

Experimental Analysis and Modelling of an Information Embedded Power System

A Thesis

SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

By

Amanullah Maung Than Oo

To



**VICTORIA
UNIVERSITY**

**A NEW
SCHOOL OF
THOUGHT**

School of Electrical Engineering

Faculty of Health, Engineering and Science

**Victoria University
Australia**

Declaration of Originality

I, Amanullah Maung Than Oo, declare that the PhD thesis entitled “Experimental Analysis and Modelling of an Information Embedded Power System” is no more than 100,000 words in length, exclusive of tables, figures, appendices and references. This thesis contains no material that has been submitted previously, in whole or in part, for the award of any other academic degree or diploma. Except where otherwise indicated, this thesis is my own work.

Amanullah Maung Than Oo

To my wonderful wife Habibah Begum

and

Our lovely son Midhad Aman

ABSTRACT

As power industry enters the new century, powerful driving forces, uncertainties and new functions are compelling electric utilities to make dramatic changes in their information communication infrastructure. Expanding network services such as real time measurement and monitoring are also driving the need for more bandwidth in the communication network and reliable communication infrastructure. These needs will grow further as new remote real-time protection and control applications become more feasible and pervasive. Information embedded power system via wide area network (IEPS-W) is the solution to accommodate the growing demand of wide area monitoring, protection and control. IEPS-W is an extension of traditional power systems with added monitoring, control and telecommunications facilities.

Various power system communication protocols are being used within IEPS-W to transmit critical data in real time along with decades old Supervisory Control and Data Acquisition System (SCADA). Most of the protocol in used are not originally developed to use in wide area computer network (WACN) environment. However, protocol developers upgrade their protocols and use it in WACN. This requires experimental investigation of various power system communication protocols before employing it on the power grid.

An experimental platform was set up at Victorian Network Switching Centre owned by SP AusNet PTY LTD (an Australian Transmission and Distribution company based in

Victoria) in order to experimentally analyse the performance characteristic of Distributed Network Protocol (DNP3) over wide area network (WAN). In this experiment, real time data were sent from Intelligent Electronic Devices to utility control center using WAN.

Experimental work reveal that measurement delays associated with DNP3 over WAN is high, as this type of network is much more complex due to the added complexities of routing and switching. This requires further development of DNP3 protocol to be reliably used in IEPS-W. Hence, DNP3 was further developed using Optimized Network Engineering Tools (OPNET). OPNET is the industry's leading simulator specialized for network research and development. Finally, a new protocol has been developed based on DNP3 protocol to reliably and securely transmit power system data for IEPS-W.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my special appreciation to my supervisor Professor Akhtar Kalam for his guidance, assistance and encouragement during this research. The opportunities and learning experiences he has given me are deeply appreciated. My experience at Victoria University is especially rewarding and helpful in my future career because of his supports not only in the research work but also in many other aspects. I would also like to show my appreciation to my co-supervisor for his timely advice and support throughout this research.

I would like to thank SP AusNet PTY LTD for providing all the hardware and software required for this project. In particular, I would like to thank Kevin Whelan, Andrew Roberts and Doug Peddler for their cooperation and assistance. I also would like to thank my colleagues at the School of Electrical Engineering for their valuable support. In particular, I would like to thank Dr. Cagil Ozansoy, Hassan AL-Khalidi, Abdulrahman Hadbah, David Fitrio, Adnand Mohan, Jaideep Chandran, Nikhil Joglekar and other friends in room D706 and G218, School of Electrical Engineering. I would also like to thank my parents, parents-in-law and other family members including Shafiqur Rahman, Dr. Faridur Rahman and Aksa Jamila for their support and encouragement.

Above all, I would like to give special thanks and appreciations to my wonderful wife Habibah Begum and my lovely son Midhad Aman for their love, patience, understandings, sacrifices and encouragements during this research.

