Smart Grid Secure Data Transmission for High Voltage Grid

Mukti Winanda, Ardianto Satriawan, Yudi Satria Gondokaryono
School of Electrical Engineering and Informatics
Institut Teknologi Bandung (ITB)
Bandung, Indonesia
mukti.winanda@students.itb.ac.id, satriawan@students.itb.ac.id, ygondokaryono@stei.itb.ac.id

***Abstract*— Smart grid is a new breakthrough in terms of transmission and distribution power lines from power plants. All communication data transmission that occurs on the smart grid is done digitally, making it easier for operators to control and monitor every transmission data as well as monitor any equipment connected to the smart grid. However, the use of digital technologies makes the security becomes an important aspect of any communication that occurs in a smart grid system. The security will focus on the delivery and transmission of data transmitted from the power plant to any existing substations, as well as data communication that occurs between substations and also inside the substation. Data communications between substations is a very critical thing, so need for security mechanisms are applied to that communication. The addition of security against any communication will affect the performance of the data transmission in smart grid. The implementation of IPSec is used as security protocols are applied to each gateway that resides on each substations. This is done so that any communication between substations can be done safely. It is also necessary that the exact configuration of the encryption and authentication algorithms used in the implementation of IPSec protocol could potentially provide the best performance. Implementation substation network design on smart grid and security of data transmission is done by simulation using OPNET modeler 14.5.**

Keywords*— *Smart grid; Substation communications; IPSec; Network performance; OPNET modeler;

I. Introduction

A Smart grid is an electricity distribution network that can monitor electricity flowing within itself and, based on this self awareness, adjust to changing conditions [1]. The benefit of the smart grid system is to change conventional grid into digital grid system so that every electricity distribution and communication can be automatically controlled and monitored.

Communication system have a central role in smart grid system. One of the important component in smart grid system is communication between substations. The role of substations is connecting electricity distribution between electricity producer and consumer [2]. At the substation, there are several important components such as switches gears (circuit breakers and isolators). At the substation transformers are also useful for changing the voltage level required. Then there is also the instrument transformers used to measure the actual current and voltage values contained in the lines, so it is useful to monitor the status of the transformer or generator system (power system).

In addition, as a means of communication used between the connected SCADA (Supervisory Control and Data Acquisition) substation and load control center. Communication protocol between the substation is a critical point in the operation contained in plant systems as responsible for receiving information from the field and sends control equipment to the equipment. SCADA systems can be useful to reduce the need for people or employees who must always stand by in front of each device within the substation. With the introduction of microprocessor-based device that came to be known as IEDs (Intelligent Electronic Devices), the need for communication protocols that can be associated with these devices to then be integrated with SCADA. IEC 61850 is used as a standard SCADA communications protocols used in substations [3].

The using of digital technologies makes the security becomes an important aspect of any communication that occurs in a smart grid system. The security will focus on the delivery and transmission of data transmitted from the power plant to any existing substations, as well as data communication that occurs between substations and also inside the substation. Data communications between substations is a very critical thing, because if all datas are lost or used by the wrong person, there can be a major disadvantage in terms of using the electrical energy. Therefore, there need security mechanisms which are applied to that communication. The additioning of security against any communication will affect the performance of the data transmission in smart grid and selecting the appropriate security mechanism is important to optimize the network performance.

II. IEC 61850 Standard

Communication is an important thing in the operation and automation of power systems. At the current generation systems, there is an Intelligent Electronic Devices (IEDs), which have high computational efficiency and higher communication bandwidth. Control and automation systems in substations in plants undergoing significant change since the discovery of the IED for protection in substations.

One of the main things of the absence of the use of communication in automation and control in substations is the absence of a common communication protocol is used. Any equipment found in substations using each communication

978-1-4799-6527-4/14/$31.00 ©2014 IEEE

protocol for communication. It can make all the different equipment vendors can not communicate with each other easily. International Electrotechnical Commission (IEC) Technical Committee (TC)-57 publish standards IEC 61850, entitled "Communication Networks and Systems in Substation" in 2003 [4]. IEC 61850 provides interoperability by defining communication protocols, data formats, and the configuration language. IEC 61850 based SAS architecture, defines three levels of data transmission in smart grid [5].

