國立臺灣大學工學院土木工程學系

碩士論文

Department of Civil Engineering

College of Engineering

National Taiwan University

Master Thesis

ATMS 通訊安全動態加密技術研究

Dynamic Security Mechanism for the Security and Efficiency of ATMS Date Transmission

張元瑞

Yuan-Jui, Chang

指導教授：張堂賢 教授

林結明 教授

Advisor: Prof. Tang-Hsien Chang

Prof. Kit Meng Lum

中華民國 98 年 6 月

June, 2009

國立臺灣大學碩士學位論文
口試委員會審定書

ATMS 通訊安全動態加密技術研究
Dynamic Security Mechanism for the Security and Efficiency of ATMS Data Transmission

本論文係張元瑞君（R95521511）在國立臺灣大學土木工程學系碩士班完成之碩士學位論文，於民國 98 年 6 月 12 日承下列考試委員審查通過及口試及格，特此證明

口試委員：

張堂賢　張堂賢（簽名）

（指導教授）

黃文鑑　黃文鑑

陶治中　陶治中

系主任　張國鎮（簽名）

序　　言

登高無畏峻風寒，拏月但得新苗青

登高峻風寒又寒，雖未必能如願拏明月；

走一遭，親體驗，將能感受嫩苗之青如明月

2009/06/15

于 國立台灣大學

摘要

ITS 的目標在於促進交通安全、減少交通擁擠、提高機動性、增進經濟生產力、減少環境衝擊、提昇能源使用效率及帶動相關產業發展。而先進交通管理系統（Advanced Transportation Management System, ATMS）乃為 ITS 下之核心系統之一，其中最重要的乃是駕駛人所需即時交通資訊之傳輸、交通控制中心須依即時收取之資料，將最正確的訊息與決策傳給用路人與路側設施；在這環環相扣的過程中涉及許多技術專業如通訊、電機、資訊工程等領域的發展。目前， ATMS 之資料傳輸中，採用 NTCIP (National Transportation Communications for ITS Protocol)作為其傳輸協定，為了與現行通用之通訊協定相結合而不致有所衝突，NTCIP 之堆疊(Stack)亦依循 ISO-OSI(Open Systems Interconnect)之七層模型架構。

採用 ISO-OSI 之模型架構使得 NTCIP 不致於與現行通訊協定不相容，但開放式的網路環境也為 NTCIP 帶來許多安全性(Security)的問題，如駭客(Hacker)可在封包傳輸途中進行攔截，並對其進行竄改、偽裝、重送等攻擊，然而在實際應用上，其資料的傳輸安全性卻往往為人們所忽略。故本研究透過現行之密碼學相關技術，針對資料傳輸之確認性(Authentication)、機密性(Confidentiality)與完整性(Integrity)等對傳輸訊息進行加密保護，對於 ATMS 之傳輸建立一套動態安全機制(Dynamic Security Mechanism, DSM)，藉此提高 ATMS 之傳輸安全性。

此外，在通訊安全的領域中並無所謂絕對性的安全機制；安全機制的安全性應取決於使用者的需求以及可使用之軟硬體設備、支援等。本研究 DSM 最大的特色為可變動式金鑰產生器 DSKG (Dynamic Secret Key Generator) 以及 DPKG (Dynamic Public Key Pair Generator)。此機制使得每一次的傳輸加密皆有不同的金鑰產生，藉此來達到防止駭客入侵、取得傳輸資料之安全漏洞。

由於在原有的資料傳輸過程中加入加解密程序對於原系統亦會產生其負效應，因此本研究尚進行實驗設計，以探討其封包於加密前後對於系統運作影響以及封包傳輸時間之影響，並進行統計檢定，以確認封包加密對其之影響幅度，最後會依實驗結果對於加密前後之封包於ISP與VPN之有線網路及無線網路傳輸架構下之傳輸與系統運作時間進行 DSM 運作效率分析，以使得採用加密機制之交控中心人員能夠依其所需，訂立相關傳輸時間之門檻值。

關鍵字：先進交通管理系統、智慧型運輸系統、動態加密、密碼學、安全性。

ABSTRACT

ITS aims at enhancing traffic safety, reducing congestion, increasing travel mobility, enlarging economic power and controlling efficient energy-use. Advanced Transportation Management System (ATMS) is the major sub-system of ITS, and it utilizes monitor apparatus, communications and other control technologies to obtain or exchange traffic information between the traffic devices. However, during the data transmission, the situation of the data packets switching is exposed and not protected. Someone can use existing software to intercept the data packets from transmission process easily and these attacks will cause ATMS to become paralysed and disorder the signal timing or impaired traffic safety seriously. Therefore, the traffic data transmission security should be the principal issue for ATMS nowadays, but less people concern with the issue.

By these reasons, this study concentrates on the information security of ATMS data transmission through modern cryptography and sets up a suitable security mechanism which aims at the message packet exchange and transmission via Java programming language. In which, the cryptography techniques would be adopted to protect the contents of data packet from masquerading, replying and tampering; and the general encryption algorithm is used to transform the plaintext into the ciphertext via the secret keys.

In the past, the secret key algorithms during the encryption/decryption procedures are invariable and regular; furthermore, and the message packets are transmitted frequently in traffic control. In these conditions, one could crack the secret key algorithms easily by the frequent transmission. Thus, this research designs and implements an encryption technique which the secret keys could be changeable for each message and suitable for the ATMS data transmission; we called it dynamic encryption technique.

On the other hand, we expect the security mechanism would not only achieve the data security but also consume less resources of the core system. Unfortunately, in the process of improving the data security, it also brings some negative-effects on the core system. Therefore, the system operation efficiency is also the major consideration of the security mechanism design. In addition, the security mechanism could be suitable for the existing communications media which transportation filed commonly uses nowadays, namely: wired network communications and 3.5G mobile communications.

Keywords: ITS, ATMS, Cryptography, Security, Efficiency, Encryption.

TABLE OF CONTENTS

引　言…………………………………………………………………………..i

摘　要………………………………………………………………….............iii

ABSTRACT……...…………………………………………………………...v

TABLE OF CONTENTS……..………………………………………………vii

LIST OF TABLES…………………..……………………………………………xi

LIST OF FIGURES……………………….……………………………………xv

LIST OF ABBREVIATIONS……………………………………………………xix

CHAPTER ONE INTRODUCTION………………………………………………1

1.1 Background……………………………………………………………..1

1.2 Objectives of this Research……………………………………………6

1.3 Scope of this Research…………………………………………………6

1.4 Research Methodology…………………………………………………7

1.5 Structure of this Research………………………………………………8

1.6 Chapter content of this Research………………………………………10

CHAPTER TWO FUNDAMENTALS……………………………………………13

2.1 Introduction……………………………………………………………13

2.2 Advanced Transportation Management System……………………………13

2.3 NTCIP……………………………………………………………………15

2.3.1 Protocol and NTCIP ………………………………………………15

2.3.2 Framework, Standards and Protocol Stacks of NTCIP………………19

2.3.3 Brief Summary…………………………………………………….23

2.4 Security Elements……………………………………………………..24

2.4.1 Network Security Model………………………………………………..24

2.4.2 Security Attack Techniques………………………………… …...26

2.4.3 Security Services……………………………………………………29

2.5 Cryptography Technologies……………………………………………30

2.5.1 Symmetric Cryptography…………………………………………31

2.5.2 Asymmetric Cryptography………………………………………...38

2.5.3 Message Digest and Message Authentication………………………43

2.6 The Possible Attack Discussions on ATMS Data Transmission ……..…46

2.7 Summary and Evaluations………………………………………………51

CHAPTER THREE SECURITY MECHANISM ESTABLISHMENT AND SECURITY PROTECTION DISCUSSION……………………………………55

3.1 Introduction………………………………………………………………55

3.2 Conceptions of Information Security in this Study…………………… …...56

3.3 Development Tool- Java Programming Language ………………………...59

3.4 Architecture of the Security Mechanism……………………………………62

3.4.1 Conceptions of the Dynamic Encryption Technique ……………...62

3.4.2 Architecture of the Dynamic Security Mechanism…………………...67

3.5 Security Analysis for the Security Mechanism……………………………76

3.5.1 Analysis of Security Protection………………………………………76

3.5.2 Cryptanalysis…………………………………………………………79

3.5.3 Brute-Force Attack……………………………………………………83

3.6 Summary…………………………………………………………… …...87

CHAPTER FOUR EXPERIMENTS FOR SYSTEM EFFICIENCY……………89

4.1 Introduction………………………………………………………………89

4.2 Experiment Design Principle ……………………………………………...89

4.3 Experiment Environment…………………………………………………92

4.3.1 Scope of Simulated Experiment……………………………………92

4.3.2 The protocol stacks and hardware for Simulation……..……………94

4.3.3 NTCIP objects for the Simulation……………………………………100

4.4 Experiment Contents……………………………………………………105

4.4.1 Experiment Methodology…………………………………………..105

4.4.2 Experiment One……………………………………………………112

4.4.2 Experiment Two……………………………………………………114

4.4.3 Experiment Three…………………………………………………...…116

4.5 Expected Outcomes……………………………………………………118

CHAPTER FIVE DATA ANALYSIS AND FINDINGS…….……………………121

5.1 Introduction……………………………………………………………121

5.2 Queue and delay phenomenon of DSM operation ………………………121

5.3 Data Analysis of Experiment One ………………………………………125

5.3.1 Analysis in the communications medium, NTCIP object size and DSM addition for the influence of transmission delay……………………………...126

5.3.2 Analysis in the NTCIP object size for the influence of encryption and decryption operations ……………………………………………………129

5.3.3 Brief summary…………………………………………………………132

5.4 Data Analysis of Experiment Two ………………………………………133

5.4.1 Analysis in the combinations of AES and RSA for the influence of data packet transmission delay …………………………………………………134

5.4.2 Analysis in the combinations of AES and RSA for the influence of operation delay……………………………………………………………136

5.5 Data Analysis of Experiment Three………………………………………142

5.5.1 Analysis in the interval of the object dispatch and the computation-capability for influence of device operation delay……………143

5.5.2 Analysis in the interval of the object dispatch and the computation-capability for influences of data transmission delay……….......147

5.5.3 Brief summary……………………………………………………………150

5.6 Regression Equation of DSM Operations…………………………………152

CHAPTER SIX CONCLUSIONS AND FUTURE RESEARC…………………156

6.1 Conclusions……………………………………………………………………156

6.2 Future Research and Suggestions ………………………………………….160

REFERENCE……………………………………………………………………162

APPENDIX A SNMP AND STMP……………………………………………166

A-1 Simple Network Management Protocol ………………………………….166

A-2 Simple Transportation Management Protocol……………………………170

APPENDIX B OPERATIONS OF AES AND RSA…………………………174

B-1 AES ……………………………………………………………………………174

B-2 RSA……………………………………………………………………………178

APPENDIX C LIST OF EXPERIMENT CONTENTS……………………182

LIST OF TABLES

Table 2.1 Characteristics of symmetric cryptography algorithms……………………..52

Table 2.2 Characteristics of asymmetric cryptosystem algorithms. ………………….53

Table 2.3 Comparisons: symmetric cryptography vs. asymmetric cryptography……53

Table 3.1 Example of encryption via ECB cipher mode. …………………………….82

Table 3.2 Example of encryption via CBC cipher mode. ………………...…..……83

Table 3.3 Time-consuming for brute-force attack in Decryption. ………………….86

Table 3.4 Effects of the dynamic security mechanism. ……………………………….88

Table 4.1 Protocol stack items of the experiments.. …………………....……………95

Table 4.2 Specification of simulated computers.. ……………………........……………96

Table 4.3 Specification for wired network………………………………………...98

Table 4.4 Specifications for 3.5G mobile communications……………………......…100

Table 4.5 NTCIP Object No.01－trafficControl Code……………………........……102

Table 4.6 NTCIP Object No.02－cmsDimSchedule Code……………………......102

Table 4.7 NTCIP Object No.03－phaseOrderTable Code……………………………102

Table 4.8 NTCIP Object No.04－timingPlantable Code……………………......……102

Table 4.9 NTCIP Object No.05－timingPlantable Code……………………......……103

Table 4.10 NTCIP Object No.06－timingPlanBacsicParatable Code………………103

Table 4.11 NTCIP Object No.07－vdCurrentDataTable Code…………………….. 104

Table 4.12 Test objects of Experiment One……………………........……………….113

Table 4.13 NTCIP object usage for Experiment One…………………….....…….…114

Table 4.14 Test objects of Experiment Two……………………....………………….116

Table 4.15 Test objects of Experiment Three……………………....…………….118

Table 5.1 Crack points of DSM continuous operations ($\boldsymbol{C_c}$) ……………….......……122

Table 5.2 Crack points of DSM continuous operations ($\boldsymbol{KP_l}$) ……………….....……123

Table 5.3 Crack points of DSM continuous operations ($\boldsymbol{M_f}$) ……………………124

Table 5.4 Statistic Descriptions of Analysis 1-1……………………………………127

Table 5.5 Mean transmission consumping time of Analysis1-1……………………127

Table 5.6 Regression equation analysis of Analysis 1-1……………………………128

Table 5.7 The observed mean of the consuming time of encryption/decryption……130

Table 5.8 One-Way ANOVA Table –Object size analysis (Encryption) ……………131

Table 5.9 One-Way ANOVA Table of Analysis 1-2 (Decryption) …………………132

Table 5.10 Two-Way ANOVA Table of Analysis 2-1………………………………135

Table 5.11 Observed mean of the consuming time of device operations……………137

Table 5.12 One-Way ANOVA Table of $\boldsymbol{C_m}$ and AES/RSA operations………………138

Table 5.13 Two-Way ANOVA Table of Analysis 2-2………………………………139

Table 5.14 The comparisons with the different length of RSA public key pair……141

Table 5.15 Observed mean of TCIS device operations (Analysis 3-1) ……………143

Table 5.16 Two-Way ANOVA Table of Analysis 3-1………………………………146

Table 5.17 Observed mean of data packet transmission (Analysis 3-2) ……………148

Table 5.18 Regression equation analysis of Analysis 3-2……………………………149

Table 5.19 Analysis results of $\boldsymbol{C_m}$, $\boldsymbol{KS_l}$, $\boldsymbol{KP_l}$, $\boldsymbol{M_s}$, $\boldsymbol{M_f}$ and $\boldsymbol{C_c}$ ……………………151

Table 5.20 Statistics descriptions of the regression equation in this research………150

Table 5.21 Regression equation analysis of DSM operation…………………………150

Table 5.22 The threshold values of DSM operation efficiency………………………155

Table A.1 SNMP Message form……………………………………………………169

Table A.2 SNMP Message Type, Purpose and Originator……………………………170

Table A.3 STMP Message Type, Purpose and Originator……………………………171

Table A.4 STMP Message form………………………………………………………173

Table B.1 Example for S-box…………………………………………………………175

Table C.1 List of Experiment One……………………………………… ……182

Table C.2 List of Experiment Two…………………….…...…………………...……183

Table C.3 List of Experiment Three……………………..…………………...……183

LIST OF FIGURES

Figure 1.1 Singapore ITS architecture……………………....…………………...……4

Figure 1.2 The traffic control system framework of Taipei City, Taiwan………………4

Figure 1.3 Structure and procedures of this research……………………...…………10

Figure 2.1 ITS subsystems and related techniques of ATMS……………………....…15

Figure 2.2 NTCIP and the National ITS Architecture……………………...………17

Figure 2.3 Example of ITS Integration Using NTCIP…………………...…………17

Figure 2.4 NTCIP Standards Framework…………………......…………………... 20

Figure 2.5 Relationships between OSI Layers and NTCIP Levels……………………20

Figure 2.6 Network Security Model……………………......…………………....……25

Figure 2.7 Illustration for active attack types……………………..………………. 28

Figure 2.8 Architecture of symmetric cryptosystem……………………......…………31

Figure 2.9 Encryption and decryption procedures of DES…………………....……35

Figure 2.10 Encryption and decryption procedures of Triple-DES……………………37

Figure 2.11 Encryption and decryption procedures of AES……………..………...…38

Figure 2.12 Architecture of asymmetric cryptosystem…………………….....………39

Figure 2.13 Architecture of message digest……………………………………...…44

Figure 2.14 Masquerading Attack in ATMS Data Transmission…………………...…48

Figure 2.15 Eavesdropping Attack in ATMS Data Transmission…………………......48

Figure 2.16 Man-In-the-Middle Attack in ATMS Data Transmission………………49

Figure 3.1 Conceptions of the dynamic encryption techniques……………………...…58

Figure 3.2The balance-point for the security mechanism consideration……………..59

Figure 3.3 Simple class hierarchy of the security mechanism in Java programming…..60

Figure 3.4 Architecture of Dynamic Encryption Technique………………….......…..63

Figure 3.5 Framework of Dynamic Key Generator……………………….……………66

Figure 3.6 TMIC Operation One－to generate a public key pair and seal byte arrays before public key transmission……………………..……………...……………68

Figure 3.7 Procedures for data packet restoration and message digest comparison….69

Figure 3.8 Procedures for data packet restoration and message digest comparison…....71

Figure 3.9 Functions of message digest algorithms of the security mechanism…….72

Figure 3.10 Procedures for the secret key separation……………………..………72

Figure 3.11 Procedures for the NTCIP object encryption and transmission…..………73

Figure 3.12 Procedures for NTCIP object ciphertext decryption…………….…………75

Figure 3.13 Flow chart of the security mechanism of this research.. …………..………..75

Figure 3.14 EBC cipher mode and CBC cipher mode...…………………......………..81

Figure 4.1 Time-consumption assignment of DSM operation. ………………………90

Figure 4.2 Framework of data transmission…………………………………………...93

Figure 4.3 Protocol stacks of the experiments…………………...…………………95

Figure 4.4 Framework of wired network.. ………………….... …………………... …98

Figure 4.5 Framework of 3.5G mobile communications…………………..........…100

Figure 4.6 Experiment situations…………………….. ………………....………107

Figure 4.7 VPN connection procedures……………………......…………………... 108

Figure 4.8 Network Time Calibration Software－NTPClock…………………….. 108

Figure 4.9 Display of programming operation…………………...………………109

Figure 4.10 Display of note items……………………......………………....………109

Figure 4.11 Data transmission procedure of the security mechanism………………110

Figure 4.12 Framework of Experiment One…………………………………………114

Figure 4.13 Framework of Experiment Two...……………………......………………116

Figure 4.14 Framework of Experiment Three……………………....………………118

Figure 5.1 DSM operation in different computeation-capability TCIS dvices………122

Figure 5.2 Crack point of DSM operations ($\boldsymbol{C_c}$) ……………....……………………......123

Figure 5.3 DSM operation in different RSA public key pair length……………......123

Figure 5.4 DSM operation in different NTCIP object dispatch interval……………..124

Figure 5.5 Crack point of DSM operations ($\boldsymbol{M_f}$) ……………......…………………......125

Figure 5.6 Line graph of mean time-consumption of NTCIP object transmission…127

Figure 5.7 Line graph of mean time-consumption of encryption/decryption………130

Figure 5.8 The mean comparisons of AES operations……………......……………141

Figure 5.9 The mean comparisons of RSA operations...…………………..…………141

Figure 5.10 The represection of the factor in $\boldsymbol{C_c}$ (Analysis 3-1) ...………..…………144

Figure 5.11 The represection of the factor in $\boldsymbol{M_i}$ (Analysis 3-1) ...………….………145

Figure 5.12 The represection of the factor in $\boldsymbol{Cc}$ (Analysis 3-2) ...……………..………148

Figure 6.1 The time-consumption trend of DSM operations………………………159

Figure A.1 The components of SNMP………………………………………………167

Figure A.2 MIB integrations………………………………………..……………168

Figure A.3 Internet authority hierarchy and TMIB structure.. …………………... …172

Figure B.1 SubBytes operation………………………………………………………176

Figure B.2 ShiftRows operation……………………. ………………………………176

Figure B.3 MixColumns operationvv………………………………………………177

Figure B.4 AddRoundKey operation…………………………………...……………178

Figure B.5 The compositions of RSA algorithm……………………………………181

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
ASN.1	Abstract Syntax Notation One
ATMS	Advanced Transportation Management System
BER	Basic Encoding Rules
CBC	Cipher Block Chaining
CCTV	Closed Circuit Television camera systems
CFB	Cipher Feedback Mode
C2C	Centre-to-Centre
C2F	Centre-to-Field
DES	Data Encryption Standard
DSKG	Dynamic Secret Key Generator
DSM	Dynamic Security Mechanism
DKG	Dynamic Key Generator
DPKG	Dynamic Public Key Pair Generator
ECB	Electronic Codebook Mode
ECC	Elliptic Curve Cryptography
FIPS	Federal Information Processing Standard
GIS	Geographic Information System
GPRS	General Packet Radio Service
IETF	Internet Engineering Task Force
ISO-OSI	International Standards Organisation-Open System Interconnect
ISP	Internet Service Providers
ITS	Intelligent Transportation System
ITU	International Telecommunication Union

ITU-T	ITU-Telecommunication Standardization Sector
IV	Initialization Vector
JAAS	Java Authentication and Authorization Service
JCA	Java Cryptography Architecture
JCE	Java Cryptography Extension
JSSE	Java Secure Sockets Extension
JVM	Java Virtual Machine
MAC	Message Authentication Codes
MD2	Message Digest 2
MD4	Message Digest 4
MD5	Message Digest 5
MIB	Management Information Base
NBS	National Bureau of Standards
NEMA	National Electrical Manufacturers Association, America
NIST	National Institute of Standard and Technology
NTCIP	National Transportation Communication for ITS Protocol
NTU	Nanyang Technological University
OER	Octet Encoding Rule
OID	Object Identifier
OS	Operating System
PDU	Protocol Data Unit
PER	Price-Earnings Ratio
RMON	0emote Network Monitoring
PMPP	Point-to-MultiPoint Protocol
PRNG	Pseudo-Random Number Generator
RSA	Rivest-Shamir-Adleman

RSU	Road-Side Unit
SCATS	Sydney Coordinated Adaptive Traffic System
SMI	Structure and Identification of Management Information
SNMP	Simple Network Management Protocol
STMP	Simple Transportation Management Protocol
TCIS	Transportation Communication and Information Station
TMIC	Transportation Management Information Centre
TMIB	Transportation Management Information Base
Triple-DES	Triple Data Encryption Standard
TSC	Traffic Signal Controller
TTP	Trusted Third Party
VMS	Variable Message Sign
VD	Vehicle Detectors
VPN	Virtual Private Network

CHAPTER ONE

INTRODUCTION

1.1 Background

Intelligent Transportation System improves transportation safety and mobility and enhances productivity through the use of advanced information and communication technologies.[07]

A transportation system is made up of various components. It comprises of people, vehicles, road systems and traffic hardware. Industrial products are made up of vehicles and the road system. The main objective of the Transportation System (ITS) is to enable industrial products to have artificial intelligence so that it will be able to tackle complicated traffic challenges so as to enhance the transportation safety, efficiency as well as comfort to the users. ITS combines with technologies such as advanced electronic, computer, information, vehicle, communication, control, so as to provide the real-time information, varied traffic management policies and it is capable of reducing the impact for traffic and natural environment simultaneously.

Advanced Transportation Management System (ATMS) is a major sub-system of ITS. ATMS makes use of monitor apparatus, communication and other control technologies to obtain traffic information and, subsequently to transmit or exchange the data from Transportation Management Information Centre (TMIC) to Transportation Communication and Information Station (TCIS) or beacons via communication. TMIC collects traffic information which are derived from vehicle detectors (VD), closed circuit television camera systems (CCTV) or others to establish traffic control in instruction and integral traffic management plans. Finally, TMIC send these traffic instructions and plans to the related traffic management apparatus, beacon devices, controller and road-side unit (RSU) or users. Because need to transmit information, communications technology becomes the most important factor for ATMS.

The protocol of ATMS is dependent on the National Transportation Communication for ITS Protocol (NTCIP). In order to combine and not to collide with the common communications protocol, the stack of NTCIP refers to the model framework of International Standards Organisation-Open System Interconnect (ISO-OSI). The ISO-OSI model makes NTCIP suitable with the common communications protocol, but open network environment also brings along many security problems. Figures 1.1 and 1.2 are respectively the ITS architecture, which is adopted from the Sydney Coordinated Adaptive Traffic System (SCATS), in Singapore and the traffic control system framework of Taipei City, Taiwan. In these traffic control systems, vehicle detectors and CCTV collect the traffic flow data and transmit these data back to the traffic control centre by network (wired or wireless network). After archiving and analysing by the central computer, the traffic centre produces the applicable traffic instructions and transmits these instructions to the traffic signal controller (TSC).

During the foregoing process in data transmission, the situation of the data packets switching is exposed and not protected. Someone can use existing software (e.g. Sniffer Pro, Iris, etc) to intercept the data packets from transmission processes easily. In addition, the internal framework of NTCIP which is similar to ISO-OSI, allows one to read, masquerade, eavesdrop, modify, tamper or reply to the original messages easily during data transmission to the traffic control system. These actions will cause ATMS to become paralysed and disorder the signal timing or impaired traffic safety seriously. A plausible solution is building an Intranet Network System up for ATMS (i.e., Virtual Private Network, VPN). While the communications environment of Intranet is closed, if the fire-wall is well-controlled, the invading opportunity will be reduced, but the cost will be more expensive.

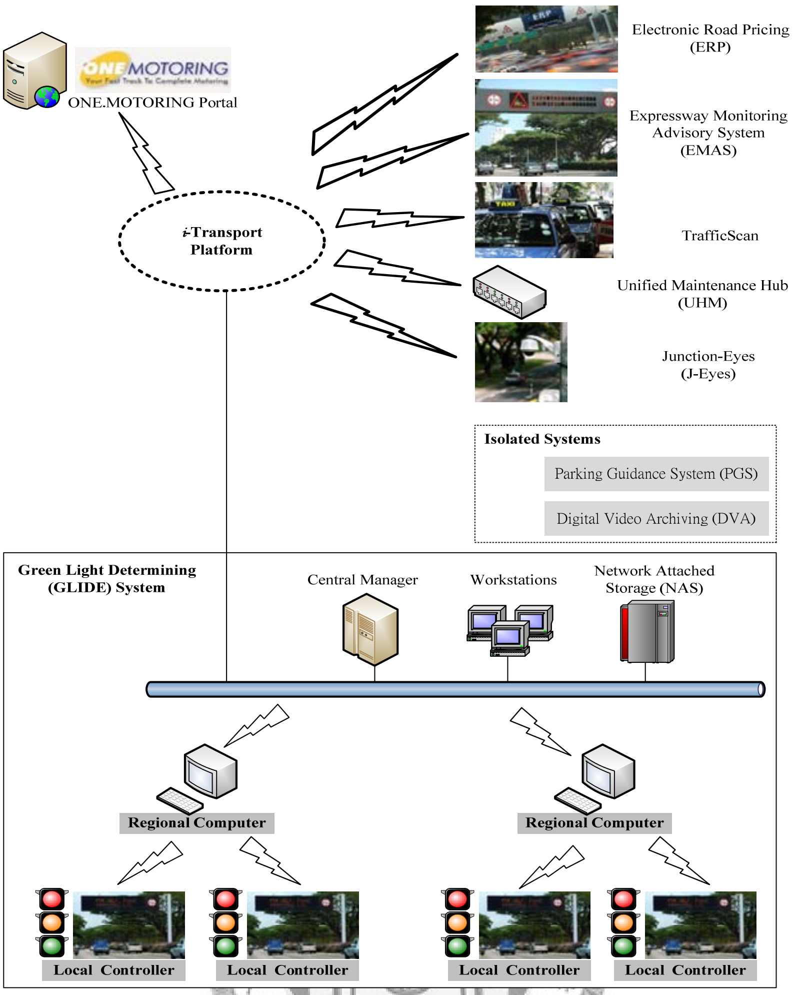

ONE MOTORING
ONE.MOTORING Portal
i-Transport Platform
Electronic Road Pricing (ERP)
Expressway Monitoring Advisory System (EMAS)
TrafficScan
Unified Maintenance Hub (UHM)
Junction-Eyes (J-Eyes)
Isolated Systems
Parking Guidance System (PGS)
Digital Video Archiving (DVA)
Green Light Determining (GLIDE) System
Central Manager
Workstations
Network Attached Storage (NAS)
Regional Computer
Regional Computer
Local Controller
Local Controller
Local Controller
Local Controller

Figure 1.1 Singapore ITS architecture (Provided by LTA, Singapore)

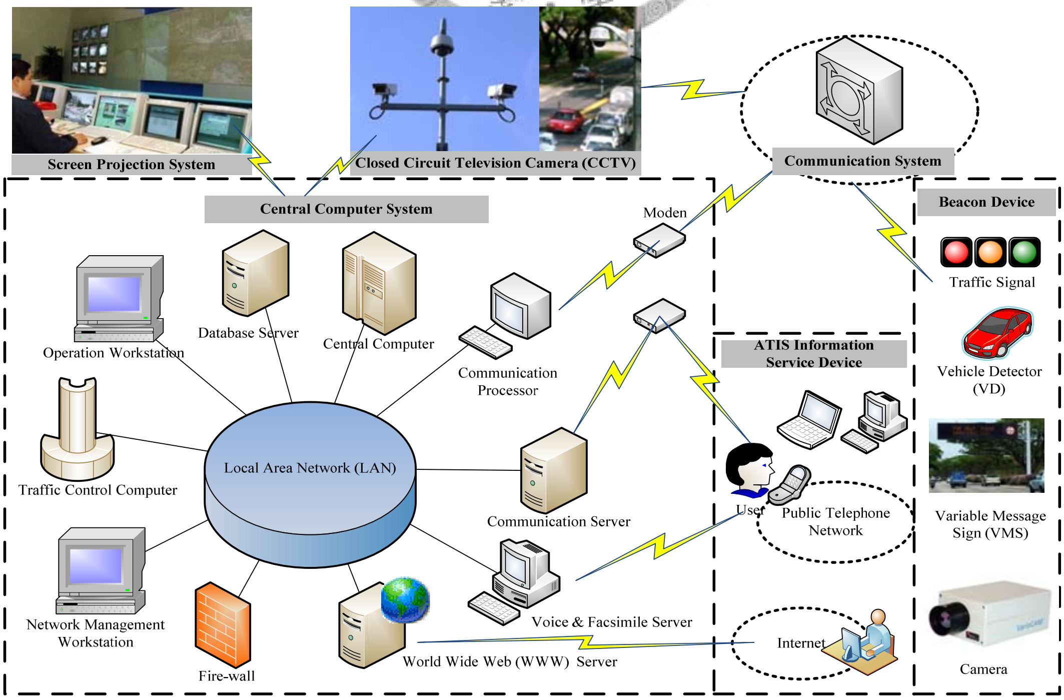


Figure 1.2 The traffic control system framework of Taipei City, Taiwan [58]

Based on the diagram above, this research focuses on the information security of data transmission through modern cryptography and sets up a suitable encryption technique which aims at message packets interchanging and transmitting. Even though hackers can intercept these message packets during transmission process but they can just get the ciphertexts and not the plaintexts (original messages). That is because the texts (or message packets) have been encrypted into ciphertexts, and each ciphertext needs opposite key (secret key) to decrypt. So hackers would not be able to know the correct content of each message packet, let alone even though they want to masquerade or modify the message packets. In each encryption process, one can provide respective security key for different message packet, or the security keys can be changed for different time. Even if hackers use Brute-Force Attack, they would not get the correct content of message packets smoothly, due to the following reasons [01]:

- During the message packet transmission, the encrypting procedures use respective security key via random or catching the characteristic characters from each message to encrypt, so hackers would not know the security formulas easily, and;
- The benefits of attacking cost might be not high enough to seduce hackers.

From the two reasons and including others, the selections of algorithms, the productions and transmissions of security keys are the important points of this research.

1.2 Objectives of this Research

This research focuses on reducing information security menaces of ATMS in data transmission and develops a security mechanism which is based on modern cryptography and developed by Java programming language. In order to improve the security level, the security mechanism would consume a lot of resource of the core system. How to increase security and at the same time not affecting the original core system are the trade-off issues that will be studied in detail.

For the sake of this security mechanism could be operated not only on Windows Operating System (OS) but also on other operating systems (e.g. Linux, Unix), this research chooses Java programming language to be the development tool, because Java programming language comprises two important properties, namely, Java byte code can be executed on any computer OS with a Java Virtual Machine (JVM) and Java programming language is also the object-oriented programming language.

1.3 Scope of this Research

The common security issues are virus invading, peeping, masquerading, message modifying, etc. Therefore, the security defences, ideally, have to deal with all kinds of attacks. In ATMS, there are fewer security defences for data transmission procedures. That means the security issues for message packets transmitting are neglected by most of the people, but the size and frequencies of data transmission are very high and huge in traffic control system, so if message packets are attacked during transmission process of ATMS, the ATMS would be paralysed or lose the functions.

As a result, this research aims at the security of data transmission for ATMS and establishes a security mechanism by modern cryptography technique using Java programming language. Encrypting plaintexts into ciphertexts at transmitter-side and decrypting ciphertexts to the original plaintexts at the receiver-side after getting the message packets form transmitter. If someone who has in mind to steal message packets from transmission procedures, one can only get the ciphertexts and cannot falsify or read the original messages to improve the security of ATMS data transmission.

1.4 Research Methodology

There are three main methodologies in this research, given in the following:

- Introduce modern cryptography techniques for information security, e.g., symmetric cryptosystems, asymmetric cryptosystems, Message Digest, Message Authentication, etc. Thereafter, using these cryptography techniques to be the basic knowledge to design the security mechanism architecture of this research;
- To develop a security mechanism by Java programming language and then try to

operate, test, analyse the security mechanism programming. In order to simulate real situations, this research uses over three computers to be TMIC and TCIS and uses the wireless network and wired network for communications. As Java programming language supports OSI communications protocol module, it is as suitable as the protocol of ATMS, and;

- Because encrypting or decrypting procedures would cause system to have the system negative effects. This research includes three experiments to probe into the variations of packet dimension, transmission delay between the encryption/decryption procedure addition or not. Eventually, discussing the reliability by probability and statistics.

1.5 Structure of this Research

The contents and procedures of this research are given below and shown in Figure 1.3.

- Aim at NTCIP that ATMS uses to proceed to assess the transmission security and point out what threats may confront in ATMS data transmission;
- Discuss the excellences, defects and basic theorems of modern cryptography techniques;
- Discuss the security threats and use modern cryptography theorems to establish a suitable security mechanism;

- Describe what is dynamic security mechanism and the characteristics and benefits of it;
- This dynamic security mechanism would be developed via Java programming language, and there are three experiments which are designed to simulate the real traffic conditions with the security mechanism;
- Because of the encrypting and decrypting process additions in the data transmission, these will affect the original system. Thus, this research would also discuss the influences for ATMS due to the security mechanism addition;
- Consider the security mechanism is subjected to be attacked and the threat analyses for security, and;
- Undertake to analyze the system effects by three designed experiments to discuss the variations between the security mechanism addition.

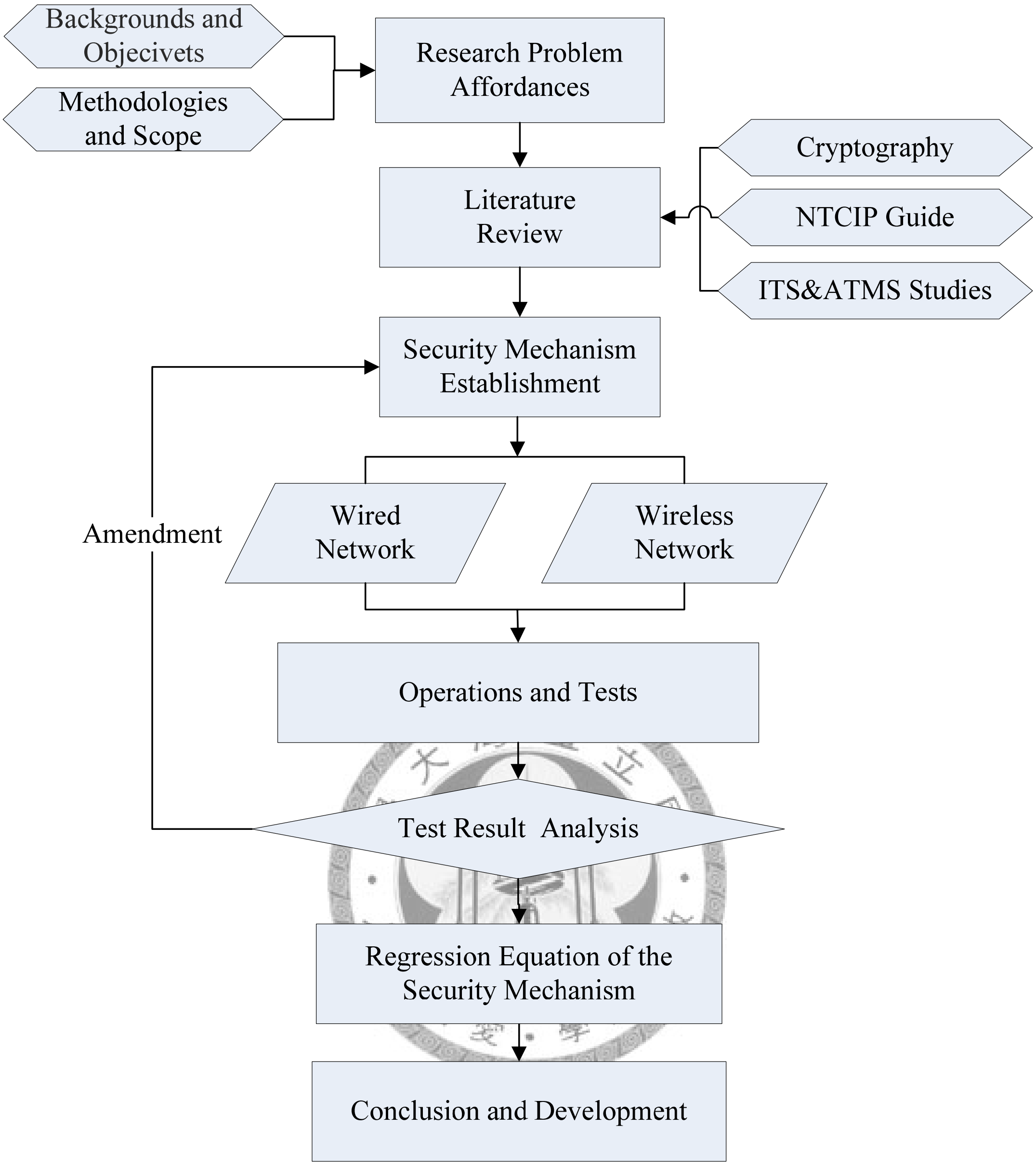

Backgrounds and Objecivets
Methodologies and Scope
Research Problem Affordances
Cryptography
NTCIP Guide
ITS&ATMS Studies
Literature Review
Security Mechanism Establishment
Amendment
Wired Network
Wireless Network
Operations and Tests
Test Result Analysis
Regression Equation of the Security Mechanism
Conclusion and Development

Figure 1.3 Structure and procedures of this research

1.6 Chapter content of this Research

Chapter One Introduction

Chapter One provides the backgrounds, objectives, scope, methodologies and structure of this research.

Chapter Two Fundamentals

There are three major parts in the fundamentals of this research; the first part discusses the research objective－ATMS and the protocol of ATMS－NTCIP, explains the characteristics of NTCIP and highlights the reasons why ITS uses NTCIP to be the main protocol in communication. The second part probes into the network security. And then the last part introduces the basic and types of modern cryptography technologies.

Chapter Three Security Mechanism Establishment and Security Protection Discussion

Introduce the contents of the security mechanism; it would include the design conceptions and the architecture of the dynamic security mechanism. In addition, this chapter introduces why this research chooses Java programming language is used as the development tool and the security analysis for the security mechanism as well. The points of security analysis are to make sure that the security mechanism can resist certain common attacks, especially in Brute-Force Attack.

Chapter Four Experiments for System Efficiency

Chapter Three introduces that the dynamic security mechanism for establishment of ATMS data transmission. In Chapter Four, three experiments are designed to test the operation efficiencies of the security mechanism. These experiments would probe into the negative-effects generated for the core systems due to the dynamic security mechanism addition and discuss the influences on the different considerations.

Chapter Five Date Analysis and Findings

Following the discussion given in Chapter Four, this chapter discusses and analyzes the test data to additionly find out the statistical significance of the results from these experiments. Finally, to obtain the regression equation of the security mechanism operation.

Chapter Six Conclusion and Future Research

Draw the conclusions and suggestions for this research and provides some ideas for future research.

CHAPTER TWO

FUNDAMENTALS

2.1 Introduction

There are three main fundamentals in this research, namely:

- The subsystem of ITS-ATMS and the communications protocol for ITS ;
- The network security themes for wired network and wireless network, and;
- The basic theorems of modern cryptography.

In this chapter, we shall not only introduce these fundamentals but also mention some possible attacks that the ATMS data transmission might meet to be the considerations for the security mechanism establishment of this research.

2.2 Advanced Transportation Management System

Traffic jam is a popular issue for advanced cities. In the past when cities were not developed so prosperously, traffic engineers could solve these traffic jam issues via building new roadways or broadening the old one. However, we cannot continue using the same old thinking nowadays. The preferred way that we can do is trying to modify or update the traffic device functionality under the existing traffic hardware. In this regard, ITS and its subsystem-ATMS are devised to achieve the desired outcome. As

Figures 1.1 and 1.2 in Chapter One, ATMS utilizes by arranging detectors, monitors, control techniques and communication in groups to collect the real-time traffic data and to transmit these data from field (road side) to the traffic management centre via communications network. The traffic management centre combines all the information and then estimates and sets traffic control policies under the integrated traffic control operation. Eventually, it sends these policies to users, such as, TCIS, RSU to achieve the best transportation efficiency and to improve the traffic safety.

