



UNIVERSITI PUTRA MALAYSIA

***OPTIMIZED SCHEME FOR EFFICIENT AND SCALABLE KEY
MANAGEMENT IN IEEE 802.16E-BASED NETWORKS***

MOHAMMAD MEHDI GILANIAN SADEGHI

FK 2015 126



**OPTIMIZED SCHEME FOR EFFICIENT AND SCALABLE KEY
MANAGEMENT IN IEEE 802.16E-BASED NETWORKS**

By

MOHAMMAD MEHDI GILANIAN SADEGHI

**Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia,
in Fulfillment of the Requirements for the Degree of Doctor of Philosophy**

February 2015

All material contained within the thesis, including without limitation text, logos, icons, photographs and all other artwork, is copyright material of Universiti Putra Malaysia unless otherwise stated. Use may be made of any material contained within the thesis for non-commercial purposes from the copyright holder. Commercial use of material may only be made with the express, prior, written permission of Universiti Putra Malaysia.

Copyright © Universiti Putra Malaysia



DEDICATION

*To my dearest family and friends,
...for their unconditional and everlasting love and support*



Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirements for the degree of Doctor of Philosophy

OPTIMIZED SCHEME FOR EFFICIENT AND SCALABLE KEY MANAGEMENT IN IEEE 802.16E-BASED NETWORKS

By

MOHAMMAD MEHDI GILANIAN SADEGHI

February 2015

Chairman : Professor Borhanuddin Mohd Ali, PhD
Faculty : Engineering

The computer industry has defined the IEEE 802.16 family of standards that will enable mobile devices to access a broadband network as an alternative to digital subscriber line (DSL) technology. Based on this standard, WiMAX which stands for worldwide interoperability for microwave access, was introduced by an industry consortium called WiMAX Forum, to offer a broadband wireless access to a plethora of mobile devices such as lap top, smart phones, and potentially any other network of devices. Subsequently, Mobile WiMAX was developed based on IEEE802.16e to support mobility where mobile devices can then roam from one coverage area to the next and remain connected.

As the mobile devices join and leave a network, security measures must be taken to ensure the safety of the network against unauthorized usage by encryption and key management. IEEE 802.16e uses multicast and broadcast service (MBS) as an efficient mechanism to distribute the same data concurrently to multiple mobile stations (MSs) through one Base Station. To generate, update and distribute the keys for secure communication over IEEE 802.16e, the MBS applies Multicast and Broadcast Rekeying Algorithm (MBRA) as a basic key management algorithm. The main performance parameters of group key management schemes are typically communications, computation and storage cost as well as scalability and energy efficiency.

This thesis focuses on improving group key management performance in IEEE 802.16e. In general, there is a trade-off among the communications, computation and storage costs of key management scheme. The aim is to enhance the group key management performance by providing a good trade-off among the communications, computation and storage costs. In addition, the proposed scheme should guarantee network scalability and consumes less energy upon rekeying process.

First, a new key management scheme called Scalable and Efficient Key Management Protocol (SEKMP) is proposed. It is built on two tree data structures that organize the MSs into subgroups which enable it to manage the group keys effectively. One of the trees is a binary tree data structure and the other is a B-tree data structure. The aim of SEKMP is to seek a balance between various performance parameters.

Next, an enhanced version of the proposed Scalable and Efficient Key Management Protocol called extended SEKMP (E-SEKMP) is developed based on SEKMP. E-SEKMP works by arranging the MSs into three main groupings based on their duration of stay in the cell, which in turn depends on the speeds of the respective MSs.

Simulation results show that SEKMP achieves a better balance among the performance parameters compared against the other schemes, while E-SEKMP shows reduced communications costs and energy consumptions. In terms of communications costs, the proposed scheme shows 77.41% improvement in comparison to MBRA, and an average of 47.87% improvement over ELAPSE in all modes, while in energy consumptions, the proposed scheme consumes less energy with an average of 38.27% improvement over that of ELAPSE. In terms of scalability, the proposed scheme shows 94.18% improvement compared to MBRA and 61.15% compared to ELAPSE.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

**SKIM YANG DIOPTIMUMKAN UNTUK PENGURUSAN KUNCI CEKAP
DAN BOLEH SKALA DALAM RANGKAIAN BERASASKAN
IEEE802.16E**

Oleh

MOHAMMAD MEHDI GILANIAN SADEGHI

Februari 2015

Pengerusi : Profesor Borhanuddin Mohd Ali, PhD
Fakulti : Kejuruteraan

Industri komputer telah mentakrifkan keluarga piawaian IEEE 802,16 yang akan membolehkan peranti mudah alih untuk mencapai rangkaian jalur lebar sebagai alternatif kepada teknologi gelung pelanggan digital (DSL). Berdasarkan piawaian ini, WiMAX yang bermaksud capaian gelombang mikro saling beroperasi seluruh dunia, diperkenalkan oleh konsortium industri yang dikenali sebagai WiMAX Forum, untuk menawarkan capaian wayarles jalur lebar untuk pelbagai jenis peranti mudah alih seperti lap top, telefon pintar, dan beberapa banyak lagi rangkaian untuk peranti. Selepas itu, Mobile WiMAX dibangunkan berdasarkan IEEE802.16e untuk menyokong mobiliti di mana peranti mudah alih itu boleh merayau dari satu kawasan liputan kepada satu kawasan lain dan kekal disambungkan.

Oleh kerana peranti mudah alih menyertai dan meninggalkan rangkaian, langkah-langkah keselamatan perlu diambil untuk memastikan keselamatan rangkaian terhadap penggunaan yang tidak dibenarkan dan pencerobohan, dengan menggunakan penyulitan dan pengurusan kekunci terjamin. IEEE 802.16e menggunakan perkhidmatan multicast dan penyiaran (MBS) sebagai mekanisme yang cekap untuk mengedarkan data yang sama secara serentak ke beberapa stesen mudah alih (MS) melalui satu Stesen Pangkalan. Untuk menjana, mengemaskini dan mengedarkan kekunci untuk komunikasi selamat melalui IEEE 802.16e, MBS menggunakan algoritma penjanaan kekunci semula Multicast dan Penyiaran (MBRA) sebagai algoritma pengurusan kekunci asas. Parameter prestasi utama skim pengurusan kekunci kumpulan biasanya adalah kos komunikasi, pengiraan dan penyimpanan serta kebolehan untuk diskala dan kecekapan tenaga.

Tesis ini memberi tumpuan kepada meningkatkan prestasi pengurusan kekunci kumpulan dalam IEEE 802.16e. Secara umum, terdapat satu tolak ansur di antara kos komunikasi, pengiraan dan penyimpanan skim pengurusan kekunci. Tujuannya adalah untuk meningkatkan prestasi pengurusan kekunci kumpulan dengan menyediakan tolak ansor yang baik antara kos komunikasi, pengiraan dan penyimpanan. Di samping itu, skim yang dicadangkan perlu menjamin kebolehan berskala untuk rangkaian dan menggunakan tenaga yang kurang dalam proses penjanaan semula kekunci .

