IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 23, 2020, accepted June 9, 2020, date of publication June 12, 2020, date of current version July 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3001926

IEC 62351-4 Security Implementations for IEC 61850 MMS Messages

TAHA SELIM USTUN, (Member, IEEE), AND S. M. SUHAIL HUSSAIN, (Member, IEEE)
Fukushima Renewable Energy Institute, AIST (FREA), National Institute of Advanced Industrial Science and Technology (AIST), Koriyama 963-0298, Japan
Corresponding author: S. M. Suhail Hussain (suhail.hussain@aist.go.jp)

This work was supported in part by the Fukushima Prefecture's Reconstruction Grant, 2019.

ABSTRACT With the deployment of advanced information and communication technologies (ICT) the legacy power grid is being transformed as smart grid. However, the extensive use of ICT makes it vulnerable to cyberattacks. Standardization of power system communication with interoperable protocols has many benefits and at the same time the standardized semantics makes it much more vulnerable to cyberattacks. IEC has published a new standard IEC 62351 which provides the security guidelines for securing power system communication against cyber-attacks. In this paper, the cybersecurity considerations for IEC 61850 Manufacturing Message Specification (MMS) messages as per the IEC 62351-4 standard are discussed in detail. Further, the implementation of IEC 62351-4 security specifications for MMS messages are demonstrated through experiments in lab.

INDEX TERMS Power system communication, security and privacy protection, IEC 61850, IEC 62351-4.

I. INTRODUCTION

With the integration of instrumentation, control and information communication technologies to conventional power system has led to power system automation and transition of legacy power grid to smart grid. Substations are digitalized with incorporation of Intelligent Electronic Devices (IEDs) which enhances the control and automation capabilities [1]. IEC 61850 is by far the most popular standard for power utility automation. Due to the object-oriented modelling approach and interoperability features, IEC 61850 has become most popular standard for power utility automation not only for substation automation systems but also for other areas of smart grid communication [2]–[4].

However, with increased automation and use of standardized communication makes the power system/substations much more vulnerable to cyberattacks. Exploiting the standardized semantics make it is much easy for adversaries to launch different types of attacks [5]. Recent events such as Ukraine black out, Stux-net virus attack, etc., are some examples of such attacks [6]. Hence, cybersecurity considerations for preventing attacks on standardized communication in smart grids is essential. IEC 61850 standard doesn't discuss the cybersecurity concerns [7]. IEC 62351 standard compliments the IEC 61850 by addressing the cybersecurity concerns [8]. Authors in [9], [10] presented a comprehensive review of IEC 62351 security standards and assessment of its applicability to IEC 61850 messages.

IEC 62351-6-part deals with cybersecurity requirements for IEC 61850 Generic Object-Oriented Substation Event (GOOSE) and Sampled Value (SV) [11]. Since GOOSE message and SV carry time critical power system messages and measurement messages respectively, much attention has been paid by researchers to secure these messages. IEC 62351-6 stipulates RSA based digital signatures for securing GOOSE and SV messages [12]. However, numerous studies showed that RSA based digital signatures result is higher processing times and cannot meet the timing requirements of GOOSE and SV messages [13], [14]. Alternatively, Message Authentication Code (MAC) based schemes were proposed for securing GOOSE and SV messages [15].

In literature the security concerns for GOOSE and SV messages have been studied and reported in detail [12]–[16]. However, the security requirements of IEC 61850 Manufacturing Message Specification (MMS) messages was not investigated extensively. The IEC 62351-4 standard enumerates integrity, confidentiality and authentication as the security requirements for IEC 61850 MMS messages [8]. For achieving these security requirements certificate-based Transport Layer Security (TLS) mechanism is specified by IEC 62351-4 standards. IEC 623451-4 recommends different cipher suites that can be used during TLS session

The associate editor coordinating the review of this manuscript and approving it for publication was Bin Zhou.

for achieving the security requirements. In [17], [18], authors have discussed the certificate-based authentication mechanism for MMS messages. IEC 623451-4 recommends different cipher suites that can be used during TLS session for achieving the security requirements. The security considerations such as TLS session introduces additional computational latencies for processing MMS messages. The computational latencies for establishing TLS (i.e. handshake) and during data transfer (encrypted MMS message exchanges) depends on the algorithms of cipher suites. Hence, evaluation of different recommend cipher suites for satisfactory and acceptable performance is required. In [19] authors presented the comparison of latencies for MMS message exchanges after TLS establishment for different cipher suites. In [20], authors presented an experimental platform for implementing TLS and calculating latencies for TLS handshake for different cipher suites. However, these works report overall latencies for implementing TLS handshake rather individual latencies for different algorithms in cipher suites. This information of computational latencies for different algorithms in a cipher suite is important to assess its applicability to MMS messages.

