Dynamic encryption technique for the security and efficiency of ATMs data transmission

Chang, Yuan Jui

2010

Chang, Y. J. (2010). Dynamic encryption technique for the security and efficiency of ATMs data transmission. Master's thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/20955>

<https://doi.org/10.32657/10356/20955>

Dynamic Encryption Technique for the Security and Efficiency of ATMS Data Transmission

CHANG, YUAN-JUI

School of Civil & Environmental Engineering

A thesis submitted to the Nanyang Technological University
in fulfilment of the requirement for the degree of
Master of Engineering

2010

ACKNOWLEDGEMENTS

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。

The encouragements above were given from Dr. Yeh,Chan-Hsiung (葉超雄) who is a professor of National Taiwan University; these encouragements gave me motivation and different perspectives not only for my studies, but also at the same time for the gains and losses in my life. Therefore, I mark them at the beginning of this thesis as utmost importance to me as I would like share it with all of my friends.

Undoubtedly, I have received much help and undeserve kindness from many respectable elders and friends during my studying period ever since I was young. If I have some little accomplishments, that would be because of them.

Studying in National Kaoshiung University of Applied Science is one of the major turning point in my life. I would not be where I am today if without for these mentors; hence, I would like to show my appreciation to Dr. Huang,Wen-Ling (黃文玲), Mr. Yeh,Yi-Jen (葉以仁), Mr. Wu,Ssu-Hsin (吳思敏),Mr. Chiu,Shu-Chuan (邱樹泉), Mr. Lo,Chih-Chan (羅志誠), Mr. Tang,Meng-Chung (唐孟忠), Mr. Chang,Peng-Ping (張澎平), Mr. Lee,Chien-Kuo (李建國), Ms. Hung,Yi-Lin (洪逸琳) and Ms. Chang,Chiung-Wen (張瓊文). Thanks for your care.

Studying abroad is definitely a special and memorable experience for me. I truly treasure and grateful that I was given the opportunity of the dual master degree programme which was offered by National Taiwan University, Taiwan and

Nanyang Technological University, Singapore. Fortunately, I met a high regarded supervisor—Dr. Lum Kit Meng, you give me a lot of undivided attention of yours in this arduous journey in my life and guidances in my studies. Not to forget, I would also like to extend my gratidue to extended the amiable members of Transportation Lab. namely Dr. Wong Yiik Diew, Ms. Ng-Ho Choo Hiang and Mr. Liew Kai Liang for your helping hands. Because of you, I could complete my studies smoothly in Singapore.

Special thanks go to Zhipeng, Qifang, Jason Poon, Seowli, Fuquan, Melvin and Zhiyan for the assistance in proofreading, you made this thesis for the better and a perfect piece of work altogether. I think it had took up a lot of your precious time and effort; thank you very much.

Besides, my classmates and friends: **NTUST** — Lee,Hui-Chuan (李慧娟), Lee,Ming-Hsiu (李名修), Ho,Chen-Yi (何貞儀), Jao,Chih-Kai (饒智凱), Wang,Chao-Ho (王詔賀), Huang,Wei-Hsiang (黃偉翔), Huang,Sheng-Yung (黃聖詠); **NTU ITS Lab.** — Lin,Shang-Chun (林尚駿), Yang,Li-Kai (楊礫凱), Yu,Shang-Min (游上民), Chou,Chen-Ju (周辰儒), Hsu,Yu-Fang (許毓芳), Chen,Yen-Cheng (陳彥政), Lee,Yen-Ning (李晏寧), Wang,Chieh (王介); and others as Cindy, Aaron, Christopher, Weijian, Ruoyi, Junhua, Carrie, Lawrence, Samuel, Peng,Chiao-Ling (彭巧伶), and lots and lots of my friends. It was because of your accompany and presence, my life has become more colorful and interesting.

Last but not least, I wish to express my gratitude to my parents and my family members for their perpetual support, unconditional love and tireless care towards me.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS.....	ii
TABLE OF CONTENTS	iv
EXECUTIVE SUMMARY.....	viii
LIST OF TABLES	x
LIST OF FIGURES	xiii
LIST OF ABBREVIATIONS	xvi
CHAPTER ONE INTRODUCTION	1
1.1 Background.....	1
1.2 Objectives of this Research	5
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.....	12
2.1 Introduction.....	12
2.2 Advanced Transportation Management System	12
2.3 NTCIP	14
2.3.1 Protocol and NTCIP	14
2.3.2 Framework, Standards and Protocol Stacks of NTCIP	17
2.3.3 Brief Summary	20

2.4	Security Elements	21
2.4.1	Network Security Model.....	21
2.4.2	Security Attack Techniques.....	23
2.4.3	Security Services	25
2.5	Cryptography Technologies.....	26
2.5.1	Symmetric Cryptography.....	26
2.5.2	Asymmetric Cryptography.....	33
2.5.3	Message Digest and Message Authentication	37
2.6	The Possible Attack Discussions on ATMS Data Transmission	40
2.7	Summary and Evaluations	44
 CHAPTER THREE SECURITY MECHANISM ESTABLISHMENT AND SECURITY PROTECTION DISCUSSION.....		 48
3.1	Introduction.....	48
3.2	Conceptions of Information Security in this Study.....	49
3.3	Development Tool- Java Programming Language.....	51
3.4	Architecture of the Security Mechanism.....	54
3.4.1	Conceptions of the Dynamic Encryption Technique	54
3.4.2	Architecture of the Dynamic Security Mechanism	58
3.5	Security Analysis for the Security Mechanism.....	66
3.5.1	Analysis of Security Protection.....	66
3.5.2	Cryptanalysis	70
3.5.3	Brute-Force Attack	73
3.6	Summary.....	75

CHAPTER FOUR	EXPERIMENTS FOR SYSTEM EFFICIENCY	77
4.1	Introduction.....	77
4.2	Experiment Design Principle	77
4.3	Experiment Environment.....	80
4.3.1	Scope of Simulated Experiment	80
4.3.2	The protocol stacks and hardware for Simulation.....	81
4.3.3	NTCIP objects for the Simulation	87
4.4	Experiment Contents	91
4.4.1	Experiment Methodology	91
4.4.2	Experiment One.....	97
4.4.2	Experiment Two	99
4.4.3	Experiment Three	101
4.5	Expected Outcomes.....	103
CHAPTER FIVE	DATA ANALYSIS AND FINDINGS	106
5.1	Introduction.....	106
5.2	Queue and delay phenomenon of DSM operation	106
5.3	Data Analysis of Experiment One.....	110
5.3.1	Analysis in the communications medium, NTCIP object size and DSM addition for the influence of transmission delay	111
5.3.2	Analysis in the NTCIP object size for the influence of encryption and decryption operations	114
5.3.3	Brief summary	117
5.4	Data Analysis of Experiment Two	117
5.4.1	Analysis in the length combinations of AES secret key and RSA	

public key pair for the influence of data packet transmission delay.....	118
5.4.2 Analysis in the length combinations of AES secret key and RSA public key pair for the influence of device operation delay.....	121
5.5 Data Analysis of Experiment Three	126
5.5.1 Analysis in the interval of the object dispatch and the computation-capability for influence of device operation delay..	127
5.5.2 Analysis in the interval of the object dispatch and the computation-capability for influence of data packet transmission delay.....	131
5.5.3 Brief summary.....	134
5.6 Regression Equation of DSM Operations	136
CHAPTER SIX CONCLUSIONS AND FUTURE RESEARCH	140
6.1 Conclusions.....	140
6.2 Future Research and Suggestions	144
REFERENCES	145
APPENDIX A SNMP AND STMP	147
A-1 Simple Network Management Protocol	147
A-2 Simple Transportation Management Protocol	150
APPENDIX B OPERATIONS OF AES AND RSA	154
B-1 AES	154
B-2 RSA	157
APPENDIX C LIST OF EXPERIMENT CONTENTS.....	161

EXECUTIVE SUMMARY

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 one of the major sub-system of ITS, and it utilizes monitor apparatus, communications and other control technologies to obtain or exchange traffic information between traffic devices. However, during 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 are concerned with the issue.

For 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 the 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 field commonly uses nowadays, namely: wired network communications and 3.5G mobile communications.

LIST OF TABLES

Table 2.1 Characteristics of symmetric cryptography algorithms.....	45
Table 2.2 Characteristics of asymmetric cryptosystem algorithms.....	46
Table 2.3 Comparisons: symmetric cryptography vs. asymmetric cryptography...	46
Table 3.1 Example of encryption via ECB cipher mode.	71
Table 3.2 Example of encryption via CBC cipher mode.....	71
Table 3.3 Time-consuming for cracking cipher algorithms by brute-force attack.	74
Table 3.4 Effects of the dynamic security mechanism.....	76
Table 4.1 Protocol stack items of the experiments.....	82
Table 4.2 Specification of simulated computers.....	83
Table 4.3 Specification for wired network.....	85
Table 4.4 Specifications for 3.5G mobile communications.....	86
Table 4.5 NTCIP Object No.01 — trafficControl Code.....	88
Table 4.6 NTCIP Object No.02 — cmsDimSchedule Code.....	88
Table 4.7 NTCIP Object No.03 — phaseOrderTable Code.....	88
Table 4.8 NTCIP Object No.04 — timingPlantable Code.....	88
Table 4.9 NTCIP Object No.05 — timingPlantable Code.....	89
Table 4.10 NTCIP Object No.06 — timingPlanBacsicParatable Code.....	89
Table 4.11 NTCIP Object No.07 — vdCurrentDataTable Code.....	90
Table 4.12 Test objects of Experiment One.....	99
Table 4.13 NTCIP object usage for Experiment One.....	99
Table 4.14 Test objects of Experiment Two.....	101
Table 4.15 Test objects of Experiment Three.....	103
Table 5.1 Crack points of continuous DSM operations (C_c)	107

