Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2016, Article ID 5793183, 11 pages
http://dx.doi.org/10.1155/2016/5793183

Research Article

Analysis of Secure TCP/IP Profile in 61850 Based Substation Automation System for Smart Grids

Omar Khaled, Andrés Marín, Florina Almenares, Patricia Arias, and Daniel Díaz

Department of Telematics Engineering, Carlos III University of Madrid, Madrid, Spain

Correspondence should be addressed to Omar Khaled; omar.khaled@alumnos.uc3m.es

Received 29 October 2015; Revised 22 March 2016; Accepted 30 March 2016

Academic Editor: Melike Erol-Kantarci

Smart grid is the term used to describe modern power grids. It aims at achieving efficient, sustainable, economic, and secure delivery of electricity supplies. In order to achieve these goals, communication between different components within the grid and control centers is required. In a rapidly growing world, the demands for substation automation are increasing. Recently, two trends have been changing Substation Automation Systems: IEC 61850 and the need for cybersecurity. IEC 61850 specifies very strict performance requirements for message transfer time. The security for the smart grid must be designed to satisfy both performance and reliability requirements. In this paper, we address a study about secure communication in the substation real-time environment, complying with the IEC 61850 specifications. We mainly focus on analyzing the proposed Secure TCP/IP profile for MMS, testing different cipher suite combinations and examining whether by applying TLS we can still achieve the strict performance requirements of IEC 61850 or not. As a result of the study, we propose a list of cipher suite combinations that should be used. The importance of this study lies mainly on future scenarios, because IEC 61850 is thought to support smart metering communications.

1. Introduction

Nowadays, investment in the electrical industry is massive, aiming at improving performance of power generation and distribution, increasing electricity production while reducing its cost, and increasing reliability and safety of electric grid systems. In order to achieve these goals, communication between different components within the grid and control centers is required. This is called *smart grid* [1]. Potential smart grid benefits can be classified into energy efficiency, financial, environmental, power reliability and safety, and cybersecurity. In order to achieve the most out of a smart grid, it is essential to transform its communications infrastructure into real-time distribution and transmission substations. The current Supervisory Control and Data Acquisition (SCADA) systems, located inside the substation, could not evolve to support next-generation intelligence [2]. Thus, the demands for substation automation (SA) are increasing, because substations are considered as critical infrastructure since these are needed for interconnecting many systems as shown in Figure 1.

Substation automation is a system that remotely monitors, coordinates, and controls energy distribution components installed in a substation. Recently, two trends have been changing Substation Automation Systems (SAS): the *61850 communication standard* introduced by the International Electrical Commission (IEC) with the aim of solving the interoperability among Intelligent Electronic Devices (IEDs) of different manufacturers within a single SAS and the need for *cybersecurity*. This international standard for communication has been developed in cooperation with several standardization organizations and manufacturers [3, 4]. It is the European standard that aims at achieving the *plug-and-play* concept. An IED is a microprocessor-based controller that performs several operational, control, and protective functions. Each IED is a group of logical nodes that can perform one or more subfunctions [5]. Utilizing 61850 IEDs along with IP routers and Ethernet switches, many power utilities are transforming their modem access and serial bus technology communication networks into IP-based ones. For that, it relies on state-of-the-art communication protocols. Hence, IEDs mainly confront security issues as

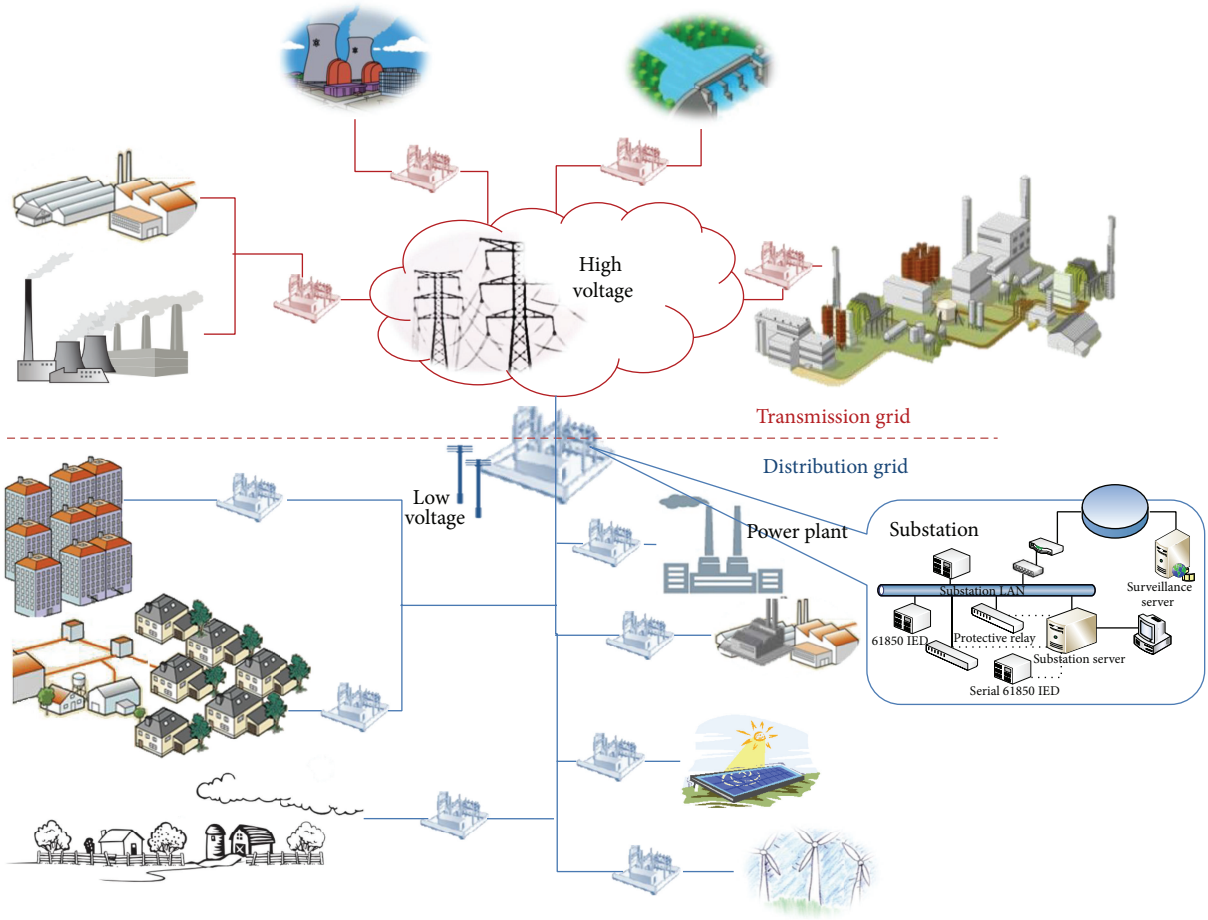

Figure 1: Next-generation substations in a smart grid.

malicious attacks, as they are critical components of the smart grid.

