# An Improved Security Scheme for IEC 61850 MMS Messages in Intelligent Substation Communication Networks

Taha Selim Ustun and S. M. Suhail Hussain

***Abstract*—Advanced connectivity in substations brings along cybersecurity considerations. Especially, the use of standardized data objects and message structures stipulated by IEC 61850 makes them much more vulnerable to unauthorized access and manipulation. In order to tackle these vulnerabilities, different methods are investigated by researchers all over the world. An important aspect of such efforts is the real-time performance consideration since power systems are bound by the rules of physics and all control/communication tasks need to be completed in a certain time frame. Security schemes for substation communication have been proposed in the recent literature. However, they must be improved to ensure a full security solution. Recently published IEC 62351 standard aims to fill this gap. Node authentication is vital for substation communication networks based on IEC 61850 to mitigate a variety of attacks such as man-in-the-middle (MITM) attack. This short communication presents a node authentication mechanism based on transport layer security (TLS) with certificates to address this knowledge gap. It also investigates the real-time performance by implementing the proposed scheme with Python.**

***Index Terms*—IEC 62351 standard, certificate authority, certificate-based authentication, cybersecurity, smart grid.**

## I. Introduction

A recent publication proposes a security scheme for intelligent substation communication based on IEC 61850 messages [1]. The proposed scheme follows the recommendations of IEC 62351 cybersecurity standard for generic object-oriented substation event (GOOSE) and sampled value (SV) messages [2], [3]. As for manufacturing message specification (MMS) messages, a novel certificateless security mechanism is proposed. However, to achieve full security within substations, some enhancements are needed. In its current form, the proposed scheme has some vulnerabilities such as unauthorized access, man-in-the-middle (MITM) attack and spoofing. Furthermore, the real-time performance of the proposed scheme is not reported based on actual implementation but computing power. In reality, operation systems and several other vital services take up finite computing power. Therefore, the real-time performance of developed schemes needs to be tested with actual implementations [4], [5].

This paper reports the vulnerabilities mentioned above and proposes a certificate-based security scheme. Finally, the real-time performance of the new security scheme is implemented and reported. The results not only show that it is feasible to use this new scheme in substations with strict timing requirements, but also emphasize the importance of actual implementation of the proposed algorithms during performance studies.

The rest of the paper is organized as follows. Section II sheds light on the vulnerabilities of the scheme developed in [1]. Then, Section III presents the improved security scheme for IEC 61850 MMS messages. It also includes the results of performance studies executed on a system which is similar to modern intelligent electronic devices (IEDs) in terms of computing ability, and Section IV presents the discussion. Finally, Section V draws the conclusion.

## II. Cybersecurity Vulnerabilities of Certificateless Security Mechanism

It is important to emphasize that the authentication achieved in [1] is message authentication, not node authentication. In other words, it is checked whether the received message is tampered with or not. There is no check on whether the nodes are legitimately identified [6]. The certificateless approach is presented based on the assumption that a device in a substation is able to acquire partial public and private keys, $p_{ID}$ and $d_{ID}$, from key generation center (KGC). After receiving this pair of keys, the device can generate a public-private key pair, $pk_{ID}$ and $sk_{ID}$, respectively. Then, it publishes its public key, $pk_{ID}$, in the substation.

This creates a very important loophole. As shown in Fig. 1, when an intruder gains access to the substation, it can request a partial key pair, $p_{ID}$ and $d_{ID}$, from KGC and generate a full key pair, $sk_{ID}$ and $pk_{ID}$. Then, it can use its own ID or another device's ID, i. e., spoofing. When this public key, $pk_{ID}$, is published in the substation, all of the other devices receive it as legitimate entity and further messages are en-

Manuscript received: February 19, 2019; accepted: September 30, 2019. Date of CrossCheck: September 30, 2019. Date of online publication: February 28, 2020.



