Journal of Electrical Engineering & Technology Vol. 7, No. 3, pp. 443~450, 2012 **443**
http://dx.doi.org/10.5370/JEET.2012.7.3.443

Optimized Security Algorithm for IEC 61850 based Power Utility System

Hyo-Sik Yang†, Sang-Sig Kim* and Hyuk-Soo Jang**

Abstract – As power grids are integrated into one big umbrella (i.e., Smart Grid), communication network plays a key role in reliable and stable operation of power grids. For successful operation of smart grid, interoperability and security issues must be resolved. Security means providing network system integrity, authentication, and confidentiality service. For a cyber-attack to a power grid system, which may jeopardize the national security, vulnerability of communication infrastructure has a serious impact on the power grid network. While security aspects of power grid network have been studied much, security mechanisms are rarely adopted in power gird communication network. For security issues, strict timing requirements are defined in IEC 61850 for mission critical messages (i.e., GOOSE). In this paper, we apply security algorithms (i.e., MD-5, SHA-1, and RSA) and measure their processing time and transmission delay of secured mission critical messages. The results show the algorithms satisfying the timing requirements defined in IEC 61850 and we observer the algorithm that is optimal for secure communication of mission critical messages. Numerical analysis shows that SHA-1 is preferable for secure GOOSE message sending.

Keywords: IEC 61850, Network performance, Performance analysis, Security, Smart grid

1. Introduction

As power grids are integrated into one big umbrella so called smart grid using communication technologies, efficient management of power grid network becomes possible. Communication network deployed in smart grid plays a key role in reliable and stable operation of power grid. For successful operation of smart grid, several issues have been raised with respect to interoperability and security [1-3].

IEC 61850 has been globally applied to substations worldwide and has influence on internal communication of a substation as well as external communication between a substation and a SCADA (Supervisory Control and Data Acquisition) system [4]. IEC 61850 is applied to other power utility industries such as DER (Distributed Energy Resource) and wind power farm [5-7]. IEC 61850 is one of the important candidate standards to be adopted in smart grid. IEC 61850 is originally legislated to resolve interoperability issues among devices in a substation.

The power system operating environment differs from the secured Internet environments [8]. For example, DoS (Denial-of-Service) has a more serious impact on the power system communication network than the public Internet. Attack to the power system communication infrastructure may jeopardize the national security. Therefore, the power system environment and the definition of security requirements and security measures for potential impacts should be understood. The importance of security aspects of power grid network has been discussed in recent research (see e.g., [9, 10]). A broad brush description of smart grid security related issues is discussed in [11, 12]. A grid wide IT architectural framework to meet the security challenges is presented in [13], while facilitating modern cyber security measures. Security mechanisms, however, are rarely adopted in power grid network. Key technologies for a secure smart grid system such as key infrastructures and trusted computing are discussed in [3]. They also discuss about security requirements and propose public key infrastructure. Cyber security issues, highlights the access points in a substation, and information security domain modeling are considered in [10].

With these research efforts, security issues of the communication services in IEC 61850 such as MMS (Manufacturing Message Specification), GOOSE (Generic Object Oriented Substation Event), and SMV (Sampled Measured Value) are currently raised and new standards are being legislated (i.e., IEC 62351) and security for IEC 61850 is described in Part 6 of IEC 62351 [14]. The current state of IEC 62351 and new use cases are addressed in [15]. The standards specify what kinds of security factors should be considered for each communication service. It, however, does not suggest performance measurement. The IEC 61850 standard specifies timing requirements for each communication service. Performance of each data service

† Corresponding Author: Dept. of Computer Science and Engineering, Sejong University, Korea. (hsyang@sejong.ac.kr)
* Dept. of Computer Science and Informatics, Oakland University, USA. (skim2345@oakland.edu)
** Dept. of Computer Science and Engineering, Myongji University, Korea. (hyuks.jang@gmail.com)
Received: April 4, 2011; Accepted: April 17, 2012

is important for strict performance and stability of the power system.

