ADVANCED METERING INFRASTRUCTURE SECURITY WITH SOFTWARE-DEFINED NETWORK IN SMART GRID

by

Yi-Chen Chung

A Thesis Submitted in

Partial Fulfillment of the

Requirements for the Degree of

Master of Science

in Engineering

at

The University of Wisconsin-Milwaukee

May 2020

ABSTRACT

FACTOR AFFECTING DEGREE PROGRESS OF GRADUATE STUDENTS AT A LARGE URBAN UNIVERSITY AND IMPLICATIONS FOR STUDENT SERVICE OPERATIONS AND UNIVERSITY POLICY

by

Yi-Chen Chung

The University of Wisconsin-Milwaukee, 2020
Under the Supervision of Professor Lingfeng Wang

Advanced Metering Infrastructure (AMI) is an important and basic element in Smart Grid systems. Technologies grow complicated as the world becomes more convenient. Power grid needs to be protected from potential cyberattacks, which may disrupt the power supply and result in huge economic loss and affect people's daily life. It is important to use secure communication technologies to enable various functions including bidirectional communications and remote controls. Since AMI needs to be widely deployed to each home user, power companies are required to build a large number of data concentrators to manage neighboring networks uniformly to ensure that meter data readings can be accurately collected as well as ensure the security of the data transmission process. Besides, since data concentrators are mostly deployed in the public environment, the devices are vulnerable to the impact from outside physical attacks. Therefore, this thesis proposes to construct an improved AMI communication network to increase security and lower its cost. The thesis discusses the security standard, and how the architecture for the AMI communication network is implemented using the Transport Layer Security (TLS) protocol based on the Software-Defined Network.

Keyword: AMI, Smart Grid, Software-Defined Network

To my parents

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

I want to thank my advisor, Professor Lingfeng Wang, who gave me this great opportunity and continuously supported me to accomplish this research project. Especially I am grateful to being given the chance as a dual M.S. degree graduate student for both CYCU in Taiwan and the University of Wisconsin-Milwaukee. Without any prior knowledge of power systems, I'm very grateful for his guidance, encouragement, and support during my pursuit of the degree. Without his help and support, I would not have been able to finish my dual M.S. degree program. Also, I want to thank CYCU for providing me with the opportunity to study aboard, and my professor from CYCU, who supported my decision.

I'm very lucky to have many colleagues in my laboratory who provided me with many useful advices and directions. I appreciate every second they spent in sharing experiences and skills with me.

Lastly, I want to thank my parents, who supported me financially and encouraged me to do my best to complete the program with full financial support, so I do not have to worry when I'm abroad.

Chapter 1 Introduction

1.1 Motivation

The Advanced Metering Infrastructure (AMI) is the basic and important facility in the Smart Grid. The AMI system not only monitors the electrical system usage amount, it also combines the communication technology, and it provides bidirectional, and it has remote control function. Compare to the conventional meter, AMI brings more flexibility and advantages, e.g. it reduces manual collecting data cost, power shut down recovery management. With environmental awareness is rising, every countries start AMI project to provide electrical system management more efficiency.

Most of the power companies are not cooperating with Internet Service Provider (ISP) very effectively, thus, we want more fast, secure, and effective way to collect energy usage information. We usually set data Concentrator at the outside space and basement, through the Power Line Communication (PLC) or Wi-Fi, and it collects Neighborhood Area Network (NAN) metering information regularly, then the data concentrator sends the information to the central system through Wide Area Network (WAN) by day. In order to let meter having standard rule when it exchanges the information, the International Electro technical Commission (IEC) and other organizations set the standards. IEC 62056 is one of the standard that widely uses when the meter information exchanges.

The AMI architecture is based on the IEC 62056 standard, it includes standards of meter module information, and definition of minimum authentication security mechanisms, and the corresponding mode when it applies to different protocols.

Since the AMI combines with communication technologies, when the data is transmitting, it includes huge amount of user privacy, and very important control signal of meter. If it doesn't have an appropriate security mechanism to protect AMI during the communication process, the information security should be concerned. Data concentrators are built in the public environment also it faces huge security challenges nowadays.

We improve AMI expansibility, availability, data transmit security, and we want to provide AMI a widely distributed characteristic. Therefore, we propose the method to use Software-Defined Network (SDN) technology as a new tool, and we develop a new AMI network system. Thesis uses Ethernet to transmit meter information, and we separate computer network with AMI network, and system maintains Quality of Service (QoS) to keep that AMI data throughput has enough bandwidth. If AMI works abnormal, the system can take the initiative to cut the throughput, and it keeps data concentrator availability. With the achievement of the above functions and analysis AMI standard rules, we can provide an effective AMI management.

The contribution of this thesis is that we integrate SDN with AMI, it can centralize and organize data flow easier and more convenient. If the attacks happen, the SDN controller can detect the malicious packet flow in time, and it only blocks single AMI instead of shutting down the whole system to protect power grid from the attacks in time. We use Ethernet to exchange data, it can improve expansibility and reduce costs. We also use virtual network skills to separate AMI throughput with other networks to ensure the security and availability.

1.2 Background

The smart grid generation is rising up; therefore, the traditional meter and manual operation process, this complicated procedures will be replaced by the AMI system, automated system, and communication system in the future. Fig. 1.1 shows that the smart grid collects and analysis electricity usage information by AMI, then it uses communication technology to send the information to the control center. Electricity resources in every area will be scheduled very flexibly by using the control center, and it transmits price information directly to achieve real-time performance [1].

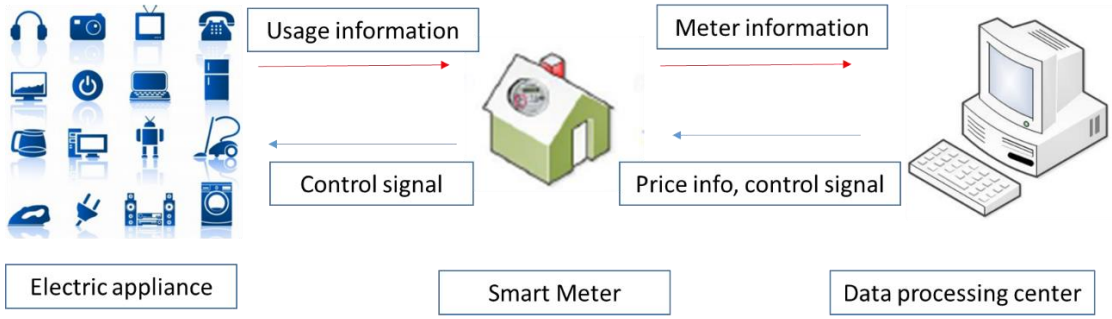

Fig 1.1: Bidirectional communication sketch

AMI compares with conventional meter, AMI combines with communication technologies, it can collect, monitor, detect by different communication protocols, and restart, remote control when system breakdowns. It can reduce the cost of manual collecting of data and maintain the system, also the efficiency can be improved.

In order to avoid the communication protocol incompatible, and system information cannot use between equipment, Utility AMI formulates the high-level requirements [5] which makes AMI suppliers can follow when they design and produce the AMI, and it includes 18 requirements, table 1.1 shows it.

Table 1.1: High level requirement [5]

Requirement	Function
Standard Communications Board Interface	Smart meter and communication interface use public standard on different protocol, and it avoids to use by single supplier
Standard Data Model	Client and smart meter use public price standard
Security	By public standard to avoid cyber-attack, e.g. man-in-the-middle, modification…
Tow-Way Communication	Provide client to control boundary network, and it can transmit reliable with bidirectional function.
Remote Download	Provide smart meter to remote update firmware, and security certificate.
Time-of-Use Metering	Provide time zone power usage amount by different time price, and it reduces peak time usage.
Bi-Directional and Net Metering	Smart meter can provide bidirectional throughput and net usage record, it helps controller monitor distributed generator.
Long-Term Data Storage	Smart meter must have storage of 40~50 days information hardware to provide usage report.
Remote Disconnect	Remote recovery and disconnect function to reduce cost.
Network Management	Remote detect smart meter and network to monitor its network status, reliability.
Self-Healing Network	When network traffic jam happens, it can detect and recover by itself, it provides usage information accuracy and reliable.
Home Area Network Gateway	Client's communication gate.
Multiple Clients	People who passes authentication can save smart meter information.
Power Quality Measurement	Provide usage quality report, and it maintains grid quality.
Tamper and Theft Detection	Detect and report theft status in order to reduce power loss and cost.
Outage Detection	Report abnormal disconnection and detection to controller, it can recover power more efficiency.
Scalability	It keeps smart meter not be effected by other systems, software, hardware.
Self-Locating	It gets meter location by GPS when accident happens, we can get location accurate.

According to the AMI requirements, and we want to satisfy AMI security, consistency, scalability. International Technical Committee formulates the IEC 62056 international standards for exchanging meter information. IEC 62056 [6] uses object recognition, modulation, access service, and it uses different protocol to communicate information, and it provides different suppliers and systems interoperability. It includes three different parts, Fig. 1.2 shows structure of COSEM:

1. Companion Specification for Energy Metering (COSEM) [6]

COSEM is a common interface model which is established for object-oriented methods. It is for the communication metering equipment. It allows us accessing the meter data through this interface, and it manages the energy meter. COSEM standard uses the model which we familiar, e.g. energy meters, water meters, gasoline meters, and it is defined as instrument interface. At the same time, the COSEM specification defines the object control interface and the communication channel.

2. Device Language Message Specification (DLMS) [6]

It is an application layer based on the objected-model idea. It is in the application layer, it includes the encoding rules, and message interaction processes, and it corresponds error handling mechanisms between client and server. The specification and the underlying communication protocols are independent in the communication medium, and they are using to support applications, such as remote meter reading, remote control, and value-added services. At the application layer, meter objects use DLMS services to ensure interoperability and interchangeability.

3. Transportation Layer communication protocol

It includes: Part 47 [7] defines the transmission layer standards to provide TCP/IP transmission rules; Part 46 [8] defines information transmission layer standards, and it uses HDLC protocol; Part 42 [9] defines physical layer standards to provide GSM, twisted pair transmission standard; Part 21 [10] defines infrared transmission to achieve local information exchange.

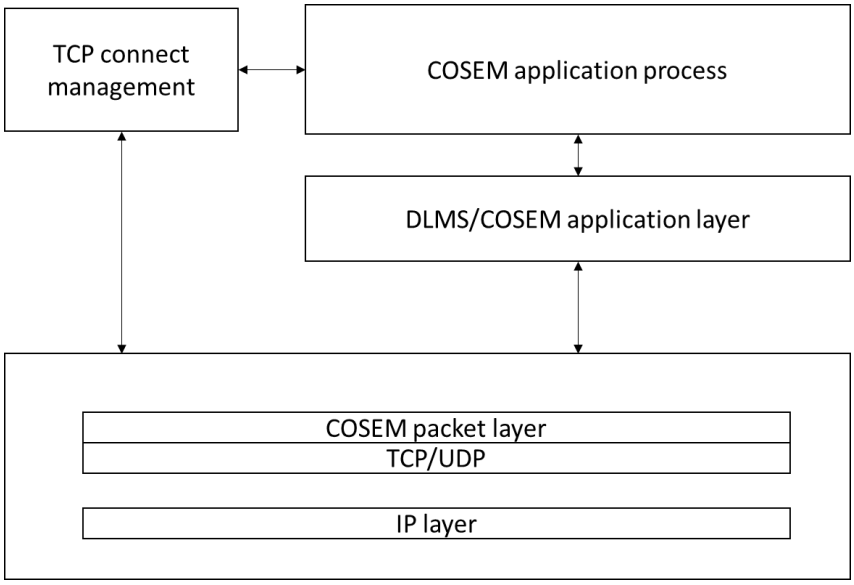

Fig 1.2 Structure of COSEM transportation layer and TCP/UDP service

As Fig 1.3 shows, smart meter includes many AMI system currently, and it highly relies on the communication infrastructure, it also makes the power system framework more complicated. The communication network not only has AMI network flow rate, it also includes Remote Terminal Units (RTU), Phasor Measurement Units (PMU) and Intelligent Electronic Devices (IED), etc... [12]

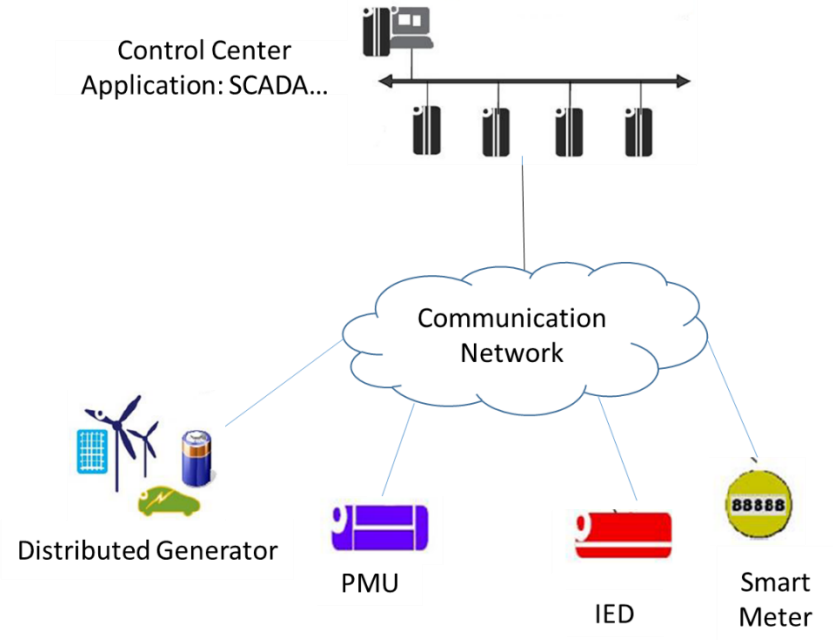

Fig 1.3 Smart grid-application and communication network [12]

Therefore, we want to manage huge amount of equipment more efficient, and we let AMI has flexible expansibility and availability, and we want to satisfy current transmission and security rules. We have to figure out more intelligent and automatic management methods to centralize and optimize the smart grid.