Station level

Including Human Machine Interface (HMI) and gatewayuntuk communicate with the central control remotedan at bay level IED integration into a substation level. There are also implementation of control command to the device based on the analysis of data derived from the bay level IEDs.

Bay level

Devices connected to the process level via the bus station bay levelyang implements the IED through monitoring, protection, control, and record keeping functions of the incident.

Process level

Including the switchyard devices, sensors, and actuators. Measurement of current and voltage on the transformer also placed at the level systems to collect data and transmit the data to the device in baylevel tersenut for automation control.

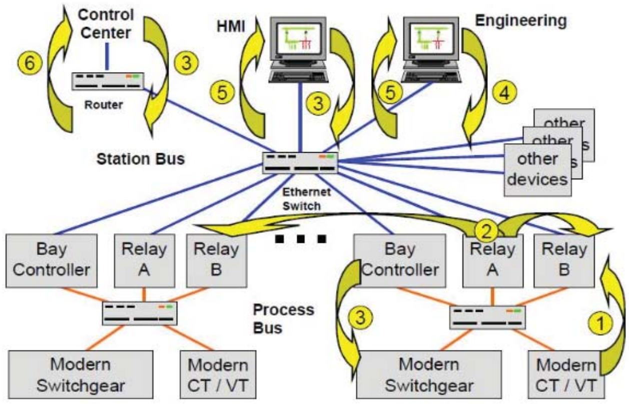


Figure 1: Automation topology according to IEC 61850[6]

IEC 61850 supports the automation of communication contained in the substation as illustrated in Figure 1. Measured values are read by the sensor devices such as Current Transformers (CT) and Voltage Transformers (VT) through the process of digitizing and sent as Sample Value (SV) (1) . Rapid exchange of data from the I / O for the protection and control (2) is used to support protection scheme at the relay. The readings will be used to control the level of the switchgear and sends trip signals are used in the trip circuit breakers (3). Computers at station level is used to configure (4), monitoring and supervision (5). Central control and access perangkatyang cooperate contained in substations through each gateway (6).

III. Secure Substations Communications

In data communications that occur in Substation Automation Systems (SAS), there are several vulnerabilities that may occur, such authorization is a violation, eavesdropping, information leakage, theft of information, change data, spoofing, replaying messages, and a denial of service (Dos) . Therefore, it is necessary that the target of the communication system to run safely. Seven security objective conducted in SAS communication systems are confidentiality, integrity, availability, authentication, authorization, auditability, and nonrepudiability [7].

Based on the layer of the Open Systems Interconnection model (OSI), there are several security protocols that can be used in the TCP / IP protocol as shown in Table 1 [6].

Table 1. Security protocol in TCP/IP

Layer	Security Protocol
Application Layer	S-HTTP
Transport Layer	SSL/TLS
Network Layer	IPSec
Data Link Layer	IEEE 802.1 AE/PPTP/L2PE

Therefore, because the communication between substations occurred on layer 3, the IPSec security is being used. In secure data packets sent, we need a protection against IP packet is assured. IPSec (Internet Protocol Security) is a method to protect IP packets that provide a powerful mechanism for securing standard package [8]. IPSec to secure network traffic with traffic define what is protected and how the traffic will be protected. IPSec uses two protocols IPSec, the Encapsulating Security Payload (ESP) and Authentication Header (AH) to protect IP traffic. AH provides data authenticity, data integrity and anti-replay protection. AH provides authentication features, while ESP provides confidentiality.

In the IPSec protocol, there are two modes in data transmission, namely the transport mode and tunnel mode. Where the transport mode to protect upper layer protocols, whereas in tunnel mode protects the entire IP datagram.

Transport mode

Typically, IPSec in transport mode is used when the required end-to-end security. IPSec header inserted between the IP header and the transport layer protocol header. Transport mode is used to achieve security IED to IED end to end communication. If the IED requires an encrypted packet, it can use the ESP protocol in transport mode. Sometimes, it takes both the ESP and AH protocols for securing packet based on the desired security requirements. When both ESP and AH in transport mode is used, the payload is protected first by AH, then protected using ESP.