Processing time of applied security mechanisms does not have a critical impact on the normal Internet traffic. For the time critical messages defined in IEC 61850 (i.e., GOOSE or SMV) a small fraction of time to process the encryption algorithm may have a critical impact on successful operation of substation. Network wise performance including usage of security mechanism in the power system, communication network must guarantee the strict performance requirement to reduce a great ripple effect of a fault as well as reliability. It, however, would be a big challenge to meet both security and timing requirements, since use of security mechanism obviously adds some amount of overheads. Among other IEC 61850 traffics, GOOSE is a very flexible high-priority reliable mechanism for fast transmission of substation events such as trips commands, interlocking, and critical status indications. GOOSE messages are used to replace the hardwired control signal exchange between IEDs for interlocking, protection purpose, and sensitive missions that are time critical and require high reliability. GOOSE messages also contain information that allows the receiving device to know status change. For these reasons, secure and reliable transmission of GOOSE messages, while meeting the timing requirements, is very important for reliable operation of Substation Automation System (SAS) [16]. For the security of GOOSE messages, the cyber security working group in NIST (National Institute of Standards and Technology), U.S.A., expected to include MAC (Message Authentication Code)-SHA (Secure Hash Algorithm)-1 and AES (Advanced Encryption Standard) with RSA (Rivest, Shamir, Adleman) signature algorithm in IEC 62351 [17]. However, there was no research effort to verify that the specified security algorithms are applicable to power utility environment, which is different from public Internet environment, as well as performance wise measurement of security algorithms.

The total transmission time for GOOSE messages between the IEDs should be below the order of a quarter of a cycle (i.e., 3 msec). This timing requirement includes the time taken by a communication processor as well as the transmission time over communication medium. Processing time for security algorithms is included in the time taken by a communication processor, because the result value calculated by the security algorithms is directly related to the length of extended PDU (Protocol Data Unit). The processing time, therefore, should be included in the total transmission time for sending and receiving party of GOOSE messages. Latency to deliver a mission critical message over communication link is measured in several literatures. Transmission time of GOOSE message over Ethernet upon different environments is measured in [18], [19]. Gigabit Ethernet based substation network architecture is proposed in [20] and transmission time is measured. These works, however, do not consider the secure communication of mission critical messages.

The purpose of this paper is to apply candidate security algorithms to GOOSE services which have strict timing constraints and raise optimal security algorithms. The optimization means to seek algorithms which meet strict timing constraints and provide security services, which offer guidelines for performance measurement and at the same time, it is possible to extend this method by applying other algorithms. In this paper, two experiments are performed to seek optimized security algorithms which satisfy the strict timing constraints for GOOSE services. One is to measure the processing time of candidate security algorithms (i.e., MD (Message Digest) 5, SHA-1, and RSA) taken by a communication processor of publisher and subscriber nodes and the other is to measure the transmission time of GOOSE over the communication link over station bus. Numerical analysis shows that the SHA-1 is preferable for secure GOOSE messages while satisfying the timing constraint.

The paper is structured as follows: Following section describes the security algorithms considered in this paper. Section 3 describes ACSI (Abstract Communication Service Interface) services defined in IEC 61850 and other communication related issues. Section 4 describes the performance measurement setup and numerical results. Section 5 concludes the paper and describes the future issues.

2. Security Algorithms

Numerous up-to-date algorithms (e.g., cryptography, message digest, and hash algorithm) are applied to the telecommunication field for secure communication. In this section, we briefly discuss the security algorithms used in this paper.

Hash function generates a fixed length hash value with an arbitrary length input bit string. Hash function has to be collision resistance to provide integrity of messages by a specific character for which the same has number cannot be found [21]. A dedicated hash function is designed only for hashing by optimized processing and never uses existing system elements (e.g., block password or modular operation). MD-4 is designed for 32 bit CPU software implementation [12]. MD-4, however, does not meet the hash collision-free requirement. Collisions are found with a few operations [22, 23]. As a result, dedicated hash functions such as MD-5 and SHA-1, and RIPEMD (RACE Integrity Primitives Evaluation Message Digest) are designed on the basis of MD-4. The output length of MD-5 and SHA-1 is 128 bits and 160 bits long, respectively.

RSA is a public key algorithm based on difficulty of prime factorization. Similar to most public keys password features, RSA password is block encrypted, but different from block encryption used in a secret key algorithm such as DES (Data Encryption Standard) in the sense that a

length of a plain text and a key is variable; in other words, a relatively long length of a key can be used in consideration of the secure and reliable system, and a relatively short length of a key can be used for efficient system. In an RSA algorithm, receiver's public key is used to encrypt messages, and the receiver decrypts encrypted messages with its own private key. In an RSA-based signature algorithm, a sender signs messages with its own private key, and a receiver verifies the signed message with sender's public key; this is how an authentication service is guaranteed through an RSA-based signature algorithm.