T. S. Ustun (corresponding author) and S. M. S. Hussain are with Fukushima Renewable Energy Institute, AIST (FREA), Fukushima, Japan, and T. S. Ustun is also with Research Institute of the Energy Frontier, Tsukuba, Japan (e-mail: selim.ustun@aist.go.jp; Suhail.hussain@aist.go.jp).

DOI: 10.35833/MPCE.2019.000104

crypted and decrypted based on this more recent, fake public key, $fakepk_{ID}$. In Fig. 1, $S_{pk}$ is the public parameter and $S_{mk}$ is the master key.

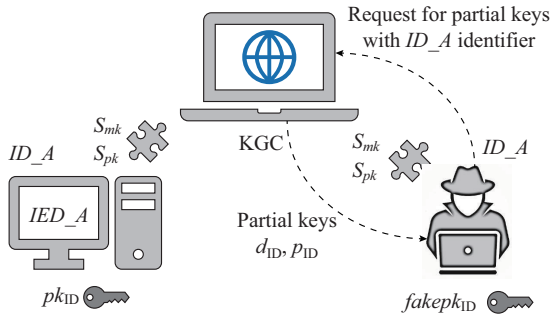


Fig. 1. Fake public key generation with false ID.

Since no mechanism is reported to mitigate this, neither in KGC nor in the substation, intruders can easily add themselves to the communication network as legitimate entities. This can lead to very big security issues. For instance, an intruder may pose as a storage device and take part in dispatch operations, while it has no ability or intention to support the power flow. Alternatively, an intruder may pose a measurement or protection unit, provide false sense of security and fail to operate in need.

Another important vulnerability stems from the fact that devices send their own public key and their own ID for verification. As shown in Fig. 2, a device can generate its public key with a certain ID yet pose to be some other devices during the verification. Since substation devices do not have the ability to verify whether a sent public key really belongs to the claimed ID, an MITM attack can easily be launched. As shown in Fig. 3, the hacker contacts *IED_M* and claims to be *IED_A*. It calculates the signatures with its own private key $C_{sk}$ (calculated with *ID_X*) with the hash value *Hash*(*M*). Upon receipt, the server calculates $H' = Ver(S', C_{pk})$ and compares this with the appended *Hash*(*M*) where $S'$ is the signature; $C_{pk}$ is the client's public key. As long as $H'$ and *Hash*(*M*) match, the authentication is successful. The authentication mechanism will continue by generating random numbers $N_{pm}$, $a$ and $b$ to establish a secure channel as outlined in [1]. In other words, the modified transport layer security (TLS) mechanism only checks whether the message is not tampered with and is intact as it is sent by other party, i.e., message authentication. It does not check whether the other party is actually what it claims to be, i.e., node authentication.

Although it is not mentioned in the published paper, a quick fix is disabling self-authentication by placing public keys physically in the devices. This will require an access to devices and regular update of the public keys of other legitimate devices. In essence, this is identical to a certificate-based mechanism, yet it is more complicated in practice. The reason is that the former requires updating public keys of all other devices in a given device whereas the latter requires updating the certificate in the device that it belongs to. Therefore, it is more efficient and convenient to implement a certificate-based security scheme.

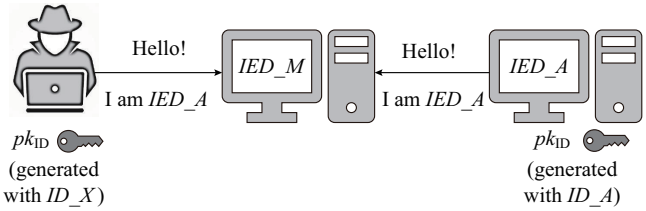


Fig. 2 False authentication with different public key, $pk_{ID}$.