1.3 Thesis structure

In chapter 1 we introduce smart meter, and we describe the standard rules. Chapter 2 describes current AMI status, it includes the body framework, weak point, and risk analysis, relevant standard and testbed. Chapter 3 raises information security and communication protocol. Chapter 4 describes the details of the requirements. Chapter 5 discusses the Software-defined network framework and how to combine it with AMI. Chapter 6 introduces system architecture. Chapter 7 shows the experiments and results. Chapter 8 concludes the paper and future works.

Chapter 2 Advantage/Disadvantage and Risk in AMI

Advanced Metering Infrastructure is the key infrastructure in the smart grid, it is a system which integrates traditional meter reading with modern communication technology. In this chapter, we discuss more details: framework, risk analysis, and smart grid advantages based on a software-defined network.

2.1 Advanced metering infrastructure framework

Advanced metering infrastructure has two different communication networks, it is wide area network (WAN), and neighborhood area network (NAN). It has three important infrastructures: smart meter, data concentrator, and central system, as Fig 2.1 shows.

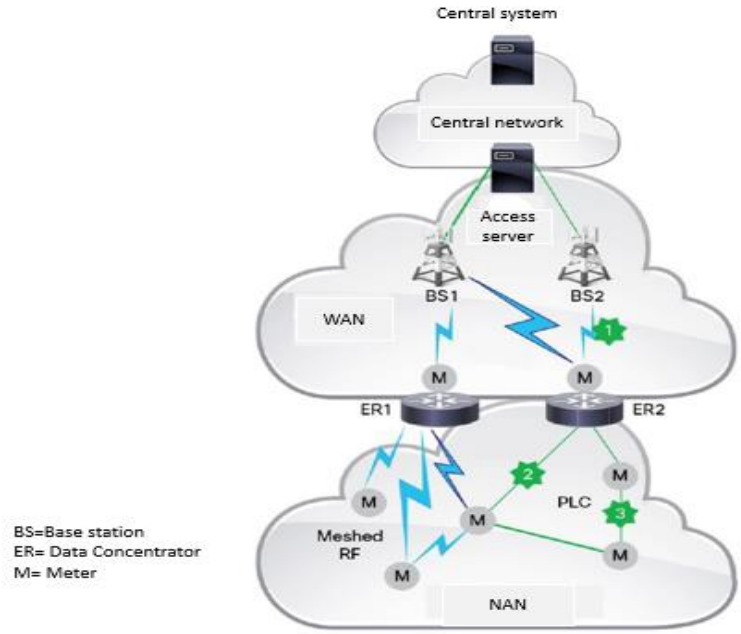

Fig 2.1 Advanced metering infrastructure framework [11]

2.1.1 Communication Network

1. Wide area network

Wide area network [15] is a data communication network that covers long distance, and forms by multiple local area network communication technical. The connection range can cover the whole country or even the whole world.

2. Neighborhood area network (Local area network)

Neighborhood area network [15] uses as short distance information and it transmits between data concentrator and advanced metering infrastructure. It uses different types of cables as the transmitting medium, and it connects small-scale computer equipment together to achieve the purpose of resource sharing.

2.1.2 Important infrastructures

1. Smart meter

Smart meter [16] has three main functions, bidirectional communication, measurement, control function. Because it supports bidirectional communication between the meter and the supplier, the communication from the meter to the network may be wireless, or a fixed wired link, such as a power line carrier.

2. Data concentrator

The main function of data concentrator [16] is the medium between central system and data concentrator. It provides the transmission of information and control signals through various communication technologies. Another function is that it can take and collect the meter information in the manage area, and it sends information to central

system. Therefore, data concentrator must have longer and bigger storage to save information.

3. Central system

Central system [16] collects all user information from data concentrator, and it can calculate the last electricity data statistic, analysis, and it provides electricity company information for power dispatching and deploying. In addition, client can search their usage information, and bill details through the power company network platform.

2.2 Advanced metering infrastructure weak point and risk analysis

Because of using communication technology to provide advanced metering infrastructure bidirectional function, AMI communication risks are being highly valued. In 2011, Ping-Hai Hsu, etc. proposed two levels of security [17]. It is high level and low level respectively. High level is the information transmitting between the central system and data concentrator by wide area network, the security mechanism uses public key infrastructure (PKI) as an end to end certificate; low level is the information transmitting between data concentrator and AMI by neighbor area network, it uses symmetrical encryption as information protection.

The data concentrator becomes an important medium for the control center and various communication protocol AMI types. It has bidirectional function, also it needs to collect and storage AMI information and control signals from everywhere. Therefore, if a low level security only uses symmetrical encryption, the security is not strong enough. Because of symmetrical encryption feature, data concentrator and the client must discuss a key to encrypt the data, but this will cause two problems.

The first problem is the key confidential during date transmitting, another is that data concentrator needs to build different key with different clients, this behavior will let data concentrator to manage huge amount of keys. It causes key management too complex or inefficient. On the other hand, a data concentrator usually builds in the public area, under the public environment, it may have some external physical destroy, and it will have different impacts on AMI stability and data privacy.

2.3 Advantages of smart grid based on SDN

Smart grid has widely distributed characteristic, and we want to maintain power infrastructure having high availability. We need to use reliable and secure communication techniques to keep data's security when transmitting. Therefore, most of the companies use a special line or closed communication network as the solution, but this solution doesn't achieve high efficient security also it costs too expensive to maintain the system. Some researches in recent years start using a software-defined network concept to the smart grid, we hope that we can use SDN advantages to improve quality of data transmission and security also lower the cost on system maintenance.

Xinshu Dong et al. [18] want to maintain the high availability of the smart grid, they aware that the cyber-attack is not only from the external network, it can also inject a back door attack to the equipment which just produces from the company. This kind of attack will make a heavy threat to the company. The conventional security mechanism such as firewalls is not enough to secure system, so it needs a more flexible detection mechanism. Therefore, they proposed the SDN concept into the smart grid, and the control center can deploy OpenFlow switch by the controller in order to surveillance

throughput and filter suspicious packet, also it prevents distributed denial of service (DDoS), and it keeps smart grid communication network available.

Jianchao Zhang et al. [19] observe that smart buildings not only improves life quality, also it can reach energy saving and reducing carbon emission by auto power switch. However, it needs efficient power management to build a huge amount of sensors and microcontrollers in the building, and SDN can help them on connection. It has flexibility and scalability, also it can achieve the purpose to customize control and management for the client.

Young-Jin Kim et al. [12] mention that the current smart grid needs to build a huge amount of sensors and controllers. Due to every equipment has different size packets and frequency, and network throughput is more complex and it is hard to manage, and if every equipment has their exclusive channel to transmit data, it can avoid mutual interference, and it can improve data's security. Current virtual network technologies are increasing with the smart grid which is more popular, it is more difficult and complex to operate also it costs higher on maintenance. Therefore, they designed a SDN-based architecture solution for virtual utility networks (SUVN), they use network slice technical to separate every equipment throughput, and then they can manage different equipment network status respectively to enhance security.

Po-Wen Chi et al. [20] propose an SDN-based AMI threaten detection mechanism to make sure that AMI data flow in a wide area network will not be attacked by malicious modification. They use a rule-based detection system combined with SDN, and they use OpenFlow switch to detect abnormal throughput to provide efficient defense, and it can protect AMI from information threaten.

Chapter 3 Information/Communication Security Issues

Since the power grid integrates with communication technology, system becomes more complicated, and the information transmits in the network getting more dangerous. This security issue might causes huge damage such as if the cities blackout, it will put people in danger. Therefore we are going to discuss some attacks and communication protocol process.

3.1 Common cyber attack

The attacks usually happen by some tempting motivation which makes attackers want to get. Power system is an important infrastructure for the human being, if the system is attacked, it might cause system breakdown, information leakage, stop working…, more serious, it could put people's life and property in danger. Therefore, how to analyze and prevent an attack is a big issue for us. In this paper, we organize a common attack type and we divide them into four security requirements according to the attack characteristic. They are confidentiality, integrity, availability, and non-repudiation.

3.1.1 Confidentiality

Confidentiality in advanced metering infrastructure is an important security requirement. If the hacker gets energy consumption information and hacker saves it from meter via wiretapping, he can analyze the consumer life routine or observe if there are people live in the house. Therefore, the consumers doesn't want any people or suppliers to save their information and personal privacy without authorization, and we want to avoid equipment in the home area network or other auto systems saves AMI's information without authorization as much as possible. Meter Data Management System

(MDMS) also needs to keep consumer information in secret, so only the system has authorization can save information.

3.1.2 Integrity

The meaning of integrity is not only for people that without authorization to modify data, it also protects control commands of system forged by hackers, it will let AMI be malicious operated without authorization. In addition, AMI needs to keep the entity integrated, and we need to prevent it from physical destroying. If the equipment was destroyed, it will cause energy usage information inaccurate, attacker can earn improper benefit and consumer will pay more money.

3.1.3 Availability

When advanced metering infrastructure doesn't work properly, it might derivative many problems such as the energy usage information can't be recorded, especially when a data concentrator doesn't work, it might cause big range AMI information collecting inefficiency e.g. hardware damage, software malfunction or communication interference and disconnection. Therefore, we need to use system detection to keep AMI availability and evaluate the method how we can reply to the center as soon as possible.

3.1.4 Non-repudiation

Non- repudiation is the most key point in the AMI information exchanging. Because of AMI measuring energy usage information is the basis for expenses, if the consumer doesn't admit that the information is correct, it will have a conflict on the side. In addition, the power company needs to identify the consumer who is legal or not, and the company wants to avoid that consumer impersonates to transmit meter information.

Therefore, they need to make sure each identities, they use asymmetric encryption technology, and it achieves non-repudiation by the correspondence between public keys and private keys.

3.2 TLS communication protocol process

Transport Layer Security (TLS) [21] is widely using in the internet, it is a communication protocol to protect information security. Because of the advanced metering infrastructure build in the public network, if the meter's data transmit without encryption or authentication source, the data information will be very easy to modify and wiretap. In this paper, we use the TLS communication protocol as the protocol when information transmitting to achieve confidentiality, integrity, correctness of the source. Current standard rules e.g. IEC 62351 [22] and NISTIR 7628 [23] are put TLS protocol as one of the security rules in data transmission protocol.

Transport layer protocol is the version that enhances Secure Socket Layer (SSL) security and information integrity by the Internet Engineering Task Force (IETF). They enhance the Message Authentication Code (MAC) algorithm and define more alert information e.g. decryption-failed, access-denied, certificate expired. Table 1.2 shows the difference between TLS and SSL. [47]

Table 3.1 Difference between SSL and TLS [47]

Features	SSL	TSL
Alert message types	12	23
MAC	No rules	Has rules, hash message authentication
Key	No rules	Has rules, Pseudo-random Function
Certificate verification	Complex	Easy

When client and server connect, it will start TLS connection process to exchange encryption and both certificates. If the protocol version aren't same or certificate verification fail, it will disconnect to avoid any illegal communication, as Fig 3.1.

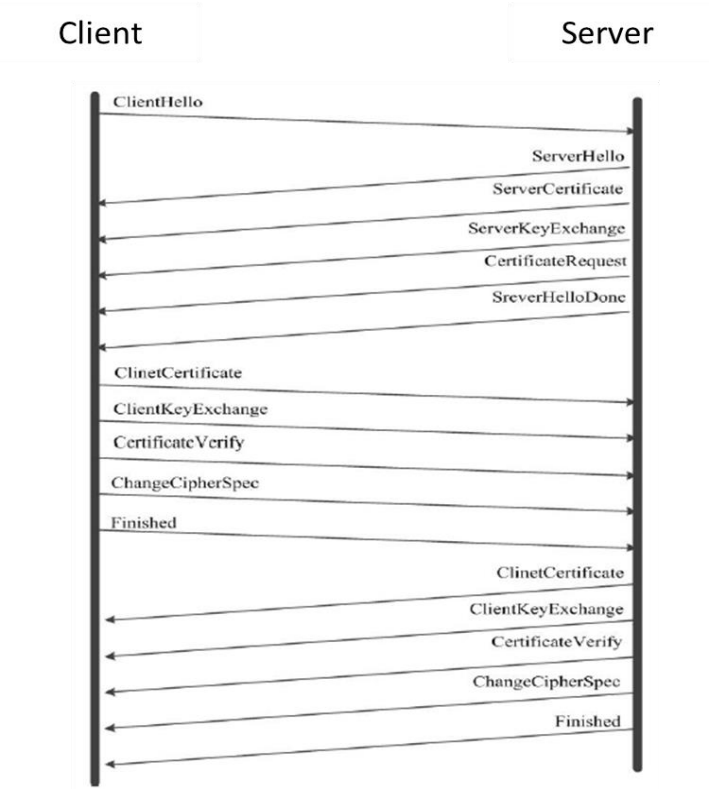

Fig 3.1 TLS communication protocol process [21]

1. Step One

The client sends "Client Hello" message to server when they connect, it includes protocol version, encryption algorithm, and random number from client.