This paper presents the experimental lab implementation of different algorithms of the IEC 62351-4 recommended cipher suites by establishing a TLS connection for securing IEC 61850 MMS messages. Further, this paper develops signed X.509 certificates, using different public key algorithms, for the IEC 61850 client and server, required to establish the TLS connections.

Section II provides a comprehensive overview of IEC 62351-4 security requirements for securing IEC 61850 MMS messages. Section III presents the implementation and evaluation of different cipher suites for IEC 61850 MMS messages. Finally, conclusions are presented in Section IV.

II. IEC 62351-4 SECURITY REQUIREMENTS FOR MMS MESSAGES

The IEC 62351-4 standard specifies security requirements for MMS messages both at the application and transport profiles. The top three layers of OSI reference model (i.e. application, presentation and session layers) form the application profile. While the bottom four layers (transport, network, data link and physical) form the transport profile.

A. SECURITY FOR TRANSPORT PROFILE

The IEC 62351-4 defines two transport security (T-security) specifications, i.e. compatible and native, for transport profile. T-security specification in compatibility mode is exclusively for MMS using OSI stack implementation according to ISO 9506-2 and this mode is not recommended for new implementations of MMS messages. Whereas the T-security specification in native mode is relevant for both MMS using IP suite and IEC 61850-8-2 XMPP implementations. For all future implementations of MMS messages native mode T-security specification shall be considered. The protocol stack of compatible and native T-security specifications for MMS message with relevant RFCs at each layer is shown in Fig. 1.

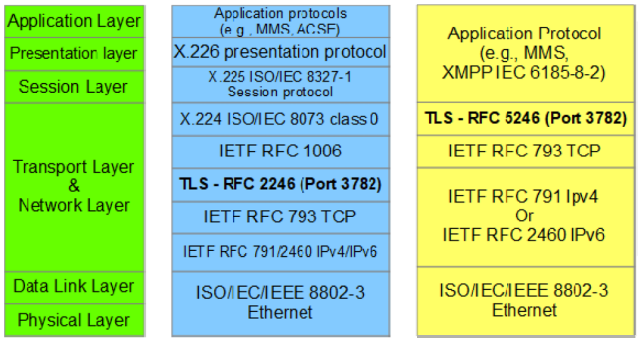

FIGURE 1. Protocol stack for compatible and native T-security specifications for MMS messages.

The T-security specification for compatibility mode recommend use of TLS 1.0 (as per RFC 2246) before a TCP session. While the native mode recommends TLS 1.2 (as per RFC 5246). Implementing TLS process provides the encryption and nodal authentication for the TCP session. For implementing the TLS at transport layer port 3782 is used instead of the usual port 102. Hence, the secure MMS messages use the port 3782 at the transport layer.

The MMS message exchange takes place in two phases, i.e. handshake phase and data transfer phase. The handshake phase refers to the establishment and negotiation of TLS session. This is followed by actual data transmission which is termed as data transfer phase. The message exchanges for establishment of TLS session is shown in Fig. 2. Initially, certificates of both client and server are exchanged and verified. Then, a secret key is exchanged between client and server

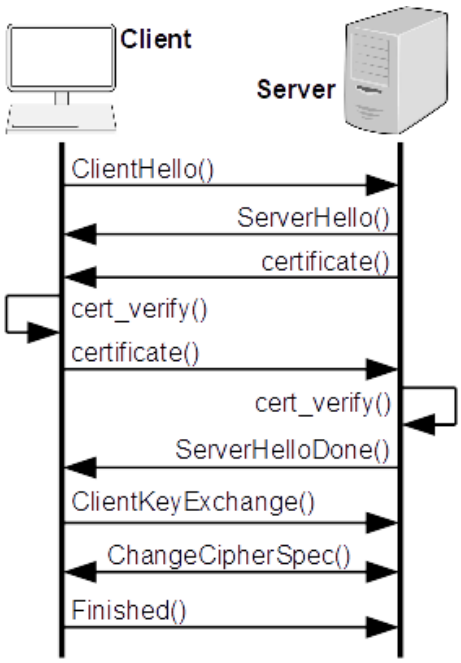

FIGURE 2. Message exchanges for TLS establishment for client and server.

TABLE 1. Recommended cipher suites for MMS messages.