Tunnel mode

IPSec Tunnel mode is used when the destination of the packets sent from the different end-point security. An example is when the data transmission between the gateway on the network substations, communication end points, and cryptographic end points are not the same. Security gateway located in substations act can act as a safety end point where the IED inside the substation is the destination of the delivery package. So when the delivery of data packets through a secure gateway, then the package will didekrip and sends the packet to the destination based on the inner IP header IED. In the picture below we can see that in tunnel mode, the entire IP datagram is encapsulated in another packet and IPsec header is inserted between the outer IP header and the inner IP header.

IV. System Design and Implementation

Design and implementation adjust the needs of the smart grid that will be applied on the Java island, Indonesia. The set up is based on the need for the topology of substation required and security will be applied to solve smart grid problems in Java.

A. Substations Network Topology Model

Before the simulation, first made in the design system located in substation. In the previous chapter, was explained that the data collection is done in the substation, data read from the sensors on the Current Transformers (CT) and Voltage Transformers (VT) were collected and combined digitally by Merging Unit (MU), and then delivered to each IED through process bus. Then each data contained in the IED will be stored in the database server can also be accessed by each control center through the bus station. In making these simulations with OPNET, the bus station is exemplified by the switch. For the network topology from the recording of each sensor to be stored on any database, not discussed in this test, it is assumed any data already stored in the database server and ready to be accessed. Here is the network topology at each substation.

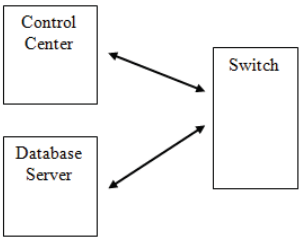


Figure 2: Local network topology in a substation

Later, in order to communicate with other substations, use the gateway as a link with outside networks as shown in Figure 3. Every network topology at the substation will be used as a subnet on OPNET which can be connected to the substation or other subnets through a gateway on each substation. Here network topology on each subnet in the substation.

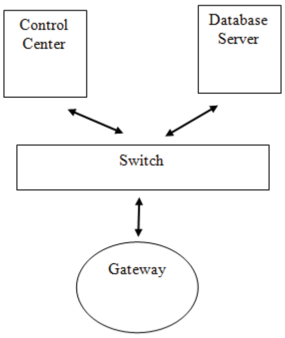


Figure 3: Topology between subnets in a substation

B. Network Topology Model Between Substations

In modeling network between substations, used scheme in Figure 4. it can be seen that the communication that occurs between the substation is done through the gateway. Then the packet exchange system between the substation and the control center using the MMS protocol where appropriate theoretical basis in the previous chapter is a mapping of the ACSI message whose function is to control the substation, such as SCADA. The MMS protocol is similar to TCP because it requires a response and request first (three-way handshake) between the client and the server before sending the data.

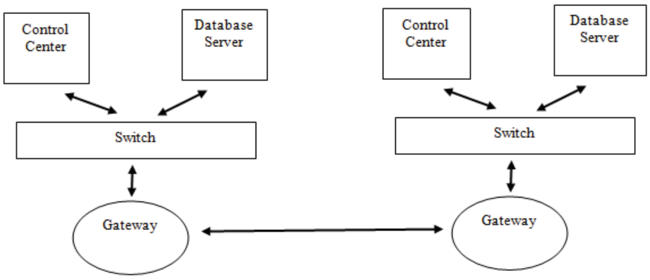


Figure 4: Topology between two or more substations

C. System Implementations

To produce a design that is appropriate, it should be to be done first simulation and design of the overall system. In designing the data delivery system between the substation network spread across the island of Java, as well as the security of data transmission using IPSec, used simulator OPNET modeler 14.5. OPNET simulation results that can produce results closer to the actual network conditions [9] where the measurement results with the simulation results in terms of throughput and delay results in differences which are always below 5%. The results of the simulation will show linkages between the substation network, throughput and delay in data transmission, security in data transmission, and network performance in data communication in substations.