2. Step Two

After server received "Client Hello", it will reply "Server Hello" to client and compare both protocol version are same or not, and if they are different, it will disconnect.

Server sends the certification to client. The certificate is based on X.509 [24] standard, it is a digital certificate issued by Certification Authority (CA), it includes public key, identity verification, and it needs to make sure integrity and authentication. Certificate has digital stamp and expire day to protect it be modified. If server needs to confirm client is legal and safety, server will sent "Certificate Request", and send "Server Hello Done" to client in the end, it means server connection process over.

3. Step Three

If the server wants to verify client, after client receives "Certificate Request" from server, it will send certificate to server, and let server verifies if client is legal or not, then client starts check server's certificate, if it is legal, then client can get the key from server's certificate; otherwise, client sends an warning sign to server then disconnect. If the connect process goes well, client will send "Change Cipher Spec" and "Finish" to server. "Change Cipher Spec" is using to tell server that client is secure, and ready to communicate. They also use the encryption algorithm when they negotiate successful by each other, add encryption on "Finish" send to server and it verifies the connection is working well.

4. Step Four

After server receives encryption data from client, it uses server's private key to decrypt and verify. Server will send "Change Cipher Spec" to client and tell client that server is ready and communication is safe, and it uses encryption algorithm. Send "Finish" with encryption and transmit to verify connection.

According to TLS communication, if client and server are both encrypt and decrypt successful, message can be verified correct, it means TLS channel is working well and connection is done. Both client and server can use this channel to encrypt, transmit, and use this to keep information's confidentiality, integrity and correct identity in the future.

Chapter 4 Requirement Documents for AMI

About the AMI standard, many international organizations have formulated some standards already, such as the American National Standards Institute (ANSI) and the International Electrotechnical Commission formulated ANSI C12 and IEC 62056 standards. The standards include the meter application layer information format, and the design of the physical layer communication protocol. Because security requirements are different in every country, they promulgate AMI standards very positively to meet the criterion. Such as Utility Communication Architecture International Users Group (UCAIug) promulgated AMI System Security Requirements [25] and AMI Security Profile [26] to give AMI supplier, and let them meet the standards; In Europe, British Energy and Department of Energy & Climate Change (DECC) formulates Smart Metering Equipment Technical Specifications [27] and Netbeheer Nederland formulates Privacy and Security of the Advanced Metering Infrastructure [28], both of them are asked for the security of meter. In addition, AMI can communicate with control center to make sure AMI will not affect the operation directly by whole power system. North American Electric Reliability Corporation (NERC) formulates Critical Infrastructure Protection (CIP) standard [29], it formulates huge power system communication security rules to maintain huge power system and let control center can operate reliably.

4.1 North America Electric Reliability Corporation (NERC) CIP

With the smart grid is increasing, its equipment starts to combine and rely on communication technologies, but it also lets the power grid facing communication and information field's threaten. When the transmission network and control center are

threatened by attackers or people who operates it incorrectly, it might cause big range power shutting down or other injuries, the loss will be uncountable. Therefore, NERC formulates the protection rules to make sure that the transmission network and control center can operate well.

NERC [29] is a reliable organization which was authenticated by the Federal Energy Regulatory Commission (FERC). They dedicate to formulate and execute some reliable standards, monitor a huge electrical system in North America, educate and train people they hired in this area. It uses some standards to protect the electrical system. E.g. NERC CIP 002 (essential communication property identity), NERC CIP 003 (security management control), NERC CIP 004 (related employee education), NERC CIP 005 (Electricity safe boundary), NERC CIP 006 (essential communication property physical security), NERC CIP 007 (system management security)…

4.2 New AMI Security Advices

Because the public enterprise purchased process and equipment supplier need to follow security rules when they build AMI [26], public enterprise communication user organization has AMI-SEC team and formulate an AMI security test standard, they proposed a standard of smart grid's home area network port to meter data management system security method. This team studied AMI used cases, AMI risk evaluation, and security service analysis to modify and enhance the Department of Homeland Security's development advice of control system, proposed a new AMI security advice shown in table 4.1.

Table 4.1 AMI development advice [26]

Suggestion items	Purpose
Protect system and communicate	Protect AMI and communication elements, keep communication integrity, confidentiality and data authenticity
Information and document management	Manage and protect AMI element develop and test, risk and influence analysis.
System development and maintenance	Planning and implement system maintain, monitor in time and upgrade system
Incident response	Planning and implement incident response and propose operation maintenance plan
System and information integrity	Make sure that secret information won't be modified or deleted by any unauthorized way
Access control	Resource only be saved by identified employee
Audit	Audit AMI elements and system journal on time to make sure system work well
Survivability	When system be attacked or some incident, it can complete mission in time

4.3 Texas Electrical Network Communication Security Report

Since the smart grid incorporates with many advanced infrastructures, and it highly relies on communication basis infrastructure, it lead to our electrical system more complex, and it increases cyber attack's risk, e.g. affect by weather, power grid hacker, or some technical problem. In Texas electrical network communication security report mentioned [29], Public Utility Commission (PUC) should put cyber-security as a target when they start building a smart grid and smart meter. Therefore, some public companies and organizations can participate in network security activities and training, and put more effort to learn cyber-attacks e.g. DoS, DDos..., they try to learn and know how to defense cyber-attacks in the future.

They should embed some basic security functions to the system when they design or build the equipment to achieve their security. There are many organizations devote to formulate smart grid security standards, their goal is to provide professional technical skills and security, and they hope they can provide consumer and supplier quality assurance. Since new threaten keep increasing, most of these network security standards are using current standards to adjust or help, and make sure each system and equipment in the smart grid has good protection.

4.4 Smart Meter Equipment Technical Standard

In England, advanced metering infrastructures include electrical meter, gas meter…, in order to keep infrastructures can at least maintain the lowest security and let it meets electricity supply licenses and gas supply licenses standards, England Ministry of Energy and Climate Change published Smart Metering Equipment Technical Specifications (SMETS) [27], when they settle AMI, it needs to meet the requirement to make sure the lowest security on physical, function, connect port and verify system to promote third party development of the AMI.

The connection method of smart meter standards, we want our software and hardware integrity, security, and availability, and communication quality of the equipment will not be affected when the fault happens. This standard shows that when smart meter executes any commands, response, or warning, it needs to encrypt and verify information's integrity, source, and receiver correctness. Therefore, encryption algorithm needs corresponding to some higher level algorithms in order to hold their security. When smart meter receives any security update from firmware, it needs to wait for firmware's

command for starting the installation or update. This procedure is to avoid the attacker's malicious installation.

The connect port security needs to have the function which can detect communicate port on smart meter to avoid any information saved without authentication or send control command from home area network port leads to housing equipment malicious operate. According to above mentioned, if any abnormal happen, smart meter must record all situation and report to higher system.

4.5 AMI Privacy and Security

Netherlands Grid Operator is highly focusing on privacy and security risks, because this risk in the power grid operator and the consumer will cause huge influence. Therefore, Netbeheer Nederlands decides to formulate strategies together [28], and it establishes national smart meter privacy and security team to manage privacy and security. All of the power grid operators need to follow the rules, they use the rules as the basic framework to design AMI, and they reduce damage which AMI might occur.

In this standard, it includes four types, general step, equipment detail requirement, information communicate requirement, and control center requirement. General step indicates that power grid operator needs to define and show their purpose on data collection, employee responsibility, AMI internal components authorization and personal identity. They set the security strategies at the same time; equipment detail requirement rules that the AMI and data concentrator entity must be protected and be able to detect entity level of damage. They need to use end-to-end encryption when they communicate to ensure information integrity, confidentiality, and source correctness; information communicate requirement shows that the power grid operator needs to use

cyber security step e.g. firewall, anti-virus software or invasion detect system to maintain smart meter's communicated channel availability, security, and quality; control center requirement formulated that control center only communicates with the equipment which authorized to avoid from the attack.

Chapter 5 Software-Defined Network

SDN creates network creativity, with each TCP / IP layer likely providing individual creativity. The SDN enables networks and software interfaces becoming more versatile and open, making it easier for network management. Compared to conventional networks, SDN will provide more accurate and precise traffic control. It gives network administrators the power to unilaterally change routing tables on routers, without having to deal individually with each router. It also offers the ability to create new services through virtualization. Finally, through the availability of the control plane, it provides better and more robust security. For example, each user may have different capabilities by the network to control their firewalls. [48]

SDN is used for several networking applications nowadays. For example, it is used for simplicity of network management, and the control of virtual machines in cloud computing and data centers. By removing proprietary architecture issues, it can link multiple data center networks. In this method, the concept of offloading workload can also be used for devices that require more powerful machines with other safety criteria. Finally, SDN can be used for internet testing, without modifying the current network, to test other ideas. [48]

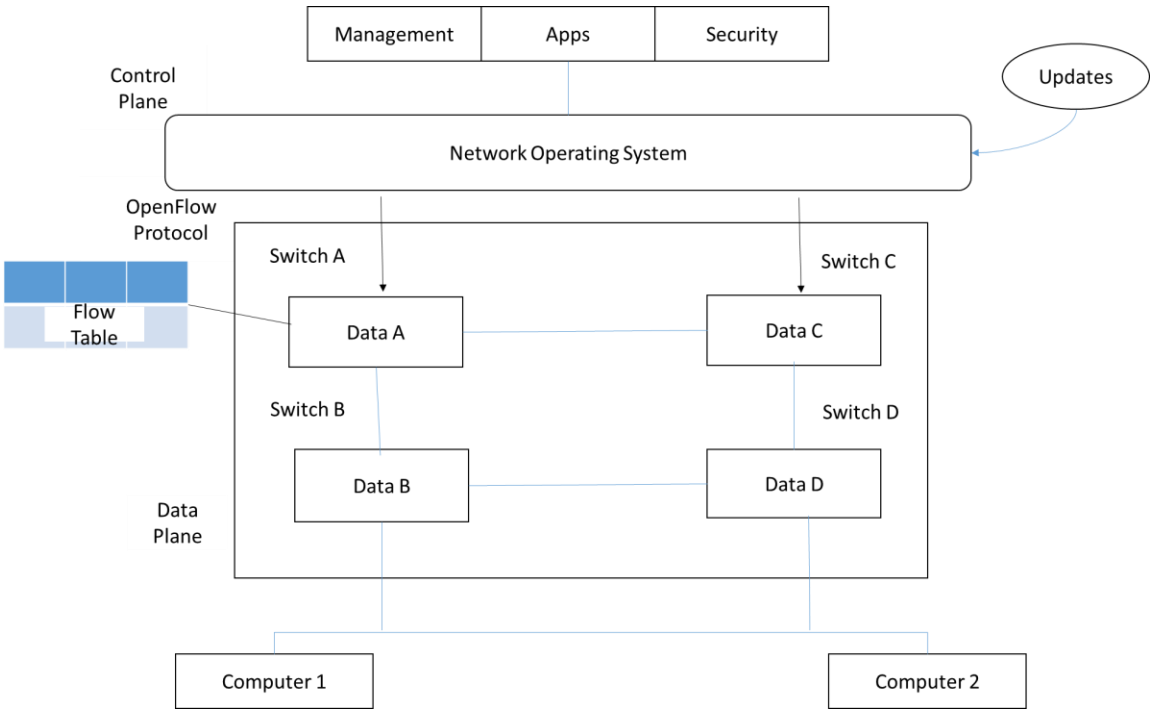

Fig 5.1 SDN networks sketch

5.1 Introduction of SDN

In 2008, Standford University initiates the SDN research project, based on software-defined network concept [30], they change traditional network control and data transmission function to the controller and OpenFlow Switch. They build network information more flexible, easier manage and control, and good enough to support the requirement of network changing fast. Network manager can program functions what network needs on the controller to manage information transmission and forwarding path in the switch. The Controller is formed by OpenFlow Protocol, Network Applications, and Network Operation System, it is in charge of switch's packet transmitting and forwarding; Switch is to implement OpenFlow protocol, Flow Table and Secure Channel.

According to the definition above, When OpenFlow switch receives packet, it will check the rule in flow table, and check if it corresponds to packet, then it forwards packet if it meets the rule; if it doesn't meet the rule, it will follow the protocol and send packet with OpenFlow header information to the controller, and controller decides packet next step, then it replies the result to the switch through secure channel. Flow table in switch will add new rule and let switch dealing with packet at the same time.

With OpenFlow network architecture, we use controller to distinguish meter's network throughput, and we design a method to separate general throughput with meter throughput. It can achieve security and monitor whole meter throughput status by controller, and it can also detect abnormal traffic anytime.

5.2 SDN Controller

The key component of SDN-based system is the SDN controller. Controller has the functionality portion, and it can be regarded as a network brain. SDN controller collects information from network switches. By considering packet information, determination and response. The SDN controller is allowed to drop the packet, and it can establish a standard, and allocate standard to the switch. The SDN controller has two interfaces, one for user applications and the other for SDN switches. First of all, called the Northbound API. This API allows a designer to update the elements of the network from distant points. Including the REST calls, which is essentially sending queries to a specific web URL, it could be done in a few ways and it gets answers from them. We can use the answer for those purposes. The second interface is the rule that is sent from the SDN controller to SDN switches. The most popular Southbound API protocol is called OpenFlow. [48]

5.3 FlowVisor

FlowVisor [33] is a virtual network tool which builds on the OpenFlow protocol, and the main function is to do logical slice network on physical network, and it sets up many virtual networks on the network device, then separates each throughput as Fig 5.2 shows. It can let multiple controllers controlling one switch. FlowVisor is a tool between controller and switch, therefore, FlowVisor is according to the deployment rule, it lets switch forwarding throughout to the corresponding controller, as Fig 5.3 shows. In addition, controller can only control corresponding throughput, but it will not know the network which controls slices network from FlowVisor. We use FlowVisor to slice network can implement separating network throughput, and it lets AMI information throughput not affected by other information throughput. It is not only protecting AMI information bandwidth size also protecting information's privacy and correctness.

