

國立交通大學

資訊管理研究所

博士論文

無基礎行動網路安全協定之研究—

以數位版權管理為例



**A Study on the Security Protocols for Wireless Ad-Hoc
Networks: A Case on Digital Rights Management**

研究生：黃俊傑

指導教授：羅濟群 教授

中華民國一〇〇年一月

無基礎行動網路安全協定之研究—
以數位版權管理為例

**A Study on the Security Protocols for Wireless Ad-Hoc
Networks: A Case on Digital Rights Management**

研究生：黃俊傑 Student : Chun-Chieh Huang

指導教授：羅濟群 Advisor : Chi-Chun Lo



Submitted to Institute of Information Management

College of Management

National Chiao Tung University

in Partial Fulfillment of Requirements

for the Degree of

Doctor of Philosophy

in

Information Management

January 2011

Hsinchu, Taiwan, Republic of China

中華民國一〇〇年一月

無基礎行動網路安全協定之研究—

以數位版權管理為例

學生：黃俊傑

指導教授：羅濟群

國立交通大學資訊管理研究所博士班

中文摘要

無基礎行動網路(Wireless Ad-Hoc Network, WAN)是由一群具無線傳輸能力之設備所構成之集合。因為無基礎行動網路具有動態拓樸、無線廣播之特性與本身網路特性的特性，使得它比其他的網路架構更容易遭受攻擊，以及更難設計出一個符合安全需求的群組通訊架構。然而，應用無基礎行動網路的環境，例如：軍事之應用，它需要更安全與穩定的通訊環境。

本研究致力於安全機制之設計，以提供應用於無基礎行動網路環境中達到安全通訊之目標。在本論文中，本研究以數位版權管理為核心思考幾個安全議題：應用於數位內容管理之執照簽署(Digital License)、於群播環境之金鑰管理、應用於點對點(Peer-to-Peer, P2P)的通訊環境中監督之管理，以及應用網頁服務(Web Service)之資源存取控制。基於上述之議題，本研究設計四個安全機制以滿足在無基礎行動網路(特別是以叢集架構所形成的無基礎行動網路(Cluster-based WANs))之安全性要求。

本研究提出了以群組為導向的提名式代理簽章機制(Group-Oriented Nominative Proxy Signature Scheme, GO-NPSS)，本機制將群組觀念融入至提名式代理簽章機制中，以滿足無基礎行動網路環境的要求。在此機制中數位內容提供者可將本身的簽章能力轉由一群代理人來完成，且數位內容提供者可以指派哪些

人具有簽章驗證能力。本研究希望在行動商務環境中，數位內容提供者可以順利的提供消費者完成執照合法性驗證的方法。於本機制中，可以保證消費者所獲得執照，確認是數位內容提供者所產生。此外，本研究亦對 GO-NPSS 機制之安全性進行分析，以證明本研究所提之機制滿足簽章機制安全上的要求。

本研究提出以 EBS(Exclusion Basis System)為基底之批次金鑰更新機制，應用於群組通訊的環境。本機制解決 EBS 不能提供群體成員同時加入與離開的要求。於此機制共有三個操作：新增成員、具抵擋部份共謀攻擊之成員離開、以及可抵共謀攻擊之成員離開。此外，於效能上之分析，本研究將從三個角度，包括：儲存空間的成本、計算上的成本、以及通訊之負荷；來比較本論文所提之機制與 EBS 之差異。從比較結果發現，本研究所提之機制較 EBS 來的更有效率及更具彈性。

本研究提出一個具監督能力之安全機制，並將其應用於點對點通訊架構之資料傳遞環境。本機制基於吳等學者所提的單一階層式監督機制，修改為可提供多個階層式監督機制。在本機制中，存在一個全域的叢集頭，由它來掌管與監督整個點對點之通訊。在每個叢集內，存在一個叢集頭，由它來掌管與監督整個叢集內點對點之通訊。藉由安全性之分析證明本論文所提之具監督能力的安全機制，達到監督之目的。在叢集內任兩個通訊節點可以產生彼此的通訊金鑰，以進行秘密通訊。叢集內或叢集外其他的節點是無法監聽通訊內容，除了該叢集內的叢集頭及全域的叢集頭才能監聽通訊內容。

最後，本研究設計一個應用於網頁服務的具彈性之存取控機制。此機制基於 RBAC(Role-Based Access Control)之存取控制模式，調適至符合本研究環境之存取控制機制。在此機制下，Web Service 伺服器依據目前需求者所在之位置資訊、該需求者在此位置下信譽度、結合所有該使用者曾經拜訪過位置的整體信譽度計算、每個領域的安全度及資料傳送路徑之信賴度等參數結合政策定義之資料庫，做為具彈性以角色為基底控制機制設計之基礎。所有信譽值的計算是由領域代理

者完成。實作結果，證明本研究可以滿足具彈性之存取控制要求，使得需求者必須依當時之條件存取到符合該條件的資料內容。

關鍵字：無基礎行動網路，批次金鑰更新機制，金鑰管理，數位簽章，監督機制，具彈性之存取控制機制



A Study on the Security Protocols for Wireless Ad-Hoc Networks: A Case on Digital Rights Management

Student: Chun-Chieh Huang

Advisor: Chi-Chun Lo

**Institute of Information Management
National Chiao Tung University**

ABSTRACT

A wireless ad-hoc network (WAN) is a collection of wireless mobile nodes and each of these can be considered as an individual portable devices. In such networks packets are relayed over multiple hops to reach their destination. Due to the infrastructure-less, dynamic, and broadcast nature of radio transmissions, communications in WANs are susceptible to security attacks. And, the inherent limitations of WANs impose major difficulties in establishing a suitable secure group communications framework. However, many applications, particularly those in military and critical civilian domains require that WANs be secure and stable.

For the sake of such reasons mentioned above, this dissertation focuses on the development of some security schemes and mechanisms to provide secure communications over WANs. In addition, this dissertation considers a scenario of digital rights management (DRM) in cluster-based WANs. Under this scenario, some security issues are announced and the corresponding solutions are proposed: Digital signature for digital license in DRM, key management for group communications, supervising management for peer nodes communications in peer-to-peer (P2P) application, and access control for managing the access privilege about the resources provided by web service. This dissertation is concerned with the design and development of such protocols in cluster-based WANs.

In dissertation, a group-oriented nominative proxy signature scheme (GO-NPSS) is proposed. This scheme adds the concept of group-oriented into nominative proxy signature scheme for cluster-based WANs. The scheme supports a content provider to delegate his/her signing ability to the partial members of a group of clearinghouses

and to designate the partial members of a group of consumers to verify their digital licenses. The proposed scheme can guarantee that the digital products come from the authorized providers. A formal security analysis demonstrates that our scheme is secure enough to be used in DRM systems.

In this dissertation, an EBS-based batch rekeying scheme is proposed. This scheme is an extension of EBS and provides the batch rekeying operations. The scheme supports three operations, join, leave with collusion-resistant (L/CR), and leave with collusion-free (L/CF). This dissertation compares the performance of the proposed scheme with that of EBS in terms of three performance metrics: storage cost, computation cost, and communications overhead. By comparison results, it indicates that the proposed scheme outperforms EBS in all three categories. The simulation results also indicate that the proposed scheme is more efficient and scalable than EBS.

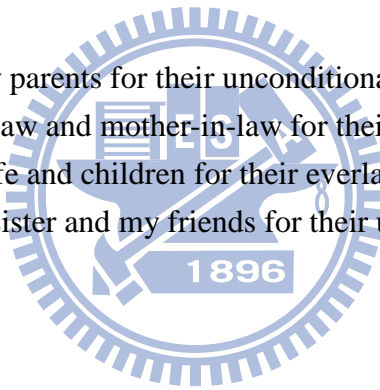
In this dissertation, a framework for supporting a supervising mechanism is introduced in the cluster-based P2P networks. This mechanism supports multiple chains partial order supervising mechanism instead of single chain partial order supervising mechanism proposed by Wu, etc. In the proposed mechanism, a global clusterhead supervises the whole network; clusterheads in each cluster supervise their own clusters' communications. Security analysis shows that the proposed mechanism is secure enough for P2P in WANs. Any two nodes within the same cluster generate their common session key. In the same cluster, no nodes gain this session key except the clusterhead.

Finally, a flexible access control mechanism is designed in this dissertation. This mechanism is an extension of role-based access control (RBAC) model and adds some profiles into a new access control mechanism. The mechanism is a combination of the requester's role, location, reputation, and the trust degree of the routing path. By this mechanism, the service provider easily calculates the requester's access privilege with respect to a specific resource. This dissertation implements this mechanism using XACML. The implementation results show that the proposed mechanism is feasible.

Keywords: Wireless ad-hoc network, Batch rekeying scheme, Key management, Digital signature, Supervising mechanism, Flexible access control mechanism

Dedications

To my parents for their unconditional love,
To my father-in-law and mother-in-law for their endless support,
To my wife and children for their everlasting love,
To my younger sister and my friends for their unlimited support



Acknowledgements

It is a pleasure to thank those who made this dissertation possible such as my Wife who gave me the moral support I required and my advisor who helped me with the research material, etc. My deepest gratitude is to my advisor, Professor Chi-Chun Lo. I appreciate very much the fact that he took me seriously when I communicated with him asking about the possibility of taking me as a Ph.D. student in his laboratory “Communication and Network” in the Institute of Information Management, National Chiao Tung University. I have been amazingly fortunate to have an advisor who gave me the freedom to explore on my own. Professor Lo taught me how to express ideas and gave me some excellent comments. His patience and continual support throughout my time in the Ph.D. program helped me overcome many problems and finish this dissertation. Without his guidance and support, this dissertation would not have been made possible. And, I hope that one day I would become as good an advisor to my students as Professor Lo has been to me.

Special thanks go to Professor Henry Ker-Chang Chang, who was my advisor when I took my master program. Professor Chang became a friend and a mentor within my Ph.D. program period. He taught me how to work hard, had confidence in me when I doubted myself, and brought out the good ideas in me. Without his encouragement and constant guidance, I could not have finished this dissertation.

I would like to thank all committee members for their comments and advice during my dissertation defense. Special thanks go to Professor Heng-Li Yang, Associate Professor Shi-Jen Lin, Professor Henry Ker-Chang Chang, and Professor Chyang Yang, for reviewing and giving me many valuable comments on my dissertation, and for kindly consenting on serving in my defense committee. Their intellectual comments about my research presentation encourage me to prepare fruitful presentation slides, thus I overcame all of my previous presentation sessions. Moreover, this dissertation would not have been possible without the financial support I received from National Science Council, recommended by Professor Chi-Chun Lo.

I also would like to make a special reference to my younger schoolmates in my Lab. Without their corporation I could not have done my dissertation and the projects. Ding-Yuan Cheng (Ph.D. student and will graduate at the same time), for helping me to prepare my dissertation defense as well as to give me many valuable suggestions

about my scenarios. Fang-Yi Lee, Kuang-Yu Chen, Ping-Hsien Ho, and Meng-Ju Lee (second-year master's students), help me for mental support in different situations, discussing many papers and exchanging many good ideas, and helping me prepare my dissertation defense.

Last but not least, I thank my family: my parents, Wen-Chih Huang and Chiu-Mien Huang, for giving me life in the first place, for encouraging me for whole of my educational life. Thanks to my younger sister, Wan-Shu Huang, for encouraging me to be brave and pursue without fear all challenging tasks coming in my way. Special thanks go to my father-in-law, Cheng-Te Chang, and mother-in-law, Yueh-Chiao Kuo. I would like to thank them for their faith in my abilities that gave me the strength to overcome all obstacles. Moreover, many thanks to my son, Sheng-Ju Huang and my daughter, Li-Ya Huang. Without their love, support, and encouragement, more than anything else, I would have never reached this stage in my life.

Finally, and most importantly, I would like to thank my wife Chao-Chun Chiang for her continuous hard work to maintain daily life and taking care of our children. She has given me tremendous love, support and encouragement. She gave infinite faith in me and unlimited support in everything I have set out to pursue, every dream I have ever had, possible or impossible. Without her encouragement, I wouldn't have been able to achieve my goals.

Table of Contents

中文摘要.....	I
ABSTRACT.....	IV
DEDICATIONS.....	VI
ACKNOWLEDGEMENTS	VII
TABLE OF CONTENTS.....	IX
LIST OF TABLES.....	XII
LIST OF FIGURES	XIII
CHAPTER 1 INTRODUCTION.....	1
1.1 RESEARCH BACKGROUND AND MOTIVATION	1
1.2 CONTRIBUTIONS OF THE DISSERTATION	8
1.3 ORGANIZATION OF THE DISSERTATION	9
CHAPTER 2 LITERATURES REVIEW.....	11
2.1 WIRELESS AD-HOC NETWORKS.....	11
2.2 SECURITY ISSUES IN WANS.....	17
CHAPTER 3 A GROUP-ORIENTED NOMINATIVE PROXY SIGNATURE SCHEME FOR DIGITAL RIGHTS MANAGEMENT.....	20
3.1 DIGITAL RIGHT MANAGEMENT INTRODUCTION	20
3.2 RELATED WORKS	25
3.2.1 Proxy Signature Scheme	25
3.2.2 Nominative Proxy Signature Scheme	27
3.3 THE PROPOSED GROUP-ORIENTED NOMINATIVE PROXY SIGNATURE SCHEME.....	28
3.3.1 Notations	28
3.3.2 The Proposed Scheme.....	29
3.4 SECURITY ANALYSIS	40
3.5 PERFORMANCE ANALYSIS	42
3.6 CONCLUSION.....	43
CHAPTER 4 AN EBS-BASED BATCH REKEYING SCHEME FOR SECURE GROUP COMMUNICATIONS	44
4.1 KEY MANAGEMENT INTRODUCTION	44
4.2 RELATED WORKS	45
4.2.1 EBS System	45

4.2.2	K-map Simplification.....	46
4.2.3	Chinese Remainder Theorem.....	46
4.3	THE BATCH REKEYING SCHEME	47
4.3.1	Notations	47
4.3.2	The Proposed Scheme.....	48
4.4	SECURITY AND PERFORMANCE ANALYSES	69
4.4.1	Security Analysis	69
4.4.2	Performance Analysis	73
4.5	SIMULATION RESULTS	75
4.6	CONCLUSION.....	78
CHAPTER 5 A TWO-KEY AGREEMENT BASED SUPERVISING MECHANISM FOR CLUSTER-BASED PEER-TO-PEER APPLICATIONS ..		79
5.1	SUPERVISING INTRODUCTION.....	79
5.2	RELATED WORKS	81
5.3	THE PROPOSED SUPERVISING MECHANISM.....	82
5.3.1	Notations	83
5.3.2	Initialization phase.....	85
5.3.3	Communication Phase.....	86
5.3.4	Supervising Phase.....	89
5.4	SECURITY ANALYSIS.....	91
5.4.1	The Security of Nodes' Private Keys.....	91
5.4.2	The Confidentiality of Communication Data	91
5.4.3	Against Replay Attack	92
5.4.4	Against Session Key Attack.....	92
5.5	CONCLUSION.....	93
CHAPTER 6 A FLEXIBLE ACCESS CONTROL MECHANISM FOR WEB SERVICES.....		94
6.1	INTRODUCTION	94
6.2	SYSTEM ARCHITECTURE	96
6.2.1	System Components.....	96
6.2.2	The System Workflow	98
6.3	THE PROPOSED FLEXIBLE ACCESS CONTROL MECHANISM.....	98
6.3.1	Reputation Management	99
6.3.2	Flexible Access Control.....	101
6.4	IMPLEMENTATION RESULTS.....	102
6.5	CONCLUSION.....	104
CHAPTER 7 CONCLUSION REMARKS		106

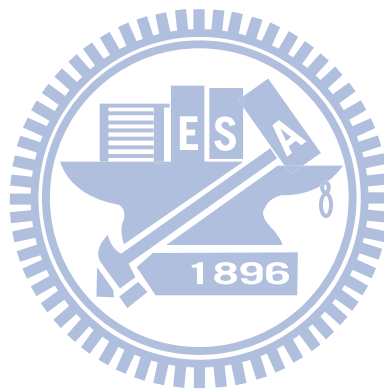
7.1 CONCLUSIONS 106

7.2 FUTURE RESEARCH DIRECTIONS 107

REFERENCES.....108

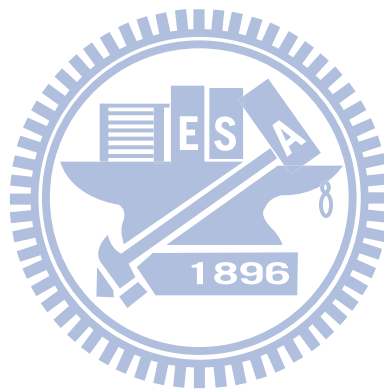
BIOGRAPHY 115

PUBLICATION LIST 116



List of Tables

TABLE 1. THE CLASSIFICATION OF ROUTING PROTOCOLS IN WANS	13
TABLE 2. THE EBS SYSTEM WITH $n = 5$, $k = 2$, AND $m = 2$	62
TABLE 3. BOOLEAN FUNCTION EXPRESSION	63
TABLE 4. THE SIMPLIFICATION PROCEDURE.....	64
TABLE 5. THE EBS SYSTEM WITH $n = 3$, $k = 2$, AND $m = 1$	64



List of Figures

FIGURE 1. THE FRAMEWORK OF THE PROPOSED DISSERTATION.....	4
FIGURE 2. THE STRUCTURE OF INFRASTRUCTURE-BASED WLANS	12
FIGURE 3. THE STRUCTURE OF WANS.....	13
FIGURE 4. THE ARCHITECTURE OF NEAR TERM DIGITAL RADIO (NTDR)	16
FIGURE 5. THE CONCEPT OF OPERATION MODE IN DRM SYSTEM.....	22
FIGURE 6. THE COMPONENTS IN DRM SYSTEM [21]	22
FIGURE 7. THE OVERALL DRM FRAMEWORK PROVIDED BY MICROSOFT CORPORATION [28].....	24
FIGURE 8. THE GO-NPSS SCHEME	30
FIGURE 9. THE FLOW CHART OF THE GROUP PRIVATE KEY GENERATION AND KEY SHARING IN <i>CHG</i>	31
FIGURE 10. THE FLOW CHART OF THE GROUP PRIVATE KEY GENERATION AND KEY SHARING IN <i>CVG</i>	34
FIGURE 11. NUMBER OF SESSION KEYS UPDATED	77
FIGURE 12. NUMBER OF ADMINISTRATION KEYS UPDATED	77
FIGURE 13. NUMBER OF REKEYING MESSAGES SENT	77
FIGURE 14. NUMBER OF ADMINISTRATION KEYS UPDATED	78
FIGURE 15. THE FRAMEWORK OF THE TWO-KEY AGREEMENT BASED SUPERVISING MECHANISM	83
FIGURE 16. THE FRAMEWORK OF THE PROPOSED FLEXIBLE ACCESS CONTROL MECHANISM	96
FIGURE 17. THE IMPLEMENTATION ENVIRONMENT	102
FIGURE 18. A TABLE WITH 7 COLUMNS.....	103
FIGURE 19. THE COLUMNS THAT THE REQUESTER CAN GET AFTER APPLYING THE RBAC MODEL	103
FIGURE 20. THE COLUMNS THAT THE REQUESTER CAN GET AFTER APPLYING THE FLEXIBLE ACCESS CONTROL MODEL	104
FIGURE 21. THE REQUESTER’S REQUEST IS DENIED. (THRESHOLD IS 0.3).....	104

Chapter 1 Introduction

In this chapter, research background and motivation, contributions of the dissertation, and organization of the dissertation are introduced.

1.1 Research Background and Motivation

Throughout the past decades, wireless communication network has become more popular than wired communication network. It is easier to deploy wireless communication network than conventional wired networks. They provide seamless connectivity within the coverage area. According to network attachment methods, there are two types of wireless networks: infrastructure-based and infrastructure-less wireless networks. In infrastructure-based networks, the mobile nodes rely on access points to attach the Internet. Typically examples of infrastructure-based networks are WLAN, GSM, and UMTS, etc. In infrastructure-less networks, the mobile nodes are capable of organizing themselves, by discovering their neighbors and communicating over the wireless medium. In other words, nodes in such networks, they communicate with their destination nodes by the help of their neighbors through store and forward technique. In recent years, infrastructure-less ad hoc networking technologies such as Wireless Ad-Hoc Networks (WANs) and Bluetooth have received critical attention in both academic and industry. In WANs, wireless mobile nodes are collected and each of these can be considered as an individual portable devices. The network topology in WANs changes frequently due to arbitrary movement of mobile nodes and is without any centralized administration or fixed infrastructure. Each node communicates directly with the nodes within its wireless range. However, the nodes need to collaborate together to deliver their information between nodes that are beyond the wireless range of the source. In WANs, nodes are more vulnerable to attacks because of their lack of a fixed infrastructure over the wireless environment. Any mobile node within the radio range of another node can always listen to what is being broadcasted, thus violating the privacy of the broadcasting node. Consequently, security is an important issue in WANs. Confidentiality, authentication, integrity, non-repudiation and access control are considered as the main services of a security system. Providing security support for WANs is a challenge because of: (1) wireless networks are susceptible to attacks ranging from passive eavesdropping to active interfering; (2)

mobile users demand anywhere and anytime services; (3) a scalable solution is a must for a large-scalable mobile network. To provide a secure communication environment for mobile users and applications over WANs is our goal.

This dissertation considers a scenario of designing some security schemes and mechanisms for digital rights management (DRM) system, electronic book as an example in this dissertation, in cluster-based WANs. This scenario provides a pure mobile commerce environment for participants. Traditionally, there are four roles in the publication system: authors, publishers, distributors, and consumers. An author or editor is responsible for writing articles and essays. A publisher is responsible for revising authors' manuscripts and adding some plates and contacting with distributors to discuss how to set up a distribution channel to sell these published books. A distributor is responsible for selling the books from publishers. And, a consumer could buy the books he/she wanted from a brick-and-mortar store. However, with the advent of digital information systems and the Internet, the scope of publishing has expanded to include electronic resources, such as the electronic versions of books. They could be sold online. There are three roles to online selling services in this dissertation: authors, distributors, and consumers. The role of a publisher is substituted by the authors and distributors. Assume there is a virtual team which offers the team work of authors. Each of them concentrates on their own expertise. Then, they integrate their works and deliver the final work to a distributor. The distributor distributes the digital contents to customers using cluster-based WANs. Hence, authors could co-work and focus on their domain knowledge to finish their works under this scenario. For example, a producing procedure of electronic voice book, to finish this work, the members should include: an editor, a drawer, and a recording engineer, etc. Because of their cooperation, the work could be done by themselves without a publisher. For a distributor, the duties of him/her include: to distribute the digital contents to his/her customers, to be a clusterhead and construct cluster-based WANs, to provide a repository to store published and protected e-books, and maintain a web service system. The web service keeps the related works which are not finished and unpublished. These works could be cited by other valid authors.

In this framework, shown in Figure 1, users or clients could request their favorite contents from a content provider, author, and then the content provider delivers the protected contents to users. The content received by client cannot be used without a

legal license because of encryption. When the user pays money and starts a license acquisition protocol with clearinghouse, the role of a distributor, for the content through DRM Agent in the client, the client can get the corresponding license for the content from the clearinghouse, and then the content can be rendered according to the usage rules in the license. A legal license should be confirmed by a consumer. This confirmation could be done by signature scheme. In addition, users in the communication network are legal group members. Members or authors, in the same cluster, could communicate and form a communication group by multicasting protocol. Thus, they could co-work to create an attractive work. Multicasting is an efficient way to deliver data to a large group of users in many applications such as Internet stock quotes, audio and music delivery, file and video distribution, etc. Data confidentiality is one of the most challenging problems in secure multicast. To achieve this goal, a secure multicast scheme must address key management issues, which include efficient organization and distribution of keys with low communication overheads, key storage cost, and scheme complexity. Moreover, in the proposed DRM system, it also supports peer-to-peer communications. Members or authors in the same cluster share their files, video, and audios with each other. For a supervising requirement, the clusterhead, the distributor, should supervise their communications to prevent the members violate some regulations. Furthermore, the proposed DRM system also provides web service for the group members. A legal member, author, who wants to get resources or gain access to the web service should register to the web service and be assigned a corresponding role associated with his/her identity. Then, he/she could issue a request in any cluster to access resources to the web service in the communications network.

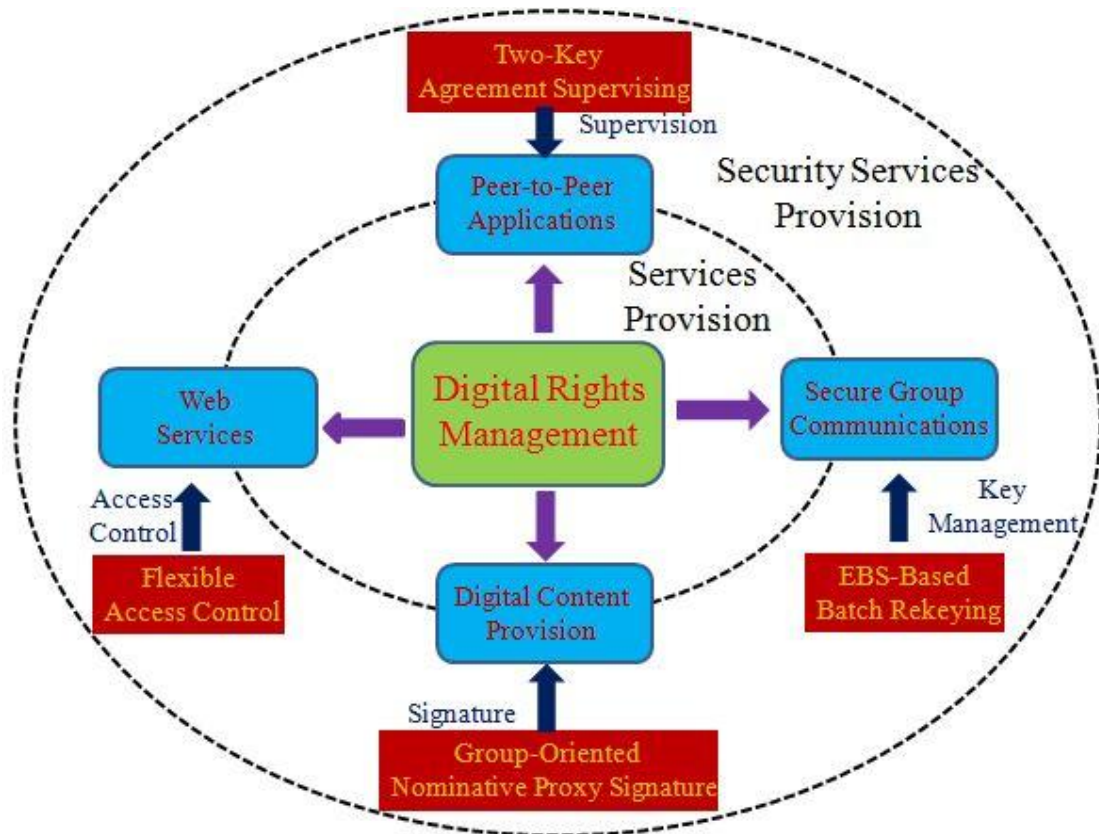


Figure 1. The framework of the proposed dissertation

For these reasons mentioned above, this dissertation focuses on the signature, key management, access control, and supervision security problems in WANs. The design principles of our study are developing some security protocols which support such security problems. Here, the related issues in signature, key management, supervision, and access control areas are described roughly, and more detailed discussions are explored in the further sections.

(1) Signature:

Signature is an important mechanism in any real applications. Digital signature is especially used in electronic-based transactions. The digital signature is analogous to the handwritten signature. The digital signature scheme allows a recipient of data to prove the source and integrity of data and protect against forgery. A group-oriented digital signature scheme is a kind of digital signature scheme. It supports a group of authenticated users to cooperatively sign a message instead of a single user. The same, the verification procedure must be done by the verifier. Such collaborative and group-oriented applications and protocols are useful in WANs.

In this work, the scenario of signature issues in DRM systems deployed in WANs is discussed. In DRM systems, digital licensing controls the contents to be accessed by the consumers. One of the major issues raised by DRM systems concerns the integrity of this license. Digital signatures provide data integrity, non-repudiation, and authentication. Therefore, digital signature is an important security mechanism for license-based DRM systems. Because of the properties of WANs, nodes may leave the network with high possibility than wired or infrastructure-based networks. In such case, a digital content provider may not sign the digital license in time. The consumer could not verify the validity of the protected digital contents and play digital contents on his/her platform. In this work, a group-oriented nominative proxy signature scheme is proposed. In such way, the content provider delegates his/her signing ability to the partial members of the proxy group having n members and to designates the partial members of the verifier group having l members to verify his/her digital licenses signed by a group of proxy signers. Therefore, (t, n) proxy signers sign the specific license on behalf of the original signer and (w, l) verifiers verify the validity of this proxy signature.

(2) Key management:

Securing group communications in resource constrained, infrastructure-less environments such as WANs has become one of the most challenging research directions in the area of wireless network security. This dissertation focuses on providing security from the perspective of enabling and protecting communication data among nodes, so that the appropriate data reaches the intended recipients and only these recipients have access right to read it. An important issue of providing such secure group communications in WANs is group key management. The group key shared by all group members is suitable for multicast communications. This key is used to encrypt communication data. Thus, only the group members could decrypt the encrypted data. Therefore, the group key must be protected from taking by non-group members. In addition, there are two important key factors while trying to design an efficient key management protocol, they are: the number of keys each node should keep and the number of rekeying operations should be done. Because of the nature topologies of WANs, nodes may join or leave the group frequently. Key management is an important security issue. In general, the key management protocol supports three kinds of rekeying operations: join, leave, and periodic rekeying operations.

In this work, a group key management protocol is proposed in WANs. It is based on the centralized key management frameworks. A key management protocol is designed such that batch rekeying operations are supported in cluster-based WANs. Therefore, the group key for encrypting multicast data is protected.

(3) Supervision:

Supervision is one of the security considerations. The term supervision is used to imply somewhat indirect degree of control over security operations. In supervising mechanism, a supervisor supervises the communications among nodes whose security level is lower than him/her. The concept of the supervising idea is especially important for government networks.

In this work, the supervising problem in Peer-to-Peer applications in cluster-based WANs is considered. A two-key agreement based supervising mechanism is proposed. The mechanism supports any two nodes within the same cluster communicate with each other and no other nodes overhear their communications other than the clusterhead of their domain and the global clusterhead. The proposed mechanism is designed for cluster-based applications in P2P.

(4) Access control:

Access control is the ability to limit and control the access to systems and applications via communications networks. It is a variety of mechanisms that enforce access rights to resources. A role-based access control model (RBAC) [43] is a kind of access control. In RBAC, roles are defined based on job functions, permissions are associated with roles, and users are made members of appropriate roles, thereby acquiring the roles' permissions. This indirect association between users and permissions greatly simplifies the management of user's permissions. There are many access control models which are designed based on the concept of RBAC model, such as Spatially Aware RBAC model [4][26][23], etc.

In this work, a scenario of access control for web services in WANs is discussed. In this scenario, the idea of reputation management is introduced into the access control model. In other words, each user's access ability is determined by both the initial assigned role and its reputation information. This access control mechanism is called flexible access control. Flexible access control is designed to enable access control while a requester asks for services from the web server. Flexible access

control is a combination of requester's role, location, requester's reputation, and the trust degree of the routing path. This mechanism is especially applicable to web services in WANs. Because users in WANs may roam randomly, they may suffer from some security attacks. The physical place where they stay may be insecure. Therefore, the user's access right has to be changed to prevent the possible attacks.

Finally, this dissertation describes the roles of each member in this communications network. They will be shown while constructing security schemes and mechanisms for a DRM system which supports digital content provision, group communication, peer-to-peer file sharing, and web service in cluster-based WANs. The roles of a global clusterhead and a clusterhead will be characterized in this session.