D. Network Topology Implementation Substation In OPNET

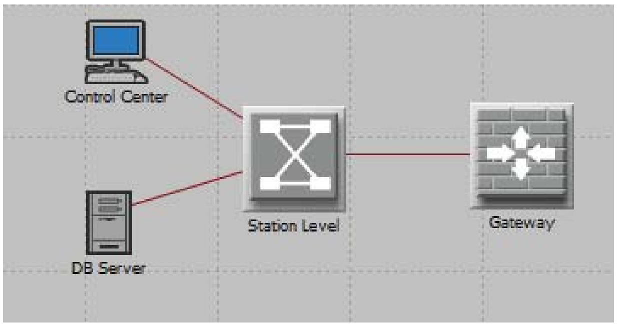


Figure 5: Map network For simulation in each substation subnet

To make a complete substation simulation mapping, first selected component corresponding to the network topology has been made in the previous chapter. In figure 5 it can be seen that each substation is represented with a single computer/PC as the control center, the database server as data storage readings each IED, one station level switches as well as a single gateway as a liaison between the substation one another. The cable used in a single subnet is 100BaseT substation with a capacity of 100 Mbps, while the gateway to the external network using a wired point to point or PPPDS1 1:54 Mbps capacity. The gateway is the entry and exit points of the data coming from inside and outside the substation. In accessing externally, as previously described, users who want to access the IED or other equipment within the substation, through a secure gateway must be the first.

E. *Implementation of Network Topology Inter substation in Java*

In making simulation using OPNET [10], first place the existence of the mapping area substations in Java, Indonesia. Each substation is represented with each subnet red. The mapping is based on the location of the substation which will implement smart grid technology in the future for the first time. It is intended to change the monitoring system originally based Time Base Monitoring to Condition Base Monitoring based on the condition of the substation. There are eight major substations scattered and each are connected to each other. The spread of these substations scattered in several areas, namely Ancol, Gambir, Petukangan, Gandul, Cibinong, Bandung, Unggaran, and Paiton. The position of substation in each region can be seen in Figure 6.

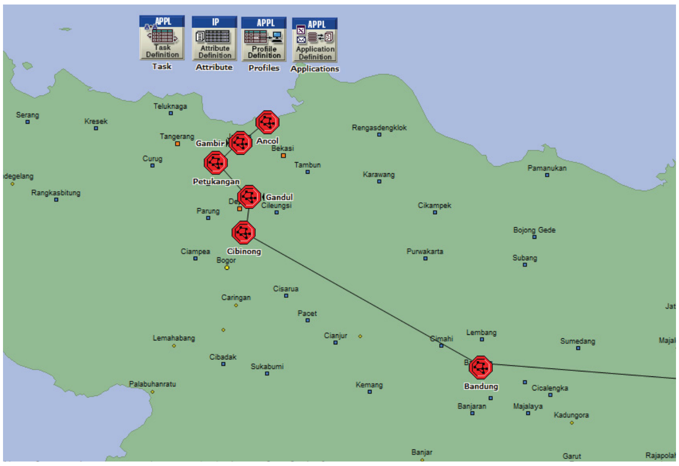


Figure 6: Regional map of substations in Jakarta & West Java

F. *IPSEC Implementation in the Communication System using OPNET*

For implementation in OPNET, can be seen above, was successfully created a secure tunnel using the tunnel IPSec. Secure indicated by red lines, and in each gateway that is located in the substation has its secure tunnel respectively. In figure 7 is shown also on substation Cibinong secure tunnel, the gateway has its own data throughput and delay.

