5-2014

Security Analysis of Phasor Measurement Units in Smart Grid Communication Infrastructures

University of Nebraska-Lincoln, mehrnaz_sharifian@yahoo.com

SECURITY ANALYSIS OF PHASOR MEASUREMENT UNITS

IN SMART GRID COMMUNICATION INFRASTRUCTURES

by

Mehrnaz Sharifian Esfahani

A THESIS

Presented to the Faculty of

The Graduate College at the University of Nebraska

In Partial Fulfillment of Requirements

For the Degree of Master of Science

Major: Telecommunications Engineering

Under the Supervision of Professor Yi Qian

Lincoln, Nebraska

May, 2014

SECURITY ANALYSIS OF PHASOR MEASUREMENT UNITS IN SMART GRID COMMUNICATION INFRASTRUCTURES

Mehrnaz Sharifian Esfahani, M.S.

University of Nebraska, 2014

Adviser: Yi Qian

Phasor Measurement Units (PMUs), or synchrophasors, are rapidly being deployed in the smart grid with the goal of measuring phasor quantities concurrently from wide area distribution substations. By utilizing GPS receivers, PMUs can take a wide area snapshot of power systems. Thus, the possibility of blackouts in the smart grid, the next generation power grid, will be reduced. As the main enabler of Wide Area Measurement Systems (WAMS), PMUs transmit measured values to Phasor Data Concentrators (PDCs) by the synchrophasor standard IEEE C37.118. IEC 61850 and IEC 62351 are the communication protocols for the substation automation system and the security standard for the communication protocol of IEC 61850, respectively. According to the aforementioned communication and security protocols, as well as the implementation constraints of different platforms, HMAC-SHA1 was suggested by the TC 57 WG group in October 2009. The hash-based Message Authentication Code (MAC) is an algorithm for verifying both message integrity and authentication by using an iterative hash function and a supplied secret key.

There are a variety of security attacks on the PMU communications infrastructure. Timing Side Channel Attack (SCA) is one of these possible attacks. In this thesis, timing side channel vulnerability against execution time of the HMAC-SHA1 authentication algorithm is studied. Both linear and negative binomial regression are used to model some security features of the stored key, e.g., its length and Hamming weight. The goal is to reveal secret-related information based on leakage models. The results would mitigate the cryptanalysis process of an attacker.

Acknowledgements

I would like to express my sincere gratitude to the College of Engineering, Department of Computer and Electronics Engineering at the University of Nebraska-Lincoln for giving me the opportunity to write an honors Master's thesis.

To my committee, Dr. Yi Qian, Dr. Hamid Sharif-Kashani, and Dr. Yaoqing (Lamar) Yang, I deeply appreciate your suggestions and guidance throughout my project. Most of all, I am fully indebted to Dr. Yi Qian, my adviser, for his timely advice, enthusiasm, kind encouragement, and support throughout the completion of this project, despite his busy schedule.

In addition, I thank Dr. Jong-Hoon Youn of the Computer Science Department at the University of Nebraska at Omaha, and Dr. Fang Yu of the Biostatistics Department at the University of Nebraska Medical Center for their assistance throughout my research. I will not forget their timely help and valued guidance.

This thesis was supported by National Science Foundation grant CNS-1065069.

Table of Contents

List of Figures 7

List of Tables 8

Acronyms 9

Chapter 1. Introduction 12

Chapter 2. Phasor Measurement Units (PMUs) and Synchrophasor Network Architecture in Smart Grid 15

- 2.1 Smart Grid versus Traditional Power Grid 16
- 2.2 Motivation for PMUs 21
- 2.3 The Functional Diagram of PMU 23
- 2.4 PMU Block Diagrams 23
- 2.5 IEEE C37.118 Standard 25
- 2.6 PMU Deployment 29
- 2.7 The Placement of PMUs in a Smart Grid 29
- 2.8 Common PMUs in Industry 31
- 2.9 Synchrophasor Network Architecture 32
- 2.10 Smart Grid Communication Infrastructure 32
- 2.11 Synchrophasor Network 33
- 2.12 WAMS Architecture 33
- 2.13 WAMS Communications Infrastructure 36
- 2.14 Security Requirements in WAMS 38
- 2.15 Phasornetwork Cyber Security Standards 39
- 2.16 IEC 61850 Communication Protocol Categories 39
  - 2.16.1 SMV (Sampled Measured Values) 41
  - 2.16.2 GSE/GOOSE communication profiles 41
- 2.17 Introduction to IEC 62351 41
  - 2.17.1 Performance concerns in IEC 62351 Part 6 42
- 2.18 WAMS Communication Network Modeling 44

Chapter 3. Overview of PMU Security 46

Chapter 4. Side Channel Attack on PMUs in Smart Grid 59

4.1 An Overview of the Security Requirement in PMUs ... 59
4.2 Introduction to Side Channel Attacks ... 59
4.2.1 History of Side Channel Attacks ... 62
4.2.2 General Assumptions in Side Channel Attacks ... 62
4.3 Introducing Popular Types of SCAs ... 63
4.3.1 Timing Attack ... 63
4.3.2 Power Analysis Attack ... 64
4.3.3 Electromagnetic Analysis Attack (EMA) ... 65
4.4 Literature Review on Side Channel Attacks ... 66
4.4.1 EM and Power Analysis Attack ... 66
4.4.2 Timing Attack ... 67
4.5 Countermeasures of Side Channel Attacks ... 71
Chapter 5. Investigating the Timing Side Channel Attacks against PMU Authentication 73
5.1 Overview of HMAC–SHA1 Algorithm ... 73
5.2 Previous Work on Timing Attacks against HMAC-SHA1 ... 76
5.3 The Analysis of Timing Attacks on HMAC-SHA1 ... 77
5.3.1 Attack Description ... 77
5.3.2 Assumptions ... 79
5.3.3 Selecting the Most Precise Execution Time ... 80
5.3.4 Optimum Number of Predictors ... 86
5.3.5 Negative Binomial with Log Link Regression Model ... 97
Chapter 6. Conclusions ... 104
Chapter 7. Future Work ... 107
References ... 108

List of Figures

Figure 2.1 An overview of a smart grid system 15

Figure 2.2 Fully integrated WAMS and SCADA Architecture and Communication Network 17

Figure 2.3 Block diagram of PMU 25

Figure 2.4 PMU installation in the smart grid for islanding detection of generators 30

Figure 2.5 WAMS hardware and communication architecture 34

Figure 2.6 skeletal network model of the smart grid in the map of the United States 44

Figure 4.1 Timing Side Channel Attack.................... 63

Figure 5.1 HMAC-SHA1 overview.................... 74

Figure 5.2 Equivalent model based on average Time 82

Figure 5.3 Equivalent model based on first observed time.................... 83

Figure 5.4 Equivalent model based on minimum execution time 86

Figure 5.5 Equivalent model based on minimum time vs data length and key length.................... 89

Figure 5.6 Equivalent model of execution time vs fixed key length and variable data length.................... 90

Figure 5.7 Equivalent models with/without considering DataHW (Considering KeyHW) 94

Figure 5.8 Equivalent model for execution time vs data length and key Hamming weight 95

Figure 5.9 Equivalent model of execution time vs fixed key HW and variable data length 96

Figure 5.10 Equivalent model via nbreg including all predictors.................... 99

Figure 5.11 Equivalent model via nbreg including encryption algorithm.................... 100

Figure 5.12 Equivalent model via nbreg including all predictors.................... 102

Figure 5.13 Equivalent model via nbreg including encryption algorithm 103

List of Tables

Table 2.1 Payload structure of data frame in synchrophasor 27

Table 2.2 Predicted number of phasor channel can be transmitted in correlation with baud rates and reporting rate of PMU over serial port 28

Table 2.3 Kbit per seconds (Kbit/s), by considering 20 measurements per PMU............. 28

Table 2.4 Sub-layer of IEC 40

Table 2.5 Execution time of RSA implementation in two different platforms................... 43

Table 5.1 Model summary based on average time of 100 iterations................................... 81

Table 5.2 Coefficient summary based on average time of 100 iterations............................ 81

Table 5.3 Model summary based on first observed time 83

Table 5.4 Coefficient summary based on first observed time 83

Table 5.5 Model summary based on Minimum Time of 100 iterations 84

Table 5.6 Coefficient summary based on Minimum Time of 100 iterations 85

Table 5.7 Model summary including all predictors (considering KeyL)............................. 87

Table 5.8 Coefficient summary including all predictors (considering KeyL) 88

Table 5.9 Model summary including all predictors (considering KeyHW) 91

Table 5.10 Coefficient summary including all predictors (considering KeyHW).............. 91

Table 5.11 Model summary of best adjusted R square (considering KeyHW).................. 92

Table 5.12 Coefficient summary of best adjusted R square (considering KeyHW) 92

Table 5.13 Model summary without knowledge of DataHW (considering KeyHW)........ 93

Table 5.14 Coefficient summary without knowledge of DataHW (considering KeyHW) 93

Table 5.15 Omnibus Test via nbreg including all predictors (considering KeyL) 98

Table 5.16 Omnibus Test via nbreg and including encryption algorithm(considering KeyL) 100

Table 5.17 Omnibus Test via nbreg including all predictors (considering KeyHW)....... 101

Table 5.18 Omnibus Test via nbreg and including encryption algorithm 102

Acronyms

PMUs	Phasor Measurement Units
PDCs	Phasor Data Concentrators
SPDC	Super Phasor Data Concentrators
GPS	Global Positioning System
UTC	Coordinated Universal Time
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
ANSI	American National Standards Institute
NASPI	North American Synchrophasor Initiative
CIP	Critical Infrastructure Protection
NIST	National Institute of Science and Technology
NTP	Network Time Protocol
WAMC	Wide Area Monitoring and Control
WAMS	Wide Area Measurement Systems
SCADA	Supervisory Control and Data Acquisition
CRC	Cyclic Redundancy Check
DOE	Department of Energy
EMS	Energy Management System
SCA	Side Channel Attack
SSCA	Simple Side Channel Attack
DSCA	Differential Side Channel Attack

EMA	Electromagnetic Analysis Attack
DPA	Differential Power Analysis
CPA	Correlation Power Analysis
DEMA	Differential Electromagnetic Analysis Attack
SEMA	Simple Electromagnetic Analysis Attack
HMAC-SHA1	Hash-based Message Authentication Code-Secure Hash Algorithm
MAC	Message Authentication Code
AES	Advanced Encryption Standard
3DES	Triple Data Encryption Algorithm
XOR	Exclusive Or
PKI	Public Key Infrastructure
CCN	Central Control Network
SS	Subscriber Station
BS	Base Station
ARX	Addition-Rotation-XOR
DOS	Denial of Service
TSMD	Time Synchronized Measuring Devices
CCA	Cyber Security Assets
MMS	Manufacturing Message Specification
GOOSE	Generic Object-Oriented Substation Events
SMV	Sampled Measured Values
HAN	Home Area Network

LAN	Local Area Network
FAN	Field Area Network
SAN	Substation Area Network
WAN	Wide Area Network
MAN	Metropolitan Area Network
AMI	Advanced Metering Infrastructure
QoS	Quality of Service
IPSEC	IP Security
SCC	System Control Center
VPN	Virtual private network
RMS	Root mean square
SGIG	Smart Grid Investment Grant

Chapter 1. **Introduction**

In this thesis, the security of Phasor Measurement Units (PMUs) in smart grid communication infrastructures is analyzed. An outline of subsequent chapters and their objectives are indicated below.

Related backgrounds are mainly discussed in Chapter 2. This chapter includes a brief introduction of the smart grid, including measurement and monitoring tools, as well as its features and benefits compared with the traditional power grid. IEEE C37.118, as a synchrophasor protocol utilized in current PMUs, will be discussed, along with the transmitting packet format and payload structure. The network architecture of the synchrophasor and the Wide Area Measurement Systems (WAMS) of the entire smart grid, as well as their communication infrastructures, are presented. In this context, WAMS is specifically known as a real-time performance system. Moreover, IEC 61850 and IEC 62351, as a substation automation system communication protocol and a security standard for the IEC 61850 communication protocol, respectively, will be discussed. Since this thesis is focused on PMUs from a security perspective, the security requirements and related performance concerns in smart grid communication infrastructure will be discussed. Considering the implementation constraints and 4 millisecond response time in IEC 61850, HMAC-SHA1 is recommended as the authentication algorithm verifying both integrity and authentication of PMU measurements in substation communication infrastructure.

A literature review of previous work in the security of PMU communication infrastructure, as well as corresponding solutions, is briefly presented in Chapter 3. The importance of several security objectives, e.g., availability and authentication, which affect the real time and wide area monitoring of the entire smart grid, is discussed. Reconnaissance, packet injection, and Denial of Service (DoS) attacks are introduced. Time synchronization attacks, mostly classified as GPS spoofing, GPS blocking, and GPS jamming, are discussed due to the importance of accuracy in timing information. In addition, PHY layer attacks such as jamming, eavesdropping, and restricting access attacks are pointed out. For instance, eavesdropping on the IEEE C37.118 network traffic reveals the IP of the PMU location. The encryption algorithm and other cyber security measures such as IPSEC and SSL are some of the recommended countermeasures to the above attacks.

After presenting an overview of PMU security, Side Channel Attacks (SCAs) on PMUs are introduced in Chapter 4. In brief, any attack based on physical implementations of security algorithms is classified as an SCA. Brute force and classical attacks related to the weakness of algorithms are not included in this definition. Several types of SCAs, e.g., Power Analysis Attacks, Electromagnetic Attacks, and Timing Attacks are defined and explained in this chapter. Thus, SCAs require information about the implemented device and operating system. With respect to the Kerckhoffs' well-known security assumptions, the supplied key is the only secret information available to the attacker. Thus, any information related to the implementation is easy to get to the attacker. Chapter 4 also presents information on a brief survey on the above mentioned SCAs against a variety of crypto implementations and algorithms. Finally, several recommended countermeasures against SCAs are shown.

Chapter 5 is the major new work of this thesis, which is focused on the timing side channel attack against the HMAC-SHA1 algorithm - the suggested authentication algorithm in IEC 62351. In other words, the execution time of the authentication algorithm applied to the communications of substations is analyzed in order to be correlated with the secret-related information of the algorithm. At the beginning of the chapter, details of the HMAC-SHA1 algorithm are illustrated. Then, the attack description and general assumptions are discussed. Finally, statistical regression models of timing side channel leakage against the security features of the stored key, e.g., its length and Hamming weight, are presented with the goal of revealing related secret information based on leakage models. Since the utilized key size in the HMAC-SHA1 can be any value larger than zero, the models would mitigate the cryptanalysis process of an attacker. All the results and figures are illustrated at the end of Chapter 5. A summary and conclusion are given in Chapter 6.

To the best of our knowledge at the time of this publication, this is the first time that timing SCA against HMAC is investigated from the execution time of algorithm viewpoint. Previous works have only considered the comparison times of received versus expected signatures in the receiver side, which could be easily resolved by coding countermeasures.

Chapter 2.

Phasor Measurement Units (PMUs) and Synchrophasor Network Architecture in Smart Grid

A smart grid is the next generation electrical power system that utilizes a modern two-way communication between power generators and consumers, with the goal of indicating a global view of the health of the entire grid to the power grid operators, e.g. utilities. Phasor Measurement Units (PMUs), as advanced measuring devices in the smart grid, precisely monitor the voltage and current phasors through a timing reference prepared by Global Positioning System (GPS). An overview of a smart grid system is shown in Figure 2.1.

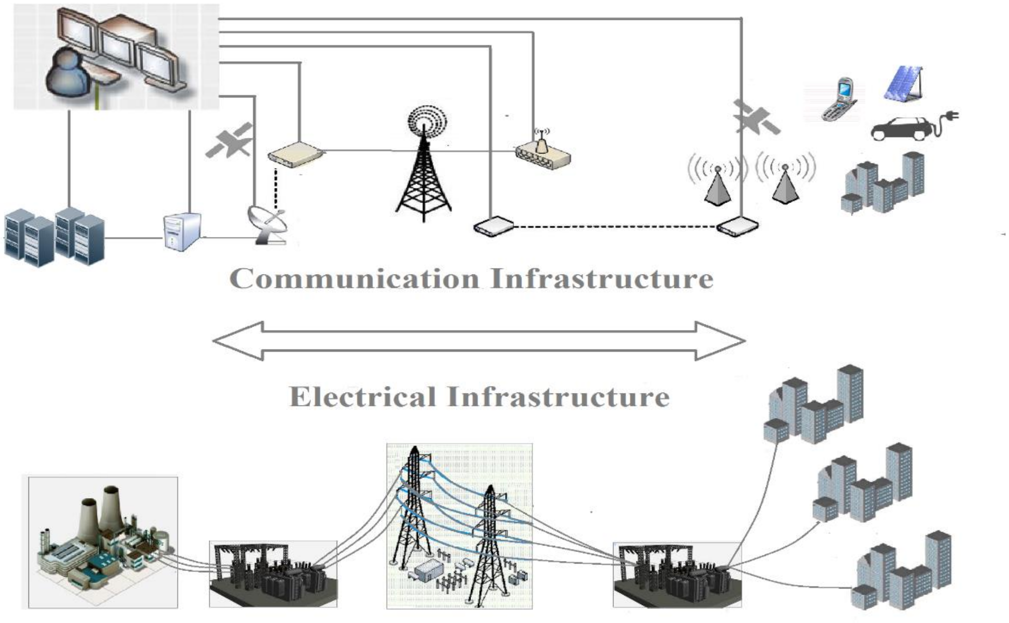


Figure 2.1 An overview of a smart grid system.

2.1 Smart Grid versus Traditional Power Grid

In addition to PMUs, a smart grid has different monitoring and measurement instruments and devices that have a variety of functions, all of which support the objectives of real-time monitoring and control. The smart grid, a modernized traditional electrical grid, comprises a variety of implemented measurements, sensors, and aggregators to achieve these objectives. A brief comparison of traditional and modernized devices, as well as their features and applications, is given below.

I. SCADA systems vs. WAMS systems

While a great deal of measurements are taken in different geographical locations and not fully synchronized, the Supervisory Control and Data Acquisition (SCADA) system is responsible for continuous measurements to provide for the safety of procedures. SCADA systems measure the voltage value and active, reactive, or injected power flow which has been utilized in the power system for a long time [1]. However, these systems have some disadvantages, such as a low transmission data rate, uncoordinated and asynchronous data acquisition, and quasi-steady state evaluations. Moreover, SCADA systems in the current power grid may not be able to dynamically monitor the power flows since they are based on steady state power flow. Typically, data is updated at the rate of 0.1 to 0.25 Hz. Wide Area Measurement Systems (WAMS) in the smart grid are responsible for presenting a time-dependent snapshot of the grid. Thus, the phasor of voltage would be examined dynamically with no state estimation required. WAMS includes high technologic measurement devices, specifically in communications infrastructure. PMUs are considered the most important and main technology of WAMS networks. Common WAMS includes

PMUs, PDCs, Super PDCs, and some ordered communications networks. However, the required bandwidth is greater than in traditional SCADA systems, which results in modifying the current communications infrastructure [2].

With respect to [3], a fully integrated WAMS and SCADA communication network is demonstrated in Figure 2.2 below.

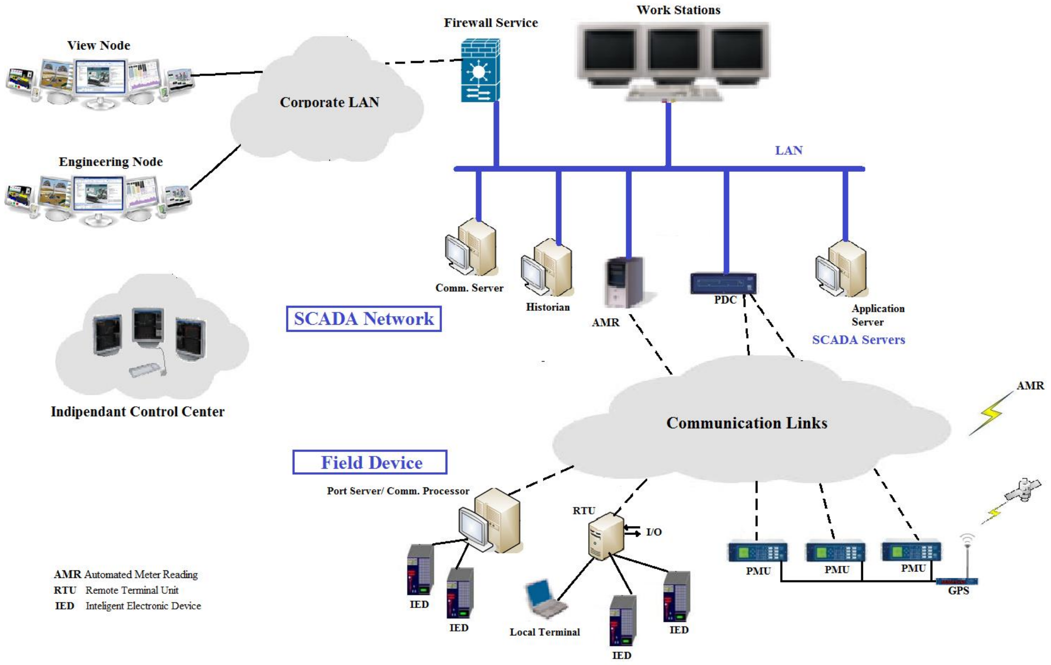


Figure 2.2 Fully integrated WAMS and SCADA architecture and communication network.

II. State Estimators vs. Phasor Measurement Units

As indicated by its name, state estimators play a key role in estimating the state variables in power system monitoring. Control centers use the SCADA measurements by implementing state estimators. However, this leads to non-linearity of measured power and state variables. State estimators have the same function as PMUs. They are responsible for measuring the phasor of voltage required for evaluating the power system. The development of WAMS is based on PMUs as advanced measurement systems. State estimation techniques use the relationships between the measurements and the state variables to be estimated which makes the grid observable in every instance. They are able to measure both current and voltage phasors. Therefore, the non-linearity problem of measurement and state variables is solved simpler and faster compared with SCADA measurements.