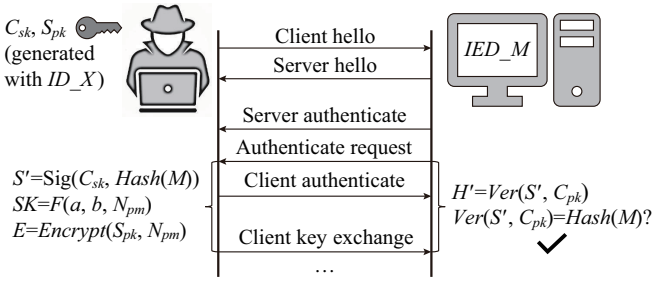


Fig. 3 Modified TLS handshake during false authentication.

## III. Certificate-based Security Scheme for Substation Communication

The solution of the above situation is to create a mechanism where different IEDs in the substation can mutually identify each other and whether the sent public key belongs to the sending entity. The proposed certificate-based mechanism can be used to that end. In this approach, a certificate authority (CA) signs the certificates to indicate that a device publishing its public key under a name is the particular device [7].

When implemented in substation environment, this mechanism requires all IEDs to crosscheck the identification of other entities with the CA [8]. If an intruder sends its own certificate to an IED for authentication, the said IED verifies the intruder's certificate with CA. If the certificate is not valid, the intruder is detected and the IED will not initiate or accept further communication.

Certificate serves the purpose of combining IED information such as name, serial number to its public key value. Unlike the certificateless scheme described above, in this case, this combination is performed by a trusted authority, CA, not the device itself. X.509 defines the format of a certificate which consists of subject name, version, certificate issuer information, serial number, IED public key, validity, and CA signature [9].

An IED generates its private-public key pair, $sk_{ID}$ and $pk_{ID}$, or receives it from an authorized location such as key distribution center. It sends a certificate signing request (CSR) to CA which includes its public key and the required information. As shown in Fig. 4, CA receives the request, formats it according to X.509 and signs it. Signing is to create a digest of the entire certificate, $MD_1$, and encrypt it with CA private key, which is only known to CA. This is appended at the end of the certificate as the encryption digest (ED).

Once an IED receives a signed certificate from CA, it will send the certificate to other devices in the substation for identity verification, i.e., node authentication. As shown in

Fig. 5, when *IED_M* receives a certificate from an entity claiming to be *IED_A*, it forwards this certificate to CA for verification. Firstly, CA checks whether the certificate exists in revocation list where the expired certificates are stored. If it does, a reject response is sent to *IED_M*, indicating that the received certificate is not valid. The storing of expired certificates mitigates the use of old legitimate devices for possible attacks.

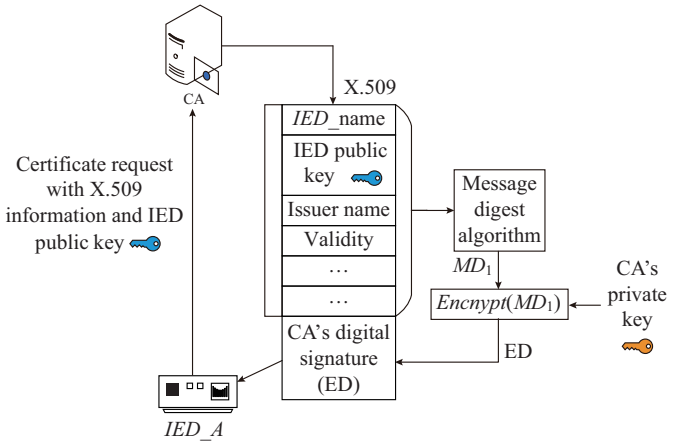


Fig. 4. Process of *IED_A* acquiring a signed certificate from CA.