The principal characteristics of ATMS are highlighting the real-time control and combining the main system and its subsystems to provide functions, such as, ramp metering, traffic signal timing plans, traffic accident management, substitute route guide, and, etc. The related techniques of ATMS are like computerized traffic signals, optimum route guide, changeable message sign, ramp metering, weight-in-motion, geographic information system (GIS), and, etc. Figure 2.1 illustrates the subsystems of ITS and the related techniques about ATMS.

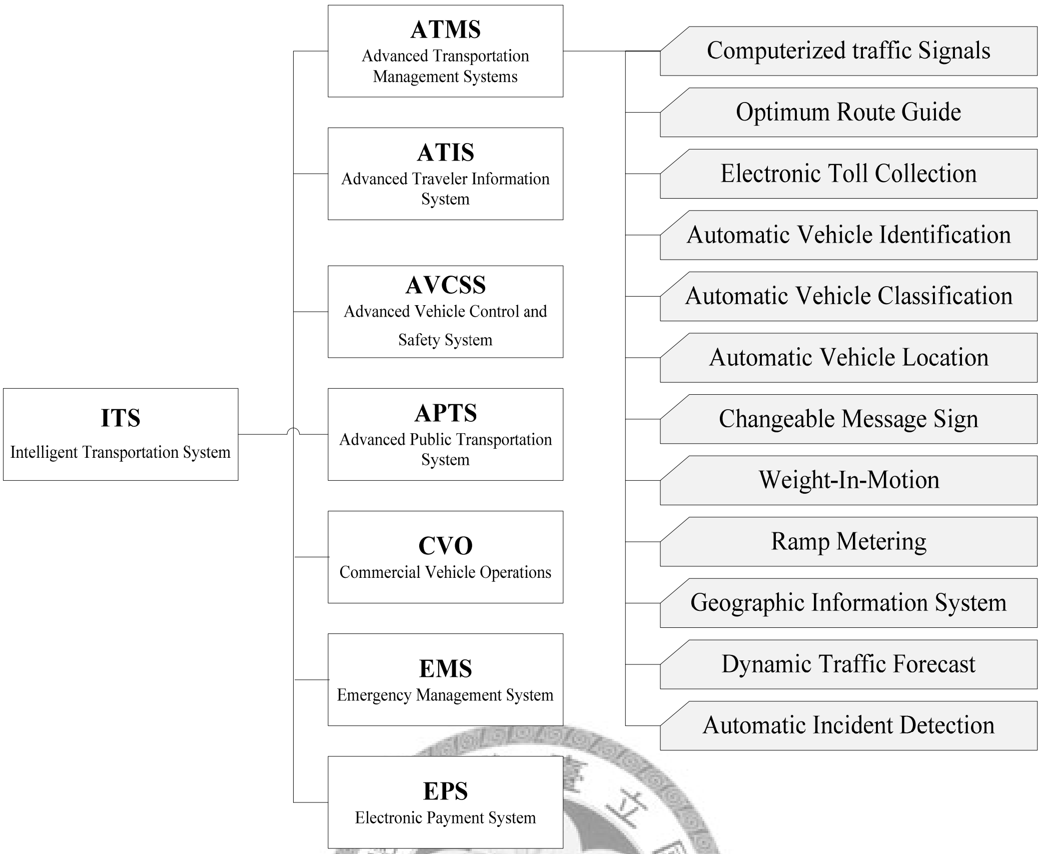

ITS
Intelligent Transportation System
ATMS
Advanced Transportation Management Systems
ATIS
Advanced Traveler Information System
AVCSS
Advanced Vehicle Control and Safety System
APTS
Advanced Public Transportation System
CVO
Commercial Vehicle Operations
EMS
Emergency Management System
EPS
Electronic Payment System
Computerized traffic Signals
Optimum Route Guide
Electronic Toll Collection
Automatic Vehicle Identification
Automatic Vehicle Classification
Automatic Vehicle Location
Changeable Message Sign
Weight-In-Motion
Ramp Metering
Geographic Information System
Dynamic Traffic Forecast
Automatic Incident Detection

Figure 2.1 ITS subsystems and related techniques of ATMS

2.3 NTCIP

2.3.1 Protocol and NTCIP [01] [57]

So far, from the descriptions of traffic control system frameworks, one can know that the communications technology is an important factor for traffic control and ATMS. However, how to make each manufacturer device and computer to communicate or exchange data and messages with each other is also equally critical. The key solution to this problem is the communications protocol. A communications protocol is a set of rules on how messages and data elements are coded and transmitted between electronic devices. In order to successfully communicate, the equipment (device) at each end of the data transmission must use the same protocol. Thus, we can image that the same communications protocol for each machine is similar to the same language for humans to reach the goal of making contact with each other.

NTCIP is a family of communications protocols and data definition standards that have been designed to accommodate the diverse needs of various subsystems and user services of ITS (Figure 2.2 illustrates the role of NTCIP in ITS Architecture). The applications for NTCIP are generally divided into two categories: Centre-to-Centre (C2C) and Centre-to-Field (C2F) communications. For each category applications, NTCIP supports devices and each of the systems used in traffic, transit, emergency management, traveller information and planning/data archiving systems. We can see how various transportation management systems and devices can be integrated by using NTCIP from Figure 2.3 illustration.

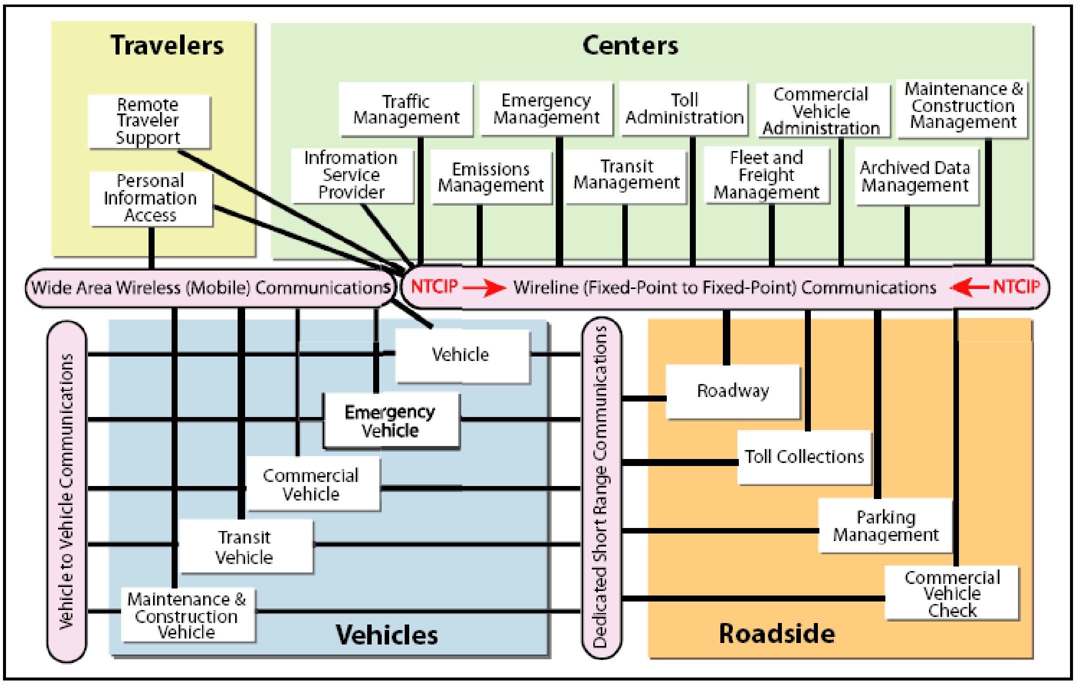

Travelers
Centers
Remote Traveler Support
Personal Information Access
Traffic Management
Emergency Management
Toll Administration
Commercial Vehicle Administration
Maintenance & Construction Management
Infromation Service Provider
Emissions Management
Transit Management
Fleet and Freight Management
Archived Data Management
Wide Area Wireless (Mobile) Communications
NTCIP
Wireline (Fixed-Point to Fixed-Point) Communications
NTCIP
Vehicle to Vehicle Communications
Vehicle
Emergency Vehicle
Commercial Vehicle
Transit Vehicle
Maintenance & Construction Vehicle
Vehicles
Dedicated Short Range Communications
Roadway
Toll Collections
Parking Management
Commercial Vehicle Check
Roadside

Figure 2.2 NTCIP and the National ITS Architecture [01]

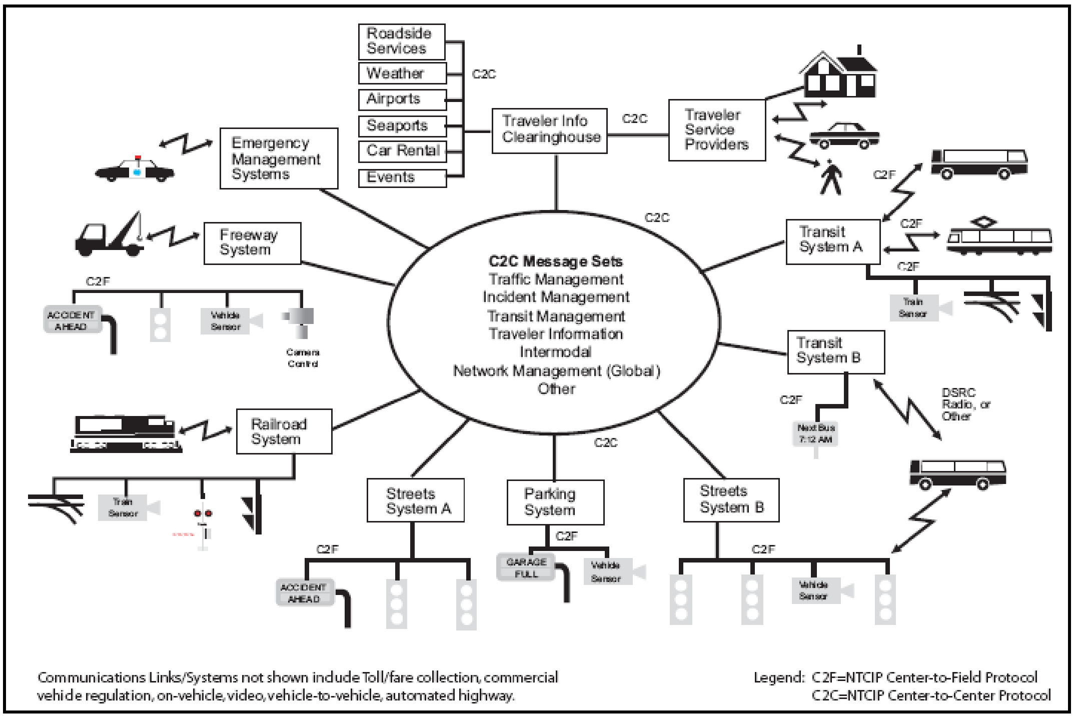


Figure 2.3 Example of ITS Integration Using NTCIP [01]

In addition, the NTCIP establishment is one of the major purposes for National Electrical Manufacturers Association, America (NEMA), the aim of NTCIP is to become the “Internet” for transportation industry to make different manufacturer devices achieve interoperability and interchangeability on the same communications channel as defined below.

- Interoperability

  The ability of multiple devices which are can be of different types to seamlessly work together and interconnect as a single system for some common purposes.

- Interchangeability

  It reflects a ability to put any brand of NTCIP-conformant traffic signal controller in the same system at the same time.

NTCIP presents increased flexibility and choices for many agencies transporting the transportation management systems. This removes obstacles to interagency coordination and allows equipment (device) of different board, types or manufactures to be mixed on the same communications line. Even though NTCIP is used in the original system, operating agencies can benefit in specifying NTCIP in future purchases and upgrades. Generally, the benefits of NTCIP can avoid the traffic devices or systems from becoming obsolete early, and it can provide more choices for manufactures to produce for users or traffic management agencies. It can also forward the control between different kind of traffic devices, and use one communications network for all purposes to ensure maximum flexibility usage of major investment and it can save the largest expense of transportation management system.

2.3.2 Framework, Standards and Protocol Stacks of NTCIP[01]

Chapter One discussed that the communications module of NTCIP is similar to ISO-OSI module. The ISO-OSI module breaks the communications process into seven layers via different functions of communications software and each layer has its defined purpose of adjacent layers.

Basically, NTCIP is originated from the ISO-OSI communications model. In transportation field, data communication between two computers or other electronic devices can be generally considered from five primary layers. However, in order to distinguish the definitions of them from OSI and Internet, NTCIP standards use “levels” to replace “layers”. Figures 2.4 and 2.5 illustrate the framework of NTCIP standards and the relationship between OSI layer modular and NTCIP levels model respectively.

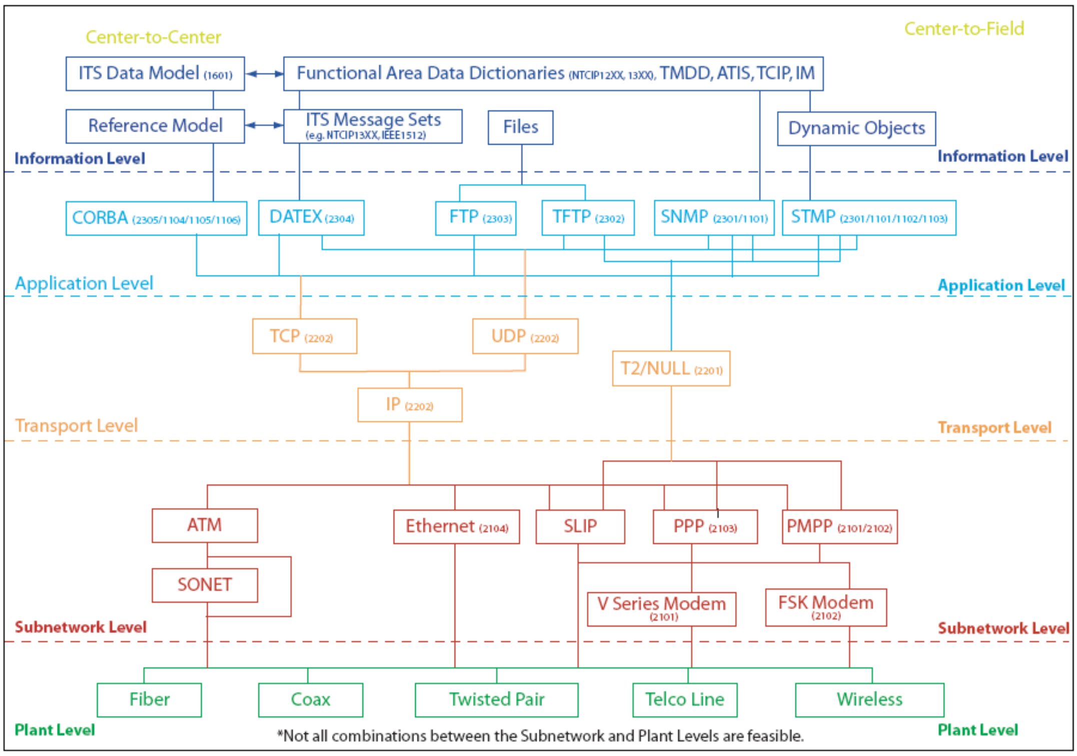
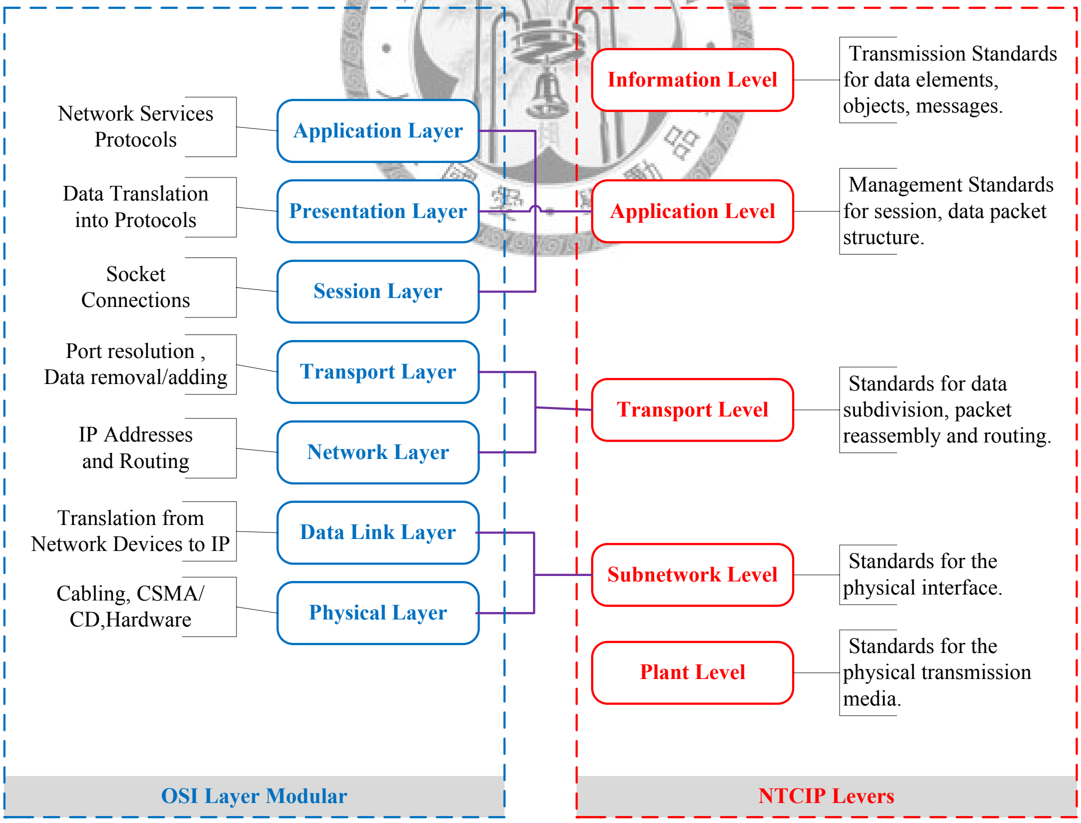


Figure 2.4 NTCIP Standards Framework [01]



Network Services Protocols
Application Layer
Data Translation into Protocols
Presentation Layer
Socket Connections
Session Layer
Port resolution , Data removal/adding
Transport Layer
IP Addresses and Routing
Network Layer
Translation from Network Devices to IP
Data Link Layer
Cabling, CSMA/ CD,Hardware
Physical Layer
Information Level
Transmission Standards for data elements, objects, messages.
Application Level
Management Standards for session, data packet structure.
Transport Level
Standards for data subdivision, packet reassembly and routing.
Subnetwork Level
Standards for the physical interface.
Plant Level
Standards for the physical transmission media.
OSI Layer Modular
NTCIP Levers

Figure 2.5 Relationships between OSI Layers and NTCIP Levels

From the above two figures and the above-mentioned discussion, NTCIP adopts five primary levels (layers) to be the components, namely Information Level, Application Level, Transportation Level, Subnetwork Level and Plant Level. They are discussed as follows:

- **Information Level**

  This level contains the information standards which are above the traditional ISO seven-layer model and represents the functionality of the system to be implemented for data element, objects and messages of ITS information. This is similar to defining a dictionary and a phrase list within a language.

- **Application Level**

  This level contains the application standards which define as the rules and procedures for the data packet structure and exchange or session message. The rules may include definitions of proper grammar and syntax of a single statement, as well as the sequence of allowed statement. These statements are roughly equivalent to Application, Presentation and Session Layers of OSI.

- **Transport Level**

  This level contains the transport standards which define as the rules and procedures for data packet subdivision, packet reassembly and routing when needed, for example, TCP, UDP, IP. The statements are roughly equivalent to

Transport and Network Layers of OSI model.

- **Subnetwork Level**

  This level contains the subnetwork standards which define as the rules and procedures for the physical interface to exchange data between adjacent devices, i.e., HDLC, PPP, Ethernet, and ATM. The statements are roughly equivalent to the Data Link and Physical Layers of the OSI model.

- **Plant Level**

  This level contains the physical transmission media used for communication, i.e., copper wire, coaxial cable, fiber optic cable and wireless. It should be noted that the plant level is an infrastructure choice and not a standard selection choice. However, the plant level selection will have an impact on the subnetwork level selection to which it must interface.

At the beginning, the first NTCIP standards developed were intended for C2F applications. This part involved a new application level standard termed Simple Transportation Management Protocol (STMP), a new subnetwork level standard called the Point-to-Multi Point Protocol (PMPP) and several sets of new standards data elements called dynamic objects definitions at information level.

Each standard specifies one or more protocols to be used at the given level, and it is allowed and required to transmit a message between each of these standards. The course uses a series of standards to transmit messages called “Stacks of Standards” or “Protocol Stack”. During the messages transmissions process between each device, it is possible that, perhaps, a portion of the messages use a set of standard to transmit while the others use another standard to transmit.

NTCIP is the communications protocol framework which is designed specially for ITS. Therefore, NTCIP considers the particular requirements of ITS development to extend a new communications protocol framework which is different from former communications protocols. STMP is a tailor-made communications protocol for transportation system in NTCIP, and it is also a variation of Simple Network Management Protocol (SNMP) developed by NEMA to address low-bandwidth communications links and real-time device monitoring. Due to these are not the main points of this research. Therefore, viewer could know about the detail of SNTP and STMP in Appendix One.

2.3.3 Brief Summary

As mentioned above, we indicate that NTCIP has certain characteristics which are similar as Internet Network; because of this, NTCIP might need to handle some security problems as network security, hacker invading and other kinds of attacks.

Therefore, a suitable security protection for the ATMS data transmission in NTCIP is indispensable and necessary.

2.4 Security Elements [59] [60]

This section utilizes the network security model and the related security definitions from the Telecommunication Standardization Sector (ITU-T) which is the under International Telecommunication Union (ITU) to discuss the security services, security demands and common attack techniques on the open network system in the first place. This is followed by the introduction on the development, types, basic theorems of the modern cryptography and the comparisons in next section.

2.4.1 Network Security Model

Figure 2.6 shows the network security model framework for security service and the security element descriptions. The figure represents, in ATMS, the principals (the transmitter and receiver) at the two extremities could be TMIC and TCIS, respectively. While the TMIC transmits a message to TCIS, both of them have to work in coordination to settle on a route (i.e., a logical information channel) and rely on a communications protocol (e.g., TCP/IP).

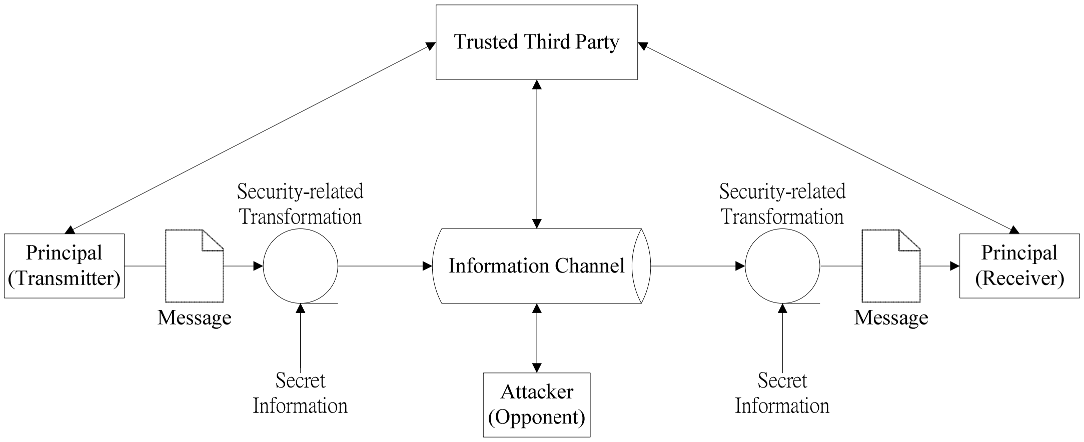


Figure 2.6 Network Security Model [59]

To preserve the information confidentiality, integrity and availability are the goals of information security. Practically, all the security techniques nowadays include two sections discussed below:

- Secure information transformation and transmission

  Briefly, it is the way to carry out the information encryption which uses mathematical calculation for the transmitted messages. It makes attackers unable to comprehend the original message clearly, and insures the transmitter identity via adding the hash code on the original message content simultaneously.

- Secret information is unknown to attackers

  The secret information (e.g., secret key) is known only for the principals. Principals could use the secret key to upset the original message to be ciphertext and utilize the key to decipher into the original message.

Additionally, in order to achieve secure transmission, sometimes, we might need to add the trusted third party (TTP) to manage the secret information and send secret keys to both principals. According to the network security model, it also shows the basic assignments as given below while one designs the security services:

- Design an algorithm which considers the information security to resist the opponent attacks;
- Generate a secret information for the algorithm;
- Design methods to share and transmit the secret information, and;
- Appoint a common communications protocol for both principals usage and utilize the above secure algorithms and secret information to achieve the specific security services for cases.

2.4.2 Security Attack Techniques

ITU-T distinguishes the usual security attack techniques into the passive attack and the active attack. The passive attack is one in which the attacker merely gains access to the asset. However, in the active attack, the attacker is able to alter, manipulate, route, or otherwise actively change the asset.

- Passive Attacks

  The essence of passive attacks is to wiretap or monitor the route which is under information transmission; the major goal of attackers is to intercept and analyse the data packets. The possible passive attack patterns in ATMS data transmission might be:

i. Eavesdropping and wiretapping;

ii. Traffic analysis;

iii. Analysis of the PUD headers of messages for the illegitimate purposes;

iv. Copy of PUD data to other systems other than the intended destinations, and;

v. Cryptanalysis.

As the passive attacks would not modify the messages; therefore, it is quite difficult to detect weather the transmitted data is attacked or not. The useful method is to utilize encryption techniques to prevent this kind of attacks.

- Active Attacks

By comparison, active attack relates to modifying and counterfeiting data. It can subdivide into the following four categories:

i. Denial of Servicer (as condition (b) of Figure 2.7)

Attackers would interrupt the communications connection and obstruct the normal operation or management of the communication devices.

ii. Reply (as condition © of Figure 2.7)

Attackers would intercept the messages and send them repeatedly.

iii. Modification of Message (as condition (d) of Figure 2.7)

It is the attack technique that needs us to pay attention, especially in ATMS, attackers could modify a part of the message or delay the message transmission to make receivers getting the wrong messages.

iv. Masquerade (see as condition (e) of Figure 2.7)

In ATMS, attackers could masquerade TMIC to issue illegitimate commands e.g., force to modify the traffic signal timing plans.

The characteristics of active attacks are contrary to passive attacks. Comparatively, it is difficult to prevent active attacks as we are unable to know when the attackers would attack the system. It is a heavy load if we protect the system at all times; hence, how to detect active attacks and prevent the destructions is the better priority than system protection.

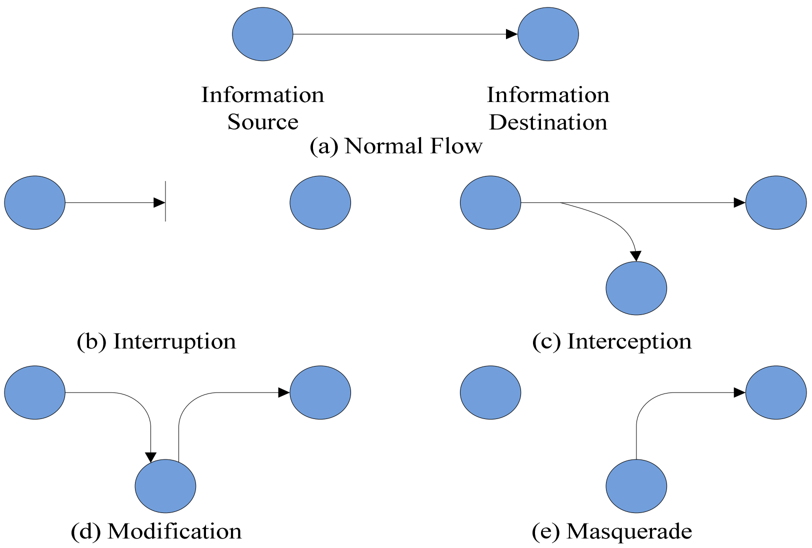


Figure 2.7 Illustration for active attack types [57]

2.4.3 Security Services

ITU-I defines the following security services upon the open communications system to ensure the security for the core system and data transmission securely [03].

- Authentication

  It is a process which allows checking with certainty identification of a party involved in a communication. It generally follows identification, establishes the validity of the claimed identity and guards against fraudulent actions.

- Access Control

  It is a protection for system resources against unauthorized access. In ATMS, we have to set up the process by which the use of system resources is regulated according to a security policy and is permitted only by authorized users according to that policy.

- Data Confidentiality

  It is to ensure that the transmission data would not be attacked by passive attacks. In ATMS, we would not expect that the transmission information to be known to the attackers. The usual protection method is to encrypt the transmission data packets via cryptography technologies.

- Data Integrity

  In data confidentiality, the objects of protection could be the message stream, single message or the section of message. Due to only protecting the segment message would reduce the operation efficiency, therefore, the most direct way is to use the cryptographic technologies to protect all the data as well.

- Non-repudiation

  It is the way to prevent a transmitter or a servicer denying the later that one has sent a message or performed an action.

2.5 Cryptography Technologies

As noted earlier, we introduced the network security model including the security members, security services and the attack techniques as well. As of now, attackers could eavesdrop, intercept, or modify the information much easier in wireless communication environment than in wired network, and the wireless communications would be the main stream for transportation control system usage additionly. Therefore, the cryptography techniques become the major solution to enhance security issues.

Overall, the modern cryptography technologies nowadays include two categories: symmetric cryptosystem and asymmetric cryptosystem. The basic procedures are to transform the plaintext into ciphertext through the use of a secret key with the encryption/decryption algorithms to ensure the data confidentiality. In addition, we need to ensure the data source and integrity, and further, to verify the data is received by the designators or the public keys of asymmetric cryptosystems not be modified. Moreover, one could adopt the message digest technique to ensure the data integrity and authentication.

2.5.1 Symmetric Cryptography

Symmetric cryptography is also called traditional, secret-key or private-key cryptography. It utilizes transformation techniques to transform the message to achieve the message encryption. The symmetric cryptosystem architecture can be depicted as shown in Figure 2.8. In the figure, the left side of the dotted line is encryption procedure while the right side is decryption procedure.

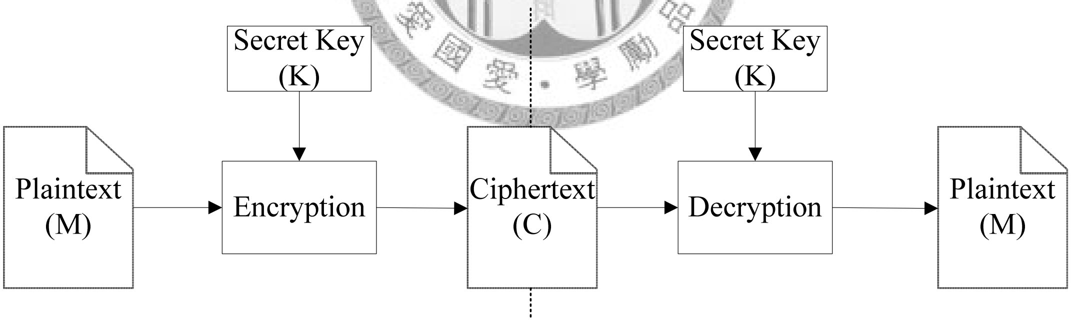


Figure 2.8 Architecture of symmetric cryptosystem

Broadly speaking, the symmetric cryptosystems is composed via following five factors, namely: plaintext, encryption algorithm, secret key, ciphertext and decryption algorithm.

- **Plaintext** is a message in its native form which one could simply read it;

- **Encryption Algorithm** is the algorithm which is the mathematical process for the scrambling and descrambling of a data stream;
- **Secret Key** is the value stream which is unrelated to the plaintext, and is the input of the encryption/decryption algorithm as well. The encryption algorithm would produce different output via different secret key. In symmetric cryptosystem, one must use the same secret key for a encryption/decryption cycle, that means one cannot use other secret key to decrypt a ciphertext which is decrypted by specific secret key;
- **Ciphertext** is the result of encryption operation and it should appear as an incomprehensible flow of byte, and
- **Decryption Algorithm** is the inverse function of encryption algorithm and could transform the ciphertext into the plaintext via the secret key.

The relationship between these factors and the formal definitions of symmetric cryptography can be expressed by the following formulae.

The encryption function **E** can be expressed by Equation 2.1:

$$\mathbf{E:\ (M) \times K = C} \tag{2.1}$$

M: The set of plaintexts

K: The set of secret keys

C: The set of ciphertexts

or by the following equation:

$$\mathbf{E_K \times (M) = C} \tag{2.2}$$

in which $\mathbf{E_K}$ is the encryption algorithm with secret key **K**. The decryption function **D** can be expressed by Equations 2.3 or 2.4:

$$\mathbf{D: (C) \times K = M} \tag{2.3}$$

$$\mathbf{D_K \times (C) = M} \tag{2.4}$$

From the above equations, one can understand that while one knows the secret key, then the plaintext can be computed easily. Thus, in essence, there are two major conditions on the security of symmetric cryptosystems:

- It is necessary to strengthen the secret key protection to prevent attackers from cracking the ciphertext or secret key even though they might know the encryption algorithms or gotten a part of the ciphertext already.
- The transmitter and the receiver have to gain the secret key via a secure way and a safe space to arrange the secret key as well. If one owns both the secret key and

the encryption algorithms, the ciphertext can be cracked easily.

After knowing these two conditions, in symmetric cryptosystems, it is important to safeguard the secret key strictly. Therefore, how to establish a secure space and transmission method to store and transmit the secret keys are more important than the encryption/decryption algorithm adoption.

On the other hand, the symmetric cryptosystems can be divided into two categories: stream cipher and block cipher. The stream algorithms perform on strings of arbitrary length by handling the plaintext as a continuous input stream and generating ciphertext output stream at the same time. In block algorithms, the plaintext is handled by blocks, and therefore, the length of the plaintext must be multiple of the block size. In addition, the block cipher consumes less core resource than stream cipher; thus, the block cipher becomes the main stream nowadays. As follows, the common block cipher techniques of symmetric cryptosystems are introduced.

(a) DES

Data Encryption Standard (DES) is developed by *Walter Tuchman* and *Carl Meyer* who are the employees of IBM, and is adapted as Federal Information Processing Standard (FIPS PUB 46-2) by the National Bureau of Standards (NBS) in 1977. After that, DES had been widely used by industry [24] [28].

The basic and principal techniques of DES are confusion and diffusion. The confusion method makes ciphertexts give no clue to the attackers about the plaintext, and the diffusion technique ensures that the slightest difference in plaintexts will result in diffusion, and hence, the results in totally different ciphertexts.

The size of a single message block in DES is limited in 64 bits and the length (size) of secret key is only 56 bits to be used. Therefore, the security level of DES declines rapidly along with the dramatically growth of computability of modern computers due to 56-bit secret key length, and which has become the greatest weakness when one attacks the protected system by brute-force attack nowadays. Figure 2.9 shows the encryption and the decryption procedures of the DES cipher algorithms.

$M_{(i)}$
$DES_{K(i)}$
$C_{(i)}$
$C_{(i)}$
$DES^{-1}_{K(i)}$
$M_{(i)}$

(a) Encryption

(b) Decryption

Figure 2.9 Encryption and decryption procedures of DES

(b) Blowfish

Blowfish is developed by *Bruce Schneier* in 1993 and has the following advantages[28]:

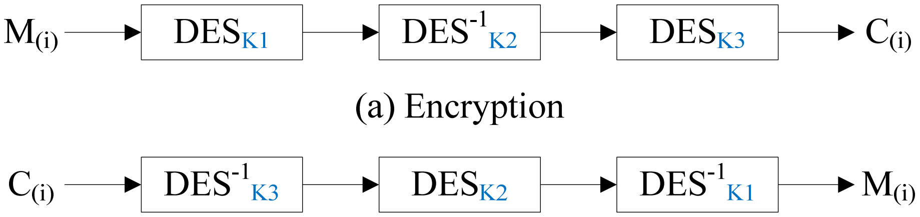
- The architecture of Blowfish cipher algorithms is simple and the operation is not complex as well;

- The memory Blowfish used is less than 5K;
- The operation rate is fast;
- The secret key is changeable, the maximum secret key length could be 448 bits, and the user could improve the security level via increasing the secret key length.

(c) Triple-DES [28] [32]

As the characteristics of DES, the short length secret key is the major misgiving for DES. Because of it, the National Institute of Standard and Technology (NIST, known as NBS) publishes the new standards for DES－Triple Data Encryption Standard (Triple-DES, 3-DES, T-DES) in 1999. The most important modification is to increase the secret key length to 168 bits via triple DES operations (see Figure 2.10).

Triple-DES had been subjected to many severe tests, so far, beside brute-force attack; one could conclude that there was no single attack could crack it effectively. However, some defects of Triple-DES restrict the behaviours. For instance, due to achieving the triple DES operation, it might increase loading onto the core system, making the operation efficiency to worsen, and on the other hand, the message block size still limits only 64 bits as DES.



(a) Encryption

(b) Decryption

Figure 2.10 Encryption and decryption procedures of Triple-DES

(d) AES [41] [44]

Advanced Encryption Standard (AES) is the newly encryption standard which was developed by two Belgian cryptographers－Dr. *Joan Deamen* and Dr. *Vincent Rijmen* and announced by NITS after DES and Triple-DES on November, 2001.

Although, the existing AES algorithm is not the original *Rijmen* pattern which supports a large range of block and secret key length as the block size is fixed at 128 bits and the secret key length could be chosen for 128, 192 or 256 bits. In computer computing, 1 byte equals 8 bits, the 128 bits fixed block is normally 128÷8=16 bytes. AES operates on a 4×4 array of bytes, called *state*, and most AES calculations are done in a special finite field.

As other cryptography algorithms, the encryption procedures are applied to make up rounds of keyed transformations between the input plaintext and the final output ciphertext. The encryption procedures could divide into four operations (stages) which one utilizes the transposition method and others use substitution techniques as Figure

2.11 shown, namely:

- **SubBytes** operation is to utilize S-box to carry out substituting for each bit of message block;
- **ShiftRows** operation is a simple raw transposition process of the 4×4 array;
- **MixColumns** operation is to utilize GF(2^8) calculation to carry out substituting for each column of the 4×4 array, and
- **AddRoundKey** is a substitution operation via XOR operation.

Generally speaking, RSA cryptography is the major algorithm of symmetric cryptosystem today. Thus, this research adopts RSA cipher algorithm to be the consideration for the security mechanism establishment as well. The internal detail operation of RSA cryptography could refer to Appendix Two.

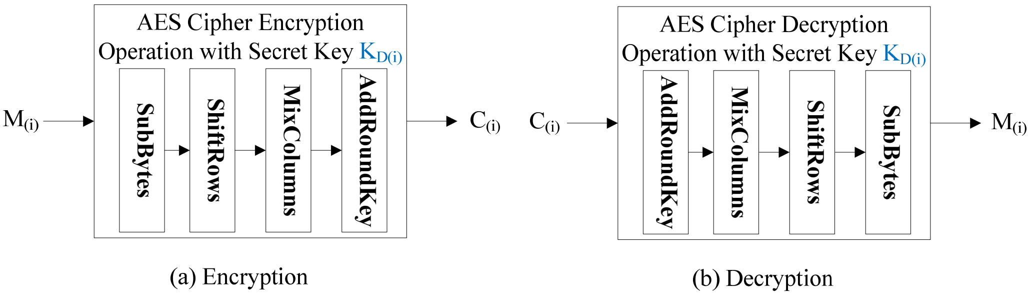


Figure 2.11 Encryption and decryption procedures of AES

2.5.2 Asymmetric Cryptography

In Section 2.5.1, we introduced about symmetric cryptosystems and pointed out that the security is in accordance with the secret key distribution and protection. However, these have also become the weakness of symmetric cryptosystems. Asymmetric cryptosystems (also termed as the public-key cryptosystem) which are sprung out by *Whitfield Diffie* and *Martin Hellman* in 1976 is the most important breakthrough in modern cryptography. Different from symmetric cryptosystem, it utilizes mathematical functions to achieve encryption/decryption. The major difference between asymmetric cryptosystem and symmetric cryptosystem is the use of separate keys (key pair): public key and private key. The separate key concept influences and increases the secret key protection for distribution and protection significantly.

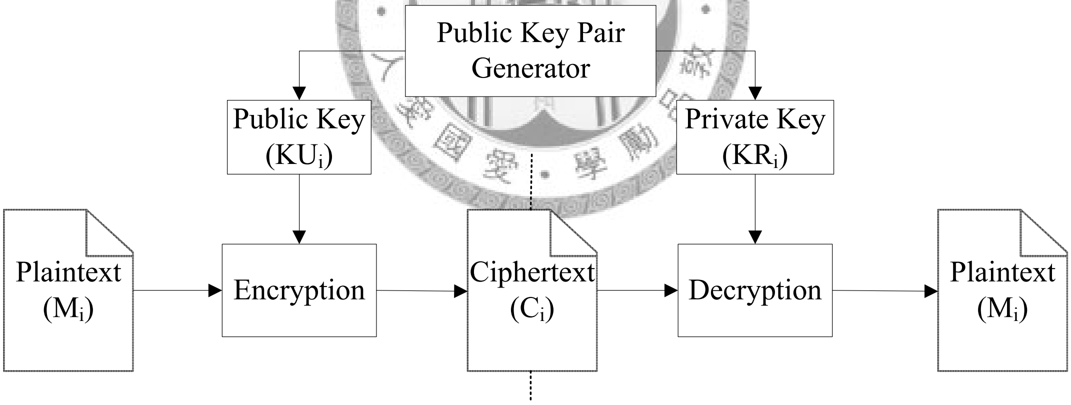


Figure 2.12 Architecture of asymmetric cryptosystem

Figure 2.12 shows the architecture of asymmetric cryptosystems. For illustration, it is noted that asymmetric cryptosystem uses one key to encrypt and another key to decrypt. The principal characteristic is that even though the algorithms and the public key (encryption key) are known, it is computationally infeasible to crack the private key. The compositions of asymmetric cryptosystems are given by the following five factors:

- **Plaintext** is a message in its native form which one could simply read it and is the input of the encryption algorithm;
- **Encryption Algorithm** is the algorithm for the plaintext transformation via asymmetrical cipher;
- **Public Key and Private Key** is the key pair which is created via the mathematical algorithm. As implied by the name, the public key is open to public; everyone can obtain the public key to encrypt the plaintext **M**. Relatively, only the right one can obtain the private key to decrypt the ciphertext;
- **Ciphertext** is the unreadable message which is decrypted from the plaintext and the public key via asymmetrical algorithm , and
- **Decryption Algorithm** is the algorithm for decryption with the matching private key and suitable asymmetrical cipher to transform the ciphertext into the original plaintext.

