Performance evaluation of IEC 61850 MMS messages under cybersecurity considerations

Available online at www.sciencedirect.com
ScienceDirect
Energy Reports 8 (2022) 1189–1199
www.elsevier.com/locate/egyr

2021 8th International Conference on Power and Energy Systems Engineering (CPESE 2021), 10–12 September 2021, Fukuoka, Japan

Performance evaluation of IEC 61850 MMS messages under cybersecurity considerations

Taha Selim Ustun[a,*], S.M. Suhail Hussain[a], Akhtar Kalam[b]

[a] *Fukushima Renewable Energy Institute, AIST (FREA), Koriyama, 963-0298, Japan*
[b] *College of Engineering and Science, Victoria University, Australia*

Received 26 October 2021; accepted 8 November 2021
Available online 29 November 2021

Abstract

IEC 62351-4 standard is published to address cybersecurity vulnerabilities of IEC 61850 Manufacturing Message Specification (MMS) messages. This standard includes a set of cipher suites that are recommended for securing MMS messages. However, these are only a set of recommendations. There is no work in the literature that implements them on an IEC 61850 MMS message and reports the performances. In order to fill this importance knowledge gap, this short communication reports results of implementing cipher suites recommended by IEC 62351-4 on IEC 61850 messages. In addition to implementation details, real message exchanges are demonstrated with lab experiments. Finally, changing certificate and message sizes are reported. The results show that cipher suite selection is critical as some suites have 29.67 % smaller certificate size than others. The novelty of this short communication is showing details of IEC 62351 application and relevant changes on message sizes and structures of IEC 61850 MMS messages. There is no similar work or publication showing such procedures and results.

Peer-review under responsibility of the scientific committee of the 8th International Conference on Power and Energy Systems Engineering (CPESE 2021).

Keywords: Power system communication; Smart grid; IEC 61850; MMS message; IEC 62351-4

1. Introduction

Smart grid operation requires high volume of information exchanges [1]. IEC 61850 is utilized to achieve interoperability between different devices present in electrical networks [2–4]. Recent cyberattacks showed that power systems are vulnerable to data manipulation attacks [5,6] and IEC 61850 standard does not address cybersecurity issues [7]. IEC 62351 standard is published to mitigate cybersecurity vulnerabilities of IEC 61850 standard [8–10]. Part 6 of IEC 62351 deals with well-known Generic Object-Oriented Substation Event (GOOSE)

* Corresponding author.
E-mail address: selim.ustun@aist.go.jp (T.S. Ustun).

https://doi.org/10.1016/j.egyr.2021.11.187

Peer-review under responsibility of the scientific committee of the 8th International Conference on Power and Energy Systems Engineering (CPESE 2021).

and Sampled Value (SV) messages [11]. Also, recent literature is rich with works that investigate cybersecurity of GOOSE and SV messages [12–17].

On the other hand, security of IEC 61850 Manufacturing Message Specification (MMS) messages is not investigated in detail. Part 4 of IEC 62351 recommends use of certain cipher suites during Transport Layer Security (TLS) session [8]. There are limited number of studies where authentication mechanisms regarding MMS message security are discussed [18,19]. A recent work has investigated implementation of IEC 62351-4 on IEC 61850 MMS messages and studied its performance [20]. However, in this paper, only one cipher suite has been implemented. The other recommended suites have not been implemented and investigated.

This short communication fills in this knowledge gap. Being an applied research paper, it shows how IEC 62351-4 recommended ciphers are implemented on IEC 61850 MMS messages. Lab experiments are run to capture real message exchanges to show-case IEC 61850 MMS messages and related TLS session details. Furthermore, certificate and message sizes for all cipher suites are reported. This is the contribution of this work to the body of knowledge as it has not been done before. The rest of this short communication is organized as follows: Section 2 gives a very brief overview of IEC 61850 MMS messages and recommendations of IEC 62351-4 to secure them. Section 3 implementation details and test results for different cipher suites. Finally, Section 4 draws the conclusions.

2. Overview of IEC 61850 and IEC 62351-4

IEC 62351-4 stipulates securing MMS messages at two profiles of protocol stack: application and transport. As shown in Fig. 1, the former consists of the top 3 layers of the stack while the latter is made up of bottom 4 layers.