(1) The roles of a clusterhead:

- It is a domain broker and a key server. To be a domain broker, it has to manage the network of this cluster. To be a key server, it has to manage all kinds of keys for its domain users.
- It is a cleaninghouse and one of the proxy signers. To be a cleaninghouse, it has to sign a message for any content provider.
- A group of clusterheads should cooperatively sign a digital license on behalf of the content provider.

(2) The roles of a global clusterhead:

- There is a unique global clusterhead in cluster-based WANs.
- In addition, being one of the clusterheads, it has to manage the whole network.

(3) The roles of a group member in a cluster

- It could be a content provider or a consumer.
- It could join or leave a cluster freely.
- Peer members in the same cluster have to cooperatively generate their common session key for file sharing.
- A group of members purchase the goods from a content provider and they should cooperatively verify a signed digital license.

1.2 Contributions of the Dissertation

In this dissertation, we contribute towards the design and development of some security schemes and mechanisms to provide secure communications over WANs. There are four security issues are discussed under a scenario of DRM in WANs, they are: Digital signature, key management, supervising, and access control. The schemes or mechanisms designed in the proposed dissertation are new ones or an extension of existing methods so that the security and performance considerations are improved. The following paragraphs depict the contributions of the proposed four schemes and mechanisms.

The group-oriented nominative proxy signature scheme is proposed in this dissertation. The scheme supports a content provider to delegate his/her signing ability to the partial members of a group of clearinghouses and to designate the partial members of a group of consumers. Because of this scheme, even though the content provider is not in the network, his/her work will be done by a group of clearinghouses. A formal security analysis demonstrates that our scheme is secure enough to be used in DRM systems in WANs.

The key management problem is addressed for secure group communications in cluster-based WANs. There are three different batch rekeying operations. These operations provide a user easily or a group of users easily join or leave the group. Both the security and performance are discussed and compared in the dissertation. These results notice that the proposed scheme is secure and efficient.

A two-key agreement based supervising mechanism is proposed. The mechanism supports any two nodes within the same cluster communicate with each other and no other nodes overhear their communications other than the clusterhead of their domain and the global clusterhead. Because of this mechanism, the communications between mobile users could be managed. Thus, P2P applications are acceptable by the supervisor in WANs. Security analysis shows that the proposed mechanism supports the security requirements and guarantees only the supervisors overlook their communications.

A framework for implementing a flexible access control mechanism for web services is outlined. The framework uses a combination of the RBAC model and a user profile-based access control model which considers the location, the trust value

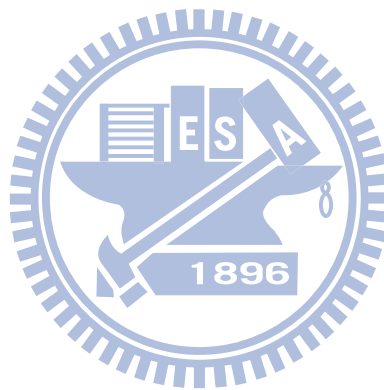
of the route path, and a requester's reputation as a profile about a specific requester. And, the access privilege for a requester is a combination of his/her access role and the profile evaluation result. Furthermore, implementation results demonstrate that the proposed mechanism dynamically adjusts requester's access privilege in no time.

1.3 Organization of the Dissertation

The remainder of the thesis is organized as follows. Chapter 2 presents background information and reviews related information security work. The characteristics and topologies of WANs are firstly reviewed. Then, information security is continued. Moreover, some security problems which may happen to WANs are discussed.

From chapter 3 to chapter 6, some security issues in WANs are discussed. Chapter 3 describes the security issue of a specific application – digital right management (DRM) in WANs. This chapter focuses on the signature of the digital license. Because of the properties of WANs, a group-oriented nominative proxy signature scheme is proposed. The scheme supports a content provider to delegate his/her signing ability to the partial members of a group of clearinghouses having n members and to designate the partial members of a group of consumers to verify their digital licenses. Some proofs are shown to demonstrate the validity of the signature. By security analysis, it shows that the proposed scheme satisfies the security requirements for proxy signatures. Chapter 4 describes the key management issue. In WANs, an important issue of providing secure group communications is group key management. In this dissertation, An EBS-based batch rekeying scheme is proposed. The scheme supports three operations, join, leave with collusion-resistant (L/CR), and leave with collusion-free (L/CF) for cluster-based communications in WANs. Some security and performance analyses with respect to the proposed scheme are given in this chapter. Chapter 5 also describes the security issue of a specific application – peer-to-peer (P2P) in cluster-based WANs. This chapter focuses on the supervising issue, one of the security issues, in P2P applications. A two-key agreement based supervising mechanism is proposed in this chapter. The mechanism supervises the communications between peer nodes. There are three phases in this mechanism to fulfill the supervising requirements. The same, security analysis shows that the proposed scheme satisfies the security requirements. Chapter 6 describes the access control mechanism for web service in cluster-based WANs. In this chapter, a flexible access control mechanism is proposed. The mechanism is a combination of the

requester's role, location, reputation, and the trust degree of the routing path. By this mechanism, the service provider easily calculates the requester's access privilege with respect to a specific resource. Therefore, a requester's access right not only depends on the initial assigned role also relies on the user's profile. The implementation results show that the proposed mechanism is feasible. Finally, in the last chapter, some conclusions are made and the possible future work in this area is described.



Chapter 2 Literatures Review

In this chapter, the characteristics and topologies of WANs are firstly reviewed. Then, information security will be reviewed. Moreover, some security problems which may happen to WANs will be discussed. These surveyed researches will be introduced respectively as follows.

2.1 Wireless Ad-Hoc Networks

It is easier to deploy wireless communication network than conventional wired networks. As the industry standards are maturing and the availability of wireless networking hardware is growing, wireless local area networks (WLANs) are being rapidly deployed in industrial, commercial, and home networks. As a result, use of wireless communications is increasingly becoming pervasive in our daily lives. Wireless networks include local, metropolitan, wide, and global areas. This dissertation focuses its attention on WLANs. In WLANs, it uses radio waves as its carrier. According to network attachment methods, there are two types of wireless networks: infrastructure-based and infrastructure-less wireless networks. Figure 2 illustrates the structure of infrastructure-based WLANs. In infrastructure-based WLANs, there is a need of an access point (AP) that bridges wireless LAN traffic into the wired LAN. An AP can also act as a repeater for wireless nodes. The basic service set (BSS) is a set of all stations that can communicate with each other. And an extended service set (ESS) is a set of connected BSSs. APs in an ESS are connected by a distribution system (DS). The concept of a DS can be used to increase network coverage through roaming between cells.

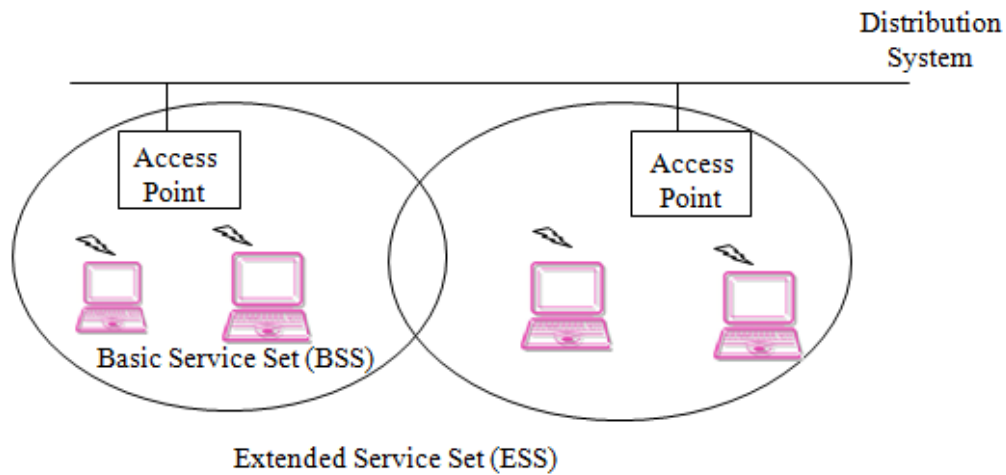


Figure 2. The structure of infrastructure-based WLANs

As wireless technology becomes more robust and sophisticated, multihop wireless networks are rapidly gaining attention. Multihop wireless networks, infrastructure-less WLANs, consist of wireless devices that communicate with each other either directly or using one or more other devices as intermediate forwarders. These networks can be deployed either as stand-alone networks or as edge networks extending the reach of the Internet. A kind of infrastructure-less topology is supported by WANs. They are a collection of mobile nodes dynamically forming a temporary network without using any existing network infrastructure. In addition, some cooperative networks are deployed in WANs with a specific purpose. They are widely used in the fields of military, collaborative business environment, etc. Unlike a fixed wireless network, the framework of WANs is characterized by the lack of infrastructure. Mobile nodes in WANs are free to move and organize themselves in an arbitrary fashion. Figure 3 illustrates the structure of WANs. In addition, each user is free to roam about while communicating with others. The path between each pair of the users may have multiple links, and the radio between them can be heterogeneous. This allows an association of various links to be a part of the same network. The challenges of WANs are included:

- Limited wireless transmission range
- Packet losses due to transmission errors
- Mobility-induced route changes

- Battery constraints
- Security issues

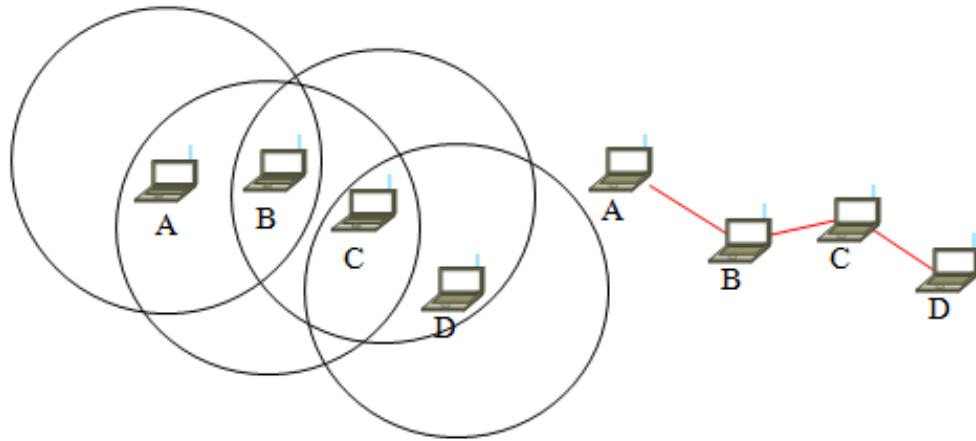


Figure 3. The structure of WANs

There are three types of routing protocols in WANs [36][41], they are: table-driven routing protocols, on-demand routing protocols, and hybrid routing protocols. Examples of some routing protocols in WANs are shown in Table 1.

Table 1. The classification of routing protocols in WANs

	Source routing	Hop-by-hop routing
Table-driven		DSDV, CGSR
On-demand	DSR	TORA, AODV, CBRP
Hybrid	ZRP	

A table-driven routing protocol is a kind of proactive protocol. It propagates topology information periodically and finds routes continuously between any two nodes in the network. Some of the well-known table-driven routing protocols, such as the Destination-Sequenced Distance Vector (DSDV) protocol [37] and the Clusterhead Gateway Switch Routing Protocol (CGSR) [2], require each mobile node

to update and maintain the route entries within their own routing table whenever a change of network topology occurs so that the most recent and shortest path can be chosen. It also requires a relatively large number of route control messages to keep each node informed of the latest network topology. Thus, this approach consumes significant amount of network resources in general.

An on-demand routing protocol is a kind of reactive protocol. It finds routes only when it needs routes to send data packets. Some of the well-known on-demand routing protocols such as Dynamic Source Routing (DSR) [13], Ad-Hoc On-Demand Distance Vector (AODV) [38], Cluster-based Routing Protocol (CBRP) [12] and Temporally-Ordered Routing Algorithm (TORA) [35], etc. They do not use up resources to maintain a routing table with the entire topology views, but instead routes are only established or maintained when a source demands a route to transmit packets or when the routes are currently in use. Taking AODV routing protocol for example, it was designed specifically for operating in WANs. Mobile nodes that are not involved in any active route do not maintain any routing information and periodic routing table exchanges. Since AODV is an on-demand routing protocol, it is not necessary for a node to discover and maintain a route to any other node in the network until a source node demands a communication with another destination node. AODV also makes use of the destination sequence numbers from the DSDV protocol to ensure that the most recent routing information is chosen between nodes. Every node in AODV maintains a sequence number which increases monotonically when it sends a new message. The greater the sequence number a route has, the fresher the route is. Thus, if there are two or more routes to a destination, the node always selects one with the greatest sequence number. In addition, CBRP is a cluster based routing algorithm like CGSR except that it is an on-demand routing mechanism as opposed to CGSR that is table-driven. The concept of the cluster will be discussed in detail in the next paragraph. In short, in table-driven protocols, each node maintain up-to-date routing information to all the nodes in the network whereas in on-demand protocols a node finds the route to a destination when it desires to send packets to the destination.

Compared to table-driven and on-demand routing protocols, a hybrid routing protocol combines features of both these two protocols such as: the Zone Routing Protocol (ZRP) [8]. In ZRP, each node dynamically maintains a zone centered at itself. A zone is a collection of neighbors and links within a predefined number of hops

called the zone radius. The construction of a zone requires a node to discover its neighbors. ZRP uses a separate Neighbor Discovery Protocol (NDP) for this purpose. In NDP, nodes typically broadcast periodic hello messages.

Because the cluster-based structure in WANs is used in the dissertation, it will be discussed in detail. Cluster-based is a kind of control structure or routing mechanism in WANs. For example, in CGSR, it organizes a network into clusters and elects a clusterhead in each cluster by running an efficient clustering algorithm. Other nodes in each cluster are one hop away from the clusterhead. Nodes that belong to more than one cluster are gateways. With cluster-based control, the physical network is transformed into a virtual network of interconnected node cluster. Each cluster has one or more controllers acting on its behalf to make control decisions for cluster members and to represent the cluster to communicate with other clusters. There are three types of controlling architectures: link-clustered, near-term digital radio (NTDR), and hierarchy [36].

In link-clustered architecture, each cluster contains a clusterhead, one or more gateways, and zero or more ordinary nodes that are neither clusterheads nor gateways. With the link-clustered architecture, all cluster members are within one hop of the clusterhead and hence within two hops of each other. This arrangement provides low-delay paths between cluster members that may communicate frequently, and it places clusterheads in the idea locations to coordinate transmissions among their cluster members.

In NTDR control architecture [40][41][53][54], it is an army data communication network component, with applications currently targeted at IP backbone responsibilities in the Tactical Internet. It produces a set of clusters, each containing a clusterhead, which when linked together form a routing backbone. The NTDR uses a contention-based, channel access protocol that utilizes a sender-receiver handshake. And, the NTDR used clustering and link state routing, and self-organized into a two-tier hierarchical ad-hoc network: intra-cluster and inter-cluster. The two-tier hierarchical ad-hoc network is used to increase capacity and reduce multiple access interference and relay delays. In NTDR, the clusterheads are themselves fully mobile. Cluster members automatically re-affiliate when moving out of range of one cluster and into another. The NTDR architecture restricts direct inter-cluster communication to clusterheads only; hence, the clusterheads function as the gateway. Inter-cluster

communication is restricted to provide secure communication among the clusterheads. Furthermore, a cluster cannot be treated as an arbitrary multihop network; neighboring nodes within one hop of each other can communicate directly, but all other intra-cluster communication must traverse the clusterhead. An NTDR node elects itself as clusterheads if it does not detect any other clusterheads in its vicinity or if it detects that it can heal a network partition. In addition, intra-cluster communication is used to provide secure communication for one cluster. Any pair nodes must complete their communication via clusterheads. Figure 4 illustrates the architecture of NTDR. There are three clusters: A, B, and C in the network. A host a in cluster A who wants to communicate with host b. Then, the messages sent from host a will be delivered to host b through the routing path $A.a \rightarrow A.CH \rightarrow B.CH \rightarrow B.b$.

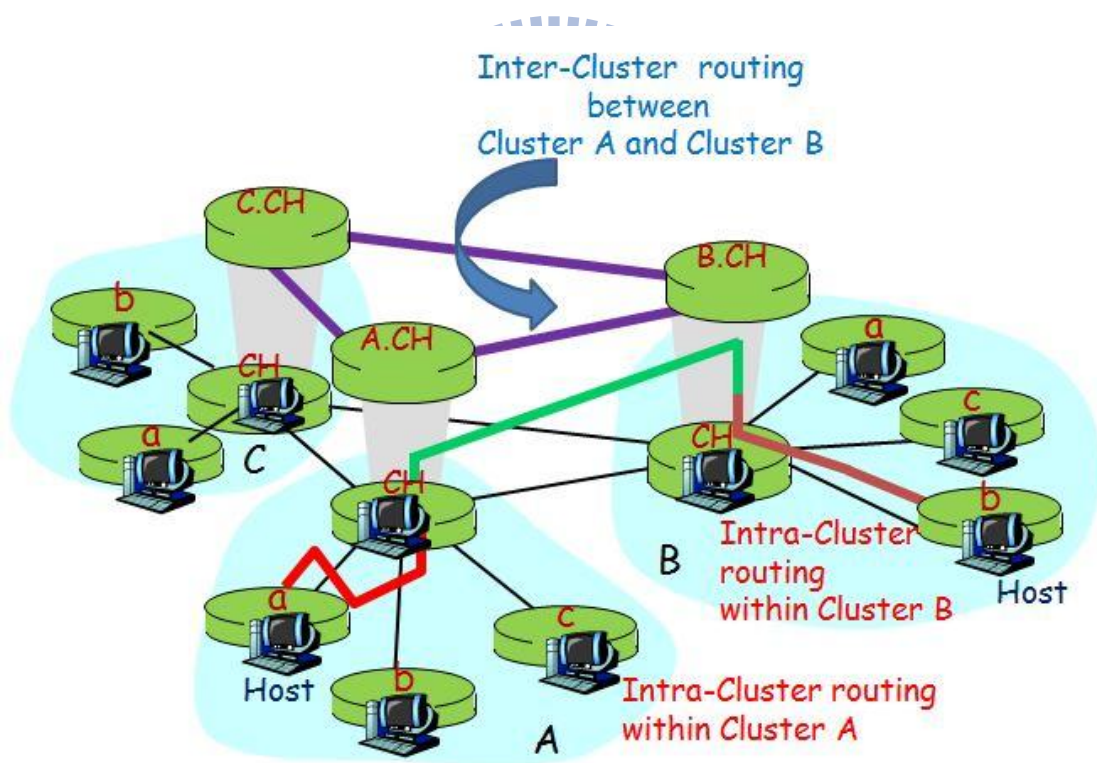


Figure 4. The architecture of Near Term Digital Radio (NTDR)

In hierarchical cluster-based control architecture, a network consisting of N nodes is organized into an m -level hierarchy of nested clusters of nodes such that all level- i clusters are disjoint for $0 \leq i \leq m$. In addition, a clusterhead selection can be

done by some criterion, e.g. lowest ID in the cluster.

2.2 Security Issues in WANs

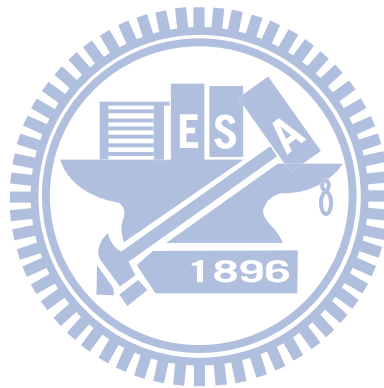
The primary object of this dissertation is to propose protocols which provide secure communications for users over WANs. Hence, this section describes some security issues. Due to dynamic nature and lack of centralized monitoring points, nodes in WANs are vulnerable to various kinds of attacks. There are several reasons that make security issues in WANs are different and more challenging than wired networks. First, owing to the broadcasting nature of WANs, the nodes use the wireless medium to communicate with each other. Any node within the radio range of another node can always listen to what is being broadcasted; thus it is easy for an adversary to eavesdrop, modify, or inject false packets as the medium is open and the attacker does not have to physically tap into network wires to gain access. Moreover, in WANs, there is no clear line of defense to prevent illegitimate access to the network. In addition, nodes in WANs also act as routers and are required to forward packets sent from their neighbors in a multi-hop manner. Thus a selfish or malicious node can choose to drop and not forward packet in order to save its energy or disrupt the network operation. It is also easy for any malicious node to broadcast false information and disturb the operation of the network. Another property of WANs posing challenging threats to its security is its constantly changing topology. The nodes in WANs are expected to join on the fly as they move in and out of the network. Therefore, key management is an important issue when users issue a join or leave request.

In addition, authentication, availability, confidentiality, integrity, authorization, and non-repudiation are also security needs in WANs. ITU-T Recommendation X.800 [46], Security Architecture for OSI, defines some security services to ensure adequate security of the systems or of data transfers and a availability service to ensure a system's availability. X.800 divides these services into five categories: Authentication, access control, data confidentiality, data integrity, and non-repudiation. X.800 also defines some security mechanisms associated with these security services. They are: Encipherment, digital signature, access control, data integrity, authentication exchange, traffic padding, routing control, and notarization. The definition of these security services [27] is described as follows:

- (1) **Authentication:** Authentication is a service related to identification. In other words, authentication is any process by which you verify that someone is who they claim they are. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc. For these reasons this aspect of cryptography is subdivided into two classes: entity authentication and data origin authentication. In entity authentication, it is required to make sure that the network is not deceived by malicious nodes, which provide false information or intercept data from genuine users.
- (2) **Availability:** Availability is a service which refers to the availability of information resources. An information system or network system that is not available when you need it. In WANs, data packets from source node are relayed over a sequence of intermediate nodes to destination node. All nodes in WANs are required to relay packets on behalf of other nodes. However, a node may misbehave by agreeing to forward packets and failing to do so, because it is overloaded, selfish, or malicious. A selfish node is unwilling to spend battery life or available network bandwidth to forward packets. A malicious node redirects the packets into another routing path or launches denial-of-service (DoS) attacks. These misbehaving nodes severely degrade the network performance and cause the network could not provide service to users. Consequently, misbehaving nodes are a significant security problem in WANs.
- (3) **Data confidentiality:** Confidentiality is a service used to keep the content of information from all but those authorized to have it. This service is important to make sure that information about the network is not exposed to malicious nodes.
- (4) **Data integrity:** Integrity is a service which addresses the unauthorized alternation of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. In WANs, integrity assures that data packets will not be modified or altered by an adversary.
- (5) **Authorization:** Authorization is a service which specifies access rights to resources, which is related to information security and computer security in general and to access control in particular. Hence, authorization is the act of checking to see if a user has the proper permission to access a particular file or

perform a particular action. In WANs, Rules and regulations define restriction of responsibilities of network and individual nodes. In addition,

- (6) Non-repudiation: Non-repudiation is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. In WANs, Non-repudiation prevents a node from denying that it has sent a message after it does so.



Chapter 3 A Group-Oriented Nominative Proxy Signature Scheme for Digital Rights Management

The increasing availability of information technology and computer networks has made the process of trading digital content through Internet very convenient. However, digital contents are easy to be copied and redistributed in ways that violate the intended use of the product. Digital Rights Management (DRM) is a system used to protect digital assets and control the distribution and usage of those digital assets. DRM systems separate protected content and digital license. A digital license controls the contents to be accessed by consumers. A consumer could download digital license after paying his/her money. DRM systems provide confidentiality, integrity and authenticity protection for digital contents.

Nowadays, mobile commerce is getting more important as the mobile networks and services expand widely. While mobility presents some special requirements and limitations, it also creates new possibility for DRM. A DRM system must be adapted into a new one, Mobile DRM (M-DRM). One of the major issues raised by M-DRM systems concerns the integrity of this license. In this dissertation, a group-oriented nominative proxy signature scheme (GO-NPSS) is proposed. The scheme supports a content provider to delegate his/her signing ability to the partial members of a group of clearinghouses having n members and to designate the partial members of a group of consumers, purchasing the same products, having l members to verify their digital licenses. In the proposed scheme, (t, n) proxy signers sign the specific digital license on behalf of the content provider and (w, l) verifiers verify the proxy signature. The proposed scheme can guarantee that the digital products come from the authorized providers. A formal security analysis demonstrates that our scheme is secure enough to be used in DRM systems.

3.1 Digital Right Management Introduction

Digital Rights Management (DRM) systems are the technologies to distribute digital contents in a secure manner that can protect and manage the rights for all participants. DRM provide a solution to the problem of illegal content distribution on the Internet. A DRM system should offer a persistent content protect against

unauthorized access to the digital content, and limiting access to only those with the proper authorization. The core concept in DRM is the use of digital licenses. Through digital licensing, content providers can gain much more control over what the consumer can do with the content. Figure 5 illustrates the concept of operation mode in DRM system. The basic DRM process involves four parties [21], as shown in Figure 6: the content provider, the distributor, the clearinghouse, and the consumer. These terms are described in detail as follows:

- Content Provider: A content provider may be an organization, a company, or a person in C2C business model who offers digital content to consumers protected with their own DRM tools. Protected content is bound to a set of rights, a notion that is described in a license.
- Distributor: A distributor provides distribution channels. The distributor receives the digital content from the content provider and creates a web catalogue presenting the contents and rights metadata.
- Clearinghouse: A clearinghouse handles the financial transaction for issuing the digital license to the consumer and pays royalty fees to the content provider and distribution fees to the distributor accordingly. The clearinghouse is also responsible for logging license consumptions for every consumer.
- Consumer: A consumer uses the system to consume the digital content by retrieving downloadable or streaming content through the distribution channel and then paying for the digital license.

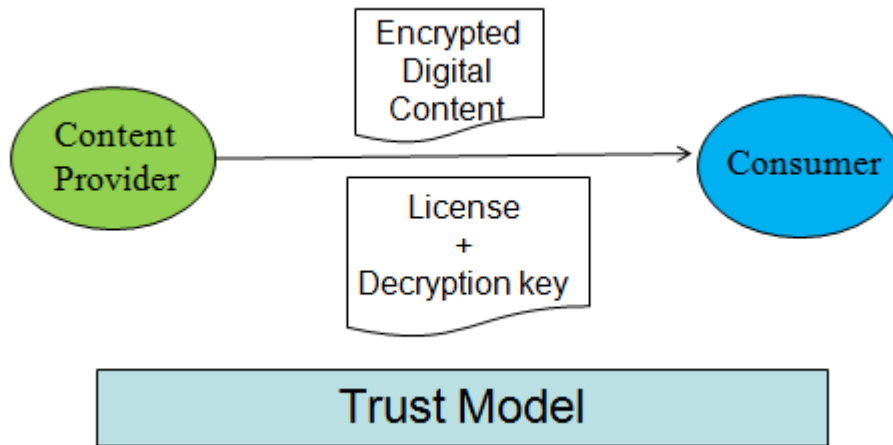


Figure 5. The concept of operation mode in DRM system

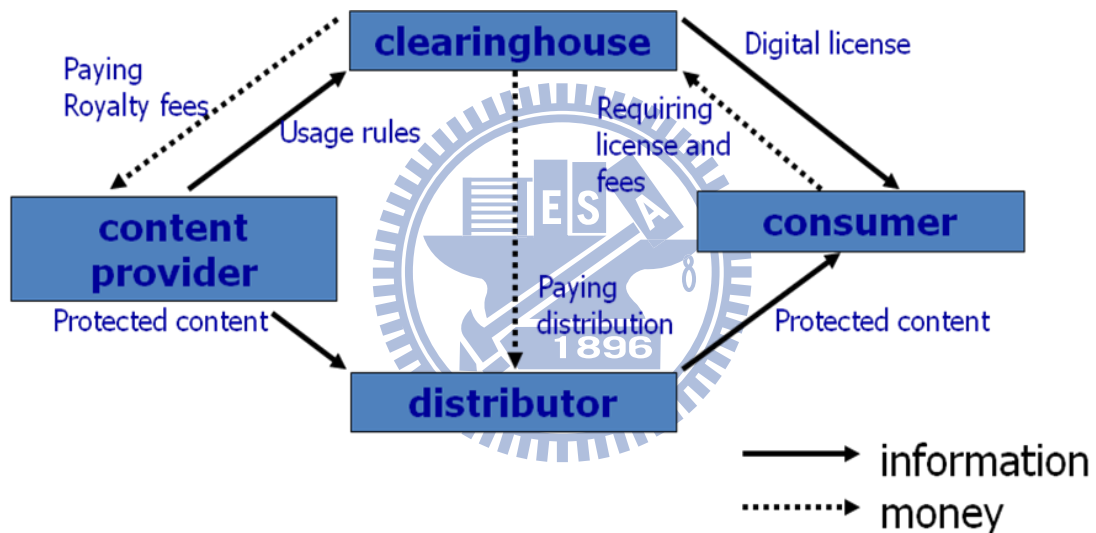


Figure 6. The components in DRM system [21]

A DRM system requires persist content protection, meaning that protection has to stay with the content. Essential security requirements in DRM systems include data protection which protects against unauthorized interception and modification, identification of recipients which protects unauthorized access and enables access control for the digital content, and tamper-resistant mechanism which manages protected data and enforces content usage rights.

Most DRM systems adopt a license-based mechanism which separates the keys from encrypted content [10]. The encrypted content is delivered to a consumer from the distributor while the license including the keys is transported to the DRM client

from a license server [10]. For example, the DRM system provided by Microsoft, as shown in Figure 7, is a license-based system [28]. There are three components in the system, they are: the content provider, the license server, and the consumer. The protected content is encrypted by an encryption key. This key is generated by the seed and key ID and is a part of signed license. A consumer downloads the protected content from the service provider. Then, the DRM management platform in end-user site checks the status of digital license associated with this content. The consumer has to get the valid digital license from the license server before using the digital content.

In addition, OMA, Open Mobile Alliance, has released two versions in DRM [32]. They are OMA DRM 1.0, approved in 2004, and OMA 2.0, approved in 2006. In OMA DRM 1.0, it specifies three main methods: Forward Lock, Combined Delivery, and Separate Delivery. In Forward Lock mode, the content is packaged and sent to the mobile terminal as a DRM message. The mobile terminal could use the content, but could not forward it to other devices or modify it. However, the Forward Lock content is not encrypted when it is received or when stored in phone memory. In Combined Delivery mode, the digital rights are packaged with a content object in the DRM message. The user could use the content as defined in the rights object, but could not forward or modify it. The rights object is written in DRMREL (DRM Rights Expression Language) and defines the number of times and length of time that the content can be used thus enabling the preview feature. In the Forward-lock mode and the Combined Delivery mode, the content is not encrypted. In the Separate Delivery mode, the content and rights are packaged and delivered separately. The content is encrypted into DRM Content Format (DCF) using a symmetric cryptograph method. In the Separate Delivery mode, the symmetric encryption key is not encrypted. The OMA DRM 2.0 standard is an extension of version 1.0. The OMA DRM 2.0 is composed of four parts: Public Key Infrastructure (PKI), Rights Object Acquisition Protocol (ROAP), DRM Content Format (DCF), and Rights Expression Language (REL). DRM 2.0 looks like the Separate Delivery in DRM 1.0 but the Rights Object (RO) is signed and passed with the PKI mechanism to assure security, authenticity and integrity. The DRM Agent is the entity in the device that manages permissions for media objects on the device. With the mobile DRM Agent, devices not connected to a network could use the DRM content.

A digital signature scheme further protects the usage rules from tampering,

especially in mobile networks. Digital signatures provide data integrity, non-repudiation, and authentication. Therefore, digital signature is an important security mechanism for license-based DRM systems.