3. Protocol Stack and Offered Service in IEC 61850 based Substation Automation System

Protocol stack used in the IEC 61850 for different ACSI services is shown in Fig. 1. Even though additional use of LLC (Link Layer Control) and ISO transport layer is described in the IEC 61850, TCP/IP and UDP over IEC 8802-3 Ethertype are shown in the figure for a simple protocol stack. Note that sampled measured values and GOOSE services do not use TCP/IP nor UDP due to strict timing constraints as shown in Table 1. The transmission delay timing requirement of GOOSE communication between IEDs (Intelligent Electrical Devices) and between substations has 3 msec which is the tightest timing requirement among services defined in IEC 61850. To achieve this timing requirement, GOOSE and SMV uses direct mapping to ISO/IEC 8802-3 Ethertype data link layer protocol without any transport and network layer protocol. To support this strict timing requirement, IEEE 802.1Q priority queuing and VLAN (Virtual Local Area Network) are used for fast transmission of GOOSE and SMV multicast messages. This, however, causes difficulties in secure GOOSE communications. It requires a security mechanism for providing security services such as confidentiality, integrity, and authentication which cause another overhead to process such secure algorithms.

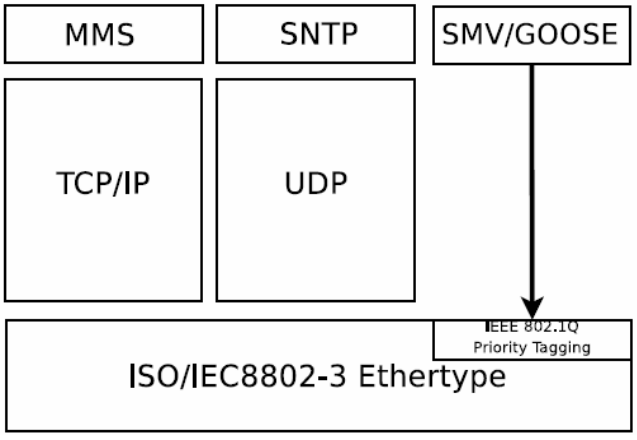

Fig. 1. Protocol stack used in IEC 61850

There are three different kinds of communication services offered in IEC 61850. First, peer to peer (P2P) based multicast services are available for sampled measured values, GOOSE, and GSSE, where GOOSE is mandatory whereas GSSE is optional. Peer to peer services shall be fully integrated into the engineering process according to IEC 61850-6. IEEE 802.1Q, which supports priority tagging, is required for P2P services in network switches. The GOOSE service is used for interlocking and communication between IEDs, which is very time and mission critical data. Sampled value messages are used to transmit digitized measured values to the appropriate IEDs, which takes large volume and bandwidth. Second, client-server based communication services are offered using MMS (Manufacturing Message Specification) on top of TCP/IP as defined in IEC 61850-8-1. Third, time synchronization service is offered using SNTP (Simple Network Time Protocol) v. 4 on top of UDP/IP protocol stack. Clock time master (e.g., GPS [Global Positioning System]) is required in SAS. Since SNTP, however, does not meet the timing requirement defined in IEC 61850, PTP (Precision Time Protocol), which is also known as IEEE 1588, is recommended in the 2nd edition of IEC 61850. Besides these services, FTP service using TCP/IP protocol stack is also required.

To apply security algorithms, an extended Ethertype PDU (Protocol Data Unit) field is defined as shown in Fig. 2 and we can apply dedicated hash algorithms such as MD-5 and SHA-1, and RSA-based signature algorithms. Using a dedicated hash algorithm, integrity is guaranteed for GOOSE messages and the inclusion of RSA-based signature algorithms guarantees the authentication and message integrity. The extended Ethertype PDU field includes extended PDU length, CRC (Cyclic Redundancy Check) code, and Extension field. The length of Extension field includes the length of Extended PDU. If the length of Extension value is set to 0, Extension field is not used. Second Byte (8th octet) of the length of Extension field is reserved for future use. 16-bit CRC field is provided for the integrity of the first 8 octets. Extension field contains the hash value calculated by applying an encryption algorithm from the address field to GOOSE/SMV APDU (Application Protocol Data Unit) field.