In [1], the authors believed that the traditional state estimators could be upgraded by PMUs to be more precise. Similar to PMUs, state estimators were responsible for providing phase angle differences but in periods of a few minutes. In contrast, smart grid PMUs could measure these differences in milliseconds or microseconds. Thus, PMUs provide high resolution synchronized clock sources from GPS receivers to measure the magnitude and phase angles of frequency, voltage, and current. They also monitor high voltage transmission lines [2].

III. Phasor Data Concentrators (PDCs)

Phasor data calculated by PMUs, or other PDCs, are correlated and interpreted as a time-stamped stream in a PDC node. In addition, PDCs evaluate the accuracy and quality of received values. Demonstrating the wide area system measurement and performance, a stream is inserted into the appropriate applications such as SCADA/EMS systems.

IV. Super Phasor Data Concentrator (Super PDC)

Similar to PDCs, Super PDCs are responsible for collecting the remote PDC and PMU phasor data prior to visualization. The collected data are accessible through a central database linked to a Super PDC. Hence, a large amount of hard disks would not be required to store all the collected data at a sampling rate of 30, 60 or 120 samples per second.

In this thesis, PMU features and vulnerabilities from a security point of view are studied. After a brief introduction to PMUs and the need for these devices, the communication and security protocols applied to the PMU substation automation system are discussed in Chapter 2. In addition, a literature review of previous works related to security vulnerability of PMUs and suggested solutions are presented. Finally, the timing side channel attack, as the main contribution of this thesis, is introduced and investigated through the security protocol of PMU substations in synchrophasor networks.

Other features of PMUs in smart grids are discussed, including the following:

1. Non-linearity of measurement and state variables;
2. More accurate state estimation by real-time and stability monitoring which improves the post-disturbance assessment ability;
3. Island detecting in the presence of generation load-matching while circuits and grid are not in time and synchronized;
4. Increased reliability and robustness in distorted situations [1];
5. Dynamic system monitoring of the power grid which causes congestion expanses to diminish and the consumed assets to grow;

6. Real-time and accurate measurements of any local bus of the system, which leads to wide area monitoring and visibility;
7. Monitoring the system's measurements in a delay-sensitive highly data rate manner, which leads to a rapid response of the system that is required in irregular and anomalous situations;
8. Overload and voltage stability monitoring;
9. Adaptive protection; and
10. Restoration of the power system.

To achieve all of the above features, PMUs have to be weighted. This is a challenging issue which is related to the final PDC, manufacturers' classes of error, different accuracies of available PMUs on the market, and the correctness of metering devices of chain. Normalization of the measurements is mostly recommended for reducing the errors. Thus, the weights of PMUs would play a key role in correctness of measured values. In other words, the error measurements of low weight PMUs may be ignored while the errors of higher weighted ones cause the entire measurements to be discarded. More details on weighting PMUs are given in [4].

After a brief introduction of PMUs in the smart grid, we further discuss the motivations of PMUs in the power grid, their block diagrams, and their placement in smart grid communication infrastructures. Also, several common PMUs in today's industry are introduced.

2.2 Motivation for PMUs

The most significant motivation for PMUs is to overcome voltage instability in the power grid which leads to blackout. Instability is caused by an imbalance of consumption compared with generation and transmission. In other words, load dynamics, transmission and generation represent the three most significant factors in voltage failures [1].

Phasor measurement devices and phasor synchronization are not needed when only one generator is available in the power grid. However, two or more generators require synchronization. The outputs of generators are altered by changing the running speed of different generators in the system, e.g., a little faster or slower running of one generator over the other. PMUs are required for synchronizing the phase and frequency of the connected generators of these power systems. For example, every two generators that produce exactly 110 VAC at 60 Hz could connect and form a grid when there are zero phase differences between them. However, any exception to this situation could result in a blackout. The GPS receivers of the PMUs are responsible for synchronizing the accurate and precise frequency and phase outputs of the generators.

Consequently, monitoring the entire grid with the goal of approaching an accurate universal overview is essential for power data management engineers. In other words, the knowledge of what exactly happens at specific times in a variety of geographic locations plays a key role in the correctness of entire grid predictions and any ongoing controlling decisions to prevent serious incidents [5].

Due to the complexity of the North American power grid, which has 300,000 km power lines and 500 entities, keeping the balance between the demand and supply of electricity relies upon the coherent performance of cooperating entities. Currently, there is no real-time exchange of power grid status and information among these entities [6].

In [7], the authors studied the monitoring role of the first set of PMUs, installed in 2004, on the June 15, 2005 blackout. The frequency and angle differences between two locations-- Little Rock, AK and Houston, TX--were examined and illustrated in detail. As depicted in publicly-available graphs and documents, 27 minutes prior to the blackout, the phase differences were steady at around 35 degrees. However, an immediate angle difference occurred at 5 p.m., which continued to increase and ended at the blackout trajectory of passing a 120 degree phase difference just prior to the collapse of the network. Recloser failure though the lines of two locations and increases in instant impedance due to line outage are some of the reasons for the jump and phase differences.

With respect to the NERC report, the shortage of grid status awareness was the main reason for the blackout in the Northeastern United States as well as southern Canada in 2003, prior to the PMUs being installed in 2004. Regarding [6], it had an economic impact of billions of dollars.

Hence, the U.S. Department of Energy (DOE) has been investigating the possibility of synchrophasor technology in the North American power grid. The North American Synchrophasor Initiative (NASPI), in collaboration with the North American Electric Reliability Corporation (NERC) and many other organizations, has been established. The complete coverage of the transmission grid by 2014 was one of the objectives of the American Recovery and Reinvestment Act [6].

2.3 The Functional Diagram of PMU

As an important instrument of Wide Area Monitoring and Control (WAMC) systems, PMU is responsible for continuous monitoring of the health and precision of the power grid. Voltage and current phases of power systems are precisely monitored by PMUs. All the measured values are based on the reference time prepared by GPS receivers of the PMUs. Thus, the accurate synchronized and real-time measurements are transmitted to the control center to monitor the operation of the power grid. Delivering the delay-sensitive measurements of PMUs is highly dependent upon the communication network's reliability and Quality of Service (QoS). In [8], the author has claimed that non-sufficient and proper communication infrastructures are the major parameters preventing the broad utilizations of PMUs in the distribution side of the power grid as it covers a huge area.

2.4 PMU Block Diagrams

The first PMU was built and assembled in 1988 by Dr. Arun G. Phadke and Dr. James S. Thorp at Virginia Tech Power Systems Research Laboratory [2]. The goal of PMUs is to continuously sample the analog measured voltage, normally 20, 30 or 60 samples per second, and the current and frequency in synchronicity and time-stamp them using the precise clock of GPS receivers. The time-stamped measurements are called synchrophasors, which lead to synchronizing and time aligning the different location measurements. Thus, a grid snapshot is created by these precise clocks [9]. Moreover, line frequencies are evaluated at each side. Hence, the phasors of different locations would be evaluated as a result of such corresponding samplings. Generally, a phasor refers to another representation of sinusoidal waveform with magnitude and phase, or a phase angle which is defined as the difference of the signal peak and a reference such as time equal to zero. Phase angle differences of a group of calculated measured phasors are calculated by assuming one phasor measurement as reference. However, the result is independence of the selected reference.

Practically, in an AC power system, a higher voltage phase angle causes the power to flow to the lower phase angle voltage. More voltage phase differences between two locations leads to more statistic stress applied to the corresponding power grid, which also affects the stability of the grid.

A block diagram of a PMU, including Digital Signal Processors for measuring the AC signal of 50/60 Hz at a variety of sampling rates, Analog to Digital Converters of each phase, as well as phase-lock oscillator alongside the GPS receiver for a synchronized sampling rate of 1 millisecond accuracy, is illustrated in Figure 2.3 [10].

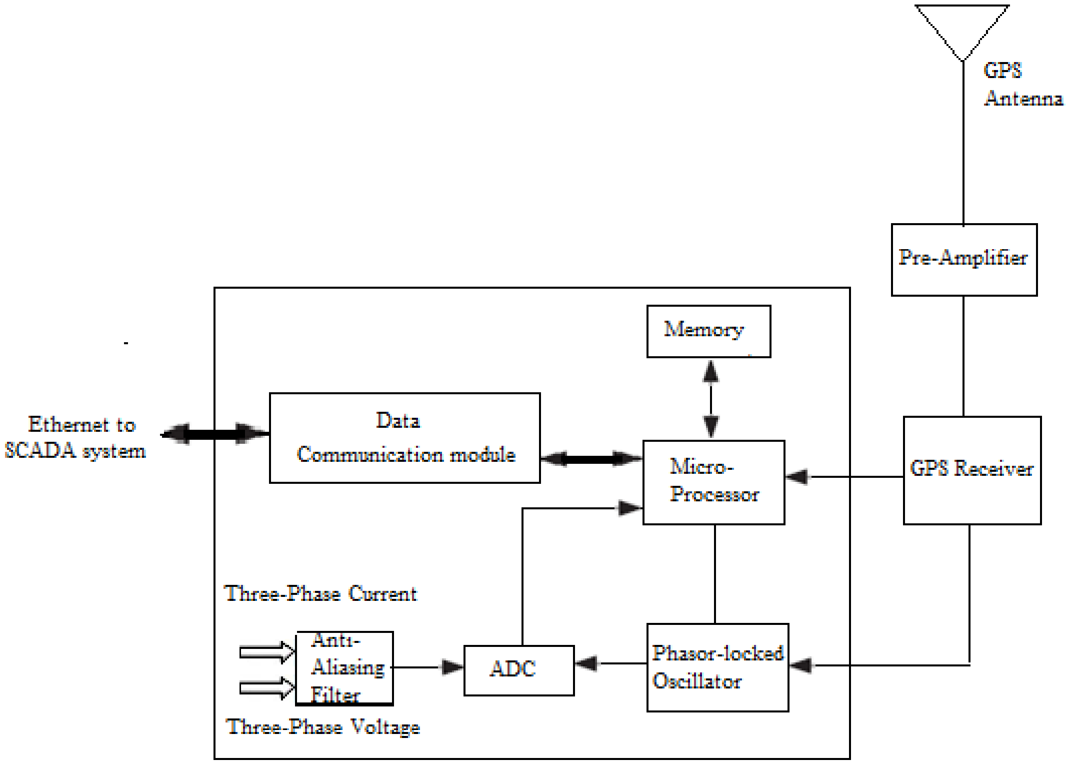


Figure 2.3 Block diagram of PMU.

2.5 IEEE C37.118 Standard

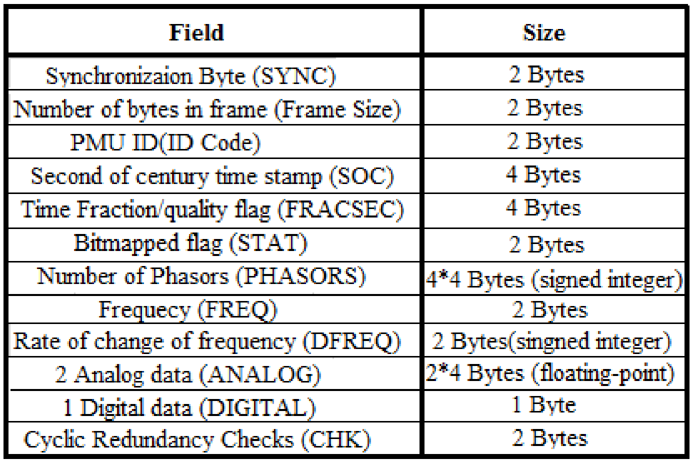
Several standards and protocols support the communication infrastructures of PMUs with other components of the smart grid. These standards are introduced in subsequent chapters. The latest version of the PMU/PDC protocol, IEEE C37.118, is discussed in this chapter.

IEEE C37.118 is the substitute for the previous IEEE 1344 synchrophasor protocol used in PMUs since 1998. IEEE 1344 did not include the response time, the accuracy of measurements, the phasor measuring process, and the hardware and software as well as security or transport specifications in implementation of the protocol. The synchronization source is the number of seconds from the epoch of January 1, 1970 (AKA seconds-of-the-century (SOC)) related to Network Time Protocol (NTP) and Coordinated Universal Time (UTC). The American National Standards Institute (ANSI) signified the IEEE C37.118 in 2006 to overcome the previous standard shortcomings. The revisions included, for example, phasor measurements of several PMUs, compatibility with other standards, and sample modification to the order of fraction of seconds compatible with the standard International Electrotechnical Commission (IEC) 61850:2000. However, neither IEEE 1344 nor IEEE C37.118 supports authentications or integrity or confidentiality features that make the WAMS vulnerable to malicious data being injected into the PDC and state estimators [3]. Thus, each PMU comes along with the IEEE C37.118 standard.

The goal of IEEE C37.118 is to clarify the "frame" format of data transmitted from PMU to PDC. The communication media is not specifically constraint while four specific frame named as: Configuration, Data, Command, and Header frame are defined. The first three are binary and the last is ASCII. The data frame is defined as the measured values of PMUs and the most frequent transmitting frame in the order of a few hundred bytes [11]. For instance, the Entergy system includes 22 PMUs and sends 84 measurements per packet, as claimed in [7]. The phasor vector, frequency, rate of changing frequency, signed three phase voltage, current, real and active power, and individual phase RMS values, and detecting unbalanced conditions are some of the values including the data message. A machine-readable message and configuration are responsible for calibration.

Finally, 16 bytes of a humanly readable header are included in each transmitted packet of a PMU and defined by the user [3]. Since the header and command messages are not frequent, e.g., per minute of header message, transmitting, they could transmit through TCP/IP. A processing computer system is utilized, which is based on “low power Xeon class CPUs configured to run Windows 2008 standard 64 bit server operating system” in the PMUs’ manufacturer specifications in the CSSP. This is in the range of $3500 [7]. An overview of the payload configuration is shown in Table 2.1.

Table 2.1 Payload structure of data frame in synchrophasor [8].



Field	Size
Synchronizaion Byte (SYNC)	2 Bytes
Number of bytes in frame (Frame Size)	2 Bytes
PMU ID(ID Code)	2 Bytes
Second of century time stamp (SOC)	4 Bytes
Time Fraction/quality flag (FRACSEC)	4 Bytes
Bitmapped flag (STAT)	2 Bytes
Number of Phasors (PHASORS)	4*4 Bytes (signed integer)
Frequecy (FREQ)	2 Bytes
Rate of change of frequency (DFREQ)	2 Bytes(singned integer)
2 Analog data (ANALOG)	2*4 Bytes (floating-point)
1 Digital data (DIGITAL)	1 Byte
Cyclic Redundancy Checks (CHK)	2 Bytes

The transmission rate of the data frame is related to the sampling rate when considering PMU. Regarding the number of phasors the desired PMU is measuring, as well as analog or digital signals, the data frame size is changed. For instance, the baud rate of a port is defined as the transmitting capability in serial communications. In a 12 phasor channel PMU, Table 2.2 indicates the reporting rate and transferring capability of data [11].

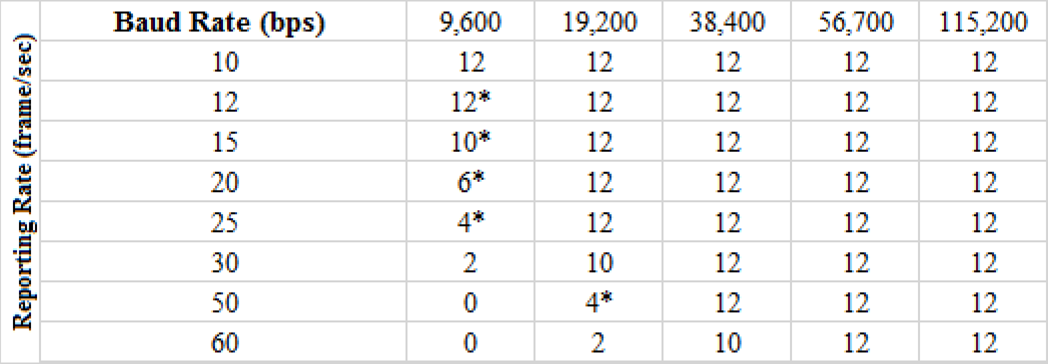
Reporting Frequency is assigned in IEEE C37.118-2005 as 10, 25 Hz for a 50 Hz power system, and 10, 12, 15, 20, 30 Hz for a 60 Hz system. Reporting frequency is defined as the load of PMU and the maximum delay of PMU to PDC communication.

If Reporting Frequency is defined as F_s, and the maximum delay as D_{max}, then:

$$D_{max} = 1 / F_s$$

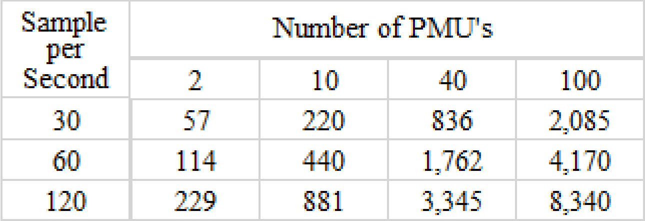
The maximum delay could be great as the packet is received before the next packet is available.

Table 2.2 Predicted number of phasor channel can be transmitted in correlation with baud rates and reporting rate of PMU over serial port. 10 bits including one start bit, one bit and 8 bits data are considered for transmitting each byte of data. (*Actual number may be less than the prepared number since calculated bandwidth is close to baud rate [11].)



	Baud Rate (bps)	9,600	19,200	38,400	56,700	115,200
Reporting Rate (frame/sec)	10	12	12	12	12	12
	12	12*	12	12	12	12
	15	10*	12	12	12	12
	20	6*	12	12	12	12
	25	4*	12	12	12	12
	30	2	10	12	12	12
	50	0	4*	12	12	12
	60	0	2	10	12	12

Table 2.3 Kbit per seconds (Kbit/s), by considering 20 measurements per PMU [9].



Sample per Second	Number of PMU's			
	2	10	40	100
30	57	220	836	2,085
60	114	440	1,762	4,170
120	229	881	3,345	8,340

Moreover, the approximate bandwidth in the order of Kbits/sec versus the PMUs' sampling rate and the number of PMUs is indicated in [9]. Thus, consumption bandwidth is about 57 kbps for two PMUs by UDP.

2.6 PMU Deployment

A 10 phasor PMU is a common model which is simply installed. Each phase shows 3 phase voltage or 3 phase current. A power connection, ground connection of station, GPS antenna connection, and communications circuit connection are required connections for each PMU. For communications circuit connections, a modem and Ethernet are needed in case of 4-wire and network connections, respectively. A GPS receiver antenna is installed on the roof of each substation. Each phasor of three phases is required for these connections. While PMU installation is complete, the PMU is linked to a PDC via communications circuit connections [10].

2.7 The Placement of PMUs in a Smart Grid

A traditional utility power system includes generation, transmission, distribution, and consumer parts. Carrying the highest voltage level of typically 138 – 1000 kV, the transmission system is responsible for some problems like blackouts [12].

Generally, PMUs are designed for the transmission network in the power grid as illustrated in Figure 2.4.

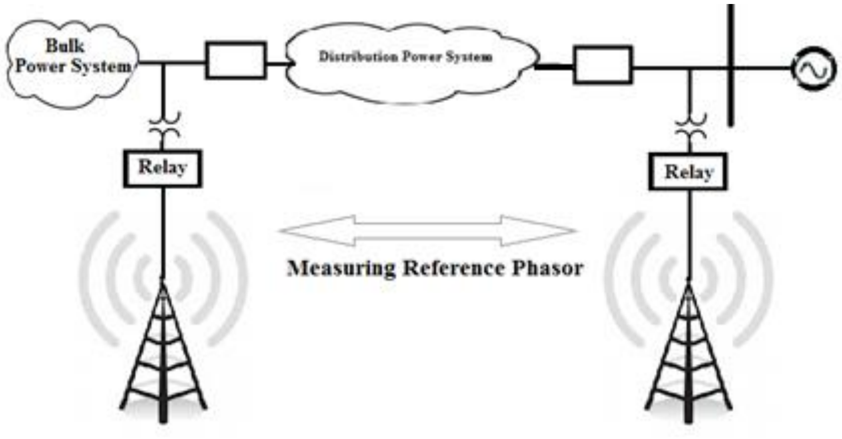


Figure 2.4 PMU installation in the smart grid for islanding detection of generators.

Most of the power utilities have currently installed PMUs in high voltage substations; however, PMUs are also intended to monitor high voltage transmission lines.

Distribution networks have different features which leads to different measurement methods. As illustrated above, locating the PMUs at two ends of the transmission line is the easiest form of monitoring the voltage and power [1]. Entergy was the first company to utilize PMUs on the transmission as well as the distribution sides [7].

Currently, many PMUs are installed in the United States due to the DOE Smart Grid Investment Grant (SGIG) programs. More than 1,000 PMUs are estimated to be installed by nine SGIG grantees in the last three years alone [7]. However, all of them are constrained by the high level voltage parts of the power grid such as power plants and transmission substations. Since the renewable energy sources, e.g., solar cells, that are located in the distribution side play a key role in the future of the smart grid, some real-time applications are recommended for the reliability of frequencies and voltages [8]. This leads to the use of an intermediary power supply of solar cells as well as electric vehicles. PMUs are also expected to be installed in commercial and residential accommodations as well [7]. SGIG grantees also suggested redundancy of PMU measurements to prevent the loss of data as much as possible.

In [13], NASPI released documents illustrating the distribution of installed PMUs in the North American Power Grid up to 2012. The installed PMUs in Europe as of 2012 are depicted in [1].

2.8 Common PMUs in Industry

Different size of PMUs are available in industry according to the variety of digital signal processing techniques. For instance, the PMUs that measure 10 phasors in addition to the frequency are categorized as large, while the three phasors plus the frequency PMUs are also found in industry. Larger sizes of PMUs cost as much as $30,000 to $40,000 more than smaller PMUs [10].

In addition, some portable types of PMUs that work over GPRS nodes are recently being used in industry. They have small dimensions and are easy to install and implement anywhere, and no ventilation is required. Moreover, measurement data are accessible through web clients such as PCs, laptops, and smart phones [14].