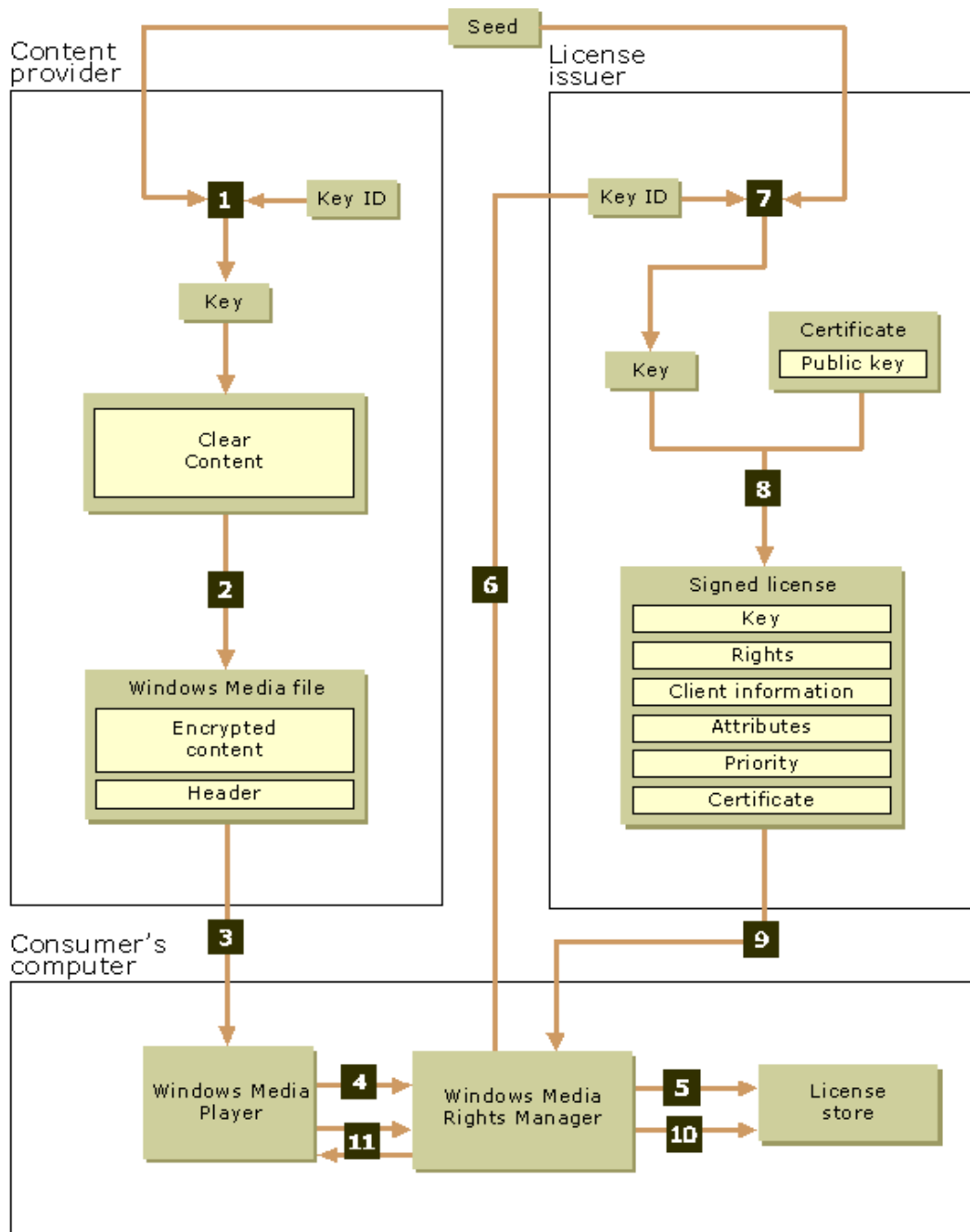


Figure 7. The overall DRM framework provided by Microsoft Corporation [28]

In mobile networks where the nodes constantly move and in some specific networks, like WANs or sensor networks, the network topology changes continuously;

thus, a normal signature scheme is not suitable for DRM systems. Instead, an original-nominative proxy signature scheme is suitable for this situation. An original-nominative proxy signature is a scheme that the original signer can delegate his/her signing power to a proxy signer who generates a proxy signature on behalf of the original signer and can designate the verifier to verify the proxy signature. In this scheme, only the nominee, the verifier, can verify the signature and if necessary, only the nominee can prove its validity to the third party [52].

In this dissertation, a group-oriented nominative proxy signature scheme (GO-NPSS) is proposed. The scheme supports a content provider, named original signer hereafter, to delegate his/her signing ability to the partial members of the distributors, named proxy group hereafter, having n members and to designate the partial members of the consumers, named verifier group hereafter, having l members to verify the validity of his/her digital licenses for the mobile users. Therefore, (t, n) proxy signers sign the specific license on behalf of the original signer and (w, l) verifiers verify the proxy signature. Most important of all, our scheme can prevent the original signer from repudiating the validity of the digital license which had delivered previously to the clients. In addition, the proposed scheme complies with all security requirements in digital signature, proxy signature and original-nominative proxy signature schemes.

The remainder of this chapter is organized as follows: In section 3.2, related works are discussed. The proposed scheme is detailed in section 3.3. In section 3.4, security analysis is given. In section 3.5, performance analysis is discussed. In the last section, conclusion is presented.

3.2 Related Works

In this section, the concepts of the proxy signature scheme and the nominative proxy signature scheme are introduced.

3.2.1 Proxy Signature Scheme

Proxy signatures originated from the concept of digital signature and have found numerous practical applications, particularly in distributed computing [7][14][18], such as: Strong proxy signature scheme [18] and one-time proxy signature scheme [14], etc. A digital signature is used to establish both of the signer authenticity and the data integrity assurance. Therefore, a digital signature has some good properties:

Integrity, authenticity, verifiability, unforgeability, and non-repudiability, etc. Proxy signature not only inherits these properties but also some useful properties. It is useful when the original signer is not available to a specific document. In 1996, Mambo et al. [25] first introduced the concept of a proxy signature scheme, which permits an entity to delegate its signing rights to one or more entities, called proxy signer(s), to sign messages on its behalf, in case of temporal absence, lack of time or computational power, etc. A delegated proxy signer can generate a verifiable proxy signature that can be verified by anyone. And a verifier can verify the proxy signature and the original signer's delegation by using a proxy verification algorithm and the public key information of both original signer and proxy signer. Furthermore, many extensions of the basic proxy signature primitive have been considered. These include threshold proxy signatures [48][49][57], nominative proxy signatures [34] and multi-proxy signature scheme [9], etc.

There are three kinds of proxy signatures: full delegation, partial delegation, and delegation by warrant. These terms are described in detail as follows:

- Full delegation: Full delegation is a kind of proxy unprotected proxy signature. In the full delegation, a proxy signer is given the same private key as the original signer has, and computes the same signatures as the original signer does. Therefore, the original signer should take all the responsibility for messages signed by the proxy signer.
- Partial delegation: partial delegation is further classified into two parts: proxy-unprotected and proxy-protected according to protection of proxy signer. In the proxy-unprotected partial delegation, the original signer uses his/her private key and a random key to create a proxy signature key and sends it to the proxy signer. The proxy signer uses the proxy signature key to compute proxy signatures on behalf of the original signer. In the proxy-protected partial delegation, the proxy signer generates the proxy signature using the delegation key generated by the original signer and its private key.
- Delegation by warrant: Delegation by warrant is a kind of proxy protected proxy signature. In the delegation by warrant, the original signer restricts the proxy signer's signing ability by warrant which records the identities of the original signer and the proxy, the type of message delegated and the delegation

period, etc. The warrant is sent to the proxy signer in conjunction with his/her own signing key to produce proxy signatures. A proxy signature contains the warrant and the proxy signer's signature.

3.2.2 Nominative Proxy Signature Scheme

In 1995, Kim et al. [15][16] first proposed the nominative signature scheme, and then in 2001 Park et al. [34] introduced a new type of proxy signature, nominative proxy signature. A nominative proxy signature scheme is an important delegation signature scheme in a mobile communication environment. By definition, unlike a normal proxy signature scheme, only the nominee can directly verify the proxy signature and if necessary, only the nominee can prove to the third party that proxy signature issued to him/her is valid. There are two kinds of nominative proxy signature schemes: an original-nominative proxy signature, i.e. the original signer is the nominator, and a proxy-nominative signature scheme, i.e. the proxy signer is the nominator. An original-nominative proxy signature scheme is used to avoid the misuse of proxy signatures. In these kinds of schemes, an original signer delegates a user as a proxy signer and designates a user as a verifier. This verifier can verify the validity of a proxy signature. A proxy-nominative proxy signature scheme is used in E-Commerce. In addition, both original-nominative proxy signature scheme and proxy-nominative proxy signature scheme must satisfy some requirements [51]. In the former scheme, it must satisfy the following requirements:

- The same properties as a digital signature.
- Only the original signer can nominate the receiver.
- The original signer and the proxy signer cannot repudiate the nominative proxy signature after the signature is generated.
- Only the nominee can directly verify the nominative proxy signature.
- If necessary, only the nominee can prove to the third party that the nominative proxy signature is valid.

In the latter scheme, it satisfies the same requirements as the former scheme except the second requirement. Instead of this requirement, it is rewritten as “Only the proxy signer can nominate the receiver.”

3.3 The Proposed Group-Oriented Nominative Proxy Signature Scheme

In this dissertation, a group-oriented nominative proxy signature scheme (GO-NPSS) is proposed to provide a way to generate and verify the signature of the digital license in the DRM system. In mobile commerce, like WANs, there is restriction to the availability of each mobile host due to the power consumption, the computation capability, and link breakage problems. Hence, the running programs may easily be suspended or stopped. For example, if the same problem happens during a digital signature generation phase, then the signer could not accomplish this work. And, the verifier could not verify the signature. Therefore, a feasible solution for solving such problems is proposed. When providing signed digital license to the consumers in the area of C2C business model, the content provider could ask someone or a group of users for help to accomplish his/her work.

In the proposed GO-NPSS scheme, an original signer delegates his/her signing ability to the partial members of the proxy group having n members and to designates the partial members of the verifier group having l members to verify his/her digital licenses signed by a group of proxy signers. Therefore, (t, n) proxy signers sign the specific license on behalf of the original signer and (w, l) verifiers verify the validity of this proxy signature. In the proposed dissertation, even though the original signer may lose its connectivity to the network, the digital signature for a specific license could be generated and verified successfully by a group of users.

3.3.1 Notations

- p : a large prime.
- q : a large prime and a factor of $p-1$.
- g : a generator in $GF(p)$ with order q , such that $g^q \equiv 1 \pmod{p}$.
- CP : Content provider, the role of original signer.
- CHG : A group of clearinghouses, the role of proxy signers.
- CVG : A group of consumers, the role of signature verifiers.
- x_i : i 's private key.

- y_i : i 's public key, such that $y_i \equiv g^x \pmod{p}$.
- PV_{CHG} : CHG 's private key.
- PPV_{CHG_i} : Partial proxy group private key generated by CHG_i .
- y_{CHG} : CHG 's public key, such that $y_{CHG} \equiv g^{PV_{CHG}} \pmod{P}$.
- PV_{CVG} : CVG 's private key.
- PPV_{CVG_j} : Partial verifier group private key generated by CVG_j .
- y_{CVG} : CVG 's public key, such that $y_{CVG} \equiv g^{PV_{CVG}} \pmod{P}$.
- M_w : A warrant which records the identities of CP , CHG , and CVG , license, t , n , w , l , and expiration time.
- T : Time stamp against replay attack.
- k_1, k_2 : Shared by CHG members.

3.3.2 The Proposed Scheme

The proposed GO-NPSS scheme is a combination of threshold-based secret sharing and original-nominative proxy signature. By secret sharing scheme, secret can be shared and reconstructed easily. By original-nominative proxy signature scheme, the signed license could be done by a group of proxy signers and a group of verifiers. In addition, the proposed original-nominative proxy signature is a kind of delegation by warrant and proxy protected signature scheme. Furthermore, the security of the proposed scheme is based on both factorization problem (FP) and discrete logarithm problem (DLP). Detailed security analysis is shown in section 3.4.

The proposed scheme has five phases: the initialization phase, the delegation phase, the proxy key generation phase, the nominative proxy signature generation phase, and the original-nominative proxy signature verification phase. Figure 8 illustrates the GO-NPSS scheme.

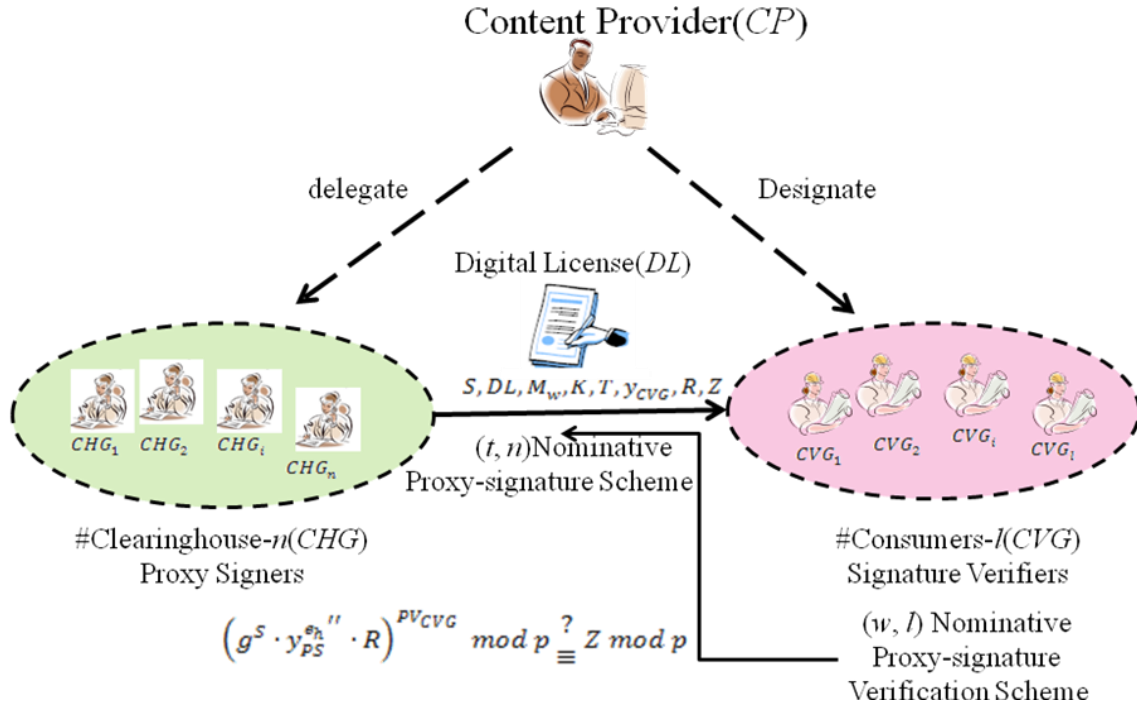


Figure 8. The GO-NPSS scheme

3.3.2.1 Initialization Phase

Before describing the proposed GO-NPSS scheme in detail, this dissertation will exhibit a user's public and private key pair generation. Before joining a cluster, all participants have contact to an offline certificate authority (CA). The CA assigns a key pair (x_i, y_i) to each joining user. These key pairs facilitate users claiming that they are the legal users. They can further get other related keys and use the related services described in the following chapters.

In the initialization phase, members in *CHG* generate their secret share, s_{CHG_i} , by themselves, and members in *CVG* also generate their secret share, s_{CVG_i} , by themselves. In the future, the group private key, PV_{CHG} , of *CHG* group will be reconstructed by a sufficient number of shares, s_{CHG_i} , are combined together; the same, the group private key, PV_{CVG} , of *CVG* group will be reconstructed by a sufficient number of shares, s_{CVG_i} , are combined together. In the proposed scheme, each member fairly contributes their partial information to construct the group private keys.

Initially, *CP* chooses both *CHG* and *CVG*'s members. This dissertation denotes a group of member set in *CHG* by $\{CHG_1, CHG_2, \dots, CHG_i\}$ and a group

member set in CVG by $\{CVG_1, CVG_2, \dots, CVG_n\}$. User authentication could be done by Wireless Public Key Infrastructure (WPKI). WPKI provides a secure and trusted trading environment. Each member issues his digital certificate to authenticate himself.

CP publishes the parameters: p , q , and g to his/her members. Then, the group private keys generation and secret sharing procedures in CHG and CVG are described as follows.

(1) Group private key share generation for CHG group:

Figure 9 illustrates the flow chart of the group private key generation and the key sharing in CHG .

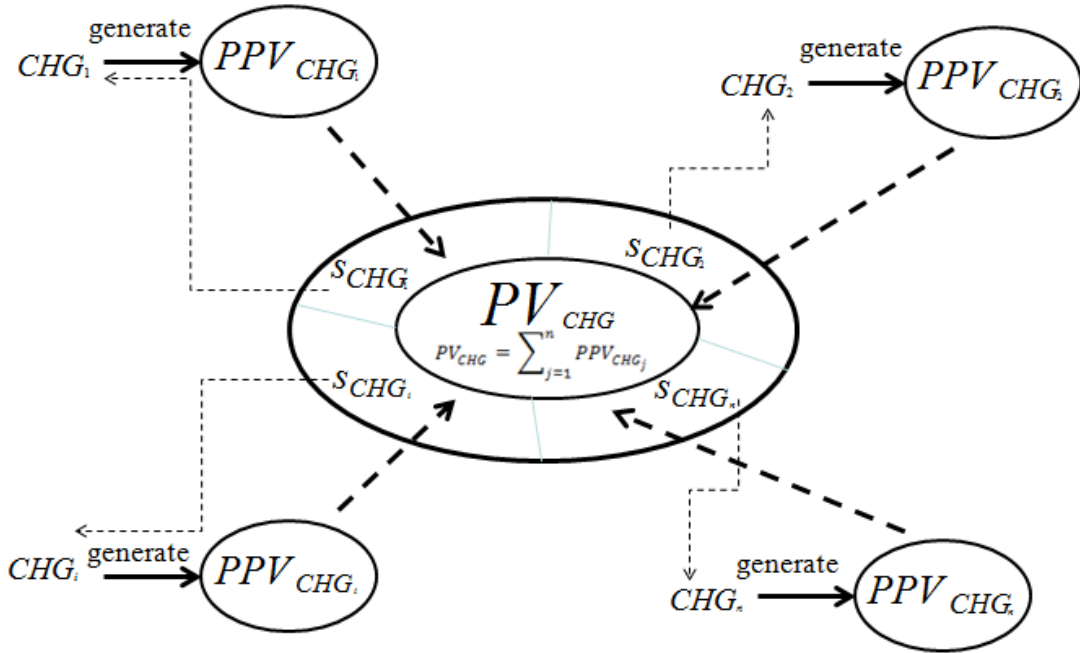


Figure 9. The flow chart of the group private key generation and key sharing in CHG

Group private key share, s_{CHG_i} , generation consists of the following five steps:

- Step 1: Partial group private key generation

In this step, each $CHG_i \in CHG$ chooses $a_{CHG_i}, PPV_{CHG_i} \in_R Z_q^*$ at random and computes. Then, CHG_i computes the following formulas, as shown in Eqs. (3.1), (3.2), and (3.3), and signs the parameters, PPV_{CHG_i} , r_{CHG_i} , and c_{CHG_i} , by

$sign(h(PPV_{CHG_i}, r_{CHG_i}, c_{CHG_i})).$

$$r_{CHG_i} \equiv g^{a_{CHG_i}} \pmod{p} \quad (3.1)$$

$$PPV_{CHG_i} \equiv x_{CHG_i} \cdot r_{CHG_i} + a_{CHG_i} \cdot c_{CHG_i} \pmod{q} \quad (3.2)$$

$$y'_{CHG_i} \equiv g^{PPV_{CHG_i}} \equiv y_{CHG_i}^{r_{CHG_i}} \cdot r_{CHG_i}^{c_{CHG_i}} \pmod{p} \quad (3.3)$$

In Eq. (3.2), partial group private key PPV_{CHG_i} is generated. Each member in CHG contributes its PPV_{CHG_i} to construct the group private key PV_{CHG} . PPV_{CHG_i} is not broadcasted directly to the CHG group. Instead, y'_{CHG_i} , which is computed in Eq. (3.3), is broadcasted directly to the proxy group. In addition, based on the difficulty of the DLP problem, anyone can not compute PPV_{CHG_i} except CHG_i itself.

- Step 2: Threshold-based secret share generation

In this step, the concept of threshold-based secret sharing scheme is used. This scheme helps each CHG_i shares its own secret PPV_{CHG_i} to the members in CHG . First, CHG_i generates a polynomial $f_i(\beta)$ of degree $t-1$, as shown in Eq. (3.4). Then, each member CHG_j obtains one share $f_i(j)$ from CHG_i , as shown in Eq. (3.5). CHG_i 's secret can be reconstructed with at least t shares using Lagrange's interpolation formula.

$$f_i(\beta) = PPV_{CHG_i} + e_{i,1} \cdot \beta + e_{i,2} \cdot \beta^2 + \dots + e_{i,t-1} \cdot \beta^{t-1} \pmod{q} \quad (3.4)$$

$$f_i(j), \quad \forall j = 1, \dots, n; j \neq i \quad (3.5)$$

- Step 3: Share delivery

In this step, CHG_i sends $f_i(j)$ to CHG_j in a secure way, and broadcasts $g^{PPV_{CHG_i}}, g^{e_{i,1}}, \dots, g^{e_{i,t-1}}$.

- Step 4: Share verification

In this step, CHG_i verifies the validity of the shares $f_j(i)$, $\forall j = 1, \dots, n$, which are from CHG_j . The verification procedure is described in Eq. (3.6).

$$g^{f_j(i)} \equiv g^{PPV_{CHG_j}} \cdot (g^{e_{j,1}})^j \cdot (g^{e_{j,2}})^{j^2} \dots (g^{e_{j,t-1}})^{j^{t-1}} \pmod{p} \equiv g^{PPV_{CHG_j}} \cdot A_{j,1}^i \cdot A_{j,2}^{i^2} \dots A_{j,t-1}^{i^{t-1}} \quad (3.6)$$

; where $A_{j,k} = g^{e_{j,k}}$, $\forall k = 1, \dots, t-1$.

- Step5: Group private key's secret share generation

In this step, CHG_i verifies all shares from the proxy group members. If all $f_j(i)$ are verified to be legal, CHG_i computes $s_{CHG_i} = \sum_{j=1}^n f_j(i) \bmod q$ as its share.

In addition, without loss of generality, let

$$f(\beta) = PV_{CHG} + e_1 \cdot \beta + e_2 \cdot \beta^2 + \dots + e_{t-1} \cdot \beta^{t-1} \bmod q = \sum_{j=1}^n f_j(\beta) \bmod q \quad (3.7)$$

; where $PV_{CHG} = \sum_{j=1}^n PPV_{CHG_j}$

And, let

$$s_{CHG_i} = f(i) = \sum_{j=1}^n f_j(i) \bmod q \quad (3.8)$$

In Eq. (3.7), $f(\beta)$ is a polynomial of degree $t-1$ which is a general form for generating PV_{CHG} 's shares. For example, CHG_i 's share s_{CHG_i} is $f(i)$ and is also equal to $\sum_{j=1}^n f_j(i) \bmod q$.

Furthermore, CHG 's public key, y_{CHG} , is computed as follows:

$$y_{CHG} \equiv g^{PV_{CHG}} \bmod p \quad (3.9)$$

In Eq. (3.9), based on the difficulty of DLP problem, no one can get PV_{CHG} even if he/she has y_{CHG} and g . Only any at least t proxy group members in CHG can compute and reconstruct the value of PV_{CHG} , but no group of $t-1$ members can do so.

(2) Group private key share generation for CVG group:

Figure 10 illustrates the flow chart of the group private key generation and the key sharing in CVG .

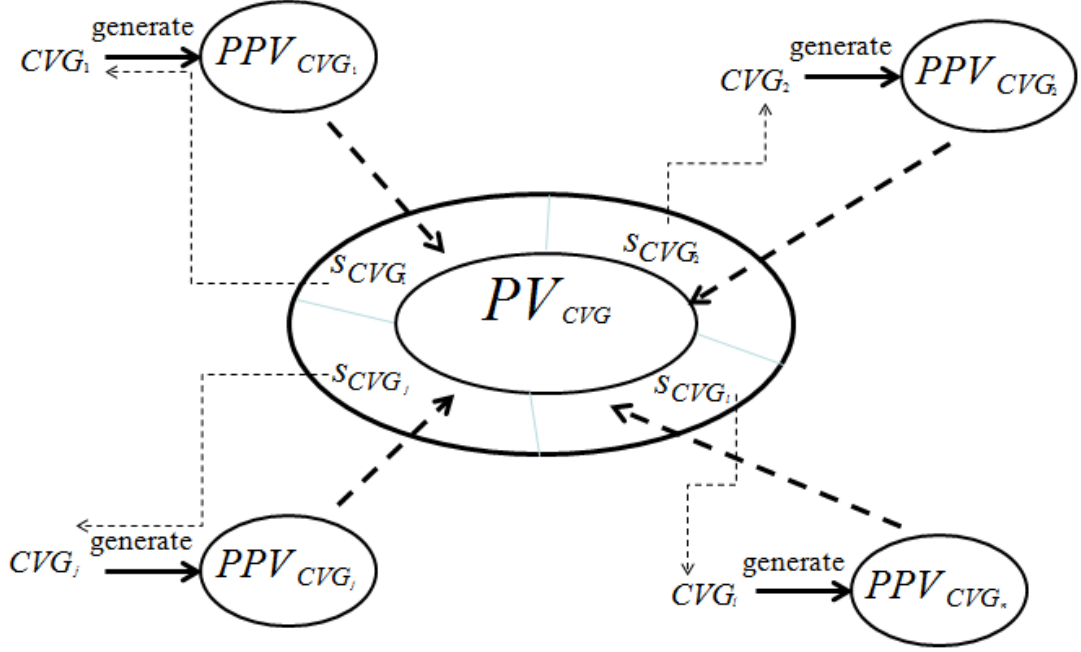


Figure 10. The flow chart of the group private key generation and key sharing in CVG

Group private key share, s_{CVG_j} , generation consists of the following five steps:

- Step 1: Partial group private key generation

In this step, each $CVG_j \in CVG$ chooses $a_{CVG_j}, PPV_{CVG_j} \in_R Z_q^*$ at random and computes. Then, CVG_j computes the following formulas, as shown in Eqs. (3.10), (3.11), and (3.12), and signs the parameters, PPV_{CVG_j} , r'_{CVG_j} , and c'_{CVG_j} , by $sign(h(PPV_{CVG_j}, r'_{CVG_j}, c'_{CVG_j}))$.

$$r'_{CVG_j} \equiv g^{a_{CVG_j}} \text{ mod } p \quad (3.10)$$

$$PPV_{CVG_j} \equiv x_{CVG_j} \cdot r'_{CVG_j} + a_{CVG_j} \cdot c'_{CVG_j} \text{ mod } q \quad (3.11)$$

$$y'_{CVG_j} \equiv g^{PPV_{CVG_j}} \equiv y_{CVG_j}^{r'_{CVG_j}} \cdot r'_{CVG_j}^{c'_{CVG_j}} \text{ mod } p \quad (3.12)$$

In Eq. (3.11), partial group private key PPV_{CVG_j} is generated. Each member in CVG contributes its PPV_{CVG_j} to construct the group private key PV_{CVG} . PPV_{CVG_j} is not broadcasted directly to the CVG group. Instead, y'_{CVG_j} , which is computed in Eq. (3.12), is broadcasted directly to the proxy group. In addition, based on the difficulty of the DLP problem, anyone can not compute PPV_{CVG_j} except CVG_j itself.

- Step 2: Threshold-based secret share generation

In this step, the concept of threshold-based secret sharing scheme is used. This scheme helps each CVG_j shares its own secret PPV_{CVG_j} to the members in CVG . First, CVG_j generates a polynomial $\omega_j(\beta)$ of degree $w-1$, as shown in Eq. (3.13). Then, each member CHG_j obtains one share $\omega_j(i)$ from CVG_j in Eq. (3.14). CVG_j 's secret can be reconstructed with at least w shares using Lagrange's interpolation formula.

$$\omega_j(\beta) = PPV_{CVG_j} + e_{j,1} \cdot \beta + e_{j,2} \cdot \beta^2 + \dots + e_{j,w-1} \cdot \beta^{w-1} \text{ mod } q \quad (3.13)$$

$$\omega_j(i), \quad \forall i = 1, \dots, l; i \neq j \quad (3.14)$$

- Step 3: Share delivery

In this step, CVG_j sends $\omega_j(i)$ to CVG_i in a secure way, and broadcasts $g^{PPV_{CVG_j}}, g^{e_{j,1}}, \dots, g^{e_{j,w-1}}$.

- Step 4: Share verification

In this step, CVG_j verifies the validity of the shares $\omega_i(j)$, $\forall i = 1, \dots, l$, which are from CVG_i . The verification procedure is described in Eq. (3.15).

$$g^{\omega_i(j)} \equiv g^{PPV_{CVG_i}} \cdot (g^{e_{i,1}})^j \cdot (g^{e_{i,2}})^{j^2} \cdot \dots \cdot (g^{e_{i,w-1}})^{j^{w-1}} \text{ mod } p \equiv g^{PPV_{CVG_i}} \cdot B_{i,1}^j \cdot B_{i,2}^{j^2} \cdot \dots \cdot B_{i,w-1}^{j^{w-1}} \quad (3.15)$$

; where $B_{i,k} = g^{e_{i,k}}, \forall k = 1, \dots, w-1$.

- Step5: Group private key's secret share generation

In this step, CVG_j verifies all shares from the proxy group members. If all $\omega_i(j)$ are verified to be legal, CVG_j computes $s_{CVG_j} = \sum_{i=1}^l \omega_i(j) \text{ mod } q$ as its share.

In addition, without loss of generality, let

$$\omega(\beta) = PV_{CVG} + e_1 \cdot \beta + e_2 \cdot \beta^2 + \dots + e_{w-1} \cdot \beta^{w-1} \text{ mod } q = \sum_{i=1}^l \omega_i(\beta) \quad (3.16)$$

; where $PV_{CVG} = \sum_{i=1}^l PPV_{CVG_i}$

And, let

$$s_{CVG_j} = \omega(j) = \sum_{i=1}^l \omega_i(j) \text{ mod } q \quad (3.17)$$

In (3.16), $\omega(\beta)$ is a polynomial of degree $w-1$ which is a general form for

generating PV_{CVG} 's shares. For example, CVG_j 's share s_{CVG_j} is $\omega(j)$ and is also equal to $\sum_{i=1}^l \omega_i(j) \bmod q$.

Furthermore, CVG 's public key, y_{CVG_j} , is computed as follows:

$$y_{CVG} \equiv g^{PV_{CVG}} \bmod p \quad (3.18)$$

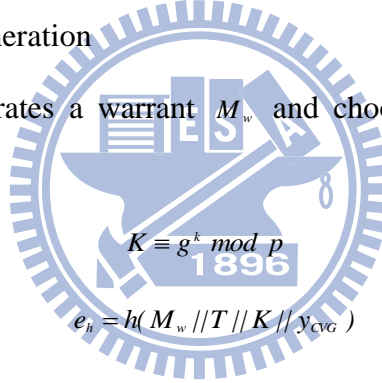
In Eq. (3.18), based on the difficulty of DLP problem, no one can get PV_{CVG} even if he/she has y_{CVG_j} and g . Only any at least w proxy group members in CVG can compute and reconstruct the value of PV_{CVG} , but no group of $w-1$ members can do so.