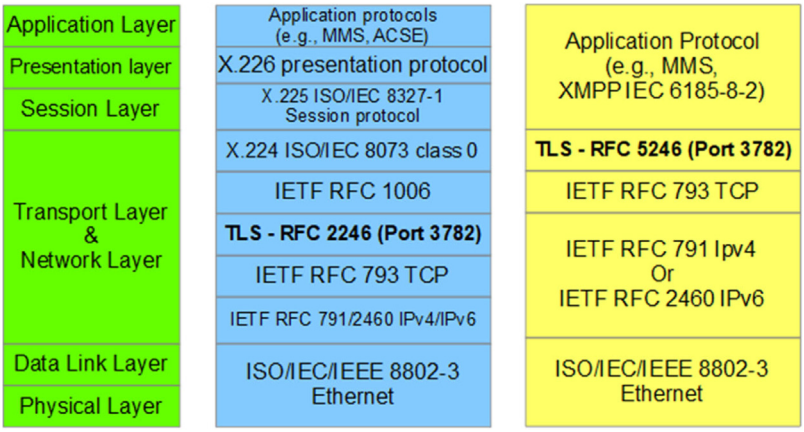

Fig. 1. Protocol stack for compatible and native T-security specifications for MMS messages [9].

For transport security (T-Security), use of TLS 1.2 is stipulated by RFC 5246. MMS messages are exchanged through port 3782 in two steps. Firstly, a handshake is performed to verify certificates of both parties and exchange a session key. With this key cipher suite that is going to be used for the actual data exchange is negotiated. Depicted in Fig. 2, this process is only performed once to establish the TLS session. Here, client and server exchange hello messages which is followed by exchange of individual certificates. This is performed to authenticate the parties, i.e. making sure they are who they claim to be. After this initial key is exchange which is, then, utilized to decide on the cipher suite that will be used for the rest of the session. Cipher suite means a set of cryptographic algorithms for all of (i) keys, (ii) digital signature, (iii) encryption and (iv) message authentication.

The list of recommended suites and their individual components are given in Table 1. For instance, initial key exchange process can be done with a selection of algorithms such as RSA, DH, DHE or ECDHE. On the other hand, digital signatures are only validated with RSA or ECDSA algorithms. Two versions of Secure Hash Algorithm (SHA 256-384) is utilized to generate a hash value which can be later used to authenticate the message contents. The message is encrypted with Advanced Encryption Standard's 128 or 256 (AES 128-256) version. In this fashion, TLS mechanism provides security for all four aspects mentioned above.

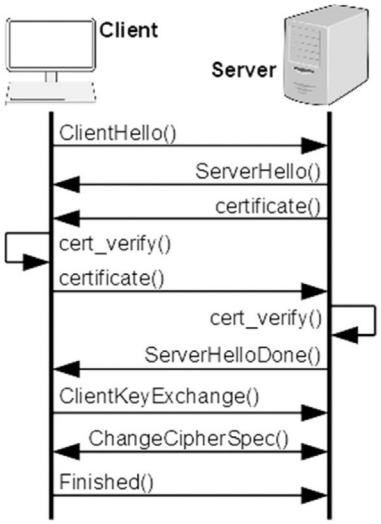

Fig. 2. Message exchanges for TLS establishment [20].

Table 1. IEC 62351-4 recommended cipher suites for MMS messages.

Key exchange		Hash function	Encryption algorithm	TLS version
Algorithm	Signature			
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

3. Implementation details and test results

In order to run lab tests, the procedure explained in [20] is followed. Two terminals emulating IEC 61850 client and server nodes are connected over TLS 1.2 protocol. The IEC 61850 client and server are emulated with the help of IEC 61850 emulation software. The corresponding system configuration description (SCD) file describing the capabilities of IEC 61850 client and server is generated and loaded to the IEC 61850 emulation software on two terminals to emulate IEC 61850 client and server.

The first step to exchange secure MMS messages is to establish a TLS connection between IEC 61850 client and server. To implement TLS in emulated IEC 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. Upon receiving the certificate request in X.509 format from the IEC 61850 client or server, CA signs the request using any of the public key algorithms such as RSA or ECDSA. In this implementation, three signed certificates ‘ENT-PC.pem’, ‘dhcert.pem’ and ‘ecdhcert.pem’ for IEC 61850 server and ‘beast-X99-s01.pem’ for IEC 61850 client are generated by trusted certificate authority (CA). ‘ENT-PC.pem’ is utilized when using the TLS_RSA_WITH_AES_128_CBC_SHA256 cipher suite. For the other cipher suites TLS_DH_XXX_XXX and TLS_ECDHE_XXX_XXX the certificates ‘dhcert.pem’ and ‘ecdhcert.pem’ certificates are utilized, respectively. Fig. 3(a) depicts the encoded signed certificate ‘ENT-PC.pem’ and Fig. 3(b) shows details of ‘ENT-PC.pem’ 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.