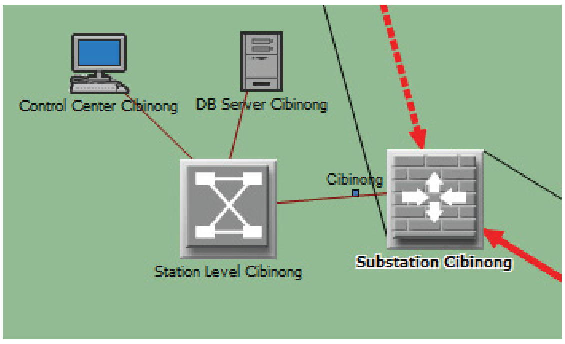
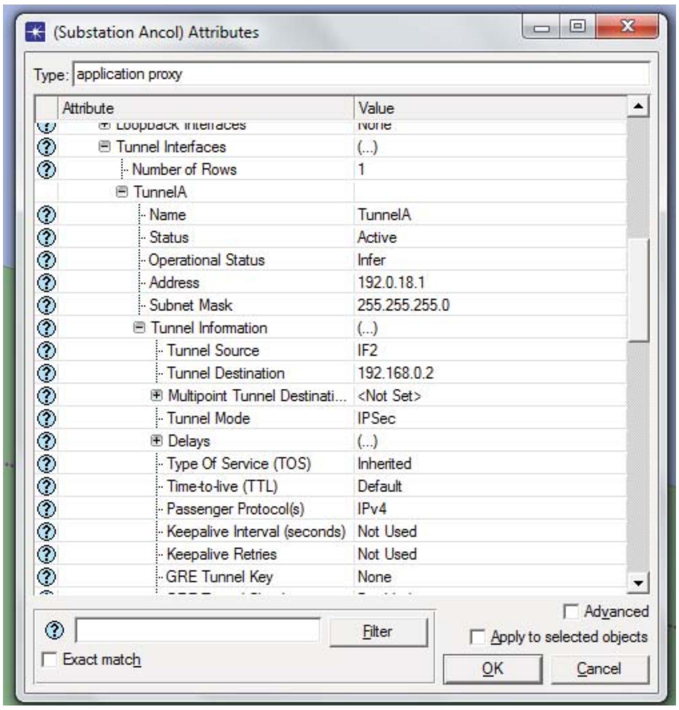


Figure 7: IPSEC Implementation in Cibinong

To perform the configuration in OPNET, takes the following steps to create a secure tunnel on every gateway. As previously explained that the gateway IP address on a different interface with an IP address assigned to the secure tunnel, because as if packets through other paths safer. In figure 8 is shown the configuration is done at the substation gateway TunnelA Ancol where given names, for secure data delivery from the Ancol substation to the Gambir substation. It can be seen that the new IP address is 192.0.18.1 given to the new interface on the secure gateway tunnel in Ancol. In the Tunnel Mode, the routes have mode IPSec [11].


(Substation Ancol) Attributes

Type: application proxy

Attribute	Value
Loopback Interfaces	None
Tunnel Interfaces	(...)
Number of Rows	1
TunnelA	
Name	TunnelA
Status	Active
Operational Status	Infer
Address	192.0.18.1
Subnet Mask	255.255.255.0
Tunnel Information	(...)
Tunnel Source	IF2
Tunnel Destination	192.168.0.2
Multipoint Tunnel Destinati...	<Not Set>
Tunnel Mode	IPSec
Delays	(...)
Type Of Service (TOS)	Inherited
Time-to-live (TTL)	Default
Passenger Protocol(s)	IPv4
Keepalive Interval (seconds)	Not Used
Keepalive Retries	Not Used
GRE Tunnel Key	None

Figure 8: IPSec configuration of Ancol substation

V. SIMULATION AND RESULTS

A. *Simulation Results to Delay and Throughput*

Simulation testing for data retrieval was tested by using OPNET modeler 14.5 because until now considered the most suitable for testing the network simulation [12]. Simulation set with an interval of one hour and tested by entering the value of different seed as producing a random number in a simulation experiment. Simulation time is exemplified on April 14, 2014 at 15:25 to 16:25 AM.

