused on a pre-distribution scheme adopted for

homogenous WSNs. As a result, they conclude that flexibility is as important requirement as efficiency in the evaluation of key management schemes.

Finally, it has been reported by [2] that the adoption of dynamic key management has a significant importance because of WSNs deployment in a hostile environment. They pointed out that plenty of schemes were proposed recently while the usage of traditional schemes used in wire and ad-hoc networks is hindered by resource limitations. Through this survey, a special requirement for dynamic key management schemes in sensor networks was investigated and several evaluation metrics were introduced. Mentioned schemes were classified in different categories as shown in Fig. 2.4.

To sum up, several studies were focusing on analysis and evaluation of recent key management schemes. Different points of views were depended by the researcher, network architecture, encryption mechanism, flexibility and dynamism. They conclude that it might be impossible to find one single scheme that has a brilliant performance according to all evaluation metrics. Consequently, they suggest several promising subjects that can be covered in future work. Some of these notations will be highlighted in the next Sections as a proposed project.

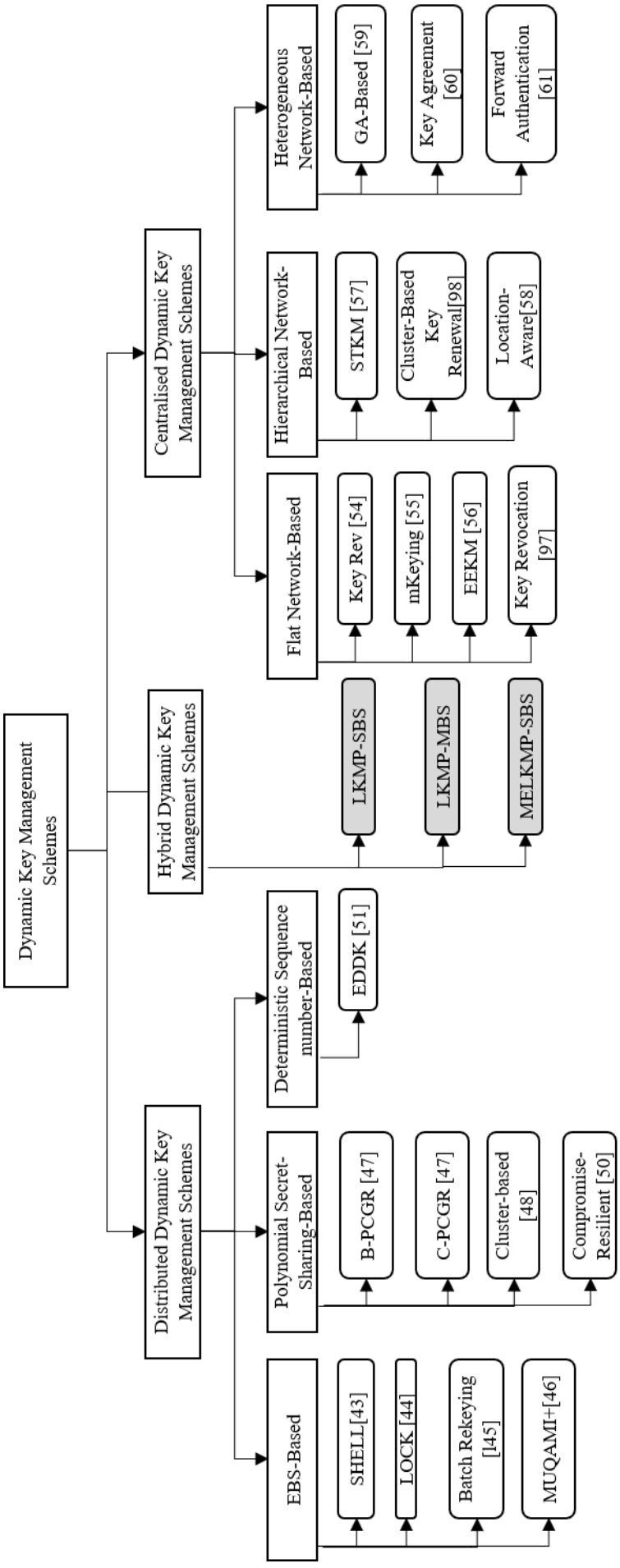


Figure 2.4: Classification of the schemes studied by [2] with references.

In addition to the surveys described previously, some significant key management schemes are selected to be described in detail due to their importance in this thesis. These schemes are chosen from both distributed and centralized groups shown in Fig. 2.4:

2.4.3 Distributed KMS

1. The exclusion basis system (EBS), which is a combinatorial design of the group key management problem, has been presented by [55]. ,The proposed schemes that designed as EBS-based schemes assign k keys for each node out of a pool of size p=k+m where (k>1, m<n and n is the number of nodes in the WSN). The Re-keying process is implemented periodically or when specific node is compromised. In this process, after a generation of replacement keys, all of them are encrypted with the m keys that anonymous to the compromised node(s). Formerly, they are distributed to other nodes which cooperatively have a complete knowledge about the m keys. Based on EBS, several schemes were proposed:

    - Scalable, hierarchical, efficient, location-aware and lightweight (SHELL) which proposed by [56] with advantage of successful re-keying and collusion preventability. However, according to [2], this scheme has some of disadvantages such as complex structure, usage of several kinds of keys and high energy consumption.
    - LOcalized, combinatorial keying (Lock), had been proposed by [57] with a hierarchy consists of three levels: BS, cluster leader and sensor nodes. According to [22], the normal operation of other clusters in WSNs does not affected by node compromising in a specific cluster. This is a unique advantage in comparison with other dynamic key management schemes.
    - The approach presented by [58] in order to enhance the collusion resistivity in SHELL by making use of innovated batch re-keying scheme.
    - MUQAMI+ which was proposed by [59] improves the WSN in the term of scalability and flexibility by increasing the ability of each node in a particular cluster to be a cluster head (CH).
    - The system proposed by [60] which optimises the problem of collusion in comparison with previous schemes.

2. Polynomial secret-sharing-based re-keying schemes (B-PCGR, C-PCGR):

   - A family of pre-distribution and local collaboration-based group re-keying (PCGR) schemes were proposed by [61] in order to solve the node compromising dilemma. In such schemes, WSNs are divided into several groups where a unique key is used by all nodes in the same group. According to this strategy, basic-PCGR (B-PCGR) was designed, then cascaded-PCGR (C-PCGR) was built as B-PCGR based with some differences. According to [2], this scheme has following fragilities:
     - Not suitable to be used in a dense sensor networks.
     - Have a high communication cost.
     - Have a probability to be affected by a DoS attack.
     - Large node compromising leads to node isolation.
     - Forward secrecy is not assured.
   - Zhang et al in [62] enhance the PCGR by letting a CH to implement the generation and distribution of group key for nodes in each cluster. A one way hash function, identifier of each node and 2t-degree bivariate polynomial g (x, y) were used by each CH to make a derivation of the new group key depending on the threshold secret sharing scheme discussed in [32]. It was reported by [2] that this scheme solved the node isolation problem that PCGR suffering from. However, He et al [63] point out following weaknesses:
     - The synchronization might be effected in group re-keying process during addition of new node.
     - It does not explain how to find an accurate value for t that ensures achievement of security and reliability.
     - Sensor node being under control of an adversary might lead to return false information related to new group key to the CH.
   - In [64], authors exploit the characteristics of perturbation polynomial proposed by [61] to construct a strong pairwise re-keying protocol for hierarchical WSNs in order to thwart node compromise attacks. According to [2], this scheme has a high robustness against compromise attacks in comparison with other polynomial based re-keying protocols. However, it seems to be unable to revoke

compromised node or CH. In addition, this protocol does not explain how to establish pairwise keys between new nodes and resident ones.

3. Deterministic sequence-number-based scheme

   - The energey-efficient distributed deterministic key management (EDDK) was proposed by [65] to maintain secure establishment and maintenance to pairwise keys and the cluster key. This scheme was proposed as an enhancement to that in OTMK [66] which is vulnerable to attacks such as resource exhausting and DoS. In this scheme, each node stores the pairwise keys, local cluster key and its own public/private keys. It is constructed from three phases: key establishment, key maintenance and data transfer, this increase its robustness against replay, Sybil and node duplication attacks. However, this scheme might be insufficient in WSNs with high node density; the network lifetime also might be affected by a higher energy consumption associated with the promiscuous listening mode. Furthermore, this scheme is possibly unable to allow a trusted mobile node to join a network because of limitation in the neighbour table.

All previously described schemes are categorized by [2] as a distributed dynamic key management schemes. In following, centralized dynamic key management schemes will be discussed and explained. Its mechanism depends on usage of a single central key controller such as a BS or a trusted third party which is responsible for key management. In comparison with distributed dynamic key management, the main advantage of this scheme is the impossibility for compromised sensor node to sabotage the process of node eviction. On the other hand, the key distribution process is much slower than that in distributed dynamic key management schemes due to multi-hop probability [67]. Centralized schemes might be classified according to their network structure into: flat, hierarchical and heterogeneous.

2.4.4 Centralised KMS

1. Flat network-based scheme

   - KeyRev was proposed by [68] as a well-organized scheme to remove compromised sensor nodes from WSNs. It assumes that each node is capable to communicate directly to the BS. Each node has four types of keys: pairwise key, path key, encryption key and MAC key. The lifetime of WSNs is divided

into sessions while session key is spread to all nodes regularly by BS. The MAC key and the encryption key are renewed with simultaneously with the session key. KeyRev might be immune to revocation attack, however, this scheme has following limitations [2]:

  - Each new node needs to be loaded with pre-distributed key materials.
  - It depends heavily on the accuracy of the scheme used to detect captured nodes.
  - There is an ability to disclose both the MAC and encryption key when the session key is not updated.
  - Ideal conditions were considered in simulating and evaluating this scheme.
  - The BS was considered as a trustworthy entity.

- mKeying scheme, which was proposed by [69], is based on the authors' previous proposal (KeyRev) [68] . In this scheme, the BS does not assume to be trusted so that it is proposed to solve the problem of revoking BS and sensor node. It is one of the literatures that dealt with the assumption of multiple BS, a study with more details in the upcoming Sections related with multiple BS.
- According to [70] an energy-efficient key management protocol (EEKM) was proposed to be suitable for large scale WSNs. In this scheme, BS was assumed to be strongly protected (cannot be compromised) and have an ability to send messages to all nodes. EEKM can be considered as a regional group-oriented re-keying strategy where the nodes are partitioned into several groups. In this scheme, several types of keys are used, almost of them are derived from the initial master key.

2. Hierarchical network-based schemes

- The spanning tree key management (STKM) proposed by [71] is employed to implement re-keying process. Each node (a) has three keys: $K_{a,BS}$, $K_{BS,a}$ and K_r. First two keys are shared with the BS to secure the message communication between them while K_r is shared by all nodes of the network. K_r is refreshed periodically by the BS during racking process. STKM has an acceptable storage cost where each node needs to store only two keys with the BS. In addition, STKM has a low complex communication and an ability to show resistance

against node compromise attack. However, according to [2] this scheme have following cons:

  - There is a possibility of trusted node eviction because of its energy consumption as a result of messages sent by an undetected compromised node.
  - The communication overhead is proportional with the augmentation of the network size.
  - Entire data communication may be affected if global key is revealed.
  - There is neither a way to estimate re-keying period nor a methodology to detect compromised nodes.

- The location-aware dynamic session-key management for grid based WSNs presented in [72] with a one-way hash function, two-way mutual authentication and a symmetric encryption mechanism. The largest residual energy node in the grid is chosen to be the CH. After each data transaction between sensor node and a CH, both the message and sensor keys are updated. This scheme may be more vigorous against various attacks, but have some of the drawbacks such as high energy consumption, unavailability of compromised node revoking and key distribution to new nodes.

3. Heterogeneous network-based schemes.

- The scheme proposed in [73] manipulates the concept of genetic algorithms to construct a suitable key-generating function for re-keying. The proposed network consists of three types of nodes: sink node, headers and sensors. The responsibility of sink node is the generation of applicable functions to generate the keys and distribute them to the headers and sensor nodes. Each key generating function is encoded as a chromosome. Those chromosomes are selected for re-keying because of their satisfaction of the power-consumption constraints and their relatively high fitness values. Because of using the chromosomes, which consume low power, the energy consumption of this scheme is controllable. However, the memory size of the pool used to store keys is very large. Furthermore, it assumes that an adversary cannot compromise any sensor node in a certain time limit.

- The authors in [74] presented an algorithm for key agreement in WSNs by making use of PKC. The architecture of the network constitutes from a gateway and

sensor nodes. The gateway is less resource constrained and tamper-resistant. The gateway is assumed to have less constraint on its resources and have ability to distinguish the nodes compromising. Sensor nodes might be aware about their locations. A specific algorithm used to establish pairwise keys among sensors, instead of loading whole keys of all the nodes in the vicinity. Sensor nodes are classified into groups. The session key for each cluster is generated by a gateway which directs it to CHs. When a node reaches its lifetime or captured/compromised, this session key can be updated. This approach might be efficient from the storage point of view. Furthermore, it achieves both forward and backward secrecy. However, all the session keys might be revealed in the case of collusion between a numbers of captured nodes.

- A scheme that provides a specified forward authentication key management for heterogeneous WSNs was proposed by [75]. The mentioned architecture consists of BS and two levels of sensor nodes, high-end nodes (H-nodes) which has functionality looks like CHs and low-end-nodes (L-nodes). While H-nodes are assumed to be in direct communication with the BS, L-nodes are capable to communicate with each other over H-nodes. This scheme uses the same hash function loaded into BS, L-nodes and H-nodes. The key chain which contains keys used for communication between H-nodes and L-nodes are mainly generated by BS. This scheme achieves accepted memory efficiency and decreases the requirements for computations of L-nodes. Also, it supports H-nodes to be robust against several attacks such as guessing, replay and "man in the middle" attack.

2.4.5 Hybrid KMS

1. The random seed distribution with transitory master key (RSDTMK) proposed in [76] is a key management scheme proposed for a WSN with an ability of node addition. It assumes that no deployment knowledge is available in any node. RSDTMK might be considered as a hybrid scheme which integrates both the transitory master key families with the random key distribution. The main idea of this scheme is based on randomly selection of seed rings from a seed pool then each node receive one of mentioned rings. To create a link between any two nodes, each one looks for shared seeds between them. Consequently, a pairwise key between them is cre-

ated according to a pre-distributed master key, pseudorandom number, permutation function and a selected mutual seeds. The main aim of this scheme is to increase the number of possible keys in comparison with the number of seeds inside a pool. Authors in [76] present the advantage of this scheme in comparison with different approaches chosen from plain global key (PGK) schemes, which use same key for each node, and full pairwise keys (FPWK), where a specific key is used for any pair of nodes. According to this comparison, RSDTMK has advantages of greater quantity of possible keys used and lower effect due to compromising of a specific quantity of seeds. However, this research did not clarify the strategy used to revoke a compromised node. Moreover, the cryptography scheme used is the AES with a key of length 128 bit which has less amount of security in comparison with other schemes. In this thesis, all presented schemes, LKMP-SBS, LKMP-MBS and EMLKMP-MBS are considered as hybrid schemes due to adoption of key generations by bot of nodes and BSs in order to balance the load between two entities.

2. A multi-level dynamic key management mechanism proposed in [49] is hybrid scheme that make use of two different level of security to protect data inside a WSN. One of low-power-consumption SKC algorithms used to protect collected data while one of more powerful security PKC schemes is used to protect key management process. The network architecture assumed to be consist of sensor nodes, CHs, mobile certification authorities MCA and sink node or a BS. Through this study, advantages of ECC over RSA were illustrated. In addition, a comparison between two SKC algorithms (RC4 and AES) highlighted. Consequently, ECC used to protect data communicated between sensors and MCA, which is responsible about key delivery for any pair of nodes, while the collected data by sensors is protected by using RC4. In contrast to other scheme, proposed one in this system is proven to more efficient in terms of communication overhead, memory usage and resilience against node compromising. However, the usage of UAV as an MCA seems to be infeasible in terms of cost.

2.4.6 KMS for Multiple BSs

1. According to Wang et al., the key management protocol (mKeying) proposed in [69] is the first key management scheme to deal with a multiple BS WSN protocol. Both of BSs and sensor nodes are considered to be vulnerable to be compromised in

the proposed scheme. mKeying consists of two sub-schemes: mKeyDist which is a key distribution sub-scheme and mRevKey which is the sub-scheme proposed to revocate security credentials from compromised node or BS. However, [21] pointed out that the storage of keys and polynomials in mKeying requires a high space of storage inside each node due to adoption Blundo's theory [3]. Therefore, (mKeying) suffers from unsuitability to be used in large-scale WSN. In addition, end-to-end security, which is a crucial requirement, is not guaranteed by mKeying.

2. The multi BS key management protocol (MKMP) proposed by [21] is a key management protocol designed for a WSN with multiple BSs. It is classified as a location-dependent key management as well, as shown in the next Section. In this scheme, the authentication process is accomplished by neighbouring nodes and BSs. It is crucial to build a routing scheme and to plan the progress followed in case of node compromising. This scheme has two advantages, firstly, high security resilience against node capture attack. Secondly, end to end data security achievement. The third advantage is the feasibility of compromised node removal without a central authority. This scheme was proved to have a significant performance in terms mentioned advantages by comparison with location-dependent end-to-end data security (LEDS) [20] and mKeying [69]schemes. However, this scheme has the same disadvantages as LEDS in terms of node-compromising consequences. In both approaches, compromising a threshold amount of nodes (e) leads to an increase of the entire cell capturing probability. Consequently, a fake report can easily be generated by the adversary inside that cell, which would then be accepted by the BS without being dropped by intermediate nodes. Also, both schemes are challenged by a high communication overhead caused by bidirectional multi-hop communication between each particular cell and the BS, in addition to the computational cost caused by the frequent derivation of authentication keys and route set-up.

It is obvious that not much research is targeting key management protocols for multiple BS WSN. therefore, our project introduces both LKMP-MBS in Chapter 4 and MELKMP-MBS in Chapter 3

2.4.7 Location Dependent KMS

In location-dependent security schemes, a group of n sensors in vicinity are considered to be capable to detect the event and generate a report specifying the relative time and

zone. Such a vital report must be validated by a group of sensors ($v : 1 \leq v \leq n$) in the event region by using a security credentials based on the their location to prevent any adversary from generating a fake report which exhausts the network resources and affect the service availability. So that, any invalidated report is dropped by either a group of intermediate nodes or by the sink itself. Depends on this scheme, plenty of schemes have been proposed in last decade [20, 21, 24, 77–80]:

1. The location-based resilient secrecy (LBRS) which is presented in [78] adopts two techniques: location-binding key generation and location-guided key selection. As a result, the usage of endorsement keys is limited to the region where the event occurs, which leads to thwarting of attacks that globally use the credentials of compromised nodes. However, according to [20, 21], LBRS does not satisfy the data authenticity requirement since the compromising of n nodes inside a particular area might enable the adversary to create a fake event in that area. Additionally, data availability is not guaranteed where it is vulnerable to selective forwarding and report disruption attacks.

2. The LEDS [20] is proposed as an improvement to the schemes proposed by [24,77,78]. It consider that a served terrain is divided virtually into several adequate square cells. Depending on their position regarding the network sink, each particular node derive three credentials, node key, cell key and authentication key. These credentials are used to endorse every generated report to facilitate the process of filtering out any bogus report. LEDS protocol is capable to guarantee the end-to-end security, service availability and limited impact of node-capturing security attacks. However, according to [21], LEDS consider a non-feasible localisation scheme to detect the location of each node. Moreover, network scalability is dramatically affected due to absence of a revocation strategy required to overcome the problems occurred due to compromised nodes the limitation of network size due to lacking for a strategy of node adding/removing. Moreover, this scheme is designed to be employed in WSN with single sink only.

3. In order to overcome the above described flaws, multi-BS key management protocol (MKMP) [21] had been proposed as a location-dependent key mangemnt protocol form a multiple BS WSNs (illustrated in the previous Section).

4. The location dependent keying (LDK) approach proposed by Anjum in [79] assumes

WSNs consist of three elements: sensor nodes (SN), anchor nodes (AN) and BS. All ANs are assumed to have a capability of transmitting at different levels of power. The life time of all nodes is considered to be divided into three phases: pre-deployment phase, initialization phase and communication phase. In the first phase, which is before node deployment, all SNs and ANs are preloaded by a single key K. Just after depolyment, the initialization phase starts by transmitting of beacon by ANs at each particular level of power. Each beacon include various sets of random number (nonce) encrypted by the common key K. Based on the nonces, received then decrypted, from the set of nearby ANs, each SN derive an updated key. For instance, a node S which is receiving R_i beacons (n_1^i, n_2^i, $...n_{R_i}^i$) from the nearby ANs transmitting at the i^{th} level of power. Consequently, S derives R_i updated keys ($K_1^i, K_2^i, \cdots K_{R_i}^i$) as: $K_j^i = H_K(n_i^j)$ where H is a hash function used by every node in the network. As a result, keys derived by any particular node will be location dependent and can be shared only with those nodes in the vicinity. Thereafter, the derived keys will be used to secure data communication in WSN dring the communication phase. However, LDK did not consider insider attackers where it focuses on the outsider attack only. Moreover, LDK suffers from a high rate of communication interference leads to a drop of 40% in packet reception ration of MicaZ motes [80,81]. Furthermore, LDK is impractical because it requires a critical specifications such as a specific number of ANs for each group of SNs in a particular region. Otherwise, the protocol will failed to produce security credentials for some nodes that do not receive any beacons and consequently have no oportuinity to participate in WSN objectives due to lacking for updated keys.

5. In 2017, Choi et al. [80] proposes LDK+ as a key management scheme overcoming the limitations of LDK [79]. In LDK+, authors introduce CHs as a forth element in WSN beside SNs, ANs and BSs where CH is responsible about data aggregation from SNs then forward them to BS. LDK+ is assumed to have two phases: key generation and key update where the latter phase is proposed to threat the insider attackers. In this scheme, a new method of key generation is suggested by combining grid information in order to solve the dilemma of number of nonces insufficiency due to communication interference. LDK+ present, by simulation, that it outperforms LDK in terms of connectivity and compromise ratio. Moreover, LDK+ shows that network cost can be decreased by acheiving hexagonal ANs deployment in the WSN

rather thean square deployement presented in [79]. However, LDK+ failed to solve the impracticality problem shown in [79] where a perssonel has to be sent to the field in order to fix the ANs in there positions which are been morde complicated in LDK+ in comparison with that in LDK. Moreover, the system complexity is increased in LDK+ by increasing the number of WSN elements to be 4 rather than 3 in LDK. Finally, both LDK and LDK+ did not investigate security requirements of confidentiality, authenticity and availability.

6. In 2017, Ferng and Nguyen proposed a new data authentication protocol, Digital Signature assisted end-to-end data authentication (DSEDA) [82], as an improvement to their MKMP presented in [21]. In this protocol, the shape of grid cells is considered as hexagonal and each cell assumed to be controlled by at least one CH. This new entity is responsible about checking the legitimacy of the secret shares generated by each node. Consequently, it requests non-participating nodes to send an alternative shares. DSEDA employs bloom filter [83] in order to achieve communication efficiency. In contrast to similar schemes [20, 21, 84], DSEDA introduce using of digital signature [85] rather than the MAC technique in order to eliminates report fraud. Accordingly, authors prove that DESDA outperforms LEDS [20], Polynomial-based compromise-resilient en-route filtering scheme (PCREF) [84] and t-PCREF [84] in terms of data authenticity, data availability, storage overhead, computation overhead and communication overhead. On the other hand, PCREF and t-PCREF are shown to be outperforming DSEDA in terms of data availability in case of report disruption attack. However, DSEDA has several limitations such as scalability in terms of key pool size which is proportionally related to the number of sensor nodes inside cluster N_c. Hence, a complete key update is required in case of increasing N_c. Moreover, DSEDA does not explain a strategy of electing CH in the network and does not discuss the revocation procedure in case of CH failure or compromisation. Furthermore, there is an ambiguity in terms of non-participating nodes functionality where nothing explained regarding how they detect the event while they did not participate in the event. In addition, there is a great threat of insider attackers whore are pretending such as non-participating nodes. Finally, DSEDA failed to overcome the major drawback presented in LEDS, MKMP, PCREF and t-PCREF which is the possibility of generating a forge report from a particular zone by only compromising the required threshold number of nodes and the impossibility of de-

tecting that. Such a critical threat is the main concern and this what had been tackled in our project as will be explained in next Chapters.

2.5 WSN integration with The Internet

2.5.1 Introduction

The main function of a WSN is physical information collection from the environment where it is positioned; these data are required to be shared for external users. The traditional WSNs share their obtained data with users via a BS which is deployed in the same region. This might be considered as a shortcoming in the accessibility and usability of WSN services. To overcome this limitation, mentioned services should be accessible from external networks [86]. This might facilitate the analyses of data collected by several applications located in miscellaneous geographical locations. In addition, an operator could control the network remotely when it became integrated with the Internet. According to [87], such an integration might lead WSN to be one of the most important technologies of the IoT. However, this integration will lead to plenty of security considerations. Thus, the paradigm of WSN integration with IoT is an emerged technology that facilitates data sharing to the users but requires some security concerns.

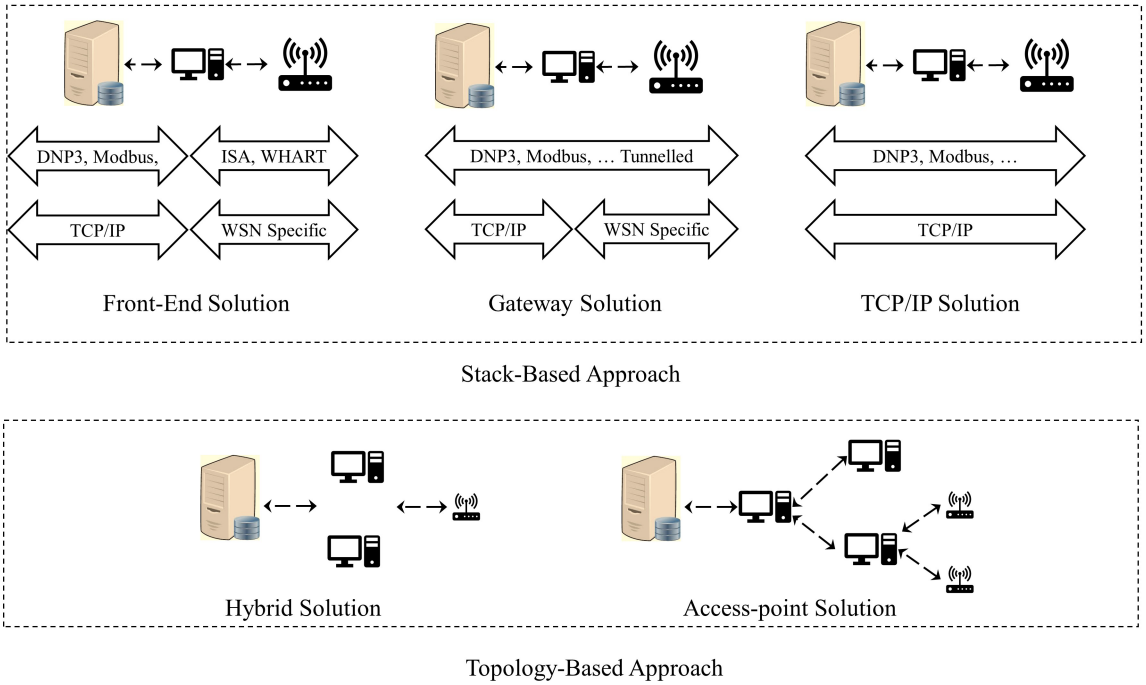


Figure 2.5: Categorisation of integration approaches [3].

2.5.2 Integration Schemes

The methods followed to implement the mentioned integration vary according to the roles of WSN main two components, sensor nodes and the BS. According to [3, 4, 88–91], integration approaches might be categorised into two different groups: stack- based and topology based as shown in Fig .2.5. In the stack-based category, the level of integration is based on the level of similarity between their network stack. According to [88], there are three integration approaches in the stack-based category: front-end, gateway and transmission control protocol Internet protocol (TCP/IP) solutions. Firstly, in the Front-End solution, a WSN is completely isolated from the Internet. A centralised device, such as a BS, is the responsible of managing all interactions between these different networks. As an instance, [11] pointed out that the BS can be as storage for all the data provided by sensors then share these data with external users. In such a case, the BS traverses any queries from the Internet hosts. In the second approach, the Gateway solution, based on presence of a centralised device (e.g. BS) to performs the same function of application layer gateway, which is translation of lower layer protocols from each side. This scheme has been reported by [92] as an efficient way to enable both the Internet and WSN to address each other to exchange the data without a truthfully direct communication. Consequently, the WSN is still isolated from the Internet. Finally, the TCP/IP based on using compatible set of protocols such as 6LoWPAN to completely connect entire sensors to the Internet. As a result, a direct connection might be created between any Internet host and any sensor [3]. Thus, depending on the match between WSN and Internet network stack, integration between them can be provided mentioned three schemes. The topology-based category consists of two approaches, Hybrid solution and access point solution. First one assumes that a group of nodes with an ability of direct

Internet access are deployed inside the WSN and used by all other network to communicate with the Internet [4] as shown in Fig. 2.6.a . According to [88], mentioned nodes might traversed by all sensor nodes in order to connect with the central system and vice versa, consequently, they claims that these nodes might be easily mapped to a BSs. In addition researchers in [89] claims that the redundancy and network intelligence are the significant features if this approach. However, the process of mapping particular sensor to perform the function of a BS is not feasible because of its limited resources and the vital roles of BS which include security credential control, node addition/ removal beside

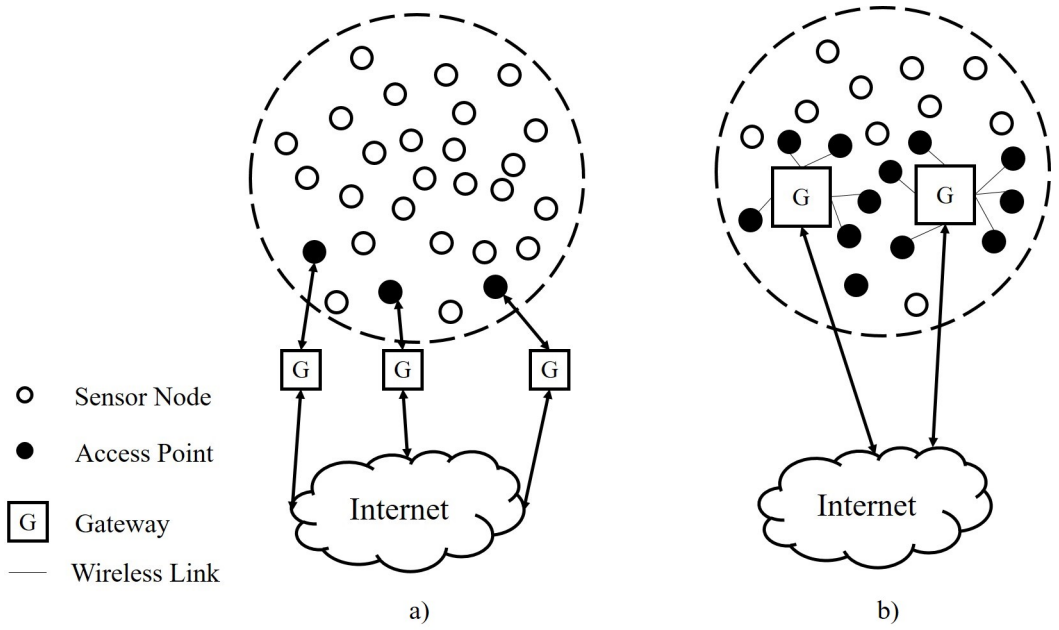


Figure 2.6: a) Hybrid approach; b) Gateway approach [4].

its function of Internet connection. The second approach, access point solution, assumes that WSN structure is inspired by wireless local area network (WLAN) star topology as shown in Fig. 2.6.b. Hence, backbone nodes which are Internet-enabled are single hop distance from other nodes which can connect with the Internet via single hop. This approach offers a direct connection with low latency [4] but its implementation is hindered by the fact of sensor limited resources. Consequently, the overall cost will be significantly increased if each Internet backbone nodes enforced by special resources. Thus, both of the described approaches are hindered with limited resources of sensor nodes; moreover, these approaches are applicable in static network configuration because of long time-required to reprogram used gateways each time a new node added.

2.6 Challenges and solutions

There are different challenges that face the integration approaches in terms of several parameters; one of these is the security issue. Potential difficulties will be explained according to our analysis and findings of some researchers. Firstly, in the Front-End solution, the BS functions as a representative of all the sensors and behaves as an internet host to provide Internet functionality. In the second solution, a BS will act such as a gateway with a responsibility of storing accountability data, it also stores a historic data that produced by nodes. Moreover, it might act as a cache server which is similar to its role in the first approach. Consequently, the implementation of these two approaches might

be hindered by the fact of BS being as a single point of failure that effect entire network when it is compromised by an adversary. Regarding to the third approach, limited storage capacity might significantly hinders the accountability of the network [3]. In addition, more security concerns are needed to be highlighted. [11] presents one of the solutions to the dilemma of resources overhead occurred due to implementation of traditional security schemes. Thus, plenty of security issue are raised when a WSN integrated with the Internet regardless of solution used. It is clear from last two paragraphs that integration process main challenges are sensor limited resources and BS being as single point of failure. The shortage in sensor resources is one natural properties of WSN [40] that is difficult to be overcome recently. On the other hand, the dependence on a BS to handle a vital role in WSN integration to the Internet is a critical attitude because of the direct impact of its failure on the availability of services for both sensor node and the users. As a result, usage of multiple BSs in the WSN might advantage the integration process. However, such a multiple BS system could be challenged by data consistency, synchronisation and message overhead. Thus, an integration approach based on multiple BSs should be designed with a support of core protocols consisting of novel key management scheme, secure routing and localisation topology, secure data aggregation and an efficient time synchronisations. Some of these challenges are addressed in our proposed scheme presented in Chapter 4

2.7 Routing attacks

- Report fabrication attack: The attacker uses the compromised nodes to inject fabricated reports in the network. Such reports might increase the congestion in WSN and lead to wrong decision or to a false alarm generation [27].

- Report disruption attack: The adversary submits a malicious report which contain wrong MACs or signature leading to report generation disruption or dropping by intermediate nodes [27].

- Spoofing attacks: In this attack, the adversary spoof acknowledgements generated in almost routing techniques to indicate the node about its report delivery. This action of spoofing is leading to disrupt nodes functionality and deceive nodes to change their routes to sink [93].

- Sensors relocation attacks: In this attack, the adversary has a physical ability to relocate nodes from their original position. As a result, a wrong report is generated

due to use different location especially in the location-dependent key management schemes.

- Black hole and selective forwarding attacks: The black hole attack occurs when an adversary advertises lowcost routes to the network. Once nodes route via it, the adversary can selectively forward/drop packets [94, 95].

- Sybil attack: In this attack, multiple malicious nodes are created by the adversary. Therefore, the attacker has an ability to be in different places at the same time by presenting different IDs in the WSN. This might significantly reduce the scheme efficiency in terms of fault tolerance and cause a negative impact on geographic routing protocols [96, 97].

- Wormhole and sinkhole attack: Such an attacker can tunnel packets through a secret and low-latency broadband channel between two distant places and replay them. On the other hand, the sinkhole attack can be created by convenience a node, which is multi-hop away from the sink, that the sink is just a few nodes away from a wormhole. Hence, all traffic from surrounding nodes are forwarded to the wormhole [98].

- Node replication attack: This type of attacker intentionally puts replies of a compromised node in many places to cause inconsistency. Like the sybil attack, the node replication attack can enable attackers to subvert data aggregation, misbehavior detection, and voting protocols by injecting.

- Hello flood attack: The attacker sends HELLO messages to the network in order to convince other nodes that the attacker is a neighbour [99]. The adversary achieve this attack by making use of his sufficient transmission power to convince far away nodes that it is a neighbour. Therefore, it can exchange a secure data with them.

- Eavesdropping attack: In this attack, the adversary has an ability to listen to the disseminated traffic. Such an attack can be thwarted by adopting a robust security protocol. However, this threat might lead to any of above mentioned attacks.

Chapter 3

Location-Dependent Key Management Protocol for a Single BS WSN

3.1 Introduction

In this Chapter, the Location Dependent Key Management Protocol for a Single BS WSNs (LKMP-SBS) is described. This protocol depends on the security credentials derived mainly from the geographical location of each sensor node within the network. The novelty of this work is the election of a particular set of nodes inside each cell, hereafter known as "cell reporters", and then nominating them as authentication entities to authenticate any report generated by that cell. The participation of cell reporters in any event report generated by that cell is considered as the unique endorsement of it, otherwise the report will be dropped by the BS. In order to assess LKMP-SBS, three main aspects will be discussed:

1. The security robustness of the LKMP-SBS in terms of data confidentiality and authenticity.
2. The optimal number of cell reporter, hereafter denoted as z.
3. Efficiency of the LKMP-SBS as a lightweight scheme in terms of computation cost and communication cost.

An extensive mathematical analysis is presented to investigate the first two points. Accordingly, LKMP-SBS has been proven to outperform other existing location dependent

schemes in terms of data confidentiality and data authenticity. In addition, both the mathematical analysis and the simulation environment results investigate the 3^{rd} points as shown in Chapter 5.

3.2 System Consideration

The LKMP-SBS protocol is considered to be employed over a wide area of a smart city of a predetermined size and shape, monitored using a large-scale WSN comprising N limited resource nodes and a sink with unlimited resources, hereafter known as a BS (BS). This unit is responsible for data collection, control of report verification, en-route filtering management and origination of all data requests. The BS is considered to have the ability to cover all sensor nodes in the monitored region as shown in Fig. 3.1. The served region is represented as a virtual grid of N' cells. All cells are assumed to have a similar number of sensor nodes that are in communication coverage of all other sensor nodes and are able to estimate their positions using secure localization schemes, such as [111–113]. It is also assumed that all elements in the network (nodes and BS) have a unique public identity and a private identity.

3.3 Threat Model

The system is assumed to be secure during the bootstrapping interval, a short period after the deployment of all elements, then the attacker is assumed to be able to capture randomly selected nodes and compromise their security credentials. On the other hand, the same adversary has no opportunity to compromise the BS due to its rigid security which prevent its facilities from being compromised or cloned. When a node is compromised, the attacker is assumed to be able to inject, drop, eavesdrop, alter, or retransmit packets. However, the attacker has no access to the uncaptured nodes.

3.4 Notation and Terms

In this Chapter, the following definitions are of significant importance:

- K: An initial master key used as a seed to derive other keys
- (x_0, y_0): The BS location

- Δ: The side length of each cell
- t: The number of authentication cells $d_i : i = 1, 2...t$
- p: A prime number
- (x_c, y_c)): The center location of cell (c)
- (x_a, y_a)): The location of a node (a)
- $\|$: The operation of concatenation
- H: A Hash function
- ID_a: Identity of each particular node (a) which is known by the BS
- t_s: A recent time slot
- K_{Lcin}: An initial cell key
- K_a^{BS} A unique key shared between each node (a) and the BS
- $K_c^{d_i}$: An authentication key derived by the BS and shared between cell mates in cell c and cell mates in the authentication cell d_i
- K_{Lc}: The cell key
- $Enc_K\{M\}$: Encryption of a message M using key K
- $MAC_K\{M\}$: The message authentication code of a message M calculated over the key K
- ε: A threshold number of endorsement nodes required to generate a legitimate report
- T: A predefined cell reporter validity
- N: Total nodes in the network
- N': Number of cells in the network
- n: Number of nodes of each cell
- z: Number of cell reporters
- λ: Packet size

- $P_{C\{\varepsilon|z\}}$: The probability of compromising a cell in terms of data confidentiality
- $P_{auth\{\varepsilon|z\}}$: The probability of compromising a cell in terms of data authenticity
- $\|$: The operation of concatenation
- H: A Hash function
- $Enc_K\{M\}$: Encryption of a message M using key K
- $MAC_K\{M\}$: The message authentication code of a message M calculated over the key K
- **The report forward route** between a particular cell (c) and the BS contains all cells traversed by a virtual line between them as shown in Fig. 3.1, denoted as dark-grey cells. The highlighted sequence is listed based on the position according to the BS.
- **Report authentication cell**: A particular cell d_i belongs to the forward report path of cell (c). Its location relative to (c) or the last authentication cell is $t+1$ cells as shown by the light-grey cells depicted in Fig. 3.1. However, there is no authentication cell in the case of a short report authentication route less than $t+1$ cells.

3.5 Setup Phase

Prior to their deployment, each node (a) is preloaded with the following parameters $\{K, (x_0, y_0), ID_a, \Delta, t, p\}$
Where:
K: An initial master key used as a seed to derive other keys.
(x_0, y_0): The BS location.
ID_a: Identity of each particular node (a) which is known by the BS.
Δ: The side length of each cell.
t: The number of authentication cells $d_i : i = 1, 2...t$.
p: A prime number.

Depending on their clocks and the application requirements, the setup phase time is divided into multiple identical time slots t_s to ensure the freshness of security credential

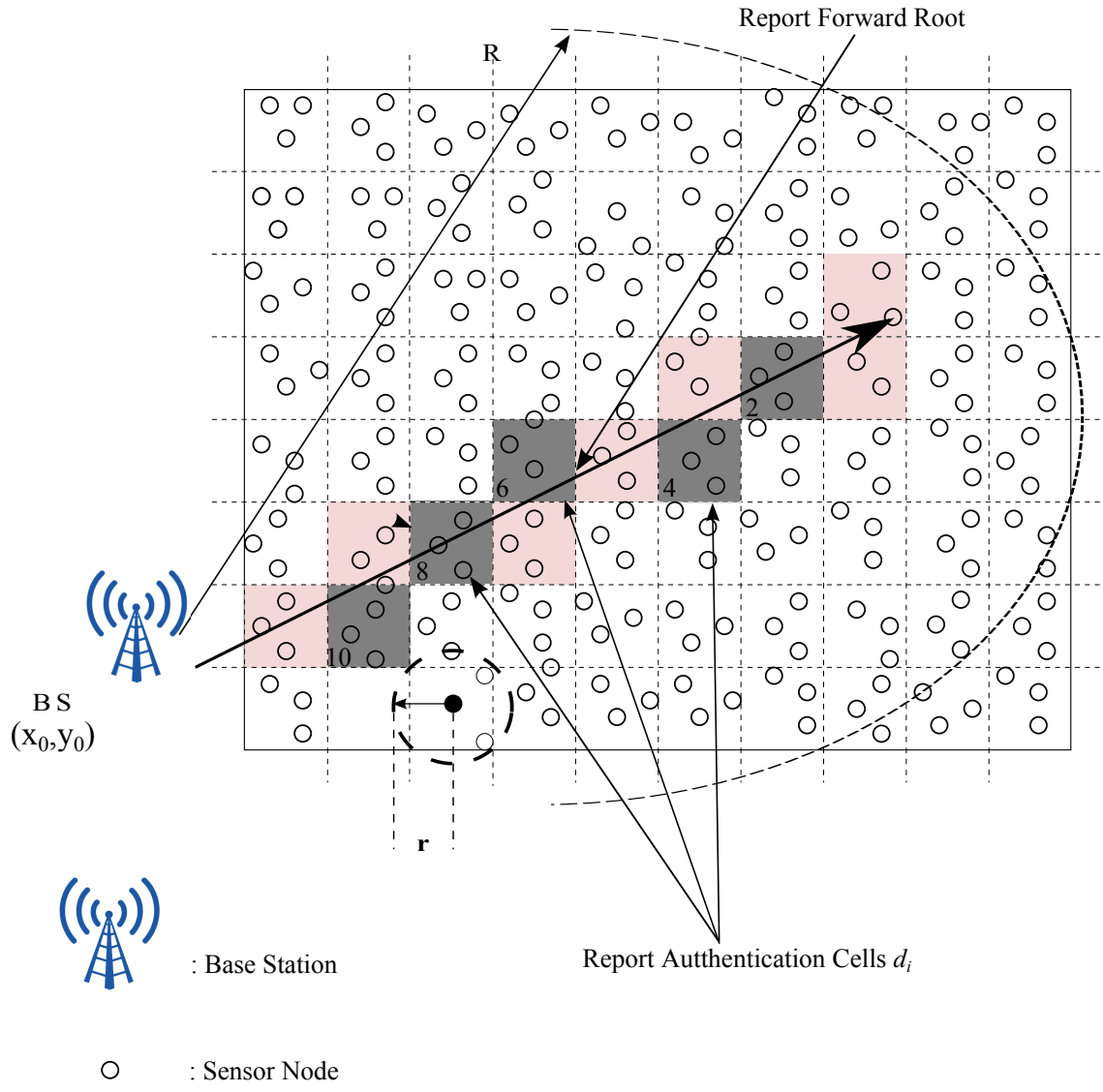


Figure 3.1: Illustration of system construction shows report forward route and authentication cells for a WSN with $n \simeq 3$ and $t = 2$.

derivations. Using its location and the BS location as a reference point, the node excludes its cell centre location using Theorem 3.1:

Theorem 3.1 *Assume a square grid comprising squared cells where the side length of each cell is* Δ*. Let cell* C *be one of these cells where point* $P(x_p, y_p)$ *lies inside this cell margin and another point* $B(x_b, y_b)$ *lies on the border of grid, then the Cartesian coordinates of the cell centre* (x_c, y_c) *are:*

$$x_c = \frac{\left\lceil x_p - x_b \right\rceil}{\Delta} + 0.5 \tag{3.1}$$

$$y_c = \frac{\left\lceil y_p - y_b \right\rceil}{\Delta} + 0.5 \tag{3.2}$$

Based on Theorem 3.1, considering that the BS is located on the border of the terrain, the coordinates of a particular cell centre is extracted. Then the following related credentials are derived as shown in Algorithm-3.1:

- An instantaneous cell key K_{ts}:
- An initial cell key (K_{Lcin})

Algorithm 3.1 *Derivation of security credentials inside each node* (a) *during the setup phase.*

Require: $K, (x_0, y_0), t_s, \Delta, (x_a, y_a)$
$K_{ts} \leftarrow K \| ts$
$x_c \leftarrow \frac{\left\lceil x_a - x_0 \right\rceil}{\Delta} + 0.5, y_c \leftarrow \frac{\left\lceil y_a - y_0 \right\rceil}{\Delta} + 0.5$
$K_{Lcin} \leftarrow H(K_{ts} \| (x_c, y_c)$
Ensure: $K_{ts}, (x_c, y_c), K_{Lcin}$

Every node in a particular cell creates a list of its neighboring nodes, hereafter known as cell-mates, and derives a unique key that is shared between each node (a) and the BS (K_a^{BS}) using this formulation as illustrated in Algorithm 3.2:

$$K_a^{BS} = H(K \| ID_a \| (x_0, y_0)) \tag{3.3}$$

The message $\{LIST\}_a$, which consists of the cell centre, the list of all cell mates and the initial cell key K_{Lcin}, is sent by each node (a) to the BS using a cell-by-cell method.

Algorithm 3.2 *Creation and broadcasting of cell-mate list of each node* (a).

Require: $ID_a, t_s, (x_a, y_a), (x_c, y_c), (x_0, y_0), K_{Lcin}$
  $a \rightarrow$ All cell-mates inside: $Enc_{K_{Lcin}}\{ID_a, t_s, (x_c, y_c)\}$
  $\{CellMateList\}_a \equiv \phi$
  for all cell-mates **do**
    $ACK \rightarrow a$
    if ACK is valid **then**
      Update $\{CellMateList\}_a$
    end if
  end for
  $K_a^{BS} \leftarrow H(K \| ID_a \| (x_0, y_0))$
  $\{LIST\}_a \leftarrow \{((x_c, y_c), \{CellMateList\}_a, K_{Lcin}\}$
  $a \rightarrow$ BS: $Enc_{K_a^{BS}}\{LIST\}_a$
Ensure: $K_a^{BS}, \{LIST\}_a, \{CellMateList\}_a$

When the BS recieves the data packet of this message, it extracts the node identification ID_a from its header then rederives K_a^{BS} using 3.3. Then the BS decrypts $\{LIST\}_a$ and extracts its contents:

1. Cell c coordinates (x_c, y_c) are used to determine the unique identity of that cell ID_c as:

$$ID_c = x_c \| y_c \tag{3.4}$$

2. The BS determines, Num_c^a, the estimated number of nodes inside the cell c according to the node a, as:

$$Num_c^a = \mid \{LIST\}_a \mid +1 \tag{3.5}$$

The last parameter is compared later with the other Num_c^a which are received from:

- The same node via different routes.
- The other nodes inside the same cell.

According to this comparison, the node reporting bogus information about its cell mates is considered as a suspicious node which might be malicious or have a technical problem. As a result, for any cell hosts (τ), a threshold number of suspicious nodes is considered as a suspicious cell. In our scheme, based on experimental results, this value is considered as:

$$\tau = \lfloor 0.5 Num_c^a \rfloor + 1 \tag{3.6}$$

At this point, if any node/cell is detected as malicious, a revocation scheme is implemented by calling Algorithm (4)/(5) to revoke nodes and cells listed in $SusbNodes$, $SusbCells$ respectively as discussed in Section (3.7) to overcome the possible consequences caused by the presence of such malicious entities in the WSN. On the other hand, the BS authenticates the illegitimate nodes inside the particular cell c by implementing the following steps which are illustrated in Algorithm. 3.3:

1. Derive $\{LIST\}_c$ as:

$$\{LIST\}_c = \{LIST\}_a \cup ID_a \tag{3.7}$$

2. Derive the cell key K_{Lc} as:

$$K_{Lc} = \begin{cases} K_{Lcin} & \tau = 0 \quad (3.8) \\ H(K_{ts} \| (x_c, y_c \| \{LIST\}_c) & \tau > 0 \quad (3.9) \end{cases}$$

3. Derive the authentication key $K_c^{d_i}$ which is shared between all nodes inside the cell c and the nodes located inside the authentication cell d_i which is dedicated by the BS to authenticate all messages generated by cell c as explained in Chapter 2.This key is derived as:

$$K_c^{d_i} = H(K_{Lc} \| K_{Ld_i} \| (x_{d_i}, y_{d_i}) \| (x_c, y_c)) \tag{3.10}$$

   where (x_{d_i}, y_{d_i}) represents the Cartesian coordinates of the cell d_i centre.

4. Disclose $\{LIST\}_c$, K_{Lc} and $K_c^{d_i}$ in one message which is encrypted using K_a^{BS} and broadcast to each node in that cell.

Algorithm 3.3 *The BS verification of* $\{LIST\}_a$ *packages sent by each node.*

Require: $\{LIST\}_a : a = 1, 2..., N$

$COUNT = 0; SuspNodes \equiv \phi$

for $a = 1, 2..., N$ **do**

BS extracts ID_a from the header of $\{LIST\}_a$

$K_a^{BS} \leftarrow H(K \| ID_a \| (x_0, y_0))$

$Dec_{K_a^{BS}}\{LIST\}_a = \{(x_c, y_c), \{CellMateList\}_a, K_{Lcin}\}$

$ID_c = x_c \| y_c$

$Num_c^a =\mid \{CellMateList\}_a \mid$

if $\{LIST\}_a \equiv \{LIST\}_{a-1}$ **then**

$COUNT++$

else

$SuspNodes \leftarrow a$

end if

end for

if $COUNT \geq \lfloor 0.5 Num_c^a \rfloor + 1$ **then**

Call $Algorithm(4)$

else

if $COUNT < \lfloor 0.5 Num_c^a \rfloor + 1$ **then**

$SuspCells \leftarrow ID_c$

Call $Algorithm(5)$

end if

Else

$K_{Lc} \equiv K_{Lc\_init}$

$\{LIST\}_c = \{LIST\}_a \cup ID_a$

$BS \rightarrow a : Enc_{K_a^{BS}}\{K_{Lc}, \{LIST\}_c\}$

if $BS \leftarrow a : ACK$ **then**

$K_c^{d_i} = H(K_{Lc} \| K_{Ld_i} \| (x_{d_i}, y_{d_i}) \| (x_c, y_c))$

$BS \rightarrow a \in c : \{d_i\} \cup \{K_c^{d_i}\}$

end if

end if

Ensure: $K_a^{BS}, SuspNodes, SuspCells, K_{Lc}, \{LIST\}_c$

$, \{d_i\}, \{K_c^{d_i}\}$

All correspondence from the BS to any node (a) is implemented directly via a single hop scheme due to the wide coverage property of the BS. An en-route-filtering scheme presented in [114] is implemented, using the authentication keys $K_c^{d_i}$, by the authentication cells d_i belonging to each particular cell (c) to reduce the amount of fake reports arriving at the BS. Hence, the computation cost is decreased dramatically in comparison with the cost of LEDS and MKMP, as shown in Chapter (5).

3.6 Report Generation

One of the main functions of the WSN is to detect particular events in the served terrain such as movement, temperature, humidity and chemical emissions. In the location dependent WSN topology 3.1, all nodes located within the margin of a particular cell will be responsible for generating a report which illustrates the detected event in that cell. This is called the event report, denoted as R and generated using the signal strength strategy presented in [115] to guarantee the accuracy of that event. The generation of R is either:

- Automatic for every pre defined particular period of time.

or

- As a response to a request received from the BS.

Figure. 3.2 shows the structure of the event report R which includes the cell ID, event location and event type.

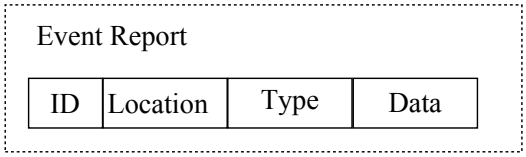


Figure 3.2: Event Report R structure.

Due to the packet encryption by K_{LC}, R, it is difficult for outside attackers to obtain R. However, the attackers could inject fabricated information or create a forged event, so some type of endorsement has to be embedded inside the generated reports in order to consider it as an authenticated report when it is received by the BS.