Table 1. Service timing requirements for different ASCI services in IEC 61850

Message type			Required Time
Fast messages	Type 1A "Trip"	Performance Class P1	10 ms
		Performance Class P2/3	3 ms
	Type 1B "Others"	Performance Class P1	100 ms
		Performance Class P2/3	20 ms
Medium speed messages			100 ms
Low speed messages			500 ms
File transfer function			1000 ms

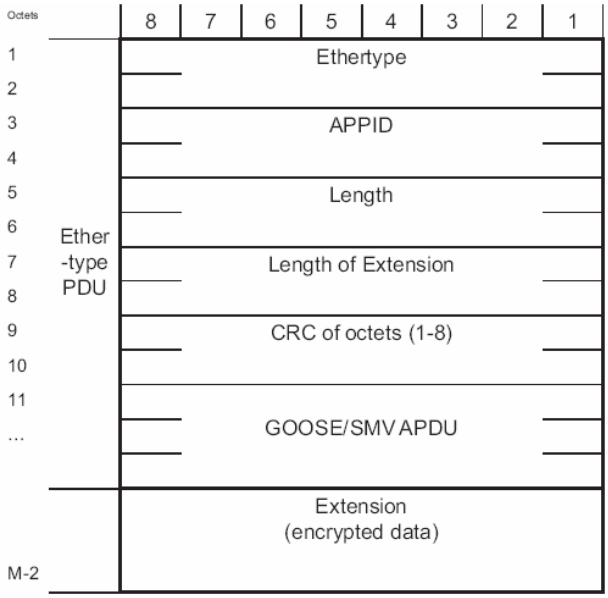

Fig. 2. Structure of extended PDU

4. Numerical Results

In this section, two experiments are performed to seek an optimized security algorithm that satisfies the strict timing constraint for the GOOSE service defined in IEC 61850. One is to measure the processing time of security algorithms taken by a communication processor of publisher and subscriber nodes and the other is to measure the transmission delay of GOOSE messages over a communication link in substation network topology by means of computer simulation.

4.1 Processing time of security algorithms

Confidentiality and integrity algorithms are considered to measure the processing time in power grid network. To support confidentiality and integrity services, four combinations of confidentiality and integrity algorithms, MD-5 only, SHA-1 only, RSA & MD-5, and RSA& SHA-1, are drawn to be candidate solutions to find an optimal security algorithm for GOOSE services, while satisfying the timing constraint described in IEC 61850. The integrity service is provided with either MD-5 or SHA-1 and RSA algorithms provide confidentiality service.

Fig. 3 shows how hash algorithms and confidentiality algorithms are applied. A publisher produces a hash value of the message with bit sequence input using MD-5 or SHA-1, signs the hash value with publisher's private key with an RSA algorithm, and attaches the signed message to the original message. When a subscriber receives the message, it produces a hash value of the original message with the same hash algorithm as the publisher used, designs the signed message with publisher's public key to get the hash value, and compares the resulting hash value with the original message's actual hash value. There is no signed and designed process when only a hash algorithm is used to the original message (without RSA).

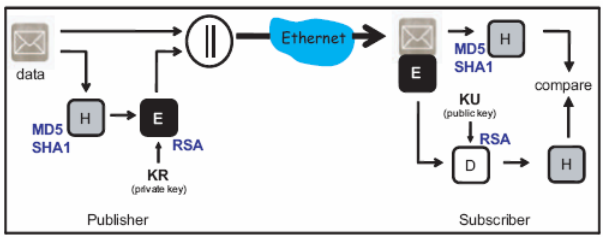

Fig. 3. Security algorithms processing procedure

A hardware specification of the system performing the integrity and authentication is summarized in Table 2. To consider the hardware limitation of practical IED, we choose an inferior machine. As for the reference, one of the commercially available IED, which support IEC 61850, uses 532 MHz CPU with 128 MB memory. The size of original message is set to 132, 620, and 1012 Bytes long.

Table 2. Hardware specification for encryption system

	Specification
CPU	Pentium III 700 MHz, 256KB cache
RAM	256MB
Development Environment	Linux kernel version 2.4.34 GCC version 3.2.2
Original Message Length	132 Bytes
	620 Bytes
	1012 Bytes

Fig. 4 shows the measured processing time with and without the MD-5 hash algorithm in the publisher side. In case of the message length of 132 Bytes, the average processing time of non MD-5 and MD-5 is 555.68 µsec and 583.16 µsec, respectively. The time difference between MD-5 and non MD-5 is 27.48 µsec, and it is of little weight in comparison with the timing constraint, which is 3 msec. In case of message length of 620 Bytes, the average processing time of non MD-5 and MD-5 are 617.42 µsec