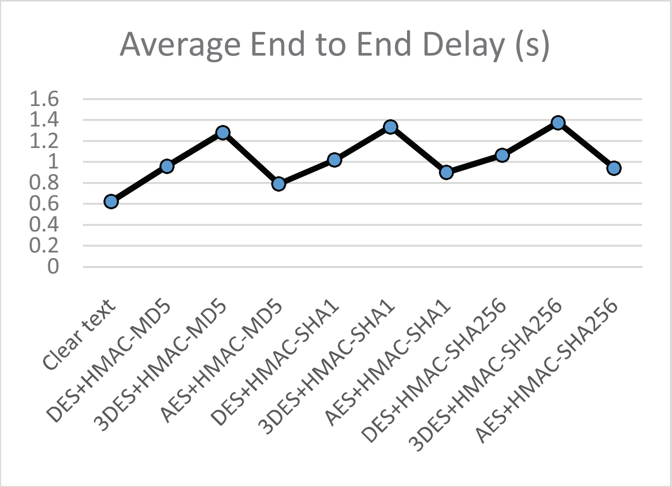


Figure 9: Average end to end delay

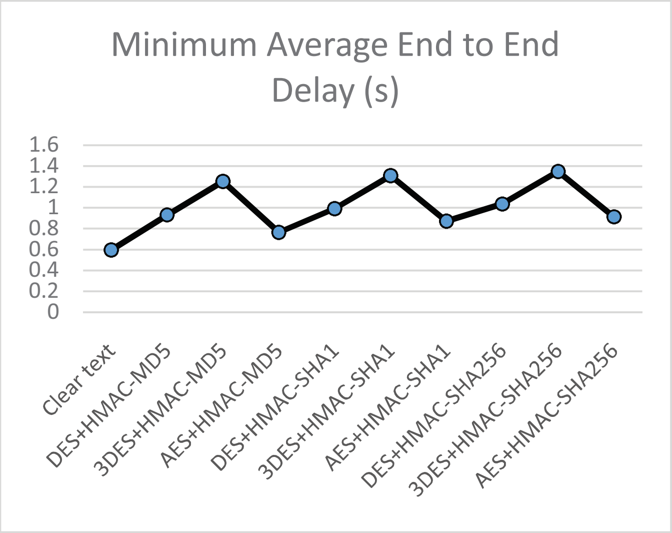


Figure 10: Minimum average end to end delay

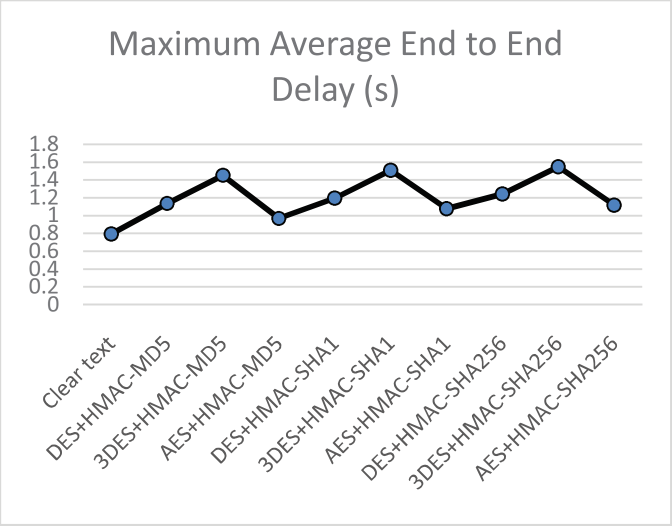


Figure 11: Maximum average end to end delay

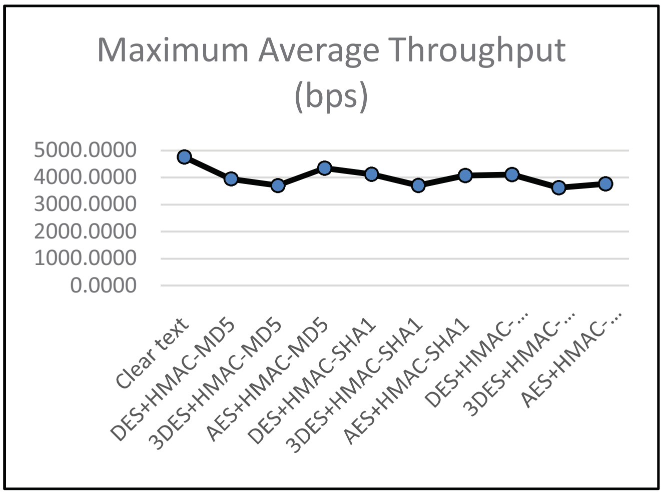


Figure 12: Maximum average throughput

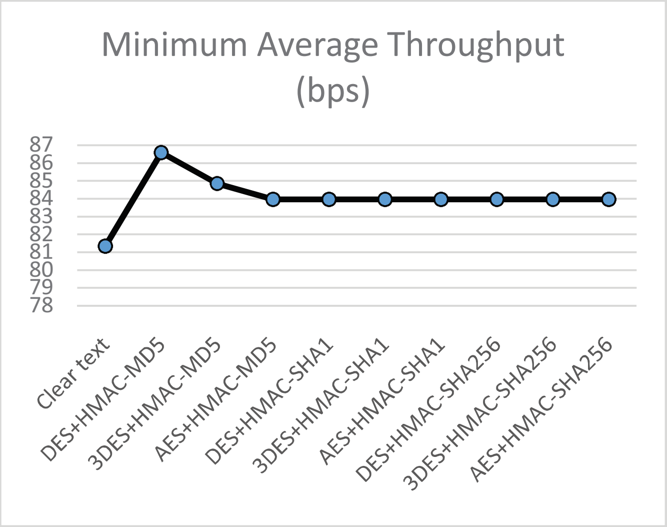


Figure 13: Minimum average throughput

ETE delay of the network is defined as the amount of time required for data packets over the network, in this case the tunnel, from the beginning of creation packets originating from the host, including encryption and decryption package, a package to arrive at the intended destination host. In this test done sending packets of TCP / IP and the time delay is measured when passing through each tunnel between gateway substations. Furthermore, it can be noted that the area between the gateway away substation to perform data communication also affect the existing delay. The farther the distance between substations, the resulting delay is also greater.

Throughput is defined as the amount of information or data packets can flow through the network during a certain time period (usually has units of bits / sec). The greater the value of the resulting throughput, the greater the information that can be transmitted within a time period. Can be seen in the results above that the average throughput values generated by each different tunnel.

As can be seen in figures above that in testing combinations tested encryption algorithms and authentication to be added as a parameter in the data transmission between gateways at the substation. In addition to the combination algorithm, trials were done varying as much as five times using the random number seed to produce different results. The results obtained in the form of minimum and maximum values of the throughput of each tunnel and also the minimum, maximum, and average of the ETE delay is measured on each tunnel. From these results it can be seen secure tunnel configuration that provides the least impact on the performance of the communication that occurs. Each configuration of a secure tunnel are compared with each other and also to the configuration when sending only a clear text only.