Thus, cybersecurity has become one of the dominant topics in electrical utilities. Security countermeasures have been specified in order to meet the strict requirements of power system operations. Nevertheless, the security for the smart grid must be also designed to satisfy both performance and reliability requirements. Severe damage to power system can be caused by any control command issued incorrectly due to any reason. Smart grids must withstand attacks without any loss of critical function. Generally, security requirements include three main properties: availability, confidentiality, and integrity. Availability ensures that resources can be used whenever needed. Confidentiality prevents any unauthorized access to information. Integrity prevents unauthorized access to modify the information. IEC 61850 provides itself with some sort of security in form of access control, but this is not enough to ensure private and secure system. Hence, more security protection must be provided. Message encryption could be an appropriate solution. However, encrypting messages results in longer processing time. Exchanging messages between substations should be secured, but still fast; therefore, the encryption must be studied carefully.

Other security mechanisms such as authentication should be also taken into consideration. However, when these security mechanisms are in use, it is important to consider their impact on the performance because the overhead may affect the end-to-end transmission time of the traffic. This fact together with the fact that IEC 61850 is a relatively new standard and it has been considered to revolutionize the global electricity distribution automation makes that huge amount of testing be done before full SASs with IEC 61850 become widely deployed.

For these reasons explained above, we describe the IEC 61850 and analyze part of the protocols defined in the framework, namely, the MMS (Manufacturing Messaging Specification) protocol suite on TCP/IP profile, whose security is provided by TLS (Transport Layer Security), in terms of security, performance, and cost. This analysis is essential as the framework is one of the main protocols used in smart grids and MMS ensures interoperability for smart grid communications. For that reason, many researchers propose the use of MMS for supporting smart metering service.

The organization of this paper is as follows. Section 2 introduces the IEC 61850 standard and describes the communication systems proposed. Section 3 discusses the security

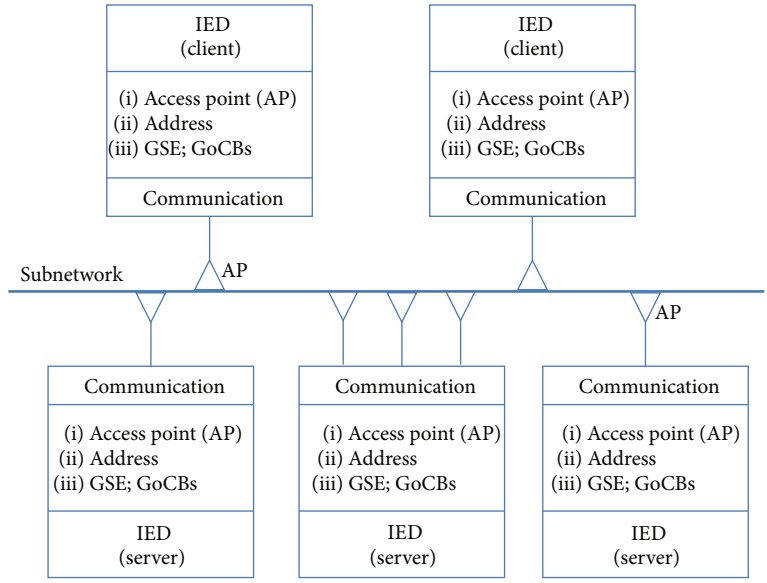

Figure 2: IEC 61850 communication network.

issues regarding the IEC 61850 standard. Section 4 describes the performance measurement setup and numerical results. Section 5 introduces some of the research that is related to our work. Finally, Section 6 concludes the paper and describes the future issues and challenges.

2. Background

2.1. The IEC 61850 Standard. IEC 61850 has been divided into ten different sections. The first five contain information about the standards concepts and ideology. The other sections are further divided into several parts containing information about services, data mapping, Abstract Communication Service Interface (ACSI), Substation Configuration Description Language (SCL), MMS, and testing. Parts seven and eight are the most important sections, because part 7 gives an overview of the communication architecture and interaction between IEDs (see Figure 2), describes relations between other parts of the whole standard, and defines how to achieve interoperability. Each device manufacturer, which is an IEC 61850 based communication network partner, has to adapt their products to the definitions and requirements given in the standard. The interaction between IEDs follows a client-server paradigm, but these can act as both roles. IEDs are communicated through local Ethernet network.

Finally, part 8 maps the time-critical and non-time-critical message services to MMS and to ISO/IEC 8802-3 frames, such as what we explained below.

2.2. Major Benefits of IEC 61850. A multimanufacturer SAS has always faced difficulties in converting between the communications protocols that could be used. So a universal protocol can be used to provide the following:

(1) *Interoperability*. It allows seamless communication among multivendor devices, easier configuration, higher reliability, and more safety. There are other protocols that can be used for SA, but none of them supports interoperability among IEDs as IEC 61850 does, for example, IEC 60870-5-101, Modbus, and Modbus plus.

(2) *Flexibility*. The standard supports different services with different performance requirements.

(3) *SCL Configuration*. IEC 61850 uses Substation Configuration Language to describe the whole substation system and each device in the network in a standardized way [6], according to user requirements. For that, it defines a set of abstract data and object models.

(4) *Lower Installation Cost*. Ethernet links based on OSI-7 are used by reducing wiring costs significantly.

2.3. Intelligent Electronic Device Modeling. An IED can be defined by one or more logical devices which are used to differentiate functions in a device. However, it is connected to the network by one network address. This virtualization is done to make the whole system and its configuration easier to model. It is easier to manage the functions when they are classified hierarchically [7].