2.9 Synchrophasor Network Architecture

PMUs, PDCs, and Super PDCs, described in the previous part of Chapter 2, are some of the important tools of a phasor network. Other devices as well as their hierarchical communication models will be discussed below. It is important to know that the Synchrophasor Network Architecture presented in this chapter is one of the most common models that are discussed in a variety of references. Many other aspects of PMU communications are also mentioned in different resources. For example, wide area PMU communications over WiMAX/IEEE 802.16 networks are analyzed in [8]. In this situation, locally IP-based PMU measurements are routed to a PDC via a local communications network and then to the Central Control Network (CCN) through the backbone network. Thus, the PMU interface performs as a Subscriber Station (SS) while the PDC acts as a Base Station (BS) in a WiMAX-based network. IP multicasting approach is also considered in [6]. At the end of this chapter, the security requirements of PMUs will be discussed.

2.10 Smart Grid Communication Infrastructure

First, a brief review of smart grid communication infrastructures will be given below. The communication infrastructures of a smart grid include Home Area Networks (HANs), e.g., industrial, commercial business, and home sites; Field Area Networks (FANs) supported by deploying Advanced Metering Infrastructure (AMI); Substation Area Networks (SANs) over an electric substation containing PMUs; Wide Area Networks (WANs) or backhaul communications defined as connections of FANs and SANs, and control centers with substations; and Local Area Networks (LANs) [12].

A substation network is a remote site of a SCADA operation. IEC 61850 is working to improve the SAN to communicate with other substations through “substation-to-substation communications.” A high level overview of a smart grid communication infrastructure compared with an electrical infrastructure is shown in Figure 2.1.

2.11 Synchrophasor Network

Communications between one PMU and one PDC form the simplest part of the phasor network in a smart grid. However, one PDC's aggregated real-time measured data come from different PMUs located in vital substations. First, the correctness of data is investigated though Cyclic Redundancy Check (CRC) and kept in internal memory. All the restored data are accessible and synchronized by a UTC clock. Finally, by comparing the time-stamped data, the measured data would be rearranged and aligned based on their UTC time similarities [2]. Different software, e.g., RTDMS, are implemented through the personal computer at the output port of each PDC to calculate and show the local measured values such as voltage, current, frequency, MW and MVAR for operators. The higher layer includes a Super PDC which is responsible for an interconnection-wide snapshot based on received data from the PDCs [10].

2.12 WAMS Architecture

Figure 2.5 shows the WAMS hardware and communication architecture [2].

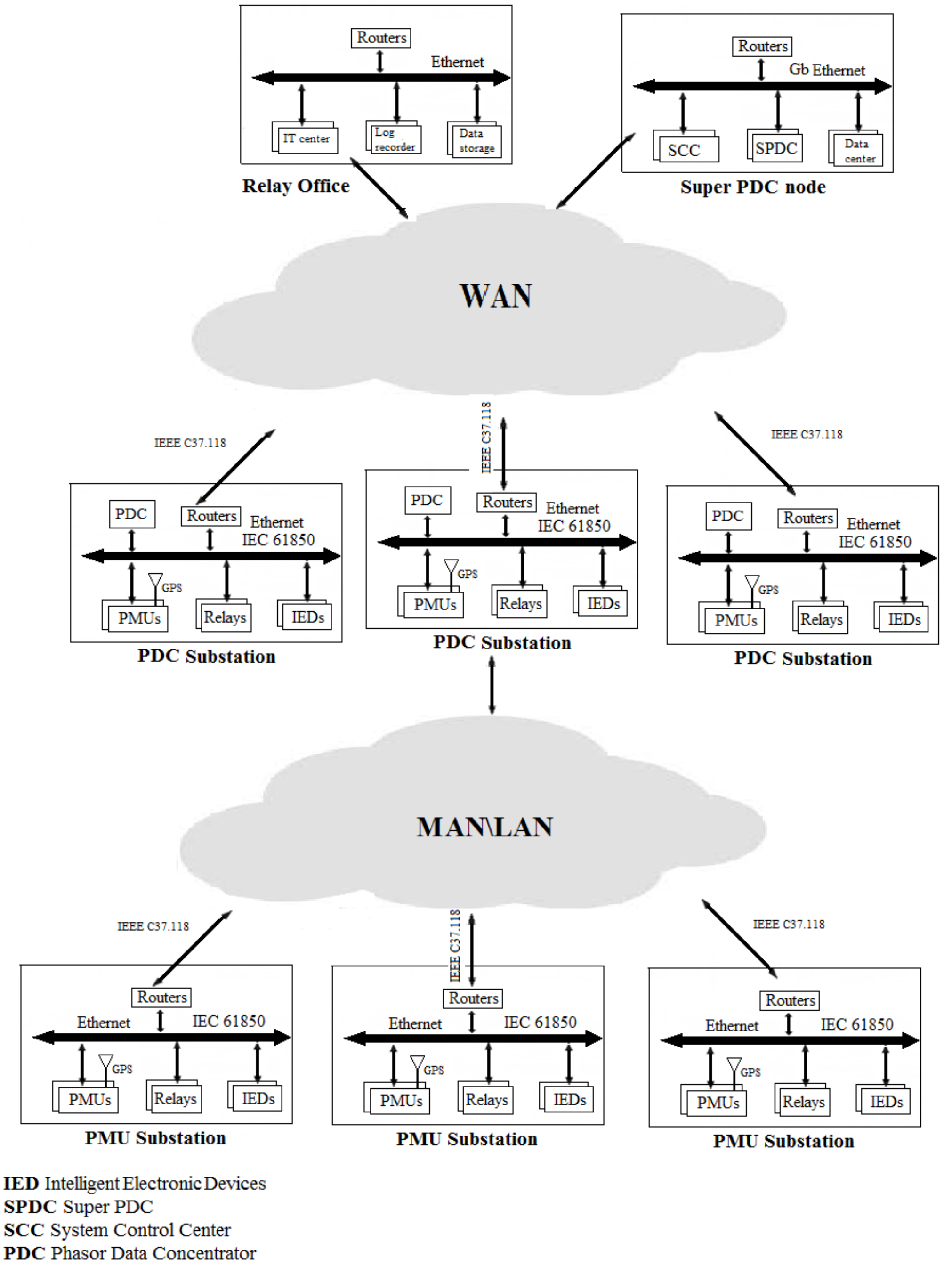


Figure 2.5 WAMS hardware and communication architecture.

The main components of WAMS are substations with PMUs, substations with PDCs, an SPDC, a real office, and WANs.

- **PMU Substation**

As depicted, PMUs are located in the lowest level of WAMS in the PMU locations. PMUs are responsible for generating more than 50% of WAMS' network data [3]. Thus, the reliability of entire WAMS in higher layers depends on the accuracy of PMUs installed in substations for measurement collection and communication. In addition to PMUs, digital relays and Intelligent Electronic Devices (IEDs) are located as basic measuring tools in PMU substations, which are all connected by shared media access 100 Mbps Ethernet. Moreover, routers are responsible for connecting the Ethernet of intra-substations with local area networks. All these phasor measurements have to be centralized in a monitoring center. Increasing the number of PMUs leads to increasing the data volume and traffic.

- **PDC Substation**

PDCs can also be linked to the Ethernet-shared media of the substations, mentioned above. The time-stamped and aligned measurements of all regional PMUs would be transmitted to the Super PDC by the PDC. Moreover, PDCs can apply specific control decisions regarding the received data. In a larger number of distributed PMUs, the communications backbone between PDCs may become a communication bottleneck in WAMS.

- **Super PDC (SPDC node)**

Located at the highest level of WAMS architecture, the Super PDC is able to store and analyze the received measurements of the lower level. Moreover, all the controlling decisions, and many of the monitoring and global protection patterns of WAMS architecture, are governed by the SPDC. Any data center, phasor data processing center, or

System Control Center (SCC) could affect the SPDC. It is also responsible for returning the time critical commands to equipment and controllers.

- **Relay Office**

The relay office records and stores any relay task logs and relay alarms, and remotely looks over the relay parameters.

2.13 WAMS Communications Infrastructure

The WAMS network uses several communication infrastructures ranging from serial communication to VPN [3].

- **Serial Communication**

As a continuance of the SCADA network, the WAMS network uses serial communication similar to SCADA, for the most part. It utilizes high speed modems to at least 30 samples per data requirement. Those modems are vulnerable to several attacks and reveal the critical data to attackers through command sequences. The data format through serial communication is RS-232 with a speed range of 2400 to 115,200 bps.

- **Analog Microwave**

Microwave is implemented in WAMS for connecting the remote PMUs to the PDC in the absence of wire communication. Similar to wireless commination, it is susceptible to jamming, traffic analyzing, and signal monitoring and recording.

- **Virtual Private Networks (VPNs)**

The secure communication of two entities over an insecure public network by utilizing a variety of technologies is defined as virtual private networks (VPNs). IPSEC is the suggested security protocol suite for authentication, encryption, and key establishment of WAMS data which are being transmitted over internet protocol (IP). Since it is assigned to layer three of the OSI model and encrypts the network data and addresses, WAMS users are able to insert incorrect data and gain access to entire and unauthorized network data.

The three layers of intra-substation local area networks (LANs), high-performance regional networks, and wide-area fiber-optic networks are defined below [2].

- **Intra-substation local area networks (LANs)**

  Implemented protocols in this LANs, e.g. IEC 61850, can run over the large transmission bandwidth gigabit Ethernet in order to guarantee the 4 millisecond response time.

- **High-performance Regional Networks**

  Connecting distributed PMUs to one PDC, these networks are controlled by independent utilities only for power systems. Measurement data received by PDC may be used for making the regional protection decisions.

- **Wide-area Fiber-optic Networks**

  PDC data are transmitted to the SPDC through this kind of network. Real-time command could be send back to a variety of equipment and controllers from SPDC. Since the volume of data will significantly increase by increasing the number of

PMUs in the smart grid, the communication backbone of PDCs could be a bottleneck in the WAMS.

2.14 Security Requirements in WAMS

Some specific features have to be considered in securing the phasor data transmission of a WAMS network to deliver real-time streaming phasor data and the state of the smart grid. The application layer of the OSI model includes the protocols of streaming data, which do not include the security standards. Thus, the author of [3] believed that those standards have to be included in lower layers. Even though confidentiality and integrity of data are so crucial, the availability and real-time response of data should not be affected. Data signatures, using Hash-based Message Authentication code (HMAC) with a shared key, are sent with the PMUs' measurements to prevent unauthorized and dishonest commands. Moreover, confidentiality has to be considered while the data is transmitted over public networks such as the Internet. A fast and light encryption algorithm, such as AES as a symmetric algorithm, is recommended. A simple solution for confidentiality and authentication of the data over Internet-based protocols would be IP Security (IPSEC) VPNs as well as a combination of TLS and IPSEC named DTLS. Another solution would be a private WAMS network such as NERCNet, used by the North American Electric Reliability Corporation (NERC), along with IEEE standards. Since UDP transport is utilized for streaming data, the TLS protocol cannot be applied. Another approach would be implementing VPN or encrypting serial link devices between the PMU and the PDC. In addition, Public Key Infrastructure (PKI) and Diffie-Hellman are some of the well-known key distribution algorithms, for a small number of devices, to prepare the shared key of different recommended symmetric security algorithms. The best key distribution is chosen by considering the network architecture and implemented protocols.

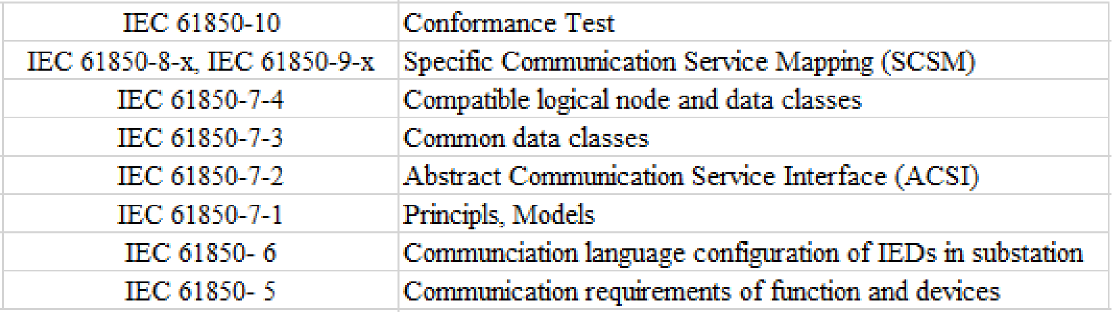
2.15 Phasornetwork Cyber Security Standards

- IEC 62351- suggested security standards and protocols through communication media
- NERC CIP 002-009 - provided cyber security standards
- IEEE 1686-2007 – investigated the security of measurements with respect to the IEEE 1686-2007, security measures over IEDs (intelligent electronic devices)
- IEEE C37.118 - communications protocol of PMU measurements and communications; previously discussed in this chapter.
- NIST Special Publication (SP) 800-53 -guidelines for federal information systems
- FIPS 199 and FIPS 200 - basis of system classifications [15].

2.16 IEC 61850 Communication Protocol Categories

Introduced by IEC Technical Committee 57 (TC57), the IEC 61850 standard signifies the communication protocol over the serial and modern computer type of technology which uses the TCP/IP model and Ethernet-shared media access encapsulation methods of PMU substations. IEC 61850 covers the entire communication requirements of substation automation systems which are not dependent on the manufacturer of instruments. It maps the data model in a group of protocols being able to run over Ethernet-shared media access, such as Manufacturing Message Specification (MMS), Generic Object-Oriented Substation Events (GOOSE), and Sampled Measured Values (SMV). Thus, 4 ms of response time is guaranteed based on the gigabit transmission bandwidth of Ethernet [2]. The sub-layers of IEC are presented in Table 2.4 [16].

Table 2.4 Sub-layer of IEC



IEC 61850-10	Conformance Test
IEC 61850-8-x, IEC 61850-9-x	Specific Communication Service Mapping (SCSM)
IEC 61850-7-4	Compatible logical node and data classes
IEC 61850-7-3	Common data classes
IEC 61850-7-2	Abstract Communication Service Interface (ACSI)
IEC 61850-7-1	Principls, Models
IEC 61850- 6	Communciation language configuration of IEDs in substation
IEC 61850- 5	Communication requirements of function and devices

The protocol is defined in both the vertical and horizontal directions. Certifying the significant connections of IEDs, which could be the encapsulation of GOOSE into the Ethernet frame or recommended serial link, and the TCP/IP model are used for horizontal and vertical directions, respectively. For time synchronization, non-reliable UDP is utilized. A connection-oriented TCP/IP protocol is recommended for ASCI MMS communications. The highest accepted time delivery is 10 milliseconds. As type one and type four, GOOSE and SV are categorized as fast and prime message data, respectively. GOOSE, SMV (Sampled Measured Values) and MMS (ACSI basics) are three main protocols utilized in IEC 61850.

2.16.1 SMV (Sampled Measured Values)

The measured data of sensors such as CTs and VTs are transmitted through the SMV method. Ethernet Multicast and unicast communication via serial lines are implemented in the lower layer of ISO. Regarding IEC 61850-7-2, four different application and transport networking profiles are addressed below:

- Client/server model
- GOOSE/GSE control
- GSSE services
- Time synchronization

2.16.2 GSE/GOOSE communication profiles

Fast and reliable data transfer is provided through the GSE (Generic Substation Event) control model, introduced in IEC 61850, by UCA2.0 status messages. Multicast data communication is mostly applied to the GOOSE and GSE events [16].

Developing the IEC 61850 communication protocols as well as IEC 62351-part 6, the cyber security standard, improves the substations automation system.

2.17 Introduction to IEC 62351

The goal of this protocol is to secure the communication protocols of IEC-TC 57, particularly the IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970, and IEC 61968 series. To secure the two main parts of IEC 61850, the client server (i.e., MMS) and real-time (GOOSE and SV), several methods are used [17].

- **MMS**

  The security is defined under the application and transport layers as peer authentication and TLS, respectively. Including the X.509 encoded certificate and time-stamped values, the authorized information are transmitted in ACSE AARQ and AARE PDUs. TLS_DH_DSS_WITH_AES_256_SHA1 and TLS_DH_RSA_WITH_AES_128_SHA2 are the minimum suggested cipher suites.

- **GOOSE/Sampled Values**

  Since the transmitted data is time-critical, only the message authentication is recommended. Thus, encryption and message confidentiality is not supported. The GOOSE/SV PDUs are concatenated with the calculated signing value of SHA256 hash using RSA.

2.17.1 Performance concerns in IEC 62351 Part 6

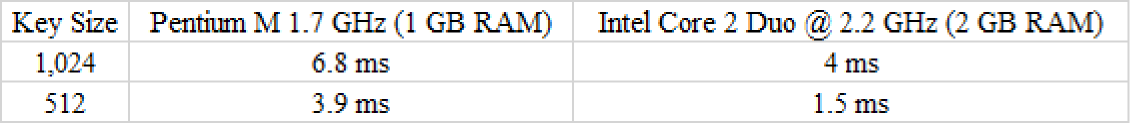
Performance issues play a key role in introducing any communication protocol, including encryption and authentication, regarding constrained resources such as response time.

In [17], the authors applied and investigated the main limitations of securing the SV and GOOSE. As an example of real-time constraints of both GOOSE and SV, a 3 millisecond response time is required for GOOSE and up to 12 KHz of sampling rate for Sampled Values. Other limitations include the computational power of RTUs and IEDs as well as changing and upgrading issues of embedded devices. As the real-time application of

PMUs, the authentication implementations of GOOSE and SV packets are investigated by authors. The RSA algorithm in C for signing the SHA256 hash value is suggested and investigated in several software and platforms. Results indicate that current IEDs would not meet the real time requirements even though those platforms' memory and CPU processors exceed the requirements for common embedded devices. In other words, at least 4 milliseconds is needed for signing the measurements by 1024 bits of key length, which is the minimum response time of the entire GOOSE message. One has to consider that significant changes in the hardware of embedded devices should not be easily adopted.

Table 2.5 shows the execution time of implementing RSA signing on two platforms. As the table shows, the minimum time is 1.5 milliseconds, corresponding to 512 bits key size, which is not an optimum assumption.

Table 2.5 Execution time of RSA implementation in two different platforms.



Key Size	Pentium M 1.7 GHz (1 GB RAM)	Intel Core 2 Duo @ 2.2 GHz (2 GB RAM)
1,024	6.8 ms	4 ms
512	3.9 ms	1.5 ms

Also, RSA crypto chips can support the response time of 23.8 microseconds for a 1024-bit key length. However, it requires remodeling and redesigning the overall hardware that contains the external memory, or even the cooling systems. Finally, the latest results show that authentication of real-time data would not be feasible by today's embedded devices. They require managing 100 and 300 packets per second in GOOSE and receiving 4000 packets per second along with several tasks, e.g., protection mechanisms, time synchronization, logging, etc. Consequently, the TC 57 WG group in October 2009 decided to replace the asymmetric signing by symmetric cryptography and use of HMACs. Moreover, according to [18], HMAC-SHA1 and AES-128 must be included in this standard.

2.18 WAMS Communication Network Modeling

Figure 2.6 shows the skeletal network model and composition of the smart grid in a wide geographic location such as the United States map.

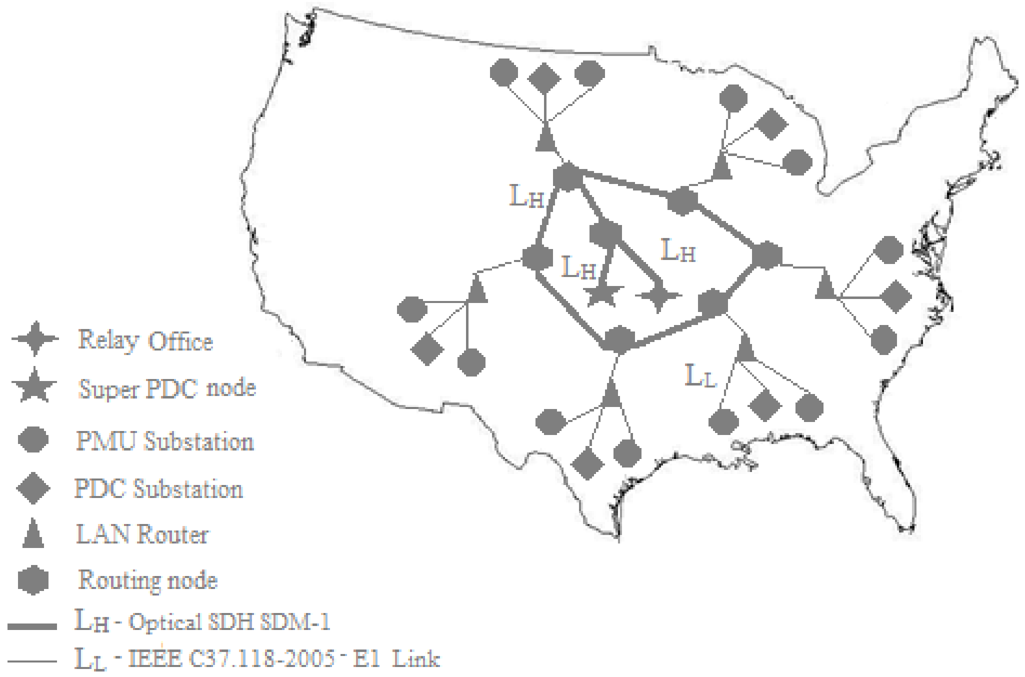


Figure 2.6 Skeletal network model of the smart grid in the map of the United States.

Formed as a ring topology of an optical fiber network implementing SDH, Routing Nodes (RN) are shown in an octagon pattern, which is located in backbone network [2]. Each RN contains a variety of numbers of high performance networking routers. Two different RNs are linked over LH as 155.520 Mbps SDH STM-1. In addition, there are triangles indicating the LAN routers. The circle and rhomb nodes illustrate the PMU substation and PDC substation nodes, respectively. In other words, the PMU substation nodes indicate ones without PDC while the others include the PDC as well as the PMU. One PDC substation node is located in any specific area and the same regional area substations are linked to one routing node. Substations and RNs are linked via L_L modeled as 2.048 Mbps E1 links, which can be modified to L_H if needed. In particular, only one SPDC is considered in the WAMS as high-level monitoring. The same L_H link also connects the SPDC and the corresponding RN.