It can be seen that a given security delivery reduces the communication performance of the data transmission is performed [13] [14] [15]. This is demonstrated by the results of a smaller throughput and delay are greater when compared to delivery without the use of safeguards. In the measurement chart simulation results overall average can be seen that on any existing tunnel showed Triple DES encryption algorithm gives smaller throughput and also the longest delivery time when compared with DES and AES encryption algorithm [16]. For the AES algorithm, it can be seen that the value generated greater throughput and data transmission time is also smaller when compared with the DES algorithm. Then for the authentication algorithm, combined with the HMAC MD5 provide better performance than the HMAC-SHA1 and HMAC-SHA256 where indicated with greater throughput and smaller delay time.

Can be seen also in testing that IPSec provides security in the form of confidentiality, integrity, authentication and non-repudiation that is needed in any data communication, particularly between substations. IPSec works at the network layer and provides protection against all who passed through the IP protocol. IPSec in tunnel mode is more secure than the transport mode. Can be seen from the level of security provided, where more tunnel mode gives more security when data transmission is done. Therefore, we recommend tunnel mode is selected in the configuration of secure gateway for secure communication between substations.

In IPSec tunnel mode, the ESP header is quite safe to use, rather than having to use ESP and AH headers as well [16]. Where ESP protects the entire IP header of packets sent. Therefore, the data transmission between the gateway, please use the ESP header course which has been providing encryption and authentication packets at once. When a packet is sent to the tunnel is encrypted or authenticated, a security force that occurs depends on the algorithm and key length used. The algorithm is selected and used to improve security with the least performance impact. Been analyzed previously that the combination of AES and HMAC-MD5 give the best performance when compared with other combinations of algorithms. In addition, based on the previous chapter, it has been shown that AES is the algorithm is still proven safe for use in encryption standards and in accordance with the recommendations in [17], while the HMAC-MD5 authentication is still considered quite safe as authentication when sending data which is not too reduce network performance.