Logical devices are further divided into one or more logical nodes (LN) that are constructed from data classes, each containing attributes. The logical nodes concept plays a major role in the standard. They are the backbone in modeling real devices and the basic objects that exchange information. They contain some obligatory predefined sets of data objects with specific attributes. These concepts have a logical structure and semantics that are related to real SA devices and tasks [8].

IEC 61850 predefines 92 logical nodes that can be extensible by manufacturers and 355 different data classes, which can be divided into seven categories: system information,

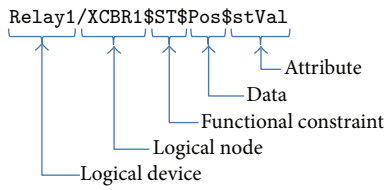

Figure 3: IEC 61850 object name structure [9].

physical device information, measurements, metered values, controllable data, status information, and settings. The data point reference converts the data into understandable form. The information can be understood just by inspecting its data point reference. Each object is named by its place and path in the information tree. This creates an easy way to refer to the object. In Figure 3, the name of the device is the first part, which is Relay1. The second part shows the logical node where the object is. The first letter in the logical node shows the group of the node, in this case, X, which signifies switchgear and the remaining letters CBR1 mean Circuit Breaker 1. The separation mark is "$" because the basic communication is mapped over MMS protocol. Functional constraint is used to specify which services can be used to access the following data. The Data part gives an understandable name to the data and finally its attributes [7].

IEC 61850 supports free allocation of functions, which means that any function may take place in any device that supports the standard. The standard achieves this by defining the LNs and Piece of Information for Communication (PICOM). PICOM is used to transfer information between two logical nodes. It contains the information to be transmitted, attributes for message performance requirement, and if needed, other requirements. PICOM uses address for point-to-point communication; hence, it cannot be used in broadcast or multicast procedures.

2.4. Communication Protocols of IEC 61850. IEC 61850 uses OSI-7 layer stack for communication and divides it into three groups; Manufacturing Messaging Specifications, TCP/IP, and Sampled Value (SV) transfer. MMS is an international standard (ISO9506). It was chosen in IEC 61850 because it supports the standard's complex naming system and services. It is particularly chosen because of its Virtual Manufacturing Device (VMD) model. Not only this but also MMS allows IEDs to act as clients and servers at the same time [7]. MMS defines communication messages sent between IEDs with the VMD model. The VMD model defines the objects that a server contains, the services that the client can use, and the behavior of the server when a client sends requests [10].

The MMS can be slightly modified to provide remote control communication services and smart metering. Not only that, but it can also provide the required complex information models to support the mapping of IEC 61850 abstract objects. Moreover, MMS is capable of providing workability as it supports both TCP/IP and OSI communication profiles.

As shown in Figure 4, there are seven types of messages and they are mapped into different communication stacks. Time-critical messages (i.e., they must be delivered within 4 milliseconds) such as GOOSE (Generic Object Oriented Substation Event) messages and SV messages used to transfer raw measured data values (types 1 and 4) are directly mapped to Ethernet which reduces the overhead and, hence, the processing time. The medium speed message, low speed message, file transfer functions, and the command message with access control (types 2, 3, and 5) are mapped to MMS protocol that operates over TCP/IP stack. The time synchronization messages (type 6) are broadcasted to all IEDs in substation using UDP/IP. Below we explain the Core ASCI Services stack, because this has been used for our security analysis.

(1) Abstract Communication Service Interface. The abstraction technique is one of the most powerful features in IEC 61850. Abstraction technique isolates services and information models from their underlying protocols. ACSI was defined to provide naming conventions in the communication of substations, a virtual substation image, real-time data access, device control, event reporting, data typing and discovery of data types, publisher/subscriber, and file transfer from the physical devices [8].

(2) Manufacturing Messaging Specifications. IEC 61850 specifies a method of communicating time-critical and non-time-critical data through local area networks by mapping the ACSI to MMS and ISO/IEC 8802-3 frames.

MMS [10] is a messaging system that is used for communicating real-time data and control information between devices in the grid. It runs independent from the application function that is being performed and the manufacturer of the devices. MMS supports the set of services and named objects that provide the mapping to IEC 61850 abstract objects and services, while Control model of ACSI is mapped to MMS read and write services. It is a mechanism through which the server can send data without an explicit request. However, an open TCP socket connection has to be initiated previously by the client.

The MMS server represents the IEDs that need to be controlled like those located in smart grid distribution networks. An MMS server can represent an individual Distribution Energy Resource (DER), a microgrid, or a home grid. Home grids are built from in-home private smart household appliances, DERs, and a Home Control and Management Center (HCMC) that controls and manages the devices. Microgrids are built from home grids, DERs, and a Regional Control and Management Center (RCMC) that controls and manages these home grids.

The MMS client represents the control center. The client and server roles can be interchanged; that is, at any point in time, any MMS entity can act as a client or a server. The entity that initiates the request to establish the association will become the client. One MMS client is capable of establishing several application associations with several servers. Afterwards, the MMS client can send requests to the server.

The message flow for the MMS Data Exchange between client and server is as follows: after the TCP three-way handshake between the MMS client and server, the Connection Oriented Transport Protocol (COTP) establishes a connection to transport ISO protocol over TCP by means

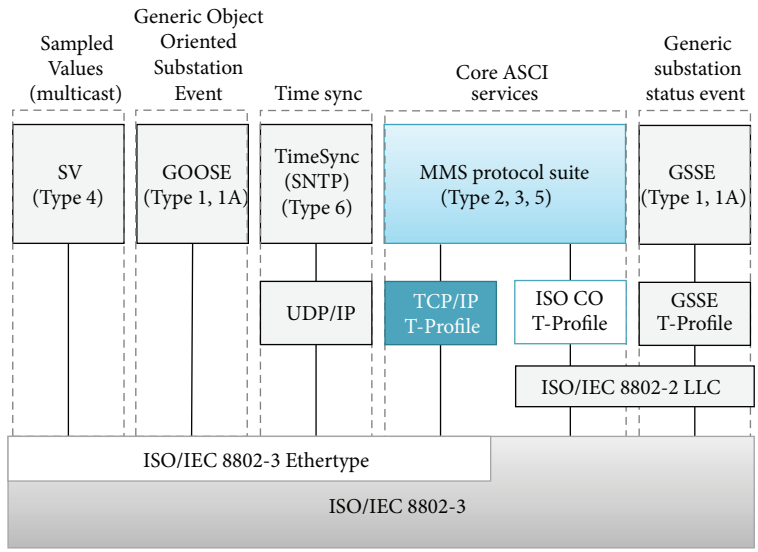

Figure 4: IEC 61850 service message types [8].

