IMPLEMENTATIO OF SECURE IEC 61850 COMMUNUCATION

Jin Cheol Kim
KEPCO KDN – Korea
kjc@kdn.com

Tae Hun Kim
KEPCO KDN - Korea
thkim@kdn.com

ABSTRACT

IEC 61850 is a specification for the design and configuration of substation automation. It supports a comprehensive set of substation functions and provides rich features for substation communications. It is also extensible enough to support system evolution.
In this paper, to evaluate the secure IEC 61850 communication, we implemented the IEC 62351-6 MAC mechanism and IEC 62351-4 Security profile. We applied our IEC 62351 MAC mechanism and MMS security profile on Smart Distribution Management System (SDMS) that uses IEC 61850 protocol. The MMS protocol is used between SDMS server and F-IED(Feeder Intelligent Electronic Device). The GOOSE protocol is used between F-IEDs.

INTRODUCTION

Smart grid is an electricity network that can integrate in a cost efficient manner the behavior and actions of all users connected to it - generators, consumers and those that do both - in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety.
Many electric sector infrastructures were designed and installed decades ago with limited cybersecurity consideration. Increasing connectivity, integration with legacy systems, the proliferation of access points, escalating system complexity and wider use of common operating systems and platforms may contribute to increased risks for the Smart Grid.[1]
NERC CIP 002-009 has developed security standards for all utilities with Critical Assets, currently just for transmission, but likely to apply more broadly.[2] IEC 62351 series for utility communications include security for utility-specific protocols (IEC 61850, DNP3), role-based access control, and network and system management.[3] AMI-SEC under the UCA Users Group is addressing security issues for Advanced Metering Infrastructure.[4] IEC TC65C(in conjunction with ISA SP99) is developing security standards for industrial automation.[5] In US, The National Institute of Standards and Technology (NIST) develops and promotes measurement, standards, and technology on the Smart Grid. In 2009, NIST formed the Smart Grid Interoperability Panel (SGIP) as a public-private cooperation with over 600 members that develops frameworks and roadmaps, not standards. SGIP's security related work is carried out in the Cyber Security Working Group (CSWG).[6]
In this paper, to evaluate the secure IEC 61850 communication, we implemented the IEC 62351-6 MAC mechanism and IEC 62351-4 Security profile. We applied our IEC 62351 MAC mechanism and MMS security profile on Smart Distribution Management System (SDMS) that uses IEC 61850 protocol. The MMS protocol is used between SDMS server and F-IED(Feeder Intelligent Electronic Device). The GOOSE protocol is used between F-IEDs.

IEC 61850 AND IEC 62351

IEC 61850 is a specification for the design and configuration of substation automation.[7] It supports a comprehensive set of substation functions and provides rich features for substation communications. It is also extensible enough to support system evolution. IEC 61850 uses object oriented data models to describe the information of various primary equipments and substation automation functions. It specifies the communication interfaces between IEDs and the schemes mapping them to a number of protocols running over TCP/IP and high speed Ethernet. GOOSE is a link-layer multicast protocol designed in IEC 61850 for transmitting timing-critical messages, such as substation events, commands and alarms, within power substation networks. Because GOOSE is directly mapped to Ethernet frames, it can take advantage of high speed switched Ethernet and is capable of fulfilling timing requirements.[8] IEC 61850 Profile is shown in Figure 1.

