

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.

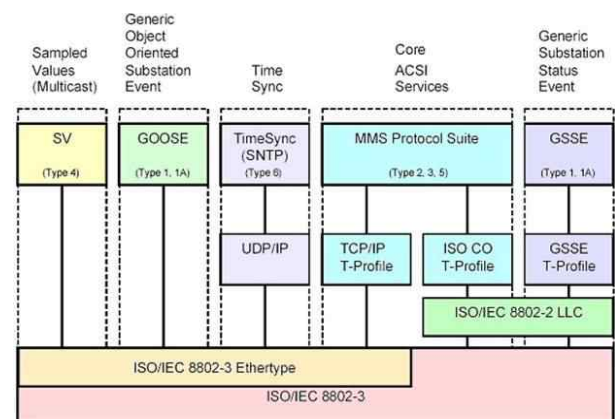


Figure 1. IEC 61850 Profile

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 msec 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.

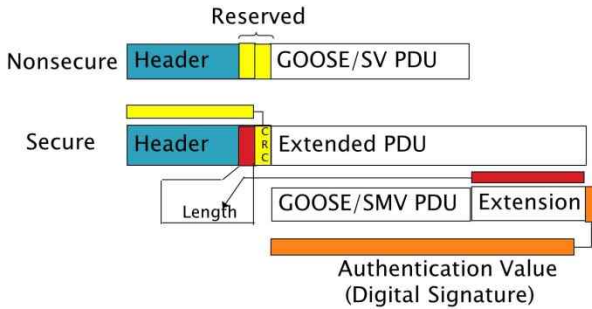


Figure 2. Secure GOOSE/SV

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.

OSI Reference Model	Secure Profile for 61 850 and ICCP-TASE.2
Application	ACSE (ISO/IEC 8650) + ACSE Authentication Definitions MMS (ISO/IEC 9506)
Presentation	ISO Presentation (ISO 9576) ASN.1 (ISO/IEC 8824:8825)
Session	ISO Session (ISO 8327)
Transport	ISO Transport (ISO/IEC 8073) Transport Class 0
	RFC 1006
Network	SSL/TLS
	TCP (RFC 793)
Data Link	IP (RFC 791) ARP (RFC 826)
	Logical Link Control (ISO 8802) Media Access Control (ISO 8803)

Figure 3. Secure MMS

SECURE IEC 61850 COMMUNICATION

Secure GOOSE Implementation

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.

$$H_{APDU_1} = h(M_{APDU}) \quad (1)$$

[Step 2] Authentication Value Calculation

Using sender's private key in HSM, the sender digitally sign the hash value

$$A_{APDU} = E_{PRI_S}(H_{APDU_1}) \quad (2)$$

[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

$$H_{APDU_1} = E_{PUB_S}(A_{APDU}) \quad (3)$$

[Step 3] Hash Value Calculation

Using hash function, the receiver calculates the hash value of GOOSE APDU.

$$H_{APDU_2} = h(M_{APDU}) \quad (4)$$

[Step 4] Verification Digital Signature

The receiver verifies message integrity and digital signature.

$$H_{APDU_1} = H_{APDU_2} \quad (5)$$

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

Secure MMS Implementation

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.

```

MMS-LITE-88X-001 Version 5.02
Copyright (c) 1986-2005 SISCO, Inc. All Rights Reserved.

** Security Mode (Server) **
1. NON-SECURE
2. SECURE
3. DON'T CARE

2012-08-17 17:20:13 tpd_sock.c
9 Info, IEC61850 Non-Security Port (102) Open
10
11 2012-08-17 17:26:13 tpd_sock.c
12 Info, IEC61850 Security Port (3782) Open

PID TTY TIME CMD
401 pts/2 00:00:00 bash
22986 pts/2 00:00:00 sositpcp_id
22987 pts/2 00:00:00 sllstend
22988 pts/2 00:00:00 sllstend
22989 pts/2 00:00:00 ps
    
```