3.3.2.2 Delegation Phase

In the delegation phase, the original signer CP generates the proxy shares to the members in CHG . This phase consists of the following four steps:

- Step 1: Proxy key generation

In this step, CP generates a warrant M_w and chooses $k \in_R Z_q^*$ at random and computes:



$$K \equiv g^k \bmod p \quad (3.19)$$

$$e_h = h(M_w || T || K || y_{CVG}) \quad (3.20)$$

$$\sigma \equiv x_{CP} \cdot e_h + k \bmod q \quad (3.21)$$

The digital license information is recorded in M_w . This operation will not cause any security problem. This is because the encryption key used for protecting the digital contents is encrypted. Only the consumers in CVG could get the encryption key. In Eq. (3.21), σ is the proxy key and will be shared among the t members in CHG . Here, e_h is one of the parameters while CP computes the value of σ . Hence, the information of CP and CVG are in σ . In addition, both M_w and the time stamp T are also in σ . The threshold-based secret sharing scheme is used to generate its shares for proxy signers. In the future, any at least t proxy group members in CHG can compute and reconstruct the value of σ .

- Step 2: Threshold-based secret share generation

In this step, CP generates the secret shares, σ_{CHG_i} , from σ by using the

following polynomial, as shown in Eq. (3.22):

$$f'(\beta) = \sigma + d_1 \cdot \beta + d_2 \cdot \beta^2 + \dots + d_{t-1} \cdot \beta^{t-1} \text{ mod } q \quad (3.22)$$

$$\sigma_{CHG_i} \equiv f'(i); \forall i = 1, \dots, n \quad (3.23)$$

In Eq. (3.23), σ_{CHG_i} is CHG_i 's shares and is from CP . Only any at least t proxy group members can compute the value of σ , but no group of $t-1$ members can do so.

- Step 3: Proxy share delivery

In this step, CP sends σ_{CHG_i} to CHG_i in a secure way, and broadcasts $D_j \equiv g^{d_j} \text{ mod } p; \forall j = 1, \dots, n$ and $(M_w || T || K || y_{CVG})$.

- Step 4: Proxy share verification

In this step, CHG_i verifies the validity of the share σ_{CHG_i} by computing e_h^* , as shown in Eq. (3.24), and checking the equality in Eq. (3.25). CHG_i accepts this share only if the equality holds.

$$e_h^* = h(M_w || T || K || y_{CVG}) \quad (3.24)$$

$$g^{\sigma_{CHG_i}} \equiv y_{CP}^{e_h^*} \cdot K \cdot \prod_{j=1}^{t-1} D_j^{i^j} \text{ mod } p \quad (3.25)$$

The formula in Eq. (3.25) will be proved as follows:

Proof:

$$\because g^{\sigma_{CHG_i}} \text{ mod } p = g^{f'(i)} \text{ mod } p$$

$$\Rightarrow g^{\sigma_{CHG_i}} \text{ mod } p = (g^{\sigma + d_1 i + d_2 i^2 + \dots + d_{t-1} i^{t-1}}) \text{ mod } p$$

$$= (g^{\sigma_{CP} \cdot e_h^*} \cdot \prod_{j=1}^{t-1} D_j^{i^j}) \text{ mod } p$$

$$= (y_{CP}^{e_h^*} \cdot K \cdot \prod_{j=1}^{t-1} D_j^{i^j}) \text{ mod } p$$

Q.E.D

3.3.2.3 Proxy key Generation Phase

In this dissertation, the proposed GO-NPSS uses the concept of proxy-protected

delegation with warrant. Thus, CHG_i does not directly use the proxy key σ_{CHG_i} . Instead of this key, CHG_i generates a new proxy key, as shown in Eq. (3.26), by itself. This is because σ'_{CHG_i} carries CHG_i 's identity information; thus, CHG_i cannot deny his contribution about some specific proxy signature.

Without loss of generality, we assume that the members $\{CHG_1, CHG_2, \dots, CHG_t\}$ in CHG are the proxy signers. Each CHG_i computes its own proxy key σ'_{CHG_i} :

$$\sigma'_{CHG_i} \equiv \sigma_{CHG_i} + s_{CHG_i} \cdot e_h \text{ mod } q \quad (3.26)$$

In Eq. (3.26), the implication of CHG_i 's identity is in σ'_{CHG_i} . Therefore, in the future, CHG_i could not deny that he/she has signed the message on behalf of CP .

3.3.2.4 Nominative Proxy Signature Generation Phase

In the nominative proxy signature generation phase, members $\{CHG_1, CHG_2, \dots, CHG_t\}$ sign the digital license (DL) without revealing their proxy keys. The proxy key, σ'_{CHG_i} , will not be disclosed during the normative proxy signature generation phase. This is because this key is protected by ξ_{CHG_i} in the step 1, as shown in Eq. (3.27). This phase consists of the following three steps:

- Step 1: ξ_{CHG_i} generation

In this step, two parameters, k_1 and k_2 are shared among these t proxy signers. The secret sharing generation scheme for these two parameters is the same as group private key share generation of the initialization phase.

Each CHG_i computes the following equations, as shown in Eqs. (3.27) and (3.28):

$$\xi_{CHG_i} \equiv (k_2)_{CHG_i} - \sigma'_{CHG_i} \cdot e'_h \text{ mod } q \quad (3.27)$$

$$e'_h = h(DL || M_w || T || K || y_{cvG}) \quad (3.28)$$

Here, $(k_2)_{CHG_i}$ is CHG_i 's share from k_2 . And, e'_h is shown in Eq. (3.28).

- Step 2: ξ_{CHG_i} delivery and verification

Each CHG_i sends ξ_{CHG_i} to other proxy signers, $\{CHG_1, CHG_2, \dots, CHG_t\}$, in a secure way. Upon receiving ξ_{CHG_j} , CHG_i verifies the validity of each ξ_{CHG_j} ,

$\forall j = 1, \dots, t$, by checking the following equation, as shown in Eq. (3.29):

$$g^{\xi_{CHG_j}} \bmod p \stackrel{?}{=} (y_{(k_2)_{CHG_j}} \cdot \prod_{i=1}^{t-1} Q_i^{j^i}) \cdot [y_{CP}^{e_h} \cdot K \cdot \prod_{j=1}^{t-1} D_j^{i^j} \cdot (y_{CHG} \cdot \prod_{i=1}^{t-1} A_i^{j^i})^{e_h}]^{-e_h} \bmod p \quad (3.29)$$

In Eq. (3.29), the value of $y_{(k_2)_{CHG_j}}$ is gotten from $g^{(k_2)_{p_j}} \bmod p$, i.e. $y_{(k_2)_{CHG_j}} \equiv g^{(k_2)_{p_j}} \bmod p$. And, $Q_i \equiv g^{q_i} \bmod p; \forall i = 1, \dots, t-1$. In addition, the formula in Eq. (3.29) will be proved as follows:

Proof:

$$\begin{aligned} \because g^{\xi_{p_j}} \bmod p &= g^{(k_2)_{CHG_j} - \sigma'_{CHG_j} e_h} \bmod p \\ \Rightarrow g^{\xi_{p_j}} \bmod p &= (g^{(k_2)_{CHG_j} + q_1 \cdot j + q_2 \cdot j^2 + \dots + q_{t-1} \cdot j^{t-1}}) \cdot (g^{\sigma'_{CHG_j}})^{-e_h} \dots \bmod p \\ &= ((y_{(k_2)_{p_j}} \cdot \prod_{i=1}^{t-1} Q_i^{j^i}) \cdot (g^{\sigma'_{CHG_j} + \sigma'_{CHG_j} e_h})^{-e_h} \bmod p \\ &= (y_{(k_2)_{CHG_j}} \cdot \prod_{i=1}^{t-1} Q_i^{j^i}) \cdot [y_{CP}^{e_h} \cdot K \cdot \prod_{j=1}^{t-1} D_j^{i^j} \cdot (y_{CHG} \cdot \prod_{i=1}^{t-1} A_i^{j^i})^{e_h}]^{-e_h} \bmod p \quad \text{Q.E.D} \end{aligned}$$

If the verification is legal, then CHG_i computes k_1 and k_2 , $R \equiv g^{k_1 - k_2} \bmod p$ and $Z \equiv y_{CVG}^{k_1} \bmod p$.

● Step 3: Nominative proxy signature generation

In this step, CHG_i generates the signature S on message DL , as shown in Eq. (3.30). In addition, $f''(0) = k_2$ and $\sigma' \equiv \sigma + PV_{CHG} \cdot e_h \bmod q$. Then, CHG_i sends $S, DL, M_w, K, T, y_{CVG}, R, Z$ to CVG .

$$S \equiv k_2 - \sigma' \cdot e_h'' \bmod q = f''(0) - (f'(0) + f(0) \cdot e_h) \cdot e_h'' \bmod q \quad (3.30)$$

$$e_h'' = h(DL || M_w || K || T || y_{CVG} || R || Z) \quad (3.31)$$

● Original-nominative Proxy Signature Verification Phase

In the original-nominative proxy signature verification phase, any w members of CVG can verify the validity of the proxy signature generated by the proxy signers. We assume without loss of generality that the members, $\{CVG_1, CVG_2, \dots, CVG_w\}$, are chosen as the verifiers. They cooperate to generate verifier group's private key PV_{CVG} and check equality in Eq. (3.32):

$$(g^S \cdot y_{PS}^{e_h''} \cdot R)^{PV_{CVG}} \bmod p \stackrel{?}{=} Z \bmod p \quad (3.32)$$

$$y_{PS} = g^{f'(0)+f(0)e_h} \bmod p \quad (3.33)$$

In Eq. (3.32), the value of y_{PS} is gotten from $g^{f'(0)+f(0)e_h} \bmod p$, as shown in Eq. (3.33), i.e. $y_{PS} = g^{f'(0)+f(0)e_h} \bmod p$. In addition, the formula in Eq. (3.32) will be proved as follows:

Proof:

$$\begin{aligned} (1) \quad & \because y_{PS} = g^{f'(0)+f(0)e_h} \bmod p \\ & = g^\sigma \cdot (y_{CHG})^{e_h} \bmod p \\ & = (g^{x_{CP} \cdot e_h + k}) \cdot (y_{CHG})^{e_h} \bmod p \\ & = y_{CP}^{e_h} \cdot K \cdot (y_{CHG})^{e_h} \bmod p \\ & = K \cdot (y_{CP} \cdot y_{CHG})^{e_h} \bmod p \end{aligned}$$

$$\begin{aligned} (2) \quad & \therefore (g^S \cdot y_{PS}^{e_h} \cdot R)^{PV_{CVG}} \bmod p \\ & = (g^{k_2 - \sigma' e_h} \cdot (K \cdot (y_{CP} \cdot y_{CHG})^{e_h})^{e_h} \cdot g^{k_1 - k_2})^{PV_{CVG}} \bmod p \\ & = (g^{k_1 - (\sigma + PV_{CHG} \cdot e_h) e_h} \cdot (K \cdot (y_{CP} \cdot y_{CHG})^{e_h})^{e_h})^{PV_{CVG}} \bmod p \\ & = (g^{k_1 - (x_{CP} \cdot e_h + k + PV_{CHG} \cdot e_h) e_h} \cdot (g^k \cdot (g^{x_{CP}} \cdot g^{PV_{CHG}})^{e_h})^{e_h})^{PV_{CVG}} \bmod p \\ & = (g^{k_1 - (x_{CP} \cdot e_h + k + PV_{CHG} \cdot e_h) e_h} \cdot (g^{k + x_{CP} \cdot e_h + PV_{CHG} \cdot e_h})^{e_h})^{PV_{CVG}} \bmod p \\ & = (g^{k_1})^{PV_{CVG}} \bmod p \equiv y_{CVG}^{k_1} \bmod p \equiv Z \end{aligned}$$

Q.E.D

3.4 Security Analysis

The proposed scheme satisfies the following security requirements: proxy signers' deviation, unforgeability, secret key's dependence, verifiability, distinguishability, identifiability, and non-repudiability.

- (1) Proxy signers' deviation: By definition, proxy signers' deviation means that the proxy signers cannot compute the original signer's secret key. They are not also able to generate the valid signature of the original signers. Assume that the proxy signers, the members in CHG , have such information: σ , K , and y_{CP} . If they can derive x_{CP} or k from above information, or generate a new and effective

signature $(\bar{\sigma}, \bar{k})$ such that $\bar{\sigma} \equiv x_{CP} \cdot \bar{e}_h + \bar{k} \pmod{q}$ and $\bar{K} \equiv g^{\bar{k}} \pmod{p}$, then, this attack is a success. However, the attacker cannot get any knowledge about x_{CP} . Hence, this attack is impossible.

- (2) **Unforgeability:** By definition, an attacker who is not a participant cannot get the secret information from the original signer, the proxy signers, and the verifiers. A valid proxy signature can only be cooperatively generated by t or more proxy signers. And, the proxy key, σ' , of the proxy group is generated from each proxy signer's proxy key σ_{CHG_i} . Each of these proxy signers' proxy keys has the partial private key information of this proxy group. Only at least t members gather could sign the valid signature. Therefore, non-delegated signers have no capability to generate a valid proxy signature. Also, $t-1$ or less proxy signers have no capability of forging a valid proxy signature. In the proposed dissertation, the attacker must have such ability to generate CP 's proxy key, $\bar{\sigma}$, such that $\bar{\sigma} \equiv x_{CP} \cdot \bar{e}_h + \bar{k} \pmod{q}$ is true. However, it is a difficulty of DLP problem when discussing how to get CP 's private key. Hence, this attacker cannot generate the actual signatures.
- (3) **Secret key's dependence:** By definition, proxy key σ or the delegation information can be computed only with the help of CP 's private key. In the proposed scheme, proxy key σ is generated from the original signer's secret key, x_{CP} . However, it is a difficulty of DLP problem when discussing how to get CP 's private key. Therefore, this attack is not possible.
- (4) **Verifiability:** From nominative proxy signature, anyone can be convinced of CP 's agreement on the signed message. Seeing from the generated signature, $(S, DL, M_w, K, T, y_{CVG}, R, Z)$, CVG can be convinced of the original signer's agreement on the signed message. By applying time stamp, T , which is determined by CP , CHG cannot generate valid proxy signature after delegation revocation. In addition, each session has its new random numbers, k , k_1 and k_2 , and these numbers stand for different shares and signatures. Hence, each signature can be verified.
- (5) **Distinguishability:** The verifiers have to distinguish the origin of the proxy signatures. Only a delegated proxy signer can generate his/her partial proxy

signature. In this dissertation, all of the proxy signers' secret keys are used in proxy share generation phase and nominative proxy signature generation phase to generate a nominative proxy signature key and a nominative proxy signature. Thus it is necessary for the verifiers to verify the signature using the proxy signers' public key. Even the original signer cannot masquerade as a proxy signer to generate a partial proxy signature. This property protects the authority of the proxy signer. The proposed scheme adopts protected partial delegation method. And, the proxy group CHG 's proxy key, $\sigma' \equiv \sigma + PV_{CHG} \cdot e_h \pmod q$ is proxy-protected. Therefore, any proxy signature is distinguishable.

- (6) **Identifiability:** Only the valid proxy signers can generate a legal proxy signature. In each session, the proxy signers get new proxy keys and produce different proxy signatures. In addition, in the proposed scheme, from the warrant M_w , the identifies of CHG and CVG are included. Thus, a verifier easily knows who the actual proxy signers are. Hence, these proxy signatures are identifiable.
- (7) **Non-repudiability:** Any valid proxy signature is generated, then, anyone cannot repudiate that they have done. This is because all the shares and proxy signatures have partial secret information about these participants. The verifier can make sure that the signed message is a correct one by using the proxy signing keys. The original signer cannot deny having delegated the power of signing messages to the proxy signers. Furthermore, the proxy signers cannot deny that they have signed the message. In the proposed scheme, the proxy keys generated from CP or CHG include both CP and CHG 's private key information. These information as well as M_w keeps CP and CHG from denying that they have ever signed the digital license. Therefore, once the verifications in Eq. (3.25) and Eq. (3.32) are passed, the actual CP and CHG cannot deny that they have sign the message.

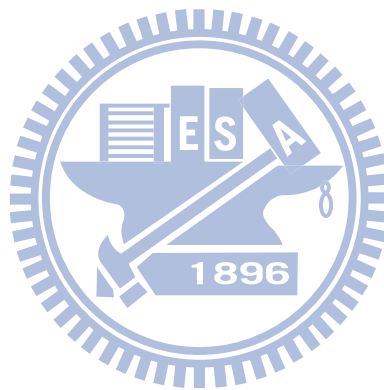
3.5 Performance Analysis

In the proposed GO-NPSS scheme, the operations in the proposed scheme include the multiplication, modular addition, and modular exponentiation operations. Among these operations, modular exponentiation takes us the most computation time and increases many computation overheads. However, security and performance are the trade-off issues. In the future, the implementation of firmware on the proposed

scheme may be a solution to solve the performance issues.

3.6 Conclusion

A digital signature scheme is a must for assuring that the digital license generated from the service provider is a legal and valid license in license-based DRM systems. The proposed scheme, group-oriented nominative proxy signature scheme (GO-NPSS), provides an original-nominative verification architecture. Under this framework, a verifier group can verify the validity of the digital license signed by the proxy group. Five phases support the proposed scheme. Security analysis notices that the proposed scheme is secure enough to be used for DRM systems. Consequently, the scheme can prevent the original signer from repudiating the validity of the license having delivered to the clients before. Especially, this scheme is applicable for mobile-based DRM systems.



Chapter 4 An EBS-based Batch Rekeying Scheme for Secure Group Communications

In a multicasting environment, group communications is essential. An important issue of providing secure group communications is group key management. The exclusion basis system (EBS) provides a framework for supporting group key management, especially in a large-size network. In EBS, a key server (KS) is used to generate both administration and session keys. In turn, KS uses these keys to distribute rekeying messages to group members so as to keep them from eavesdropping and taping. However, the EBS system does not allow member nodes to join or leave their group. In this dissertation, an EBS-based batch rekeying scheme is proposed. The scheme supports three operations, join, leave with collusion-resistant (L/CR), and leave with collusion-free (L/CF). To provide the join operation, KS periodically performs batch rekeying. Karnaugh map (K-map) is used in operation L/CR while the Chinese Remainder Theorem (CRT) is applied to operation L/CF. Both backward secrecy and forward secrecy are guaranteed in the proposed scheme. This dissertation compares the performance of the proposed scheme with that of EBS in terms of three performance metrics: storage cost, computation cost, and communications overhead. By comparison results, it indicates that the proposed scheme outperforms EBS in all three categories. The simulation results also indicate that the proposed scheme is more efficient and scalable than EBS.

4.1 Key Management Introduction

There are three kinds of group key management protocols [39]: centralized, decentralized, and distributed. In this dissertation, it focuses on the centralized ones. In centralized protocols, a key server (KS) is employed for controlling group activities. Most of them, such as LKH [55], OFT [45], etc, are tree-based. A tree-based approach employs a hierarchy of keys in which each group member, based on his/her location, is assigned a set of keys. For a group of n members in a k -ary tree-based group key management system, each member keeps $\log_k n$ administration keys and KS has to send $(k-1) \times \log_k n$ rekeying messages. Existing research has proposed periodical batch rekeying schemes [3][22][30][44][59] to reduce

computational overheads so as to improve the efficiency of batch rekeying. The exclusion basis system (EBS) [6], which employs a combinatorial formulation, is more efficient and scalable than tree-based systems. In EBS, both the number of administration keys and the number of rekeying messages are the logarithm of the number of rekeying messages incurred in tree-based systems, i.e., $\log(\log_k n)$. However, EBS only supports a single-rekeying which is not efficient in handling frequent join/leave requests.

In this dissertation, an EBS-based batch rekeying scheme is proposed in cluster-based WANs which supports three operations, join, leave with collusion-resistant (L/CR), and leave with collusion-free (L/CF). To provide the join operation, KS periodically performs batch rekeying. Karnaugh map (K-map) is used in operation L/CR. Operation L/CR updates session keys and delivers them with a few rekeying messages. The Chinese Remainder Theorem (CRT) is applied to operation L/CF. Operation L/CF prevents the collusion attacks but still maintains the same communications overhead as operation L/CR does.

A key management system has to satisfy four security requirements: confidentiality, authenticity, backward secrecy, and forward secrecy. In some circumstances, collusion prevention is also a must. The proposed scheme not only meets the four security requirements but also prevents the departed group members from conspiring to decipher the rekeying messages. By examining both analytical and simulation results, they indicate that the proposed scheme is more efficient and scalable than EBS.

The remainder of this chapter is organized as follows: In section 4.2, related works are discussed. The proposed scheme is detailed in section 4.3. In section 4.4, both security and performance analyses are given, followed by a discussion on the simulation results in section 4.5. In the last section, conclusion is presented.

4.2 Related Works

In this section, the EBS system, the K-map simplification method, and CRT are briefly discussed.

4.2.1 EBS System

Eltoweissy et al. [6] introduced the EBS framework which provides a scalable and

efficient key management scheme for secure group communications. They use a combinatorial formulation to produce optimal results with respect to the parameters n, k and m , where n is the size of the group, k the number of keys owned by each member, and m the number of rekeying messages. In their scheme, three keys are used: session key, administration key, and individual key. Session key is used to encrypt multicast data. Administration key is used to encrypt session key in single-rekeying. Each member has individual key which is also known by KS .

In [6], EBS has shown a better performance both in storage and communications costs than that of tree-based schemes. EBS also guarantees both forward secrecy and backward secrecy for single join/leave operation. In general, EBS provides a better key management in group communications. However, it may suffer from collusion attacks if the departed members tried to breach the system.

4.2.2 K-map Simplification

The K-map simplification [29] is a method used in Boolean function simplification. It is used to reduce the number of products and the number of literals. The term K-map has been used to minimize the number of messages required to distribute new keys to the existing group members for tree-based key management protocol in [1]. K-map is a way of representing a Boolean function so that logically adjacent terms, with Hamming distance 1, are physically adjacent. Minterms are entered on the map as 1s. Each block corresponding to a minterm will have a value of 1. The loops around the groups of 1s in the map represent a possible simplification by applying the rules of Boolean algebra. Therefore, when two adjacent cells both have 1s, then those cells can be factored, eliminating the variable that is different for the cells. The same operations can be applied two or more adjacent cells which have 1's. By these operations, the number of literals is less than before.

Hence, the final result of employing K-map is to reduce a function to a sum of its essential prime implicants (PI). Here, a PI is a product term that is not contained by any other product term of the function. And an essential PI is a PI that covers a minterm that is not covered by any other PI.

4.2.3 Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) [47] states a system of congruences which can be replaced by a single congruence under certain conditions. Suppose

$\beta_1, \beta_2, \dots, \text{and } \beta_r$ are relatively prime integers. Then, for integers $a_1, a_2, \dots, \text{and } a_r$, there exists a unique integer X as a common solution to the system of congruence.

$$\begin{cases} X \equiv a_1 \pmod{\beta_1} \\ X \equiv a_2 \pmod{\beta_2} \\ \vdots \\ X \equiv a_r \pmod{\beta_r} \end{cases}$$

Then, X can be rewritten, as shown in Eq. (4.1):

$$\sum_{i=1}^r a_i \times B_i \times B_i^{-1} \equiv 1 \pmod{B} \quad (4.1)$$

where $B = \prod_{i=1}^r \beta_i$; $B_i = \frac{B}{\beta_i}$; and $B_i \times B_i^{-1} \equiv 1 \pmod{\beta_i}$.

4.3 The Batch Rekeying Scheme

The proposed batch rekeying scheme is an extension of the EBS system and provides batch rekeying for allowing users to join and leave their group freely. Three operations, join, leave with collusion-resistant (L/CR), and leave with collusion-free (L/CF) are supported.

4.3.1 Notations

- P : a group member set, $\{p_1, p_2, \dots, p_n\}$, where $p_i, i = 1, 2, \dots, n$, is the i^{th} member.
- A : a set of administration keys, $\{A_1, A_2, \dots, A_{k+m}\}$; where k is the number of administration keys each member has and m the number of rekeying messages.
- A' : a set of administration keys to replace A .
- A_i : $i = 1, 2, \dots, n$, the i^{th} administration key. In addition, A_i is a set and its elements are chosen from P to indicate that these chosen members keep administration key A_i .
- A_i' : a new administration key to replace A_i .
- (A_i, p_j) : $(A_i, p_j) = 1$ if and only if $p_j \in A_i$; or $(A_i, p_j) = 0$ if and only if $p_j \notin A_i$.
- SK : the current group session key.
- SK' : a new group session key to replace SK .

- $EBS(n, k, m)$: an EBS system with n members in which each member keeps k administration keys and the number of rekeying messages is m .
- $EBS(n', k', m')$: due to batch rekeying, join or leave, the EBS system is changed from $EBS(n, k, m)$ to $EBS(n', k', m')$.
- K_i : member p_i 's individual key.
- $h(\cdot)$: a strong one-way collision free hash function with a fixed-length output. In other words, this function operates on an arbitrary length input message M and returns with fixed length.
- $\{ \cdot \}_{ek}$: an encryption function which is used to encrypt message ' \cdot ' by using key ek .
- $Canonical(k, m)$: a matrix representing canonical enumeration of all $C(k+m, k)$ combinations.
- $Canonical(k', m')$: a matrix representing canonical enumeration of all $C(k'+m', k')$ combinations.
- $\|$: Concatenation, a string concatenation. It is the operation of joining two character strings end to end a string concatenation.
- $\Delta(A_1, A_2, \dots, A_{k+m}) = \sum mlf(i | \text{the value of the } i\text{th item in } K\text{-map is } 1) + \sum d(j | \text{the } j\text{th item's value is "don't-care"})$:

Here, Δ is a simplification function, and its output is the results of the sum of products (SOP) simplification using the K-map method; $mlf()$ a minterm list form and it is a compact representation for canonical SOP form; and, $d()$ can be treated as either 1 or 0 when groups of 1s are formed on K-map. Moreover, this output determines the number of rekeying messages needed to be sent to the group.

An example of the simplification procedure is illustrated in the section 4.3.2.2.2.

4.3.2 The Proposed Scheme

The proposed batch rekeying scheme has two phases: the initialization phase and the rekeying phase.

4.3.2.1 Initialization Phase

In this phase, a group of n members is formed. The initialization phase is described as follows:

Input: A group member set $\{p_1, p_2, \dots, p_n\}$

Output: Member p_i is assigned SK and a subset of A with k elements

Procedure *Initialization*(p_1, p_2, \dots, p_n)

Step 1: /* KS verifies users' identities */

For $i \leftarrow 1$ to n

 Verify p_i 's identity;

Step 2:

/* KS generates session key, SK , and a set of administration keys, A . The size of A is determined by $Canonical(k, m)$. */

$k \leftarrow 1$;

$m \leftarrow 0$;

/* KS generates $Canonical(k, m)$, SK , and A . $Canonical(k, m)$ has to provide enough capacity for $EBS(n, k, m)$. */

While $C(k+m, k) < n$ //The term ' C ' stands for combinations.

{

 If $(k+m)$ is odd then

$m \leftarrow m+1$;

 Else

$k \leftarrow k+1$;

}

Step 3:

/* KS distributes both SK and a subset of A to each group member. */

For $i \leftarrow 1$ to n

{

$p_i \leftarrow SK$;

$p_i \leftarrow$ a subset of A ;

}

4.3.2.2 Rekeying Phase

In this phase, KS generates SK' and distributes it to all group members. SK' is used by batch rekeying. In addition, some members have to update their administration keys for supporting operations join and leave.

4.3.2.2.1 Operation Join

The batch rekeying method is used in operation join. For a given time interval, operation join processes all joining requests altogether instead of processing them one by one as EBS does. Because of dynamic group communications, the batch rekeying method reduces rekeying overheads and improves the efficiency of batch rekeying. The disadvantage of batching join requests is that it postpones a joining member from accessing multicast data until batch rekeying is completed. However, in most cases, batch rekeying can result in a significant savings in terms of reducing the number of rekeying messages.

$Canonical(k, m)$ is used in both join and leave operations. In operation join, if the number of existing members is less than or equal to $C(k+m, k)$ after x members has joined the group, then $Canonical(k, m)$ will not be changed; otherwise, $Canonical(k, m)$ has to be reconstructed. Before presenting operation join, this dissertation firstly proves Theorem 4.1. Theorem 4.1 presents the reconstruction procedure.

Theorem 4.1: For a group of n members, if the number of joining requests is x , then $Canonical(k', m')$ can be reconstructed as follows:

$$EBS(n', k', m') \equiv \begin{cases} n+x \leq C(k+m+i, k + \lfloor \frac{i}{2} \rfloor), & \text{if } k+m \text{ is odd} \\ n+x \leq C(k+m+i, k + \lceil \frac{i}{2} \rceil), & \text{if } k+m \text{ is even} \end{cases},$$

$i = 1, 2, \dots, n' = n+x$, and

$$\begin{cases} k' = k + \lfloor \frac{i}{2} \rfloor, m' = m + \lceil \frac{i}{2} \rceil, & \text{if } k+m \text{ is odd} \\ k' = k + \lceil \frac{i}{2} \rceil, m' = m + \lfloor \frac{i}{2} \rfloor, & \text{if } k+m \text{ is even} \end{cases}$$

Here, $EBS(n', k', m')$ is an EBS system with $n' = n+x$ members in which each member keeps k' administration keys and the number of rekeying messages is m' . i is a control item used to determine the size of canonical matrix when the matrix has to be reconstructed. The new matrix ensures that the EBS system supports n'

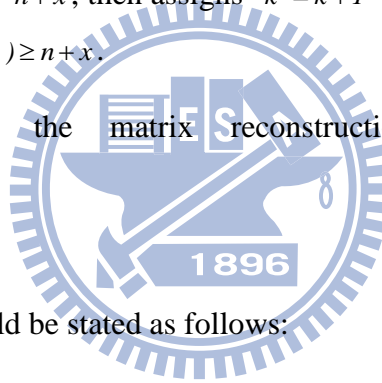
members. At beginning, i is 1 and is increased by 1 until the condition in Theorem 4.1 is matched.

Proof:

First, if $k+m$ is odd, then $k=m+1$; else, $k=m$. If $n+x > C(k+m, k)$, then matrix reconstruction is necessary. Thus, the number of administration keys will be increased from $k+m$ to $k'+m'$ such that $C(k'+m', k') \geq n+x$. There are two possible cases:

- (1) If $k+m$ is odd, then assigns $k'=k$ and $m'=m+1$. If $C(k+m+1, k)$ is not larger than or equal to $n+x$, then assigns $k'=k+1$ and $m'=m+1$. Then, checks again until $C(k'+m', k') \geq n+x$.
- (2) If $k+m$ is even, then assigns $k'=k+1$ and $m'=m$. If $C(k+m+1, k)$ is not larger than or equal to $n+x$, then assigns $k'=k+1$ and $m'=m+1$. Then, checks again until $C(k'+m', k') \geq n+x$.

From (1) and (2), the matrix reconstruction rule can be built.
Q.E.D



Now, operation join could be stated as follows:

Input: $n, k, m, \{ p_1, p_2, \dots, p_x \}$

Output:

- (i) Each existing member is assigned SK' and possibly some administration keys.
- (ii) Each p_i is assigned SK' and a subset of A with k' elements.