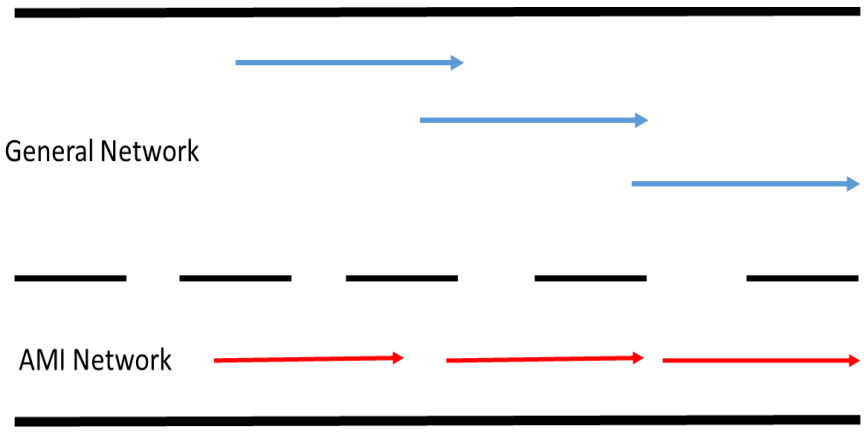

Fig 5.2 Slice network sketch

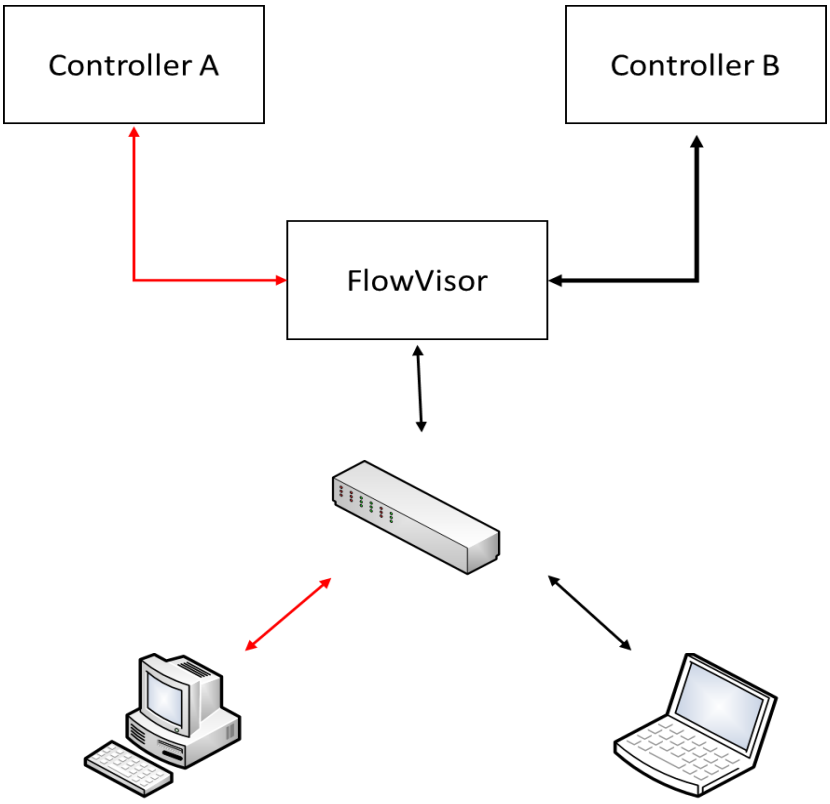

Fig 5.3 Multiple controller manage one switch together

5.4 OpenFlow

SDN allows the control plane to communicate with the data plane by using those protocols. One such protocol is the OpenFlow. OpenFlow is the first standard interface for communication specifying between the SDN architecture's control, and forward layers. It enables direct accessing and manipulating of the forward path, both physical and virtual of network devices such as switches and routers. In other words, it is a communication protocol that proposed to offer routing decision center (control plane) communicates between routers and network switches (data plane). Simply, it gives programmer leverage over router routing protocol. [48]

5.4.1 OpenFlow Switch

OpenFlow [2] switch main function is to manage flow in the OpenFlow framework, it includes three parts:

(1) Flow Table: It uses controller, and it saves the action which sends from switch in the flow table, and switch can use this action to decide where flow to go.

(2) Secure Channel: A secure channel between controller and switch communicate.

(3) OpenFlow Protocol: Define how controller and switch communicate and transmit information.

5.4.2 Flow Table

(1) Header file: Flow's header information, OpenFlow packets has the OpenFlow header different with other packets, it define all packet information e.g. source, destination.

(2) Action: Deal with flow action, e.g. command packet in or out from which port.

(3) Counter: Statistic packet information, e.g. packet send how many time, action table.

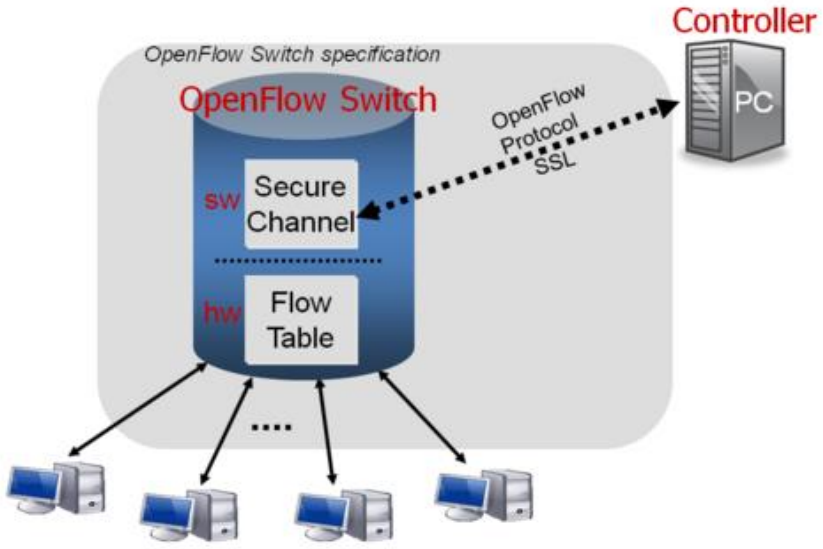

Fig 5.4 OpenFlow inner and connected with controller [2]

Chapter 6 System Architecture

6.1 Comparison of AMI Communication Architecture

The AMI needs to build in every houses, and it always builds different environment, this will affect AMI location evaluating result, and we want to avoid that quality of information in data concentrator be affected. Also, data concentrator needs to build in public, it might suffer some physical attack from outside or cyber-attack inside, and it affects whole area. In this paper, network service suppliers play a role that has SDN already, and it uses SDN to provide network service for clients. We also integrate SDN advantages, and we propose a new AMI network communication architecture, we let AMI transmitting information through Ethernet, and we compare advantage and disadvantage with traditional AMI.

6.1.1 Conventional AMI Communication Architecture

The conventional AMI communication architecture is shown as Fig 6.1. The data concentrator collects meter information in neighbor network every 15 minutes, and it consolidates information then transmits to the meter reading information management system in control center. We want to keep information integrity and availability, data concentrator uses middle and short distance transmission technical, e.g. Zigbee, PLC, it receives information in neighbor network, and wide area network usually uses long distance transmit technical, e.g. GPRS, LTE.

In information confidentiality, because of neighbor area network and wide area network are using different communication technologies; therefore, some researchers use two levels security method [17]. Neighbor network uses IEC 62056-53

security mechanism, and it allocates AMI and data concentrator encryption key from key distributed center; Wide area network uses public key infrastructure to manage data concentrator and meter reading data management system key by a special certificate center. This key can encrypt and decrypt information and verify it, so we can keep information integrity, legality, and we can check the source correctness to achieve two levels of security mechanism.

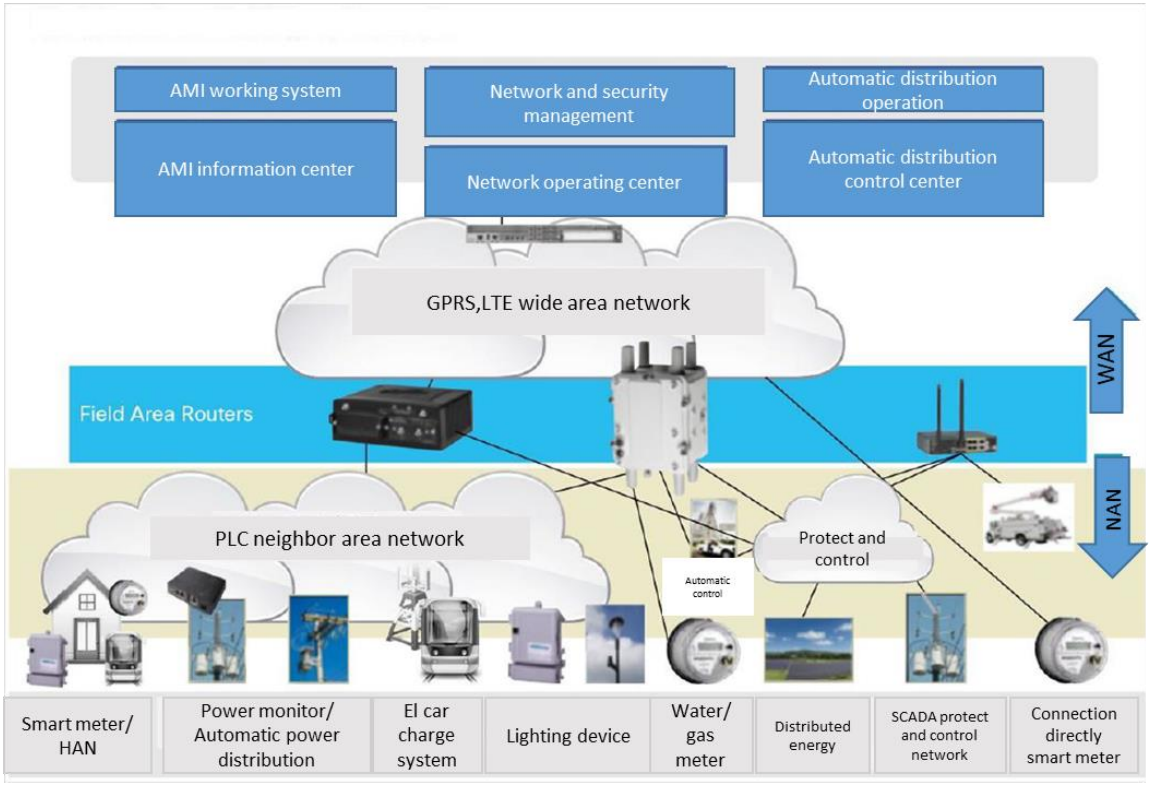

Fig 6.1 Current AMI communication architecture [34]

6.1.2 SDN Based AMI Communication Architecture

In this paper, we propose a new SDN based AMI communication architecture, as Fig 6.2 shows, we integrate SDN with AMI, and we let AMI transmitting meter information to data concentrator every 15 minutes by general household network.

We want to keep information's confidentiality and integrity, the AMI uses TLS connection with data concentrator, also we keep information security and source authenticity. On the other side, we want to ensure that other network throughput not affects information transmission bandwidth, we use virtual slice network, and then AMI can have independent bandwidth.