The novel scheme, LKMP-SBS, presented in this Chapter considers each event report generated by a specific cell and sent to the BS have to include three kinds of endorsements. Hence, the BS accept the received report as a legitimate report if it is:

1. The same as those received from each node in the event cell.

2. Contains the MAC generated by all authentication nodes.

3. Contains the signature of all z cell reporters of that cell.

3.6.1 The first endorsement: similar report is received from different nodes

The first endorsement is achieved by using the fundamentals of an (ε, n) threshold linear secret sharing scheme (LSSS) [32] where the BS can regenerate the report by using the received report shares generated by a threshold number ε of nodes. In contrast to similar schemes, our scheme makes use of the uniqueness of the K_a^{BS} key which is shared between each node in a particular cell and the BS as described in Algorithm. 4.7. Accordingly, this key is used by each node in c to derive its unique share C_a from the encrypted event report $C = E_{K_{LC}}\{R\}$:

$$C_a = C \sum_{0 \leq i \leq \varepsilon - 1} (K_a^{BS})^i \mod p \tag{3.11}$$

Obviously, C_a is generated uniquely by node a depending on its unique key K_a^{BS} which is shared with the BS only. Moreover, each node inside cell (c) broadcasts its share, as a tuple $\{Ca, ID_a\}$ to all its cell-mates. As a result, each node has an ability to collect and concatenate a total of $n-1$ shares received from its cell mates to create C_{new}:

$$C_{new} = C_1 \| C_2 ... \| C_n \tag{3.12}$$

3.6.2 The second endorsement: MAC of authentication nodes

The second endorsement of the report consists of multiple MACs calculated over C_{new}. These MACs are derived using the authentication keys dedicated and broadcast to each node by the BS (Algorithm 3.3). For example, in the case of dedicating two authentication cells $d1$ and $d2$ as intermediate cells between the cell (c) and the BS, each node inside (c) broadcasts the following to its cell-mates.

$$MAC_{K_{Lc}}\{C, MAC_{K_c^{d1}}(C_{new}), MAC_{K_c^{d2}}(C_{new})\}$$

When a node (a) receives different $i(n-1)$ MACs, where i refers to the number of

authentication cells, it sends a synthesized report containing the ID of all cell-mates and the hosting cell, C_{new} and i MACs, shared with each authentication cell. A random timer scheme [78] is used to avoid report duplication. Based on the enclosed MACs, the en-route filtering scheme is implemented by each authentication cell.

3.6.3 The third endorsement: signature of cell reporters

The third and the most important endorsement presented in this scheme is the signature of the set of z cell reporters randomly selected out of a total of n cell nodes by the BS. This set is changed every $\frac{1}{T}$ seconds, where T is a predefined cell reporter validity period which may be changeable based on multiple parameters like data importance, estimated frequency of attacks and rhythm of event occurrences. The participation of the cell reporter signatures in report generation overcomes the major security limitations in recent schemes. In other schemes, the capture of a threshold number of nodes in a particular cell enables the adversary to generate fake reports that might deceive all verification processes of the intermediate cell and the BS. Therefore, the received packet from the BS in LKMP-SBS is accepted if and only if all cell reporters are involved in the report generation.

3.7 Key Revocation

As a part of its role, the BS is responsible for checking the reason of listing a node/cell in the of $SusbNodes$ and $SusbCells$, created previously in Agorithm. 3.3 depending on the analysis of the information received from the surrounding nodes. If the node/cell is found to be compromised, then a revocation scheme is implemented by the BS in order to change all critical credentials shared with the suspicious entities and to overcome the possible vulnerabilities caused by them such as:

1. Colluding with other malicious cells/nodes.

2. Starting any correspondences with secure cells/nodes

LKMP-SBS include two schemes to implement the required revocation in the case of a suspicious node/cell being detected as illustrated in following subsections:

3.7.1 Key revocation in case of detecting a suspicious node

This scheme is implemented in order to neutralise the possible impact of each node in *SusbNodes* list. This is achieved by updating all nodes (except suspicious nodes) with new credentials as shown in following steps:

1. a new list of nodes $\{LIST\}_{new}$ is created rather than the list of nodes inside a particular cell c ($\{LIST\}_c$). This list exclude any malicious node.

2. Based on (3.9), a new cell key K_{Lc_new} is derived as:

$$K_{Lc\_new} = H((x_c, y_c \| ts \| \{LIST\}_{new}) \tag{3.13}$$

3. Based on (3.10), a new authentication key $K_{c\_new}^{d_i}$ is derived using the K_{Lc_new}:

$$K_{c\_new}^{d_i} = H(K_{Lc\_new} \| K_{Ld_i} \| (x_{d_i}, y_{d_i}) \| (x_c, y_c)) \tag{3.14}$$

4. Both new credentials K_{Lc_new} and $K_{c\_new}^{d_i}$ are broadcasted to each non-malicious nodes ($\check{a}$) in that cell as a $\{K_{Lc\_new}, ID_c, K_c^{d_i} : i = 1, 2...t\}$ encrypted by $K_{\check{a}}^{BS}$ which is derived in (3.3).

This procedure is illustrated in Algorithm. 3.4

For all nodes $\in$ *SusbNodes* list, the BS calls Algorithm (3.4) to revoke their credentials as shown below.

Algorithm 3.4 *Revocation of suspicious node* (s) *located inside a cell* (c) *implemented by the BS.*

Require: $ID_s \in SusbNodes, ID_c, K_{Lc}, K_c^{d_i} : i = 1, 2...t$
$\{LIST\}_{new} = \forall ID_a (ID_a \in \{LIST\}_c \bigwedge ID_a \neq ID_s)$
$K_{Lc\_new} \leftarrow H((x_c, y_c \| ts \| \{LIST\}_{new})$
$K_{c\_new}^{d_i} = H(K_{Lc\_new} \| K_{Ld_i} \| (x_{d_i}, y_{d_i}) \| (x_c, y_c))$
for $\forall a (a \in \{LIST\}_{new}$ **do**
$BS \rightarrow a : \{K_{Lc\_new}, ID_c, K_c^{d_i} : i = 1, 2...t\}$
end for
$RemoveK_c^{BS}$
Ensure: $\{LIST\}_{new}, K_{Lc\_new}, K_c^{d_i} : i = 1, 2...t\}$

3.7.2 Key revocation in case of detecting a suspicious node

Obviously, the potential consequences caused by a suspicious cell in a WSN is critically high in comparison with the impact of a suspicious node. As a result, the following

credentials have to be removed in order to neutralise any suspicious cell *sc*, as well as all its nodes, immediately:

1. Remove the cell key K_{sc}^{BS} from the BS data base to prevent any further communication.

2. Update all other cells that have *sc* as their authentication cell by a new list of authentication keys based on (3.10).

3. Remove all node-BS keys K_a^{BS} of any node belongs to the cell *sc*.

4. Update all security credentials of the adjacent cells by following all steps illustrated in Algorithm. 3.1, 3.2 and 3.3.

The set of adjacent cells shown in the above point is defined as all cells that have a mutual border or point with the *sc* and denoted as $\{AdjacentCells\}_{sc}$ as shown in Fig. 3.3. Based on the centre coordinates, for a suspicious cell *sc* which its centre located at (x_{sc}, y_{sc}), the list of adjacent cells is defined as :

$$\begin{aligned}\{AdjacentCells\}_{sc} =\{&(x_{sc}-1, y_{sc}+1), (x_{sc}, y_{sc}+1), (x_{sc}+1, y_{sc}+1),\\ &(x_{sc}-1, y_{sc}), (x_{sc}+1, y_{sc}), (x_{sc}-1, y_{sc}-1),\\ &(x_{sc}, y_{sc}-1), (x_{sc}+1, y_{sc}-1)\}\end{aligned} \tag{3.15}$$

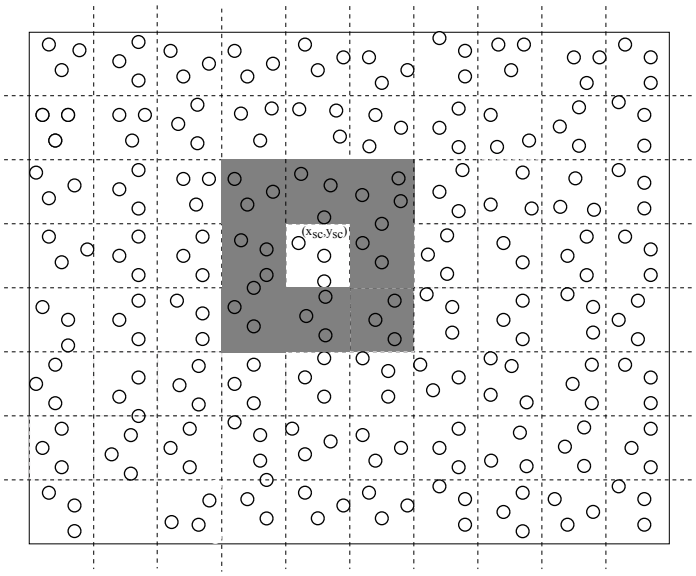


Figure 3.3: Adjacent cells of a suspicious cell (*sc*).

Algorithm. 3.5 illustrates the above described procedure.

Algorithm 3.5 *Revocation of suspicious cell* (sc) *implemented by the BS.*

Require: $ID_{sc}, K_{Lsc}, \{AdjacentCells\}_{sc}, K_{sc}^{d_i} : i = 1, 2...t$
  Remove K_{sc}^{BS}
  for $\forall d_i : i = 1, 2...t$ **do**
    Remove $K_{sc}^{d_i}\}$
  end for
  for $\forall a(a \in \{LIST\}_c$ **do**
    Remove $K_a^{BS}\}$
  end for
  for $\forall adjacentcellsofID_c$ **do**
    Algorithm. 3.1
    Algorithm. 3.2
    Algorithm. 3.3
  end for

3.8 Security Analysis of LKMP-SBS

The main role of the key management scheme present in this Chapter is to increase the rigidity of a WSN security. Therefore, the main outcome of this Chapter is to analyse the security of LKMP-SBS and compare it with some similar approaches. This system security analysis is presented based on three aspects:

1. System's capability of thwarting typical routing attacks.
2. The role of the number of cell reporters (z) in the security of each particular cell.
3. The system rigidity in terms of wireless security requirements for data confidentiality and authenticity.

The last two points will be investigated using the likelihood of compromising the entire WSN as a result of launching a Random Node Capture Attack (RNCA), which is described in Chapter 2. This likelihood is measured by the percentage of compromised cells and presented by a graph depicting the relationship between the total number of compromised nodes versus the percentage of compromised cells as will shown in the rest of this Chapter.

3.8.1 System Robustness Against Routing Attacks

As presented earlier, LKMP-SBS uses the node positions to derive the security credentials required to protect both cell-by-cell communication and the required correspondence between cell-mates. Hence, our scheme is secure enough to thwart almost all typical attacks. For instance, our scheme is strong enough to thwart the following routing attacks:

- Black hole and selective forwarding attacks: as a location dependent scheme, the routing decision in LKMP-SBS is made by the data source based on the location of both source and destination, which are represented by node(s) and the BS. Accordingly, this scheme has enough resistance to thwart black hole and selective forwarding attacks.

- Sybil attack: Any message disseminated between two entities in a WSN employing LKMP-SBS is encrypted by a key derived depending on the location of the data source. Such authentication prevents any node from pretending to be a different node in the network. Thus, Sybil attack has no ability to be launched in this scheme.

- Wormhole attack: Because of LKMP-SBS dependency on nodes location-dependent credentials in each packet authentication, it is an effective scheme in addressing this type of attacks.

- Node replication attack: LKMP-SBS can detect the node replication attack and thwart it because of the location awareness of each group of nodes within a cell. Any replicated node can be easily detected by cell mates and reported to the BS to be revoked using the key revocation scheme explained in 3.7.2.

- Hello flood attack: Because of the precise setup-phase pf the LKMP-SBS explained in Section 3.5, accepting or dealing with any HELLO massage is bounded by both the cell and node keys which are location dependent. Therefore, this scheme has an effective ability to detect and thwart this type of attacks.

3.8.2 The impact of z value on the security of each particular cell

As explained earlier in Section 3.6, the validity of any received report depends on three aspects:

1. Same report is recieved from a threshold number of nodes, denoted as ε.

2. MAC(s) generated by authentication nodes.

3. The participation of all z cell reporters in generating the event report.

The number of cell reporters z is selected depending on the application protocol, security level required and available resources. Because of this system being location dependant, z may change due to security attacks, node failures and geographical alterations. Therefore, the effect of the value of z is worth investigating in order to realize the optimum design of our scheme. This Section investigates the effect of z on the likelihood of compromising a particular cell. The probability of an adversary compromising all z cell reporters inside a cell that contains n nodes can be calculated using the compromising strategy illustrated in the following example:

Example 3.1

Assume a WSN consisting of N' cells where each cell contains 10 nodes ($n = 10$), 3 of them are selected by the BS to be cell reporters ($z = 3$). The adversary has a:

1. probability of $P(E1) = \frac{3}{10}$ to compromise all z cell reporters in the 1^{st} trial.
2. probability of $P(E2) = \frac{2}{9}$ to compromise the remaining 2 cell reporters from the remaining 9 nodes in the 2^{nd} trial.
3. probability of $P(E3) = \frac{1}{8}$ to compromise the last cell reporter from the remaining 8 nodes in the 3^{rd} trial.

The probability of compromising all 3 cell reporters in a row is:
$P = P(E1)P(E2)P(E3) = \frac{1}{120}$ This can be generalised as follows:

$$\begin{aligned} P_{zcomp} =& (\frac{z}{n})(\frac{z-1}{n-1})(\frac{z-2}{n-2})...(\frac{1}{n-z+1}) \\ P_{zcomp} =& \frac{z(z-1)(z-2)...(1)}{n(n-1)(n-2)...(n-z+1)} \end{aligned} \tag{3.16}$$

The numerator is clearly a factorial of z while the denominator can be simplified to:

$$\begin{aligned} n(n-1)(n-2)...(n-z+1) =& \prod_{i=1}^{x}(N-z+i) \\ =& \frac{n!}{(n-z)!} \end{aligned} \tag{3.17}$$

By substituting ((3.17)) in ((3.16)):

$$P_{zcomp} = \frac{(z!)(n-z)!}{n!} \tag{3.18}$$

The above mentioned equation describes the relationship between the probability of compromising a particular cell and the number of its cell reporters (z). This equation has a vital importance as it is the cornerstone that is used to determine the optimum value of z as shown in Section 3.9.

3.8.3 Security Strength Regarding Data Confidentiality

The content of the generated report by an event cell is only revealed to its nodes because it is encrypted by the cell key K_{Lc} owned by them. This guarantees the data confidentiality even when a number of intermediate nodes are compromised. However, if one of the nodes involved in report generation is compromised, the report contents could be revealed. In order to understand the security strength in this case, the effect of a random node capture attack (RNCA) on the entire system is investigated by determining the probability of compromising all cells due to RNCA. The cell is considered compromised if and only if:

1. The threshold number ε of nodes are compromised.

2. All the z cell reporters are compromised.

Regarding the first point, assume that x nodes are compromised out of a total of N nodes in the network. As explained in 3.6.1, the number of nodes inside each cell is considered to be n while only ε of them can generate a report. Let x nodes be compromised so the adversary has $\binom{N}{x}$ methods to compromise x nodes. Additionally, each cell has $\binom{n}{\varepsilon}$ different methods to create a legitimate report. The total number of different methods to implement both processes is $\binom{N}{x}\binom{n}{\varepsilon}$. Regarding the whole network, suppose j nodes out of ε endorsement nodes are compromised. Then the adversary picks ε nodes randomly out of n sensor nodes, captures j nodes out of the ε nodes participating in the report generation and then compromises $(x-j)$ out of $(N-\varepsilon)$ nodes as a final step. The resultant probability P_j of capturing j nodes out of ε endorsement nodes is

$$\begin{aligned} P_{e\{j\}} &= \frac{\binom{N}{\varepsilon}\binom{\varepsilon}{j}\binom{N-\varepsilon}{x-j}}{\binom{N}{x}\binom{N}{\varepsilon}} \\ &= \frac{\binom{\varepsilon}{j}\binom{N-\varepsilon}{x-j}}{\binom{N}{x}} \end{aligned} \tag{3.19}$$

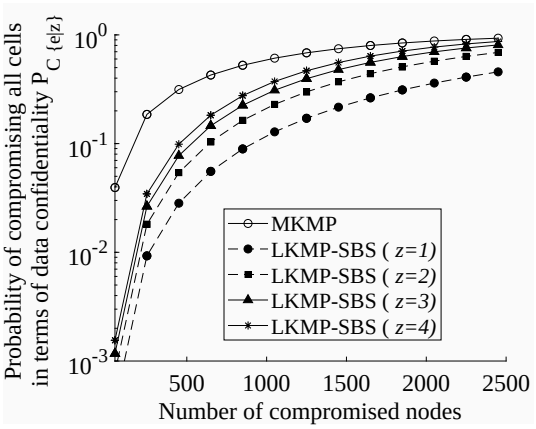
As a result, the probability of compromising none of the ε nodes is determined by substituting $(j = 0)$ into (3.19)

$$P_{e\{0\}} = \frac{\binom{N-\varepsilon}{x}}{\binom{N}{x}} \tag{3.20}$$

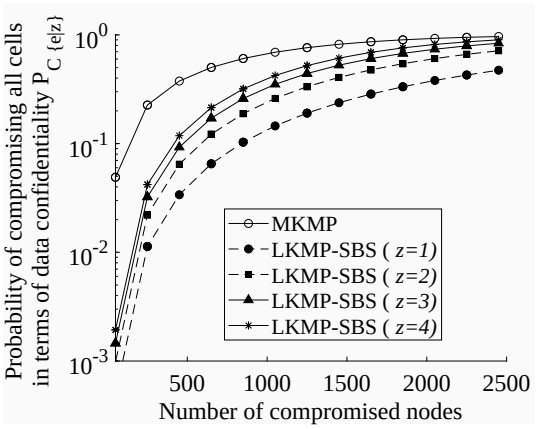
On the other hand, the probability $P_{z\{j\}}$ of capturing j cell reporters out of the z cell reporter set needs to be calculated. To achieve this, a set of z cell reporters is assumed to be static (as a worst case scenario), so that the same computations shown in (3.20) are followed. Bayes' theorem [116] is used to calculate the probability of capturing a particular cell in terms of data confidentiality:

$$P_{C\{\varepsilon|z\}} = \left(1 - \frac{\binom{N-\varepsilon}{x}}{\binom{N}{x}}\right)\left(1 - \frac{\binom{N-z}{x}}{\binom{N}{x}}\right) \tag{3.21}$$

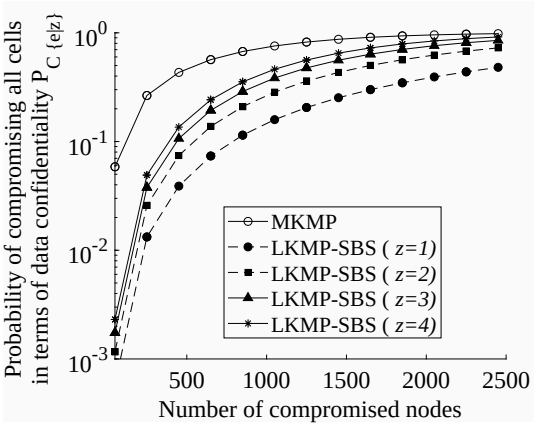
For different values of N, n and z, the percentage of captured cells concerning data confidentiality in terms of the number of compromised nodes is shown in Fig. 3.4, 3.5, 3.6 and 3.7.



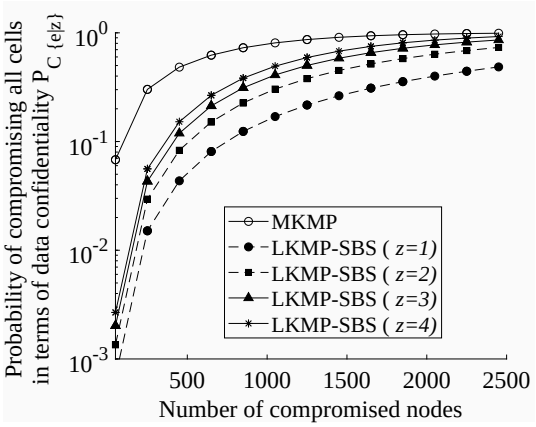
(a) $\varepsilon = 4$



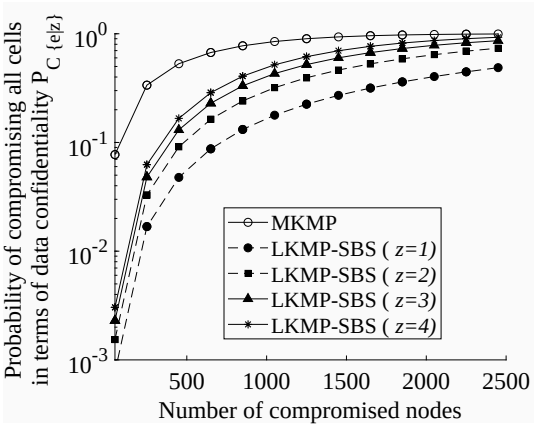
(b) $\varepsilon = 5$



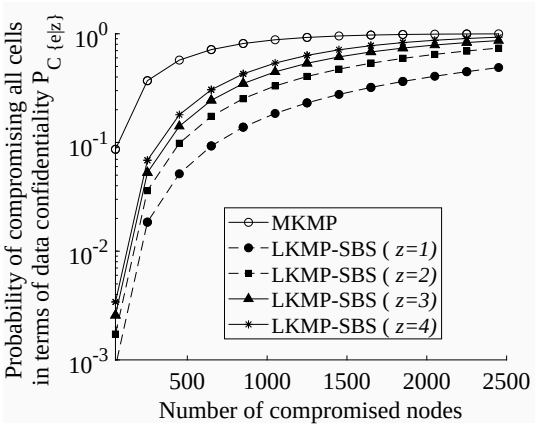
(c) $\varepsilon = 6$



(d) $\varepsilon = 7$

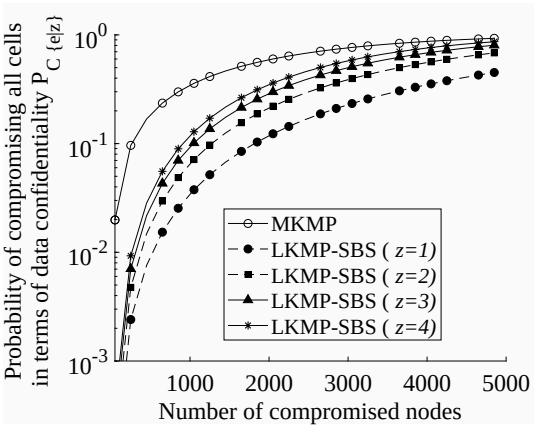


(e) $\varepsilon = 8$

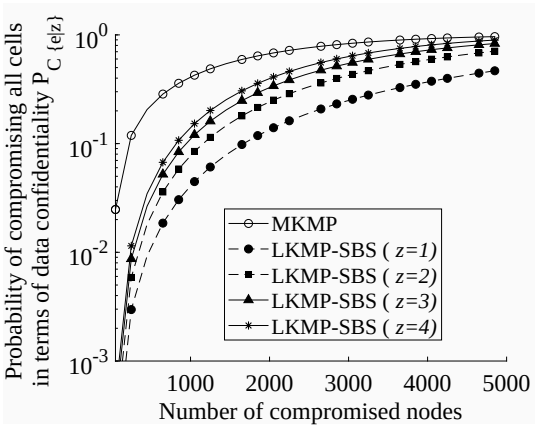


(f) $\varepsilon = 9$

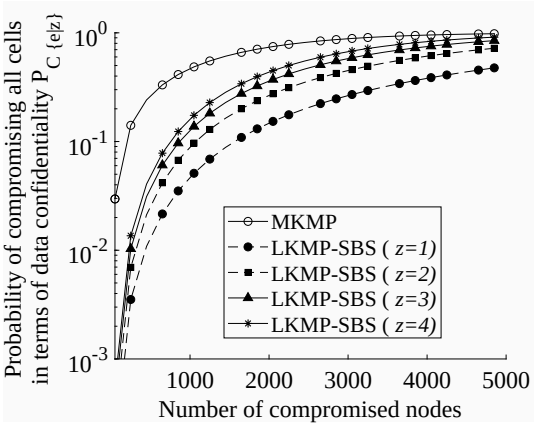
Figure 3.4: Data confidentiality of LKMP-SBS and MKMP under random capture attack in a WSN consist of $N = 5,000$ for different values of ε and z.



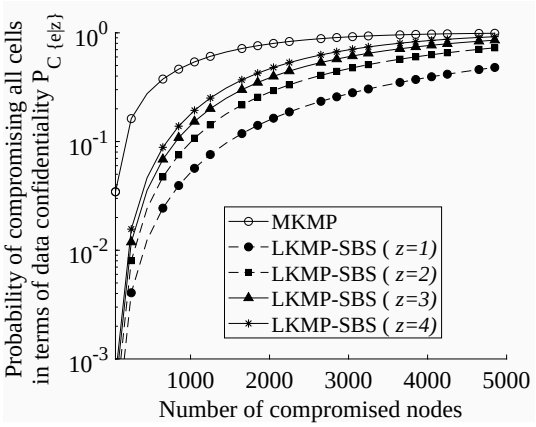
(a) $\varepsilon = 4$



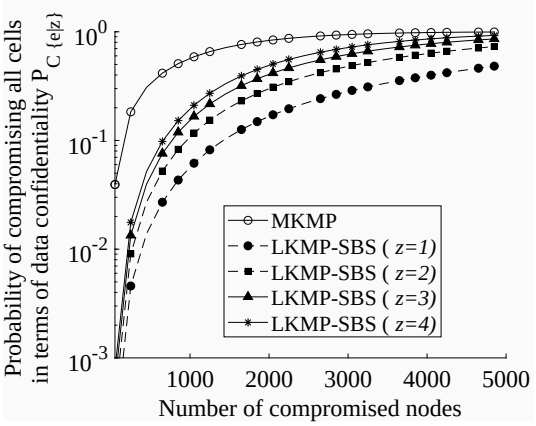
(b) $\varepsilon = 5$



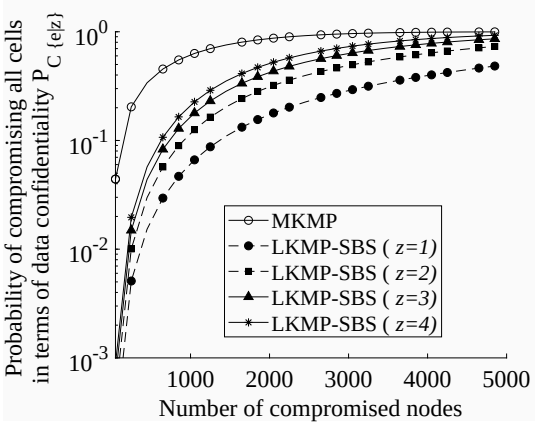
(c) $\varepsilon = 6$



(d) $\varepsilon = 7$

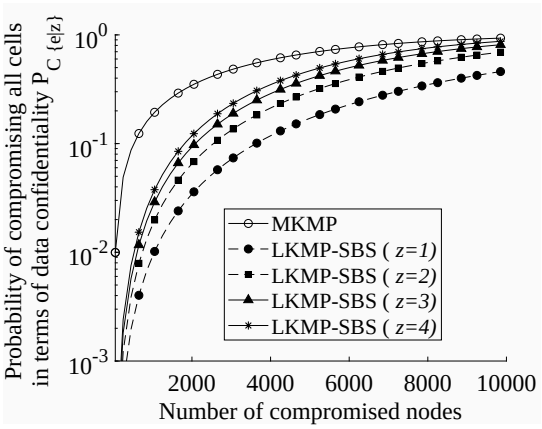


(e) $\varepsilon = 8$

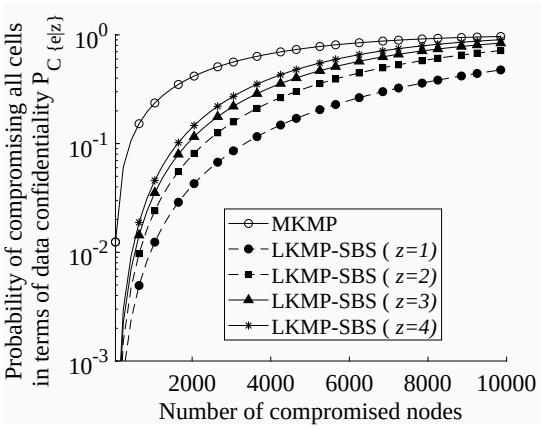


(f) $\varepsilon = 9$

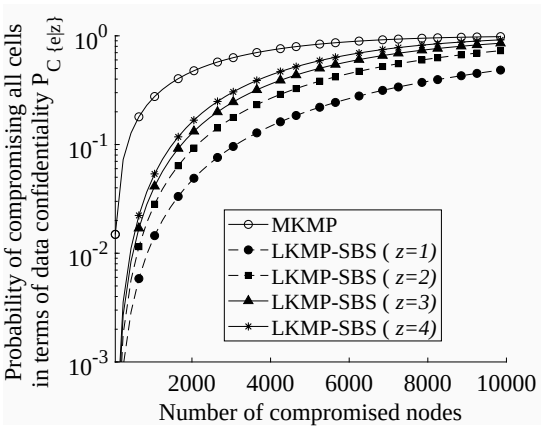
Figure 3.5: Data confidentiality of LKMP-SBS and MKMP under random capture attack in a WSN consist of $N = 10,000$ for different values of ε and z.



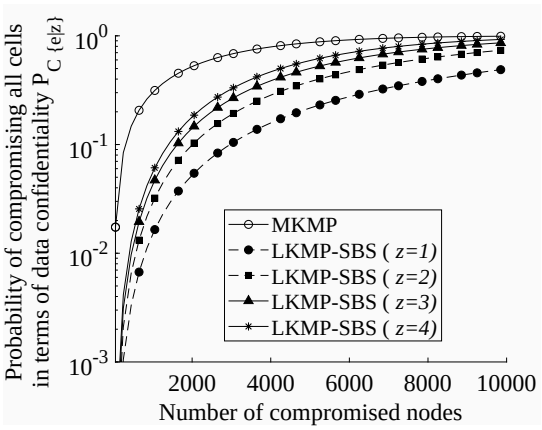
(a) $\varepsilon = 4$



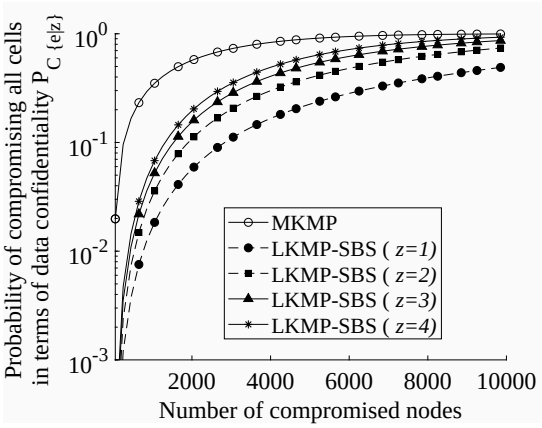
(b) $\varepsilon = 5$



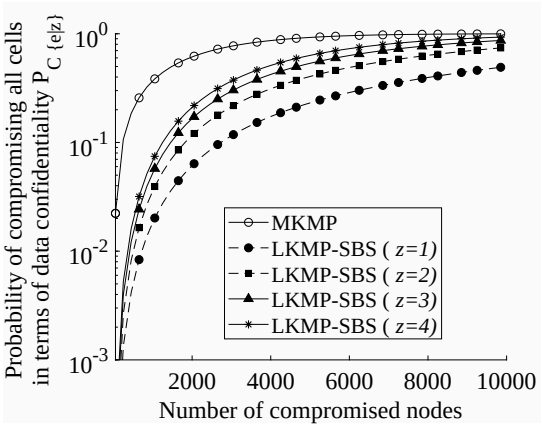
(c) $\varepsilon = 6$



(d) $\varepsilon = 7$

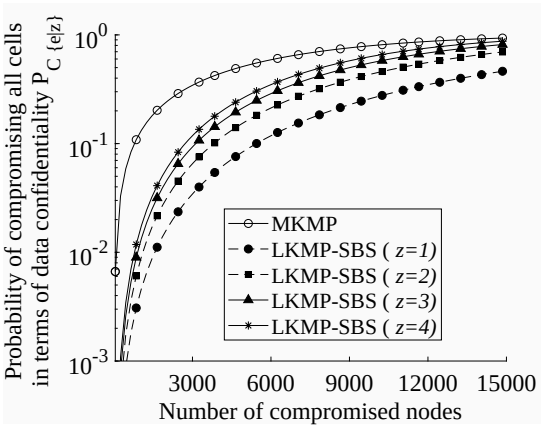


(e) $\varepsilon = 8$

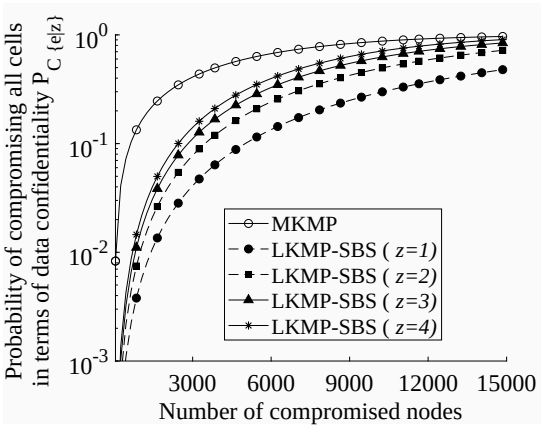


(f) $\varepsilon = 9$

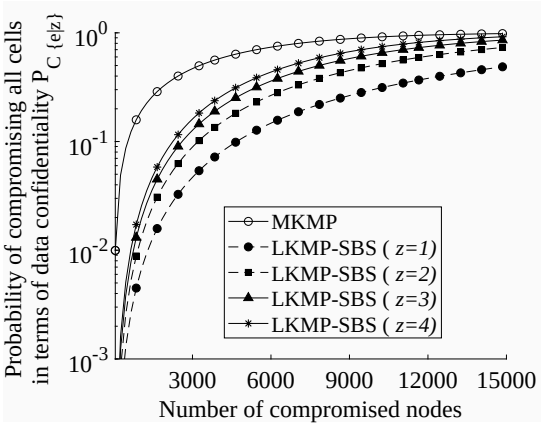
Figure 3.6: Data confidentiality of LKMP-SBS and MKMP under random capture attack in a WSN consist of $N = 20,000$ for different values of ε and z.



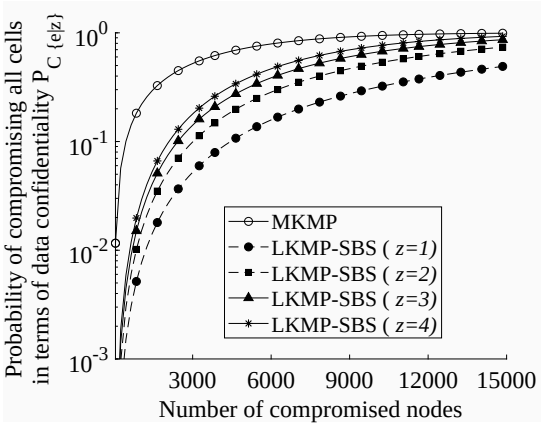
(a) $\varepsilon = 4$



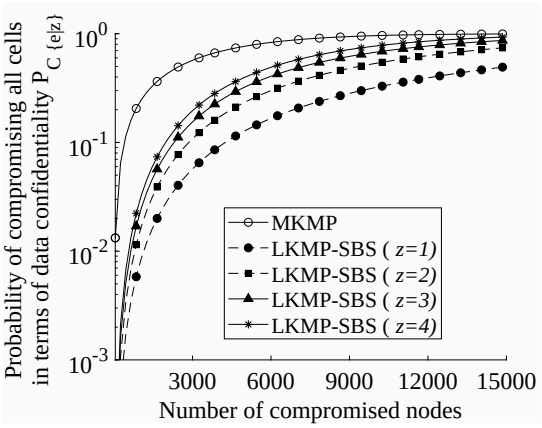
(b) $\varepsilon = 5$



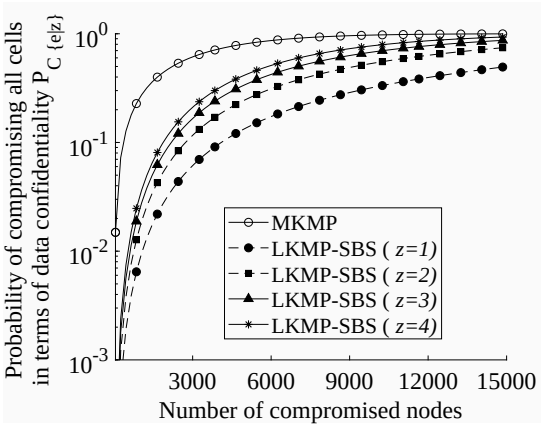
(c) $\varepsilon = 6$



(d) $\varepsilon = 7$



(e) $\varepsilon = 8$



(f) $\varepsilon = 9$

Figure 3.7: Data confidentiality of LKMP-SBS and MKMP under random capture attack in a WSN consist of $N = 30,000$ for different values of ε and z.

Those figures showing obviously that:

1. The security of LKMP-SBS in terms of data confidentiality, $P_{C\{\varepsilon|z\}}$, is observed to be reversely proportional to the values of z.

2. LKMP-SBS outperforms MKMP for any value of (N,ε and z).

3. MKMP and LKMP-SBS is proved to outperform LEDS in terms of data confidentiality because of the findings of [21] which reflects that MKMP is significantly superior to LEDS in terms of data confidentiality.

The behaviour of the relationship between x and $P_{C\{\varepsilon|z\}}$ is the same for any value of N and ε where $P_{C\{\varepsilon|z\}}$ cureve is increasing by x increment. However, the curve slope varies depending on N and ε values. These differences are depicted in Fig. 3.8 and Fig. 3.9 respectively. The two figures showing that:

$$P_{C\{e|z\}} = f(\frac{1}{N}, \varepsilon) \tag{3.22}$$

Following two sections discuss and explains the mathematical proof of both (3.22).

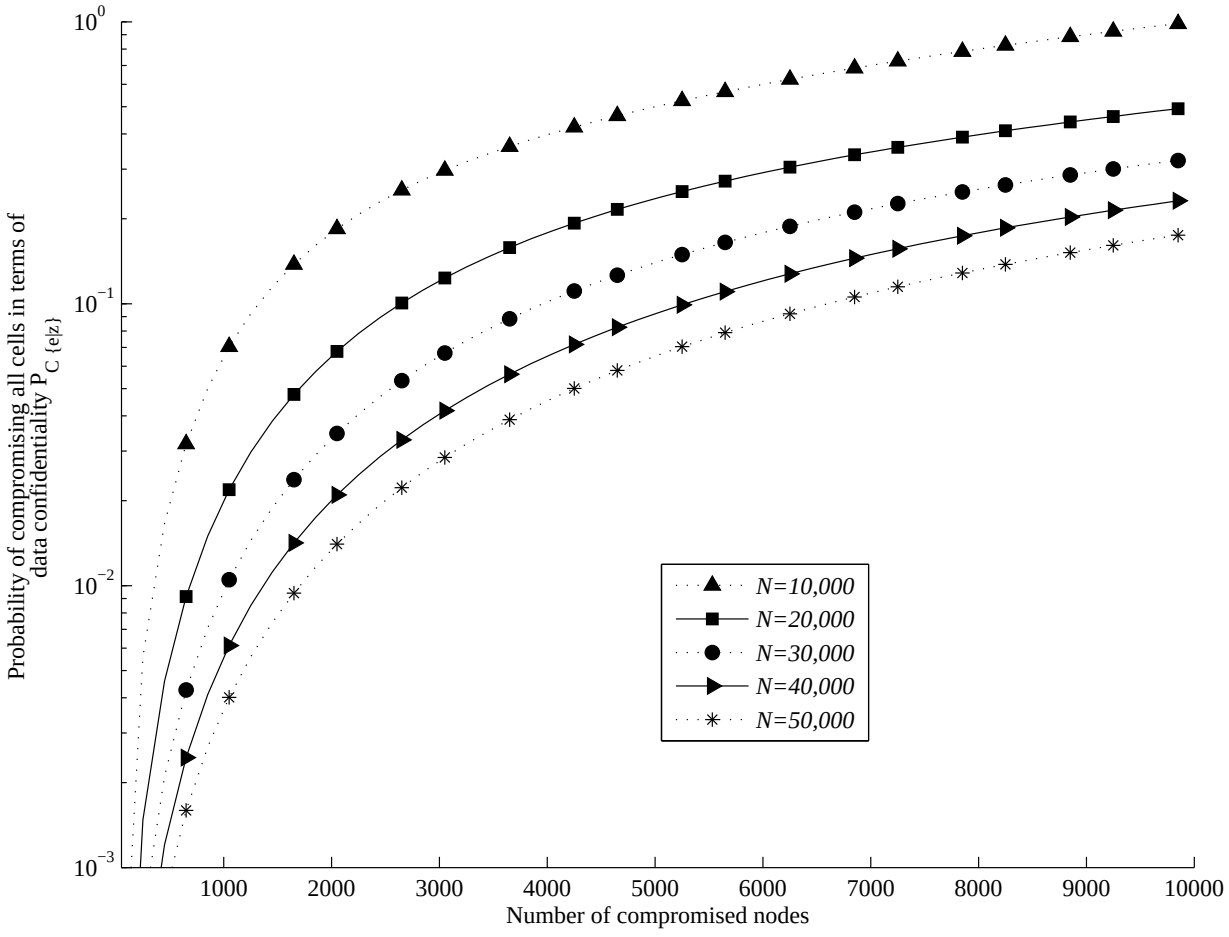


Figure 3.8: The effect of changing the number of whole nodes in the network N on the Probability of compromising all cells in terms of data confidentiality due to RNCA, $\varepsilon = 10$, $z = 5$.

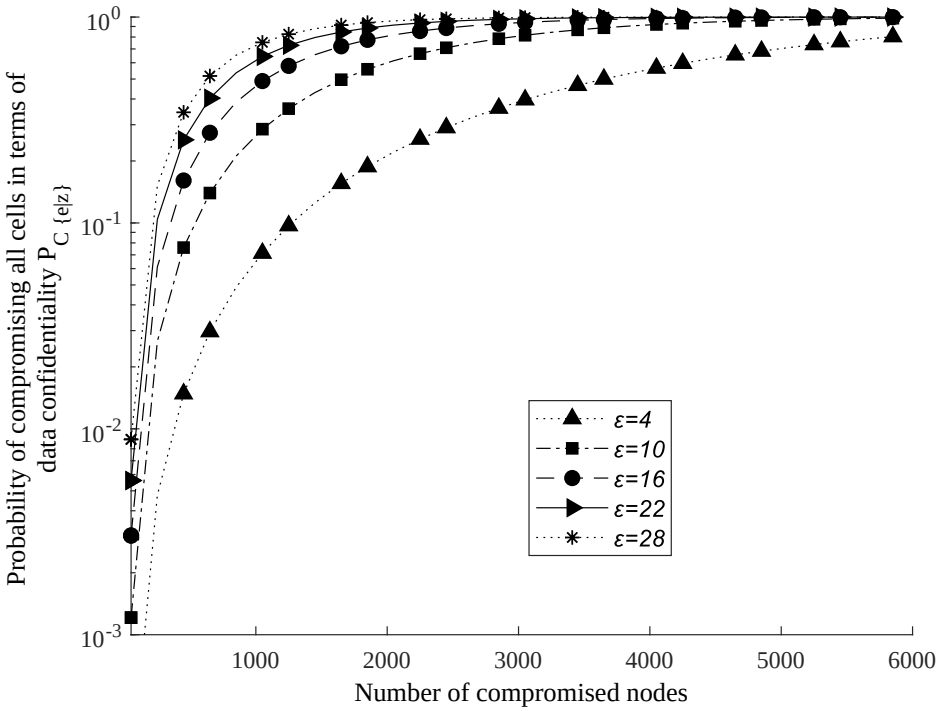


Figure 3.9: The effect of changing the number of endorsement nodes in the network ε on the Probability of compromising all cells in terms of data confidentiality due to RNCA, $N = 10,000$, $z = \frac{\varepsilon}{2}$.

3.8.3.1 The effect of N on the value of $P_{C\{\varepsilon|z\}}$

The used metric in the measurement of data confidentiality robustness, as mentioned in (3.8), is the ratio of compromised cells caused by implementing the RNCA. However, increasing the entire number of nodes, N, in the WSN increases the number of total cells assuming the number of nodes per cell is constant. Therefore, increasing the value of N definitely decrease the ratio of compromised cells and leading to an enhancement in the security of the system in terms of data confidentiality.

The mathematical proof of (3.22) is achieved, based on (3.21), as:

Proof 3.1

$$\begin{aligned} P_{C\{\varepsilon|z\}} &= \left(1 - \frac{\binom{N-\varepsilon}{x}}{\binom{N}{x}}\right)\left(1 - \frac{\binom{N-z}{x}}{\binom{N}{x}}\right) \\ &= P_1 P_2 \\ \Rightarrow P_{C\{\varepsilon|z\}} &= f(P_1, P_2) \end{aligned} \tag{3.23}$$

$$
\begin{aligned}
P_1 &= f(\frac{\binom{N}{x}}{\binom{N-\varepsilon}{x}}) \\
&\propto \frac{\frac{N!}{x!(N-x)!}}{\frac{(N-\varepsilon)!}{x!(N-\varepsilon-x)!}} \\
\frac{N!}{x!(N-x)!} \cdot \frac{x!(N-\varepsilon-x)!}{(N-\varepsilon)!} &= \frac{(N-\varepsilon)! \prod_{i=1}^{\varepsilon}(N-\varepsilon+i)(N-\varepsilon-x)!}{(N-\varepsilon)!(N-x-\varepsilon)! \prod_{i=1}^{x+e}(N-\varepsilon-x+i)} \\
&= \frac{\prod_{i=1}^{\varepsilon}(N-\varepsilon+i)}{\prod_{i=1}^{x+e}(N-\varepsilon-x+i)} \\
&= \frac{1}{\prod_{i=1}^{x}(N-x-\varepsilon+i)} \quad \text{for } N, x \text{ and } n \in \mathbb{N} \\
&= \frac{1}{N^x - a_1 N^{x-1} + a_2 N^{x-2} - \cdots a_x N}
\end{aligned} \tag{3.24}
$$

From both (3.23) and (3.24):

$$
\begin{aligned}
P_1 &= f(\frac{1}{N}) \\
P_2 &= f(\frac{1}{N}) \\
\Rightarrow P_{C\{\varepsilon|z\}} &= f(\frac{1}{N})
\end{aligned} \tag{3.25}
$$

■

3.8.3.2 The effect of ε on the value of $P_{C\{\varepsilon|z\}}$

There are two reasons that explain the relationship between ε and $P_{C\{\varepsilon|z\}}$:

1. Increasing the number of endorsement nodes while keeping a constant value of z increase the likelihood of generating a fake report from that cell.

2. Increasing ε will increase the value of n which leads to a decrease in the number of cells in the WSN assuming the total number of nodes N in the WSN is constant. Hence, the ratio of compromised cells is increased which reduces the security level of the system in terms of data confidentiality.

The mathematical proof of (3.22) is achieved, based on (3.21), as:

Proof 3.2

$$P_{C\{\varepsilon|z\}} = \left(1 - \frac{\binom{N-\varepsilon}{x}}{\binom{N}{x}}\right)\left(1 - \frac{\binom{N-z}{x}}{\binom{N}{x}}\right) \tag{3.26}$$

While the second part of above equation is not a function of ε, it is considered as a constant k:

$$\begin{aligned} P_{C\{\varepsilon|z\}} &= kP_1 \\ \Rightarrow P_{C\{\varepsilon|z\}} &= f(P_1) \qquad (3.27) \\ P_1 &= f(\frac{1}{\binom{N-\varepsilon}{x}}) \\ &= f(\frac{x!(N-\varepsilon-x)!}{(N-\varepsilon)!}) \qquad (3.28) \end{aligned}$$

While $x \lll e$, (3.28) can be written as:

$$\begin{aligned} P_1 &= f(\frac{x!(N-x)!}{(N-\varepsilon)!}) \\ &= f(\frac{1}{(N-\varepsilon)!}) \\ \Rightarrow P_1 &= f(\varepsilon) \qquad (3.29) \end{aligned}$$

Based on both (3.27) and (3.29):

$$P_{C\{\varepsilon|z\}} = f(\varepsilon) \tag{3.30}$$

■

3.8.4 Security Strength for Data Authenticity

Data authenticity in a particular cell is compromised if the attacker creates a forged report as a result of capturing at least ε sensor nodes including all z cell reporters. To show the security strength of our scheme, a formula to calculate the probability of all compromised cells in terms of data authenticity is derived using Bayes' theorem [116] in order to calculate the probability of an event resulted by two events:

- Compromising ε nodes:

$$P_{auth\{\varepsilon\}} = \sum_{j=1}^{\varepsilon} \frac{\binom{\varepsilon}{j}\binom{N-\varepsilon}{x-j}}{\binom{N}{x}} \tag{3.31}$$

- Sending a bogus report signed by the whole z nodes:

$$P_{auth\{z\}} = \sum_{j=1}^{z} \frac{\binom{z}{j}\binom{N-z}{x-j}}{\binom{N}{x}} \tag{3.32}$$

Hence, the fraction of compromised cell caused by compromising x nodes in terms of data authenticity can be written as:

$$P_{auth\{\varepsilon|z\}} = \sum_{j=1}^{\varepsilon} \frac{\binom{\varepsilon}{j}\binom{N-\varepsilon}{x-j}}{\binom{N}{x}} \sum_{j=1}^{z} \frac{\binom{z}{j}\binom{N-z}{x-j}}{\binom{N}{x}} \tag{3.33}$$

For different values of N, n and z, the percentage of captured cells concerning data authenticity in terms of the number of compromised nodes is shown in Fig. 3.10, 3.11, 3.12, 3.13, 3.14, 3.15, 3.16, 3.17, 3.18, 3.19, 3.20 and 3.21. Those figures show that:

1. The fraction of captured cells, measured as $P_{auth\{\varepsilon|z\}}$, increases with the number of captured nodes.

2. $P_{auth\{\varepsilon|z\}}$ is found to be reversely proportional to the value of z.

3. LKMP-SBS clearly outperforms MKMP in terms of data authenticity for all values of x, N, n and z.

4. LKMP-SBS shows an improvement in comparison to LEDS only for higher number of compromised nodes. For each set of variables, LKMP-SBS shown to be outperforming LEDS just when x is more than a threshold value x_t as reflected in Table. 3.1.

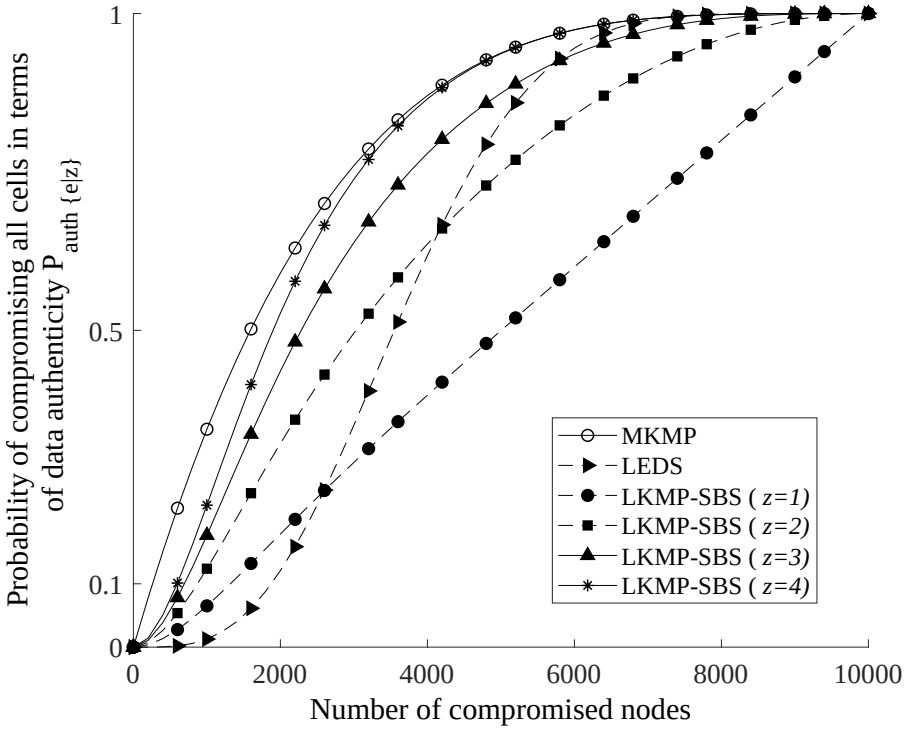


Figure 3.10: Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 10,000$, $\varepsilon = 4$ and $z = 1, 2, 3, 4$.

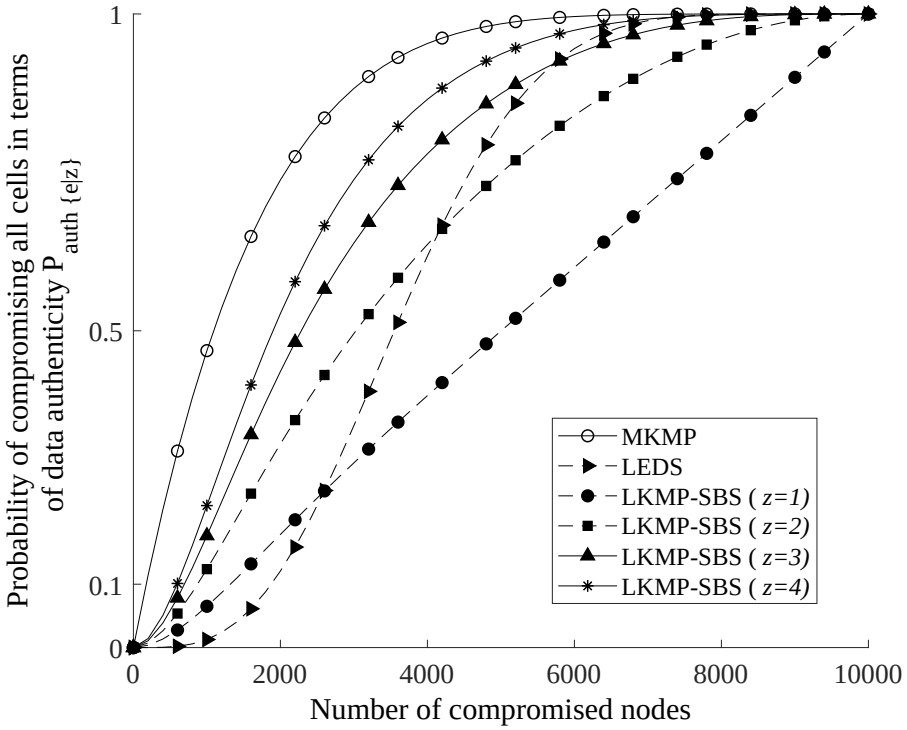


Figure 3.11: Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 10,000$, $\varepsilon = 6$ and $z = 1, 2, 3, 4$.