Table 5.2 Crack points of continuous DSM operations (KP_l).....	109
Table 5.3 Crack points of continuous DSM operations (M_f).....	109
Table 5.4 Statistic Descriptions of Analysis 1-1.....	111
Table 5.5 Mean time-consumption of NTCIP object transmission of Analysis1-1.....	112
Table 5.6 Regression equation analysis of Analysis 1-1.....	113
Table 5.7 The observed mean of the consuming time of encryption/decryption.....	114
Table 5.8 One-Way ANOVA Table of Analysis 1-2 (Encryption).....	116
Table 5.9 One-Way ANOVA Table of Analysis 1-2 (Decryption).....	116
Table 5.10 Observed mean of the consuming time of data transmission.....	118
Table 5.11 Two-Way ANOVA Table of Analysis 2-1.....	120
Table 5.12 Observed mean of the consuming time of device operations.....	121
Table 5.13 One-Way ANOVA Table of C_m and AES/RSA operations.....	123
Table 5.14 Two-Way ANOVA Table of Analysis 2-2.....	124
Table 5.15 The comparisons with the different length of RSA public key pair...	125
Table 5.16 Observed mean of device operations (Analysis 3-1).....	128
Table 5.17 Two-Way ANOVA Table of Analysis 3-1.....	131
Table 5.18 Observed mean of data packet transmission (Analysis 3-2).....	132
Table 5.19 Regression equation analysis of Analysis 3-2.....	133
Table 5.20 Analysis results of C_m , KS_l , KP_l , M_s , M_f and C_c	135
Table 5.21 Statistics descriptions of the regression equation in this research....	137
Table 5.22 Regression equation analysis of DSM operation.....	137
Table 5.23 The threshold values of DSM operation efficiency.....	139
Table A.1 SNMP Message form.....	150
Table A.2 STMP Message form.....	150

Table A.3 STMP Message Type, Purpose and Originator.....	151
Table A.4 SNMP Message Type, Purpose and Originator.....	152
Table B.1 Example for S-box.....	155
Table C.1 List of Experiment One.....	161
Table C.2 List of Experiment Two.....	162
Table C.3 List of Experiment Three.....	162

LIST OF FIGURES

Figure 1.1 Singapore ITS architecture.....	3
Figure 1.2 The traffic control system framework of Taipei City, Taiwan.....	4
Figure 1.3 Structure and procedures of this research.....	9
Figure 2.1 ITS sub-systems and related techniques of ATMS.....	13
Figure 2.2 NTCIP and the National ITS Architecture.....	15
Figure 2.3 Examples of ITS Integration Using NTCIP.....	15
Figure 2.4 NTCIP Standards Framework.....	17
Figure 2.5 Relationships between OSI Layers and NTCIP Levels.....	18
Figure 2.6 Network Security Model.....	21
Figure 2.7 Illustration for active attack types.....	24
Figure 2.8 Architecture of symmetric cryptosystem.....	27
Figure 2.9 Encryption and decryption procedures of DES.....	30
Figure 2.10 Encryption and decryption procedures of Triple-DES.....	31
Figure 2.11 Encryption and decryption procedures of AES.....	33
Figure 2.12 Architecture of asymmetric cryptosystem.....	34
Figure 2.13 Architecture of message digest.....	38
Figure 2.14 Masquerading Attack in ATMS Data Transmission.....	41
Figure 2.15 Eavesdropping Attack in ATMS Data Transmission.....	42
Figure 2.16 Man-In-the-Middle Attack in ATMS Data Transmission.....	43
Figure 3.1 Conceptions of the dynamic encryption techniques.....	50
Figure 3.2 The balance-point for the security mechanism consideration.....	51
Figure 3.3 Simple class hierarchy of security mechanism in Java programming....	52
Figure 3.4 Architecture of Dynamic Encryption Technique.....	55

Figure 3.5 Framework of Dynamic Key Generator.....	57
Figure 3.6 TMIC Operation One — to generate a public key pair and seal byte arrays before the public key transmission.....	59
Figure 3.7 Procedures for data packet restoration and message digest comparison.....	60
Figure 3.8 Procedures for data packet restoration and message digest comparison.....	61
Figure 3.9 Functions of message digest algorithms of the security mechanism.....	62
Figure 3.10 Procedures for the secret key separation.....	62
Figure 3.11 Procedures for the NTCIP object encryption and transmission.....	63
Figure 3.12 Procedures for NTCIP object ciphertext decryption.....	65
Figure 3.13 Flow chart of the security mechanism of this research.....	65
Figure 3.14 ECB cipher mode and CBC cipher mode.....	70
Figure 4.1 Time-consumption assignment of DSM operation.....	78
Figure 4.2 Framework of ATMS data transmission.....	80
Figure 4.3 Protocol stacks of the experiments.....	82
Figure 4.4 Framework of wired network.....	85
Figure 4.5 Framework of 3.5G mobile communications.....	86
Figure 4.6 Experiment situations.....	93
Figure 4.7 VPN connection procedures.....	94
Figure 4.8 Network Time Calibration Software — NTPClock.....	94
Figure 4.9 Display of DSM programming operation.....	95
Figure 4.10 Display of note items.....	95
Figure 4.11 Operation procedures of DSM.....	96
Figure 4.12 Framework of Experiment One.....	99
Figure 4.13 Framework of Experiment Two.....	101

Figure 4.14 Framework of Experiment Three.....	103
Figure 5.1 DSM operation in different computation-capability TCIS dvices....	107
Figure 5.2 Crack point of DSM operations (C_c)	108
Figure 5.3 DSM operation in different RSA public key pair length.....	108
Figure 5.4 DSM operation in different NTCIP object dispatch interval.....	109
Figure 5.5 Crack point of DSM operations (M_f)	110
Figure 5.6 Line graph of mean time-consumption of NTCIP object transmission.....	112
Figure 5.7 Line graph of mean time-consumption of encryption/decryption.....	115
Figure 5.8 The mean comparisons of AES operations.....	126
Figure 5.9 The mean comparisons of RSA operations.....	126
Figure 5.10 The resection of the factor in C_c (Analysis 3-1)	129
Figure 5.11 The resection of the factor in M_f (Analysis 3-1).....	129
Figure 5.12 The resection of the factor in C_c (Analysis 3-2).....	133
Figure 6.1 The time-consumption trend of DSM operations.....	143
Figure A.1 The components of SNMP.....	147
Figure A.2 MIB integrations.....	148
Figure A.3 Internet authority hierarchy and TMIB structure.....	153
Figure B.1 SubBytes operation.....	156
Figure B.2 ShiftRows operation.....	156
Figure B.3 MixColumns operation.....	157
Figure B.4 AddRoundKey operation.....	157
Figure B.5 The compositions of RSA algorithm.....	160

LIST OF ABBREVIATIONS

AES	<u>A</u> dvanced <u>E</u> ncryption <u>S</u> tandard
ASN.1	<u>A</u> bstract <u>S</u> yntax Notation <u>O</u> ne
ATMS	<u>A</u> dvanced <u>T</u> ransportation <u>M</u> anagement <u>S</u> ystem
BER	<u>B</u> asic <u>E</u> ncoding <u>R</u> ules
CBC	<u>C</u> ipher <u>B</u> lock <u>C</u> haining
CCTV	<u>C</u> losed <u>C</u> ircuit <u>T</u> ele <u>v</u> ision camera systems
CFB	<u>C</u> ipher <u>F</u> eed <u>b</u> ack Mode
C2C	<u>C</u> entre- <u>t</u> o- <u>C</u> entre
C2F	<u>C</u> entre- <u>t</u> o- <u>F</u> ield
DES	<u>D</u> ata <u>E</u> ncryption <u>S</u> tandard
DSKG	<u>D</u> ynamic <u>S</u> ecret <u>K</u> ey <u>G</u> enerator
DSM	<u>D</u> ynamic <u>S</u> ecurity <u>M</u> echanism
DKG	<u>D</u> ynamic <u>K</u> ey <u>G</u> enerator
DPKG	<u>D</u> ynamic <u>P</u> ublic <u>K</u> ey Pair <u>G</u> enerator
ECB	<u>E</u> lectronic <u>C</u> ode <u>b</u> ook Mode
ECC	<u>E</u> lliptic <u>C</u> urve <u>C</u> ryptography
FIPS	<u>F</u> ederal <u>I</u> nformation <u>P</u> rocessing <u>S</u> tandard
GIS	<u>G</u> eographic <u>I</u> nformation <u>S</u> ystem
GPRS	<u>G</u> eneral <u>P</u> acket <u>R</u> adio <u>S</u> ervice
IETF	<u>I</u> nternet <u>E</u> ngineering <u>T</u> ask <u>F</u> orce
ISO-OSI	<u>I</u> nternational <u>S</u> tandards <u>O</u> rganisation- <u>O</u> pen <u>S</u> ystem <u>I</u> nterconnect
ISP	<u>I</u> nternet <u>S</u> ervice <u>P</u> roviders
ITS	<u>I</u> ntelligent <u>T</u> ransportation <u>S</u> ystem

ITU	<u>I</u> nternational <u>T</u> elecommunication <u>U</u> nion
ITU-T	<u>I</u> TU- <u>T</u> elecommunication Standardization Sector
IV	<u>I</u> nitialization <u>V</u> ector
JAAS	<u>J</u> ava <u>A</u> uthentication and <u>A</u> uthorization <u>S</u> ervice
JCA	<u>J</u> ava <u>C</u> ryptography <u>A</u> rchitecture
JCE	<u>J</u> ava <u>C</u> ryptography <u>E</u> xtension
JSSE	<u>J</u> ava <u>S</u> ecure <u>S</u> ockets <u>E</u> xtension
JVM	<u>J</u> ava <u>V</u> irtual <u>M</u> achine
MAC	<u>M</u> essage <u>A</u> uthentication <u>C</u> odes
MD	<u>M</u> essage <u>D</u> igest
MD2	<u>M</u> essage <u>D</u> iges <u>2</u>
MD4	<u>M</u> essage <u>D</u> igest <u>4</u>
MD5	<u>M</u> essage <u>D</u> igest <u>5</u>
MIB	<u>M</u> anagement <u>I</u> nformation <u>B</u> ase
NBS	<u>N</u> ational <u>B</u> ureau of <u>S</u> tandards
NEMA	<u>N</u> ational <u>E</u> lectrical <u>M</u> anufacturers <u>A</u> ssociation, America
NIST	<u>N</u> ational <u>I</u> nstitute of <u>S</u> tandard and <u>T</u> echnology
NTCIP	<u>N</u> ational <u>T</u> ransportation <u>C</u> ommunication for <u>I</u> TS <u>P</u> rotocol
NTU	<u>N</u> anyang <u>T</u> echnological <u>U</u> niversity
OER	<u>O</u> ctet <u>E</u> ncoding <u>R</u> ule
OID	<u>O</u> bject <u>I</u> dentifier
OS	<u>O</u> perating <u>S</u> ystem
PDU	<u>P</u> rotocol <u>D</u> ata <u>U</u> nit
PER	<u>P</u> rice- <u>E</u> arnings <u>R</u> atio
RMON	<u>R</u> emote Network <u>M</u> onitoring