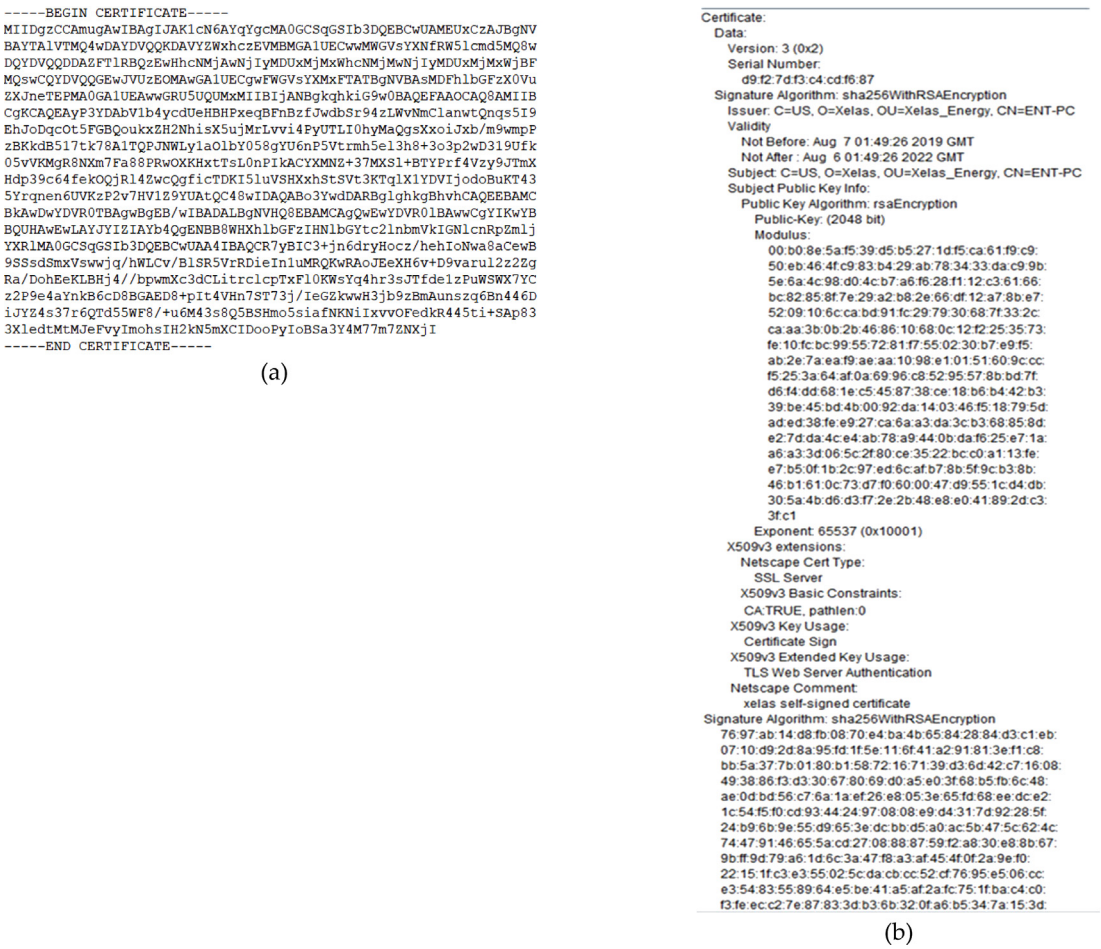

Fig. 3. Certificate of IEC 61850 server in X.509 format (a) encoded and (b) decoded.

These generated certificates are configured in emulated IEC 61850 client and server using the security module. Fig. 4(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.

However, this time, instead of a single cipher suite, all IEC 62351-4 recommended suites are implemented and validated. Same MMS message is relayed from server to the client and the messages are captured as shown in Figs. 5–14.

As shown, Fig. 5 shows a plain MMS message without any security features. For this reason, the network analyzer detects protocol as “MMS”, parses the message and shows its contents as “initiate request”. Also, from Fig. 5 it is noticed that the destination port for MMS message is the default ‘102’. For all the other captures. Figs. 6–14, protocol is shown as TLS1.2 proving that client and server are connected via secure transport layer as stipulated by IEC 62351-4. Furthermore, from Figs. 6–14 it can be noticed that the destination port for all the secure MMS messages is 3782 as specified by the IEC 62351-4 standards. Also, additional TLS establishment messages discussed in Fig. 2 are shown: Client Hello, Server Hello-Certificate, Client Key Exchange and Change Cipher Specs. The message captures are selected to show which cipher suites are utilized during TLS establishment, e.g. in Fig. 9 below cipher suite is used: TLS_DH_RSA_WITH_AES_128_CBC_SHA256.