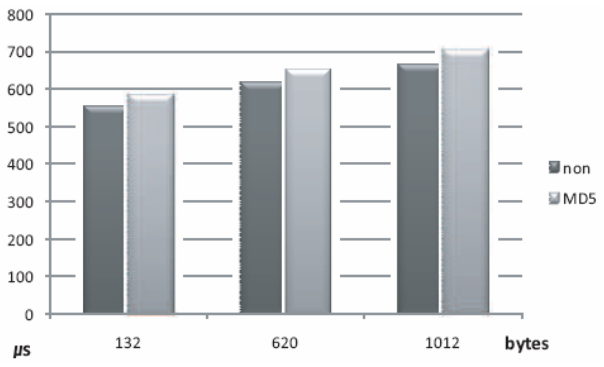

Fig. 4. GOOSE with MD5 and non-MD5 processing time in publisher's side

and 651.55 μsec, respectively. Finally, in case of message length of 1024 Bytes, the processing time of non MD-5 and MD-5 are 668.49 μsec and 704.63 μsec, respectively. The maximum time difference between non MD-5 and MD-5 is 36.14 μsec when the message length is the maximum (i.e., 1024 Bytes long).

Fig. 5 shows the measured processing time with and without the MD-5 hash algorithm in the subscriber side. Without MD-5, the average processing time of GOOSE messages with length of 132, 620, and 1024 Bytes are 575.71, 581.18, 588.26 μsec, respectively. With MD-5, the time is 716.53, 722.26, 737.82 μsec, respectively. The maximum time difference between non MD-5 and MD-5 is 149.56 μsec, when the message length is the maximum, (i.e., 1024 Bytes).

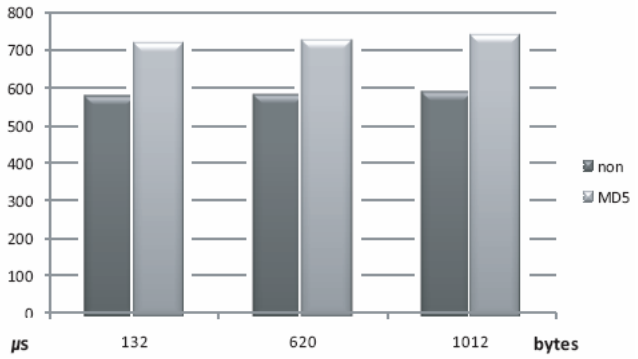

Fig. 5. MD5 and non-MD5 processing time in subscriber's side

The total processing time of the MD-5 hash algorithm in both publisher side and subscriber side for message length is summarized in Table 3. The maximum processing time for the MD-5 hashing algorithm is 185.7 μs with message length of 1012 Bytes. As shown in the Table 3, processing time for MD-5 increases as message length increases.

Table 3. Total processing time for MD-5 hashing algorithm

Length (Bytes)	132	620	1012
MD-5 hash	168.3 usec	175.2 usec	185.7 usec

The processing time for the SHA-1 and RSA algorithms is summarized in Table 4 with processing time of the MD-5 hash algorithm. The way to measure the total processing time for the other algorithm is the same as MD-5 as described above. Table 4 shows the hash algorithms such as MD-5 and SHA-1 which are enough to be applied to GOOSE services. Processing time of RSA algorithm, however, takes more than 15 msec, so we cannot apply RSA algorithms in IEC 61850 based power gird network. The transmission time also needs to be considered to check availability of security algorithm for GOOSE services.

Table 4. Total processing time for secure communication

Length (Bytes)	132	620	1012
MD-5 hash	168.3 usec	175.2 usec	185.7 usec
SHA-1 hash	196.6 usec	238.3 usec	259.9 usec
RSA	15092.6 usec	15112.5 usec	15147.6 usec

4.2 Network performance analysis

Communication network of a substation automation system consists of two communication bus, station bus and process bus. Station bus is used for communication between IEDs and HMI or supervisory systems. Process bus is used for communication between primary equipment, i.e., PT (Power Transformer), CT (Current Transformer), or circuit breaker, and protection and control IEDs. To measure the transmission delay of GOOSE messages, we model the IEC 61850 based substation station bus with one bay. Since traffic in process bus does not have serious impact on station bus, we model only the station bus. Modeled station bus consists of 25 nodes, (i.e., 17 IEDs, 6 network switches, one HMI, and one gateway to the SCADA system with mesh topology for redundancy) as shown in Fig. 6. 17. IEDs exchange GOOSE messages each other. IEDs and HMI exchange MMS messages. Performance analysis of transmission delay of GOOSE messages is conducted by means of computer simulation using NS (Network Simulator)-2. Simulation parameters are summarized in Table 5.