PMPP	<u>P</u> oint-to- <u>M</u> ulti <u>P</u> oint <u>P</u> rotocol
PRNG	<u>P</u> seudo- <u>R</u> andom <u>N</u> umber <u>G</u> enerator
RSA	<u>R</u> ivest- <u>S</u> hamir- <u>A</u> dleman
RSU	<u>R</u> oad- <u>S</u> ide <u>U</u> nit
SCATS	<u>S</u> ydney <u>C</u> oordinated <u>A</u> daptive <u>T</u> raffic <u>S</u> ystem
SMI	<u>S</u> tructure and Identification of <u>M</u> anagement <u>I</u> nformation
SNMP	<u>S</u> imple <u>N</u> etwork <u>M</u> anagement <u>P</u> rotocol
STMP	<u>S</u> imple <u>T</u> ransportation <u>M</u> anagement <u>P</u> rotocol
TCIS	<u>T</u> ransportation <u>C</u> ommunication and <u>I</u> nformation <u>S</u> tation
TCP/IP	<u>T</u> ransmission <u>C</u> ontrol <u>P</u> rotocol/ <u>I</u> nternet <u>P</u> rotocol
TMIC	<u>T</u> ransportation <u>M</u> anagement <u>I</u> nformation <u>C</u> entre
TMIB	<u>T</u> ransportation <u>M</u> anagement <u>I</u> nformation <u>B</u> ase
Triple-DES	<u>T</u> riple <u>D</u> ata <u>E</u> ncryption <u>S</u> tandard
TSC	<u>T</u> raffic <u>S</u> ignal <u>C</u> ontroller
TTP	<u>T</u> rusted <u>T</u> hird <u>P</u> arty
VMS	<u>V</u> ariable <u>M</u> essage <u>S</u> ign
VD	<u>V</u> ehicle <u>D</u> etectors
VPN	<u>V</u> irtual <u>P</u> rivate <u>N</u> etwork

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.

(ITS Society, America, 2008)

Transportation system is composed of many members, including people, vehicles, road systems, traffic hardware, etc. Vehicles and the road systems or other traffic hardware are the industrial products. How to make these industrial products possess “intelligent” to solve the complicated traffic problems and improve the transportation safety, efficiency and comfortable are the aims of Intelligent Transportation System (ITS). ITS combines with many technologies applying, e.g. advanced electronic, computer, information, vehicle, communication, control, etc to provide the real-time information, varied traffic management policies and reduce 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 apparatuses, communications 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

communications. TMIC collects traffic information which is derived from vehicle detectors (VD), closed circuit television camera systems (CCTV) or others to establish the traffic control in instruction and integrate the traffic management policies. Finally, TMIC sends these traffic instructions and policies to the related traffic management apparatus, beacon devices, controller and road-side unit (RSU) or users. Because need to transmit information, the communications technology becomes one of the important factors 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 analyzing 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 processes in data transmission, the situation of the data packet switching nowadays 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 the data transmission of traffic control systems. These actions will cause ATMS to become paralysed and disorder the signal timing or influence the traffic safety seriously further. A possible solution is to build an Intranet Network System up for ATMS (i.e., Virtual Private Network, VPN). While the communications environment of Intranet is closed, and the fire-wall is well-controlled additionally, the invading opportunity will be reduced, but the cost will be more expensive.

Figure 1.1 Singapore ITS architecture (LTA, Singapore, 2008)

Figure 1.2 The traffic control system framework of Taipei City, Taiwan
(Institute of Transportation. MOTC, Taiwan, 2008)

Based on the above-mentioned, this research focuses on the information security of data transmission through modern cryptography and sets up a suitable encryption technique which aims at the message packet interchanging and transmitting. Even though hackers 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. Hence, 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 procedure, the security mechanism of this research can provide respective secret key for different message packet, and the secret key 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:

- During the message packet transmission, the encrypting procedure uses respective secret key via random or catching the characteristic characters from each message to encrypt, so hackers would not know the security formulae easily, and;
- The cost-benefit of attacking security mechanisms might be high to seduce hackers.

From the two reasons and including others, the cipher algorithm selection, the secret key generation and transmission 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 might 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 due to 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 the data 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 from 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;
- Develop a security mechanism by Java programming language and then undertake to operate, test, analyze the security mechanism programming. In order to simulate real situations, this research uses five computers to simulate 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 of the encryption or decryption procedures would cause the negative-effects for the core systems. 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 advantages 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 encryption and decryption procedure additions in the data transmission would affect the original system. Thus, this research shall also discuss the influences for the ATMS operation due to the security mechanism addition;

- Consider the security mechanism is subjected to be attacked and the threat analysis for security, and;
- Undertake to analyze the system effects by three designed experiments to discuss the variations between the security mechanism addition.

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 communications. 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. Additionally, this chapter introduces why this research chooses Java programming language to be the development tool and the security analysis for the security mechanism as well. The points of the 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 is established for ATMS data transmission. In Chapter Four, there are three experiments designed to test the operation efficiencies of the security mechanism. These experiments would probe into the negative-effect generations for the core systems due to the dynamic security mechanism addition and discuss the influences on the different considerations.

Chapter Five Data Analysis and Findings

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

Chapter Six Conclusion and Future Research

Draw the conclusions and suggestions to 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 sub-system 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 sub-system—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 communications 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 sub-systems 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 sub-systems of ITS and the related techniques about ATMS.

Figure 2.1 ITS sub-systems and related techniques of ATMS

2.3 NTCIP

2.3.1 Protocol and NTCIP

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 equipments (devices) 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 sub-systems 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 system usage in traffic, transit, emergency management, traveller information and planning/data archiving systems (NTCIP Guide v.03.02b, 2002). We can see the various transportation management systems and device integrations by using NTCIP from Figure 2.3 illustration.

Figure 2.2 NTCIP and the National ITS Architecture
(NTCIP Guide v.03.02b, 2002)

Figure 2.3 Example of ITS Integration Using NTCIP
(NTCIP Guide v.03.02b, 2002)

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 can be in different types work together and interconnect as a single system for some common purposes seamlessly.

- 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 equipments (devices) in different boards, types or manufactures to be mixed on the same communications link. 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

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 relationships between OSI layer modular and NTCIP levels model respectively.

Figure 2.4 NTCIP Standards Framework (NTCIP Guide v.03.02b, 2002)

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 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 about the traditional OSI 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 as TCP, UDP and 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 medium usage for communications, 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

of data elements called dynamic object 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 specially designed 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 SNMP and STMP in Appendix A.

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

This section utilizes the network security model and the related security definitions from the Telecommunication Standardization Sector (ITU-T) which is under International Telecommunication Union (ITU) to discuss the security services, security demands and common attack techniques on the open network system. 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 (William Stallings, 2003)

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 transmission securely; 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 the both principals 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 (ITU-T,1995)

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 analyze the data packets. The possible passive attack patterns in ATMS data transmission might be:

- 1) Eavesdropping and wiretapping;
- 2) Traffic analysis;
- 3) Analysis of the protocol data unit (PDU) headers of messages for the illegitimate purposes;
- 4) Copy of PDU data to other systems other than the intended destinations, and;
- 5) Cryptanalysis.

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

● Active Attacks (ITU-T,1995)

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

1) Interruption [as condition (b) of Figure 2.7]

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

2) Reply [as condition (c) of Figure 2.7]

Attackers would intercept the messages and send them repeatedly.

3) 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.

4) Masquerade [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 (William Stallings, 2004)

2.4.3 Security Services

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

- Authentication

It is a process which allows for checking with certainty the identity 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 by attackers. The usual protection method is to encrypt the transmission data packets via cryptography technologies.

- Data Integrity

In data confidentiality, the protection objects 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 communications environment than in wired network, and the wireless communications would be the main stream for transportation control system usage additionally. 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 the 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 source of data and its integrity, and further, to verify that the data is received by the designators or the public keys of asymmetric cryptosystems are not modified. Moreover, we can adopt the message digest technique to ensure the data integrity and user authentication as well.

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 this figure, the left side is the encryption procedure and the right side is the decryption procedure.

Figure 2.8 Architecture of symmetric cryptosystem
(Jason Weiss, 2004)

Broadly speaking, the symmetric cryptosystem 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 it transforms the ciphertext into the plaintext via the secret key further.

The relationships 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:

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

M: The set of plaintexts

K: The set of secret keys

C: The set of ciphertexts

or by the following equation:

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

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:

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

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

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 know the encryption algorithms or own 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 algorithm, 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 (Coppersmith, D, 1994).

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

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.

Figure 2.9 Encryption and decryption procedures of DES

(b) Blowfish

Blowfish is developed by *Bruce Schneier* in 1993 and has the following advantages (B.Schneier, 1993):

- 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, and;
- 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

As the characteristics of DES, the short length secret key is the major misgiving for DES. Because of it, 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 (William Stallings, 2003). 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; hence, so far, beside brute-force attack; we 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 more loading onto the core system and make the operation efficiency to worsen further. On the other hand, the message block size still limits in 64 bits as DES.

Figure 2.10 Encryption and decryption procedures of Triple-DES

(d) AES

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 $128 \div 8 = 16$ bytes. AES operates on a 4×4 array of bytes, called *state*, and most AES calculations are done in a special finite field (Jonathan Knudsen, 1999).

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 utilize one transposition method and three 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 row 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, AES cryptography is the major algorithm of symmetric cryptosystem today. Thus, this research adopts AES cipher algorithm to be the consideration for the security mechanism establishment as well. Reader can understand the internal detail operations of AES cryptography as Appendix B.

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 cryptosystem (also termed as the public-key cryptosystem) which is 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 (Jason Weiss, 2004)

Figure 2.12 shows the architecture of asymmetric cryptosystems and notes that asymmetric cryptosystems 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 2.12 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:

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

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:

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

in which **E_{KU}** is the encryption algorithm with public key **KU**, and;

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

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

or the another form:

$$\mathbf{D}_{\mathbf{KR}} \times (C) = \mathbf{M} \quad (2.8)$$

in which **KR** and **D_{KR}** are the private key and decryption algorithm with the private key **KR** respectively.

As mentioned above, the major difference between symmetric cryptosystems and asymmetric cryptosystems is the key generator, and it diminishes the weakness in symmetric cryptosystems. Subsequent contents 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 B.

(a) RSA

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 popular usage in

asymmetric cryptosystems. Therefore, the security mechanism of this research also adopts 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 (Boneh, D., 1999).