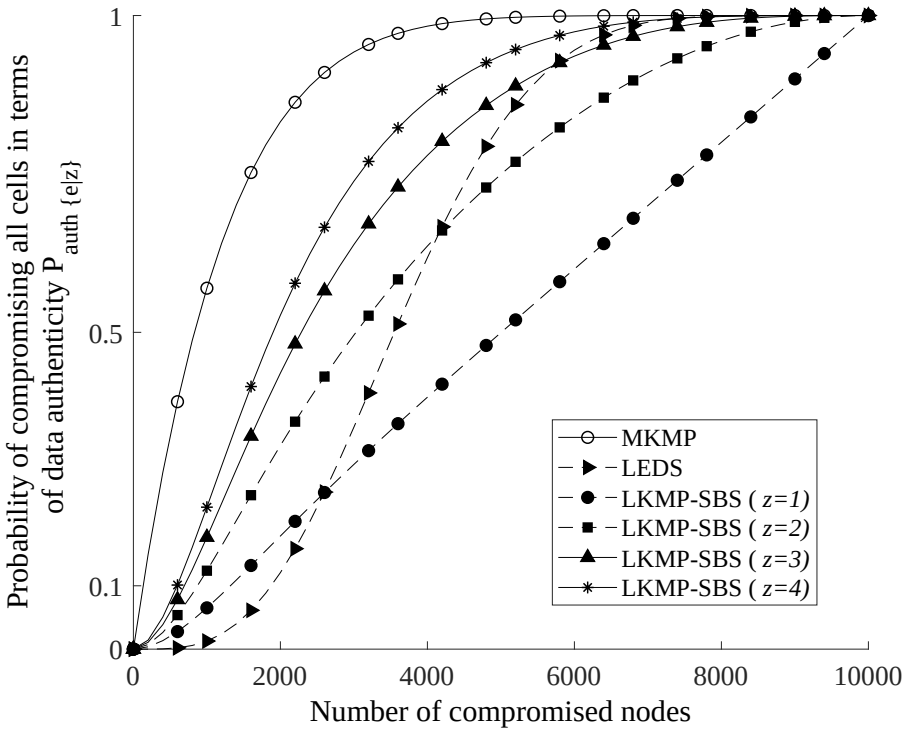


Figure 3.12: Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 10,000$, $\varepsilon = 8$ and $z = 1, 2, 3, 4$.

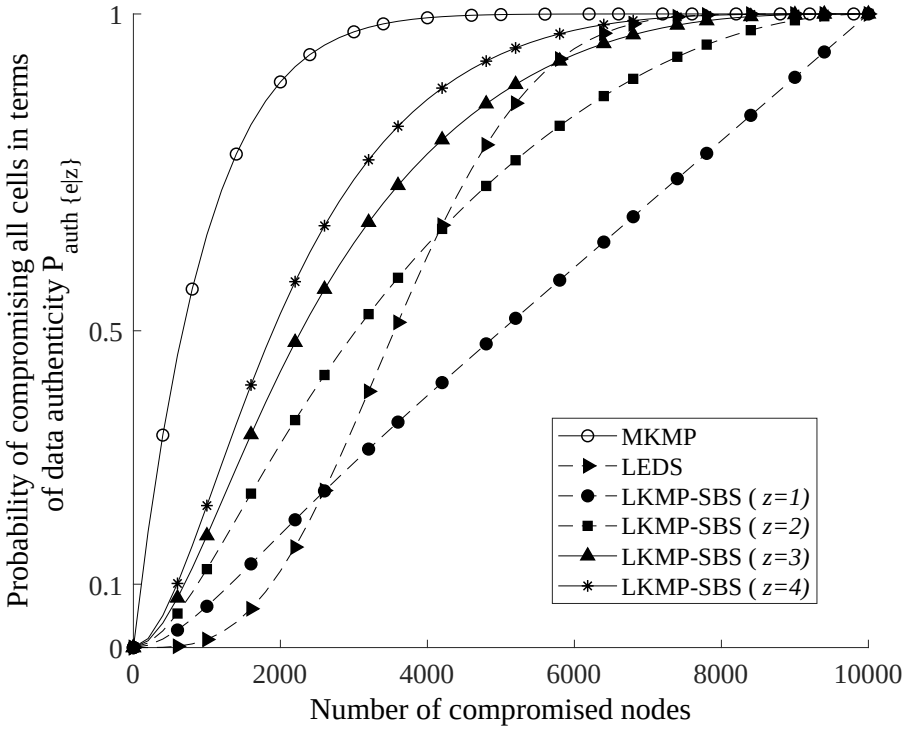


Figure 3.13: Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 10,000$, $\varepsilon = 10$ and $z = 1, 2, 3, 4$.

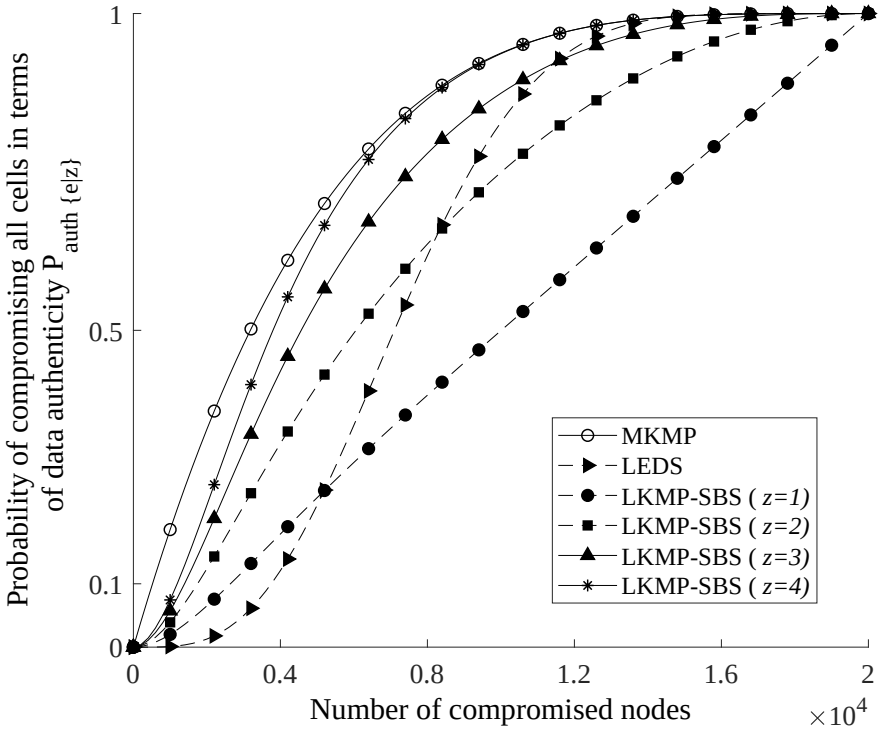


Figure 3.14: Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 20,000$, $\varepsilon = 4$ and $z = 1, 2, 3, 4$.

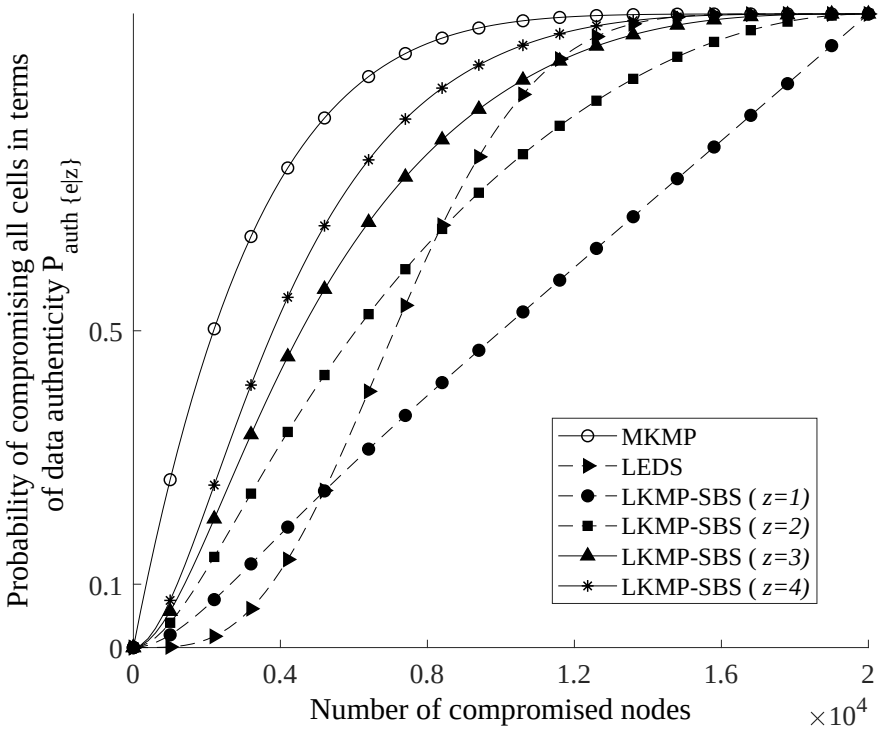


Figure 3.15: Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 20,000$, $\varepsilon = 6$ and $z = 1, 2, 3, 4$.

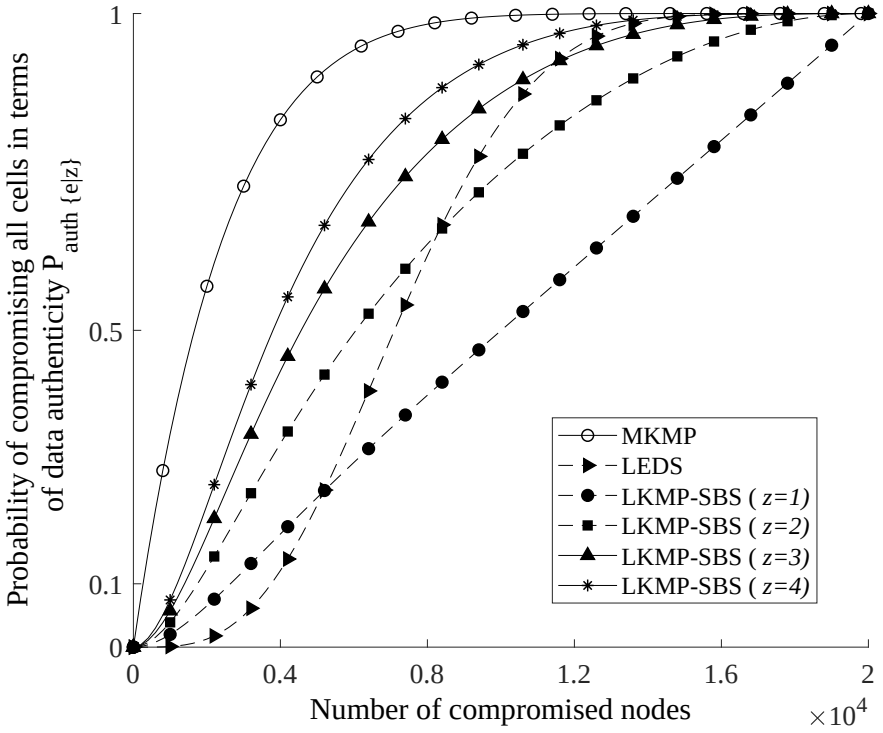


Figure 3.16: Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 20,000$, $\varepsilon = 8$ and $z = 1, 2, 3, 4$.

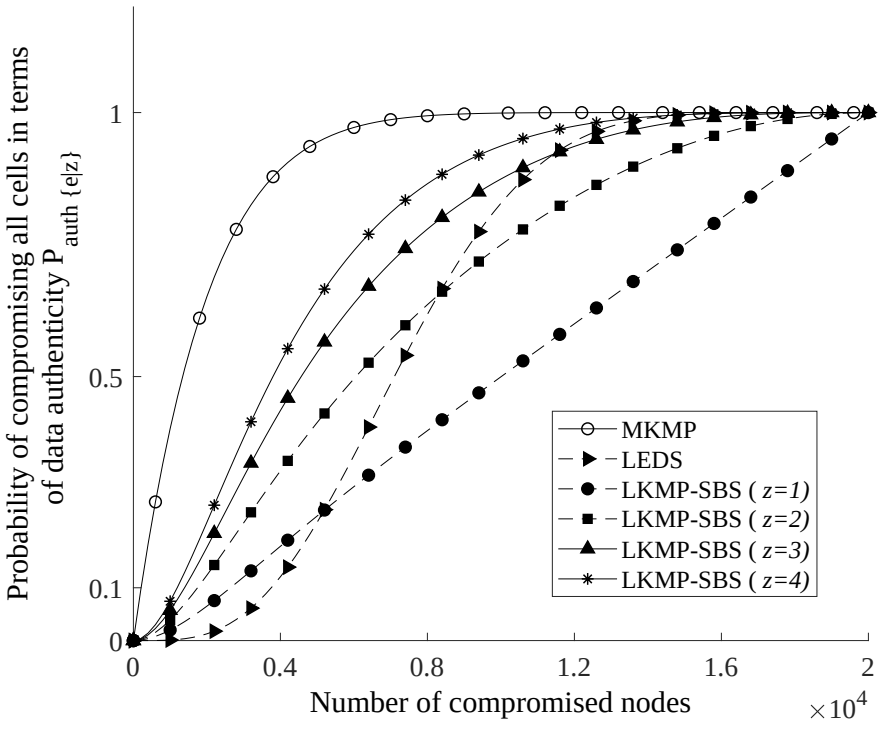


Figure 3.17: Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 20,000$, $\varepsilon = 10$ and $z = 1, 2, 3, 4$.

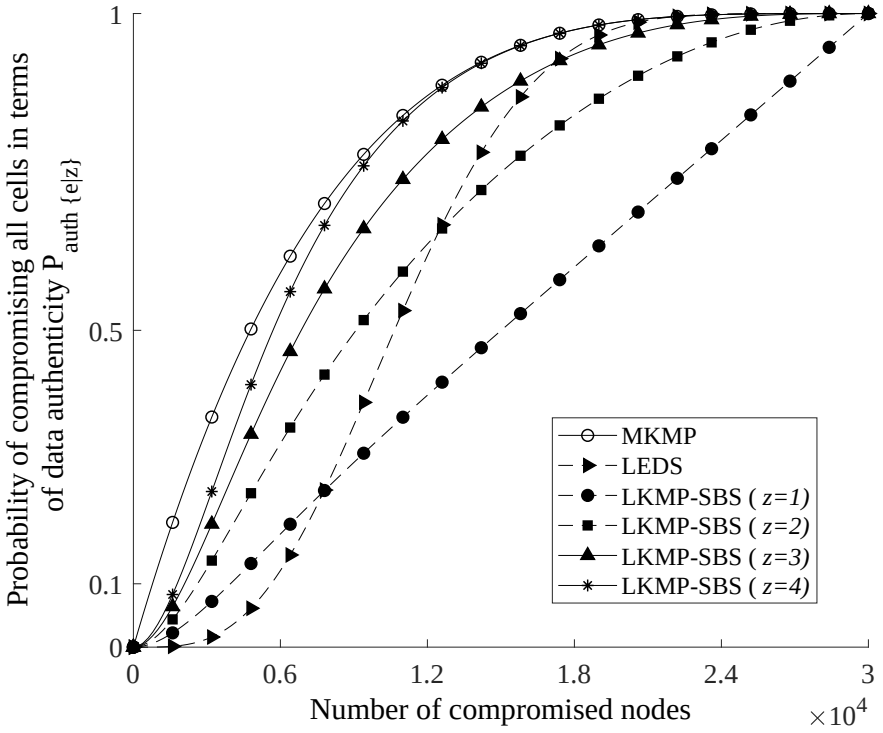


Figure 3.18: Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 30,000$, $\varepsilon = 4$ and $z = 1, 2, 3, 4$.

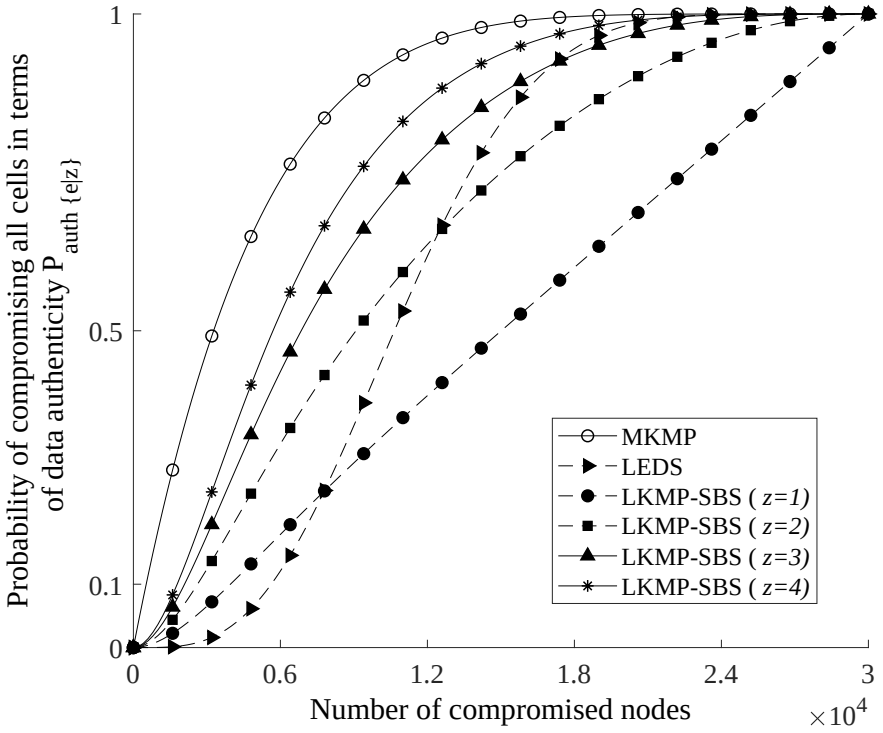


Figure 3.19: Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 30,000$, $\varepsilon = 6$ and $z = 1, 2, 3, 4$.

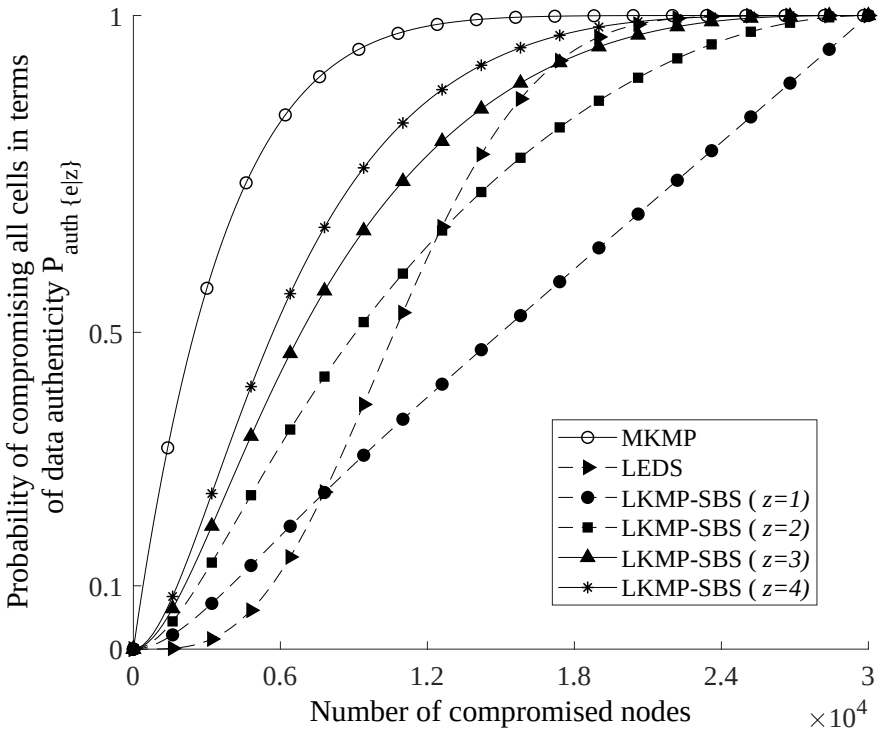


Figure 3.20: Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 30,000$, $\varepsilon = 8$ and $z = 1, 2, 3, 4$.

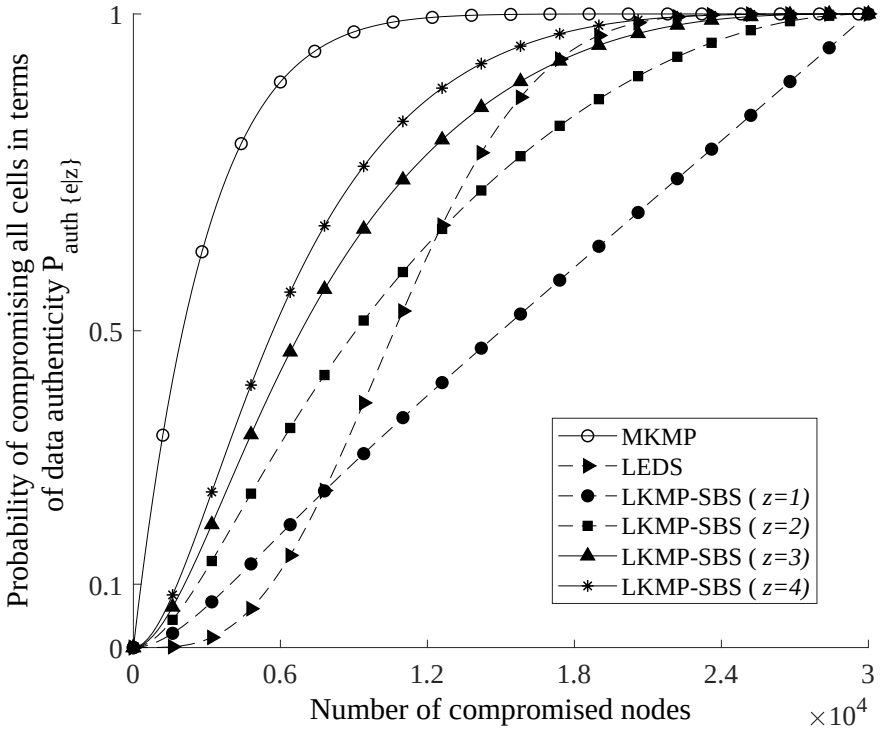


Figure 3.21: Data authenticity of LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 30,000$, $\varepsilon = 10$ and $z = 1, 2, 3, 4$.

Table 3.1: Approximate value of x_t for different values of N, ε and z.

N	ε	X_t		
		$z=1$	$z=2$	$z=3$
$10,000$	4	1850	3375	4875
	6	2250	3900	5700
	8	2375	4090	5825
	10	2500	4100	5875
$20,000$	4	4000	6750	9750
	6	4600	7900	11050
	8	5000	8200	11350
	10	5100	8750	11500
$30,000$	4	6000	10500	15500
	6	7000	12000	17300
	8	7500	12900	17400
	10	8000	13000	17500

It is obvious that the behaviour of the relationship between x and $P_{auth\{\varepsilon|z\}}$ is the same for any value of N and ε where $P_{auth\{\varepsilon|z\}}$ curves are increasing by x increment. However, the curve slope varies depending on N and ε values. These differences are depicted in Fig. 3.22 and Fig. 3.23 respectively. The two figures showing that:

$$P_{auth\{\varepsilon|z\}} = f(\frac{1}{N}, \varepsilon) \tag{3.34}$$

The following two sections discuss and explain the mathematical proof of (3.34).

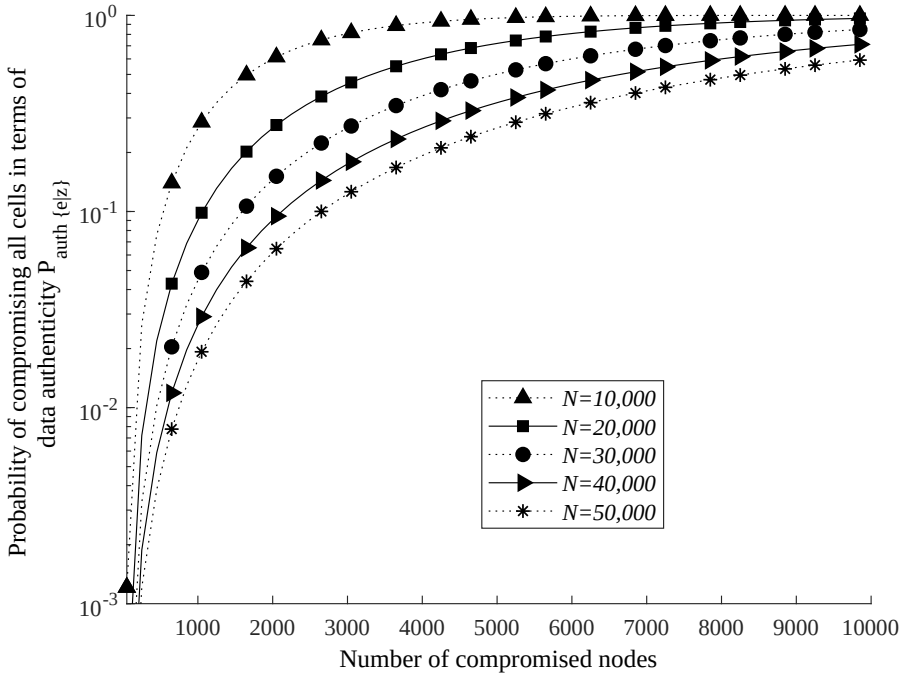


Figure 3.22: The effect of changing the number of whole nodes in the network N on the Probability of compromising all cells in terms of data authenticity due to RNCA, $\varepsilon = 10$, $z = 5$.

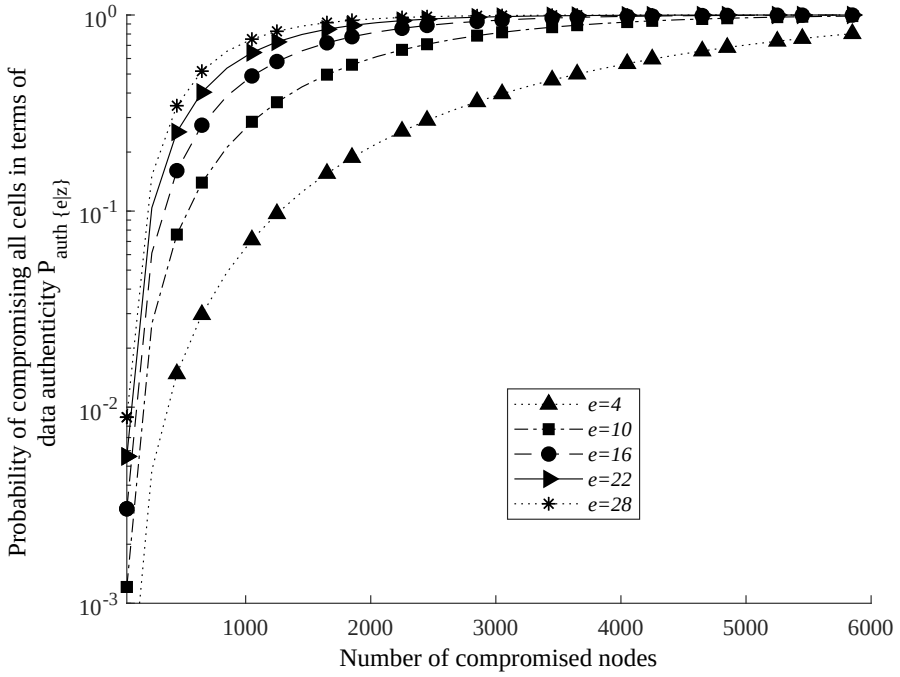


Figure 3.23: The effect of changing the number of endorsement nodes in the network ε on the Probability of compromising all cells in terms of data authenticity due to RNCA, $N = 10,000$, $z = \frac{\varepsilon}{2}$.

3.8.4.1 The effect of N on the value of $P_{auth\{\varepsilon|z\}}$

The used metric in the measurement of data authenticity robustness, as mentioned in (3.8), is the ratio of compromised cells caused by implementing the RNCA. However, increasing the entire number of nodes, N, in WSN increases the number of total cells assuming the number of nodes per cell is constant. Therefore, increasing the value of N definitely decrease the ratio of compromised cells and leads to an enhancement in the security of the system in terms of data authenticity.

The mathematical proof of (3.34) is achieved, based on (3.33), as:

Proof 3.3

$$P_{auth\{\varepsilon|z\}} = \sum_{j=1}^{\varepsilon} \frac{\binom{\varepsilon}{j}\binom{N-\varepsilon}{x-j}}{\binom{N}{x}} \sum_{j=1}^{z} \frac{\binom{z}{j}\binom{N-z}{x-j}}{\binom{N}{x}} \tag{3.35}$$

$$= P_1 P_2$$

$$\Rightarrow P_{auth\{\varepsilon|z\}} = f(P_1, P_2) \tag{3.36}$$

While $\binom{\varepsilon}{j}$ in (3.36) is a non N dependent term, it is considered as a constant:

$$\begin{aligned} P_1 &\propto \sum_{j=1}^{\varepsilon} \frac{\binom{N-\varepsilon}{x-j}}{\binom{N}{x}} \\ &\propto \sum_{j=1}^{\varepsilon} \frac{\frac{(N-\varepsilon)!}{(x-j)!(N-\varepsilon-x+j)!}}{\frac{(N)!}{x!(N-x)!}} \\ &\propto \sum_{j=1}^{\varepsilon} \frac{x!(N-\varepsilon)!(N-x)!}{N!(x-j)!(N-\varepsilon-x+j)!} \\ &\propto \sum_{j=1}^{\varepsilon} \frac{(N-\varepsilon)!(N-x)!}{N!(N-\varepsilon-x+j)!} \end{aligned} \tag{3.37}$$

$$\begin{aligned} \sum_{j=1}^{\varepsilon} \frac{(N-\varepsilon)!(N-x)!}{N!(N-\varepsilon-x+j)!} &= \sum_{j=1}^{\varepsilon} \frac{\prod_{k=1}^{\varepsilon-j}(N-x-\varepsilon+j+k)}{\prod_{k=1}^{\varepsilon}(N-\varepsilon+k)} \\ &= \frac{N^{\varepsilon-j} - a_1 N^{\varepsilon-j-1} + a_2 N^{\varepsilon-j-2} - \cdots a_{\varepsilon-j} N}{N^{\varepsilon} x - a_1 N^{\varepsilon-j-1} + a_2 N^{\varepsilon-j-2} - \cdots a_{\varepsilon} N} \end{aligned}$$

While $(\varepsilon - j) < \varepsilon$

$$\sum_{j=1}^{\varepsilon} \frac{(N-\varepsilon)!(N-x)!}{N!(N-\varepsilon-x+j)!} = f(\frac{1}{N}) \tag{3.38}$$

$$\begin{aligned} P_1 = f = f(\frac{1}{N}) \\ P_2 = f(\frac{1}{N}) \\ \Rightarrow P_{auth\{\varepsilon|z\}} = f(\frac{1}{N}) \end{aligned} \tag{3.39}$$

■

3.8.4.2 The effect of ε on the value of $P_{auth\{\varepsilon|z\}}$

There are two reasons explaining the relationship between ε and $P_{C\{\varepsilon|z\}}$:

1. Increasing the number of endorsement nodes while keeping a constant value of z increase the likelihood of generating a fake report from that cell.

2. Increasing ε will increase the value of n which leads to decrease the number of cells in the WSN assuming the total number of nodes N in the WSN is constant. Hence, the ratio of compromised cells is increased which reduces the security level of the system in terms of data confidentiality.

The mathematical proof of (3.34) is achieved, based on (3.33), as:

Proof 3.4

$$P_{auth\{\varepsilon|z\}} = \sum_{j=1}^{\varepsilon} \frac{\binom{\varepsilon}{j}\binom{N-\varepsilon}{x-j}}{\binom{N}{x}} \sum_{j=1}^{z} \frac{\binom{z}{j}\binom{N-z}{x-j}}{\binom{N}{x}} \tag{3.40}$$

While the second part of above equation is not a function of ε, it is considered as a constant k:

$$\begin{aligned} P_{auth\{\varepsilon|z\}} = kP_1 \\ \Rightarrow P_{auth\{\varepsilon|z\}} = f(P_1) \\ P_1 \propto \sum_{j=1}^{\varepsilon} \frac{\binom{\varepsilon}{j}\binom{N-\varepsilon}{x-j}}{\binom{N}{x}} \end{aligned} \tag{3.41}$$

While: $j \lll x$ and $\varepsilon \lll N$, (3.41) can be rewritten as:

$$\begin{aligned} P_1 &\propto \sum_{j=1}^{\varepsilon} \binom{\varepsilon}{j} \\ &\propto \sum_{j=1}^{\varepsilon} \frac{\prod_{k=1}^{j}(\varepsilon - j + k)}{j!} \\ &\propto \frac{1}{j!} \cdot [\varepsilon^j - a_1\varepsilon^{j-1} + a_2 N^{j-2} - \cdots a_j\varepsilon] \\ \Rightarrow P_1 &= f(\varepsilon) \end{aligned} \tag{3.42}$$

Based on both (3.41) and (3.42):

$$P_{auth\{\varepsilon|z\}} = f(\varepsilon) \tag{3.43}$$

■

3.9 Optimum number of Cell Reporters

Previous sections showed the number of cell reporters z as a cornerstone of LKMP-SBS. On the one hand, it is obvious from the theory that increasing the value of z will definitely decrease the likelihood of generating a fake report inside any cell in the network. On the other hand, the results shown in the last sections indicated by three security parameters $P_{C\{\varepsilon|z\}}$, $P_{auth\{\varepsilon|z\}}$ and P_{zcomp} have a different proportionality to z as stated in (3.18), (3.21) and (3.33). Therefore, in order to guarantee the optimality of the proposed system, the following two sections investigate the optimum value of cell reporters. In the first Section, a mathematical analysis for the relationship between $P_{C\{\varepsilon|z\}}$ and z is achieved to find its margins. Furthermore, the optimality of z is investigated by considering its effect on the security of the cell itself using the parameter P_{zcomp}.

3.9.1 Mathematical Analysis of optimum z based on $P_{C\{\varepsilon|z\}}$ and $P_{auth\{\varepsilon|z\}}$

In this Section, the optimum number of cell reporters z will be investigated based on the expressions $P_{C\{\varepsilon|z\}}$ and $P_{auth\{\varepsilon|z\}}$ given in ((3.21)) and ((3.33)) respectively. The

mathematical investigation aims to calculate the optimum number of cell reporters z_{min} which leads to minimizing both (P_c) and (P_{auth}). It is obvious that ((3.21)) and ((3.33)) consists of two parts:

- For the $P_{C\{\varepsilon|z\}}$, it consist of two terms:
  1. $\left(1-\frac{\binom{N-\varepsilon}{x}}{\binom{N}{x}}\right)$ which is a constant term in term of z
  2. $\left(1-\frac{\binom{N-z}{x}}{\binom{N}{x}}\right)$ which is a function of z.
- For the $P_{auth\{\varepsilon|z\}}$, it is also consist of two terms:
  1. $\sum_{j=1}^{\varepsilon}\frac{\binom{\varepsilon}{j}\binom{N-\varepsilon}{x-j}}{\binom{N}{x}}$ which is a constant term in term of z
  2. $\sum_{j=1}^{z}\frac{\binom{z}{j}\binom{N-z}{x-j}}{\binom{N}{x}}$ which is a function of z.

Hence, the set of optimum values of z_{opt} can be expressed as:

$$z_{opt}=\arg\min_{z}\left(\sum_{j=1}^{z}\frac{\binom{z}{j}\binom{N-z}{x-j}}{\binom{N}{x}}\right)\cap\arg\min_{z}\left(1-\frac{\binom{N-z}{x}}{\binom{N}{x}}\right) \tag{3.44}$$

It is obvious that in the first part $z_{min}=1$ according to the summation limits of the first part. However, the second part of the equation above shows that $z_{max}\leq N-x$. As a result:

$$1\leq z_{opt}\leq(N-x) \tag{3.45}$$

By substituting (3.45) in both ((3.21)) and ((3.33)):

$$P_c|_{z_{min}}=\frac{x}{N}\left(1-\frac{\binom{N-\varepsilon}{x}}{\binom{N}{x}}\right) \tag{3.46}$$

$$P_c|_{z_{max}}=\frac{N!-x!(N-x)!}{N!}\left(1-\frac{\binom{N-\varepsilon}{x}}{\binom{N}{x}}\right) \tag{3.47}$$

$$P_{auth}|_{z_{min}}=\frac{x}{N}\sum_{j=1}^{\varepsilon}\frac{\binom{\varepsilon}{j}\binom{N-\varepsilon}{x-j}}{\binom{N}{x}} \tag{3.48}$$

$$P_{auth}|_{z_{max}}=\sum_{j=1}^{N-x}\frac{\binom{N-x}{j}\binom{x}{x-j}}{\binom{N}{x}}\sum_{j=1}^{\varepsilon}\frac{\binom{\varepsilon}{j}\binom{N-\varepsilon}{x-j}}{\binom{N}{x}} \tag{3.49}$$

Next the optimality of z in terms of cell capturing and its effect on the integrity of generated reports is investigated.

3.9.2 Mathematical Analysis of optimum z based on P_{zcomp}

As explained early in Section 3.24, the relationship between a probability of compromising a particular cell with the number of its cell reporters is stated by (3.18) as:

$$P_{zcomp} = \frac{(z!)(n-z)!}{n!}$$

This relationship is depicted as shown in Fig. 3.24 which shows that P_{zcomp} approaches zero when z lies in a specific range of values indicated as Δz. In addition, n and Δz are related as:

$$n = f(\Delta z) \tag{3.50}$$

This indicates that increasing the number of nodes inside a cell increases the flexibility in terms of selecting the optimum number of cell reporters. For instance, when the number of nodes inside a cell is 10, the operator has to select $z \in [3, 7]$ to ensure a very low probability of compromised cells. On the other hand, the operator can choose $z \in [2, 28]$ when $n = 30$ and be sure of the same compromised cell probability ($P \leq 0.01$). To be more precise about the optimal value of z, we investigate the minimum point for each graph in Fig. 3.24 to find the optimum value of z_{opt}. However, $f(x) = x!$ is a discrete function which require a continuous mathematical approximation to be differentiable. According to [117], Gamma approximation is one of the promising methods:

$$x! = \Gamma(x-1) \tag{3.51}$$

Where:

$$\Gamma(z) = \int_0^\infty x^{z-1} e^{-x}\, dx \tag{3.52}$$

Accordingly, z_{opt} is calculated as:

$$\begin{aligned} z_{opt} &= \arg\min_{z} \left\{ \frac{(z!)(n-z)!}{n!} \right\} \\ &\frac{\partial}{\partial z}(z!)(n-z)! = 0 \\ &(n-z)!\Gamma(z+1)\psi^0(z+1) \\ &= z!\Gamma(n-z+1)\psi^0(n-z+1) \\ \psi^0(z+1) &= \psi^0(n-z+1) \end{aligned}$$

While $\psi^m(x)$ is a monotonic function [118]:

$$z = \frac{n}{2} \tag{3.53}$$

It is clear that ((3.53)) represents a critical point for P_{zcomp}, so the first derivative test is applied in order to check weather it is a local minima or not. Two points are selected as $(0 \in (-\infty, \frac{n}{2}))$ and $(n \in (\frac{n}{2}, \infty))$ in order to implement this test. Therefore, the first derivative of P_{zcomp} is calculated as:

$$\begin{aligned} \frac{\partial}{\partial z}(P_{zcomp}) =& \frac{\partial}{\partial z}\frac{z!(n-z)!}{n!} \\ =& \frac{1}{n!}[(n-z)!\Gamma(z+1)\psi^0(z+1) - \\ & z!\Gamma(n-z+1)\psi^0(n-z+1)] \end{aligned} \tag{3.54}$$

As a result, at $z = 0$

$$\begin{aligned} \frac{\partial}{\partial z}(z!)(n-z)!/n!|_{z=0} &= \frac{n!\Gamma(1)\psi^0(1)}{n!} - \frac{\Gamma(n+1)\psi^0(n+1)]}{n!} \\ &= \psi^0(1) - \psi^0(n+1) \end{aligned} \tag{3.55}$$

On the other hand, when $z = n$:

$$\begin{aligned} \frac{\partial}{\partial z}(z!)(n-z)!/n!|_{z=n} =& \frac{\Gamma(n+1)\psi^0(n+1)}{n!} - \frac{n!\Gamma(1)\psi^0(1)]}{n!} \\ =& \psi^0(n+1) - \Gamma(1)\psi^0(1) \end{aligned} \tag{3.56}$$

Based on Theorem. 3.2, (3.55) is a negative term for all values of n while (3.56) is a positive term for all n values. As a result, $z = \frac{n}{2}$ is proved to be the optimum value of cell

reporters that give the lowest probability of compromising a particular cell P_{zcomp}. As an example, three different values of n are chosen as 10, 20 and 30. The resultant optimum value of z are obviously 5, 10 and 15 respectively. This is shown in Fig. 3.24.

Theorem 3.2 *For all* $m, n \in \mathbb{R}^+$*:*
$\psi^m(n+1) \geq \psi^m(1)$

Proof 3.5

For all $n, x \in \mathbb{R}^+$:

$$x^n \geq 1$$
$$x^n e^{-x} \geq e^{-x}$$

According to domination rule for definite integration [119]

$$\int_0^\infty x^n e^{-x} dx \geq \int_0^\infty e^{-x} dx$$
$$\int_0^\infty x^{(n+1)-1} e^{-x} dx \geq \int_0^\infty x^0 e^{-x} dx$$
$$\int_0^\infty x^{(n+1)-1} e^{-x} dx \geq \int_0^\infty x^{1-1} e^{-x} dx$$
$$\Gamma(n+1) \geq \Gamma(1)$$
$$\ln \Gamma(n+1) \geq \ln \Gamma(1)$$
$$\frac{\partial^m}{\partial z^m} \ln \Gamma(n+1) \geq \frac{\partial^m}{\partial z^m} \ln \Gamma(1)$$
$$\psi^m(n+1) \geq \psi^m(1) \tag{3.57}$$

■

3.10 Conclusion

In this Chapter, a novel Location Dependent Key Management Protocol for a Single BS WSNs (LKMP-SBS) is presented and it is proved to achieve an improved performance compared to existing schemes. Each node has its unique credentials derived based on its position, which removes the influence of the capturing of a node on other sensor nodes

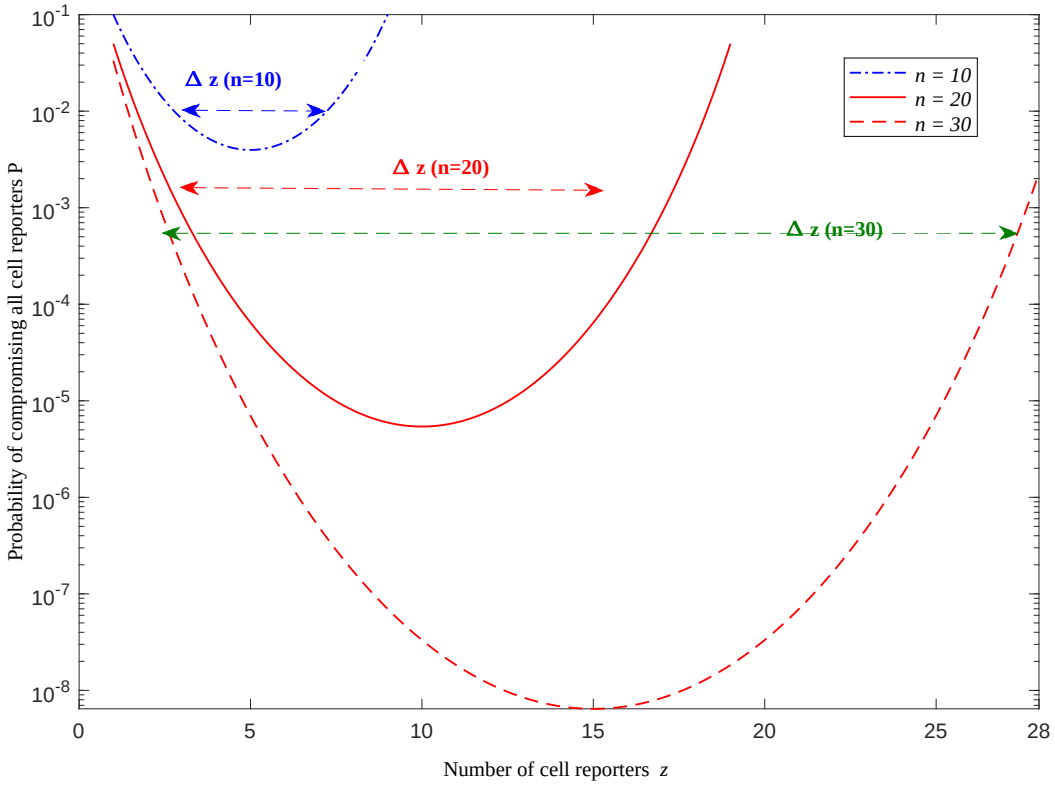


Figure 3.24: The relationship between number of cell reporters (z) and the probability of compromising all cell reporters inside a cell of 10, 20 and 30 nodes.

in its vicinity. Each cell has a particular number of cell reporters z which are randomly chosen by the BS. The involvement of cell reporters in report generation is compulsory, otherwise, the received report at the BS side will be discarded. An extensive analysis was presented to evaluate this scheme, which shows a distinct robustness against a significant number of captured nodes. In contrast to other schemes, our system shows a considerable improvement in terms of data confidentiality and data authenticity. Regarding the data confidentiality, for three values of z (1,2,3) the improvement is 95%, 90% and 85% respectively when 1000 nodes are compromised. This is due to the ability of the adversary to disclose event contents in the case of compromising one of the ε endorsement nodes in MKMP and LEDS, whereas in our new scheme the data is disclosed if and only if the entire set of z cell reporters and all ε endorsement nodes are captured. On the other hand, the improvement drops to 75%, 57% and 43% when the number of compromised nodes increased to 5000 due to the increment in the probability of compromising the entire set of cell reporters when more nodes are compromised. Furthermore, in terms of data authenticity an enhancement of 49%, 24%, 12.5% is gained using our approach with $z = 1, 2, 3$ respectively when half of all nodes are compromised. However, LKMP-SBS shows an improvement in comparison to LEDS only for higher values of x. Hence, It

outperform LEDS when $(x \geq 4000, x \geq 7000, x \geq 10000)$ and $z = 1, 2, 3$ respectively. As a result, LKMP-SBS is superior compared to the other schemes in terms of the fraction of compromised cells caused by RNCA thwarting data authenticity, especially when 50% of the nodes are captured. Finally, the optimum number of cell reporters was extensively investigated related to the security requirements, which was proven to be $z = \frac{n}{2}$.

Chapter 4

Location-Dependent Key Management Protocol for a Multiple BSs WSN

4.1 Introduction

The usage of multiple BS with WSN is one of hot topics targeted recently by research community. The employed BSs are used to collect data, control sensor functionalities and integrate WSN with the Internet. Recent researches are proposing multiple BS to address high power consumption [120,121], routing difficulties [122] and security challenges [3,123, 124]. According to [3,124] the usage of a single BS is considered as a single point of failure in IoT integrated WSN as presented in Chapter 2. Therefore, this Chapter presents state-of-the art of multiple BS WSN structure and the possible control schemes. Accordingly, a Location Dependent Key Management Protocol for a Multiple BS WSN (LKMP-MBS) is proposed. This protocol is built on a similar foundation as the LKMP-SBS discussed in the previous Chapter. Hence, this protocol depends on security credentials derived mainly from the geographical location of each sensor node within the network. However, most of procedures are different from those used in LKMP-SBS due to the significant change in the WSN structure and relevant protocols. Moreover, this Chapter address the expected challenges, such as the impact of the number of BSs on the overall security and the mechanism of selecting cell reporters by each BS. In this Chapter, the following aspects will be discussed:

1. The security robustness of the LKMP-MBS in terms of data confidentiality and

authenticity.

2. The optimum number of cell reporters.

Both an extensive mathematical analysis and simulation results are presented to investigate the above points. Accordingly, LKMP-MBS had been compared with the LKMP-SBS to show the possible challenges faced when multiple BSs are employed. In addition, LKMP-MBS is proved to outperform other existing multiple BSs location dependent schemes in terms of data confidentiality data authenticity and computation cost. Moreover, the efficiency of the LKMP-MBS as a lightweight scheme in terms of communication cost is presented in Chapter 5.

4.2 WSN Control Scheme by Multiple BSs

It is obvious that the BS has vital responsibilities such as objective requesting, strategy planning, collecting reports from the WSN nodes, adding/removing nodes and accordingly, controlling the related procedures. in the proposed scheme, the topology of a multiple BS WSN is classified, according to the manner of BS control, into:

- Individual control (IndCon): The WSN terrain is divided into subregions where each region is controlled by a particular BS as shown in Fig. 4.1. Every node is connected to a BS assigned to the node's region and responsible for handling the functionality of each node there by arranging the nodes' issuing, controlling, reporting and data collection.

- Collaborative control (ColCon): The entire WSN is controlled collaboratively by every BS as shown in Fig.4.2. Hence, each BS governs a particular function which is implemented by a specific cell or set of cells. Accordingly, each node in this case has a connection with each BS controlling that region, storing the required security credentials and collecting the reports related to the particular function implemented by that node. This scheme is the cornerstone of the emerging technology for multi-functional WSNs or shared-WSNs [125, 126]

Based on this classification, Section 4.9 will investigate the optimality number of cell reporters. In addition, Chapter 5 will consider the same classification in the analysis of node mobility.

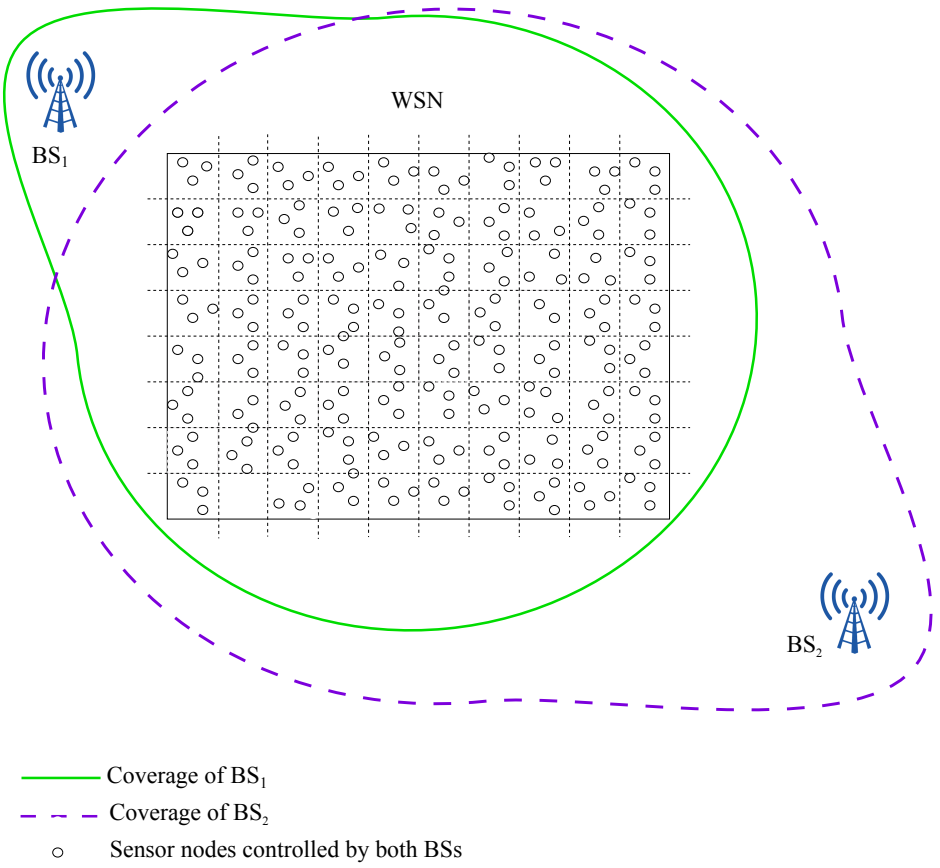


Figure 4.1: A WSN controlled individually by two BSs BS_1 and BS_2

4.3 System Consideration

The LKMP-MBS is considered to be used by a WSN employed over a wide border (maritime or terrestrial) terrain to be used in surveillance missions. Such a WSN is assumed to have a predefined shape, size, number of sensors and number of BSs. The sensor nodes are considered to have limited resources, whereas all BSs have no limitation in their resources. There are two schemes to allocate load balance between different BSs The set of BSs in this WSN is responsible for requesting surveillance reports from the sensors in service, collecting the data generated by sensor nodes and controlling the en-route filtering processes. Each BS is considered to have a communication facility with coverage over most of the sensors as depicted in Fig. 1. The monitored region is divided virtually into square cells have similar size. While all nodes are assumed to be distributed uniformly, each cell is considered to contain the same number of nodes. Each node has an ability to calculate its position using a secure localisation scheme [111–113]. Finally, every sensor and BS is considered to have a unique public key (its name) and a private key (ID). As mentioned in the previous section, a set of z sensor nodes inside each cell are selected randomly by a BS or a set of BSs and selected as cell reporters, which are considered

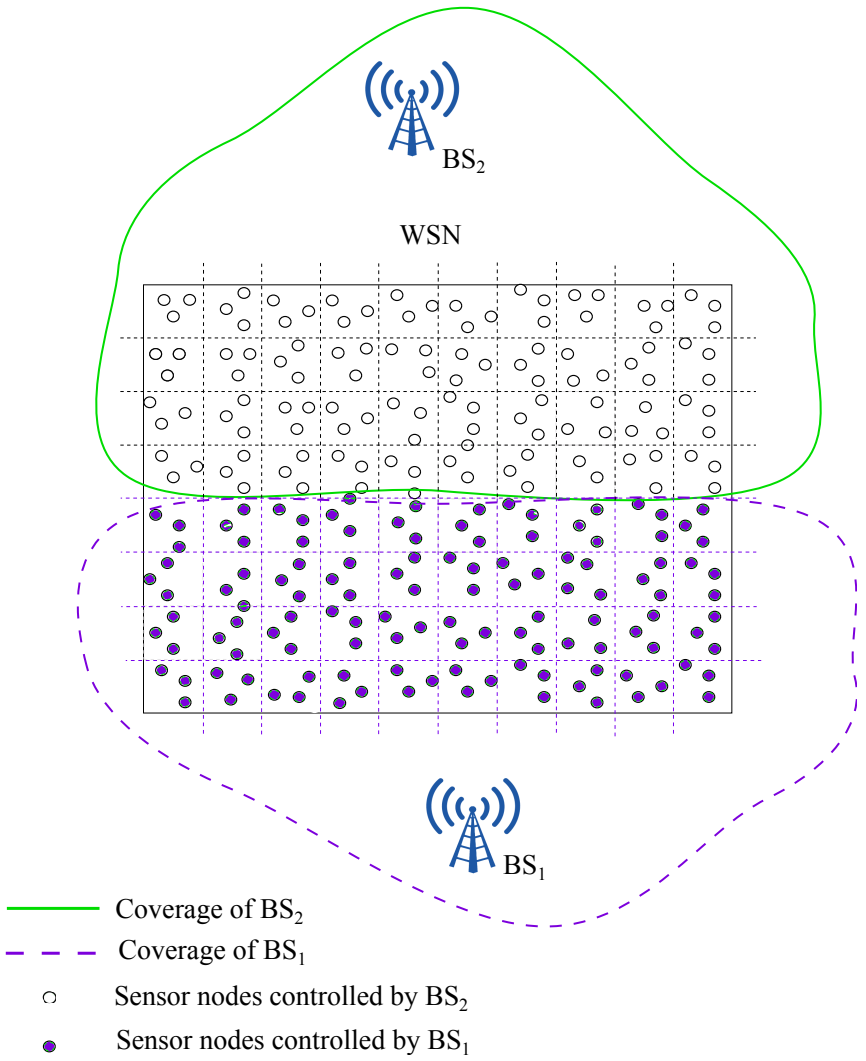


Figure 4.2: A WSN controlled collaboratively by two BSs BS_1 and BS_2

as jury members, where the signature of any one is considered as a firm condition of the report to be accepted. Otherwise, the report is considered as a bogus report and denied by all BSs receiving it. As explained in Chapter 2, in other schemes, the compromising of a threshold number of sensor nodes in a specific cell gives the adversary an ability to generate a bogus reports which might pass all verification process of the intermediate cell and the BS. Therefore, the presence of the cell reporter signature condition prevents any attacker from generating a fake report unless it succeeds in compromising all cell reporters in the event cell. The cell reporters set is modified every $\frac{1}{T}$ seconds, where the predefined validity period T of the cell reporters might be varied according to several parameters such as estimated attack frequency, data importance the the data occurrence rhythm.