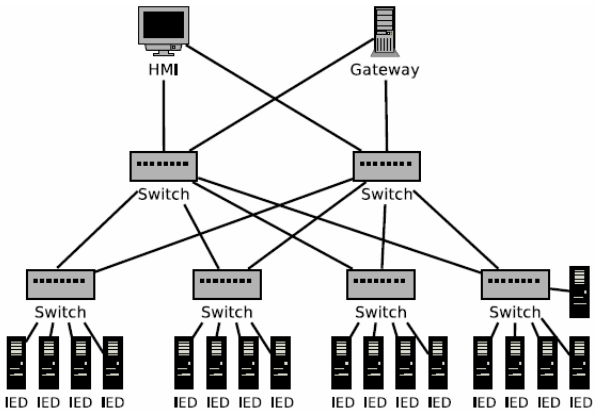

Fig. 6. Station bus topology for the performance analysis of GOOSE message

Table 5. GOOSE simulation parameters

Parameter	Values
Link bandwidth	100 Mbps
MMS traffic source	TCP
GOOSE traffic source	UDP
MMS interval	0.5 sec
GOOSE interval	0.25 sec
Simulation time	1000 sec
MMS packet size	500 Bytes
GOOSE packet size	132 Bytes
	620 Bytes
	1012 Bytes

As described in the previous section, GOOSE messages are mapped directly on top of Ethernet layer. NS-2 network simulator, however, does not support direct mapping of application layer to the data-link layer. We use UDP for transport layer for GOOSE services, because UDP adds minimum overhead for application data with no error and flow control between sender and receiver.

We define two different scenarios, light traffic load and heavy traffic load. In a light traffic load scenario, only GOOSE messages are exchanged between IEDs. In a heavy traffic load scenario, both GOOSE and MMS messages are exchanged. IEDs send MMS messages to HMI in every 0.5 second and GOOSE messages are exchanged between IEDs every 0.25 second. MMS packet size is set to 500 Bytes. We change the size of GOOSE packet with 132, 620, 1012 Bytes long to analyze the impact of size of GOOSE messages on transmission delay. We measure the transmission time of GOOSE messages. Fig. 6 shows the transmission delay of GOOSE message over the heavy traffic between two nodes in pair which are far most apart to get the maximum value, worst case scenario. The transmission time under both light and heavy traffic load are summarized in Table 6.

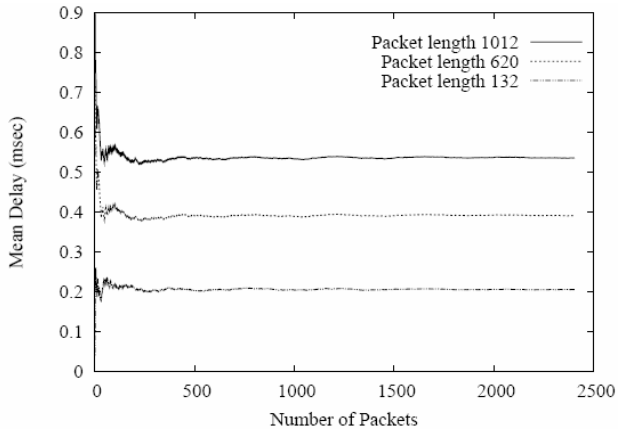

Fig. 7. Transmission delay of GOOSE message

Table 6. Transmission delay of GOOSE message on station bus

Length (Bytes)	132	620	1012
Light traffic	205.8 usec	391.4 usec	535.9 usec
Heavy traffic	239.4 usec	405.7 usec	556.7 usec

Transmission delay does not exceed the 3 msec timing constraint with all 3 different GOOSE message sizes even in heavy traffic load. MMS traffic has little effect on transmission delay. We, however, need to consider the processing time of security algorithms as well. Following section describes the total latency of delivering secure GOOSE messages over the station bus.

4.3 Total latency of delivering a secured GOOSE message

Based on the processing time of security algorithm and the transmission time of GOOSE messages discussed in the previous sections, total latency for delivering secure GOOSE messages over the station bus under heavy traffic loads is summarized as in Table 7.