Procedure $Join(n, k, m, \{ p_1, p_2, \dots, p_x \})$

Step 1: /* KS verifies x . */

For $i \leftarrow 1$ to x

Verify p_i 's identity;

Step 2:

/ According to Theorem 4.1, KS reconstructs Canonical(k', m'). */*

If $C(k+m, k) < n+x$ then

{

/ KS generates Canonical(k', m'), SK' along with some new administration key(s), and A' */*

While $C(k+m, k) < n+x$

{

If ($k+m$ is odd) then

$m \leftarrow m+1$;

Else

$k \leftarrow k+1$;

}

Call Step 3;

}

Else

Call Step 3;

Step 3:

/ KS encrypts rekeying message and distributes it to existing group members. */*

If A has been changed then

```

{
    /* Rekeying message generation. */

    { SK' || A_{k+m+1} || ... }_{KK};

    /* KS distributes rekeying message to existing group members. */

    For i ← 1 to n

        p_i ← { SK' || A_{k+m+1} || ... }_{KK};

    }

Else

    {

        /* Rekeying message generation. */

        { SK' }_{SK};

        /* KS distributes rekeying message to existing group members. */

        For i ← 1 to n

            p_i ← { SK' }_{SK};

        }

```



Step 4:

/* KS generates individual keys and distributes these keys to x joining requests. Then, KS encrypts the concatenation of SK' and administration keys with K_{n+i} , where $i = 1, 2, \dots, x$, and sends these encrypted messages to them. */

```

For i ← n+1 to n+x

    p_i ← { SK' || a subset of A }_{K_i};

```

4.3.2.2.2 Operation L/CR

In this operation, we assume that all departed members would not cooperate to compromise the proposed system. Under this assumption, how to deliver SK'

securely to existing group members is an outstanding issue. KS has to encrypt SK' by using one or more administration keys. In operation L/CR, KS can derive one or more subsets of administration keys which are produced by applying the K-map simplification method. Administration keys are input variables and its output is one or more subsets of administration keys.

The K-map simplification method reduces the number of rekeying messages that KS has to send. Using this approach, KS can protect SK' from eavesdropping and deliver SK' to group members securely. The problem of simplifying the number of rekeying messages needed to be sent in the proposed operation is equivalent to the simplification of a Boolean function using the K-map approach.

Since the number of members is reduced from n to n' , $Canonical(k, m)$ has to be reorganized in a way to keep it in optimal situation. In addition, KS temporarily suspends some members in order to keep the proposed system in an optimal condition. All removed members will be resumed by KS after the proposed system is reconstructed.

Theorem 4.2 defines two subsets of P , L and R , used in operations L/CR and L/CF. In addition, a suspended member is a user who is expelled from the system to keep $Canonical(k, m)$ in optimal situation and will be resumed after all members of set L in Theorem 4.2 have left. Before presenting L/CR, Theorem 4.2 will be proved.

Theorem 4.2: Let L and R be two subsets of P ; each has v elements. Let L be the set of leaving members and R the set of suspended members. Then, the following three properties hold:

- (1) $0 < |L| = |R| = v < n$; and $|L \cup R| \leq n$.
- (2) If $L \cap R = \emptyset$, then $|L \cup R|$ is $2v$; where the number of resumed members is $|R - L| = v$.
- (3) If $L \cap R \neq \emptyset$, then $|L \cup R|$ is less than $2v$; where the number of resumed members is $|R - L| < v$.

Proof:

(1) Suppose $|L \cup R| > n$, it implies that $\exists x \in L \cup R$ and $x \notin P$, which contradicts the assumption that L and R are two subsets of P .

(2) Since $L \cap R = \emptyset$, it implies that $|L \cap R| = 0$. By set operation, $|L \cup R| = |L| + |R| - |L \cap R| = |L| + |R| = 2v$. In addition, In Eq. (4.4), both sets, $R-L$ and $L \cap R$ are disjoint, i.e., $|(R-L) \cup (L \cap R)| = |R-L| + |L \cap R|$. By Eqs. (4.2), (4.3), (4.4), and $|L \cap R| = 0$, Eq. (4.5) is determined, i.e., $|R-L| = v$.

$$R = (R-L) \cup (L \cap R) \quad (4.2)$$

$$|R| = v = |(R-L) \cup (L \cap R)| \quad (4.3)$$

$$|(R-L) \cup (L \cap R)| = |R-L| + |L \cap R| \quad (4.4)$$

$$|R| = |R-L| + |L \cap R| = |R-L| = v \quad (4.5)$$

(3) Since $L \cap R = \emptyset$, it implies that $|L \cap R| \neq 0$, i.e., $\exists p_i \in L \cap R$, such that p_i is being removed forever, i.e., $|L \cup R| < 2v$. In addition, In Eq. (4.8), both sets, $R-L$ and $L \cap R$ are disjoint, i.e., $|(R-L) \cup (L \cap R)| = |R-L| + |L \cap R|$. By Eqs. (4.6), (4.7), (4.8), and $|L \cap R| \neq 0$, Eq. (4.9) is determined, i.e., $|R-L| < v$.

$$R = (R-L) \cup (L \cap R) \quad (4.6)$$

$$|R| = v = |(R-L) \cup (L \cap R)| \quad (4.7)$$

$$|(R-L) \cup (L \cap R)| = |R-L| + |L \cap R| \quad (4.8)$$

$$|R| = v = |R-L| + |L \cap R| > |R-L| \quad (4.9)$$

Q.E.D

In operations L/CR and L/CF, if the number of existing members is larger than $C(k+m-1, k-1)$ when $k+m$ is odd or larger than $C(k+m-1, k)$ when $k+m$ is even after v members has left, then $Canonical(k, m)$ will not be changed; otherwise, $Canonical(k, m)$ has to be reconstructed. There are two steps to support $Canonical(k, m)$ reconstruction. Before presenting operation L/CR, Theorems 4.3 and

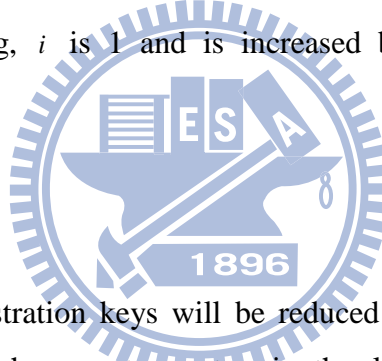
4.4 will be proved. First, Theorem 4.3 presents how to find the lower bound of $n-v$ after v members has left. Second, according to Theorem 4.3, Theorem 4.4 presents the reconstruction procedure to reconstruct $Canonical(k', m')$.

Theorem 4.3: For a group of n members, if the number of leaving members is v , then the lower bound of $n-v$ is as follows:

$$\left\{ \begin{array}{l} n-v \geq C(k+m-i, k - \left\lfloor \frac{i}{2} \right\rfloor), \text{ if } k+m \text{ is odd } \dots (i) \\ n-v \geq C(k+m-i, k - \left\lfloor \frac{i}{2} \right\rfloor), \text{ if } k+m \text{ is even } \dots (ii) \end{array} \right. ,$$

$$i = 1, 2, \dots, \text{ and } n' = n-v$$

Here, i is a control item used to determine the size of canonical matrix when the matrix has to be reconstructed. The new matrix ensures that the EBS system supports n' members. At beginning, i is 1 and is increased by 1 until the condition in Theorem 4.3 is matched.



Proof:

The number of administration keys will be reduced from $k+m$ to $k'+m'$ such that $n-v \geq C(k'+m', k')$, where $C(k'+m', k')$ is the lower bound of $n-v$. The following two cases are discussed to find the lower bound of $n-v$:

● Case 1: $k+m$ is odd

If $C(k+m-1, k-1)$ is not the lower bound of $n-v$, then checks $C(k+m-2, k-1)$ again until $C(k+m-i, k - \left\lfloor \frac{i}{2} \right\rfloor) \leq n-v < C(k+m-i+1, k - \left\lfloor i - \frac{1}{2} \right\rfloor)$, where $i = 1, 2, \dots$; thus,

$C(k+m-i, k - \left\lfloor \frac{i}{2} \right\rfloor)$ is the lower bound of $n-v$. Therefore, $k^* = k - \left\lfloor \frac{i}{2} \right\rfloor$ and

$$m^* = m - \left\lfloor \frac{i}{2} \right\rfloor.$$

● Case 2: $k+m$ is even

If $C(k+m-1, k)$ is not the lower bound of $n-v$, then checks $C(k+m-2, k-1)$

again until $C(k+m-i, k - \lfloor \frac{i}{2} \rfloor) \leq n-v < C(k+m-i+1, k - \lfloor i - \frac{1}{2} \rfloor)$, where $i=1, 2, \dots$; thus,

$C(k+m-i, k - \lfloor \frac{i}{2} \rfloor)$ is the lower bound of $n-v$. Therefore, $k^* = k - \lfloor \frac{i}{2} \rfloor$ and

$$m^* = m - \lfloor \frac{i}{2} \rfloor.$$

Q.E.D

Theorem 4.4: For a group of n members, if the number of leaving members is v , then $Canonical(k', m')$ can be reconstructed as follows:

$$EBS(n', k', m') \stackrel{A}{\equiv} \begin{cases} n-v \leq C(k^* + m^* + i, k^* + \lfloor \frac{i}{2} \rfloor), & \text{if } k^* + m^* \text{ is odd} \\ n-v \leq C(k^* + m^* + i, k^* + \lceil \frac{i}{2} \rceil), & \text{if } k^* + m^* \text{ is even} \end{cases}$$

$i=0, 1$; $n' = n-v$; k^* and m^* are two lower bound parameters in Theorem 4.3; and

$$\begin{cases} k' = k^* + \lfloor \frac{i}{2} \rfloor, m' = m^* + \lfloor \frac{i}{2} \rfloor, & \text{if } k^* + m^* \text{ is odd} \\ k' = k^* + \lceil \frac{i}{2} \rceil, m' = m^* + \lceil \frac{i}{2} \rceil, & \text{if } k^* + m^* \text{ is even} \end{cases}$$

Here, i is a control item used to determine the size of canonical matrix when the matrix has to be reconstructed. The new matrix ensures that the EBS system supports n' members.

Proof:

- (1) According to Theorem 4.3, the lower bound of $n-v$ is found. In other words, $n-v \geq C(k^* + m^*, k^*)$ is found.
- (2) There are two cases to discuss to reconstruct $Canonical(k', m')$:

● Case 1: $i=0$

It implies that $n-v = C(k^* + m^*, k^*)$.

● Case 2: $i = 1$

It implies that the lower bound $C(k^* + m^*, k^*)$ is less than $n - v$. Then, Theorem 4.1 is used to reconstruct $Canonical(k', m')$. Q.E.D

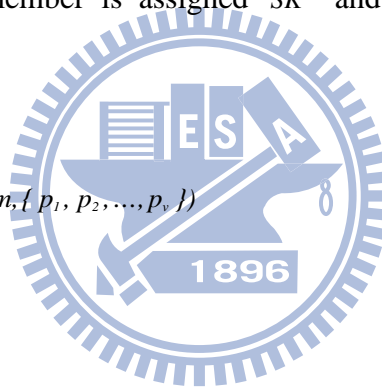
Operation L/CR consists of the following five steps:

Input: $n, k, m, \{p_1, p_2, \dots, p_v\}$

Output:

- (i) Each existing member updates old administration keys and then be assigned SK'' and possibly some new administration keys.
- (ii) Each resuming member is assigned SK'' and their own administration keys.

Procedure $L/CR(n, k, m, \{p_1, p_2, \dots, p_v\})$



Step 1:

/* Let the number of leaving members be $|L \cup R|$. In addition, according to Theorem 4.2, $|R - L|$ members will be added into the proposed system again. */

$l \leftarrow |L \cup R|;$

Step 2:

/* According to Theorems 4.3 and 4.4, KS determines the parameters: k and m after v members left. */

While $C(k + m, k) > n - l$

{

If $(k + m$ is odd) then

```

     $k \leftarrow k - 1;$ 

    Else

         $m \leftarrow m - 1;$ 

    }

    /* KS generates Canonical( $k, m$ ) and  $A^*$  */

    If  $C(k+m, k) < n-1$  then

    {

        If ( $k+m$  is odd) then

             $m \leftarrow m + 1;$ 

        Else

             $k \leftarrow k + 1;$ 

    }

    Else

         $A^*$  is generated;

        /* KS generates  $SK^*$ ; encrypts it with each subset of administration keys
        derived from the results of the K-map simplification; and distributes encrypted
        messages to the existing members. The input of K-map is two-valued-input with
         $k+m$  variables,  $A_1, A_2, \dots, A_{k+m}$ , and its output is two-valued-output. In addition, the
        variables that are complemented in each product term in the output are ignored. */

        /*One or more subsets of administration keys are generated. */

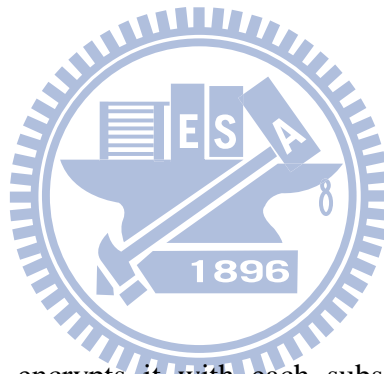
        Call K-map( $A, P$ );

        For  $i \leftarrow 1$  to  $n-1$ 

            //  $A^*$  is a combination of administration keys and is one of product terms in
            K-map's output.

             $p_i \leftarrow \{SK^*\}_{A^*};$ 

```



Step 4:

/* After receiving rekeying message, each existing group member is assigned SK' . They update their administration keys, which are affected, by calculating $h(SK', A_j)$. In addition, the number of administration keys that p_i holds is reduced to k' , $k' < k$. */

For $j \leftarrow 1$ to k'

$A_j' \leftarrow h(SK', A_j)$;

Step 5:

/* KS resumes the suspended members, assigns them to the positions where the departed members stayed before, and gives them administration keys. Finally, these resumed members have a new session key and some administration keys.*/

Call $Join(n, k, m, \{p_1, p_2, \dots, p_{|R-1|})$;

The K-map method is used to find the minimum combinations of administration keys. Each combination is a subset of A . Anyone who had left the group has no or only partial information about each subset. Therefore, he/she could not decrypt any rekeying messages without knowing all of the keys of a subset. The only issue is that it cannot resist collusion attacks from the compromised departed members. Theorem 4.5 proves the above conclusion.

Theorem 4.5: Suppose the proposed system has n members, and its set of administration keys is $A = \{A_1, A_2, \dots, A_{k+m}\}$, and each member holds k administration keys. If the colluding members with $k+i$ administration keys, then KS protects at most $\sum_{l=0}^{m-i} C(m-i, l) \times C(k+i, k-l)$ existing group members. According to the above information, there are three possible cases:

- Case 1: $i=0$, it is called a single user attack.

- Case 2: $0 < i < m$, an attack is successful with probability p , $0 < p < 1$.
- Case 3: $i = m$, an attack is always successful.

Note, cases 2 and 3 are both multiple-member collusion attack.

Proof:

We assume, without loss of generality, that the colluding members have $\{A_1, A_2, \dots, A_{k+i}\}$ administration keys. If an existing group member wants to be assigned SK' successfully, then he/she must have at least one administration key chosen from $\{A_{k+i+1}, \dots, A_{k+m}\}$. Hence, this is a combinatorial problem. The combinatorial formula is $\sum_{l=1}^{m-i} C(m-i, l) \times C(k+i, k-l)$. These $\sum_{l=1}^{m-i} C(m-i, l) \times C(k+i, k-l)$ members are protected from collusion attack.

Three cases are proved as follows:

- Case 1: There is only one attacker out of departed members.

Since there is only one attacker, KS can protect at most $\sum_{l=1}^m C(m, l) \times C(k, k-l) = C(k+m, k) - 1$ members. This result shows that if there are v members left the proposed system and an attacker cannot compromise the system.

- Case 2: The colluding attackers gather their administration keys and the number of different administration keys is $k+i$.

Since the collusion attackers gather $k+i$ administration keys, KS can protect at most $\sum_{l=1}^{m-i} C(m-i, l) \times C(k+i, k-l)$ members. If there are v members left the proposed system, then:

If the number of existing group members is larger than $\sum_{l=1}^{m-i} C(m-i, l) \times C(k+i, k-l)$, then the attack is success.

If the number of existing group members is less than or equal to $\sum_{l=1}^{m-i} C(m-i, l) \times C(k+i, k-l)$, then the attack is success with probability p depending on the state of the proposed system.

- Case 3: The colluding attackers gather their administration keys to form a key set which is equivalent to A .

KS cannot produce any combinations of administration keys to protect SK .
Q.E.D

Example:

Suppose that there are five members in the group, $P = \{ p_1, p_2, p_3, p_4, p_5 \}$, and a set of administration keys, $A = \{ A_1, A_2, A_3, A_4 \}$; where $A_1 = \{ p_1, p_3, p_4 \}$, $A_2 = \{ p_2, p_3, p_5 \}$, $A_3 = \{ p_1, p_2 \}$ and $A_4 = \{ p_4, p_5 \}$. Then, KS establishes *Canonical(2,2)* matrix for *EBS(5,2,2)* in Table 2. If members p_2 and p_4 want to leave the system. KS has to expel p_2 , p_4 , and p_5 from the system i.e., $L = \{ p_2, p_4 \}$ and $R = \{ p_4, p_5 \}$. p_5 is a suspended member and removed temporarily. Then, KS builds Boolean function expression, as shown in Table 3, and the canonical SOP form is $\Delta(A_1, A_2, A_3, A_4) = A_1 A_2 A_3 A_4 + A_1 A_2 A_3 A_4 = \sum m f(10, 12)$. The key server translates the Boolean function expression into K-map form (in fact, Boolean function expression can be ignored and K-map can be used directly). By using K-map, as shown in Table 4, the simplified form is as follows:

$$\Delta(A_1, A_2, A_3, A_4) = \sum m f(10, 12) + \sum d(0, 1, 2, 3, 4, 7, 8, 11, 13, 14, 15) = A_1 A_2 + A_1 A_3$$

Table 2. The EBS system with $n = 5$, $k = 2$, and $m = 2$

	p_1	p_2	p_3	p_4	p_5
A_1	1	0	1	1	0
A_2	0	1	1	0	1
A_3	1	1	0	0	0
A_4	0	0	0	1	1

Table 3. Boolean function expression

	A_1	A_2	A_3	A_4	Δ	<i>minterm</i>
0	0	0	0	0	d^1	
1	0	0	0	1	d	
2	0	0	1	0	d	
3	0	0	1	1	d	
4	0	1	0	0	d	
5	0	1	0	1	0	
6	0	1	1	0	0	
7	0	1	1	1	d	
8	1	0	0	0	d	
9	1	0	0	1	0	
10	1	0	1	0	1	$A_1A_2A_3A_4$
11	1	0	1	1	d	
12	1	1	0	0	1	$A_1A_2A_3A_4$
13	1	1	0	1	d	
14	1	1	1	0	d	
15	1	1	1	1	d	

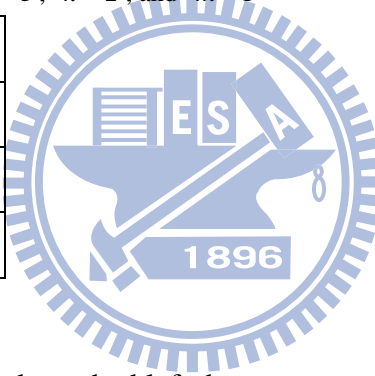
¹ d means don't care. d can be treated as either a 1 or a 0.

Table 4. The simplification procedure

$A_1 A_2$				
	00	01	11	10
$A_3 A_4$				
00	d	d	1	d
01	d	0	d	0
11	d	d	d	d
10	d	0	d	1

Table 5. The EBS system with $n = 3$, $k = 2$, and $m = 1$

	p_1	p_5	p_3
A_1	1	0	1
A_2	0	1	1
A_3	1	1	0



Because members p_2 and p_4 had left the system, KS has to reconstruct matrix, as shown in Table 5. In other words, the matrix is changed from $Canonical(2, 2)$ to $Canonical(2, 1)$ for $EBS(3, 2, 1)$. Then, KS encrypts new session key, SK' , by $\{SK'\}_{A_1 A_2}$ and $\{SK'\}_{A_1 A_3}$. KS sends these two rekeying messages to existing group members and reconstructs canonical matrix into $Canonical(2, 1)$. Each member updates his/her administration keys by calculating $h(SK', A_i)$. In addition, the suspended member, p_5 , has to be rejoined into the group. KS generates new administration keys, A_2 and A_3 , and new session key, SK'' . KS sends a rekeying message, $\{SK''\}_{SK'}$, to existing group members. The same, each member updates his/her administration keys by calculating $h(SK'', A_i)$. Finally, KS distributes A_2 , A_3 , and SK'' to p_5 encrypted by p_5 's individual key.

4.3.2.2.3 Operation L/CF

In this operation, we assume that departed members would cooperate to compromise the proposed system. Under this assumption, how to deliver SK' to existing group members securely is an important issue. In operation L/CF, CRT is applied to avoid collusion attacks. An adversary may have a chance to derive all subsets of A if some of departed members' administration keys were compromised. To deal with this issue, KS encrypts SK' by using an encryption key which is known only to him/her, and then broadcasts this encrypted message to the group members. No one can decrypt this encrypted message except the existing members. The compromised departed members cannot derive SK' even if they have colluded.

There is an easy way to deal with this problem. KS distributes SK' which is encrypted with each member's individual key. This is known as a point-to-point exchange. It involves sending multiple copies of the same message to existing group members. The advantage of this method is that KS has to execute n times encryption and unicast. It wastes a lot of time and bandwidth. An alternative way is to concatenate these individual encryptions and broadcast them as a single message. However, this does not remove the need for individual encryptions.

In this dissertation, to achieve this goal, CRT and prime number generator must be introduced into this case. In operation L/CF, some terms in CRT are modified to meet this case and to accomplish a session key batch rekeying. Let $\beta_1, \beta_2, \dots, \beta_r$ are prime integers. Then, CRT is redefined as a modified CRT in Eq. (4.10).

$$X \equiv \sum_{i=1}^r a_i \times B_i \times B_i^{-1} \pmod{B}; \quad (4.10)$$

where $B = \prod_{i=1}^r \beta_i$; $B_i = \frac{B}{\beta_i}$; and $B_i \times B_i^{-1} \equiv 1 \pmod{\beta_i}$.

SK' is randomly chosen by KS but not more than $\min\{\beta_1, \beta_2, \dots, \beta_r\}$. This is because KS has to guarantee that SK' has a unique inverse value under modular operation. KS calculates $SK' \times SK'^{-1} \equiv 1 \pmod{B}$. SK'^{-1} is uniquely determined because $\gcd(SK', B) = 1$. Let SK'^{-1} be the ciphertext and be broadcasted to group members. After receiving the message, SK'^{-1} , the group members calculate their own congruence by executing modular operation $SK'^{-1} \equiv a_i \pmod{\beta_i}$. Each of them can decrypt message by executing extended Euclidean algorithm to get the inverse value

of a_i , i.e., $a_i \times a_i^{-1} \equiv 1 \pmod{\beta_i}$. Hence, p_i obtains SK' , where $SK' = a_i^{-1}$.

Operation L/CF consists of the following seven steps:

Input: $n, k, m, \{p_1, p_2, \dots, p_v\}$

Output:

- (i) Each existing member updates old administration keys and then be assigned SK'' and possibly some new administration keys.
- (ii) Each resuming member is assigned SK'' and their and their own administration keys.

Procedure $L/CF(n, k, m, \{p_1, p_2, \dots, p_v\})$

Step 1:

/ Let the number of leaving members be $|L \cup R|$. According to Theorem 4.2, $|R - L|$ members will be added into the proposed system again. */*

$l \leftarrow |L \cup R|;$

Step 2:

/ According to Theorems 4.3 and 4.4, KS determines the parameters: k and m after v members left. */*

While $C(k+m, k) > n-l$

{

 If $(k+m)$ is odd then

$k \leftarrow k-1;$

 Else

```

        m ← m - 1;
    }
    /* KS generates Canonical(k', m') and A' */

```

```

If C(k+m, k) < n-1 then

```

```

{
    If k+m is odd then
        m ← m + 1;
    Else
        k ← k + 1;
}

```

```

Else

```

```

    A' is generated;

```

```

Step 3:

```

/* KS generates $(n - |L \cup R|)$ prime numbers, $\{\beta_1, \beta_2, \dots, \beta_{n-|L \cup R|}\}$, by executing $h(SK, K_i)$ for the existing members. If it is not a prime number, then KS executes prime number generation function to generate a prime number which is the least prime number larger than $h(SK, K_i)$. Then, KS computes $B = \prod_{i=1}^{n-|L \cup R|} \beta_i$. In addition, p_i computes its own prime β_i as well. */

```

For i ← 1 to n-1

```

```

{
    If (h(SK, K_i) is not a prime number) then
        βi ← call Prime Number Generation(); //generate the least
        prime number larger than h(SK, K_i).
    Else
        βi ← h(SK, K_i);
}

```

}

$$B \leftarrow \prod_{i=1}^{n-[L \cup R]} \beta_i;$$

Step 4:

/* KS randomly chooses a number, SK' , from $Z_{\min\{\beta_1, \beta_2, \dots, \beta_{n-[L \cup R]}\}}$ as a new session key. Then, KS calculates $SK' \times SK'^{-1} \equiv 1 \pmod B$. KS broadcasts SK'^{-1} to the group. */

$$SK' \leftarrow \text{Random}(Z_{\min\{\beta_1, \beta_2, \dots, \beta_{n-[L \cup R]}\}});$$

$SK'^{-1} \leftarrow \text{Inverse}(SK', B)$; //compute the inverse value of SK' such that $SK' \times SK'^{-1} \equiv 1 \pmod B$

KS broadcasts SK'^{-1} to the group;

Step 5:

/* p_i calculates $SK'^{-1} \equiv a_i \pmod{\beta_i}$. Then, p_i computes $a_i \times a_i^{-1} \equiv 1 \pmod{\beta_i}$.
Ultimately, p_i derives SK' , where $SK' = a_i^{-1}$. */

For $i \leftarrow 1$ to $n-1$

{

$$a_i \leftarrow SK'^{-1} \pmod{\beta_i};$$

$$a_i^{-1} \leftarrow \text{Inverse}(a_i, \beta_i); // p_i \text{ derives } SK' = a_i^{-1}$$

}

Step 6:

/* After receiving rekeying message, each existing group member is assigned SK' . Then, they update their administration keys, which are affected, by calculating $h(SK', A_i)$. In addition, the number of keys that p_i holds is reduced to k' , $k' < k$. */

For $j \leftarrow 1$ to k

$A_j' \leftarrow h(SK', A_j)$;

Step 7:

/ KS resumes the suspended members, assigns them to the positions where the departed members stayed before, and gives them administration keys. Finally, these resumed members have a new session key and some administration keys.*/*

Call $Join(n, k, m, \{p_1, p_2, \dots, p_{R-L}\})$;

Since all departed members do not have any knowledge about β_i , they cannot derive a_i . Consequently, no adversary can attack the proposed system even though he/she has gotten all administration keys from the departed members; thus, forward secrecy is guaranteed.

4.4 Security and Performance Analyses

In this section, both the security and performance of the proposed scheme are analyzed.

4.4.1 Security Analysis

In the following paragraphs, we analyze the security of the proposed scheme with respect to data confidentiality, authenticity, backward secrecy and forward secrecy, and collusion attack.

4.4.1.1 Data Confidentiality

To provide data confidentiality service, an encryption scheme must be applied. In this dissertation, transmitted messages are encrypted with SK , i.e. $\{Messages\}_{SK}$, to keep undesirable users from eavesdropping and tapping. The encryption algorithm could be any one of the symmetric encryption standards, like AES (Advanced Encryption Standard). An attacker who is not a group member could not get session key SK and could not decrypt the encrypted messages except the brute-force attack.

Thus, data confidentiality of transmitted messages is guaranteed. No one can decrypt the encrypted messages without SK . Therefore, data confidentiality is guaranteed by the proposed scheme.

4.4.1.2 Authenticity

Authentication protocols include entity authentication and message authentication which are used to verify the identity of a user and the resource of a message, respectively. Entity authentication is provided by the first step of operation join. In operation join, a new member $x_i \in x$ who wants to join the group has to issue its own identity to announce that he/she is the right one. Therefore, entity authentication is provided before operation join. If a group member p_i wants to communicate with KS , a mutual authentication algorithm is proposed as follows:

- Step 1: $p_i \rightarrow KS : ID_{p_i}, ID_{KS}, \{ ID_{p_i} || ID_{KS} || N_{p_i} || CK'_{p_i,KS} \}_{K_i}$
- Step 2: $p_i \leftarrow KS : ID_{KS}, ID_{p_i}, \{ ID_{KS} || ID_{p_i} || N_{p_i} + 1 || N_{KS} || CK''_{KS,p_i} \}_{K_i}$
- Step 3: $p_i \rightarrow KS : ID_{p_i}, ID_{KS}, \{ ID_{p_i} || ID_{KS} || N_{KS} + 1 \}_{CK_{p_i,KS}}$

Both ID_{p_i} and ID_{KS} are the identities of p_i and KS , respectively. Random nonces, N_{p_i} and N_{KS} are used to prevent replay attack. And, both $CK'_{p_i,KS}$ and CK''_{KS,p_i} are partial common session key between p_i and KS . The common session key $CK_{p_i,KS}$ could be computed by XOR operation, i.e. $CK'_{p_i,KS} \oplus CK''_{KS,p_i}$, by themselves. Finally, p_i and KS could communicate with each other by sending encrypted messages, e.g. $\{ Messages \}_{CK_{p_i,KS}}$.

Moreover, Message authentication is not considered in this dissertation. However, the message authentication protocol can be implemented by keyed one-way hash function, such as HMAC described in RFC 2104 [17].

4.4.1.3 Backward Secrecy

A security scheme supports backward secrecy only if new members cannot collaborate to learn the previous traffic patterns. Hence, it is often required that a

member who joins be denied access to messages that were sent to the group prior to its membership.

In operation join, since a joining request does not have any knowledge about both SK and administration keys; thus, $\{SK\}_{SK}$ is not compromised. Given a key space $K = \{SK_0, SK_1, \dots, SK_i, \dots, SK_j, \dots, SK_q\}$, where $i < j < q$. SK_j is assigned to joining requests. These new members cannot get any session key $SK \in \{SK_0, SK_1, \dots, SK_i, \dots, SK_{j-1}\}$ even though they have contiguous session keys from SK_j to SK_q . The reason is as follows:

Let E_1 and E_2 be two events such that $E_1 = \{SK_0, SK_1, \dots, SK_i, \dots, SK_{j-1}\}$ and $E_2 = \{SK_j, \dots, SK_q\}$, respectively. Let $SK_i \in E_1$ which new members want to learn. Let $Pr(SK_i)$ be the probability that the new members could learn session key SK_i from the group communications. Then, $(\forall SK_i \in E_1) Pr(SK_i/E_2)$ is equivalent to $Pr(SK_i)$.

Hence, backward secrecy is guaranteed in operation join and the collusion attack is never happened.

4.4.1.4 Forward Secrecy

A security scheme supports forward secrecy only if the departed members cannot collaborate to learn the future traffic patterns. Hence, the rekeying operation is needed to assure that messages sent to the group cannot be accessed by a former member whose membership has been revoked.

In operation L/CR, we assume that departed members would not cooperate to compromise the proposed system and they had contiguous session keys, $\{SK_0, SK_1, \dots, SK_i\}$. But they do not have any future session keys. Therefore, the departed members cannot get any new session key $SK \in \{SK_{i+1}, SK_{i+2}, \dots, SK_q\}$ even though they had contiguous session keys from SK_0 to SK_i . The reason is as follows:

Let E_1 and E_2 be two events such that $E_1 = \{SK_0, SK_1, \dots, SK_i\}$ and $E_2 = \{SK_{i+1}, SK_{i+2}, \dots, SK_q\}$. Let $SK_i \in E_2$ which departed members want to learn. Let $Pr(SK_i)$ be the probability that the departed members could learn session key SK_i from the group communications. Then, $(\forall SK_i \in E_2) Pr(SK_i/E_1)$ is equivalent to

$Pr(SK_i)$. Therefore, forward secrecy is clear.

In operation L/CF, all departed members conspire still cannot compromise SK' although they may have all administration keys before they left. Therefore, forward secrecy is clear.

From sections 4.4.1.3 and 4.4.1.4, this dissertation demonstrates that the proposed scheme holds both backward secrecy and forward secrecy. In addition, session keys are generated independently and are protected by old sessions in operation join and administration keys in operations L/CR and L/CF. Each member's administration keys are updated by themselves if a rekeying operation happens. This means that the proposed batch rekeying scheme supports both perfect forward secrecy and perfect backward secrecy. The disadvantages of proposed batch rekeying scheme are: for batching join and leave requests, a joining member postpones accessing multicast data and a departing member constantly gets communication data until batch rekeying is completed.