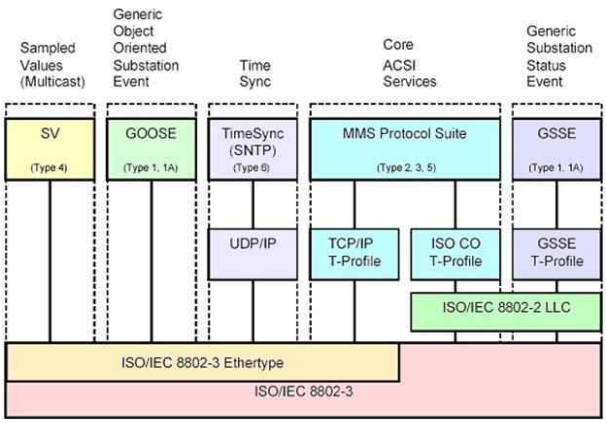

Figure 1. IEC 61850 Profile

In IEC 61850, the messages need to be transmitted within 4 milliseconds and so that encryption or other security measures which affect transmission rates are not acceptable. Therefore, authentication is the only security measure included, so IEC 62351-6 provides a mechanism that involves minimal compute requirements for these profiles to digitally sign the messages. The Virtual LAN (VLAN) high speed profiles used for GOOSE, GSSE, IEC 61850-9-1, and

IEC 61850-9-2, has performance requirements (e.g. 4 msecs or less) that prohibit the use of full encryption. Current thoughts within IEC TC57 WG15 are to use a CRC based Message Authentication Code/Seal to provide integrity. Secure GOOSE/SV protocol is shown in Figure 2.

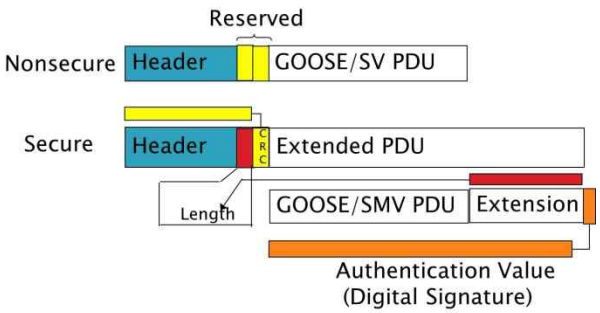

Figure 2. Secure GOOSE/SV

Authentication would be provided via an address-based credential. Confidentiality would need to be provided through appropriate communication path selection. It is expected that the MAC mechanism will be addressed in IEC 62351-6. It is also expected IEC 62351-6 will reference IEC 62351-3 (Security for profiles including TCP) and IEC 62351-4 (Security for profiles including MMS) in regards to the IEC 61850 MMS based profile. Secure profile for IEC 61850 is shown in Figure 3.

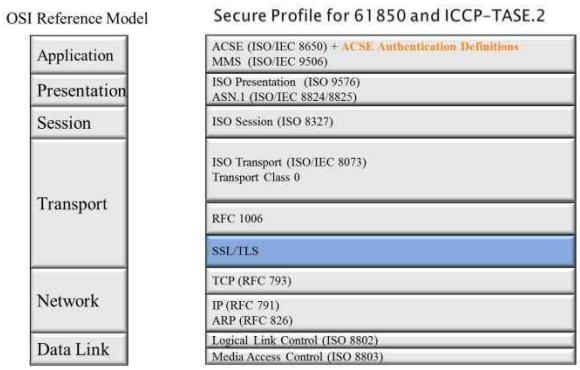

Figure 3. Secure MMS

SECURE IEC 61850 COMMUNICATION

Secure GOOSE Implmentation

To implement IEC 62351-6 MAC mechanism, we used the IEC 61850 GOOSE stack and the Hardware Security Module (HSM). Our MAC mechanism is as following.

<Sender>
[Step 1] Hash Value Calculation
Using hash function, the sender calculates the hash value of GOOSE APDU.

$$H_{APDU\_1} = h(M_{APDU}) \qquad (1)$$

[Step 2] Authentication Value Calculation
Using sender's private key in HSM, the sender digitally sign the hash value

$$A_{APDU} = E_{PRI\_S}(H_{APDU\_1}) \qquad (2)$$

[Step 3] Message Sending
The Sender sends secure GOOSE message

<Receiver>
[Step 1] Message Receiving

[Step 2] Decryption Authentication Value
Using sender's public key, the receiver decrypt signed Authentication Value

$$H_{APDU\_1} = E_{PUB\_S}(A_{APDU}) \qquad (3)$$

[Step 3] Hash Value Calculation
Using hash function, the receiver calculates the hash value of GOOSE APDU.

$$H_{APDU\_2} = h(M_{APDU}) \qquad (4)$$

[Step 4] Verification Digital Signature
The receiver verifies message integrity and digital signature.

$$H_{APDU\_1} = H_{APDU\_2} \qquad (5)$$

[Step 5] GOOSE APDU Processing
The receiver process GOOSE APDU.