LIST OF ABBREVIATIONS

ACSI	Abstract Communication Service Interface
AGC	Automatic Generation Control
ALP	Application Layer Protocol
ATM	Asynchronous Transfer Mode
CASM	Common Application Service Models
CORBA	Common Object Request Broker Architecture
CRC	Cyclic Redundancy Code
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DA	Destination Address
DCOM	Distributed Component Object Model
DES	Data Encryption Standard
DMS	Distributed Management System
DNP3	Distributed Network Protocol version 3
DPU	Data Processing Unit
DTS	Dispatcher Training Simulator
EMS	Energy Management Systems
EPRI	Electric Power Research Institute
FACTS	Flexible AC Transmission System
GOMSFE	Generic Object Models for Substation and Feeder Equipment
GOOSE	Generic Object-Oriented Substation Events

ICCP	Inter-control Centre Communications Protocol
ICV	Integrity Check Value
IEC	International Electrotechnical Commission
IEDs	Intelligent Electronic Devices
IEEE	Institute of Electrical and Electronics Engineers
IEPS-W	Information Embedded Power System over Wide Area Network
IETF	Internet Engineering Task Force
IIN	Internal Indications
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
IT	Information Technology
LAN	Local Area Network
LPDU	Link Protocol Data Unit
LSDU	Link Service Data Unit
MMS	Manufacturing Message Specification
MTU	Master Terminal Units
NIS	Network Integrated System
NTP	Network Time Protocol
OO	Object Oriented
OPNET	Optimised Network Engineering Tools
OSI	Open Systems Interconnection
PGP	Pretty Good Privacy

PKI	Public Key Infrastructure
PLC	Power Line Carrier
PSTN	Public Switched Telephone Networks
PVC	Permanent Virtual Circuit
RTS	Richmond Terminal Station
RTU	Remote Terminal Unit
SA	Substation Automation
SCADA	Supervisory Control and Data Acquisition System
SCSM	Specific Communication Service Mapping
SDU	Service Data Unit
SEL	Schweitzer Engineering Laboratories
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SSL/TLS	Secure Sockets Layer / Transport Layer Security
SVC	Switched Virtual Circuit
TCP/IP	Transmission Control Protocol/Internet Protocol
TH	Transport layer Header
TPCI	Transport Protocol Control Information
TPDU	Transport Protocol Data Unit
TSDU	Transport Service Data Unit
UCA	Utility Communication Architecture
UDP	User Datagram Protocol
UDP/IP	User Datagram Protocol/Internet Protocol

VHF/UHF	Very High Frequency / Ultra High Frequency
VNSC	Victoria Network Switching Centre
VOIP	Voice Over Internet Protocol
VON	Virtual Overlay Network
VPN	Virtual Private Network
WAN	Wide Area Network
WACN	Wide Area Computer Network
XML	Extensible Markup Language

TABLE OF CONTENTS

ABSTRACT	ii
ACKNOWLEDGEMENTS	iv
LIST OF ABBREVIATIONS	v
TABLE OF CONTENTS	ix
LIST OF FIGURES	xiv
LIST OF TABLES	xvii
LIST OF PUBLICATIONS	xviii

CHAPTER 1 THESIS OVERVIEW

1.0	Introduction	1
1.1	Motivation	4
1.2	Research methodologies and techniques	6
1.3	Organization of the Thesis	9
1.4	Originality of the Thesis	11

CHAPTER 2 LITERATURE REVIEW

2.0	Introduction	13
2.1	Wide area power system monitoring, protection and control	15
2.1.1	Impact of the information technology on power system	16
2.1.2	Obstacles to technology	21
2.1.3	Possible solutions to technology obstacles	27
2.2	Deregulated utility communication requirements	33

2.2.1	Importance of real time information in power system	41
2.2.2	Future power system information needs	44
2.3	Current power system data communication media	45
2.4	Power system communication protocols	48
2.5	SCADA system design for electric utilities	53
2.6	Conclusion	56
CHAPTER 3 AN OVERVIEW OF MODERN INFORMATION EMBEDDED POWER SYSTEMS		
3.0	Introduction	58
3.1	Information embedded power system	59
3.1.1	Measurement system	59
3.1.2	Communication system	62
3.1.3	Energy control centre	64
3.2	Power system communication protocols	68
3.2.1	Distributed Network Protocol (DNP3)	68
3.2.2	IEC 61850	76
3.2.3	Other commonly used power system communication protocols	79
3.3	Conclusion	82
CHAPTER 4 EXPERIMENTAL ANALYSIS OF DNP3 PROTOCOL FOR AN IEPS-W		
4.0	Introduction	83
4.1	Experimental setup	84