The encryption/decryption procedures can be compared with Figure 2.18 and expressed by the following statements and formulae.

1) The terminal system on the Internet Network would create a key pair to encrypt/decrypt the message;

2) The terminal system would announce the public keys on the open network, public could access them from the terminal system;

3) While transmitter **A** wants to send a message to receiver **B**, the transmitter **A** has to transform the message into the cryptograph via the public keys. The encryption procedure can be expressed by Equation 2.5:

$$\mathbf{E:\ (M)\ \times\ KU\ =\ C} \tag{2.5}$$

M: The set of plaintext or the original message

KU: The set of encryption key, termed as the public key

C: The set of cryptograph as ciphertext

or in the following form:

$$\mathbf{E_{KU}\ \times\ (M)\ =\ C} \tag{2.6}$$

in which $\mathbf{E_{KU}}$ is the encryption algorithm with public key **KU**.

4) When the receiver **B** receives the message which is the unreadable message, **B** has to decrypt the unreadable message via the public key. Due to the public key is only owned by **B**, therefore, no one could decrypt the message which transmitted from **A**. In essence, the decryption process can be expressed by the following equations:

$$\mathbf{D:\ (C) \times KR = M} \tag{2.7}$$

or the another form:

$$\mathbf{D_{KR} \times (C) = M} \tag{2.8}$$

in which **KR** and $\mathbf{E_{KR}}$ are the public key and decryption algorithm with the public key **KR** respectively.

As mentioned above, the major difference between symmetric cryptosystem and asymmetric cryptosystem is the key generator, and it could diminish the weakness for symmetric cryptosystem. Subsequent content shall introduce two representative asymmetric cryptosystems: RSA and ECC. As RSA algorithm is the main stream of asymmetric cryptosystems, it warrants a more thorough discussion in Appendix Two.

(a) RSA [29] [41]

The Rivest-Shamir-Adleman (RSA) cryptography algorithm is invented and confirmed by *Ron Rivest, Adi Shamir* and *Leonard Adleman* in 1977. Before that, the public cryptography is just only a concept which published by *Diffie* and *Hellman* in 1976. Nowadays, RSA has become the most popularly used in asymmetric cryptosystems. Therefore, the security mechanism of this research also uses RSA cipher algorithm in asymmetric cryptosystem. In addition, Bouncy Castle Cryptography Extensive which is one of the Java programming extensions provides 768-bit, 1024-bit and 2048-bit public key pair in implementation.

(b) ECC [28] [29]

The Elliptic Curve Cryptography (ECC) is invented by *Neal Koblitz* and *Victor Miler* in 1985. Before ECC, RSA is the major chipper algorithm in asymmetric cryptosystems. In order to improve the security level, the secret key length has become longer in RSA. The characteristic of ECC is that it could use shorter key length to achieve the security level as the long length key in RSA, e.g., the security level at 205 bits secret key in ECC is similar to the 2048 bits secret key in RSA.

Although ECC has already developed for a span, however, its commercial application has yet to be fully exploited. That is because the reliance in ESS is not as well as RSA; therefore, RSA algorithms are still the main stream algorithms in asymmetric cryptosystems nowadays.

2.5.3 Message Digest and Message Authentication [29] [42]

The message digest and the message authentication codes (MAC) are based on a notion of hashing as well. The hash function is to chop or concert a large piece of data into a smaller one; it could be more manageable piece of data that we can easily work with in memory. Hence, the hash function is essentially a compression function. In generally, the output from the hash functions is called the Message Digest or Hash Value. A hash function can be expressed by Equation 2.9 and illustrated as Figure 2.13.

$$H : X \Rightarrow Y, \{0,1\}^{*} \Rightarrow \{0,1\}^{n} \qquad (2.9)$$

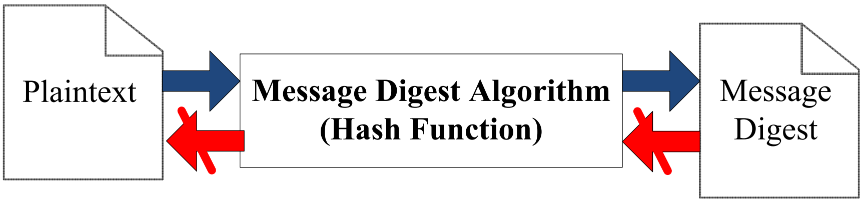


Figure 2.13 Architecture of message digest

Another characteristic of hash function is its irreversibility and the hash algorithms must be collision resistance as well. Namely, it is impossible to deduce *x* if only *h(x)* is known and generate the same message digest for different message. That is because why hash functions are sometimes called one-way hash function.

In essence, hash functions are widely used in many aspects of security and hash values could be used to maintain data integrity by attaching hash values to the message. As above, the MAC is a type of the hash functions as well; it provides reasonable assurances that the content of a message which has not been tampered with. In other words, only the owners of the secret keys could generate or verify the message digest.

The popular and recommendable message digest algorithms nowadays are the MD series algorithm and SHA-1 algorithm. Additionly, the Java Cryptography Architecture (JCA) introduced an engine specific for working with cryptography one-way hash functions, the message digest engine. The Sun Microsystems provider supports MD5 and SHA-1 natively, and other providers may offer their alternative message digest algorithms; following are the descriptions of these two message digest algorithms.

(a) MD Series Algorithm

This series of message digest algorithms is designed by Dr. *Ron Rivest* who is also one of the inventors of RSA, and there are three types of MD series algorithms, namely: message digest 2 (MD2), message digest 4 (MD4) and message digest 5 (MD5). Each of these message digest algorithms is 128 bits in length, and the fastest and slowest operation rate of MD series algorithms are MD2 and MD5 respectively. In addition, there are papers published from RSA Laboratory that describe a weakness in the underlying mechanics of the algorithm that could lead to collisions-a violation of collision-free properties we expect for a cryptographic on-way hash. While there is no known documentation that describes how to exploit this information to attack the algorithm, knowing that the risk is there would suggest that it is prudent to avoid the use of MD2 where possible.

(b) SHA-1 Algorithm

The other predominate one-way hashing algorithm is the Secure Hash Algorithm 1 function, or simply SHA-1. SHA-1 is an algorithm designed by National Security Agency (NSA) and every hashing operation resulting in a 160-bit hash. It is slightly larger than the 128-bit hash produced by an MD5 operation. In addition, in cryptography, every bit counts, literally, and the meagre increase in hash size may result in a noticeable slower hash generation on large files compared with MD5.

2.6 The Possible Attack Discussions on ATMS Data Transmission

On the first half of this chapter, the relationship between ITS, ATMS and NTCIP were introduced and discussed in detail. Besides, one of the major goals of NTCIP is expected to become the "Internet" in transportation file. As mentioned earlier, NTCIP follows the ISO-OSI modulus as well; this means that NTCIP would face the security issues as Internet Network. On the other hand, strictly speaking, the NTCIP object transmission nowadays is exposed and unprotected on the open network and very few studies concern with these points so far.

One could utilize existing software to intercept the object packets during the transmission processes. In addition, due to the data packet structure of NTCIP object is similar to ISO-OSI modulus, and the STMP message form is much simply than the

SNMP message form; therefore, attackers could read, modify or attack the message easily while they intercept these message packets. Nobody could imagine the consequence of our traffic control management system is invaded. Hence, the NTCIP standards publisher－NEMA also points out that it is necessary to establish a set of security mechanism to resist the attacks and this security mechanism should be provided with flexibility for different environments and conditions.

Therefore, this section shall discuss some possible attacks that ATMS might meet during the NTCIP object transmission even if we have already added cryptography techniques in it; namely: masquerade, man-in-the-middle-attack, eavesdrop, modification of message and message reply, various attack, host invading and etc.

- **Masquerading**

  As Figure 2.14 illustrated, one might try to masquerade the TMIC manager to transmit the malicious or illegal messages (commands) to TCIS, RSU, VMS, etc to cause the traffic confusion. Additionly, on the other hand, attackers might generate the counterfeit secret key or public key pair while the transmission process has already added a security mechanism to achieve the illegal activities.

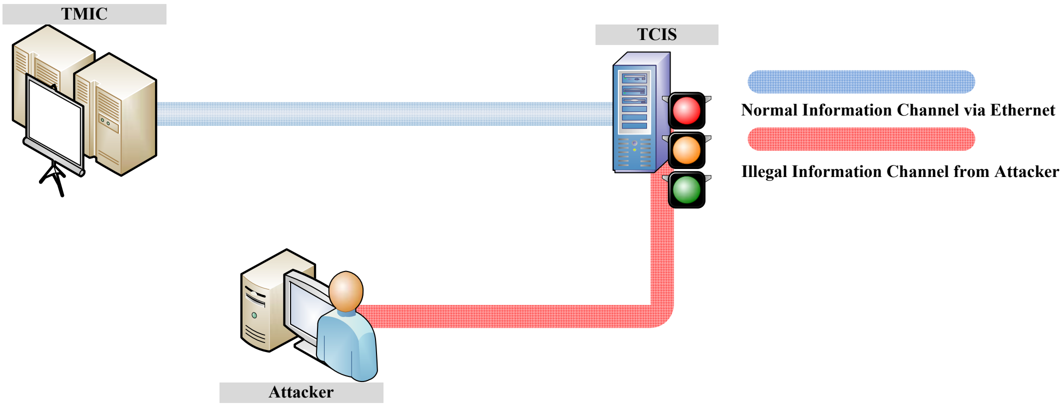

TMIC
TCIS
Normal Information Channel via Ethernet
Illegal Information Channel from Attacker
Attacker

Figure 2.14 Masquerading Attack in ATMS Data Transmission

- **Eavesdropping**

One might attempt to intercept the transmitted messages or data packets and read the content of them as shown in Figure 2.15. However, if the transmitted messages have been protected during the information channel, one might need to catch the secret key/private key first or crack the secret information via cryptanalysis. On some situations which the encryption/decryption algorithms and the secret key length are known by attackers, attackers might obtain the secret key via brute-force attack to guess all the possible secret key combinations.

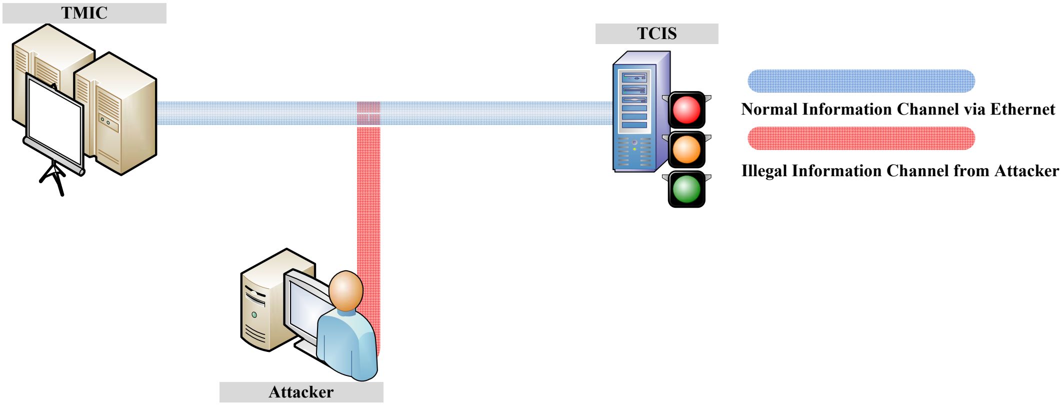

TMIC
TCIS
Normal Information Channel via Ethernet
Illegal Information Channel from Attacker
Attacker

Figure 2.15 Eavesdropping Attack in ATMS Data Transmission

- **Man-In-the-Middle Attack**

Shown as Figure 2.16, one might collect the net flow rate between TMIC and TCIS by eavesdropping and then analyze the observational data to get the point of time of the secret key exchange. After obtaining these data, one might intercept the data packets which are transmitted between TMIC and TCIS (e.g., NTCIP object, secret key, public key pair and etc) and carry the illegal messages to TMIC and TCIS respectively to control the traffic management system successfully.

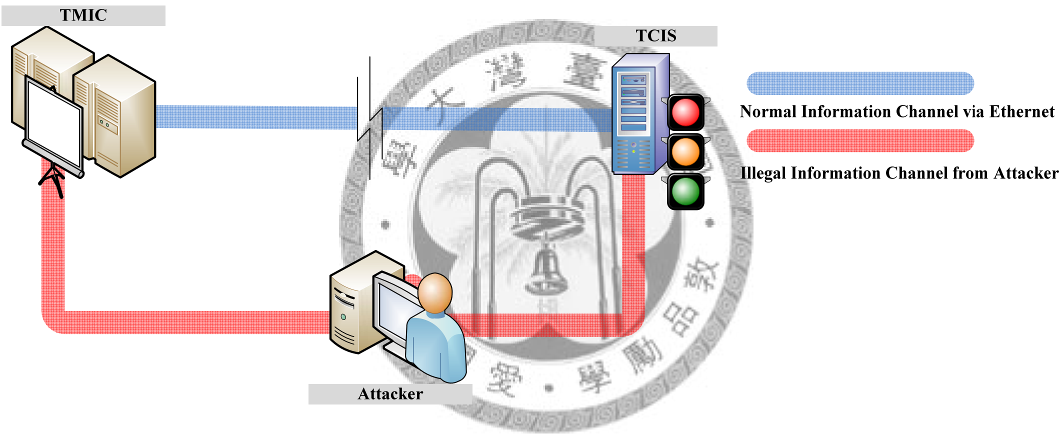

TMIC
TCIS
Normal Information Channel via Ethernet
Illegal Information Channel from Attacker
Attacker

Figure 2.16 Man-In-the-Middle Attack in ATMS Data Transmission

- **Message Modification**

As man-in-the-middle attack, one might intercept the message packets and further to add/delete characters in the messages or modify them to achieve the illegal goals. For instance, attackers could catch the VMS message, modify the content of it and then sent the modified VMS message to road-side. In this case, road users would receive the wrong messages and cause some unnecessary traffic accidents finally.

On the other hand, one has to crack the related ciphers and own the secret keys as mentioned in eavesdropping first if a security mechanism is added for the data transmission. However, even though one has already cracked the ciphers and gained the secret keys, but the message is modified and the character numbers or message length are not agreeable with the original message, this would make the ciphertexts be decrypted unsuccessfully as well as to ensure transmitted message is still protected safely by the properties of cryptography technologies (refer to Section2.5, the combinations of decryption procedure are the right key, acceptable ciphertext and decryption algorithm). Therefore, while the TCIS often receive the unsuitable data packets that could not be decrypted smoothly; this kind of phenomenon provides system managers a warning that the system might be eavesdropped.

- **Message Reply**

As noted above, another possible attack is that one might intercept the transmitted message and send it to TCIS after a while without modifying it. It seems that there is no serious influence for the control system. However, "real-time" is one of the important characteristics of traffic control. For instance, if one catch traffic signal timing packets at off-peak hour and transmit the packet at peak hour; this would make the traffic signal phasing to be in disorder and then cause traffic confusion.

2.7 Summary and Evaluations

ATMS adopts NTCIP to be the communications protocol; however, the range of NTCIP is very wide; it not only includes the transportation filed but also touches on the telecommunication, electron, communication and others. Therefore, the studies of this research are limited and focus on the traffic control under the NTCIP implementation.

From the characteristics of ATMS and the potential attacks for data transmission in traffic control systems, the first thing we notice is that we could realize that a suitable security mechanism establishment is necessary and an urgent demand in traffic control management system. In addition, the basic security elements indicate the requirements for information security demand and the cryptography technologies are the ways to satisfy these needs as below:

- Attackers might pretend to be member of the traffic control centre to carry out the illegitimate purpose, e.g., obtain the system controller's passwords;
- The control management should establish an access control mechanism to avoid unauthorized invasion into the core system;
- We should ensure the integrity during the data packet transmission, and
- One could read the content of STMP message easily due to the simply form.

On the other hand, as the mentioned in Section 2.5, the major advantage and weakness of symmetric cryptosystems are the fast operation and the weak secret key protection (i.e., secret key store and transmission). In addition, in asymmetric cryptosystems, the public key pair protections are enough sufficiently, but the encryption/decryption operations are not efficiently and not fast as symmetric cryptosystems. Tables 2.1 and 2.2 represent the characteristics and evaluations of each cryptography algorithm for the symmetric cryptosystem and asymmetric cryptosystem respectively, and Table 2.3 provides the comparison between these two cryptosystems.

Table 2.1 Characteristics of symmetric cryptography algorithms

	DES	**Triple-DES**	**Blowfish**	**AES**
Key length	56 bits	168 bits	Changeable; Max=448bits	128/192/256 bits
Block size	64 bits	64 bits	64 bits	128 bits
Specific	－Simple and small －Fast operation －Security nowadays is insufficiently	－Security might be enough －Complex operation －Hard to implement	－　Fast operation －Simple and small －The key length could be changeable	－Security lever is well －The block size is bigger －Development well and high reliability
Year	1970	1999	1993	2001

Table 2.2 Characteristics of asymmetric cryptosystem algorithms

	RAS	**ECC**
Key length	768/1024/2048 bits	160 bits (recommendable)
Specific	－ Long-time development and highly reliability －The mathematical theories of RSA are easy than other asymmetric algorithms. －The representative of asymmetric cryptosystems	－It uses shorter keys to approach the higher security level than other asymmetric algorithms －The mathematical theories of ECC are more complex －Not well-development
Year	1978	1985

Table 2.3 Comparisons: symmetric cryptography vs. asymmetric cryptography

	Symmetric cryptosystem	**Asymmetric cryptosystem**
Operation Conditions	－Use the same secret key for encryption and decryption. －Use the same cipher algorithms and secret key in transmitter-side and receiver-side community.	－Use the same algorithm and a key pair for encryption/decryption procedure; in which, the public key is used for encryption and the private key is used for decryption. －The transmitter-side and the receiver-side need to hold the public key and private key respectively.
Security Requirements	－Require to ensure the secret keys are not owned by attackers. －If there is no usability security information, it is difficult to decrypt the ciphertext. － Even though one obtains the cipher algorithm and certain quantity of ciphertexts, one cannot calculate the secret key from these data.	－Require to protect the private keys only. －If there is no usability security information, it is difficult to decrypt the ciphertext also. － Even though one obtains the cipher algorithm, certain quantity of ciphertexts and the public key, one still cannot calculate the private key and decrypt the ciphertexts to get the plaintexts as well.
Comparisons	The encryption/decryption operations are fast; but the secret key protections are insufficient and not enough.	It is effective to secure the private key via using key pair; but the encryption/decryption operations are much slower than symmetric cryptosystem.

It seems that in order to protect the transmitted data and avoid the possible attacks during the data transmission, we have to add a suitable security mechanism in it. However, how to choose and establish the suitable and secure sufficiency security mechanism are the indispensable issues. It follows from what has been discussed thus far that utilizing hybrid cryptosystem is the appropriate method to integrate the advantages in both of symmetric cryptosystem and asymmetric cryptosystem. In hybrid cryptosystem, the functions of asymmetric cryptosystem are to verify the user identity and ensure the data packet integrity; in addition, it uses symmetric cryptosystem to protect the data packets due to the operation in symmetric cryptosystem is much faster than in asymmetric cryptosystem

CHAPTER THREE

SECURITY MECHANISM ESTABLISHMENT AND SECURITY PROTECTION DISCUSSION

3.1 Introduction

The characteristics of the ATMS data transmission, network security and the modern cryptographic technologies were introduced in Chapter Two. In view of this discussion, this research utilizes a hybrid cryptosystem which integrates with symmetric cryptosystem in AES, asymmetric cryptosystem in RSA and massage digest (MD5/SHA1) to establish a security mechanism for ATMS data transmission. The security level in ATMS would be improved, and the security loopholes in data transmission would be modified via this security mechanism establishment as well.

Naturally, “security” is the essential factor for the security mechanism. This chapter discusses the protection capability against attacker invasion of the security mechanism. On the other hand, cryptanalysis is too complicated to be examined in detail for the intent of this research study. However, the use of the related cryptanalysis research and data to verify and analyse the security level of the security mechanism in this research would be explored. As noted earlier, the encryption/decryption procedure addition would consume the source of the core system and generate more negative-effects for it as well. These kinds of issues about the system operation efficiency shall be discussed and examined in the next chapter via the designed experiments.

3.2 Conceptions of Information Security in this Study

Li Gong who is a Java security designer had presented a briefing about the cryptography security issues in 1997 [32]. In which, he indicated some inequalities to interpret the security issues for cryptography. These have provided ideas on the starting point and the conceptions of the security mechanism in this research. The inequalities and the explanations are given below:

i.Security! ≠ Cryptography

First, one should realize that the security mechanism addition onto an application program is not equated to the total security protection. The security level is decided by the whole system operation and implementation. In other words, the cryptography technologies are just the tools to establish a security system, and the security level should be comparative and not be absolute; therefore, it should be considered from the requirements and expenses.

ii.Correct Security Model! ≠ Bug-Free Implementation

Even if we have a faultless security model, inevitably, there are still some bugs would be discovered by attackers. That means if the security model is correct and nothing wrong in it, security designers only need to find out the bugs during the implementation. On the contrary, if the security model is wrong or not secure originally, designers should design it afresh.

iii.Testing! ≠ Formal Verification

Generally, testing seems a good idea to examine the system security, but it does not ensure the system is absolutely secured. However, the formal verification means that the security mechanism should pass through the cryptanalysis by professionals or cryptanalysts.

iv.Component Security! ≠ Overall System Security

System security is closely connected and inseparable from all the links of the system, and each link of the system might be attacked.

From the standpoints given above, strictly speaking, one could say that there is no unexceptionable security mechanism; one could only have a suitable one which is dependent on the security requirements like the system efficiency, expenditure on security mechanism design or establishment, security level demand or others.

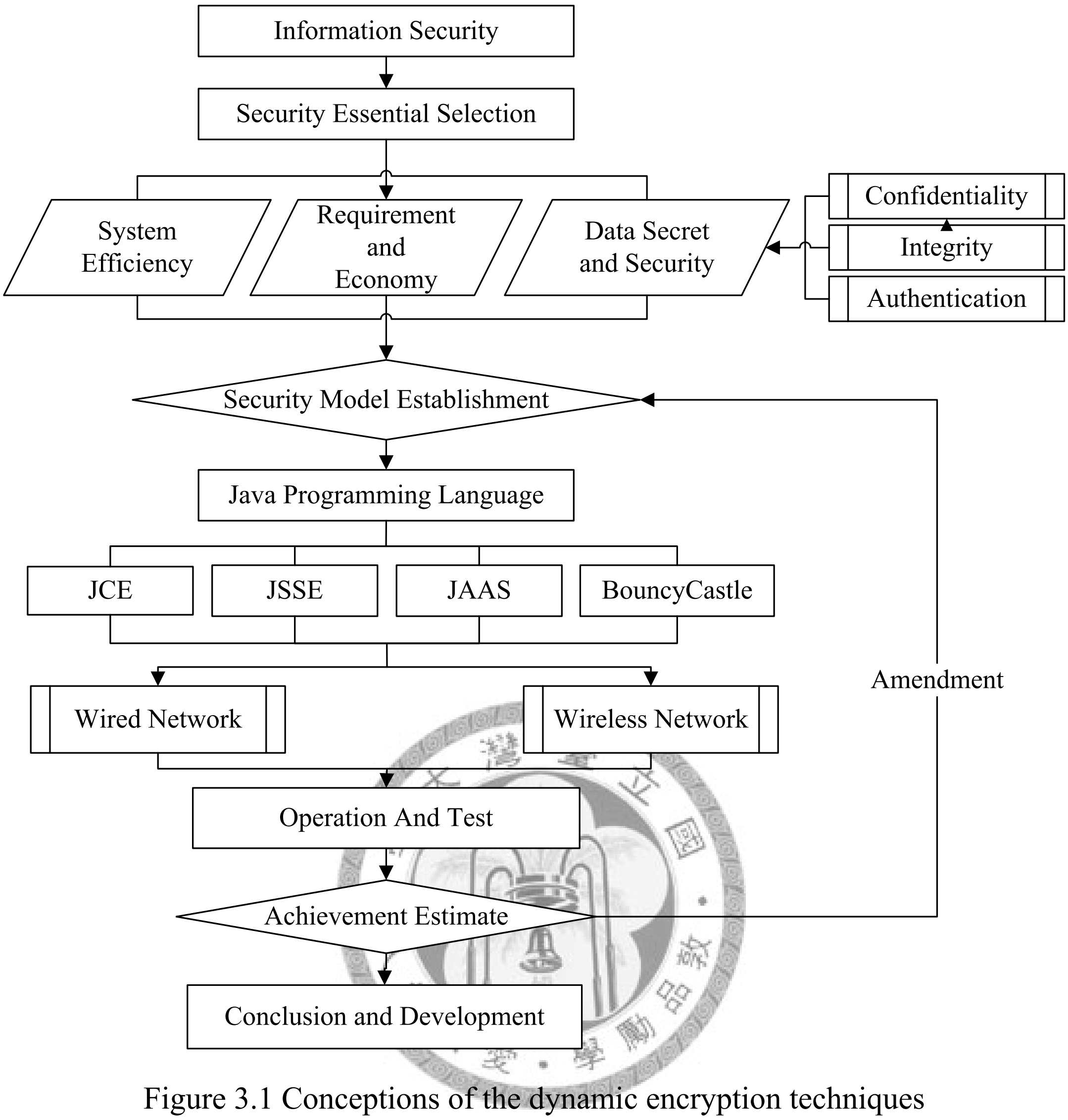


Figure 3.1 Conceptions of the dynamic encryption techniques

Figure 3.1 illustrates the conceptions of the security mechanism in this research. At the beginning, we have to make sure that the protected objectives, conditions and then decide the security level needed. Essentially, in this research, the security mechanism would be designed and used for traffic devices in data transmission, i.e., TMIC, TCIS, RSU, etc. The major characteristic of these devices in the transportation field emphasizes on the time-effectiveness, and most traffic commands are prompt and not long period. Due to these, if we focus only on the system security totally and do not care about the system operation efficiency and the consuming time from the encryption/decryption procedure; this would transgress our requirements thus. Therefore, we should consider the profit and the loss and then find out the balance-point between requirements, system operation efficiency and the economy as Figure 3.2 shown.

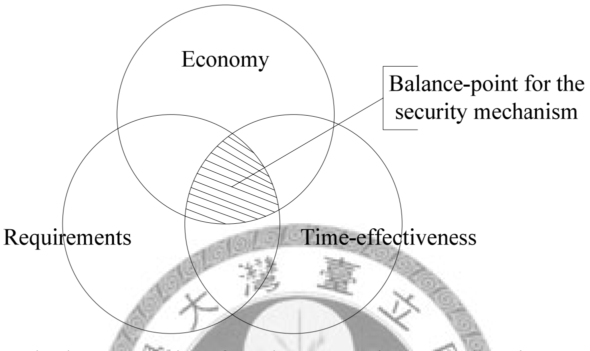


Figure 3.2The balance-point for the security mechanism consideration

3.3 Development Tool- Java Programming Language

Java programming language is developed by the Sun Microsystems and is the popular programming language nowadays. As Java programming language possesses the following specific characteristics to satisfy with the demands for the security mechanism in ATMS, this research uses Java to implement the protection system.

- **Java is cross-platform**

  This advantage makes Java applications to be operated not only on Windows OS but also on other OS, e.g., Linux, UNIX. This is the major reason why this research chooses Java to be the development tool, as Java byte code can be executed on any computer OS with JVM. Thus, it is useful for the security mechanism to be installed in all kinds of traffic devices subsequently.

- **Java is object-oriented**

Java is an object-oriented programming language as well. With the exception of simple types like numbers and Booleans, most things in Java are objects. Additionly, Java code is organized into classes. Each class defines a set of methods that form the behavior of an object. A class can inherit behaviors from another class. At the root of the class hierarchy it is always the class object. Figure 3.3 represents the simple class hierarchy of the security mechanism in this research, in which, we could easily understand the security mechanism is composed of different objects and each of them can be divided into several classes. Due to this property, Java is an easy compilation programming.

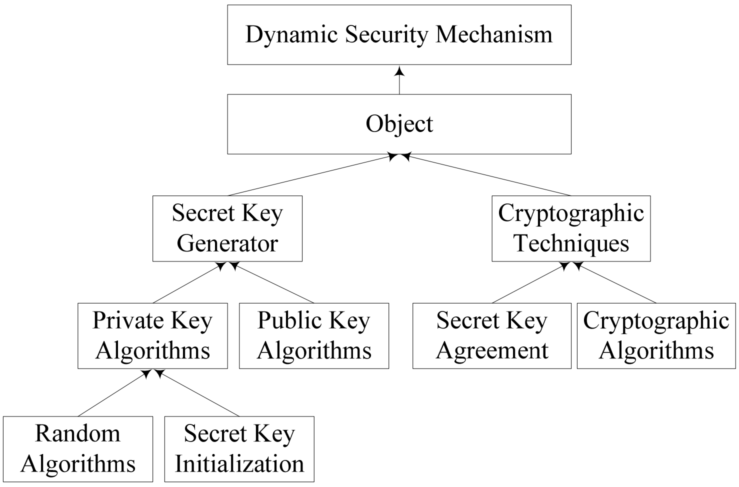


Figure 3.3 Simple class hierarchy of the security mechanism in Java programming

- **Java is extensible**

It is also possible to interface Java programs to existing software libraries written in other programming languages. Therefore, programmers could increase the functions that programmers need via the libraries. As illustrated in Figure 3.2, this research uses the four extensions discussed below:

i.Java Cryptography Extension (JCE)

This extension is in terms of the cryptographic algorithm implementation which includes ciphers, secret key exchange, message digest and secret key management. It could make programmers use the existing cryptographic algorithms directly and easily without paying attention to the specialized mathematical calculations of the cryptographic algorithms.

ii.Java Secure Sockets Extension (JSSE)

One could make communications with secure sockets layer (SSL) service or receivers via this extension.

iii.Java Authentication and Authorization Service (JAAS)

This extension provides functions for user authentication, it permits that programmers could approbate or refuse the limits of authority for users.

iv.Bouncy Castle Cryptography Extension

Java owns JCE itself; however, JCE does not cover RSA and AES algorithms which are the main stream cryptographic algorithms nowadays for symmetric cryptosystems and asymmetric cryptosystems. Because of these, this research add the Bouncy Castle Cryptography Extension to mend the insufficiencies in JCE.

- **Java is small, simple and fast**

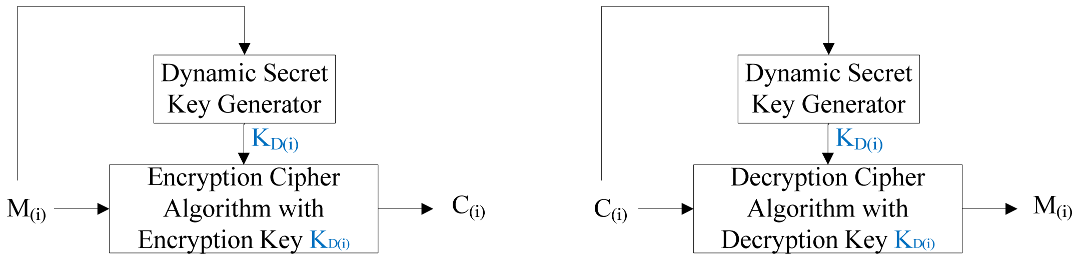
  Java is a high-level programming language and is very similar to C++, but it is much simpler than other high-level programming languages. Originally, Java is designed to run on small computers such as personal computers with 4Mb of RAM or more. Thus, Java is a lot more efficient than typical scripting languages, but it is about twenty times slower than C. Therefore, Java is acceptable for most applications to make code generations

3.4 Architecture of the Security Mechanism

3.4.1 Conceptions of the Dynamic Encryption Technique

Chapter Two discusses the cryptographic technologies and their strong/weak points. The fast encryption/decryption operation and the secret key protection are the particular advantage and weakness of symmetric cryptosystems respectively. However, asymmetric cryptosystems could be complementary to symmetric cryptosystems. In view of this, this research arranges them in groups: utilizes symmetric cryptosystems to encrypt/decrypt the message packets and on the other hand, uses asymmetric cryptosystems to transmit or exchange the secret keys and co-operates message digest to ensure the message integrity additionly.

In order to improve the security level for ATMS data transmission, one of the characteristics of this research is to adopt a dynamical (variable) encryption model for the hybrid cryptosystems. Nevertheless, what is the definition for “dynamic” of a encryption model? In the past, the secret key algorithms during the encryption/decryption procedures of a security mechanism are invariable and regular generally; furthermore, the message packets are transmitted frequently in traffic control. In these conditions, someone could crack the secret key algorithms easily by the frequent transmission. Thus, from these considerations, this research undertakes to design and implement an encryption technique which the secret keys could be changeable for each message transmission and suitable for ATMS data transmission; we call an encryption that owns the above characteristics are dynamic encryption technique.


Dynamic Secret Key Generator
$K_{D(i)}$
Encryption Cipher Algorithm with Encryption Key $K_{D(i)}$
$M_{(i)}$
$C_{(i)}$
Dynamic Secret Key Generator
$K_{D(i)}$
Decryption Cipher Algorithm with Decryption Key $K_{D(i)}$
$C_{(i)}$
$M_{(i)}$

(a) Encryption

(b) Decryption

Figure 3.4 Architecture of Dynamic Encryption Technique

Figure 3.4 illustrates the architecture of the dynamic encryption technique, in which, the fingerprint and the difference to existing encryption/decryption cipher are the dynamic key generator (DKG) and the dynamic keys $K_{D(i)}$. The encryption/decryption functions can be modified and expressed by the following formulae.

The encryption function $\mathbf{E_{KD(i)}}$ is expressed as:

$$\mathbf{E_{KD(i)}:\ M_{(i)} \times K_{D(i)} = C_{(i)}} \qquad (3.1)$$

$\mathbf{M_{(i)}}$: A set of plaintexts which are composed of *i* message blocks

$\mathbf{K_{D(i)}}$: A set of dynamic keys for the message *i*.

$\mathbf{C_{(i)}}$: A set of ciphertexts which are composed of *i* message blocks

in which the dynamic secret key $K_{D(i)}$ can be expressed as:

$$\mathbf{K_{D(i)} = DKG\ (\beta)} \qquad (3.2)$$

DKG: Dynamic Key Generator

β:the input of the dynamic key generator and the decryption function can be expressed as Equation 3.3:

$$\mathbf{D}_{\mathbf{KD(i)}}\mathbf{:}\ \mathbf{C}_{\mathbf{(i)}} \times \mathbf{K}_{\mathbf{D(i)}} = \mathbf{M}_{\mathbf{(i)}} \tag{3.3}$$

From Equation 3.2 and Figure 3.4, these represent that the dynamic keys are originated with the input, which is the certain characters from the plaintexts. Furthermore, using plaintexts to be the initial sources of DKG directly might generate another security loophole; namely someone might gain the plaintexts by cracking the encryption key algorithms. Therefore, as shown in Figure 3.5 which is the framework of DKG, we add a message digest algorithm in it to make the plaintext become a message digest first and then feed the message digest into a secure random number generator to generate a series of secure random numbers later. Finally, the secure random numbers become the sources of DKG to produce secret keys or public key pair for encryption and decryption as well.

In this way, it could modify some defects of random-number which cryptography usually use to generate secret key or public key pair in computers to have the following advantages:

i. In general, the random-numbers in computers are produced from Pseudo-Random Number Generator (PRNG), and PRNG utilizes the seed-number to be the initialization. However, the computer is a regular operation machine that normally selects the system-time or others to be the seed-number. Therefore, someone could crack the random-number generation by the regulations readily. The DKG usage of this research could modify the problems about the source of seed-numbers;

ii. As the seed-numbers are originated from each message differently, we could control them definitely and avoid getting the regular random-numbers or the unknown source to achieve the characteristic of dynamic keys, and;

iii. The most notable characteristic of message digest is irreversibility; that means that one cannot figure out the original data from message digest. Therefore, attackers can only get the message digest of the original data even though attackers crack the secret key/public key pair generator and the secure random number generator to provide more protections for transmitted message.

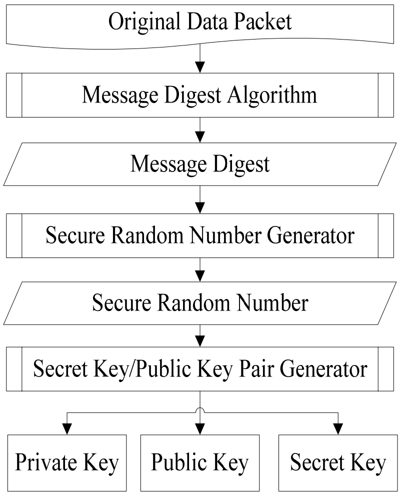


Figure 3.5 Framework of Dynamic Key Generator

3.4.2 Architecture of the Dynamic Security Mechanism

Next, we shall introduce the architecture and operations of the dynamic security mechanism in this research. As above, the security mechanism of this research adopts a hybrid cryptosystem which utilizes symmetric cryptosystems to encrypt/decrypt the NTCIP objects and uses asymmetric cryptosystems to transmit and exchange secret key .

Upon the architecture of this security mechanism, TMIC, the transmitter is sending a message to TCIS, the receiver. Now, while the TMIC needs to send a message to TCIS, the encryption/decryption procedures and message transmission processes can be described by four stages where the TMIC and TCIS operates alternately as below:

- **Step One－the first operation of TMIC: to generate a public key pair and seal byte arrays before public key transmission**

  As TMIC transmits or issues a message to TCIS, TMIC would produce a public key pair, which includes a public key $\mathbf{KU}_{\mathbf{TMIC}}$ and a private key $\mathbf{KR}_{\mathbf{TMIC}}$ via the dynamic public key pair generator (DPKG), and then store the private key $\mathbf{KR}_{\mathbf{TMIC}}$ in the TMIC system first. Next, it utilizes the public key $\mathbf{KU}_{\mathbf{TMIC}}$ and password $\mathbf{PW1}_{\mathbf{TMUC}}$ which originated in a specific number composition to be the input for the message digest algorithm (hash function) $\mathbf{H1}_{\mathbf{TMIC}}$. After the message digest algorithm calculation, we get a message digest $\mathbf{MD1_{TMIC}}$, and $\mathbf{MD1_{TMIC}}$ can be expressed by Equation 3.4:

$$\mathbf{MD1_{TMIC} = H1_{TMIC}\ (PW1_{TMUC}\ ,\ KU_{TMIC})} \tag{3.4}$$

In addition, the TMIC would create a secret key request message $\mathbf{M_k}$ as well, the content of this message is to ask the TCIS to produce and transmit the secret keys of the symmetric cipher to TMIC. The secret key message is not a secret, therefore, it would not be encrypted, and the content of it is:

$\mathbf{M_k}$: Please produce and transmit secret keys to TMIC!!

Finally, the TMIC would proceed with a succession of operations for $\mathbf{M_k}$, $\mathbf{MD_{TMIC}}$ and $\mathbf{KU_{TMIC}}$, namely, seal them to a byte array and transmit the byte array to the TCIS. The procedure is illustrated as shown in Figure 3.6.

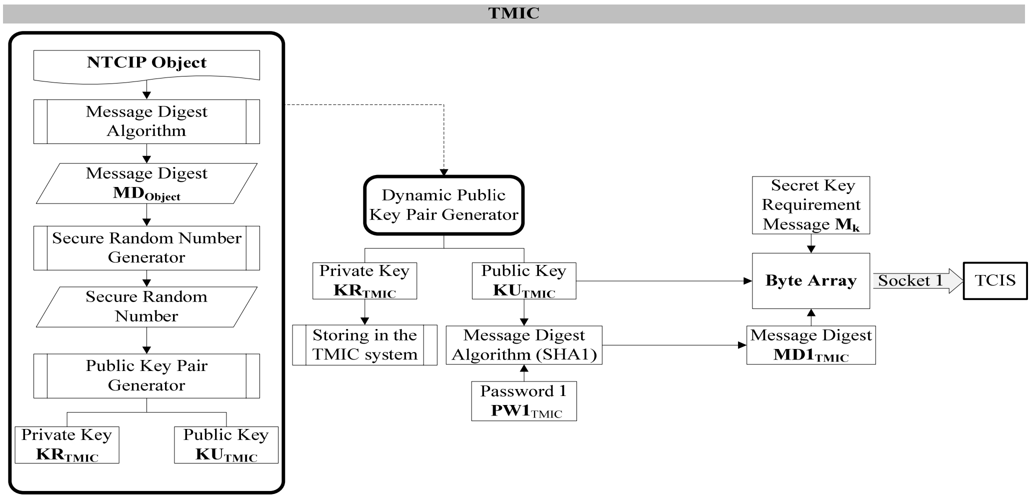


Figure 3.6 TMIC Operation One－to generate a public key pair and seal byte arrays before public key transmission

- **Step Two－the first operation of TCIS: procedures for the public key integrity confirmations and secret key generation**

As the TCIS receives the data packet (byte array); the TCIS would proceed to separate out the $\mathbf{M_k}$, $\mathbf{MD_{TMIC}}$ and the received public key from the data packet. Here we call the public key which is received by TCIS is $\mathbf{KU_{TCIS}}$. Then, the TCIS would make a new message digest $\mathbf{MD1_{TCIS}}$ which is from the pre-stored password $\mathbf{PW1_{TCIS}}$ and the $\mathbf{KU_{TCIS}}$ given by Equation 3.5.

$$\mathbf{MD1_{TCIS} = H\ (PW1_{TCIS},\ KU_{TCIS})} \tag{3.5}$$

The TCIS would continue to compare between the $\mathbf{MD1_{TMIC}}$ and the $\mathbf{MD1_{TCIS}}$. As shown in Figure 3.7, if $\mathbf{MD1_{TMIC}}$ or $\mathbf{MD1_{TCIS}}$ is not acceptable; this means the transmitted data array might be tampered, and the TCIS would ask TMIC to produce a new key pair and transmit the public key again.