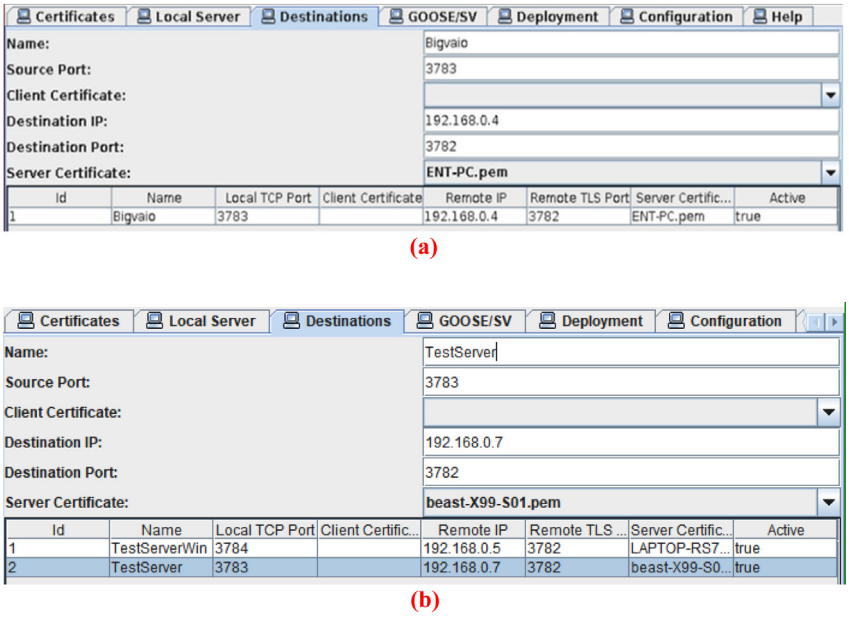

Fig. 4. Certificate configuration in emulated IEC 61850 client and server [20].

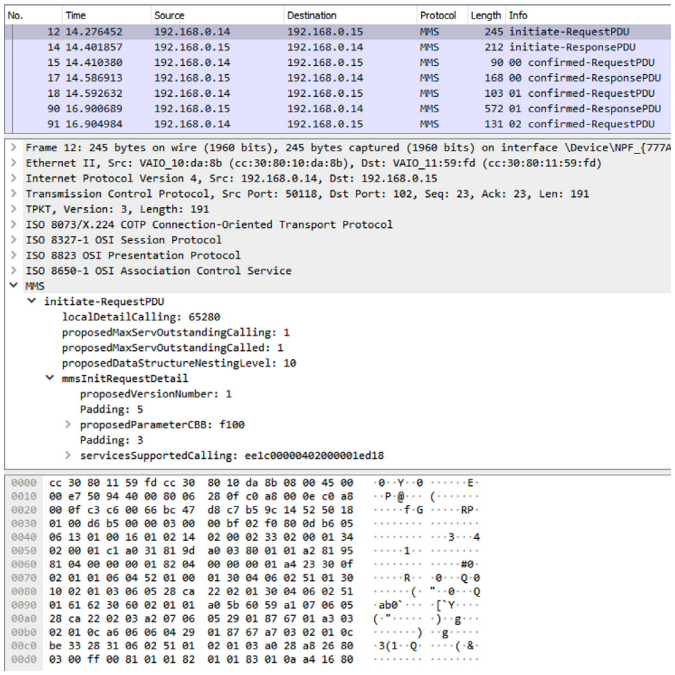

Fig. 5. Plain MMS message (No Security).

The very first message after this block is the actual MMS message that is sent by the server to the client. Since it is encrypted by AES128 or AES 256, network analyzer cannot parse the message or show its contents. It is only shown as applicated data, as a chunk of data.

The important finding of this work is to report changes in sizes of certificate and application data exchanges (ADE). As shown in Figs. 5–14 and summarized in Table 2, MMS messages that use different cipher suites as well

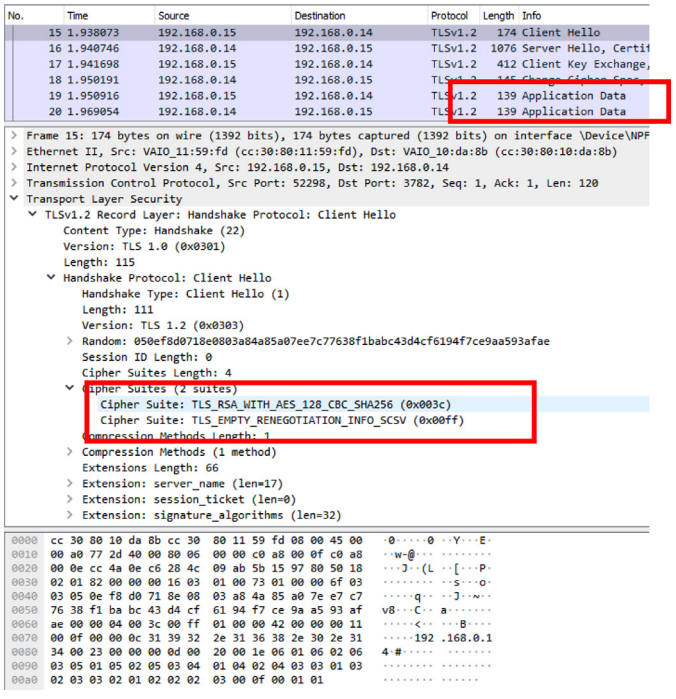

Fig. 6. TLS_RSA_WITH_AES_128_CBC_SHA25.