Pertama, skim pengurusan kekunci baru yang dikenali sebagai Protokol Pengurusan Kekunci Boleh diskala dan Cepak (SEKMP) adalah dicadangkan. Ia dibina di atas dua struktur data pohon yang mengaturkan MS ke dalam kumpulan kecil yang membolehkannya mengurus kekunci kumpulan dengan berkesan. Salah satu pohon adalah struktur data pohon binari dan satu lagi struktur data pohon B order 2. Tujuan SEKMP adalah untuk mendapatkan keseimbangan antara pelbagai parameter prestasi.

Seterusnya, versi protokol Pengurusan Kekunci Boleh diskala dan Cepak yang dipertingkatkan (E-SEKMP) telah dibangunkan berdasarkan kepada SEKMP. E-SEKMP berfungsi dengan menyusun MS kepada tiga kumpulan kekunci berdasarkan tempoh mereka tinggal di dalam sel, yang seterusnya bergantung kepada kelajuan MS masing-masing.

Keputusan simulasi menunjukkan SEKMP mencapai keseimbangan yang lebih baik di antara parameter prestasi berbanding dengan skim lain manakala E-SEKMP menunjukkan kos komunikasi dan konsumsi tenaga yang rendah. Dari segi kos komunikasi, skim yang dicadangkan menunjukkan peningkatan 77.41% berbanding dengan MBRA, dan purata peningkatan 47.87% berbanding dengan ELAPSE dalam kesemua mod, manakala dalam konsumsi tenaga, skim yang dicadangkan menggunakan tenaga yang kurang dengan purata peningkatan 38.27% berbanding dengan ELAPSE. Dari segi kebolehan untuk diskala, skim yang dicadangkan menunjukkan peningkatan 94.18% berbanding dengan MBRA dan 61.15% berbanding dengan ELAPSE.

ACKNOWLEDGEMENTS

I humbly thank Allah Almighty, the Beneficent and the Merciful, who gave me health, thoughts and co-operative people to enable me achieve this goal. This work would not be accomplished without the help of so many people. In the following lines is a brief account of some but not all who deserve my thanks. First, I would like to thank Professor Borhanuddin Mohd Ali for taking the burden of supervising this research. His theoretical insight and his relentless enthusiasm for help created such inspiration to make this direction and finally, to succeed in this study.

I am also delighted to convey my appreciations to my committee, Professor Nor Kamariah Noordin , Professor Sabira Khatun and Dr. Jamalul-lail Ab Manan for their support and guidance throughout this research. Their supports, suggestions, criticisms and frequent encouragements have been pivotal in improving my thesis. I am grateful to Professor Maode Ma from Nanyang Technological University for his advices. My warmest gratitude goes to all of my family members, especially my father, my mother and my brother and sisters for their endless love and persistent support, understanding and encouragement throughout my life.

Although few words do not justice to their contribution, I am grateful to have such helpful friends around who always showed concern in my work and helped me. Among those I would like to name Messrs Abbas, Pouria, Farhad, Ayyoub, Mojtaba, and of course, many others. I must also express my sincere gratitude to staff members in the Department of Computer and Communication Systems Engineering and Qazvin Azad University for their help and support. My heartfelt thanks to all of you, again, with our nice memory that I never could forget them.

I certify that a Thesis Examination Committee has met on 16 February 2015 to conduct the final examination of Mohammad Mehdi Gilanian Sadeghi on his Doctor of Philosophy thesis entitled “Optimized Scheme For Efficient And Scalable Key Management In IEEE 802.16e-Based Networks” in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

Alyani Ismail, PhD

Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Mohd Fadlee A. Rashid, PhD

Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Abd Rahman Ramli, PhD

Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Abdallah M’hamed, PhD

Professor
RST department
Telecom Sudparis France
(External Examiner)



ZULKARNAIN ZAINAL, PhD

Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 19 March 2015

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Borhanuddin Mohd Ali, PhD

Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Nor Kamariah Noordin, PhD

Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Sabira Khatun, PhD

Professor
Faculty of Computer and Communication Engineering,
Universiti Malaysia Perlis
(Member)

Jamalul-lail Ab Manan, PhD

Assistant Professor
Advanced Analysis and Modeling (ADAM) Cluster
MIMOS Berhad
(Member)

BUJANG BIN KIM HUAT, PhD

Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by Graduate Student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: _____



Date: _____

Name and Matric No.: Mohammad Mehdi Gilanian Sadeghi, GS21094


Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature:


Name of Chairman
of Supervisory
Committee:



Prof. Dr. Borhanuddin Mohd Ali
Pegawai Kanan
Kementerian Kejuruteraan Sistem Komputer dan Komunikasi
Pakulti Kejuruteraan
Universiti Putra Malaysia

Signature:


Name of Member of
Supervisory
Committee:



PROF. DR. NOR KAMARIAH NOORDIN
Pegawai Kanan
Pejabat Strategi Korporat dan Komunikasi
Universiti Putra Malaysia
Professor Dr. Nor Kamariah Noordin

Signature:


Name of Member of
Supervisory
Committee:



Prof. Dr. Sabira Khatun
Pegawai Kanan
Kementerian Kejuruteraan Sistem Komputer dan Komunikasi
Pakulti Kejuruteraan
Universiti Putra Malaysia
Professor Dr. Sabira Khatun

Signature:

Name of Member of
Supervisory
Committee:



Prof. Dr. Jamalul-lail Ab Manan
Pegawai Kanan
Kementerian Kejuruteraan Sistem Komputer dan Komunikasi
Pakulti Kejuruteraan
Universiti Putra Malaysia
Assistant Professor Dr. Jamalul-lail Ab Manan