Chapter 3. **Overview of PMU Security**

Secure real-time data measurement and transmission is required in a smart grid. Thus, a great deal of security and measurement protocols are applied to PMUs to protect and increase the safety of monitoring data. These protocols constrain heavy computation and time and energy consumption, and result in many other limitations to the PMUs. All these constraints, as well as some application PMUs such as real-time data delivery, lead to a tradeoff between energy consumption and the level of security. Consequently, the safety of measured data could not be guaranteed and different security threats would affect the integrity of data. More details on the balance between security and energy consumption, as well as different security levels of PMU monitoring in a smart grid, are discussed in [19]. The authors have classified the level of sensor node security into four groups: level zero, non-security service; level one, single security service (one encryption or authentication); level two, double security services (one encryption and authentication); and level 3, triple security services (two encryptions and authentication). Each of these levels would be required for specific type of WAMS sensors, and not all the security algorithms are needed for all sensors. As a proof of this classification, the level one authentication by digital signature, is the only security algorithm included in IEC 62351. Also, the integrity and tamper detection can be ensured by authentication and digital signature. More details on synchrophasor protocols, communication protocols, and security standards were discussed in Chapter 2.

With respect to [20], availability is one of the fundamental security objectives of data. However, any lack of functionality in monitoring systems such as power outages in the PMUs leads to not delivering the real-time data. It also causes inaccuracy in the continuous monitoring data and the smart grid in general. In this regard, a UPS-like power source is the suggested solution indicated in [5]. Storing system files and momentary acquisition files on separate storage are organized in order to recover the corrupted data.

The goal of this paper is to improve a cost-effective PMU-like device. In addition, the GPS receiver plays a key role in time-stamping and synchronizing of the measured data by PMUs. In addition, the environmental conditions of measuring humidity, temperature, power quality, etc., play a key role in the PMU functionality and accuracy of measured data. The authors also suggested the VPN tunnel implementation in order to achieve the authentications and security, although it has to carry the tunnel data and it reduces the MTU.

In [21], the authors explored how reconnaissance attacks, packet injection attacks, and denial of service attacks on PMUs and PDCs can affect the wide area monitoring systems and wide area protection systems, as a part of such systems. All mentioned attacks experience losses in the visibility of power and control systems. The authors recommended some cyber security testing of PMUs and PDCs to reduce these vulnerabilities. For instance, containing SSL and IPSEC features in order to achieve integrity and confidentiality is recommended. Moreover, the U.S. NERC - CIP states that entities should recognize the Cyber Security Assets (CCAs). Thus, PMUs and PDCs, as added systems, must decide if they are CCAs, which relates to the specific application that would implement the synchrophasor data.

The details of the above-mentioned attacks and the proposed solutions of the authors are explained below.

- Reconnaissance Attacks: Reconnoitering and identifying the system before attack by cyber attackers is defined as a reconnaissance attack. It leads to finger printing the connected systems and learning about opening ports, as well as maintaining remote operating system versions and remote network stack daemons. For testing these attacks over PMUs and PDCs, NMAP has been used [22]. The MODBUS address and MODBUS point are also scanned. The Wireshark network protocol analyzer is applied for catching the plaintext passwords in flight between remote systems, the PMU and the PDC. A password is required for authentication prior to remote access and control [23]. In addition to the information obtained by eavesdropping on IEEE C37.118 network traffic, attackers could access the PMU location. The IP addresses of PMUs and PDCs are identified in NMAP by an insider or network penetrator. Regarding the authors' idea, putting SSL or IPSEC between a firewall at the substation and the remote control room to encrypt network traffic is suggested as a solution for this type of attack. However, the traffic of the control room LAN or substation would not be encrypted. Although the authors believe in the essence of encryption algorithms, to the best of our knowledge, IEC 61850 90-5 is not a suggested encryption algorithm due to implementation constraints and the importance of real-time data transmission in the smart grid over PMUs.
- Packet Injection Attacks: sensor measurement injection and command injection are defined as two types of Packet Injection Attacks. As the name implies, injecting

false sensor data and commands into the control system defines each type, respectively. Also, the attackers aim to inject false supervisory control actions into a control system and overwrite the C code, ladder logic, and the register settings of a substation’s devices such as PMUs, PDCs, IEDs, etc. This attack is achieved through a PDC or multi PMUs. Ettercap, as a man-in-the-middle attack node, is implemented to alternate the IEEE C37.118 frame of data to invalid measurement, and inject and transmit from PMU to PDC. Some of the PMUs contains MODBUS or DNP3 interfaces for remote monitoring with no cryptographic signatures which would be vulnerable to a man-in-the-middle attack. IPSEC and SSL are recommended for each node. They lead to confidentiality and integrity [21]. Recently, IEC 61850 is considered as a communication protocol of a substation’s LAN between PMUs, IEDs, relays, etc. and the router. This protocol includes the security part by cryptographic signature, which obviously reduces the possibility of such an attack. In the previous chapter, these standards as well as their vulnerabilities were discussed in detail. As another countermeasure for a false data injection attack to mitigate its effect on the estate estimation process, in [24], the authors introduced a novel algorithmic process for the trust metrics attributed to the agents. Their method is based on a multi-agent filtering scheme. For this, intelligent agents, such as PDCs which are in the communication network with SCADA and receive measurement from PMUs, apply a trust metric to their neighbors. In other words, they compute local estimation of the state based on both their own measurements and those of their neighbors. Hence, it is based on the long-term performance of the agents. Any untrusted agents’ measurement would be discarded in the future as the filtering pattern. Also, low trusted agents have less impact on evaluating the estate estimation. Thus, the multi-agent filtering and trust-based mechanism are combined. In [25], the author presented another approach for dealing with and detecting false data injection attacks on DC state estimation. In addition, another type of injecting the false data includes the Time Synchronization Attack and GPS Spoofing, which attack the synchrophasor measurement systems by forged GPS signals. More details of these attacks are further discussed in this chapter.

- Denial of Service Attacks: generally, any distraction of communication links between remote terminal units and master terminals or human machine resources is defined as a DOS attack, according to [21]. A DOS attack leads to non-responsive hardware and software in control systems. In synchrophasor devices such as PMUs and WAMPAC systems, it leads to loss of visibility and breaks the control loop, respectively. Thus, the automated event detection algorithm would be blocked. The MU Dynamics MU-4000 Analyzer [26] has been implemented for evaluating and testing denial of service. The database of the analyzer indicates some known DOS attacks such as LAND attacks, tear-drop attacks, ICMP attacks, etc. which are experienced in PMUs and PDC as well. The tests also included the man-in-the-middle attack. Different methods for testing DOS attacks are presented in the paper. For instance, fuzzing as a protocol mutation method is discussed. In fuzzing, network packets are created randomly and assigned all alternate values of the packet fields. The goal is to evaluate all the value possibilities prior to being discovered by an adversary. This method could vary based on different devices. ARP, TCP, UDP, IP, ICMP, DNP3, MODBUS, IEEE C37.118, and HTTP are the mutated protocols for the PMU and PDCs. Some of the recognized problems of fuzzing include crashing of individual network services, crashing of applications running on devices, and unintended soft resetting of affected devices. The authors recommended analyzing the protocol mutation of all PMUs before inserting them in the network. As another method, all the devices become non-responsive when there is a huge volume of traffic, although they will react differently such as reset and hang. The experimental results showed that PMUs and PDCs become more non-responsive in the presence of huge network traffic. As a result, packet rate has to be considered in planning these systems, and the maximum accepted level of traffic congestion has to be evaluated within the substation. Human administrators can control and mitigate the packet rates while observing systems. The traffic between the PMU and the PDC could automatically be configured, although the possibility of closing the port carrying critical traffic is also considered by the authors. Moreover, transmitting and time-stamping a great deal of measurements leads to not meeting the requested accuracy of one microsecond with respect to IEEE C37.118 and increases the delay. Since PDC will drop any delayed packets and begin to interpolate, testers have to be sure about the queue level of PMU packets. Redundancy is revealed as another approach dealing with DOS attacks [27]. However, the network complexity and scalability would be affected, which has to be considered in network design.

The authors of [27] also believed in having a high level of resources for dealing with latency and security issues from the availability point of view. A wireless scheme of DOS attack is named a PHY attack in [28]. The authors have classified the PHY attacks in four groups: eavesdropping, jamming, restricting access, and injecting. Any malicious performance impacting the wireless network communications is defined as a PHY attack. Since the wireless medium has a shared nature, everyone in range can interrupt transmissions. This could possibly done by simply injecting false data.

The Data Integrity Cyber Attack is another type of attack in a smart grid, as demonstrated in [29]. In a Data Integrity Cyber Attack, the attackers change the measurements and readings of some cooperating and compromised power meters. These cyber-attacks are essentially unobservable. They could pass over any bad data detection algorithms to remain unobservable. Obviously, this leads to a great deal of mistakes in state estimation algorithms. Known and secure PMUs located in certain buses are implemented in this research. In this paper, finding the minimum number of PMUs with the goal of mitigating such attack is discussed. PMUs are networked on the newer NASPInet architecture for secure data transmission. The authors show that p+1 PMUs at certain chosen buses could neutralize the group of p cyber-attacks.

Evaluating and investigating the traffic features such as time, volume data, etc. on links and finding their correlations leads to another type of attack in synchrophasor measurements, called Traffic Analysis Attacks [30]. The relevant parameters, such as number of packets, could be released by dividing the time into fixed size across two links. In synchrophasor measurements such as PMUs, whether any encryption algorithms are provided or not, the timing transmission data would be released by traffic analyzers.

Moreover, random delays or similar approaches would not apply to the real-time data. As a passive attack, attackers can identify the network hosts such as PMUs as well as their locations. Consequently, those identified nodes could be attacked. Mixing the data concatenation and dropping the selective ones is suggested as a countermeasure for these challenges in [30]. Therefore, the same size packets periodically generated in the PMUs make the correlation process simpler for adversaries. As a countermeasure, PMU random size single packets are produced by concatenating the random number of contiguous measurements. However, the maximum required network latency is as defined by the maximum number of measurement data to be concatenated. Thus, data concatenation thwarts any size correlations. Encryption is also suggested to destroy the packet content correlations.

Regarding the importance of synchronization in the smart grid, the authors in [31] challenged and analyzed the impact of Time Synchronization Attacks to WAMS in the smart grid. Accurate timing information has a significant impact on fault detection and event location estimation in the smart grid. Thus, the well-known GPS spoofing is one of the highly probable attacks in smart grid measurement systems. The three main functions of PMUs, namely fault detection in the transmission line, monitoring the stability of voltage, and event locationing, could be affected by TSAs. GPS receivers play a key role in PMU operations. However, by injecting forged time signals, an attacker could alternate the time samples. Although much research has identified the possibility of a GPS spoofing attack, [32] recently studied a real and practical one. Also, a complete GPS spoofing attack as well as experimental results are examined in [33]. No physical contact, hacking or authentication is required. The attacker only needs to move around the Time Synchronized

Measuring Devices (TSMDs). The problem is that most of the TSMDs are only resistant to the noise and loss packets. Smoothing filtering as a suggested countermeasure is suggested in [31].

In addition to GPS spoofing, GPS jamming is also studied; however, GPS jamming is not as distressing as spoofing due to its elective error effects compared with false decisions of spoofing. In [34], the GPS Spoofing Receiver Clock Offset of PMUs is discussed in detail. Since the PMU measurement would be synchronized and time-stamped by implementing the clock offset, incorrect time information leads to incorrect phasor computations of voltage and currents.

The GPS received signal is used by PMUs to evaluate its position and clock offset with the onboard satellite clock. The goal of the authors is to maximize alternations among the receiver's clock offset with and without attack. As the most difficult attack to detect, according to the authors' opinion, any number of observable satellites are highly vulnerable. An attacker could increase the power and number of malicious signals to any number of victims. The maximum phase differences based on spoofing are also evaluated by authors. While the proposed attack is based on changing the encoded data and not the signal characteristics, the authors of [35] defined another type of spoofing, namely the Replay Attack. This attack is based on inserting a delay in satellite signals and not modifying the encoding process. Since the attacker manipulates the delay of signals and not their content, having a closely calculated position relative to that before the attack is impossible through a few number of visible satellites. The receiver would alarm in the presence of huge and sudden changes and jumps possibly made by an attacker. Thus, the proposed formulation of a spoofing attack in [34] included some restraints to overcome the alarm systems.

In addition to jamming and spoofing, blocking is named as another vulnerability of GPS systems that could disturbance the correctness of PMU measurements. It is defined as blocking the GPS signal to be received by the GPS system antennas in a phasor network and in PMUs. Thus, strong physical security is essential, such as placement of antennas and using physical security sensors. The authors also suggested different timing sources as a solution for spoofing and jamming. These could be supplied from installed devices in substations or some PMU ports, e.g., management ports [3].

In [36], the authors pointed out how important effective cybersecurity solutions are in terms of cryptographic key management, authentication, and encryption for SCADA and PMU.

According to the critical role of topology and state estimation in real-time operation of control centers and the smart grid, a novel cyber-attack called a State and Topology Attack is introduced. By modifying the network data and state, an attacker deceives the state estimators' parts. As a result of a topology attack, a connected transmission link could be configured as disconnected or vice versa. In this event, there is an improper delay response or load shedding by the control center. Therefore, an undetectable state attack is achievable while an undetectable topology attack is executable. The authors in [37] and [38] also investigated the significant impact of state and topology attacks on real-time pricing. [39] claimed that changing the meter data such as PMUs measurements, which leads to incorrect state estimations, would not be detected by control centers. However, the adversary has to overcome bad network and meter data detectors in power systems. Secure placement of

PMU is suggested by the authors of the paper in order to achieve the secure measurements' resistance to a man-in-the-middle attack as well.

The paper assumed the possibility of attacking all measurements except those from secure PMUs. They believed that buses with secure PMUs which construct a vertex of cover of topology are able to recognize these attacks. In recent years, many studies have proposed countermeasures for undetectable state and topology attacks [40, 41, and 42]. In particular, secure PMUs are suggested and investigated by numerous researchers [29, 44], although algorithmic methods are also proposed. While a countermeasure is successful on a topology attack, a state attack would be prohibited as well. The proposed methods are based on current graph algorithms as well as the graph of both the connected and disconnected links. These methods allocate some instruments to illustrate the optimal secure PMU placement in which the vertex cover would be minimized. Those devices are installed on a group and subset of line flow and injection meters.

In [45], a greedy algorithm is proposed that simplifies secure PMU placement. These PMUs and the algorithm are presented as an avoidance of a Data Injection Attack. Detecting the data injection is harder in the presence of measurement noise in the environment.

With respect to all the above mentioned attack scenarios as well as proposed solutions, potential attacks would not be neglected. To be sure about the reliability of received measurements and dealing with their respective consequences on state estimations, in [46], the authors proposed a credentials scheme based on a Chi-square test. Regarding the Chi-square test, any measurement satisfying the statement below could be defined as a damaged measurement with a certain confidence:

$$J_i\ (x_i) > \chi^2{}_{m\text{-}n,0.05}$$

where:

i^{th} measurement is damaged,

m-n: degree of freedom while m is the number of overall states, n is the number of redundant states,

$J_i\ (x_i)$ objective function defined as: $e_i^{T} \cdot R_i^{-1.}\ e_i$

$e_{i:}$ the measurement error vector,

x_i : the state vector to be estimated in subsystem I, and

R_i^{-1} : a weighted matrix which corresponds to the inverse of the error covariance matrix.

They claimed that any changes in PMU measurements lead to significant changes in objective function. When faced with any attack, conventional measurements would be considered instead of the received ones. Thus, the precision of estimation and measurement is based on a state estimation solution before the attack occurs.

In [3], message availability and integrity are introduced as the main objectives of the WAMS network. One feature of trusted time-stamped measurements is related to the GPS system reliability, as well as the robustness of both the PMU and PDC from a hardware and software point of view. A non- properly functioning GPS leads to invalid real-time data and lack of WAMS visibility.

Moreover, authentication is considered as a part of configuration management of PMUs in the NERC-CIP. The authors of [3] claimed that the recovery of PMU and PDC from cyber security attacks is not yet known and considered.

To achieve availability, the whole power grid coverage of PMUs is another controversial issue. The topic of PMU placement in power electronics has been discussed by several researchers. Also, some researchers have investigated the placement of PMUs in the power grid at several locations, e.g., the U.K., Korea, and India [47], [48], and [49].

Human intervention is another concern that leads to lack of integrity, incomplete measurements, and non-proper functionality of the network. Another vulnerability is based on different communication infrastructures implemented in WAMS networks such as SONET, analog microwave, and VPN.

As a one-way communication protocol with push technology, the environment is much more predictable and secure compared with SCADA. Most of the PMUs restart after any configuration modification. Thus, any recently restarted PMU would be identified through health monitoring tools which are designed to detect any PMU failure quickly and in near-real time [3].

Chapter 4. **Side Channel Attack on PMUs in Smart Grid**

4.1 An Overview of the Security Requirement in PMUs:

Regarding the discussions in the previous chapter, the lack of an authentication mechanism leads to undesired injection and changes in PMU measurements which decreases the correctness of the situational awareness of the entire power grid as the main goal of wide area measurements. The most important security mechanism, authentication, is vulnerable to Side Channel Attacks (SCAs) from different points of view. A brief introduction and literature review on different types of SCAs is presented below. Since HMAC is suggested as an authentication algorithm for PMU measurements, literature reviews on SCAs in this chapter mostly cover the HMAC's vulnerabilities.

4.2 Introduction to Side Channel Attacks

The physical constraints of implementing cryptographic algorithms in real-life devices lead to new cryptanalysis concepts in security. In [50], the authors believed that these types of attacks were more efficient than the well-known classic type of cryptanalytic primitive attacks since experts and professional hackers have investigated and analyzed the algorithms themselves for many years. Thus, attackers focused on the hardware and software implementations of cryptographic algorithms. Generally, primitive attacks are classified into classical and physical attacks. Introduced by Kocher, physical attacks refer to the specific features of a given environment such as the processor used, which releases the secret information of the device related to the computations of the security algorithm.

Execution time, power consumption, and electromagnetic fields are some of the main constraints utilized to expose the secret information of the devices. Although this is limited to specific implementations, it is more powerful than classical ones that are only related to the algorithm itself. In other words, there is a correlation between the physical measurements and features taken in different intermediate points of the implemented algorithms and the secret key related information. For instance, a variety of security protocols include different cipher suites to ensure the correctness of the communicated data irrespective of implementation, whether they will run on processor or custom hardware, or whether any intermediate registers and memory will be used [51].

Physical attacks or side channel attacks are defined as having two phases: an interaction that exploits the physical characteristics, and an exploitations phase that investigates the measured values in the previous phase and correlates them to the secret information. Moreover, this type of attack could be categorized as general and specific. Since they could apply to any similar devices of similar physical principles, they are categorized as general. However, specific practical implementations of each security algorithm categorize them as specific.

Divide-and-conquer attacks are generally used by these types of attacks to recover the secret key part by part. Regarding this method, the partial key, the independence of the remaining partial key, correlated with observable physical characteristic of the leakage, are retrieved. Next, another partial key is retrieved through the same process. Thus, a divide and conquer attack could be iterative or non-iterative. Iterative is more vulnerable to error in previous rounds and makes the entire key incorrect in the presence of any previous errors.

The exploitation phase is mostly based on two methods: a simple side channel attack and a differential side channel attack [51]. A simple side channel attack (SSCA) is related to the physical features of the operation itself and key-related information is released by tracing the leakages. Since the presence of noise in practice can interrupt the SSCA results, many statistical methods are applied by an attacker to overcome the effects of noise, resulting in a so-called differential side channel attack (DSCA). DSCA is more practical than SSCA and releases the secret key, or key-related information, based on processed data. Thus, the correlation between the secret data and leakage exploited by DSCA uses a hypothetical model as well as a statistical model to increase the efficiency. The side channel output is calculated by a hypothetical model. Regarding the side-channel output taken from the hypothetical model, the authors have named it a "first-order attack," "second-order attack," and "higher-order attack" while one, two, or more output parameters, respectively, are utilized for the attack.

Consequently, even a well-known cryptographic algorithm could not guarantee security. The device carrying the algorithm has to be evaluated from a different point of SCA view with respect to the variety of implementations.

Regarding the device environment, one type could be more practical than others. For example, power analysis should not be a big concern of a device located in a highly secure room, while EM analysis should. As another example, many of the sensors and actuators in a smart grid are at the risk of a differential power analysis attack.

4.2.1 History of Side Channel Attacks

Even though SCA is a recent term in the security discipline (circa 1998), SCAs were part of the spy operations of the British Secret Service (MI5) close to the Egyptian embassy in London during the Suez Crisis. They planted bugs near the cipher machines and captured noise and clicking sounds made by them to decode the secret information. Moreover, EM signals of cipher devices were monitored aound the French embassy in London, and the plaintext data were detected before any encryption algorithm [54]. For many years, the Soviet Union listened to the American consulate in Moscow through wooden seal prepared for the U.S. Ambassador [55]. It was hung in the ambassador's office after examining it for covert transmitters and finding it to be clean. However, the seal included a cavity that vibrated with any sound in the room, transmitting a radio beam, and recreating sounds and conversations.

4.2.2 General Assumptions in Side Channel Attacks

We assume that a cryptographic algorithm is applied on a secret key which is stored in the device and hidden to the attacker. However, the attacker would know about the cryptographic algorithm and the implemented hardware and software. Also, the attacker has access to the device at his disposal and can run the device for several required times to extract enough information, possibly by the optional input data. This could result in complete control of the device, like stealing a smart card, or be hidden and monitoring the electromagnetic fields around the target running device from a distance, or investigating the time between the request and answer of a device. To put everything in a nutshell, Kerckhoffs' well-known assumption summarized all the security information of the entire device to the secret key, which means that the attackers have complete knowledge of the cryptographic algorithm, implementation, etc. [50].

In the rest of this thesis, the vulnerability of timing side channel attacks over a C code HMAC algorithm, applied to the PMU security protocol of IEC 62351, is evaluated. In the following, after a brief description of timing, power analysis, and EM attacks, related timing SCAs over several cryptographic algorithms, as well as other types of SCAs such as Differential Power Analysis, are discussed.

4.3 Introducing Popular Types of SCAs

4.3.1 Timing Attack

The idea of a timing attack was first introduced and investigated by Kocher in [52] which indicates that the execution time of a cryptographic device released the secret information about the key. Since the device is assumed to be at the attacker's disposal, a bunch of messages can be processed by the target device to exploit the corresponding time. If the attacker can provide the precise clock ticks of the device through its terminal, the precise timing information would be obtained more easily.