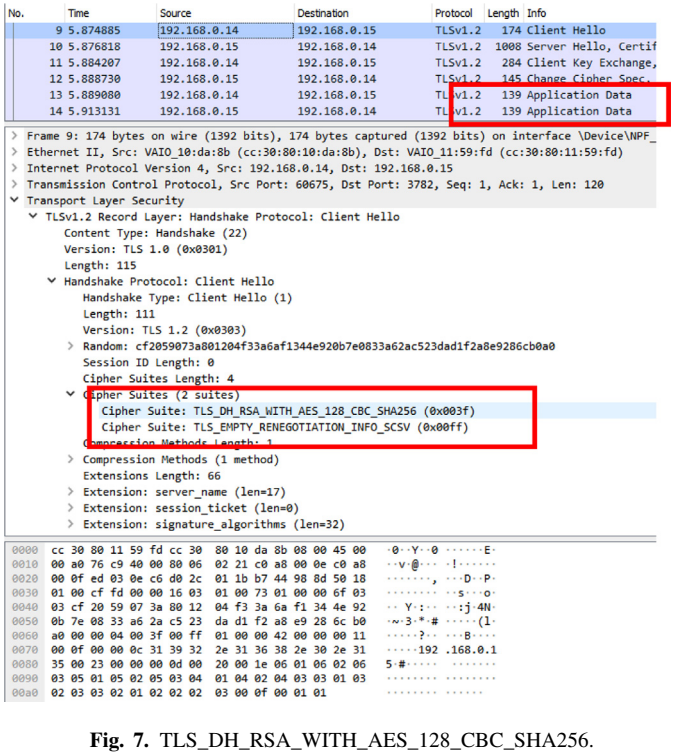

Fig. 7. TLS_DH_RSA_WITH_AES_128_CBC_SHA256.

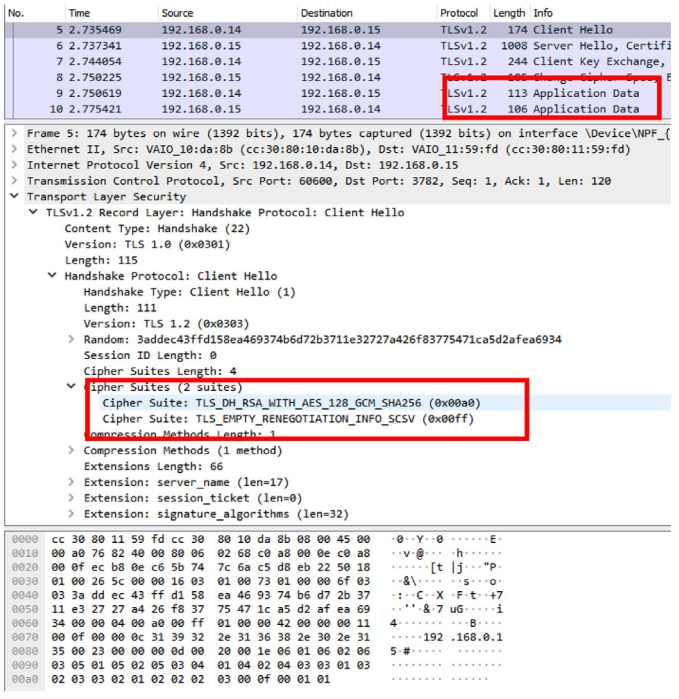

Fig. 8. TLS_DH_RSA_ WITH_AES_128_GCM_SHA256.

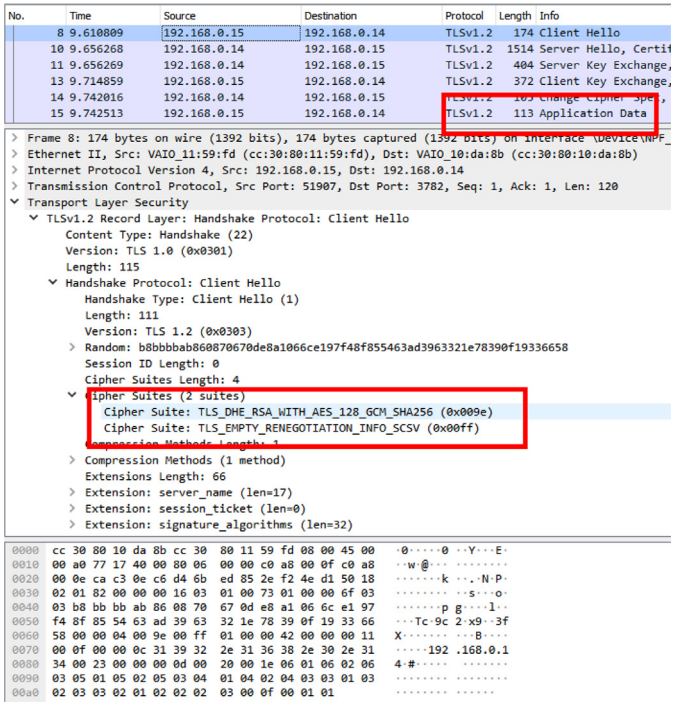

Fig. 9. TLS_DHE_RSA_ WITH_AES_128_GCM_SHA256.