TABLE OF CONTENTS

| | Page |
|---|-------------|
| ABSTRACT | i |
| ABSTRAK | iii |
| ACKNOWLEDGEMENTS | v |
| APROVAL | vi |
| DECLARATION | viii |
| LIST OF TABLES | xii |
| LIST OF FIGURES | xiii |
| LIST OF ABBREVIATIONS | xvi |
| | |
| CHAPTER | |
| | |
| 1 INTRODUCTION | 1 |
| 1.1 Background | 1 |
| 1.2 Problem Statement and Motivation | 2 |
| 1.3 Research Aim and Objectives | 3 |
| 1.4 Thesis Scope | 3 |
| 1.5 Brief Methodology | 4 |
| 1.6 Study Module | 5 |
| 1.7 Thesis Organization | 5 |
| | |
| 2 LITERATURE REVIEW | 6 |
| 2.1 Introduction | 6 |
| 2.2 Group Key Management Schemes | 6 |
| 2.2.1 Centralized Group Key Managements Schemes | 9 |
| 2.2.2 Decentralized Group Key Managements Schemes | 12 |
| 2.2.3 Distributed Group Key Managements Schemes | 12 |
| 2.3 IEEE 802.16 Standard Architecture | 13 |
| 2.3.1 Protocol Layers within IEEE 802.16 | 13 |
| 2.3.2 Security Sub-layer | 15 |
| 2.4 Key Management in IEEE 802.16e: Privacy Key Management Version2 | 18 |
| 2.5 Related Works on Key Management in IEEE 802.16 | 21 |
| 2.5.1 Enhancement of the MBRA algorithm | 21 |
| 2.5.2 Secure Multicast Protocols | 21 |
| 2.5.3 Group-Based Key Distribution Algorithm | 22 |
| 2.5.4 Efficient sub-Linear rekeying Algorithm with Perfect Secrecy | 22 |
| 2.5.5 Hybrid Group Key Management | 24 |
| 2.5.6 n-ary Group Key Management | 25 |
| 2.5.7 Asymmetric Group Key Management | 26 |
| 2.6 Summary | 28 |
| | |
| 3 METHODOLOGY | 29 |
| 3.1 Introduction | 29 |
| 3.2 Proposed Scalable and Efficient Key Management Protocol (SEKMP) | 31 |
| 3.2.1 Splitting the trees | 34 |

| | | |
|----------|---|------------|
| 3.2.2 | Merging the trees | 41 |
| 3.2.3 | System Description | 43 |
| 3.2.4 | Performance parameters | 44 |
| 3.3 | Extended Scalable and Efficient Key Management Protocol (E-SEKMP) | 51 |
| 3.4 | Summary | 62 |
| 4 | RESULTS AND DISCUSSION | 63 |
| 4.1 | Introduction | 63 |
| 4.2 | System Design and Performance Parameters | 63 |
| 4.3 | Performance Evaluation of SEKMP | 65 |
| 4.3.1 | Analysis of the Communications overhead | 65 |
| 4.3.2 | Analysis of the Storage | 71 |
| 4.3.3 | Analysis of the Computation cost | 79 |
| 4.3.4 | Analysis on the Scalability | 88 |
| 4.3.5 | Security Analysis | 89 |
| 4.4 | Performance Evaluation of E-SEKMP | 94 |
| 4.4.1 | Analysis of the Communications overhead | 94 |
| 4.4.2 | Analysis of the Storage | 95 |
| 4.4.3 | Analysis of the Computation cost | 96 |
| 4.4.4 | Analysis on the scalability | 98 |
| 4.4.5 | Analysis of Energy Consumption | 98 |
| 4.5 | Summary | 100 |
| 5 | CONCLUSIONS AND FUTURE RESEARCH directions | 101 |
| 5.1 | Conclusions | 101 |
| 5.2 | Future Research Directions | 102 |
| | REFERENCES | 104 |
| | BIODATA OF STUDENT | 111 |
| | LIST OF PUBLICATIONS | 112 |

LIST OF TABLES

| Table | Page |
|---|------|
| 2.1 Nomenclature of key management | 21 |
| 2.2 Summary of the main performance parameters of rekeying algorithms | 27 |
| 3.1 An example of subgroup-IDs | 32 |
| 3.2 Communications cost upon member leave event | 46 |
| 3.3 Storage costs | 47 |
| 3.4 Scalability analysis | 50 |
| 3.5 The number of received keys | 60 |
| 3.6 Number of received keys by MSs upon an MS joins SG_{1a1} | 61 |
| 3.7 Number of received-broadcast keys by MSs | 61 |
| 4.1 Considered scenarios parameters in each Scenario | 64 |
| 4.2 Average number of current MSs for all scenarios | 69 |
| 4.3 Communications cost by way of analytical model | 70 |
| 4.4 Storage cost comparison by way of analytical model | 78 |
| 4.5 Computation cost comparison by way of analytical model | 86 |

LIST OF FIGURES

| Figure | Page |
|--|------|
| 1.1 Study module | 5 |
| 2.1 Challenges in group key management | 8 |
| 2.2 Group key management classification | 9 |
| 2.3 Trade-off between storage and communication costs | 9 |
| 2.4 Three types of typical tree structures: (a) Star (b) Tree (c) Hybrid | 10 |
| 2.5 A logical key hierarchy tree | 11 |
| 2.6 Protocol stack of IEEE 802.16 [9] | 13 |
| 2.7 Security sub-layer architecture [9] | 15 |
| 2.8 Key derivation and message exchange flow in initial network entry [9] | 17 |
| 2.9 Key generation at initial network entry [9] | 18 |
| 2.10 MBRA messages [9] | 20 |
| 2.11 Key hierarchy with four subgroups [19] | 23 |
| 2.12 A revised version of ELAPSE [22] | 25 |
| 2.13 A 3-ary tree [18] | 25 |
| 3.1 Overview of the proposed schemes | 29 |
| 3.2 Block diagram showing the methodology of the proposed key management schemes | 30 |
| 3.3 The binary tree of Table 3.1 | 32 |
| 3.4 B-tree structure | 33 |
| 3.5 Making two subgroups: initial state | 34 |
| 3.6 Making three subgroups by way of splitting the tree | 35 |
| 3.7 Making four subgroups by way of splitting the tree | 38 |
| 3.8 Making five subgroups by way of splitting the tree | 39 |

| | | |
|------|--|----|
| 3.9 | Flowchart of the proposed SEKMP scheme upon member joining | 41 |
| 3.10 | Making four subgroups by way of merging two subgroups | 42 |
| 3.11 | Flowchart of the proposed SEKMP scheme upon member leaving | 43 |
| 3.12 | A tree with five subgroups | 48 |
| 3.13 | Schematic diagram of the proposed E-SEKMP | 51 |
| 3.14 | The proposed E-SEKMP scheme | 54 |
| 3.15 | Flowchart of the proposed E-SEKMP | 56 |
| 4.1 | Simulation scenario with different number of MSs | 64 |
| 4.2 | The cost of broadcast and unicast messages upon joining and leaving member for all scenarios | 68 |
| 4.3 | The total cost of broadcast and unicast messages for all scenarios | 70 |
| 4.4 | The cost of broadcast and unicast messages (analytical model) | 71 |
| 4.5 | The storage costs of MSs upon join event and leave event for various network sizes in terms of the current number of MSs | 74 |
| 4.6 | The storage costs of BS upon join event and leave event for various network sizes in terms of the current number of MSs | 77 |
| 4.7 | Average storage costs of BS upon join and leave events | 78 |
| 4.8 | Average storage costs of MSs upon join and leave events | 78 |
| 4.9 | The costs of storage for MS and BS (analytical model) | 79 |
| 4.10 | The computation costs of MS upon join and leave events for all scenarios | 82 |
| 4.11 | The computation costs of BS upon join and leave event for all scenarios | 85 |
| 4.12 | Average computation costs of BS | 86 |
| 4.13 | Average Computation costs of MS | 86 |
| 4.14 | Computation costs of MS and BS based on analytical model | 87 |
| 4.15 | Group size in key managements schemes | 88 |