4.2	Experimental procedures	89
4.3	Experimental results	93
4.4	Conclusion	101
CHAPTER 5 MODELLING OF DNP3 PROTOCOL FOR AN IEPS-W		
5.0	Introduction	102
5.1	Brief overview of OPNET modeller	103
5.2	Development and modelling of DNP3 protocol using OPNET modeller	104
5.2.1	Implementation of DNP3 data link layer	107
5.2.2	Implementation of DNP3 transport layer	110
5.3	Development and implementation of DNP3 Application Layer	116
5.3.1	Message structure	118
5.3.2	Fragment rules	125
5.3.3	Classes	128
5.3.4	Time synchronisation	129
5.3.5	Level 1 Implementation	130
5.3.6	Implementation of DNP3 application layer	136
5.3.7	Master solicited response reception state	148
5.4	Conclusion	153
CHAPTER 6 MODELLING OF AN EFFICIENT INFORMATION EMBEDDED POWER SYSTEM		
6.0	Introduction	154

6.1 Importance of time critical communication infrastructure for power system	156
6.2 Development and modelling of efficient IEPS – W	157
6.2.1 Implementation of unsolicited response for IEPS-W	158
6.2.2 Master unsolicited response reception state table	178
6.3 Conclusion	184
 CHAPTER 7 MODELLING OF SECURE INFORMATION EMBEDDED POWER SYSTEM	
7.0 Introduction	185
7.1 Secure communication system for utilities	185
7.1.1 Threats analysis of DNP3 protocol	187
7.1.2 SCADA securities issues	191
7.1.3 Approaches to enhance IEPS – W security	192
7.2 Development and implementation of DNPSec for IEPS – W	201
7.2.1 DNP3 security framework	201
7.2.2 Key management	206
7.2.3 Analysis of the approach	208
7.2.4 SCADA/DNP3 over IP	210
7.2.5 Implementation of DNPSec in IEPS – W	212
7.3 Conclusion	219
 CHAPTER 8 CONCLUSIONS AND FUTURE WORK	

8.1 Introduction	221
8.2 Summary and achievements of the research	223
8.3 Future work	226
REFERENCES	229
APPENDIX	
A. Experimental data for DNP3	251
B. Detailed function code procedures	276

LIST OF FIGURES

Figure 1.1: Information embedded power system over WAN (IEPS-W)	1
Figure 2 .1: Substation communication protocols [38]	26
Figure 2.2: SCIMS - base architecture [46]	33
Figure 2.3: Computer network controlling the electric network with a tree topology [49]	36
Figure 2.4: Integrated WAN communication network [50]	38
Figure 2.5: The circle of measurement, information and decision making	42
Figure 2.6: Future power system information needs	45
Figure 2.7: The OSI reference model	50
Figure 2.8: The Ethernet network concept [80]	51
Figure 2.9: TCP/IP protocols and functional layers [26]	52
Figure 2.10: RTU components [91]	55
Figure 3.1: Energy control centre [103]	65
Figure 3.2: DNP3 common system architecture [105]	70
Figure 3.3: Client and server relationship [105]	71
Figure 3.4: DNP3 frame	72
Figure 3.5: DNP3 protocol stack [105]	75
Figure 3.6: Network topology [105]	76
Figure 3.7 ACSI Conceptual model	78
Figure 3.8 Three levels of UCA [113]	80
Figure 4.1: Experimental set-up	86