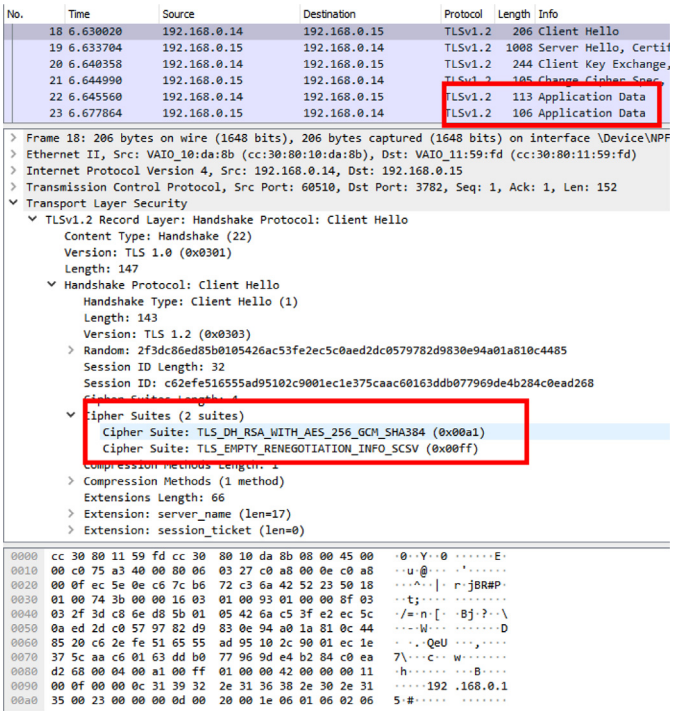

Fig. 10. TLS_DH_RSA_ WITH_AES_256_GCM_SHA384.

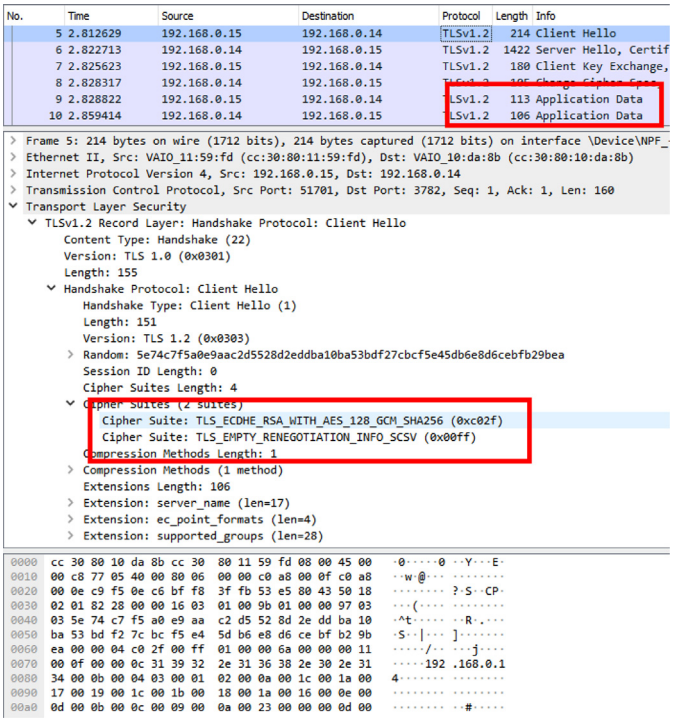

Fig. 11. TLS_ECDHE_RSA_ WITH_AES_128_GCM_SHA256.