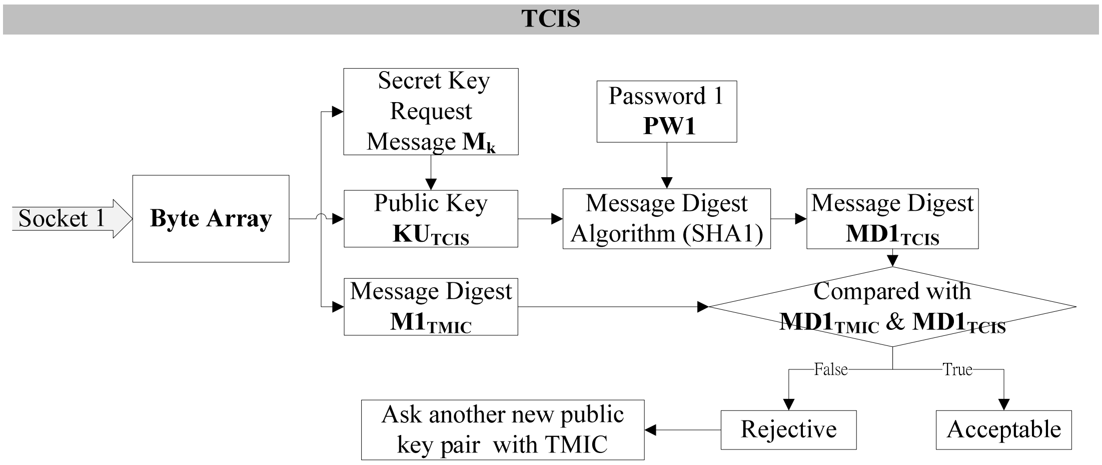

TCIS
Socket 1
Byte Array
Secret Key Request Message $\mathbf{M_k}$
Public Key $\mathbf{KU_{TCIS}}$
Message Digest $\mathbf{M1_{TMIC}}$
Password 1 **PW1**
Message Digest Algorithm (SHA1)
Message Digest $\mathbf{MD1_{TCIS}}$
Compared with $\mathbf{MD1_{TMIC}}$ & $\mathbf{MD1_{TCIS}}$
False
True
Rejective
Acceptable
Ask another new public key pair with TMIC

Figure 3.7 Procedures for data packet restoration and message digest comparison

On the contrary, if $\mathbf{MD1_{TCIS}}$ is in agreement with $\mathbf{MD1_{TMIC}}$; this indicates that the original public key $\mathbf{KU_{TMIC}}$ and the message digest $\mathbf{MD_{TMIC}}$ are not tampered during the transmission period. As represented in Figure 3.7, the TCIS would continue to generate a secret key $\mathbf{KS_{TCIS}}$ via the dynamic secret key generator (DSKG) and store the secret key in the TCIS system after the TCIS receives the secret key request message $\mathbf{M_k}$ and confirms the $\mathbf{MD1_{TCIS}}$ as well. Next, the TCIS would encrypt this secret key via public key $\mathbf{KU_{TCIS}}$ and RSA cipher usage (see Equation 3.8). Additionly, it generate a new message digest $\mathbf{MD2_{TCIS}}$ which is originated from pre-stored password $\mathbf{PW2_{TCIS}}$ and the ciphertext of secret key $\mathbf{C_{KS}}$. Finally, the TCIS now would integrate the ciphertext and $\mathbf{MD2_{TCIS}}$ in a byte array and transmit the byte array to TMIC.

$$\mathbf{E_{KU_{TCIS}}\ :\ (KS_{TCIS})\times KU_{TCIS} = C_{KS}} \tag{3.6}$$

$\mathbf{E_{KU_{TCIS}}}$ **:** The encryption formula for the secret keys $\mathbf{KS_{TCIS}}$ with the public key $\mathbf{KU_{TCIS}}$

$\mathbf{KS_{TCIS}}$ **:** The secret key which is produced from the TCIS

$\mathbf{KU_{TCIS}}$**:** The public key which is produced from the TCIS

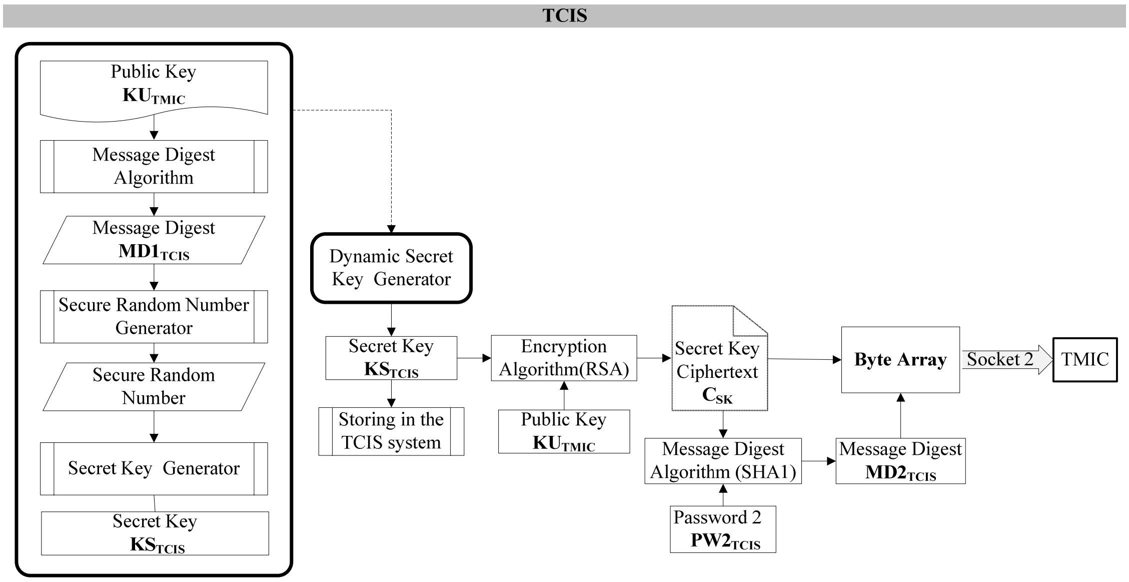


Figure 3.8 Procedures for data packet restoration and message digest comparison

In addition, the message digest algorithm addition of the security mechanism for each transmission procedure to ensure the integrity of transmitted objects. Figure 3.9 illustrates that receivers need to offer not only the right received object but also the correct password; or the receivers cannot create the agreeable message digests with transmitters. Due to the passwords are pre-restored in both of transmitter-side and receiver-side respectively; therefore, attackers would not know the correct password if the transmitter/receiver systems are not be invaded. It could also achieve the authentication of users by this way in other words.

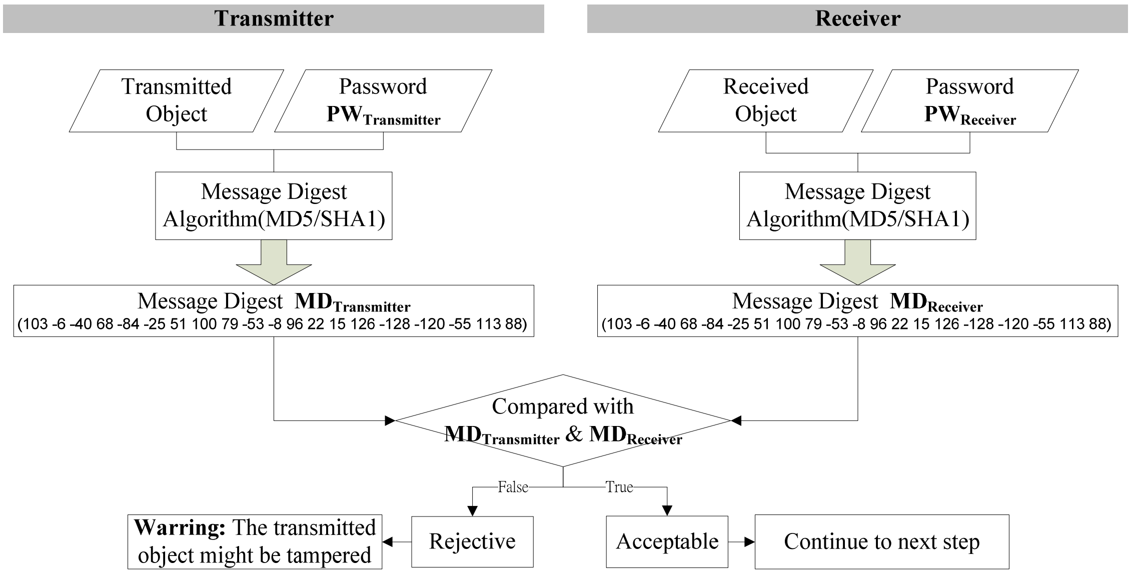


Figure 3.9 Functions of message digest algorithms of the security mechanism

- **Step Three－the second operation of TMIC: procedures for the secret key separation, NTCIP Object encryption and transmission**

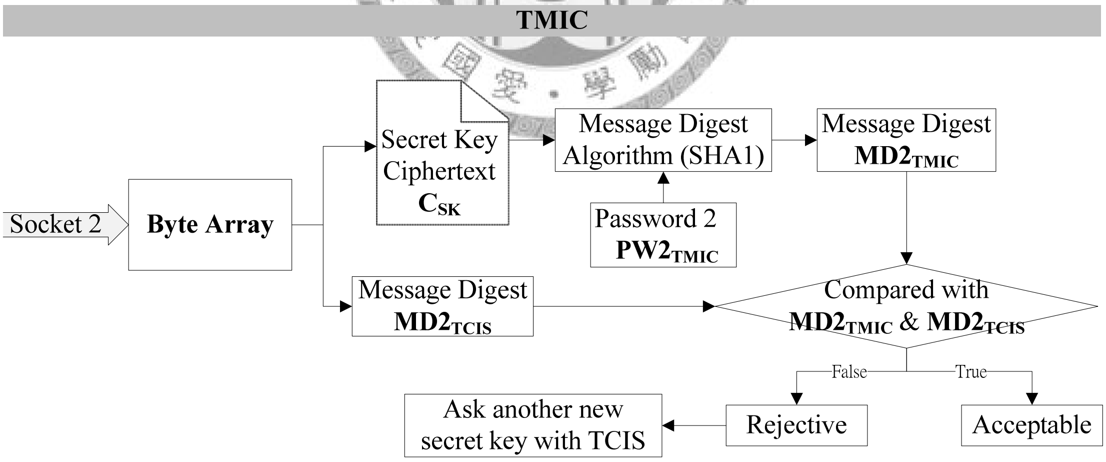

TMIC
Socket 2
Byte Array
Secret Key Ciphertext CSK
Message Digest Algorithm (SHA1)
Message Digest MD2TMIC
Password 2 PW2TMIC
Message Digest MD2TCIS
Compared with MD2TMIC & MD2TCIS
False
True
Ask another new secret key with TCIS
Rejective
Acceptable

Figure 3.10 Procedures for the secret key separation

Figure 3.10 represents that while the TMIC receives the data packet from TCIS, TMIC would separate the byte array into the ciphertext of secret key $\mathbf{C_{KS}}$ and the received message digest $\mathbf{MD3_{TCIS}}$. Next, the TMIC proceeds to decrypt $\mathbf{C_{KS}}$ to get the secret key by the pre-stored private key $\mathbf{KR_{TMIC}}$ and RSA cipher algorithm after a series of processes of user authentication and transmitted object integrity as above step. So far, both of the TMIC and TCIS own the secret key $\mathbf{KS_{TCIS}}$; hence, the TMIC could transmit NTCIP objects to the TCIS safely through the encryption/decryption procedures of AES cipher.

One thing that should be mentioned deservedly is the encryption procedure of NTCIP object. As Figure 3.11 depicted, this security mechanism adopts the cipher mode termed cipher block chaining (CBC); the major characteristic of CBC is that it adds a initialization vector (IV) in between the encryption and decryption processes. Broadly speaking, we could imagine the IV is the another secret key, one must own the primary secret key and IV for encryption and decryption at the same time, the encryption procedure can expressed as Equation 3.7.

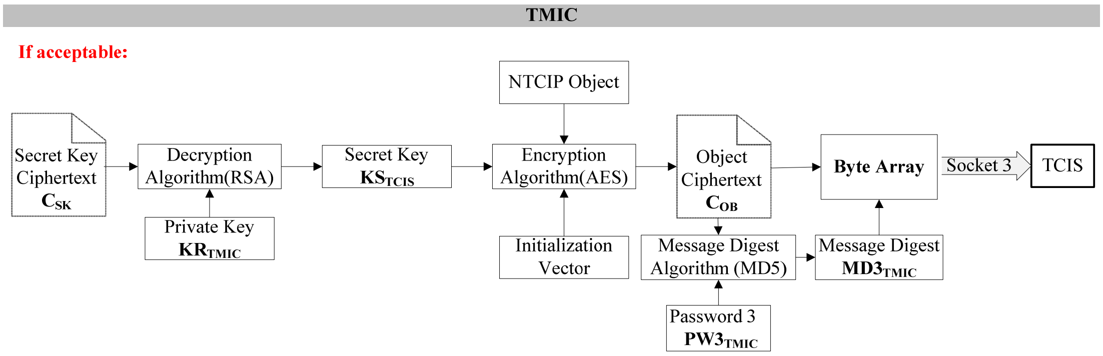

TMIC
If acceptable:
NTCIP Object
Secret Key Ciphertext $\mathbf{C_{SK}}$
Decryption Algorithm(RSA)
Private Key $\mathbf{KR_{TMIC}}$
Secret Key $\mathbf{KS_{TCIS}}$
Encryption Algorithm(AES)
Initialization Vector
Object Ciphertext $\mathbf{C_{OB}}$
Message Digest Algorithm (MD5)
Password 3 $\mathbf{PW3_{TMIC}}$
Byte Array
Message Digest $\mathbf{MD3_{TMIC}}$
Socket 3
TCIS

Figure 3.11 Procedures for the NTCIP object encryption and transmission

Afterward the TMIC sends the byte array which includes $\mathbf{MD3_{TMIC}}$ that is grated from password $\mathbf{PW3_{TMIC}}$ and the ciphertext of NTCIT Object to TCIS.

$$\mathbf{E_{KS,IV} : M_{OB} \times KS_{TCIS} \times IV = C_{OB}} \qquad (3.7)$$

$\mathbf{E_{KU,IV}}$ **:** The encryption formula for the NTCIP objects $\mathbf{M_{OB}}$ with secret key $\mathbf{KS_{TCIS}}$ and **IV**

$\mathbf{M_{OB}}$ **:** The transmitted plaintext of NTCIP Object

$\mathbf{KS_{TCIS}}$ **:** The secret key which is produced from the TCIS

IV **:**The pre-stored initialization vector

- **Step Four－the second operation of TCIS: to decrypt the ciphertext of NTCIP objects**

Finally, as Figure 3.12 represented, while the TCIS receives the ciphertext of NTCIP Object, it needs to confirm the authenticity of the received data by message digest. If the message digest $\mathbf{MD3_{TCIS}}$ is acceptable to $\mathbf{MD3_{TMIC}}$, then the TCIS would proceed to decrypt the ciphertext of NTCIP Object via the pre-stored secret key $\mathbf{KS_{TCIS}}$ and initialization vector to make the TCIS get the NTCIP object in conclusion.

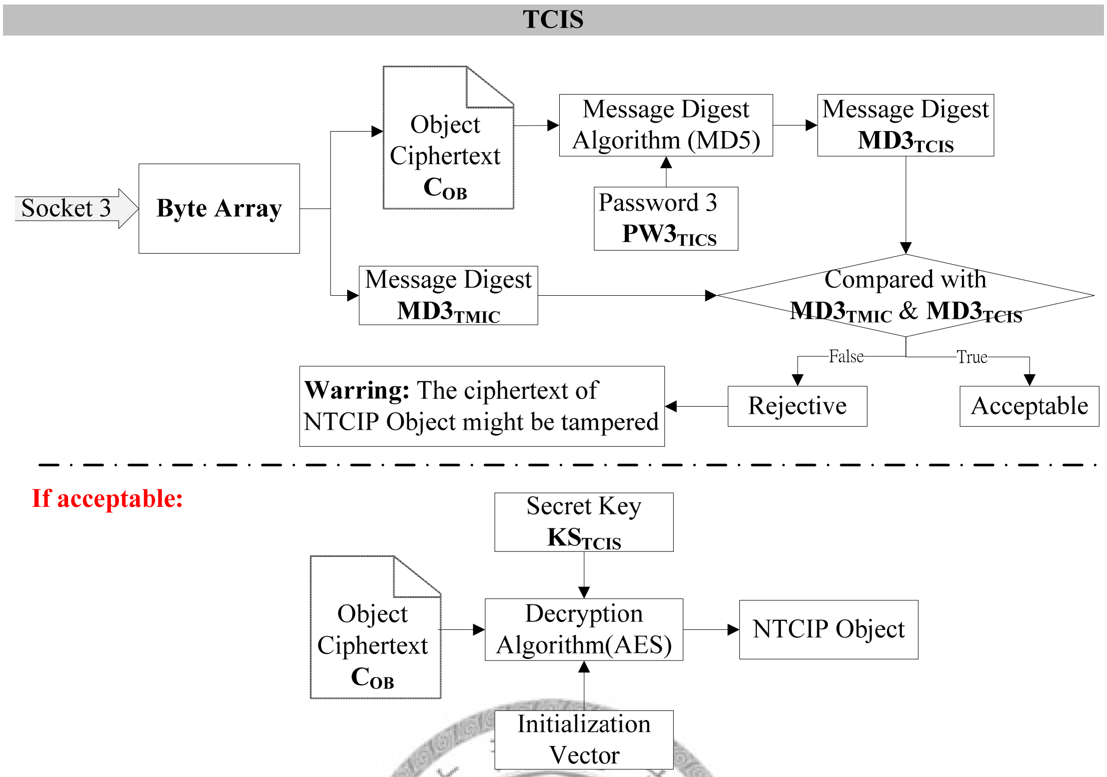


Figure 3.12 Procedures for NTCIP object ciphertext decryption

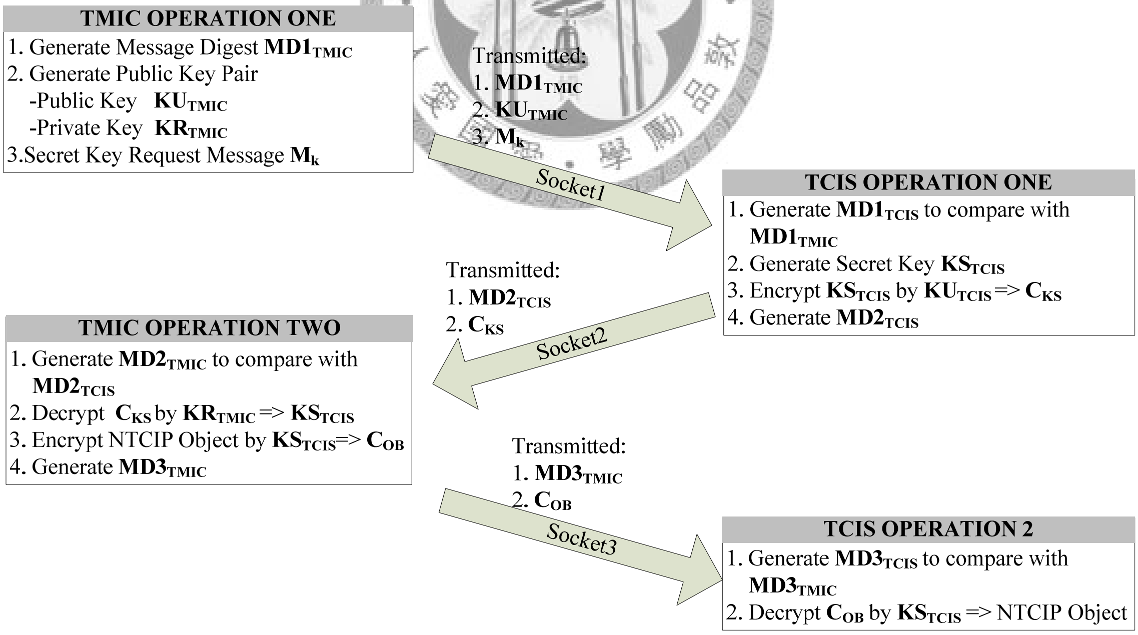

TMIC OPERATION ONE
1. Generate Message Digest MD1_TMIC
2. Generate Public Key Pair
-Public Key KU_TMIC
-Private Key KR_TMIC
3.Secret Key Request Message M_k
Transmitted:
1. MD1_TMIC
2. KU_TMIC
3. M_k
Socket1
TCIS OPERATION ONE
1. Generate MD1_TCIS to compare with MD1_TMIC
2. Generate Secret Key KS_TCIS
3. Encrypt KS_TCIS by KU_TCIS => C_KS
4. Generate MD2_TCIS
Transmitted:
1. MD2_TCIS
2. C_KS
Socket2
TMIC OPERATION TWO
1. Generate MD2_TMIC to compare with MD2_TCIS
2. Decrypt C_KS by KR_TMIC => KS_TCIS
3. Encrypt NTCIP Object by KS_TCIS => C_OB
4. Generate MD3_TMIC
Transmitted:
1. MD3_TMIC
2. C_OB
Socket3
TCIS OPERATION 2
1. Generate MD3_TCIS to compare with MD3_TMIC
2. Decrypt C_OB by KS_TCIS => NTCIP Object

Figure 3.13 Flow chart of the security mechanism of this research

Thus far, both TMIC and TCIS own the secret keys securely by a security channel. Then TMIC would encrypt NTCIP objects into ciphertexts and transmit them to the assigned

TMIC. The above procedures of the security mechanism could be illustrated as Figure 3.13.

In general, in the asymmetric cryptosystems, the public keys are spread publicly. This means that the public keys do not need to be protected, and everyone could encrypt the plaintexts while one owns the public key. In the View of this, the public key **KU_{TMIC}** in this security mechanism need not be protected during the public key transmission from TMIC to TCIS.

Nevertheless, one might intercept and tamper with the public key to be the illegal-owner if one knows the algorithms and key length of the public key; therefore, this research utilizes the message digest and multiple security protections to enhance the security for the public key during the transmission.

3.5 Security Analysis for the Security Mechanism

The major purpose of this research is to establish a dynamic security mechanism for the ATMS data transmission. Needless to say, security is an important factor for this security mechanism and the security analysis which can be categorized in two parts; namely: analysis of security protection and cryptanalysis. We will be looking at the security analysis of the security mechanism in this research.

3.5.1 Analysis of Security Protection

- As mentioned earlier, the security mechanism utilizes a hybrid cryptosystem that translates with symmetrical cryptosystems, asymmetrical cryptosystems and message digest, and is implemented by Java programming language. In addition, Section 2.6 indicated that there are some potential attacks that might threaten ATMS data transmission. For example, the data packet interception, masquerade, eavesdropping, message modification and etc. one of the major conceptions of this security mechanism establishment is to ensure confidentiality, integrity and authentication of transmitted data. Now, we shall discuss on the above issues and of how to withstand the attacks in focus via this security mechanism.

- **Data Confidentiality**

The goal of data confidentiality is to ensure that transmitted data would not be peeked by illegal ones. Hence to achieve confidentiality, the security mechanism utilizes a set of hybrid cryptosystem. The hybrid cryptosystem of this research modifies the weakness of symmetric cryptosystems in secret key exchange and protection. Not forgetting, the AES cipher which this security mechanism used in symmetric cryptosystem adopts a cipher mode termed cipher block chaining (CBC) and the CEC cipher mode usage improves the secure protection much and also increases the security level sufficiently.

Nevertheless, whether the security level is secure sufficiently might be dependent on the cryptanalysis. Therefore, we will be discussing about the cryptanalysis of the security mechanism of this research later. Generally speaking, a well secured security mechanism makes life difficult for crackers. ~~or~~ At most, they can only retrieves the data in ciphertexts but can't transfer it into plaintext even if they steal the data packet from transmission channel. From this, system managers could make use of this security mechanism to prevent attackers to eavesdrop, modify or reply to the accurate contents of transmitted data.

- **Data Integrity**

If we say that the methods which are to ensure the data confidentiality are the active protections, then we could deem the ways of data integrity are the passive protections as well. This is because the methods of data integrity are usually used to confirm whether the data received is accurate if there is a security mechanism in transmission processes. In another words, TCIS could ensure that the received data packets are accurate, not modified, and sent from the right methods through TMIC.

From the architecture of the security mechanism in the above section, the transmitter would generate and transmit a message digest of transmitted ciphertexts before each transmission processes respectively, and the receivers need to create a message digest which is originated from the received data by the same message digest algorithms. Then the receivers would compare with these two message digests to confirm the soundness of received data. Although the well secured security mechanism should possess to resist and prevent the attackers' tamper of transmitted data or modifications; still the message digest algorithm usage provides further protections for data transmission and prevention against some attacks; namely: masquerading, message modification, man-in-the-middle attacks effectively.

- **User Authentication**

The authentication in cryptography is to ensure that both of the principals (transmitter/receiver) are the actual ones, not the impostor essentially. The asymmetric cryptosystems could be used for authentication as well. For instance of this security mechanism, TCIS utilizes the public key to encrypt the plaintext of secret key, and only the other TMIC could use the right private key to decrypt the ciphertext additionally.

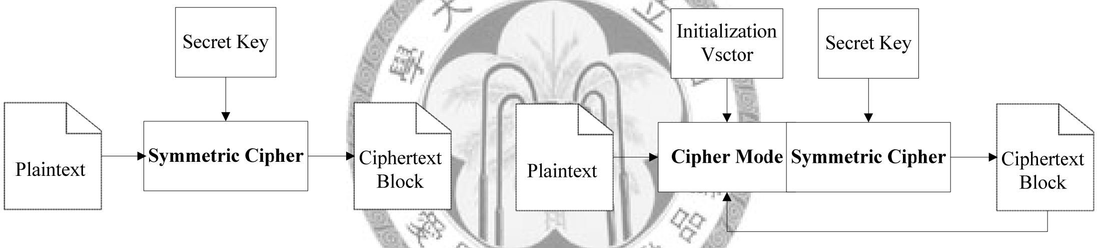
On the other hand, this security mechanism also adds four sets of password (three of these are for message digests and the other is for initialization vector) both in the TMIC and in the TCIS respectively. As shown in Figure 3.8, these two message digests not only come from the transmitted/received data but also from the according pre-stored passwords in the comparative processes of message digests.

In addition, due to the system protections of TMIC and TCIS which are not the concerns of this research. Therefore, on the basis of this, we assume that either TMIC or TCIS is not invaded and protects well, attackers cannot create the right message digests without knowing the correct passwords. It is almost impossible for the attackers to crack these passwords easily even if they use brute-force attack with the unknown of the number characters or number combinations. Hence, this security mechanism uses the above mechanism to ensure access control and the authentication of user identifications to prevent masquerading, eavesdropping or other attacks.

3.5.2 Cryptanalysis

The cryptanalysis is dependent on the cipher algorithms, the characteristics of plaintexts, secret key/public key pair generations or the combinations of ciphertexts. Taken in this light, attackers might know the cipher algorithms previously and infer the plaintext or the algorithms of secret key from the characteristics of the cipher algorithm analysis. Therefore, the ciphertexts which are generated from those secret key would be threatened.

As mentioned earlier, the security mechanism in this research uses the CEC cipher mode in the AES algorithm. Figure 3.14 represents the electronic code book (ECB) cipher mode and CBC cipher mode; the characteristics and differences between ECB and CBC are the initialization vector and the second cipher mode additions, and these improve the weaknesses of ECB as succeeding discussion.



(a) EBC Cipher Mode

(b) CBC Cipher Mode

Figure 3.14 EBC cipher mode and CBC cipher mode

As shown in Figure3.13, in ECB cipher mode, a secret key is fed into the block cipher which takes one plaintext block and generates one ciphertext block. For instance, as shown in Table 3.1, if the message happens to contain identical blocks (in this example, each of the block is 16 bytes), in each block identical ciphertext are produced. One of the benefits of ECB is that the message does not have to be encrypted linearly, since each block is effectively in its own independent message. The ECB cipher mode is fast, but so far it is still the weakest cipher mode due to no attempt made to hide the patterns in the plaintext.

Table 3.1 Example of encryption via ECB cipher mode

	ECB Cipher Mode
Plaintext	[01][02][03][04][0a][0b][0c][0d][01][02][03][04][0a][0b][0c][0d]
	[01][02][03][04][0a][0b][0c][0d][01][02][03][04][0a][0b][0c][0d]
	[01][02][03][04][0a][0b][0c][0d][01][02][03][04][0a][0b][0c][0d]
Ciphertext	[1e][6b][4c][6e][67][44][f5][8c][0b][63][ca][b9][35][7c][62][e3]
	[1e][6b][4c][6e][67][44][f5][8c][0b][63][ca][b9][35][7c][62][e3]
	[1e][6b][4c][6e][67][44][f5][8c][0b][63][ca][b9][35][7c][62][e3]

The CBC cipher mode introduces a feedback mechanism into the encryption process such that each block is dependent on all of the blocks before it. CBC employs an XOR operation between the plaintext and the previous ciphertext block, as demonstrated in Figure 3.13. Before the next plaintext is fed into the cipher engine, the previous ciphertext block is XOR'ed with the incoming plaintext block. The result of this XOR operation is then fed into the cipher engine for encryption using the provided secret key. This chaining mechanism addresses the major weakness of ECB－identical plaintext result in identical ciphertext blocks. As per example shown in Table 3.2, this example uses the same plaintext blocks and identical secret key as Table 3.1, however it results in different ciphertext blocks for each identical plaintext block.

Table 3.2 Example of encryption via CBC cipher mode

	CBC Cipher Mode
Plaintext	[01][02][03][04][0a][0b][0c][0d][01][02][03][04][0a][0b][0c][0d]
	[01][02][03][04][0a][0b][0c][0d][01][02][03][04][0a][0b][0c][0d]
	[01][02][03][04][0a][0b][0c][0d][01][02][03][04][0a][0b][0c][0d]
Ciphertext	[99][cf][f5][ac][8f][a7][3b][26][1c][92][9f][ac][41][4b][2a][78]
	[3f][27][57][b2][83][a2][a7][9b][68][20][65][5e][a4][67][ce][ba]
	[0b][92][aa][d3][ef][4c][35][19][17][5a][20][26][30][a3][f6][43]

As a result, the initialization vector is needed to prime the encryption operation. The IV has no meaningful relations to the plaintext. In fact, its sole purpose is to populate the feedback registers inside the cipher mode box because there is no preceding ciphertext block to do the job. Although there is nothing confidential about the IV and the strength of the cipher should remain with the secret key. But one must own both the right secret key and identical IV for an encryption/decryption process at the same time. Therefore, the IV could be assumed of the second secret key of the encryption/decryption process. In view of these, the security mechanism of this research pre-stores the according IV in each end to improve the security level even if the attackers gotten the transmitted secret key and know the encryption algorithm, they still cannot crack the ciphertext without owning the according IV. On the other hand, the pre-stored IV could be regarded as the function in the authentication of user identity as well.

From the comparisons between Table 3.1 and Table 3.2, even if we use the same secret key and feed the same plaintext into the cipher, it would result in a lot of differences between ciphertexts and plaintexts. Therefore attackers cannot crack the ciphertexts easily via using the CBC cipher mode due to CBC which would generate the irregular ciphertexts. However this phenomenon is not the major concernment for a professional cryptographer. Therefore one should consider and analyze the common attacks of cryptanalysis. Nevertheless, the cryptanalysis is too complicated to be examined in details in this research. Hence we shall discuss about this part from other related researches or conferences.

The attacks of cryptanalysis could be commonly separated into five cracking methods which are dependent on how much secret information is made known by attackers; namely: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext and chosen text. In which, the ciphertext is the only difficult method to be cracked because attackers might only know a few secret information ~~as~~ due to encryption algorithms and ciphertext. Furthermore the encryption algorithms of symmetry cryptosystem (AES) and asymmetry cryptosystem (RSA) are not hidden. Therefore, attackers could use some attacks such as brute-force attack, time attack, differential cryptanalysis, linear cryptanalysis and mathematical attack to proceed to crack ciphertexts. However with the improvements of technology, the AES algorithms and RSA algorithms cannot be cracked by these attacks effectively. So far, these results and analyses of cryptanalysis lead us to the conclusion that the cryptography algorithms of the security mechanism in this research can resist the attacks of cryptanalysis well and sufficiently.

3.5.3 Brute-Force Attack

In many attacks such as message modification or message reply, if one could not crack the security protections by utilizing cryptanalysis, one might eventually use the brute-force attack to crack them again. As implied in the name, the brute-force attack is to try all the possible secret key combinations to decrypt the ciphertexts. In another word, the method is just to keep on trying till the spot on of right secret key combination. Generally, test frequencies required for finding out the secret key combination successfully would be about half numeral values of the secret key quantity. Table 3.3 shows the time-consumption in carrying out the brute-force attack for different computers computation-capability and the different lengths of secret key.

In Table 3.1, are the test results of four different lengths of secret keys; namely: 32 bits, 56 bits for AES, 128 bits for DES, 168 bits for Triple-DES, and each secret key is arranged in the 26 characters. In which, firstly, we assume that the computer computation-capability for decryption is using one possible secret key calculation for each millisecond. The results show that one could try all the secret key combinations and decrypt the ciphertexts via using the 32-bit secret key in 35.8 minutes. Therefore, one might assumed that the security level of it is not sufficient. On the other hand, the security levels of the 56-bit, 128-bit, and 168-bit secret keys are beyond sufficiency under this level of computer computation-capability.

Table 3.3 Time-consuming for brute-force attack in Decryption

Length of secret key	**Quantity of secret key**	**Time-consuming in Decryption**	
		(1 times/ms)	(10^6 times/ms)
32 bits	2^{32}=4.3×10^9	2^{31} ms (35.8 minutes)	2.15 ms
56 bits (AES)	2^{56}=7.2×10^{16}	2^{55} ms (1142 years)	10.01 hours
128 bits (DES)	2^{128}=3.4×10^{38}	2^{127} ms (5.4×10^{24} years)	5.4×10^{18} years
168 bits (Triple-DES)	2^{168}=3.7×10^{50}	2^{167} ms (5.9×10^{36} years)	5.9×10^{30} years
Arrange in 26 characters	2!=4×10^{26}	2×10^{26} ms (6.4×10^{12} years)	6.4×10^6 years

ms: milliseconds

However, attackers might not utilize only just one computer to attack and crack the cryptosystems. They might connect several high computation-capability computers to calculate together at the same time, and this way could improve the computation-capability level substantially. Due to this, the last row of Table 3.3 represents the computer computation-capability for decryption via using one million possible secret key calculations for each millisecond. The results show that one could crack the cryptosystem via utilizing the 56-bit secret key in 10 hours and the security level of it is not sufficiently enough.

From the table, the 128-bit secret key usage for AES cipher algorithm of this research could resist being cracked for almost 5.4×10^{18} years normally. It is sufficiently enough to resist the brute-force attack nowadays.

3.6 Summary

This chapter introduced about the design conceptions, architectures of the dynamic security mechanism in this research, and the potential attacks for ATMA data transmission. Broadly speaking, Table 3.4 indicates the characteristics of this security mechanism and represents the applications for each mechanism of it. In addition, we shall discuss the system operation efficiency and the core system source usage issues by the security mechanism addition.

Thus far and from many viewpoints as started, we ensure that the security mechanism can supply multiple protections from the hybrid cryptosystem to resist the above possible attacks nowadays. Even the security mechanism might not be absolute security, but the security level of this security mechanism in this research is sufficiently enough to be applied to ATMS data transmission.

Table 3.4 Effects of the dynamic security mechanism

Mechanism	**Application**	**Purpose**
AES Cipher	－Fast encryption/decryption operation for transmitted data －Resist time attack, differential cryptanalysis and linear cryptanalysis efficiently －Avoid masquerading attack, man-in-the-middle attack, eavesdrop attack and message modification and reply well	Data confidentiality
RSA Cipher	－Modify the defects in secret key transmission and protection of symmetric cryptography －Related attacks of cryptanalysis and the brute-force attack are invalid for RSA algorithm －Avoid masquerading attack, man-in-the-middle attack, eavesdrop attack and message modification and reply －Way to ensure the according users	Data confidentiality/ Data integrity
CBC Cipher Mode	－Result the distinct ciphertext －IV could be treated as another secret key to improve the security protections and ensure the identity of user as well	Data confidentiality/ User authentication
MD Algorithm	－Make sure the transmitted message is not modified and the received message is right and correct －Make attackers cannot guess the original plaintext by using the message digest in DKG	Data integrity
Re-stored Password	－Confirm the use identity of users to avoid attackers masquerade system managers	User authentication
DSKG/DPKG	－Improve the weaknesses of PRNG －Generate different and irregular secret information for each transmission	Data confidentiality/ Data integrity

CHAPTER FOUR

EXPERIMENTS FOR SYSTEM EFFICIENCY

4.1 Introduction

Real-time controlling is the principal characteristic of ATMS; TMIC receives the real-time information from TCIS and gives out commands to RSU or CMS immediately. However, the data transmission processes are on the Internet Network which is under the open network environment; therefore, the stability and security of the Internet Network would greatly influence the ATMS operation efficiency. For these reasons, Chapter Three introduces the conceptions and the framework of DSM and discusses the security protections of it. Upon the DSM establishment, we expect it would not only achieve the data security but also consume less resource from the core system. Unfortunately, in the progress of improving data security, it also brings some negative-effects for the core system operation. Thus, in this chapter, we design three experiments to investigate the operations efficiency of the core system which combines with DSM for ATMS data packet transmission.

4.2 Experiment Design Principle

According to the architecture of DSM in Section 3.4.2, there are totally three times in data transmission and thirteen stages in encryption/decryption procedures within the DSM. On the other hand, as Figure 4.1 shown, it indicates that the consuming time of AES operations (i.e., AES secret key generation, NTCIP object encryption and decryption), RSA operations (i.e., RSA public key pair generation, AES secret key encryption by public key and decryption by private key) and data transmission procedures respectively occupy almost one third of the total time-consumption of DSM operations. Therefore, in this research, we roughly separate the sources of the negative-effect generations from two segments and proceeding discussions are base upon these two points, namely:

- Operation delay: Efficiencies in device operations of TMIC and TCIS, and;
- Transmission delay: Efficiencies in data packet transmission procedures.

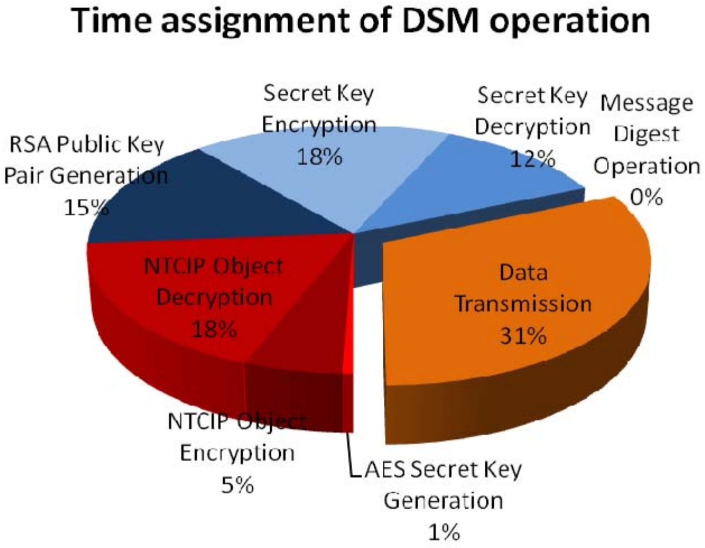


Figure 4.1 Time-consumption assignment of DSM operation

Next, we consider in terms of the possible factors in negative-effect generation for core system due to the DSM addition and discuss as below:

- The larger size of NTCIP object or transmitted message might raise more delay and in transmission and encryption/decryption procedure;
- The different communications media would provide different bandwidth, and it might influence the efficiency and stability in data transmission further;
- The length in secret key or public key pair might be the direct proportion to the negative-effect increment;
- The tight frequencies in message dispatch might increase the loads not only for transmission but also for device action, and;
- In view of the computation-capability of the existing TCIS outdoor is not as well as the computers for the experiment usage indoor, and the encryption/decryption procedures would consume the equal sources of the core system additionly. Due to these, this research utilizes different computation-capability computers to confirm these viewpoints.