Key exchange		Hash	Encryption	TLS
Algorithm	Signature	function	algorithm	version
TLS RSA		SHA256	WITH AES 128 CBC	TLS 1.2
TLS DH	RSA	SHA256	WITH AES 128 CBC	TLS 1.2
TLS DH	RSA	SHA256	WITH AES 128 GCM	TLS 1.2
TLS DHE	RSA	SHA256	WITH AES 128 GCM	TLS 1.2
TLS DH	RSA	SHA384	WITH AES 256 GCM	TLS 1.2
TLS ECDHE	RSA	SHA256	WITH AES 128 GCM	TLS 1.2
TLS ECDHE	RSA	SHA384	WITH AES 256 GCM	TLS 1.2
TLS ECDHE	ECDSA	SHA256	WITH AES 128 GCM	TLS 1.2
TLS ECDHE	ECDSA	SHA384	WITH AES 256 GCM	TLS 1.2

using some public key exchange algorithm such as "*Diffie–Hellman (DH)" or RSA* based key exchange algorithm. Using this secret key, a cipher suite is negotiated. Cipher suite is a set of cryptographic algorithms which specifies an algorithm each for key exchange, digital signature, encryption and message authentication. Further data exchanges during the session are secured by applying the negotiated algorithms.

Initially, after exchanging the hello messages, server sends its certificate along with public key to the client. The certificates shall have X.509 format with a maximum size of 8192 bytes to be in conformance with IEC 62351-4 specifications. The client verifies the certificate by contacting a Certificate Authority (CA) and if the certificate is valid it replies by sending its own certificate along with public key to server. The server again verifies the client certificate. If the certificate verification is successful, server sends a '*ServerHelloDone*' message to client. Which signifies that the mutual node authentication of both client and server is complete successfully. By using any public key cryptographic algorithm, a secret key is exchanged. Utilizing this secret key, cipher suite is negotiated. IEC 62351-4 recommended cipher suites for MMS message exchanges are shown in Table 1.

Among the listed cipher suites, it is further mandated at a minimum "*TLS_RSA_WITH_AES_128_CBC_SHA256*" cipher suite should be supported in order to claim conformance to IEC 62351-4. Where RSA algorithm is used for both key exchange and digital signatures, AES_128_CBC is used for encryption and SHA256 for HASH generation.

In these mandated cipher suites Advanced Encryption Standard (AES) 128/256 is used for encryption and Secure Hash Algorithm (SHA 256/384) is used for generating Hash values. Furthermore, either RSA or DH or DHE or ECDHE are specified for secure key exchanges. SHA256 and RSA/ECDSA algorithms are utilized to generate digital signatures which are used for message authentication. Hence, with the TLS security mechanism the transport profile of the MMS messages is secured to provide confidentiality (AES 128/256 encryption), node authentication (X.509 certificates during TLS) and message authentication (digital signatures using SHA and RSA/ECDSA) to the MMS messages.

B. SECURITY FOR APPLICATION PROFILE

For application profile security two security specifications namely peer-to-peer (or A-security) and End to End application security (E2E security) are specified by IEC 62351-4 standards.

In A-security specification only peer entity authentication during association setup is specified. For providing peer entity authentication, authentication information is added to association setup messages i.e. the Association Control Service Element (ACSE)-association request (AARQ) and association response (AARE) messages. The authentication information is added to authentication value fields in ACSE-AARQ and AARE messages. The authentication information contains BER encoded X.509 certificate, digital signature and time value (it is the GMT value of the time at which the authentication values are generated). The certificates for both client and server participating in authentication are exchanged and verified. The verification is carried out by comparing the digital signatures which are generated using "*RSASSA-PKCS1-v1_5"* algorithm implementation. During the data transfer phase after the association setup, no security is applied. Hence, the use of only application profile security without transport profile security will result in a non-secure system. For Transport profile security, TLS mechanism is specified which gives reasonable security. Hence, any system implementing Transport profile security is reasonably secure. Table 2 gives the comparison of different security implementations with application and transport profile securities.

In E2E security specification peer authentication and message integrity and confidentiality both during association setup and data transfer phase is specified. Public key signature algorithms and symmetric encryption algorithms are utilized to achieve the above security requirements in E2E security specification. When the E2E security specifications

TABLE 2. Security specifications for application and transport profiles.