Figure 5. Security Mode and Port Configuration

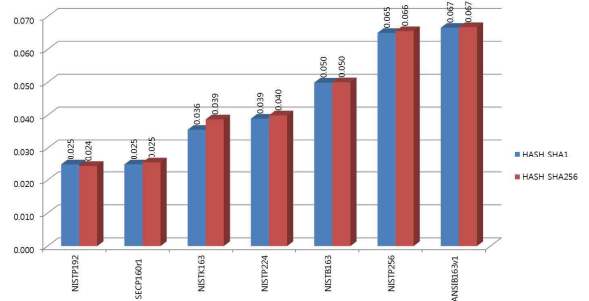


Figure 8. Signature Mean Time

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.

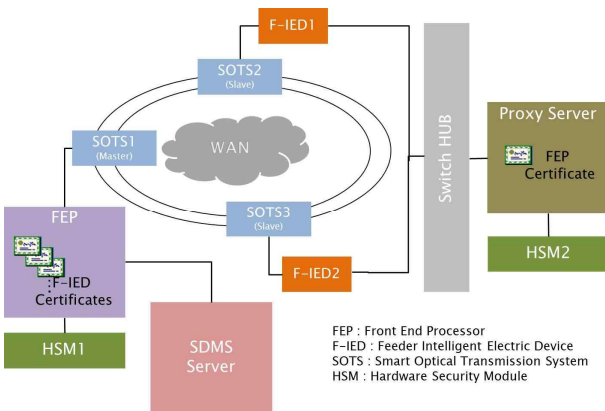


Figure 6. Test Environment for Secure GOOSE

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

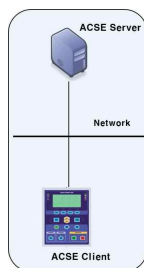


Figure 7. Test Environment for Secure MMS

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.

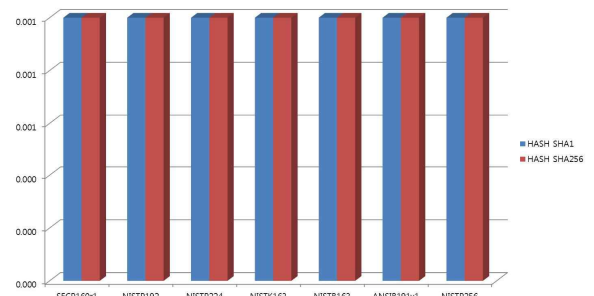


Figure 9. Verification Mean Time

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

```

ISO 8658-1 OSI Association Control Service
aarp
  Padding: 7
  protocol-version: 80 (version1)
  a50-context-name: 1.0.9506.2.3 (MMS)
  called-AP-title: ap-title-form2 (1)
  called-AE-qualifier: aso-qualifier-form2 (1)
  calling-AP-title: ap-title-form2 (1)
  calling-AE-qualifier: aso-qualifier-form2 (1)
  Padding: 7
  sender-acse-requirements: 80 (authentication)
  mechanism-name: 0.1.2.3.4.5.6.7.8.9.10.11.12.13.14.15 (itu-t.1.2.3.4.5.6.7.8.9.10.11.12.13.14.15)
  calling-authentication-value: external (2)
  external
  user-information: 1 item
MMS
0140 82 43 41 31 20 30 10 06 80 2a 86 40 86 f7 04 01 CA1 0...t.H...
0150 89 01 16 11 73 6b 61 74 61 64 65 40 6e 61 76 63 ...skat ade@nave
0160 72 2e 63 6f 6d 30 1e 17 0d 31 32 30 30 32 30 30 P.com@...1208200
0170 36 30 34 32 38 5a 17 0d 31 33 30 38 32 30 30 36 B4282...13082000
0180 30 34 20 30 2a 36 81 06 31 00 36 09 00 03 55 04 B4282...1.0...U...
0190 06 13 02 4b 52 31 0e 30 0c 00 03 55 04 08 0c 05 ...01.0...U...
01a0 53 65 6f 75 6c 31 0b 30 09 06 03 55 04 07 0c 02 Seoul1.0...U...
01b0 4a 52 31 17 30 15 06 03 55 04 0a 0c 0e 53 65 6f JRI.0...U...Seo
01c0 4b 79 75 6e 67 20 55 6e 69 76 2e 31 0c 30 8a 06 Kyung Un iv.1.0...
01d0 03 55 04 00 0c 03 50 40 4e 31 0f 30 00 00 63 55 ...PI N1.0...U...
01e0 04 03 0c 0e 43 6c 69 65 6e 74 31 22 30 20 06 09 ...Clie nt@p...
01f0 2a 86 48 86 f7 0d 01 09 01 16 13 43 6c 69 65 6e *.H...Client
0200 74 48 73 6b 75 6e 69 76 2e 61 63 2e 6b 72 30 81 t@skuniv .ac.kr@...
0210 0f 30 06 06 09 2a 86 48 86 f7 0d 01 01 01 05 06 @.H...
    
```