(b) ECC

Elliptic Curve Cryptography (ECC) is invented by *Neal Koblitz* and *Victor Miler* in 1985. Before ECC, RSA is the major cipher algorithm in asymmetric cryptosystems. In order to improve the security level, one needs to increase the length of RSA public key pair before. The characteristic of ECC is that it could use shorter length key to achieve the security level as the longer length key in RSA, e.g., the security level of 205-bit public key pair in ECC is similar to the 2048-bit public key pair 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 (Enge, A, 1999).

2.5.3 Message Digest and Message Authentication

The message digest (MD) and the message authentication codes (MAC) are based on a notion of hashing. 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 (Jason Weiss,2004). 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.

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

Figure 2.13 Architecture of message digest

Another characteristic of hash function is 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, MAC is a type of the hash functions as well; it provides reasonable assurances that the content of a message would not be 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. Additionally, 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 were papers published from RSA Laboratory that describe a weakness in the certain mechanics of the algorithm that might lead to collisions — the violations of collision-free properties we expect for a cryptographic one-way hash. In addition, there is no known documentation that describes how to exploit this information to attack the algorithm. Knowing the risk; hence, there is the suggestion 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 one 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 relationships 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 field. As mentioned earlier, NTCIP follows the ISO-OSI modulus; 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 (Davies, D., and Price, W. ,1989).

● 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. Additionally, 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.

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.

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.

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 Section 2.5, the combinations of decryption procedure are the right key, acceptable ciphertext and decryption algorithm). Therefore, while the TCIS receives the unsuitable

data packets that could not smoothly be decrypted frequently; 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 field 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 realize that a suitable security mechanism establishment is necessary and is an urgent demand in traffic control management system nowadays. 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., to 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 (Scott Oaks, 2002).

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	<ul style="list-style-type: none"> — Simple and small — Fast operation — Security nowadays is insufficiently 	<ul style="list-style-type: none"> — Security might be enough — Complex operation — Hard to implement 	<ul style="list-style-type: none"> — Fast operation — Simple and small — The key length could be changeable 	<ul style="list-style-type: none"> — 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	<ul style="list-style-type: none"> – Long-time development and highly reliability – The mathematical theories of RSA are easy than other asymmetric algorithms. – The representative of asymmetric cryptosystems nowadays 	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – Use the same secret key for encryption and decryption. – Use the same cipher algorithms and secret key in transmitter-side and receiver-side community. 	<ul style="list-style-type: none"> – Use 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	<ul style="list-style-type: none"> – 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 quantities of ciphertexts, one cannot calculate the secret key from these data. 	<ul style="list-style-type: none"> – 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 quantities of ciphertexts and the public key, one still cannot calculate the private key and decrypt the ciphertexts to get the plaintexts further.
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 approach; but the encryption/decryption operations are much slower and more complex 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 (Rich Helton and Johennie Helton, 2004) 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; on the other hand, 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 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 message 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 shall discuss 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 analyze 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. 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 (Jonathan Knudsen, 1999):

i. Security! $\neq$ 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! $\neq$ 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! $\neq$ 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! $\neq$ 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 demand. 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 the period of validity of most traffic commands is 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 3.2 The 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; hence, this research uses Java to implement the protection system as well.

● 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. Additionally, Java code is organized into classes. Each class defines a set of methods from the behavior of an object. A class can inherit behaviors from another class. At the root of the class hierarchy 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 3.1, this research uses four extensions discussed below (Y. Daniel Liang, 2003):

1) 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 attentions to the specialized mathematical calculations of the cryptographic algorithms.

2) Java Secure Sockets Extension (JSSE)

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

3) 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.

4) 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 adds 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. Due to Java is designed to run on small computers such as personal computers with 4Mb of RAM or more originally. Thus, Java is more efficient and is the typical scripting languages, but it is about twenty times slower than C. This, however, 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 discussed 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. On the other hand, it uses asymmetric cryptosystems to transmit or exchange the secret keys and co-operates message digest to ensure the message integrity additionally.

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 cryptosystem. Nevertheless, the definition for “dynamic” of the encryption model is also the point of this research. 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 transmissions. 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 the encryption technique which owns the characteristics above is dynamic encryption technique.

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 $E_{KD(i)}$ is expressed as:

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

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

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

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

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

$$\mathbf{K}_{D(i)} = \mathbf{DKG}(\beta) \quad (3.2)$$

DKG : Dynamic Key Generator

β : The input of the dynamic key generator

and the decryption function can be expressed as Equation 3.3:

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

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, shown as Figure 3.5 which is the framework of DKG, we add a message digest algorithm in it to make the plaintext becomes 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.

These ways could modify some defects of random-number which cryptography usually used to generate secret key or public key pair in computers and have the following advantages:

- 1) 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;

- 2) 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;
- 3) The most notable characteristic of message digest is irreversibility; this means that one cannot figure out the original data form 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 of 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 additionally.

Upon the architecture of this security mechanism; TMIC, which is the transmitter, is sending a message to TCIS, which is the receiver as well. 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 which the TMIC and TCIS operate alternately as below:

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

As TMIC transmits or issues a message to TCIS, TMIC would produce a public key pair which includes a public key $\mathbf{KU}_{\text{TMIC}}$ and a private key $\mathbf{KR}_{\text{TMIC}}$ via the dynamic public key pair generator (DPKG), and then store the private key $\mathbf{KR}_{\text{TMIC}}$ in the TMIC system first. Next, it utilizes the public key $\mathbf{KU}_{\text{TMIC}}$ and password $\mathbf{PW1}_{\text{TMIC}}$ which is originated in a specific number composition to be the input for the message digest algorithm (hash function) $\mathbf{H1}_{\text{TMIC}}$. After the message digest algorithm calculation, we get a message digest $\mathbf{MD1}_{\text{TMIC}}$, and $\mathbf{MD1}_{\text{TMIC}}$ can be expressed by Equation 3.4:

$$\mathbf{MD1}_{\text{TMIC}} = \mathbf{H1}_{\text{TMIC}} (\mathbf{PW1}_{\text{TMIC}} , \mathbf{KU}_{\text{TMIC}}) \quad (3.4)$$

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 need to 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 $\mathbf{M}_k$, $\mathbf{MD1}_{\text{TMIC}}$ and $\mathbf{KU}_{\text{TMIC}}$, namely: sealing them in 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 the 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 $\mathbf{M}_k$, $\mathbf{MD1}_{\text{TMIC}}$ and the received public key from the data packet. Here we call the public key which is received by TCIS is $\mathbf{KU}_{\text{TCIS}}$. Then, the TCIS would make a new message digest $\mathbf{MD1}_{\text{TCIS}}$ which is from

the pre-stored password $PW1_{TCIS}$ and the $MD1_{TCIS}$ given by Equation 3.5.

$$MD1_{TCIS} = H1_{TCIS} (PW1_{TCIS}, KU_{TCIS}) \quad (3.5)$$

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

Figure 3.7 Procedures for data packet restoration and message digest comparison

On the contrary, if $MD1_{TCIS}$ is in agreement with $MD1_{TMIC}$; this indicates that the original public key KU_{TMIC} and the message digest $MD1_{TMIC}$ are not tampered during the transmission period. As represented in Figure 3.8, the TCIS would continue to generate a secret key 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 M_k and confirms the $MD1_{TMIC}$ as well. Next, the TCIS would encrypt this secret key via public key KU_{TCIS} and RSA cipher (see Equation 3.6). Additionally, it generates a new message digest $MD2_{TCIS}$ which is originated from pre-stored password $PW2_{TCIS}$ and

the ciphertext of secret key C_{KS} . Finally, the TCIS now would integrate the ciphertext C_{KS} and $MD2_{TCIS}$ in a byte array and transmit the byte array to TMIC.

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

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

KS_{TCIS} : The secret key which is produced from the TCIS

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 is used 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 the transmitter-side and receiver-side respectively; therefore, attackers would not know the correct password if the transmitter/receiver hosts 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**

Figure 3.10 Procedures for the secret key separation

Figure 3.10 represents that while the TMIC receives the data packet from TCIS, the TMIC would separate the byte array into the ciphertext of secret key C_{KS} and the received message digest $MD2_{TCIS}$. Next, the TMIC proceeds to decrypt C_{KS} to get the secret key by the pre-stored private key KR_{TMIC} and RSA cipher algorithm after a series of processes of user authentication and transmitted object integrity as above steps. So far, both of the TMIC and TCIS own the secret key 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 that 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 be expressed as Equation 3.7.

Figure 3.11 Procedures for the NTCIP object encryption and transmission

Afterward the TMIC would send the byte array which includes the ciphertext of NTCIP object C_{OB} and $MD3_{TMIC}$ that is grated from password $PW3_{TMIC}$ and C_{OB} to TCIS further.

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

$E_{KS,IV}$: The encryption formula for the NTCIP object

M_{OB} with secret key KS_{TCIS} and IV

M_{OB} : The transmitted plaintext of NTCIP object

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 C_{OB} , it needs to confirm the authenticity of the received data by message digest. If the message digest $MD3_{TCIS}$ is acceptable to $MD3_{TMIC}$, then the TCIS would proceed to decrypt the ciphertext of NTCIP object via the pre-stored secret key KS_{TCIS} and initialization vector IV to make the TCIS gains the NTCIP object in conclusion.

Figure 3.12 Procedures for NTCIP object ciphertext decryption

Figure 3.13 Flow chart of the security mechanism of this research

Thus far, both of the TMIC and TCIS own the secret keys securely by a security channel. Then the TMIC would encrypt NTCIP objects into ciphertexts and transmit them to the assigned TCIS. 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. Viewed in this light, the public key KU_{TMIC} in this security mechanism could also not need to be protected during the public key transmission from TMIC to TCIS.

Nevertheless, one might intercept and tamper with the public key to be the ones-owned if one knows the public key algorithms and key length; therefore, this research utilizes the message digest and multiple security protections to enhance the security for the public key during public key 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. Without exception, the security is the important point for this security mechanism and the security analysis might include two categories roughly, namely: analysis of security protection and cryptanalysis. Following discussions are the security analysis of the security mechanism in this research.

3.5.1 Analysis of Security Protection

As mentioned earlier, this security mechanism utilizes a hybrid cryptosystem that

combines 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 might threaten for ATMS data transmission, e.g., the data packet interception, masquerade, eavesdropping, message modification and etc; and the major conceptions of this security mechanism establishment are to ensure the confidentiality, integrity and authentication of transmitted data. Next, we shall discuss on the above issues and discuss how to withstand these attacks in focus via this security mechanism.