Secure MMS Implmentation

To implement secure MMS protocol, we used the IEC 61850 MMS stack and Open SSL library. Our TLS Cipher Renegotiation is shown in Figure 4.

Figure 4. TLS Cipher Renegotiation

Figure 5 illustrates security mode and port number in MMS stack.

Figure 5. Security Mode and Port Configuration

TEST RESULTS

We apply our IEC 62351 MAC mechanism and MMS security profile on Smart Distribution Management System (SDMS) that uses IEC 61850 protocol. The MMS protocol is used between SDMS server and F-IED. The GOOSE protocol is used between F-IEDs. We build the security test environment for secure GOOSE as shown in Fig 6. The F-IEDs send/receive secure GOOSE messages using HSM.

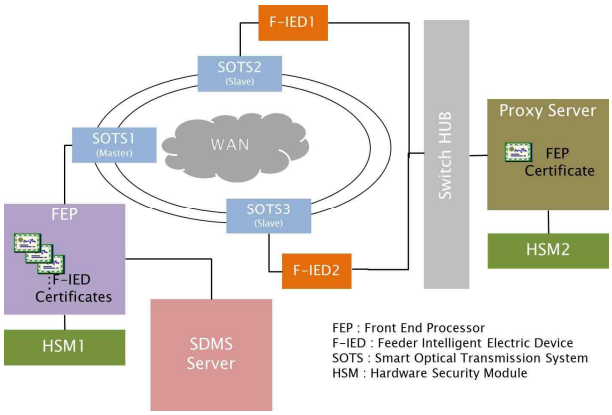

Figure 6. Test Environment for Secure GOOSE

We build the security test environment for secure MMS as shown in Fig 7. Secure MMS messages are transmitted between FEP and F-IED.

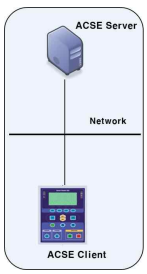

Figure 7. Test Environment for Secure MMS

In GOOSE security test environment, we use SHA1/SHA256 as hash algorithm and ECDSA as digital signature algorithm. We compare the signature mean time of 1000 times and the verification mean time of 1000 times. Our test results are shown in Fig 8 and 9.

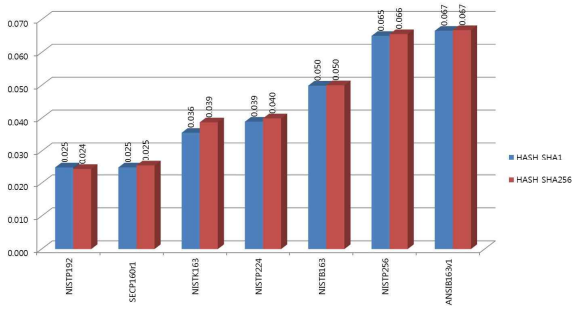

Figure 8. Signature Mean Time

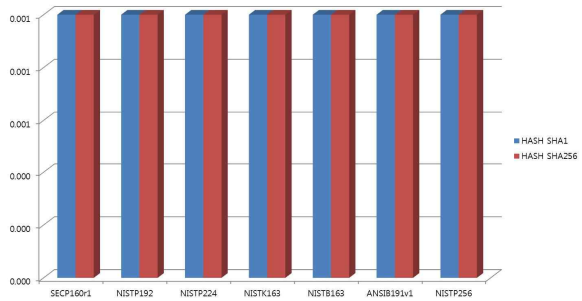

Figure 9. Verfication Mean Time

In MMS security test environment, we use ECDH, ECDSA, AES 256 CBC mode, and SHA. Figure 10 illustrates authentication value of AARQ message.