of the *Connection Request* message from MMS client and *Connection Confirm* message from MMS server (i.e., *Connection Setup* phase). Afterwards, an *MMS Initiation/Association* phase begins. The MMS `INITIATE-REQUEST` is mapped onto AARQ (Application Association Request) of the Association Control Service Element (ACSE) layer. The MMS server replies with the `INITIATE-RESPONSE` message, mapping it onto Application Association Response (AARE) of the ACSE layer. Both messages are transported over COTP Data TPDU (Transport Protocol Data Unit). After the MMS client receives the `INITIATE-RESPONSE`, both MMS parties are associated and can begin the *MMS Data Exchange* phase, through *MMS Request* and *MMS Response* messages.

MMS offers several services such as *Read Service* that uses the V-Get function in order to transmit the current value of a real variable, *Write Service* that uses the V-Put function to replace the current value of the real variable, and *Define Named Variable Service* that creates a new Named Variable Object that will be assigned real data.

There are two transport profiles (T-Profile) that can be used by the client/server, TCP/IP, or ISO. The TCP/IP T-Profile uses ISO Transport Service on top of the TCP (RFC1006) [11], ICMP (RFC792) [12], and TCP (RFC793) [13]. The ISO CO T-Profile uses Connection Oriented Transport (ISO8072). MMS does not have any built-in security and, accordingly, security measures are left to the TLS protocol. These protocols are used on the physical interface that can use several solutions; for example, wireless technologies would be possible.

2.5. Communication Performance Requirements. The performance requirements are specified for allowed message transfer time; therefore, the requirements are defined per message; hence, they are independent of the substation size. IEC 61850 specified several types of performance requirements presented in Table 1.

Table 1: Message type performance requirement [6].

Type	Application	Performance class	Requirements (transmission time allows)
1A	Fast messages (trip)	P1	10 ms
		P2/P3	3 ms
1B	Fast messages (other)	P1	100 ms
		P2/P3	20 ms
2	Medium speed		100 ms
3	Low speed		500 ms
4	Raw data	P1	10 ms
		P2/P3	3 ms
5	File transfer		>1000 ms
6	Time synchronization		(Accuracy)

2.6. Security Considerations in IEC 61850. Substations communicate with several networks such as remote monitoring and controlling systems; other substations and third-party data networks raise security concerns as they are a target for malicious cyberattacks. Security threats can be originated either outside or inside the electronic security boundary. Threats originated internally inside the electronic security boundary are usually introduced by the mistakes employees may make or by disgruntled employees. Mistakes such as inadvertently tripping generation or transmission assets directly affect the power system. However, employees may make mistakes without any intention of causing harms to the power system. There are also external threats from outside the electronic security boundary, such as hackers and terrorists, that exploits the security of the network in order to gain access

to computer assets of electric power systems. This can cause major damage to power supply [14].

Cybersecurity has become one of the most dominant topics for control systems in general and electrical utilities particularly. Securing IEC 61850 based communications has been one of the goals of the published technical specification IEC 62351 [15]. IEC 62351 is considered a good starting point to help secure 61850 communications. However, there are several shortcomings of the current standard and several challenges that must be addressed before the standard can gain wide acceptance and be implemented.

IEC 62351 provides different methods for securing the different communication types:

(i) MMS: securing MMS traffic is performed on the application and transport level. On the application level, peer authentication is performed by carrying authentication information in the ACSE AARQ and AARE PDUs. Authentication information comprises a X.509 encoded certificate, a timestamp, and a digitally signed time value. On the transport level, IEC 62351 refers to TLS. It specifies port 3782 for secure communications instead of the standard port 102. Besides, it specifies a set of recommended and mandatory cipher suites to be supported, at a minimum: TLS_DH_DSS_WITH_AES_256_SHA and TLS_DH_RSA_WITH_AES_128_SHA.

(ii) GOOSE/Sampled Values: security for this real-time traffic is limited to message authentication. Message authentication is defined by extending the GOOSE/SV PDUs with an authentication value that is calculated by signing a SHA256 hash using RSA. The exchange of certificate is not done as part of the messages; the receiving nodes must have X.509 encoded certificates preinstalled.

3. Security Analysis of IEC 61850

Performance impacts must be considered for any communication infrastructure before introducing encryption and/or message authentication. This is particularly true if asymmetric cryptography, real-time traffic, or systems with limited resources are involved. IEC 61850 separates the application from the communication by some abstract interface. Specific performance classes are defined for the different communication methods.

On one hand, GOOSE messages like interlocking and intertrip signals belong to the fast messages which must be transmitted within 10 ms. Some signals event must be transmitted within 3 ms. For SV, the standard defines several performance classes for raw data messages from digitizing transducers and digital instrument transformers.

On the other hand, the goal of security in IEC 61850 is to provide confidentiality, tamper detection, and message-level authentication for SCADA and telecontrol protocols that run over TCP/IP. Many information technology protocols have short duration connections, which allow the renegotiation of the encryption algorithms at connection re/establishment. However, within a telecontrol environment, connections tend to have longer durations, often "*permanent*." In this sense, special considerations are needed where only TLS 1.0 (or higher) shall be allowable. The symmetric keys shall be renegotiated based on a time period and a maximum allowed number of packets/bytes sent. This is an issue of PIXIT (Protocol Implementation Extra Information for Testing). The renegotiation values shall be configurable.

Although TLS has the message authentication code specified as an option, in IEC 61850, it is mandatory to use it in order to aid in countering and detection of man-in-the-middle attacks. Any implementation that conforms to the technical specification shall do the following:

(i) *Support More Than One Certificate Authority (CA) [16, 17]*. The connection shall be terminated if any entity failed to provide its certificate. The certificate exchange and validation shall be bidirectional. Certificate verification can be based upon CA or upon individual certificates.