Table 7. Total latency for delivering secure GOOSE messages over the station bus under heavy traffic loads

Length (Bytes)	132	620	1012
MD-5 hash	407.7 usec	580.9 usec	742.41 usec
SHA-1 hash	436.0 usec	644.0 usec	816.6 usec
RSA	15212 usec	15518.2 usec	15704.3 usec
MD-5 & RSA	15500.3 usec	15693.5 usec	15889.7 usec
SHA-1&RSA	15714.9 usec	15969.7 usec	17450.6 usec

When we apply the MD-5 or SHA-1 hash algorithm only, the performance of GOOSE satisfies the timing requirements specified in IEC 61850, which is 3 msec. If we apply the RSA signature algorithm with the MD-5 or SHA-1 algorithm to provide the confidentiality, the timing requirement is violated. As collision may occur in the MD-5, the SHA-1 hash algorithm is preferable in this case. Regardless of hash algorithms, RSA-based signature algorithms cannot guarantee the performance of GOOSE messages. Based on the performance measurement presented in this paper, the SHA-1 algorithm is optimal for GOOSE messages in an IEC 61850-based power utility system.

5. Conclusion

In applying IEC 61850 to a substation automation system, security becomes one of the most critical factor to run a smart grid. Power utility systems differ from Internet systems in a sense that power systems should guarantee the strict performance as well as reliability. It is very important to find an optimal security mechanism satisfying both constraints.

In this paper, two experiments were conducted measuring the total processing time of security algorithms and the transmission time between nodes to find an optimal security mechanism for the GOOSE service. The total processing time of four combinations of hash algorithms and authentication algorithms including MD-5 and SHA-1, and RSA signature algorithm is measured in consideration of integrity and authentication services. The transmission time between nodes is measured by means of computer simulation using NS-2. Numerical results show that only hash algorithms can currently be applied to the secure GOOSE service. Due to synchronization problems among devices, two experiments are separately performed. More

practical processing and transmission time would be measured under the environment in which all devices are synchronized. We consider only station bus in this paper which does not have sampled measured value messages. Sampled measured value messages, however, take large volume of traffic on process bus through consideration of sampled measured valued messages.

Acknowledgements

The authors are grateful to the careful consideration of an earlier version of this manuscript by the anonymous reviewers and their thoughtful comments on it. The present work was financially supported by the international collaborative R&D program (20118530020020) of the Korea Institute of Energy Technology Evaluation and Planning (KETEP), by the MKE (The Ministry of Knowledge Economy), Korea, under the CITRC (Convergence Information Technology Research Center) support program (NIPA-2012-H0401-12-1003) supervised by the NIPA (National IT Industry Promotion Agency), and by the Human Resources Development of the KETEP grant funded by the Korea government MKE (No. 20114010203030).

References

[1] E. Santacana, G. Rackliffe, T. Tang, and F. Xiaoming, "Getting Smart," *IEEE Power and Energy Magazine*, vol. 8, no. 2, pp. 41–48, Mar. 2010.

[2] G. N. S. Prasanna, A. Lakshmi, S. Sumanth, V. Simha, J. Bapat, and G. Koomullil, "Data Communication over the Smart Grid," *in Proc. of IEEE Int. Sump. Power Line Communications and Its Applications*, Apr. 2009, pp. 273–279.

[3] S. M. Amin and B. F. Wollenberg, "Toward a Smart Grid: Power Delivery for 21st Century," *IEEE Power and Energy Magazine*, vol. 3, no. 5, pp. 34–41, Sept. 2005.

[4] S.-J. Rim, S.-W. Zeng, and S.-J. Lee, "Development of an Intelligent Station HMI in IEC 61850 Based Substation," *Journal of Electrical Engineering & Technology*, vol. 4, no. 1, pp. 13-18, 2009.

[5] IEC 61850, Communication Networks and System in Substation Automation, IEC Std., 2002–2005, available at www.iec.ch.

[6] B. K. Yoo, S. H. Yang, H. S. Yang, W. Y. Kim, Y. S. Jeong, B. M. Han, K. S. Jang, "Communication Architecture of IEC 61850 based Micro Grid System," *Journal of Electrical Engineering & Technology*, vol. 6, no. 5, pp. 605-612, 2011

[7] J.-H. Jeon, S.-K. Kim, C.-H. Cho, J.-B. Ahn, and E.-S. Kim, "Development of Simulator Systems for Microgrids with Renewable Energy Sources," *Journal of Electrical Engineering & Technology*, vol. 1, no. 4, pp. 409-413, 2006.

[8] F. Cleveland, "IEC TC57 Security Standards for the Power System's Information Infrastructure – Beyond Simple Encryption," *in Proc. of IEEE Transmission and Distribution Conf. and Exhib*., May 2006, pp. 1079–1087.