Application Profile security	Transport Profile security	Remarks	Security level
A-security Profile	None	Only peer authentication at application profile	Non-Secure system
A-security Profile	TLS	Peer authentication, confidentiality and integrity provided by TLS at transport profile and peer authentication at application profile	Reasonably secure
E2E security	None	peer authentication, end to end integrity and confidentiality at application profile	Reasonably secure
E2E security	TLS	Peer authentication, confidentiality and integrity provided by TLS at transport profile and peer authentication, end to end integrity and confidentiality at application profile	Secure system
None	TLS	Peer authentication, confidentiality and integrity provided by TLS at transport profile	Reasonably secure

```
     2 6.070897    192.168.0.4     192.168.0.7     TCP      66 54313 → 102 [SYN] Seq=0 Win=65534 Len=0 MSS=1460 WS
     3 6.071725    192.168.0.7     192.168.0.4     TCP      66 102 → 54313 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
     4 6.071791    192.168.0.4     192.168.0.7     TCP      54 54313 → 102 [ACK] Seq=1 Ack=1 Win=65534 Len=0
     5 6.087600    192.168.0.4     192.168.0.7     COTP     84 CR TPDU src-ref: 0x00c9 dst-ref: 0x0000
     6 6.088448    192.168.0.7     192.168.0.4     TCP      60 102 → 54313 [ACK] Seq=1 Ack=31 Win=29312 Len=0
     7 6.088454    192.168.0.7     192.168.0.4     COTP     77 CC TPDU src-ref: 0x005b dst-ref: 0x00c9
     8 6.090029    192.168.0.4     192.168.0.7     MMS     251 initiate-RequestPDU
     9 6.101465    192.168.0.7     192.168.0.4     MMS     214 initiate-ResponsePDU
    10 6.143299    192.168.0.4     192.168.0.7     TCP      54 54313 → 102 [ACK] Seq=228 Ack=184 Win=65351 Len=0

▸ Frame 8: 251 bytes on wire (2008 bits), 251 bytes captured (2008 bits) on interface 0
▸ Ethernet II, Src: Vaio_10:da:8b (cc:30:80:10:da:8b), Dst: Micro-St_1e:7c:ea (d8:cb:8a:1e:7c:ea)
▸ Internet Protocol Version 4, Src: 192.168.0.4, Dst: 192.168.0.7
▸ Transmission Control Protocol, Src Port: 54313, Dst Port: 102, Seq: 31, Ack: 24, Len: 197
▸ TPKT, Version: 3, Length: 197
▸ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
▸ ISO 8327-1 OSI Session Protocol
▸ ISO 8823 OSI Presentation Protocol
▸ ISO 8650-1 OSI Association Control Service
▸ MMS

0000  d8 cb 8a 1e 7c ea cc 30  80 10 da 8b 08 00 45 00   ....|..0 ......E.
0010  00 ed 29 1f 40 00 80 06  4f 90 c0 a8 00 04 c0 a8   ..).@... O.......
0020  00 07 d4 29 00 66 cc 2a  fe f5 78 0f c5 f4 50 18   ...).f.* ..x...P.
0030  ff e7 c8 6e 00 00 03 00  00 c5 02 f0 80 0d bc 05   ...n.... ........
0040  06 13 01 00 16 01 02 14  02 00 02 33 04 80 80 00   ........ ...3....
0050  03 34 02 00 01 c1 a4 31  81 a1 a0 03 80 01 01 a2   .4.....1 ........
0060  81 99 81 04 80 80 00 03  82 04 00 00 00 01 a4 23   ........ .......#
0070  30 0f 02 01 01 06 04 52  01 00 01 30 04 06 02 51   0......R ...0...Q
0080  01 30 10 02 01 03 06 05  28 ca 22 02 01 30 04 06   .0...... (."..0..
0090  02 51 01 61 66 30 64 02  01 01 a0 5f 60 5d 80 02   .Q.af0d. ..._`]..
00a0  07 80 a1 07 06 05 28 ca  22 02 03 a2 07 06 05 29   ......(. "......)
00b0  87 67 01 01 a3 03 02 01  0c a6 07 06 05 2b ce 0f   .g...... .....+..
00c0  01 08 a7 03 02 01 00 be  32 28 30 06 02 51 01 02   ........ 2(0..Q..
00d0  01 03 a0 27 a8 25 80 02  40 00 81 01 0a 82 01 0a   ...'.%.. @.......
00e0  83 01 14 a4 16 80 01 01  81 03 05 fb 80 82 0c 03   ........ ........
00f0  ce 1c 00 00 00 02 00 00  40 fd 18                 ........ @..
```

FIGURE 3. MMS message exchanges between IEC 61850 client and server without security features.

are fully implemented without TLS security at transport profile results in a reasonably secure system. When E2E security is implemented with TLS security results in a secure system.

III. IMPLEMENTATION AND EVALUATION

From the Section II, it can be noted that transport profile security is more important for securing the MMS messages. In this paper, for reducing complexity only transport profile security is implemented and evaluated.

In order to implement the IEC 62351-4 transport profile security for MMS messages a test setup consisting of an IEC 61850 client and IEC 61850 server is developed. The IEC 61850 client and server are emulated with the help of a commercial software. A SCD file is loaded on two computers A and B, which now emulates as an IEC 61850 server (IP:192.168.0.4) and IEC 61850 client (IP:192.168.0.7) respectively.