● Data Confidentiality

The goal of data confidentiality is to ensure the transmitted data would not be peeked by illegal one; hence, this security mechanism utilizes a set of hybrid cryptosystem to achieve it. The hybrid cryptosystem of this research modifies the weakness of symmetric cryptosystems in secret key exchange and protection. Besides, the AES cipher which this security mechanism used in symmetric cryptosystem adopts the CBC cipher mode, and the CEC cipher mode usage improves the secure protection a lot and increases the security level sufficiently as well.

However, the security level is secure sufficiently or not might be dependent on the cryptanalysis; therefore, we shall discuss about the cryptanalysis of the security mechanism of this research later. Generally speaking, a well (secure enough) security mechanism makes attackers crack hardly or they can only own the ciphertexts and cannot know the plaintext clearly even if they steal the data packet from the transmission channel as well. Due to these, system managers could make use of this security mechanism to avoid

attackers to eavesdrop, modify or reply the correct content of transmitted data easily by these ways.

● 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. That is because the methods of data integrity are usually used to confirm whether the received data is correct or not even if there is a security mechanism already added between the transmission processes. In other words, TCIS could make sure the received data packet is the true one which is not modified by attackers and is sent from the right TMIC by the methods.

From the architecture of the security mechanism in the above section, the transmitters would generate and transmit a message digest of transmitted ciphertext before each transmission process respectively; and the receivers need to create the corresponding message digest which is originated from the received data and the pre-stored password 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 security mechanism should possess to resist and avoid the attackers tamper the transmitted data or modified them; and the message digest algorithm usage provides the further protections for data transmission and resist some attacks, namely: masquerading, message modification, man-in-the-middle attacks effectively.

● User Authentication

The user authentication in cryptography is to ensure the both of the principals (transmitter/receiver) are the true one, not the impostors essentially. The asymmetric cryptosystems could be used for user authentication thus. For instance of this security mechanism; TCIS utilizes the public key to encrypt the plaintext of secret key, and only the opposite TMIC could use the right private key to decrypt the ciphertext additionally.

On the other hand, this security mechanism also adds four sets of passwords (three of these are for message digests and one is the initialization vector) both in the TMIC and in the TCIS respectively. As the Figure 3.9 shown, these two message digests come from not only the transmitted/received data but also from the according pre-stored passwords in the comparative processes of message digests.

In addition, due to the host protections of TMIC and TCIS are not the concerns of this research. Therefore, on the basis of this, we assume that either TMIC or TCIS is not invaded and protected well, attackers cannot create the right message digests without knowing the correct passwords. The attackers are almost impossible to crack these passwords easily even if they use brute-force attack with the unknown number of characters or number combinations. Hence, this security mechanism uses the above mechanism to ensure the access control and the authentication of user identifications to avoid 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 CBC cipher mode in the AES algorithm. Figure 3.14 represents the electronic code book (ECB) cipher mode and the CBC cipher mode as well; 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.

Figure 3.14 ECB cipher mode and CBC cipher mode

As Figure 3.14 shown, 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 Table 3.1 shown, if the message happens to contain identical blocks (in this example, each of the block is 16 bytes), then the identical blocks of the

ciphertext are produced. The advantages of ECB are that the plaintexts do not need to be encrypted linearly, since, each block is independent, and the operation of ECB cipher mode is fast. However, it is by far the weakest cipher mode due to no attempt is made to hide patterns in the plaintext and the identical block generation of the ciphertext.

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]

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]

The CBC cipher mode introduces a feedback mechanism into the encryption process such that each block is dependent on all of the previous blocks before it. CBC employs an XOR operation (a logical operation exclusive disjunction) between the plaintext and the previous ciphertext block, as demonstrated in Figure 3.14. 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 the example shown in Table 3.2, this example uses the same plaintext blocks and identical secret key as Table 3.1; however it results different ciphertext blocks for each identical plaintext block.

In addition, as a result of the initialization vector **IV** is needed to prime for the encryption operation and the **IV** has no meaningful relation to the plaintext. In fact, its sole purpose is to populate the feedback registers inside of the cipher mode box because there was 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 of the right secret key and identical **IV** for the encryption/decryption process at the same time; therefore, the **IV** could be assumed the second secret key of the encryption/decryption process as well. In view of these, the security mechanism of this research pre-stores the according **IV** in each host of TMIC and TCIS to improve the security level even if the attackers catch 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 Tables 3.1 and 3.2, even we use the same secret key and feed the same plaintext into the same cipher, it would result a lot of differences between ciphertexts and plaintexts in the CBC. Therefore, attackers cannot crack the ciphertexts easily due to CBC cipher mode would generate the

irregular blocks of 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 detail 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 known by attackers, namely: ciphertext only, known plaintext, chosen plaintext, chosen ciphertext and chosen text. In which, the ciphertext only is the difficult method to be cracked due to attackers might only know the fewer secret information as encryption algorithms and ciphertexts. Furthermore, the encryption algorithms of symmetry cryptosystem (e.g., AES) and asymmetry cryptosystem (e.g., 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, the AES algorithms and RSA algorithms nowadays cannot be cracked by these attacks efficiently and these two cipher algorithms are used in this research as well. Hence, 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 certain attacks of cryptanalysis well and the security might be enough sufficiently.

3.5.3 Brute-Force Attack

In many attacks as message modification or message reply, if one could not crack the security protections by utilizing cryptanalysis approaches, one might finally

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 other words, the method is just trying and trying until finding out the right secret key combination. Generally, the test frequency requirements for finding out the secret key combination successfully would be about half numeral values of the secret key quantity. Table 3.3 shows the consuming time in carrying out the brute-force attack for the different computer computation-capability and the different length of secret key.

Table 3.3 Time-consuming for cracking cipher algorithms by brute-force attack
(William Stallings, 2004)

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

ms: milliseconds

In Table 3.3, it shows the test results of the four different lengths of secret keys, namely: 32 bits, 56 bits for AES, 128 bits for DES, 168 bits for Triple-DES, and the secret key that 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, the security level of it might not be enough sufficiently for ATMS data transmission. On the other hand, the security level of the 56-bit, 128-bit, and 168-bit secret keys might be sufficiently enough under this level of computer computation-capability that attackers used for real conditions.

However, attackers might not only utilize 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 column 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 might crack the cryptosystem via utilizing the 56-bit secret key in 10 hours and the 128-bit secret key for AES cipher algorithm which this research used could resist being cracked for almost 5.4×10^{18} years normally. Hence, the 128-bit AES secret key is sufficiently enough to resist the brute-force attack and satisfy with the demands of ATMS data transmission 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 ATMS 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 in next chapter.

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

Table 3.4 Effects of the dynamic security mechanism

Mechanism	Application	Purpose
AES Cipher	— Fast encryption/decryption operations for transmitted data	Data confidentiality
	— 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	
RSA Cipher	— Modify the defects in secret key transmission and protection of symmetric cryptography	Data confidentiality/ Data integrity
	— Certain 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	
CBC Cipher Mode	— Result the distinct ciphertext	Data confidentiality/ User authentication
	— IV could be treated as another secret key to improve the security protections and ensure the identity of user as well	
Message Digest Algorithm	— Make sure the transmitted message is not modified and the received message is right and correct	Data integrity
	— Make attackers cannot guess the original plaintext by using the message digest in DKG	
Pre-stored Password	— Confirm the identity of users to avoid attackers masquerade system managers	User authentication
DSKG/DPKG	— Improve the weaknesses of PRNG	Data confidentiality/ Data integrity
	— Generate different and irregular secret information for each transmission	

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 or traffic policies 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 introduced the conceptions and the framework of DSM and discussed 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 operation 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, 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 in transmission and encryption/decryption procedures;
- The different communications media would provide different bandwidth, and it might influence the efficiency and stability in data transmission further;

- The length of secret key or public key pair might be the direct proportion to the negative-effect increment;
- The tight frequencies in message dispatch might increase more loading 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 additionally. 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 equation $\mathbf{R}_e$ 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 $\mathbf{R}_e$ can be expressed by Equation 4.1.

$$\mathbf{R}_e = \{C_m, KS_l, KP_l, M_s, M_f, C_c\} \quad (4.1)$$

$\mathbf{R}_e$: The regression equation from the factors below

C_m : The factor for communications media

KS_l : The factor for AES secret key length

KP_l : The factor for RSA 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 TCIS

4.3 Experiment Environment

4.3.1 Scope of Simulated Experiment

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

Figure 4.2 Framework of ATMS data transmission

● Procedure for encoding

The procedure describes that TMIC encodes the NTCIP object according to encoding rules (e.g., EBR, OER, etc) to make the object 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 that the secret key and NTCIP object are fed into the cipher to make the NTCIP object transform into the ciphertext via encryption algorithms before transmission.

- **Procedure for data transmission**

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

- **Procedure for decryption**

The procedure describes the ciphertext transformation into the original NTCIP object while the ciphertext is received by TCIS.

- **Procedure for decoding**

The procedure describes that the NTCIP object is 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 experiment procedures upon these 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 operation efficiency and saving testing 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 <u>Q9400@2.66GHz</u>
		RAM	5GB
		OS	Microsoft Windows XP Professional SP3
2	TCIS-i	CPU	Intel(R) Core(TM)2 Quad CUP <u>Q9400@2.66GHz</u>
		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 decided 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 additionally, 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 simulated 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
▪ Communications 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 generally; 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
▪ Communications 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, STMP is the variation of SNMP and is the exclusive communications protocol for NTCIP as well. Both of the STMP and SNMP use MIBs to carry out the data management. Basically, we could use the STMP syntax to make the NTCIP objects become suitably for transmission via a process termed coding. Practically, the coding 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 out the influence 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 Tables 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 usages, 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 simulated NTCIP objects of these experiments.

Table 4.5 NTCIP Object No.01 — trafficControl Code

Object Name	Traffic Control
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
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
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
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
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
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
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 major goal of these experiments in this research is to know the degree of the negative-effect generation due to the DSM addition and set up regression equations which can represent the relationships between the variables as given in Equation 4.1. Therefore, in this research, the experiments are designed under the different communications media; the goal of this way is to understand the delay in data transmission by different communications media and provide the results for engineers or managers in security design further.