4.4.1.5 Administration Keys Secrecy

The administration keys are kept by the legal group members. Each of them holds a subset of a set A and updates their own administration keys by themselves. The administration key's updating operation based on one-way hash function, i.e. $A_i' = h(SK', A_i)$, is executed after a rekeying operation has been done. Since an attacker has no knowledge about the administration keys and the group session key, he/she can only launch the birthday attack on the underlying hash function. To avoid this attack, the length of the output stream of the hash function has to be long enough so as to make the birthday attack computationally infeasible.

4.4.1.6 Collusion Attack

A collusion attack is a kind of attack where a number of nodes collaborate to reveal all administration keys and even the session key and consequently capture the network. EBS solution as well as tree-based solutions, however, may suffer from collusion attacks. Two or more departed members collude when they share their keys

with each other. In other words, colluding nodes would grow their knowledge about the network security measures. When using EBS scheme, administration keys are reused in multiple members and only key combinations are unique. Therefore, it is conceivable that few departed nodes can collude and reveal all the administration keys. Take an example in Table 2, if members p_1 and p_5 left the group at the same time, and they collaborate to reveal the administration keys A_1 , A_2 , A_3 , and A_4 . Therefore, KS could not distribute SK' to its group members by any combinations of administration keys. In this dissertation, operation L/CR has the same problem as EBS scheme. But operation L/CF, mentioned in section 4.3.2.2.3, solves this problem.

In addition, from the previous discussions in sections 4.4.1.3 and 4.4.1.4, they indicate that the proposed operation L/CF supports both backward secrecy and forward secrecy. Thus, key independency is guaranteed. Consequently, the proposed scheme can resist collusion attacks from adversaries.

4.4.2 Performance Analysis

The proposed batch rekeying scheme is compared with EBS with respect to three performance metrics: storage cost, computation cost and communications overhead.

4.4.2.1 Storage Cost

Storage cost is measured by the number of session keys and administration keys held and updated by both KS and group members. As for the join operation of the proposed scheme, both KS and group members keep SK' and each group member updates their administration keys only for a batch of join requests. In EBS, however, each join request causes KS and group members to update their session keys and administration keys. In the proposed scheme, only one batch rekeying is required to keep session key and administration keys up to date. Similarly, for leave operations, EBS makes at least v times more effort in updating keys than the proposed scheme.

4.4.2.2 Computation Cost

The computation cost is measured by the number of encryptions and decryptions that KS and group members have performed for batch rekeying. In this dissertation,

since the number of keys updated is the major concern, i.e., the computational cost of the K-map simplification is neglected in operation L/CR.

In operation join, KS performs encryption to update group members' session key and several encryptions for joining requests. For each existing group member, he/she performs decryption to derive SK' , or the concatenation of SK' and new administration keys, and then executes several hash operations to update his/her administration keys. The number of update times for administration keys by the existing group members must be counted. In EBS, for x joining requests, the number of update times is $\sum_{i=1}^{n+x} \sum_{j=1}^l \sum_{(A_j, p_i) \neq I \wedge (A_j, p_{new})=I}^{k+m} 1$. In the proposed batch rekeying scheme, the number of update times is $\sum_{i=1}^n \sum_{j=1}^{k+m} \sum_{(A_j, p_i) \neq I \wedge \exists p_{new} (A_j, p_{new})=I} 1$.

In operation L/CR, the computation cost depends on the complexity of one or more subsets of administration keys'. SK' is encrypted with any one of these subsets derived from the K-map simplification. The number of encryptions performed by KS is equivalent to the outcome of the K-map simplification on the sum of product terms, i.e., the number of encryptions used for updating group members' session key is $\sum_{\# \text{ product terms}} \sum_{\# \text{ literals in each product term}} \mathcal{A}(A_1, A_2, \dots, A_{k+m})$. Furthermore, KS takes $|R-L|$ encryptions to resume suspended members. For each p_i , the number of decryptions depends on the SOP term that he/she got and it is no more than k times. In addition, he/she has to perform several hash operations to update his/her administration keys. For resumed members, they perform decryptions to derive SK' and administration keys by using their new individual keys.

In operation L/CF, the computation cost is determined by the number of modular operations and inverse operations under some specific modulus. Both KS and each p_i execute one modular operation and one inverse operation. Hence, the computation cost is low.

In the proposed scheme, both of these two leave operations have the same number in the number of update times for updating administration keys by group members. In EBS, the leave operations with v leaving members, the number of update times is at least $\sum_{i=1}^v \sum_{j=1}^{n-l} \sum_{(A_j, p_i) \neq I \wedge (A_j, p_{left})=I}^{k+m} 1$. In the proposed scheme, the number of administration keys that the existing group members have to update is $\sum_{i=1}^{n-|L \cup R|} \sum_{j=1}^{k+m} \sum_{(A_j, p_i) \neq I \wedge \exists p_{left} (A_j, p_{left})=I} 1$.

4.4.2.3 Communications Overhead

The communications overhead is evaluated by the number of rekeying messages. In EBS, for operation join, the number of rekeying messages sent by KS depending on the number of joining requests. In the proposed scheme, each p_i only receives $\{SK'\}_{SK}$. For joining requests, KS sends x unicast messages. Hence, the proposed scheme is more efficient and scalable than EBS. In leave operations, both operation L/CR and operation L/CF are concerned. In operation L/CR, the number of rekeying messages sent by KS depends on the results of the K-map simplification, i.e., $\sum_{\# \text{ products terms}} A(A_1, A_2, \dots, A_{k+m})$. In addition, KS sends $|R-L|$ unicast messages for resumed members. In operation L/CF, the number of rekeying messages is one. The number of unicast messages is the same as that in operation L/CR. In EBS, for v users leave, KS performs $v \times m$ rekeying messages. In addition, KS sends v unicast messages for resumed members. Compared with EBS, the proposed scheme for leave operations is more efficient and scalable.

From the performance analysis above, it shows that:

- (1) The proposed scheme is more efficient than EBS in terms of storage cost, computation cost, and communications overhead.
- (2) In the batch rekeying, the proposed scheme is more scalable than EBS in terms of the number of join users and departed members.

4.5 Simulation Results

Simulation is implemented using the Java programming language based on the Pentium 5 platform. The simulation focuses on the number of rekeying messages and the number of administration keys updated with respect to operations join, L/CR, and L/CF.

Initially, a group of 10 members is assumed. In operation join, ten cases are considered. For cases one to ten, KS processes 10, 20, ..., and 100 joining requests. In Figure 11, the communications overheads, i.e., the number of session keys updated by KS , of EBS and the proposed scheme are compared by varying the number of joining requests. Figure 11 does not consider the communications overheads of

individual keys. In EBS, KS generates SK' only if a user joins the group. The proposed scheme, however, KS only performs one session key generation. In Figure 12, the number of administration keys that group members must update during batch rekeying of operation join is presented. In EBS, each existing group member updates their own administration keys while a new user joins group. In the proposed scheme, all joining requests' administration keys are processed at once and are compared with each p_i 's administration keys. And the computation cost of EBS is much higher than that of the proposed scheme. The simulation results show that the proposed scheme is more efficient and scalable than EBS.

In operation L/CR and operation L/CF, a group of 110 members is assumed. The metrics of interest are the number of rekeying messages that KS delivers to group members and the total number of administration keys updated by group members in every rekeying case among EBS and the proposed two leave operations.

In Figure 13, the number of rekeying messages sent by KS is compared among three methods. In EBS, KS executes three rekeying operations for every leaving member. The number of rekeying messages in each batch rekeying depends on the proposed scheme except the join operation for suspended members. In operation L/CR, the number of rekeying messages depends on the results of the K-map simplification. In operation L/CF, the number of rekeying messages is 2. Simulation results show that the proposed scheme is more efficient and scalable than EBS.

Similarly, Figure 14 shows the simulation results with respect to the number of administration keys to be updated during batch rekeying of operation leave. As a result of batch rekeying operations, both operation L/CR and operation L/CF have the same numbers in the number of administration keys to be updated. The number of administration keys to be updated in both operation L/CR and operation L/CF is decreased significantly compared with EBS. This is because the proposed scheme adopts the batch rekeying operations and these keys are updated by existing group members themselves; therefore, the administration keys must be updated only if the group members leave the network.

The above simulation results demonstrate that the proposed scheme is more efficient and scalable than EBS.

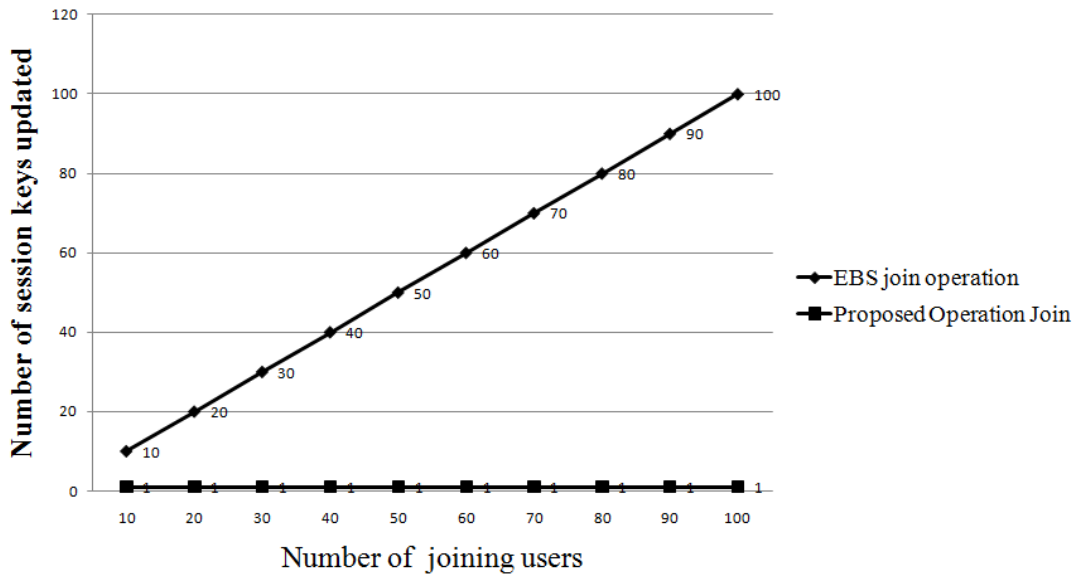


Figure 11. Number of session keys updated

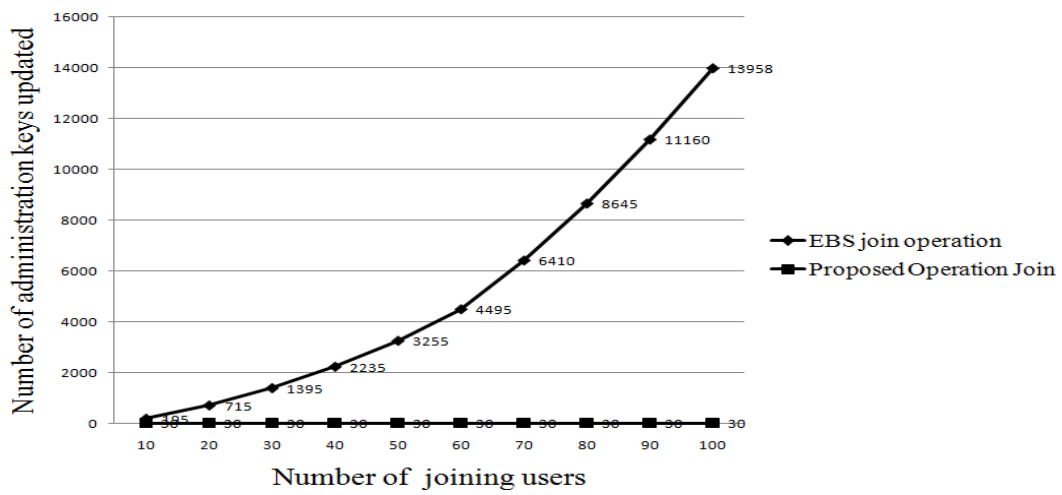


Figure 12. Number of administration keys updated

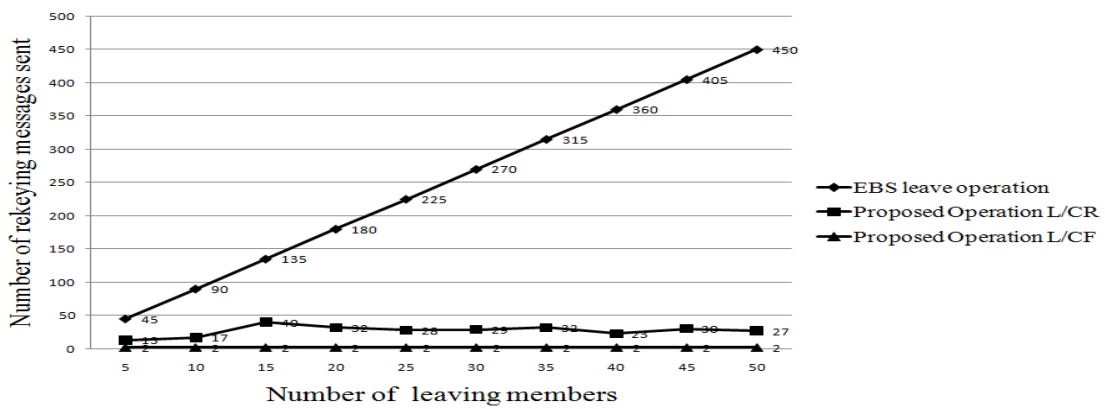


Figure 13. Number of rekeying messages sent

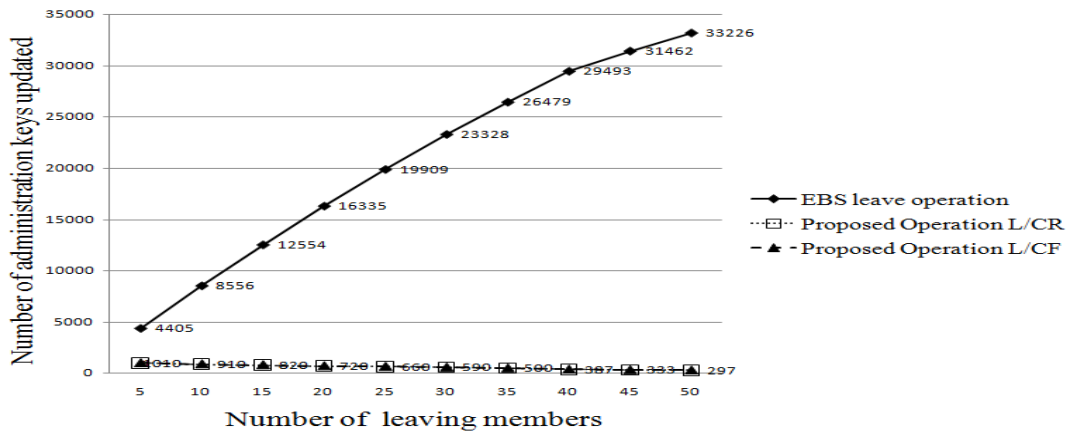


Figure 14. Number of administration keys updated

4.6 Conclusion

In this dissertation, a batch rekeying scheme based on EBS has been proposed. In operation join, KS makes it easy to deliver session keys to existing group members. In operation L/CR, the K-map method is used to reduce the number of rekeying messages required to deliver SK' to existing group members. By doing this, each group member can obtain SK' easily by performing decryptions using a subset of their own administration keys. In operation L/CF, a modified CRT is used to protect session key and only group members can derive this key. Session key protection is guaranteed. Moreover, operation L/CF can withhold collusion attack from departed members. Security analysis indicates that the proposed scheme is secure with respect to collusion attacks. The proposed scheme outperforms EBS. Also, the proposed scheme has been shown to be efficient and scalable, especially in a large group communications environment.

Chapter 5 A Two-Key Agreement Based Supervising Mechanism for Cluster-Based Peer-to-Peer Applications

Peer-to-Peer (P2P) technologies are developing rapidly and have gained popularity. The application of P2P to areas such as file sharing, collaborative business environment, and distributed computing requires secure communication among the nodes. Cluster-based P2P structure provides an efficient way to do file sharing and distributed computing. A key agreement protocol is a set of communication rules whereby two users establish a shared common key. The shared key is used by users in the future communications. Supervising service for governing communications between two nodes is an important topic, especially in the area of government affairs. The proposed mechanism provides a framework for supporting a supervising mechanism in cluster-based P2P networks in WANs. The proposed mechanism is based on the concept of two-key agreement protocol. This mechanism uses the idea of hash-based two-key agreement protocol which helps the nodes in higher level supervise the nodes in lower level in cluster-based P2P communication environment. In the proposed mechanism, a global clusterhead supervises the whole network; clusterheads in each cluster supervise their own clusters' communications. Security analysis shows that the proposed mechanism is secure enough to P2P communications in cluster-based WANs. Any two nodes within the same cluster generate their common session key for the future communications. In the same cluster, no nodes gain this session key except the clusterhead. Moreover, there are only two kinds of operations, hash operation and XOR operation, in the proposed mechanism. Hence, the proposed mechanism provides an efficient way to supervise the P2P network.

5.1 Supervising Introduction

With the rapid development of Peer-to-Peer (P2P) technology, it is widely used in the fields of file sharing, collaborative business environment, and distributed computing. P2P systems are emerging as a new paradigm. A node in P2P plays two roles: a service requester and a service provider. The nodes exchange their files and information by P2P technology. A number of cluster-based P2P protocols have been

proposed by different research groups recently [5][11][20][24]. There are many ways to decompose the network into disjoint clusters. For example, in [5], they used the concept of semantic proximity that exploits the file exchange patterns exhibited among peer users to partition the network into clusters. The benefit of clustering technology to P2P applications is reducing the average hop distance among nodes. Hence, Cluster-based structure provides an efficient way to do file sharing and distributed computing. [5] illustrates one of the methods to form the clusters. They use the method that the probability that a node finds content within its own cluster is maximized but the probability of finding this content in other clusters is minimized to construct clusters in P2P networks. Security issues are important in cluster-based P2P networks. Supervising file sharing and communications among peers is an important security topic. However, current research in cluster-based P2P networks does not propose a way to deal with this security issue.

Supervising is one of the access control mechanisms. A supervisor supervises the communications among nodes whose security level is lower than him/her. The concept of the supervising idea is especially important for government networks. Two-key agreement protocols allow peer nodes to generate a common session key by themselves. The key is used to encrypt communication data between nodes. In general, there are two ways to generate a common session key between two communication nodes: centralized and key agreement protocols. In centralized protocols, a key server generates a common session key and distributes this key to the users after identifying their identities. However, centralized based key management protocol easily suffers from single point failure and performance problems. On the other hand, a key agreement protocol is an alternative way to do key management. By this way, peer nodes generate their common session keys by themselves without the key server's help. Consequently, the problems in centralized protocols is hardly happens.

In this dissertation, a two-key agreement based supervising mechanism is proposed. The mechanism supports any two nodes within the same cluster communicate with each other and no other nodes overhear their communications other than the clusterhead of their domain and the global clusterhead. The proposed mechanism is designed for cluster-based applications in P2P for NTDR clustering WANs. The proposed two-key agreement supervising mechanism is an extension of [56][60]. In their researches, both a tamper-proof chip and hash operations are used to generate

nodes' common session key. Furthermore, in [56], they designed supervising-based key agreement protocol. However, their paper only discussed a single chain partial order supervising problem. In the proposed P2P network scenario, there are many clusters, each clusterhead supervises their cluster domain's communications and a global clusterhead supervises the whole network. Thus, the supervising mechanism must support the multiple chains partial order supervising requests. The proposed two-key agreement based supervising mechanism accommodates peer nodes with governing network and secure communications. Security analysis shows that the proposed mechanism supports the security requirements and guarantees only the supervisors overlook their communications.

The remainder of this chapter is organized as follows: In section 5.2, related works are discussed. The proposed mechanism is detailed in section 5.3. In section 5.4, security analysis is given. In the last section, conclusion is presented.

5.2 Related Works

In this section, the concept of tamper-proof based two-key agreement protocol is briefly discussed.

Key agreement is an important topic in the design of secure communications. A key agreement protocol is a protocol that supports a group of users cooperatively generates their common session keys. By this session key, they encrypt messages using symmetric algorithms and send encrypted messages to other nodes.

Leighton and Micali [19] first proposed key agreement protocol which is based on the tamper-proof hardware and a one-way hash function. However, this protocol has a security flaw. The security flaw makes a user who is not a member of two-agreement users but learns the same session key. Based on the concept of Leighton and Micali, Zheng [60] proposed a method to overcome the security issue in [19]. He generates a public key vector for each user. The elements in every public vector do not totally dominate any one of other public key vectors. Based on [60], Wu and Wu [56] proposed a supervising secure communication protocol for level-based hierarchy. In their protocol, any user in higher level supervises the pairwise communications in the lower level. The protocol is proved to be a secure protocol. However, this protocol is only used for single chain partial order hierarchy.

Based on their concepts, the proposed mechanism extends supervising two-key

agreement protocol for cluster-based multiple chain partial order hierarchy P2P network applications.

5.3 The Proposed Supervising Mechanism

In this section, a two-key agreement based supervising mechanism is proposed. The proposed mechanism is an extension of [56] and [60] and provides supervising abilities. The supervising abilities allow the clusterheads and a global clusterhead supervising communications over peers. Under the same cluster, hash operations are used to generate a common session key for two communication nodes. To prevent illegal file sharing among users in P2P network, both a clusterhead and a global clusterhead are designated to supervise the communications between nodes. They play two roles: a coordinator for controlling file sharing and a supervisor for governing communications. Figure 15 illustrates the framework of the two-key agreement based supervising mechanism.

There are three phases in the proposed mechanism, they are: initialization phase, communication phase, and supervising phase are supported. In addition, the proposed mechanism has the same assumption as described in [60], i.e., a tamper-proof hardware in each node. Here, the tamper-proof chip such as Clipper contains a Law Enforcement Agency Field (LEAF), which provides the authorizers with a certification. To prevent users to delete the LEAF, the Clipper will not decrypt a message if the LEAF is not embedded in the ciphertexts.

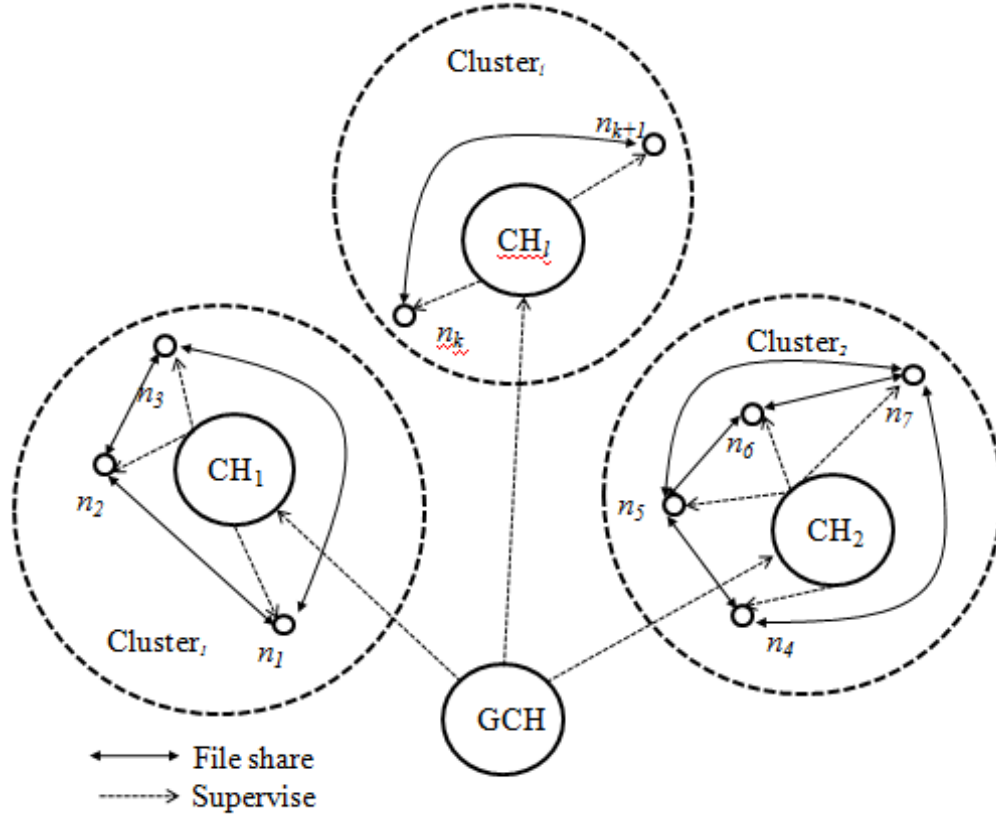


Figure 15. The framework of the two-key agreement based supervising mechanism

5.3.1 Notations

- GCH : a global clusterhead, a manager managing the whole network, and supervises the communications in the network.
- CH : a group clusterhead set, $\{CH_1, CH_2, \dots, CH_t\}$, where CH_i , $i = 1, 2, \dots, t$, is the i^{th} clusterhead in the i^{th} cluster. They are used to manage the intra-network and supervise the peer communications in this domain.
- U_j : a user j belongs to cluster i , CH_i .
- PW_{GCH} : the secret key stored in GCH .
- PW_{CH_i} : the secret key stored in CH_i . This key is generated by GCH .
- r_{GCH} : a random number generated by GCH . Its length is the same as PW_{GCH} .
- r_{CH_i} : a random number generated by CH_i . Its length is the same as PW_{CH_i} .
- $\{PK_{CH_1}, PK_{CH_2}, \dots, PK_{CH_t}\}$: a row vector with t elements. This vector is CH_i 's

public key and is generated by GCH .

- $\{PK_{U_{ij}1}, PK_{U_{ij}2}, \dots, PK_{U_{ij}t}\}$: a row vector with t elements. This vector is U_{ij} 's public key and is generated by CH_i .
- X : a value generated by GCH . It is used to generate $\{h^{PK_{CH_{i1}}}(X), h^{PK_{CH_{i2}}}(X), \dots, h^{PK_{CH_{it}}}(X)\}$.
- X_{CH_i} : a value generated by CH_i . It is used to generate $\{h^{PK_{U_{ij}1}}(X_{CH_i}), h^{PK_{U_{ij}2}}(X_{CH_i}), \dots, h^{PK_{U_{ij}t}}(X_{CH_i})\}$.
- $\{h^{PK_{CH_{i1}}}(X), h^{PK_{CH_{i2}}}(X), \dots, h^{PK_{CH_{it}}}(X)\}$: a row vector with t elements. This vector is CH_i 's private key and is generated by GCH .
- $\{h^{PK_{U_{ij}1}}(X_{CH_i}), h^{PK_{U_{ij}2}}(X_{CH_i}), \dots, h^{PK_{U_{ij}t}}(X_{CH_i})\}$: a row vector with t elements. This vector is U_{ij} 's private key and is generated by CH_i .
- N_i : a random nonce generated by CH_i . The nonce keeps the system from replay attack.
- $k_{i,j}$: the common session key between node i and node j .
- $h^k(\bullet)$: execute hash operations k times, i.e., $h^k(\bullet) = h(h^{k-1}(\bullet))$.
- \oplus : an XOR operation. Its inputs are two bit patterns of equal length.
- $MAC_k(m)$: a message authentication code used to authenticate a message m . Its inputs are a secret key k and an arbitrary-length message m .
- ID_{GCH} : the identity of GCH .
- ID_{CH_i} : the identity of CH_i .
- N_i : a random number generated by CH_i . This values is used to keep the freshness of X_{CH_i} and prevent replay attack.
- N_i' : a random number generated by U_{i1} . This values is used to keep the freshness of the communication data between U_{i1} and U_{i2} and prevent replay attack.
- N_i'' : a random number generated by CH_i . This values is used to keep the freshness of the communication data between CH_i and CH_j and prevent

replay attack.

5.3.2 Initialization phase

According to cluster-based P2P data sharing applications, nodes are completely partitioned into clusters. In this phase, we assume a group of l public key and private key pairs for clusterheads and a group of m public key and private key pairs for users in any clusters are formed. The initialization phase has two parts: GCH generates CH 's public key and private key pairs and another one is U_{ij} 's public key and private key pairs generation. This phase is described as follows:

(1) CH 's public key and private key pairs generation:

- Step 1: GCH generates a public key vector $\{PK_{CH_1}, PK_{CH_2}, \dots, PK_{CH_l}\}$ for each $CH_i, \forall i = 1, 2, \dots, l$.
- Step 2: GCH computes $X = h(PW_{GCH} \oplus r_{GCH})$.
- Step 3: GCH generates a private key vector $\{h^{PK_{CH_1}}(X), h^{PK_{CH_2}}(X), \dots, h^{PK_{CH_l}}(X)\}$ for each $CH_i, \forall i = 1, 2, \dots, l$.
- Step 4: GCH delivers public key pairs to all CH s and injects private key pairs into tamper-proof chips, then sends them to each CH_i .

This dissertation notices that in step1, the public key pairs for each CH_i , no public key vector totally dominates others. In other words, $\forall i, j; i \neq j; \exists V(PK_{CH_k}) > V(PK_{CH_j}); \forall k = 1, 2, \dots, l$. Definition 5.1 defines the meaning of totally domination.

Definition 5.1: A vector V_i totally dominates a vector V_j if and only if all elements in V_i are larger than those in V_j .

(2) U_{ij} 's public key and private key pairs generation:

- Step 1: CH_i generates a public key vector $\{PK_{U_{ij1}}, PK_{U_{ij2}}, \dots, PK_{U_{ijm}}\}$ for each $U_{ij}, \forall j = 1, 2, \dots, m$.
- Step 2: CH_i computes $X_{CH_i} = h(r_{CH_i} \oplus PW_{CH_i})$.
- Step 3: CH_i generates $(ID_{CH_i}, ID_{GCH}, N_i, E_{PW_{CH_i}}(r_{CH_i}), MAC_{PW_{CH_i}}(h(ID_{CH_i} || ID_{GCH} || N_i || r_{CH_i})))$ and then delivers

this message to GCH . The purpose of this step is to help GCH supervise the nodes' communications in some specific cluster. Given a parameter, $E_{PW_{CH_i}}(r_{CH_i})$, GCH could compute X_{CH_i}' by executing decryption operation and then a combination of hash and XOR operation, i.e. $h(r_{CH_i} \oplus PW_{CH_i})$. Thus, GCH successfully supervises the nodes' communications.

- Step 4: CH_i generates a private key vector $\{h^{PK_{U_{j1}}}(X_{CH_i}'), h^{PK_{U_{j2}}}(X_{CH_i}'), \dots, h^{PK_{U_{jm}}}(X_{CH_i}')\}$ for each U_{ij} , $\forall j = 1, 2, \dots, m$.
- Step 5: CH_i delivers public key pairs to U_{ij} s and injects private key pairs into tamper-proof chips, then sends them to each U_{ij} .

This dissertation notices that in step1, the public key pairs for each U_{ij} , no vector totally dominates the other ones. In other words, $\forall j, k; j \neq k; \exists! V(PK_{U_{jd}}) > V(PK_{U_{kd}}); \forall d = 1, 2, \dots, m$.

5.3.3 Communication Phase

In this phase, peer nodes in the same cluster communicate with each other and share their files. Moreover, clusterheads also communicate with each other. Theorem 5.1 proofs that any two nodes in the same cluster generate their common session key by themselves.

Theorem 5.1: If two nodes, U_{i1} and U_{i2} , belong to the same cluster i , they have the ability to generate their common session by themselves, i.e. $k_{i,12} = k_{i,21}$.