Figure 3 shows connection establishment between IEC 61850 client and server without any security. A TCP connection is established using ports 102 as per the IEC 61850 specifications for MMS messages without security. After the TCP connection establishment, MMS initiate-request and initiate-response messages are exchanged. Figure 3 gives the wireshark capture of the unsecure MMS exchanges between IEC 6180 client and server.

For establishing secure MMS message exchanges TLS connection between IEC 61850 client and server must be established. To implement TLS security in emulated IEC

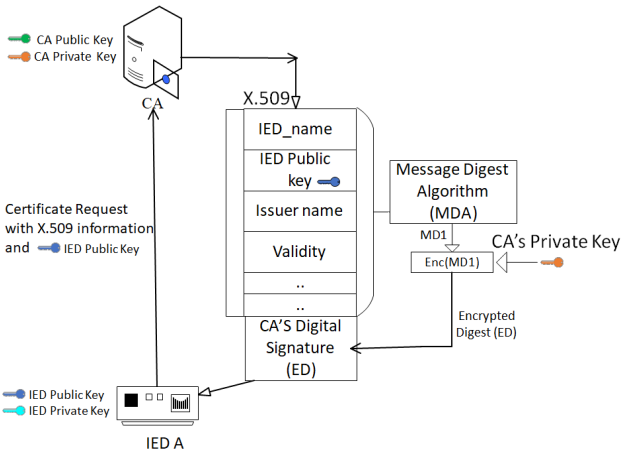

FIGURE 4. Certificate generation process.

61850 client and server, security module is configured with the security profile. The first step for configuring security profile is to setup certificates for client and server. Signed certificates '*ENT-PC.pem*' and '*beast-X99-s01.pem*' are generated by trusted CA for IEC 61850 server and client respectively. As shown in Fig. 4, the IEC 61850 client/server (IED) send a request to CA for issuing a certificate. The CA receives the request, formats it according to X.509 and signs with its private key using any public key algorithms such as RSA or ECDSA. In this paper, the signature for certificates is generated using RSA and ECDSA algorithms with different key sizes.

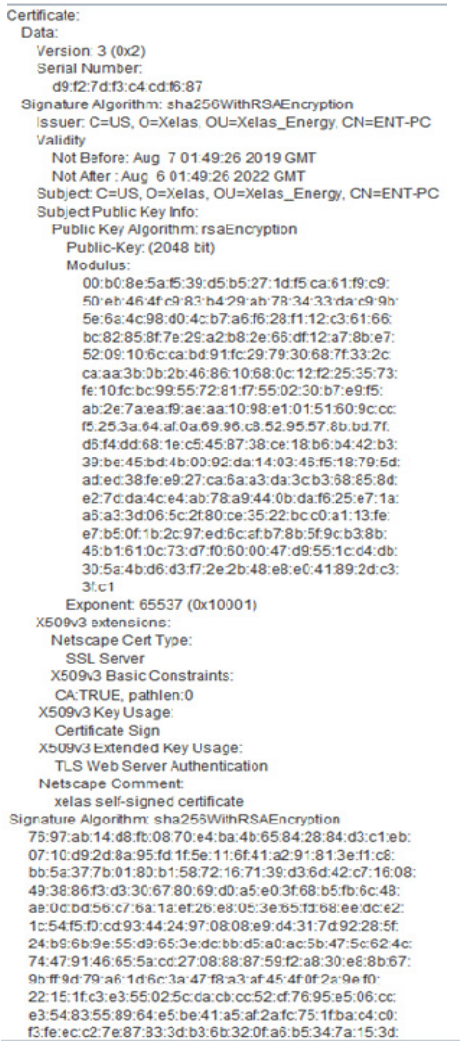

FIGURE 5. Certificate of IEC 61850 server in X.509 format.

Figure 5 shows encoded signed certificate '*ENT-PC.pem*' of IEC 61850 server generated by CA. It can be noticed that the certificate follows X.509 format and the algorithm used for generating signature is SHA256 with RSA. The '*beast-X99-s01.pem*' certificate is similar to '*ENT-PC.pem*' certificate.

These generated certificates are configured in emulated IEC 61850 client and server using the security module. Figure 6 (a) and (b) shows the configuration process of certificates in emulated IEC 61850 client and server respectively. Once the certificates are configured in emulated IEC 61850 client and server, a TLS connection can be established. Initially, client hello and server hello messages along with certificates are exchanged. Both the client and server verify the respective certificates. If the certificates verification process fails, the TLS connection is aborted. Table 3 presents the computation times required for verification of different certificates signed by different RSA and ECDSA algorithms with different key sizes and curves on a test system. The test system is an Intel(R) Celeron (R) with 4GB RAM.