4.4 Notation and Terms

In this Chapter, the following notations and terms have a significant importance:

- K: An initial master key used as a seed to derive other keys
- $(x_0^{(i)}, y_0^{(i)})$: The location of the $(i)^{th}$ BS
- Δ: The side length of each cell
- t: The number of authentication cells $d_\omega : i = 1, 2...t$
- p: A prime number
- M: The number of BSs in the network.
- $\boldsymbol{x_c}$: $M \times 1$ vector contains the x coordination of the center of cell c regarding each BS.
- $\boldsymbol{y_c}$: $M \times 1$ vector contains the y coordination of the center of cell c regarding each BS.
- (x_a, y_a): The location of a sensor node (n)
- $\|$: The operation of concatenation
- H: A Hash function
- ID_a: Identity of each particular sensor node (n) which is known by the BS
- t_s: A recent time slot
- $\boldsymbol{K_{Lcin}}$: $M \times 1$ vector contains M initial cell key derived by the cell c regarding the location of each BS
- $K_a^{BS^{(i)}}$ A unique key shared between each node (a) and the $(i)^{th}$ BS
- $K_c^{d_\omega}$: An authentication key derived by the BS and shared between cell mates in cell c and cell mates in the authentication cell d_ω
- K_{Lc}: The cell key
- $Enc_K\{M\}$: Encryption of a message m using key K
- $MAC_K\{M\}$: The message authentication code of a message M calculated over the key K
- ε: A threshold number of endorsement nodes required to generate a legitimate report

- T: A predefined cell reporter validity
- N: Total nodes in the network
- N': Number of cells in the network
- n: Number of nodes of each cell
- z: Number of cell reporters
- λ: Packet size
- $P_{C\{\varepsilon|z\}}$: The probability of compromising a cell in terms of data confidentiality
- $P_{auth\{\varepsilon|z\}}$: The probability of compromising a cell in terms of data authenticity
- **The report forward route** between a particular cell (c) and the BS contains all cells traversed by a virtual line between them as shown in Fig. 4.3, denoted as dark-grey cells. The highlighted sequence is listed based on the position according to the BS.
- **Report authentication cell**: A particular cell d_ω belongs to the forward report path of cell (c). Its location relative to (c) or the last authentication cell is $t+1$ cells as shown by the light-grey cells depicted in Fig. 4.3. However, there is no authentication cell in the case of a short report authentication route less than $t+1$ cells.

4.5 Setup Phase

Before the deployment process, each sensor node n is loaded by following parameters: $\{K, ID_a, \Delta, p, t, \boldsymbol{S}\}$.

$$\text{Where: } \boldsymbol{S} = [\boldsymbol{S_1} \quad \boldsymbol{S_2}] = \begin{bmatrix} x_0^{(1)} & y_0^{(1)} \\ x_0^{(2)} & y_0^{(2)} \\ . & . \\ . & . \\ . & . \\ x_0^{(M)} & y_0^{(M)} \end{bmatrix}$$

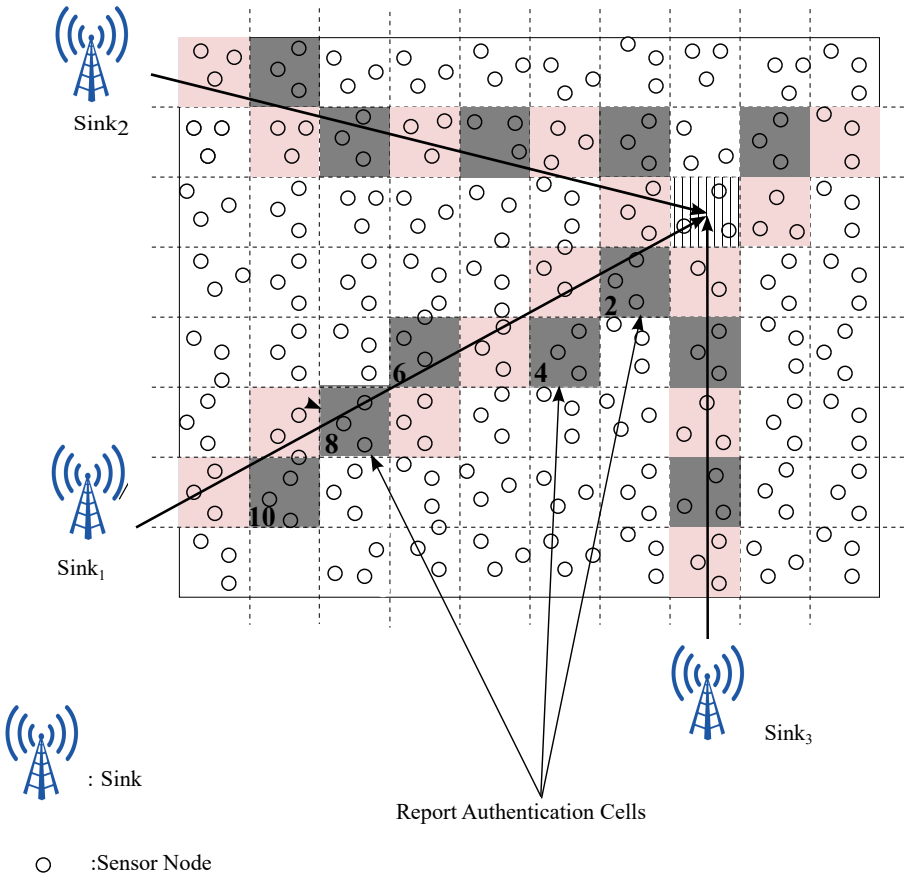


Figure 4.3: Illustration of system construction showing report forward route and authentication cells for a WSN with $M = 3$,$n \simeq 3$ and $t = 2$

Moreover, in order to guarantee the freshness of derived credentials, the setup phase duration is divided into adequate time slots τ depending on each node clock and the WSN application. Using its location and the first BS location as a reference point, each node excludes its cell centre location using Theorem 3.1. Thereafter, based on the location of each node and the preloaded BSs locations, each node derives the matrix of the hosting cell c centre coordinates $\boldsymbol{x_c}$ and $\boldsymbol{y_c}$ by using Algorithm. 3.1. Accordingly, the matrix of initial cell keys $\boldsymbol{K_{Lcin}}$ is derived by all nodes in the cell c as shown in Algorithm. 4.6.

Algorithm 4.6 *Security credentials derivation by each particular node during setup phase*

Require: $K, \boldsymbol{S}, \tau, \Delta, (x_s, y_s)$

$K_\tau \leftarrow K \| \tau$

$\boldsymbol{x_c} \leftarrow 0.5 \left\lceil \frac{x_a - \boldsymbol{S_1}}{\Delta} \right\rceil, \boldsymbol{y_c} \leftarrow 0.5 \left\lceil \frac{y_a - \boldsymbol{S_2}}{\Delta} \right\rceil$

$$\boldsymbol{K_{Lcin}} \leftarrow \begin{bmatrix} H(K_\tau \| \boldsymbol{x_c}(1) \| \boldsymbol{y_c}(1)) \\ H(K_\tau \| \boldsymbol{x_c}(2) \| \boldsymbol{y_c}(2)) \\ . \\ . \\ H(K_\tau \| \boldsymbol{x_c}(M) \| \boldsymbol{y_c}(M)) \end{bmatrix}$$

Ensure: $K_\tau, (\boldsymbol{x_c}, \boldsymbol{y_c}), \boldsymbol{K_{Lcin}}$

Then, each sensor node inside a cell c discovers and creates a list of its cell-mates, which refers to all sensor nodes located inside the same cell. This list is sent each node to the M BSs of the WSN as shown in Algorithm. 4.7.

Algorithm 4.7 *Cell-mate list created by each sensor node n and sent to each BS BS_ℓ : $\ell = 1, 2...M$*

Require: $ID_a, \tau, (x_a, y_a), \boldsymbol{x_c}, \boldsymbol{y_c}, \boldsymbol{S}, \boldsymbol{K_{Lcin}}$
  for each BS BS_ℓ **do**
    $K_{Lcin_\ell} = \boldsymbol{K_{Lcin}}(1, \ell)$
    $n \rightarrow *$: $Enc_{K_{Lcin_\ell}}\{ID_a, \tau, \boldsymbol{x_c}(1, \ell), \boldsymbol{y_c}(1, \ell)\}$
    $\{CellMateList\}_{n,\ell} \equiv \phi$
    for all cell-mates **do**
      $ACK \rightarrow a$
      if ACK is valid **then**
        Update $\{CellMateList\}_{n,\ell}$
      end if
    end for
    $K_a^{BS_\ell} \leftarrow H(K \| ID_a \| x_0^\ell \| y_0^\ell)$
    $\{LIST\}_a \leftarrow \{\boldsymbol{x_c}(1, \ell), \boldsymbol{y_c}(1, \ell), \{CellMateList\}_a,$
      $K_{Lcin_\ell}\}$
    $n \rightarrow BS_\ell$: $Enc_{K_a^{BS_\ell}}\{LIST\}_a$
  end for
Ensure: $K_a^{BS_\ell}, \{LIST\}_a, \{CellMateList\}_a$

After that, a hybrid scheme described in Chapter 3 is followed to govern the communication inside the WSN as:

- The cell-by-cell scheme is followed by each sensor node n during sending the message $\{LIST\}_a$ to all BSs.
- The single hop scheme is followed by all BSs, that have a wide coverage, to correspond with any sensor node n.

Each BS, denoted as BS_ℓ, follows the verification steps shown in Algorithm. 4.8 where receiving a similar message from all nodes in a cell c via a different path indicates the absence of any malicious node in that cell. However, both Algorithm-4 and Algorithm-5 might be implemented to revoke the detected suspicious node and cells in order to overcome the resultant consequences. During its journey from the event cell to the BSs, each message is authenticated by using the en-route-filtering scheme shown in Chapter 3. This is implemented by each filtering cell $d_{i,\ell}$ belonging to each cell c using the authentication key $K_c^{d_{i,\ell}}$ which is derived by the BS_ℓ as shown in Algorithm-4.8. The derivation of this key by the BS helps to decrease the computation cost in contrast with other schemes discussed in Chapter 5

4.6 Report Generation

During the surveillance mission, each node create two types of report:

- Event report: this reports any event happening in the vicinity such as a moving person or vehicle, human voice and temperature change. This report is generated by the sensor node without any BS request and usually contains: cell ID, event location, event occurrence time and event type. It is generated by all n sensor nodes inside the cell c by making use of the signal strength strategy [115].
- Responding report: this is a report created as a response to a request sent by a BS. It is generated by a particular sensor node or by the entire n nodes inside a specific cell. such a report is used to establish routing schemes, authentication cells dedication and revocation of suspected sensors and cells.

While this work focuses on the packet security regardless of the nature of its contents, both reports will be referred to as an incident report $\Re$ throughout the rest of this thesis. In order to thwart outsider attackers, $\Re$ is encrypted by K_{Lc}. However, these attackers might be able to inject fake information or create bogus incidents. Therefore, a rigid endorsement must be enclosed in the generated report. For the MS-LKMP, the following conditions must be available in the incident report to be accepted as an authenticated report:

- The received data from different nodes inside the cell of the event occurrence must be unique.
- A generation of ε MAC generated by the authentication nodes.
- The availability of the cell reporters signature.

The fundamentals of the threshold linear secret sharing scheme (LSSS) [32] is used to achieve the first condition where the unique cell-BS key is employed to calculate the unique sensor node share $\overline{\Re}_a$ of the encrypted incident report $\overline{\Re} = E_{K_{LC}}\{\Re\}$:

$$\overline{\Re}_a = \overline{\Re} \sum_{\imath=0}^{\varepsilon-1} (K_a^{BS_\ell})^\imath \, mod \, p, \tag{4.1}$$

each particular sensor node inside the cell c broadcasts its own share, as a tuble $\{\overline{\Re}_a, n\}$ to all sensor nodes in the cell. As a result, each node collects and then concatenates $n-1$ shares:

$$\overline{\Re}_{Final} = \overline{\Re}_1 \| \overline{\Re}_2 \| \overline{\Re}_n \tag{4.2}$$

To achieve the second condition, multiple MACs are calculated over $\overline{\Re}_{Final}$ by making use of the authentication keys $K_c^{d_{(i,\ell)}}$, which are calculated by the BS ℓ and broadcasted to the authentication cell $d_{(i,\ell)}$ as shown in Algorithm-4.8. Based on these MACs, The en-route filtering scheme [20] is achieved by each authentication cell. As an example, if two authentication cells ($d_{(1,3)}$ and $d_{(2,3)}$) are dedicating to the cell c by the third BS, denoted as BS_3, each node inside c disseminates following packet to the surrounding cell-mates:

$$MAC_{K_{Lc}}\{\Re, MAC_{K_c^{d_{(1,3)}}}(\overline{\Re}_{Final}), MAC_{K_c^{d_{(2,3)}}}(\overline{\Re}_{Final})\} \tag{4.3}$$

Thereafter, if the sensor node n receives $i(n-1)$ MACs (i: number of authentication cells), n creates the synthesized incedent report which includes the ID list of all cell-mates, the ID of the event cell $\overline{\Re}_{Final}$ and i of MACs. Then, the random timer procedure [78] is utilised to prevent any possible duplication in the generated incident report.

The third condition, which is the most important endorsement presented in MS-LKMP ,is the signature generated by the set of z cell reporters which are selected randomly (out of the total n sensor nodes) by a BS or a set of BSs as will be discussed briefly in following section.

4.7 Key Revocation

As shown in Algorithm-4.8, any suspicious node or cell is listed in the *SusbNodes*, *SubCells* lists respectively. Such a node/cell has an ability to threaten the entire WSN security. Therefore, this section presents two schemes proposed to revocate any element that is identified as suspicious or compromised. These schemes are significantly important in order to prevent any possible colluding between the suspicious elements. Accordingly,

Algorithm 4.8 *BS_ℓ verification of the $\{LIST\}_a$ packages sent by each node.*

Require: $\{LIST\}_a : n = 1, 2..., N$
  $COUNT = 0; SuspNodes \equiv \phi$
  for $n = 1, 2..., N$ **do**
    BS extracts ID_a from the header of $\{LIST\}_a$
    $K_a^{BS_\ell} \leftarrow H(K \| ID_a \| x_0^\ell \| y_0^\ell)$
    $Dec_{K_a^{BS_\ell}}\{LIST\}_a = \{\boldsymbol{x_c}(\ell), \boldsymbol{y_c}(\ell),$
      $\{CellMateList\}_a, K_{Lcin_\ell}\}$
    $ID_c = 10\boldsymbol{x_c}(\ell) + \boldsymbol{y_c}(\ell)$
    $Num = Length\{LIST\}_a$
    if $\{LIST\}_a \equiv \{LIST\}_{n-1}$ **then**
      $Num = Num + 1$
    else
      $SuspNodes \leftarrow n$
    end if
  end for
  if $COUNT \geq \lfloor 0.5Num \rfloor + 1$ **then**
    Call $Algorithm(4)$
  else if $COUNT < \lfloor 0.5Num \rfloor + 1$ **then**
    $SuspCells \leftarrow ID_c$
    Call $Algorithm(5)$
  else
    $K_{Lc} \equiv K_{Lcin_\ell}$
    $\{LIST\}_c = \{LIST\}_a \cup ID_a$
    $BS_\ell \rightarrow n : Enc_{K_q^{BS_\ell}}\{K_{Lc}, \{LIST\}_c\}$
    if $BS_\ell \leftarrow n : ACK$ **then**
      $K_c^{d_{(i,\ell)}} = H(K_{Lc} \| K_{Ld_{(i,\ell)}} \| \boldsymbol{x_{d_{(i,\ell)}}} \| \boldsymbol{y_{d_{(i,\ell)}}} \| \boldsymbol{x_c}(\ell) \| \boldsymbol{y_c}(\ell))$
      $BS_\ell \rightarrow n \in c : \{d_{(i,\ell)}\} \cup \{K_c^{d_{(i,\ell)}}\}$
    end if
  end if
Ensure: $K_a^{BS_\ell}, SuspNodes, SuspCells, K_{Lc}, \{LIST\}_c$
  $, \{d_{(i,\ell)}\}, \{K_c^{d_{(i,\ell)}}\}$

every BS BS_ℓ calls the Algorithm-4.9 to revoke the credentials of every sensor node $s \in SusbNodes$. On the other hand, each BS BS_ℓ follows Algorithm-4.10 to revocated each cell $c \in SusbCells$.

Algorithm 4.9 *Revocation process implementation of the BS BS_ℓ for each suspicious sensor node $(n) \in SuspNodes$ of the cell (c) .*

Require: $ID_n \in SusbNodes, ID_c, K_{Lc}, K_c^{d_{i,\ell}} : i = 1, 2...t$
$\{LIST\}_{new} = \forall ID_n(ID_n \in \{LIST\}_c \bigwedge ID_n \neq ID_c)$
$K_{Lc\_new} \leftarrow H(\boldsymbol{x_c}(\ell)\|\|\boldsymbol{y_c}(\ell)ts\|\{LIST\}_{new})$
$K_c^{d_{i,\ell}} = H(K_{Lc\_new}\|K_{Ld_{i,\ell}}\|(x_{d_{i,\ell}}, y_{d_{i,\ell}})\|\boldsymbol{x_c}(\ell)\|\boldsymbol{y_c}(\ell))$
for $\forall n(n \in \{LIST\}_{new}$ **do**
$BS_\ell \rightarrow n : \{K_{Lc\_new}, ID_c, K_c^{d_{i,\ell}} : i = 1, 2...t\}$
end for
$RemoveK_c^{BS_\ell}$
Ensure: $\{LIST\}_{new}, K_{Lc\_new}, K_c^{d_{i,\ell}} : i = 1, 2...t\}$

Algorithm 4.10 *Revocation process implementation of the BS BS_ℓ for each suspicious cell (c).*

Require: $ID_c, K_{Lc}, K_c^{d_{i,\ell}} : i = 1, 2...t$
Remove $K_c^{BS_\ell}$
for $\forall d_{i,\ell} : i = 1, 2...t$ **do**
Remove $K_c^{d_{i,\ell}}\}$
end for

4.8 Security Analysis of LKMP-MBS

The main purpose of this Chapter is to analyse the security of LKMP-MBS and compare it with the LKMP-SBS to investigate the feasibility of using multiple BSs in terms of data security. On the same hand, MKMP-SBS is compared with the MKMP [21] based on following aspects:

1. The role of both the number of cell reporters ($z^{(\ell)}$), selected by each BS, and the number of BSs (M) in the security of each particular cell.

2. The system rigidity in terms of wireless security requirements for data confidentiality and authenticity.

The second point will be investigated using the likelihood of compromising the entire WSN as a result of launching a Random Node Capture Attack (RNCA). This likelihood is measured by the percentage of compromised cells and presented by a graph depicting

the relationship between the total number of compromised nodes versus the percentage of compromised cells. The outcome of the last point is the cornerstone of Section 4.9, which investigates the optimum value of $(z^{(\ell)})$.

4.8.1 Security Strength in Terms of Data Confidentiality

The contents of the incident report $\Re$ generated inside a cell c is only revealable by the sensor nodes located in that cell due to its encryption by the K_{Lc}. This guarantees the data confidentiality even when a number of intermediate nodes are compromised. However, if one of the nodes involved in report generation is compromised, the report contents could be revealed. In order to investigate the security robustness of MS-LKMP in terms of data confidentiality, the impact of the RNCA is investigated. The cell is considered compromised if and only if:

1. The threshold number ε of nodes are compromised.
2. All the $z^{(\ell)}$ cell reporters, belonging to each particular BS, are compromised.

Accordingly, the expression of $P_{C\{\varepsilon|z\}}$ is derived for MS-LKMP as:

$$P_{C\{\varepsilon|z\}} = (1 - P_{\varepsilon\{0\}})(1 - P_{z\{0\}}) \tag{4.4}$$

While the first condition is not related to the number of BSs or to $z^{(\ell)}$, the same expression derived in Chapter 3 as (3.20) is followed to determine $P_{\varepsilon\{0\}}$ as:

$$P_{\varepsilon\{0\}} = \frac{\binom{N-\varepsilon}{x}}{\binom{N}{x}} \tag{4.5}$$

The second term, $P_{z\{0\}}$, is analysed regarding each particular BS. This is achieved for the ℓ^{th} BS by assuming that x nodes are compromised out of a total of N nodes in the network, so the adversary has $\binom{N}{x}$ methods to compromise x nodes. Additionally, inside each cell there are $\binom{n}{z^{(\ell)}}$ different methods to create a report endorsed by whole cell reporters. The total number of different methods to implement both processes is $\binom{N}{x}\binom{n}{z^{(\ell)}}$. Regarding the whole network, suppose j nodes out of $z^{(\ell)}$ cell reporters are compromised. Then the adversary picks $z^{(\ell)}$ nodes randomly out of n sensor nodes, captures j nodes out of the $z^{(\ell)}$ nodes participating in the report generation and then compromises $(x - j)$ out

of $(N - z^{(\ell)})$ nodes as a final step. The resultant probability P_j of capturing j nodes out of $z^{(\ell)}$ endorsement nodes is:

$$\begin{aligned} P^{(\ell)}_{z\{j\}} &= \frac{\binom{N}{z^{(\ell)}}\binom{z^{(\ell)}}{j}\binom{N-z^{(\ell)}}{x-j}}{\binom{N}{x}\binom{N}{z^{(\ell)}}} \\ &= \frac{\binom{z^{(\ell)}}{j}\binom{N-z^{(\ell)}}{x-j}}{\binom{N}{x}} \\ \Rightarrow P^{(\ell)}_{z\{0\}} &= \frac{\binom{N-z^{(\ell)}}{x}}{\binom{N}{x}} \end{aligned} \tag{4.6}$$

Regarding only a single BS, $BS^{(1)}$, the probability of a particular cell to be compromised is calculated as the probability of compromising all its cell reporter as: $(1 - P^{(\ell)}_{z\{j\}})$. As a result, the probability for a particular cell to be compromised by capturing all BSs' cell reporters P_z is calculated as:

$$P_z = (1 - P^{(1)}_{z\{0\}})(1 - P^{(2)}_{z\{0\}}) \cdots (1 - P^{(\ell)}_{z\{0\}})$$

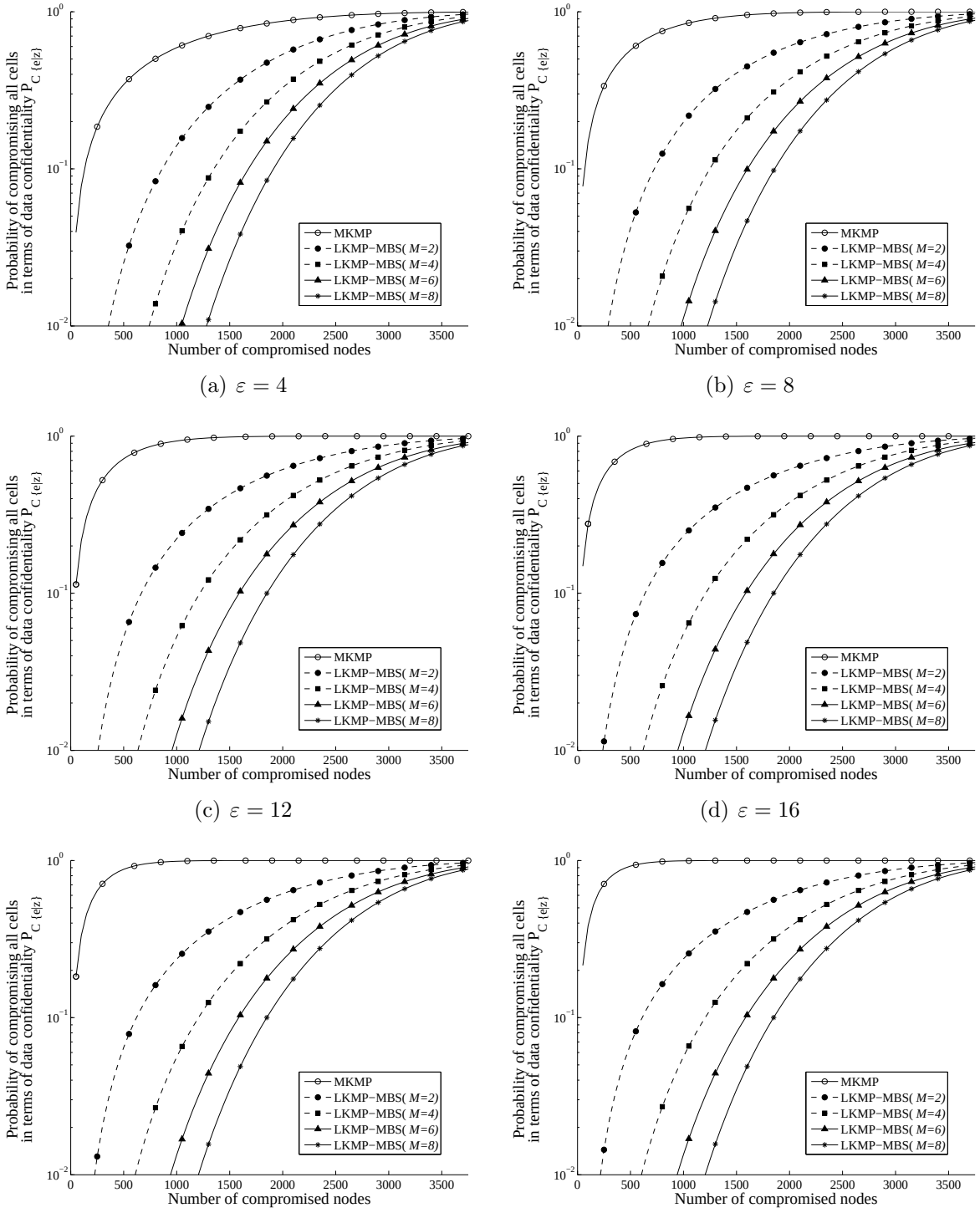
Seeking for simplicity, $z^{(\ell)}$ is assumed to be similar for all values of ℓ, as a result:

$$P_{C\{\varepsilon|z\}} = \left(1 - \frac{\binom{N-\varepsilon}{x}}{\binom{N}{x}}\right) \prod_{\ell=1}^{M} \left(1 - \frac{\binom{N-z^{(\ell)}}{x}}{\binom{N}{x}}\right) \tag{4.7}$$

This equation is one of the main findings of this Chapter where it is used to test the robustness of LKMP-MBS in terms of data confidentiality in terms of different parameters. Moreover, it is significantly used to determine the optimum number of cell reporters $z^{(\ell)}$ as shown in Section 4.9. For different values of N, n and M, the percentage of captured cells regarding data confidentiality in terms of the number of compromised nodes is shown in Fig. 4.4, 4.5, 4.6 and 4.7. Figures are plotted based on simulation results collected from the environment built by the Contiki OS Cooja simulator [127] and analysed by MATLAB following Monte Carlo simulation concepts [128] which are perfectly match the analytical results gained by using (4.7). These figures show that:

1. The security of LKMP-MBS in terms of data confidentiality, $P_{C\{\varepsilon|z\}}$, is observed to be proportional to the values of z.

2. LKMP-MBS outperforms MKMP for any value of (N,ε and z).

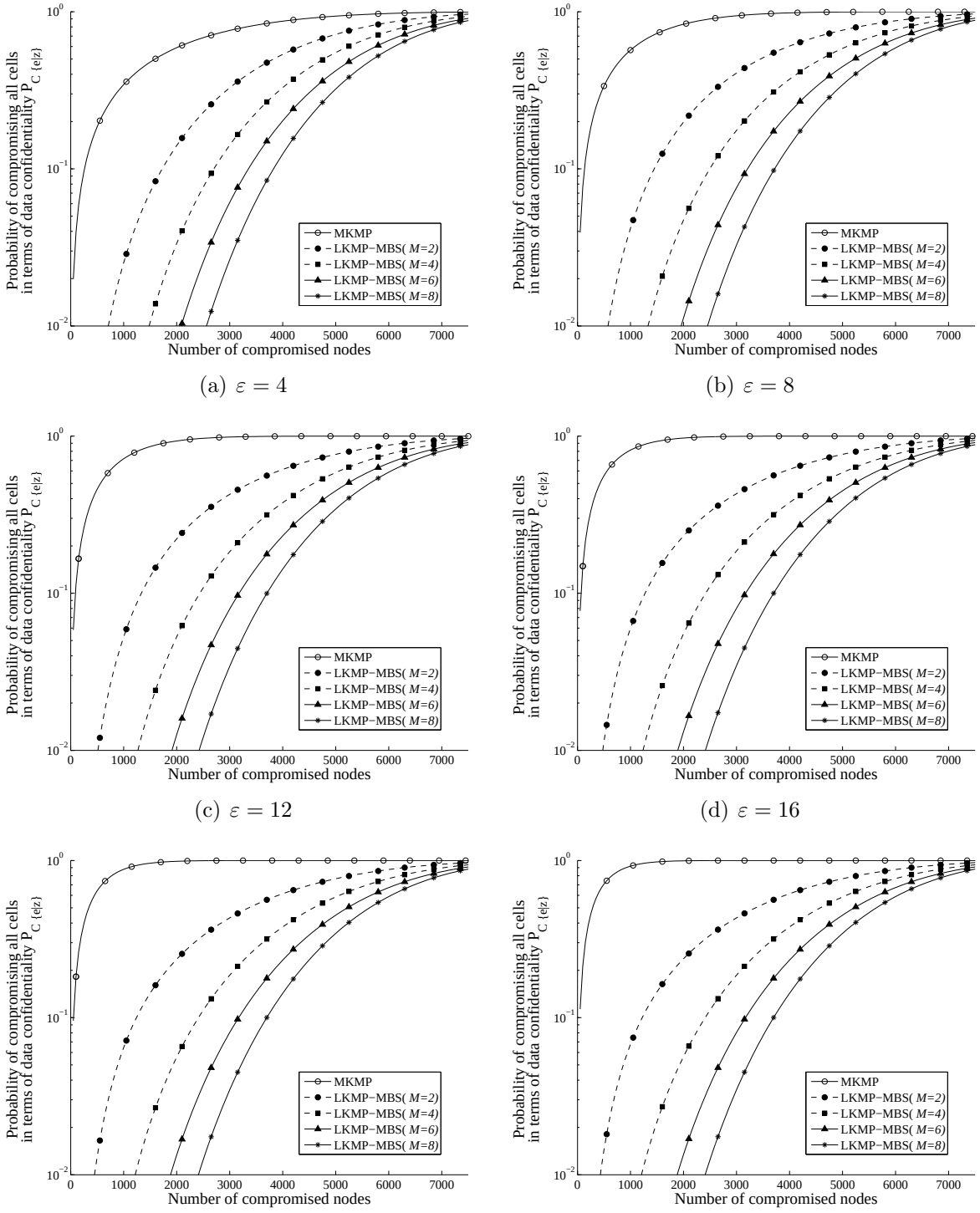


(a) $\varepsilon = 4$ (b) $\varepsilon = 8$

(c) $\varepsilon = 12$ (d) $\varepsilon = 16$

(e) $\varepsilon = 20$ (f) $\varepsilon = 24$

Figure 4.4: Data confidentiality of LKMP-MBS and MKMP under random node capture attack in a WSN consist of $N = 5,000$, $z = 3$ and for different values of ε.

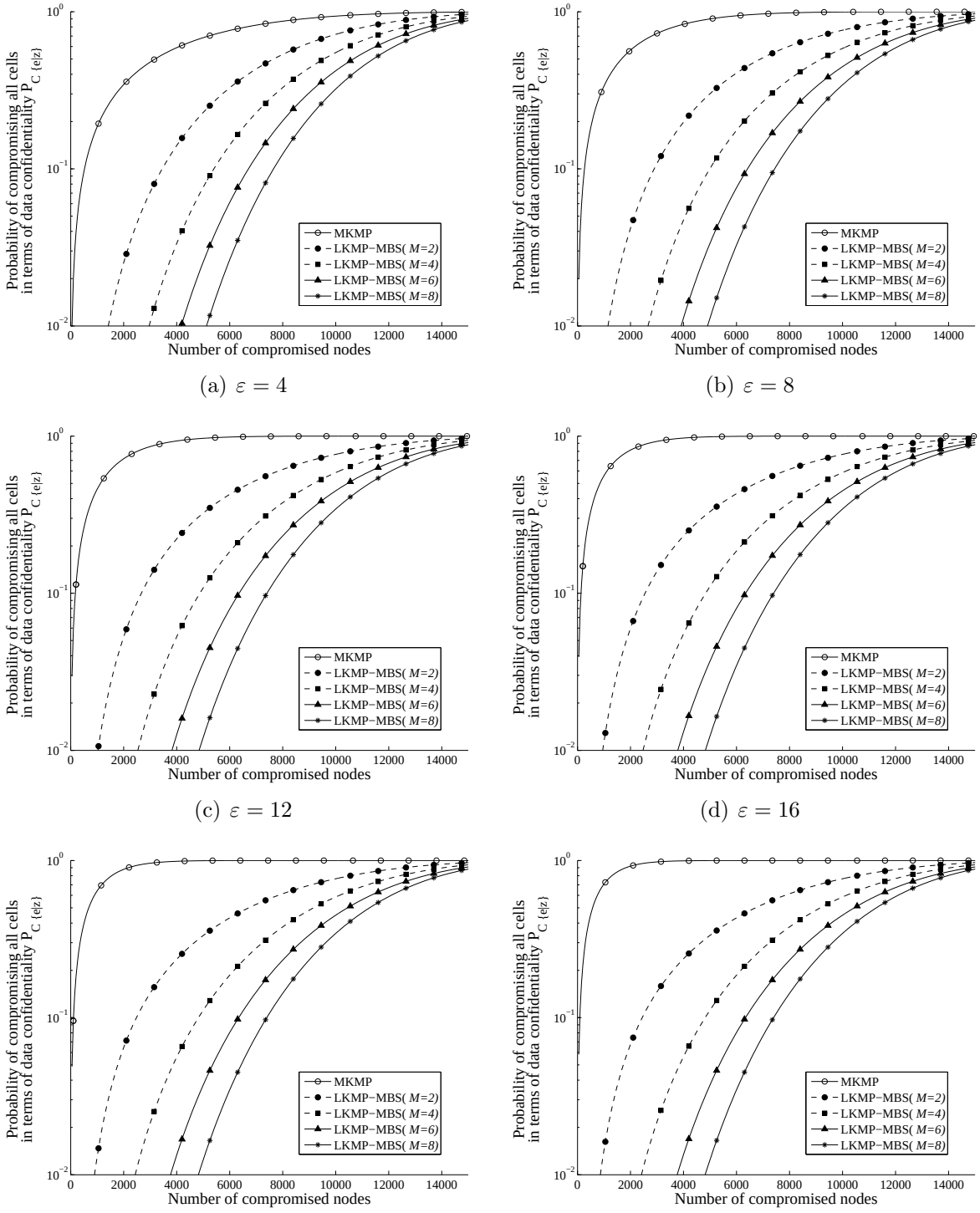


(a) $\varepsilon = 4$ (b) $\varepsilon = 8$

(c) $\varepsilon = 12$ (d) $\varepsilon = 16$

(e) $\varepsilon = 20$ (f) $\varepsilon = 24$

Figure 4.5: Data confidentiality of LKMP-MBS and MKMP under random node capture attack in a WSN consist of $N = 10,000$, $z = 3$ and for different values of ε.

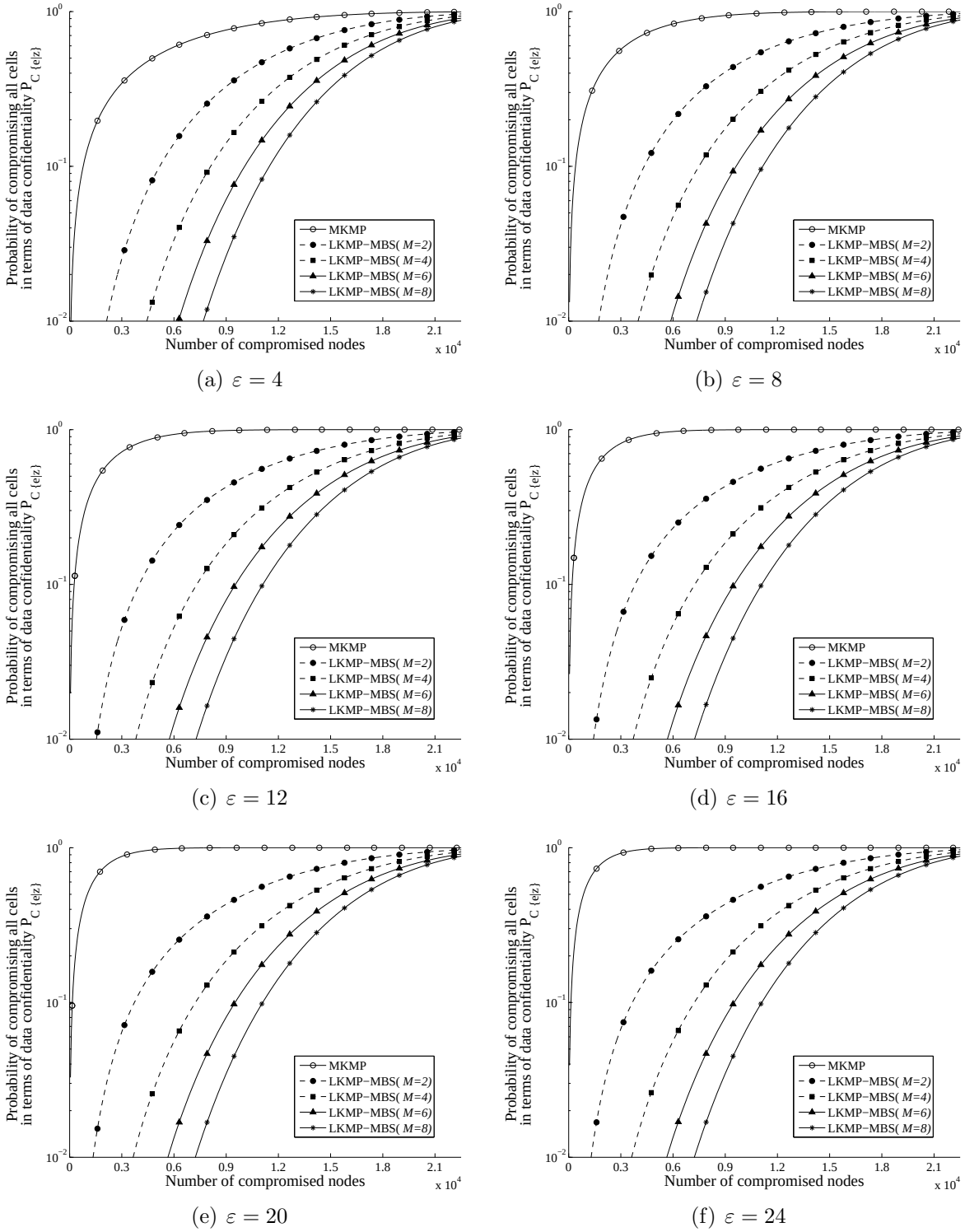


(a) $\varepsilon = 4$ (b) $\varepsilon = 8$

(c) $\varepsilon = 12$ (d) $\varepsilon = 16$

(e) $\varepsilon = 20$ (f) $\varepsilon = 24$

Figure 4.6: Data confidentiality of LKMP-MBS and MKMP under random node capture attack in a WSN consist of $N = 20,000$, $z = 3$ and for different values of ε.



(a) $\varepsilon = 4$ (b) $\varepsilon = 8$

(c) $\varepsilon = 12$ (d) $\varepsilon = 16$

(e) $\varepsilon = 20$ (f) $\varepsilon = 24$

Figure 4.7: Data confidentiality of LKMP-MBS and MKMP under random node capture attack in a WSN consist of $N = 30,000$, $z = 3$ and for different values of ε.

The behaviour of the relationship between x and $P_{C\{\varepsilon|z\}}$ is the same for any value of N and ε where $P_{C\{\varepsilon|z\}}$ is increasing as x increments. However, the curve slope varies depending on N and ε. These differences are depicted in Fig. 4.8 and Fig. 4.9 respectively. The two figures showing that:

$$P_{C\{\varepsilon|z\}} = f(\frac{1}{N}, \varepsilon) \tag{4.8}$$

The following two sections discuss and explains the mathematical proof of (4.8).

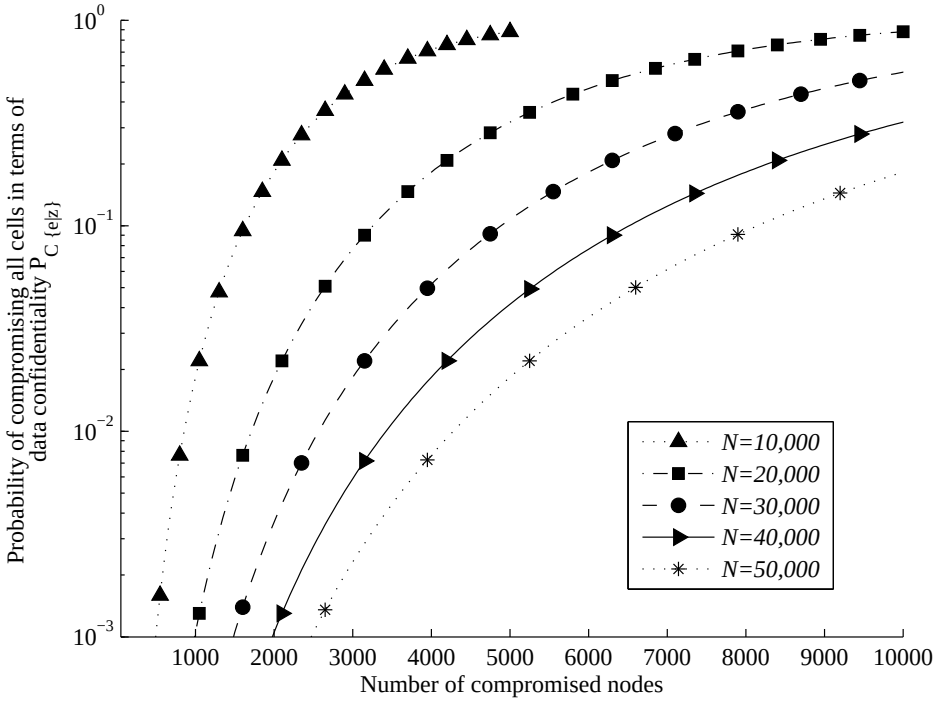


Figure 4.8: The effect of changing the number of nodes in the network N on the probability of compromising all cells in terms of data confidentiality due to RNCA, $M = 4$,$\varepsilon = 10$ and $z = 5$.

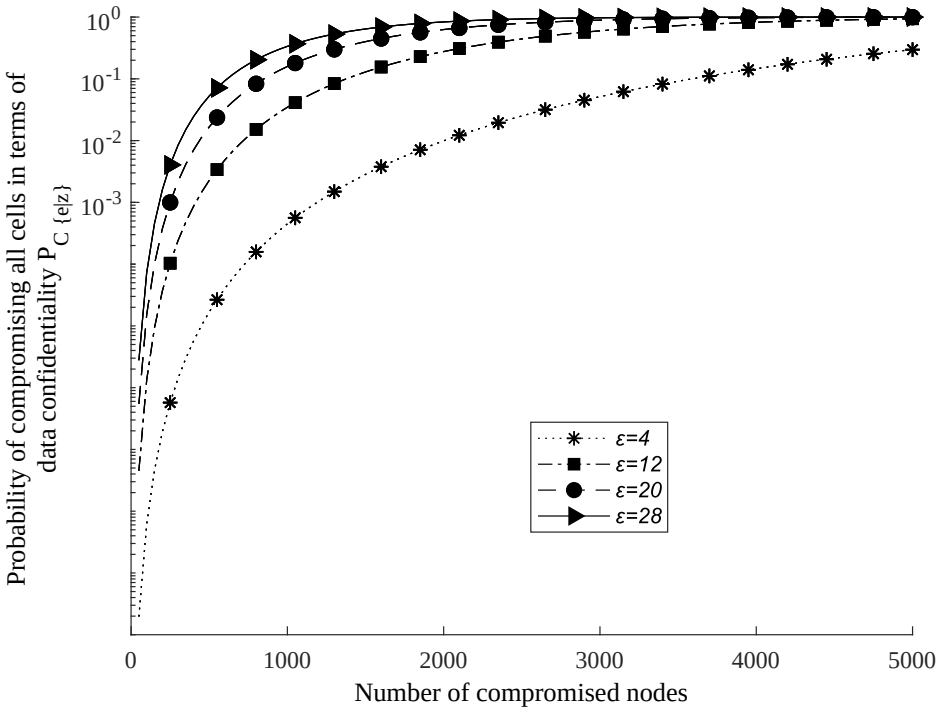


Figure 4.9: The effect of changing the number of endorsement nodes in the network ε on the probability of compromising all cells in terms of data confidentiality due to RNCA, $N = 10,000$, $M = 4$ and $z = \frac{\varepsilon}{2}$.

- **The effect of N on the value of $P_{C\{\varepsilon|z\}}$ in LKMP-MBS**

  As mentioned in Section 4.8, the ratio of compromised cells caused by implementing the RNCA is the metric used to measure the robustness of the LKMP-MBS in terms of data confidentiality. However, assuming the number of nodes in each cell is constant, increasing N leads to increasing the number of total cells. As a result, increasing the value of N decreases the ratio of compromised cells and leads to improving the security of the system in terms of data confidentiality. The mathematical proof of (4.8) is achieved from (4.7) as:

  Proof 4.1

$$\begin{aligned} P_{C\{\varepsilon|z\}} &= \left(1 - \frac{\binom{N-\varepsilon}{x}}{\binom{N}{x}}\right) \prod_{\ell=1}^{M} \left(1 - \frac{\binom{N-z^{(\ell)}}{x}}{\binom{N}{x}}\right) \\ &= P_1 P_2 \\ \Rightarrow P_{C\{\varepsilon|z\}} &= f(P_1, P_2) \end{aligned} \tag{4.9}$$

  Regarding (4.9), it is proved that $P_1 = f(\frac{1}{N})$ in Chapter 3.

On the other hand :

$$P_2 = \prod_{\ell=1}^{M} \left(1 - \frac{\binom{N-z^{(\ell)}}{x}}{\binom{N}{x}}\right)$$

$$\because \left(1 - \frac{\binom{N-z^{(\ell)}}{x}}{\binom{N}{x}}\right) > 0 \text{ for all } \ell$$

$$\therefore P_2 \propto \left(1 - \frac{\binom{N-z^{(\ell)}}{x}}{\binom{N}{x}}\right)$$

$$P_2 \propto \frac{\binom{N}{x}}{\binom{N-z^{(\ell)}}{x}}$$

$$\propto \frac{\frac{N!}{x!(N-x)!}}{\frac{(N-z^{(\ell)})!}{x!(N-z^{(\ell)}-x)!}} \tag{4.10}$$

$$\frac{N!}{x!(N-x)!} \cdot \frac{x!(N-z^{(\ell)}-x)!}{(N-z^{(\ell)})!} = \frac{(N-z^{(\ell)})! \prod_{i=1}^{z^{(\ell)}} (N-z^{(\ell)}+i)(N-z^{(\ell)}-x)!}{(N-z^{(\ell)})!(N-x-z^{(\ell)})! \prod_{i=1}^{x+z^{(\ell)}} (N-z^{(\ell)}-x+i)}$$

$$= \frac{\prod_{i=1}^{z^{(\ell)}} (N-z^{(\ell)}+i)}{\prod_{i=1}^{x+z^{(\ell)}} (N-z^{(\ell)}-x+i)}$$

$$= \frac{1}{\prod_{i=1}^{x} (N-x-z^{(\ell)}+i)} \quad \text{for } N, x \text{ and } n \in \mathbb{N}$$

$$= \frac{1}{N^x - a_1 N^{x-1} + a_2 N^{x-2} - \cdots a_x N} \tag{4.11}$$

Where: $b_1, b_2 \cdots b_x$ are constants in terms of N.

From both (4.10) and (4.11):

$$P_2 = f(\frac{1}{N})$$

$$\Rightarrow P_{C\{\varepsilon|z\}} = f(\frac{1}{N}) \tag{4.12}$$

■

- **The effect of ε on the value of $P_{C\{\varepsilon|z\}}$ in LKMP-MBS**

  There are two reasons for the relationship between ε and $P_{C\{\varepsilon|z\}}$:

  1. Increasing the number of endorsement nodes with keeping a constant value of $z^{(\ell)}$ selected by each BS increase the likelihood of generating a fake report from that cell.

2. Increasing ε will need an increment in the value of n which leads to a decrease in the number of cells in the WSN assuming the total number of nodes N in the WSN is constant. Hence, the ratio of compromised cells is increased, which reduces the security level of the system in terms of data confidentiality.

The same mathematical proof shown in 3.8.3.2 is considered while the ε- dependent parts of both (3.21) and (4.7) are the same.

- **The effect of $z^{(\ell)}$ on the value of $P_{C\{\varepsilon|z\}}$ in LKMP-MBS**

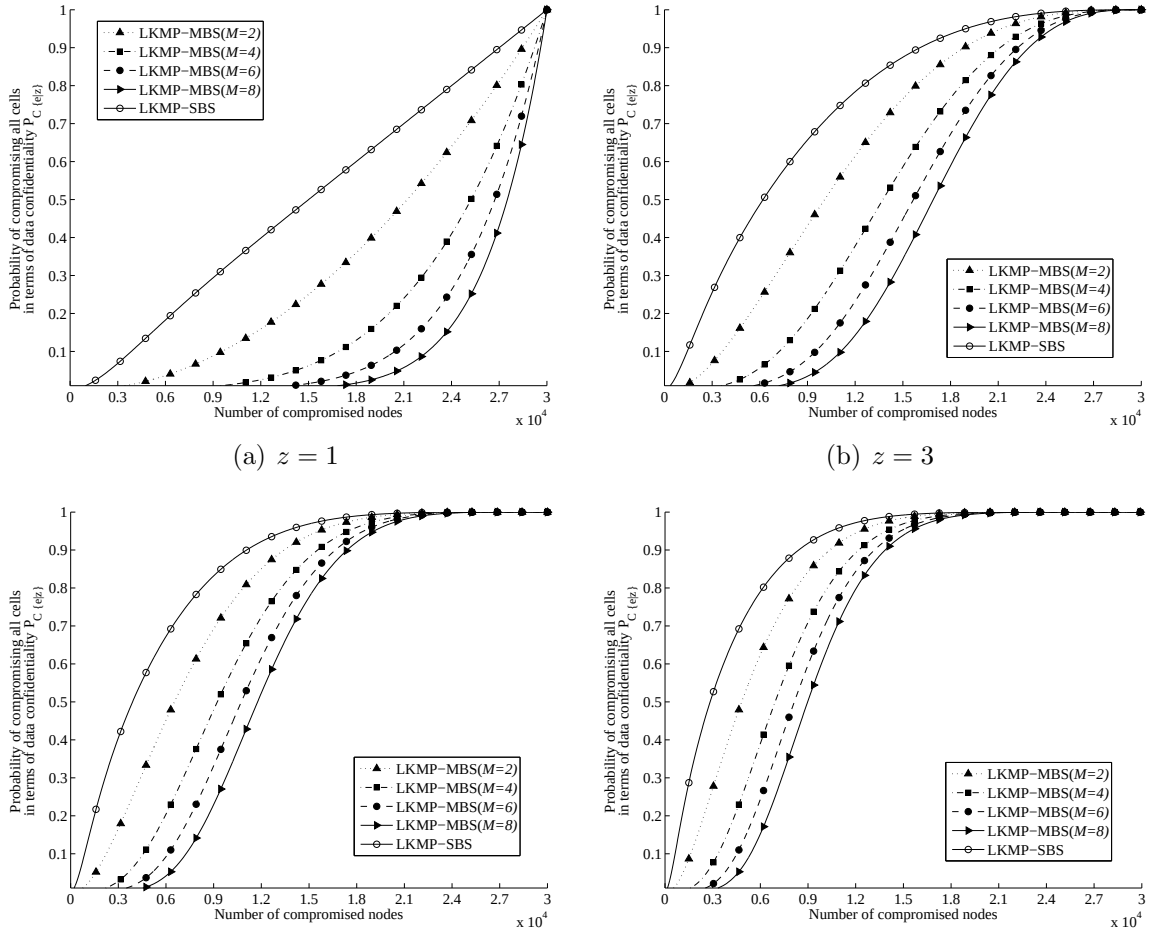
In contrast to the LKMP-SBS, described in the previous Chapter, LKMP-MBS shows a lower value of $P_{C\{\varepsilon|z\}}$ for all values of x. These values are varies based on the number of cell reporters $z^{(\ell)}$ selected by each BS. This attitude is the same for variable N and ε. A WSN consisting of $N = 5,000$, $n = 10$ and $M = 4, 6, 8$ performance in terms of $P_{C\{\varepsilon|z\}}$ is depicted in Fig. 4.10 where $z = 1, 3, 5, 9$:

It is obvious that the improvement in $P_{C\{\varepsilon|z\}}$ is proportional to the number of BSs. This is due to the increment in the difficulty of compromising a particular cell when more BSs are involved. For any adversary, it is crucial to compromise all z cell reporters selected by all BSs rather than compromising one set of cell reporters as described in LKMP-SBS.