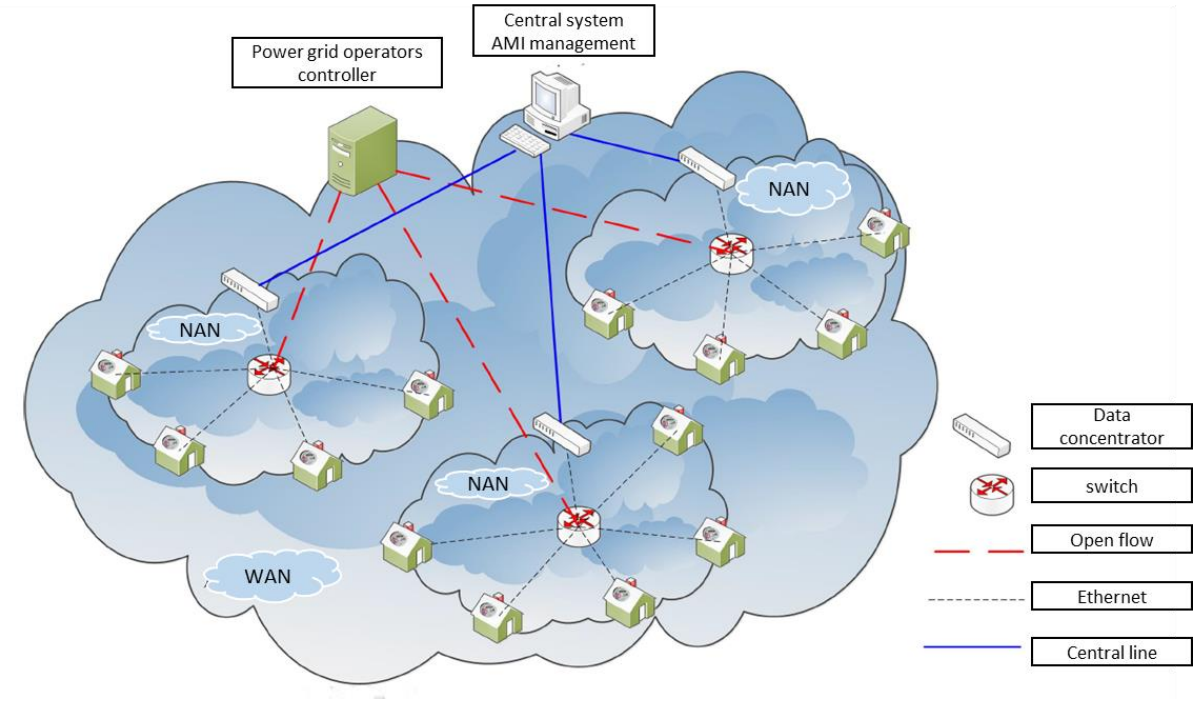

Fig 6.2 SDN based AMI communication architecture simulation

6.1.3 Comparison between Traditional and SDN Based AMI Architecture

We do a comparison of the current communication architecture with software-defined network communication architecture. With this comparison, we can understand why the software-defined network can do much better work than current conventional architecture. Table 6.1 shows the comparison details.

Table 6.1 Current V.S SDN based communication architecture

	Advantage	Disadvantage
Current communication architecture	1. High availability 2. Support multiple communication technologies	1. High cost 2. Low expandability 3. Low security
SDN based communication architecture	1. Easy to build 2. Easy to manage	1. Might has potential risks

Current communication architecture needs to build lots of data concentrator, and it get meter information by different communication technologies, but it costs a lot of maintenance cost to build data concentrator, e.g. it needs at least two special lines on every data concentrator, and data concentrator has allowable number of specific connections, if connections exceed the allowable quantity it might cause data concentrator works abnormal. Therefore, it costs a lot to build the infrastructure. The more internet routing table, the more complicated it is. Current network architecture causes many problems which is becoming more and more inadequate. The switch and router must constantly extend and reassemble the packets to implement different network protocols, resulting in low transmission efficiency and unable to efficiently use the network bandwidth. In addition, there is a high risk of manually setting one by one. Once the network administrator enters the wrong command, it is easy to cause the network service paralyzed.

Data concentrators usually build in public and open environments, the equipment entity is very easily destroyed from outside, it threatens AMI stability and information privacy. Therefore, we propose AMI integrate with SDN technology, and information exchanges under household network to centralize and manage AMI information destination. If some malicious attacks happen, the SDN controller can detect malicious attack packet in time, or it can block single AMI, malicious throughput in time to protect power grid equipment. The potential risk exists, e.g. if client plugs out meter system network cable or shuts down network connection equipment, it might cause meter system can't transmit information.

6.2 System Architecture

We use software-defined network advantage, and we propose new AMI network communication architecture. We use Floodlight [35] as SDN controller to manage and monitor meter throughput, and we use OpenSSL [36] to implement transport layer security (TLS) encryption channel as information transmission protocol to achieve information confidentiality, integrity, and source verification, then we use Raspberry Pi [37] embedded system as platform and simple Python to simulate meter information transmission, and we build a test platform as Fig 6.3 shows. This test platform follows standards to achieve user interface, throughput separated, bandwidth usage, abnormal detection, and active blocking, and we ensure AMI throughout confidentiality, availability, and security when data transmitting in Ethernet.

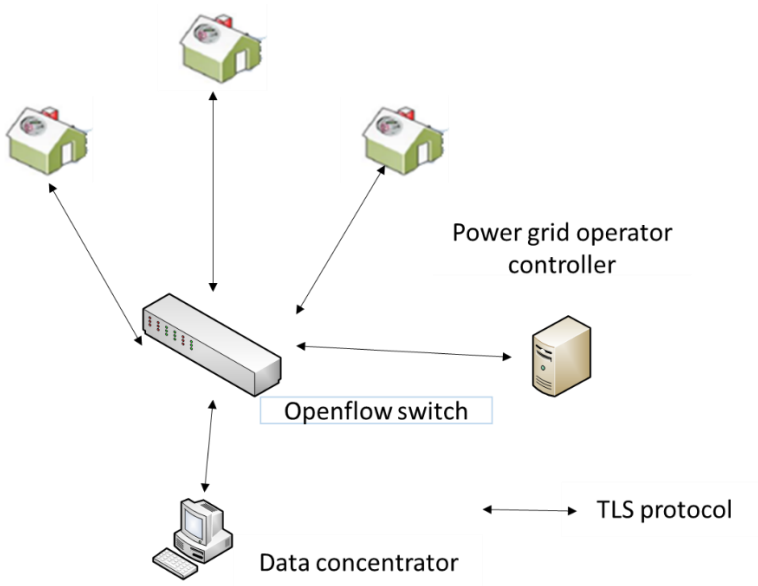

Fig 6.3 New AMI communication architecture

6.2.1 Controller and Switch

The main function for controller is to manage whole network throughput and packet direction, it masters network channel's availability. We use computer with Ubuntu operation system to run control, processor is Intel I5-3470, and 16GB memory and two 1Gbps Ethernet network port. Floodlight use as the controller operation system. Switch is Pica8 P-3290 as OpenFlow switch with 48 1Gbps Ethernet network port.

6.2.2 Data Concentrator

Data concentrator responses multiple AMI connection at the same time, and it receives meter information. This system is based on Ubuntu operation system, processor is Intel I5-3470, and 8GB memory, two 1Gbps Ethernet network port. When system starts running, it will wait AMI connecting with system by TLS communication

protocol, if connection is successful, it will receive meter information at regular time, and reply information to show that receive success. Fig 6.4 shows the process.

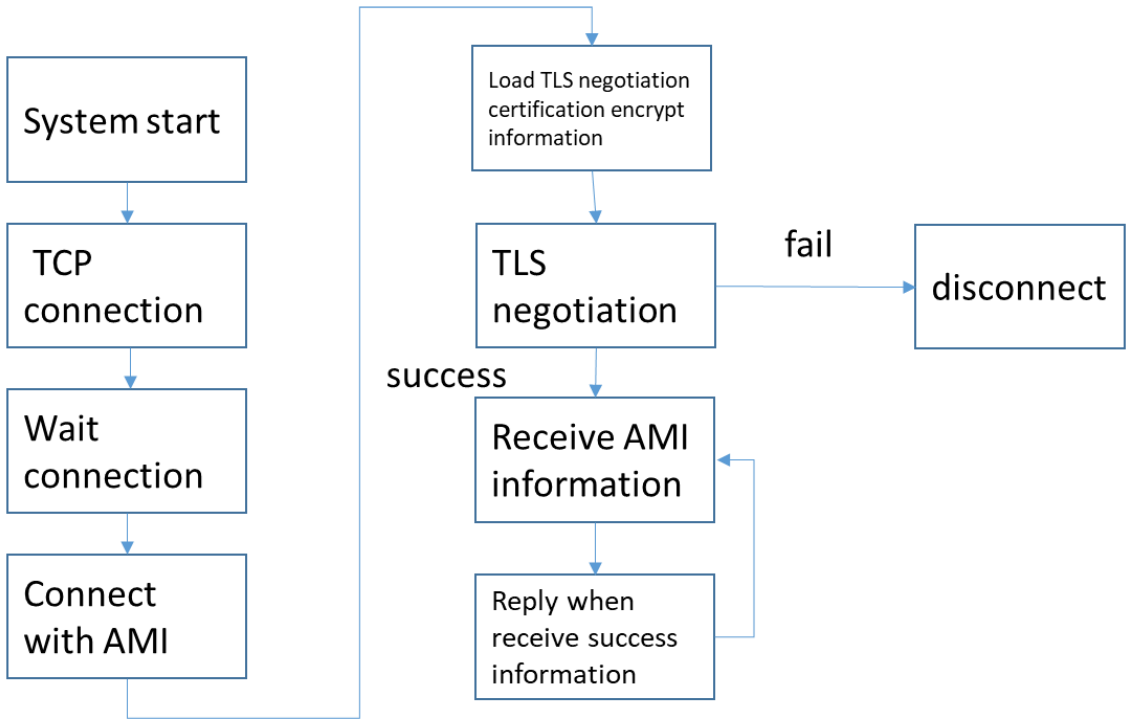

Fig6.4 Data concentrator process

6.2.3 Advanced Metering Infrastructure Simulate

We use embedded system Raspberry Pi [40] as our advanced metering infrastructure hardware, it has central processor Quad-core ARM Cortex-A7, 1GB memory, and 100Mbps Ethernet network port. When system starts, it connects with data concentrator by TLS communication protocol, after connection successful transmits meter information to data concentrator at definite time. We want to reduce information complexity, we use time mark to generate a measurement value, it follows IEC 62056-61 standards, and it lets AMI measuring value and related information maps to 6 different object identification number, then it transmits to data concentrator by TLS encrypted channel.

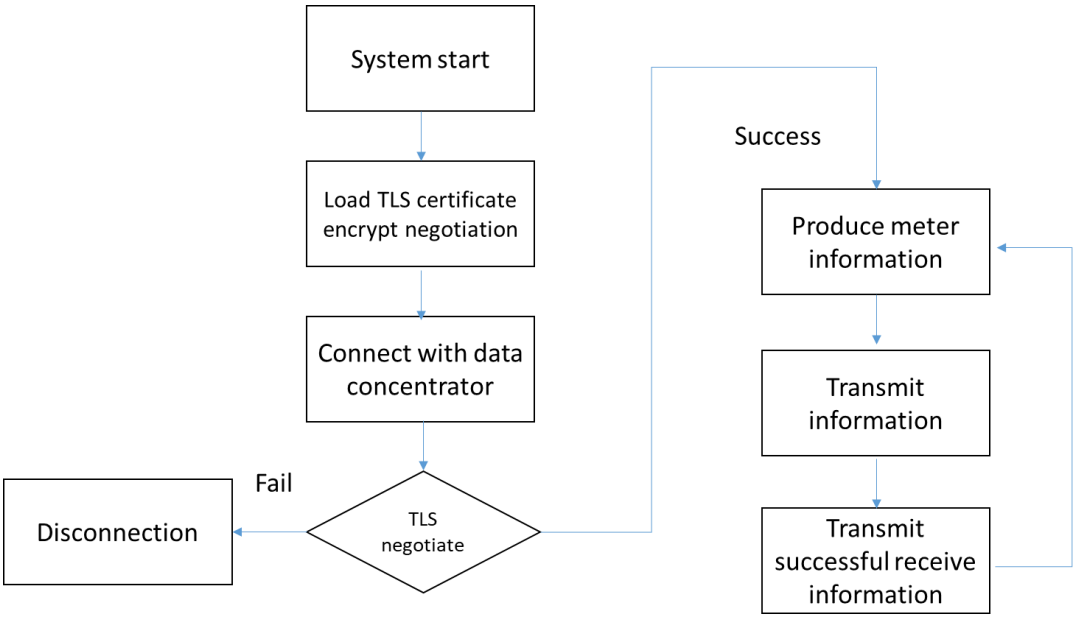

Fig 6.5 AMI operation process

6.2.4 OBIS identification number

DLMS and COSEM protocol use the object identification system [41] to make every value in meter, e.g. measurement value, data has united and unique identification number. In IEC62056-61 shows this standard details, companies can build identification number for their own meter information. OBIS is formed by 6 numbers as Fig 6.5. [46]

A	B	C	D	E	F

Fig 6.6 OBIS number

The code consists of 6 groups sub-identifiers marked by letters A to F. All these do not need to be presented in the identifier. Groups A and B are often omitted. They cover metering data as well as configuration of metering equipment and status for all applications. E.g. we can usually observe that if a meter has active power, its OBIS shows like 1.1.1.8.0.255. [41]

6.2.5 TLS Communicate Process (handshake)

We use TLS communication protocol to transfer information, and we ensure the information confidentiality, integrity and accuracy of the source. Before TLS connects, this system will make the asymmetric encryption pair of key, certificate and CA certificates, this pair of key have public key encryption transmitting information; receiver uses private key to decrypt, and validate identity by certificate; as a trustworthy third party, CA certificate is a certificate that verifies all identities correctly. Consequently, all devices certificate requires signature from CA certificate to prove that identity is checked by third parties.

When AMI and data concentrator connects, it starts TLS communication process to verify others correctness, we use Wireshark to prove communication process shows in Fig 6.7.

Fig 6.7 TLS connect success

During TLS communication process, it shows alarm details and it disconnects if any particular version or verify goes wrong. This process can avoid communication illegally. As shown in Figure 6.8, when the opponent certificate has expired by data concentrator confirmation, it will disconnect to prevent unauthorized accessibility.

Fig6.8 TLS connect fail

It has an encryption type due to TLS communication procedure. It includes certificate, encryption, certificate number of information, and key exchange encryption algorithm and it also meets most regulations. It makes information while transmitting, preserve confidentiality, integrity, and source accuracy, and also it meets the standard requirement.