4.4.1 Experiment Methodology

In order to make these experiments operate effectively, this research uses computers to displace and simulate the real-TMIC and the real-TCIS in the traffic control system. This method could let us control the data dispatching and receiving rightly and take down the point of time in encryption, decryption and transmission procedures precisely as well. In addition, in behalf of the real condition simulation in the wired network with the ISP usage, we move the equipments out of the campus 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. Figures 4.6 (a) and (b) show the experiment situations and used equipment installations at Transportation Lab. in NTU campus and out of the NTU-campus respectively. Figure 4.7

represents the VPN connection procedure as well;

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 consuming time of each procedure in data transmission and encryption/decryption operations. Figures 4.9 and 4.10 are the displays 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

Figure 4.7 VPN connection procedures

Figure 4.8 Network Time Calibration Software — NTPClock

Figure 4.9 Display of DSM programming operation

Figure 4.10 Display of note items

● Programming operation procedure

Figure 4.11 Operation procedures of DSM

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) TMIC 1-1 : Produce the $\mathbf{MD}_{\text{Object}}$ from the transmitted NTCIP object;
- 2) TMIC 1-2 : Generate the public key pair via DPKG;
- 3) TMIC 1-3 : Create the $\mathbf{MD1}_{\text{TCIS}}$ from $\mathbf{KU}_{\text{TMIC}}$ and $\mathbf{PW1}_{\text{TMIC}}$;
- 4) Socket 1 : Transmit the $\mathbf{MD1}_{\text{TMIC}}$, $\mathbf{KU}_{\text{TMIC}}$ and $\mathbf{M}_k$ to TCIS;
- 5) TCIS 1-1 : Produce the $\mathbf{MD1}_{\text{TCIS}}$ and compare with the $\mathbf{MD1}_{\text{TMIC}}$;
- 6) TCIS 1-2 : Generate the secret key $\mathbf{KS}_{\text{TCIS}}$ via DSKG;
- 7) TCIS 1-3 : Encrypt the $\mathbf{KS}_{\text{TCIS}}$ by $\mathbf{KU}_{\text{TCIS}}$;
- 8) TCIS 1-4 : Create the $\mathbf{MD2}_{\text{TCIS}}$ from $\mathbf{C}_{\text{KS}}$ and $\mathbf{PW2}_{\text{TCIS}}$;
- 9) Socket 2 : Transmit the $\mathbf{MD2}_{\text{TCIS}}$ and $\mathbf{C}_{\text{KS}}$ to TMIC;
- 10) TMIC 2-1 : Produce the $\mathbf{MD2}_{\text{TMIC}}$ and compare with the $\mathbf{MD2}_{\text{TCIS}}$;
- 11) TMIC 2-2 : Decrypt the $\mathbf{C}_{\text{KS}}$ by $\mathbf{KR}_{\text{TMIC}}$ to own the $\mathbf{KS}_{\text{TCIS}}$;
- 12) TMIC 2-3 : Encrypt the NTCIP object by $\mathbf{KS}_{\text{TCIS}}$;
- 13) TMIC 2-4 : Create the $\mathbf{MD3}_{\text{TMIC}}$ from $\mathbf{C}_{\text{OB}}$ and $\mathbf{PW3}_{\text{TMIC}}$;
- 14) Socket 3 : Transmit the $\mathbf{MD3}_{\text{TMIC}}$ and $\mathbf{C}_{\text{OB}}$ to TCIS;

15) TCIS 2-1 : Produce the $\mathbf{MD3_{TCIS}}$ and compare with the $\mathbf{MD3_{TMIC}}$, and;

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

Note:

The Socket 1, Socket 2 and Socket 3 here are calculated from the data sealing process by transmitters until to the unsealing process by receivers; hence, the total time-consumption of these three segments can be expressed as below:

$$\mathbf{Socket = (Data\ packet\ sealing) + (Data\ packet\ transmission) + (Data\ packet\ unsealing)} \quad (4.2)$$

● **Note items**

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

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 the efficiencies of data transmissions and device operations due to the differences in NTCIP object size, namely:

- 1) Confirm the NTCIP object size M_s is one of the causes of negative-effect generation in data packet transmissions or device operations of TMIC and TCIS;
- 2) Discuss whether the DSM addition would influence the data packet transmission or not, and;
- 3) Compare the efficiencies of data packet transmission upon the different communications media.

● Test Objects and Methodologies:

In this experiment, we utilize computers no. 1 and no. 3 to respectively simulate TMIC and TCIS, 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 twenty-eight test conditions and over three 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 objects 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*	: Objects 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

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 length combinations of AES secret key and RSA public key pair

- **Test Purpose:**

As described in Chapter Three, DSM is constructed from the hybrid cryptosystem which combines with the AES cryptography and RSA cryptography. Taken in this light, this could modify the weaknesses both in the symmetric cryptosystems and in the asymmetric cryptosystems and provide multiple secured protections for the ATMS data transmission as well. 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 might consume more system resources and also bring more negative-effects for the core system. From these reasons, this experiment is designed to verify the relationships between the AES secret key length KS_l and RSA public key pair length KP_l , and discuss whether the different communications medium usage C_m is the effective factor for the device operation of TMIC and TCIS further.

- **Test Objects and Methodologies:**

As Experiment One represented, Experiment Two also utilizes computers 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 130 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 RSA public key pair length through the different

communications media, and the fixed factors are the transmitted object size, interval of object dispatch and the TCIS device usage. Hence, there would be total night secret information combinations in this experiment.

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 as the simulated TCIS at laboratory. In addition, it is convinced that the DSM

addition would consume more sources from the core system, and the tight interval of the NTCIP object dispatch might increase more loading for network transmissions. Taken in this light, 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 as well.

● **Test Objects and Methodology:**

The main differences between Experiment Three and the two experiments above are that it utilizes four 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 be the simulated TMIC device and the communication medium usages are the wired network and the 3.5G mobile communications under the VPN framework as well.

As Figure 4.14 shown, there are total forty test conditions in this experiment and detail 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 simulated computers of TCIS and the communication media, 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

Figure 4.14 Framework of Experiment Three

4.5 Expected Outcomes

As mentioned above, people invariably tend to concern about the security and ignore the system operation efficiency by contrast. Of course, the security is quite important and essential for a security mechanism without doubt. However, upon the security requirements, one should be interested in the operation efficiencies of the core systems further. 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 shown as below:

- From the notions of computer usages, the larger size of transmitted objects might cause the more delays in data transmissions and device operations as

well; therefore, we infer that the NTCIP object size would influence the efficiencies of the network transmissions and device operations;

- The different communications media would possess the differences in network bandwidth, and it might influence the whole operation efficiency of DSM due to the diversity delays in transmission; generally speaking, we believe that the wire network communications would be better and stable than 3.5G mobile communications;
- There are much research and studies to support that the operation efficiencies of symmetric cryptosystems are better than the asymmetric cryptosystems. Hence, we expect that the 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 operations 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 narrower 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 C_c , the interval of object dispatch M_f , the DSM addition, the NTCIP size M_s , and the length of AES secret key KS_l and RSA public key pair KP_l .
- Transmission delay: the computation-capability of TCIS devices C_c , the interval of object dispatch M_f , different communications media C_m , and the NTCIP size 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 results further. The goals of these experiments are to test and verify the potential factors in operation delay and transmission delay in between the DSM operations and set up the regression questions which represent the influences and relationships between these factors via these test results.

In additions, due to the DSM programming has to perform the initialization procedure while 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 signifiante lever of $\alpha=0.050$.

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 Figures 5.1, 5.3 and 5.4 shown; certain factors as C_e , KP_l and M_f which deal with the device computation-capability present the queue and delay phenomenon 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 the DSM operation.

Figure 5.1 DSM operation in different computation-capability TCIS devices

Table 5.1 Crack points of continuous DSM operations (C_c)

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

Table 5.1 shows the crack points (frequency of DSM operations) of the continuous operations of DSM under the condition while $M_f=10$ seconds, $KS_l=128$ bits and $KP_l=1024$ bits. 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 which is calculated via linear equation from those crack points further.

$$Y_1=0.02X_1+109.83 \quad (5.1)$$

Y_1 : Crack point for the continuous operations of C_c

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 the continuous operations of DSM in different public key pair length under the condition while C_c = TCIS-iii , KS_t = 128 bits and M_f = 10 seconds thus.

Figure 5.3 DSM operation in different RSA public key pair length

Table 5.2 Crack points of continuous DSM operations (KP_I)

KP_I	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 continuous DSM operations (M_f)

M_f (second)	2	5	10	30	60
Crack Point	117	121	125	141	179

Besides, the interval of NTCIP object dispatch is also the critical factor of the queue phenomena generation and it could be shown as Figure 5.4, and Table 5.3 indicates the crack points of the continues operations of DSM under the condition while C_c =TCIS-iii , KS_I =128 bits and KP_I =1024 bits additionally. Next, Figure 5.5 represents the trend line of the crack points for the change in object dispatch interval and it can be expressed by Equation 5.2 which is calculated via linear equation from those crack points as well.

$$Y_2 = 1.07X_2 + 114.86 \quad (5.2)$$

Y_2 : Crack point for the continuous operations of M_f

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 describe the relative importance of the delay effects under these factors and explain 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 test data of each condition of these three experiments

5.3 Data Analysis of Experiment One

The analysis shows that whether the NTCIP object size is the noticeable factor both in device 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

Tables 5.4 and 5.5 represent the statistic descriptions and the test results of the time-consumption under the different object size transmission respectively, and Figure 5.6 is the line graph of the mean time-consumption of object transmission in different sizes with different communications media additionally.

Table 5.4 Statistic Descriptions of Analysis 1-1

Communications Medium	DSM Addition	Mean(ms)	Std. Deviation	N
3.5G Mobile	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 time-consumption of NTCIP object transmission 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 as 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 results can be shown as Table 5.6 and Equation 5.3 from the observations in Table 5.5.

Table 5.6 Regression equation analysis of Analysis 1-1

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

^a Computed using alpha = .05

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

^c R Squared = .268 (Adjusted R Squared = .268)

According to the results 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:

$$\hat{\mu}_{Analysis1-1} = 258.988 + 91.668(if : C_m = 3.5GMobile) - 36.753(if : W / ODSM) + 0.025 * M_s \quad (5.3)$$

Thus, in response Equation 5.3:

- 1) The value 258.988 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 time-consumption of the data transmission, it would decrease 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 $0.000 < 0.050$; therefore, the DSM addition is the effective factor in data packet transmission as well;

- 3) The coefficient of C_m indicates the change in mean time-consumption of the data transmission, it would increase 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 C_m is $0.000 < 0.050$; therefore, the communications medium usage is also the effective factor in data packet transmission, and;
- 4) The P-value of M_s is 0.130 and is greater than 0.050; 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 represent that the transmitted object size is not the effective factor in data transmission delay. Furthermore, this section shall analyze whether the object size is the noticeable factor in encryption or decryption operations.

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

Object Size	Encryption Operation			Decryption Operation		
	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 5.7 lists the descriptive of statistics and observed mean of the consuming time both of the encryption and decryption operations and the changes in mean values could be illustrated as Figure 5.7 as well.