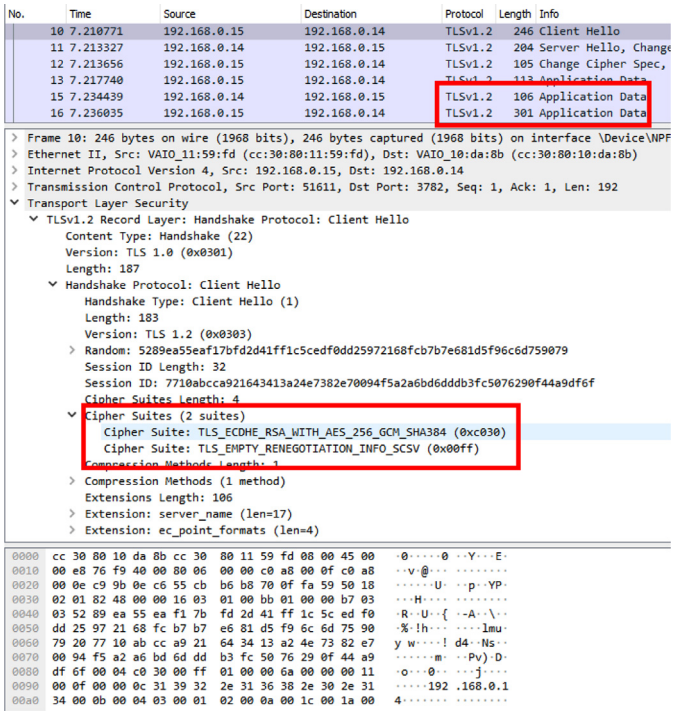

Fig. 12. TLS_ECDHE_RSA_ WITH_AES_256_GCM_SHA384.

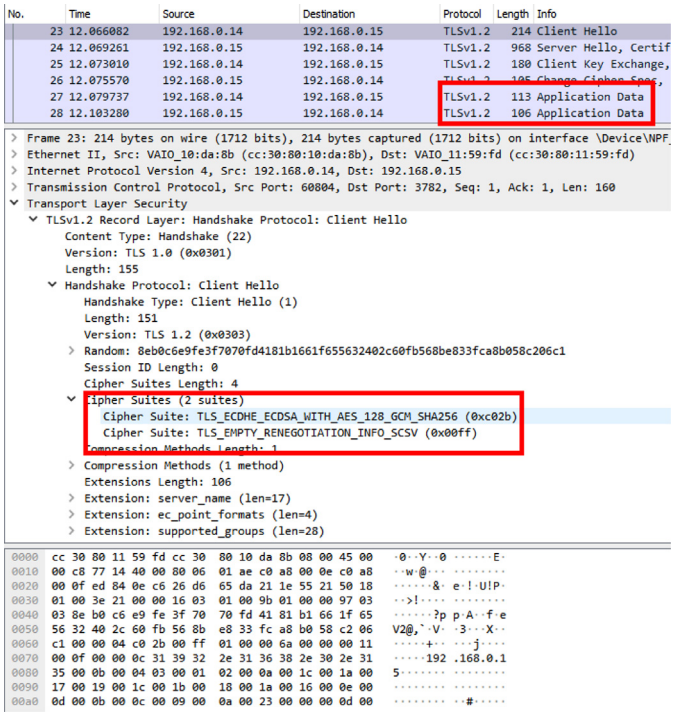

Fig. 13. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256.

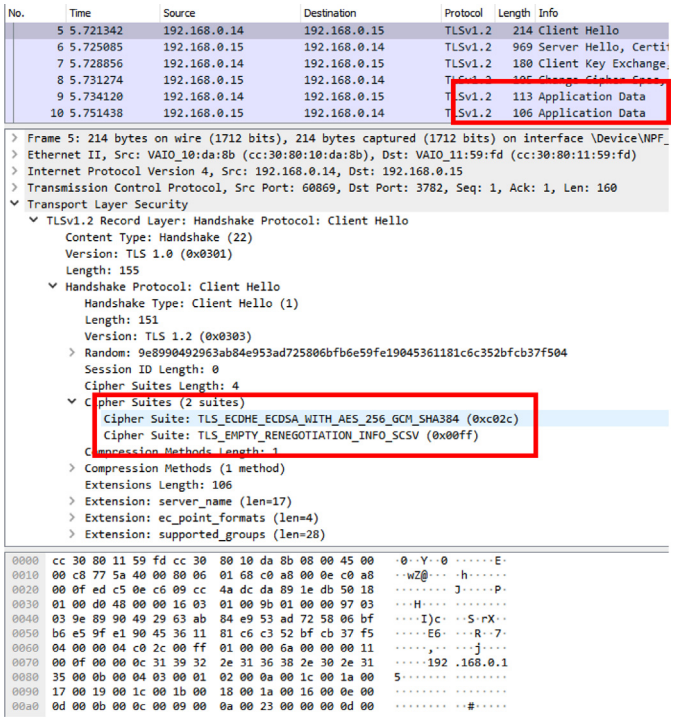

Fig. 14. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.

as unsecured MMS messages have different certificate and ADE sizes. An interesting finding is that all cipher suites had ADE sizes smaller than the unsecured MMS message. Reported certificate sizes vary, last two suites yielding the smallest size. That being said, certificates are only exchanged during TLS sessions establishment and is not used during IEC 61850 MMS exchanges. Their impact is not significant.

4. Conclusions

All cipher suites recommended by IEC 62351-4 have been implemented on IEC 61850 MMS messages and secure information exchanges have been demonstrated. TLS 1.2 has been used for creating a secure communication channel between the client and the server while X.509 certificates have been used for authentication purposes. Lab experiments have been conducted and real MMS messages secured with different cipher suites have been captured.