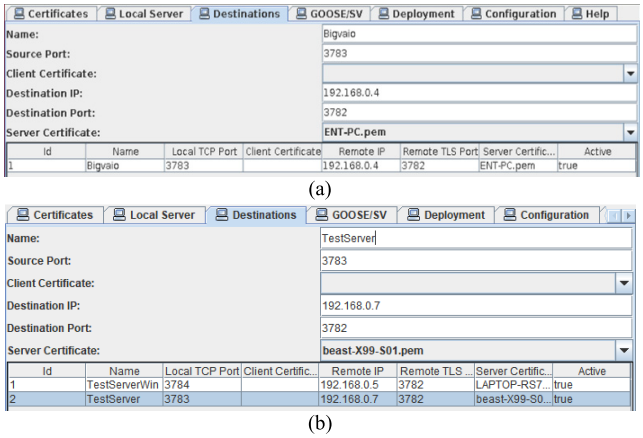

FIGURE 6. Certificate configuration in emulated IEC 61850 client and server.

TABLE 3. Certificate verification computational times for different digital signature algorithms.

Digital Signature Algorithm	Key size / Curve	Verification time (ms)
RSA	1024	7
	2048	7
	3072	8
	7680	8
	15360	13
ECDSA	secp224r1	8
	secp521r1	9
	prime192v1	8
	prime256v1	7
	brainpoolP384r1	10
	brainpoolP512r1	12
	brainpoolP384r1	10
	brainpoolP512r1	12

Figure 7 shows captured sequence of message exchanges for TLS connection establishment. After the certificate exchanges the server sends the cipher specifications. Here the cipher used is "*TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*".

The IEC 61850 client accepts the cipher suite by sending an acknowledgement message. Once the chipper suite is negotiated, it concludes the TLS process. Further message exchanges are encrypted by AES 256_GCM encryption algorithm. And all the message exchanges during this TLS session as encrypted by AES 256_GCM and shown as application data in Fig. 7. From Fig. 7 it can be noticed that the port no. 3782 is utilized for secure message exchanges as specified by the IEC 62351-4 standards.

The MMS message exchanges between emulated IEC 61850 server and client during the TLS session are shown as application data in Fig. 7. At the receiving side the encrypted messages are decrypted as normal MMS messages. The encryption of MMS messages provides confidentiality security requirement. In [20] authors provided the delays for establishing TLS session for different cipher suites listed in Table 1. The time delay for establishing TLS session is the time elapsed from sending of 'client hello' message till