4.8.2 Security Strength in Terms of Data Authenticity

Inside any particular cell, data authenticity is compromised if the attacker succeeds in capturing the threshold number of sensor nodes which allow him\ her to generate a fake event report and send it to the BS(s). Once a message is received by any particular node, it can be forwarded if that node has the ability to recover ε MAC addresses, as explained in (4.2). In order to present our system robustness in terms of data authenticity, (4.15) is derived using Bayes' theorem [116] to calculate the probability of an event resulting from two events:

- An event of compromising ε and send a bogus report signed by the whole ε nodes. The probability of this event $P_{auth\{\varepsilon\}}$ is calculated by assuming that x nodes are compromised. Then, as the probability of a cell not affected has been derived in (4.5) as: $P_{\varepsilon\{0\}} = \frac{\binom{N-\varepsilon}{x}}{\binom{N}{x}}$ the probability of generating a bogus report by ε compromised sensor nodes then sending it to the BS(s) along with all credentials can by illustrated



(a) $z = 1$ (b) $z = 3$

(c) $z = 5$ (d) $z = 7$

Figure 4.10: Comparison between LKMP-MBS and LKMP-SBS for different values of M in terms of $P_{C\{\varepsilon|z\}}$ due to a RNCA in a WSN consisting of $N = 5,000$, $z = 1, 3, 5, 7$ and $n = Mz + 3$.

as

$$P_{auth\{\varepsilon\}} = \sum_{j=1}^{\varepsilon} \frac{\binom{\varepsilon}{j}\binom{N-\varepsilon}{x-j}}{\binom{N}{x}} \tag{4.13}$$

- An event of sending a bogus report signed by the whole $z^{(\ell)}$ cell reporters selected by all BSs. First of all, the probability of generating such a report signed by only one BS's cell reporters set, $BS^{(1)}$, is derived by following the same analysis of the

previous point as:

$$P^{1}_{auth\{z\}} = \sum_{j=1}^{z} \frac{\binom{z}{j}\binom{N-z}{x-j}}{\binom{N}{x}} \tag{4.14}$$

Accordingly, the probability $P_{auth\{z\}}$ of sending a bogus report signed by all BSs' cell reporters is calculated as:

$$P_{auth\{z\}} = P^{1}_{auth\{z\}} P^{2}_{auth\{z\}} \cdots P^{(\ell)}_{auth\{z\}}$$

For simplicity, $z^{(\ell)}$ is assumed to be similar for all values of ℓ and as a result the fraction of compromised cell caused by compromising x nodes in terms of data authenticity is written as:

$$P_{auth\{e|z\}} = \sum_{j=1}^{\varepsilon} \frac{\binom{\varepsilon}{j}\binom{N-\varepsilon}{x-j}}{\binom{N}{x}} \prod_{\ell=1}^{M} \sum_{j=1}^{z^{(\ell)}} \frac{\binom{z^{(\ell)}}{j}\binom{N-z^{(\ell)}}{x-j}}{\binom{N}{x}} \tag{4.15}$$

For different values of N, n and z, the percentage of captured cells concerning data authenticity in terms of the number of compromised nodes is shown in Fig. 4.11, 4.12, 4.13, 4.14, 4.15, 4.16, 4.17, 4.18, 4.19, 4.20, 4.21 and 4.22. These figures show that:

1. The fraction of captured cells, measured as $P_{auth\{\varepsilon|z\}}$, increases with the number of captured nodes.

2. $P_{auth\{\varepsilon|z\}}$ is found to be proportional to the value of M. As a result, LKMP-MBS shows a better performance in comparison to LKMP-SBS.

3. LKMP-MBS clearly outperforms MKMP in terms of data authenticity for all values of x, M, N and n.

4. LKMP-MBS overcomes the shortage of LKMP-SBS related to the comparison with the performance of LEDS. For all values of $M > 2$, LKMP-MBS outperforms LEDS in terms of $P_{auth\{\varepsilon|z\}}$. However, only when $M = 2$, LKMP-MBS outperforms LEDS when x exceeds a threshold value x_t as reflected in Table. 4.1. It is obvious that even when $M = 2$ LKMP-MBS show a significant improvement in terms of x_t which means that the usage of multiple BSs give better performance in comparison to LEDS even when a lower number of nodes are compromised.

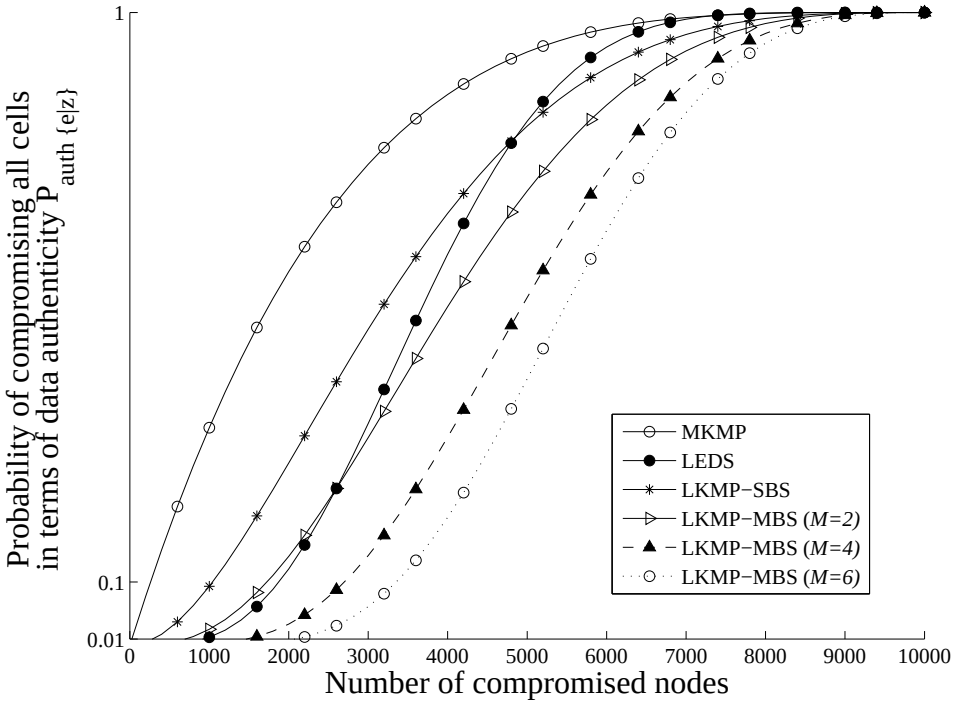


Figure 4.11: Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 10,000$, $\varepsilon = 4$ and $z = 3$.

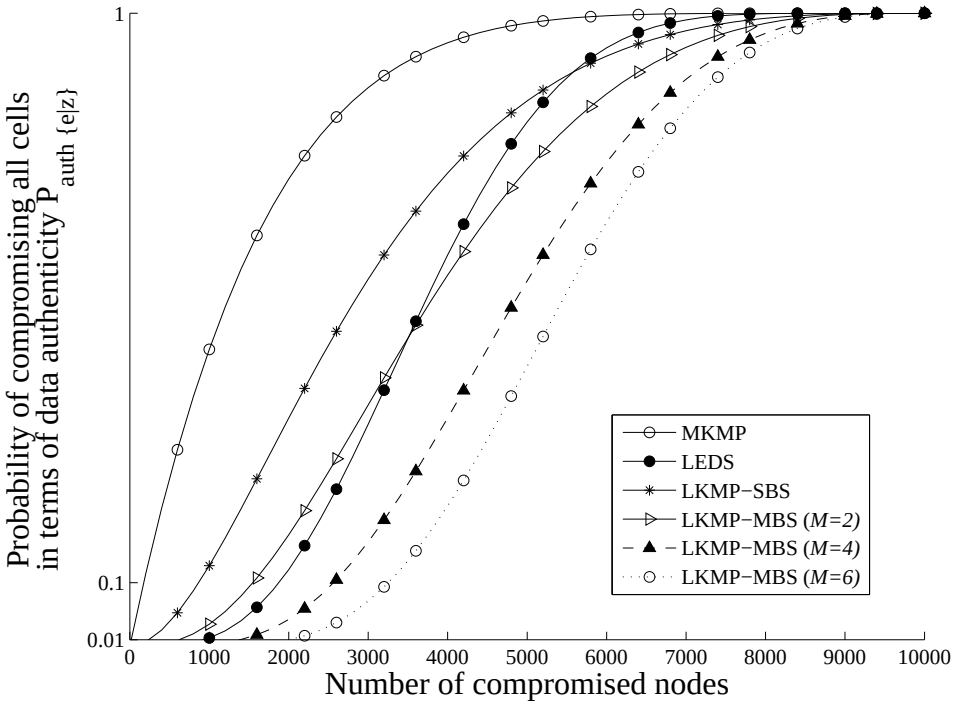


Figure 4.12: Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 10,000$, $\varepsilon = 6$ and $z = 3$.

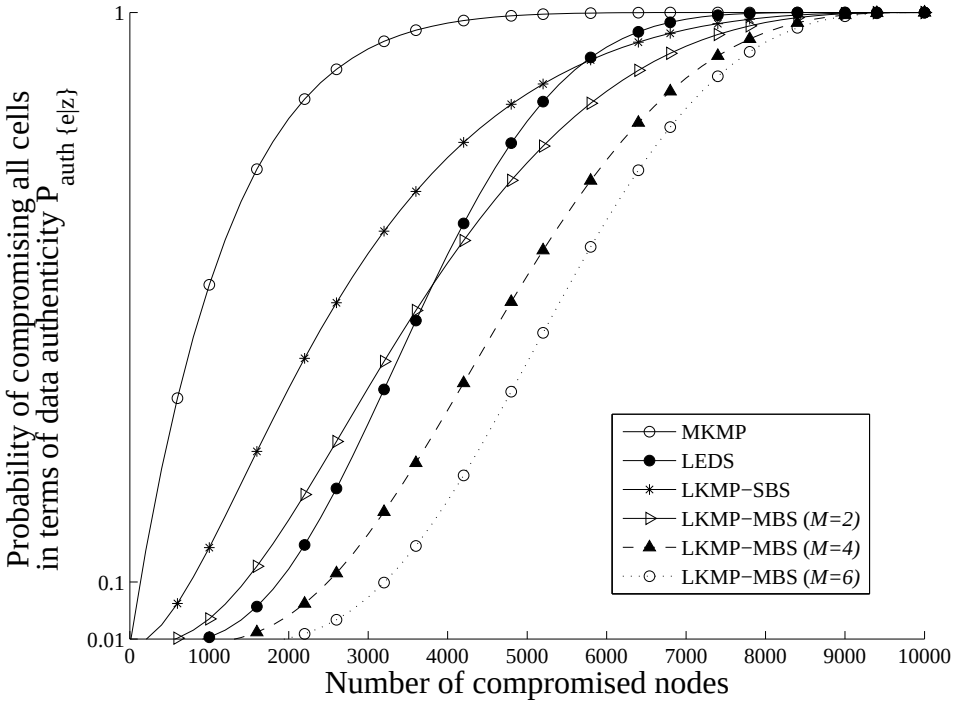


Figure 4.13: Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 10,000$, $\varepsilon = 8$ and $z = 3$.

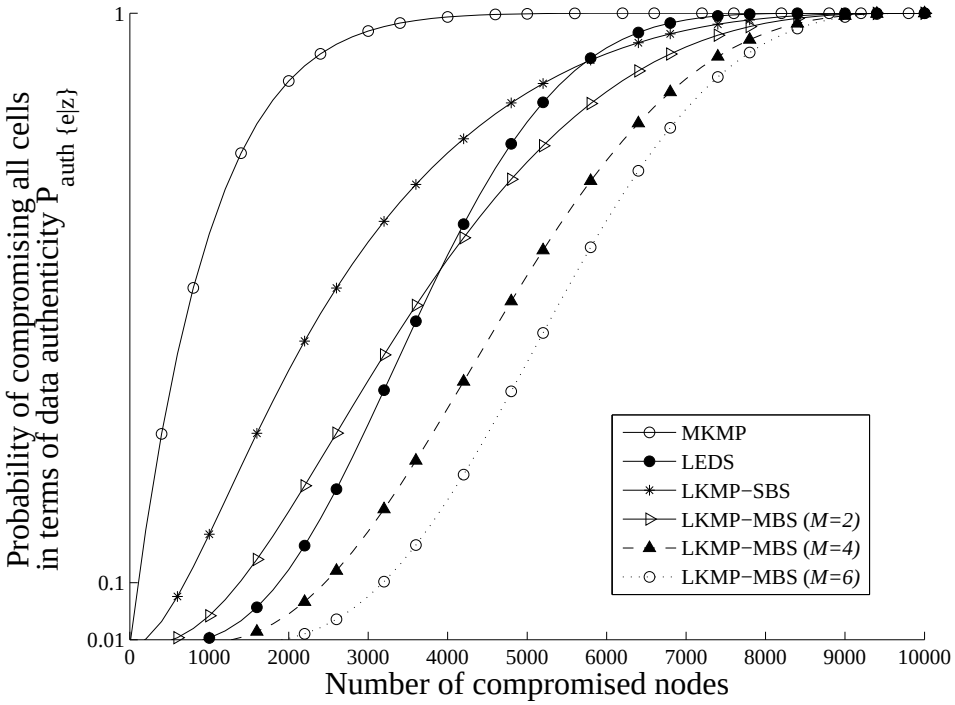


Figure 4.14: Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 10,000$, $\varepsilon = 10$ and $z = 3$.

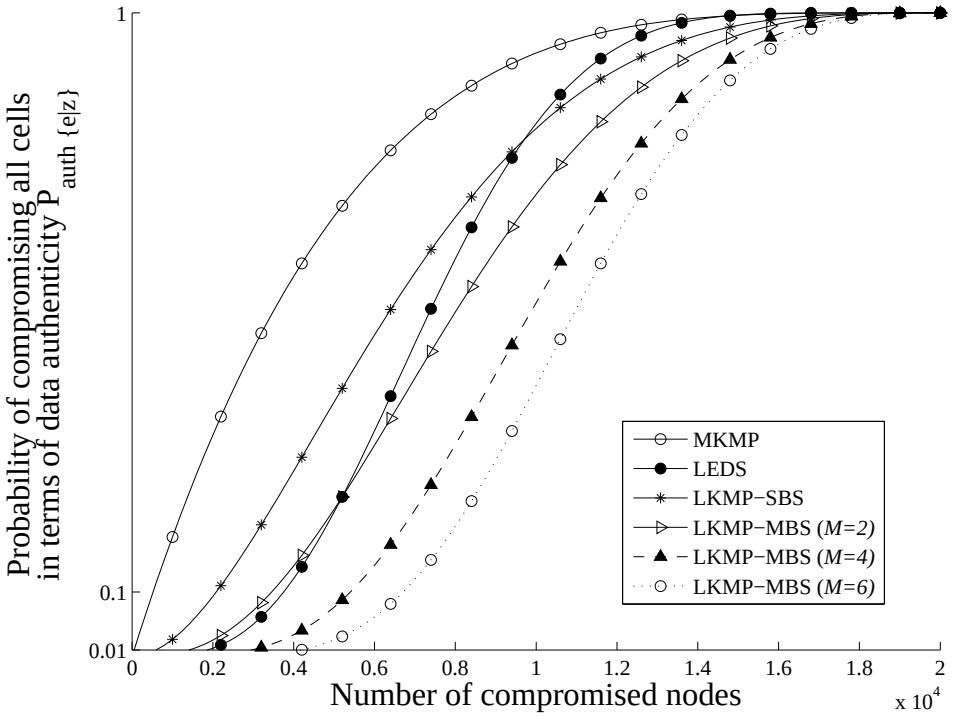


Figure 4.15: Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 20,000$, $\varepsilon = 4$ and $z = 3$.

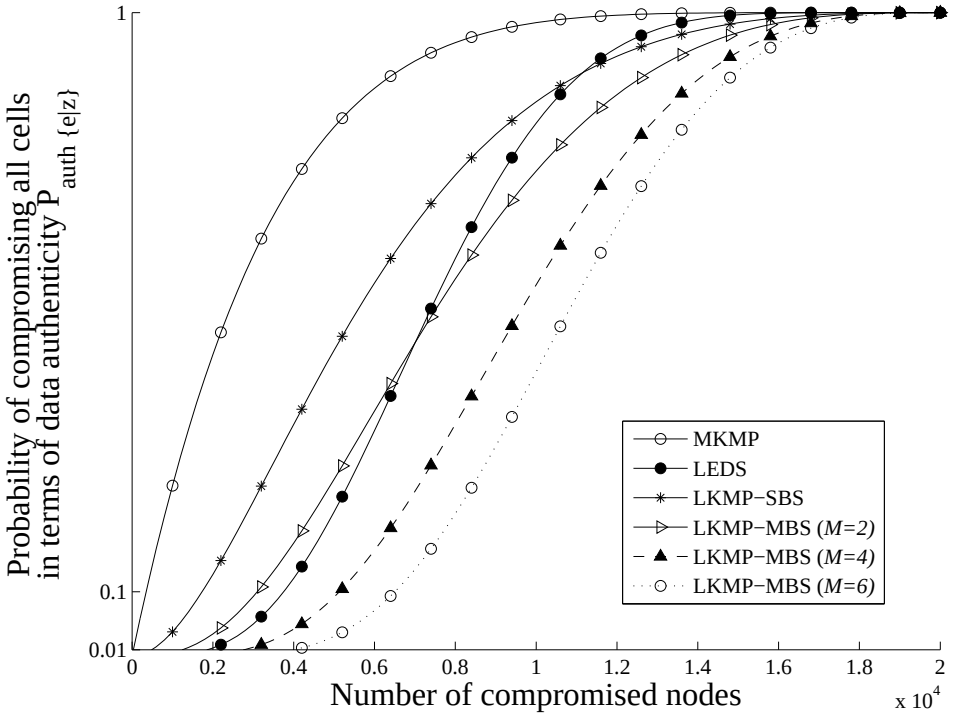


Figure 4.16: Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 20,000$, $\varepsilon = 6$ and $z = 3$.

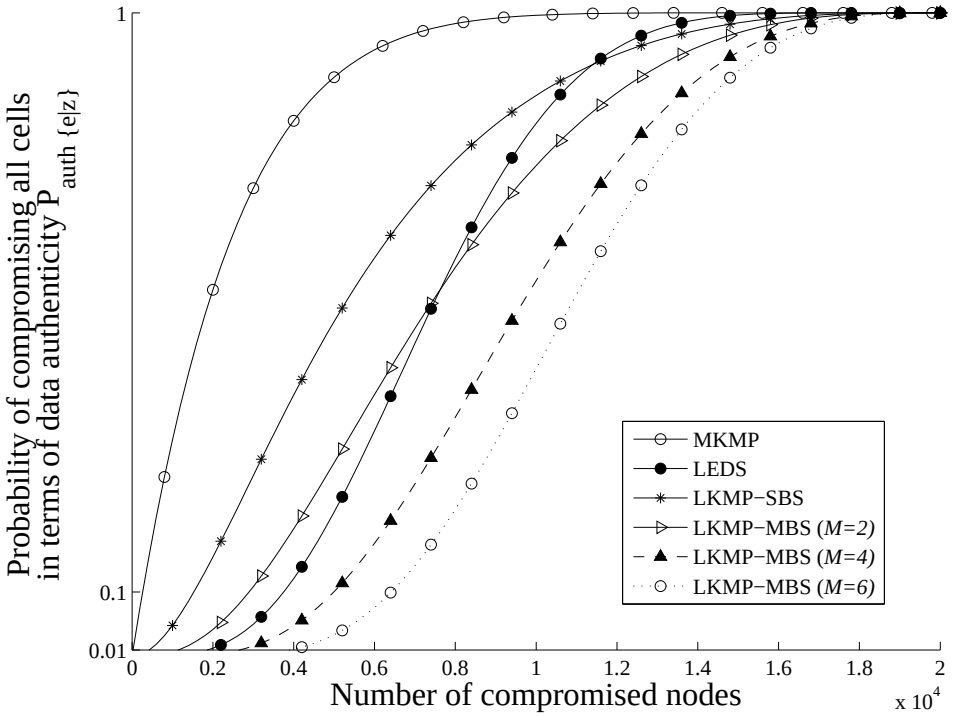


Figure 4.17: Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 20,000$, $\varepsilon = 8$ and $z = 3$.

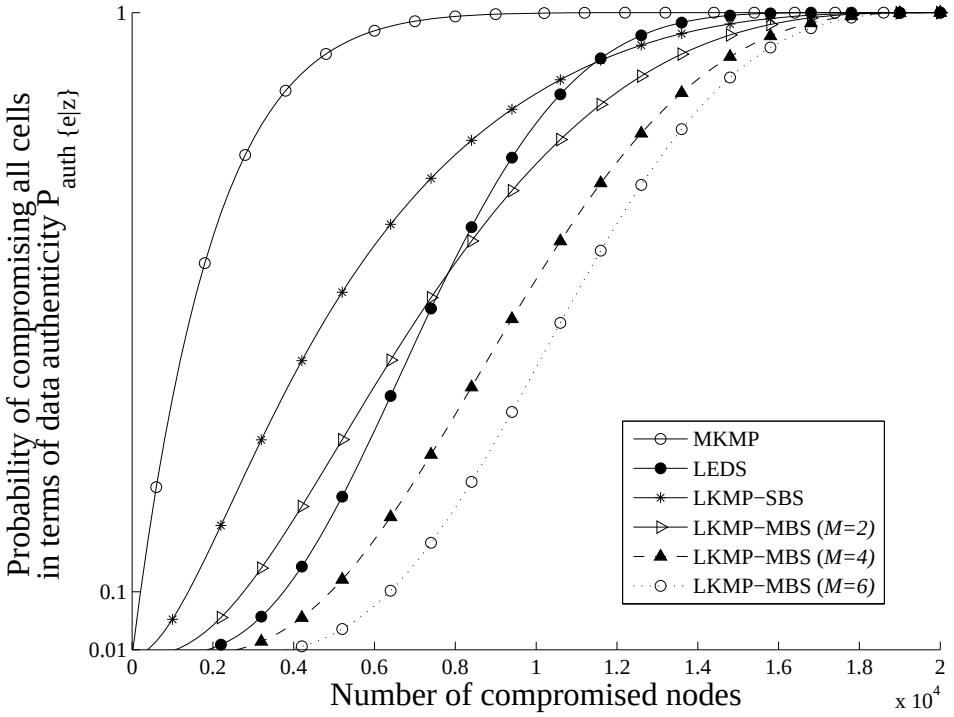


Figure 4.18: Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 20,000$, $\varepsilon = 10$ and $z = 3$.

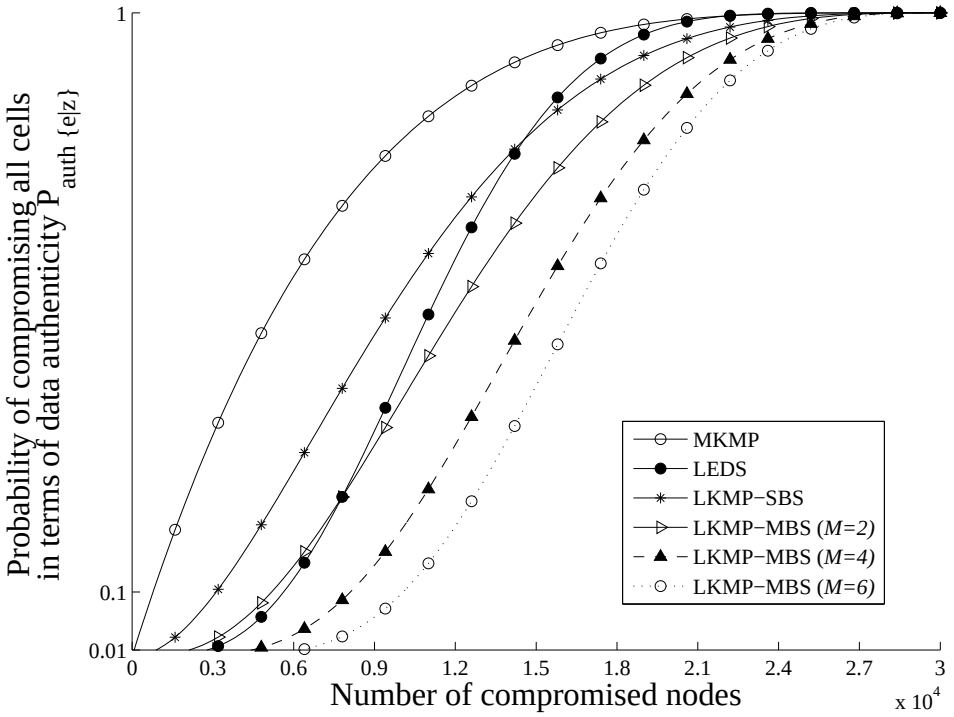


Figure 4.19: Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 30,000$, $\varepsilon = 4$ and $z = 3$.

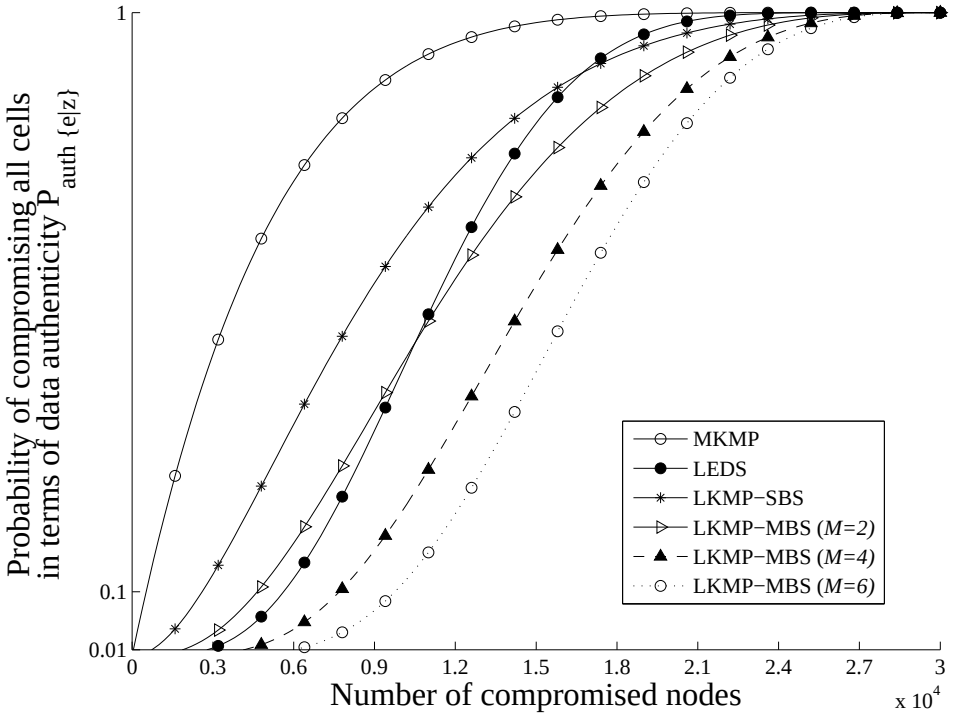


Figure 4.20: Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 30,000$, $\varepsilon = 6$ and $z = 3$.

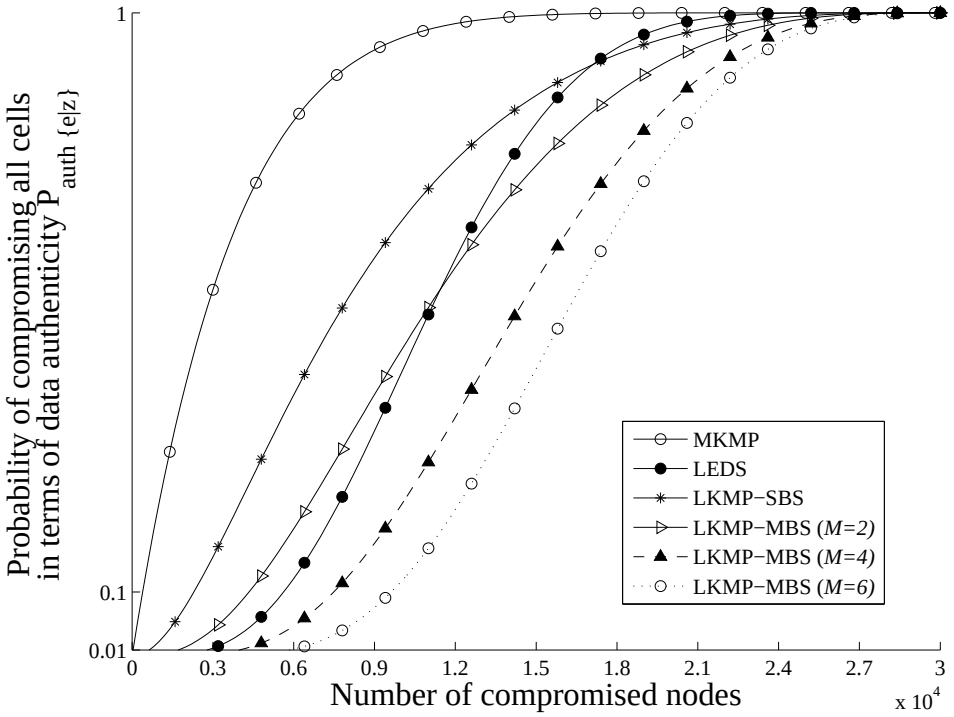


Figure 4.21: Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 30,000$, $\varepsilon = 8$ and $z = 3$.

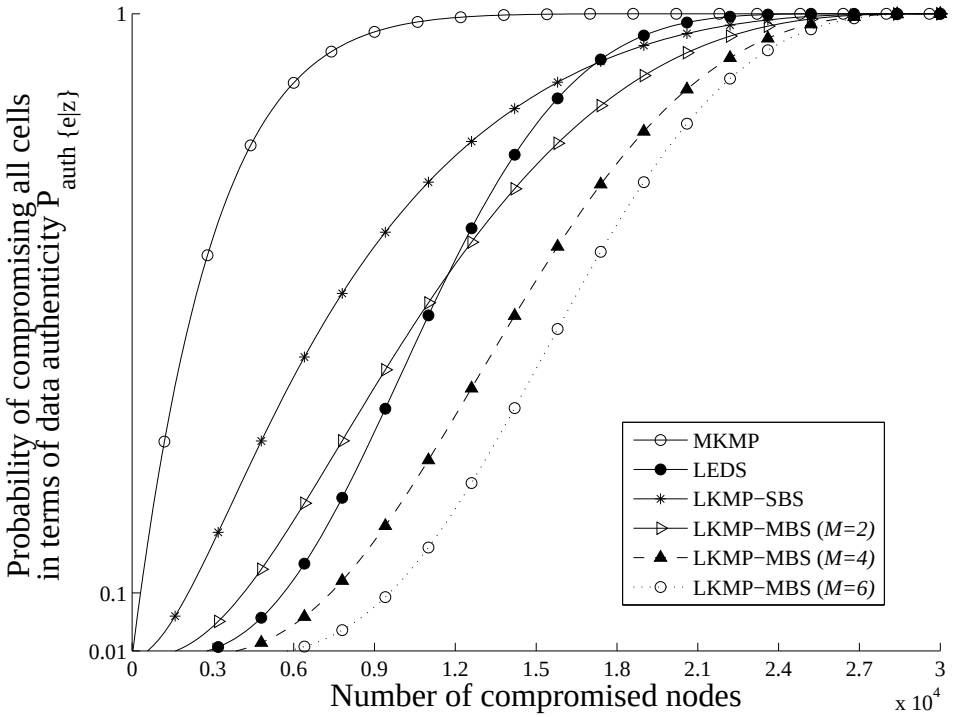


Figure 4.22: Data authenticity of LKMP-MBS ($M = 2, 4, 6$), LKMP-SBS, LEDS and MKMP vesus a number of compromised nodes due to RNCA in a WSN of parameters $N = 30,000$, $\varepsilon = 10$ and $z = 3$.

It is obvious that, regardless of the value of M, the behaviour of the relationship between x and $P_{auth\{\varepsilon|z\}}$ is the same for any value of N and ε where $P_{auth\{\varepsilon|z\}}$ increases

Table 4.1: Comparison between LKMP-MBS and LKMP-SBS in terms of X_t.

N	ε	X_t		Improvement Percentage
		LKMB-SBS $z = 3$	LKMB-MBS $z = 3$	
$10,000$	4	4875	2600	46.67%
	6	5700	3600	36.84%
	8	5825	3800	34.76%
	10	5875	4000	31.91%
$20,000$	4	9750	5200	46.67%
	6	11050	7000	36.65%
	8	11350	7600	33.04%
	10	11500	7800	32.17%
$30,000$	4	15500	8000	48.39%
	6	17300	10600	38.73%
	8	17400	11400	34.48%
	10	17500	11800	32.57%

by x increases. However, the slope of the curve varies depending on N, M and ε values. These differences are depicted in Fig. 4.23 and Fig. 4.24 respectively. The two figures show that:

$$P_{auth\{\varepsilon|z\}} = f(\frac{1}{N}, \varepsilon) \tag{4.16}$$

The following two sections discuss and explain the mathematical proof of (3.34) .

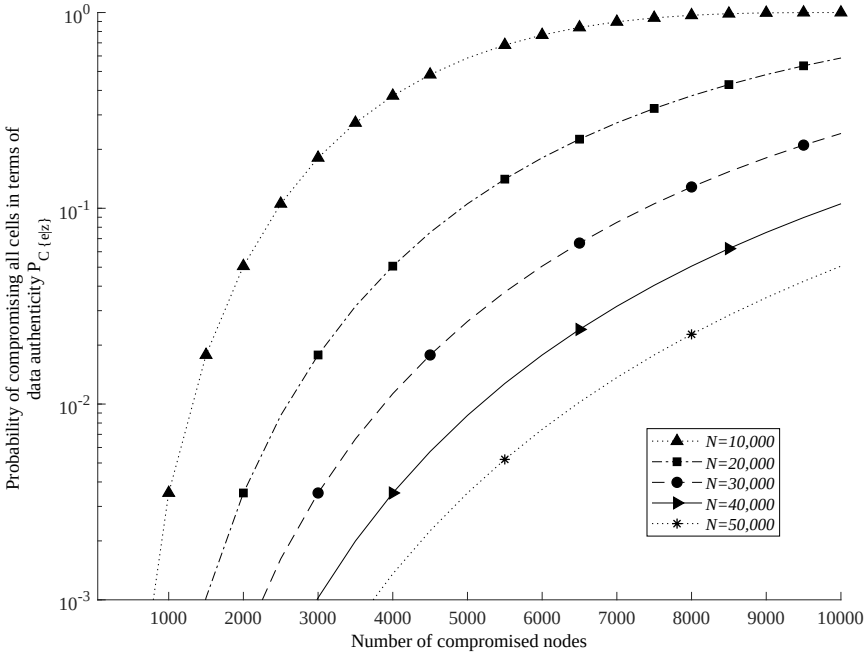


Figure 4.23: The effect of changing the number of nodes in the network N on the probability of compromising all cells in terms of data authenticity due to RNCA, $\varepsilon = 10$, $z = 3$.

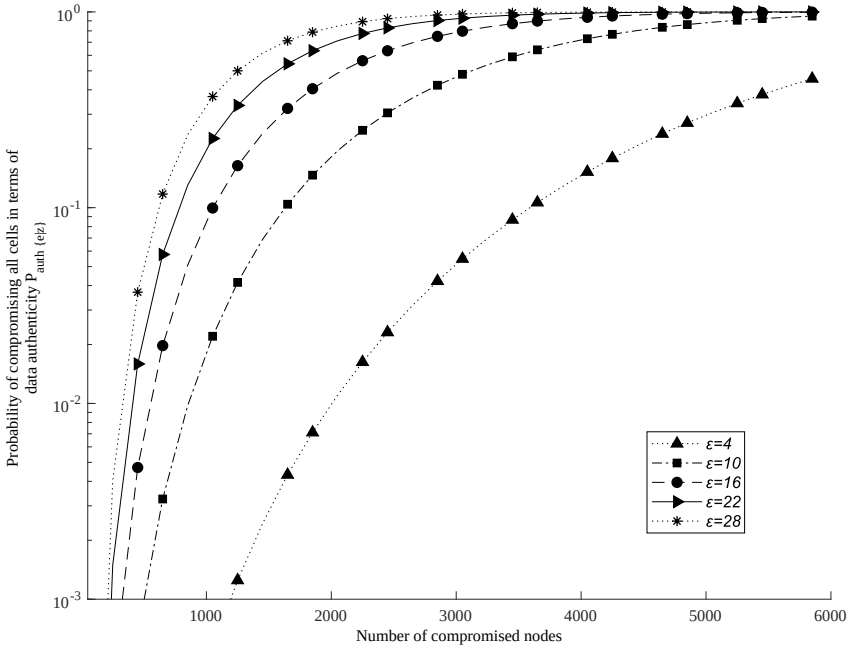


Figure 4.24: The effect of changing the number of endorsement nodes in the network ε on the Probability of compromising all cells in terms of data authenticity due to RNCA, $N = 10,000$, $z = \frac{\varepsilon}{2}$.

- **The effect of N on the value of $P_{auth\{\varepsilon|z\}}$**

  As mentioned in 4.8.1, any increment in the the value of N in a WSN increases the

number of total cells assuming the number of nodes per cell is constant. Therefore, increasing the value of N decreases the ratio of compromised cells and leads to enhancing the security of the system in terms of data authenticity.

The mathematical proof of (4.16) is achieved, based on (4.15), as:

Proof 4.2

$$\begin{aligned} P_{auth\{e|z\}} &= \sum_{j=1}^{\varepsilon} \frac{\binom{\varepsilon}{j}\binom{N-\varepsilon}{x-j}}{\binom{N}{x}} \prod_{\ell=1}^{M} \sum_{j=1}^{z^{(\ell)}} \frac{\binom{z^{(\ell)}}{j}\binom{N-z^{(\ell)}}{x-j}}{\binom{N}{x}} \\ &= P_1 P_2 \\ \Rightarrow P_{auth\{\varepsilon|z\}} &= f(P_1, P_2) \end{aligned} \tag{4.17}$$

The term P_1 is proved to be $f(\frac{1}{N})$ as shown in Chapter 3. ON the other hand, while $\binom{\varepsilon}{j}$ in (3.36) is a not depending on N, it is considered as a constant:

$$\begin{aligned} P_1 &\propto \sum_{j=1}^{\varepsilon} \frac{\binom{N-\varepsilon}{x-j}}{\binom{N}{x}} \\ &\propto \sum_{j=1}^{\varepsilon} \frac{\frac{(N-\varepsilon)!}{(x-j)!(N-\varepsilon-x+j)!}}{\frac{(N)!}{x!(N-x)!}} \\ &\propto \sum_{j=1}^{\varepsilon} \frac{x!(N-\varepsilon)!(N-x)!}{N!(x-j)!(N-\varepsilon-x+j)!} \\ &\propto \sum_{j=1}^{\varepsilon} \frac{(N-\varepsilon)!(N-x)!}{N!(N-\varepsilon-x+j)!} \end{aligned} \tag{4.18}$$

$$\begin{aligned} \sum_{j=1}^{\varepsilon} \frac{(N-\varepsilon)!(N-x)!}{N!(N-\varepsilon-x+j)!} &= \sum_{j=1}^{\varepsilon} \frac{\prod_{k=1}^{\varepsilon-j}(N-x-\varepsilon+j+k)}{\prod_{k=1}^{\varepsilon}(N-\varepsilon+k)} \\ &= \frac{N^{\varepsilon-j} - a_1 N^{\varepsilon-j-1} + a_2 N^{\varepsilon-j-2} - \cdots a_{\varepsilon-j} N}{N^{\varepsilon} x - a_1 N^{\varepsilon-j-1} + a_2 N^{\varepsilon-j-2} - \cdots a_{\varepsilon} N} \end{aligned}$$

While $(\varepsilon - j) < \varepsilon$

$$\sum_{j=1}^{\varepsilon} \frac{(N-\varepsilon)!(N-x)!}{N!(N-\varepsilon-x+j)!} \propto \frac{1}{N} \tag{4.19}$$

From both (4.18) and (4.19):

$$
\begin{aligned}
P_1 &= f(\frac{1}{N}) \\
P_2 &= f(\frac{1}{N}) \\
\Rightarrow P_{auth\{\varepsilon|z\}} &= f(\frac{1}{N})
\end{aligned} \tag{4.20}
$$

■

- **The effect of ε on the value of $P_{auth\{\varepsilon|z\}}$**

There are two reasons for the relationship between ε and $P_{auth\{\varepsilon|z\}}$:

1. Increasing the number of endorsement nodes and keeping a constant value of z increases the likelihood of generating a fake report from that cell.

2. Increasing ε will increase the value of n which leads to a decrease in the number of cells in the WSN assuming the total number of nodes N in the WSN is constant. Hence, the ratio of compromised cells is increased which reduces the security level of the system in terms of data confidentiality.

While the ε value dependant of the (4.15) is the same as the relevant part of (3.33), the mathematical proof explained in 3.4 is considered here.

4.9 The Optimum Number of Cell Reporters

As illustrated previously, each BS BS_ℓ selects its own set of cell reporters $z^{(\ell)}$ inside each particular cell c. However, as illustrated in Section 4.2, there are two control topologies: IndCon and ColCon. Accordingly, the selected set of cell reporters might have:

1. No mutual elements with any sets of cell reporters within the same cell in the case of IndCon.

2. Some mutual elements with different sets of cell reporters within the same cell in the case of ColCon.

In this section, the optimality of the number of cell reporters ($z^{(\ell)}$) is investigated for both cases.

4.9.1 IndCon: Cell reporter sets having no mutual elements

In this situation, any particular node n could be a cell reporter selected by only one BS in the network. Accordingly, the probability of compromising all cell reporters, selected by the M BSs, out of the total n sensor nodes P_{z_comp} can be calculated. The expression of P_{z_comp} varies based on the length $z^{(\ell)}$ selected by each BS where there are two cases:

1. The length of the cell reporter set $|z^{(\ell)}|$ is the same for all BS_ℓ
2. The length of the cell reporter sets is not unified for all BSs.

- **The length of the cell reporter set $|z^{(\ell)}|$ is the same for all BS_ℓ**

  In this case, it is considered that $(|z^{(1)}| = |z^{(2)}| \ldots = |z^{(M)}| = z)$. Accordingly, the calculation of P_{z_comp} can be determined using the compromising strategy explained in the following example:
  Assuming a WSN with $M = 2, z = 2$ and $n = 10$, the adversary has:

  - A probability of $P_1 = \frac{2\cdot 2}{10} = \frac{4}{10}$ to compromise all set reporters belonging to all BSs in the first trial.
  - A probability of $P_2 = \frac{(2\cdot 2)-1}{9} = \frac{3}{9}$ to compromise the remaining cell reporters from the remaining 9 nodes in the 2^{nd} trial.
  - A probability of $P_3 = \frac{(2\cdot 2)-2}{8} = \frac{2}{8}$ to compromise the remaining cell reporters from the remaining 8 nodes in the 3^{rd} trial.
  - probability of $P_4 = \frac{(2\cdot 2)-3}{7} = \frac{1}{7}$ to compromise the remaining cell reporters from the remaining 7 nodes in the 4^{th} trial.

  Then the probability of compromising all cell reporters is calculated as:

$$P_{z\_comp} = P_1 P_2 P_3 P_4 = \frac{1}{210}$$

  This can be generalised as:

$$P_{z\_comp} = \left(\frac{Mz}{n}\right)\left(\frac{(Mz)-1}{n-1}\right)\cdots\left(\frac{1}{n-(Mz)+1}\right)$$
$$P_{z\_comp} = \frac{(Mz)!(n-Mz)!}{n!} \tag{4.21}$$

  Hence, in order to estimate the optimum value of z, the minimum point of the P_{z_comp} is investigated:

$$
\begin{aligned}
&z_{opt} = \arg\min_{z} \left\{ \frac{(Mz)!(n-Mz)!}{n!} \right\} \\
&\frac{\partial}{\partial z}(Mz)!(n-Mz)! = 0 \\
&(n-Mz)!\Gamma(Mz+1)\psi^0(Mz+1) = \\
&(Mz)!\Gamma(n-Mz+1)\psi^0(n-Mz+1) \\
&\psi^0(Mz+1) = \psi^0(n-Mz+1)
\end{aligned}
$$

According to [118], $\psi^m(x)$ is a monotonic function. Therefore:

$$k = \frac{n}{2M} \tag{4.22}$$

The first derivative test is applied to test the critical point z shown in (4.22). This is implemented by selecting two test points ($z^- = 0 \in (-\infty, \frac{n}{2M})$) and ($z^+ = \frac{n}{M} \in (\frac{n}{2M}, \infty)$):

$$
\begin{aligned}
\frac{\partial}{\partial z}(P_{z\_comp}) =& \frac{\partial}{\partial z}\frac{(Mz)!(n-Mz)!}{n!} \\
=& \frac{1}{n!}[(n-Mz)!\Gamma(Mz+1)\psi^0(Mz+1) - \\
& (Mz)!\Gamma(n-Mz+1)\psi^0(n-Mz+1)]
\end{aligned} \tag{4.23}
$$

As a result, at $z = z^- = 0$

$$
\begin{aligned}
\frac{\partial}{\partial z}P_{z\_comp}(z=0) &= \frac{n!\Gamma(1)\psi^0(1)}{n!} - \frac{\Gamma(n+1)\psi^0(n+1)]}{n!} \\
&= \psi^0(1) - \psi^0(n+1)
\end{aligned} \tag{4.24}
$$

On the other hand, when $z = z^+ = \frac{n}{M}$:

$$
\begin{aligned}
\frac{\partial}{\partial z}P_{z\_comp}(z=\frac{n}{M}) =& \frac{\Gamma(n+1)\psi^0(n+1)}{n!} - \frac{n!\Gamma(1)\psi^0(1)]}{n!} \\
=& \psi^0(n+1) - \psi^0(1)
\end{aligned} \tag{4.25}
$$

The expression of ((4.24)) and ((4.25)) is shown to be negative, positive respectively for all $n \in \mathbb{R}^+$ according to 3.2. Therefore, $k = \frac{n}{2M}$ is the unique minimum point of P_{z_comp}. Figure. 4.25 depicts this fact for ($n = 20, 30$ and 40).

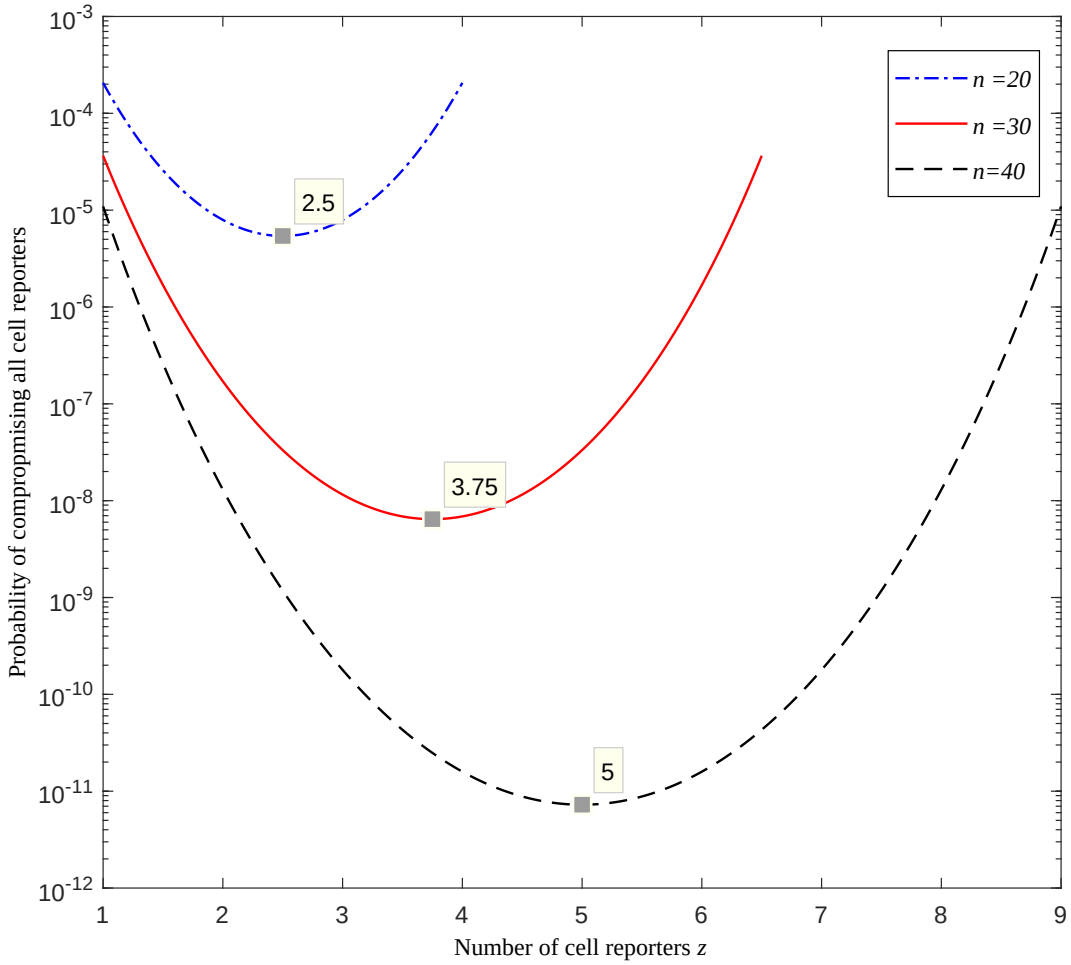


Figure 4.25: The relationship between the number of cell reporters (z) and the probability of compromising all cell reporters (P_{z_comp}) for a WSN with four BSs ($M = 4$) when the number of sensor nodes inside each cell $n = 20, 30$ and 40.

- **The length of the cell reporter sets is not unified for all BSs**

Following up the strategy followed in the derivation of (4.21), the following equation is derived to determine the probability of compromising all cell reporters P_{z_comp} selected by all M BSs in the network:

$$P_{z\_comp} = \frac{(\sum_{\ell=1}^{M} |z^{(\ell)}|)!(n - (\sum_{\ell=1}^{M} |z^{(\ell)}|)!}{n!} \tag{4.26}$$

Hence, the optimum number of cell reporters is calculated as:

$$\sum_{\ell=1}^{M} |z_{opt}^{(\ell)}| = \frac{n}{2M} \tag{4.27}$$

In such a case, if $|z^{(i)}|$ of any BS_i is increased for any reason, $|z^{(\ell)}|$ of other BSs must be deceased to keep the optimality conditions of (4.27). This will require a reliable real time cooperation between all BSs and will negatively affect the security of those cells having a lower number of cell reporters. As a result, this consideration will increase the complexity of the system and affect its security balance where the same attacker, who fails to compromise the cell reporters of one BS, has the ability to compromise cell reporters of remaining BSs. Therefore, in the case of no mutual elements between several cell reporters sets, choosing cell reporters sets of the same length for all BSs is better than choosing them with different lengths.

4.9.2 ColCon: Some elements are mutual between different cell reporter sets

In this case, each specific node n could be a cell reporter selected by more than one BS in the network. It is obvious that taking such case into account will definitely complicate the process of the probability calculation. However, the discussion of this assumption is found to be crucial where it is more realistic due to:

1. Both the randomness and the secrecy of cell reporter selection increase the possibility of this event occurring.

2. The possibility of losing some nodes because of a physical failure or security attack might lead to secrecy in the number of nodes inside a particular cell.

3. The consideration of uniform node distribution is an ideal assumption and might be altered by different conditions.

4. Some applications allocate more than one function for each particular cell in the WSN. Hence, a particular node might be in charge of reporting more than one BS at the same time and this increases the possibility of choosing that node as a cell reporter for the mentioned BS.

For simplicity, the number of cell reporters selected by every BS is assumed to be the same ($|z^{(1)}| = |z^{(2)}| \ldots = |z^{(M)}| = z$). Accordingly, the probability of compromising all cell reporters in a row by an adversary P_{z_comp} is calculated by considering a worst case scenario where the adversary has full knowledge of M, z and n. The adversary's objective is to compromise all cell reporters. As mentioned earlier, there are M BSs in

the WSN where each BS had selected z cell reporters, Therefore, the adversary's aim is to compromise $Mz - \hat{z}$ cell reporters where $\hat{z}$ refers to the number of mutual cell reporters in the network. However, $\hat{z}$ is assumed to be outside the adversary's knowledge due to its variance and unpredictability. Accordingly, the main purpose of the assumed attack is to compromise Mz cell reporters among n nodes inside a particular cell. As a result, this attack is considered to launch through Mz consecutive stages where one node is compromised at each stage. Our target is to calculate P_{z_comp} after launching this attack. The main challenge of this problem is the change of z after each stage depending on the previous stage. Therefore, a mathematical model of this system had been considered as a Markov chain [129]. Accordingly a status matrix for our problem is manipulated as shown in Table. 4.2. The following variables are illustrated in this matrix:

- T_{old} represents the total number of non compromised nodes before implementing a stage of attack.
- T_{new} represents the total number of non compromised nodes after implementing a stage of attack.
- R_{old} represents the total number of non compromised cell reporters before implementing a stage of attack.
- R_{new} represents the total number of non compromised cell reporters after implementing a stage of attack.

Then each cell with index (i, j) in this matrix is filled by the value, based on the cell indices of a transition matrix T which is derived to specify the transition between each two consecutive stages as:

$$T(i,j) = \frac{\binom{R_{new}(i)}{\Delta R(i,j)}\binom{Mz - R_{new}(i)}{M - \Delta R(i,j)}}{\binom{Mz}{M}} \tag{4.28}$$

Where:

$$\Delta R(i,j) = R_{new}(i) - R_{old}(j)$$

Finally, T is used to determine the probability of compromising all cell reporters in the WSN after implementing Mz stages as [129]:

$$\omega = \nu T^{Mz} \tag{4.29}$$

$$P_{z\_comp} = \sum_{i=1}^{M+1} \omega[i] \tag{4.30}$$

Where:
$\nu = [0\ 0\ \cdots\ 1]$
$\omega[i]$ is the i^{th} column of ω.
While the main target is to calculate the probability of compromising all cell reporters after the completion of the last stage.