Figure 4.2: Control room (master) and slaves (RTUs) setting	89
Figure 4.3: Time interval setting	90
Figure 4.4: Time setting up to milliseconds	90
Figure 4.5: DNP3 classes	91
Figure 4.6: ASE2000 communication test set: TCP as transport mode	92
Figure 4.7: Activity timeline for DNP3-LAN/WAN (TCP/IP)	92
Figure 4.8: Propagation delay with 10% data traffic in DNP3-WAN (TCP/IP)	94
Figure 4.9: Propagation delay in DNP3-WAN (TCP/IP) with 20% traffic increase	96
Figure 4.10: Propagation delay in DNP3-WAN (TCP/IP) with 40 % traffic increase	97
Figure 4.11: Propagation delay in DNP3-WAN (TCP/IP) with 60 % traffic increase	98
Figure 4.12: Propagation delay in DNP3-WAN (TCP/IP) with 80 % traffic increase	99
Figure 4.13: Mean propagation delay for DNP3-WAN (TCP/IP)	100
Figure 5.1: DNP3 protocol stack [105]	104
Figure 5.2: Control centre and IED in OPNET platform	105
Figure 5.3: DNP3 protocol stack in OPNET environment	106
Figure 5.4: DNP3 data link layer in OPNET environment	110
Figure 5.5: Transport layer message layout	113
Figure 5.6: TH Bit definitions	113
Figure 5.7: Transmission of a single frame message	115
Figure 5.8: DNP3 transport lawyer in OPNET platform	115
Figure 5.9: DNP3 device interface	116
Figure 5.10: Message sequence	117
Figure 5.11: Application request header	118

Figure 5.12: Application response header	119
Figure 5.13 Application control fields	119
Figure 5.14: Outstation fragment state diagram	146
Figure 5.15: Outstation fragment state diagram in OPNET environment	147
Figure 5.16: Master solicited response reception diagram	152
Figure 5.17: Master solicited response reception diagram in OPNET	153
Figure 6.1: Unsolicited timing diagram	159
Figure 6.2: Ideal mixed unsolicited and solicited communications	169
Figure 6.3: Unsolicited response or confirmation not received	170
Figure 6.4: Read request received in region A	172
Figure 6.5: Read request received in region A (2)	174
Figure 6.6: Read request received in period B (1)	176
Figure 6.7: Read request received in period B (2)	177
Figure 6.8: Master unsolicited response reception diagram	179
Figure 6.9: Master unsolicited response in OPNET platform	181
Figure 6.10 IEPS-W in OPNET environment	182
Figure 6.11: Mean propagation delay of efficient IEPS-W	183
Figure 7.1: Planning the attack	189
Figure 7.2 DNPsec protocol structure	203
Figure 7.3: DNPsec request / respond link communication	207

LIST OF TABLES

Table 4.1: Summary of experimental features and characteristics involved in DNP3-WAN (TCP/IP) experiment	85
Table 4.2: Propagation delay with 10% data traffic	94
Table 4.3: Propagation delay with 20% increased data traffic	95
Table 4.4: Propagation delay with 40% increased data traffic	96
Table 4.5: Propagation delay with 60 % increased data traffic	97
Table 4.6: Propagation delay with 80 % increased data traffic	99
Table 4.7: Summary of experimental results in different network traffic	100
Table 5.1: Function code table	120
Table 5.2: Level 1 Implementation (DNP-L1)	133
Table 5.3: Outstation fragment state table	138
Table 5.4: Master reception state table, solicited responses	150
Table 6.1: Master reception state table, unsolicited responses	180
Table 7.1: Dynamic behaviour and relative performance characteristics of large scale VPN environments	209
Table 7.2: Advantages and disadvantages of DNPsec (proposed solution), DNP3/IPSec and DNP3/SSL/TLS architectures	210
Table 7.3: The performance of DNPsec implementation in IEPs-W model	218