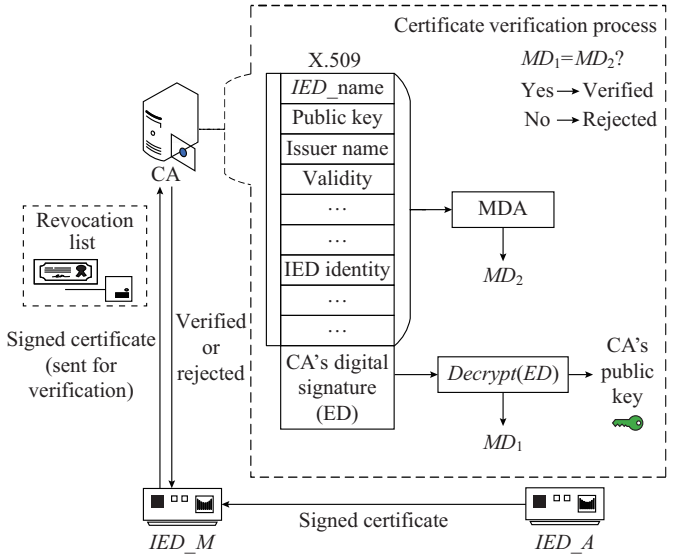


Fig. 5. Process of *IED_M* verifying *IED_A* certificate through CA.

If the received certificate has not been revoked, CA performs an integrity check on the certificate. It decrypts ED, $MD_1$=*Decrypt*(*ED*) using its own public key. Then, it generates a message digest of the received certificate, $MD_2$=*MDA* (*certificate*). If both digests match, $MD_1$=$MD_2$, it means that the certificate has not been tampered with and is legitimate. Therefore, CA sends a verification message back to *IED_M*.

The benefit of this approach is that *IED_A* identity and its public key are located inside the certificate. *IED_A* does not publish them within the substation in an arbitrary fashion. Therefore, upon successful verification, *IED_M* will try to decrypt the messages from *IED_A* with $pk_{IED\_A}$ inside the certificate. Since *IED_A* private key, $sk_{IED\_A}$ is only known to *IED_A*, the legitimate messages from *IED_A* will be received correctly. Even if a hacker captures this certificate during the transmission and establishes a connection with *IED_M*, its messages will never be accepted by *IED_M* since the hacker does not know $sk_{IED\_A}$.

Secondly, the certificates are issued and signed by CA using its private key. Therefore, no one can change the generated ED. Since ED stays intact, any change within the rest of the certificate can easily be caught by the CA during verification process. If the hacker tries to change the contents of the certificate, e.g. replacing *IED_A* public key with its own, this will create a discrepancy with certificate's digest $MD_2$ and CA's signature $MD_1$.

Thirdly, it is also important to note that this certificate verification is not repeated every time when *IED_A* wants to communicate with *IED_M*. It is only performed for the first time and subsequent message exchanges are just performed based on public-private key pair, $pk_{IED\_A}$ and $sk_{IED\_A}$. The certificateless approach discussed in Section II requires TLS connection to perform authentication before every session and this requires more time and energy.

After showing that certificate-based security mechanism solves the vulnerabilities, it is important to report real-time performance as well. Python-based implementations of client and server are utilized to investigate the required time for certificate verification [10], [11]. Firstly, public-private key pair is generated for an IED. Then, a certificate is issued as per X.509 format and is signed by CA. CA uses 256-bit secure Hash algorithm (SHA256) to create MDA. Encryption with CA's private key, *Encrypt*(*MDA*), is performed using different key sizes and elliptic curves of RSA and elliptic curve digital signature algorithm (ECDSA), respectively. This diversity in implementation is intended to contrast performances.

Table I shows all key sizes/curves and the corresponding sizes of CA's private key, CSR and actual certificate [12]. The last column shows the required time for CA to verify a certificate for that encryption and size combination. As shown, all results are less than 13 ms and the majority of the cases can be completed in 9 ms. Considering that time delay requirement for IEC 61850 MMS messages is 100 ms, this performance is excellent. Furthermore, TLS delay time reported in [1] is more than 31 ms and needs to be repeated at the beginning of every session. The proposed certificate-based solution can be implemented with RSA-1024 and will only require 7 ms for authentication. Furthermore, it is not needed to repeat before every session.