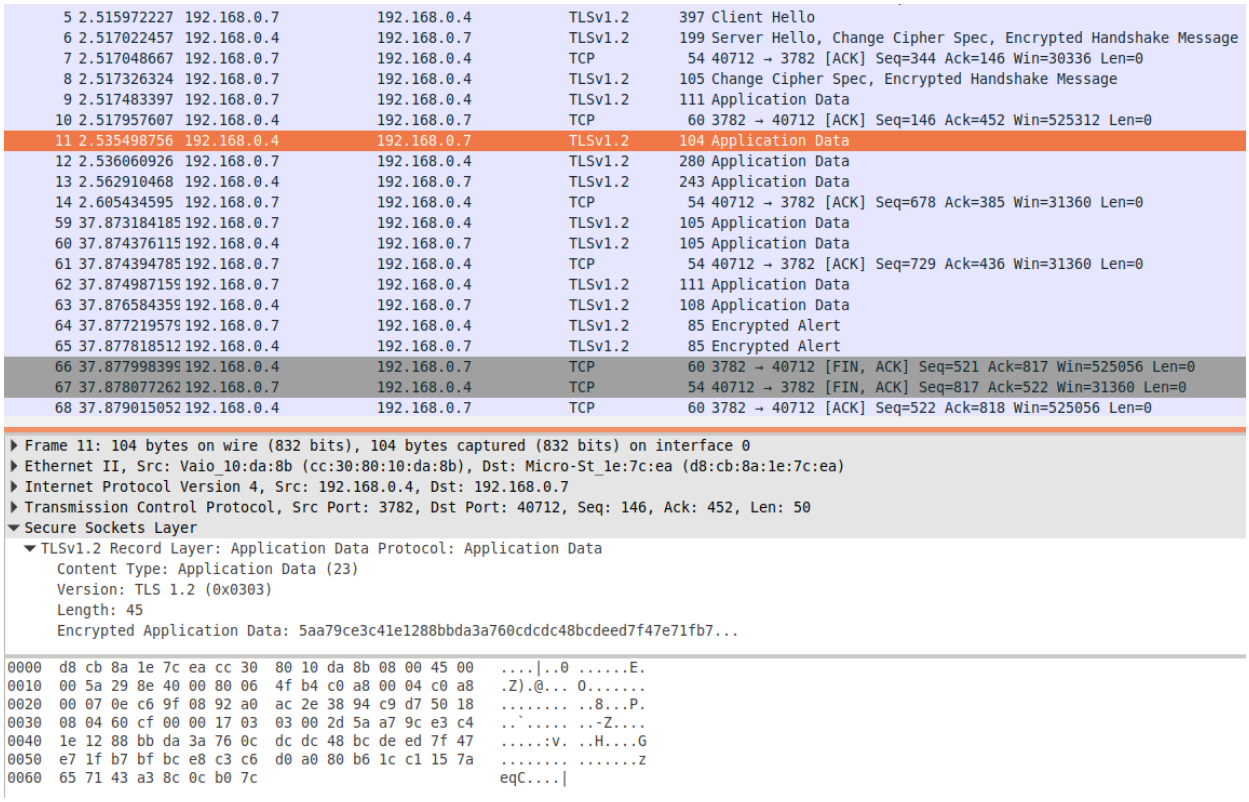

FIGURE 7. MMS message exchanges between IEC 61850 client and server with TLS security.

TABLE 4. Computational times for encryption and HASH algorithms in different cipher suites.

S.No	Encryption Algorithm	Encryption (ms)	Decryption (ms)
1	AES128-GCM	0.0084	0.0062
2	AES256-GCM	0.0086	0.0069
	HASH Algorithm	**Generation (ms)**	
1.	SHA_256	0.0106	
2	SHA_384	0.011	

receiving 'change cipher spec' message. This time delay includes the time required for processing different cryptographic algorithms listed in cipher suite and communication delays for exchanging TLS messages. In this paper, in order to obtain the computational performance of each algorithm individually, these algorithms are implemented in C language using OpenSSL libraries. Table 4 presents the computation times required for verification of different certificates signed by different RSA and ECDSA algorithms with different key sizes and curves on a test system. The test system is an Intel(R) Celeron (R) with 4GB RAM. The computational delays are obtained by sampling the CPU times at the start and end of C program using the clock() functions. The procedure is repeated several times and average values computational delays is reported.

Similarly, the computational times for implementing different encryption and HASH algorithms specified in Table 1 are shown in Table 4. From Table 3 and Table 4, it can be observed that computational times of different algorithms in different cipher suites specified for MMS messages well within the accepted limits for MMS messages. However, in legacy IEDs with computational powers the timing performance of different algorithms becomes very vital for successful implementation.

IV. CONCLUSIONS

This paper has implemented and demonstrated secure MMS message exchanges by implementing TLS security as specified in IEC 62351-4 standards. For implementing TLS, signed X.509 certificates were developed for both IEC 61850 client and server. The computational times for verifying digital certificates using different digital signature algorithms is presented. Secure IEC 61850 server and clients were emulated, and TLS connection based on IEC 62351-4 recommended security cipher suite was established successfully. The secure encrypted messages were successfully exchanged over the established TLS connection. This study provides insights on implementing IEC 62351-4 security specifications for IEC 61850 MMS messages and their performance before actual deployment is planned in the field.

REFERENCES

[1] I. Ali, S. M. S. Hussain, A. Tak, and T. S. Ustun, "Communication modeling for differential protection in IEC-61850-based substations," *IEEE Trans. Ind. Appl.*, vol. 54, no. 1, pp. 135–142, Jan. 2018.
[2] S. M. S. Hussain, T. S. Ustun, P. Nsonga, and I. Ali, "IEEE 1609 WAVE and IEC 61850 standard communication based integrated EV charging management in smart grids," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7690–7697, Aug. 2018.