Next, Tables 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 further; 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 of Analysis 1-2 (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 (M_s)	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 (M_s)	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 M_s is 0.435 and is greater than 0.050; 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 M_s is 0.537 and is greater than 0.050 as well; hence, the transmitted object size is also **not** the effective factor in decryption 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 in wired network would be faster than in 3.5G mobile communications due to the bandwidth of 3.5G mobile communications is not as wide as wired network that the experiments use.

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 effective factors in device 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 length combinations of AES secret key and RSA public key pair for the influence of data packet transmission delay, and;
- Analysis 2-2: Analysis in the length combinations of AES secret key and RSA public key pair for the influence of device operation delay.

Besides, as the previous analyses, the following analyses are also analyzed by the ANOVA approaches under the significance level of $\alpha=0.050$.

5.4.1 Analysis in the length combinations of AES secret key and RSA public key pair 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 approach 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.

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

Furthermore, the statistic descriptions and observed mean of device operations are listed in Table 5.10.

Table 5.10 Observed mean of the consuming time of data transmission

AES secret key	RSA public key pair	Mean(ms)	Std. Deviation	N	C_m
128-bit	768-bit	273.0900	63.70511	200	
	1024-bit	456.9450	200.70587	200	
	2048-bit	329.7617	74.53122	200	
	Total	353.2656	149.98786	600	

192-bit	768-bit	308.9067	73.25927	200	3.5G mobile + Wired Network Communication
	1024-bit	257.5400	66.57431	200	
	2048-bit	340.9783	253.19649	200	
	Total	302.4750	160.42620	600	
256-bit	768-bit	289.8800	78.83528	200	
	1024-bit	286.3517	77.39280	200	
	2048-bit	402.3217	283.58357	200	
	Total	326.1844	183.51302	600	
Total	768-bit	290.6256	73.55580	600	
	1024-bit	333.6122	156.84986	600	
	2048-bit	357.6872	225.56466	600	
	Total	327.3083	166.44453	1800	

Finally, the analysis results are shown in Table 5.11 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

H₁: The 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:

H₀: The AES and RSA operations would **not** possess the noticeable interaction effects in data packet transmission delay

H₁: The AES and RSA operations would possess the noticeable interaction effects in data packet transmission delay

Table 5.11 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 5.11 are all higher than 0.050; 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 length combinations of AES secret key and RSA public key pair for the influence of device operation delay

Analysis 2-1 tested 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 still not the effective factors in operation delay. This analysis uses the Two-Way ANOVA approach 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. The statistic descriptions and observed mean of device operations are listed in Table 5.12. Besides, in order to test the influences upon the device operations and changes in key length 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.

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

Table 5.12 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
	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	+ Wired Network Communication
	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 5.12 shown, the communications medium usages of the observed data are not only upon the 3.5G mobile communications but also upon the wired network as well. There is no proof indicates that the communications medium usage would not influence the operations of AES and RSA. Therefore, we should test this consideration first via the One-Way ANOVE approach. The analysis results and alternatives are shown in Table 5.13 as below.

The alternatives for C_m and AES/RSA operations are:

H_0 : The communications medium usage C_m is **not** the noticeable factor in device operations

H_1 : The communications medium usage C_m is the noticeable factor in device operations

Table 5.13 One-Way ANOVA Table of 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
C_m	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 5.13 indicate that the communications medium usage C_m is not the effective factor in device operations of AES and RSA due to the P-value of C_m here is $0.377 > 0.050$.

Next, we continue to the analysis above; the analysis results of Analysis 2-2 are shown in Table 5.14 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

H₁: 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:

H₀: The AES and RSA operations would **not** possess the noticeable interaction effects in device operation delay

H₁: The AES and RSA operations would possess the noticeable interaction effects in device operation delay

Table 5.14 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 0.183>0.050. In addition, there is no interaction effect between AES and RSA 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 noticeably. Table 5.15 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 Figures 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 attentions on this point more.

Table 5.15 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 computation-capability of devices might cause more negative-effects for the core

system and network transmission as well. The objectives of the following analyses in this section are to confirm and discuss these considerations, namely:

- 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 analysis objects certainly; the time-consumption of data packet transmissions and device operations in this section are respectively adopted as the same as Equations 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 the influence of device operation delay

According to the test results in Analysis 2-2, it indicated that the different communications medium usages would not influence the device operation noticeably. Take in this light, we proceed to understand the relationships between C_c and M_f in the operation efficiencies of devices without the distinctions between the communications medium usages further. Table 5.16 shows the observed mean of device operations in different C_c and M_f of Analysis 3-1.

Table 5.16 Observed mean of device operations (Analysis 3-1)

C_c	M_f	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	

According to Table 5.16, the relationships between C_c and M_f can be illustrated as Figures 5.10 and 5.11. We can clearly know that the device operation delay might be influenced by C_c more, and the lower C_c might operate slower.

Figure 5.10 The mean comparison of the factor in C_c (Analysis 3-1)

Figure 5.11 The mean comparison of the factor in M_f (Analysis 3-1)

Next, Table 5.17 shows the analysis results which are analyzed by the Two-Way ANOVA approach and the alternative conclusions for the test are below:

The alternatives for the analysis of the different computation-capability of TCIS device operations (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 (M_f) 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 C_c and M_f are:

H_0 : The C_c and M_f would **not** possess the noticeable interaction effects in device operation delay

H_1 : The C_c and M_f would possess the noticeable interaction effects in device operation delay

Table 5.17 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
C_c	6.728E9	3	2.243E9	10124.854	.000
M_f	885994.784	4	221498.696	1.000	.406
$C_c * M_f$	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 (M_f) is **not** the effective factor in device operations due to the P-value of M_f is $0.406 > 0.050$. On the other hand, because of the P-value of C_c is $0.000 < 0.050$. Therefore, the factor in the computation-capability of TCIS devices might be the noticeable factor in device operation delay further, and these results also confirm to Figure 5.10 additionally. Besides, the M_f and C_c would not have interaction effects between them due to the P-value of $C_c * M_f$ is $0.711 > 0.050$.

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

Although the interval of object dispatch M_f is not the noticeable factor in device operations, but it does not mean that it would also not influence the delay in data packet transmission. Hence, Analysis 3-2 is to test the conditions for both of M_f and C_c in data packet 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 the DSM addition at least. Therefore, the analyses below are discussed on the factors in differences in the communications media (C_m), the interval of object dispatch (M_f) and the compitaion-capability of TCIS devices (C_c) via the muliple regression equation as Table 5.19 and Equation 5.6 shown.

First, the statistic describuations of Analysis 3-2 are listed in Table 5.18 and Figure 5.12 illustrates that the relationships between M_f and C_c , we could know that the C_c and M_f might be the factors in data packet transmission by this figure.

Table 5.18 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 represeption of the factor in C_c (Analysis 3-2)

Table 5.19 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
[$C_m=Wired\ Network$]	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	.	.	.
[M_f]	-.702	.076	-9.288	.000

^a Computed using alpha = .05

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

^c R Squared = .201 (Adjusted R Squared = .200)

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

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

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., C_m , C_c and M_f) and the responses are described as following.

- 1) 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;
- 2) The coefficient of C_m indicates the change in mean of different communications medium usages, it would increase 89.620 ms while the 3.5G mobile communications usage and all the other independent variables remain constant;
- 3) The compilation-capability would also be the noticeable factor in data packet transmission as well, and;
- 4) The tight interval of object dispatch might cause more loading for network transmission; therefore, it would reduce 0.702 ms when 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 C_c would not only influence the device operations but also affect the data packet transmission as well. In addition, according to Equation 4.2 (see as page 97), the time-consumption of data transmission (socket processes) in this research is caculated from the procedures in data packet sealing by transmitters, data packet transmission by Enternet and data packet unsealing by servicers; therefore, the lower computation-capability would cause the more negative-effects in sealing

and unsealing procedures for the devices. This explanation not only interprets that the factor C_c is one of the noticeable factors in data packet transmission but also confirms that why the DSM addition would influence the data packet transmission in Equation 5.3 due to the DSM addition would cause more loading for the core systems and the sealing/unsealing operations further.

On other hand, the time-consumption of data packet transmission is explained by Equations 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 5.6, we can get the formula as Equation 5.7.

$$\hat{\mu}'_{Analysis_{3-2}} = 258.891 + 89.620(\text{if : } C_m = 3.5G\text{Mobile}) \quad (5.7)$$

Equation 5.7 accords with the results in Equation 5.3 without the ineffective factor M_s further. Hence, in this condition, 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. Therefore, the means of data packet transmission in wired network and in 3.5G mobile network are around 258 ms and 345 ms respectively. Finally, Table 5.20 shows the analysis results for all the considered factors (i.e., C_m , KS_t , KP_t , M_s , M_f and C_c) from the above analyses.

Table 5.20 Analysis results of C_m , KS_t , KP_t , M_s , M_f and C_c

Item \ Factor	C_m	KS_t	KP_t	M_s	M_f	C_c
Device Operation Delay	-	-	⊙	-	-	⊙
Data Transmission Delay	⊙	-	-	-	⊙	⊙
Interaction effect with C_c	-	⊙	⊙	-	⊙	-

⊙: The noticeable and effective factor

As Figures 5.10 and 5.12 shown, the factor in computation-capability C_c is the important and major factor for the whole DSM operations, it would influence all the operation procedures of DSM. Besides, 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 the 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 mechanism 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, these showed that there would be no interaction effect between the device operations and data packet transmissions in DSM operations, but the device computation-capability would be the noticeable factor for both of them. Due to these, we can deem that the device operations and data packet transmissions are the independent factors under the fixed computation-capability devices of TCIS and TMIC. Therefore, the regression equation below are considered and discussed for the efficiencies of DSM operations under the simulated TMIC in computer no.1 and simulated TCIS in computer no. 2. We utilize the test results of these three experiments to figure out the regression equation which includes the factors in C_m , KS_l , KP_l , M_s , M_f and C_c further. The statistics descriptions are shown in Table 5.21 and, the analysis results are represented as Table 5.22 and Equation 5.8 additionally.

Table 5.21 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 5.22 Regression equation analysis of DSM operation

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

^a Computed using $\alpha=.05$ ^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.

$$\hat{\mu}_{DSMoperation} = 5142.129 - 67.108(\text{if : } KS_I = 128\text{bits}) - 2248.678(\text{if : } KP_I = 1024\text{bits}) + 93.501(\text{if : } C_m = 3.5G\text{Mobile}) + 0.243M_s - 5.653M_f \quad (5.8)$$

Because of the P-value of M_s is 0.256 and greater than 0.050 a lot; therefore, it is unnecessary to consider the factor M_s in DSM operations. Hence, Equation 5.8 can be represented as Equation 5.9 further.