The main purposes of these experiments are trying to find out the effective factors and the reciprocal effects between them. Finally, this research limits the discussions to set up the regression equations $\boldsymbol{R_e}$ which can represent these variables and estimate the time-consumption of DSM operation for each NTCIP object transmission with DSM to provide treatments for traffic engineers in the information security design; and ***R_e*** can be expressed by Equation 4.1.

$$R_e = \{C_m, KS_l, KP_l, M_s, M_f, C_c\} \qquad (4.1)$$

***R_e*:** The regression equation from these factors

***C_m*:** The factor for communications media

***KS_l*:** The factor for secret key length

***KP_l*:** The factor for public key pair length

***M_s*:** The factor for NTCIP object size

***M_f*:** The factor for the frequency of message dispatch

***C_c*:** The factor for the computation-capability of simulated TCIS

4.3 Experiment Environment

4.3.1 Scope of Simulated Experiment

As illustrated in Figure 4.2, the data transmission processes which combine with DSM could be distributed into six procedures on the whole, described below:

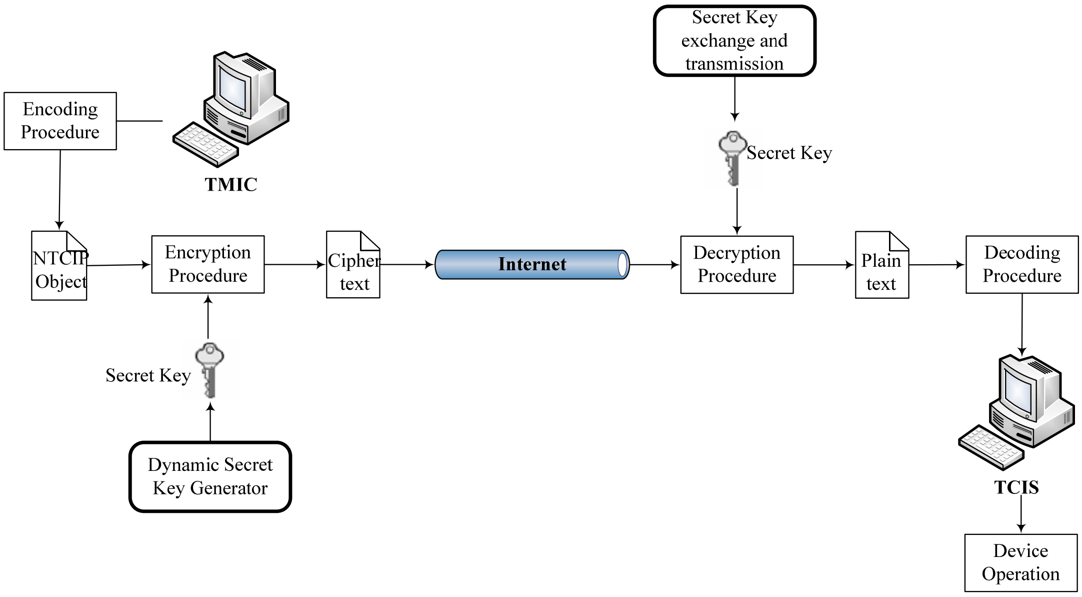


Figure 4.2 Framework of data transmission

- **Procedure for encoding**

  The procedure describes that TMIC generates NTCIP Objects according to encoding rules (e.g., EBR, OER, etc) to make the objects transform into the STMP code style which is suitable for transmission.

- **Procedure for secret key generation**

  The procedure describes the secret key generation by DSKG and the secret key transmission or exchange.

- **Procedure for encryption**

  The procedure describes the secret key and NTCIP objects are fed into the cipher to make NTCIP objects transform into ciphertexts via the encryption algorithm before transmission.

- **Procedure for data transmission**

The procedure describes the ciphertexts transmission from TMIC to TCIS via the Internet Network.

- **Procedure for decryption**

  The procedure describes the ciphertexts transformation into the original NTCIP objects while the ciphertexts are transmitted to TCIS.

- **Procedure for decoding**

  The procedure describes the NTCIP objects are decoded from the STMP code to the original style to supply the related device usage.

Basically, this research concentrates on the security and efficiency in ATMS data transmission; thus, the major theme is to discuss the influences on data transmission under the DSM addition. Therefore, we are not concerned with the encoding/decoding procedures in this research.

4.3.2 The protocol stacks and hardware for Simulation

(a) Protocol Stacks for Simulation

To transmit a data object, we first need to select the protocols which are used for transmission. In order to confirm the reliability of DSM, we use several communications protocol stacks to be the groundwork to carry out the data quantification and analysis, and then to design the procedures for the experiments upon the protocol stacks. The protocol stack selections of this research are illustrated as the thick lines in Figure 4.3. In which, the application level, transport level and subnetwork level respectively select the STMP, TCP/IP and Ethernet. Besides, there are two different communications media in the plant level; they are twisted pair (wired network) and wireless network. The protocol stacks and the combinations are shown as Table 4.1 and Figure 4.3.

Table 4.1 Protocol stack items of the experiments

Combination	Application Level	Transport Level	Subnetwork Level	Plant Level
I	STMP	TCP/IP	Ethernet	Twisted Pair
II	STMP	TCP/IP	Ethernet	Wireless

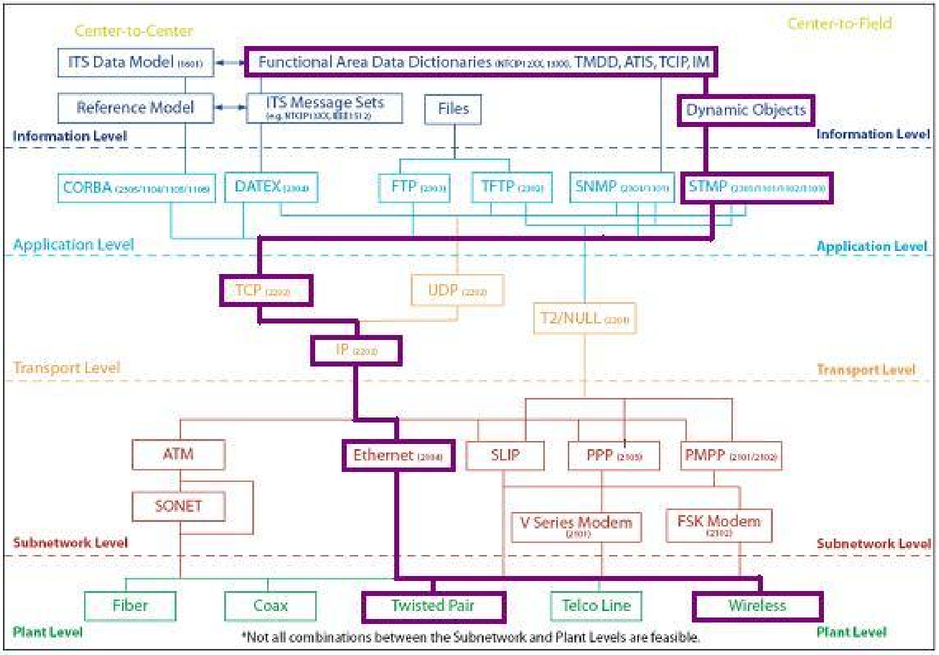


Figure 4.3 Protocol stacks of the experiments

(b) Hardware for Simulation

The experiments utilize computers to simulate TMIC and TCIS in the laboratory environment with a view to improving the efficiencies in operations and saving time in progress. This manner could also overcome the difficulties in controlling the data despatching/receiving well, taking down the time-consuming in encryption/decryption procedures precisely and avoiding other uncertain factors suitably under the real machines and traffic devices. The specifications of each computer which the experiments used are listed as Table 4.2.

Table 4.2 Specification of simulated computers

No.	**Role**		**Specifications**
1	**TMIC**	CPU	Intel(R) Core(TM)2 Quad CUP Q9400@2.66GHz
		RAM	5GB
		OS	Microsoft Windows XP Professional SP3
2	**TCIS-i**	CPU	Intel(R) Core(TM)2 Quad CUP Q9400@2.66GHz
		RAM	5GB
		OS	Microsoft Windows XP Professional SP3
3	**TCIS-ii**	CPU	Pentium(R) 4 CPU1.80GHz
		RAM	1GB
		OS	Microsoft Windows XP Professional SP3
4	**TCIS-iii**	CPU	Intel Pentium 3 processor 863 MHz
		RAM	256 MB
		OS	Microsoft Windows XP Professional
5	**TCIS-iv**	CPU	Intel Pentium 2 processor 451 MHz
		RAM	256 MB
		OS	Microsoft Windows XP Professional SP3

(c) Communications Media for Simulation

Generally speaking, the existing communications media are into two categories: the wired network and the wireless network. Moreover, there are three categories of wired network: fibre cable, twisted pair and coax cable; and the wireless network could be further divided into the short distance wireless network communications and the long distance wireless network communications as well. On the other hand, the traffic control system nowadays usually establishes its own communications channels as VPN and it offers an exclusive and secured connection that is layered on top of a public network as well.

Therefore, in order to simulate the real conditions, this research chooses the existing communications media which the traffic control systems commonly use and are under the VPN framework additionly, namely: the twisted pair communications of wired network and the 3.5G mobile communications of wireless network. Figure 4.4 illustrates the VPN framework of Nanyang Technological University, Singapore (NTU) and it is also adopted by the experiments; it makes use of the Internet's infrastructure to move secured data to and from the campus network. Users can access the University's online resources in the comfort of their own computer through the Internet Service Providers (ISP).

- **Wired Network Communications**

Table 4.3 lists the wired network specifications of the experiments, and Figure 4.4 shows the framework of the wired network communications with VPN which these experiments implement. In which, we install the TMIC and TCIS at the Transportation Lab. in NTU campus and off-campus respectively. In addition, the ISP is provided by StarHub Ltd. Corp, Singapore as well.

Table 4.3 Specification for wired network

Specific		**Description**
▪ Communication style	:	Wired Network
▪ Test site	:	Transportation Lab. of NTU, Singapore
▪ ISP	:	StarHub Ltd. Corp, Singapore
▪ Plant level	:	Twisted pair
▪ Maximum transmission speed	:	100Mbps
▪ Throughput	:	100Mbps

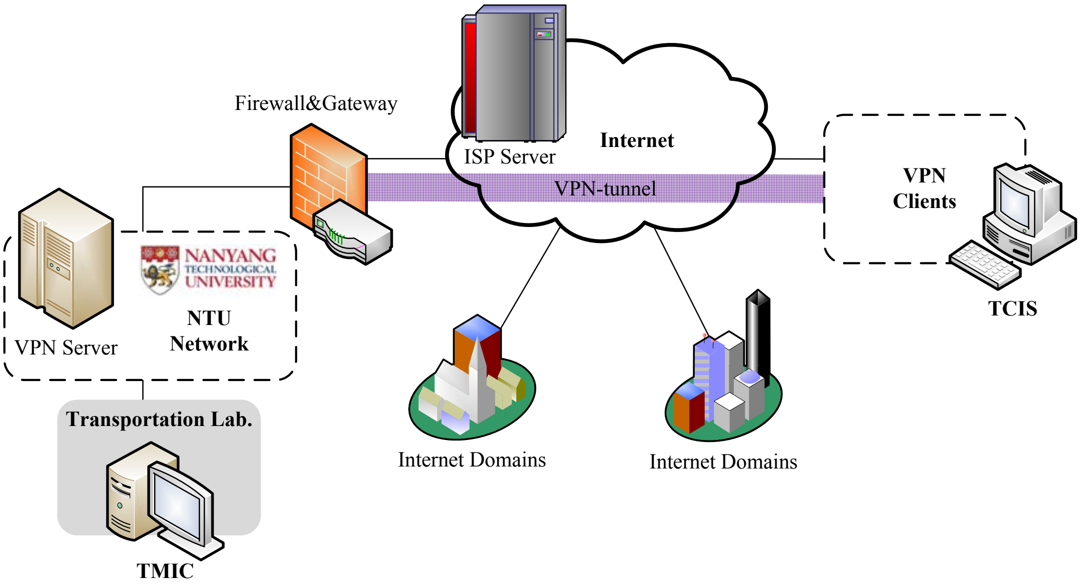


Figure 4.4 Framework of wired network

● Wireless Network Communication

Overall, the wireless network communications could separate into short distance wireless network communications (e.g., wireless local area network (WLAN), Bluetooth, infrared communications) and long distance wireless network communications (e.g., GPRS, 3G mobile communications). Due to the communications media of long distance wireless network are more stable and effectively than short distance wireless network; for instance, as Figure 1.2 shown, the traffic control system of Taipei, Taiwan uses GPRS mobile communications in long distance wireless network communications.

Table 4.4 and Figure 4.5 show the specifications for communications media of the long distance wireless network that the experiments use. As wired network communications, we install both of the simulated computers at the Transportation Lab., in NTU campus and set up the 3.5G wireless module at the TCIS-side. On the other hand, the ISP is provided by Mobile One Ltd. Corp.; and the network scheme is under the VPN framework of NTU as well.

Table 4.4 Specifications for 3.5G mobile communications

	Specific		Description
▪	Communication style	:	3.5G mobile communication
▪	Test site	:	NTU Transportation Lab., Singapore
▪	ISP	:	Mobile One Ltd. Corp., Singapore
▪	Wireless module	:	HUAWE E220
▪	Frequency	:	2100MHz
▪	Maximum transmission speed	:	3.6Mbps
▪	Throughput	:	7.2Mbps

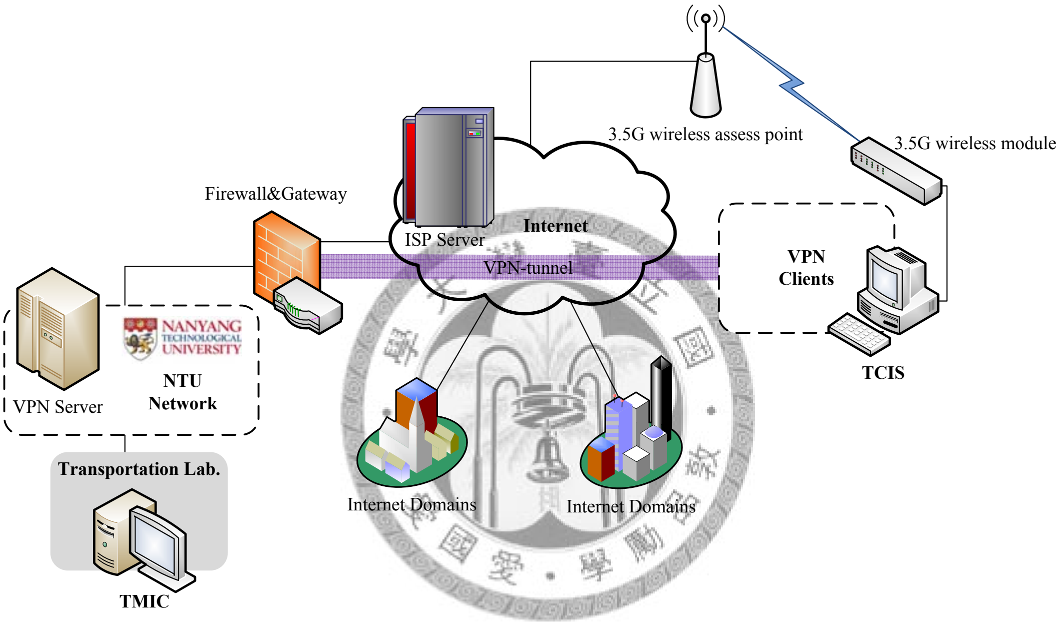


Figure 4.5 Framework of 3.5G mobile communications

4.3.3 NTCIP objects for the Simulation

NTCIP is the specialized communications protocol framework which is designed for ITS, SNTP is the variation of SNMP and is the exclusive communications protocol for NTCIP as well. Both SNTP and SNMP use MIBs to carry out the data management. Basically, we could make the STMP syntax becomes suitable for transmission via a process termed code. Practically, the code process separates into two segments: the encoding procedure and the decoding procedure. The transmitter has to encode the NTCIP object to be the digital data which can be transmitted easier before sending it. Correspondingly, the receiver needs to decode the digital data into the original NTCIP object and then read out the content while the receiver receives the digital data from the transmitter.

The principle in NTCIP object choice of this research is dependent on the message size. In order to test the influences on the transmitted message size in encryption, transmission and decryption, we select the following seven types of NTCIP objects to be the test objects. Tables 4.5 to 4.11 are the STMP codes of NTCIP objects which are used for the experiments in this research and each of them has different message size.

In which, there are three dynamic objects (see Table 4.5~4.7), by contrast, the message size of dynamic objects which are encoded by the dynamic object style are shorter than others. We could say that if the STMP dynamic object style is used, a dynamic object could be configured to include this data element; it means that only the object identifier would not be transmitted (because each end of the link would already be aware of what data to expect next). Furthermore, the data value would be encoded using OER, which is more efficient than BER. Therefore, due to the OER encoding rule and the dynamic object usage, these would shorten the message size to achieve the advantage of less network bandwidth usage. As the encoding rule is not within the scope of this research, we just pick the available STMP codes to be the simulate NTCIP objects of these experiments.

Table 4.5 NTCIP Object No.01－trafficControl Code

Object Name	Traffic Control
OID	1,3,6,1,4,1,1206,4,2,7,7
STMP Code (Byte Stream)	[86][30][06][02][01][00][02][01][00]
Object Size	9 bytes

Table 4.6 NTCIP Object No.02－cmsDimSchedule Code

Object Name	CMS Dim Schedule
OID	1,3,6,1,4,1,1206,4,2,9,11
STMP Code (Byte Stream)	[c9][30][0f][02][01][03][02][01][04][02][01][05][02][01][06][02][01][07]
Object Size	18 bytes

Table 4.7 NTCIP Object No.03－phaseOrderTable Code

Object Name	Phase Order Table
OID	1,3,6,1,4,1,1206,4,2,7,14
STMP Code (Byte Stream)	[82][30][1b][30][19][02][01][00][02][01][00][02][01][00][02][01][00][02][01][00][02][01][00][30][05][30][03][02][01][00]
Object Size	30 bytes

Table 4.8 NTCIP Object No.04－timingPlantable Code

Object Name	Timing Plan Table
OID	1,3,6,1,4,1,1206,4,2,7,3
STMP Code (Byte Stream)	[a0][06][0b][2b][06][01][04][01][89][36][04][02][07][03][30][1f][30][1d][02][01][03][02][01][03][02][01][03][02][01][03][02][01][03][02][01][03][30][09][02][01][00][02][01][04][02][01][02]
Object Size	47 bytes

Table 4.9 NTCIP Object No.05－timingPlantable Code

Object Name	VD Current Data Table
OID	1,3,6,1,4,1,1206,4,2,8,11,1
STMP Code (Byte Stream)	[b0][06][0c][2b][06][01][04][01][89][36][04][02][08][0b][01][30][44][30][42][02][01][01][02][01][01][02][01][01][02][01][01][02][01][01][02][01][01][02][01][01][30][03][02][01][02][30][03][02][01][02][30][03][02][01][02][30][03][02][01][02][30][03][02][01][02][30][03][02][01][02][30][03][02][01][02][30][03][02][01][02][30][03][02][01][02]
Object Size	87 bytes

Table 4.10 NTCIP Object No.06－timingPlanBacsicParatable Code

Object Name	Timing Plan Basic Para Table
OID	1,3,6,1,4,1,1206,4,2,7,4
STMP Code (Byte Stream)	[a0][06][0b][2b][06][01][04][01][89][36][04][02][07][04][30][81][a5][30][81][a2][02][01][03][02][01][08][30][18][02][01][00][02][01][04][02][01][02][02][01][02][02][01][02][02][01][02][02][01][02][02][01][02][30][18][02][01][00][02][01][04][02][01][02][02][01][02][02][01][02][02][01][02][02][01][02][02][01][02][30][18][02][01][00][02][01][04][02][01][02][02][01][02][02][01][02][02][01][02][02][01][02][02][01][02][30][18][02][01][00][02][01][04][02][01][02][02][01][02][02][01][02][02][01][02][02][01][02][02][01][02][30][18][02][01][00][02][01][07][02][01][02][02][01][02][02][01][02][02][01][02][02][01][02][02][01][02][30][18][02][01][00][02][01][04][02][01][02][02][01][02][02][01][02][02][01][02][02][01][02][02][01][02]
Object Size	182 bytes

Table 4.11 NTCIP Object No.07－vdCurrentDataTable Code

Object Name	VD Current Data Table
OID	1,3,6,1,4,1,1206,4,2,8,11,1
STMP Code (Byte Stream)	[c0][06][0c][2b][06][01][04][01][89][36] [04][02][08][0b][01][30][82][01][02][30] [81][ff][02][01][69][02][01][04][02][01] [03][02][01][17][02][01][1e][02][01][1a] [02][01][04][30][18][02][01][01][02][01] [01][02][01][01][02][01][01][02][01][01] [02][01][01][02][01][01][02][01][01][30] [18][02][01][46][02][01][46][02][01][46] [02][01][46][02][01][46][02][01][46][02] [01][46][02][01][46][30][18][02][01][02] [02][01][02][02][01][02][02][01][02][02] [01][02][02][01][02][02][01][02][02][01] [02][30][18][02][01][50][02][01][50][02] [01][50][02][01][50][02][01][50][02][01] [50][02][01][50][02][01][50][30][18][02] [01][05][02][01][05][02][01][05][02][01] [05][02][01][05][02][01][05][02][01][05] [02][01][05][30][18][02][01][37][02][01] [37][02][01][37][02][01][37][02][01][37] [02][01][37][02][01][37][02][01][37][30] [18][02][01][41][02][01][41][02][01][41] [02][01][41][02][01][41][02][01][41][02] [01][41][02][01][41][30][18][02][01][41] [02][01][41][02][01][41][02][01][41][02] [01][41][02][01][41][02][01][41][02][01] [41][30][18][02][01][41][02][01][41][02] [01][41][02][01][41][02][01][41][02][01] [41][02][01][41][02][01][41]
Object Size	277 bytes

4.4 Experiment Contents

As mentioned earlier, the primary goal of the experiments in this research is to know the degree of the negative-effect generated due to the DSM addition and set up regression equations which can represented by the relationship between the variables as given in Equation 4.1. Therefore, in this research, the experiments are designed under different communications media; the goal is to understand the delay in data transmission by different communication media and provide the result for engineers or managers in system security to further improve their designs.

4.4.1 Experiment Methodology

In order for these experiments to operate effectively, this research uses computers to displace and simulated the real-TMIC and the real-TCIS in the traffic control system. This method could let us control data dispatching and receiving correctly, so that the precise point where encryption, decryption and transmission takes place can be taken down. Additionally, under real condition simulation with wired network being used, equipments are located outside campus premises to avoid operating under the local area network (LAN) of NTU-campus.

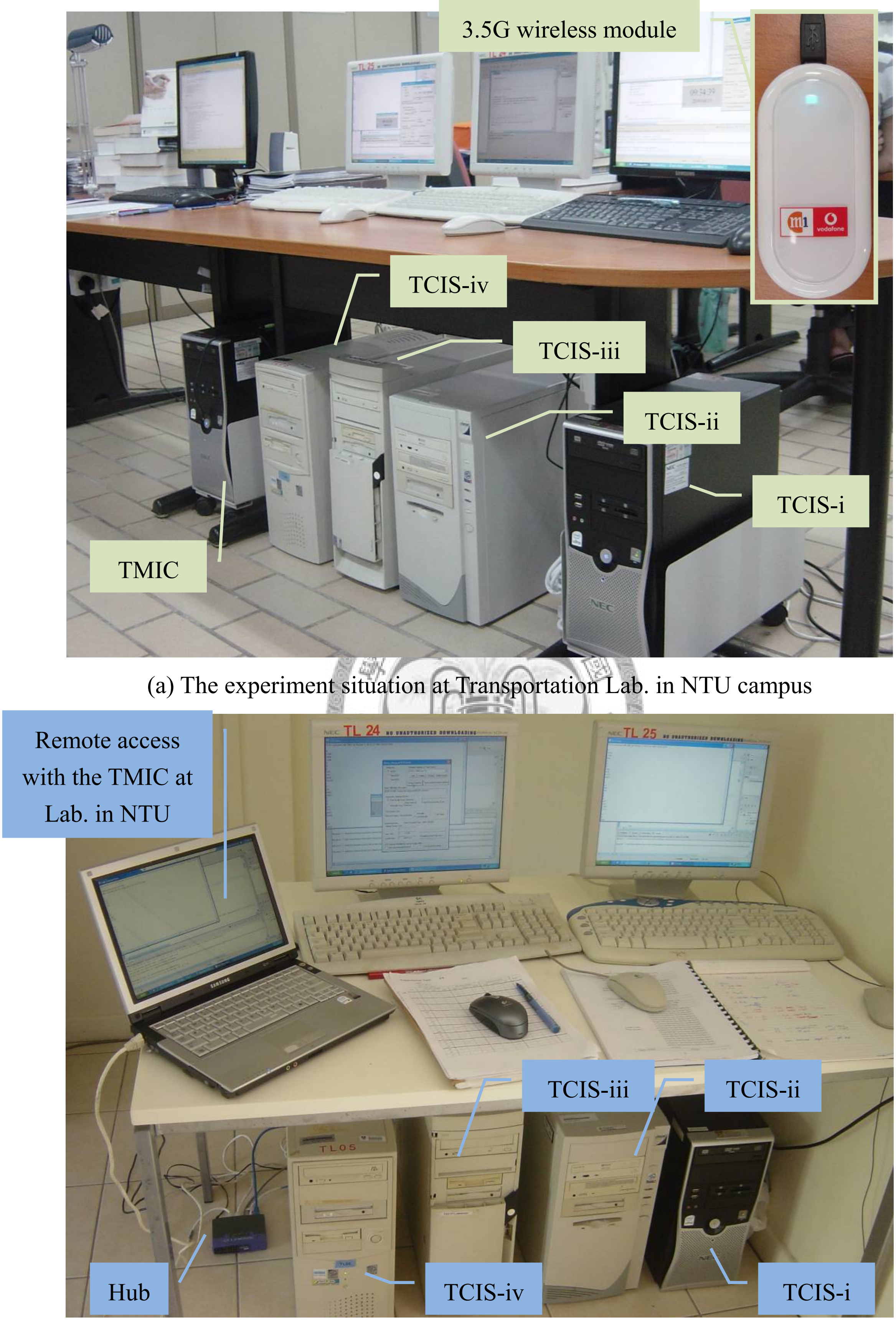
- **Experiment procedures**

Step1. Set up the simulated TMIC/TCIS, communications media and VPN connection first. Figure 4.6 (a) and (b) show the experiment situations and used equipment installation at Transportation Lab. in NTU campus and out of the NTU-campus respectively. Figure 4.7 represents the VPN connection procedure;

Step2: Install the network time calibration software termed NTPClock which synchronizes watches with National Standard Time and Frequency Laboratory, Taiwan per 20 seconds automatically for each side to ensure both of the simulated TMIC and TCIS are on the same synchronization and reduce the inaccuracy in time calculation further (the interface of the NTPClock is shown in Figure 4.8);

Step3: Input the related arguments, namely: port, host address, transmitted message, length of secret key and public key pair, etc into the DSM programming, and

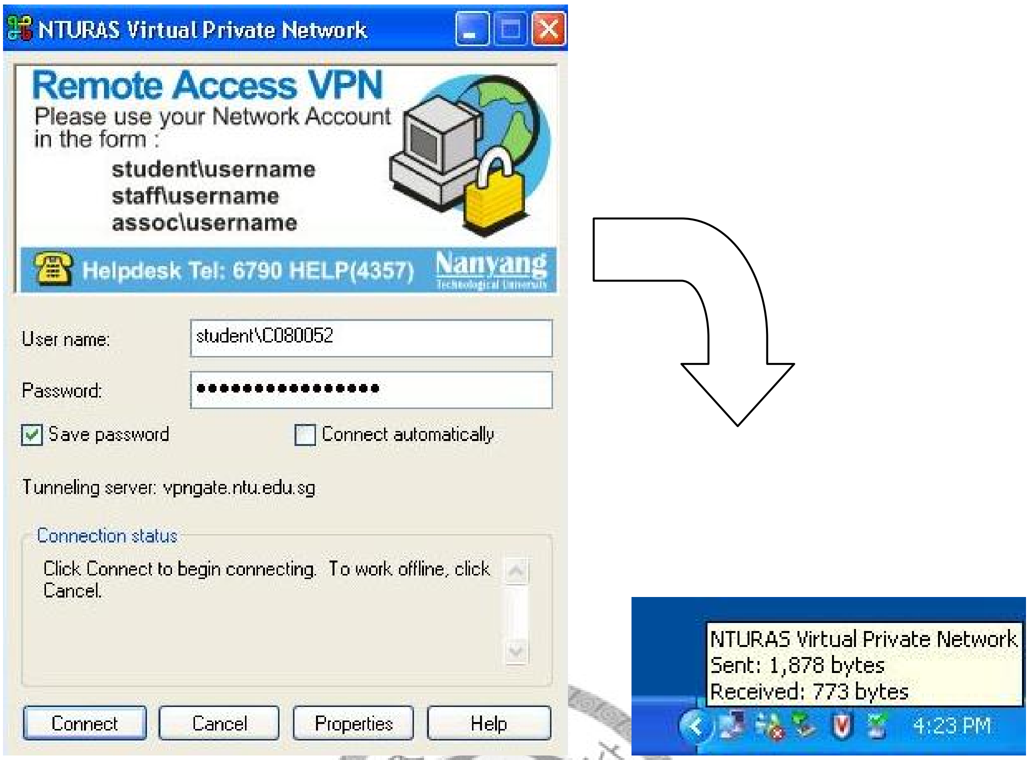
Step4: Start the experiment and take down the time-consumption of each procedure in data transmission and encryption/decryption; Figure 4.9 and 4.10 are the display of the DSM programming operation and note items respectively.



(a) The experiment situation at Transportation Lab. in NTU campus

(b) The simulated TCIS installation out of the NTU-campus

Figure 4.6 Experiment situations



NTURAS Virtual Private Network

Remote Access VPN

Please use your Network Account in the form :

student\username
staff\username
assoc\username

Helpdesk Tel: 6790 HELP(4357)

User name: student\C080052

Password: ●●●●●●●●●●●●●●●●

☑ Save password □ Connect automatically

Tunneling server: vpngate.ntu.edu.sg

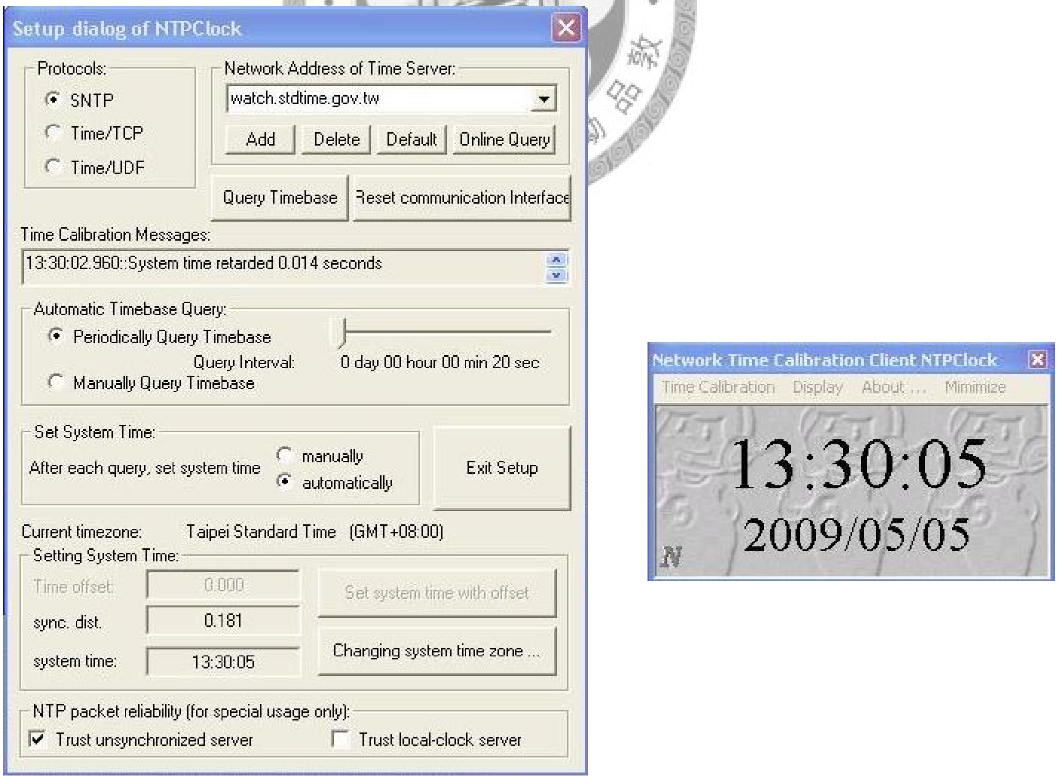
Connection status

Click Connect to begin connecting. To work offline, click Cancel.

NTURAS Virtual Private Network
Sent: 1,878 bytes
Received: 773 bytes

4:23 PM

Figure 4.7 VPN connection procedures



Setup dialog of NTPClock

Protocols:
● SNTP
○ Time/TCP
○ Time/UDF

Network Address of Time Server: watch.stdtime.gov.tw

Time Calibration Messages:
13:30:02.960::System time retarded 0.014 seconds

Automatic Timebase Query:
● Periodically Query Timebase
Query Interval: 0 day 00 hour 00 min 20 sec
○ Manually Query Timebase

Set System Time:
After each query, set system time ○ manually ● automatically

Current timezone: Taipei Standard Time (GMT+08:00)

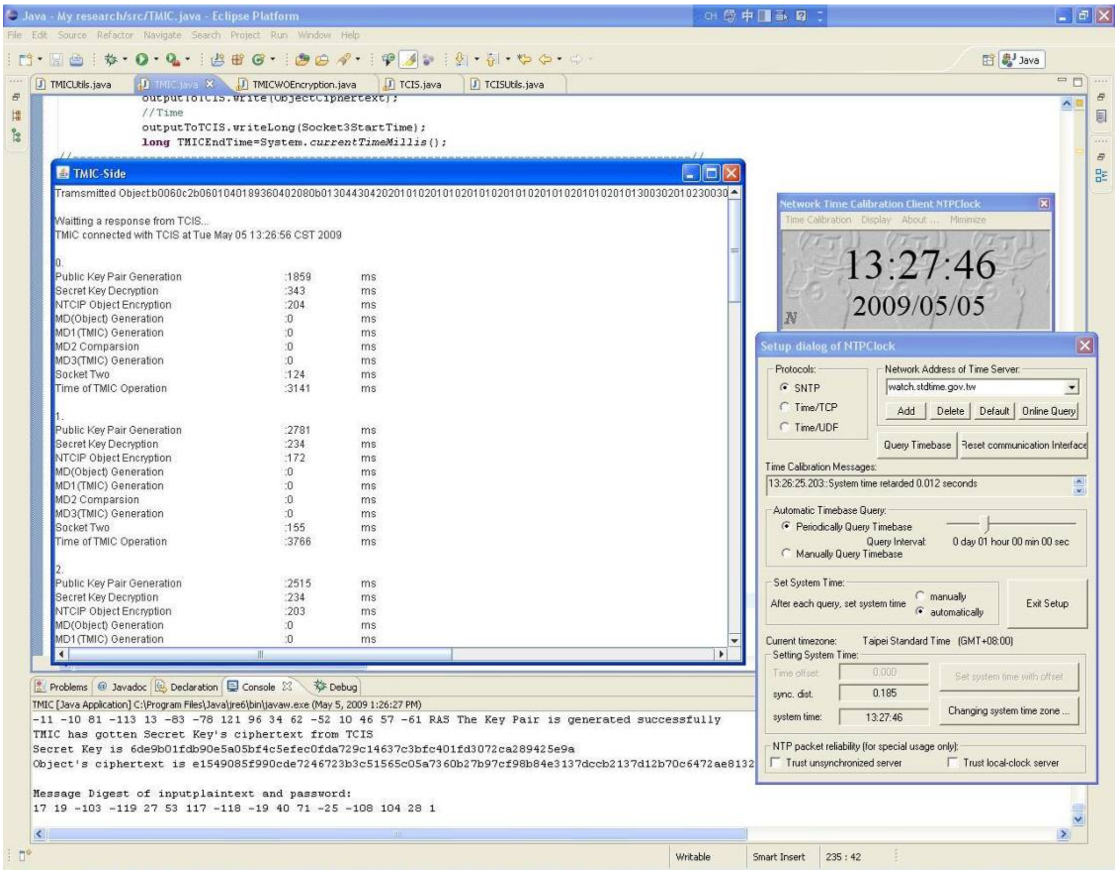
Setting System Time:
Time offset: 0.000
sync. dist. 0.181
system time: 13:30:05

NTP packet reliability (for special usage only):
☑ Trust unsynchronized server □ Trust local-clock server

Network Time Calibration Client NTPClock

13:30:05
2009/05/05

Figure 4.8 Network Time Calibration Software－NTPClock



Java - My research/src/TMIC.java - Eclipse Platform
File Edit Source Refactor Navigate Search Project Run Window Help
TMICUtils.java
TMIC.java
TMICWOEncryption.java
TCIS.java
TCISUtils.java
Java

```
outputToTCIS.write(ObjectCiphertext);
//Time
outputToTCIS.writeLong(Socket3StartTime);
long TMICEndTime=System.currentTimeMillis();
```

```
Tramsmitted Object:b0060c2b0601040189360402080b0130443042020101020101020101020101020101020101020101300302010230030

Waitting a response from TCIS...
TMIC connected with TCIS at Tue May 05 13:26:56 CST 2009

0.
Public Key Pair Generation          :1859     ms
Secret Key Decryption               :343      ms
NTCIP Object Encryption             :204      ms
MD(Object) Generation               :0        ms
MD1(TMIC) Generation                :0        ms
MD2 Comparsion                      :0        ms
MD3(TMIC) Generation                :0        ms
Socket Two                          :124      ms
Time of TMIC Operation              :3141     ms

1.
Public Key Pair Generation          :2781     ms
Secret Key Decryption               :234      ms
NTCIP Object Encryption             :172      ms
MD(Object) Generation               :0        ms
MD1(TMIC) Generation                :0        ms
MD2 Comparsion                      :0        ms
MD3(TMIC) Generation                :0        ms
Socket Two                          :155      ms
Time of TMIC Operation              :3766     ms

2.
Public Key Pair Generation          :2515     ms
Secret Key Decryption               :234      ms
NTCIP Object Encryption             :203      ms
MD(Object) Generation               :0        ms
MD1(TMIC) Generation                :0        ms
```

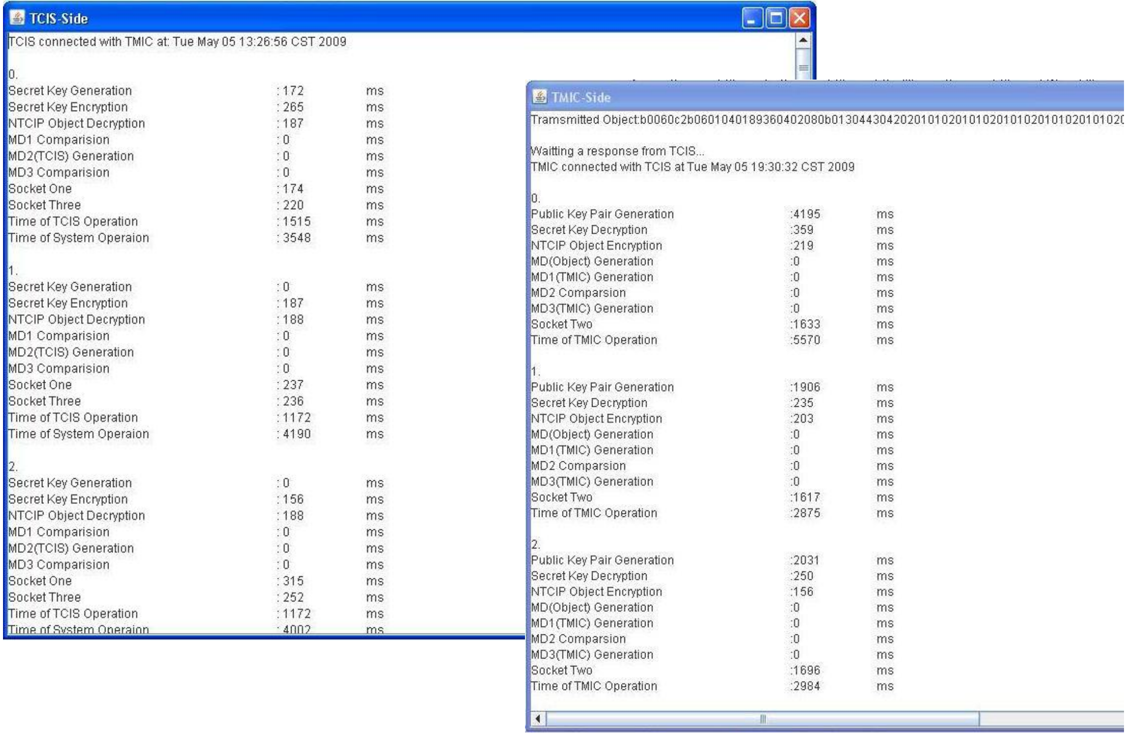
```
TMIC [Java Application] C:\Program Files\Java\jre6\bin\javaw.exe (May 5, 2009 1:26:27 PM)
-11 -10 81 -113 13 -83 -78 121 96 34 62 -52 10 46 57 -61 RAS The Key Pair is generated successfully
TMIC has gotten Secret Key's ciphertext from TCIS
Secret Key is 6de9b01fdb90e5a05bf4c5efec0fda729c14637c3bfc401fd3072ca289425e9a
Object's ciphertext is e1549085f990cde7246723b3c51565c05a7360b27b97cf98b84e3137dccb2137d12b70c6472ae8132

Message Digest of inputplaintext and password:
17 19 -103 -119 27 53 117 -118 -19 40 71 -25 -108 104 28 1
```