| | | |
|------|--|----|
| 4.16 | Average number of subgroups versus current number of MSs | 89 |
| 4.17 | The procedure of splitting subgroups | 90 |
| 4.18 | The procedure of merging subgroups | 92 |
| 4.19 | Total broadcast and unicast keys for all scenarios | 95 |
| 4.20 | Average storage cost of MSs upon join and leave events | 95 |
| 4.21 | Average storage cost of BS upon join and leave events | 96 |
| 4.22 | The computation cost of MS | 97 |
| 4.23 | The computation cost of BS | 97 |
| 4.24 | Group size in the key management schemes | 98 |
| 4.25 | Energy consumed upon join event | 99 |
| 4.26 | Energy consumed upon leave event | 99 |

LIST OF ABBREVIATIONS

| | |
|------|---|
| AAA | Authorization, Authentication and Accounting |
| AK | Authorization Key |
| ARQ | Automatic Repeat Request |
| ATM | Asynchronous Transfer Mode |
| BS | Base Station |
| BW | Bandwidth |
| BWA | Broadband Wireless Access; Bandwidth Allocation |
| CID | Connection Identifier |
| CPS | Common Part Sub-layer |
| CS | Convergence Sub-layer |
| DL | Downlink |
| DSL | Digital Subscriber Line |
| EAP | Extensible Authentication Protocol |
| FDD | Frequency Division Duplexing |
| FDMA | Frequency Division Multiple Access |
| GKA | Group Key Agreement |
| GKEK | Group Key Encryption Key |
| GTEK | Group Traffic Encryption Key |
| ID | Identifier |
| IEEE | Institute of Electrical and Electronics Engineers, Inc. |
| IETF | Internet Engineering Task Force |
| KDC | Key Distribution Centre |

| | |
|-------|---|
| KEK | Key Encryption Key |
| LOS | Line of Sight |
| LTE | Long Term Evolution |
| MAC | Media Access Control |
| MAC | Message Authentication Code |
| MAN | Metropolitan Area Network |
| MBRA | Multicast and Broadcast Rekeying Algorithm |
| MBS | Multicast Broadcast Service |
| MS | Mobile Station |
| MSK | Master Session Key |
| MAN | Metropolitan Area Network |
| NLOS | Non Line of Sight |
| OFDMA | Orthogonal Frequency Division Multiple Accesses |
| OSI | Open Systems Interconnection |
| PDU | Packet Data Unit |
| PHY | Physical Layer |
| PKM | Privacy Key Management |
| PMK | Pairwise Master Key |
| PPP | Point to Point Protocol |
| PS | Privacy Sub-layer |
| QoS | Quality of Service |
| SA | Security Association |
| SAID | Security Association Identifier |
| SeS | Security Sub-layer |

| | |
|-------|---|
| SDU | Service Data Unit |
| SAP | Service Access Point |
| SS | Subscriber Station |
| TEK | Traffic Encryption Key |
| UL | UPLink |
| VLAN | Virtual Local Area Network |
| WiFi | Wireless Fidelity |
| WiMAX | Worldwide Interoperability for Microwave access |
| WLAN | Wireless Local Area Network |

CHAPTER 1

INTRODUCTION

1.1 Background

Wireless networks have become the principal technology for deployment of communications infrastructure due to their many benefits and advantages in comparison with the wired ones. In future the wireless networks will become the primary interface for network communication and main platform of applications and services [1].

Worldwide Interoperability for Microwave Access (WiMAX) [2] is a heterogeneous wireless network technology. WiMAX is designed to serve as the Metropolitan Area Networks (MANs), and it is an easier and cheaper alternative to wired networks such as backhauling cables, digital subscriber line (DSL) and T1 for various types of networks. WiMAX, which is an industry branding for IEEE 802.16 based networks [3], is an open standard that offers high throughput and wider coverage compared to that of traditional wireless networks and is the predominant technology for wireless network deployment [4, 5].

IEEE 802.16 which is derived from the IEEE 802.16 working group [6] is used to identify the air interface for Broadband Wireless Access (BWA) over a metropolitan area. Among the series of IEEE 802.16 standards, IEEE 802.16-2001 [7] was first defined to provide the last mile for fixed Wireless MAN working at 10-66 GHz bands with Line-of-Sight (LOS). Then, IEEE 802.16d-2004 [8], consolidates the earlier standards working on 2-11 GHz bands with Non Line-of-Sight (NLOS) plus mesh nodes. The amendment in IEEE 802.16e-2005 [9] versions also known as Mobile WiMAX provides mobility support in BWA. It is by far the most popular version, even though newer versions i.e. IEEE 802.16m [10], have also been formulated.

As for the security model of IEEE 802.16, it has been designed to guarantee authentication, confidentiality, integrity, privacy and access control. The main aspect of security is to transfer the security keys between Base Stations (BS) and Mobile Stations (MSs), in a secure way. The IEEE 802.16d [8] which was defined for fixed wireless access uses Privacy Key Management Version 1 (PKMv1) to define, manage and distribute the keys, but there are several security issues in PKMv1 [11, 12]. Hence, in IEEE 802.16e, an enhanced key management scheme called Privacy Key Management Version 2 (PKMv2) [9] was introduced to mitigate the security shortcomings of PKMv1.

PKMv2 uses Extensible Authentication Protocol (EAP) [13] and RSA algorithm [14] as authentication methods. The authentication mechanism ensures that when an MS enters a particular BS coverage area, it should perform authentication and authorization for access in order to obtain the keys that will protect data traffic more securely.

IEEE 802.16 supports multicast applications such as pay-per-view, teleconferencing, online auction through Multicast and Broadcast Service (MBS) [9]. Multicast is a very efficient technique for group communications. Several applications, such as online games, newscast, stock quotes, multiparty conferences, and military communications, can benefit from secure multicast communications. MBS, which is a new application feature for broadband wireless standards, constitutes an integral part of the IEEE 802.16e. In fact, MBS of IEEE 802.16e provides an efficient mechanism to distribute the same data concurrently to multiple MSs through the BS using shared radio resources. The MBS can be used to transfer any type of data, e.g., text, streaming media and multimedia based on local policy. In order to generate, update and distribute the security keys for secure communication over IEEE 802.16e, the MBS applies Multicast and Broadcast Rekeying Algorithm (MBRA) [9] as a basic rekeying algorithm.