The relationship between z and P_{z_comp} is depicted in Fig. 4.26. It is obvious that increasing the number of BS in the WSN leads to an increase in the value of P_{z_comp}. Moreover, this figure depicts the optimum value of z (z_{min}) that causes a minimum value of P_{z_comp} which is shown to be decreasing by increasing the number of BSs. The reason behind the recorder results is due to the increment in the number of mutual cell reporters which increases the probability if compromising more cell reporters.

4.10 Conclusion

In this Chapter, a novel multiple BS location-dependent key management protocol (LKMP-MBS) is presented based on a randomly selected cell reporter scheme and is proven to achieve better performance in comparison with existing schemes and with the (LKMP-SBS) presented in the previous Chapter. The problem of the degraded performance of LKMP-SBS in comparison with LEDS had been overcame in this scheme. An extensive mathematical analysis was presented to evaluate this scheme in terms of system security by considering data confidentiality, authenticity and overall robustness against attacks targeting cell reporters. Both data confidentiality and authenticity have been proven to be $f(\varepsilon, \frac{1}{N})$. Moreover, the system optimality in terms of the number of selected cell reporters has been analysed for different considerations. In the case of considering that all cell reporters sets have no mutual elements, the optimum number of cell reporters had

Table 4.2: Status matrix of the Markov module

	$R_{old}\downarrow$	T_{new}=0				$\cdots$	T_{new}=nM			
$R_{new}\rightarrow$		0	1	$\cdots$	Mz	$\cdots$	0	1	$\cdots$	Mz
T_{old}=0	0					$\cdots$				
	1					$\cdots$				
	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
	Mz					$\cdots$				
T_{old}=M	0					$\cdots$				
	1					$\cdots$				
	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
	Mz					$\cdots$				
T_{old}=$2M$	0					$\cdots$				
	1					$\cdots$				
	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
	Mz					$\cdots$				
$\cdots$	$\cdots$					$\cdots$				
T_{old}=nM	0					$\cdots$				
	1					$\cdots$				
	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
	Mz					$\cdots$				

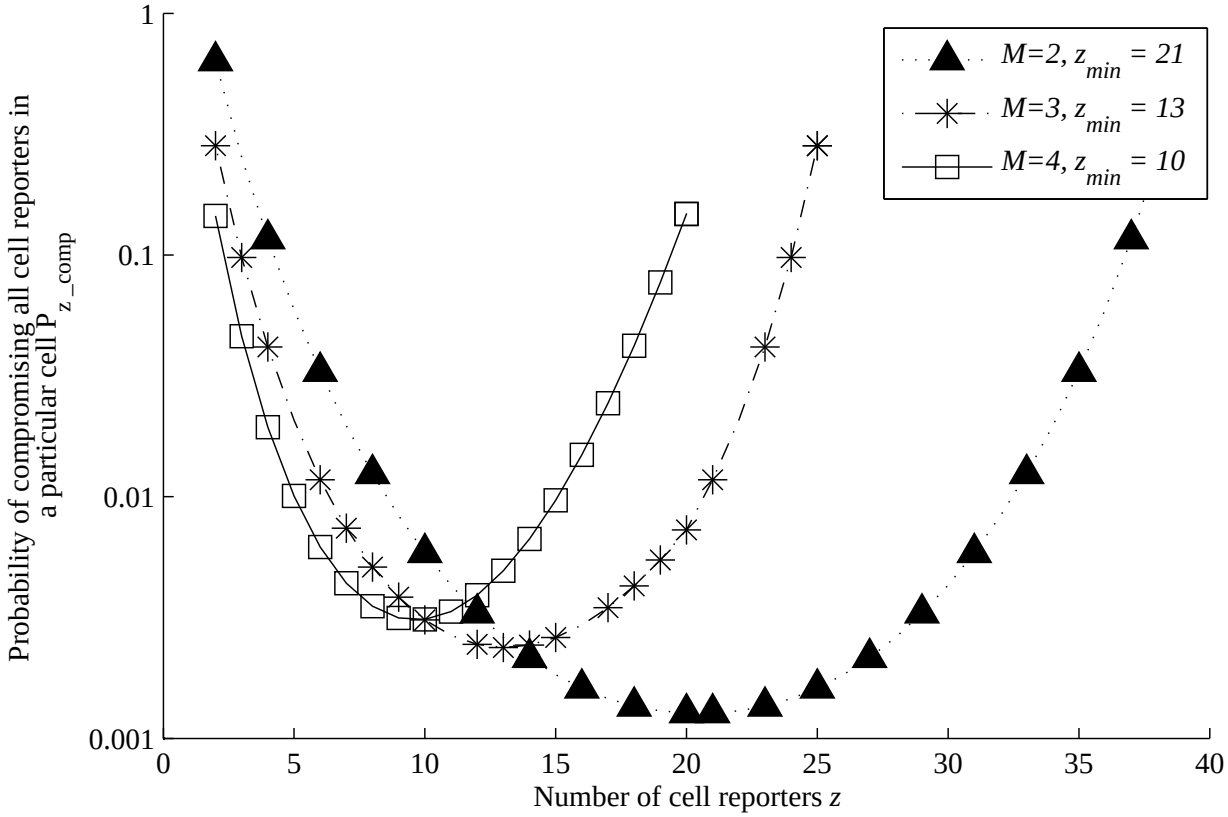


Figure 4.26: The relationship between the number of cell reporters (z) and the probability of compromising all cell reporters (P_{z_comp}) inside a a particular cell for different numbers of BS ($M = 1, 2, 3$).

been calculated as $z_{opt} = \frac{n}{2M}$, $\sum_{\ell=1}^{M} |z_{opt}^{(\ell)}| = \dfrac{n}{2M}$ when they have unified and not unified lengths respectively. On the other hand, if these sets are considered to have a mutual file between them, a mathematical model is built bases on Markov chain analysis and the z_{opt} is found to be varying according to the M value.

Chapter 5

MELKMP-MBS: Protocol Description and Communication Overhead Analysis

5.1 Introduction

As described in both of Chapter 3 and 4, each node in the network has an ability to perform all required functions based on the credentials derived according to its location within the hosting cell. This guarantees the node service availability while it is located within the area of its hosting cell. However, the availability is significantly altered when a node or a group of nodes move between different cells, increasing the likelihood that they will be treated as an adversary in the new hosting cell after movement. Therefore, this chapter proposes the Mobility Enable Location Dependant Key Management Protocol for Multiple Base Stations (MELKMP-MBS) as an improvement to the LKMP-MBS, which has the disadvantage of not supporting node mobility. Dynamic WSNs, which may contain some mobile nodes, could be easily managed by this protocol by achieving several types of handover strategies to keep the availability of a mobile node when it is moving between two (or more) zones inside the WSN. As a key contribution of this chapter, the communication overhead is analysed extensively for MELKMP-MBS in order to estimate the impact of handover processes using an extensive mathematical analysis and simulation results obtained by MATLAB and Contiki simulator. Following the same methodology, communication overhead of both LKMP-SBS, LKMP-MBS are presented and compared. On the other hand, the security evaluation of this protocol is omitted in this chapter while

it is similar to the analysis of LKMP-MBS presented in previous chapter.

5.2 Nodes Mobility between different BS coverage regions

As explained in Chapter 4 , the topology of a multiple BS WSN is classified into:

- Individual control (IndCon)
- Collaborative control (ColCon)

Accordingly, there is a high possibility for a mobile node in WSN to traverse between two ore more cells that are covered by different BSs. Therefore, a Mobility Enabled Location Dependent Key Management Protocol for a Multiple Base Station WSNs (MELKMP-MBS) is presented in this section as a novel key management scheme includes all the facilities required to govern the mobility of sensor nodes between different cells (C_{old} and C_{new}) in order to handle a smooth handover between the two BSs, hereafter known as BS_{old} and BS_{new}. Moreover, such a protocol has an ability to implement the required processes of adding/removing new nodes which are significantly crucial in dynamic networks. Regardless of the control topology of the network, there are two types of handover as shown in Fig. 5.1:

1. local handover: when a node is moving between two cells belonging to the same BS. For example, a local handover is implemented by the BS_{old} in the case of node **A** mobility from its $C_{old} = 1$ to $C_{new} = 2$.
2. global handover: when a node is moving between two regions each one belongs to a different BS. For example, a global handover is implemented by BS1 and BS2 in the case of node **B** mobility from its $C_{old} = 5$ to $C_{new} = 9$.

As shown in the previous chapters, both LKMP-SBS and LKMP-MBS consist of three phases: **Setup phase**, **Report Generation Phase** and **Key Revocation Phase**. On the other hand, MELKMP-MBS consists of four phases:

1. Setup phase
2. Report Generation Phase

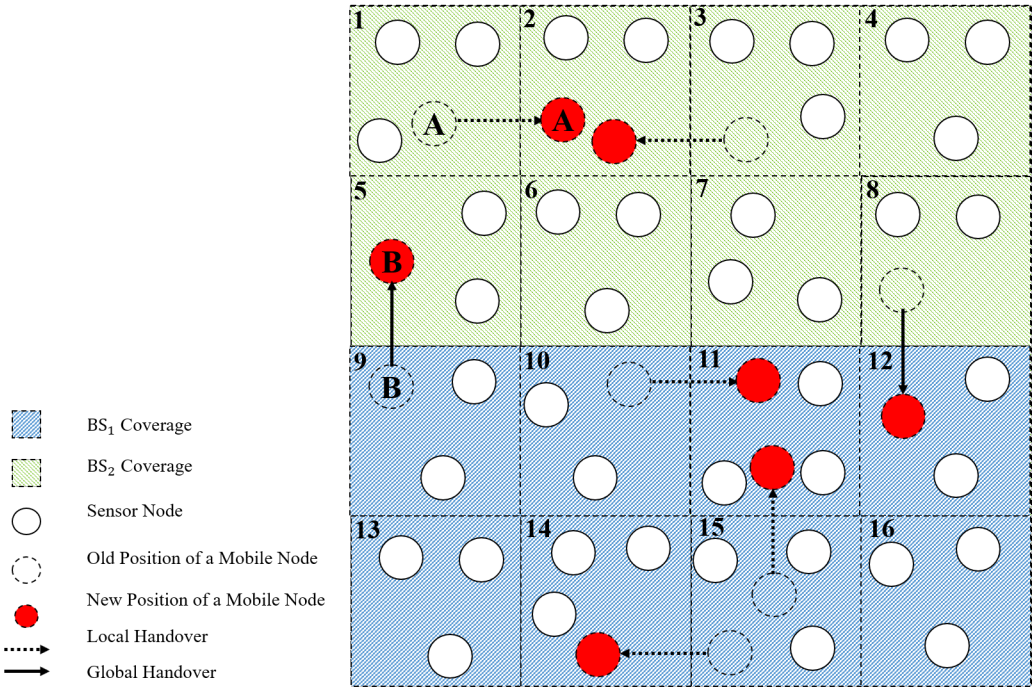


Figure 5.1: A 16 cell WSN controlled collaboratively by two BSs, i.e., BS_1 and BS_2.

3. Handover phase

4. Key Revocation Phase

Both the 2^{nd} and 4^{th} phases are the same as those used in LKMP-MBS and described by Algorithms.4.8, 4.9 and 4.10. On the other hand, the remaining two new phases are illustrated in the following sections.

5.3 Setup Phase

In this protocol, each node (a) is preloaded with the following parameters:$\{K, ID_a, ID_a^m, \Delta, p, t, \boldsymbol{S}\}$ Where:
ID_a^m: Node mobility identity that is used to identify itself to the C_{new}, this ID is preloaded as well as ID_a to all BSs.
Based on their locations, the preloaded $\boldsymbol{S}$ and the value of τ, each particular node determines:

- Its cell centre location using Theorem 3.1.
- The set of adjacent cells

$$C_{adj} = \begin{bmatrix} C^1_{adj} \\ \\ C^2_{adj} \\ . \\ . \\ . \\ C^M_{adj} \end{bmatrix}$$

Where:

$$C^i_{adj} = \{(x^i_c - 1, y^i_c + 1), (x^i_c, y^i_c + 1), (x^i_c + 1, y^i_c + 1), (x^i_c - 1, y^i_c), (x^i_c + 1, y^i_c), (x^i_c - 1, y^i_c - 1), (x^i_c, y^i_c - 1), (x^i_c + 1, y^i_c - 1)\} \quad (5.1)$$

In addition, the matrix of initial cell keys $\boldsymbol{K_{Lcin}}$ is derived by all nodes in the cell c as shown in Algorithm. 5.11.

Algorithm 5.11 *Security credentials derivation by each particular node during setup phase*

Require: $K, \boldsymbol{S}, \tau, \Delta, (x_s, y_s)$

$K_\tau \leftarrow K \| \tau$

$\boldsymbol{x_c} \leftarrow 0.5 \left\lceil \frac{x_a - \boldsymbol{S_1}}{\Delta} \right\rceil, \boldsymbol{y_c} \leftarrow 0.5 \left\lceil \frac{y_a - \boldsymbol{S_2}}{\Delta} \right\rceil$

for i=1:M **do**

$$\boldsymbol{C_{adj}} \leftarrow \begin{bmatrix} C^1_{adj} \\ \\ C^2_{adj} \\ . \\ . \\ . \\ C^M_{adj} \end{bmatrix}$$

end for

$$\boldsymbol{K_{Lcin}} \leftarrow \begin{bmatrix} H(K_\tau \| \boldsymbol{x_c}(1) \| \boldsymbol{y_c}(1)) \\ \\ H(K_\tau \| \boldsymbol{x_c}(2) \| \boldsymbol{y_c}(2)) \\ . \\ . \\ H(K_\tau \| \boldsymbol{x_c}(M) \| \boldsymbol{y_c}(M)) \end{bmatrix}$$

Ensure: $K_\tau, (\boldsymbol{x_c}, \boldsymbol{y_c}), \boldsymbol{K_{Lcin}}, \boldsymbol{C_{adj}}$

Then, each sensor node inside a cell c discovers and creates a list of its cell-mates as described in Algorithm. 4.7 shown in the previous chapter. Finally, the verification procedure for the received report is implemented following similar steps to Algorithm. 4.8.

5.3.1 Handover Phase

This section explains the procedure of implementing both the local and global handover explained previously. The main purpose is to guarantee the service availability of the mobile node or at least maintain a minimum time of its unavailability. Such a procedure has to be as secure as possible in order to prevent any vulnerability caused by inside or outside attackers, such as the node clone attack and node replication attack in both static and mobile WSNs [130–133].

5.3.1.1 Local handover

In the case of a node mobility between two cells belonging to the same BS, it is crucial to report that movement to different entities in the WSN such as:

- The BS: in order to consider this node as a legitimate node by updating the hosting cell of this node.
- The entire set of nodes in C_{old}: In order to update the e value and overcome the criticality of considering the mobile node as a node which does not record that event, hereafter know as a "**Dereporter Node**".
- The whole node within C_{new}: In order to legitimize the new node as a "**Reporter Node**" and update the value of e.

In order to sketch a handover process based on the above requirements, the local handover can be further classified based on node mobility into:

- Intended mobility: where a node is moving to its C_{new} based on a BS request, according to a pre sketched plan or by a self decision. In such a type of mobility, the node has an opportunity to send a message indicating its movement, its target and the time of movement occurrence as illustrated in Algorithm. 5.12.
- Non-intended mobility: where a node is forced to be moved to a new region due to external effects such as weather conditions. In this case, the node has no enough time to alert other entities such as the BS, C_{new} and C_{new} nodes. This type of handover is illustrated in Algorithm. 5.13.

It is obvious that the second class, Non-intended mobility, is the worst case scenario and needs to be addressed efficiently by MELKMP-MBS. Figure. 5.2 illustrate the message

sequence chart of the intended mobility local handover. On the other hand, the message sequence chart of the Non-intended mobility local handover is depicted in Fig. 5.3.

Algorithm 5.12 *Intended local handover procedure followed when a node a is moved from C_{new} to C_{old}, both are belonging to BS_{old}*

Require: $K, ID_a, ID_a^m, (x_{C_{new}}, y_{C_{new}}), (x_{C_{old}}, y_{C_{old}}), MovTime, \boldsymbol{S}, K_a^{BS_{old}}, , \tau$

$a \rightarrow * \ (C_{old})$: $Enc_{K_{L_{c(old)}}} ImMoving(ID_a, ID_a^m, (x_{C_{new}}, y_{C_{new}}), MovTime)$

for all cell-mates (α) **do**

$\alpha \rightarrow BS_{old}$: $Enc_{K_\alpha^{BS_{old}}} MovingNode(ID_a, ID_a^m, (x_{C_{new}}, y_{C_{new}}), MovTime)$

end for

$BS_{old} \rightarrow C_{old}$ $Enc_{K_{L_{c(old)}}} Ack(Akn)$

$BS_{old} \rightarrow a$ $Enc_{K_a^{BS(old)}} \{Akn, K_{L_{c(temp)}}\}$

$BS_{old} \rightarrow C_{new}$ $Enc_{K_{L_{c(new)}}} AddNew(ID_a, ID_a^m, MovTime, K_{L_{c(temp)}})$

$a \rightarrow * \ (C_{new})$: $Enc_{K_{L_{c(temp)}}} Hello(ID_a, ID_a^m, (x_{C_{new}}, y_{C_{new}}), MovTime)$

$C_{new} \rightarrow a$ $Enc_{K_{L_{c(temp)}}} Ack(\tau)$

for $C_{new} \cup a$ **do**

$K_\tau \leftarrow K \| \tau$

$\boldsymbol{x_c} \leftarrow 0.5 \left\lceil \frac{x - \boldsymbol{S_1}}{\Delta} \right\rceil, \boldsymbol{y_c} \leftarrow 0.5 \left\lceil \frac{y - \boldsymbol{S_2}}{\Delta} \right\rceil$

$$\boldsymbol{K}^{\boldsymbol{M}}_{\boldsymbol{L_{c(new2)}}} \leftarrow \begin{bmatrix} H(K_\tau \| \boldsymbol{x_c}(1) \| \boldsymbol{y_c}(1)) \\ H(K_\tau \| \boldsymbol{x_c}(2) \| \boldsymbol{y_c}(2)) \\ . \\ . \\ H(K_\tau \| \boldsymbol{x_c}(M) \| \boldsymbol{y_c}(M)) \end{bmatrix}$$

end for

$C_{new} \rightarrow BS_{old}$ $Enc_{K_{L_{c(new)}}} NewCellKey((\boldsymbol{x_c}, \boldsymbol{y_c}), \{CellMateList\}, K^{old}_{L_{c(new2)}})$

$BS_{old} \rightarrow C_{BS_{old}}$ $Enc_{K_{L_{c(old)}}} MovedNode(ID_a, ID_a^m, MovTime)$

Ensure: $K_{L_{c(temp)}}, K^{old}_{L_{c(new2)}}$

Algorithm 5.13 *Non-intended local handover procedure followed when a node a is moved from C_{new} to C_{old} , both are belonging to BS_{old}*

Require: $K, ID_a, ID_a^m, MovTime, \boldsymbol{S}, K_a^{BS_{old}}, , \tau$

$\boldsymbol{x_c} \leftarrow 0.5 \left\lceil \frac{x - \boldsymbol{S_1}}{\Delta} \right\rceil, \boldsymbol{y_c} \leftarrow 0.5 \left\lceil \frac{y - \boldsymbol{S_2}}{\Delta} \right\rceil$

$a \rightarrow * \ (C_{new})$: Enc_K $Hello(ID_a, ID_a^m, (\boldsymbol{x_{C_{new}}}, \boldsymbol{y_{C_{new}}}), MovTime)$

$C_{new} \rightarrow BS_{old}$ $Enc_{K_{L_{c(new)}}} NewNode((\boldsymbol{x_c}, \boldsymbol{y_c}), ID_a, ID_a^m)$

$BS_{old} \rightarrow C_{new}\ Enc_{K_{L_{c(new)}}} Ack(K_{L_{c(temp)}})$
$BS_{old} \rightarrow a\ Enc_{K_a^{BS(old)}} Ack(K_{L_{c(temp)}})$
$C_{new} \rightarrow a\ Enc_{K_{L_{c(temp)}}} Ack(\tau)$
for $C_{new} \cup a$ **do**
$K_\tau \leftarrow K \| \tau$

$\boldsymbol{x_c} \leftarrow 0.5\left\lceil \frac{x - \boldsymbol{S_1}}{\Delta} \right\rceil, \boldsymbol{y_c} \leftarrow 0.5\left\lceil \frac{y - \boldsymbol{S_2}}{\Delta} \right\rceil$

$$\boldsymbol{K}^{\boldsymbol{M}}_{\boldsymbol{L_{c(new2)}}} \leftarrow \begin{bmatrix} H(K_\tau \| \boldsymbol{x_c}(1) \| \boldsymbol{y_c}(1)) \\ H(K_\tau \| \boldsymbol{x_c}(2) \| \boldsymbol{y_c}(2)) \\ . \\ . \\ H(K_\tau \| \boldsymbol{x_c}(M) \| \boldsymbol{y_c}(M)) \end{bmatrix}$$

end for
$C_{new} \rightarrow BS_{old}\ Enc_{K_{L_{c(new)}}} NewCellKey((\boldsymbol{x_c}, \boldsymbol{y_c}), \{CellMateList\}, K^{old}_{L_{c(new2)}})$
$BS_{old} \rightarrow C_{old}\ Enc_{K_{L_{c(old)}}} MovedNode(ID_a, ID_a^m, MovTime)$
Ensure: $(x_{C_{new}}, y_{C_{new}}), K_{L_{c(temp)}}, K^{BS_{old}}_{L_{c(new2)}}$

5.3.1.2 Global handover

In the case of node mobility between two cells belonging to different BSs, it is crucial to report this movement to different entities in the WSN:

- The BS (BS_{old}) covers its original cell (C_{old}): in order to remove this node's credentials from its database to:
  - Thwart attackers from cloning identity of the mobile node.
  - Prevent the mobile node from encrypt/decrypt messages to/from nodes of (C_{old}).
- The entire set of nodes in C_{old}: In order to update the e value and overcome the criticality of considering the mobile node as a node which does not record that event, hereafter know as a "**Dereporter Node**".
- The BS (BS_{new}) covers its destination cell (C_{new}) : in order to legitimize the new node and to generate the required credentials.
- The whole node within C_{new}: In order to legitimize the new node as a "**Reporter Node**" and update the value of e.

To achieve the global handover process, three means of communication are used:

1. BS-BS communication via a Backbone link between each of the two BSs such as: fibre optic, terrestrial and satellite microwave.

2. One hop communication between the BS and remote cells as mentioned in Chapter 1 and Chapter 3.

3. cell-by-cell communication between the mobile node and the BS.

As same as local handover, global handover can be classified into: Intended and Non-intended, as shown in Fig. 5.4 and Fig. 5.5 respectively. Moreover, both classes are illustrated by Algorithm. 5.14 and Algorithm. 5.15.

Algorithm 5.14 *Intended global handover procedure followed when a node a is moved from BS_{old} coverage area to BS_{new} coverage area*

Require: $K, ID_a, ID_a^m, (x_{C_{new}}, y_{C_{new}}), (x_{C_{old}}, y_{C_{old}}), MovTime, \boldsymbol{S}, K_a^{BS_{old}}, \tau$

$a \rightarrow * \ (C_{old})$: $Enc_{K_{L_{c(old)}}} ImMoving(ID_a, ID_a^m, (x_{C_{new}}, y_{C_{new}}), MovTime)$

for all cell-mates (α) **do**

$\alpha \rightarrow BS_{old}$: $Enc_{K_{L_{c(old)}}} MovingNode(ID_a, ID_a^m, (x_{C_{new}}, y_{C_{new}}), MovTime)$

end for

$BS_{old} \rightarrow C_{old}\ Enc_{K_{L_{c(old)}}} \{Akn\}$

$BS_{old} \rightarrow a\ Enc_{K_a^{BS(old)}} Akn(K_{L_{c(temp)}}, K_a^{BS_{new(temp)}})$

$BS_{old} \rightarrow BS_{new}\ Enc_{K_{BS_{old}}^{BS_{new}}} AddNode(ID_a, ID_a^m, MovTime, K_a^{BS_{new(temp)}})$

$BS_{new} \rightarrow C_{new}\ Enc_{K_{L_{c(new)}}} AddNode(ID_a, ID_a^m, K_{L_{c(temp)}})$

$BS_{new} \rightarrow a\ Enc_{K_a^{BS_{new(temp)}}} Ack(ID_a, ID_a^m, K_{L_{c(temp)}})$

$a \rightarrow * \ (C_{new})$: $Enc_{K_{L_{c(temp)}}} Hello(ID_a, ID_a^m, (\boldsymbol{x_{C_{new}}}, \boldsymbol{y_{C_{new}}}), MovTime)$

$C_{new} \rightarrow BS_{new}\ Enc_{K_{L_{c(new)}}} NewNode((\boldsymbol{x_c}, \boldsymbol{y_c}), ID_a, ID_a^m,)$

$C_{new} \rightarrow a\ Enc_{K_{L_{c(temp)}}} Ack(\tau)$

for $C_{new} \cup a$ **do**

$K_\tau \leftarrow K \| \tau$

$\boldsymbol{x_c} \leftarrow 0.5 \left\lceil \frac{x - \boldsymbol{S_1}}{\Delta} \right\rceil, \boldsymbol{y_c} \leftarrow 0.5 \left\lceil \frac{y - \boldsymbol{S_2}}{\Delta} \right\rceil$

$$\boldsymbol{K}^{\boldsymbol{M}}_{\boldsymbol{L_{c(new2)}}} \leftarrow \begin{bmatrix} H(K_\tau \| \boldsymbol{x_c}(1) \| \boldsymbol{y_c}(1)) \\ H(K_\tau \| \boldsymbol{x_c}(2) \| \boldsymbol{y_c}(2)) \\ . \\ . \\ H(K_\tau \| \boldsymbol{x_c}(M) \| \boldsymbol{y_c}(M)) \end{bmatrix}$$

end for

$C_{new} \rightarrow BS_{new}\ Enc_{K_{L_{c(new)}}} NewCellKey((\boldsymbol{x_c}, \boldsymbol{y_c}), \{CellMateList\}, K_{L_{c(new2)}})$

$K_a^{BS_{new}} \leftarrow H(K \| ID_a \| x_0^{new} \| y_0^{new})$

$BS_{new} \rightarrow BS_{old}\ Enc_{K_{BS_{new}}^{BS_{old}}} Ack(ID_a, ID_a^m, MovTime)$

$BS_{old} \rightarrow C_{old}\ Enc_{K_{L_{c(old)}}} MovedNode(ID_a, BS_{new}, C_{new})$

Ensure: $K_{L_{c(temp)}}, K_a^{BS_{new(temp)}}, K_{L_{c(new2)}}$

Algorithm 5.15 *Non-intended global handover procedure followed when a node a is moved from BS_{old} coverage area to BS_{new} coverage area*

Require: $K, ID_a, ID_a^m, (x_{C_{new}}, y_{C_{new}}), (x_{C_{old}}, y_{C_{old}}), MovTime, \boldsymbol{S}, K_a^{BS_{old}}, \tau$
$a \rightarrow * \ (C_{new})$: $Enc_K \ Hello(ID_a, ID_a^m, (\boldsymbol{x_{C_{new}}}, \boldsymbol{y_{C_{new}}}), MovTime)$
$C_{new} \rightarrow BS_{new} \ Enc_{K_{L_{c(new)}}} NewNode((\boldsymbol{x_c}, \boldsymbol{y_c}), ID_a, ID_a^m, MovTime)$
$BS_{new} \rightarrow BS_{old} \ Enc_{K_{BS_{new}}^{BS_{old}}} NewNode(ID_a, ID_a^m, MovTime)$
$BS_{old} \rightarrow BS_{new} \ Enc_{K_{BS_{old}}^{BS_{new}}} NodeKeys(ID_a, K_a^{BS_{old}})$
$BS_{new} \rightarrow C_{new} \ Enc_{K_{L_{c(new)}}} Ack(ID_a, ID_a^m, MovTime, K_{L_{c(temp)}})$
$BS_{new} \rightarrow a \ Enc_{K_a^{BS_{old}}} Ack(ID_a, ID_a^m, MovTime, K_{L_{c(temp)}}, K_a^{BS_{new(temp)}})$

for $C_{new} \cup a$ **do**
$K_\tau \leftarrow K \| \tau$
$\boldsymbol{x_c} \leftarrow 0.5 \left\lceil \frac{x - \boldsymbol{S_1}}{\Delta} \right\rceil, \boldsymbol{y_c} \leftarrow 0.5 \left\lceil \frac{y - \boldsymbol{S_2}}{\Delta} \right\rceil$

$$\boldsymbol{K}_{\boldsymbol{L_{c(new2)}}}^{\boldsymbol{M}} \leftarrow \begin{bmatrix} H(K_\tau \| \boldsymbol{x_c}(1) \| \boldsymbol{y_c}(1)) \\ H(K_\tau \| \boldsymbol{x_c}(2) \| \boldsymbol{y_c}(2)) \\ . \\ . \\ H(K_\tau \| \boldsymbol{x_c}(M) \| \boldsymbol{y_c}(M)) \end{bmatrix}$$

end for
$C_{new} \rightarrow BS_{new} \ Enc_{K_{L_{c(new)}}} NewCellKey((\boldsymbol{x_c}, \boldsymbol{y_c}), \{CellMateList\}, K_{L_{c(new2)}})$
$K_a^{BS_{new}} \leftarrow H(K \| ID_a \| x_0^{new} \| y_0^{new})$
$BS_{new} \rightarrow BS_{old} \ Enc_{K_{BS_{new}}^{BS_{old}}} Ack(ID_a, ID_a^m, MovTime)$
$BS_{old} \rightarrow C_{old} \ Enc_{K_{L_{c(old)}}} MovedNode(ID_a, BS_{new}, C_{new})$

Ensure: $K_{L_{c(temp)}}, K_a^{BS_{new(temp)}}, K_{L_{c(new2)}}$

5.4 Communication overhead

In order to assess the proposed protocols, the number of messages disseminated through the network, which is defined as "**communication overhead**", is investigated mathematically and then measured based on a simulation environment built using the Contiki OS Cooja simulator [127] and MATLAB. For all key management schemes, the served region by the WSN is assumed to be a square terrain of size A where N nodes are uniformly distributed around the terrain as shown in Fig. 5.6. Because of the uniform distribution, the number of nodes deployed on each side of the terrain is considered to be ($\approx \sqrt{N}$). The size of each packet constituting the generated report, acknowledgement message and bootstrapping correspondences are assumed to be of a fixed size (λ) Bytes. As described previously, LKMP-SBS, LKMP-MBS and ELKMP-MBS are sharing three main phases: Setup, Report Generation and Key Revocation. In this section, the communication over-

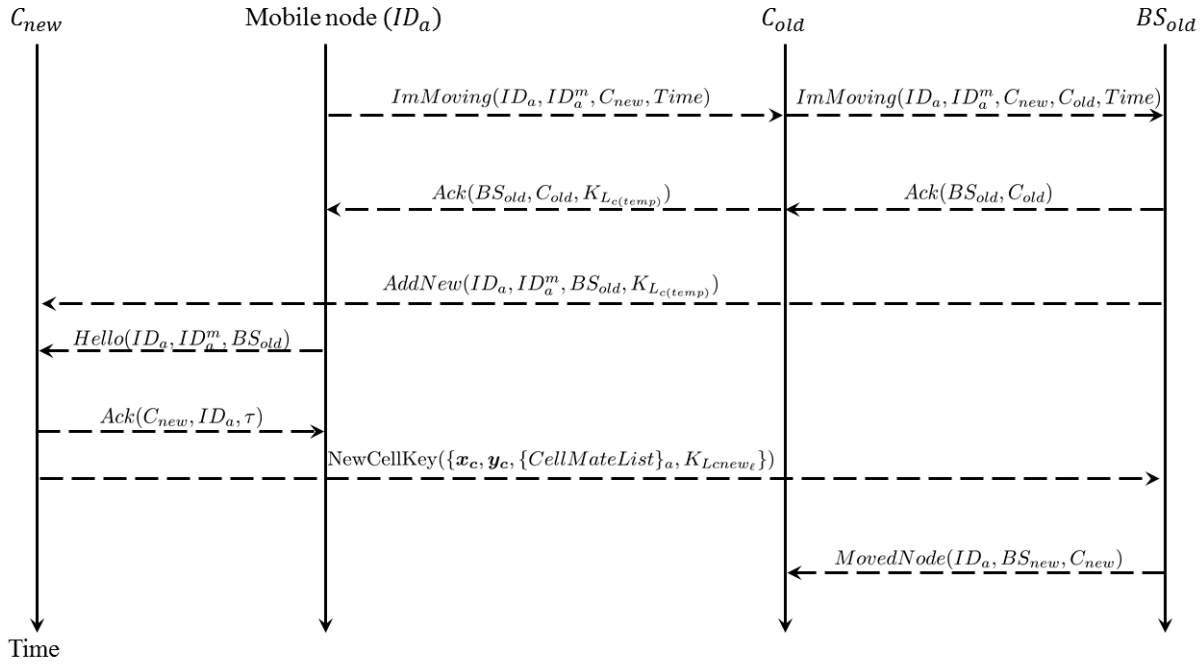


Figure 5.2: Message sequence chart of the intended mobility local handover.

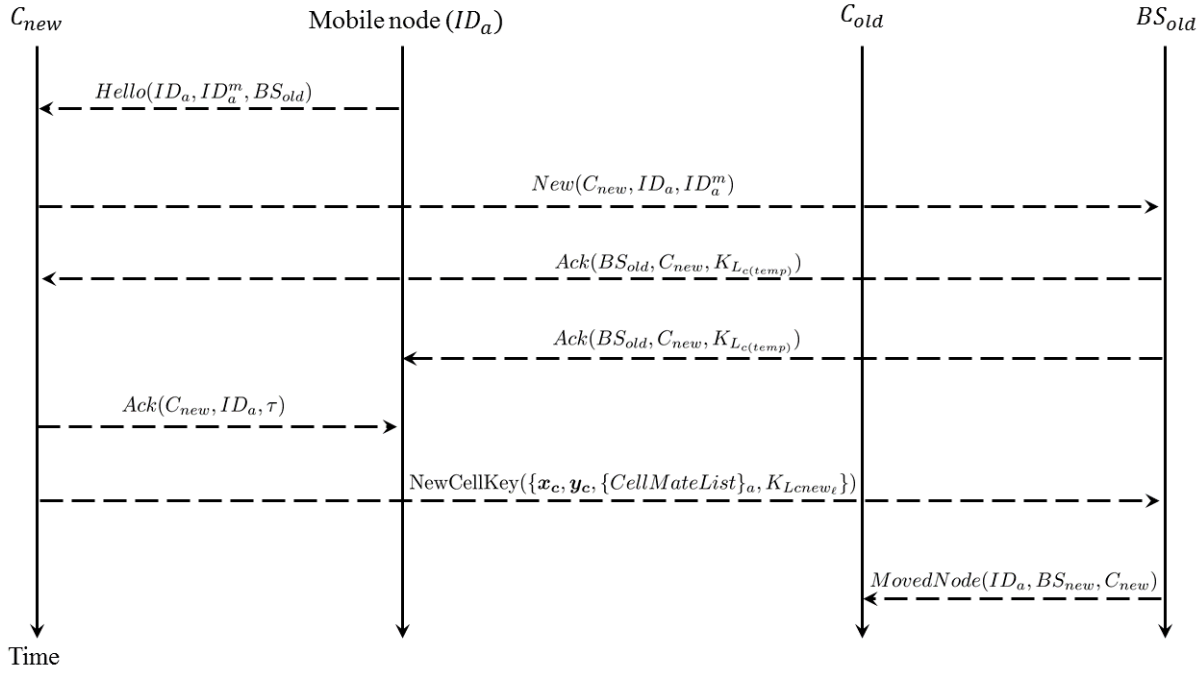


Figure 5.3: Message sequence chart of the Non-intended mobility local handover.

head caused by the 1^{st} and the 2^{nd} phases is considered while the communication cost of the revocation phase will be analysed in a separate section.

As a new terminology, *NodalDistance* is introduced to express the distance between any two point or regions in a WSN defined as:

- In traditional protocols: *The approximate number of nodes lying in a straight line between two zones.*

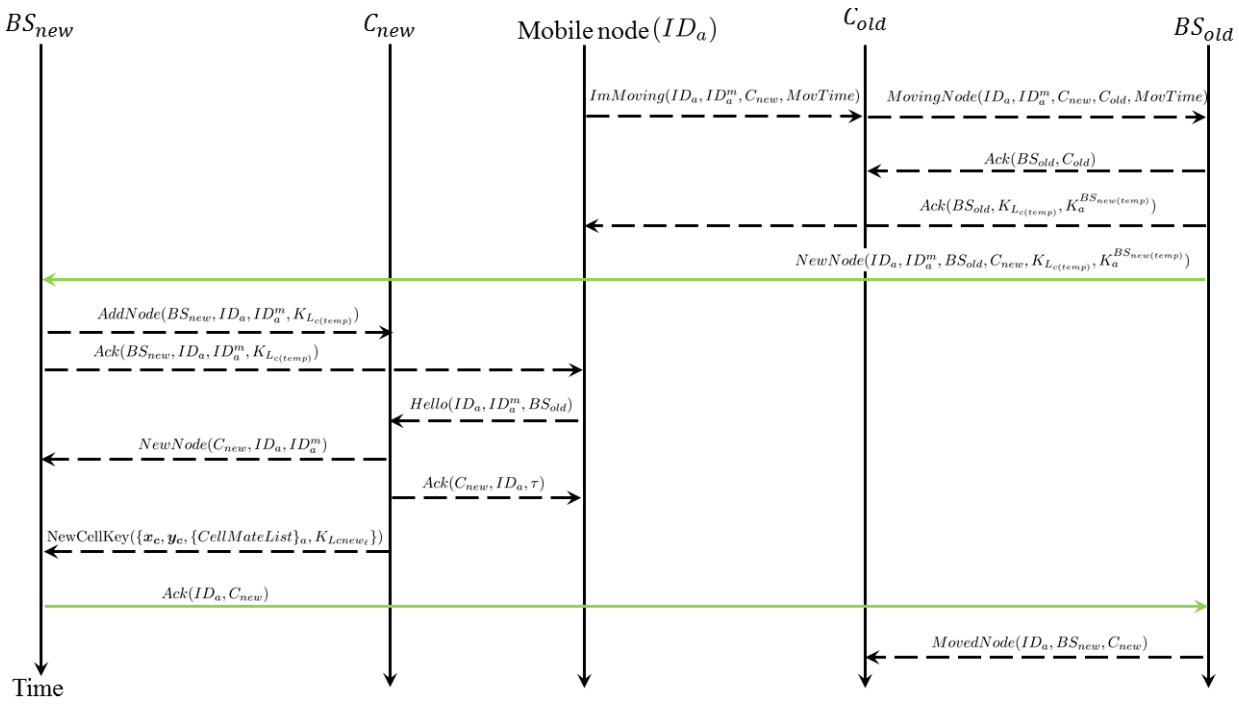


Figure 5.4: Message sequence chart of the intended mobility global handover followed when a node a is moved from BS_{old} coverage area to BS_{new} coverage area .

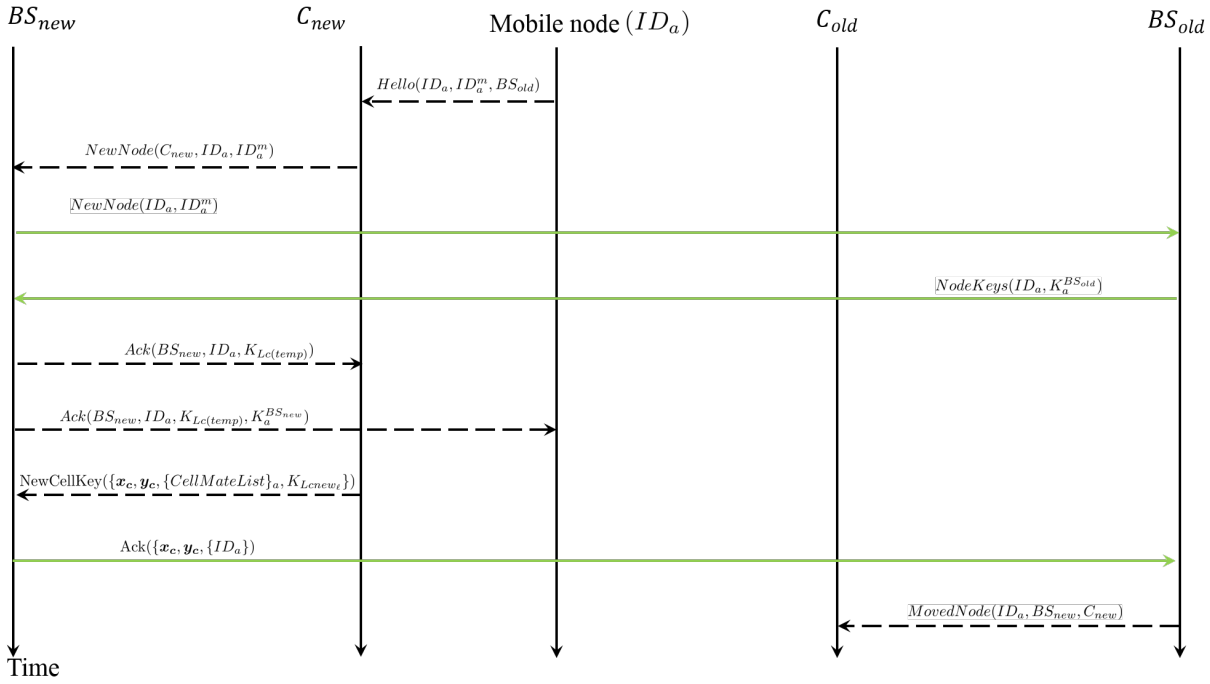


Figure 5.5: Message sequence chart of the Non-intended mobility global handover followed when a node a is moved from BS_{old} coverage area to BS_{new} coverage area.

- LKMP-SBS, LKMP-MBS and MELKMP-MBS: *The approximate number of cells lying in a straight line between two zones.*

For the traditional protocols such as MKMP [21] and LEDS [20], all nodes constituting the $NodalDistance$ between two nodes A and B are participating in message delivery

between them using a node by node communication in the worst case scenario. Hence, in the square terrain constituting of N nodes, where ($\approx \sqrt{N}$) nodes are lying on each side, the longest $NodalDistance$ is its diameter ($\approx \sqrt{2N}$).
On the other hand, all cells constituting the $NodalDistance$ between two zones A and B are participating in message delivery between them using a cell by cell communication in the proposed schemes. Hence, in the square terrain constituting of N nodes, where ($\approx \sqrt{\frac{N}{n}}$) nodes are lying on each side, the longest $NodalDistance$ is its diameter ($\approx \sqrt{2\frac{N}{n}}$). Therefore, as a worst case scenario where the originating cell (C_{org}) is located in one corner while the related BS is located in an opposite corner, the communication overhead is calculated as a summation of the following items :

- Setup Phase:

  1. CC_{set}: Communication cost of transmitting the setup phase messages from the (C_{org}) to BS.
  2. CC_{set_Ack}: Communication cost of acknowledging (C_{org}) by the BS.

- Report Generation Phase:

  3. CC_{Rep_Req}: Communication cost of requesting a report from the (C_{org}) by the BS.
  4. CC_{Rep_Gen}: Communication cost of creating a report inside the (C_{org}).
  5. CC_{Rep_Send}: Communication cost of sending the generated report from the (C_{org}) to the BS.

5.4.1 MELKMP-MBS

The calculation of MELKMP-MBS communication overhead is based on two main parameters:

1. Implementation of the setup phase and report generation phase: CC_{set}, CC_{set_Ack}, CC_{Rep_Req} CC_{Rep_Gen} and CC_{Rep_Send}.
2. Mobility communication cost $CC_{mobility}$, which is related to overhead implementation, in case of a node mobility.

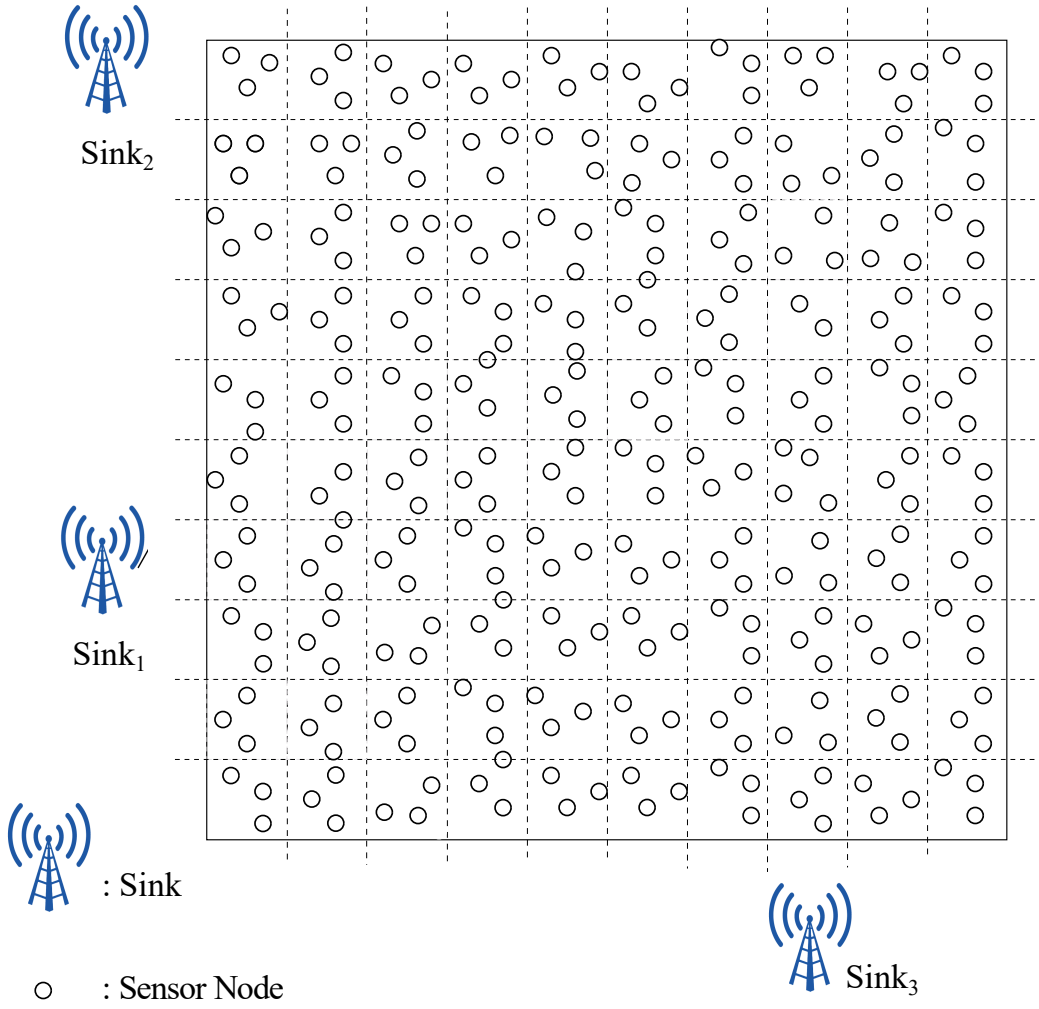


Figure 5.6: A square terrain of size A divided into 100 cells and covered by a WSN consists of $N = 300$ where each side contains $\backsimeq \sqrt{300}$.

As a result, the entire communication overhead might be expressed as:

$$CC_{MELKMP-MBS} = \widehat{CC}_{MELKMP-MBS} + CC_{mobility} \tag{5.2}$$

Where the derivition of both terms is described briefly in following sections

5.4.1.1 Communication Overhead of Setup Phase and Report Generation Phase

First of all, during the setup phase, each node a out of the n nodes inside C_{org} sends its $\{LIST\}_a$ as described in Algorithm 4.7. Due to the uniform distribution, every node has a similar number of cell-mates and accordingly the communication cost of this phase is $n\lambda$ which is the number of messages generated by the C_{org}. However, this message will be re-sent by each cell alongside the $NodalDistance$ which has a very long distance in the worst case scenario. The length of $NodalDistance$ is $\ggg n$ for MELKMP-MBS, LEDS

and MKMP. As a result, the communication cost of the setup phase is ($CC_{set} \simeq \sqrt{2\frac{N}{n}}\lambda$), ($CC_{set} \simeq \sqrt{2N}\lambda$) for MELKMP-MBS, MKKMP/LEDS respectively. On the other hand, the communication cost related to all BS acknowledgements is λ in MELKMP-MBS due to the single node communication pattern followed in the BS-cell communication. In contrast, it is ($\simeq \sqrt{2N}\lambda$) in LEDS/MKMP due to the node to node communication pattern followed there.

Secondly, all mentioned protocols are sharing the same process of event report generation by a particular cell where all n nodes are participating. As a result, the communication cost of report generation is $CC_{Rep\_Gen} \simeq n\lambda$. However, these protocols differ in the value of CC_{Rep_Req} where it is $CC_{Rep\_Req} \simeq \lambda$, $CC_{Rep\_Req} \simeq \sqrt{2N}\lambda$ for MELKMP-MBS, LKMP/LEDS respectively due to the difference in communication pattern followed to achieve the BS-cell communication. Also, $CC_{Rep\_Send} \simeq \sqrt{2\frac{N}{n}}\lambda$, $CC_{Rep\_Send} \simeq \sqrt{2N}\lambda$ for the MELKMP-MBS, LKMP/LEDS respectively due to the difference in communication pattern followed to achieve the Cell-BS communication. The communication cost patterns are illustrated in Table. 5.1 and accordingly, the entire communication cost, for each protocol, is expressed as:

$$\widehat{CC}_{MELKMP-MBS} = \lambda(2\sqrt{2\frac{N}{n}} + n + 2) \tag{5.3}$$

$$CC_{LEDS} = \lambda(4\sqrt{2N} + n) \tag{5.4}$$

$$CC_{MKMP} = \lambda M(4\sqrt{2N} + n) \tag{5.5}$$

Table 5.1: Communication cost analysis for LEDS/MKMP and LKMP-SBS

Communication Cost pattern(CC)	**MKMP/LEDS**	**MELKMP-MBS**
CC_{set}	$\sqrt{2N}\lambda$	$\sqrt{2\frac{N}{n}}\lambda$
CC_{set_Ack}	$\sqrt{2N}\lambda$	λ
CC_{Rep_Req}	$\sqrt{2N}\lambda$	λ
CC_{Rep_Gen}	$n\lambda$	$n\lambda$
CC_{Rep_Send}	$\sqrt{2N}\lambda$	$\sqrt{2\frac{N}{n}}\lambda$

Moreover, according to [134]:

$$CC_{SODD} = N\lambda + \frac{4N}{\sqrt{n}}\lambda + kmn\iota + kc(m\lambda + d)\sqrt{2N} \tag{5.6}$$

$$CC_{TTDD} = kmN\lambda + kcd\sqrt{N} \tag{5.7}$$

Where, based on the system specifications shown in [21, 134], k is the number of BSs, m is the number of cells traversed by each mobile BS, $0 \leq c \leq \sqrt{2}$ and d is the number of data packets received from a particular cell. To be consistent, a single stationary BS is assumed $(k, m = 1)$ for TTDD and SODD. Also, $(M = 1)$ is considered for the MKMP. Therefore, it is reflected by the same graph of LEDS.

5.4.1.2 Communication Overhead of Node Mobility

In this section, the derivation of $CC_{mobility}$, which is related to overhead implementation in the case of a node mobility, is presented. As described in Section. 5.3.1, a set of messages is disseminated through the network between the mobile node and its cell mate in C_{old}, cell mates in C_{new}, BS_{old} and BS_{new} according to the mobility nature and the implemented handover. The communication overhead caused by these actions is affected mainly by following parameters:

1. Node speed υ and mobility duration t.
2. Number of mobile nodes.
3. Number and the type of occurred handover.

As a worst case scenario, m nodes are considered to be moving inside a WSN coverage area where each node is travelling at a speed of $\upsilon\ m/s$. Regarding this mobility, the related BS (BS_{old} or BS_{new}) is located at the farthest distance away from both of C_{old} and C_{new} where: $NodalDistance = \sqrt{2\frac{N}{n}}$. The node trajectory is considered to be traversing as much cells as possible. Therefore, mobile nodes are assumed to pass through each cell via the shortest path which is the "cell side = λ" in case of square cells. As a result, a mobile node is passing through $\frac{\upsilon t}{\lambda}$ cells during its movement. Hence, there are $\frac{\upsilon t}{\lambda}$ local handovers occurred during this journey. However, it is crucial to determine the number of global handovers when a node is moving from one BS coverage to another BS coverage area. Therefore, a new term **Cellular Area** (CA) is defined as:
The number of cells inside a WSN coverage area"
Assuming that the cellular area is divided adequately between all BSs, CA of the ℓ^{th} BS is:

$$\begin{aligned} CA_{\ell} &= \frac{N^{'}}{M} \\ &= \frac{N}{nM} \end{aligned} \tag{5.8}$$

Accordingly, the number of cells that are visited by a mobile node (r) until it reaches the coverage area of an adjacent BS can be estimated based on the shape of BS coverage area as shown in Fig. 5.7, 5.8 and 5.9 to be:

$$r = \begin{cases} \sqrt{\frac{N}{nM}} & \text{Square coverage} \\ \sqrt{\frac{N}{\pi nM}} & \text{Circular coverage} \\ \sqrt{\frac{N}{2\sqrt{3}nM}} & \text{Hexagonal coverage} \end{cases} \tag{5.9}$$

It is obvious that, regardless of the assumed shape of BS coverage, a global handover occurs after traversing r cells by the mobile nodes. As a result, the approximate number of global handovers is:

$$GH(t) = \left\lfloor \frac{\upsilon t}{\Delta r} \right\rfloor \tag{5.10}$$

On the other hand, the approximate number of local handovers is:

$$LH(t) = \frac{\upsilon t}{\Delta} - \left\lfloor \frac{\upsilon t}{\Delta r} \right\rfloor \tag{5.11}$$

Hence, $CC_{mobility}$ as a function of time is illustrated as:

$$CC_{mobility}(t) = GH(t) \times CC_{GH} + LH(t) \times CC_{LH} \tag{5.12}$$

Where:
CC_{GH}: Communication cost of global handover. CC_{LH}: Communication cost of local handover.