(ii) *Be Able to Check the Local Certificate Revocation List (CRL) at a Configurable Interval*. Any connection established using a certificate shall be terminated if that certificate got revoked. However, an inability to access the CRL shall not cause the connection to be terminated.

In MMS, the security recommendations for the TCP T-Profile do not specify security recommendations for TCP, IP, or Ethernet. However, it specifies how to properly use TLS as well as the securing of RFC1006. In order to provide TLS, several aspects must be discussed: cipher renegotiation, certificate size, certificate revocation, and recommended cipher suites.

An implementation that conforms to the specification shall support *minimum-maximum renegotiation* if either 10 minutes has elapsed or five thousand ISO TPUs have been sent from the previous renegotiation. A minimum-maximum certificate size of 8192 octets shall be supported. Connections must be terminated if one of the certificates used to establish the connection is revoked. The key exchange algorithms must support *a size of at least 1024 bits for the key.* Both RSA and Diffie-Hellman mechanisms shall be supported. For cipher suites, the suite *TLS_DH_DSS_WITH_AES_256_SHA* must be supported at a minimum. Table 2 shows the list of recommended cipher suite combinations.

4. Security Evaluation

As discussed in the previous sections, IEC 61850 communications can be divided into real-time communications (i.e., GOOSE and SV) and point-to-point communications (i.e., MMS). In this research, we focus mainly on analyzing the proposed Secure TCP/IP profile for MMS as follows:

ISO/IEC 8073 TP0,

RFC1006,

SSL/TLS,

TCP (RFC793),

Table 2: Recommended cipher suite combinations [7].

Key exchange		Encryption	Hash
Algorithm	Signature		
(1) TLS_RSA_		WITH_RC4_128_	SHA
(2) TLS_RSA_		WITH_3DES_EDE_CBC_	SHA
(3) TLS_DH_	DSS_	WITH_3DES_EDE_CBC_	SHA
(4) TLS_DH_	RSA_	WITH_3DES_EDE_CBC_	SHA
(5) TLS_DHE_	DSS_	WITH_3DES_EDE_CBC_	SHA
(6) TLS_DHE_	RSA_	WITH_3DES_EDE_CBC_	SHA
(7) TLS_DH_	DSS_	WITH_AES_128_	SHA
(8) *TLS_DH_*	*DSS_*	*WITH_AES_256_*	*SHA*
(9) TLS_DH_		WITH_AES_128_	SHA
(10) TLS_DH_		WITH_AES_256	SHA

IP (RFC791), ARP (RFC826),

Logical Link Control (ISO 8802),

Media Access Control (ISO 8803).

The main aim of our research is to evaluate the recommended cipher suites' performance and examine whether by applying TLS we can still achieve the very strict performance requirements of IEC 61850 or not.

We use OpenIEC61850 which is an open source implementation of the IEC 61850 standards series licensed under the LGPL. It has been developed by several institutes and is currently maintained by Fraunhofer ISE [18]. The library consists of MMS client and server and is written in Java. More information about the implementation can be found at [19].

We have extended the implementation to include security by adding SSL/TLS support through using Java SSL sockets and SSL certificates as the current OpenIEC61850 does not support any of these.

The messages that we use in the test are "`Get(variable)`" messages that read a certain MMS variable in the VMD model or, in other words, the server. The MMS variable is a virtual object that represents a mechanism for the client to access a real variable. It is considered to be the most important model of all MMS models.

To satisfy the minimum requirements specified in the specification, we use SSLv3 with X.509 certificates to achieve authenticity of clients and servers and to exchange a symmetric key that will be used to encrypt data flowing between the communicating parties. The client and server also decide upon a cipher suite to use. In our test, the client chooses a cipher suite to use and negotiates it with the server, and then the connection is established upon agreement. This cipher suite states the algorithms to be used (asymmetric key agreement, symmetric encryption, and integrity check). For instance, if the client chooses the following cipher suite (TLS_RSA_WITH_3DES_EDE_CBC_SHA), this means that the session key will be transmitted with RSA (asymmetric encryption, using the RSA public key from the server certificate), the data will be symmetrically encrypted with 3DES, and the integrity check will use the SHA-1 hash function.

One MMS client at one SAS connects to an MMS server at another SAS performing the TLS handshake and then starts transmitting `Get(variable)` requests. We perform the test two times; in the first time the client sends 10 requests, and in the second time it sends 1000 requests. We measure the handshake latency when using RSA keys of lengths 1024 and 2048 bits, respectively. We measure using the minimum size that must be supported, as well as the recommended 2048-bit length. Although it is recommended to use at least one CA, we use self-signed certificates in order to minimize the validation cost. There is a common misconception that certificates sold by commercial CAs are inherently more secure than self-signed ones.

The handshake latency is the time taken for the client to successfully connect to the server. It is measured from the client side. We also measure the time taken (request latency) to send the `Get(variable)` requests using different cipher suites. The request latency is the time taken by the client to send the request and receive the response from the server. The test was performed two times, one on machines running an Intel Core 2 Duo processor at 2.53 GHz (scenario A) and another on machines running two Intel Core 2 Duo processors at 2.20 GHz each (scenario B). These machines have similar features to IEDs being currently deployed.

Without applying TLS, the handshake latency is 196 ms for scenario A and 74.31 ms for scenario B. While by applying TLS, for scenario A, the handshake latency is 514.2 ms and 899.8 ms for keys of lengths 1024 and 2048 bits, respectively, for scenario B the handshake latency is 212.3 ms and 371.6 ms for the same key lengths. In all the previous cases, the connection is permanent, which means that the handshake is performed at first and then all the data is sent without the need for reestablishing the session. Since the generation of the shared key is extremely CPU intensive, the session is being reused as this requires less CPU operations (up to 80% less). Hence, this fulfills the security requirements of the specification.

For the request latency of 1 `Get(variable)` request, without applying TLS, the request latency is 1.244 ms and 0.3131 ms for 1 request for scenarios A and B, respectively, while by applying TLS, for scenario A, the request latency using cipher suite number 1 in Table 2 is 3.0153 ms. On the other hand, in scenario B for the same cipher suite, the request latency is 0.4742 ms.