VI. Conclusion

From the research that has been done can be concluded as follows.

- Modeling and simulation of communication network system between the substation has been done and can produce throughput and delay on each trial.
- Obtained value of average delay on the delivery of data with no security is 0.978741 ms. Value also obtained the best average delay with added security with IPSec in data transmission which is 1.146105 ms on a combination of AES and HMAC MD5 algorithm.
- Provided the value of the average throughput in data delivery with no security is 5760.176 bps. Obtained the value of the average throughput of the best with the added security with IPSec 4994.895 bps data transmission, namely the combination of AES and HMAC MD5 algorithm.
- Can be seen from the results, that selection of the appropriate security mechanism in data transmission between substations can optimize network performance (time and throughput), so this could make the developers of smart grid system must be careful in choosing the appropriate security mechanism.

References

[1] L. Chris Beard, “Smart Grid for Dummies”, John Wiley & Sons, Ltd., England, pp. 4-7, 2010.

[2] ___________, Gardu Induk, [Online], Available: http://www.pln.co.id/p3bjawabali/?p=451. [Accessed: February 24, 2014].

[3] G. Isaac, Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks, Pier Public Interest Energy Research, Sacramento State, May 2012, pp.43-50.

[4] T. Sidhu and P. K. Gangadharan, “Control and Automation of Power System Substation using IEC61850 Communication,” 2005.

[5] A.Ikbal, S. Mini, S. G. Thomas, “Substation Communication Architecture to Realize the Future Smart Grid”, Jurnal of Energy Technologies and Policy, ISSN 2224-3232, Vol. 1, No. 4, 2011.

[6] W. Pubudu, “Security Aspects of Smart Grid Communication”, Thesis of Masters of Engineering Science, Western University, London, Ontario, Canada, 2012.

[7] D. Dzung, M. Naedele, T.P.V. Ho, and M. Crevatin, “Security for industrial communicationsystems,” Proceedings of the IEEE, vol. 93, pp. 1152 – 1177, June 2005.

[8] A. Oluwaranti, E. O. Adejumo, “Performance Evaluation of Network Security Protocols on Open Source and Microsoft Windows”, Network and Complex System, Vol 3 No.7 2013, ISSN 2224-610X.

[9] B. B. Van Den, P. Leys, J. Potemans, et al., “Validation of Router Models in OPNET”, Belgium.

[10] Laboratory Assignment Network Simulation Using OPNET, City University, School of Engineering and Mathematical Sciences, MSc in Telecommunication and Networks, London, November 2006.

[11] M. Sparsh, “OPNET: An Integrated Design Paradigm for Simulations”, Software Engineering: An International Journal (SEIJ), Vol.2 No.2, September 2012.

[12] F. Ya-qin, L. Chi, “Secure VPN Based on Combination of L2TP and IPSec”, Journal of Networks, Vol. 7, No. 1, January 2012.

[13] S. Gouda, S. M. Elemam, M. Zaki, et. al., “Performance Analysis of Transmitting Voice Over Communication Links Implementing IPSec”, 13th International Conference on Aerospace Sciences & Aviation Technology, May 2009.

[14] B. Masqueen, “Performance Analysis of IPSec VPN Over VoIP Networks Using OPNET”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012.

[15] X. Christos, M. Lazaros (1 Juli 2004), “IPSec Base End to End VPN Deloyment Over UMTS”, [Online], Available : http://www.sciencedirect.com, [Accessed: February 2, 2014].

[16] N. Ferguson and B. Schneier, “A cryptographic evaluation of IPsec,” 2000.

[17] Technical Specification IEC/TS 62351-5, Power Systems Management and Associated Information Exchange –Data and Communications Security – Part 5: Security for IEC 60870-5 and derivatives, edition 1.0, 2009-08.

[18] W. Mukti, “Keamanan Pengiriman Data Pada Smart Grid Untuk Grid Tegangan Tinggi Antar Gardu Induk”, Thesis of Masters of Engineering, Institut Teknologi Bandung, Bandung, Indonesia, 2014.