## IV. Discussion

KGC provides the partial public and private keys to any entity in substation communication network which put forwards the request. There is no mechanism to check if the entity is legitimate (i.e., it is really the entity it claims to be). Hence, the scheme discussed in Section II is prone to hackers as they can always provide the basic credentials of any other IED (say *IED_x*) and get partial keys from KGC to start a communication with other IEDs acting as *IED_x*.

TABLE I
COMPUTATION TIME FOR EXPLICIT CERTIFICATE VERIFICATION WITH DIFFERENT KEY SIZES OF RSA AND ECDSA

| Encryption | Key size/curve | Private key (byte) | CSR size (byte) | Certificate size (byte) | Verification time (ms) |
|---|---|---|---|---|---|
| RSA | 1024 | 891 | 745 | 1029 | 7 |
| | 2048 | 1769 | 1147 | 1371 | 7 |
| | 3072 | 2459 | 1496 | 1753 | 8 |
| | 7680 | 5973 | 3081 | 3321 | 8 |
| | 15360 | 11823 | 5701 | 5986 | 13 |
| ECDSA | secp224r1 | 278 | 627 | 895 | 8 |
| | secp521r1 | 436 | 838 | 1099 | 9 |
| | prime192v1 | 270 | 627 | 912 | 8 |
| | prime256v1 | 302 | 619 | 839 | 7 |
| | brainpoolP384r1 | 367 | 725 | 981 | 10 |
| | brainpoolP512r1 | 436 | 806 | 1070 | 12 |
| | brainpoolP384r1 | 367 | 741 | 985 | 10 |
| | brainpoolP512r1 | 436 | 826 | 1123 | 12 |

However, in the proposed scheme presented in Section III, each IED presents its credentials to CA and requests for a certificate. The CA verifies the legitimacy of particular IED and then signs (i.e., encrypt with its private key) the certificate request. Whenever this IED wants to establish a connection with other IEDs, it presents its certificate, which can be always verified through CA. Hence, the legitimacy of IED can be established through this mechanism.

In this scheme, the private key of CA and IED is not shared with any other party. This removes any threat of the disclosure of private keys unless the whole device is compromised. In this scheme, it is not just an assumption that private keys of CA and IED cannot be obtained by hackers.

The security scheme presented in this paper discusses only node authentication. On top of the proposed node authentication scheme, any message authentication scheme can be applied for ensuring the integrity of message. This is beyond the scope of this paper, but is a very viable item for future extensions.

For signing the certificate, the CA encrypts the CSR sent by an IED with its own private key. Hence, different encryption algorithms may be employed for signing (encrypting) the certificates. Similarly, for verification of certificates, CA first decrypts the signature employing the appropriate decryption algorithm.

Therefore, different encryption algorithms might be applied such as different variants of RSA and ECDSA. The computation time required for the verification of signatures for these variants is presented in Table I. It also presents the size of certificates generated for different variants of RSA and ECDSA. It is found that the sizes of certificates are on the order of few kilobytes and exchanged only once. The additional throughput added to the substation communication network is negligible and further investigation of sizes may not be required. On the other hand, certificate verification is performed more often and the reduction of verification time is an important item when resource-constraint IEDs are employed.

## V. CONCLUSION

Increased communication and control capabilities bring along undesirable cybersecurity vulnerabilities in intelligent substations. There is a need to successfully authenticate the nodes within a substation to avoid the intrusion and manipulation. Considering the real-time operation of power systems, this needs to be done fairly quick. Moreover, since IEDs have limited computing power, the solutions need to be lightweight.

In this paper, a certificate-based security mechanism is proposed for IEC 61850 MMS messages. The solution is robust as the certificates prevent unwanted access to the substation or spoofing by using the certificate of other devices. It is also efficient as the certificate verification is only required once, not for every session between the IEDs. The proposed solution is implemented with OpenSSL libraries with different algorithms and key sizes. The results show that the timing performance is excellent, and the proposed solution can be safely used in real substations.