The results are presented in terms of full message bodies as well as different certificate and message sizes. It is found that use of cipher suites may decrease ADE size to 46.1% of unsecured message size. It is also discovered that cipher suite selection is critical as some suites have 29.67% smaller certificate size than others.

Table 2. Performance results for recommended cipher suites.

Cipher suites	Certificate size (bytes)	ADE size (bytes)
None	N/A	245
TLS_RSA_WITH_AES_128_CBC_SHA256	903	139
TLS_DH_RSA WITH_AES_128_CBC_SHA256	835	139
TLS_DH_RSA_ WITH_AES_128_GCM_SHA256	838	113
TLS_DHE_RSA_ WITH_AES_128_GCM_SHA256	903	113
TLS_DH_RSA_ WITH_AES_256_GCM_SHA384	838	113
TLS_ECDHE_RSA_ WITH_AES_128_GCM_SHA256	903	113
TLS_ECDHE_RSA_ WITH_AES_256_GCM_SHA384	903	113
TLS_ECDHE_ECDSA_ WITH_AES_128_GCM_SHA256	635	113
TLS_ECDHE_ECDSA_ WITH_AES_256_GCM_SHA384	635	113

In addition to validating cybersecurity recommendations of IEC 62351-4, this paper also gives application insights about how these recommendations impact IEC 61850 MMS sizes and performances. These results are useful for pre-testing security recommendations for MMS messages before the deployment is planned in the field. Both researchers and engineers active in this field will benefit from these application details and test results.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Ali I, et al. Communication modeling for differential protection in IEC-61850-based substations. IEEE Trans Ind Appl 2018;54:135–42.
[2] Hussain SMS, et al. IEEE 1609 WAVE And IEC 61850 standard communication based integrated EV charging management in smart grids. IEEE Trans Veh Technol 2018;67(8):7690–7.
[3] Aftab MA, et al. IEC 61850 And XMPP communication based energy management in microgrids considering electric vehicles. IEEE Access 2018;6:35657–68.
[4] Hussain SMS, et al. Communication modeling of solar home system and smart meter in smart grids. IEEE Access 2019;6:16985–96.
[5] Farooq SM, et al. S-GoSV: FRamework for generating secure IEC 61850 GOOSE and sample value messages. Energies 2019;12(13):2536.
[6] Cyber-Attack Against Ukrainian Critical Infrastructure. Industrial control systems cyber emergency response team (ICSCERT). Incident report. 2016.
[7] Communication networks and systems for power utility automation. 2.0. 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. IEC 62351-4, IEC. 2018.
[9] S.M.S. Hussain, Ustun TS, Kalam A. A review of IEC 62351 security mechanisms for IEC 61850 message exchanges. IEEE Trans Ind Inf 2020;16(9):5643–54. http://dx.doi.org/10.1109/TII.2019.2956734.
[10] R. Schlegel, Obermeier S, Schneider J. A security evaluation of IEC 62351. J Inf Secur Appl 2017;34(2):197–204.
[11] Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850, 1.0. IEC 62351-6, IEC. 2007.
[12] Farooq SM, et al. Performance evaluation and analysis of IEC 62351-6 probabilistic signature scheme for securing GOOSE messages. IEEE Access 2019;7:32343–51.
[13] F. Hohlbaum, Braendle M, Fernando F. Cyber security practical considerations for implementing IEC 62351. In: PAC world conference. 2010.
[14] D. Ishchenko, Nuqui R. Secure communication of intelligent electronic devices in digital substations. In: IEEE/PES transmission and distribution conference and exposition. 2018.
[15] Hussain SMS, et al. Analysis and implementation of message authentication code (MAC) algorithms for GOOSE message security. IEEE Access 2019;7:80980–4.
[16] S.M.S. Hussain, Farooq SM, Ustun TS. A method for achieving confidentiality and integrity in IEC 61850 GOOSE messages. IEEE Trans Power Deliv 2020;35(5):2565–7. http://dx.doi.org/10.1109/TPWRD.2020.2990760.
[17] Mikel Rodríguez, et al. A fixed-latency architecture to secure GOOSE and sampled value messages in substation systems. IEEE Access 2021;(9):51646–58.
[18] T.S. Ustun, Hussain SMS. An improved security scheme for IEC 61850 MMS messages in intelligent substation communication networks. J Mod Power Syst Clean Energy 2020;8(3):591–5.
[19] J. Zhang, Li J, Chen X, Ni M, Wang T, Luo J. A security scheme for intelligent substation communications considering real-time performance. J Mod Power Syst Clean Energy 2019;7(4):948–61.
[20] T.S. Ustun, Hussain SMS. IEC 62351-4 security implementations for IEC 61850 MMS messages. IEEE Access 2020;8:123979-123985.