1.2 Problem Statement and Motivation

In broadband wireless access networks such as WiMAX, there is an increased demand for an efficient and secure group communications, where applications like pay-per-view, video conferencing and online games are commonplace. The group communication uses a shared security key by way of group key management to encrypt the data in order to secure the group and prevent unauthorized users from accessing the data through encryption. This procedure is referred to as access control [15]. An ideal, group key management should be secure, scalable to extend to a larger group size and provide good efficiency. Hence, group key management schemes faces issues on performance, efficiency, security and scalability. This situation motivates us to pursue the research in this thesis to solve the issues of key management and propose a new scalable and efficient group key management solution for the IEEE 802.16 wireless networks.

In IEEE 802.16e standard, group key management scheme is handled by MBS, but its usage in the standard is still in its infancy. It does not take any consideration on scalability and efficiency during group key distribution among MSs and it does not support backward and forward secrecy [16]. There are a few group key management schemes for IEEE 802.16 such as those described in [17-25] that used fixed tree structures to group members to implement group key management, but the key updating costs, in term of operational efficiency and scalability is not balanced, so this reduces the overall performance of the network. The main problem here is to define a constant tree structure to manage key updating process. Thus, the aim of this thesis is to overcome the aforementioned

shortcoming. This is achieved by way of a dynamic group key management mechanism to establish a trade-off among various performance parameters.

1.3 Research Aim and Objectives

This thesis focuses on improving group key management performance of the existing schemes in IEEE 802.16e in terms of efficiency and scalability. As a general rule, there is trade-off among the performance parameters of group key management scheme, and the key management can only improve some of the performance parameters. Thus, the aim of this thesis is to enhance the group key management performance by providing a good enough trade-off among the communications, computation and storage costs in order to optimize (near optimal) the performance parameters. In addition, the group key management scheme will guarantee network scalability and consumes less energy in doing group key management. The main objectives of the thesis can be summarized as follows:

1. To propose a scalable, efficient group key management scheme in IEEE 802.16e by dynamic grouping of MSs in the BS coverage area using tree structures.
2. To develop an analytical model that can analyze the performance parameters of group key management in IEEE 802.16e.
3. To evaluate, through simulations, the proposed group key management scheme in terms of communications, computation and storage costs as well as scalability and energy consumption, and comparing the performance of the proposed scheme with the current schemes specified in IEEE 802.16e and some extension schemes on the standard.

1.4 Thesis Scope

The scope of this thesis is on the study and analyses of group key management for IEEE 802.16e, and developing an efficient and dynamic group key management scheme. It mainly focuses on operational efficiency, scalability and energy consumption specified for group key management in IEEE 802.16e networks. To be more specific, this thesis focuses on performance parameters on the following points:

1. The operational efficiency measured in terms of communications, computation and storage costs. The communications costs refer to the number of transmitted messages upon a key management; the computation costs refer to the time required of ciphering operations in order to get the updated group

keys, and the storage costs refer to the number of keys stored by the BS and MSs

2. Scalability which means the capability of key management protocol to handle a large group of members, and also its ability to manage highly dynamic membership changes. The 1-affect-n phenomenon is estimated from the number of members affected by rekeying operations.
3. A key management protocol that consumes small amount of energy especially for MSs which normally run on small batteries.

1.5 Brief Methodology

The focus of this thesis is to develop a dynamic group key management algorithm for IEEE 802.16e networks. The proposed schemes, referred to as Scalable and Efficient Key Management Protocol (SEKMP) and Extended Scalable and Efficient Key Management Protocol (E-SEKMP) are offered to solve the scalability and efficiency issues in the standard and existing group key management schemes.

Briefly, the proposed scheme dynamically establishes hierarchical trees in order to ensure the optimisation on the communications, computation and storage costs of the network. It further improves the scalability issue as well as minimizes energy consumption in the network.

This is achieved by means of two tree data structures that arrange the MSs into subgroups and manage the group keys effectively. A group of MSs forms a subgroup. One of the trees is a special binary tree data structure, called Set-pruning Trie described in [26, 27]. For simplicity, it will be referred to as a binary tree for the rest of the thesis. The other tree is a B-tree of order 2 data structure [28] that allows fast split and merge operations. After that, three above structures are applied to group the MSs in three main groups based on duration of stay in the cell.

1.6 Study Module

Figure 1.1 summarizes the scope of this thesis within the research issues for IEEE 802.16.

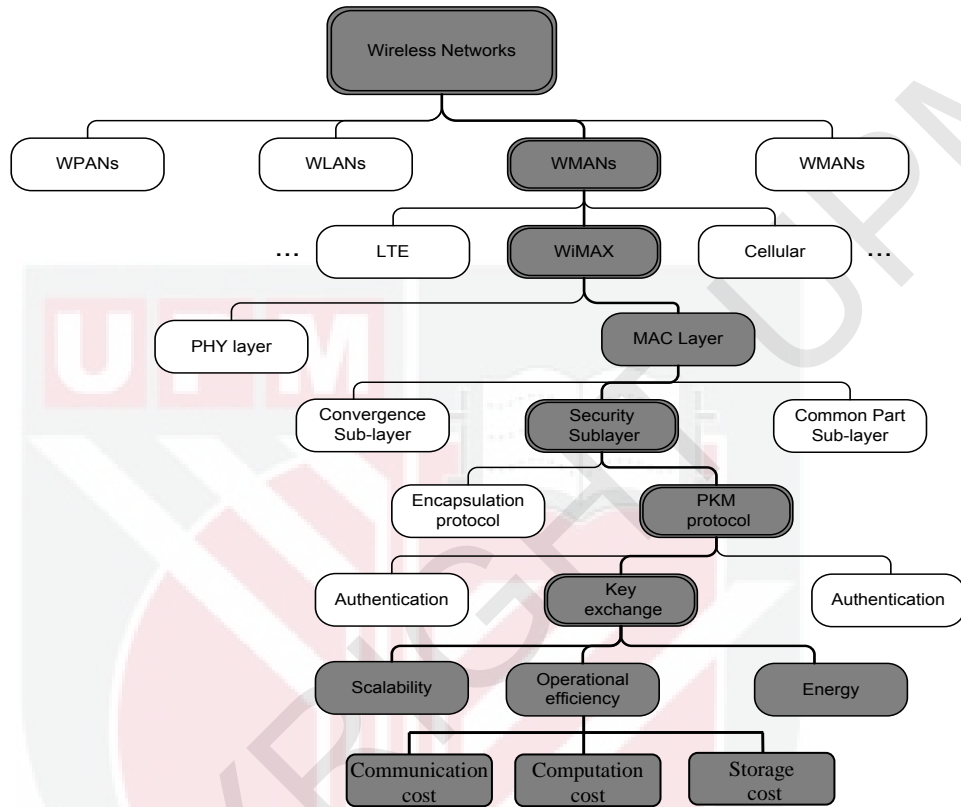


Figure 1.1 : Study module

1.7 Thesis Organization

This thesis is organized as follows. Chapter 1 gives a broad overview of the thesis and spells out its objectives. In Chapter 2, the literature review on group key management schemes especially on IEEE 802.16 is presented. Chapter 3 describes the proposed key management scheme which is an improvement on group key management in IEEE 802.16e. The results and discussion are explained in Chapter 4 to show the results from the numerical analysis and simulation approaches. We conclude our work and propose future works in the Chapter 5.