## REFERENCES

[1] J. Zhang, J. Li, X. Chen *et al*., "A security scheme for intelligent substation communications considering real-time performance," *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 4, pp. 948-961, Jul. 2019.

[2] *Power Systems Management and Associated Information Exchange – Data and Communications Security Part 1: Communication Network and System Security – Introduction to Security Issues*, IEC Standard 62351-1, 2007.

[3] *Communication Networks and Systems in Substations Part 5: Communication Requirements for Functions and Device Models*, IEC Standard 61850-5, 2013.

[4] S. M. Farooq, S. M. S. Hussain, and T. S. Ustun, "Performance evaluation and analysis of IEC 62351-6 probabilistic signature scheme for securing GOOSE messages," *IEEE Access*, vol. 7, pp. 32343-32351, Mar. 2019.

[5] S. M. S. Hussain, S. M. Farooq, and T. S. Ustun, "Analysis and implementation of message authentication code (MAC) algorithms for GOOSE message security," *IEEE Access*, vol. 7, pp. 80980-80984, Jun. 2019.

[6] T. S. Ustun, S. M. Farooq, and S. M. S. Hussain, "A novel approach for mitigation of replay and masquerade attacks in smartgrids using IEC 61850 standard," *IEEE Access*, vol. 7, pp. 156044-156053, Oct.

2019.
[7] M. P. Barrett. (2018, Apr.). Framework for improving critical infrastructure cybersecurity. [Online]. Available: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11
[8] A. Lee. (2014, Sept.). Guidelines for smart grid cyber security. [Online]. Available: https://www. nist. gov/publications/guidelines-smart-grid-cybersecurity?pub_id=916068
[9] R. Housley, W. Polk, W. Ford *et al*. (2013, Mar.). Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile. [Online]. Available: https://datatracker.ietf.org/doc/rfc3280/?include_text=1
[10] *Python Interface to OpenSSL*. [Online]. Available: https://www. pyopenssl.org/en/stable/api.html
[11] *GitHub Site for Pyopenssl Library*. [Online]. Available: https://github.com/pyca/pyopenssl
[12] S. M. Farooq, S. M. S. Hussain, S. Kiran *et al*., "Certificate based authentication mechanism for PMU communication networks based on IEC 61850-90-5," *Electronics*. DOI: 10.3390/electronics7120370.

**Taha Selim Ustun** received the Ph.D. degree in electrical engineering from Victoria University, Melbourne, Australia. He was an Assistant Professor of electrical engineering with the School of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, USA. He is currently a Researcher with the Fukushima Renewable Energy Institute, AIST (FREA), Fukushima, Japan, where he leads the Smart Grid Cybersecurity Laboratory. He has edited several books and special issues with international publishing houses. He is a member of the IEEE 2004 and 2800 Working Groups and the IEC Renewable Energy Management Working Group 8. He is also a reviewer in reputable journals and has taken active roles in organizing international conferences and chairing sessions. He has been invited to run specialist courses in Africa, India, and China. He has delivered talks for the Qatar Foundation, the World Energy Council, the Waterloo Global Science Initiative, and the European Union Energy Initiative (EUEI). He is also an Associate Editor of IEEE Access and a Guest Editor of the IEEE Transactions on Industrial Informatics, Energies, Electronics, and Information journals. His current research interests include power systems protection, communication in power networks, distributed generation, microgrids, electric vehicle integration, and cybersecurity in smart grids.

**S. M. Suhail Hussain** received the Ph.D. degree in electrical engineering from Jamia Millia Islamia (a Central University), New Delhi, India, in 2018. He is a Postdoctoral researcher in Fukushima Renewable Energy Institute, AIST (FREA), Fukushima, Japan. He was a recipient of IEEE Standards Education Grant approved by the IEEE Standards Education Committee for implementing project and submitting a student application paper in 2014-2015. His research interest includes microgrid, power system communications and cybersecurity in power systems.