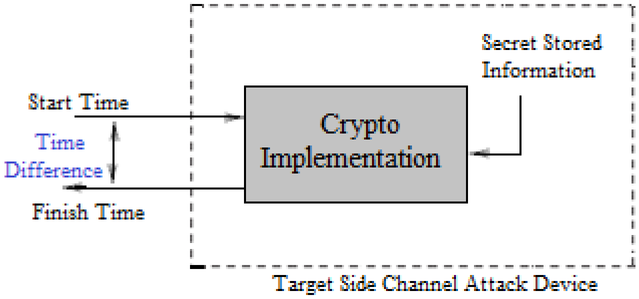


Figure 4.1 Timing side channel attack.

The overall execution time of an algorithm consists of the summations of different running times corresponding to the steps of algorithms as random variables. The computational time up to step S is executed based on the guessed key to be subtracted from the total time. Thus, the exactness of measured time plays a key role in timing side channel attacks. The observation probability would be generalized from different characterizations whether the guessed key is correct, and would reduce the variance, or not [50]. Since Kocher, different researchers have improved the practical timing attack on a variety of encryption algorithms such as CASCADE smart cards [53]. Revealed by the encryption implementation, timing information helped an attacker to break the key though a smaller amount of guess-work. The authors of [54] believed that timing information about inter-keystrokes decreased the number of guessed keys down to 1/50 on average compared with brute force attacks.

4.3.2 Power Analysis Attack

It is clear that the power tracing of an executed algorithm is expected to reveal the secret information in a power analysis attack. As mentioned above, power values illustrate more information about power consumption per time unit while timing is only about the leakage of the scalar value of time. Thus, more dimensional power information leads to a more efficient attack, although it costs more for processing and storage. Differential Power Analysis (DPA) and Correlation Power Analysis (CPA) have been discussed in a large number of resources and publications [56]. DPA was first introduced by Kocher [57], who formalized it in [58]. In general, power analysis is expected to be correlated with the assumed leakage model. For instance, CPA is based on the correlation between power leakage and data Hamming weight. Thus, the accuracy and correctness of the predicted model, model fitting, plays a significant role in effectiveness as well as the efficiency of an attack. Therefore, the variety of statistical tests of distinguishers, with respect to the author of [59], is demonstrated through a Difference-of-Means test, or Pearson's correlation coefficient or Gaussian templates. By comparing different distinguishers, the authors prove that the results are asymptotic; however, they highly affect the attack efficiency.

4.3.3 Electromagnetic Analysis Attack (EMA)

Introduced by Quisquater and Samyde [60], EMA takes advantage of EM fields around the crypto implementation to access the stored secret data. The core idea is based on placing a coil around the device and analyzing the measured EM fields through Simple EMA (SEMA) or differential EMA (DEMA). One interesting issue about EMA is its capability of attacking from a large distance of about 15 feet without any de-packaging of the target device, although it needs a professional EM probe to reduce the noise effect. A broader perspective of EM leakage attacks and methodologies is presented in [61]. Since EM leakage provides more information on cryptographic implementations, the authors claimed that it would individually be enough to break the algorithm's implementations, compared with power and timing attacks. In other words, timing and power attacks exploits the one scalar running time leakage and single-dimension power consumption per time unit, respectively. However, four dimensional features of the device, including spatial locations and time, are released by EM leakage. The EM side channel signal over CMOS devices is quantitatively modeled and applied for improving and experimentally analyzing the other security devices such as smart cards.

4.4 Literature Review on Side Channel Attacks

4.4.1 EM and Power Analysis Attack

As mentioned above, Timing, Power and Electromagnetic analysis are three main types of SCAs. An EM analysis attack for smart cards is designed and tested in [62]. The implemented system calculates the EM fields radiating around the smart cards that carry the 3DES encryption algorithm as well as estimating their capability to resist an EMA attack. HMAC-Whirpool susceptibility to a power analysis attack, based on most common methods named DPA and CPA, is demonstrated in [63]. In addition to timing SCA vulnerability, RSA is susceptible to power analysis even though many countermeasures are proposed [64]. The DES encryption algorithm is another algorithm considered against DPA in many publications since it is implemented via a nonlinear substitution box [65]. In [66], the authors simulated the DPA attack against the HMAC-SHA2 family through the Hamming distance leakage model. Implementing authentication algorithms such as HMAC involves combining a variety of algebraic functions and no look-up tables. Thus, appropriate function-released intermediate values related to secret keys must be selected. A group of operations such as XOR, addition modulo 2^n, modular multiplication, etc. are simulated and practically experimented against DPA in [65].

In [72], the power consumption leakage of Xilinx Spartan-3e FPGA carried MAC-Keccak is practically tested. For this purpose, each round of algorithm, including operations, and their level of vulnerability to power consumption leakage, were evaluated in detail. Also, the optimum key length to reach the minimum leakage probability as well as the correlation of key size to attack difficulty, defined as the ratio of the unknown bits to an adversary to known ones, were analyzed. In other words, while a smaller length of key is a better target of a brute force attack and a larger one consumes more energy and cost, no maximum key length is suggested. Thus, they investigated the optimum size from a side channel point of view, and concluded that security will not increase for every larger key length due to more leakage and information revealed to the adversary.

The authors believed that target operations for SCA in each round must depend on both known values to the adversary and unknown secret information. Also, linear operations such as XOR are not a proper target of SCA. Finally, several techniques to mitigate side channel leakage were demonstrated.

4.4.2 Timing Attack

One of the typical examples of an SCA is against smart cards. Being light weight, easy to carry, a target for pickpockets, causing significant security issues, and easy to monitor are some of the specific features of smart cards that lead to the simplicity of this kind of attack. Moreover, all the information of a smart card could be explored by a simple processor, typically, an 8-bit or 32-bit card reader. Thus, execution time, power consumption, and EM radiations could be revealed in a straightforward manner. The card reader supplies the battery and clock of the card, which makes the attacker able to monitor both power and time consumption, respectively.

Since the RSA algorithm and other public key cryptographic algorithms are working with large values, smaller than even recent CPU word size, different mathematical and arithmetical algorithms are utilized by crypto implementations. Even though they speed up the encryption process, timing attack probability is increased. Using RSA with Montgomery reduction algorithms, to increase the speed of operations, is another well-known example of timing attack vulnerability. It is an intuitive but not optimal attack to get the secret modular exponent d of RSA. A square and multiply algorithm is implemented for performing modular exponentiation in order to pinpoint the weak points of the algorithms [50].

Algorithm: Square and Multiply [50]

```
1. x = m
2.  for i = w-2 down to 0 do
3.       $x=x^2 \bmod n$
4.       if $d_i$ == 1 then
5.           x = x.m mod n
6.        end if
7.  end for
8. Return x
```

Depending on different inputs, any intermediate results bigger than the modulus lead to an extra subtraction which increases the consumption time. Thus, whether any final reduction is required or not, two sets of execution time named as “long ones” and “short ones” are provided. Next, the first unknown bit is assumed as 1, which requires the multiplication by m in line 5 of the algorithm above. It could be either long or short based on the m value. Since no secret information is required in this step, many messages are evaluated in an iterative process and grouped in one of two sets. The "long ones" set is expected to be executed in a longer period of time than the "short ones." The remaining bits are considered as noise since they depend on secret information and cannot be simulated. All the above results are based on the first assumption of the first bit equal to 1. Consequently, the execution time of two sets of long and short would not result in significant differences and would be roughly random if the assumption was not correct. After determining the first bit, the same processes are continued for all remaining bits.

As one of the first published resources in this area, timing attacks on Diffie-Hellman, DSS, and other system implementations are introduced in [67]. Although a timing attack against Diffie-Hellman cryptographic schemes is categorized as one of the first ones, dating back to the 1990s, it was experimentally investigated in 2005 by the authors of [68]. Moreover, a variety of conditional statements, branches and loops can apply for implementing and coding a single algorithm, which leads to extensive differences in running time of the same algorithm. Even in a single implementation, the running time of an algorithm reveals information for an attacker while these statements are based on secret information.

Breaking the stored key in an Xbox 360 CPU through a timing attack for a forging authenticator is another practical example of SCAs. It shows that timing attacks are not only constrained network-based attacks to the SSL library, but that software developers as well as embedded system designers have to consider the effects of SCAs. Any other data-dependent behaviors such as cache processing increase the probability of SCA attacks with higher precision measurements [55]. A cache timing attack against AES encryption algorithms was comprehensively investigated in [69]. The reason is that many look-up tables stored in cache are utilized for implementing and speeding up the AES algorithm. However, variable computation time occurs because all tables do not fit into the cache. Whether the requested data is available in cache or not, cache hits and misses would occur, leading to different running times. Even though NIST declared that look-up tables are not susceptible to timing attacks, recent researchers indicated the capability of timing attacks against some AES implementations [70]. However, eliminating look-up tables would not reduce side channel attacks from a power and EM radiation point of view. Another group of algorithms such as hash functions do not make use of look-up tables for implementation. In contrast, addition modulo, bitwise XOR, and shift and rotation denoted by ARX (Addition-Rotation-XOR) are used. The author claimed that those are harder to remain secure against side channel attacks, while applying a limited choice of bitwise Boolean operations, and (cyclic) shifts could be more efficient under some conditions. More details on their assumptions and outcomes are discussed in [69].

Regarding the importance of SCA, different candidates of the NIST SHA-3 hash function competition are asked for efficient operations against SCA in [71] and [72]. Remote timing attacks are also experimented with in [73] to break the 1024-bit RSA in only two hours.

4.5 Countermeasures of Side Channel Attacks

A great many solutions against different types of SCAs are demonstrated, mostly at the algorithm level, although none of them can guarantee complete security even for a single attack. In other words, resistance against all type of SCAs through one implementation is tremendously challenging. Since accessing the secret information is the goal of attackers in SCAs, frequently refreshing a key would reduce the success probability of EM and power analysis attacks, although it does not appear to be a helpful method for timing. In general, countermeasures are categorized into both hardware and software levels. Noise addition, extra shields, removable power supplies, encrypting bus and memory, and randomizing the interrupt processes or clock cycle are some of the suggested hardware countermeasures against a variety of SCAs. Masking, or hiding, the leakage is one of the well-known techniques for making different SCAs unpredictable. Avoiding the attacker to read the intermediate values, blinding is another widely used approach introduced by Kocher [50]. In other words, blinding is referred to as randomly mixing the input data of a crypto algorithm as well as applying the correlated operation to the algorithm's output with the goal of retrieving the correct and expected results. Thus, the attacker would not learn about processing data and its intermediate operation leakage. Also, using nonce in blinding and masking can highly disrupt the correlation of leakage to the adversary. Even though it could prevent an SCA, e.g., timing at a high level, designing the correct correlated operation to reveal the expected result is hard, especially for symmetric cipher algorithms.

A more comprehensive list of solutions against SCAs is presented in [74]. Thus, protecting against SCAs imposes extra cost and overhead which must be considered in countermeasures. In [75], the authors discussed some optimization techniques to decrease the occupied memory in order to minimize the masking overhead related to utilized memory. Several masking methods against DPA are also discussed in [84] in a variety of arithmetical and Boolean operations utilized for implementing AES, SEED, SHA1, etc.

Chapter 5. **Investigating the Timing Side Channel Attacks against PMU Authentication**

For the IEC 62351 security algorithm discussed in the previous chapter, HMAC-SHA1 is a suggested authentication algorithm for signing the measured values by PMUs. In this thesis, the vulnerability of the HMAC-SHA1 authentication algorithm against a timing SCA is investigated. Prior to any further discussions, a brief introduction of the HMAC-SHA1 algorithm is presented.

5.1 Overview of HMAC–SHA1 Algorithm

With respect to NIST documents, FIPS PUB 198 [77] and FIPS PUB 180-4 [78], message M and a key K with any desired length, key length mostly larger than the message digest, are used as the two inputs of the HMAC algorithm, which is defined as:

$$\text{HMAC}\ (M, K) = H\ ((K^{+} \oplus \text{opad})\ ||\ H\ ((K^{+} \oplus \text{ipad})\ ||M))$$

Where:

ipad: 00110110 (36 in hexadecimal) repeated (block size)/8 times

opad: 01011100 (5C in hexadecimal) repeated (block size)/8 times

K^{+} : K padded with zero on left to reach b bits in length of block size

$\oplus$: Bitwise exclusive OR

($K\oplus$ipad) and ($K\oplus$opad) are key variant values prepending to the message and the previous output of the hash value, respectively. The hash function of the above equation might be any SHA1, SHA3, SHA256, SHA512, etc. HMAC-SHA1 is assumed in the following as a suggested authenticator of PMU's measurement transmitted to the PDC via IEC 61850.

Since a variety of lengths of message M is acceptable as an input of HMAC-SHA1 and the message has to be divided into an integer number of the same block size, the message is padded by one bit of 1 followed by the required number of zeroes to complete a block size, or 512 bits in HMAC-SHA1. In addition, an extra 64 bits is padded at the end of the message, indicating the initial message length. Figure 5.1 illustrates the HMAC-SHA1 algorithm:

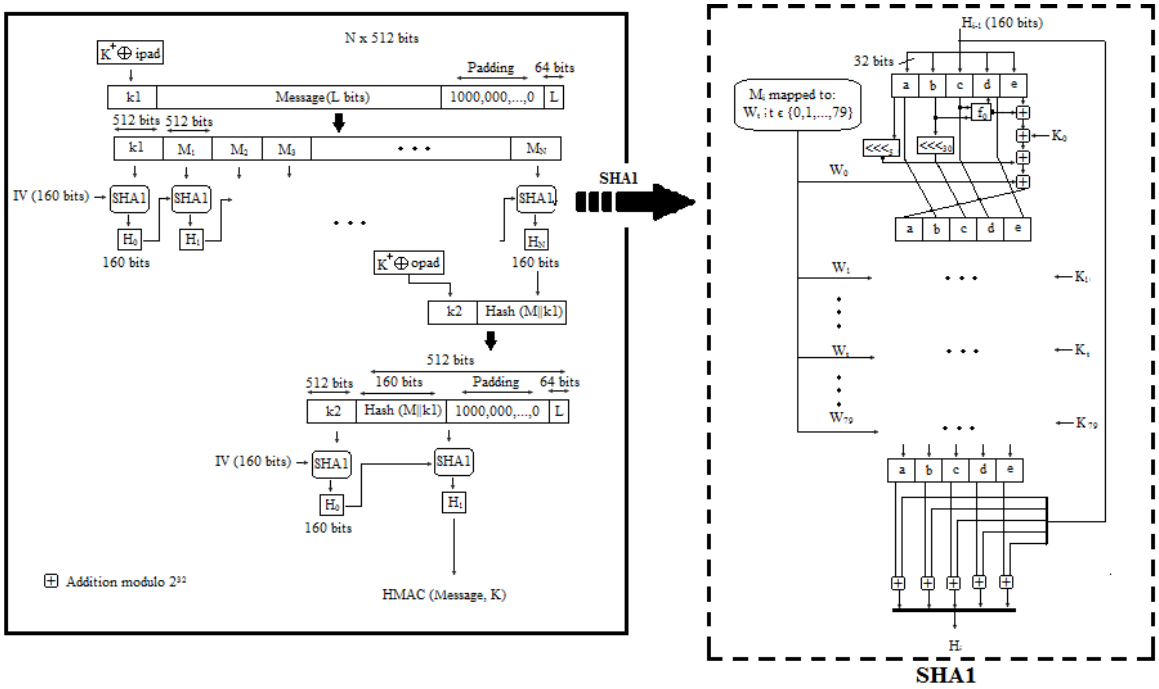


Figure 5.1 HMAC-SHA1 overview.

Where:

$$\mathrm{Wt} = \begin{cases} \mathrm{Mt} & 0 \leq \mathrm{t} \leq 15 \\ ROTL(\mathrm{Wt} - 3 \oplus \mathrm{Wt} - 8 \oplus \mathrm{Wt} - 14 \oplus \mathrm{Wt} - 16) & 16 \leq \mathrm{t} \leq 79 \end{cases}$$

$$\mathrm{Kt} = \begin{cases} 5a827999 & 0 \leq t \leq 19 \\ \mathrm{6ed9eba1} & 20 \leq t \leq 39 \\ 8f1bbcdc & 40 \leq \mathrm{t} \leq 59 \\ \mathrm{ca62c1d6} & 60 \leq \mathrm{t} \leq 79 \end{cases}$$

$$f\mathrm{t}(x, y, z) = \begin{cases} \mathrm{Ch}(\mathrm{x}, \mathrm{y}, \mathrm{z}) = (x\ AND\ y) \oplus (\mathrm{NOT}\ x\ AND\ z) & 0 \leq t \leq 19 \\ \mathrm{Parity}(\mathrm{x}, \mathrm{y}, \mathrm{z}) = \mathrm{x}\ \oplus \mathrm{y}\ \oplus \mathrm{z} & 20 \leq t \leq 39 \\ Maj(x, y, z) = (x\ AND\ y)\ \oplus (\mathrm{x\ AND\ z}) \oplus (\mathrm{y\ AND\ z}) & 40 \leq \mathrm{t} \leq 59 \\ \mathrm{Parity}\ (\mathrm{x}, \mathrm{y}, \mathrm{z}) = \mathrm{x} \oplus \mathrm{y} \oplus \mathrm{z} & 60 \leq \mathrm{t} \leq 79 \end{cases}$$

$$\mathrm{H0} = \begin{cases} 67452301 & a \\ \mathrm{efcdab89} & \mathrm{b} \\ 98badcfe & \mathrm{c} \\ 10325476 & \mathrm{d} \\ c3d2e1f0 & \mathrm{e} \end{cases}$$

As shown in the figure, the first block is the only key-dependent value, which can be calculated and stored in a register once updating the key. It speeds up processing and delivering the real-time measurement of PMUs since it is not required to calculate hashing of $K^{+}\oplus$ipad of each measured value separately. In the same way, $K^{+}\oplus$opad is also pre-computed by the processor and registered. Then, each block of messages is inserted into a hash function as illustrated.

In addition, there is a tradeoff between frequently updating the supplied key and SCA vulnerability. In particular, it leads to revealing more leakages because K+$\oplus$ipad and

K+⨁opad must be pre-computed and registered to speed up process. However, more frequently updating key cause to more leakage to reveal for attacker.

5.2 Previous Work on Timing Attacks against HMAC-SHA1

To the best of our knowledge, previously discussed timing attacks on the HMAC algorithm are limited to comparisons of digest data. In other words, without any knowledge of the utilized key for signing a measured value, an attacker can find the correct signature of the desired plaintext by evaluating the consumed time to compare the received signature by an attacker and the expected one in the receiver side and not the execution time in the sender. Regarding byte wise comparison in high level language, the comparison loop should be terminated early if any element is not matched. In contrast, the comparison loop should continue while all bytes of received signature and expected ones in the receiver are the same. It leads to leakage of time when the attacker is resubmitting large numbers of guessed digests iteratively and monitoring executed time. Thus, an attacker can get the expected signature of a desired fault value by comparing the execution time of each individually guessed byte of signature, assuming the remaining to be zero, without any knowledge of the secret key. The predicted byte is assumed as an expected one if longer time is consumed by the processor.

Although secret key information is not required in performing this type of timing side channel attack, the entire attack process is required for each individual fault data that is willing to be inserted into the recipient by the attacker.

Obviously, this type of attack could be simply spoiled. For instance, a comparison function should not end in occurrence of any dissimilarity. Also, the XOR function could be applied over the received signature and the expected ones. Thus, the received signature is correct if the XOR output is equal to zero.

5.3 The Analysis of Timing Attacks on HMAC-SHA1

Regarding the above mentioned drawback, our contribution is targeted to the HMAC-SHA1 algorithm itself, with the goal of retrieving some information about the stored key length and Hamming weight. The number of bits turned one in data is defined as the data Hamming weight, while the Hamming distance is the difference of Hamming weight between two codes that are calculated by the XOR of both codes. Data leakage can be observed in SCAs by the number of bits turned to one.

5.3.1 Attack Description

This thesis examines the weakness of the HMAC-SHA1 authentication crypto implementation algorithm from a leakage of execution time viewpoint. The attack includes two phases, named the interaction and exploitation phases, which are explained below.

- **Interaction Phase:** In this phase, the physical feature, i.e., execution time of the algorithm, is exploited. For this, 48 samples including 48 different numbers of values, as input measurements, and 48 different keys are assumed. In other words, each sample has a different Data Length (DataL), Data Hamming Weight (DataHW), Key Length (KeyL), and Key Hamming Weight (KeyHW). Therefore, the signature of each sample could have different Hamming Weight values as well, called DigestHW. Since the encryption algorithm is not considered in IEC 62351, the attacker can simply access each pair of samples and corresponding execution times. Next, these 48 samples are applied to the algorithm and corresponding execution times are measured.

- **Exploitation Phase:** In this phase, the correlation of results obtained in the interaction phase with secret information is investigated. Introduced in the previous chapter, DSCA is utilized here. Thus, statistical methods are applied to the previous results to demonstrate the correlation between secret data and leakage. For this, two different models of regression, named as Negative Binomial Regression (nbreg) and Linear Regression, are run using IBM SPSS Statistics. Particularly, linear regression models the execution time versus five predictors of DataL, DataHW, KeyL, (KeyHW), and DigestHW, while nbreg models KeyL (or KeyHW) versus other sets of predictors named as execution time (Time), DataL, DataHW, and DigestHW. The reason is that linear regression constraints the output (Time) to be a continuous variable while nbreg does not have such limitation. Moreover, an optimum number of predictors in each model is indicated with the help of backward-stepwise regression. The goal is to estimate the length and Hamming weight of the utilized key in the target device. After fitting these 48 samples on regression models, called training data, another 48 samples are applied to the obtained model, called test data, to investigate the model exactness and accuracy.