Analyzing the cipher suites in Table 2, it is clear that suite number 3 uses the same server authentication algorithm, as well as the bulk encryption algorithm and hash function as suite number 5. The only difference is that suite number 5 uses Ephemeral Diffie-Hellman (DHE) algorithm for key exchange. The same applies for suites numbers 4 and 6.

We propose another list of recommended cipher suite combinations, presented in Table 3, that provide more security than the one proposed by the specification. This list recommended is based on the last NIST (National Institute of Standards and Technology) security recommendations [20]. These suites provide more security as they use DHE instead of DH and Cipher Block Chaining (CBC) bulk encryption algorithm that provides confidentiality and authenticity as well as RSA server authentication.

Figure 5 shows the request latency of one request using each cipher suite in Table 3.

Table 3: Our proposed cipher suite combinations.

Key exchange		Encryption	Hash
Algorithm	Signature		
(1) TLS_RSA_		WITH_RC4_128_	SHA
(2) TLS_RSA_		WITH_3DES_EDE_CBC_	SHA
(3) TLS_DHE_	DSS_	WITH_3DES_EDE_CBC_	SHA
(4) TLS_DHE_	RSA_	WITH_3DES_EDE_CBC_	SHA
(5) TLS_DHE_	DSS_	WITH_AES_128_CBC_	SHA
(6) *TLS_DHE_*	*DSS*	*WITH_AES_256_CBC_*	*SHA*
(7) TLS_DHE_	RSA_	WITH_AES_128_CBC_	SHA
(8) TLS_DHE_	RSA_	WITH_AES_256_CBC_	SHA

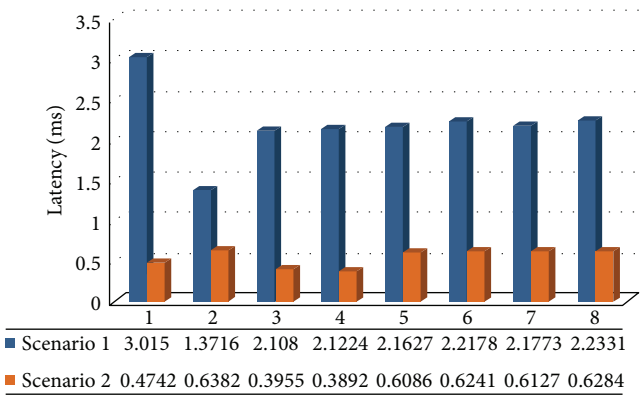

Figure 5: Request latency for each cipher suite.

Table 4 shows the request latency for each of the proposed cipher suites presented in Table 3 for 1 request. There is a negligible difference between the latencies measured when sending 10 requests and 1000 requests. This is because the CPUs used reach a very high crypto/AES throughput (hundreds of Mbits/second). However, the difference may be significantly large when using a resource-constrained system. It is clear that all the cipher suites satisfy the performance constraints of the specifications. However, when applying TLS, the request latency has increased by an average of 75% for both scenarios.

Furthermore, we expect extra computational cost to be introduced as a result of the process of establishing and communicating over a secure and encrypted channel. This extra computational cost can be divided into two parts: connection establishment and data transfer over established connection. Connection establishment introduces extra delay due to the additional round-trips, extra bandwidth consumption (network overhead) due to the exchange of certificates, and additional CPU usage as a result of the handshake. The measured additional CPU usage was around 60%. The cryptooperations took 90% of this SSL handshake. After the SSL session has been established, the transfer of data uses less CPU and network overhead. While network overhead is negligible, CPU overhead mainly depends on cryptography or in other words the cipher suite used. CPU overhead is quite low and can be neglected because AES hardware support is present in the CPUs used in this experiment. It is also expected to be present in the CPUs of IEDs.

Table 4: Request latency of one request.

Cipher suite	Scenario A		Scenario B	
	Latency (ms)	Overhead	Latency (ms)	Overhead
1	**3.0150**	142%	**0.4742**	52%
2	**1.3716**	11%	**0.6382**	102%
3	**2.1080**	69%	**0.3955**	26%
4	**2.1224**	72%	**0.3892**	24%
5	**2.1627**	74%	**0.6086**	94%
6	**2.2178**	79%	**0.6241**	99%
7	**2.1773**	75%	**0.6127**	96%
8	**2.2331**	80%	**0.6284**	100%

Table 5: Average CPU overhead for one request.

Cipher suite	Scenario A Overhead	Scenario B Overhead
1	34.85%	19.47%
2	15.85%	26.21%
3	24.36%	16.24%
4	24.53%	15.98%
5	25.14%	24.47%
6	25.63%	25.63%
7	25.16%	25.16%
8	25.81%	25.81%

Table 6: Average memory overhead by one request.

Cipher suite	Scenario A		Scenario B	
	Handshake	Data transfer	Handshake	Data transfer
1	17.48%	18.12%	17.65%	18.79%
2	13.23%	13.72%	13.84%	13.86%
3	23.72%	24.12%	23.93%	23.4%
4	21.43%	21.84%	21.78%	22.95%
5	14.89%	15.76%	15.12%	14.58%
6	13.74%	14.54%	14.45%	14.28%
7	13.42%	14.12%	13.92%	14.5%
8	13.48%	14.36%	14.98%	14.14%

Table 5 shows the average CPU overhead introduced by each one of the cipher suites. CPUs are expected to reach a crypto/AES throughput of several hundred MBits/s. Therefore, overhead in real-situation IEDs of smart grids should be lower as they transfer more data.

Table 6 shows the average memory overhead introduced by each of the cipher suites. It is believed to be negligible.

The results show that, using the current testing scenarios, available hardware, and proposed cipher suites, performance constraints specified by IEC 61850 could be successfully satisfied when introducing a SSL/TLS layer on top of the TCP. Since our proposed cipher suite combinations satisfied

the performance constraints, we can conclude that the cipher suite combinations recommended by the specification would also be satisfied, even for smart metering scenarios, whose end-to-end delay requirement would be from 500 to 1000 milliseconds. Hence, we recommend upgrading the recommended cipher suite combinations of the specification to our proposed suites as they provide more security while satisfying the performance constraints. Nevertheless, the performance on more limited devices should be evaluated, for example, smart meters.