Chapter 7 Experiment Results and Discussion

We follow NERC CIP, Netherlands AMI privacy and security strategy and America AMI security standards to implement 4 system functions for designing experiment and test, and we prove that our AMI communication architecture meets standards, it includes:

- Graphical user interface (GUI): GUI can observe AMI's network topology and connection status, then we can monitor AMI network situation any time.
- Throughput separated: Ensure third party can't observe or get AMI's packet information.
- Quality of Service: Ensure AMI has enough bandwidth during information exchange.
- Abnormal throughput detect and active block: If some abnormal behavior happen in AMI, we can block single infrastructure to protect power grid without block all infrastructures.

7.1 Graphical User Interface (GUI)

The information management system is according to NERC CIP criteria. It is an essential resource in the control center. Therefore it must fulfill all the specifications of NERC CIP. NERC CIP 005 establishes the definition of electrical protective boundary where electrical safety boundary equipment communicates with exterior equipment, the control center must define external equipment. We can observe all correlations in this paper.

7.1.1 Experiment purpose

We want our power providers knows the current AMI connection status and location of the equipment clearly and accurately, thus, it can handle the network status of all switches and it links equipment with controller management. By controller topology interface, we can observe all AMI networking under controller with data concentrator status and throughput.

7.1.2 Experiment result

As Fig 7.1 shows, we use graphical user interface by controller to observe whole network topology. When we want to build new AMI, GUI can identify AMI's location.

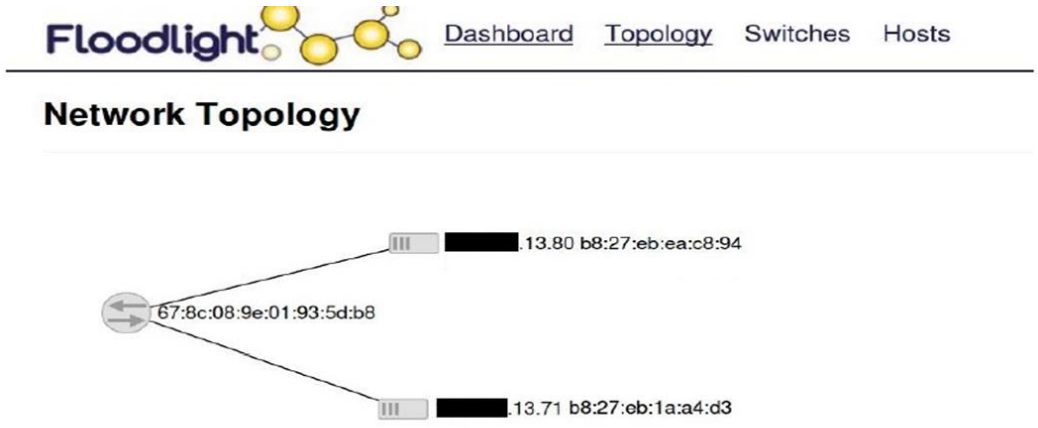

Fig 7.1 Topology status

As Fig 7.2 shows, controller can search any packet router on OpenFlow switch to get AMI throughput information.

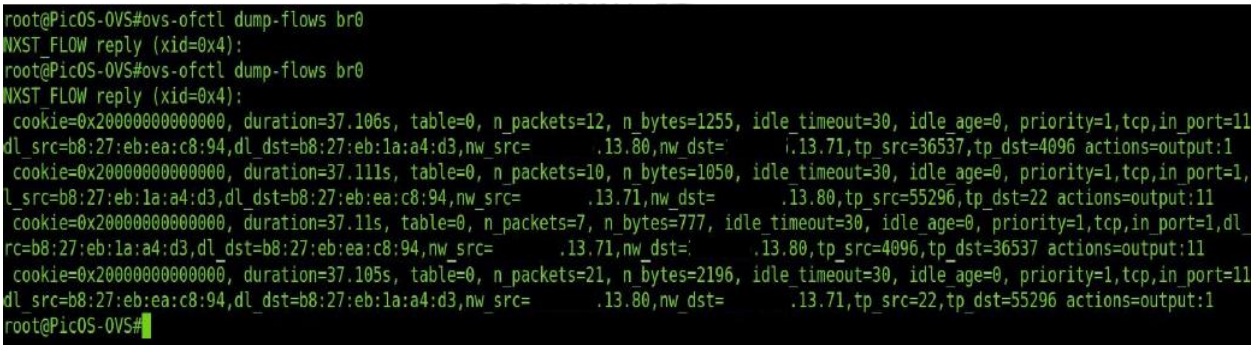

Fig7.2 Throughput status

7.2 Advanced Metering Infrastructure Throughput Separate

Due to the requirement of AMI privacy and security strategy conceived by the Netherlands power grid operator organization [28]. It includes that AMI throughput is transmitted via communication channel, quality, availability, and security of the channel should be guaranteed. One of the criteria suggests that people are unable to measure customer preferences from the size of the AMI packet and the frequency of transmission. Therefore, we want to ensure availability and security, we use FlowVisor network slice technique, and it separates AMI throughput from public network.

7.2.1 Experiment architecture and purpose

In this paper, we use Ethernet to transmit data, and the bandwidth of the meter will share with the general computer. We want to make sure that the bandwidth of the computer network not influences AMI communicating bandwidth, and we maintain AMI having essential and adequate bandwidth. We use SDN technical virtual network to do the general network slice, and we let computer network throughput and AMI throughput be divided, then we let controller control network bandwidth be sliced. As

shown in Figure 7.3, power grid operator can control AMI throughput to ensure the throughput from another network which sends to the public company is not disrupted.

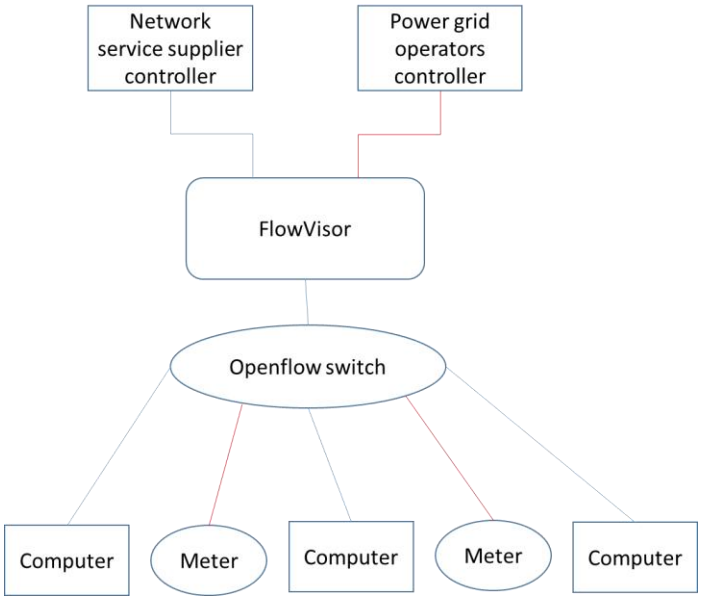

Fig 7.3 Throughput separated diagram

7.2.2 Experiment result

In Fig 7.4 shows, we use Raspberry Pi and computers to simulate meters and terminal equipment.

Fig 7.4 Raspberry Pi

Before FlowVisor sets, we can observe all equipment which plug into the switch and information, as Fig 7.5 and 7.6 shows.

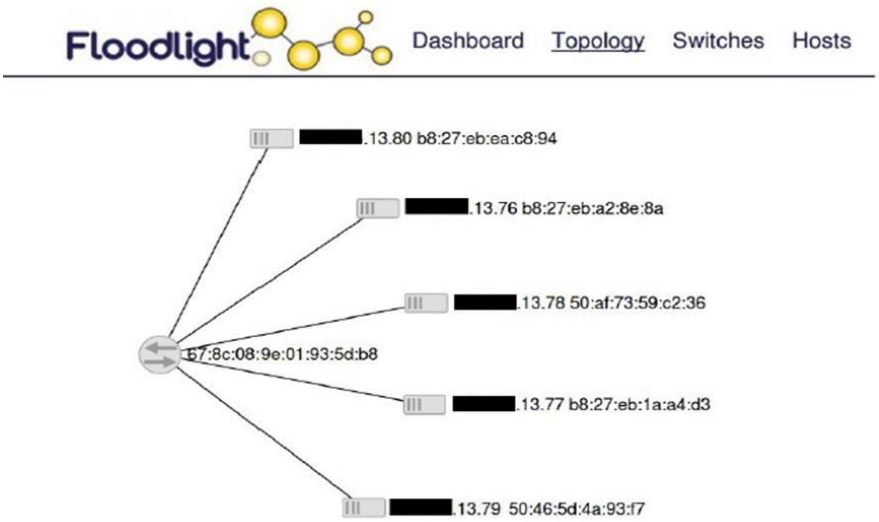

Fig 7.5 Before FlowVisor, GUI shows whole network topology has five equipment

MAC Address	IP Address	Switch Port
50:af:73:59:c2:36	[redacted].13.78	67:8c:08:9e:01:93:5d:b8-8
b8:27:eb:a2:8e:8a	[redacted].13.76	67:8c:08:9e:01:93:5d:b8-12
50:46:5d:4a:93:f7	[redacted].13.79	67:8c:08:9e:01:93:5d:b8-6
b8:27:eb:1a:a4:d3	[redacted].13.77	67:8c:08:9e:01:93:5d:b8-1
b8:27:eb:ea:c8:94	[redacted].13.80	67:8c:08:9e:01:93:5d:b8-11

Fig 7.6 After FlowVisor, GUI shows complete network equipment and information

When we construct FlowVisor, and we set the rule for FlowVisor as Fig 7.7, the first and second commands mean that we're adding a slice and commands active, and we let special IP address controller to manage the network. Third and fourth commands,

we can observe the IP address of the packet source, and the IP address of the destination, the address of the Media access control and the destination executing the slice of the network to achieve throughput separated.

```
fvctl -p 7777 add-slice slice1 tcp:[redacted].69.80:6633
fvctl -p 7777 add-slice slice2 tcp:[redacted].69.79:6653

fvctl -p 7777 add-flowspace flowspace1-1 all 65534 dl_src=b8:27:eb:ea:c8:94,nw_dst=[redacted]13.71 slice1=7
fvctl -p 7777 add-flowspace flowspace1-2 all 65534 dl_dst=b8:27:eb:ea:c8:94,nw_src=[redacted]13.71 slice1=7
```

Fig 7.7 FlowVisor information

We use FlowVisor as a tool, we separate switch port throughput, and every equipment plug into port 1 and port 11 are using as AMI, and others use as terminal equipment, and we can observe it from different controller.

Fig 7.8 and 7.9 show this experiment uses power grid operator controller visual, it can only observe AMI's network topology and information, and it can't observe other equipment on switch.

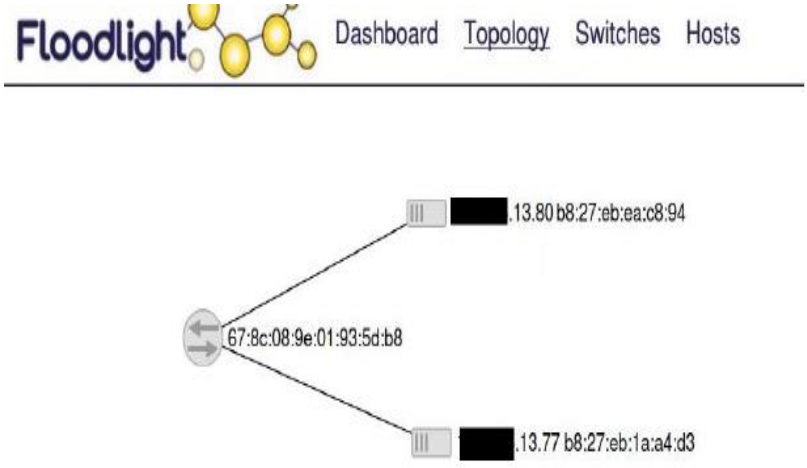

Fig 7.8 Power grid operator controller's GUI shows AMI topology

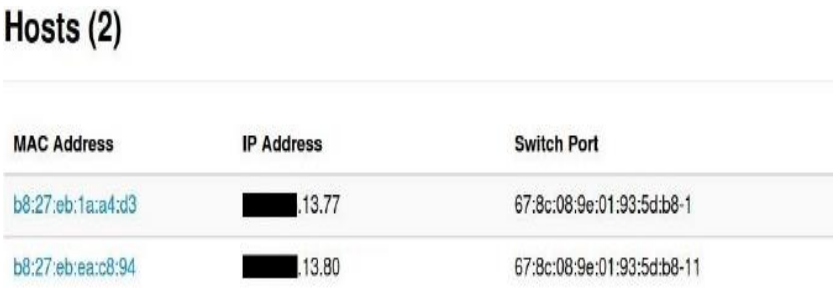

Fig 7.9 Power grid operator controller's GUI shows AMI information

The view of network service supplier, it can only observe other terminal equipment network topology and information, as Fig 7.10 and 7.11.