Writable
Smart Insert
235 : 42
Network Time Calibration Client NTPClock
Time Calibration Display About ... Minimize
13:27:46
2009/05/05
Setup dialog of NTPClock

```
Protocols:
● SNTP
○ Time/TCP
○ Time/UDF
Network Address of Time Server: watch.stdtime.gov.tw
[Add] [Delete] [Default] [Online Query]
[Query Timebase] [Reset communication Interface]
Time Calibration Messages:
13:26:25.203::System time retarded 0.012 seconds
Automatic Timebase Query:
● Periodically Query Timebase
    Query Interval:   0 day 01 hour 00 min 00 sec
○ Manually Query Timebase
Set System Time:
After each query, set system time   ○ manually
                                    ● automatically
[Exit Setup]
Current timezone:     Taipei Standard Time   (GMT+08:00)
Setting System Time:
Time offset:   0.000      [Set system time with offset]
sync. dist.    0.185
system time:   13:27:46   [Changing system time zone ...]
NTP packet reliability (for special usage only):
□ Trust unsynchronized server     □ Trust local-clock server
```

Figure 4.9 Display of programming operation



```
TCIS connected with TMIC at: Tue May 05 13:26:56 CST 2009

0.
Secret Key Generation               : 172     ms
Secret Key Encryption               : 265     ms
NTCIP Object Decryption             : 187     ms
MD1 Comparision                     : 0       ms
MD2(TCIS) Generation                : 0       ms
MD3 Comparision                     : 0       ms
Socket One                          : 174     ms
Socket Three                        : 220     ms
Time of TCIS Operation              : 1515    ms
Time of System Operaion             : 3548    ms

1.
Secret Key Generation               : 0       ms
Secret Key Encryption               : 187     ms
NTCIP Object Decryption             : 188     ms
MD1 Comparision                     : 0       ms
MD2(TCIS) Generation                : 0       ms
MD3 Comparision                     : 0       ms
Socket One                          : 237     ms
Socket Three                        : 236     ms
Time of TCIS Operation              : 1172    ms
Time of System Operaion             : 4190    ms

2.
Secret Key Generation               : 0       ms
Secret Key Encryption               : 156     ms
NTCIP Object Decryption             : 188     ms
MD1 Comparision                     : 0       ms
MD2(TCIS) Generation                : 0       ms
MD3 Comparision                     : 0       ms
Socket One                          : 315     ms
Socket Three                        : 252     ms
Time of TCIS Operation              : 1172    ms
Time of System Operaion             : 4002    ms
```

```
Tramsmitted Object:b0060c2b0601040189360402080b0130443042020101020101020101020101020101020

Waitting a response from TCIS...
TMIC connected with TCIS at Tue May 05 19:30:32 CST 2009

0.
Public Key Pair Generation          :4195     ms
Secret Key Decryption               :359      ms
NTCIP Object Encryption             :219      ms
MD(Object) Generation               :0        ms
MD1(TMIC) Generation                :0        ms
MD2 Comparsion                      :0        ms
MD3(TMIC) Generation                :0        ms
Socket Two                          :1633     ms
Time of TMIC Operation              :5570     ms

1.
Public Key Pair Generation          :1906     ms
Secret Key Decryption               :235      ms
NTCIP Object Encryption             :203      ms
MD(Object) Generation               :0        ms
MD1(TMIC) Generation                :0        ms
MD2 Comparsion                      :0        ms
MD3(TMIC) Generation                :0        ms
Socket Two                          :1617     ms
Time of TMIC Operation              :2875     ms

2.
Public Key Pair Generation          :2031     ms
Secret Key Decryption               :250      ms
NTCIP Object Encryption             :156      ms
MD(Object) Generation               :0        ms
MD1(TMIC) Generation                :0        ms
MD2 Comparsion                      :0        ms
MD3(TMIC) Generation                :0        ms
Socket Two                          :1696     ms
Time of TMIC Operation              :2984     ms
```

Figure 4.10 Display of note items

- **Programming operation procedure**

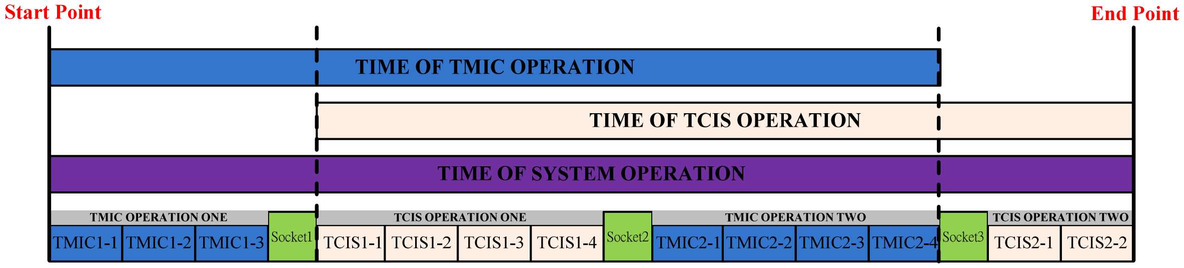


Figure 4.11 Data transmission procedure of the security mechanism

According to Figure 3.13, the DSM operation could be divided into four parts through the TMIC and TCIS operations. Figure 4.11 illustrates the detail of each operation and describes as below:

1) TMIC1-1 : Produce the $\mathbf{MD}_{\mathbf{Object}}$ from the transmitted NTCIP object;

2) TMIC1-2 : Generate the public key pair via DPKG;

3) TMIC1-3 : Create the $\mathbf{MD1}_{\mathbf{TCIS}}$ from $\mathbf{KU}_{\mathbf{TMIC}}$ and $\mathbf{PW1}_{\mathbf{TMIC}}$;

4) Socket1 : Transmit the $\mathbf{MD1}_{\mathbf{TMIC}}$, $\mathbf{KU}_{\mathbf{TMIC}}$ and $\mathbf{M}_{\mathbf{k}}$ to TCIS;

5) TCIS1-1 : Produce the $\mathbf{MD1}_{\mathbf{TCIS}}$ and compare with the $\mathbf{MD1}_{\mathbf{TMIC}}$;

6) TCIS1-2 : Generate the secret key $\mathbf{KS}_{\mathbf{TCIS}}$ via DSKG;

7) TCIS1-3 : Encrypt the $\mathbf{KS}_{\mathbf{TCIS}}$ by $\mathbf{KU}_{\mathbf{TMIC}}$;

8) TCIS1-4 : Create the $\mathbf{MD2}_{\mathbf{TCIS}}$ from $\mathbf{C}_{\mathbf{SK}}$ and $\mathbf{PW2}_{\mathbf{TCIS}}$;

9) Socket2 : Transmit the $\mathbf{MD2}_{\mathbf{TCIS}}$ and $\mathbf{C}_{\mathbf{SK}}$ to TMIC;

10) TMIC2-1 : Produce the $\mathbf{MD2}_{\mathbf{TMIC}}$ and compare with the $\mathbf{MD2}_{\mathbf{TCIS}}$;

11) TMIC2-2 : Decrypt the $\mathbf{C}_{\mathbf{KS}}$ by $\mathbf{KR}_{\mathbf{TMIC}}$ to own the $\mathbf{KS}_{\mathbf{TCIS}}$;

12) TMIC2-3 : Encrypt the NTCIP object by $\mathbf{KS_{TCIS}}$;

13) TMIC2-4 : Create the $\mathbf{MD3_{TMIC}}$ from $\mathbf{C_{OB}}$ and $\mathbf{PW3_{TMIC}}$;

14) Socket3 : Transmit the $\mathbf{MD3_{TMIC}}$ and $\mathbf{C_{OB}}$ to TCIS;

15) TCIS2-1 : Produce the $\mathbf{MD3_{TCIS}}$ and compare with the $\mathbf{MD3_{TMIC}}$, and;

16) TCIS2-2 : Decrypt the $\mathbf{C_{OB}}$ by $\mathbf{KS_{TCIS}}$ to get the NTCIP object.

Note:

The Socket1, Socket2 and Socket3 here are calculated from the data sealing process by transmitters until the unsealing process by receivers; hence, the total time-consumption of these three segments can be expressed as below:

Socket= (Data packet sealing) + (Data packet transmission) + (Data packet unsealing) (4.2)

- **Note items**

The programming would take down the time-consuming of the seventeen procedures (as Figure 4.11 shown) automatically in each experiment for further analyses.

4.4.2 Experiment One

- **Test Title:**

  Experiment on the influences upon the NTCIP object size and communications medium

- **Test Purposes:**

  This experiment focuses on the variations and interactions for transmission efficiency and device operations due to the differences in NTCIP object size.

  i. Confirm if the NTCIP object size $\boldsymbol{M_s}$ is one of the causes of negative-effect generation in data packet transmission or device operation of TMIC and TCIS;

  ii. Discuss the influence of DSM addition on data packet transmission, and;

  iii. Compare the efficiencies of data packet transmission upon the different communications media.

- **Test Objects and Methodologies:**

In this experiment, we utilize computer no. 1 and no. 3 to respectively simulate TMIC and TCIS respectively, and each test condition which is under the different combinations in NTCIP object size, communications media and with DSM addition or without is tested for 130 times. Therefore, there are total of twenty-eight test conditions and over four thousand test data for this experiment; Table C.1 (in Appendix C) lists the detail items of this experiment additionally.

Table 4.12 and Figure 4.12 indicate the test objects and the framework of this experiment respectively; in which, the variables are the NTCIP object size and communications medium. We use these seven different sizes of NTCIP object from the minimum of 9 bytes to the maximum of 277 bytes as shown in Table 4.13, and the communications medium usages are wired network and 3.5G mobile communications under the VPN framework. In addition, the fixed factors of this experiment are the interval of object dispatch, TCIS device usage and the length of AES secret key and RSA public key pair.

Table 4.12 Test objects of Experiment One

Items		Contents
NTCIP object*	:	Object no.1 to no.7 (9 bytes to 277 bytes)
Interval of object dispatch	:	10 seconds
Communications medium*	:	Wired Network/3.5G mobile communications
Simulated computer for TCIS	:	TCIS-ii (as computer no.3 in Table 4.2)
Length of RSA public key pair	:	1024 bits
Length of AES secret key	:	128 bits

＊:The variables of this experiment

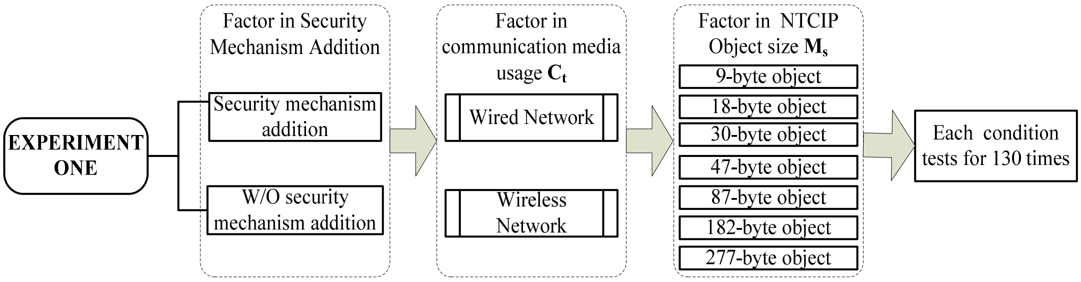

EXPERIMENT ONE
Factor in Security Mechanism Addition
Security mechanism addition
W/O security mechanism addition
Factor in communication media usage $\mathbf{C_t}$
Wired Network
Wireless Network
Factor in NTCIP Object size $\mathbf{M_s}$
9-byte object
18-byte object
30-byte object
47-byte object
87-byte object
182-byte object
277-byte object
Each condition tests for 130 times

Figure 4.12 Framework of Experiment One

Table 4.13 NTCIP object usage for Experiment One

No.	Object Name	Object Size	Note
1	Traffic Control	9-byte	Dynamic Object
2	CMS Dim Schedule	18-byte	Dynamic Object
3	Phase Order Table	30-byte	Dynamic Object
4	Timing Plan Table	47-byte	
5	VD Current Data Table (one lane)	87-byte	
6	Timing Plan Basic Para Table	182-byte	
7	VD Current Data Table (eight lanes)	277-byte	

4.4.2 Experiment Two

- **Test Title:**

Experiment on the influences upon the different lengths of AES secret key and RSA public key pair combinations

- **Test Purpose:**

As described in Chapter Three, DSM is constructed from the hybrid cryptosystem which combines with the AES cryptography and RSA cryptography. Taken into consideration, this could modify the weaknesses in both the symmetric cryptosystems and in the asymmetric cryptosystems and provide multiple secured protections for the ATMS data transmission. On the other hand, it is possible to improve the security level via increasing the AES secret key or RSA public key pair length thus; however, this treatment would consume more system resources and bring increased negative-effects to the core system. From these reasons, this experiment is designed to verify the relationships between the AES secret key length $\boldsymbol{KS_l}$ and RSA public key pair length $\boldsymbol{KP_l}$, and discuss whether the different communications medium usage $\boldsymbol{C_m}$ is an effective factor for the device operation of TMIC and TCIS further.

- **Test Objects and Methodologies:**

Similar as Experiment One, Experiment Two also utilizes computer no. 1 and no. 3 to simulate TMIC and TCIS respectively, and each test condition that is under the different combinations in secret information (i.e., the length of AES secret key and RSA public key pair) and communications media (i.e., wired network and 3.5G mobile communications under the VPN framework) would be tested for 150 times. Therefore, there would be eighteen test conditions in this experiment (see Table C.2 in Appendix C).

As Figure 4.13 and Table 4.14 shown; the variables are the AES secret key length and the length of RSA public key pair through the different communications media, and the fixed factors are the transmitted object size, interval of object dispatch and TCIS device usage. Hence, there would be total night secret information combinations additionally.

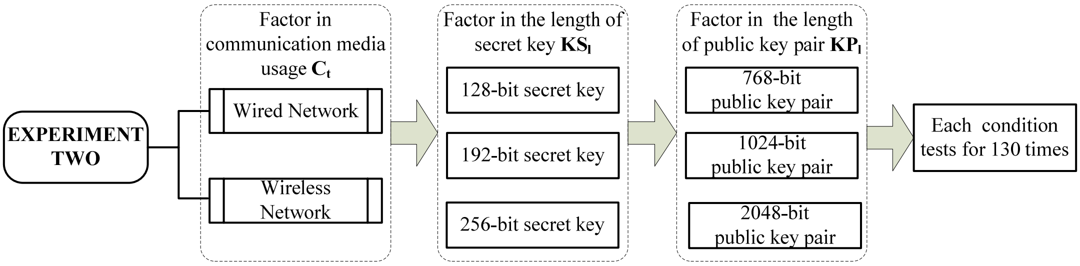

EXPERIMENT TWO
Factor in communication media usage $\mathbf{C_t}$
Wired Network
Wireless Network
Factor in the length of secret key $\mathbf{KS_l}$
128-bit secret key
192-bit secret key
256-bit secret key
Factor in the length of public key pair $\mathbf{KP_l}$
768-bit public key pair
1024-bit public key pair
2048-bit public key pair
Each condition tests for 130 times

Figure 4.13 Framework of Experiment Two

Table 4.14 Test objects of Experiment Two

Items		Contents
NTCIP object	:	Object no.5 (87 bytes)
Interval of object dispatch	:	10 seconds
Communications medium*	:	Wired Network/3.5G mobile communications
Simulated computer for TCIS	:	TCIS-ii (as computer no.3 in Table 4.2)
Length of RSA public key pair*	:	168 bits,1024 bits and 2048 bits
Length of AES secret key*	:	128 bits, 192 bits and 256 bits

∗:The variables of this experiment

4.4.3 Experiment Three

- **Test Title:**

Experiment on the influences upon the computation-capability of TCIS-side and the interval of the NTCIP object dispatch

- **Test Purpose:**

- As discussed earlier, it pointed out that the computation-capability of real-TCIS or other traffic devices on roads outdoor is normally not as well simulated as TCIS at laboratory. In addition, it is evident that the DSM addition would consume more resources from the core system, and the tight interval of the NTCIP object dispatch would increase more loads in network transmissions. With this taken into consideration, we boldly assume that the computation-capability of TCIS and the interval of object dispatch are the effective factors not only in TCIS device operation but also in data packet transmission. Therefore, this experiment is designed to confirm these considerations and discuss the correlations between device operations and efficiencies on data packet transmission.

- **Test Objects and Methodology:**

The main differences between Experiment Three and the first two experiments are that it utilizes three different computation-capability computers (i.e., TCIS-i, TCIS-ii, TCIS-iii and TCIS-iv) to simulate the different operation efficiencies of TCIS device, and the intervals of object dispatch are changeable (the minimum is 3 seconds and the maximum is 60 seconds). Besides, the experiment still uses computer no.1 to simulate the TMIC device and the communication medium which uses wired network and 3.5G mobile communications under the VPN framework.

As Figure 4.14 shown, there are a total of forty test conditions in this experiment and detailed test items are listed as Table C.3 (in Appendix C). In addition, Table 4.15 indicates the test objects of this experiment; the variables are the TCIS simulated computers and the communication medium usages, and the fixed factors are the transmitted NTCIP object size, the interval of the NTCIP object dispatch and the length of AES secret key and RSA public key pair.

Table 4.15 Test objects of Experiment Three

Items		Contents
NTCIP object	:	Object no.5 (87 bytes)
Interval of object dispatch	:	10 seconds
Communications medium*	:	Wired Network/3.5G mobile communications
Simulated computer for TCIS*	:	TCIS-i, TCIS-ii, TCIS-iii and TCIS-iv
Length of RSA public key pair	:	1024 bits
Length of AES secret key	:	128 bits

∗:The variables of this experiment

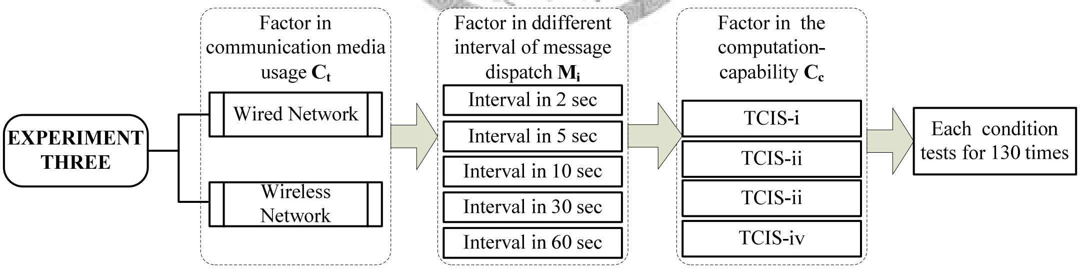

EXPERIMENT THREE
Factor in communication media usage $\mathbf{C}_t$
Wired Network
Wireless Network
Factor in ddifferent interval of message dispatch $\mathbf{M}_i$
Interval in 2 sec
Interval in 5 sec
Interval in 10 sec
Interval in 30 sec
Interval in 60 sec
Factor in the computation-capability $\mathbf{C}_c$
TCIS-i
TCIS-ii
TCIS-ii
TCIS-iv
Each condition tests for 130 times

Figure 4.14 Framework of Experiment Three

4.5 Expected Outcomes

As mentioned above, by contrast, people invariably tend to be more concerned about security and ignore the system operation efficiency. Of course, without a doubt, security is indeed important and essential for a security mechanism. However, upon considering security requirements, one should be more interested in the operational efficiencies of the core systems. Thus, the above experiments are implemented to investigate the issues in system operation efficiencies due to the security mechanism addition, and the expected outcomes are as shown below:

- From the experiences gathered from computer usages, larger sized transmitted objects might cause more delays in data transmission and device; therefore, we infer that the NTCIP object size would influence the efficiencies of the network transmission and system operation;
- Different communications media would differ in network bandwidth, and it might influence the total operational efficiency of DSM due to diversified delays in transmission; generally speaking, we believe that the wired network communications would achieve better performance and stability than 3.5G mobile communications;
- There are many researches and studies to support the fact that the operation efficiencies of symmetric cryptosystems are better than the asymmetric cryptosystems. Hence, we expect that RSA cipher operation would generate more operation delays than AES. Besides, we are also interested in whether the ASE cryptography and RSA cryptography would have the interaction effects within the hybrid cryptosystem in this research further;

- We infer that the DSM addition in ATMS data transmission might influence the device operation both of the TMIC and TCIS, but it might not influence the efficiency in network transmission;
- The tight interval of object dispatch would cause higher workloads for network transmission and generate delay effects in between; in addition, this kind of effects would be evident in the more narrow bandwidth network, and;
- The computation-capability of TCIS devices might be the major point in operation delays; we infer that the lower computation-capability devices would have more delays in operation due to the devices cannot deal with the large or complex data in a short time.

So far, as mentioned above, the possible factors in the operation delay and transmission delay generation could be represented as following:

- Operation delay: the computation-capability of TCIS devices $\boldsymbol{C_c}$, the interval of object dispatch $\boldsymbol{M_i}$, the DSM addition, the NTCIP size $\boldsymbol{M_s}$, and the length of AES secret key $\boldsymbol{KS_l}$ and RSA public key pair $\boldsymbol{KP_l}$.
- Transmission delay: the computation-capability of TCIS devices $\boldsymbol{C_c}$, the interval of object dispatch $\boldsymbol{M_i}$, different communications media $\boldsymbol{C_m}$, and the NTCIP size $\boldsymbol{M_s}$.

CHAPTER FIVE

DATA ANALYSIS AND FINDINGS

5.1 Introduction

After the DSM establishment upon the sufficiently security and a series of experiments, this chapter shall proceed with the data analysis and discuss the experiment result further. The goals of these experiments are to test and verify the potential factors in operation delay and transmission delay in between the DSM operation and set up the regression questions which represent the influences and relationships between these factors via these test results.

In additions, due to DSM programming has to perform the initialization procedure before it starts; hence, all of the first test data are forsaken and not included in analysis results. Besides, the analyses below are all analyzed by the SPSS statistics software and are under the signifiance lever of α=0.05.

5.2 Queue and delay phenomenon of DSM operation

As mentioned in previous chapters, each of the test conditions was tested for 130 times and we should analyze and find out the results from these original data. However, as Figure 5.1, 5.3 and 5.4 shown; certain factors in $\boldsymbol{C_c}$, $\boldsymbol{KP_l}$ and $\boldsymbol{M_f}$ which deals with the device computation-capability present the queue and delay phenomena after the continuous operations. Due to these phenomena represent the nonlinear trend and not easy to analyze further; therefore, in this research, we also set up the threshold values for the normal usage range of DSM operation.

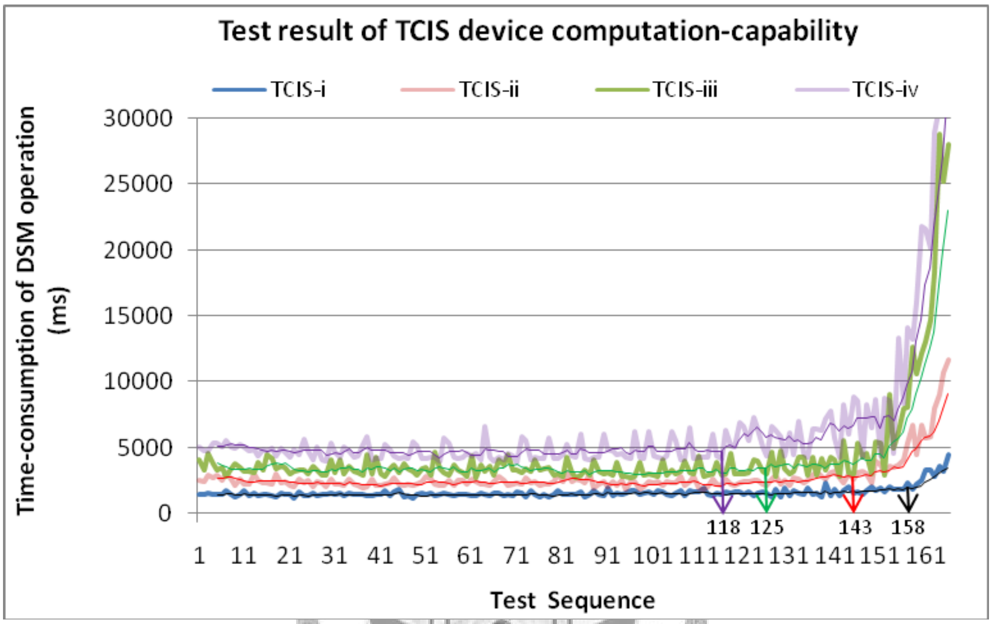


Figure 5.1 DSM operation in different computeation-capability TCIS dvices

Table 5.1 Crack points of DSM continuous operations ($\boldsymbol{C_c}$)

CPU Specifications (MHz)	451	863	1800	2660
Crack Point	118	125	143	158

Table 5.1 shows the crack points of DSM continues operations, and Figure 5.2 represents the trend line of crack points for the different CPU specifications. In addition, the trend line can be expressed by Equation 5.1 further.

$$\mathbf{Y_1=0.002X_1+109.83} \qquad (5.1)$$

$\mathbf{Y_1}$**:** Crack point for the continuous operations of $\boldsymbol{C_c}$

$\mathbf{X_1}$**:** CPU specifications (MHz)

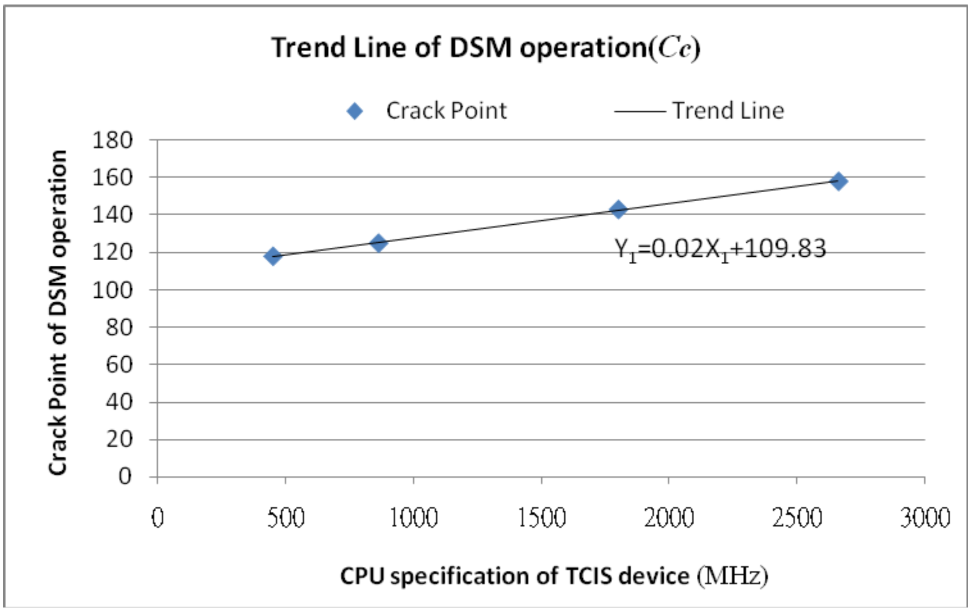


Figure 5.2 Crack point of DSM operations (***C_c***)

Furthermore; Table 5.2 and Figure 5.3 indicate the crack points of DSM continues operation in each public key pair length under ***C_c***=TCIS-iii and ***M_f***=10 second thus.

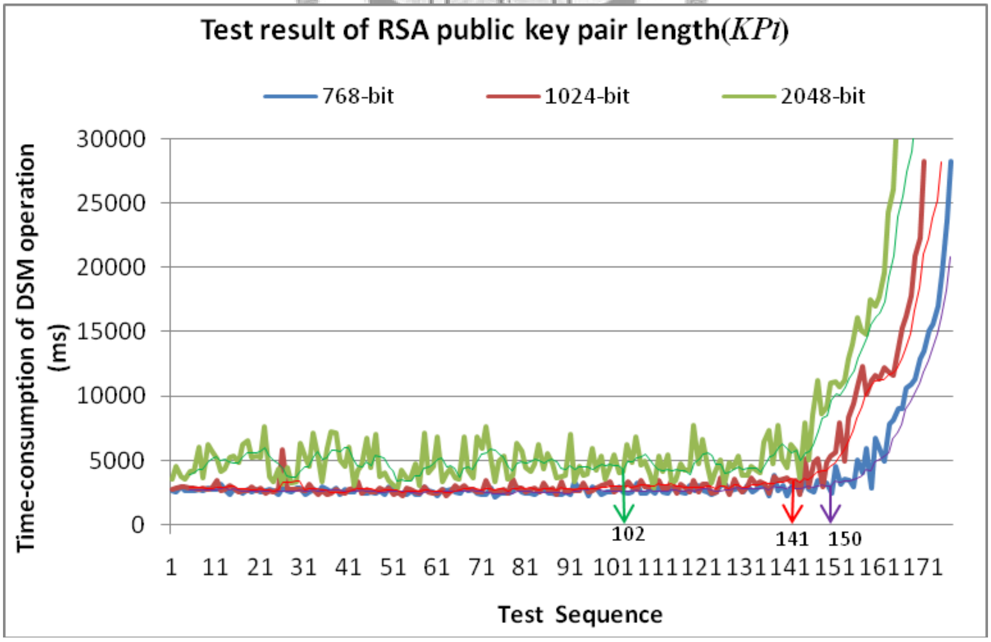


Figure 5.3 DSM operation in different RSA public key pair length

Table 5.2 Crack points of DSM continuous operations (***KP_l***)

KP_l	768-bit	1024-bit	2048-bit
Crack Point	102	141	150

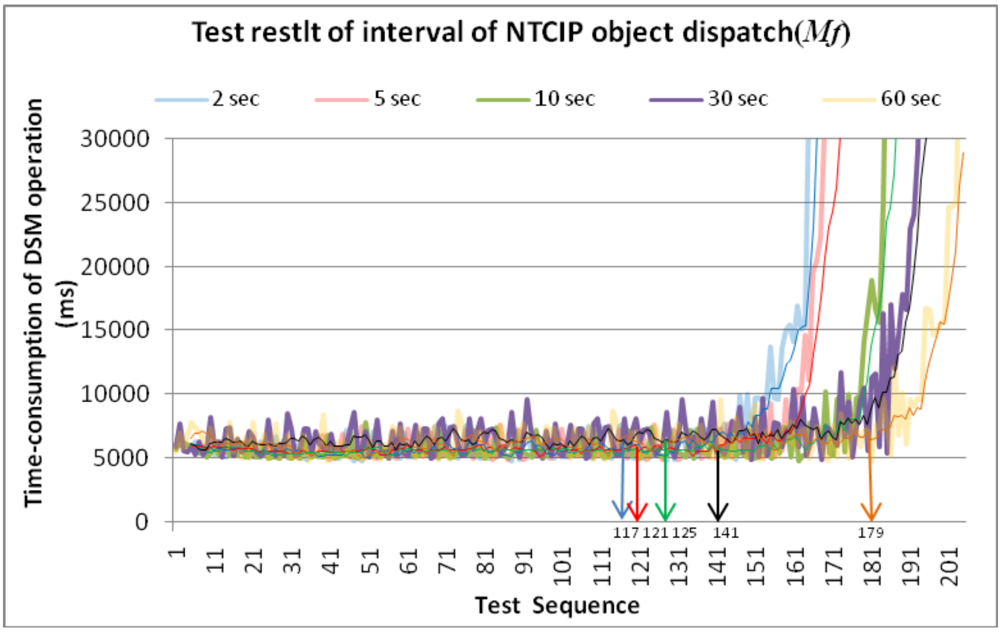


Figure 5.4 DSM operation in different NTCIP object dispatch interval

Table 5.3 Crack points of DSM continuous operations ($\boldsymbol{M_f}$)

$\boldsymbol{M_f}$ **(second)**	2	5	10	30	60
Crack Point	117	121	125	141	179

Furthermore, the interval of NTCIP object dispatch is also the critical factor of the queue phenomena generations and it could be shown as Figure 5.4, and Table 5.4 indicates the crack points of DSM continues operations additionly. Next, Figure 5.5 represents the trend line of crack points for the changes in object dispatch interval and it can be expressed by Equation 5.2 as well.

$$\mathbf{Y_2=1.07X_2+114.86} \tag{5.2}$$

$\mathbf{Y_2}$: Crack point for the continuous operations of $\boldsymbol{M_f}$

$\mathbf{X_2}$: Interval of NTCIP object dispatch (second)

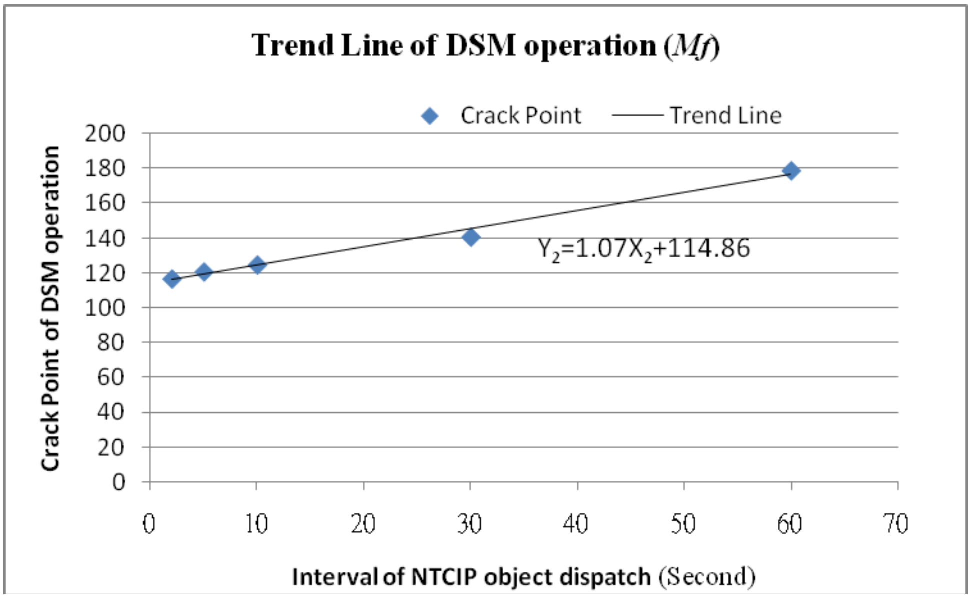


Figure 5.5 Crack point of DSM operations (***M****f*)

On the other hand, lesser NTCIP objects would be dispatched continuously for a hundred times in the real conditions. Taking in these perspectives, the nonlinear zones of these line graphs only describes the relative importance of the delay effects under these factors and explains the normal usage ranges of DSM as well. However, it cannot efficiently represent any phenomenon if the DSM was implemented in the real conditions. Therefore, all of the succeeding analytical data are taken from the forward 100 tests data of each condition of these three experiments

5.3 Data Analysis of Experiment One

The analyses shows that whether the NTCIP object size is the noticeable factor both in deivce operation delay and data transmission delay of DSM operations. Therefore, there are two analyses in this section, namely:

- Analysis 1-1: Analysis in the communications medium, NTCIP object size and DSM addition for the influence of transmission delay and;
- Analysis 1-2: Analysis in the NTCIP object size for the influence of encryption and decryption operations.

In addition, in order to control the size differences in each transmitted object precisely; the time-consumption of data packet transmission here adopts the data the third transmission of the DSM operations (i.e., Socket-3 in Figure 4.11).

5.3.1 Analysis in the communications medium, NTCIP object size and DSM addition for the influence of transmission delay

Table 5.4 and 5.5 represent the statistic descriptions and the analysis results of the time-consumption under the different object size transmission represpectively, and Figure 5.6 is the line graph of the mean time-consumption of object transmission in different sizes with different communications media additionly.

Table 5.4 Statistic Descriptions of Analysis 1-1

Communications Medium	DSM Addition	Mean(ms)	Std. Deviation	N
3.5GMobile	W/O DSM	316.1429	73.48099	700
	With DSM	353.2371	69.13519	700
	Total	334.6900	73.68969	1400
Wired Network	W/O DSM	224.6243	99.77295	700
	With DSM	261.4200	81.27842	700
	Total	243.0221	92.80741	1400
Total	W/O DSM	270.3836	98.82798	1400
	With DSM	307.3286	88.30607	1400
	Total	288.8561	95.50227	2800

Table 5.5 Mean transmission consumping time of Analysis1-1

Object Size (byte)		9	18	30	47	87	182	277
W/O DSM	Wired Network	208.58	227.43	237.26	217.56	159.77	243.18	242.59
	Average				224.62			
	3.5G Mobile	310.55	314.88	310.75	313.37	347.54	306.50	309.41
	Average				316.14			
With DSM	Wired Network	249.99	245.39	258.40	277.13	266.40	273.00	266.63
	Average				261.42			
	3.5G Mobile	350.00	362.09	339.34	367.73	362.00	347.55	363.95
	Average				353.24			

Unit: milliseconds

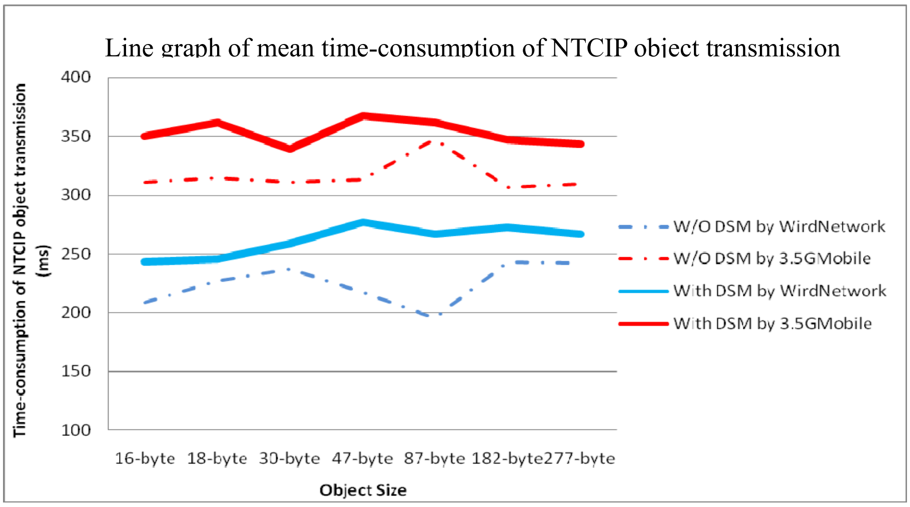


Figure 5.6 Line graph of mean time-consumption of NTCIP object transmission

As Table 5.5 and Figure 5.6 represented, the DSM addition and the 3.5G mobile communications medium usage would increase more negative-effects in data packet transmission a well. Next, we use a multiple regression equation to explain the relationships between the mean time-consumption of data packet transmission and certain factors, namely; the transmitted object size, the communications medium usage and the DSM addition; the analysis result can be shown as Table 5.6 and Equation 5.3.

Table 5.6 Regression equation analysis of Analysis 1-1

Parameter	**β**	**Std. Error**	**t**	**Sig.**
Intercept	258.988	3.145	82.337	.000
[$\boldsymbol{C_m}$=3.5GMobile]	91.668	3.089	29.675	.000
[$\boldsymbol{C_m}$ =Wired Network]	0^b	.	.	.
[DSM Addition=W/O DSM]	-36.753	3.092	-11.888	.000
[DSM Addition=With DSM]	0^b	.	.	.
[$\boldsymbol{M_s}$]	.025	.016	1.515	.130

a. Computed using alpha = .05 b. This parameter is set to zero because it is redundant.

According to the result as Table 5.6 represented, the multiple regression equation of the consuming time in data transmission $\hat{\mu}_{Analysis1-1}$ can be expressed by Equation 5.3 and discussed below:

$$\hat{\mu}_{Analysis_{1-1}} = 258.988 + 91.668(if : C_m = 3.5GMobile) - 36.753(if : W/ODSM) + 0.025 * M_s \qquad (5.3)$$

Thus, in response Equation 5.3:

1) The value 258.998 is the $\hat{\mu}_{Analysis1-1}$ intercept; it indicates the mean of the distribution of the time-consumption in data transmission at least;

2) The coefficient of DSM addition indicates the change in mean of the transmission time, it would increase 36.753 ms while without the DSM addition and all the other independent variables remain constant. In addition, due to the P-value of this factor is 0.000<0.05; therefore, the communications medium usage is the effective factor in data packet transmission as well;

3) The coefficient of $\boldsymbol{C_m}$ indicates the change in mean of the transmission time, it would reduce 91.668 ms while using 3.5G mobile communications and all the other independent variables remain constant. In addition, due to the P-value of $\boldsymbol{C_m}$ is 0.00<0.05; therefore, the DSM addition is also the effective factor in data packet transmission, and;

4) The P-value of $\boldsymbol{M_s}$ is 0.130 and is greater than 0.05; therefore, the transmitted object size is **not** the effective factor in data packet transmission.

5.3.2 Analysis in the NTCIP object size for the influence of encryption and decryption operations

The analysis results of Analysis 1-1 represents that the transmitted object size is not the effective factor in data trnsmission delay. Furthermore, this section shall analyzes whether the object size is a noticeable factor in encryption or decryption prscedure operations.