5. Related Work

Security in smart grid has been discussed and numerous amount of research has been done to address privacy issues and security in cyber physical systems. There are several organizations, institutes, and research groups working on effectively securing smart grid communications. For instance, NIST in USA released several frameworks and guidelines for smart grid cybersecurity [21]. Smart Grid Information Security (SGIS) group, which is a subgroup of ETSI/CEN/CENELEC, and Smart Grid Task Force in the European Union as well are producing reports, requirements, and recommendations for data safety, data handling, and data protection in smart grids.

The authors in [22] provide an overview of security concerns and classify them into three categories, communication and device security, trust, and potential issues caused by smart grid's scale and complexity. In [23], a study about the difference between traditional power grid and the smart grid to identify new vulnerabilities is presented. In [24], an attacks classification on smart grid into network availability, information privacy, and data integrity is performed. The authors in [25] discuss key security technologies for a smart grid system, including public key infrastructures (PKI) and trusted computing elements. Finally, [26] summarizes the security requirements and possible threats in smart grid communications and surveys the solutions for them regarding privacy, integrity, authentication, and trusted computing.

Although huge amount of research on security in Internet is being carried out, only little was in the area of security in automation systems. IEC 61850 does not include these extensions in its current release. The authors of [27] focus on IEC 62351 to help secure IEC 61850. In case of securing GOOSE and SV data using IEC 62351, all three constraints apply the following:

(i) Protection and Control IEDs typically have limited computational power. Hence, security solutions should not require major hardware capabilities.

(ii) For GOOSE and SV messages, strict real-time constraints exist, 3 ms response time for GOOSE and sampling rate of 12 KHz for SV.

(iii) IEC 62351 specifies the use of digital signatures for authentication of broadcast GOOSE and SV packets.

On one hand, the performance evaluation done in [28] showed that neither software nor hardware solutions could satisfy the performance requirements of IEC 61850 for SV and GOOSE data.

On the other hand, in [29], the authors were focusing on applying security algorithms (i.e., MD-5, SHA-1, and RSA) to seek optimized security while satisfying the strict timing constraints for the GOOSE service defined in the standard. Their results show that only hash algorithms can be applied to the secure GOOSE service. The hash algorithm that they recommend is SHA-1. However, studies have shown that it is possible to find the collisions in it by using 2^{69} numbers of operations and this hash algorithm has officially been violated. It would be recommended to move to the variants of SHA-1 or to a more powerful algorithm such as one of the SHA-2 algorithms family (e.g., SHA-256).

The fact that IEC 61850 uses mainstream communication technology makes a variety of solutions available. Hence, further research can be done in order to provide security in IEC 61850 while complying with its performance requirements.

While in [28, 29] the authors focus on securing GOOSE and SV data, types 1 and 4, respectively, which are transmitted directly over Ethernet, our research is focused on analyzing the proposed Secure TCP/IP profile securing MMS messages, types 2, 3, and 5, respectively, which are transmitted over TCP. The Secure TCP/IP profile is based on introducing a SSL/TLS layer above the TCP.

Finally, in [30] the authors describe IEC 62351, give an overview of new use cases, and discuss potential enhancements of this standard in order to allow parallel sessions based on MMS using HTTP Digest or H.325 (i.e., an ITU-T based standard that describes security functions for the multimedia communication standard H.323).

6. Conclusions and Discussion

A substation is a critical infrastructure. The fact of applying the IEC 61850 standard to automation of a substation is therefore risky to security threats, which consist of attacks against physical facilities as well as cyber information, databases, and software applications. It becomes a critical factor to run the smart grid. Unlike normal Internet systems, power utility systems should guarantee the strict performance as well as reliability. It is important to find a security mechanism that satisfies both constraints.

In this paper, we conduct an experiment to measure the total time (processing and transmission) to transfer MMS Requests between clients and servers while applying TLS as recommended by the specification. The total time of a combination of hash algorithms and authentication algorithms including SHA-1 and RSA and DSA signature algorithms is measured in consideration of integrity and authentication services. The transmission time between nodes is measured by means of an open source IEC 61850 implementation (OpenIEC61850). We also measured the memory and CPU overhead introduced by applying TLS. The results suggest that TLS can satisfy the strict requirements of the IEC 61850 specification. The aim of security in smart grid is not just to secure the electronic security perimeter. It is about offering a more secure end-to-end architecture. Applying TLS when using IEC 61850 plays a vital role in enabling an

essential part of the end-to-end security architecture as well as allowing operators to control network devices, traffic, and also users. We suggest upgrading the recommended cipher suite combinations to your proposed combinations that offer higher level of security while satisfying the performance requirements.

Nevertheless, the model used in this study is not an accurate representation of a Substation Automation System since in a typical system more clients and servers are used and they do not reside in the same network. Also we only used one type of requests, `Get(variable)` requests.

There has been an average increase in latency of 75%. Therefore, a significant future work is required to further study and analyze the effect of applying TLS to consider several clients and servers residing in different networks as well as larger data exchange. Besides, it would be interesting to further study the effect of applying TLS to the communication between clients residing in end-user networks and servers in the smart grid, because one important service for this kind of communication is the smart metering service, which has been researched in different works [31–34].

MMS would support communication between smart meters and the meter data management systems in order to get instantaneous meter readings. A smart meter represents individual smart meter functionality, but it can also act as a data concentrator that aggregates information from several smart meters. MMS works according to the same point-to-point principle as DLMS/COSEM (Device Language Message Specification/Companion Specification for Energy Metering), integrated in IEC 62056 [32] as standard for metering applications. Both specifications work on peer-to-peer architectures. In [33], authors demonstrated that DLMS/COSEM and IEC 61850 outperform other languages and these have similar benefits. Although MMS TCP/IP profile was not defined to support any additional lower layer protocols, using IEC 61850 has the advantage that it can be used for other smart grid applications besides smart metering. Likewise, the interoperability solution can be applied to advanced metering infrastructure where a large number of smart meters from different vendors are used. DLMS/COSEM, in its turn, has limitations with respect to the bandwidth requirement in large scale considering that advanced distribution automation bandwidth requirement can potentially go into the several hundred kbps or even Mbps range, such as stated in [34]. This is because underlying technologies (e.g., G3 and PRIME) can only achieve data rate up to a maximum of 128 kbps.