REFERENCES

- [1] R. Prasad and F. J. Velez, *WiMAX Networks*: Springer, 2010.
- [2] J. G. Andrews, et al., *Fundamentals of WiMAX: Understanding Broadband Wireless Networking*: Pearson Education, 2007.
- [3] C. Eklund, et al., "IEEE standard 802.16: A Technical Overview of the Wireless MAN Air Interface for Broadband Wireless Access," 2002.
- [4] K. Lu, et al., "WiMAX Networks: From Access to Service Platform," *IEEE Network*, 22 (3), pp. 38-45 2008.
- [5] "IEEE 802.16 Work Group. IEEE Std 802.16: Air Interface for Broadband Wireless Access Systems ", ed: IEEE, 2004.
- [6] IEEE 802.16 Working Group website. Available: <http://WirelessMAN.org>, August 2015
- [7] "IEEE 802.16 Work Group. IEEE std 802.16: Air Interface for Fixed Broadband Wireless Access System," ed: IEEE, 2002.
- [8] "IEEE 802.16 Work Group. IEEE std 802.16: Air Interface for Fixed Broadband Wireless Access System," ed: IEEE, 2004.
- [9] "IEEE 802.16 Work Group. IEEE Std 802.16e: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Amendment and Corrigendum to IEEE Std 802.16-2004," ed: IEEE, 2006.
- [10] "IEEE 802.16 Work Group: IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems Amendment 3: Advanced Air Interface," ed, 2011.
- [11] B. Kwon, et al., "Key Challenges in Securing WiMAX Mesh Networks," *Security and Communication Networks*, 2,(5), pp. 413-426, 2009.
- [12] D. Johnston and J. Walker, "Overview of IEEE 802.16 Security," *IEEE Security and Privacy*, 2,(3), pp. 40-48, 2004.
- [13] B. Aboba, et al., "Extensible Authentication Protocol," RFC 3748, 2004.
- [14] R. Laboratories, PKCS #1: RSA Cryptography Standard, 2002.
- [15] W. Stallings, *Network Security Essentials: Applications and Standards*: Prentice Hall, 2013.
- [16] S. Rafaeli and D. Hutchison, "A Survey of Key Management for Secure Group Communication " *ACM Computing Surveys*, 35,(3), pp. 309-329, 2003.
- [17] S. Xu, et al., "Secure Multicast in WiMAX," *Journal of Networks*, 3,(2), pp. 48-57, 2008.
- [18] J. Brown, et al., "Efficient Rekeying Algorithms for WiMAX Networks," *Security and Communication Networks*, 2,(5), pp. 392-400, 2009.
- [19] C. T. Huang and J. M. Chang, "Responding to Security Issues in WiMAX Networks," *IEEE IT Professional* 10,(5), pp. 15-21, 2008.

- [20] G. Kambourakis, et al., "Revisiting WiMAX MBS security," *Computers and Mathematics with Applications*, 60,(2), pp. 217-223, 2010.
- [21] H. Li, et al., "GKDA: A Group-Based Key Distribution Algorithm for WiMAX MBS Security," in *Pacific-Rim Conference on Multimedia*, 2006 pp. 310-318.
- [22] S. Chakraborty, et al., "A Scalable Rekeying Scheme for Secure Multicast in IEEE 802.16 Network," *Communications in Computer and Information Science*, Springer, 132,(2), pp. 471-481, 2011.
- [23] M. Ginley, et al., "Efficient and Secure Multicast in Wireless MAN," in *2nd International Symposium on Wireless Pervasive Computing*, 2007.
- [24] C.-T. Huang, et al., "Efficient and Secure Multicast in Wireless MAN: A Cross-layer Design," *Journal of Communications Software and Systems*, 3,(3), pp. 199-206, 2007.
- [25] J. Brown and X. Du, "Towards Efficient and Secure Rekeying for IEEE 802.16e WiMAX Networks," in *IEEE Global Telecommunications Conference*, 2009, pp. 1-6.
- [26] D. Medhi and K. Ramasamy, *Network Routing Algorithms, Protocols and Architectures*, 2007.
- [27] P. Gupta and N. McKeown, "Algorithms for Packet Classification," *IEEE Network*, 15,(2), pp. 24-32, 2001.
- [28] J. A. Store, *An Introduction to Data Structures and Algorithms*. Waltham, USA: Birkhauser, Springer, 2001.
- [29] S.-Y. Tang, et al., *WiMAX Security and Quality of Service: an end-to-end Perspective*: John Wiley & Sons, 2011.
- [30] K.-C. Chen and J. R. B. d. Marca, *Mobile WiMAX*: JohnWiley & Sons, 2008.
- [31] M. Baugher, et al., "Multicast Security (MSEC) Group Key Management Architecture," in *RFC 4046*, ed, 2005
- [32] C. Guo and C.-C. Chang, "An Authenticated Group Key Distribution Protocol Based on the Generalized Chinese Remainder Theorem," *International Journal of Communication Systems*, 27,(1), pp. 126-134, 2014.
- [33] A. Chan, et al., "Approximation Algorithms For Key Management In Secure Multicast," in *15th International Computing and Combinatorics Conference*, 2009, pp. 148-157.
- [34] C. K. Wong, et al., "Secure Group Communications Using Key Graphs," *IEEE/ACM Transaction on Networking*, 8,(1), pp. 16-30, 2000.
- [35] J. A. M. Naranjoa, et al., "A suite of Algorithms for Key Distribution and Authentication in Centralized Secure Multicast Environments," *Journal of Computational and Applied Mathematics*, 236,(12), pp. 3042-3051, 2012.
- [36] H. Guo, et al., "A Provably Secure Authenticated Key Agreement Protocol for Wireless Communications," *Computers & Electrical Engineering*, 38,(3), pp. 563-572, 2012.