Proof:

- (1) We assume without loss of generality that $ID_{i2} > ID_{i1}$, then

$$k_{i,12} = h(h^{\delta_1}(h^{PK_{U_{i11}}}(X_{CH_i}')) || h^{\delta_2}(h^{PK_{U_{i12}}}(X_{CH_i}')) || \dots || h^{\delta_i}(h^{PK_{U_{i1i}}}(X_{CH_i}')) || ID_{i2} || ID_{i1} || N_i')$$

- (2) If $PK_{U_{i1j}} \geq PK_{U_{i2j}}$, for any j , then

$$h^{\delta_j}(h^{PK_{U_{i1j}}}(X_{CH_i}')) = h^{PK_{U_{i1j}}}(X_{CH_i}'); \text{ and } h^{\delta_j}(h^{PK_{U_{i2j}}}(X_{CH_i}')) = h^{PK_{U_{i1j}} - PK_{U_{i2j}}}(h^{PK_{U_{i2j}}}(X_{CH_i}')) = h^{PK_{U_{i1j}}}(X_{CH_i}')$$

- (3) If $PK_{U_{i1j}} < PK_{U_{i2j}}$, for any j , then

$$h^{\delta_j}(h^{PK_{U_{1j}}}(X_{CH_i})) = h^{PK_{U_{2j}} - PK_{U_{1j}}}(h^{PK_{U_{1j}}}(X_{CH_i})); \text{ and } h^{g_j}(h^{PK_{U_{2j}}}(X_{CH_i})) = (h^{PK_{U_{2j}}}(X_{CH_i})) \\ = h^{PK_{U_{2j}}}(X_{CH_i})$$

(4) By 2 and 3, $k_{i,12} = k_{i,21}$ is derived. Q.E.D

The communication phase is described as follows:

(1) Peer nodes', U_{i1} and U_{i2} , common session key $k_{i,12}$ generation:

- Step 1: U_{i1} generates their common session key $k_{i,12}$.

Hash-based operations are used while a common session key is generated. Tamper-proof chip stores user's private key. The identities of U_{i1} and U_{i2} are denoted, respectively, by ID_{i1} and ID_{i2} . A random nonce N_i is also one of the input terms. This value is used to against replay attack. Eq. (5.1) and (5.2) illustrate how U_{i1} generates a common session key, $k_{i,12}$. If $ID_{i1} > ID_{i2}$ is true, then Eq. (5.1) is used; otherwise, Eq. (5.2) is used.

$$k_{i,12} = h(h^{\delta_1}(h^{PK_{U_{i11}}}(X_{CH_i}))) // h^{\delta_2}(h^{PK_{U_{i12}}}(X_{CH_i}))) // \dots // \tag{5.1}$$

$$h^{\delta_i}(h^{PK_{U_{i1i}}}(X_{CH_i}))) // ID_{i1} // ID_{i2} // N_i), \text{ if } ID_{i1} > ID_{i2}$$

$$k_{i,12} = h(h^{\delta_1}(h^{PK_{U_{i11}}}(X_{CH_i}))) // h^{\delta_2}(h^{PK_{U_{i12}}}(X_{CH_i}))) // \dots // \tag{5.2}$$

$$h^{\delta_i}(h^{PK_{U_{i1i}}}(X_{CH_i}))) // ID_{i2} // ID_{i1} // N_i), \text{ if } ID_{i2} > ID_{i1}$$

The value of δ_j , $\forall j = 1, 2, \dots, t$, is determined by the following conditions:

$$\begin{cases} \delta_j = 0, \text{ if } PK_{U_{1j}} \geq PK_{U_{2j}} \\ \delta_j = PK_{U_{2j}} - PK_{U_{1j}}, \text{ if } PK_{U_{1j}} < PK_{U_{2j}} \end{cases}$$

- Step 2: U_{i1} broadcasts $\{ID_{i1} // ID_{i2} // N_i // MAC_{k_{i,12}}(ID_{i1} // ID_{i2} // N_i)\}$.
- Step 3: U_{i2} receives the message in step 2, and then computes common session key by Eq. (5.3) or (5.4). If $ID_{i1} > ID_{i2}$ is true, then Eq. (5.3) is used; otherwise, Eq. (5.4) is used.

$$k_{i,21} = h(h^{g_1}(h^{PK_{U_{i21}}}(X_{CH_i}))) // h^{g_2}(h^{PK_{U_{i22}}}(X_{CH_i}))) // \dots // \tag{5.3}$$

$$h^{g_i}(h^{PK_{U_{2i}}}(X_{CH_i}))) // ID_{i1} // ID_{i2} // N_i), \text{ if } ID_{i1} > ID_{i2}$$

$$k_{i,21} = h(h^{g_1}(h^{PK_{U_{i21}}}(X_{CH_i}))) // h^{g_2}(h^{PK_{U_{i22}}}(X_{CH_i}))) // \dots // \tag{5.4}$$

$$h^{g_i}(h^{PK_{U_{2i}}}(X_{CH_i}))) // ID_{i2} // ID_{i1} // N_i), \text{ if } ID_{i2} > ID_{i1}$$

The value of \mathcal{G}_j , $\forall j = 1, 2, \dots, t'$, is determined by the following conditions:

$$\begin{cases} \mathcal{G}_j = 0, \text{ if } PK_{U_{i2j}} \geq PK_{U_{i1j}} \\ \mathcal{G}_j = PK_{U_{i1j}} - PK_{U_{i2j}}, \text{ if } PK_{U_{i2j}} < PK_{U_{i1j}} \end{cases}$$

- Step 4: U_{i2} verifies the message in step 2 by Eq. (5.5).

$$MAC_{k_{i,12}}(ID_{i1} || ID_{i2} || N_i') = MAC_{k_{i,21}}(ID_{i1} || ID_{i2} || N_i') \quad (5.5)$$

- Step 5: by Theorem 5.1, $k_{i,12} = k_{i,21}$ is guaranteed.

(2) Peer clusterheads', CH_i and CH_j , common session key $k_{i,j}$ generation:

- Step 1: CH_i generates common session key $k_{i,j}$.

Hash-based operations are used for generating their common session key. Tamper-proof chip stores clusterhead's private key. The identities of CH_i and CH_j are denoted, respectively, by ID_i and ID_j . A random nonce N_i'' is also one of the input terms. The same, this value is used to against replay attack. Eqs. (5.6) and (5.7) illustrate how CH_i generates a common session key, $k_{i,j}$. If $ID_i > ID_j$ is true, then Eq. (5.6) is used; otherwise, Eq. (5.7) is used.

$$k_{i,j} = h(h^{\delta_1}(h^{PK_{U_{i1}}}(X)) || h^{\delta_2}(h^{PK_{U_{i2}}}(X)) || \dots || h^{\delta_t}(h^{PK_{U_{it}}}(X)) || ID_i || ID_j || N_i''), \text{ if } ID_i > ID_j \quad (5.6)$$

$$k_{i,j} = h(h^{\delta_1}(h^{PK_{U_{i1}}}(X)) || h^{\delta_2}(h^{PK_{U_{i2}}}(X)) || \dots || h^{\delta_t}(h^{PK_{U_{it}}}(X)) || ID_j || ID_i || N_i''), \text{ if } ID_j > ID_i \quad (5.7)$$

The value of δ_d , $\forall d = 1, 2, \dots, t$, is determined by the following conditions:

$$\begin{cases} \delta_d = 0, \text{ if } PK_{U_{id}} \geq PK_{U_{jd}} \\ \delta_d = PK_{U_{jd}} - PK_{U_{id}}, \text{ if } PK_{U_{id}} < PK_{U_{jd}} \end{cases}$$

- Step 2: CH_i broadcasts $\{ID_i || ID_j || N_i'' || MAC_{k_{i,j}}(ID_i || ID_j || N_i'')\}$.
- Step 3: CH_j receives the message in step 2, and then computes common session key by Eq. (5.8) or (5.9). If $ID_i > ID_j$ is true, then Eq. (5.8) is used; otherwise, Eq. (5.9) is used.

$$k_{j,i} = h(h^{g_1}(h^{PK_{U_j^1}}(X)) || h^{g_2}(h^{PK_{U_j^2}}(X)) || \dots || h^{g_t}(h^{PK_{U_j^t}}(X)) || ID_i || ID_j || N_i''), \text{ if } ID_i > ID_j \quad (5.8)$$

$$k_{j,i} = h(h^{g_1}(h^{PK_{U_j^1}}(X)) || h^{g_2}(h^{PK_{U_j^2}}(X)) || \dots || h^{g_t}(h^{PK_{U_j^t}}(X)) || ID_j || ID_i || N_i''), \text{ if } ID_j > ID_i \quad (5.9)$$

- Step 4: U_j verifies the message in step 2 by Eq. (5.10).

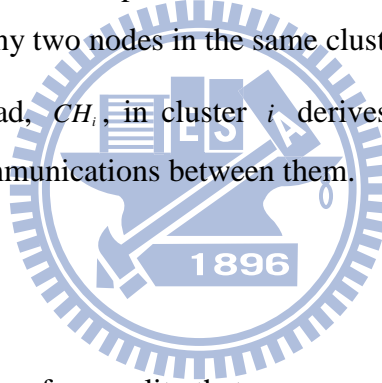
$$MAC_{k_{i,j}}(ID_i || ID_j || N_i'') \stackrel{?}{=} MAC_{k_{j,i}}(ID_i || ID_j || N_i'') \quad (5.10)$$

- Step 5: by Theorem 5.1, $k_{i,j} = k_{j,i}$ is guaranteed.

5.3.4 Supervising Phase

This phase demonstrates that any clusterhead supervises the peer nodes' communications in its cluster and the global clusterhead supervises the whole communications. Theorem 5.2 proofs that a clusterhead supervises the communications between any two nodes in the same cluster.

Theorem 5.2: A clusterhead, CH_i , in cluster i derives U_{i1} and U_{i2} 's session key $k_{i,12}$ and supervises the communications between them.



Proof:

- (1) We assume without loss of generality that $ID_{i2} > ID_{i1}$, then

$$k_{i,12} = h(h^{\delta_1}(h^{PK_{U_{i1}^1}}(X_{CH_i})) || h^{\delta_2}(h^{PK_{U_{i1}^2}}(X_{CH_i})) || \dots || h^{\delta_t}(h^{PK_{U_{i1}^t}}(X_{CH_i})) || ID_{i2} || ID_{i1} || N_i')$$

- (2) CH_i computes their session key by Eq. (5.11)

$$k_{i,12} = h(h^{\xi_1}(X_{CH_i}') || h^{\xi_2}(X_{CH_i}') || \dots || h^{\xi_t}(X_{CH_i}') || ID_{i2} || ID_{i1} || N_i') \quad (5.11)$$

; where $\xi_j = \max(PK_{U_{i1j}}, PK_{U_{i2j}})$, $\forall j = 1, 2, \dots, t$.

- (3) Recall that the proof steps 2 and 3 in Theorem 5.1, the number of hash operations must be done is determined by $\max(PK_{U_{i1j}}, PK_{U_{i2j}})$, $\forall j = 1, 2, \dots, t$. Therefore, CH_i supervises the communications between U_{i1} and U_{i2} . Q.E.D

The supervising phase is described as follows:

(1) A clusterhead, CH_i , in cluster i supervises the communications between U_{i1} and U_{i2} :

- Step 1: CH_i gets a random nonce N_i' from U_{i1} 's broadcast message

$$\{ID_{i1} || ID_{i2} || N_i' || MAC_{k_{i,12}}(ID_{i1} || ID_{i2} || N_i')\}.$$

- Step 2: CH_i calculates U_{i1} and U_{i2} 's common session key $k_{i,12}$ by Eq. (5.12) if $ID_{i1} > ID_{i2}$ or Eq. (5.13) if $ID_{i2} > ID_{i1}$.

$$k_{i,12} = h(h^{\xi_1}(X_{CH_i'}) || h^{\xi_2}(X_{CH_i'}) || \dots || h^{\xi_i}(X_{CH_i'}) || ID_{i1} || ID_{i2} || N_i') \quad (5.12)$$

$$k_{i,12} = h(h^{\xi_1}(X_{CH_i'}) || h^{\xi_2}(X_{CH_i'}) || \dots || h^{\xi_i}(X_{CH_i'}) || ID_{i2} || ID_{i1} || N_i') \quad (5.13)$$

- Step 3: CH_i successfully supervises the communications between U_{i1} and U_{i2} by step 2 and Theorem 5.2.

(2) A global clusterhead, GCH , supervises the communications between CH_i and CH_j by:

- Step 1: GCH gets a random nonce N_i'' from CH_i 's broadcast message

$$\{ID_i || ID_j || N_i'' || MAC_{k_{i,j}}(ID_i || ID_j || N_i'')\}.$$

- Step 2: GCH calculates CH_i and CH_j 's common session key $k_{i,j}$ by Eq. (5.14) if $ID_i > ID_j$ or Eq. (5.15) if $ID_j > ID_i$.

$$k_{i,j} = h(h^{\xi_1}(X) || h^{\xi_2}(X) || \dots || h^{\xi_i}(X) || ID_i || ID_j || N_i'') \quad (5.14)$$

$$k_{i,j} = h(h^{\xi_1}(X) || h^{\xi_2}(X) || \dots || h^{\xi_i}(X) || ID_j || ID_i || N_i'') \quad (5.15)$$

- Step 3: GCH successfully supervises the communications between CH_i and CH_j by step 2 and Theorem 5.2.

(3) A global clusterhead, GCH , supervises the communications between U_{i1} and U_{i2} :

- Step 1: GCH gets a random nonce N_i' from U_{i1} 's broadcast message

$$\{ID_{i1} || ID_{i2} || N_i' || MAC_{k_{i,12}}(ID_{i1} || ID_{i2} || N_i')\}.$$

- Step 2: GCH decrypts $E_{PW_{CH_i}}(r_{CH_i})$ to get the value r_{CH_i}' .

- Step 3: GCH verifies the validity of $MAC_{PW_{CH_i}}(h(D_{CH_i} || ID_{GCH} || N_i' || r_{CH_i}'))$ by Eq.

(5.16).

$$MAC_{PW_{CH_i}}(h(D_{CH_i} || ID_{GCH} || N_i || r_{CH_i})) = MAC_{PW_{CH_i}}(h(D_{CH_i} || ID_{GCH} || N_i || r_{CH_i}')) \quad (5.16)$$

- Step 4: GCH computes X_{CH_i}' by $h(r_{CH_i} \oplus PW_{CH_i})$.
- Step 5: GCH successfully supervises communications between U_{i1} and U_{i2} .

5.4 Security Analysis

In this section, security analysis about the proposed two-key agreement based supervising mechanism is discussed.

5.4.1 The Security of Nodes' Private Keys

The private keys of both clusterheads and users are generated and injected into their temper-proof chips. These chips prevent anyone from gaining access. In addition, it is also impossible to derive the clusterheads' or users' private keys from their corresponding public key vectors. This is because:

- (1) For a clusterhead CH_i , its private key vector, $\{h^{PK_{CH_{i1}}}(X), h^{PK_{CH_{i2}}}(X), \dots, h^{PK_{CH_{in}}}(X)\}$, is computed by one-way hash function with two parameters: CH_i 's public key vector and X . However, X is computed from $h(PW_{GCH} \oplus r_{GCH})$ and is changed when a new session is started. Hence, anyone cannot compute X without knowing GCH 's secret key and the random number r_{GCH} .
- (2) The same, for a user U_{ij} , its private key vector, $\{h^{PK_{U_{ij}1}}(X_{CH_i}'), h^{PK_{U_{ij}2}}(X_{CH_i}'), \dots, h^{PK_{U_{ij}n}}(X_{CH_i}')\}$, is computed by one-way hash function with two parameters: U_{ij} 's public key vector and X_{CH_i}' . However, X_{CH_i}' is computed from $h(r_{CH_i} \oplus PW_{CH_i})$ and is changed when a new session is started. Hence, anyone cannot compute X_{CH_i}' without knowing CH_i 's secret key and the random number r_{CH_i} .

Therefore, these private keys are protected by the proposed mechanism.

5.4.2 The Confidentiality of Communication Data

In the proposed mechanism, any two legal users in the same cluster generate their common session key. By this key, they communicate with each other and share their resources. Anyone who is not a clusterhead in the same cluster or a GCH , he/she does

not have such ability to compute their session key. This is because:

- (1) The private key of a user is kept in a tamper-proof chip, no one has the right to access and modify it.
- (2) All of public keys in the same cluster are generated by the clusterhead. Each public key is presented in the form of a public key vector with t elements. Each of them does not totally dominate the other ones. Therefore, anyone who is not the real one does not have the ability to generate the same session key.
- (3) The same, all public keys in each clusterhead are generated by a global clusterhead. Each public key is presented in the form of a public key vector with t elements. Each of them does not totally dominate the other ones. Therefore, anyone who is not the real one does not have the ability to generate the same session key.

5.4.3 Against Replay Attack

Replay attack is a kind of security attack. In this attack, the attacker reuses some messages sent by sender site or receiver site. Either sender or receiver site does not identify the message sent by an attacker is not a new one. An attacker gathers more information about their communications.

The proposed mechanism uses some random nonces, e.g. r_{GCH} , r_{CH_i} and N_i , are used to keep the private keys' freshness in each session, and e.g. N_i' and N_i'' in each transcript, are used to keep the freshness of communication data. Moreover, a MAC-based message authentication protocol is used to help receiver verify the messages. Hence, the proposed mechanism provides against replay attack.

5.4.4 Against Session Key Attack

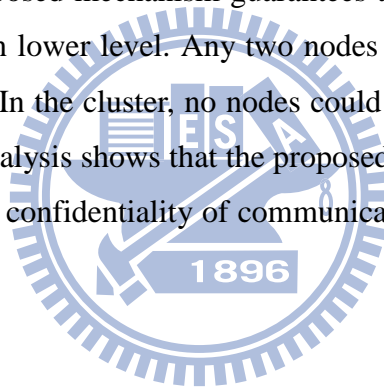
Session key attack is a kind of security of attack. In this attack, the attacker tries to get the common session keys among the users. Having a common session key, the attacker could supervise users' communications.

In this paper, no public key vector totally dominates others. The value of any common session key is unique. This key is generated exclusively by two communication users except the clusterhead or the global clusterhead. Therefore, if an attacker who is not in the same cluster, then he/she does not have a private key vector in his/her tamper-proof chip and he/she could not get the session key; if an attacker

who is in the same cluster, because of the property of each user's public key vector, he/she still could not get the session key belonging to other two users. Hence, the proposed mechanism provides against session key attack.

5.5 Conclusion

In this dissertation, a two-key agreement based supervising mechanism is proposed for cluster-based P2P applications. The mechanism is used to help clusterheads in their clusters supervise the communications between peer nodes and help a global cluster supervise the whole network communications. Any two nodes or two clusterheads in the same cluster or different clusters generate their common session key by themselves. The procedure of session key generation is based on hash operations and a tamper-proof device. There are three phases in the proposed mechanism: initialization phase, communication phase, and supervising phase. By these three phases, the proposed mechanism guarantees that only the nodes in higher level supervise the nodes in lower level. Any two nodes in the same cluster generate their common session key. In the cluster, no nodes could gain this session key except the clusterhead. Security analysis shows that the proposed mechanism supports nodes' private keys protection, the confidentiality of communication data, and against replay attack.



Chapter 6 A Flexible Access Control Mechanism for Web Services

Role-Based Access Control (RBAC) is a kind of access control which assigns the access privilege to a role. The extensible access control markup language (XACML) is a standard access control language for web services. Current XACML only supports the RBAC model or an extension of RBAC, like geographic-based RBAC. However, reputation information about the requester and the trust value of routing path, etc., are also the important factors while designing a flexible access control mechanism for web services. This dissertation introduces an access control mechanism called flexible access control. Flexible access control is designed to enable access control while a requester asks for services from the web server. Flexible access control is a combination of the requester's role, location, reputation, and the trust degree of the routing path. By this mechanism, the service provider easily calculates the requester's access privilege with respect to a specific resource. If a requester is in an unsecure network domain, the routing path is not trusted by the service provider, or the requester's reputation is significantly low, the requester's access privilege will be less than the role which was initially assigned. This dissertation implements this mechanism using XACML. The implementation results show that the proposed mechanism is feasible. Flexible access control thus incorporates the advantages of both the role-based access control model and a user profile-based access control model.

6.1 Introduction

Service-oriented Architecture (SOA) is emerging as a new software development paradigm and introduced by recent research. Nowadays, security is an essential issue and a relevant requirement for any distributed application, and in particular for those enabled by the Web. Web service security encompasses several requirements: integrity, confidentiality, and availability. Web service security methods have been recently developed and are under development by various standardizations bodies, e.g. OASIS (Organization for the Advancement of Structured Information Standards); standards include: Web Service Security (WSS), which encompasses a large number of components addressing various security aspects; XACML [31][31], which is related

to access control and has been recently extended with a profile for Web services access control. For access control, different models of access control have been proposed over the years, for instance, Role-Based Access Control model (RBAC) [43] and Spatially Aware RBAC model (GEO-RBAC) [4][26]. The main advantage of RBAC over other access control models is the ease of security administration. In the RBAC model, access permissions are not assigned directly to the users but to the roles. Users are assigned to different roles and indirectly receive the relevant permissions. Current XACML only supports the RBAC model or an extension of RBAC which uses a geographic component. However, reputation information about the requester and the trust value of routing path, etc., are important factors while designing a flexible and feasible access control mechanism for web services. Therefore, designing a mechanism such as the RBAC model adapted to the web service environment is an important issue. In a mobile network environment, users roam randomly; hence, the users' histories of behavior with other users and web services must be kept and feedback sent to the access control system. Reputation is used to estimate the trustworthiness of peers and prevent illegal actions from spreading via untrustworthy peers. In a trust management system, feedback provides an efficient and effective way to build reputation-based trust relationships among peers [23].

This dissertation outlines a framework for implementing a flexible access control mechanism for web services by using a combination of the RBAC model and a user profile-based access control model which considers the location, the trust value of the route path, and a requester's reputation as a profile about a specific requester. This dissertation addresses the issue of access control for the purpose of the service provider providing data according to the requester's role and its profile. The access privilege for a requester is a combination of his/her access role and the profile evaluation result. This result is calculated by the requester's location, reputation, and the trust of the routing path. This dissertation has implemented this flexible access control model via a policy specification language, XACML. In addition, the proposed mechanism also implements mutual authentication between the web server and a requester. Implementation results demonstrate that the proposed mechanism dynamically adjusts requester's access privilege in no time.

The remainder of this chapter is organized as follows: In section 6.2, system architecture is described. The proposed mechanism is detailed in section 6.3. In

section 6.4, implementation results are given. In the last section, conclusion is presented.

6.2 System Architecture

In this section, the framework of the proposed flexible access control mechanism is described. Figure 16 illustrates the proposed framework. The system encompasses two security functions: authentication and access control. In the authentication part, the proposed system implements mutual authentication between web server and requester. In the access control part, a new model is introduced. This model incorporates the RBAC model and a user profile-based access control model.

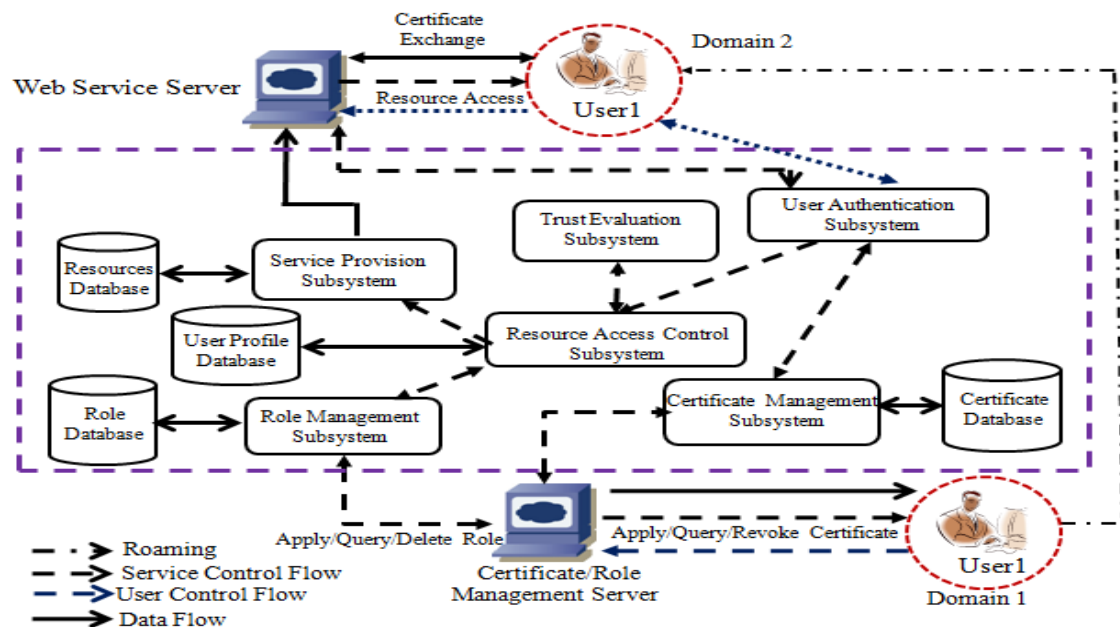


Figure 16. The framework of the proposed flexible access control mechanism

6.2.1 System Components

The system consists of three components: servers, databases, and subsystems. There are two servers in the system. The web server provides all the services requested by the requesters. The certificate/role management server (C-RMS) is used to manage the security requirements for the web services. There are four types of databases. The certificate database (CERTDB) on the C-RMS is used to store the participants' certificates; the role database (ROLEDB) on the C-RMS is responsible for storing the roles associated with the participants; the user profile database

(PROFDB) on the web server is responsible for keeping the records related to the requesters' behavior; and the resources database (RESDB) on the web server is responsible for storing all the resources. In addition, there are six subsystems: the certificate management subsystem (CMS), the role management subsystem (RMS), the user authentication subsystem (UAS), the resource access control subsystem (RACS), the trust evaluation subsystem (TES), and the service provision subsystem (SPS).

- (1) CMS: CMS is used to generate, revoke, and maintain certificates. A new user must register with C-RMS to get his/her certificate. Anyone querying others' certificates from the CERTDB does so via this subsystem. A certificate associated with a specific requester will be revoked if it is lost or expires.
- (2) RMS: Users' roles are assigned after registration. RMS is responsible for generating, deleting, and maintaining the roles with respect to the corresponding users. The RBAC model is used to define the access policies for each role.
- (3) UAS: UAS is used to authenticate the identities of communicators. It provides mutual authentication. It provides mutual authentication when a requester issues an access request to the web server. Both the requester and service provider exchange their certificates and verify the validity of the certificates exchanged. In this way, end to end authentication is confirmed, securing the system against forgery attacks.
- (4) RACS: RACS is responsible for delivering a requester's access request, collecting the trust evaluation information, and sending evaluation results, which may cause an access privilege lower than his/her original, or may deny the access request if this request conflicts with the evaluation result after trust assessment. In addition, XACML is used to store the access policies.
- (5) TES: TES is responsible for determining the requester's reputation value. The reputation value and its functions about the requester are calculated by the number of attacks, the number of failure requests, and the number of large packet deliveries.
- (6) SPS: SPS is used to deliver the resources to the requesters according to the access policies kept in ROLEDB and PRFDB.

6.2.2 The System Workflow

The system workflow of the proposed mechanism has five steps: registration, role assignment, user authentication, resource access control and trust evaluation, and service delivery.

- (1) Step1: Firstly, a user must register with C-RMS to get his/her certificate.
- (2) Step2: The role is assigned according to the user's registration information.
- (3) Step3: The user roams to a new location or domain, and he/she issues a request to access resources in the web service. The SSL-based authentication service is executed for confirming the identities of the two parties. In addition, if the requester has never been assigned a role, then step2 is executed.
- (4) Step4: RACS collects the requester's profile including the requester's information and its location, etc. The subsystem asks the domain brokers that the requester has visited (current and prior) to calculate the requester's reputation information by using TES. RACS calculates the trust value of the requester according to the feedback reputation values from the domain brokers, and the trust values of the domain brokers. RACS writes them into PRFDB and adjusts the requester's access privileges according to the role and trust evaluation result.
- (5) Step5: Web server adjusts the requester's access privileges according to its assigned role and trust evaluation result. SPS sends the resources complying with the current access policy.

6.3 The Proposed Flexible Access Control Mechanism

Both authentication and access control are security issues while designing web services. This section introduces how the proposed dissertation addresses these two areas.

The proposed mechanism supports mutual authentication. Mutual authentication is an authentication protocol which provides bidirectional identity verification. By this method, two communicators are able to confirm the identities of each other. In the proposed mechanism, certificate-based mutual authentication protocol is used. Certificates are exchanged for authentication purposes. These certificates are signed and are verified by C-RMS and anyone.

Access control is an important mechanism which provides the right people with the right access to resources according to predefined access policies. XACML is one of the access control mechanisms, especially for XML security. Current XACML approaches do not consider location information, except GeoXACML [26]. However, the author does not take the reputation and trust value of the routing path into consideration. Therefore, this dissertation introduces a mechanism to incorporate the RBAC model, user profile, and XACML into web services. The locations in the proposed paper are separated by the routing domain. In other words, each cluster is a routing domain. Each domain has a broker to manage the reputation information about the users. Definition 6.1 shows that the network domains are completely separated and disjointed.

Definition 6.1: A group of domain set, $D = \{d_1, d_2, \dots, d_k\}$, where $D = \bigcup_{i=1}^k d_i$ and $d_i \cap d_j = \emptyset$ if $i \neq j$.

In addition, each domain has a domain broker, b_i , used to collect the distributed reputation ratings. A user provides the transaction rating to its broker after every transaction with any service in order to build up the reputation database on all services. All users in the domain return observation results about others. By delegating trust management to brokers, the web service provider only needs to ask the brokers about the reputation of a requester before a transaction with it.

6.3.1 Reputation Management

A reputation management system can be classified by the following groups [58]: Subjective vs. Objective, Transaction-based vs. Opinion-Based, Complete information vs. Localized information, and Rank-based vs. Threshold-based. This dissertation adopts hybrid subjective and objective, transaction-based, hybrid complete and localized information, and threshold-based in designing the reputation system. In addition, a successful reputation system should make it hard to build up good reputation so that a user is less likely to abuse his/her hard-earned reputation.

In this dissertation, there are three reputation functions that must be calculated: the number of attacks (calculated by $F(A)$), the number of failure requests (calculated by $F(FR)$), and the number of large packets delivery (calculated by $F(PD)$). Reputation calculation for a transaction comes from two parts: direct

observation by the domain broker and indirect observation feedback from the domain users. Eq. (6.1) illustrates the reputation calculation for a single transaction about U_i in domain d_i . Eq. (6.2) illustrates the reputation calculation about U_i in domain d_i . Eq. (6.3) illustrates the aggregated reputation about U_i . A threshold value is used to filter the aggregated reputation. If the value of the aggregated reputation is larger than that of the threshold, the web service provider will deny the request.

$$REP_Trans_{U_i}^{d_j} = \alpha_1 \times (F(A) + F(FR) + F(PD)) / 3 + \alpha_2 \times \left(\sum_{U_l \rightarrow U_i, U_l \in d_i \wedge U_l \neq U_i}^{U_l \rightarrow U_i} (F(A) + F(FR) + F(PD)) / 3 \right) / \#U \quad (6.1)$$

; where $\alpha_1 + \alpha_2 = 1$, $U_l \rightarrow U_i$ presents U_l 's observation about U_i , and $F(\cdot) = e^{-q^n}$.