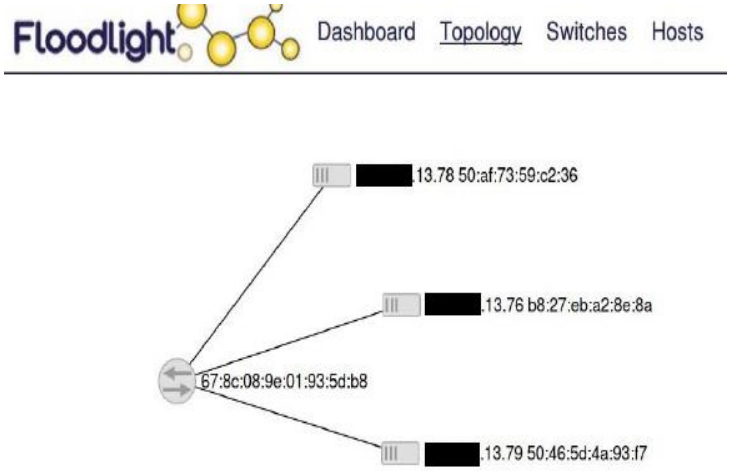

Fig 7.10 Network service supplier controller's GUI shows network topology

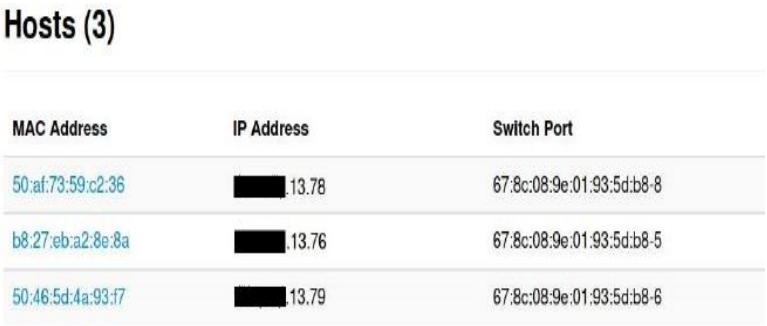

Fig 7.11 Network service supplier controller's GUI shows network information

We want to do network slice, FlowVisor can follow packet IP address, MAC, or port. Because of this experiment is using Raspberry Pi to simulate the transmission of data, and it compares with actual AMI, Raspberry Pi produces a lot of unnecessary packet. It may trigger some discrepancies between real AMI. The aim of this experiment is to let people know that FlowVisor can implement this feature, and it can achieve separating AMI and other terminal equipment throughput, it only needs to do network slice on switch port.

7.3 Quality of Service (QoS)

In this experiment, we ensure channel quality and availability, and let it not affected by household network. It may causes that AMI can't exchange information with data concentrator.

7.3.1 Experiment architecture and purpose

When terminal equipment are separated, we want to ensure quality and availability of AMI channels, and we want to prevent that other computer network throughput not influence AMI and results in packet loss, delay occurs, we use controller to command switch and start Quality of Service (QoS) mechanism. In order to ensure that the information bandwidth can achieve an effective working situation, QoS should take priority position on specific information.

Fig 7.12 shows experiment environment, and table 7.1 is the network details. We use Iperf [42] as network bandwidth testing tool, and we use Iperf to simulate general network and AMI.

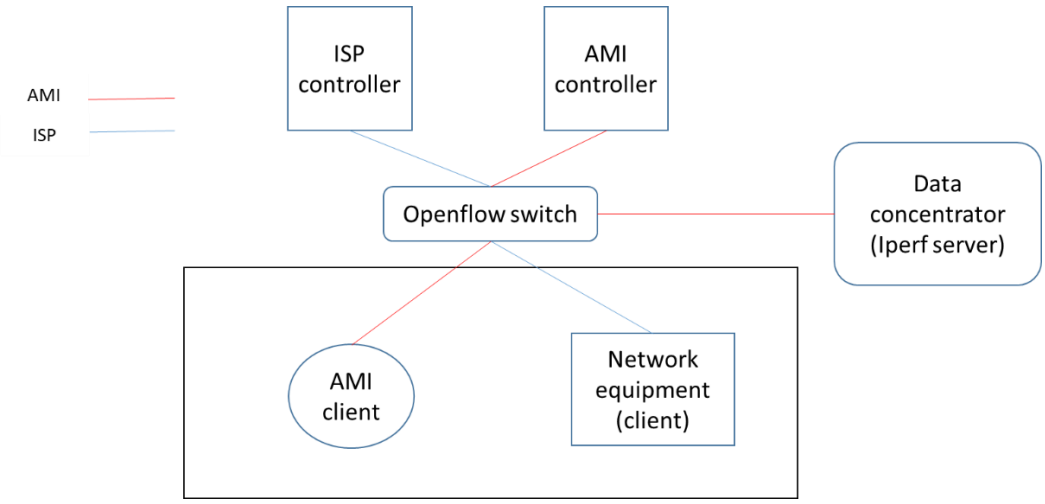

Fig 7.12 Implementation of QoS environment

Table 7.1 Implementation of QoS network configuration

Name	IP	Network card rate
ISP controller	192.*.*.79	1Gbps
AMI controller	192.*.*.80	1Gbps
Data concentrator (server)	140.*.*.* (public IP)	100 Mbps
AMI (client)	10.0.0.10	100 Mbps
Household network(client)	10.0.0.50	100 Mbps

7.3.2 Experiment result

We build a priority Queue to deploy in this trial. Queue is a first in first out buffer zone, it measures the throughput rate through this buffer zone, and it changes the throughput rate due to Queue state, and it reaches a restricted bandwidth. We set two Queues, Q0 and Q1. Q0 in our experiment is the AMI information throughput and high priority with network bandwidth of 0~20Mbps; Q1 is a common information rate, and

low priority with a bandwidth of 0~100network. When system launches, the low priority Queue can very change bandwidth flexibly, and it lets that high priority Queue has adequate bandwidth to use, and it can achieve QoS mechanism.

Because of server and transmitter only have 100Mbps network card, after test, we find out that overload bandwidth can achieve 94.4Mbps transmission rate; therefore, we set Iperf server 100Mbps rate to simulate as household bandwidth. The transmitter uses as household network equipment and AMI uses Iperf to keep sending TCP packet to the server during testing, then we observe that we achieve QoS or not. With this QoS strategy, it can occupy 20% of household bandwidth and it has high priority, and other household equipment which occupies 100% bandwidth has low priority. When AMI stops working, household equipment can use whole bandwidth; QoS starts working when AMI starts to transmit meter information, and we ensure AMI can have 20% of whole household bandwidth, and it is not affected by another throughput. Fig 7.13 shows the result. Blue line is general network; Red line is AMI network.

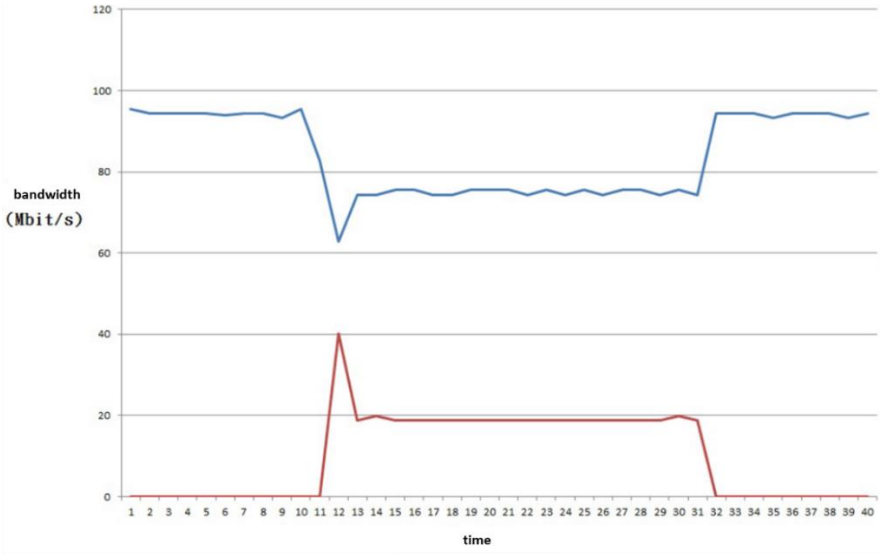

Fig 7.13 Before/After AMI transmit information bandwidth

At first, household network equipment starts sending information to extranet server by Iperf, as figure shows. Household network occupies almost 100 Mbps bandwidth, and AMI starts transmitting information after 10 seconds by Iperf, QoS starts working, and it adjusts household network bandwidth occupation percentage, and it is distributed to AMI which has high priority, and it lets that AMI throughput can transmit normally. After AMI transmission stops after 30 seconds, it returns 20% to household network.

7.4 Abnormal Throughput Block

In this experiment, we need to follow Netherlands and America AMI security rules, when we verify that source identity is abnormal, and it fails three times, we need to disconnect communication equipment, and it reports to upper system. The main purpose is to avoid that any people without authorization access the information.

7.4.1 Experiment architecture and purpose

If attacker wants to attack power grid, our data concentrator service can be challenged, and it may works abnormally. Therefore, if it fails 3 times, we count the outcome of the communication process, the data concentrator must report to the controller and it sends the IP address and MAC address of the alleged malicious attacker. Controller can block this address, and it tells switch to block the throughput from this address, and it achieves detection and controller handles it in time.

7.4.2 Experiment result

In Fig 7.14, IP address *.*.13.80 has three times connection failed, data concentrator records the IP address and MAC of this abnormal status, and controller keeps checking that if data concentrator has any abnormal connection, if it happens, controller receives abnormal connecting IP and MAC address which records from data concentrator, then it commands switch to block this abnormal throughput.

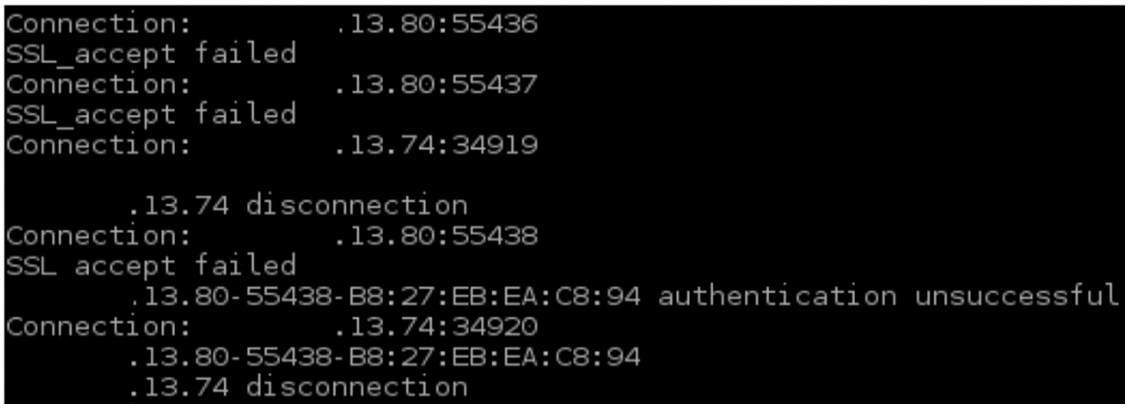

Fig 7.14 Abnormal connect information record

After controller receives abnormal connecting IP and MAC address, it will check switch which connecting with this AMI, and it sends block-commands to switch, and it drops all throughput from this abnormal source. Fig 7.15 shows the detail.

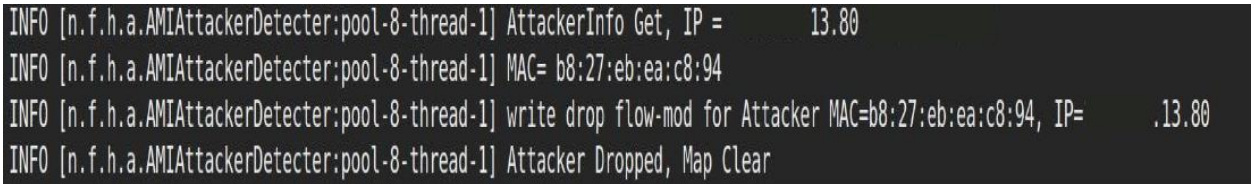

Fig 7.15 Controller's move after receive abnormal information

Controller Floodlight provides us to observe packet router, the packet from MAC address b8:27:eb:ea:c8:94 is dropped, and Apply Action shows space which means drop. This AMI is not able to connect with other equipment. Shown in Fig7.16.

Cookie	Table	Priority	Match	Apply Actions	Write Actions	Clear Actions	Goto Group	Goto Meter	Write Metadata	Experimenter	Packets	Bytes	Age (s)	Timeout (s)
9007199254740992	0x0	1	in_port=7 eth_src=b8:27:eb:ea:c8:94	---	---	---	---	---	---	---	10	1040	49	30

Fig 7.16 AMI be block

We can observe from AMI (Raspberry Pi platform), when it fails three times, controller blocks it in time, it is not able to connect with it again. Shown in Fig 7.17.

```
pi@raspberrypi ~/client-c $ ./ssl-client          .13.71 4096
TLS Client: Connect Failed!
pi@raspberrypi ~/client-c $ ./ssl-client          .13.71 4096
TLS Client: Connect Failed!
pi@raspberrypi ~/client-c $ ./ssl-client          .13.71 4096
TLS Client: Connect Failed!
pi@raspberrypi ~/client-c $ ./ssl-client          .13.71 4096
140.135.13.71: No route to host
```

Fig 7.17 AMI disconnect information

7.4.3 DoS attack experiment

If malicious attacker uses DoS to attack system, it might cause system overload beyond its capabilities. Most DoS attacks are based on the exploitation of vulnerabilities in the used communication protocol, such as TCP/IP protocol or the underlying data link layer technologies, and their related protocols. There are three common DoS attacks: TCP SYN Flood Attack, Land Attack, Ping Flood Attack... [43]

TCP SYN flood attack takes advantage of the flaws in the TCP handshake in three ways. The basic approach is: the attacker host sends a SYN message to the target host, and it initiates a TCP link, but the attacker host does not respond to the last ack message, making it difficult to complete the TCP handshake, and the target host needs to

devote resources to maintain this unfinished link until such a connection is reached a certain amount. The destination host can no longer address certain requests for connections. Construction of a SYNflood message is fairly simple, as long as the SYN bit is set to 1, and then it connects to a port of the target host available service.