For these scenarios, use of TLS cipher suites based on Elliptic Curve Cryptography (ECC) should be analyzed, because it could reduce overhead.

Furthermore, we used self-signed certificates in order to minimize the validation costs, but it is recommended to use more than one CA. Although 2048-bit-length RSA keys are secure enough, with AES, 256 is secure against any likely future technology and 512 is even much more secure. Therefore, these keys could be used in securing IEC 61850 messages. Also more secure SHA-2 cryptographic hash functions could be used instead of SHA-1 as they are stronger and better suited to security-sensitive applications such as digital signing.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work has been funded by the Spanish Ministry of Science and Innovation (MINECO) through the Project Incident Monitoring in Smart Communities (INRlSCO), TEC2014-54335-C4-2-R.

References

[1] ABB Group, *An Introduction to Smart Grids*, 2010.

[2] A. Leonardi, K. Mathioudakis, A. Wiesmaier, and F. Zeiger, "Towards the smart grid: substation automation architecture and technologies," *Advances in Electrical Engineering*, vol. 2014, Article ID 896296, 13 pages, 2014.

[3] R. E. Mackiewicz, "Overview of IEC 61850 and Benefits," Member, IEEE, 2006.

[4] R. P. Gupta, "Substation automation using IEC61850 standard," in *Proceedings of the 15th National Power Systems Conference (NPSC '08)*, IIT Bombay, December 2008.

[5] K. C. Budka, J. G. Deshpande, T. L. Doumi, M. Madden, and T. Mew, "Communication network architecture and design principles for smart grids," *Bell Labs Technical Journal*, vol. 15, no. 2, pp. 205–227, 2010.

[6] IEC, "Substation automation system configuration description language," IEC 61850-6, 2009.

[7] R. Mackiewicz, "Technical overview and benefits of the IEC 61850 standard for substation automation," in *Proceedings of the Power Systems Conference and Exposition*, pp. 623–630, Atlanta, Ga, USA, May 2006.

[8] IEC, "IEC 61850: Communication networks and systems in substations," 2003.

[9] ABB Group, "IEC 61850 Communication Protocol Manual," December 2013.

[10] System Integration Specialists Company (SISCO), "Overview and introduction to the manufacturing message specification (MMS)," Tech. Rep., System Integration Specialists Company (SISCO), Sterling Heights, Mich, USA, 1995.

[11] T. Rose and E. Cass, "ISO transport service on top of the TCP version: 3," RFC 1006, 1987.

[12] J. Postel, "Internet control message protocol (ICMP)," RFC 792, 1981.

[13] IETF, "Transmission Control Protocol (TCP)," RFC 793, IETF, 1981.

[14] D. Hou and D. Dolezilek, "IEC 61850—what it can and cannot offer to traditional protection schemes," *Journal of Reliable Power*, vol. 1, no. 2, pp. 1–11, 2010.

[15] IEC, "IEC 62351 Technical Specification," 2007.

[16] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile," RFC 5280, 2008.

[17] P. Yee, "Updates to the internet X.509 public key infrastructure certificate and Certificate Revocation List (CRL) profile," RFC 6818, 2013.

[18] Fraunhofer ISE, September 2015, http://www.ise.fraunhofer.de/en.

[19] Fraunhofer ISE, "OpenIEC61850," September 2015, http://www.openmuc.org/index.php?id=35.

[20] T. Polk, K. McKay, and S. Chokhani, "Guidelines for the selection, configuration, and use of transport layer security (TLS) implementations," NIST Special Publication 800-52, 2014.

[21] NIST, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0," 2014, http://www.nist.gov/smartgrid/upload/NIST-SP-1108r3.pdf.

[22] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security and Privacy*, vol. 7, no. 3, pp. 75–77, 2009.

[23] S. Clements and H. Kirkham, "Cyber-security considerations for the smart grid," in *Proceedings of the IEEE Power and Energy Society General Meeting*, pp. 1–5, IEEE, Minneapolis, Minn, USA, July 2010.

[24] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," in *Proceedings of the Military Communications Conference (MILCOM '10)*, pp. 1830–1835, IEEE, San Jose, Calif, USA, November 2010.

[25] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, 2010.

[26] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 998–1010, 2012.

[27] K. P. Brand, C. Brunner, and W. Wimmer, "Design of IEC 61850 Based Substation Automation Systems According to Customer Requirements," November 2005.

[28] F. Hohnlbaum, M. Braendle, and F. Alvarez, "Cyber security practical considerations for implementing IEC 62351," in *Proceedings of the PAC World Conference*, Dublin, Ireland, June 2010.

[29] H.-S. Yang, S.-S. Kim, and H.-S. Jang, "Optimized security algorithm for IEC 61850 based power utility system," *Journal of Electrical Engineering and Technology*, vol. 7, no. 3, pp. 443–450, 2012.

[30] S. Fries, H. J. Hof, and M. Seewald, "Enhancing IEC 62351 to improve security for energy automation in smart grid environments," in *Proceedings of the 5th International Conference on Internet and Web Applications and Services (ICIW '10)*, pp. 135–142, Barcelona, Spain, May 2010.

[31] G. T. Pham, *Integration of IEC 61850 MMS and LTE to support smart metering communications [M.S. thesis]*, University of Twente, 2013.

[32] IEC, "Electricity metering—data exchange for meter reading, tariff and load control—part 53: COSEM application layer," IEC 62056-53, IEC, 2006.

[33] S. Feuerhahn, M. Zillgith, C. Wittwer, and C. Wietfeld, "Comparison of the communication protocols DLMS/COSEM, SML and IEC 61850 for smart metering applications," in *Proceedings of the IEEE 2nd International Conference on Smart Grid Communications (SmartGridComm '11)*, pp. 410–415, Brussels, Belgium, October 2011.

[34] C.-W. Chao, Q.-D. Ho, and T. Le-Ngoc, "Challenges of power line communications for advanced distribution automation in smart grid," in *Proceedings of the IEEE Power and Energy Society General Meeting (PES '13)*, pp. 1–5, Vancouver, Canada, July 2013.