Table 5.7 The observed mean of the consuming time of encryption/decryption

	Encryption Operation			Decryption Operation		
Object Size	Mean(ms)	Std. Deviation	N	Mean(ms)	Std. Deviation	N
9-byte	172.9950	50.02778	200	598.4450	154.90726	200
18-byte	164.2200	38.98114	200	581.9050	128.50171	200
30-byte	168.5050	44.78200	200	589.6650	133.96641	200
47-byte	172.6900	54.09209	200	582.7350	133.88972	200
87-byte	166.7250	42.13688	200	580.4700	129.77874	200
182-byte	169.9650	45.94276	200	571.7050	114.14043	200
277-byte	167.7850	38.18678	200	590.6700	131.87851	200
Total	168.9836	45.19347	1400	585.0850	132.85951	1400

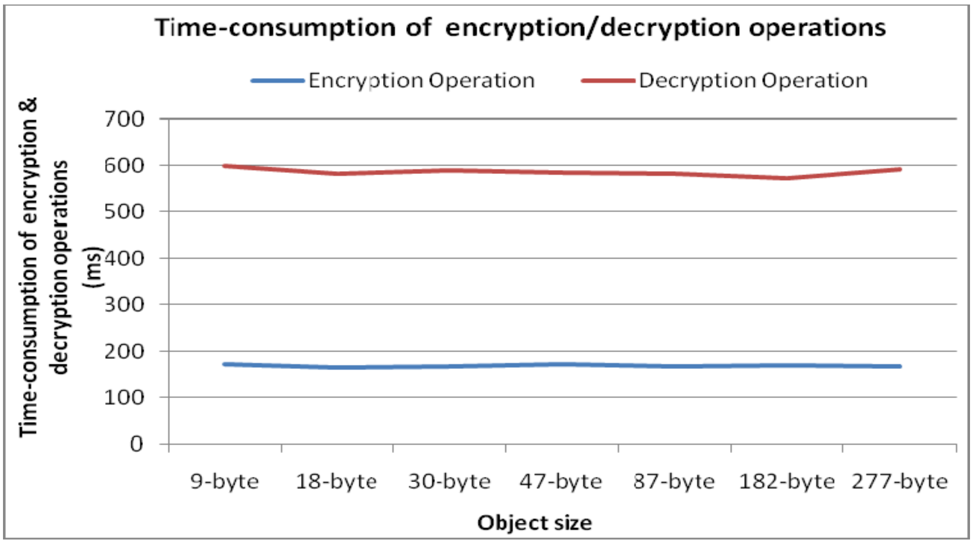


Figure 5.7 Line graph of mean time-consumption of encryption/decryption

Therefore, Analysis 1-2 tests whether the conjectures are tenable or not by the One-Way (Single-Factor) ANOVA approach. Table 5.4 lists the descriptive of statistics and observed mean of the consuming time both of the encryption and decryption procedure operations and the changes in mean value could be illustrated as Figure 5.7 as well.

Next, Table 5.8 and 5.9 are the One-Way ANOVA tables that represent the variance analyses of the factor in transmitted object size for the encryption operation and decryption operation as well; the alternative conclusions for the tests and the test results are the followings,

The alternatives for the encryption operation analysis are:

H_0: The factor in object size would **not** influence the encryption operations

H_1: The factor in object size would influence the encryption operations

Table 5.8 One-Way ANOVA Table –Object size analysis (Encryption)

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	12050.147[a]	6	2008.358	.983	.435
Intercept	3.998E7	1	3.998E7	19571.968	.000
Object Size	12050.147	6	2008.358	.983	.435
Error	2845336.475	1393	2042.596		
Total	4.284E7	1400			
Corrected Total	2857386.622	1399			

a. R Squared = .004 (Adjusted R Squared = .000)

b. Computed using alpha = .05

The alternatives for the decryption operation analysis are:

H_0: The factor in object size would **not** influence the decryption operations

H_1: The factor in object size would influence the decryption operations

Table 5.9 One-Way ANOVA Table of Analysis 1-2 (Decryption)

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	89323.150[a]	6	14887.192	.843	.537
Intercept	4.793E8	1	4.793E8	27132.373	.000
Object Size	89323.150	6	14887.192	.843	.537
Error	2.461E7	1393	17663.558		
Total	5.039E8	1400			
Corrected Total	2.469E7	1399			

a. R Squared = .004 (Adjusted R Squared = -.000)

b. Computed using alpha = .05

As Table 5.8 shown, the P-value of $\boldsymbol{M_s}$ is 0.435 and is greater than 0.05; therefore, the transmitted object size is **not** the effective factor in encryption operation. On the other hand, Table 5.9 indicates that the P-value of $\boldsymbol{M_s}$ is 0.537 and is greater than 0.05 as well; hence, the transmitted object size is also **not** the effective factor in encryption operation.

5.3.3 Brief summary

These analyses show that the transmitted object size is **not** the noticeable factors both in the data packet transmission and in the encryption/decryption operations. In addition, the effective factors in data packet transmission might be the communications medium usage and the DSM addition at least.

On the other hand, these test results confirm the previous expected outcomes that the data transmission would be faster in wired network than in 3.5G mobile communications due to the bandwidth of 3.5G mobile communications is not as wide as wired network.

5.4 Data Analysis of Experiment Two

From the analysis results of Experiment One, we can conclude that the transmitted object size is not the noticeable factor both in the operation delay and in the data packet transmission delay. Next, the following analyses shall discuss whether the length combinations of the AES secret key and RSA public key pair are the effevtive factors in operation delay or in data packet transmission delay as well. Therefore, there are two analyses in this section, namely:

- Analysis 2-1:Analysis in the combinations of AES and RSA for the influence of data packet transmission delay, and;
- Analysis 2-2: Analysis in the combinations of AES and RSA for the influence of device operation delay.

Besides, as the previouse analyses, the following analyses are also analyzed by the ANOVA approachs under the signifiance lever of α=0.05.

5.4.1 Analysis in the combinations of AES and RSA for the influence of data packet transmission delay

The main purpose of this analysis is to confirm that whether the changes in the AES secret key length or in the RSA public key pair length are the noticeable factors in data pack transmission. Therefore, we use the Two-Way ANOVA to test the relationships between mean consuming time of data packet transmission and different length combinations in AES secret key and RSA public key pair. In addition, the consuming time of data packet transmission $\hat{\mu}_{Analysis2-1}$ here is the mean of the three data transmission procedures within the DSM operations and can be explained by Equation 5.4.

$$\hat{\mu}_{Analysis2-1} = [(Socket1) + (Socket2) + (Socket3)] \div 3 \tag{5.4}$$

Furthermore, the analysis results are shown in Table 5.10 and the alternative conclusions are represented below.

The alternatives for the analysis of different AES secret key length operations are:

H$_0$: The AES secret key length is **not** the noticeable factor in data packet transmission delay

H$_1$: The AES secret key length is the noticeable factor in data packet transmission delay

The alternatives for the analysis of different RSA public key pair length operations are:

H_0: The RSA public key pair length is **not** the noticeable factor in data packet transmission delay

H_1: RSA public key pair length is the noticeable factor in data packet transmission delay

The alternatives for the interaction effects between AES and RSA operations are:

H_0: The AES and RSA operations would **not** possess the noticeable interaction effects in data packet transmission delay

H_1: The AES and RSA operations would possess the noticeable interaction effects in data packet transmission delay

Table 5.10 Two-Way ANOVA Table of Analysis 2-1

Source	**Type III Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
Corrected Model	6.770E6	8	846243.782	35.190	.377
Intercept	1.928E8	1	1.928E8	8018.920	.243
AES	775040.974	2	387520.487	16.115	.236
RSA	1384945.254	2	692472.627	28.796	.157
AES*RSA	4609964.029	4	1152491.007	47.926	.067
Error	4.307E7	1791	24047.545		
Total	2.427E8	1800			
Corrected Total	4.984E7	1799			

a. R Squared = .136 (Adjusted R Squared =-.132)

b. Computed using alpha = .05

Thus, both of the P-values of AES and RSA in Table 5.10 are all higher than 0.05;

hence, we conclude that both of the length changes in AES secret key and RSA public key pair are **not** the noticeable factors in data transmission delay. In addition, as the P-value of AES*RSA represented; there is no interaction effect between the AES and RSA operations in data transmission as well.

5.4.2 Analysis in the combinations of AES and RSA for the influence of operation delay

Analysis 2-1 test out the AES and RSA operations would not influence in data packet transmission delay. Next, we shall discuss whether the length changes in the AES secret key and RSA public key pair are also not the effective factors in operation delay. This analysis still use the Two-Way ANOVA to examine on the relationships between the mean consuming time of device operations and different length combinations in AES secret key and RSA public key pair and the statistic descriptions and observed mean of device operations are listed in Table 5.11. Besides, in order to test the influences upon the device operations and changes in key combinations certainly; hence, the mean consuming time of device operations $\hat{\mu}_{Analysis2-2}$ here are calculated from all the device operation procedures without the data packet transmission procedures within the DSM operations and can be explained as Equation 5.5.

$$\hat{\mu}_{Analysis2-2} = \text{(Time of DSM operation)} - [\text{(Socket1)} + \text{(Socket2)} + \text{(Socket3)}] \qquad (5.5)$$

Table 5.11 Observed mean of the consuming time of device operations

AES secret key	RSA public key pair	Mean(ms)	Std. Deviation	N	C_m
128-bit	768-bit	1600.7750	193.21728	200	3.5G mobile communications + Wired Network Communications
	1024-bit	1772.4300	242.07940	200	
	2048-bit	3687.1300	1394.37773	200	
	Total	2353.4450	1254.41853	600	
192-bit	768-bit	1613.3350	207.10960	200	
	1024-bit	1809.5100	276.84380	200	
	2048-bit	3790.2800	1547.86950	200	
	Total	2404.3750	1343.15814	600	
256-bit	768-bit	1630.6400	206.19689	200	
	1024-bit	1806.9300	238.63958	200	
	2048-bit	3897.5200	1429.51597	200	
	Total	2445.0300	1331.82402	600	
Total	768-bit	1614.9167	202.30760	600	
	1024-bit	1796.2900	253.25269	600	
	2048-bit	3791.6433	1458.83085	600	
	Total	2400.9500	1310.20122	1800	

In addition, as Table 5.11 shown, the communications medium usages of the observed data are not only upon the 3.5G mobile communications but also the wired network as well. There is no proof that the communications medium usages would not influence the operations of AES and RSA. Therefore, we should test this consideration first via the One-Way ANOVE method. The analysis results and alternatives are shown in Table 5.12 as below.

The alternatives for C_m and AES/RSA operations are:

H_0: The communications medium usage $\boldsymbol{C_m}$ is **not** the noticeable factor in device operations

H_1: The communications medium usage $\boldsymbol{C_m}$ is the noticeable factor in device operations

Table 5.12 One-Way ANOVA Table of $\boldsymbol{C_m}$ and AES/RSA operations

Source	**Type III Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
Corrected Model	1.340E6	1	1339993.636	.781	.377
Intercept	1.038E10	1	1.038E10	6043.795	.000
Communication Media	1339993.636	1	1339993.636	.781	.377
Error	3.087E9	1798	1716836.723		
Total	1.346E10	1800			
Corrected Total	3.088E9	1799			

a. R Squared = .000 (Adjusted R Squared =.000)

b. Computed using alpha = .05

The test results in Table 5.12 indicate that the communications medium usage $\boldsymbol{C_m}$ is not the effective factor in device operations of AES and RSA due to the P-value of $\boldsymbol{C_m}$ here is $0.377>0.05$.

Next, we continue to the analysis above; the analysis results of Analysis 2-2 are shown in Table 5.13 and the related alternative conclusions are represented below.

The alternatives for the analysis of different AES secret key length operations are:

H_0: The AES secret key length is **not** the noticeable factor in device operation delay

H_1: The AES secret key length is the noticeable factor in device operation delay

The alternatives for the analysis of different RSA public key pair length operations are:

H_0: The RSA public key pair length is **not** the noticeable factor in device operation delay

H_1: RSA public key pair length is the noticeable factor in device operation delay

The alternatives for the interaction effects between AES and RSA operations are:

H_0: The AES and RSA operations would **not** possess the noticeable interaction effects in device operation delay

H_1: The AES and RSA operations would possess the noticeable interaction effects in device operation delay

Table 5.13 Two-Way ANOVA Table of Analysis 2-2

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	1.755E9	8	2.194E8	294.773	.000
Intercept	1.038E10	1	1.038E10	13941.015	.000
AES	2526901.230	2	1263450.615	1.698	.183
RSA	1.750E9	2	8.752E8	1175.943	.000
AES*RSA	2161449.427	4	540362.357	.726	.574
Error	1.333E9	1791	744293.709		
Total	1.346E10	1800			
Corrected Total	3.088E9	1799			

a. R Squared = .568 (Adjusted R Squared =.566)

b. Computed using alpha = .05

Thus, the results indicate that the AES operations are not the noticeable factors in operation delay due to the P-value here is $0.138>0.050$. In addition, there is no interaction effect between AES and RSA operations in device operations due to the P-value of AES*RSA is $0.574>0.050$.

However, the P-value of RSA operation is $0.000<0.050$; therefore, we can say that the RSA operations and the different RSA public key pair length would influence the efficiencies of device operations. Table 5.14 shows the comparisons with the different length of RSA public key pair by LSD method further. We can understand that the operation efficiency of 2048-bit public key pair would be lower than 768-bit and 1024-bit greatly; and Figure 5.8 and 5.9 illustrate the results and indicate that the operation efficiencies of different key length of AES/RSA operations. Finally, we get the following two perspectives from this analysis, namely: the changes in AES secret key length would not influence the operation efficiency in evidence; therefore, we can choose the longer length in AES secret key for DSM; and the RSA public key pair length is one of the major reasons to control the device operation efficiencies; hence, we need to pay attrition on this point more.

Table 5.14 The comparisons with the different length of RSA public key pair

	(I) RSA	(J) RSA	Mean Difference(I－J)	Std.Error	Sig.
LSD	RSA0768	RSA1024	-126.9133	74.83700	.207
		RSA2048	-2302.2900*	74.83700	.000
	RSA1024	RSA0768	126.9133	74.83700	.207
		RSA2048	-2175.3767*	74.83700	.000
	RSA2048	RSA0768	2302.2900*	74.83700	.000
		RSA1024	2175.3767*	74.83700	.000

*:The valuable mean difference for usage

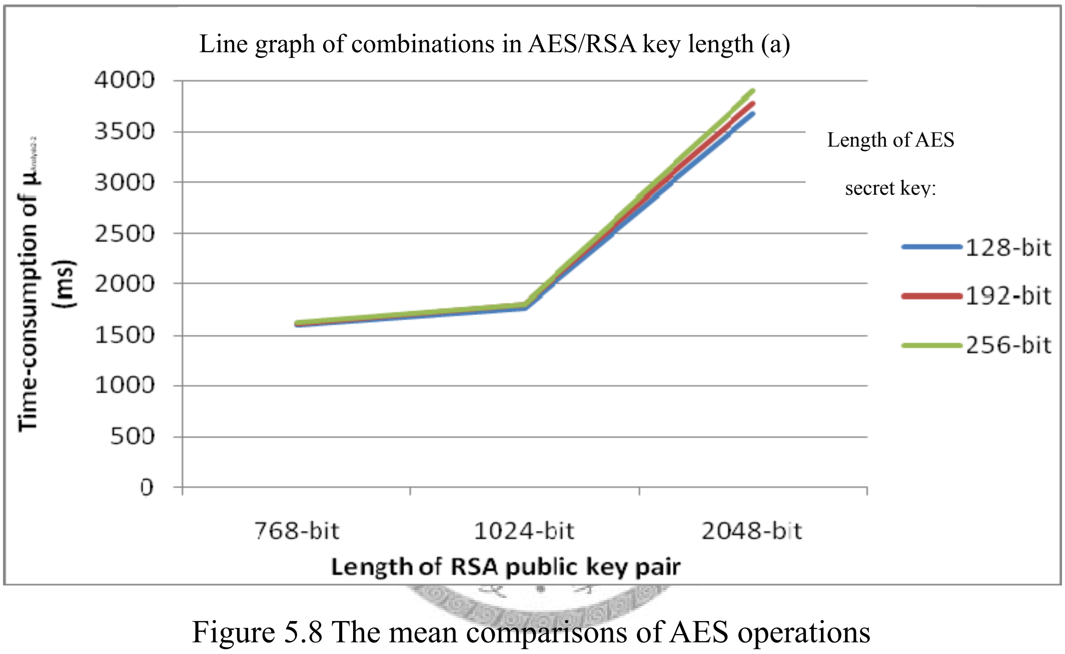


Figure 5.8 The mean comparisons of AES operations

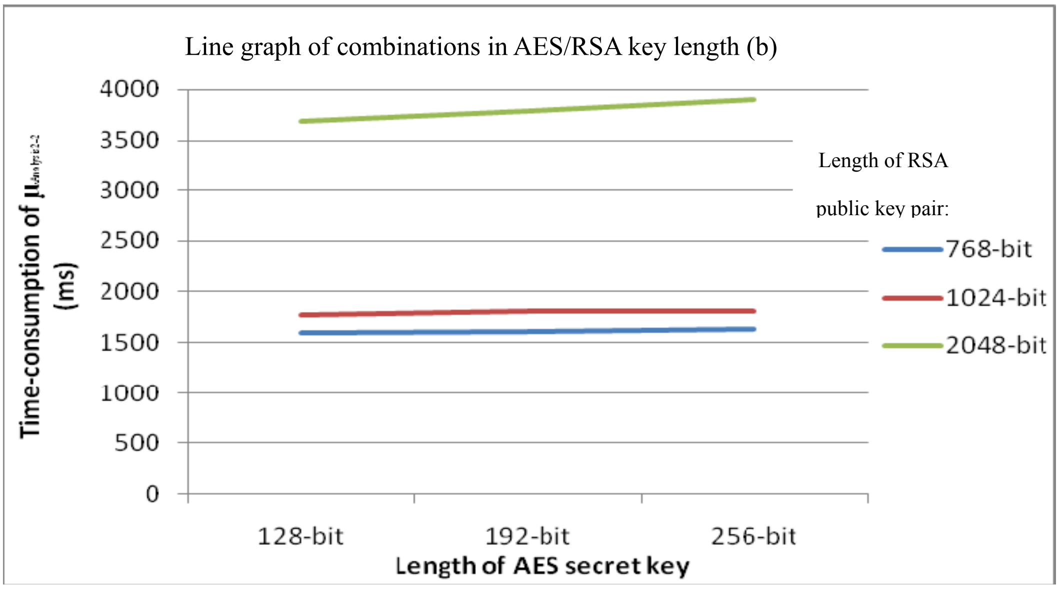


Figure 5.9 The mean comparisons of RSA operations

5.5 Data Analysis of Experiment Three

As mentioned earlier, the tight interval of object dispatch and the lower compitation-capability of devices might cause more negative-effects for the core system and network transmission as well. The ojectives of these analyses of this section are to confirm and discuss these considerations. The analyses could be indived into the following two parts:

- Analysis 3-1: Analysis in the interval of the object dispatch and the computation-capability of TCIS devices for the influence of device operation delay, and;
- Analysis 3-2: Analysis in the interval of the object dispatch and the computation-capability of TCIS devices for the influence of data packet transmission.

In addition, in order to control the anaysis objects certainly; the time-consumption of data packet transmissions and device operations in this section are respectively adopted as the same as Equation 5.4 and 5.5 in Section 5.4.

5.5.1 Analysis in the interval of the object dispatch and the computation-capability for influence of device operation delay

According to the test results in Analysis 2-2, it indicated that the different communications medium usages would not infulence the device operation noticeably. Therefore, we have to continue to understand the relationships between these two factors in the operation efficiencies of TCIS devices without the distinctios between the communications medium usages futher. Table 5.15 shows the observed mean of TCIS device operatios in different $\boldsymbol{C_c}$ and $\boldsymbol{M_i}$ of Anaiysis 3-1.

Table 5.15 Observed mean of TCIS device operations (Analysis 3-1)

C_c	M_i	**Mean(ms)**	**Std. Deviation**	**N**	C_m
TCIS-i	2-second	945.3450	166.44662	200	3.5G mobile communications + Wired Network Communications
	5-second	920.7750	139.17851	200	
	10-second	912.5800	137.13051	200	
	30-second	925.3350	154.82719	200	
	60-second	924.0200	142.32290	200	
	Total	925.6110	148.49386	1000	
TCIS-ii	2-second	1786.6150	243.19388	200	
	5-second	1860.4950	245.72702	200	
	10-second	1766.2200	245.53423	200	
	30-second	1869.7050	605.03442	200	
	60-second	1861.2900	262.38932	200	
	Total	1828.8650	352.61996	1000	
TCIS-iii	2-second	2457.4900	473.64275	200	
	5-second	2433.1000	433.78753	200	

	10-second	2446.6000	408.93746	200
	30-second	2464.1950	354.22174	200
	60-second	2507.0350	428.18940	200
	Total	2461.6840	421.45668	1000
TCIS-iv	2-second	4466.6150	791.07827	200
	5-second	4447.3550	770.67694	200
	10-second	4448.0600	735.94570	200
	30-second	4479.1100	785.31021	200
	60-second	4436.6550	662.16477	200
	Total	4455.5590	749.18885	1000
Total		2417.9297	1379.69010	4000

As Table 5.15 represcented, the relationships between ***C****c* and ***M****i* can be illustrated as Figure 5.10 and 5.11. We can cleanly know that the operation delay might be infulenced by ***C****c* more, and the lower ***C****c* might operate slower.

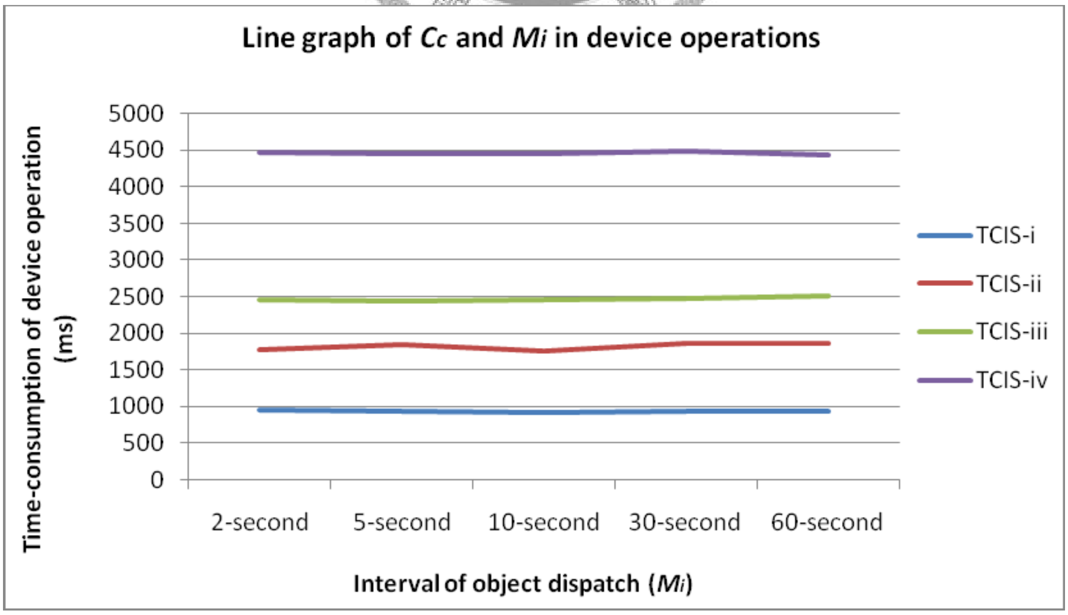


Figure 5.10 The represection of the factor in ***C****c* (Analysis 3-1)

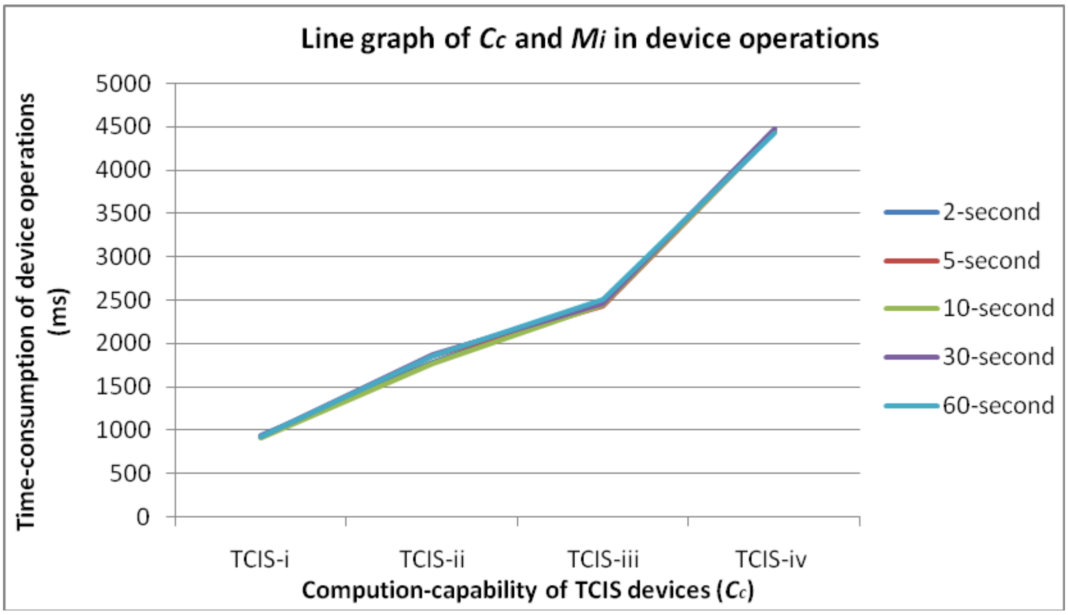


Figure 5.11 The represection of the factor in $\boldsymbol{M_i}$ (Analysis 3-1)

Next, Table 5.16 is the analysis results which are analyzed by Two-Way ANOVA method and the alternative conclusions for the test are below:

The alternatives for the analysis of the different computation-capability of TCIS device operations ($\boldsymbol{C_c}$) are:

H$_0$: The factor in the computation-capability of TCIS devices would **not** influence the device operation delay

H$_1$: The factor in the computation-capability of TCIS devices would influence the device operation delay

The alternatives for the analysis of the interval of object dispatch ($\boldsymbol{M_i}$) are:

H$_0$: The interval of object dispatch is **not** the noticeable factor in device operation delay

H$_1$: The interval of object dispatch is the noticeable factor in device operation delay

The alternatives for the interaction effects between $\boldsymbol{C_c}$ and $\boldsymbol{M_i}$ are:

H_0: The $\boldsymbol{C_c}$ and $\boldsymbol{M_i}$ would **not** possess the noticeable interaction effects in device operation delay

H_1: The $\boldsymbol{C_c}$ and $\boldsymbol{M_i}$ would possess the noticeable interaction effects in device operation delay

Table 5.16 Two-Way ANOVA Table of Analysis 3-1

Source	**Type III Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
Corrected Model	6.731E9	19	3.542E8	1599.341	.000
Intercept	2.339E10	1	2.339E10	105579.705	.000
$\boldsymbol{C_c}$	6.728E9	3	2.243E9	10124.854	.000
$\boldsymbol{M_i}$	885994.784	4	221498.696	1.000	.406
$\boldsymbol{C_c}$ *$\boldsymbol{M_i}$	1973485.288	12	164457.107	.742	.711
Error	8.816E8	3980	221496.518		
Total	3.100E10	4000			
Corrected Total	7.612E9	3999			

a. R Squared = .884 (Adjusted R Squared =.884) b. Computed using alpha = .05

The results represent that the interval of object dispatch ($\boldsymbol{M_i}$) is **not** the effective factor in device operations due to the P-value of $\boldsymbol{M_i}$ is 0.406>0.050. On the other hand, because of the P-value of $\boldsymbol{C_c}$ is 0.000<0.050. Therefore, the factor in the computation-capability of TCIS devices might be noticeable factor in the operation delay further, and this result also confirm to Figure 5.10 additionly. Besides, the $\boldsymbol{M_i}$ and $\boldsymbol{C_c}$ would not have interaction effects between them.

5.5.2 Analysis in the interval of the object dispatch and the computation-capability for influences of data transmission delay

Although the interval of object dispatch $\boldsymbol{M_i}$ is not the noticeable factor in device operations, but it does not mean that these would also not influence the delay in data packet transmission. Hence, Analysis 3-2 is to test the conditions for both of $\boldsymbol{M_i}$ and $\boldsymbol{C_c}$ in transmission delay.

As mentioned in the results of Experiment One, the noticeable factors in the data packet transmission delay might be the communications medium usages and DSM addition at least. Therefore, the analyses below are discussed on the factors in differences in the communications media($\boldsymbol{C_m}$), the interval of object dispatch ($\boldsymbol{M_i}$) and the compitaion-capability of TCIS devices ($\boldsymbol{C_c}$) via the muliple regression equation as Table 5.18 and Equation 5.6 shown.

First, the statistic describuations of Analysis 3-2 are listed in Table 5.17 and Figure 5.12 illustrates that the relationships between $\boldsymbol{M_i}$ and $\boldsymbol{C_c}$, we could know that the $\boldsymbol{C_c}$ and $\boldsymbol{M_i}$ might be the factors in data packet transmission by this figure.

Table 5.17 Observed mean of data packet transmission (Analysis 3-2)

C_m	C_c	**Mean(ms)**	**Std. Deviation**	**N**
3.5G mobile communications	TCIS-i	332.3420	90.55983	500
	TCIS-ii	340.4680	102.15671	500
	TCIS-iii	367.1920	142.83247	500
	TCIS-iv	392.0860	69.62912	500
	Total	358.0220	107.27733	2000
Wired network communications	TCIS-i	248.3107	99.61598	500
	TCIS-ii	250.9160	89.64893	500
	TCIS-iii	280.6913	105.39957	500
	TCIS-iv	293.6893	120.25834	500
	Total	268.4018	106.02680	2000
Total	TCIS-i	290.3263	104.02031	1000
	TCIS-ii	295.6920	105.99110	1000
	TCIS-iii	323.9417	132.70940	1000
	TCIS-iv	342.8877	109.85616	1000
	Total	313.2119	115.67478	4000

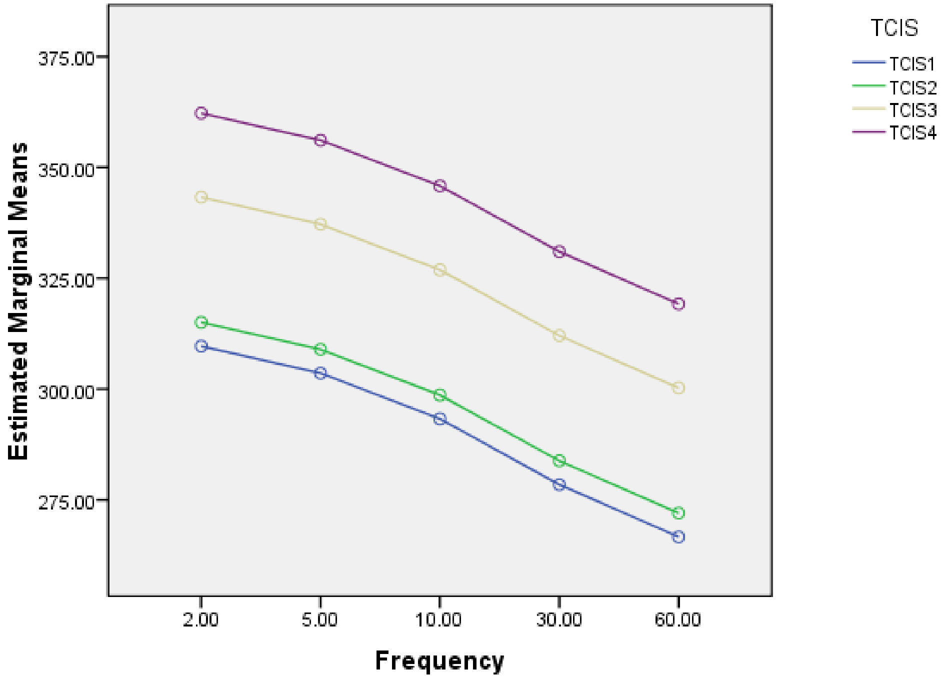


Figure 5.12 The represection of the factor in ***Cc*** (Analysis 3-2)

Table 5.18 Regression equation analysis of Analysis 3-2

Parameter	β	Std. Error	t	Sig.
Intercept	313.107	3.999	78.300	.000
[***C***$_m$=3.5GMobile]	89.620	3.271	27.400	.000
[$\boldsymbol{C_m}$ =Wired Network]	0^b	.	.	.
[TCIS=TCIS-i]	-52.561	4.626	-11.363	.000
[TCIS=TCIS-ii]	-47.196	4.626	-10.203	.000
[TCIS=TCIS-iii]	-18.946	4.626	-4.096	.000
[TCIS=TCIS-iv]	0^b	.	.	.
[$\boldsymbol{M_f}$]	-.702	.076	-9.288	.000

a. Computed using alpha = .05

b. This parameter is set to zero because it is redundant.

Therefore, the multiple regression equation can be expressed by Equation 5.6 and discussed below:

$$\hat{\mu}_{Analysis_{3-2}} = 313.107 + 89.620 * (if : C_m = 3.5GMobile) - 47.196 * (if : TCIS2) - 0.702 * M_f \quad (5.6)$$

Thus, the P-values of each factor is equal 0.000<0.050, therefore all the factors in this table are the noticeable factors for the data packet transmission as well (i.e., $\boldsymbol{C_m}$, $\boldsymbol{C_c}$ and $\boldsymbol{M_f}$) and the responses are described as following.

i. The value 313.107 is the intercept of $\hat{\mu}_{Analysis3-2}$; it indicates the mean of the distribution of the time-consumption in data transmission at least;

ii. The coefficient of $\boldsymbol{C_m}$ indicates the change in mean of different communications medium usages, it would increase 89.620 ms while the 3.5G mobile communication usage and all the other independent variables remain constant;

iii. The compilation-capability would also be the noticeable factor in data packet transmission as well, and;

iv. The tight interval of object dispatch might cause more loads for network transmission; therefore, it would reduce 0.702 ms when $\boldsymbol{M_f}$ increases by one second while all the other independent variables remain constant.

5.5.3 Brief summary

So far, we have understood that the factor in computation-capability $\boldsymbol{C_c}$ would not only influence the device operations but also affect the data packet transmission as well. In addition, acccording to Equation 4.2, the time-consumption of data transmission (socket processes) in this research is caculated from the procedures in data packet sealing by transmitter, data packet transmission by Enternet and data packet unsealing by servicers; therefore, the lower computation-capability would cause the more native-effects in sealing and unsealing procedures for the device operations.This explainations not only interprets that the Factor $\boldsymbol{C_c}$ is one of the noticeable factors in data packet transmission but also confirm that why the DSM addition would infulence the data transmission in Equation 5.3 due to the DSM addition adds more loads for core systmes and it infulence the sealing/unsealing operations further.

On other hand, the time-consumption of data packet transmission is explained by Equation 5.3 and 5.6. Equation 5.3 indicates that the DSM addition and **C_m** are the noticeable factors in data packet transmission under the fixed **M_f** and **C_c** factors. If we respectively set up the **M_f** and **C_c** in 10-second and TCIS-ii for Equation 5.7, we can get the formala as Equation 5.6.

$$\hat{\mu}'_{Analysis_{3-2}} = 258.891 + 89.620(if : C_m = 3.5GMobile) \tag{5.7}$$

Equation 5.6 accords with the results in Equation 5.3 without the ineffective factor **M_s** further. Hence, we can support that the efficiency difference of data packet transmission between the wired network and the 3.5G mobile communications is around 90 ms, and the mean of data packet transmission in wired network is around 258 ms additionlly.

Finally, Table 5.19 shows the analysis results for all the considered factors (i.e., **C_m**, **KS_l**, **KP_l**, **M_s**, **M_f** and **C_c**) from the above analyses.

Table 5.19 Analysis results of **C_m**, **KS_l**, **KP_l**, **M_s**, **M_f** and **C_c**

Item Factor	**C_m**	**KS_l**	**KP_l**	**M_s**	**M_f**	**C_c**
Device Operation Delay	-	-	◎	-	-	◎
Data Transmission Delay	◎	-	-	-	◎	◎
Interaction effect with C_c	-	◎	◎	-	◎	-

◎:The noticeable and effective factor

As Figure 5.12 shown, the factor in computation-capability $\boldsymbol{C_c}$ is the most important and major factor for the whole DSM operations, it would influence all the operation procedures of DSM. In addition, Figure 5.1 also illustrates that the lower computation-capability device would reach the limits of device operations (or crash) earlier. In addition, due to there are three procedures in data packet transmission in the DSM operations; hence, the network transmission efficiency is another main factor for DSM operations as well. Therefore, as discussed before, we should not only consider or focus on the security level for the security mechanisms but also need to pay more attentions in the efficiencies of both the device operations and network transmissions.

5.6 Regression Equation of DSM Operations

As discussed above, this showed that there would be no interaction effect between the device operations and data packet transmissions of the DSM operations, but the device computation-capability would be the noticeable factor on both of them. Due to these, we can deem that the device operations and data packet transmissions are the independent factors under the certain computation-capability of TCIS and TMIC devices. Therefore, the regression equation below are considered and discussed for the operation efficiencies of DSM operations under the TMIC in computer no.1 and TCIS in computer no. 2. We utilize the test results of these three experiments in this research to figure out the regression equation which includes the factors in $\boldsymbol{C_m}$, $\boldsymbol{KS_l}$, $\boldsymbol{KP_l}$, $\boldsymbol{M_s}$, $\boldsymbol{M_f}$ and $\boldsymbol{C_c}$ further. The statistics descriptions are shown in Table 5.20 and, the analysis results are represented as Table 5.21 and Equation 5.8 additionly.

Table 5.20 Statistics descriptions of the regression equation in this research

	Value Label(key length)	**N**
AES	128-bit	3000
	192-bit	600
	256-bit	600
RSA	768-bit	600
	1024-bit	3000
	2048-bit	600
Communications Media	Wired Network	2100
	3.5G Communications	2100
Total		4200

Table 5.21 Regression equation analysis of DSM operation

Parameter	**β**	**Std. Error**	**t**	**Sig.**
Intercept	5142.129	46.833	109.798	.000
[$\boldsymbol{KS_l}$=128-bit]	-67.108	37.775	-1.777	.076
[$\boldsymbol{KS_l}$=192-bit]	-55.808	43.838	-1.273	.203
[$\boldsymbol{KS_l}$=256-bit]	0^b	.	.	.
[$\boldsymbol{KP_l}$=768-bit]	-2672.103	43.838	-60.955	.000
[$\boldsymbol{KP_l}$=1024-bit]	-2248.678	37.775	-59.528	.000
[$\boldsymbol{KP_l}$=2048-bit]	0^b	.	.	.
[$\boldsymbol{C_m}$=3.5GMobile]	93.501	23.432	3.990	.000
[$\boldsymbol{C_m}$ =Wired Network]	0^b	.	.	.
[$\boldsymbol{M_s}$]	.243	.214	1.136	.256
[$\boldsymbol{M_f}$]	-5.653	1.023	-5.524	.000

a. Computed using α=.05 b. This parameter is set to zero because it is redundant.

Therefore, the regression equation of DSM operations can be explained as Equation 5.8 below.

$$\begin{aligned}\hat{\mu}_{DSMoperation} &= 5142.129 - 67.108(if: KS_l = 128bits) - 2248.678(if: KP_l = 1024bits) \\ &+ 93.501(if: C_m = 3.5GMobile) + 0.243M_s - 5.653M_f\end{aligned} \tag{5.8}$$

Because of the P-value of ***M_s*** is 0.256 and less than 0.050 a lot; therefore, this factor cannot be considered in DSM operations. Hence, Equation 5.5 can be represented as Equation 5.9 further.

$$\begin{aligned}\hat{\mu}'_{DSMoperation} &= 5142.129 - 67.108(if: KS_l = 128bits) - 2248.678(if: KP_l = 1024bits) \\ &+ 93.501(if: C_m = 3.5GMobile) - 5.653M_f\end{aligned} \tag{5.9}$$

Thus, in response Equation 5.9:

i. The value 5142.129 is the intercept of DSM operations, it indicates that the mean of the distribution of the time-consumption in DSM operations while the $\boldsymbol{KS_l}$=256-bit, $\boldsymbol{KP_l}$=2048-bit, $\boldsymbol{M_f}$=2-second and using the 3.5G communications as well;

ii. Although the P-value of $\boldsymbol{KS_l}$ is less than 0.050, but this would influence the decryption procedure in TCIS device operations; therefore, we deem that we should consider the factor in DSM operation;

iii. The coefficient of $\boldsymbol{KU_l}$ indicates that the changes in mean of the RSA operations of DSM operations. For instance, while we use the 1024-bit public key pair, the DSM operation would reduce 2248.678 ms. In addition, due to the P-value of $\boldsymbol{KU_l}$ is 0.000<0.050; therefore, $\boldsymbol{KU_l}$ is the noticeable factor for DSM operations, and;

iv. From the coefficient of $\boldsymbol{M_f}$, we cleanly understand that the tight interval of object dispatch would cause more native-effects for the core system, it would deduce 5.653 ms while $\boldsymbol{M_f}$ increases one second and all the other independent variables remain constant.

Finally, Table 5.22 lists the maximum ($\boldsymbol{M_f}$=2 sec) and minimum ($\boldsymbol{M_f}$=60 sec) threshold values of DSM operation efficiency for each secret information combinations from Equation 5.9.

Table 5.22 The threshold values of DSM operation efficiency

		RSA Public Key Pair		
		768-bit	1024-bit	2048-bit
AES Secret Key	128-bit	[2063.738,2391.522]	[2487.163,2814.947]	[4735.84,5063.625]
	192-bit	[2075.038,2402.822]	[2498.463,2826.247]	[4747.141,5076.925]
	256-bit	[2130.846,2458.63]	[2554.271,2882.055]	[4898.45,5226.234]
AES Secret Key	128-bit	[2157.639,2485.023]	[2580.664,2908.448]	[4829.342,5157.126]
	192-bit	[2196.539,2496.323]	[2591.964,2919.748]	[4840.642,5170.426]
	256-bit	[2224.347,2552.131]	[2647.772,2975.556]	[4991.951,5319.735]

CHAPTER SIX

CONCLUSIONS AND FUTURE RESEARCH

6.1 Conclusions

The purpose of this research is to establish a suitable and dynamical security mechanism for ATMS data transmission using the modern cryptography technologies. However, the security mechanism addition would also cause the native-effects for the core system due to the complex operations of security mechanism. Therefore, the operation efficiencies are the important considerations further. Because of these, we design three experiments to test the DSM operations under the different conditions that we can well imagine. The conclusions are described below.