The Land Attack uses two main methods: IP spoofing, and SYNflood. The Land Attack theory is filling in the target host IP as the source and destination addresses in the IP header, and then it encapsulates a SYN TCP packet to send out. The receiving host must, therefore, responds to the source address and maintain an unfinished connection, and the source address is alone, so this loop will inevitably cause the host to 0 run out of resources, and it is not able to answer requests.

The Smurf attack is a method of attacking which combines IP spoofing with flooding attack. First, the message content is configured as a particular request to be replied to (such as an ICMP request), and the message source address is transformed into the target host to be targeted. The host receives the message must initiate a message response (such as ICMP response), and it gives a response message to the fake source address.

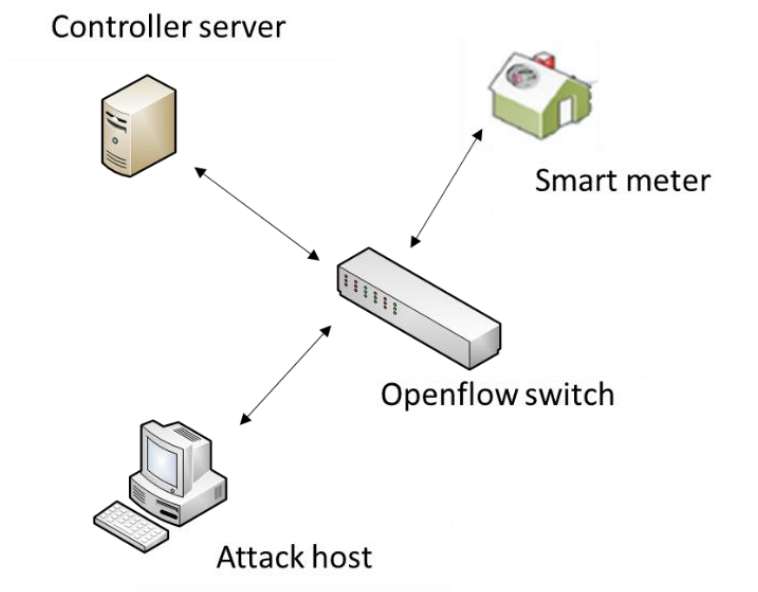

Fig 7.18 Attack simulation diagram

We simulate SYNflood attack for experiment, the SYNflood tool command line uses to generate a SYN flood attack at the computer which we use as attacker. The fake TCP SYN packet sends to the target, and this attack can be triggered individually or simultaneously by the same attack host.

Fig 7.19 shows that if we set an attack host to attack the system, huge amount of the packets be forwarded to the server at time 300, and starts DoS attack. When the attack continues, the server breaks down at time 500 and starts losing all incoming packets. After controller detect attack from overload packet status from switch, it will disconnect the attack host computer by IP, MAC address, and smart meter can keep sending normal packet to the controller.

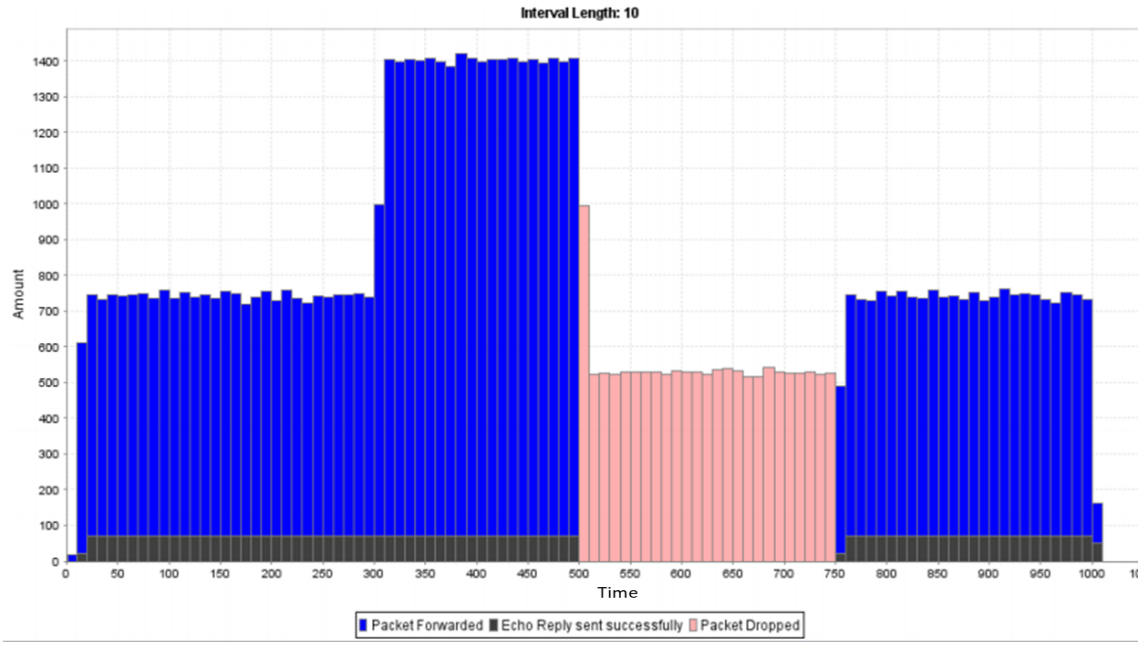

Fig 7.19 Packet flow during DoS attack

The percentage of packets lost rising drastically, almost 24% or more of the packets lost was capture by Wireshark. When the rate of DoS attack rises considerably, smart meters may breakdown and disconnect from the network.

Chapter 8 Conclusion and Future Work

Currently, AMI security issue is the most important in whole world. If smart grid is getting popular, no matter power companies, equipment suppliers, or consumers, they all need more good standards and security methods to ensure their rights not under a dangerous environment. No one wants their smart meter information or personal privacy to be accessed by others. Also, they want to collect AMI information more efficiently, and lower the cost to achieve flexible expandability which is also a serious development target.

In this paper we implement that SDN integrates AMI communication architecture, with SDN concept to solve security and expandability problems in current communication architecture, and we follow international standards at the same time.

The methods we propose has many advantages:

- Using Ethernet to exchange information, improve the expandability.
- Integrate SDN, centralize mange AMI network status.
- Using virtual network technology to separated general network throughput with AMI throughput to ensure security and availability.
- Using TLS communication protocol to ensure confidentiality, integrity and source correctness when information transmit.

Although we have the above advantages to solve current AMI system problems, it still has a big range to enhance the system. E.g. If attacker destroys AMI from its entity, and because of SDN very rely on controller, if controller is attacked, it will stop the whole network system. Therefore, it is very valuable to do research on it. In this thesis,

we only simulate a small range of AMI systems. In the real world, power grid network is much bigger than our experiment, how to implement this concept to the real situation is the most important for us to figure out. I hope this thesis can give a big view to the people who want to do the research on it in the future.

References

[1]. Vijay Kumar, Muzzammil Hussain. Secure communication for advance metering infrastructure in smart grid. Annual IEEE India Conference 2014

[2]. OpenFlow Overview: MediaWiki Available: yuba.stanford.edu/cs244wiki/index.php/overview

[3]. Rajesh Kalluri, Langineni Mahendra, R.K. Senthik Kumar, G.L. Ganga Prasad. Simulation and Impact Analysis of Denial-of-Service Attacks on Power SCADA. *National Power System Conference 2016*

[4]. Kenneth C. Budka, Jayant G. Deshpande, Tewfik L. Doumi, Mark Madden, Tim Mew. Communication Network Architecture and Design Principles for Smart Grids. September 2010

[5]. Utility AMI. High-Level Requirement August 2006

[6]. Lin ChenLe, Chimin Chou, Bin Sun. DLMS/COSEM standards meter communication protocol basis research and implementation. May 2006

[7]. I.E Commission. IEC 62056 Electricity metering- Part47 COSEM transport layers for IPv4. 2006.

[8]. I.E Commission. IEC 62056 Electricity metering- Part46 Data link layer using HDLC protocol. 2006.

[9]. I.E Commission. IEC 62056 Electricity metering- Part42 Physical layer services and procedures for connection-oriented asynchronous data exchange. 2002.

[10]. I.E Commission. IEC 62056 Electricity metering- Part 21 Direct local data exchange. 2002.

[11]. IPv6. What is IPv6? https://www.internetsociety.org/deploy360/ipv6/

[12]. Young-Jin Kim, Keqiang He, M. Thottan, and J.G Deshpande. Virtualized and self-configurable utility communications enabled by SDN. IEEE international Conference on Smart Grid Communications, November 2014

[13]. Feng Ye, Yi Qian. Secure Communication Networks in the Advanced Metering Infrastructure of Smart Grid. September 2015

[14]. Mubashir Husain Rehmani, Alan Davy, Brendan Jennings, Chadi Assi. Software Define Networks based Smart Grid Communication: A Comprehensive Survey. March 2019

[15]. Wide area network and neighborhood area network available http://opencourse.ncyu.edu.tw/ncyu/file.php/15/week08/%E5%BB%A3%E5%9F%9F%E7%B6%B2%E8%B7%AF.pdf

[16]. Goure R. Barai, Sridhar Krishnan, Bala Venkatesh. Smart metering and functionalities of smart meters in smart grid-A Riview

[17]. Ping Hai Hsu, Wenshiang Tang, Chiakai Tsai, Bo Chao Cheng. Two-Layer Security Scheme for AMI System in Taiwan. Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops, May 2011.

[18]. Xinshu Dong, Hui Lin, Rui Tan, Ravishankar K. Iyer, Zbigniew Kalbarczyk. Software-Defined Networking for Smart Grid Resilience: Opportunities and

Challenges. In Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, 2015.
[19]. Jianchao Zhang, Boon-Chong Seet, Tel-Tjing Lie, Chuan Heng Foh. Opportunities for Software-Defined Network in Smart Grid. Communications and Signal Processing. December 2013
[20]. Po-Wen Chi, Chien-Ting Kuo, He-Ming Ruan, Shih-Jen Chen, Chin-Laung Lei. AN AMI Threat Dection Mechanism Based on SDN Networks. SECURWARE 2014
[21]. GlobalSign: SSL vs TLS-what's the difference?
[22]. I.E Commission. IEC 62351 Power systems management and associated information exchange- Data and communications security
[23]. The Smart Grid Interoperability Panel-Smart Grid Cybersecurity Committee. Guidelines for smart grid cybersecurity. Technical Report NIST IR 7628, National Institute of Standards and Technilogy, September 2014
[24]. R. Barnes, M. Thomson, A. Pironti, A. Langley. Deprecating Secure Sockets Layer Version 3.0. Technical Report RFC Editor, June 2015.
[25]. Security Profile for Advanced Metering Infrastructure. December 2009
[26]. ASAP-SG. AMI Security Profile. October 2012
[27]. Department of Energy and Climate Change. Smart Metering Equipment Technical Specifications. November 2014.
[28]. NERC. Available at: www.nerc.com/Pages/default.aspx.
[29]. Public Utility Commission of Texas. Electric Grid Cybersecurity in Texas. November 2012
[30]. SDN-Wikipedia
[31]. Michael Cooney. What is SDN and where SDN is going. April 2019
[32]. Nils Dorsch, Fabian Kurtz, Hanno Georg, Christian Hagerling, Christian Wietfeld. SDN for Smart Grid Communications: Applications, challenges and advantages. November 2014
[33]. What is FlowVisor?-Definition from WhatIs.com. Available at:www.searchsdn.techtarget.com/definition/FlowVisor
[34]. Cisco. A Standardized and Flexible IPv6 Architecture for Field Area Networks.
[35]. Floodlight OpenFlow Controller
[36]. OpenSSL: The Open Source toolkit for SSL/TLS.
[37]. Vignesh D, S. Sathish. Raspberry Pi Based Control and Monitoring of Smart Grid Under An Embedded System Using WSN and Internet-of-Things. International Journal of Science, Engineering and Technology Research, May 2016
[38]. Davinder Pal Sharma, Avatar Baldeo, Cassiel Phillip. Raspberry Pi based Smart Home for Deployment in the Smart Grid. International Journal of Computer Applications, June 2015
[39]. B. Gopinath, T.Ramya, V. Sevvanthi, T. Sathiya priya. The Congnitive Power Meter using Raspberry pi. International Journal of Scientific & Engineering Research, January 2019.
[40]. Raspberry Pi. https://www.raspberrypi.org/products/
[41]. Dlms. DLMS User Association-COSEM Interface Classes and OBIS object Identification System.

[42]. Iperf- The TCP, UDP and SCTP network bandwidth measurement tool.
[43]. Savia Lobo. The 10 most common types of DoS attacks you need to know. June 2018
[44]. IEC 62056. Wikipedia.
[45]. Wen-chin Lin. IEC 62056-47 protocol in Automatic Meter Reading System research. October 2016
[46]. Description of OBIS code for IEC 62560 standard protocol. https://www.promotic.eu/en/pmdoc/Subsystems/Comm/PmDrivers/IEC62056_OBIS.htm
[47]. Transport layer security. Wikipedia
[48]. Abdullah Aydeger. Software Defined Networking for Smart Grid Communications.