- [37] K. Fukushima, et al., "Optimization of Group Key Management Structure with a Client Join-Leave Mechanism," *Journal of Information Processing* 16,(0), pp. 130-141, 2008
- [38] R. Wittmann and M. Zitterbart, *Multicast Communication: Protocols, Programming & Applications: Los Altos: Morgan Kaufmann, 2000.*
- [39] Q. Xie, "A New Authenticated Key Agreement for Session Initiation Protocol," *International Journal of Communication Systems*, 25,(1), pp. 47-54, 2012.
- [40] C.-C. Chang, et al., "A Novel Key Management Scheme for Dynamic Multicast Communications," *International Journal of Communication Systems*, 22,(1), pp. 53–66, 2009.
- [41] L. Ni, et al., "Strongly Secure Identity-based Authenticated Key Agreement Protocols," *Computers & Electrical Engineering*, 37,(2), pp. 205-217, 2011.
- [42] L. Chen, "Recommendation for Key Derivation Using Pseudorandom Functions," NIST Special Publication, 2009, available at: <http://dx.doi.org/10.6028/NIST.SP.800-108>
- [43] X. He, et al., "Dynamic Key Management in Wireless Sensor Networks: A survey," *Journal of Network and Computer Applications*, 36,(2), pp. 611-622, 2013.
- [44] E. E. Mohamed and E. Barka, "OMAC: A New Access Control Architecture for Overlay Multicast Communications," *International Journal of Communication Systems*, 24,(6), pp. 761-775, 2011.
- [45] T. Hardjono and L. R. Dondeti, *Multicast And Group Security. USA, 2003.*
- [46] Y. Challal and H. Seba, "Group Key Management Protocols: A Novel Taxonomy," *International Journal of Information Technology*, 2,(1), pp. 105-118, 2005.
- [47] S. Gharout, et al., "Key Management With Host Mobility in Dynamic Groups," in *International conference on Security of information and networks 2010*, pp. 186-193.
- [48] Y. Wang, et al., "Efficient Key Management for Secure Wireless Multicast," in *3rd International Conference on Convergence and Hybrid Information Technology, 2008*, pp. 1131-1136.
- [49] D. He, et al., "A Pairing-Free Certificateless Authenticated Key Agreement Protocol," *International Journal of Communication Systems*, 25,(2), pp. 221-230, 2012.
- [50] H. Lee, et al., "User-Oriented Key Management Scheme for Content Protection in OPMD Environment," *IEEE Transactions on Consumer Electronics*, 58,(2), pp. 484-490, 2012.
- [51] H. Harney and C. Muckenhirn, "Group Key Management Protocol (GKMP) Specification," in *RFC 2093*, ed, 1997.
- [52] H. Harney and C. Muckenhirn, "Group Key Management Protocol (GKMP) Architecture " in *RFC 2094*, ed, 1997.
- [53] A. Ballardie, "Scalable Multicast Key Distribution," *RFC 1949*, 1996.

- [54] M. Waldvogel, et al., "The VersaKey Framework: Versatile Group Key Management," *IEEE Journal on Selected Areas in Communications*, 17,(9), pp. 1614-1631, 1999.
- [55] A. Perrig, et al., "ELK, a New Protocol for Efficient Large-Group Key Distribution," in *IEEE Symposium on Security and Privacy*, 2001, pp. 247-262.
- [56] D. Naor, et al., "Revocation and Tracing Schemes for Stateless Receivers," in *21st Annual International Cryptology Conference on Advances in Cryptology*, 2001, pp. 41-62.
- [57] S. Setia, et al., "Kronos: A Scalable Group Re-Keying Approach for Secure Multicast," in *The IEEE Symposium on Security and Privacy*, 2000, pp. 215-228.
- [58] D. Liu, et al., "Efficient Self-Healing Group Key Distribution with Revocation Capability," in *10th ACM Conference on Computer and Communications Security*, 2003, pp. 231-240.
- [59] H. Xiong, et al., "New Identity-based Three-party Authenticated Key Agreement Protocol with Provable Security," *Journal of Network and Computer Applications*, 36,(2), pp. 927-932, 2013.
- [60] A. T. Sherman and D. A. McGrew, "Key Establishment in Large Dynamic Groups Using One-way Function Trees," *IEEE Transactions on Software Engineering*, 29,(5), pp. 444-458 2003.
- [61] B. DeCleene, et al., "Secure Group Communications for Wireless Networks," in *Military Communications Conference*, 2001, pp. 113-117.
- [62] O. Rodeh, et al., "Optimized Group Rekey for Group Communications Systems," in *Network and Distributed Systems Security Symposium*, 2000, pp. 39-48.
- [63] Y. Sun, et al., "Topology-aware Key Management Schemes for Wireless Multicast," in *Global Telecommunications Conference*, 2003, pp. 1471-1475.
- [64] A. Ghosh and F. Anjum, "Last Hop Topology Sensitive Multicasting Key Management," in *ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks*, 2005, pp. 63-70.
- [65] Y. Amir, et al., "Secure Group Communication Using Robust Contributory Key Agreement," *IEEE Transactions on Parallel and Distributed Systems*, 15,(5), pp. 468-480, 2004.
- [66] Y. Challal, et al., "SAKM: A Scalable and Adaptive Key Management Approach for Multicast Communications," *Computer Communication Review*, 34,(2), pp. 55-70, 2004.
- [67] J.-S. Li, et al., "Distributed Key Management Scheme for Peer-to-Peer Live Streaming Services," *International Journal of Communication Systems*, 26,(10), pp. 1259-1271, 2013.
- [68] R. Canetti, et al., "Efficient Communication-storage Trade-offs for Multicast Encryption," in *International Conference on the Theory and Applications of Cryptographic Techniques*, 1999, pp. 459-474.