5.3.2 Assumptions

- The attacker is able to measure the execution time of algorithm for each desired plaintext. It is the first assumption considered in the first paper in introducing SCA by Kocher [50].
- Execution time is reproducible. In other words, fixed time is assumed for fixed data.
- The attacker has access to the PMU measurement since the encryption algorithm is not considered in all above-mentioned communication standards and security protocols.
- The signature is appended to the measurement data and sent from the PMU substation to PDC through the IEC 61850 communication protocol. Since no encryption algorithm is considered, the attacker can access the corresponding signature, $S_{i,}$ of each desired measurement, M_i. Thus, each pair of ($M_{i,}$ S_i) is accessible by the attacker.
- The attacker has access to the target PMU installed in the PMU substation at his disposal.
- The attacker has full knowledge of the cryptographic algorithm, implemented hardware and software, etc. The secret key is the only hidden information to the attacker.
- The written C code of the HMAC-SHA1 algorithm, released in rfc4634 [76], is used and SCA’s vulnerability is investigated.
- Nanoseconds-level precision of running time is examined over the Linux PC Operating System, Intel ® Core™2 CPU, 6700 @ 2.66GHz, 2.00 GB RAM.

- MATLAB and IBM SPSS Statistics are used for analyzing results and generating graphs.

5.3.3 Selecting the Most Precise Execution Time

Regarding many sources of variance in timing data, several methods have to be considered in preciseness of measured execution time of the implemented crypto algorithm in a given processor. For instance, cache hits and misses, pipelining, branch prediction, register overwriting, counter overflow, out-of-order execution, and many invisible and optimization tasks in programs and compilers lead to significant differences in cycle count and measured execution time of a given cryptographic algorithm such as HMAC [43]. Several solutions such as minimum execution time and average time are suggested against cache effect to go over these system events that affect the cycle count. In this thesis, we consider both iteration and minimum time solutions. All times have been measured after 100 iterations of execution and the minimum time is considered as final. However, these results are compared with the execution time measured from ‘first observed time after booting up the PC’ as well as ‘average execution time of 100 iterations’. Therefore, the most precise execution time leading to better regression model fitting is investigated in the following by assuming three types of execution time corresponding to each sample: first observed time (after booting up the PC), average time of 100 iterations, and minimum execution time of 100 iterations.

In this step, we only model the execution time versus DataL and KeyL through linear regression models based on the least square method. The reason for considering only these two predictors will be shown in Section 5.3.4 Optimum Number of Predictors.

I. Average Time

Table 5.1 Model summary based on average time of 100 iterations. Predictors: (Constant), KeyL, DataL; Dependent Variable: Avg. Time

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.795[a]	.632	.616	21.84841

Adjusted R Square is defined as square of the correlation between the observed (executed time here) and the estimated modeled data values. Regarding this definition, the higher value of adjusted R square, closer to 1, is more acceptable and signifies a better model.

Table 5.2 Coefficient summary based on average time of 100 iterations; Dependent Variable: Average Time

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	-10.839	7.074		-1.532	.132
DataL	.858	.103	.800	8.308	.000
KeyL	-.017	.097	-.016	-.171	.865

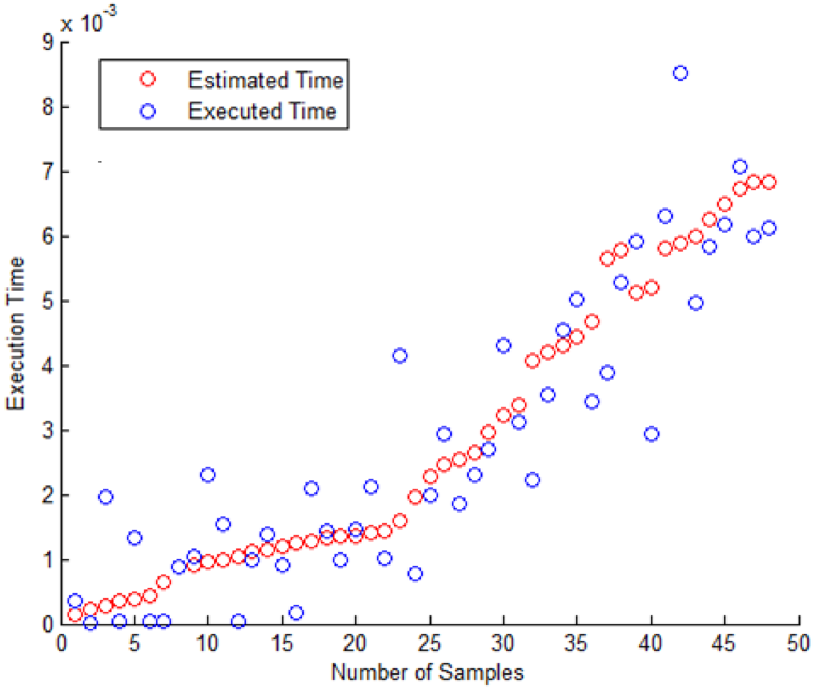


Figure 5.2 Equivalent model based on average time.

Considering the average execution time of over 100 iterations, Figure 5.2 indicates the observed execution time versus the estimated ones through linear regression analysis of least square methods. As can be seen, the final model summary, Table 5.1, does not indicate the acceptable adjustable R square. Also, estimated time is not suitably tracing the executed ones in Figure 5.2 (i.e., a scatter plot of estimated time versus the executed time). Corresponding Coefficients of DataL and KeyL, as independent variables considered in linear regression model, is shown in column B of Table 5.2.

II. First Observed Time

Table 5.3 Model summary based on first observed time. Predictors: (Constant), KeyL, DataL; Dependent Variable: FirstTime

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.922[a]	.850	.844	.46796

Table 5.4 Coefficient summary based on first observed time. Dependent Variable: First Observed Time

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	.810	.152		5.348	.000
DataL	.028	.002	.779	12.678	.000
KeyL	.010	.002	.293	4.763	.000

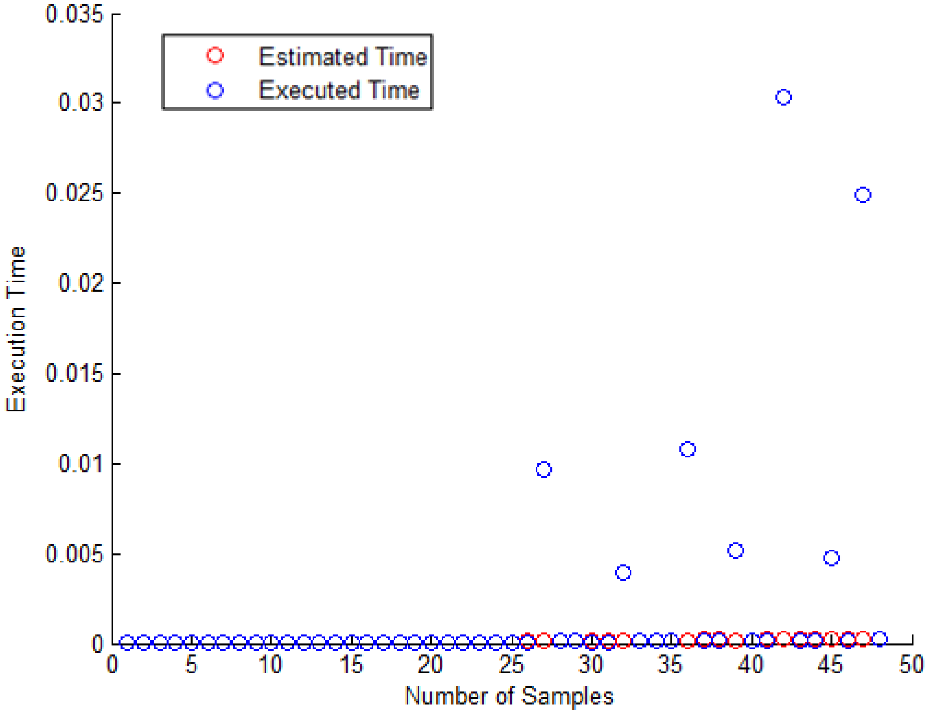


Figure 5.3 Equivalent model based on first observed time.

By comparing the results with the prior results of average execution time, this model represents a more acceptable equivalent model. In other words, the adjustable R square increased from 0.616 of the first model based on average time, shown in Table 5.1, to 0.844 of the second model based on the first observed time, shown in Table 5.3. Also, both predictors are significant. The Sig. column in Table 5.4 is zero for both predictors, which means it is a better model.

In comparison with Figure 5.2, Figure 5.3 shows more tracing of expected time with the estimated model in most of the samples; however, of 48 samples, 7 are modeled extremely differently compared with the observed ones. To overcome this problem, a third model is evaluated based on the minimum execution time observed over 100 runs.

III. Minimum Time of 100 runs

Table 5.5 Model summary based on minimum time of 100 iterations. Predictors: (Constant), KeyL, DataL

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.991[a]	.982	.982	.09296

Table 5.6 Coefficient summary based on minimum time of 100 iterations. Dependent Variable: Minimum Time.

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	1.007	.030		33.444	.000
DataL	.018	.000	.877	41.652	.000
KeyL	.005	.000	.250	11.861	.000

Table 5.5 clearly shows a significant increase in adjustable R square value from 0.844 based on the first observed time, shown in Table 5.3, to 0.982 based on the minimum execution time over 100 iterations.

Table 5.6 shows that both predictors are significant since the Sig. column is zero for both predictors. Finally, Figure 5.4 shows the best equivalent model, tracing executed time by estimated ones, in comparison with the previous two models. Therefore, in the rest of this thesis, a minimum execution time of 100 iterations is considered as a reference for computing regression models.

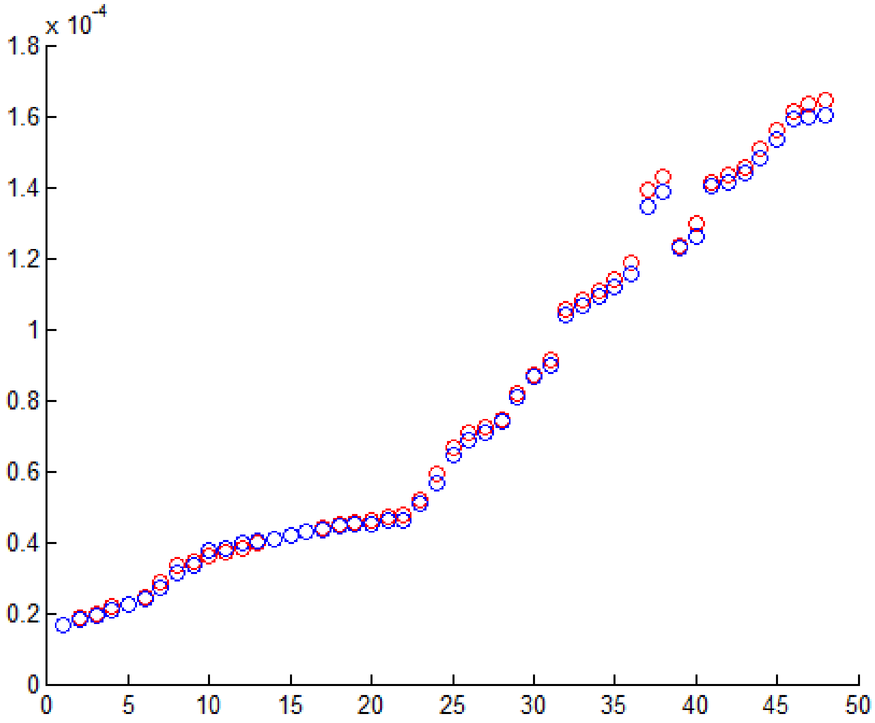


Figure 5.4 Equivalent model based on minimum execution time.

5.3.4 Optimum Number of Predictors

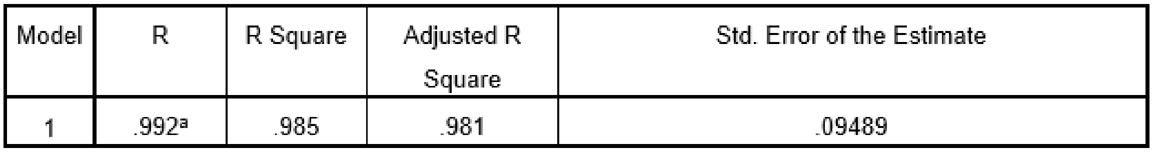
In all the previous tables and figures, only two predictors, DataL and KeyL, are considered. The reason is discussed below. Particularly, the optimum number of predictors is investigated since more predictors cause an attacker to prepare more information and consume more resources. Thus, a fewer number of predictors are more desirable.

Stepwise regression in statistics leads to the choice of predictor variables in an automatic procedure. It is included in several approaches, in which two main approaches are forward selection, i.e., starting without any variables and comparing the model criterions by addition of each individual predictor gradually as one step, and backward selection, which includes all the variables and compares the model criteria by deleting each predictor variable gradually. The latter one is utilized in this thesis. Thus, all the predictors are first involved in estimating execution time. Then, by analyzing and comparing the significance of coefficients (Sig. column of coefficient summary tables), adjusted R square, etc., the least significant predictor is chosen and deleted from the list of predictors. The process is continued with the goal of obtaining an efficient model and predictors. Also, the interaction of predictors is calculated and applied as new predictors.

Since an attacker explores the values of KeyL and KeyHW in a target device independently, estimating the execution time relying on KeyL and KeyHW is investigated in separate scenarios in the following sections.

I. Estimating Execution Time vs. Key Length (Linear Regression)

Table 5.7 Model summary including all predictors (considering KeyL). Predictors: (Constant), DigestHW*KeyL, DigestHW, DataHW, DataL, DataHW*KeyL, DataL*DataHW, KeyL*DataL, KeyL, DataL*DigestHW, DataHW*DigestHW



Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.992[a]	.985	.981	.09489

Table 5.8 Coefficient summary including all predictors (considering KeyL). Dependent Variable: Minimum Time of 100 iterations

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	1.303	.437		2.979	.005
KeyL	.005	.006	.272	.911	.368
DataL	.004	.009	.197	.478	.635
DigestHW	-.003	.005	-.030	-.535	.596
DataHW	.003	.002	.775	1.805	.079
KeyLByDataL	1.352E-005	.000	.066	.795	.431
DataLByDataHW	-2.003E-006	.000	-.055	-.541	.592
DataLByDigestHW	.000	.000	.732	1.664	.105
DataHWByDigstHW	-4.138E-005	.000	-.854	-1.778	.084
DataHWByKeyL	4.391E-006	.000	.081	1.152	.257
DigestHWByKeyL	-2.795E-005	.000	-.114	-.368	.715

As shown in Table 5.8, all of the interaction predictors and some of the simple predictors (non-interaction ones) are not significant. Particularly, predictors are called significant while the Sig. value in coefficient summary table is less than or equal to 0.05. In addition, the adjusted R square of Table 5.7 is less than the same value in Table 5.5. Thus, this model is not efficient. The next deleting predictor of the backward selection procedure is the one with the biggest Sig. value, 0.715, i.e., interaction of DigestHW and KeyL, DigestHWByKeyL. By deleting the predictor carrying the greatest Sig. value, and comparing the adjusted R square value as Sig. of the remaining, the most efficient models are those shown in Table 5.5, Table 5.6, and scatter plot of estimated time versus executed time ,shown in Figure 5.5 .

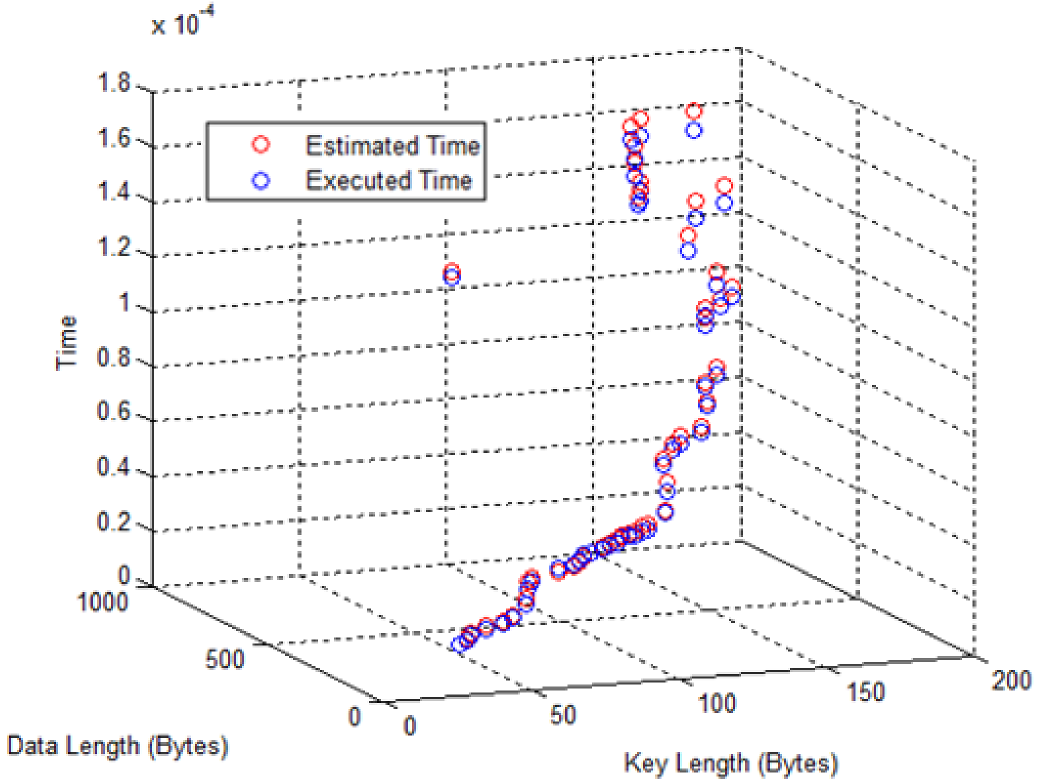


Figure 5.5 Equivalent model based on minimum time vs data length and key length

As it is shown in Figure 5.5, key length and data length, as the optimum predictors, are highly correlated with execution time of algorithm. In addition, Figure 5.6 shows the equivalent model of real execution time of algorithm versus estimated time over the new samples of training and testing data when the key length is fixed to 35 bytes.

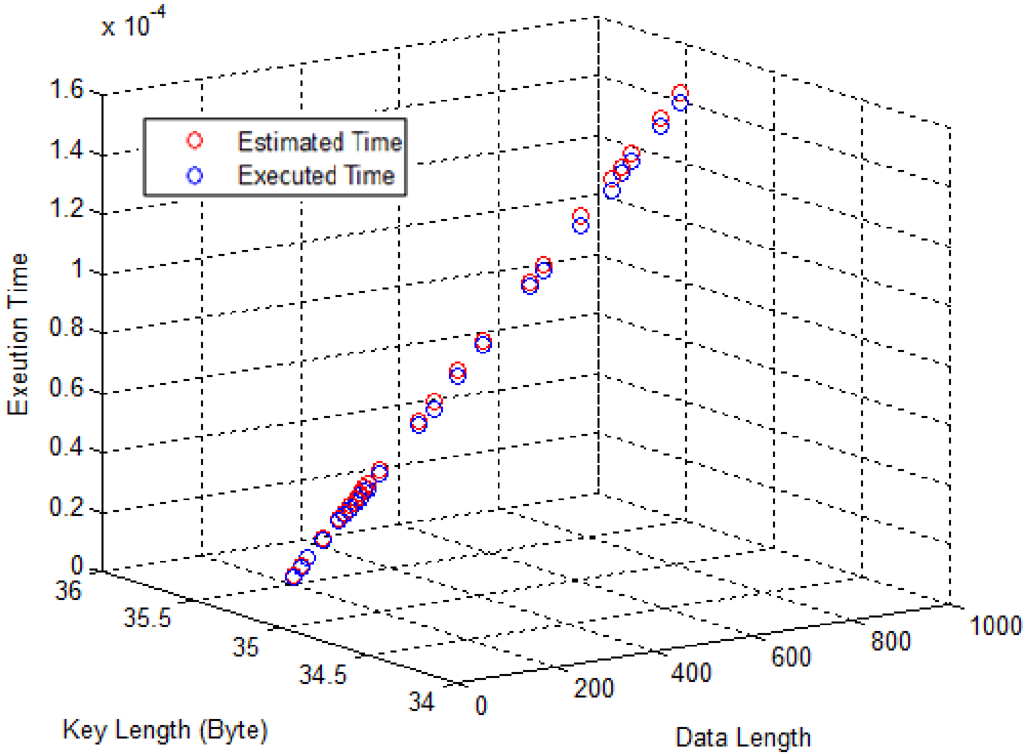


Figure 5.6 Equivalent model of execution time vs fixed key length and variable data length

Similar to the equivalent model of Figure 5.6, an attacker should create a set of equivalent models by calculating the execution time of algorithm for a set of fixed-length keys and variable length of data. Since both the execution time and data length are accessible by the attacker, supplied key length could be predicted. In other words, by comparing the real executed time and data length with the estimated time of different equivalent models, which is correspond to each fixed-length key, the length of utilized key of the target device is estimated.

II. Estimating Execution Time vs. Key Hamming Weight (Linear Regression)

The goal of the above model fitting is to predict the stored key length by considering the execution time of the algorithm. In the same way, correlation of KeyHW with execution time of the algorithm will be investigated in the following section. Considering all predictors and interactions, the adjusted R square and coefficients are shown in Table 5.9 and Table 5.10, respectively.

Table 5.9 Model summary including all predictors (considering KeyHW). Predictors: (Constant), DigestHW*KeyHW, DigestHW, DataL, DataHW, DataHW*KeyHW, KeyHW*DataL, DataL*DataHW, DataL*DigestHW, KeyHW, DataHW*DigestHW

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.984[a]	.969	.960	.13643

Table 5.10 Coefficient summary including all predictors (considering KeyHW).

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	1.297	.635		2.044	.048
DataL	.009	.011	.429	.808	.424
DataHW	.003	.002	.673	1.167	.251
DigestHW	-.002	.008	-.022	-.267	.791
KeyHW	.000	.002	.070	.149	.883
KeyHWByDataL	9.656E-006	.000	.191	1.655	.106
DataHWByKeyHW	-3.925E-007	.000	-.033	-.313	.756
DataLByDataHW	-1.277E-006	.000	-.035	-.238	.813
DataLByDigestHW	.000	.000	.543	.958	.344
DataHWByDigstHW	-3.784E-005	.000	-.781	-1.257	.217
DigestHWByKeyHW	-2.807E-007	.000	-.005	-.011	.991

Similar to Table 5.8, most predictors in Table 5.10 are not significant. In the same way as deleting predictors by greater Sig. value, most efficient models are discussed in the following. Table 5.11 and Table 5.12 show the best model summary from an adjusted R square viewpoint and the best coefficient summary from a Sig. viewpoint, respectively.