CC_{GH} and CC_{LH} are calculated according to their message sequence chart shown in Fig.5.2, 5.3, 5.4 and 5.5 as:
Assume that each message sent during the handover process, discussed in Section. 5.3.1, has a length of λ following a consideration of:

- The cost of each report sent from a cell to a BS is $(n-1)\lambda \times NodalDistance$ because it is generated by all nodes except the mobile node and forwarded through

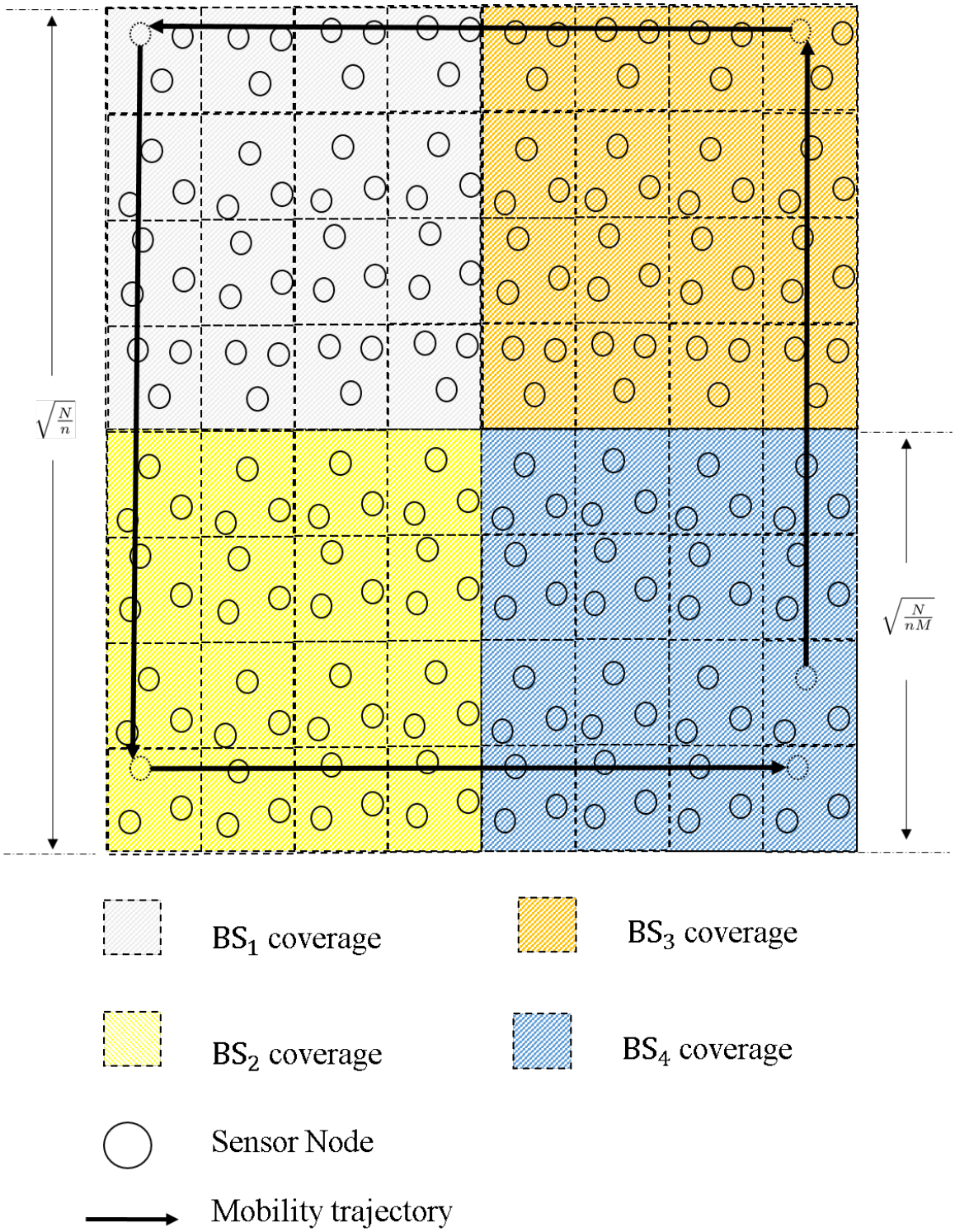


Figure 5.7: Node mobility in a square terrain consist of N nodes, $N' = \frac{N}{n}$ cells and covered by 4 BS each one has a square coverage.

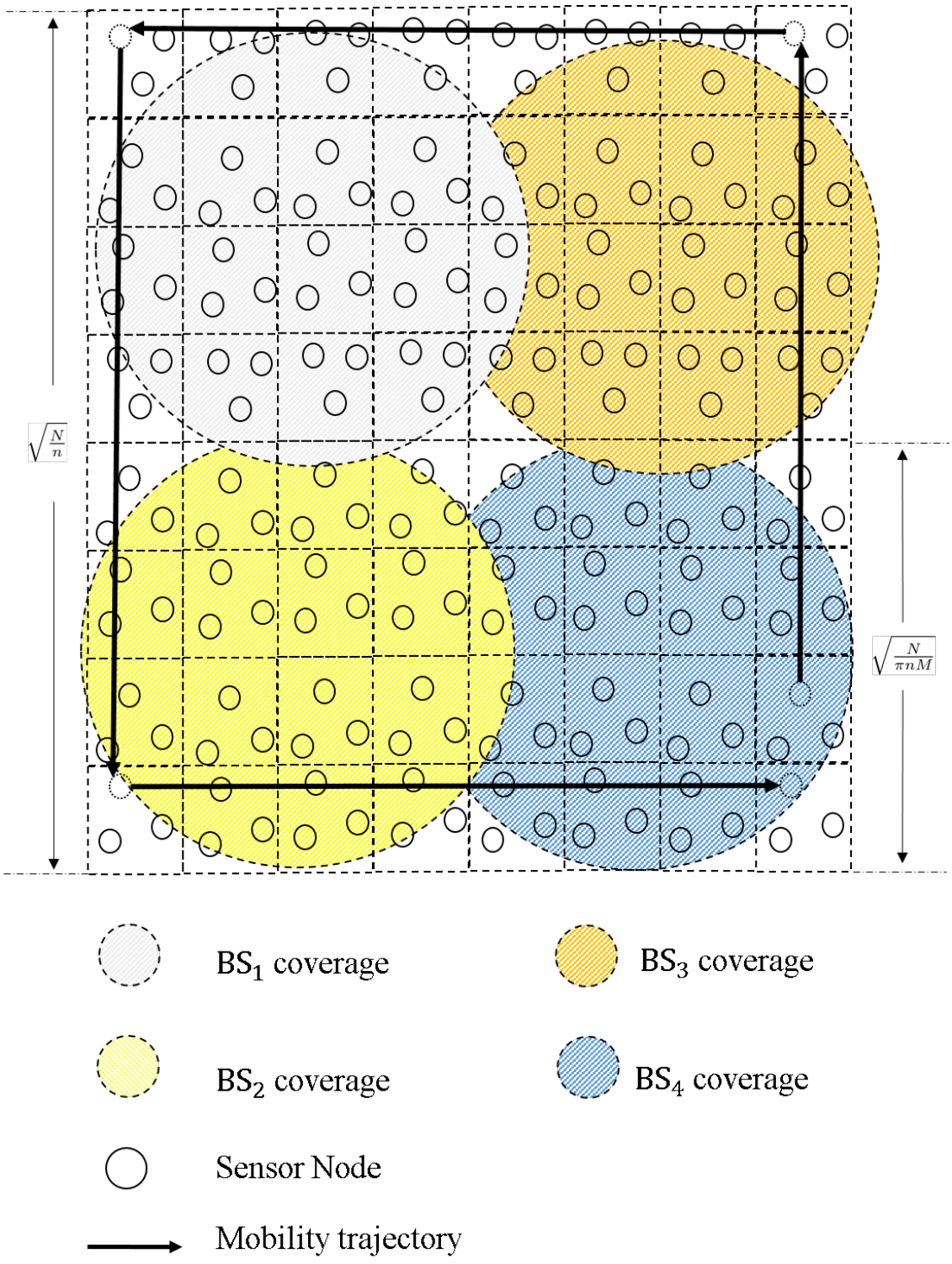


Figure 5.8: Node mobility in a square terrain consist of N nodes, $N^{'} = \frac{N}{n}$ cells and covered by 4 BS each one has a circular coverage.

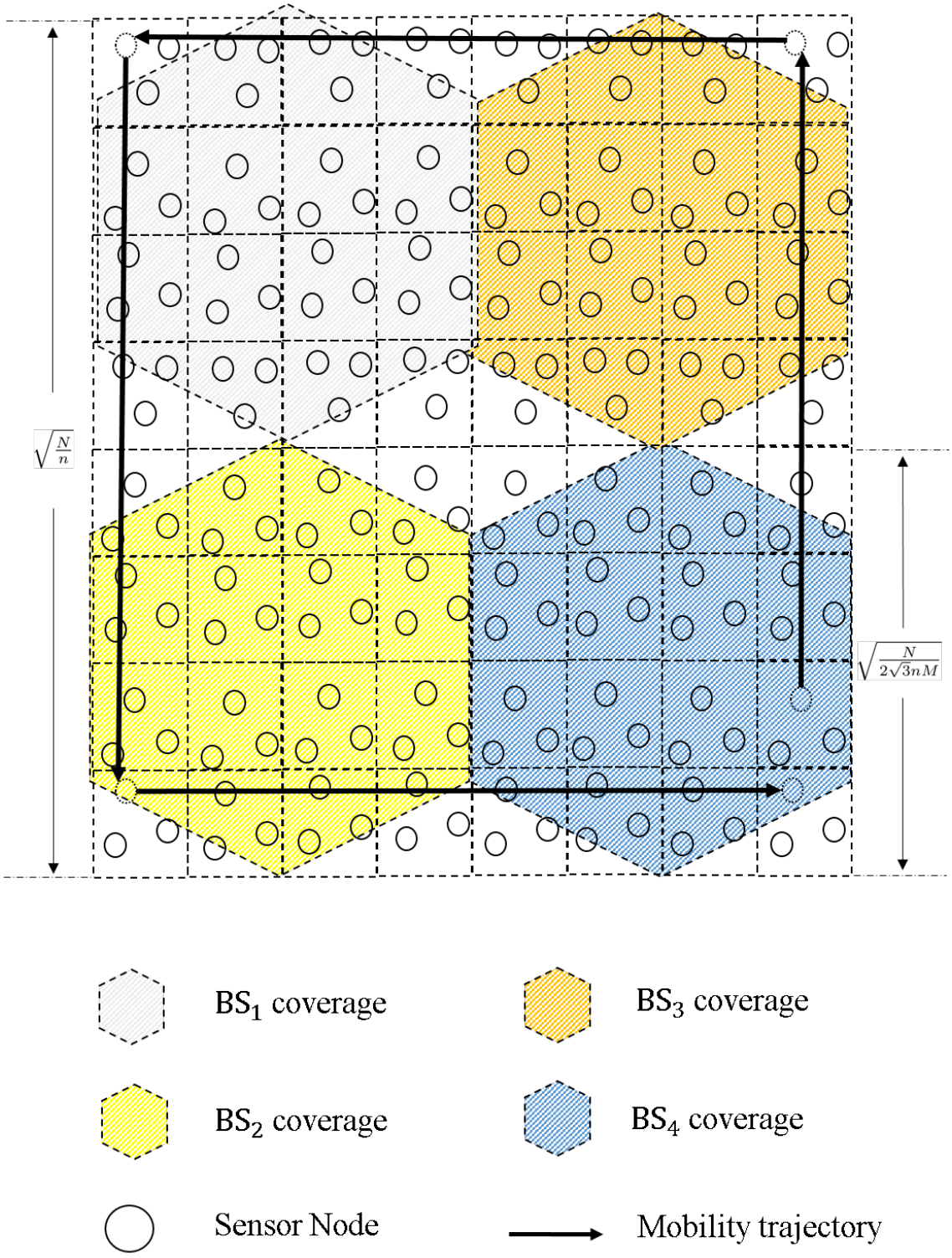


Figure 5.9: Node mobility in a square terrain consist of N nodes, $N^{'} = \frac{N}{n}$ cells and covered by 4 BS each one has a hexagonal coverage.

$NodalDistance$ of nodes/cells.

- The cost of each report sent from a cell to the mobile node is $(n-1)\lambda$.

In contrast, messages between BSs are assumed to be of length Λ. Therefore:

$$\begin{aligned} CC_{LH} \text{ (Intended Mobility)} &= 5\lambda + (n-1)\lambda + 3(n-1)\sqrt{2\frac{N}{n}} \\ &= \lambda\Big[3(n-1)\sqrt{2\frac{N}{n}} + n + 4\Big] \end{aligned} \tag{5.13}$$

$$\begin{aligned} CC_{LH} \text{ (Non-Intended Mobility)} &= 4\lambda + (n-1)\lambda + 2(n-1)\sqrt{2\frac{N}{n}} \\ &= \lambda\Big[2(n-1)\sqrt{2\frac{N}{n}} + n + 3\Big] \end{aligned} \tag{5.14}$$

$$\begin{aligned} CC_{GH} \text{ (Intended Mobility)} &= 7\lambda + (n-1)\lambda + 3(n-1)\sqrt{2\frac{N}{n}} + 2\Lambda \\ &= \lambda\Big[3(n-1)\sqrt{2\frac{N}{n}} + n + 6\Big] + 2\Lambda \end{aligned} \tag{5.15}$$

$$\begin{aligned} CC_{GH} \text{ (Non-Intended Mobility)} &= 4\lambda + 2(n-1)\sqrt{2\frac{N}{n}} + 3\Lambda \\ &= \lambda\Big[2(n-1)\sqrt{2\frac{N}{n}} + 4\Big] + 3\Lambda \end{aligned} \tag{5.16}$$

The main target is to analyse the communication overhead inside the WSN caused by using MELKMP-MBS, therefore, Λ is considered to be zero while the BS-BS communication is implemented via a different link and has no overhead in the network. As a result, a simulation is implemented and the recorded $CC_{mobility}$ is depicted in Fig. 5.11, Fig. 5.12 and Fig. 5.13.

It is obvious from (5.2), (5.12), (5.13), (5.14), (5.15), (5.16) that:

$$CC_{mobility} \gg \widehat{CC}_{MELKMP-MBS} \tag{5.17}$$

Based on simulation results and above equations, this overhead has following relationships with the other network parameters:

1. $CC_{mobility} \propto \frac{1}{r}$: Where increasing the radius of BS coverage will reduce the number of global handovers and, as a result, decrease the value of $GH(t)$ at a particular moment. However, this requires physical modification in the BS structure and increases the power cost. In addition, any modification to BS coverage specification will contravene the control topology of the WSN.

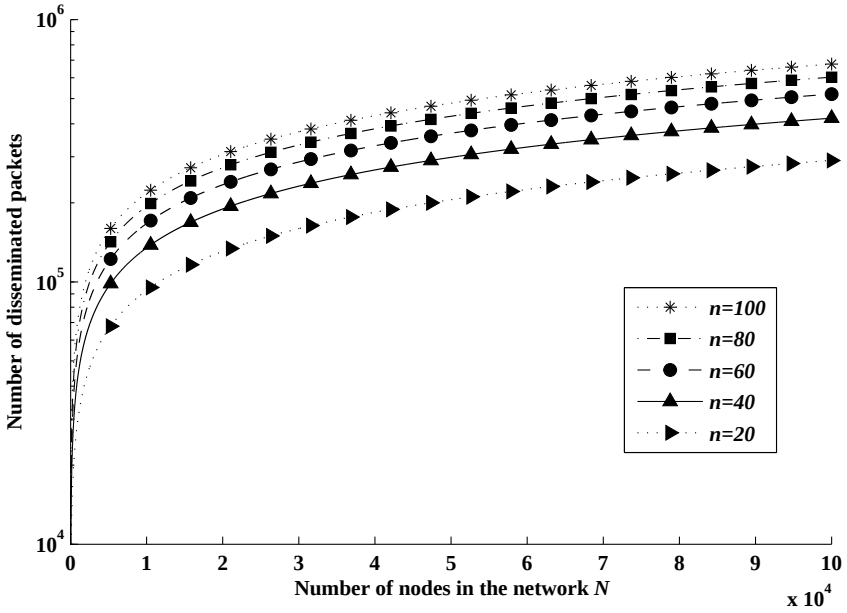


Figure 5.10: Comparison between communication cost of ELKMP-MBS for different values of n, N.

2. $CC_{mobility} \propto \upsilon \propto t$: This obviously happens when the number of visited cells by a fast mobile node is greater than that visited by a slower mobile node. Also, the same mobile node is visiting more cells when the travelling duration is increased. In our simulation, the average speed of a walking human $1.2m/s$ [135] is considered.

3. $CC_{mobility} \propto n$: This is proved by simulation results as shown in Fig. 5.10. The reason behind this is the increment in the messages created by the nodes inside C_{old} and C_{new} during the implementation of local and global handover.

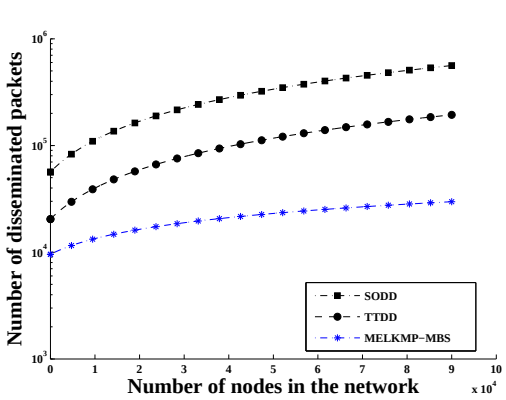
4. $CC_{mobility} \propto N$: The increment in the value of N increases the number of cells and leads to a significant increment in local handover occurrence.

5.4.2 LKMP-SBS

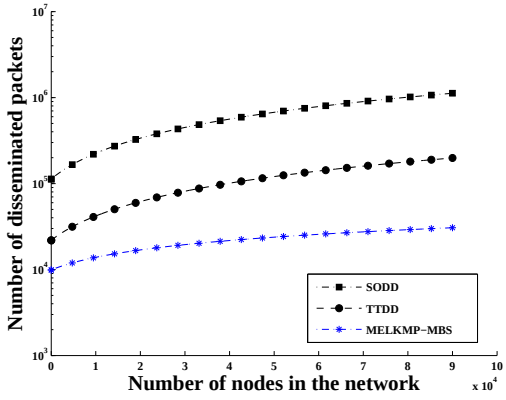
The communication overhead of LKMP-SBS is illustrated using the same analysis of the previous sections where only the communication overhead of implementing the setup phase and report generation phase are considered with $M = 1$:

$$CC_{LKMP-SBS} = \lambda(2\sqrt{2\frac{N}{n}} + n + 2) \tag{5.18}$$

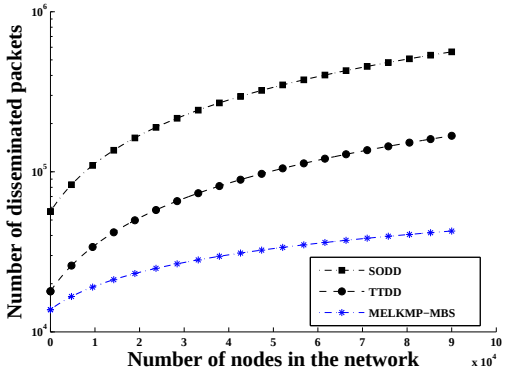
For different values of n, LKMP-SBS, MKMP, LEDS, SODD and TTDD are simulated as shown in Fig. 5.14, 5.15, 5.16, 5.17, 5.18, 5.19, 5.20, 5.21.



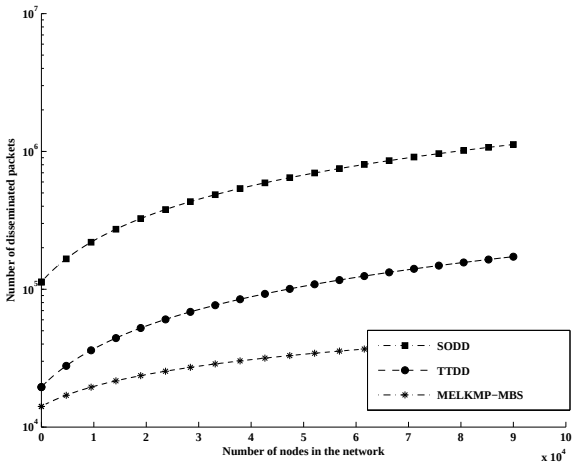
(a) $n = 20, M = 4$



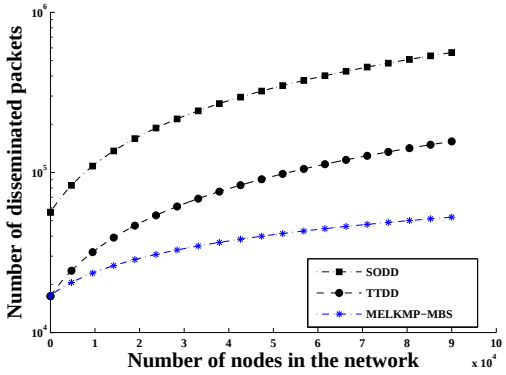
(b) $n = 20, M = 8$



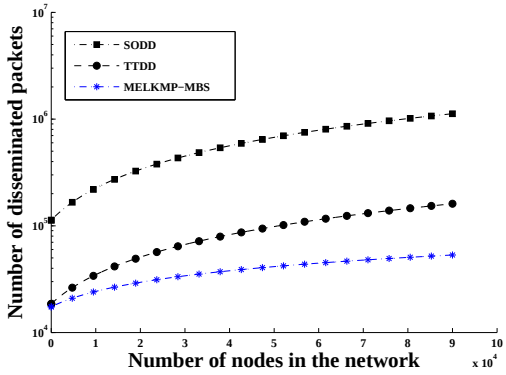
(c) $n = 40, M = 4$



(d) $n = 40, M = 8$

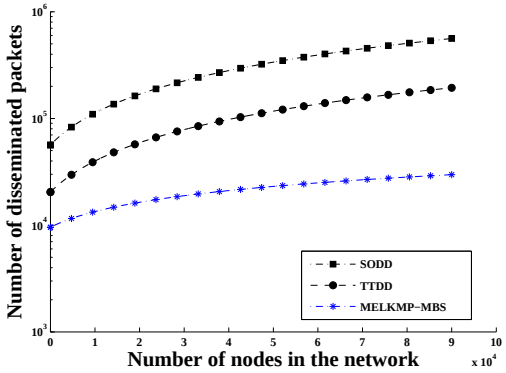


(e) $n = 60, M = 4$

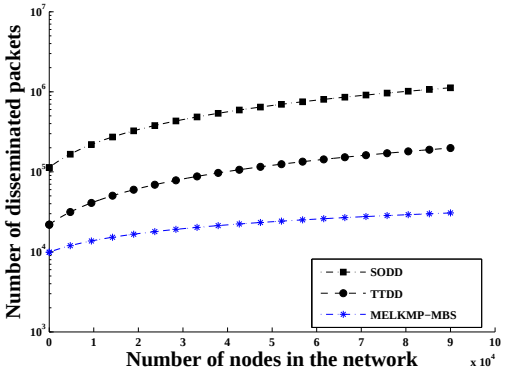


(f) $n = 60, M = 8$

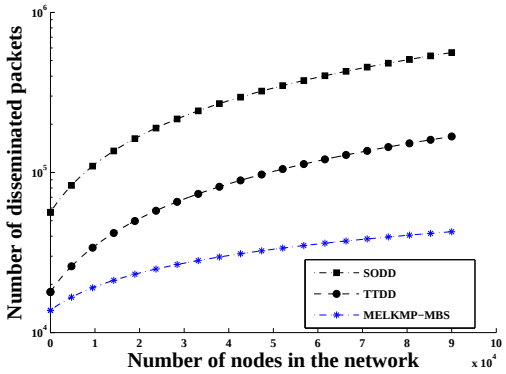
Figure 5.11: Communication overhead vs. N for MELKMP-MBS, SODD and TTDD (Circular BS coverage, intended mobility, $d = 100$ packet, $\lambda = 1$ packet).



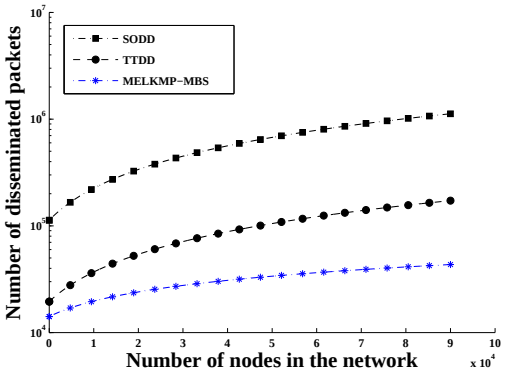
(a) $n = 20, M = 4$



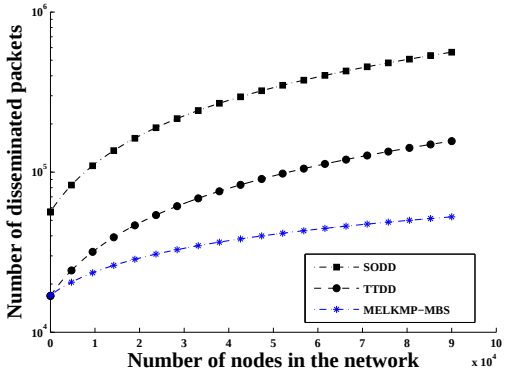
(b) $n = 20, M = 8$



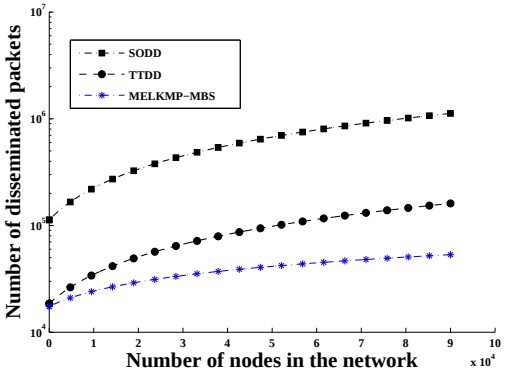
(c) $n = 40, M = 4$



(d) $n = 40, M = 8$

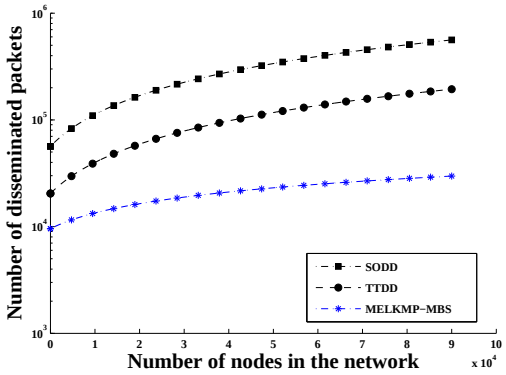


(e) $n = 60, M = 4$

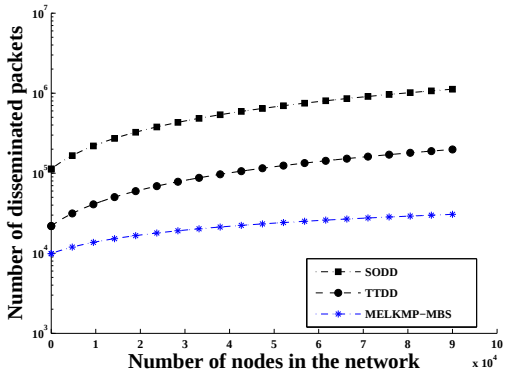


(f) $n = 60, M = 8$

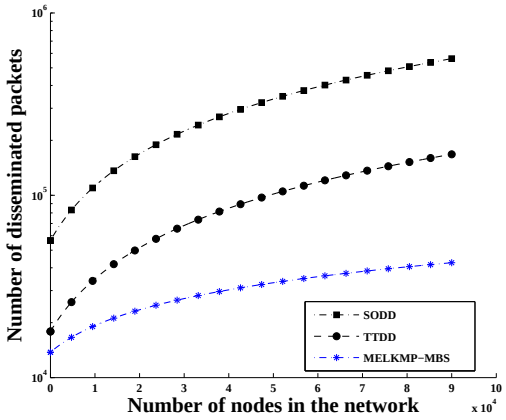
Figure 5.12: Communication overhead vs. N for MELKMP-MBS, SODD and TTDD (Hexagonal BS coverage, intended mobility, $d = 100$ packet, $\lambda = 1$ packet).



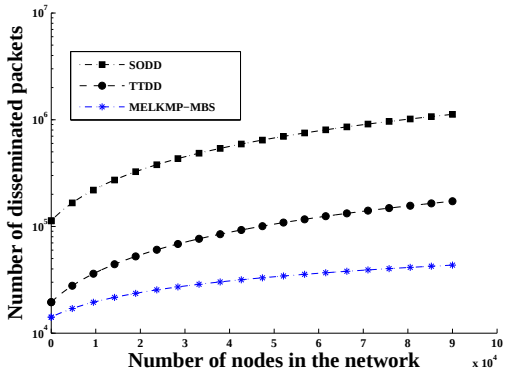
(a) $n = 20, M = 4$



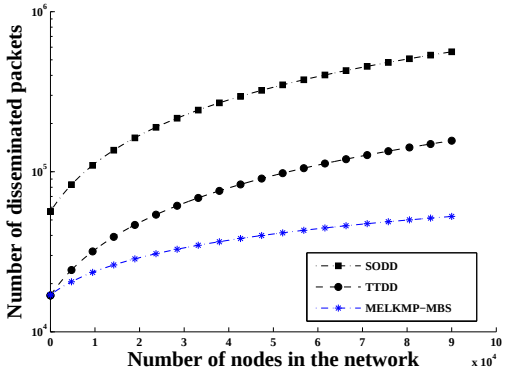
(b) $n = 20, M = 8$



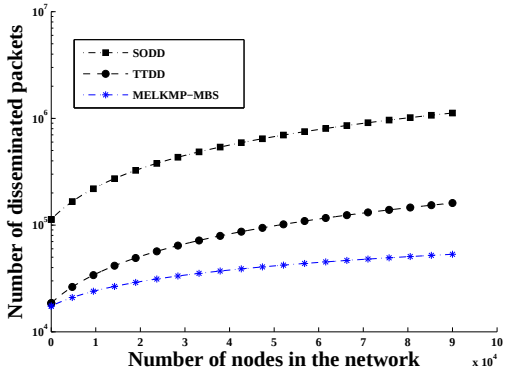
(c) $n = 40, M = 4$



(d) $n = 40, M = 8$



(e) $n = 60, M = 4$



(f) $n = 60, M = 8$

Figure 5.13: Communication overhead vs. N for MELKMP-MBS, SODD and TTDD (Square BS coverage, intended mobility, $d = 100$ packet, $\lambda = 1$ packet).

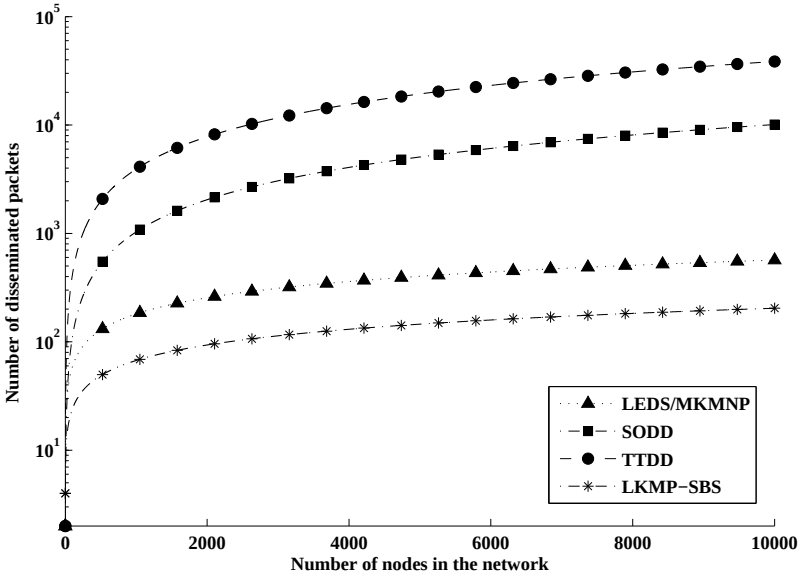


Figure 5.14: Communication cost of LKMP-SBS, LEDS/MKMP, TODD and SODD ($n = 2$, $d = 100$ packet, $\lambda = 1$ packet).

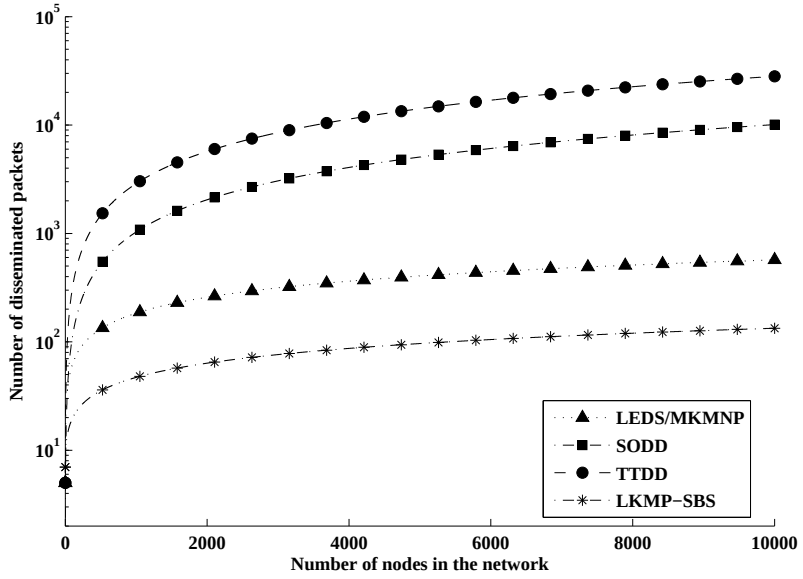


Figure 5.15: Communication cost of LKMP-SBS, LEDS/MKMP, TODD and SODD ($n = 5$, $d = 100$ packet, $\lambda = 1$ packet).

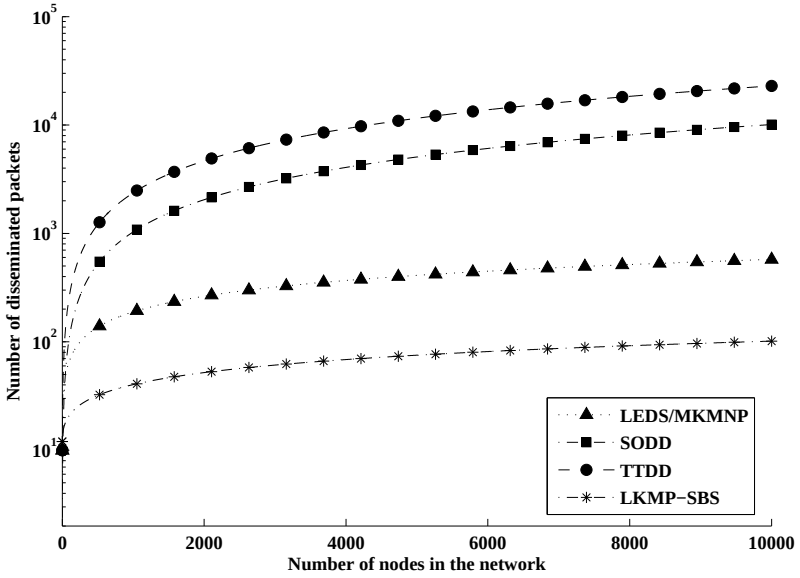


Figure 5.16: Communication cost of LKMP-SBS, LEDS/MKMP, TODD and SODD ($n = 10$, $d = 100$ packet, $\lambda = 1$ packet).

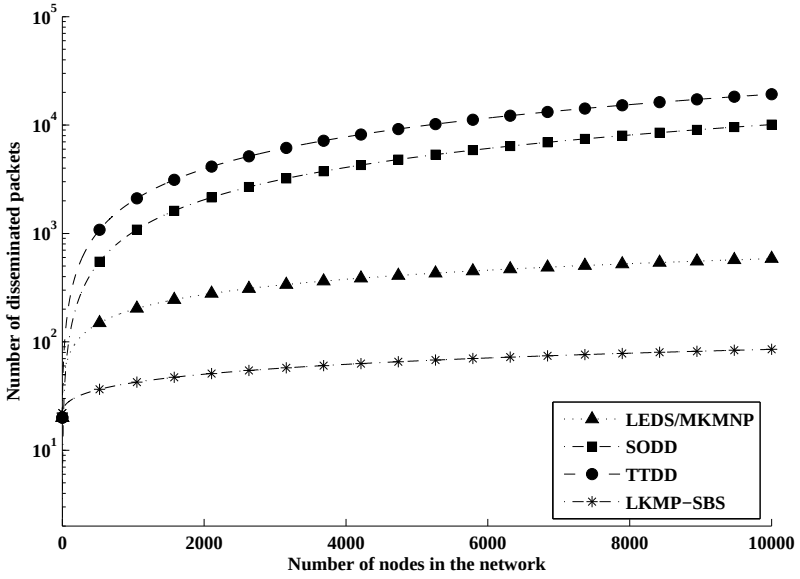


Figure 5.17: Communication cost of LKMP-SBS, LEDS/MKMP, TODD and SODD ($n = 20$, $d = 100$ packet, $\lambda = 1$ packet).

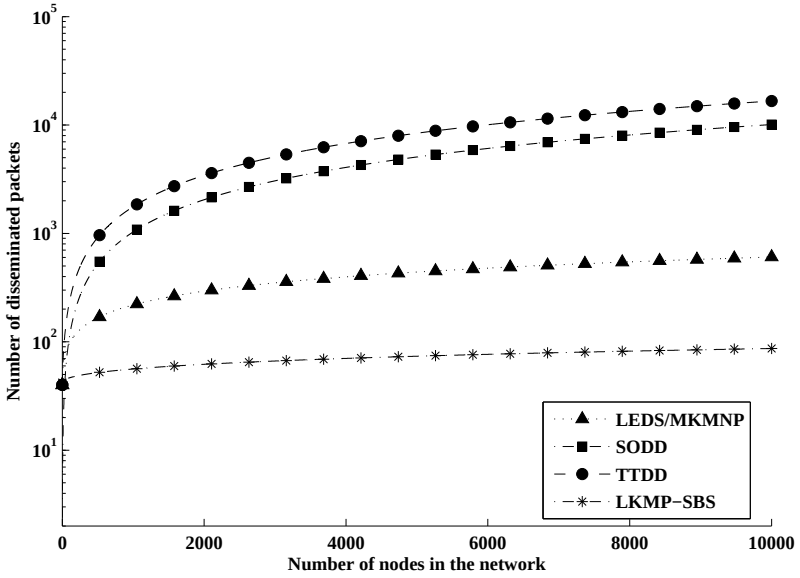


Figure 5.18: Communication cost of LKMP-SBS, LEDS/MKMP, TODD and SODD ($n = 40$, $d = 100$ packet, $\lambda = 1$ packet).

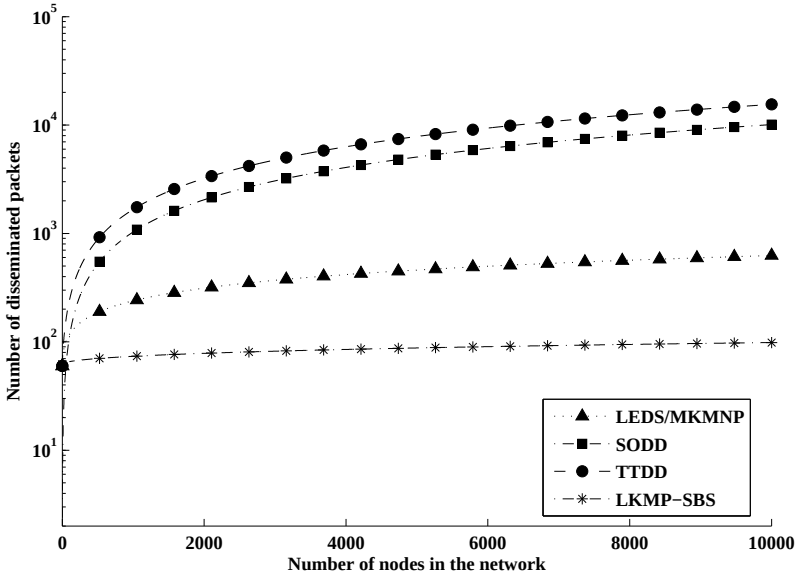


Figure 5.19: Communication cost of LKMP-SBS, LEDS/MKMP, TODD and SODD ($n = 60$, $d = 100$ packet, $\lambda = 1$ packet).

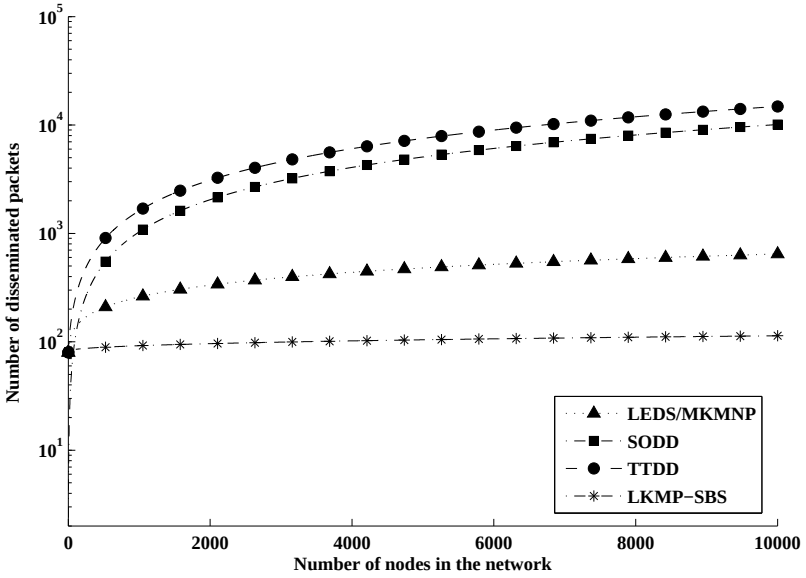


Figure 5.20: Communication cost of LKMP-SBS, LEDS/MKMP, TODD and SODD ($n = 80$, $d = 100$ packet, $\lambda = 1$ packet).

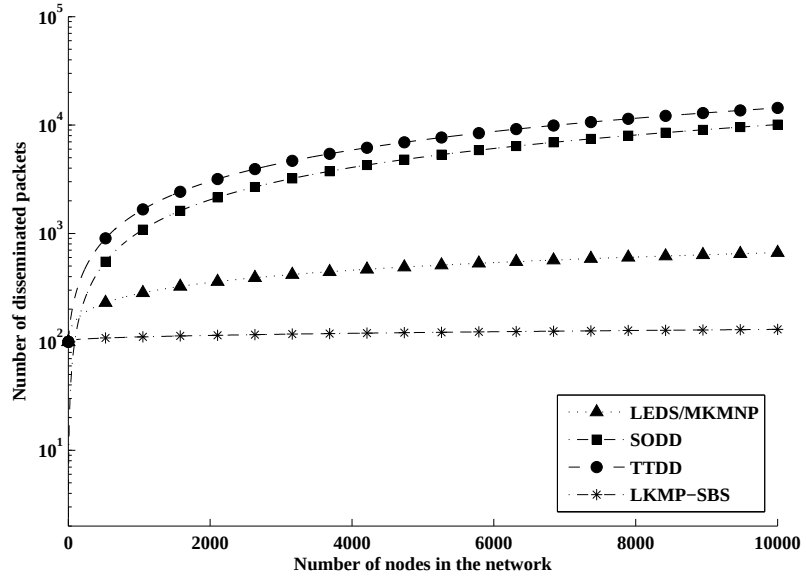


Figure 5.21: Communication cost of LKMP-SBS, LEDS/MKMP, TODD and SODD ($n = 100$, $d = 100$ packet, $\lambda = 1$ packet).

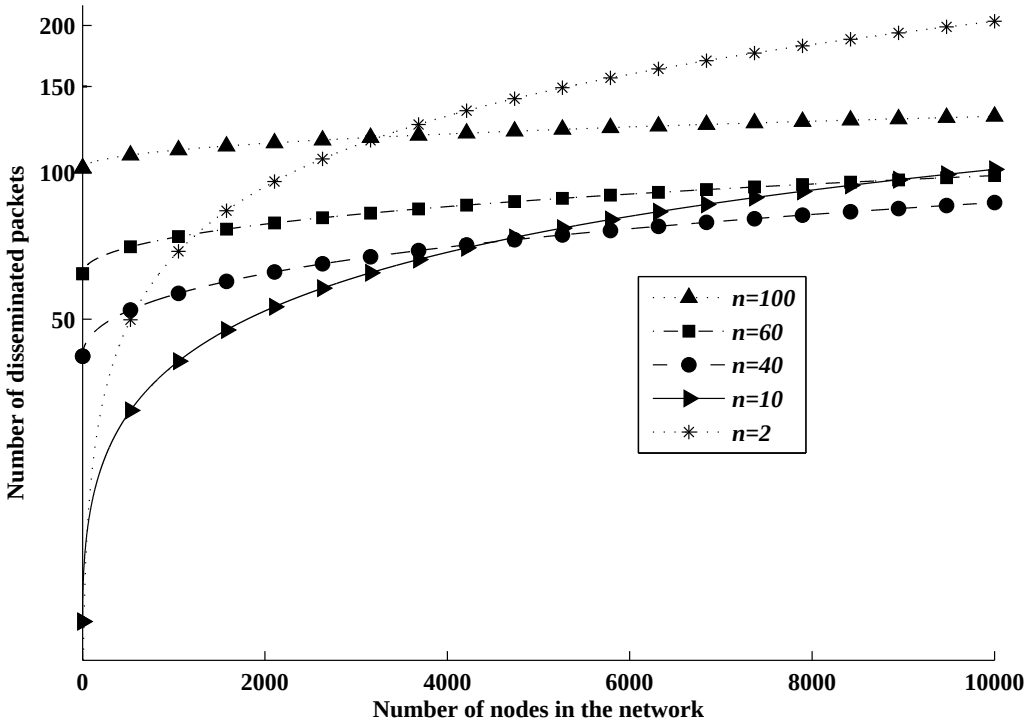


Figure 5.22: Communication cost of LKMP-SBS versus the number of total nodes in the network (N) for different number of nodes inside each cell ($n = (100, 60, 40, 10, 2)$).

It is obvious from those figures that n has a direct impact on the communication overhead. Therefore, the LKMP-SBS had been simulated by using different values of n to understand its impact on the total communication overhead as shown in Fig. 5.22. It is obvious that neither decreasing n nor increasing it will decrease the communication overhead in the WSN. Therefore, a mathematical analysis is implemented in order to find the optimum value of n that gives the minimum overhead.

5.4.2.1 Optimum value of n

The LKMP-SBS is simulated using the Contiki OS Cooja simulator in order to simulate the number of messages disseminated through a WSN consisting of 2000 sensor nodes and covering an area of 1000×1000 m^2 divided into $N^{'}$ cells where each cell consists of n nodes. The value of n is changed from 0 to 100 for values of $N = 10,000, 30,000, 50,000, 70,000, 90,000$ and the simulation is repeated, the number of messages disseminated is measured 1000 times in order to obtain the most accurate results following Monte Carlo simulation concepts [128]. The analysed data is presented in Fig. 5.23,

It is obvious that optimum values of n that reflect a minimum level of communi-

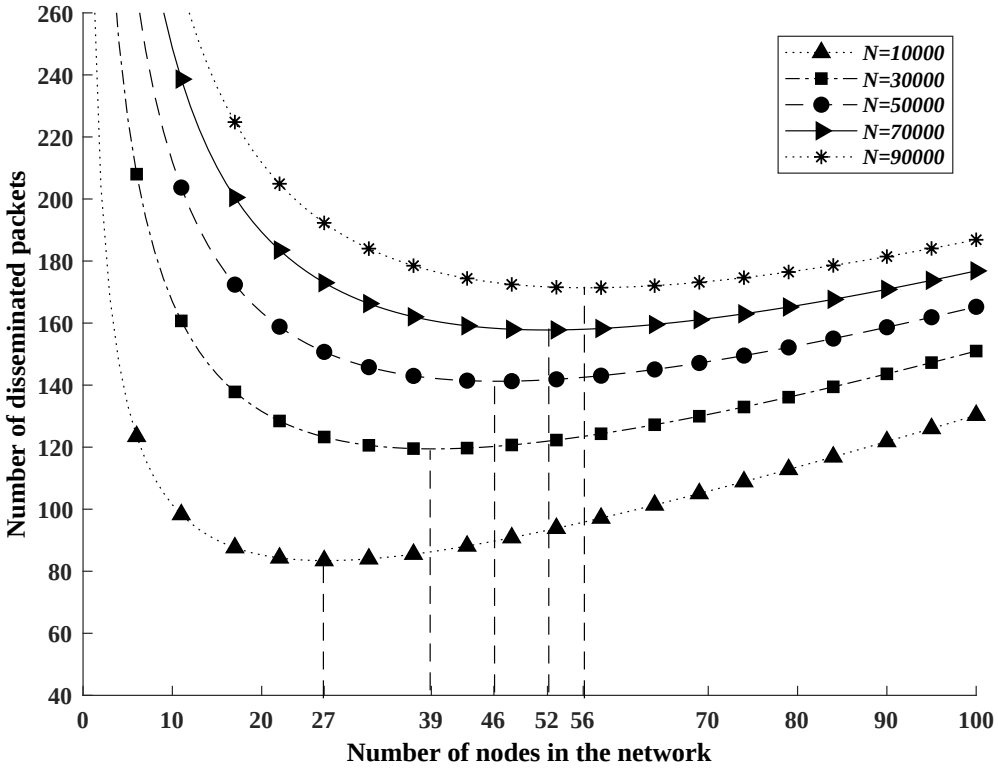


Figure 5.23: Communication cost of LKMP-SBS vs. the number of nodes inside each cell n for $N = 10,000, 30,000, 50,000, 70,000, 90,000$.

cation overhead are varied according to N, which are $27, 39, 39, 46, 52, 56$ when $N = 10000, 30000, 50000, 70000, 90000$ respectively. Therefore, further mathematical analysis is required to investigate the relationship between n, N and the communication overhead. Accordingly, the optimum value of n which leads to decrease the communication overhead is determined given that N is a constant. Finding this is significantly crucial in order to allow the network operator to design the grid in an optimum way in terms of communication overhead regardless of the area of the monitored region. As mentioned in 5.18:

$$CC_{LKMP-SBS} = \lambda(2\sqrt{2\frac{N}{n}} + n + 2)$$

In order to investigate the optimality of n, $CC_{LKMP-SBS}$ is derived in terms of n, then $\frac{\partial}{\partial n}\, CC_{LKMP-SBS}$ is equalled to zero to determine its critical points:

$$\frac{\partial}{\partial n} CC_{LKMP-SBS} = \lambda(1 - \frac{\sqrt{2nN}}{n^2})$$
$$= 0$$

$\Rightarrow n = \sqrt[3]{2N}$ is a critical point

In order to investigate whether the determined critical point is a local minima or a local maxima, a second derivative method is followed. Accordingly:

$$\frac{\partial^2}{\partial n^2} CC_{LKMP-SBS} = \lambda(\frac{3N}{n^2\sqrt{2nN}})$$
$$\frac{\partial^2}{\partial n^2} CC_{LKMP-SBS}|_{n=\sqrt[3]{2N}} = \lambda\frac{3N}{(\sqrt[3]{2N})^2\sqrt{2N\sqrt[3]{2N}}} \tag{5.19}$$

While $N, n \in \mathbb{N}^+$, above term is positive for all values of N and $n = \lfloor\sqrt[3]{2N} + 0.5\rfloor$ is a local minima. For the five values of N used in the simulation, the mathematical analysis shows similar values as shown in Table. 5.2

Table 5.2: Simulation vs. Mathematical results of the optimum n in terms of communication overhead

N	**Simulation Result**	$(n = \sqrt[3]{2N})$	**Mathematical Model Result** $(n = \lfloor\sqrt[3]{2N} + 0.5\rfloor)$
10,000	27	27.144	27
30,000	39	39.148	39
50,000	46	46.415	46
70,000	52	51.924	52
90,000	56	56.462	56

5.4.3 LKMP-MBS

To calculate the overall communication cost of LKMP-MBS, the same analysis of the last section is followed to derive the communication cost where M cells are individually:

1. Implementing the setup phase.
2. Generating reports.
3. Sending the generated report to a relevant BS which is located in the farthest destination.

Doing so, the worst case scenario is represented to study the communication overhead using the LKMP-MBS. The communication cost of each particular route is the same as that explained in (5.18), as a result:

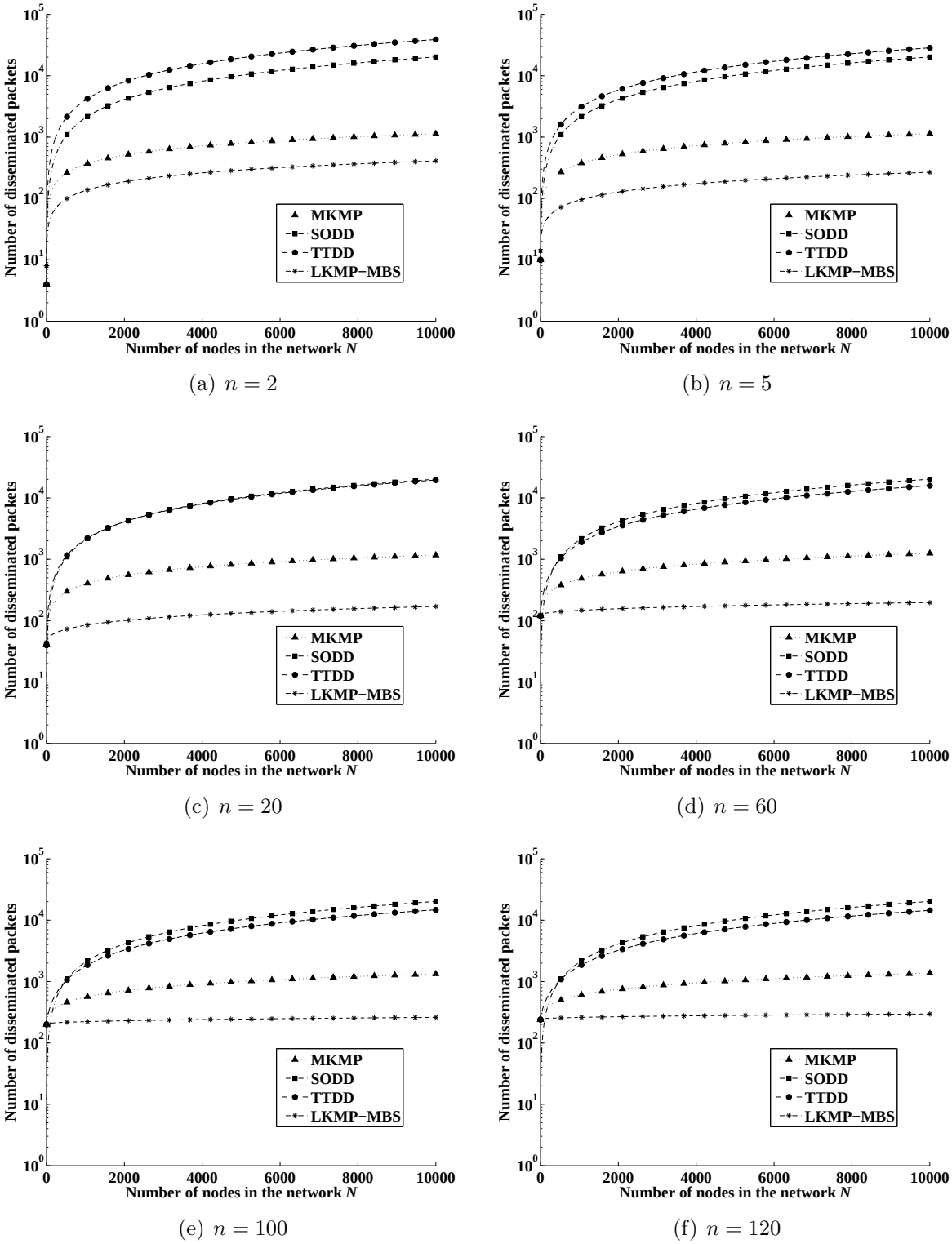
Due to the consideration of a square terrain and the entire nodes normal distribution, the entire communication cost of LKMP-MBS is expressed as:

$$CC_{LKMP-MBS} = \lambda M(2\sqrt{2\frac{N}{n}} + n + 2) \tag{5.20}$$

On the other hand, the communication cost of MKMP is calculated using (5.5) derived previously where number of BS is more than 1

$$CC_{MKMP} = \lambda M(4\sqrt{2N} + n) \quad M \neq 1 \tag{5.21}$$

LKMP-MBS, MKMP, TTDD SODD are simulated and the communication overhead is presented versus the total number of nodes N for different values of M as shown in Fig. 5.24, 5.25, 5.26 and 5.27.