Figure 10. Authentication Value of AARQ Message

Figure 11 illustrates authentication value of AARE message.

```

ISO 8650-1 OSI Association Control Service
  aare
    Padding: 7
    protocol-version: 80 (version1)
    a50-context-name: 1.0.9506.2.3 (MMS)
    result: accepted (0)
    result-source-diagnostic: acse-service-user (1)
    responding-AP-title: ap-title-form2 (1)
    responding-AE-qualifier: aso-qualifier-form2 (1)
    Padding: 7
    responder-acse-requirements: 80 (authentication)
    mechanism-name: 0.1.2.3.4.5.6.7.8.9.10.11.12.13.14.15 (itu-t.1.2.3.4.5.6.7.8.9.10.11.12.13.14.15)
    responding-authentication-value: external (2)
  external
    user-information: 1 item
  MMS
    00d0 0a 0b 0c 0d 0e 0f aa 02 03 30 a2 02 03 2c b8 02 .....0....
    00e9 93 28 a8 02 02 06 30 02 02 02 30 02 01 ed 02 09 {...0...0....
    00f6 00 0b 1c cf 03 08 30 0d 4c 30 04 06 02 2a 06 05 .....00M0...
    0100 36 f7 0d 01 01 05 05 00 30 01 83 31 05 30 09 06 .....0.1.0..
    0110 03 55 04 06 13 02 4b 52 31 0e 30 0c 06 03 55 04 ..U...KR 1.0...U.
    0120 08 0c 05 53 65 6f 75 6c 31 0b 30 09 06 03 55 04 ...Seoul 1.0...U.
    0130 07 0c 02 4a 52 31 17 30 15 06 03 55 04 00 06 04 ...JRI 0...U...
    0140 53 65 6f 4b 75 75 6e 67 20 55 6e 09 76 2e 31 07 seokkyung Univ.1.
    0150 30 0d 06 03 55 04 0b 0c 06 50 49 4e 4c 61 62 31 0...U...PINLab1
    0160 0b 30 09 06 03 55 04 03 0c 02 43 41 31 20 30 16 0...U...CA1 6
    0170 08 09 2a 05 4b 06 17 00 01 09 01 16 13 73 00 01 ...H...3M
    0180 24 61 64 05 40 06 61 70 05 72 2e 63 6f 6d 30 10 tadelnav er.com0
    0190 17 0d 31 32 30 38 32 30 30 36 30 34 32 30 5a 17 ...120820 0604202
    01a0 0d 31 33 30 38 32 30 30 36 34 32 30 5a 30 01 ...1308200 0604202
    01b0 08 31 0b 30 09 06 03 55 04 06 15 02 40 57 21 06 ...1.0...U...KR1
    01c0 00 0c 06 03 55 04 0b 0c 05 53 65 6f 75 6c 31 00 ...U...Seoul1
  
```

Figure 11. Authentication Value of AARE Message

communications”, Int. J. Security and Networks, Vol. 6, 40-52.

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