[9] A. R. Metke and R. L. Ekl, "Security Technology for Smart Grid Networks," *IEEE Trans. on Smart Grid,* vol. 1, no. 1, pp. 99-107, 2010.

[10] G. N. Erricsson, "Cyber Security and Power System Communication–Essential Parts of a Smart Grid Infrastructure," *IEEE Trans. on Power Delivery*, vol. 25, no. 3, pp. 1501–1507, Apr. 2010.

[11] H. Khurana, M. Hadley, L. Ning, and D. Frincke, "Smart-Grid Security Issues," *IEEE Security and Privacy,* vol. 8, no. 1, pp. 81–85, Feb. 2010.

[12] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," *IEEE Security and Privacy*, vol. 7, no. 3, pp. 75–77, June 2009.

[13] K. Moslehi and R. Kumar, "A Reliability Perspective of the Smart Grid," *IEEE Trans. on Smart Grid*, vol. 1, no. 1, pp. 57–64, May 2010.

[14] IEC 62351, Power Systems Management and Associated Information Exchange – Data Communications Security, IEC Std., 2007–2010, available at www.iec.ch.

[15] S. Fries, H. J. Hof, and M. Seewald, "Enhancing IEC 62351 to Improve Security for Energy Automation in Smart Grid Environments," *in Proc. of Int. Conf. on Internet and Web App.,* pp. 135–142, 2010.

[16] H. K. Kim, S.-H. Kang, S.-R. Nam, and S.-S. Oh, "Improved Operating Scheme using an IEC 61850-based Distance Relay for Transformer Backup Protection," *in Proc. of IEEE Bucharest Power Tech.,* pp. 1-6, 2010.

[17] Cyber security working group, NIST, Smart Grid Interoperability Panel – "Cyber Security Working Group Standards Review," pp. 52-54, phase 1 Report, 2010

[18] T. Skiei, S. Johannessen, and C. Brunner, "Ethernet in Substation Automation," *IEEE Control Systems Mag*., pp. 43–51, June 2002.

[19] T. S. Sidhu and Y. Yin, "Modeling and simulation for performance evaluation of IEC61850-based substation communication systems," *IEEE Trans. on Power Delivery*, pp. 1482-1489, July 2007.

[20] H. S. Yang and et. al., "Gigabit Ethernet based substation," *Jourl. of Power Electronics*, pp. 100–108, Jan. 2009.

[21] S. G. Stubblebine and V. D. Gligor, "On Message Integrity in Cryptographic Protocols," *in Proc. of IEEE Computer Society Sym. on Research in security and Privacy,* 1992, pp. 85–104.

[22] B. D. Boer and A. Bosselaers, "An Attack in the Last Two Rounds of MD4," *Lecture Notes in Computer Science*, vol. 576, pp. 194–203, 1992.
[23] H. Dobbertin, "Cryptanalysis of MD4," Lecture Notes in Computer Science, vol. 1039, pp. 53–69, 1996.

Hyo-Sik Yang He is an assistant professor at Sejong University, Department of Computer Science and Engineering, Seoul, Korea. Before he joined Sejong University, he was an assistant professor at Kyungnam University, Masan, Korea. He joined Sejong University on fall 2006. He was a faculty research associate at Arizona State University, 2005. He received the B. E. degree in the Department of Information and Communication Engineering from Myongji University, Yongin, Korea, in 1998 and the M. S. and Ph. D. in Electrical Engineering from Arizona State University, Tempe, AZ, U.S.A., in 2000 and 2005, respectively.

His research interests are wavelength-division-multiplexing (WDM) all-optical networks, and Smart grid.

Sang-Sig Kim He is a Ph.D. candidate in Computer Science and Informatics at Oakland University. He received the MS and BEE in Computer Software from Myongji University, Korea in 2008 and 2006, respectively. During the undergraduate and master programs, he participated in the Substation Automation System (IEC 61850) project funded by Korea Electric Power Corporation (KEPCO). His research interests include design patterns, access control modeling, formal methods and IEC 61850 based substation automation system. He is a student member of the IEEE.

Hyuk-Soo Jang He was born in Oakcheon Korea in 1956. He received the B.S. degree in industrial engineering from the Seoul National University, Seoul Korea in 1983 and the Ph.D. degree in Computer and Information Science from the Ohio State University, Columbus Ohio USA in 1990. Since 1992, he has been with the Department of Computer Science and Engineering in Myongji University, where he is currently a professor. He is engaged in research and standardization on Power IT, IEC 61850 based Substation Automation Systems, and Smart Grid.