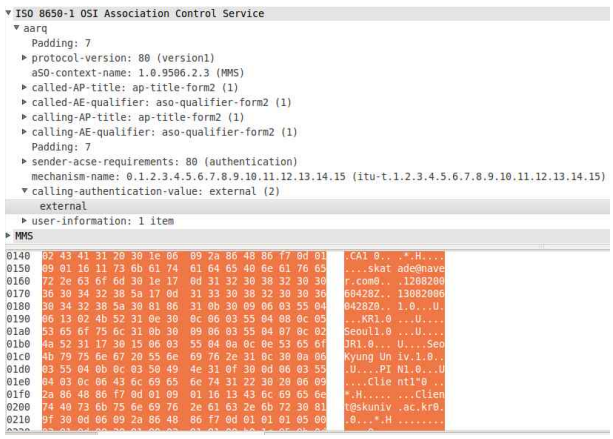

Figure 10. Authentication Value of AARQ Message

Figure 11 illustrates authentication value of AARE message.

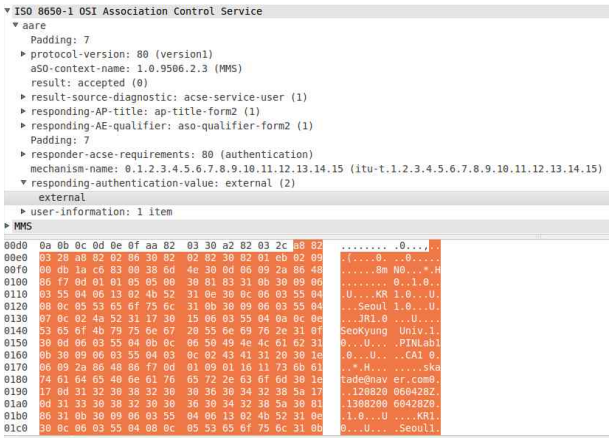

Figure 11. Authentication Value of AARE Message

CONCLUSIONS

Many electric sector infrastructures were designed and installed decades ago with limited cybersecurity consideration. Increasing connectivity, integration with legacy systems, the proliferation of access points, escalating system complexity and wider use of common operating systems and platforms may contribute to increased risks for the Smart Grid.

In this paper, to evaluate the secure IEC 61850 communication, we implement the IEC 62351-6 MAC mechanism and IEC 62351-4 Security profile. We apply our IEC 62351 MAC mechanism and MMS security profile on Smart Distribution Management System (SDMS) that uses IEC 61850 protocol. The MMS protocol is used between SDMS server and F-IED(Feeder Intelligent Electronic Device). The GOOSE protocol is used between F-IEDs.

Through our security test results, we could know which ECDSA curves are suitable as digital signature algorithm for Smart Grid device and there are some possibilities of the authentication value using the digital signature algorithm in IEC 61850 messages. Using the IEC 61850 MMS stack and Open SSL library, we got authentication values of AARQ and AARE message.

REFERENCES

[1] Anthony R. Metke, Randy L. Ekl, 2010, “Security Technology for Smart Grid Networks”, IEEE Transactions on Smart Grid, Vol 1, No.1, 99-107.

[2] NERC, North American Reliability Corporation, Standards

[3] ISO-IEC 62351, Part 1-8

[4] AMI SEC, 2010, Security Profile for Advanced Metering Infrastructure

[5] ISA 99 Standards Framework

[6] NIST, 2010, Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security

[7] ISO-IEC 61850, Part 1-9

[8] Jianqing Zhang and Carl A. Gunter, 2011, “Application-aware secure multicast for power grid communications”, Int. J. Security and Networks, Vol. 6, 40-52.