- The DSM is basic upon the hybrid cryptosystem which is composed of symmetry cryptosystems and asymmetry cryptosystems. In which, there are now useful techniques in cracking the RSA algorithms and they also cannot be cracked via brute-force attack nowadays. In addition, as Table 3.6 shown, attackers might spend over 10 hours to crack the 56-bit secret key of AES algorithms by the high computation-capability computers. On the other hand, the data transmission in ATMS or traffic control is real-time. Therefore, the 128-bit secret key is enough for ATMS data transmission sufficiently;

- The DSM utilizes the message digest algorithms in between the transmission processes to ensure the data integrity, and these message digests are composed of not only the ciphertexts but also the re-stored passwords as well; therefore, one could not masquerade the transmitters or receivers easily. Besides, from the test results of these experiments represent that the message digest operations cause lesser native-effects for the core systems further;

- The security information (AES secret key and RSA public key pair) of DSM is made from the security random number generator and it utilizes the message digest which is calculated from each original data to be the seed-number. It modifies the seed-number issues of random number generations of computers;

- As represented above, DSKG and DPKG use the message digest to be the seed-number and do not directly use the original message due to the message digest algorithm is the one-way function; therefore, one cannot figure out the original data from the message digest even if they crack the secret-public key pair generators and the secure random number generators to provide more protections further ;

- From the test results, we know that the time-consumption of DSM operations are dependent on the factors in the device operations and data transmission procedures; especially in the device operations. Therefore, both of the network bandwidth and device operation efficiencies should be considered for DSM operations upon the security is enough sufficiently;

- Although the test results indicated the AES operations are not the noticeable factor for the DSM operations; however, as Figure 4.1 shown, the NTCIP decryption procedures occupy almost the one fifth of the DSM operations and it is operated by TCIS devices. Therefore, we should consider the AES operations for the lower computation-capability TCIS devices;

- Experiment One represented that the object size is not the noticeable factor in encryption, decryption and data transmission procedures; due to the maximum object size of ATMS commonly are 277 bytes nowadays. Therefore. we cannot be sure whether the digger object size would also give the same results;

- The results of Experiment Two showed that the time-consumption of 2048-bit RSA public key pair operations would be the highest than 768-bit and 1024-bit ; therefore, by this perspective, we should consider the device operation efficiencies more while we need to use the larger RSA public key pair;

- As Experiment Two represented, the operation differences in different AES secret key length are not evidently; hence, we suggest that one can choose the larger secret key to improve the security level for transmitted object;

- We confirm that the computation-capability of device operation is the main factor in the DSM operations by the results of Experiment Three;

- Experiment Three showed the device computation-capability here is the one of the noticeable factors in the data packet transmission due to the lower computation-capability devices need more time to deal with the data sealing/unsealing procedures. Besides, it does not mean that the device computation-capability would influence the efficiencies of network transmissions further;

- Section 5.2 showed the common usage frequency of DSM; therefore, one can refer to the analysis results to understand the operation limitation of DSM for the continuity operations, and;

- Figure 6.1 represents the time-consumption of DSM operations under the different factor combinations; one could choose the suitable combination for his needs and design the security mechanism further.

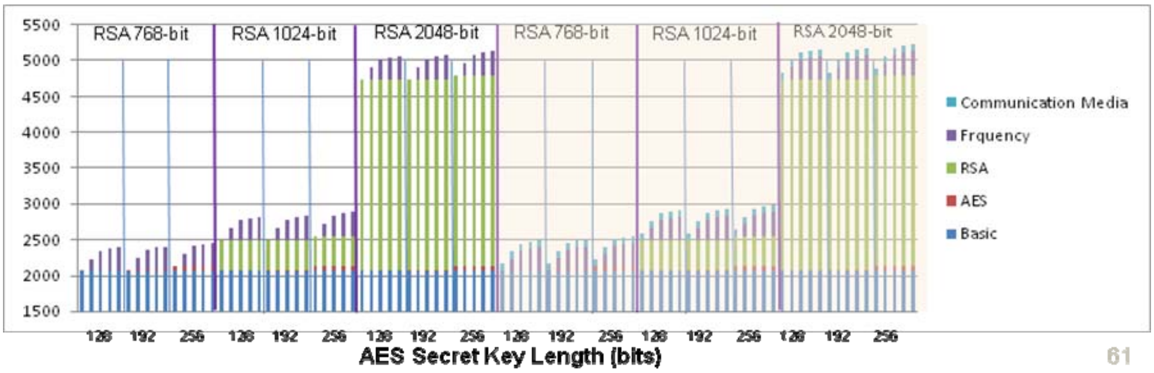


Figure 6.1 The time-consumption trend of DSM operations

6.2 Future Research and Suggestions

Due to the limited resources; therefore, there is still room for discussion about more considerations and the conditions in the real-practice further. Hence, the future researches and suggestions are described below:

- The transmission efficiencies of the ISP operations are not the objective for this research; therefore, we only consider the normal usage conditions and do not discuss with the delay of the internal operations of ISP; furthermore, we only consider the one ISP for the network and 3.5G mobile communications, and different ISP might cause different results in data transmission efficiencies and influence the DSM operations further;
- All of the experiments of this research use computers to simulate TMIC and TCIS; the purposes are to make the test efficient. However, it might have some differences in the real conditions;
- The secret information managements in this research utilize the I/O methods of Java programming language, and store the secret information in the hard discs of the TMIC and TCIS devices. It possesses certain risks while the core systems are invaded by attackers. The better way is to manage the secret information via the third parts, but it would need addition payments;

- This research focuses on the ATMS data transmissions, and does not stress on the security for the hosts. One could invade the hosts by cracking the fire-walls; therefore, the access control might the valuable research further;

- The final regression equation is set up on the certain computation-capability devices and communications media; although, this regression equation provides important and valuable information for the traffic control systems.

REFERENCE

1. NTCIP Joint Standards Committee, “National Transportation Communications for ITS Protocol (NTCIP) Guide” , Draft Version 03.02b, October 2002

2. Joint Standard of AASHTO, ITE and NEMA, “National Transportation Communications for ITS Protocol and Simple Transportation Management Framework”, Draft Version 01.12, December 2001.

3. Telecommunication Standardization Sector of ITU, “Data Networks and Open System Communications”, X.814, November 1995.

4. Land Transportation Authority, Singapore, http://www.lta.gov.sg.

5. Daemen, J., and Rijmen, V., “Rijndael: The Advanced Encryption Standard”, Dr.Dobb’s Journal, March 2001.

6. The Legion of the Bouncy Castle, http://www.bouncycastle.org/

7. ITS, America, http://www.itsa.org/

8. Lidl, R., and Niederreiter, H., “Introduction to Finite Fields and Their Applications”, Cambridge: Cambridge University Press, 1994.

9. Benjamin Arazi, Senior Member, IEEE “Vehicular Implementations of Public Key Cryptographic Techniques”, IEEE Transportations on Vehicular Technology, Vol.40, No.3, August 1991.

10. Tzong-Chen We and Chien-Lung Hsu, “Cryptanalysis of Digital Multisignature Schemes for Authenticating Delegates in Mobile Code Systems”, IEEE Transportations on Vehicular Technology, Vol.52,No.2, March 2003.

11. Xun Yi Kheong Siew and Chik How Tan, “A Secure and Efficient Conference Scheme for Mobile Communications”, IEEE Transportations on Vehicular Technology, Vol.52,No.4, July 2003.

12. Archana Khetan, “M-Commerce: A JAVA Approach”, Master Thesis, Nanyang Technological University, 2002.

13. Ng Churn Wai, “On the Security of DES, Blowfish and Rijnedael”, Master Thesis, Nanyang Technological University, 2003.

14. Choy Sok Sien, “Security in Mobile AD HOC Netowrk”, Master Thesis, Nanyang Technological University, March 2003.

15. Lee Chit Boon, “Security Monitor using Java Mobile Agent”, MSc Project, Nanyang Technological University, December 2000.

16. Mar Kai Liat, “Study of Wireless LAN Security Issues”, Master Thesis, Nanyang Technological University, 2004.

17. Zhou Gang, “Wireless Network Security Analysis”, Master Thesis, Nanyang Technological University, 2002.

18. Nol Premasathian, “Design and Analysis of Dynamic Key-driven crypto Engines”, Ph.D. Thesis, University of Louisiana, Spring 2002.

19. Whitfield Diffie and Martin E. Hellman, Member, IEEE, “New Directions in Cryptography”, Proceedings of the AFIPS National Computer Conference, June 1976.

20. Rivest. R., Shamir, A., and Adleman, L., “A Method for Obtaining Digital Signatures and Public Key Cryptosystems”, Communications of the ACM, February 1978.

21. Koblitz, N., “Elliptic Curve Cryptosystems”, Mathematics of Computation Vol. 48, Number 177, January 1987, pp 203-209.

22. Hevia, A., and Kiwi, M., “Strength of Two Data Encryption Standard Implementations Under Timing Attacks”, ACM Transactions on Information and System Security, November 1999.

23. Coppersmith, D., “The Data Encryption Standard (DES) and Its Strength against Attacks”, IBM Journal of Research and Development, May 1994

24. B.Scneier, “Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)”, Fast Software Encryption, Cambridge Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp 191-201.

25. Murphy, S., “The Cryptanlysis of FEAL-4 with 20 Chosen Plaintexts”, Journal of Cryptography, No. 3, 1990.

26. William Stallings, “Cryptography and Network Security-Principles and Practices Third Edition”, May 2004.

27. Rich Helton and Johennie Helton, “Java^{TM} Security Solutions”, 2004.

28. Jonathan Knudsen, “Java Cryptography”, O’REILLY, March, 1999.

29. Scott Oaks, “Java Security” O’REILLY, February, 2002.

30. Boneh, D., "Twenty Years of Attacks on the RSA Cryptosystem", Notices of the American Mathematical Society, February 1999.

31. Adams, C., "Simple and Effective Key Scheduling for Symmetric Ciphers", Proceedings, Workshop in Selected Areas of Cryptography, SAC'94. 1994.

32. Doroty E. Denning and Giovanni Maria Sacco, "Timestamps in Key Distribution Protocols", Communications of the ACM, August 1981

33. Alberto Partida and Diego Andina, "Applied Cryptography in Java", 1999 IEEE

34. Enge, A., "Elliptic Curves and Their Applications to Cryptography", Norwell, MA; Kluwer Academic Publishers, 1999.

35. Davies, D., and Price, W., "Security for Computer Networks", New York Wiley, 1989.

36. Jueneman, R., Matyas, S. and Meyer, C., "Message Authentication", IEEE Communications Magazine, September 1988.

37. David Hook, "Beginning Cryptography with Java" ,Wiley Publishing, Inc., 2005.

38. Jason Weiss, "Java Cryptography Extensions", Morgan Kaufmann Publishers, 2003.

39. Michael D.Meyer and Eric J.Miller, "Urban Transportation Planning" Mc Graw Hill, 2000.

40. Y. Daniel Liang, "Introduction to Java Programming", Prentice Hall, 2003.

41. George A. Morgan, Nancy L. Leech, Gene W. Gloeckner and Karen C. Barrett, "SPSS for Introductory Statistics", Lawrence Erlbaum Associates, Publishers, 2004.

42. Julie Pallant, "SPSS Survival Manual", Open University Press, 2005.

43. John Enter,William Wasserman and G.A. Whitmore, "Applied Statistics", Allyn and Bacon, 1992.

44. 張有恆,「運輸學」,1993。

45. 中華智慧型運輸系統協會,「台灣地區智慧型運輸系統實驗城規劃計畫(一)&(二)」,交通部委託研究計劃,2001 年 3 月。

46. 中華智慧型運輸系統協會,「符合 NTCIP 的無線寬頻 ATMS 交控示範系統（一）」,交通部委託研究計劃,2004 年 12 月。

47. 交通部，「都市交通控制通訊協定 3.0 版」，2004 年 11 月。

48. 中華顧問工程司，「先進交通控制系統協定 NTCIP-CTCIP-TTCIP 與我國 V3.0 協定轉換機制研究」，2006 年 11 月。

49. 黃韋凱，「台灣地區專用交通管理資訊庫(TMIB)之研究」，國立台灣大學土木工程所交通組研究所碩士論文，2003 年 6 月

50. 陳佳良，「NTCIP 物件利用 GPRS 傳輸之時間可靠度研究」，國立台灣大學土木工程所交通組研究所碩士論文，2005 年 6 月。

51. 劉宜傑，「ATMS 資料傳輸之資訊安全研究」，國立台灣大學土木工程所交通組研究所碩士論文，2006 年 6 月。

52. 胡育銘，「應用資訊安全於分散式測驗系統之研究」，國立台南師範學院資訊教育研究所碩士論文，2002 年 6 月。

53. 王青青，巫坤品譯，William Stallings 原著，「密碼學與網路安全原理與實務第三版」，碁峯資訊股份有限公司，2004 年五月。

54. 王旭正，柯宏叡「密碼學與網路安全理論、應用與實務」，博碩文化股份有限公司，2004 年 5 月。

55. 阮韻芳譯。Jonathan Knudsen 原著，「JAVA 密碼學」，1999 年三月。

56. 王文中，「EXCEL 於資料分析與統計學上的應用」，博碩文化股份有限公司，1997 年 9 月。

57. 潘南飛譯，「工程統計」，全威圖書有限公司，2002 年 11 月。

58. 鄒修銘譯，「Eclipse 實用手冊」，博碩文化股份有限公司，2004 年。

59. 林傑斌、林川雄、劉明德，「SPSS 統計建模與應用實務」，博碩文化股份有限公司，2004 年 7 月。

60. 楊松諺、上官飛鳳，「Java Security 全方位解決方案」，碁峰資訊股份有限公司，2004 年。

61. 洪維恩，「Java2.0 JDK5.0 教學手冊」，博碩文化股份有限公司，2005 年 5 月。

62. 楊豐瑞，楊豐任，「網路概論與實務」，松崗電腦圖書資料股份有限公司，2001 年 1 月。

63. 交通部運研所網站(http://www.iot.gov.tw/mp.asp?mp=1)

64. 冠陞工程企業有限公司(http://www.kangsang.com.tw/control_center.htm)

APPENDIX A

SNMP AND STMP

A-1 Simple Network Management Protocol

The Internet environment is dispersive and heterogeneous, hence it is impossible to manage Internet network without a suitable management system that can make all kinds of devices to communicate and connect with each other. The SNMP performs the role of a making manager establishing contacts with agents. SNMP which is a communications protocol developed by the Internet Engineering Task Force (IETF), is used for the configuration and monitoring of network devices and it follows TCP/IP transmissions protocol using get/set message parading to provide the information about agents for manager to directly reach the goal of Internet network management. Commonly, SNMP is used in Internet and computer industry applications, and it is composed of the following four requirements as illustrated in Figure A.1 which shows the components of SNMP.

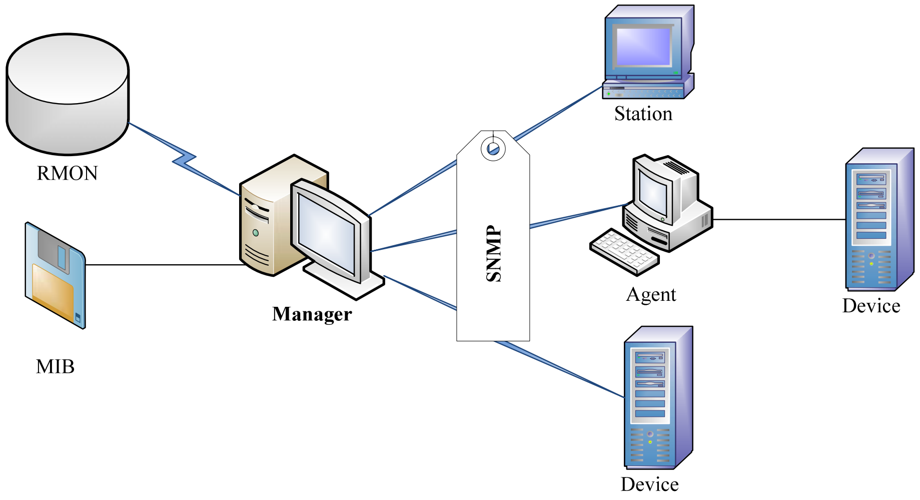


Figure A.1 The components of SNMP

- Manger

The entity sends commands to entities and processes their responses via the Internet management tool or software to monitor, control, and collect information with agents on Internet.

- Agent

The entity receives commands and transmits responses to the received commands. It is a kind of node devices of Internet requirements, such as host server, workstations, hub, switch or bridge.

- MIB (Management Information Base)

The unit of management information is called a managed object and the managed object is the smallest entity that can be transmitted or exchanged between a device and a management application. A collection of related managed object is defined in a document termed as a Management Information Base (MIB) module.

Management applications running on the central control hosts can read this module, and other modules such as controller MIBs and manufactures' specific MIBs. Figure A.2 shows the MIB integration with other vendor controllers.

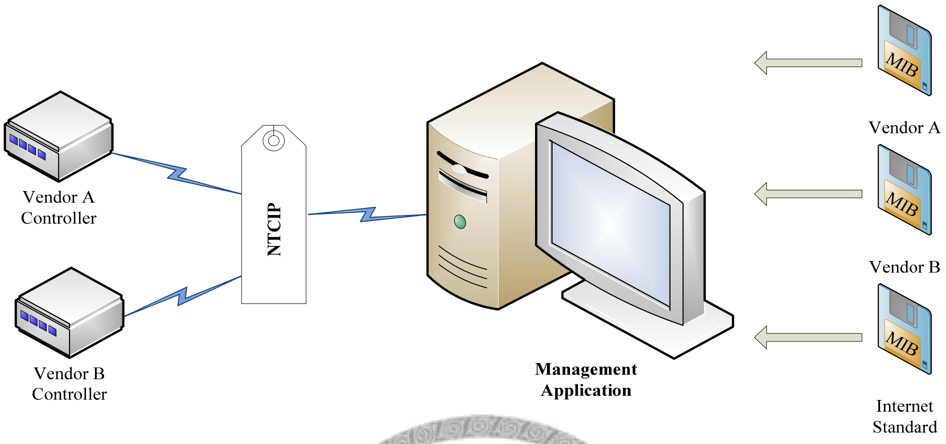


Figure A.2 MIB integrations

- RMON

Remote Network Monitoring (RMON) can compare with a remote MIB. In order to gain information about the capabilities of remote devices, the major functionality of RMON is to let many SMNP management applications to dynamically load and unload modules (MIBs) describing the information within remote networking devices.

Therefore, the MIB is the leading element of these components. This is because in SNMP management, manager utilizes the MIB modified to reach the aim of network management and monitoring. Upon the MIB establishment, SNMP defines three syntaxes to establish the MIB framework; they are Structure and Identification of Management Information (SMI), Abstract Syntax Notation One (ASN.1) and Basic

Encoding Rules (BER).

- SMI

  A definition on how to create management objects and a hierarchical (tree-link) definition of nodes where management objects will be attached for unique identification. The relationships are clearly as shown in Figure 2.8.

- BER

  RER is one of the ISO standards which include the rules for encoding data for transmission used with ASN.1.

- ASN.1

  ASN.1 is also one of the ISO standards and it is a formal language for describing information to be processed by computer.

Table A.1 shows the SNMP message form. The message form is distributed into two sections: Protocol Data Unit (PDU) header and PDU main body. The PUD is the packet data for specific communications layer or communications protocol.

Table A.1 SNMP Message form

PUD Header			PUN main body						
Application Header	Version	Community	PUD Type	Request ID	Error Status	Error Index	Sequence	Identity	Value

A-2 Simple Transportation Management Protocol

The STMP is the exclusive communications protocol which is established for transportation system and designed for considering the characters about data transmission in transportation field. Basically, the STMP is developed upon the SNMP and has the following differences:

- Difference in Message Type

  NTCIP defines STMP dependent on SNMP; there are eight kinds of message types of STMP. Tables A.2 and A.3 respectively list the message content, purposes and the originators of SNMP and STMP.

Table A.2 SNMP Message Type, Purpose and Originator

Version		Message Type	Purpose	Originator
V.1	V.2			
○	○	Get Request	Contains a list of data elements, the agent is to return the values	Management Application
○	○	Get Next Request	Contains a list of elements, the agent is to return the values of the next sequential data element from these indicated.	Management Application
○	○	Set Request	Contains a list of data elements and values, the agent is to set the values in its MIB per this message.	Management Application
○	○	Get Response	Agent response to either a Get or a Set request	Agent Application
○	○	Trap	An Agent initiated transmission to indicate that a defined event has occurred.	Agent Application
×	○	Get Bulk	Utilize to read a lot of data objects.	Management Application
×	○	Inform	Utilize to notify other management stations the related information actively.	Management Application

Table A.3 STMP Message Type, Purpose and Originator

Message Type	Purpose	Originator
Get Request	Shall be sent from a manager to an agent to request the values of specified objects.	Management Application
Set Request	Shall be sent from manger to an agent to request the values of specified objects be set to specified values.	Management Application
Set Request-No Reply	Shall be sent from manage to an agent to request that specified objects be sent to specified values.	Management Application
Get next Request	Shall be sent from a manager to an agent to request the value of the next object instance in lexicographic order	Agent Application
Get Response	Shall be used to send specified object data from an agent to manager. This response contains the object values that correspond to the prior get require or get next require from the manager. Get response message shall not be sent unless the agent has received a get request packet from the manager	Agent Application
Set Response	Shall be sent from an agent to manager to indicate that the set request for the specified objects was completed without error.	Agent Application
Error Response	Shall be sent from an agent to the manager in response to a set require, get request, or get next request that contained an error.	Agent Application
Trap Response	Shall be used to send specified object data from an agent to a manger. The trap is generated due to some event occurring within the agent, and is not a response to any manager request.	Agent Application

- Difference in Encoding Rule

SNMP uses the BER to be the encoding rule; by contrast, STMP selects the Octet Encoding Rule (OER) which is a variation of BER developed for use on low-bandwidth communications link.

- Difference in MIB

As shown in Figure A.3, NTCIP adds the transportation node of the NAME sub-tree under the original SMI to put the objects which are the special MIB established for transportation field called Transportation MIB (TMIB). Under the branch, it co-operates the dynamic object groups to reduce the bandwidth requirements of communicating sets of objects between a management station and agents. The dynamic object management (*dynObjMgmt*) contains three groups: Dynamic Object Definition Group, Dynamic Object Data Group and Dynamic Object Configuration Table Group.

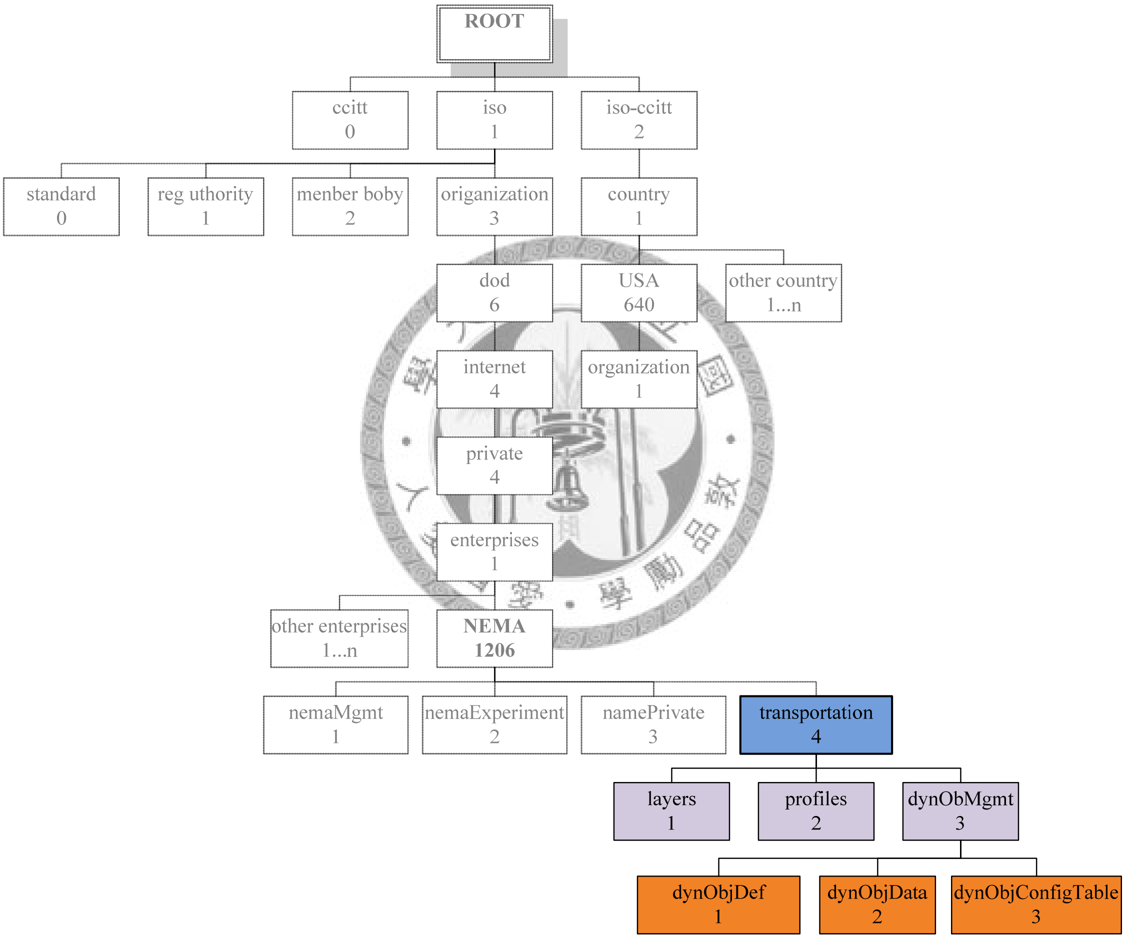


Figure A.3 Internet authority hierarchy and TMIB structure

- Difference in Message Form

The STMP message form is aimed at the characters of data transmission in transportation system. Accordingly, it omits many complicated procedures. There are only the PUD header and value as the two parts of the STMP message form (shows as Table A.4); it is quite different from SNMP. For this reason, STMP can also reach the goal of bandwidth saving.

Table A.4 STMP Message form

PUD Header	Value

- The Dynamic Objects used

The main difference between STMP and SNMP is that STMP co-operates the dynamic objects which NTCIP defines. As in the preceding discussion about dynamic object, we know the dynamic objects can reduce the unnecessary header of data packet to improve the bandwidth efficiency.

APPENDIX B

OPERATIONS OF AES AND RSA

B-1 AES [11] [27]

Before discussing the content of each operation, we have to introduce the definitions of Lookup Table, S-box and GF(2^8) calculation given below.

- Lookup Table

  In computer science, a lookup table is a data structure, usually an array or an associative array, and is often used to replace a runtime computation with a simpler array indexing operation.

- S-box

  The substitution box (S-box) is a basic component of symmetric key algorithms which perform substitution in cryptography. In block ciphers, they are typically used to obscure the relationship between the Key and the ciphertext. In many cases, the S-boxes are carefully chosen to resist cryptanalysis.

  The S-box takes some number of input bits, m, and transforms them into some number of output bits, n: an m×n S-box can be implemented as a lookup table with 2^m words of n bits each. One good example is this 6×4-bit S-box from DES (S_5) given below in Table B.1:

Table B.1 Example for S-box

S_5		Middle 4 bits of input															
		0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
Outer bits	**01**	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Given a 6-bit input, the 4-bit output is found by selecting the row using the outer two bits, and the column using the inner four bits. For example, an input "011011" has outer bits "01" and inner bits "1101"; the corresponding output would be "1001".

- $GF(2^8)$

Since in computing each byte holds 8 bits; in computer, it use zeros and ones to represent. Therefore, one could handle a byte to consider as a polynomial of seven degree which is composed of zeros and ones. For example, a byte **B** which is composed by b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0, one could consider the byte **B** as the polynomial as:

$$b_7x^7+ b_6x^6+ b_5x^5+ b_4x^4+ b_3x^3+ b_2x^2+ b_1x^1+ b_0 \qquad (A.1)$$

e.g., the polynomial of $(25)^{16}= (00100101)_2$ is x^5+x^2+1 (A.2)

Next, we introduce the operation in the AES algorithms:

- SubBytes

As shown in Figure B.1, it is a non-linear substitution operation step; each byte in the state is replaced with its entry in a fixed 8-bit lookup table **S** and each byte in the array is updated using the 8-bits S-box, as below:

$$b_{ij}=S(a_{ij}) \tag{A.3}$$

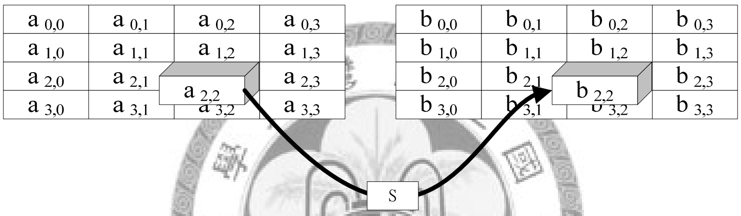


Figure B.1 SubBytes operation

- ShiftRows

The ShiftRows operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. As shown in Figure B.2, in AES, the first row is left unchanged; each byte of the second row is shifted on the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively.

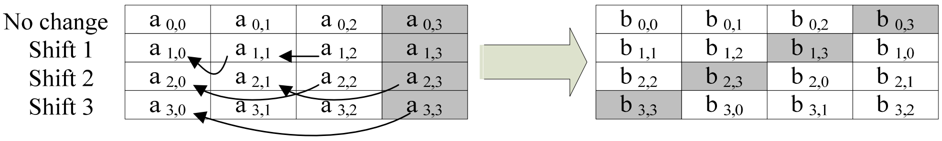


Figure B.2 ShiftRows operation

- MixColumns

See as Figure B.3, in MixColumns operation, the four bytes of each column of the state are combined using an invertible linear transformation which is multiplied with a fixed polynomial *c(x)*. The MixColumns function takes four bytes as input and output four bytes, where each input byte affects all four output bytes. Together with ShiftRows, MixColumns provides diffusion in the cipher. Each column is treated as a polynomial over GF(2^8) and is then multiplied modulo *(x^4+1)* with a fixed polynomial given as Equation A.4.

$$c(x)=3x^3+x^2+x+2 \qquad (A.4)$$

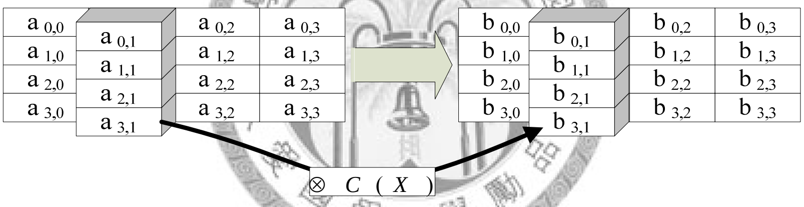


Figure B.3 MixColumns operation

- AddRoundKey

Figure B.4 represents the AddRoundKey operation; the subkeys which are the same size at the state are added by combining each byte of the state with the corresponding byte of the subkeys using the XOR (a logical operation exclusive disjunction).

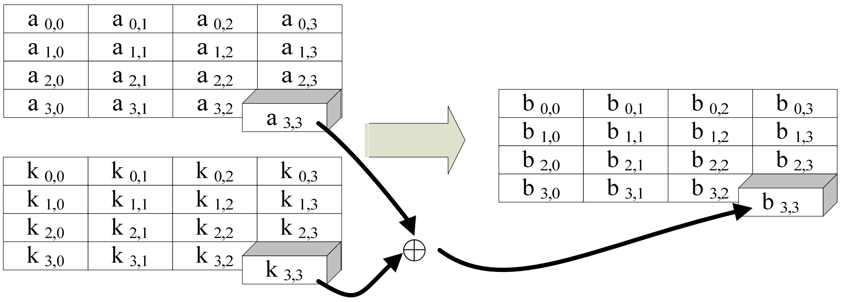


Figure B.4 AddRoundKey operation

B-2 RSA[12] [17] [31]

Asymmetric cryptosystems utilize mathematical operations to achieve encryption/decryption and replace the transposition and substitution techniques in symmetric cryptosystems. In terms of the mathematical operations which RSA algorithm used is the exponent operation. In RSA, the plaintext is separated into many blocks, and the value of each block is smaller than an integer *n*. This means that the size of each block might be equal or smaller than *log₂(n)*; actually, the size of the block should be *k* bits (*k* is a normal integer) and $2^k < n \le 2^{k+1}$, therefore , in terms of certain plaintext **M** and ciphertext **C**, the encryption and decryption can be expressed by Equations A.5 and A.6 respectively.

$$\mathbf{C = M^e \bmod n} \tag{A.5}$$

$$\mathbf{M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n} \tag{A.6}$$

Both of the transmitter and the receivers know the value *n*, however, only the transmitters and receivers know the value *e* and *d* respectively. Hence, it is the public-key cryptography algorithm which the public key is KU= {e, *n*}, and the private key is KR= {d, *n*}. In order to confirm as the asymmetric cryptosystem algorithm model like Figure 2.18, the algorithms should satisfy the given conditions stated below:

1) One should gain the value *e*, *d* and *n* to satisfy $M<n$ and

   $M^{ed}=M \bmod n$;

2) For any different $M<n$, it is easy to calculate M^e and C^d*, and*

3) It is impossible to calculate value *d* for given values of *e* and *n*.

With reference to point 1 mentioned above, one have to look for the relationship with the equation $M^{ed}=M \bmod n$ first.

By the Euler Theorem:

$$\begin{aligned} m^{k\phi(n)+1} &\equiv [(m^{\phi(n)})^k \times m] \bmod n \\ &\equiv [(1)^k \times m] \bmod n \\ &\equiv m \bmod n \end{aligned} \tag{A.7}$$

Using Equation 2.15, give two prime numbers *p*, *q* and two integers *n* and *m*, let *n=pq* and *0<m<n*, then for any integer *k* could get Equation A.8:

$$m^{k\phi(n)+1} \equiv m^{k(p-1)q(p+1)+1} \equiv \bmod n \tag{A.8}$$

in which, the $\phi(n)$ is the Euler phi function. That means, if the integer quantity which is smaller than *n* and the prime to *n*, and as *p, q* are the prime numbers, therefore, $\phi(pq) = (p-1)(q-1)$, thus we could get the relationship as Equation A.9.

$$ed = k\phi(n) + 1 \tag{A.9}$$

or by the following form:

$$ed = 1 \bmod \phi(n) \tag{A.10}$$

then

$$d = e^{-1} \bmod \phi(n) \tag{A.11}$$

that means that while gains the congruence of $\phi(n)$, *e* is the multiplication inverse letter to *d*, and the statement is established under the *d* (or *e*) is prime to $\phi(n)$.

After introducing the mathematics theory of RSA, in the RSA operations, the main elements are given below, and illustrated in Figure B.5:

- Choose *p*, *q,* in which *p*, *q* are different large primes;
- Calculate n=p×q;
- Choose e, in which $\gcd(\phi(n), e) = 1 and 1 < e < \phi(n)$,and;
- Calculate $d \equiv e^{-1} \bmod \phi(n)$

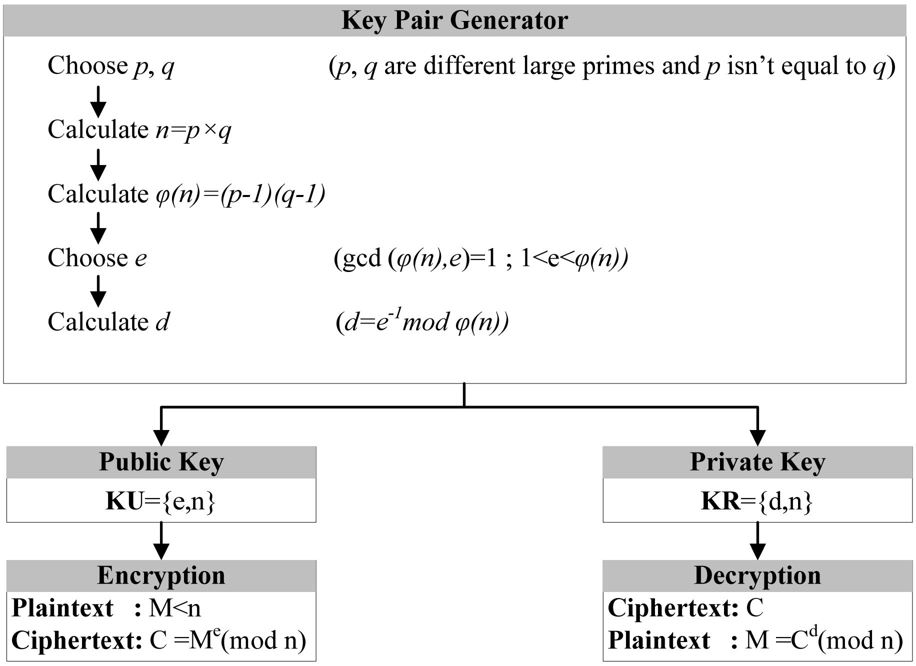

Key Pair Generator
Choose p, q
(p, q are different large primes and p isn't equal to q)
Calculate $n=p\times q$
Calculate $\varphi(n)=(p-1)(q-1)$
Choose e
(gcd ($\varphi(n),e$)=1 ; $1<e<\varphi(n)$)
Calculate d
($d=e^{-1} mod\ \varphi(n)$)
Public Key
KU={e,n}
Private Key
KR={d,n}
Encryption
Plaintext : M<n
Ciphertext: C =M^e(mod n)
Decryption
Ciphertext: C
Plaintext : M =C^d(mod n)

Figure B.5 The compositions of RSA algorithm

APPENDIX C

LIST OF EXPERIMENT CONTENTS

Table C.1 List of Experiment One

No	NTCIP Object Size (byte)							DSM Addition		Communications Medium	
	9	18	30	47	87	128	277	With	W/O	Wired	3.5G
1	◎							◎		◎	
2		◎						◎		◎	
3			◎					◎		◎	
4				◎				◎		◎	
5					◎			◎		◎	
6						◎		◎		◎	
7							◎	◎		◎	
8	◎							◎			◎
9		◎						◎			◎
10			◎					◎			◎
11				◎				◎			◎
12					◎			◎			◎
13						◎		◎			◎
14							◎	◎			◎
15	◎								◎	◎	
16		◎							◎	◎	
17			◎						◎	◎	
18				◎					◎	◎	
19					◎				◎	◎	
20						◎			◎	◎	
21							◎		◎	◎	
22	◎								◎		◎
23		◎							◎		◎
24			◎						◎		◎
25				◎					◎		◎
26					◎				◎		◎
27						◎			◎		◎
28							◎		◎		◎

Table C.2 List of Experiment Two

No	**Length of AES Secret Key (bit)**			**Length of RSA Public Key Pair (bit)**			**Communications Medium**	
	128	192	256	768	1024	2048	Wired	3.5G
1	◎			◎			◎	
2		◎		◎			◎	
3			◎	◎			◎	
4	◎				◎		◎	
5		◎			◎		◎	
6			◎		◎		◎	
7	◎					◎	◎	
8		◎				◎	◎	
9			◎			◎	◎	
10	◎			◎				◎
11		◎		◎				◎
12			◎	◎				◎
13	◎				◎			◎
14		◎			◎			◎
15			◎		◎			◎
16	◎					◎		◎
17		◎				◎		◎
18			◎			◎		◎

Table C.3 List of Experiment Three

No	**Interval of Message Dispatch (second)**					**Computation-capability of simulated TCIS**				**Communication Medium**	
	2	5	10	30	60	TCIS-i	TCIS-ii	TCIS-iii	TCIS-iv	Wired	3.5G
1	◎					◎				◎	
2		◎				◎				◎	
3			◎			◎				◎	
4				◎		◎				◎	
5					◎	◎				◎	
6	◎						◎			◎	

7		◎					◎			◎	
8			◎				◎			◎	
9				◎			◎			◎	
10					◎		◎			◎	
11	◎							◎		◎	
12		◎						◎		◎	
13			◎					◎		◎	
14				◎				◎		◎	
15					◎			◎		◎	
16	◎								◎	◎	
17		◎							◎	◎	
18			◎						◎	◎	
19				◎					◎	◎	
20					◎				◎	◎	
21	◎					◎					◎
22		◎				◎					◎
23			◎			◎					◎
24				◎		◎					◎
25					◎	◎					◎
26	◎						◎				◎
27		◎					◎				◎
28			◎				◎				◎
29				◎			◎				◎
30					◎		◎				◎
31	◎							◎			◎
32		◎						◎			◎
33			◎					◎			◎
34				◎				◎			◎
35					◎			◎			◎
36	◎								◎		◎
37		◎							◎		◎
38			◎						◎		◎
39				◎					◎		◎
40					◎				◎		◎

About the Author

Name : Yuan-Jui Chang

Birthday : 28 / February / 1983

Birthplace : Taipei, Taiwan

Education :

- Master degree in Division of Transportation Engineering, Department of Civil Engineering, National Taiwan University, Taiwan. (2007~2009)
- Master degree in Division of Transportation Engineering, School of Civil & Environmental Engineering, Nanyang Technological University, Singapore. (2008~2009)
- Bachelor degree in Department of Construction Engineering, National Taiwan University of Science and Technology, Taiwan. (2003~2005)

E-mail : R95521511@ntu.edu.tw