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

Thus, in response Equation 5.9:

- 1) The value 5142.129 is the intercept of DSM operation, it indicates that the maximum mean of the distribution of the time-consumption for a cycle of the DSM operation;
- 2) Although the P-values of KS_l are greater than 0.050; however, this would influence the decryption procedure in TCIS device operations as well. Therefore, we deem that we should consider this factor of DSM operations. The coefficient of KS_l indicates that the changes in mean of the AES operation of DSM operations upon the criterion in 256-bit secret key. For instance, it would reduce 67.108 ms and 55.808 ms while one uses the 128-bit and 192-bit secret key respectively;
- 3) The coefficient of KP_l indicates that the changes in mean of the RSA operations of DSM operations upon the criterion in 2048-bit public key pair. For instance, it would reduce 2248.678 ms and 2672.103 ms while one uses the 1024-bit and 768-bit public key pair respectively. In addition, due to the P-value of KP_l is $0.000 < 0.050$; therefore, KP_l is the noticeable factor for DSM operation, and;

- 4) From the coefficient of M_f , we clearly understand that the tight interval of object dispatch would cause more negative-effects for the core system, it would deduce 5.653 ms while M_f increases one second and all the other independent variables remain constant.

Finally, Table 5.23 lists threshold values of the DSM operation efficiency for each secret information combinations from Equation 5.9. Each bracket indicates the maximum and minimum consuming time of ATMS data transmission under the DSM addition while $M_f=2$ seconds and $M_f=60$ seconds respectively. This table provides the security designers or engineers a reference to choose the suitable requirements for data security to their system.

Table 5.23 The threshold values of DSM operation efficiency

			RSA Public Key Pair		
			768-bit	1024-bit	2048-bit
Wired Network	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]
3.5G Mobile Network	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]

Unit: milliseconds

CHAPTER SIX

CONCLUSIONS AND FUTURE RESEARCH

6.1 Conclusions

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

- All of the experiments of this research use computers to simulate TMIC and TCIS; the purposes are to make the test efficiently, and it might have some differences in the real conditions. However, this research provides a conception for the information security in ATMS data transmission;
- 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.
- The DSM is basic upon the hybrid cryptosystem which is composed of symmetry cryptosystems and asymmetry cryptosystems. In which, there is no useful techniques in cracking the RSA and AES algorithms in a short time

nowadays even though the brute-force attack. In addition, as shown in Table 3.3, attackers might need to spend over 10 hours to crack the 56-bit secret key of AES algorithms by the high computation-capability computers via the brute-force attack. On the other hand, the data transmission in ATMS or traffic control is real-time. Therefore, the 128-bit AES 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 pre-stored passwords at each host as well; therefore, one could not masquerade the transmitters or receivers easily by the way. Besides, from the test results of these experiments represent that the message digest operations cause lesser negative-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 one cracks the secure random number generator to provide more protections for the data transmission 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 that the AES operations are not the noticeable factor for the DSM operations; however, as shown in Figure 4.1, the NTCIP decryption procedures occupy almost 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 are commonly 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 length of 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 length of AES secret key to improve the security level for the security mechanism;

- We confirm that the computation-capability of devices is the main factor in the DSM operations by the results of Experiment Three;
- Experiment Three showed that the device computation-capability here is 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 or bandwidth 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 operational limitations of DSM for the continuous operations, and;
- Figure 6.1 represents the time-consumption of DSM operations under the different factor combinations; one could choose the suitable combination for the demands and design the security mechanism by the data 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. 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 wired network and the 3.5G mobile communications; however, different ISP might cause different results in data transmission efficiencies and influence the DSM operations further;
- 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 hosts are invaded by attackers. Hence, the better way is to manage the secret information via the third parts, but it would need additional payments, and;
- 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.

REFERENCES

1. Boneh, D. (1999), “Twenty Years of Attacks on the RSA Cryptosystem”, Notices of the American Mathematical Society, USA.
2. Coppersmith, D. (1994), “The Data Encryption Standard (DES) and Its Strength against Attacks”, IBM Journal of Research and Development.
3. Davies, D., and Price, W. (1989), Security for Computer Networks, New York Wiley Publishers, USA.
4. Hevia, A., and Kiwi, M. (1999), “Strength of Two Data Encryption Standard Implementations Under Timing Attacks”, ACM Transactions on Information and System Security, USA.
5. Institute of Transportation. MOTC, Taiwan (2008), ITS Related.
[Online]Available:
<http://www.iot.gov.tw/english/ct.asp?xItem=106040&CtNo=1407>
[Access Data 23/10/2008]
6. Intelligent Transportation Society of America (2008), ITS Knowledge Resources.
[Online]Available:
<http://www.itsa.org/itsknowledgeresources.html>
[Access Data 11/11/2008]
7. Jason Weiss (2003), Java Cryptography Extensions, Morgan Kaufmann Publishers, UK.
8. Joint Standard of AASHTO, ITE and NEMA (2001), National Transportation

- Communications for ITS Protocol and Simple Transportation Management Framework, NTCIP Joint Standards Committee, Draft Version 01.12, USA.
9. Joint Standard of AASHTO, ITE and NEMA (2002), “National Transportation Communications for ITS Protocol (NTCIP) Guide”, NTCIP Joint Standards Committee, Draft Version 03.02b, USA.
 10. Jonathan Knudsen (1999), Java Cryptography, O'REILLY, USA.
 11. Liu, Yi-Chieh (2006), “Information Security Algorithm for ATMS Data Transmission through Internet”, Master Thesis, National Taiwan University, Taiwan.
 12. Rich Helton and Johennie Helton (2004), JavaTM Security Solutions, Wiley Publishers, USA.
 13. Scott Oaks (2002), Java Security, O'REILLY Publishers, USA.
 14. Telecommunication Standardization Sector of ITU, “Data Networks and Open System Communications”, X.814, USA.
 15. William Stallings (2003), Cryptography and Network Security-Principles and Practices, 3rd ed., Prentice Hall, USA.
 16. Y. Daniel Liang (2003), Introduction to Java Programming, Prentice Hall Publishers, USA.

APPENDIX A

SNMP AND STMP

A-1 Simple Network Management Protocol

The environment of Internet Network 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 (NTCIP Guide v.03.02b, 2002). 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.

- **Management Information Base (MIB)**

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 the 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 modification 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.

- **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 main body of PDU. The PDU is the packet data for specific communications layer or communications protocol.

Table A.1 SNMP Message form

PDU Header			Main body of PDU						
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 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 PDU header and value as the two parts of the STMP message form (shows as Table A.2); it is quite different from SNMP. For this reason, STMP can also reach the goal of bandwidth saving.

Table A.2 STMP Message form

PDU Header	Value
------------	-------

- 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 Message Type

NTCIP defines that STMP is dependent on SNMP; there are eight kinds of message types of STMP. Tables A.3 and A.4 respectively list the message contents, purposes and the originators of STMP and SNMP.

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

Table A.4 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

- The Dynamic object usage

The main difference between STMP and SNMP is that STMP co-operates the dynamic objects which NTCIP defines. In addition, the major characteristic of the dynamic objects is that it can reduce the unnecessary header of data packet to reduce the bandwidth usage.

- 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

APPENDIX B

OPERATIONS OF AES AND RSA

B-1 AES

Before discussing the contents of each operation in AES, 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 $m \times n$ 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 (Hevia, A., and Kiwi, M., 1999)

		Middle 4 bits of input															
Outer bits	S ₅																
		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
		01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	0110
		10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000
		11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101

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(2⁸)

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 b₇, b₆, b₅, b₄, b₃, b₂, b₁, b₀, one could consider the byte **B** as the polynomial as:

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0 \quad (B.1)$$

$$\text{e.g., the polynomial of } (25)^{16} = (00100101)_2 \text{ is } x^5 + x^2 + 1 \quad (B.2)$$

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 $\mathbf{S}$ and each byte in the array is updated using the 8-bits S-box, as below:

$$b_{ij} = S(a_{ij}) \quad (\text{B.3})$$

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 B.4.

$$c(x)=3x^3+x^2+x+2 \quad (B.4)$$

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

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 $\log_2(n)$; actually, the size of the block should be k bits (k is a normal integer) and $2^k < n \leq 2^{k+1}$, therefore, in terms of certain plaintext $\mathbf{M}$ and ciphertext $\mathbf{C}$, the encryption and decryption can be expressed by Equations B.5 and B.6 respectively.

$$\mathbf{C} = \mathbf{M}^e \bmod n \quad (\text{B.5})$$

$$\mathbf{M} = \mathbf{C}^d \bmod n = (\mathbf{M}^e)^d \bmod n = \mathbf{M}^{ed} \bmod n \quad (\text{B.6})$$

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 $\text{KU} = \{e, n\}$, and the private key is $\text{KR} = \{d, n\}$. In order to confirm as the asymmetric cryptosystem algorithm model like Figure 2.12, 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:

$$\begin{aligned} m^{k\phi(n)+1} &\equiv [(m^{\phi(n)})^k \times m] \bmod n \\ &\equiv [(1)^k \times m] \bmod n \\ &\equiv m \bmod n \end{aligned} \quad (\text{B.7})$$

Using Equation B.7, 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 B.8:

$$m^{k\phi(n)+1} \equiv m^{k(p-1)q(p+1)+1} \equiv m \bmod n \quad (\text{B.8})$$

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 B.9.

$$ed = k\phi(n) + 1 \quad (\text{B.9})$$

or by the following form:

$$ed = 1 \bmod \phi(n) \quad (\text{B.10})$$

then

$$d = e^{-1} \bmod \phi(n) \quad (\text{B.11})$$

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 $n=p \times q$;
- Choose e , in which $\gcd(\phi(n), e) = 1$ and $1 < e < \phi(n)$, and;
- Calculate $d \equiv e^{-1} \bmod \phi(n)$

Figure B.5 The compositions of RSA algorithm
(Liu, Yi-Chieh ,2006)

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 : Chang, Yuan-Jui

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)
- Bachelor degree in Department of Construction Engineering, National Taiwan University of Science and Technology, Taiwan. (2003~2005)
- Associate bachelor degree in Department of Civil Engineering, National Kaohsiung University of Applied Sciences, Taiwan. (1998~2003)

E-mail : R95521511@ntu.edu.tw