Here, $F(\cdot) \in \{F(A), F(FR), F(PD)\}$. q , a parameter used to adjust the earning reputation ratio, is a value which ranges from 0 to 1. If the value of q approaches 1, it implies that U_i loses his/her reputation rapidly if U_i does something bad. n is a parameter used for counting the number of events in any reputation function.

$$REP_{U_i}^{d_j} = \beta_1 \times REP_Trans_{U_i}^{d_j}(T_{i-1}) + \beta_2 \times REP_Trans_{U_i}^{d_j}(T_i) \quad (6.2)$$

; where $\beta_1 + \beta_2 = 1$

$$AREP_{U_i} = \left(\sum_{V=\{d_j|d_j \in D \wedge REP_{U_i}^{d_j}\}}^{U_i \prec d_j} f \times REP_{U_i}^{d_j} \right) / \#V \quad (6.3)$$

; where $U_i \prec d_j$ implies U_i has visited domain d_j ; f is a fading function, $f = (0.5)^k$. If $k=0$, it implies U_i in current domain; $k=1$, it implies the domain that U_i visited last time, etc.

In addition, the proposed mechanism also takes the trust value of each domain, named RPT_{d_i} hereafter, into consideration. The calculating method for RPT_{d_i} is the same as the one in AREP, except with different functions. In RPT_{d_i} , the trust functions consists of the number of failure packets forwarded (calculated by $F(FPF)$), the number of incorrect routes (calculated by $F(IR)$), and the number of failure protections (calculated by $F(FP)$). Eq. (6.4) illustrates the reputation calculation for a single transaction about d_i by a web service. Eq. (6.5) illustrates the reputation calculation about d_i by a web service.

$$RPT_Trans_{d_i}^{ns} = \alpha_1 \times (F(FPF) + F(IR) + F(FP)/3) + \alpha_2 \times \left(\sum_{D=\{d_i | d_i \in D \wedge d_i \neq d_i\}}^{d_i \rightarrow d_i} (F(FPF) + F(IR) + F(FP)/3) \right) / \#D \quad (6.4)$$

; where $\alpha_1 + \alpha_2 = 1$, $d_i \rightarrow d_i$ presents d_i 's observation about d_i , and $F(\cdot) = e^{-q^{pn}}$.

$$RPT_{d_i}^{ns} = \beta_1 \times RPT_Trans_{d_i}^{ns}(T_{i-1}) + \beta_2 \times RPT_Trans_{d_i}^{ns}(T_i) \quad (6.5)$$

; where $\beta_1 + \beta_2 = 1$.

Finally, the trust value of the routing path, named RPT hereafter, is equivalent to

$$\prod_i RPT_{d_i}.$$

6.3.2 Flexible Access Control

The proposed flexible access control mechanism incorporates the RBAC and user profile-based access control models into a new model, which guarantees that any requester in any domain gains the appropriate access privilege when issuing a resource request. Definitions 6.2 to 6.5, define the relevant relation sets and the relationships among users, roles, and permissions. By these definitions, the access policies are generated and are parsed by XACML.

Definition 6.2: A group of role scheme set, $RS = \{RS_1, RS_2, \dots, RS_m\}$

RS_i is one of the role schemes and corresponds to role r_i . Moreover, $RS_i = \{p_j \mid \text{permission } p_j \text{ is assigned to role } r_i\}$.

Definition 6.3: URA is a relation, $URA \subseteq USERS \times ROLES$, where $USERS = \{U_1, U_2, \dots, U_n\}$ and $ROLES = \{r_1, r_2, \dots, r_t\}$. Relation URA indicates that $UserApplyRole_{v_i}(r_j) = \{U_i \in USERS \mid (U_i, r_j) \in URA\}$.

Definition 6.4: A vector space, PRF , with six tuples, $\{User, Domain, SLV, REP, AREP, RPT\}$ is kept by the web server.

Here, SLV , which ranges from 0 to 1, is the security level of the correspondence domain and determined by the web service provider; REP the reputation information; $AREP$ the aggregated reputation information from the domains where the requester has been; and RPT the trust value of the routing path. Finally, a requester's profile is calculated by Eq. (6.4).

$$\{User, Domain, SLV, REP, AREP, RPT\} \rightarrow ARET \times SLV \times RPT = PRF \quad (6.4)$$

Definition 6.5: PRA is a relation, $PRA \subseteq PRMS \times ROLES \times PRF$. Relation PRA indicates that $PRMSAss_p(r, prf) = \{p \in PRMS \mid (p, r, prf) \in PA\}$.

Here, $ROLES \times PRF$ is a role instance for a user. This definition defines the final permission for a requester while asking for a resource.

6.4 Implementation Results

In this section, both the implementation environment and results are described. The OpenCA project [33] is used to generate, distribute, and maintain certificates. Sun's XACML Implementation [50] is used to parse XACML. The JSP programming language is used to implement the system. Moreover, glassfish v3 is used as a container for web services. Figure 17 illustrates the implementation environment.

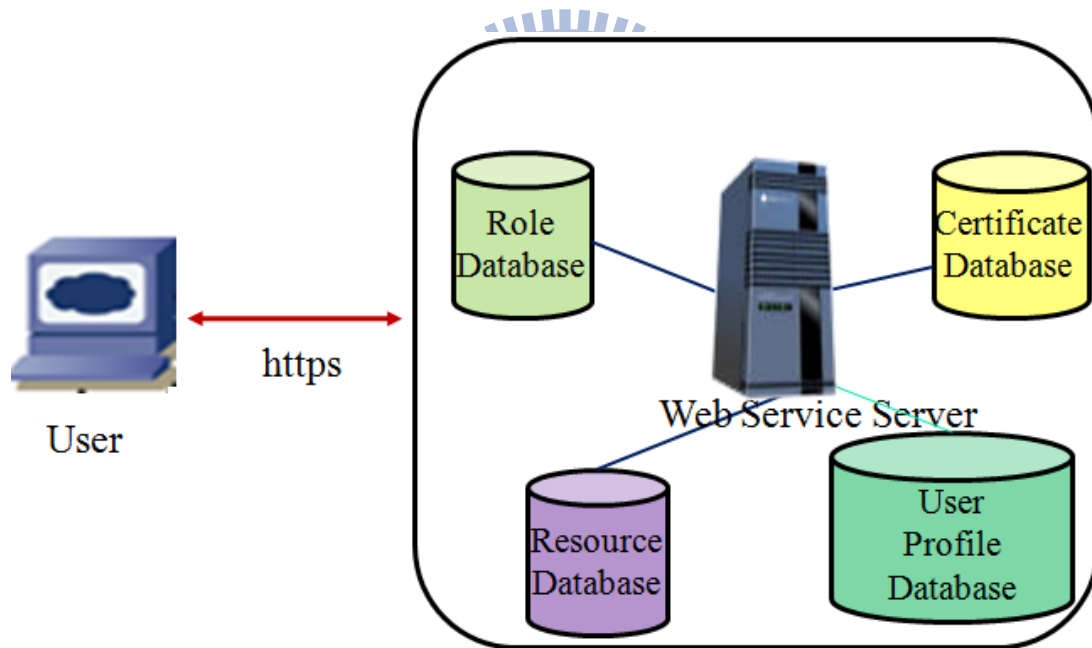


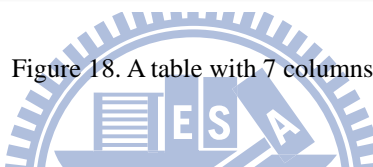
Figure 17. The implementation environment

We assume that there are five domains and twenty users in the environment. Detailed implementation steps are presented in section 6.2.2. Figure 18 illustrates the table which the requester wants to access. In this table, there are seven fields. Figure 19 illustrates the implementation results after applying the RBAC model. This result shows that the requester in the fourth domain could gain access to all the fields in

Human Resource Database except the PWD field. Figure 20 illustrates the implementation results after applying the proposed flexible access control mechanism. The requester now is in the second domain and he/she could gain access to four fields. Obviously, the proposed mechanism has changed the requester's access privilege. Figure 21 illustrates the system denying the requester's request when the reputation value is too low.

name	title	email	tel	mobile	ssc	PWD
Chen, Kuang-Yu	Assistant	ha1802000@hotmail.com	11111111	912111111	1111	123
Ho, Ping-Hsien	Assistant	bsho.iim98g@nctu.edu.tw	33333333	911333333	3333	456
Huang, Chun-Chieh	CEO	chuchieh.iim91g@nctu.edu.tw	44444444	963444444	4444	789
Lee, Fang-Yi	Assistant	cakerap.iim98g@nctu.edu.tw	22222222	934222222	2222	987
Lo, Chi-Chun	COB	cclo@faculty.nctu.edu.tw	55555555	930555555	5555	654

Figure 18. A table with 7 columns



Hi, Hank Now you're in Broker_4

your Role belong to **Role0**, And the Role's right is **AnyResource**

Choose the Database you want, and press "send"

Human Resource Database

name	title	email	tel	mobile	ssc	PWD
Chen, Kuang-Yu	Assistant	ha1802000@hotmail.com	11111111	912111111	1111	
Ho, Ping-Hsien	Assistant	bsho.iim98g@nctu.edu.tw	33333333	911333333	3333	
Huang, Chun-Chieh	CEO	chuchieh.iim91g@nctu.edu.tw	44444444	963444444	4444	
Lee, Fang-Yi	Assistant	cakerap.iim98g@nctu.edu.tw	22222222	934222222	2222	
Lo, Chi-Chun	COB	cclo@faculty.nctu.edu.tw	55555555	930555555	5555	

Figure 19. The columns that the requester can get after applying the RBAC model

**Hi, Hank Now you're in Broker_2
And your "servieRep"=5.0**

your Role belong to **Role0**, And the Role's right is **AnyResource**

Choose the column you want, and press "send"

Human Resource Databse

name	title	email	tel	mobile	ssc	PWD
Chen, Kuang-Yu	Assistant	ha1802000@hotmail.com	11111111			
Ho, Ping-Hsien	Assistant	bsho.iim98g@nctu.edu.tw	33333333			
Huang, Chun-Chieh	CEO	chuchieh.iim91g@nctu.edu.tw	44444444			
Lee, Fang-Yi	Assistant	cakerap.iim98g@nctu.edu.tw	22222222			
Lo, Chi-Chun	COB	cclo@faculty.nctu.edu.tw	55555555			

Figure 20. The columns that the requester can get after applying the flexible access control model

**Hi, Hank Now you're in Broker_0
And your "servieRep"=0.2**

your Role belong to **Role0**, And the Role's right is **AnyResource**

Choose the column you want, and press "send"

Human Resource Databse

Sorry! you're in a **DANGEROUS** place. So you can't read these data!

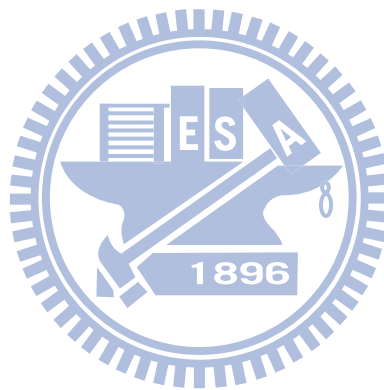
name	title	email	tel	mobile	ssc	PWD
------	-------	-------	-----	--------	-----	-----

Figure 21. The requester's request is denied. (Threshold is 0.3)

6.5 Conclusion

To enable secure web service transactions to occur, an authentication protocol and access control mechanism must be added. This dissertation has shown that mutual authentication and a flexible access control mechanism can create a secure environment for web services. To provide flexible access control, the proposed mechanism integrates the RBAC model and a user profile-based access control model to dynamically adjust the requester's access privileges. A user's profile includes the reputation about the requester in the current domain, the aggregated reputation of the requester, the trust value of the route path, and the security level of the requester's current domain. Each domain has a broker to collect feedback from its users on past

transactions. The web service provider gathers these reputation values from the domains the requester has previously visited. It then determines the final access privilege using the proposed flexible access control mechanism. Finally, the requester receives the resources according to the new access policy. The implementation results show that the proposed mechanism is feasible.



Chapter 7 Conclusion Remarks

7.1 Conclusions

In this dissertation, some security issues under a scenario of DRM in WANs are discussed and the corresponding schemes and mechanisms are proposed. Toward these goals, from chapter 3 to chapter 6, the related schemes and mechanisms are proposed to support these security requirements.

In chapter 3, to guarantee that the digital license provided by the service provider is legal, a group-oriented nominative proxy signature scheme is proposed. The proposed scheme has five phases: the initialization phase, the delegation phase, the proxy key generation phase, the nominative proxy signature generation phase, and the original-nominative proxy signature verification phase. By signature proof and security analysis, the proposed scheme is secure enough to be used for DRM systems.

In chapter 4, to support dynamic secure group communications over WANs, an EBS-based batch rekeying scheme is proposed. The scheme supports three operations, join, leave with collusion-resistant (L/CR), and leave with collusion-free (L/CF). In operation join, KS makes it easy to deliver session keys to existing group members. In operation L/CR, the K-map method is used to reduce the number of rekeying messages required to deliver SK' to existing group members. In operation L/CF, a modified CRT is used to protect session key and only group members can derive this key. Security analysis indicates that the proposed scheme is secure with respect to collusion attacks. The proposed scheme outperforms EBS.

In chapter 5, a two-key agreement based supervising mechanism is proposed for cluster-based P2P applications in WANs. The mechanism helps the clusterheads in their clusters supervise the communications between peer nodes and helps a global cluster supervise the whole network communications. Any two nodes or two clusterheads in the same cluster or different clusters generate their common session key by themselves. There are three phases in the proposed mechanism: initialization phase, communication phase, and supervising phase. By these three phases, the proposed mechanism guarantees that only the nodes in higher level supervise the nodes in lower level. Any two nodes in the same cluster generate their common

session key. In the cluster, no nodes could gain this session key except the clusterhead. Security analysis shows that the proposed mechanism supports nodes' private keys protection, the confidentiality of communication data, and against replay attack.

In chapter 6, a flexible access control mechanism is proposed. The mechanism can create a secure environment for web services. A combination of the RBAC model and a user profile-based access control model is proposed. In the user profile-based access control model, it considers the location, the trust value of the route path, and a requester's reputation as a profile about a specific requester. Therefore, a requester's access right not only depends on the initial assigned role also relies on the user's profile. The implementation results show that the proposed mechanism is feasible.

7.2 Future Research Directions

Two possible future research directions are merited for further investigation. They are:

- (1) How to support the proposed batch rekeying operations on the multiple cluster-based WANs? And, how to support an efficient simplification method when there are many variables in Boolean simplification functions?
- (2) The proposed protocol is two-key agreement protocol. How to support multiple users' key agreement protocol in the same cluster?

References

- [1] Chang, I., Engel, R., Kandlur, D., Pendrakakis, D., and Saha, D., “Key Management for Secure Internet Multicast using Boolean Function Minimization Techniques”, *Proceedings of the Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies(INFOCOM'99)*, Vol. 2, pp. 689-698, New York, NY, USA, March 1999.
- [2] Chiang, C.C., Wu, H.K., Liu, W., and Gerla, M., “Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel”, *In Proceedings of IEEE Singapore International Conference on Networks, SICON'97*, pp. 197-211, Singapore, April 1997.
- [3] Cho, J.H., Chen, I.R., and Eltoweissy, M., “On Optimal Batch Rekeying for Secure Group Communications in Wireless Networks”, *Wireless Networks*, Vol. 14, No. 6, pp. 915-927, December 2008.
- [4] Damiani, M.L., Bertino, E., Catania, B., and Perlasa, P., “GEO-RBAC: A Spatially Aware RBAC”, *ACM Transactions on Information and System and Security (TISSEC)*, Vol. 10, No. 1, pp. 1-34, February 2007.
- [5] Doulamis, N.D., Karamolegkos, P.N., Doulamis, A.N., and Protonotarios, E.N., “Cluster-Based Proactive Replication of Multimedia Files in Peer-to-Peer Networks”, *2nd International Conference on Digital Information management (ICDIM'07)*, Vol. 1, pp. 368-375, Lyon, France, October 2007.
- [6] Eltoweissy, M., Hossain, M., Morales, L., and Sudborough, I.H., “Combinatorial Optimization of Group Key Management”, *Journal of Network and Systems Management*, Vol. 12, No. 1, pp. 33-50, March 2004.
- [7] Foster, I., Kesselman, C., Tsudisk, G., and Tuecke, S., ”A Security Architecture for Computational Grids”, *CCS'98: Proceedings of the 5th ACM Conference on Computer and Communication Security*, pp. 83-92, San Francisco, CA, USA, November 1998.
- [8] Haas, Z. J., Pearlman, M.R., and Samar, P., “The Zone Routing Protocol (ZRP) for Ad-Hoc Networks,” *IETF Draft*, July 2002. (<http://tools.ietf.org/html/draft-ietf-manet-zone-zrp-04>)

- [9] Hwang, S.J. and Shi, C.H., "A Simple Multi-proxy Signature Scheme", *Communications of the CCISA*, Vol. 8, No. 1, pp. 88-92, December 2001.
- [10] Jeong, Y., Yoon, K., and Ryou, J., "A Trusted Key Management Scheme for Digital Rights Management", *The Journal of Electronics and Telecommunications Research Institute (ETRI Journal)*, Vol. 27, No. 1, pp.114-117, February 2005.
- [11] Jia, J. and Meng, C., "A Cluster-Based Peer-to-Peer File Sharing Protocol for Mobile Ad Hoc Networks", *International Symposium on Computer Network and Multimedia Technology*, pp. 1-4 (CD), Wuhan, China, January 2009.
- [12] Jiang, M., Li, J., and Tay, Y.C., "Cluster Based Routing Protocol", *IETF Draft*, August 1999. (<http://tools.ietf.org/html/draft-ietf-manet-cbrp-spec-01>)
- [13] Johnson, D.B. and Maltz, D. A., "Dynamic Source Routing in Ad Hoc Wireless Networks", *Mobile Computing*, Kluwer Academic Publishers, Vol. 353, pp. 153-181, 1996.
- [14] Kim, H., Baek, J., Lee, B., and Kim, K., "Secret Computation with Secrets for Mobile Agent Using One-time Proxy Signature", *In Proceedings of the 2001 Symposium on Cryptography and Information Security (SCIS'01)*, pp. 845-850, Oiso, Japan, January 2001.
- [15] Kim, S.J., Park, S.J., and Won, D.H., "Nominative Signatures", *Proceedings of International Conference on Electronics, Information and Communications (ICEIC'95)*, pp. 68-71, Yanji, Jilin, China, August 1995.
- [16] Kim, S.J., Park, S.J., and Won, D.H., "Zero-knowledge Nominative Signature", *Proceedings of Pragocrypt'96: The first International Conference on the Theory and Applications of Cryptology*, pp. 380-392, Prague, Czech Republic, October 1996.
- [17] Krawczyk, H., Bellare, M., and Canetti, R., "HMAC: Keyed-Hashing for Message Authentication", *RFC 2104*, February 1997. (<http://tools.ietf.org/pdf/rfc2104.pdf>)
- [18] Lee, B., Kim, H., and Kim, K., "Strong Proxy Signature and Its Applications", *In Proceedings of the 2001 Symposium on Cryptography and Information Security (SCIS'01)*, Vol. 2, No. 2, pp. 603-608, Oiso, Japan, January 2001.

- [19] Leighton, F.T. and Micali, S., “Secret-Key Agreement without Public-Key Cryptography”, *Proceedings of the Thirteenth Annual International Cryptology Conference on Advances in Cryptology (Crypto '93)*, Santa Barbara, CA, USA, pp. 456-479, August 1993.
- [20] Liu, N. and Liu, F., “A Bidirectional Ring Cluster-based Peer to Peer System”, *First IEEE International Symposium on Information Technologies and Applications in Education (ISITAE'07)*, pp. 568-571, Kunming, China, November 2007.
- [21] Liu, Q., Reihaneh, S.N., and Nicholas, N.P., “Digital Rights Management for Content Distribution”, *Proceedings of the Australasian Information Security Workshop conference on ACSW frontiers 2003*, Vol. 21, pp. 49-58, Adelaide, South Australia, February 2003.
- [22] Li, X., Yang, Y.R., Gouda, M.G., and Lam, S.S., “Batch Rekeying for Secure Group Communications”, *Proceedings of the Tenth International Conference on World Wide Web*, pp. 525-534, Hong Kong, May 2001.
- [23] Li, X. and Gui, X., “Tree-Trust: A Novel and Scalable P2P Reputation Model Based on Human Cognitive Psychology”, *International Journal of Innovative Computing, Information and Control*, Vol. 5, No. 11(A), pp. 3797-3807, November 2009.
- [24] Li, X. and Wu, J., “Cluster-based Intelligent Searching in Unstructured Peer-to-Peer Networks”, *Proceedings of the 25th IEEE international Conference on Distributed Computing Systems Workshops (ICDCSW'05)*, pp. 642-645, Columbus, Ohio, USA, June 2005.
- [25] Mambo, M., Usuda, K., and Okamoto, E., “Proxy Signatures for Delegating Signing Operation”, *CCS'96: Proceedings of the 3rd ACM Conference on Computer and Communications Security*, pp. 48-57, New Delhi, India, January 1996.
- [26] Matheus, A., “Declaration and Enforcement of Fine Grained Access Restrictions for A Service-based Geospatial Data Infrastructure”, *In Proceedings of the 10th ACM Symposium on Access Control Models and Technologies (SACMAT'05)*, pp. 21–28, Stockholm, Sweden, June 2005.

- [27] Menezes, A.J., Oorschot, P.C.V., and Vanstone, S.A., “Handbook of Applied Cryptography”, *CRC Press*, Boca Raton, Florida, USA, 1996.
- [28] Microsoft DRM,
<http://www.microsoft.com/windows/windowsmedia/forpros/drm>.
- [29] Miller, J.F., Job, D., and Vassilev, V.K., “Principles in the Evolutionary Design of Digital Circuits – Part I”, *Genetic Programming and Evolvable Machines*, Vol. 1, No. 1-2, pp.7-35, April 2000.
- [30] Ng, W.H.D., Cruickshank, H., and Sun, Z., “Scalable Balance Batch Rekeying for Secure Group Communication”, *Computers & Security*, Vol. 25, No. 4, pp. 265-273, June 2006.
- [31] OASIS, eXtensible Access Control Markup Language (XACML),
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml/.
- [32] OMA DRM, <http://www.openmobilealliance.org>.
- [33] OpenCA Labs, <http://www.openca.org/>.
- [34] Park, H.U. and Lee, I.Y., “A Digital Nominative Proxy Signature Scheme for Mobile Communication”, *In Proceedings of the Third International Conference on Information and Communications Security (ICICS'01)*, Lecture Notes in Computer Science 2229, Springer-Verlag, pp. 451-455, Xian, China, November 2001.
- [35] Park, V.D. and Corson, M.S., “A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks”, *Proceedings of Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM'97*, Vol. 3, pp.1405-1413, Kobe, Japan, April 1997.
- [36] Perkins, C.E., “Ad Hoc Networking”, *Addison-Wesley*, Boston, MA, USA, 2001.
- [37] Perkins, C.E. and Bhagwat, P., “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers”, *ACM SIGCOMM: Proceedings of the Conference on Communications Architectures, Protocols and Applications*, pp. 234-244, London, UK, August 1994.

- [38] Perkins, C.E., and Royer, E.M., “Ad-Hoc On-Demand Distance Vector Routing”, *Proceedings of 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90-100, New Orleans, LA , USA , February 1999.
- [39] Rafaeli, S. and Hutchison, D., “A Survey of Key Management for Secure Group Communication”, *ACM Computing Surveys*, Vol. 35, No. 3, pp. 309-329, September 2003.
- [40] Ramanathan, R. and Redi, J., “A Brief Overview of Ad Hoc Networks: Challenges and Directions”, *IEEE Communications Magazine*, Vol. 40, No. 5, pp. 20-22, May 2002.
- [41] Royer, E.M. and Toh, C.K., “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks”, *IEEE Personal Communications*, Vol. 6, No. 2, pp. 46-55, April 1999.
- [42] Ruppe, R. and Griswald, S., “Near Term Digital Radio (NTDR) System”, *Proceedings of the IEEE Military Communications Conference (MILCOM 97)*, Vol. 3, pp. 1282-1287, Monterey, CA, USA, November 1997.
- [43] Sandhu, R.S., Coyne, E.J., Feinstein, H.L., and Youman, C.E., “Role-Based Access Control Models”, *IEEE Computer*, Vol. 29, Issue 2, pp. 38-47, February 1996.
- [44] Setia, S., Koussih, S., Jajodia, S., and Harder, E., “Kronos: A Scalable Group Re-Keying Approach for Secure Multicast”, *Proceedings of IEEE Symposium on Security and Privacy*, pp. 215-228, Berkeley, CA, May 2000.
- [45] Sherman, A.T. and McGrew, D.A., “Key Establishment in Large Dynamic Groups Using One-Way Function Trees”, *IEEE Transactions on Software Engineering*, Vol. 29, No. 5, pp. 444-458, May 2003.
- [46] Stallings, W., “Cryptography and Network Security: Principles and Practices Third Edition”, *Prentice Hall*, New Jersey, USA, 2003.
- [47] Stinson, D.R., “Cryptography Theory and Practice”, *CRC Press*, Boca Raton, Florida, USA, 1995.
- [48] Sun, H.M., “An Efficient Nonrepudiable Threshold Proxy Signatures with Known Signers”, *Computer Communications*, Vol. 22, No. 8, pp. 717-722, May 1999.

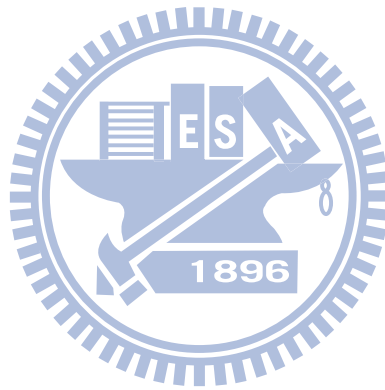
- [49] Sun, H.M., Lee, N.Y., and Hwang, T., “Threshold Proxy Signatures”, *IEE Proceedings of Computers and Digital Techniques*, Vol. 146, No. 5, pp. 259-263, London, UK, September 1999.
- [50] Sun’s XACML Implementation, <http://sunxacml.sourceforge.net/>.
- [51] Tan, Z.W., “Improvement on Nominative Proxy Signature Schemes”, *International Journal of Network Security*, Vol. 7, No. 2, pp. 175-180, September 2008.
- [52] Tan, Z.W. and Liu, Z.J., “Nominative Proxy Signature Schemes”, *Cryptology ePrint Archive: Report 2004/298*, November 2004.
- [53] Welsh, B. and Rehn, N., “Multicasting with the Near Term Digital Radio (NTDR) in the Tactical Internet”, *Proceedings of the IEEE Military Communications Conference (MILCOM 98)*, Vol. 2, pp.452-456, Boston, Massachusetts, USA, October 1998.
- [54] Williams, L. and Emery, L., “Near Term Digital Radio – A First Look”, *Proceedings of the 1996 Tactical Communications Conference*, pp. 423-425, Fort Wayne, IN, USA, May 1996.
- [55] Wong, C.K., Gouda, M., and Lam, S.S., “Secure Group Communications Using Key Graphs”, *IEEE/ACM Transactions on Networking*, Vol. 8, No. 1, pp. 16-30, February 2000.
- [56] Wu, T.S. and Wu, T.C., “Supervising Secure Communications for Level-Based Hierarchy”, *Joint Conference of 1996 International Computer Symposium*, pp. 125-130, Kaohsiung, Taiwan, December 1996.
- [57] Zhang, H., “Threshold Proxy Signature Schemes”, *Proceedings of Information Security Workshop (ISW’97)*, pp. 282-290, Tatsunokuchi, Japan, September 1997.
- [58] Zhang, Q., Yu, T., and Irwin, K., “A Classification Scheme for Trust Functions in Reputation-Based Trust Management”, *In Proceedings of the Third International Semantic Web Conference (ISWC’04): The Workshop of Trust, Security, and Reputation on the Semantic Web*, pp. 1-10, Hiroshima, Japan, November 2004.

- [59] Zhang, X.B., Lam, S.S., Lee, D.Y., and Yang, Y.R., “Protocol Design for Scalable and Reliable Group Rekeying”, *IEEE/ACM Transactions on Networking*, Vol. 11, Issue 6, pp. 908-922, December 2003.
- [60] Zheng, Y., “On Key Agreement Protocols Based on Tamper-proof Hardware”, *Information Processing Letters*, Vol. 53, No.1, pp. 49-54, January 1995.



Biography

Chun-Chieh Huang is a Ph.D. candidate of Institute of Information Management at National Chiao Tung University in Taiwan. He received the B.S. degree in Computer Science from Chung Cheng Institute of Technology, National Defense University, Dasi, Taiwan, in 1994, the M.B.A degree in Resource Management from Management College, National Defense University, Jhonghe, in 1997. His current major researches include network security, information security, network topology, electronic commerce security, and network management.



Publication List

Journal:

1. Chi-Chun Lo, **Chun-Chieh Huang**, and Wen-Tian Liang, "Mitigating Routing Misbehavior Using Ant-Tabu-Based Routing Algorithm for Wireless Ad-Hoc Networks," *International Journal of Computer Science and Network Security (IJCSNS)*, Vol.10, No.5, pp.46-51, May, 2010.
2. Chi-Chun Lo, **Chun-Chieh Huang**, Fang-Yi Lee, Kuang-Yu Chen, Ping-Hsien Ho, and Anni Graebner, "A Flexible Access Control Mechanism for Web Services," *ICIC Express Letters*, Vol. 5, No. 4(B), pp. 1377-1383, April 2011. (EI)
3. 羅濟群、黃俊傑，"一個應用於行動商務環境中以群體為導向—提名式代理簽章機制為基底之數位版權管理架構，" *資訊管理學報*，第十七卷，pp. 117-139，12月，2010年。(TSSCI)

Proceedings (International conference):

1. Chin-Chun Lo, Chun-Chieh Huang, and Yong-Xin, Huang, "A Key Agreement Protocol Using Mutual Authentication for Ad-Hoc Networks," Proceedings of ICSSSM'05 2005 International Conference, Vol 2, pp. 814-818, June 2005.
2. Chi-Chun Lo, Chun-Chieh Huang, and Shu-Wen Chen, "An Efficient and Scalable EBS-based Batch Rekeying Scheme for Secure Group Communications," MILCOM 2009 Proceedings, pp. 1-7, October 2009.
3. Chun-Chieh Huang and Chi-Chun Lo, "Threshold Based Group-Oriented Nominative Proxy Signature Scheme for Digital Rights Management," 6th IEEE International Workshop on Digital Rights Management on IEEE CCNC 2010 (CCNC'2010 – DRM Workshop), pp. 1-5, January 2010.
4. Chi-Chun Lo, Chun-Chieh Huang, and Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," The 2nd International Workshop on Security in Cloud Computing (SCC'2010) in 39th International Conference on Parallel Processing, San Diego, CA, USA, pp. 280-284, September 2010.
5. Shi-Hong Chou, Chi-Chun Lo, and Chun-Chieh Huang, "Mitigating Routing Misbehavior in Dynamic Source Routing Protocol Using Trust-Based Reputation Mechanism for Wireless Ad-Hoc Networks," The 8th Annual IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, pp. 463-467, January 2011.
6. Chi-Chun Lo, Chun-Chieh Huang, and Meng-Ju Lee, "A Channel-Based Key Management Protocol for IPTV Service," The 8th Annual IEEE Consumer

Communications and Networking Conference - Work in Progress, Las Vegas, NV, USA, pp. 715-716, January 2011.

7. Chun-Chieh Huang and Chi-Chun Lo, "A Two-Key Agreement Based Supervising Mechanism for Cluster-Based Peer-to-Peer Applications," The 2nd International Workshop on Peer-To-Peer Networking on ICPADS 2010 (The 16th International Conference on Parallel and Distributed Systems), Shanghai, China, pp. 823-828, December 2010.
8. Chi-Chun Lo, Chun-Chieh Huang, and Chung-Huan Chang, "A Flexible Access Control Mechanism for Mobile Commerce," 29th International Conference on Consumer Electronics, Las Vegas, NV, USA, pp. 145-146, January 2011.