(a) $n = 2$ (b) $n = 5$

(c) $n = 20$ (d) $n = 60$

(e) $n = 100$ (f) $n = 120$

Figure 5.24: Communication overhead vs. N for LKMP-MBS, MKMP, SODD and TTDD ($M = 2$, $d = 100$ packet, $\lambda = 1$ packet).

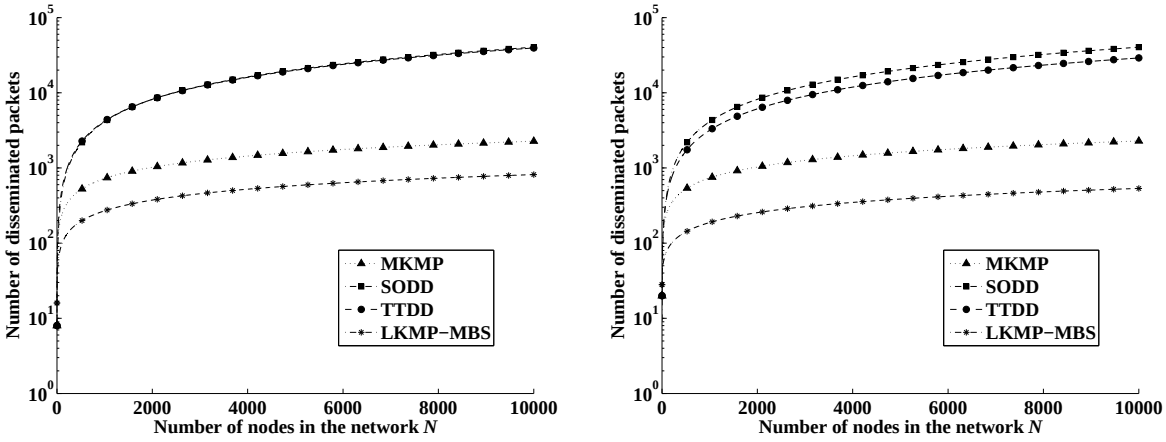
Table 5.3: Reduction in computational overhead ΔP vs. N, t

N	t	$\Delta P(\mu J)$
100	4	17.7
	8	5.9
	12	5.9
250	4	29.5
	8	11.8
	12	5.9
500	4	41.3
	8	17.7
	12	11.8
1000	4	64.9
	8	29.5
	12	17.7

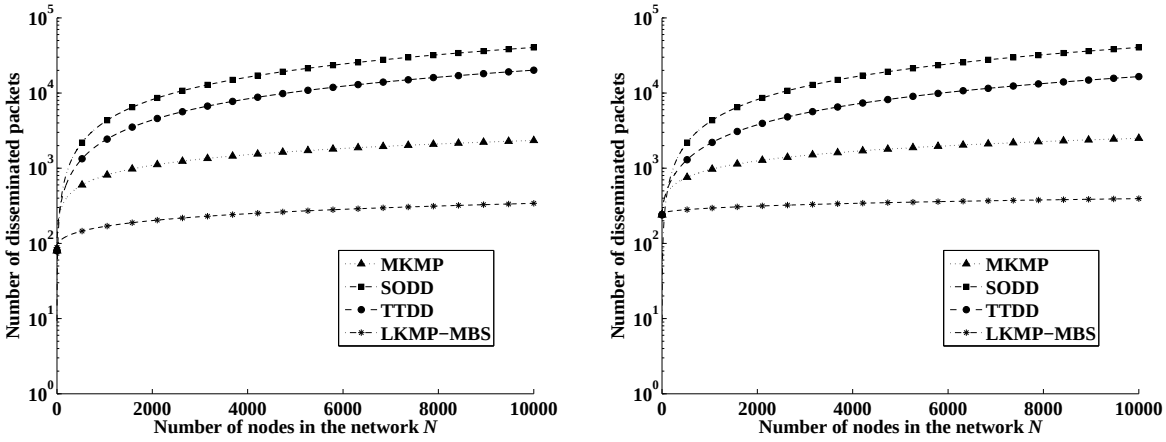
It is obvious that the relationship between communication overhead and N has the same behaviour for different values of M, n where the overhead caused by using LKMP-MBS is always less than that of the other schemes. However, it is varying according to the number of BSs where it is obvious from (5.20) that $CC_{LKMP-MBS} = f(M)$ as shown in Fig. 5.28. In addition, according to the same equation (5.20) and the analysis shown in section 5.4.2.1 the optimum value of $n = \sqrt[3]{2N}$.

5.5 Computational cost

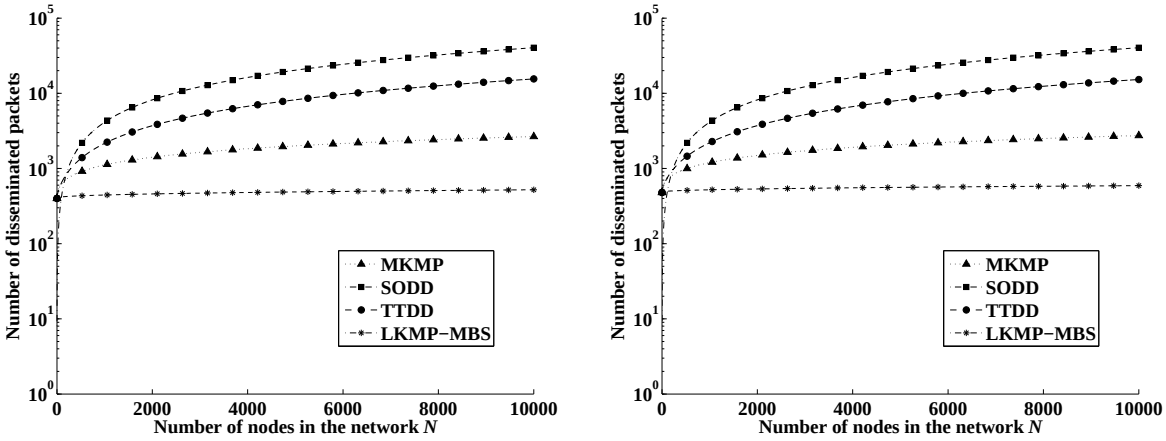
In contrast to LEDS and MKMP, the security credential derivation and virtual grid construction of LKMP-SBS, LKMP-MBS and MELKMP-MBS are facilitated by the assumption of BS's wide coverage presented in Chapter 1. This allow the BS to implement the mentioned derivation rather than their implementation by each particular node. In contrast, in the MKMP scheme, the authentication keys shared with the relevant authentication nodes are derived individually by each node. On the other hand, these derivations are implemented by a robot in LEDS which is an impractical assumption, especially in a harsh environment. Hence, less computation is required to be implemented by each node when employing our schemes. According to [136], power consumption of hashing 1 byte by Mica2 is $5.9\mu J$ in case of employing SHA-1. In the worst case scenario presented in 5.4, $NodalDistance$ between the event cell and the BS is $\sqrt{2N}$. In addition, the number of report authentication cell alongside the authentication route is t. As a result, the amount of reduction in computational overhead ΔP by using our proposed schemes is illustrated in Table. 5.3 for different network parameters.



(a) $n = 2$ (b) $n = 5$

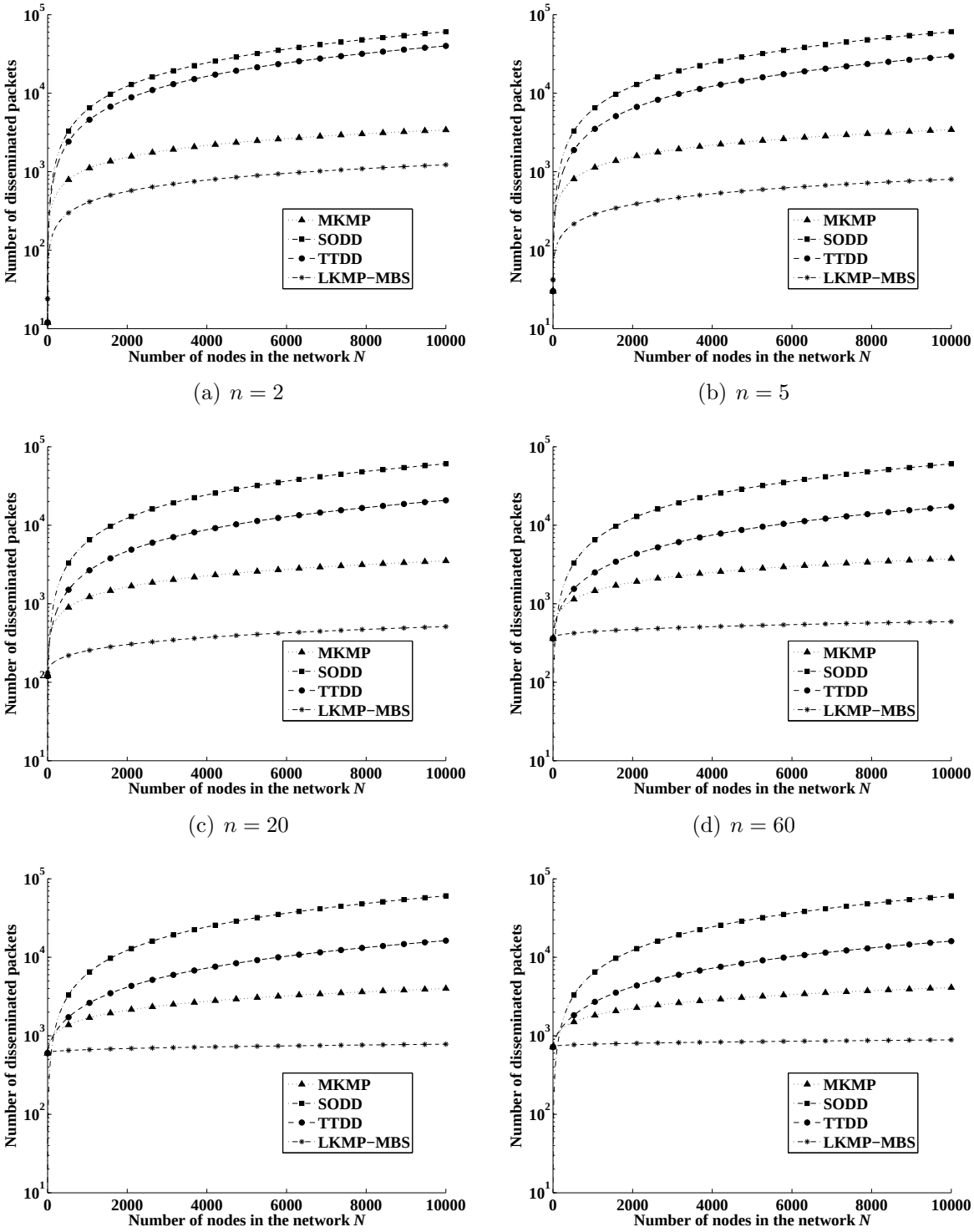


(c) $n = 20$ (d) $n = 60$



(e) $n = 100$ (f) $n = 120$

Figure 5.25: Communication overhead vs. N for LKMP-MBS, MKMP, SODD and TTDD ($M = 4$, $d = 100$ packet, $\lambda = 1$ packet).

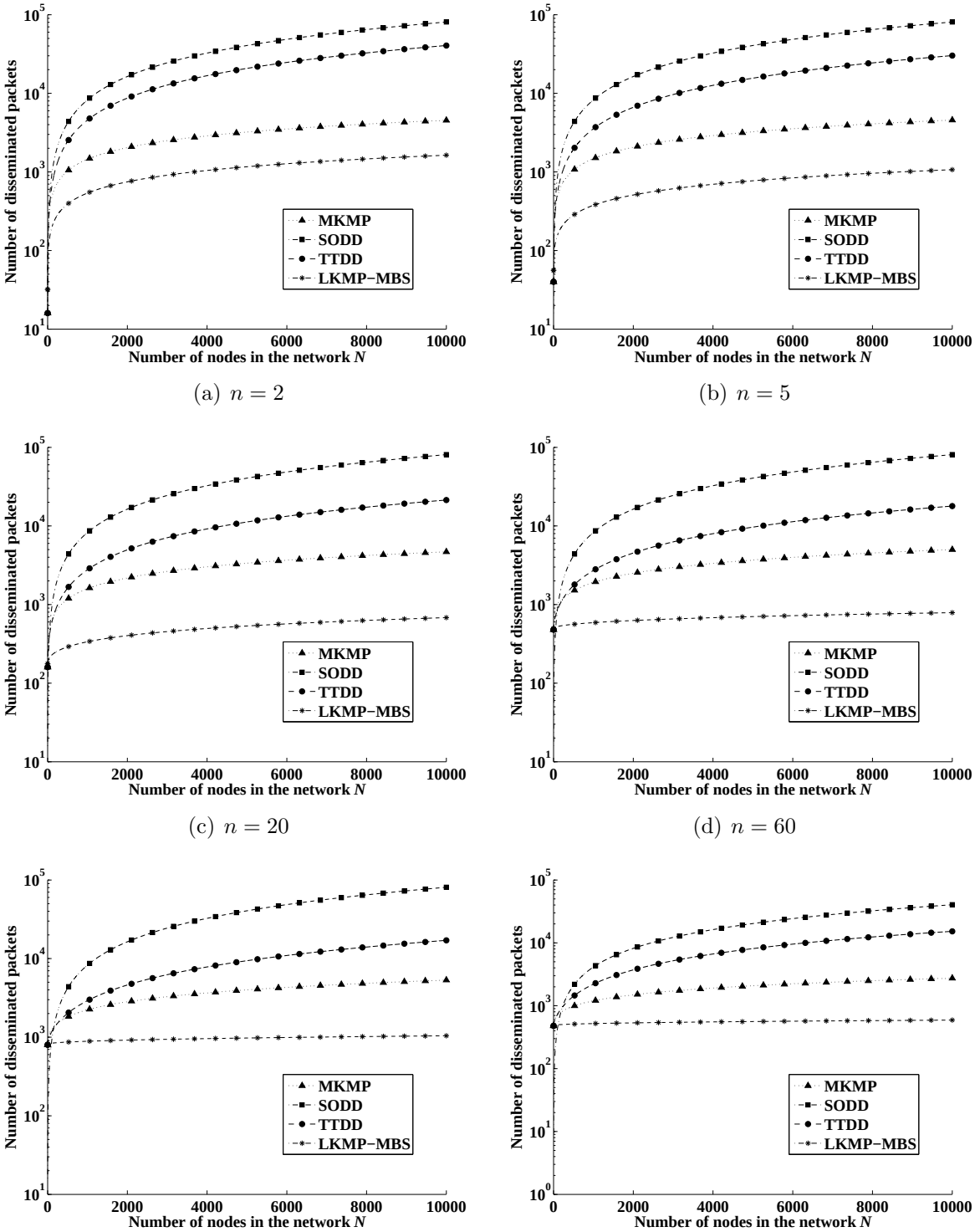


(a) $n = 2$ (b) $n = 5$

(c) $n = 20$ (d) $n = 60$

(e) $n = 100$ (f) $n = 120$

Figure 5.26: Communication overhead vs. N for LKMP-MBS, MKMP, SODD and TTDD ($M = 6$, $d = 100$ packet, $\lambda = 1$ packet).



(a) $n = 2$ (b) $n = 5$

(c) $n = 20$ (d) $n = 60$

(e) $n = 100$ (f) $n = 120$

Figure 5.27: Communication overhead vs. N for LKMP-MBS, MKMP, SODD and TTDD ($M = 8$, $d = 100$ packet, $\lambda = 1$ packet).

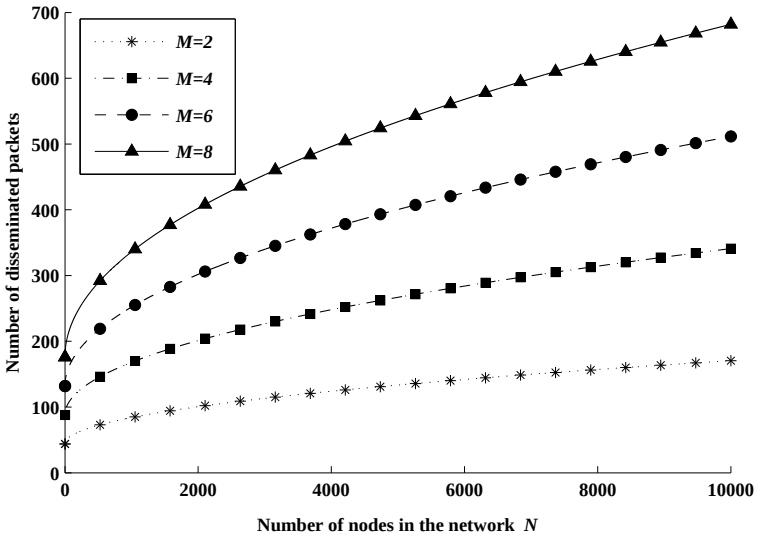


Figure 5.28: Communication cost of LKMP-MBS for different values of $M = 2, 4, 6, 8$.

5.6 Conclusion

In this chapter, a novel Mobility-Enabled Location-dependent Key Management Protocol for multiple BSs (MELKMP-MBS) was presented to overcome the limitation of LKMP-MBS in supporting a WSN that contains moile node(s). In the same way as other presented protocols, this protocol was based on a randomly selected cell reporter scheme. The possible control schemes of a WSN by multiple BSs was discussed. Accordingly, different possible handovers are presented based on the nature of mobility between different WSN zones controlled by different BSs. Data security was briefly discussed in the previous chapter, but the main focus of this chapter was on the communication overhead of MELKMP-MBS. This protocol was proven to achieve lower communication overhead in comparison with existing schemes. A thorough analysis for the potential communication overhead in a WSN governed by a location dependent key management was presented. In addition, the presented mathematical model was validated by a simulation environment for both LKMP-SBS and LKMP-MBS. Accordingly, the communication overhead of MELKMP-MBS was presented by considering all possible handover procedures. Furthermore, the optimality of WSN design such as the value of N, n was investigated in terms of communication overhead in all protocols and it was shown that the optimum number of nodes in each cell, which cause the minimum communication overhead in the network , was $n = \sqrt[3]{2N}$.

Chapter 6

Conclusions and Future Work

6.1 Conclusion

Due to its resilience against several types of attacks and security threats, location-dependant key management schemes have gained a significant amount of attention recently. This was facilitated by emerging technologies in location positioning which miniaturise GPS circuitry and decrease their cost in terms of power budget and price. This thesis presented the most critical open issues in employing location-dependent key management schemes. Accordingly, it presents novel methods to address the highlighted problems.

In Chapter. 1, a general introduction to WSN was presented along with the challenges facing data security inside these types of networks. In addition, the definition of cell reporter, as a main paradigm, was presented. Moreover, the motivation and thesis contribution are shown. Finally, this chapter illustrates the outcome of this thesis as a list of author publications.

In Chapter. 2, WSN background and security primitives are explained. In addition, a brief history of key management schemes and En-Route filtering was presented showing the evaluation metrics, the development of these schemes and their popular taxonomy. Furthermore, WSN integration with the Internet, its challenges and solutions are introduced. Finally a brief description to routing attacks are presented.

In Chapter. 3, a novel Location-Dependent Key Management Protocol for a Single Base Station (LKMP-SBS) was presented to address the problem of weaknesses in both confidentiality and authenticity in recent location-dependent key management schemes. The virtual division of WSN terrain into N square cells was introduced in this chapter. Accordingly, any event report generated inside each particular cell is endorsed by three

entities where one of these entities is the set of cell reporters. This system is analysed and proved to outperform recent schemes in terms of data security requirements. As an instance, data confidentiality of LKMP-SBS outperforms other schemes by 95%, 90% and 85% if the cell-reporter set is selected to be $z = 1, 2, 3$ when 1000 nodes are compromised. This is due to the ability of the adversary to disclose event contents in the case of compromising one of the e endorsement nodes in other schemes (MKMP and LEDS), whereas in the proposed new scheme, the data is disclosed if and only if the entire set of z cell reporters and all e endorsement nodes are captured. On the other hand, the improvement drops to 75%, 57% and 43% when the number of compromised nodes is increased to 5000 due to the increment in the probability of compromising the entire set of cell reporters when more nodes are compromised. Furthermore, in terms of data authenticity an enhancement of 49%, 24%, 12.5% was gained using the proposed approach with $z = 1, 2, 3$ respectively when half of all nodes were compromised. However, LKMP-SBS shows an improvement in comparison to LEDS only for higher values of x. Hence, it outperform LEDS when $x \geq 4000, x \geq 7000, x \geq 10000$ and $z = 1, 2, 3$ respectively. As a result, LKMP-SBS is superior compared to the other schemes in terms of the fraction of compromised cells caused by RNCA thwarting data authenticity, especially when 50% of the nodes are captured. Finally, an extensive mathematical analysis was performed to investigate the effect of network characteristics on both of confidentiality $P_{C\{e|z\}}$ and authenticity $P_{auth\{e|z\}}$. It is proved that both values are $\propto \frac{1}{N} \propto e$. In addition, the optimum number of cell reporters was extensively investigated in terms of the security requirements and was proven to be $z = \dfrac{n}{2}$.

In Chapter. 4, a novel multiple BS location-dependent key management protocol (LKMP-MBS) was presented based on a randomly selected cell reporter scheme and was proven to achieve better performance in comparison with existing schemes and with the LKMP-SBS presented in Chapter 3. The problem of the degraded performance of LKMP-SBS in comparison with LEDS had been overcame in this scheme. An extensive mathematical analysis was presented to evaluate this scheme in terms of system security by considering data confidentiality, authenticity and overall robustness against attacks targeting cell reporters. Both data confidentiality and authenticity have been proven to be $\propto e \propto \frac{1}{N}$. Moreover, the system optimality in terms of the number of selected cell reporters has been analysed for different considerations. In the case of all cell reporters sets having no mutual elements, the optimum number of cell reporters had been calculated as

$z_{opt} = \frac{n}{2M}$, $\sum_{\ell=1}^{M} |z_{opt}^{(\ell)}| = \frac{n}{2M}$ when they have unified and not unified lengths respectively. On the other hand, if these sets are considered to have mutual elements, a mathematical model is built base on Markov chain analysis and the z_{opt} is found to be $\propto \frac{1}{M}$ where increasing the number of mutual cell reporters increases the probability of compromising more cell reporters inside each particular cell.

In Chapter. 5, a novel Mobility-Enabled Location-dependent Key Management Protocol for multiple BS (MELKMP-MBS) was presented to overcome the limitation of LKMP-MBS in supporting a WSN that contains mobile node(s). As with the other presented protocols, this protocol is based on a randomly selected cell reporter scheme. The possible control schemes of a WSN by multiple BSs is discussed. Accordingly, different possible handovers were presented based on the nature of mobility between different WSN zones controlled by different BSs. While The data security is briefly discussed in the previous chapter, the main focus of this chapter is on the communication overhead of MELKMP-MBS. This protocol is proven to achieve lower communication overhead in comparison with existing schemes. A thorough analysis for the potential communication overhead in a WSN governed by a location dependent key management was presented. In addition, the presented mathematical model is validated by a simulation environment for both LKMP-SBS and LKMP-MBS. Accordingly, the communication overhead of MELKMP-MBS was presented by considering all possible handover procedures. Furthermore, the optimality of the WSN design such as the value of N, n was investigated in terms of communication overhead in all protocols and it was shown that the optimum number of nodes in each cell, which cause the minimum communication overhead in the network , is $n = \sqrt[3]{2N}$. The reduction in power consumption due to adoption of our scheme is calculated and shown to be a subject of N and t values where it si proved to be varying between $5.9(\mu J)$ to $64.9(\mu J)$ when $(N = 100, t = 12)$, $(N = 1000, t = 4)$ respectively. It is obvious that using the proposed scheme will definitely increase the life cycle of the sensor nodes where the computation cost is balanced between these nodes and the corresponding BS. According to [136], sending one byte requires $59.2(\mu J)$, therefore LKMP-SBS consumes $(3.328mJ)$ in total for packets dissemination inside a network consists of $N = 10,000, n = 27$.

6.2 Future Work

Widespread research on location-dependent key management schemes and the promising performance of using cell-reporters in these schemes confirm their suitability to be used

as a rigid system to secure data inside a WSN. Nevertheless, there are still open problems for different aspects such as location accuracy, security threats, data availability, network construction and resource allocation. It is difficult to cover all theses aspects and address all relevant system challenges in one thesis. Some of the proposed ideas that can be considered as future work are divided into following categories:

- **Location accuracy**: Indoor localisation accuracy has emerged as one of the hottest research areas recently. The Geographical Positioning System (GPS) lacks an ability to be used indoor. Therefore, signalling from multiple BS can be used to detect node position rather than using GPS.

- **lightweight credentials**
  Investigate the possibility of using physical Uncloneable Function (PUF) [137, 138] facilities to generate rigid, lightweight and scalable security credentials.

- **Timing synchronisation**
  Digital clock drift is a major risks to data accuracy and availability. In addition such a drift might lead to a significant impact on data security where attackers can make use of this drift to create malicious reports or to drop genuine reports. Therefore, a time synchronisation protocol assisted by cell reporters is worthy to be developed in future.

- **Data consistency**: One of the major problems facing the usage of multiple BSs is the data consistency, especially when each node is related to multiple BSs at the same time. Therefore, one proposed future work is to build a system to maintain on-line data consistency between BSs.

- **Security of BS**: In most recent schemes, BSs are considered as a secure network entity due to their unlimited resources and being established in secure regions. It is worthy to build a security scheme that thwarts any external attacks targeting BSs. Such a scheme has to have an ability to detect and revoke a malicious BS. A promising ideas inspired by random selected reporters might be considered as a future work. It builds on comparing random selected data generated by more than one BS as a final report regarding a particular region and decides whether one of these BSs is forging data or not. Figure. 6.1 illustrate a general block diagram of the scheme which is in implementation phase. As shown, all credentials are synchronised

between different BSs and the decision maker is a council of threshold number of BSs.

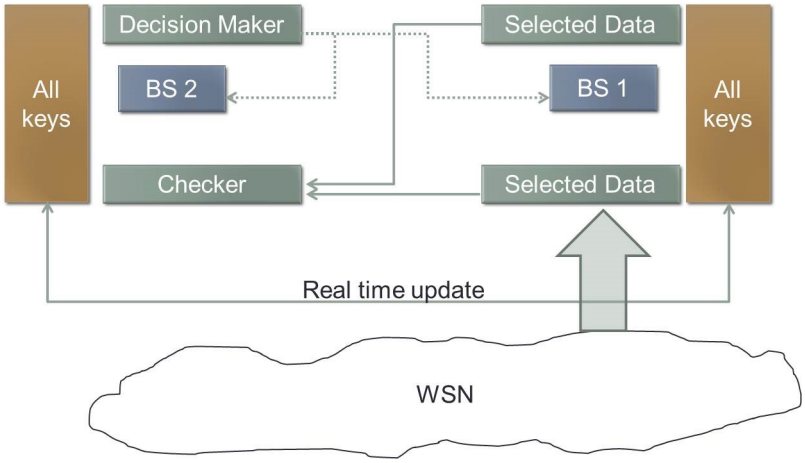


Figure 6.1: BS performance monitoring system

- **Optimum BS location**

  Investigating the optimum BS(s) position(s) inside the network is worth investigating. The optimality could be studied in terms of data security, overall network traffic, the accuracy of malicious entities detection and time taken to implement required revocation.

- **Data Aggregation**

  Recent data aggregation schemes are challenged by:

  - Collection of different data format in multi-purpose WSNs.
  - Forwarding data to multiple BS WSNs.
  - Handling mobile nodes' generated data.

  Therefore, an investigation into these challenges to innovate a novel scheme capable of addressing these problems should be carried out.

References

[1] A. Kumar and A. R. Pais, "En-route filtering techniques in wireless sensor networks: a survey," *Wireless Personal Communications*, vol. 96, no. 1, pp. 697–739, 2017.

[2] X. He, M. Niedermeier, and H. De Meer, "Dynamic key management in wireless sensor networks: A survey," *Journal of Network and Computer Applications*, vol. 36, no. 2, pp. 611–622, 2013.

[3] C. Alcaraz, R. Roman, P. Najera, and J. Lopez, "Security of industrial sensor network-based remote substations in the context of the internet of things," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1091–1104, 2013.

[4] D. Christin, A. Reinhardt, P. S. Mogre, and R. Steinmetz, "Wireless sensor networks and the internet of things: selected challenges," *Proceedings of the 8th GI/ITG KuVS Fachgespräch "Drahtlose Sensornetze*, pp. 31–33, 2009.

[5] T. Adame, A. Bel, A. Carreras, J. Melià-Seguí, M. Oliver, and R. Pous, "Cuidats: An rfid–wsn hybrid monitoring system for smart health care environments," *Future Generation Computer Systems*, vol. 78, pp. 602–615, 2018.

[6] A.-S. K. Pathan, *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2016.

[7] L. Chen, J. Ji, and Z. Zhang, *Wireless Network Security*. Springer, 2013.

[8] I. F. Akyildiz and M. C. Vuran, *Wireless sensor networks*. John Wiley & Sons, 2010, vol. 4.

[9] M. A. Feki, F. Kawsar, M. Boussard, and L. Trappeniers, "The internet of things: The next technological revolution," *Computer*, vol. 46, no. 2, pp. 24–25, 2013.

[10] R. Roman and J. Lopez, "Integrating wireless sensor networks and the internet: a security analysis," *Internet Research*, vol. 19, no. 2, pp. 246–259, 2009.

[11] F. Li and P. Xiong, "Practical secure communication for integrating wireless sensor networks into the internet of things," 2013.

[12] "Rfid global solution website." http://www.rfidgs.com/, accessed: 2018-03-21.

[13] "Stanley healthcare website." http://www.stanleyhealthcare.com/, accessed: 2018-03-21.

[14] "Ekahau website." http://www.ekahau.com/, accessed: 2018-03-21.

[15] "Awarepoint website." http://www.awarepoint.com/, accessed: 2018-03-21.

[16] "Centrak website." http://www.centrak.com/, accessed: 2018-03-21.

[17] "Teletracking website." http://www.teletracking.com/, accessed: 2018-03-21.

[18] "Zebra website." https://www.zebra.com, accessed: 2018-03-21.

[19] "Radianse website." http://www.radianse.com/, accessed: 2018-03-21.

[20] K. Ren, W. Lou, and Y. Zhang, "Leds: Providing location-aware end-to-end data security in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 7, no. 5, pp. 585–598, 2008.

[21] H.-W. Ferng, J. Nurhakim, and S.-J. Horng, "Key management protocol with end-to-end data security and key revocation for a multi-bs wireless sensor network," *Wireless networks*, vol. 20, no. 4, pp. 625–637, 2014.

[22] J. López and J. Zhou, *Wireless Sensor Network Security*. IOS Press, 2008, vol. 1.

[23] D. Liu and P. Ning, *Security for wireless sensor networks*. Springer, 2007.

[24] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 4, pp. 839–850, 2005.

[25] C. I. Sun, H. Y. Lee, and T. H. Cho, "A path selection method for improving the detection power of statistical filtering in sensor networks." *Journal of Information Science & Engineering*, vol. 25, no. 4, 2009.

[26] Q. Sun and M. Wu, "A double key-sharing based false data filtering scheme in wireless sensor networks," in *International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 2011, pp. 509–516.

[27] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward resilient security in wireless sensor networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*. ACM, 2005, pp. 34–45.

[28] L. Yu and J. Li, "Grouping-based resilient statistical en-route filtering for sensor networks," in *INFOCOM 2009, IEEE*. IEEE, 2009, pp. 1782–1790.

[29] H. Yang and S. Lu, "Commutative cipher based en-route filtering in wireless sensor networks," in *Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th*, vol. 2. IEEE, 2004, pp. 1223–1227.

[30] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," *IEEE Journal on selected areas in communications*, vol. 24, no. 2, pp. 247–260, 2006.

[31] H. Wang and Q. Li, "Achieving robust message authentication in sensor networks: a public-key based approach," *Wireless Networks*, vol. 16, no. 4, pp. 999–1009, 2010.

[32] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[33] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[34] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks," *IEEE communications surveys & tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[35] K. Bauer, D. McCoy, D. Grunwald, T. Kohno, and D. Sicker, "Low-resource routing attacks against tor," in *Proceedings of the 2007 ACM workshop on Privacy in electronic society*. ACM, 2007, pp. 11–20.

[36] B. Yu and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," in *Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International*. IEEE, 2006, pp. 8–pp.

[37] Y. Hu, Y. Lin, Y. Liu, and W. Zeng, "Ras: A robust authentication scheme for filtering false data in wireless sensor networks," in *15th IEEE International Conference on Networks, 2007. ICON 2007.* IEEE, 2007, pp. 200–205.

[38] C. I. Sun, H. Y. Lee, and T. H. Cho, "A path selection method for improving the detection power of statistical filtering in sensor networks." *Journal of Information Science & Engineering*, vol. 25, no. 4, 2009.

[39] S. Kumar, C. R. Krishna, and A. Solanki, "A survey on security architecture and key management systems in a wireless sensor network," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 17, no. 4, p. 263, 2017.

[40] L. Chen, J. Ji, and Z. Zhang, *Wireless Network Security*. Springer, 2013.

[41] Y. W. Law, J. Doumen, and P. Hartel, "Survey and benchmark of block ciphers for wireless sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 2, no. 1, pp. 65–93, 2006.

[42] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes," in *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*. ACM, 2003, pp. 151–159.

[43] K. J. Choi and J.-I. Song, "Investigation of feasible cryptographic algorithms for wireless sensor network," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 4, no. 2, pp. 3 pp.–1381, 1996.

[44] N. Sastry and D. Wagner, "Security considerations for ieee 802.15. 4 networks," in *Proceedings of the 3rd ACM workshop on Wireless security*. ACM, 2004, pp. 32–42.

[45] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 1996.

[46] H. Wang and Q. Li, "Efficient implementation of public key cryptosystems on micaz and telosb motes," *College of William and Mary, Tech. Rep. WM-CS-2006*, vol. 7, 2006.

[47] A. Liu and P. Ning, "Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks," in *International Conference on Information Processing in Sensor Networks, 2008. IPSN'08.* IEEE, Conference Proceedings, pp. 245–256.

[48] L. Batina, N. Mentens, K. Sakiyama, B. Preneel, and I. Verbauwhede, *Low-cost elliptic curve cryptography for wireless sensor networks*. Springer, 2006, pp. 6–17.

[49] O. K. Sahingoz, "Large scale wireless sensor networks with multi-level dynamic key management scheme," *Journal of Systems Architecture*, vol. 59, no. 9, pp. 801–807, 2013.

[50] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Computer communications*, vol. 30, no. 11, pp. 2314–2341, 2007.

[51] S. A. Camtepe and B. Yener, "Key management in wireless sensor network," *Wireless Sensor Network Security,(J. Lopez and JY Zhou Eds)*, 2008.

[52] S. Mishra, "Key management in large group multicast," Technical Report CU-CS-940-02, Department of Computer Science, University of Colorado, Boulder, CO, Report, 2002.

[53] M. A. Simplício Jr, P. S. L. M. Barreto, C. B. Margi, and T. C. M. B. Carvalho, "A survey on key management mechanisms for distributed wireless sensor networks," *Computer Networks*, vol. 54, no. 15, pp. 2591–2612, 2010.

[54] J. Zhang and V. Varadharajan, "Wireless sensor network key management survey and taxonomy," *Journal of Network and Computer Applications*, vol. 33, no. 2, pp. 63–75, 2010.

[55] M. Eltoweissy, M. H. Heydari, L. Morales, and I. H. Sudborough, "Combinatorial optimization of group key management," *Journal of Network and Systems Management*, vol. 12, no. 1, pp. 33–50, 2004.

[56] M. F. Younis, K. Ghumman, and M. Eltoweissy, "Location-aware combinatorial key management scheme for clustered sensor networks," *IEEE transactions on parallel and distributed systems*, vol. 17, no. 8, pp. 865–882, 2006.

[57] M. Eltoweissy, M. Moharrum, and R. Mukkamala, "Dynamic key management in sensor networks," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 122–130, 2006.

[58] C.-C. Lo, C.-C. Huang, and S.-W. Chen, "An efficient and scalable ebs-based batch rekeying scheme for secure group communications," in *IEEE Military Communications Conference, 2009. MILCOM 2009.* IEEE, Conference Proceedings, pp. 1–7.

[59] S. M. K.-u.-R. Raazi, H. Lee, S. Lee, and Y.-K. Lee, "Muqami+: a scalable and locally distributed key management scheme for clustered sensor networks," in *Annales des Télécommunications*, vol. 65, Conference Proceedings, pp. 101–116.

[60] F. R. Kong, C. W. Li, Q. Q. Ding, F. Jiao, and Q. Gu, "Collusion problem of the ebs-based dynamic key management scheme," *Journal of Software*, vol. 20, no. 9, pp. 2531–2541, 2009.

[61] W. Zhang, S. Zhu, and G. Cao, "Predistribution and local collaboration-based group rekeying for wireless sensor networks," *Ad hoc networks*, vol. 7, no. 6, pp. 1229–1242, 2009.

[62] Y. Zhang, Y. Shen, and S. Lee, "A cluster-based group key management scheme for wireless sensor networks," in *Web Conference (APWEB), 2010 12th International Asia-Pacific.* IEEE, 2010, Conference Proceedings, pp. 386–388.

[63] X. He, M. Niedermeier, and H. De Meer, "Dynamic key management in wireless sensor networks: A survey," *Journal of Network and Computer Applications*, vol. 36, no. 2, pp. 611–622, 2013.

[64] S. Guo and A.-N. Shen, "A compromise-resilient pair-wise rekeying protocol in hierarchical wireless sensor networks," *Computer Systems Science and Engineering*, vol. 25, no. 6, p. 397, 2010.

[65] X. Zhang, J. He, and Q. Wei, "Eddk: energy-efficient distributed deterministic key management for wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, p. 12, 2011.

[66] J. Deng, C. Hartung, R. Han, and S. Mishra, "A practical study of transitory master key establishment forwireless sensor networks," in *First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005.* IEEE, 2005, pp. 289–302.

[67] Y. Wang, B. Ramamurthy, X. Zou, and Y. Xue, "An efficient scheme for removing compromised sensor nodes from wireless sensor networks," *Security and Communication Networks*, vol. 3, no. 4, pp. 320–333, 2010.

[68] Y. Wang, B. Ramamurthy, and Y. Xue, "ukeying: A key management framework for wireless sensor networks utilizing a unique session key," *CSE Technical reports*, p. 84, 2007.

[69] Y. Wang, B. Ramamurthy, X. Zou, and Y. Xue, "A key management protocol for wireless sensor networks with multiple base stations," in *IEEE International Conference on Communications, 2008. ICC'08.* IEEE, 2008, pp. 1625–1629.

[70] K.-J. Paek, U.-S. Song, H.-Y. Kim, J. Kim, and J.-N. Hwang, "Energy-efficient key-management (eekm) protocol for large-scale distributed sensor networks," *Journal of Information Science & Engineering*, vol. 24, no. 6, 2008.

[71] M. L. Messai, M. Aliouat, and H. Seba, "Tree based protocol for key management in wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, p. 59, 2010.

[72] C.-L. Chen and I. Lin, "Location-aware dynamic session-key management for grid-based wireless sensor networks," *Sensors*, vol. 10, no. 8, pp. 7347–7370, 2010.

[73] C.-L. Wang, T.-P. Hong, G. Horng, and W.-H. Wang, "A ga-based key-management scheme in hierarchical wireless sensor networks," *Int J Innov Comput Inf Control*, vol. 5, pp. 4693–4702, 2009.

[74] M. H. Eldefrawy, M. K. Khan, and K. Alghathbar, "A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography," in *2010 International Conference on Anti-Counterfeiting Security and Identification in Communication (ASID).* IEEE, 2010, Conference Proceedings, pp. 1–6.

[75] J.-Y. Huang, I. E. Liao, and H.-W. Tang, "A forward authentication key management scheme for heterogeneous sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, p. 6, 2011.

[76] F. Gandino, B. Montrucchio, and M. Rebaudengo, "Key management for static wireless sensor networks with node adding," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1133–1143, 2014.

[77] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in *2004 IEEE Symposium on Security and Privacy, 2004. Proceedings.* IEEE, 2004, pp. 259–271.

[78] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward resilient security in wireless sensor networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ser. MobiHoc '05. New York, NY, USA: ACM, 2005, pp. 34–45. [Online]. Available: http://doi.acm.org/10.1145/1062689.1062696

[79] F. Anjum, "Location dependent key management in sensor networks without using deployment knowledge," *Wireless Networks*, vol. 16, no. 6, pp. 1587–1600, 2010.

[80] J. Choi, J. Bang, L. Kim, M. Ahn, and T. Kwon, "Location-based key management strong against insider threats in wireless sensor networks," *IEEE Systems Journal*, vol. 11, no. 2, pp. 494–502, 2017.

[81] Y. Wu, J. A. Stankovic, T. He, and S. Lin, "Realistic and efficient multi-channel communications in wireless sensor networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE.* IEEE, 2008, pp. 1193–1201.

[82] H.-W. Ferng and N. M. Khoa, "On security of wireless sensor networks: a data authentication protocol using digital signature," *Wireless Networks*, vol. 23, no. 4, pp. 1113–1131, 2017.

[83] M. Mitzenmacher, "Compressed bloom filters," *IEEE/ACM transactions on networking*, vol. 10, no. 5, pp. 604–612, 2002.

[84] X. Yang, J. Lin, W. Yu, P.-M. Moulema, X. Fu, and W. Zhao, "A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems," *IEEE Transactions on Computers*, vol. 64, no. 1, pp. 4–18, 2015.

[85] D. Naccache and J. Stern, "Signing on a postcard," in *International Conference on Financial Cryptography.* Springer, 2000, pp. 121–135.

[86] J. Duan, D. Gao, D. Yang, C. H. Foh, and H.-H. Chen, "An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for iot applications," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 58–69, 2014.

[87] C. Qingping, Y. Hairong, Z. Chuan, P. Zhibo, and X. Li Da, "A reconfigurable smart sensor interface for industrial wsn in iot environment," *IEEE Transactions on Industrial Informatics.*, vol. 10, no. 2, pp. 1417–1425, 2014.

[88] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[89] C. Alcaraz, P. Najera, J. Lopez, and R. Roman, "Wireless sensor networks and the internet of things: Do we need a complete integration?" in *1st International Workshop on the Security of the Internet of Things (SecIoT'10)*, 2010.

[90] N. Kushwaha, R. Mahule, A. P. Singh, O. Vyas, and B. Singh, "Integration of service oriented wsn and iot for e-commerce," in *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, 2015, pp. 1731–1736.

[91] J. A. Manrique, J. S. Rueda-Rueda, and J. M. Portocarrero, "Contrasting internet of things and wireless sensor network from a conceptual overview," in *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2016, pp. 252–257.

[92] A. Whitmore, A. Agarwal, and L. Da Xu, "The internet of things—a survey of topics and trends," *Information Systems Frontiers*, pp. 1–14, 2014.

[93] H. Chan and A. Perrig, "Security and privacy in sensor networks," *computer*, vol. 36, no. 10, pp. 103–105, 2003.

[94] W. Xin-Sheng, Z. Yong-Zhao, X. Shu-ming, and W. Liang-min, "Lightweight defense scheme against selective forwarding attacks in wireless sensor networks," in *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2009. CyberC'09.* IEEE, 2009, pp. 226–232.

[95] S. Kaplantzis, A. Shilton, N. Mani, and Y. A. Sekercioglu, "Detecting selective forwarding attacks in wireless sensor networks using support vector machines," in *3rd International Conference on Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007.* IEEE, 2007, pp. 335–340.

[96] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks*, vol. 1, no. 2, pp. 293–315, 2003.

[97] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Proceedings of the 3rd international symposium on Information processing in sensor networks*. ACM, 2004, pp. 259–268.

[98] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 3. IEEE, 2003, pp. 1976–1986.

[99] M. A. Hamid, M. Rashid, and C. S. Hong, "Routing security in sensor network: Hello flood attack and defense," *IEEE ICNEWS*, pp. 2–4, 2006.

[100] H. M. Choi, S. M. Nam, and T. H. Cho, "A secure routing method for detecting false reports and wormhole attacks in wireless sensor networks," *Wireless Sensor Network*, vol. 5, no. 03, p. 33, 2013.

[101] Z. Liu, J. Wang, S. Zhang, H. Liu, and X. Zhang, "A cluster-based false data filtering scheme in wireless sensor networks." *Adhoc & Sensor Wireless Networks*, vol. 23, 2014.

[102] J. Wang, Z. Liu, S. Zhang, and X. Zhang, "Defending collaborative false data injection attacks in wireless sensor networks," *Information Sciences*, vol. 254, pp. 39–53, 2014.

[103] S. M. Nam and T. H. Cho, "Context-aware architecture for probabilistic voting-based filtering scheme in sensor networks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 10, pp. 2751–2763, 2017.

[104] Z. Yu and Y. Guan, "A dynamic en-route filtering scheme for data reporting in wireless sensor networks," *IEEE/ACM Transactions On Networking*, vol. 18, no. 1, pp. 150–163, 2010.

[105] T. Yuan, S. Zhang, Y. Zhong, and J. Ma, "Kaef: An en-route scheme of filtering false data in wireless sensor networks," in *IEEE International Performance, Computing and Communications Conference, 2008. IPCCC 2008.* IEEE, 2008, pp. 193–200.

[106] C. Kraub, M. Schneider, K. Bayarou, and C. Eckert, "Stef: A secure ticket-based en-route filtering scheme for wireless sensor networks," in *The second international*

conference on Availability, reliability and security, 2007. ARES 2007. IEEE, 2007, pp. 310–317.

[107] Y.-S. Chen and C.-L. Lei, "Filtering false messages en-route in wireless multi-hop networks," in *Wireless Communications and Networking Conference (WCNC), 2010 IEEE.* IEEE, 2010, pp. 1–6.

[108] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen, "Becan: A bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks," *IEEE transactions on parallel and distributed systems*, vol. 23, no. 1, pp. 32–43, 2012.

[109] G. Dini and I. M. Savino, "An efficient key revocation protocol for wireless sensor networks," in *Mobile and Multimedia Networks Proceedings of the 2006 International Symposium on World of Wireless.* IEEE Computer Society, 2006, pp. 450–452.

[110] G. Wang, S. Kim, D. Kang, D. Choi, and G. Cho, "Lightweight key renewals for clustered sensor networks." *JNW*, vol. 5, no. 3, pp. 300–312, 2010.

[111] M. Wei, R. Aragues, C. Sagues, and G. Calafiore, "Noisy range network localization based on distributed multidimensional scaling," *Sensors Journal, IEEE*, vol. 15, no. 3, pp. 1872–1883, March 2015.

[112] S. Tomic, M. Beko, and R. Dinis, "Rss-based localization in wireless sensor networks using convex relaxation: Noncooperative and cooperative schemes," *IEEE Transactions on Vehicular Technology.*, vol. 64, no. 5, pp. 2037–2050, May 2015.

[113] O. Gungor, F. Chen, and C. Koksal, "Secret key generation via localization and mobility," *IEEE Transactions on Vehicular Technology.*, vol. 64, no. 6, pp. 2214–2230, June 2015.

[114] X. Li, R. Lu, X. Liang, and X. Shen, "Side channel monitoring: Packet drop attack detection in wireless ad hoc networks," in *2011 IEEE International Conference on Communications (ICC)*, June 2011, pp. 1–5.

[115] F. Ye, G. Zhong, S. Lu, and L. Zhang, "A robust data delivery protocol for large scale sensor networks," in *Information Processing in Sensor Networks.* Springer, 2003, pp. 658–673.

[116] J. Pitman, *Introduction*, ser. Springer Texts in Statistics. Springer Berlin Heidelberg, 1993, vol. 5576, book section 1, pp. 47–49, bayes' Rule/ Example 1. [Online]. Available: http://books.google.co.uk/books?id=L6IWgaCuilwC

[117] J. Dutka, "The early history of the factorial function," *Archive for history of exact sciences*, vol. 43, no. 3, pp. 225–249, 1991.

[118] C.-P. Chen, "Complete monotonicity and logarithmically complete monotonicity properties for the gamma and psi functions," *Journal of Mathematical Analysis and Applications*, vol. 336, no. 2, pp. 812–822, 2007.

[119] M. Weir, G. Thomas, and J. Hass, *Thomas' Calculus*, ser. Always Learning. Addison-Wesley, 2009. [Online]. Available: https://books.google.co.uk/books?id=yavIPgAACAAJ

[120] K. Rastogi and K. Ghosh, "The effect of multiple sink on the lifetime of wsn for different grid geometry," *International Journal*, vol. 6, no. 2, 2017.

[121] R. Teja and S. Indu, "A priority based wsn clustering of multiple sink scenario using artificial bee colony algorithm," in *2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*, Oct 2016, pp. 130–134.

[122] L. Leao, V. Felea, and H. Guyennet, "Mac-aware routing in multi-sink wsn with dynamic back-off time and buffer constraint," in *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Nov 2016, pp. 1–5.

[123] A. R. Malviya and B. N. Jagdale, "Location privacy of multiple sink using zone partitioning approach in wsn," in *2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, Oct 2015, pp. 449–454.

[124] N. Jeyanthi and R. Thandeeswaran, *Security Breaches and Threat Prevention in the Internet of Things*. IGI Global, 2017.

[125] F. C. Delicá to, P. F. Pires, and T. Batista, *The Activity of Resource Modelling*. Springer International Publishing, 2017, pp. 19–32. [Online]. Available: https://doi.org/10.1007/978-3-319-54247-8_3

[126] C. M. D. Farias, W. Li, F. C. Delicato, L. Pirmez, A. Y. Zomaya, P. F. Pires, and J. N. D. Souza, "A systematic review of shared sensor networks," *ACM Comput. Surv.*, vol. 48, no. 4, pp. 51:1–51:50, Feb. 2016. [Online]. Available: http://doi.acm.org/10.1145/2851510

[127] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with cooja," in *31st IEEE conference on Local computer networks, proceedings 2006.* IEEE, 2006, pp. 641–648.

[128] L. M. Leemis, *Monte Carlo Simulation in Reliability.* John Wiley & Sons, Inc., 2005. [Online]. Available: http://dx.doi.org/10.1002/0471654507.eme275

[129] W. Ching, X. Huang, M. Ng, and T. Siu, *Markov Chains: Models, Algorithms and Applications*, ser. International Series in Operations Research & Management Science. Springer US, 2013. [Online]. Available: https://books.google.co.uk/books?id=NWpDAAAAQBAJ

[130] S. V. Autkar, M. R. Dhage, and S. P. Bholane, "A survey on distributed techniques for detection of node clones in wireless sensor networks," in *2015 International Conference on Pervasive Computing (ICPC)*, Jan 2015, pp. 1–4.

[131] Z. Li and G. Gong, "On the node clone detection in wireless sensor networks," *IEEE/ACM Transactions on Networking*, vol. 21, no. 6, pp. 1799–1811, Dec 2013.

[132] P. Uma Maheswari and P. Ganesh Kumar, "Dynamic detection and prevention of clone attack in wireless sensor networks," *Wireless Personal Communications*, vol. 94, no. 4, pp. 2043–2054, Jun 2017.

[133] J. Zhao, "On resilience and connectivity of secure wireless sensor networks under node capture attacks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 557–571, March 2017.

[134] F. Ye, H. Luo, J. Cheng, S. Lu, and L. Zhang, "A two-tier data dissemination model for large-scale wireless sensor networks," in *Proceedings of the 8th annual international conference on Mobile computing and networking.* ACM, 2002, pp. 148–159.

[135] R. Knoblauch, M. Pietrucha, and M. Nitzburg, "Field studies of pedestrian walking speed and start-up time," *Transportation Research Record: Journal of the*

Transportation Research Board, vol. 1538, pp. 27–38, 1996. [Online]. Available: https://doi.org/10.3141/1538-04

[136] A. S. Wander, N. Gura, H. Eberle *et al.*, "Energy analysis of public–key cryptography on small wireless devices [c]," in *Proceedings of the 3rd IEEE Intl Conference on Pervasive Computing and Communications. California: IEEE Computer Society Press*, 2005, pp. 324–328.

[137] P. W. Simons and E. Van Der Sluis, "Physical unclonable function," May 24 2016, uS Patent 9,350,330.

[138] G. Selimis, M. Konijnenburg, M. Ashouei, J. Huisken, H. de Groot, V. van der Leest, G. J. Schrijen, M. van Hulst, and P. Tuyls, "Evaluation of 90nm 6t-sram as physical unclonable function for secure key generation in wireless sensor nodes," in *2011 IEEE International Symposium of Circuits and Systems (ISCAS)*, May 2011, pp. 567–570.