Table 5.11 Model summary of best adjusted R square (considering KeyHW). Predictors: (Constant), KeyHW, DataHW, DataL

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.982[a]	.964	.962	.13380

Table 5.12 Coefficient summary of best adjusted R square (considering KeyHW).

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	1.048	.043		24.486	.000
DataL	.021	.001	1.018	22.407	.000
DataHW	.000	.000	-.116	-2.569	.014
KeyHW	.001	.000	.184	6.327	.000

As shown above, the best adjustable R square model is based on DataL, DataHW, and KeyHW. Thus, as considered in our assumption, an attacker needs full knowledge of the measured values by PMUs, DataL and DataHW, inserted as input values to the authentication algorithm (HMAC-SHA1). However, if the encryption algorithm is considered in the security protocol of IEC 62351, the efficient model would be as shown in Table 5.13 and Table 5.14. Table 5.13 shows that the adjusted R square value is decreased to 0.957 compared with Table 5.11, which carries a value of 0.962. However, all predictors are significant in Table 5.14.

Table 5.13 Model summary without knowledge of DataHW (considering KeyHW). Predictors: (Constant), KeyHW, DataL

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.979[a]	.959	.957	.14188

Table 5.14 Coefficient summary without knowledge of DataHW (considering KeyHW).

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	1.057	.045		23.381	.000
DataL	.019	.001	.928	30.177	.000
KeyHW	.001	.000	.181	5.891	.000

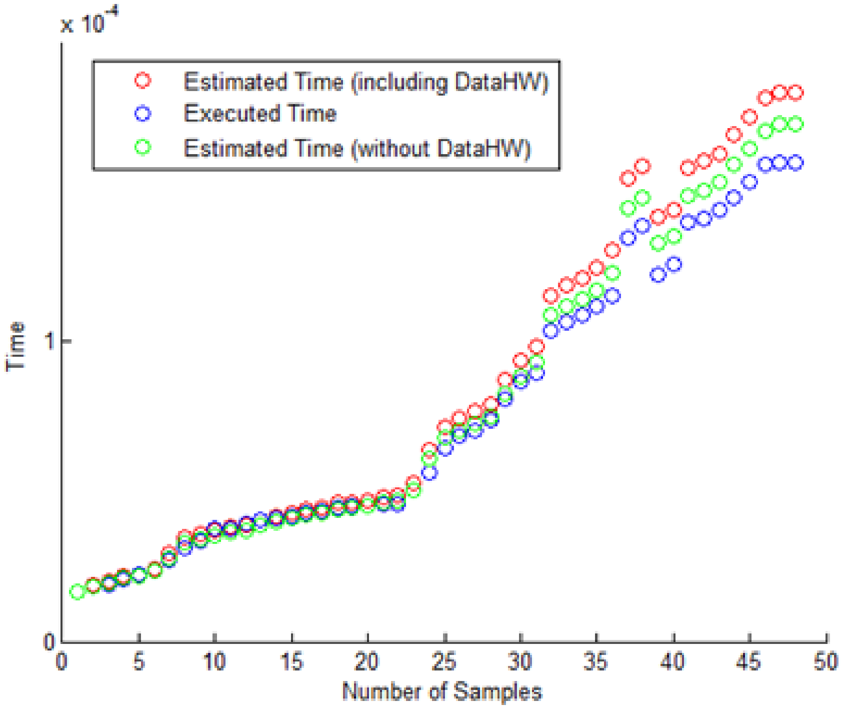


Figure 5.7 Equivalent models with/without considering DataHW (considering KeyHW).

The scatter plot of the equivalent model is the best method to compare the most significant variables which predict the independent one. Regarding Figure 5.7, DataHW could be excluded for modeling the execution time, considering KeyHW and DataL, which is shown in Figure 5.8. Accuracy of the model is evaluated by a new set of data, called test data, illustrated in Figure 5.8.

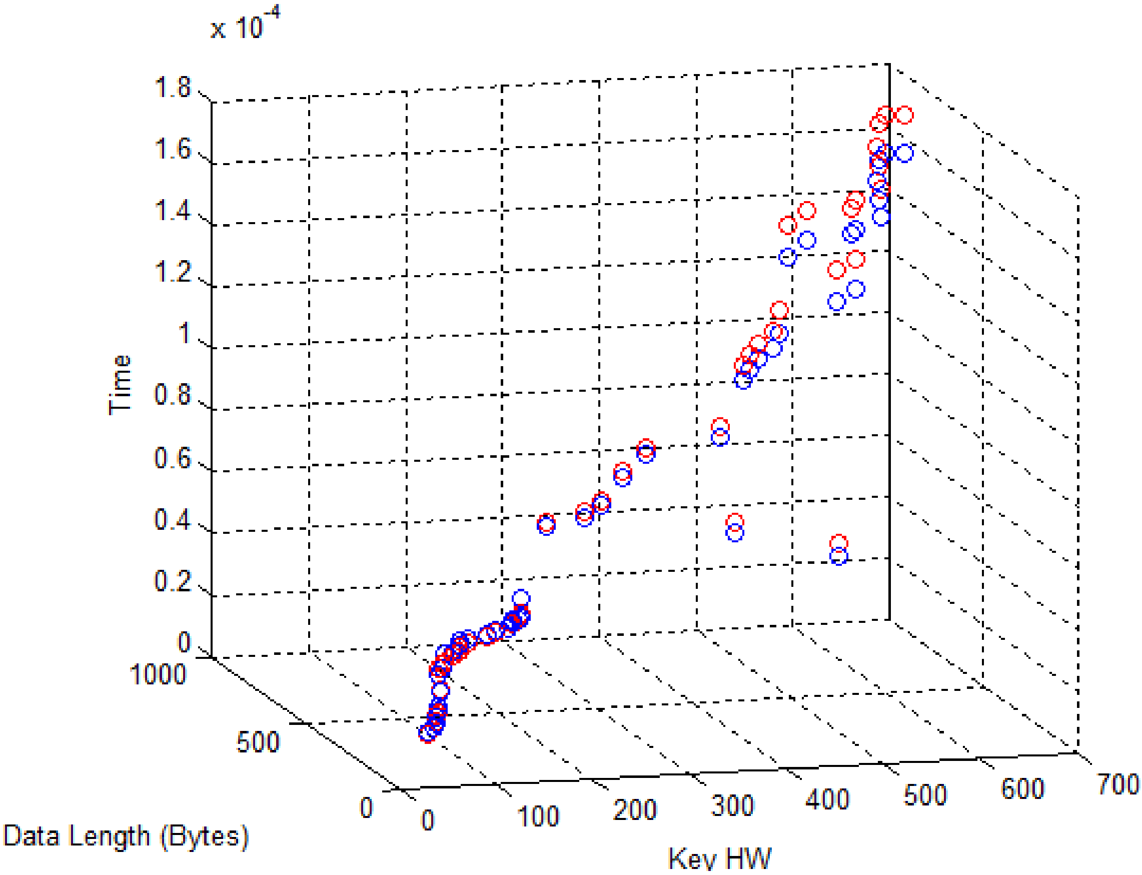


Figure 5.8 Equivalent model for execution time vs. data length and key Hamming weight.

According to Figures 5.5 and 5.8, there is a correlation between the execution time of the HMAC-SHA1 authentication algorithm and secret related information as KeyL and KeyHW, respectively. In particular, since the encryption algorithm is not included in the communication protocol of a PMU substation, an attacker has full knowledge of DataL, which simplifies the attack to estimate the KeyHW and KeyL. Thus, the cryptanalysis process of an attacker would be narrowed down to a limited number of possibilities.

Similar to the previous section of estimating key length of target device, Figure 5.9 shows the equivalent model of real execution time of algorithm versus estimated time over the new samples of training and testing data when the key Hamming weight is fixed to 78 bytes.

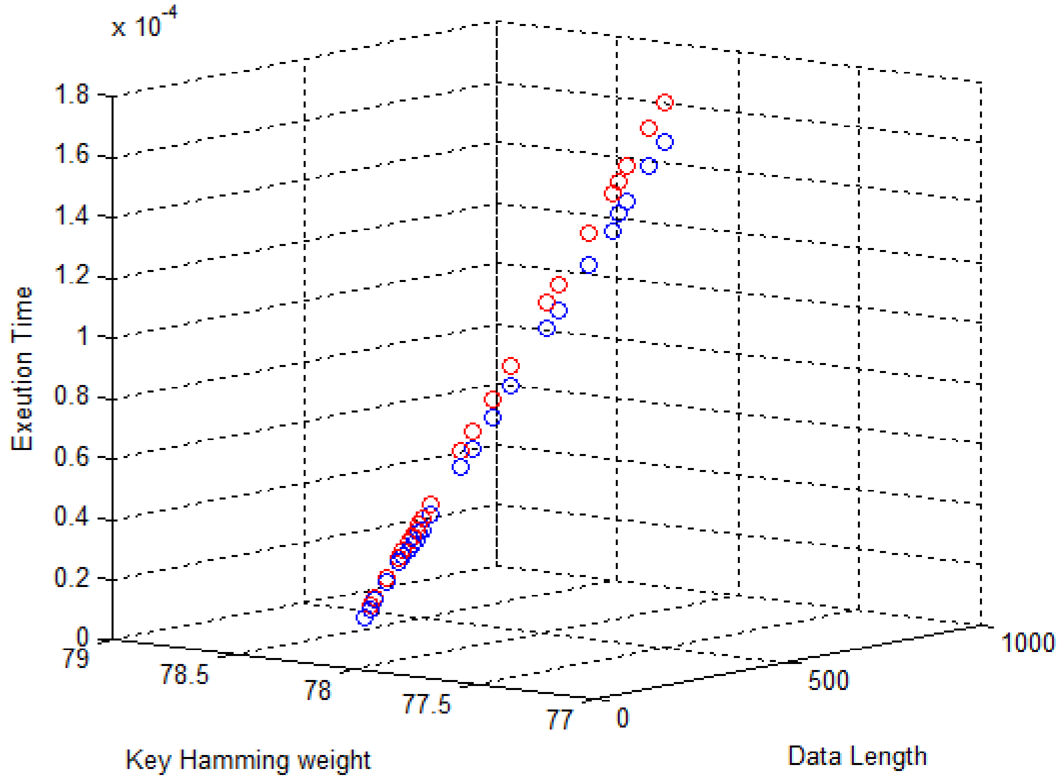


Figure 5.9 Equivalent model of execution time vs fixed key HW and variable data length

An attacker needs to create a set of equivalent models, similar to Figure 5.9, by calculating the execution time of algorithm for a set of fixed length of key Hamming weight and variable length of data.

Obviously, an attacker needs an extra attempt to predict the key length and key Hamming weight while the linear regression is utilized. In other words, linear regression is able to predict the execution time of algorithm while secret-related information, e.g. key length and key Hamming weight, are the goal of attacker. Thus, an attacker should estimate those desired information based on the equivalent models, e.g. Figure 5.6 and Figure 5.9 for a set of fixed key length and key Hamming weight, and compares them by the observed execution time of algorithm. To overcome this shortcoming, next section investigates another type of regression which is called negative binomial regression.

5.3.5 Negative Binomial with Log Link Regression Model

In addition to the above mentioned analysis, the Negative Binomial with Log Link Regression (nbreg) based on minimum execution time will be discussed below. The reason for nbreg utilization, as another modeling of the HMAC-SHA1 authentication algorithm, is to model separately the Hamming weight and length of stored key based on execution time, with DataL, DataHW, and DigestHW as predictors, instead of modeling the execution time based on keyL and KeyHW. It simplifies the attacker cryptanalysis process by revealing the information about KeyL and KeyHW as the output of nbreg regression, called the dependent variable. Also, we cannot use the same linear regression model and consider KeyL or KeyHW dependent variables because they are not continuous values, which causes linear regression to not perform properly. On the contrary, nbreg is suitable for count data. Moreover, negative binomial distribution is more general than the Poisson.

In the following, KeyL and KeyHW are modeled separately as dependent variables through nbreg regression.

I. Estimating Key Length vs. Execution Time (nbreg)

Table 5.15 Omnibus test via nbreg including all predictors (considering KeyL). Predictors: (Intercept), DataL, DataHW, Time, DigestHW, DataL*DataHW, DataL*Time, DataL*DigestHW, DataHW*Time, DataHW*DigestHW, Time*DigestHW. Dependent variable: KeyL

Likelihood Ratio Chi-Square	df	Sig.
8.477	10	.582

Table 5.15 shows the significance of the model for estimating the KeyL while including all possible predictors and interactions, as listed in the table. As shown in Table 5.15, the model is not significant. Sig. is significantly greater than 0.05, due to including so many predictors. However, the equivalent model, illustrated in Figure 5.10, indicates a reasonable and admirable tracing of expected KeyL values compared with the predicted ones.

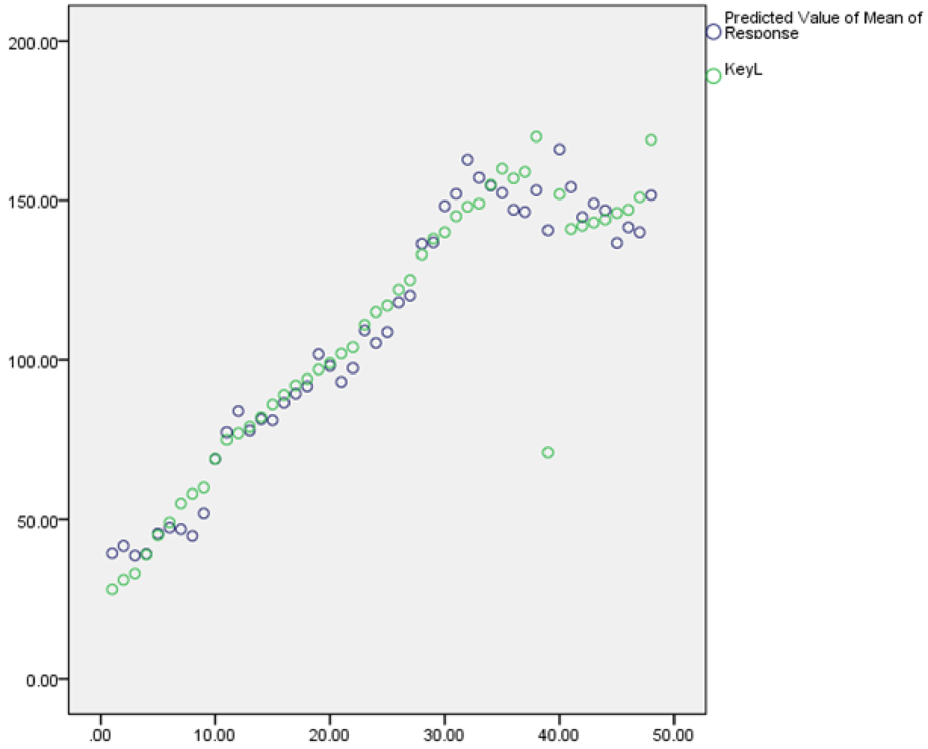


Figure 5.10 Equivalent model via nbreg including all predictors (comparing the expected KeyL vs predicted values of mean response over 100 estimations and confidence interval of 0.95).

Obviously, an attacker is assumed to have full knowledge of measurement values and signatures indicated as DataHW and DigestHW. In the following, the model fitting by considering the encryption algorithm is indicated. In other words, DataHW and DigestHW are assumed to be concealed from the attacker.

Table 5.16 Omnibus test via nbreg and including encryption algorithm (considering KeyL). Predictors: (Intercept), DataL, Time, DataL * Time; Dependent Variable: KeyL

Likelihood Ratio Chi-Square	df	Sig.
8.078	3	.044

Although the numbers of predictors are significantly decreased, which leads to better Sig. values in Table 5.16, Figure 5.11 does not present a desirable tracing of expected KeyL by estimated ones compared with Figure 5.10.

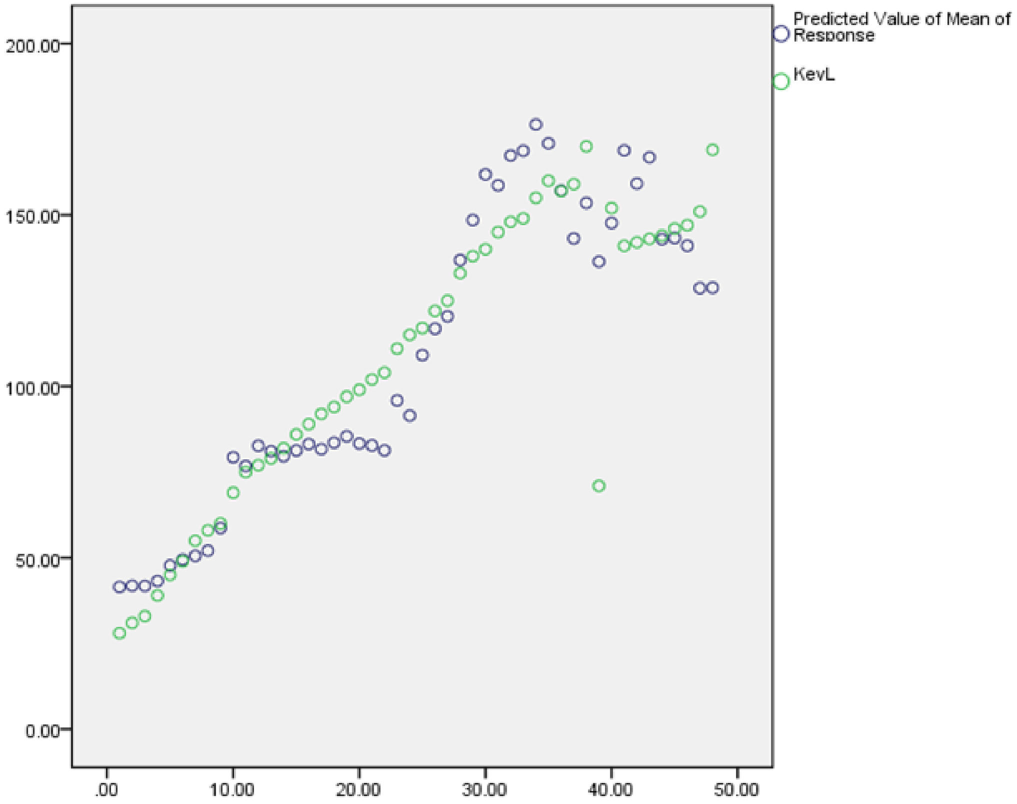


Figure 5.11 Equivalent model via nbreg including the encryption algorithm (compared expected KeyL vs predicted values of mean response over 100 estimations, confidence interval of 0.95).

II. Estimating Key Hamming Weight vs. Execution Time (nbreg)

The same scenario is applied to model the KeyHW by nberg with and without including the encryption algorithm, which conceals the information of DataL and DigestHW.

Table 5.17 Omnibus test via nbreg including all predictors (considering KeyHW). Predictors: (Intercept), DigestHW, DataL, DataHW, Time, DigestHW*DataL, DigestHW*DataHW, DigestHW*Time, DataL*DataHW, DataL*Time, DataHW*Time, Dependent value: KeyHW

Likelihood Ratio Chi-Square	df	Sig.
34.906	10	.000

Table 5.17 shows a significant model (Sig. is equal to zero) although it includes many predictors. Thus, as expected, a reasonable tracing of expected KeyHW values compared with estimated ones by nbreg is illustrated in Figure 5.12.

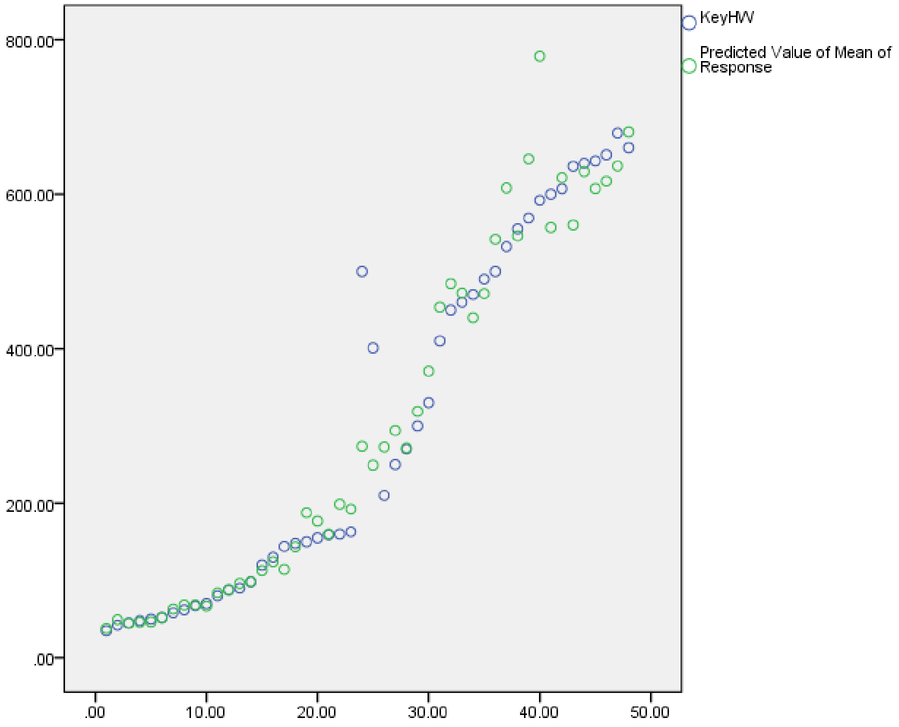


Figure 5.12 Equivalent model via nbreg including all predictors (comparing expected KeyHW vs predicted values of mean responses over 100 estimations and confidence interval of 0.95).

Next, by considering the encryption algorithm, a new equivalent model based on nbreg is shown in Table 5.18. Similarly, the model is significant; Sig. is zero. However, the Likelihood Ratio Chi-Square is reduced in comparison with Table 5.17.

Table 5.18 Omnibus test via nbreg and including encryption algorithm (considering KeyHW). Predictors: (Intercept), DataL, Time, DataL * Time; Dependent Variable: KeyHW

Likelihood Ratio Chi-Square	df	Sig.
33.626	3	.000

As expected, by reducing the number of predictors in nbreg model fitting, the accuracy of tracing the predicted KeyHW value compared with expected ones is decreased even though it is somehow acceptable. The equivalent model is shown in Figure 5.13.