[3] M. A. Aftab, S. M. S. Hussain, I. Ali, and T. S. Ustun, "IEC 61850 and XMPP communication based energy management in microgrids considering electric vehicles," *IEEE Access*, vol. 6, pp. 35657–35668, 2018.
[4] S. M. S. Hussain, A. Tak, T. S. Ustun, and I. Ali, "Communication modeling of solar home system and smart meter in smart grids," *IEEE Access*, vol. 6, pp. 16985–16996, 2018.
[5] S. M. Farooq, S. M. S. Hussain, and T. S. Ustun, "S-GoSV: Framework for generating secure IEC 61850 GOOSE and sample value messages," *Energies*, vol. 12, no. 13, p. 2536, Jul. 2019.
[6] *Cyber-Attack Against Ukrainian Critical Infrastructure*, document ICS Alert (IR-ALERT-H-16-056-01), Industrial Control Systems Cyber Emergency Response Team (ICSCERT), Feb. 2016.
[7] *Communication Networks and Systems for Power Utility Automation, 2.0*, Standard IEC 61850, IEC, 2013.
[8] *Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 4: Profiles Including MMS and Derivatives, 1.0*, Standard IEC 62351-4, IEC, 2018.
[9] S. M. S. Hussain, T. S. Ustun, and A. Kalam, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," *IEEE Trans. Ind. Informat.*, doi: 10.1109/TII.2019.2956734.
[10] R. Schlegel, S. Obermeier, and J. Schneider, "A security evaluation of IEC 62351," *J. Inf. Secur. Appl.*, vol. 34, no. 2, pp. 197–204, 2017.
[11] *Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 6: Security for IEC 61850, 1.0*. Standard IEC 62351-6, IEC, 2007.
[12] S. M. Farooq *et al.*, "Performance evaluation and analysis of IEC 62351-6 probabilistic signature scheme for securing GOOSE messages," *IEEE Access*, vol. 7, pp. 32343–32351, 2019.
[13] F. Hohlbaum, M. Braendle, and A. Fernando, "Cyber Security Practical considerations for implementing IEC 62351," in *Proc. PAC World Conf.*, 2010.
[14] D. Ishchenko and R. Nuqui, "Secure communication of intelligent electronic devices in digital substations," in *Proc. IEEE/PES Transmiss. Distrib. Conf. Expo. (T D)*, 2018.
[15] S. M. S. Hussain *et al.*, "Analysis and implementation of message authentication code (MAC) algorithms for GOOSE message security," *IEEE Access*, vol. 7, pp. 80980–80984, 2019.
[16] S. M. S. Hussain, S. M. Farooq, and T. S. Ustun, "A method for achieving confidentiality and integrity in IEC 61850 GOOSE messages," *IEEE Trans. Power Del.*, to be published, doi: 10.1109/TPWRD.2020.2990760.
[17] T. S. Ustun and S. M. S. Hussain, "An improved security scheme for IEC 61850 MMS Messages in intelligent substation communication networks," *J. Modern Power Syst. Clean Energy*, early access.
[18] J. Zhang, J. Li, X. Chen, M. Ni, T. Wang, and J. Luo, "A security scheme for intelligent substation communications considering real-time performance," *J. Mod. Power Syst. Clean Energy*, vol. 7, no. 4, pp. 948–961, Jul. 2019.
[19] O. Khaled, A. Marín, F. Almenares, P. Arias, and D. Díaz, "Analysis of secure TCP/IP profile in 61850 based substation automation system for smart grids," *Int. J. Distrib. Sensor Netw.*, 2016.
[20] M. G. Todeschini, G. Dondossola, and R. Terruggia, "Impact evaluation of IEC 62351 cybersecurity on IEC 61850 communications performance," in *Proc. 25th Int. Conf. Electr. Distrib. (CIRED)*, Jun. 2019.

TAHA SELIM USTUN (Member, IEEE) received the Ph.D. degree in electrical engineering from Victoria University, Melbourne, VIC, Australia.

He is currently a Researcher with the Fukushima Renewable Energy Institute, AIST (FREA), National Institute of Advanced Industrial Science and Technology (AIST), and leads the Smart Grid Cybersecurity Lab. Prior to that, he was an Assistant Professor of electrical engineering with the School of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, USA. His research interests include power systems protection, communication in power networks, distributed generation, microgrids, electric vehicle integration, and cybersecurity in smartgrids. He is a member of the IEEE 2004, the IEEE 2800 Working Groups, and IEC Renewable Energy Management Working Group 8. He has been invited to run special courses in Africa, India, and China. He delivered talks for the Qatar Foundation, the World Energy Council, Waterloo Global Science Initiative, and European Union Energy Initiative (EUEI). He has edited several books and special issues with international publishing houses. He is a Reviewer of reputable journals and has taken active roles in organizing international conferences and chairing sessions. He is an Associate Editor of IEEE Access and a Guest Editor of the IEEE Transactions on Industrial Informatics.

S. M. SUHAIL HUSSAIN (Member, IEEE) received the Ph.D. degree in electrical engineering from Jamia Millia Islamia (A Central University), New Delhi, India, in 2018.

He is currently a Postdoctoral Researcher with the Fukushima Renewable Energy Institute, AIST (FREA), National Institute of Advanced Industrial Science and Technology (AIST), Koriyama, Japan. His research interests include power system communication, cybersecurity in power systems, substation automation systems, IEC 61850 standards, electric vehicle integration, and smart grids. He was a recipient of the IEEE Standards Education Grant approved by the IEEE Standards Education Committee for implementing projects and submitting a student application paper, from 2014 to 2015. He is a Guest Editor of the IEEE Transactions on Industrial Informatics.