LIST OF PUBLICATIONS

Journals

1. Amanullah M.T.O, Kalam A. and Zayegh A., "Information Embedded Power System: The effects of 'larger switched computer network' on the controllability of power system," Journal of the Australian Institute of Energy, March 2005, Australia
2. Amanullah M.T.O, Kalam A. and Zayegh A., "Wide area power system monitoring, protection and control," Association for the Advancement of Modelling and Simulation Techniques in Enterprises (AMSE), France, 2006
3. Amanullah M.T.O, Kalam A. and Zayegh A., "The effects of computer network on the controllability of an information embedded power system," Journal of Information and Communication Technology, Vol. 1, No. 1, (Summer 2005) pp: 29-35, TECHNOLOGICS
4. Amanullah M.T.O, Kalam A. and Zayegh A., "Power System Communications Review: Data Communications Requirement in a Deregulated Environment," Australian Journal of Electrical & Electronics Engineering, 07. (Accepted for publication)

Conference papers

1. Amanullah M.T.O, Kalam A. and Zayegh A., "Information embedded power system: the effective communication system of the 21st century power system industry," AUPEC 04, September 26-29, Brisbane, Australia.
2. Amanullah M.T.O, Kalam A. and Zayegh A., "Effective power system communication requirements for deregulated power industry," APCCAS 04, December 6-9, Tainan, Taiwan.
3. Mahajan M.M, Amanullah M.T.O and Kalam A., "Renewable hydrogen based distributed power generation systems," ICECE 04, December 28-30, Dhaka, Bangladesh.
4. Amanullah M.T.O, Kalam A. and Zayegh A., "Network Security Vulnerabilities in SCADA and EMS," IEEE/PES T&D 2005 Asia Pacific, August 14-18, 2005, Dalian, China.
5. Amanullah M.T.O, Kalam A. and Zayegh A., "Communication in power system: Time to use information embedded power system in developing countries for efficient transmission of power system data," ROVISIP 2005: International Conference on Robotics, Vision, Information and Signal processing, 20-22 July 2005, Penang, Malaysia.

6. Mahajan M.M, Amanullah M.T.O and Kalam A., "Soft start and solid state speed control of a D.C. shunt drive," ROVISIP 2005: International Conference on Robotics, Vision, Information and Signal processing, 20-22 July 2005, Penang, Malaysia.

7. Amanullah M.T.O, Kalam A. and Zayegh A., "Fiber Optic Network Infrastructure as next generation power system communications", The 6th Jordanian International Electrical & Electronics Engineering Conference, JIEEEEC 2005, November 15-17, 2005, Amman, Jordan.

8. Amanullah M.T.O, Kalam A. and Zayegh A., "Power system communication laboratory," AUPEC 05, 25th - 28th September 2005, Hobart, Tasmania, Australia.

9. Amanullah M.T.O, Kalam A. and Zayegh A., "Wide area power system monitoring, protection and control," International Conference on Modelling and Simulation Marrakesh, Morocco, 22- 24 November 2005.

10. Amanullah M.T.O, Kalam A. and Zayegh A., "Experimental analysis and modelling of an information embedded power system," AUPEC 05, 25th - 28th September 2005, Hobart, Tasmania, Australia.

11. Amanullah M.T.O, Kalam A. and Zayegh A., “Intelligent control and protection of power system with IEPs-W,” 8th International Conference on AC and DC power transmission, 28-31 March 2006, London, United Kingdom.

12. Amanullah M.T.O, Kalam A. and Zayegh A., “Development of information embedded power system using OPNET,” AUPEC 06, 10-13 December 06, Melbourne, Australia.

13. M.T.O Amanullah, Md Mainuddin, H. Md Safayat, A. Kalam, A. Zayegh, “Development of Real Life Power System Communication and Protection Laboratory At Victoria University,” AUPEC 06, 10-13 December 06, Melbourne, Australia.

14. Amanullah M.T.O, Kalam A. and Zayegh A., “Experimental Investigations of DNP3 Protocol for an Information Embedded Power System,” IASTED, PES 2007, USA.

15. Amanullah M.T.O, Kalam A. and Zayegh A., “Performance Analysis of Power System Communication Protocols for an Information Embedded Power System,” Oman, International Conference on Communication, Computer and Power (ICCCP'07), February 19 to 21, 2007, Sultanate of Oman.

16. Al-Khalidi H., Kalam A, Amanullah M.T.O., “Investigation of aging devices in power network” AUPEC 06, 10-13 December 06, Melbourne, Australia.