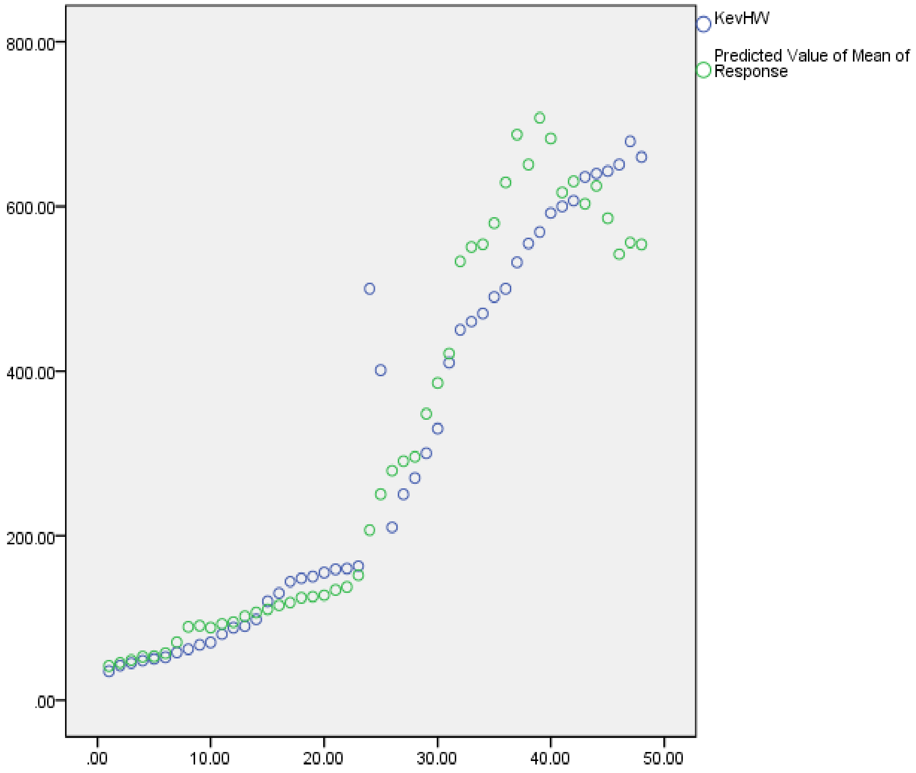


Figure 5.13 Equivalent model via nbreg including the encryption algorithm (compared expected KeyHW vs predicted values of mean response over 100 estimations; confidence interval 0.95).

Chapter 6. **Conclusions**

In this thesis, the security of PMUs in the smart grid communication infrastructure is analyzed. After the introduction, PMUs are introduced from a communications infrastructure viewpoint. In this regard, several synchrophasor, communication, and security standards, considered and implemented in transmitting the real-time PMU measurements to PDCs, are discussed. PDCs are interpreted and correlated to the received data as a time-stamped data stream to demonstrate a time-dependent snapshot of the entire smart grid. However, PMU to PDC communication is vulnerable to a variety of attacks. Previously discussed attacks demonstrate several vulnerabilities, constraints, and issues that must be considered in communication infrastructures of PMUs. For instance, delivering the real-time streaming phasor data of PMUs to the PDC is one of the main limitations which leads to eliminating the encryption algorithm in IEC 62351, as the security protocol of PMU substation communication. On the other hand, the importance of authenticity and integrity of PMU measurement values, received by PDCs, leads to deploying a lightweight HAMC-SHA1 authentication algorithm. First investigated in this thesis, HMAC-SHA1 is vulnerable to timing SCAs. In other words, an attacker can obtain the secret-related information about the supplied key HMAC by monitoring the execution time of the algorithm. In this thesis, linear regression and negative binomial regression are applied to model the correlation of the stored-key length and the stored-key Hamming weight with the execution time of the algorithm. All analyses are based on a variety of predictors, such as data length, data Hamming weight (HW), and HMAC digest HW, with the goal of predicting the length and HW of the utilized key. Since the HMAC-SHA1 can take any key length larger than zero (mostly more than 20 bytes or 160 bits), results can help an attacker to narrow down a brute force attack to a smaller number of keys with the knowledge of key lengths and number of bits, which are one and zero. In addition, even though the encryption algorithm is not considered in current released security standards of PMU communications, the analysis presented here considered the encryption algorithm as well.

HMAC-SHA1 is highly vulnerable to timing SCAs from a key length and Hamming weight viewpoint. In this thesis, the correlation of stored-key length and Hamming weight with the execution time of HMAC-SHA1, as the authentication algorithm recommended in IEC 62351, is modeled and investigated. To achieve this, the execution time of algorithm is considered as the main variable in all analysis. With accuracy in the order of nanoseconds, measured execution time can be affected by many parameters, such as cache functionality and parallel processing. Results show that minimum execution time over 100 iterations presents the best model fitting compared with first observed time and average time over 100 measurements.

A linear regression model (with least square method) indicated that data length, key length, and key Hamming weight have more significance in predicting the execution time of the algorithm compared with both the Hamming weight of the data and HMAC digest. Therefore, including the encryption algorithm, concealing the pair of data and corresponding digest (M_i, S_i) would not be a countermeasure to timing SCAs against HMAC. Although it indicates the proper equivalent models whether encryption algorithm is considered or not, an attacker needs an extra attempt to estimate the desire information of target device, e.g. key length and key Hamming weight. In particular, a set of equivalent models must be created by calculating the execution time of algorithm for a set of fixed key length and fixed key Hamming weight over variable data length. Thus, attacker could estimate the desire information based on calculated equivalent model and compared them with the observed execution time of algorithm. To overcome this shortcoming, negative binomial regression is investigated.

Negative binomial regression with log link regression (nbreg) is applied to model the key length and key HW as count data. Generally, nbreg is more feasible to apply by an attacker since target values are released directly from the output. However, the preciseness of the estimated model is reduced in the presence of an encryption algorithm, by concealing the data and corresponding signature, compared with the equivalent linear regression model. By the way, it reveals a highly proper model for estimating the key length and HW by considering the currently released security and communication standards.

As countermeasures, random delay or similar approaches could not be applied to PMU data due to their real time applications. However, randomizing the packet length could mitigate the success of an attacker since data length is highly correlated with the execution time in linear regression, and both are applied as the predictors to estimate the length and Hamming weight of the secret key. In addition, since the substations are not assumed to be secure in the power grid, some compensation methods for the physical security of substations, e.g., surveillance cameras, should be the simplest countermeasures to SCAs for authenticated data of PMUs.

Chapter 7. **Future Work**

Through this thesis, the correlation of execution time of algorithm with length and Hamming weight of the supplied key to the HAMC-SHA1 authentication algorithm is investigated. Thus, an attacker can estimate the length and the number of zeroes and ones in the stored key of a target device. However, this does not indicate the absolute value of the key which could be considered as future work. Particularly, a divide-and-conquer attack must target the intermediate values of an algorithm to recover the key part-by-part. For each predicted key length and Hamming weight, all pairs of key possibilities and corresponding execution times must be measured. Also, the intermediate operations of HMAC from a timing SCA viewpoint must be analyzed. In brief, those operations must be dependent to both the unknown values, i.e. the secret key, and some known values to the attacker.

Then, the correlation coefficients of stored key with the estimated ones must be calculated to figure out how the estimated value differs from the real supplied key.

References:

[1]. M. Hurtgen, J-C. Maun, “Applications of PMU Measurements in The Belgian Electrical Grid”, technical report, May 2012.

[2]. Smart Grid Communications and Networking, Yi Deng, Hua Lin, Arun G. Phadke, Sandeep Shukla, James S. Thorp, Cambridge University Press, 2012, Print ISBN: 9781107014138.

[3]. M.D. Hadley, J.B. McBride, T.W. Edgar, L.R. O’Neil, R.D. Johnson, “Securing Wide Area Measurement Systems,” Pacific Northwest National Laboratory, Prepared for the U.S. Department of Energy Office of Electricity Delivery and Energy reliability Under Contract DE-AC05-76RL01830, June 2007.

[4]. L. Zhang, A. Abur, “Assigning Weights for PMU Measurements: Two Alternative Methods,” Power and Energy Society General Meeting, 2012 IEEE.

[5]. M. Popa, M. Albu, “Implementation Overview of PMU Functionalities on A Regular Computer," smfg, pp.40-44, IEEE International Conference on Smart Measurements of Future Grids Proceedings, 2011.

[6]. A. Goodney, S. Kumar, A. Ravi, Y. H. Cho, “Efficient PMU Networking with Software Defined Networks,” IEEE SmartGridComm Symposium - Communication Networks for Smart Grids and Smart Metering, 2013.

[7]. C. H. Wells, A. Moore, K. Tjader, W. Isaacs, “Cyber Secure Synchrophasor Platform,” Power Systems Conference and Exposition (PSCE), 2011 IEEE/PES.

[8]. R. H. Khan, J. Y. Khan, “Wide Area PMU Communication over a WiMAX Network in the Smart Grid,” IEEE SmartGridComm Symposium - Communication Networks for Smart Grids and Smart Metering, 2012.

[9]. “Real-Time Application of Synchrophasors for Improving Reliability”, NERC report. http://www.nerc.com/docs/oc/rapirtf/RAPIR%20final%20101710.pd, October 2010.

[10]. Consortium for Electric Reliability Technology Solutions (CERT). Phasor Technology. [Online] Available at: http://www.phasor-rtdms.com/phaserconcepts/phasor_adv_faq.html#Question2 [Accessed 30 May 2014].

[11]. K. Narendra, T. Weekes, “Phasor Measurement Unit (PMU) Communication Experience in a Utility Environment,” Conference on Power Systems, October 2008.

[12]. Smart Grid Standards Assessment and Recommendations for Adoption and Development, technical report, EnerNex Corporation, October 2008.

[13]. North American SynchroPhasor Initiative (NASPI). 2012. PMU Location Map. [Online] (Updated November 2012) Available at: www.naspi.org [Accessed 15 May 2014].

[14]. Studio Electronike Rijeka. 2012. WAMSTER Ad Hoc Phasor Measurement Network. [Online] (Updated 4 May 2012) Available at: www.ster.hr [Accessed 30 May 2014

[15]. M. Govindarasu, “Cyber Security of Smart Grid,” Tutorial at IEEE IMSAA, December 2011.

[16]. J. Horalek, V. Sobeslav, “Datanetworking Aspects of Power Substation Automation,” Communication and Management in Technological Innovation and Academic Globalization, pp 147-153, ISBN: 978-960-474-254-7, 2010.

[17]. F. Hohlbaum, M. Braendle, F. Alvarez, “Cyber Security Practical Considerations for Implementing IEC62351”, ABB, 2010.

[18]. “Smart Grid Interoperability Panel-Cyber Security Working Group Standards Review”, Phase1 Report, October 2010.

[19]. M. Qiu, H. S. Chen, Z. Ming, L. T. Yang, “Balance of Security Strength and Energy for a PMU Monitoring System in Smart Grid,” IEEE Communications Magazine, May 2012.

[20]. Cryptography and Network Security Principles and Practice, W. Stallings, Prentice Hall, 2011, ISBN 13: 978-0-13-609704-4.

[21]. T. H. Morris, S. Pan, U. Adhikari, “Cyber Security Recommendations for Wide Area Monitoring, Protection, and Control Systems,” Power and Energy Society General Meeting, 2012 IEEE.

[22]. NMAP Security Scanner. [Online] Available at http://www.nmap.org.

[23]. Wireshark. [Online] Available at: http://www.wireshark.org.

[24]. I. Matei, J. S. Baras, V. Srinivasan, “Trust-Based Multi-Agent Filtering for Increased Smart Grid Security,” Mediterranean Conference on Control & Automation (MED) Barcelona, Spain, July 2012.

[25]. R.B. Bobba, K.M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and TJ. Overbye. Detecting false data injection attacks on DC state estimation. Proceedings of the First Workshop on Secure Control Systems (SCS 2010), CPS WEEK201 0, April 2010.

[26]. MU Dynamics. [Online] Available at: http://www.mudynamics.com.

[27]. C.-H. Lo, N. Ansari, "The Progressive Smart Grid System from Both Power and Communications Aspects," IEEE Communications Surveys & Tutorials, vol. 14, No. 3, Third Quarter 2012.

[28]. E.-K. Lee, M. Gerla, S. Y. Oh, "Physical Layer Security in Wireless Smart Grid," IEEE Communications Magazine, August 2012.

[29]. A. Giani, E. Bitary, M. Garciay, M. McQueen, "Smart Grid Data Integrity Attacks: Characterizations and Countermeasures," International Conference on Smart Grid Communications (SmartGridComm), 2011 IEEE.

[30]. B. Sikdar, J. H. Chow, "Defending Synchrophasor Data Networks Against Traffic Analysis Attacks," IEEE Transactions on Smart Grid, vol. 2, No. 4, December 2011.

[31]. Z. Zhang, S. Gong, A. D. Dimitrovski, H. Li, "Time Synchronization Attack in Smart Grid: Impact and Analysis," IEEE Transactions on Smart Grid, vol. 4, No. 1, March 2013.

[32]. D. Goodin, "US spy drone hijacked with GPS spoof hack," Dec. 2011 [Online]. Available: http://www.theregister.co.uk/2011/12/15/ us_spy_drone_gps_spoofing.

[33]. A. Jafarnia-Jahromi, T. Lin, A. Broumandan, J. Nielsen, and G. Lachapelle, "Detection and mitigation of spoofing attacks on a vector-based tracking GPS receiver," in Proc. ION ITM, Newport Beach, CA, Jan. 2012, pp. 790–800.

[34]. X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, A. D. Dominguez-Garcia, "Spoofing GPS Receiver Clock Offset of Phasor Measurement Units," IEEE Transactions on Power Systems, vol. 28, No. 3, August 2013.

[35]. D. Shepard, T. Humphreys, and A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," in Proc. Int. Conf. Critical Infrastructure Protection, Washington, DC, USA, 2012.

[36]. J. Steven, G. Peterson, D. A. Frincke, "Smart-Grid Security Issues," IEEE Computer and Reliability Societies, 2010 IEEE.

[37]. L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in Proc. IEEE 2010 SmartGridComm, Gaithersburg, MD, USA., October 2010.

[38]. J. Kim and L. Tong, “On Topology Attack of a Smart Grid,” in Proc. The fourth Conference on Innovative Smart Grid Technologies (ISGT 2013), Washington, DC, February 2013.

[39]. Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” in Proceedings of the 16th ACM conference on Computer and communications security, 2009, pp. 21–32.

[40]. R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt,and T. J. Overbye, “Detecting false data injection attacks on dc state estimation,” in First Workshop on Secure Control Systems,CPSWEEK 2010, Stockholm, Sweeden, April 2010.

[41]. O. Kosut, L. Jia, R. J. Thomas, L. Tong, “Malicious data attacks on the smart grid,” IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 645 –658, December 2011.

[42]. O. Vukovic, K. C. Sou, G. Dan, and H. Sandberg, “Network-layer protection schemes against stealth attacks on state estimators in power systems,” in Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on, oct. 2011, pp. 184 –189.

[43]. Intel, “Using the RDTSC Instruction for Performance Monitoring”, 1998, [Online] Available at: http://developer.intel.com/drg/pentiumII/appnotes/RDTSCPM1.HTM.

[44]. T. Kim and H. Poor, “Strategic protection against data injection attacks on power grids,” IEEE Transactions on Smart Grid, vol. 2, no. 2, pp. 326 –333, June 2011.

[45]. T. T. Kim, H. V. Poor, “Strategic Protection against Data Injection Attacks on Power Grids”, IEEE Transactions on Smart Grid”, vol. 2, No. 2, June 2011.

[46]. Y. Yang, X. Guan, Y. Zhou, J. Wu, T. Liu, “Impact of Information Security on PMU-based Distributed State Estimation”, IEEE PES ISGT ASIA 2012 1569527815.

[47]. P. M. Ashton, G. A. Taylor, M. R. Irving, “Prospective Wide Area Monitoring of the Great Britain Transmission System using Phasor Measurement Units”, Power and Energy Society General Meeting, 2012 IEEE.

[48]. S. Han, B. Lee, “Wide Area Monitoring System for the Korean Smart Transmission Grid Using PMUs”, the International Conference on Advanced Power System Automation and Protection, 2011 IEEE.

[49]. M. Rihan, M. Ahmad, M. S. beg, “Phasor Measurement Units in the Indian Smart Grid”, Innovative Smart Grid Technologies - India (ISGT India), 2011 IEEE PES.

[50]. Koeune, F., Standaert, F-X.: A Tutorial on Physical Security and Side-Channel Attacks. In: Aldini, A., Gorrieri, R., Martinelli, F. (eds.) FOSAD 2005. LNCS, vol. 3655, pp. 78-108. Springer, Heidelberg (2005).

[51]. Y. Zhou and D. Feng, Side-Channel Attacks: Ten Years after Its Publication and the Impacts on Cryptographic Module Security Testing. ; In Proceedings of IACR Cryptology ePrint Archive. 2005, 388-388.

[52]. P. Kocher, Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems, Advances in Cryptology - CRYPTO '96, Santa Barbara, California (N. Koblitz, ed.), LNCS, vol. 1109, Springer, 1996, pp. 104–113.

[53]. J.-F. Dhem, F. Koeune, P.-A. Leroux, P. Mestr_e, J.-J. Quisquater, and J.-L. Willems. A practical implementation of the timing attack. In J.-J. Quisquater and B. Schneier, editors, Proceedings of CARDIS 1998, volume 1820 of LNCS, pages 167{182. Springer-Verlag, 1998.

[54]. Yau, A. K. L., Side Channel Analyses of CBC Mode Encryption, Ph.D. thesis, University of London, 2009.

[55]. Peter Gutmann, David Naccache, Charles C. Palmer, "Side-Channel Attacks on Cryptographic Software", IEEE Computer and Reliability Societies, 2009.

[56]. Fan Zhang and Zhijie Jerry Shi, "Differential and Correlation Power Analysis Attacks on HMAC-Whirlpool", 2011 Eighth International Conference on Information Technology: New Generations.

[57]. P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In Advances in Cryptology — CRYPTO'99, LNCS 1666, pp. 388–397, Springer-Verlag, 1999.

[58]. T. Messerges, E. Dabbish, and R. Sloan. Investigation of power analysis attacks on smartcards. In Usenix Workshop on Smartcard Technology 1999. [Online] Available at: http://www.usenix.org.

[59]. Doget, J., Prouff, E., Rivain, M., Standaert, F.-X.: Univariate Side Channel Attacks and Leakage Modeling. Journal of Cryptographic Engineering (to appear).

[60]. Jean-Jacques Quisquater and David Samyde, A new tool for non-intrusive analysis of smart cards based on electro-magnetic emissions: the SEMA and DEMA methods, Eurocrypt rump session, 2000.

[61]. Agrawal D., Archambeault B., Rao J.R., Rohatgi P.: The EM Side–Channel(s): Attacks and Assessment Methodologies. In: Cryptographic Hardware and Embeded Systems – CHES'2002.

[62]. Kun Gu, Liji Wu, XiangYu Li, XiangMin Zhang, “Design and Implementation of an Electromagnetic Analysis System for Smart Cards”, Seventh International Conference on Computational Intelligence and Security, 2011.

[63]. Fan Zhang and Zhijie Jerry Shi, “Differential and Correlation Power Analysis Attacks on HMAC-Whirlpool”, 2011 Eighth International Conference on Information Technology: New Generations.

[64]. E. Brier, C. Clavier, F. Olivier: Correlation Power Analysis with a Leakage Model. CHES 2004: 16-29.

[65]. Lemke, K., Schramm, K., Paar, C.:DPA on n-Bit Sized Boolean and Arithmetic Operations and Its Application to IDEA, RC6, and the HMAC-Construction. In: Joye, M. Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 205–219, Springer, Heidelberg (2004).

[66]. S. Belaïd, L. Bettale, E. Dottax, L. Genelle, F. Rondepierre, “Differential Power Analysis of HMAC SHA-2 in the Hamming Weight Model”, SECRYPT 2013 - 10th International Conference on Security and Cryptography, October 2013.

[67]. Paul C. Kocher: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. CRYPTO 1996: 104-113.

[68]. D. Brumley and D. Boneh. Remote timing attacks are practical. Computer Networks, 48(5):701{716, 2005.

[69]. G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, “Note on Side-Channel Attacks and Their Countermeasures”, NIST hash forum, May 2009.

[70]. D. Jayasinghe, J. Fernando, R. Herath, R. Ragel, “Remote Cache Timing Attack on Advanced Encryption Standard and Countermeasures”, International Conference on Information and Automation for Sustainability (ICIAFs), December 2010.

[71]. Ç. Çalık, "An Efficient Software Implementation of Fugue", Second SHA-3 Candidate Conference, Santa Barbara, California, USA, 23-24 August 2010.

[72]. Mostafa M. I. Taha, Patrick Schaumont: Side-Channel Analysis of MAC-Keccak. HOST 2013: 125-130.

[73]. D. Brumley and D. Boneh. Remote Timing Attacks are Practical. In Proceedings of the 12th USENIX Security Symposium, pages 1{14, 2003.

[74]. Jean-Jacques Quisquater, Fran¸cois Koeune, Side-channel attacks: state-of-the-art, CRYPTREC project deliverable, available at http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047 Side Channel report.pdf, October 2002.

[75]. F. Regazzoni, Y. Wang, F.-X. Standaert, "FPGA Implementations of the AES Masked Against Power Analysis Attacks", in Proceedings of 2nd International Workshop on Constructive Side- Channel Analysis and Secure Design (COSADE) Germany, February 2011.

[76]. Eastlake, D., Hansen, T. 2006. US Secure Hash Algorithms (SHA and HMAC-SHA). [Online] (Updated July 2006) Available at: http://tools.ietf.org/search/rfc4634 [Accessed 30 May 2014].

[77]. Federal Information Processing Standards Publication-FIPS PUB 198-1. 2008. The Keyed-Hash Message Authentication Code (HMAC). [Online] (Updated July 2008) Available at: http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf [Accessed 30 May 2014].

[78]. Federal Information Processing Standards Publication- FIPS PUB 180-4. 2012. Secure Hash Standard (SHS). [Online] (Updated March 2012) Available at: http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf [Accessed 30 May 2014].