- [69] J. Snoeyink, et al., "A Lower Bound for Multicast Key Distribution," in 20th Annual Joint Conference of the IEEE Computer and Communications Societies, 2001, pp. 422-431.
- [70] L. Xu and C. Huang, "Computation-Efficient Multicast Key Distribution," IEEE Transactions on Parallel and Distributed Systems, 19,(5), pp. 577-587, 2008.
- [71] D. Micciancio and S. Panjwani, "Optimal Communication Complexity of Generic Multicast Key Distribution," IEEE/ACM Transactions on Networking, 16,(4), pp. 803-813, 2008.
- [72] K. Fukushima, et al., "Design of Gradual Key Management Schemes for Mobile Content Distribution," IPSJ Journal, 47,(12), pp. 3137-3148, 2006.
- [73] M. Li, et al., "Optimization of Key Storage for Secure Multicast," in 35th Annual Conference on Information Sciences and Systems, 2001, pp. 771-774.
- [74] Y. Kim, et al., "Communication-Efficient Group Key Agreement," in 16th International Conference on Information Security: Trusted Information, 2001, pp. 229-244.
- [75] X. S. Li, et al., "Batch Rekeying for Secure Group Communications," in 10th International Conference on World Wide Web, 2001, pp. 525-534.
- [76] S. S. Kulkarni and B. Bruhadeshwar, "Distributing Key Updates in Secure Dynamic Groups," in Distributed Computing and Internet Technology, ed: Springer, 2005, pp. 410-419.
- [77] Z. Wen Tao, "Optimizing the Tree Structure in Secure Multicast Key Management," IEEE Communications Letters, 9,(5), pp. 477-479, 2005.
- [78] Y. R. Yang, et al., "Reliable Group Rekeying: A Performance Analysis," Computer Communication Review, 31,(4), pp. 27-38, 2001
- [79] M. Onen and R. Molva, "Group Rekeying With a Customer Perspective," in 10th International Conference on Parallel and Distributed Systems, 2004, pp. 223-229.
- [80] Y. Xu and Y. Sun, "A New Group Rekeying Method in Secure Multicast," in Computational Intelligence and Security, ed: Springer, 2005, pp. 155-160.
- [81] S. Zhu, et al., "Performance Optimizations for Group Key Management Schemes for secure multicast," in 23rd International Conference on Distributed Computing Systems, 2003, pp. 163-171.
- [82] H. Harney and E. Harder, "Logical Key Hierarchy Protocol," in Internet-Draft, Internet Engineering Task Force (IETF), 1999.
- [83] X. Zou, et al., Secure Group Communications over Data Networks: Springer, 2007.
- [84] T. Hardjono, et al., "Intra-Domain Group Key Management Protocol," Internet Draft, 2000.
- [85] F. Du, et al., "Towards Solving Multicast Key Management Problem," in 8th International Conference on Computer Communications and Networks, 1999, pp. 232-236.

- [86] S. Mitra, "Iolus: A Framework for Scalable Secure Multicasting," *Computer Communication Review*, 27,(4), pp. 277-288, 1997.
- [87] S. Rafaeli and D. Hutchison, "Hydra: A Decentralised Group Key Management," in 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002, pp. 62-67.
- [88] M. Steiner, et al., "Diffie-Hellman Key Distribution Extended to Group Communication," in 3rd ACM Conference on Computer and Communications Security, 1996, pp. 31-37.
- [89] K. Becker and U. Wille, "Communication Complexity of Group Key Distribution," in 5th ACM Conference on Computer and Communications Security, 1998, pp. 1-6.
- [90] Y. Kim, et al., "Tree-Based Group Key Agreement," *ACM Transactions on Information and System Security*, 7,(1), pp. 60-96, 2004.
- [91] "IEEE 802.16 Work Group. IEEE Std 802.16: Air Interface for Broadband Wireless Access Systems and Revision of IEEE Std 802.16-2004," ed: IEEE, 2009.
- [92] S. Ahson and M. Ilyas, *WiMAX: Standards and Security*. CRC Press, Inc. Boca Raton, FL, USA, 2008.
- [93] F. I. P. S. Publication, "Announcing the Advanced Encryption Standard (AES)," ed, 2001.
- [94] A. Deininger, et al., "Security Vulnerabilities and Solutions in Mobile WiMAX " *IJCSNS International Journal of Computer Science and Network Security* 7,(11), pp. 7-15, 2007.
- [95] T. Shon, et al., "Novel Approaches to Enhance Mobile WiMAX Security," *EURASIP Journal on Wireless Communications and Networking*, 2010,(1), pp. 1-11, 2010.
- [96] "P802.16m/D6, IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Broadband Wireless Access Systems - Advanced Air Interface," May 2010
- [97] J. Hur, et al., "Security Considerations for Handover Schemes in Mobile WiMAX Networks," in IEEE Wireless Communications and Networking Conference, 2008, pp. 2531-2536.
- [98] S. Jeon and Y. Kim, "WiMAX Multicast/Broadcast Services Support in Home Environments," *IEEE Transactions on Consumer Electronics*, 56,(3), pp. 1333-1339, 2010.
- [99] C. Koliass, et al., "Attacks and Countermeasures on 802.16: Analysis and Assessment," *IEEE Communications Surveys and Tutorials*, 15,(1), pp. 487-514, 2013.
- [100] S. Naseer, et al., "Vulnerabilities Exposing IEEE 802.16e Networks to DoS Attacks: A Survey," in 9th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008, pp. 344-349.
- [101] J. Fan, et al., "HySOR: Group Key Management With Collusion-Scalability Tradeoffs Using a Hybrid Structuring of Receivers," in 11th

- International Conference on Computer Communications and Networks, 2002, pp. 196-201.
- [102] "Scalable Network Technologies," <http://web.scalable-networks.com>.
- [103] "Microsoft Visual C++ 2010 Express Edition," <http://www.microsoft.com/visualstudio/eng/products/visual-studio-2010-express>.
- [104] K. C. Almeroth and M. H. Ammar, "Collecting and Modeling the join/leave Behavior of Multicast Group Members in the MBone," in 5th IEEE International Symposium on High Performance Distributed Computing, 1996, pp. 209-216.
- [105] K. C. Almeroth and M. H. Ammar, "Multicast Group Behavior in the Internet's Multicast Backbone (MBone)," IEEE Communications Magazine, 35,(6), pp. 124-129, 1997.
- [106] M. M. G. Sadeghi, et al., "Key Management in Mobile WiMAX Networks," in Selected Topics in WiMAX", ed: InTech, 2013.
- [107] J.-C. Lin, et al., "Secure and Efficient Group Key Management With Shared Key Derivation," Computer Standards & Interfaces, 31,(1), pp. 192-208, 2009.
- [108] M. M. G. Sadeghi, et al., "Scalable Rekeying Algorithm in IEEE 802.16e," in 17th Asia-Pacific Conference on Communications, 2011, pp. 726-730.
- [109] A. Daeinabi and A. G. Rahbar, "An Advanced Security Scheme Based on Clustering and Key Distribution in Vehicular Ad-hoc Networks," Computers & Electrical Engineering, 40,(2), pp. 517-529, 2013.
- [110] R. Nelson, Probability, Stochastic Processes, and Queueing Theory: The Mathematics of Computer Performance Modeling: Springer Verlag, 1995.
- [111] M. M. G. Sadeghi, et al., "An Energy Saving Scheme for Key Management Protocol in IEEE802.16e," in TENCON Spring Conference, 2013 pp. 525-529.
- [112] V. Bernardo, et al., "Towards Energy Consumption Measurement in a Cloud Computing Wireless Testbed," in International Symposium on Network Cloud Computing and Applications, 2011, pp. 91-98.
- [113] M. M. G. Sadeghi, et al., "Scalable and Efficient Key Management for Mobile WiMAX networks," International Journal of Communication Systems, 27,(10), pp. 2166-2189, 2014.