energies

Article

Secure Communication Modeling for Microgrid Energy Management System: Development and Application

Taha Selim Ustun and S. M. Suhail Hussain *

Fukushima Renewable Energy Institute, AIST (FREA), Koriyama 963-0298, Japan; selim.ustun@aist.go.jp
* Correspondence: suhail.hussain@aist.go.jp

Received: 19 November 2019; Accepted: 20 December 2019; Published: 21 December 2019

Abstract: As the number of active components increase, distribution networks become harder to control. Microgrids are proposed to divide large networks into smaller, more manageable portions. The benefits of using microgrids are multiple; the cost of installation is significantly smaller and renewable energy-based generators can be utilized at a small scale. Due to the intermittent and time dependent nature of renewables, to ensure reliable and continuous supply of energy, it is imperative to create a system that has several generators and storage systems. The way to achieve this is through an energy management system (EMS) that can coordinate all these generators with a storage system. Prior to on-site installation, validation studies should be performed on such controllers. This work presents a standardized communication modeling based on IEC 61850 that is developed for a commercial microgrid controller. Using commercial software, different terminals are set up as intelligent electronic devices (IEDs) and the operation of the EMS is emulated with proper message exchanges. Considering that these messages transmit sensitive information, such as financial transactions or dispatch instructions, securing them against cyber-attacks is very important. Therefore; message integrity, node authentication, and confidentiality features are also implemented according to IEC 62351 guidelines. Real-message exchanges are captured with and without these security features to validate secure operation of standard communication solution.

Keywords: IEC 61850; power system communication; cybersecurity; energy management

1. Introduction

In the past decade, power systems have witnessed a very rapid transformation, yet there are many unelectrified communities around the globe [1]. While some isolated communities in developed countries can be counted in this category, the bulk of this population lives in Sub-Saharan Africa, South Asia, and Latin America [2]. Traditional grid extension solution does not apply, as most of these locations are far from cities and costs of such projects are simply too high, i.e., prohibitive [3]. Isolated islands have inherent limitations and require scalable solutions. Reports show that electricity, or lack thereof, has great impact on quality of life, gender equality, and poverty eradication [4].

Traditionally, diesel generators are used in isolated communities. However, diesel generators have significant drawbacks such as high cost of fuel and its availability, environmental pollution, and regular maintenance and service costs. Alternatively, renewable energy source based-distributed generators are emerging [5]. They are less intrusive to the environment and have much less capital cost [6]. For over a century, bulk generation and transmission dominated the scene [7], and it was simply impossible for these sites to be electrified. However, with the advent of renewable energy-based generators, microgrids are picking up pace. Their ability to provide energy in small scale lends itself to geographically limited areas, e.g., communities in deserts or small islands. Intermittency and time-dependent generation profile of these systems require storage systems and coordination to supply reliable energy [8].

To address this gap, equipment that can track several generators and the load within a microgrid to coordinate charging and discharging of a battery energy storage system (BESS) has been developed [9]. The energy management system (EMS) needs to follow the load profile in a microgrid, estimate generation profile of the generators, and keep the battery charge at an appropriate level [10]. In addition, EMS is responsible for responding to system disturbances, such as generator loss or frequency deviation, to ensure the operation is as smooth as possible [11].

All these capabilities need to be integrated over a standard communication infrastructure for interoperability between different equipment. These are required to monitor the current status of the power network and to notify new operating conditions from EMS. There are many EMS algorithms in the literature [12–15]. However, these works only focus on the development and solution of an optimization equation. There is no detail about how such dispatch information is relayed. For instance, an EMS algorithm may be run, and as a result, storage needs to start discharging [16]. How this information will be sent from the EMS controller to the storage device is not discussed. It is assumed that there is a reliable and functioning communication solution that will enable transmission of such messages. There is some literature which focuses on developing communication architecture for an EMS [16–18]. However, these only focus on the information model development and not real implementations. Also, detailed communication models of the components are not given.

The main contribution of the work presented in this manuscript is to develop a real-life communication system that enables EMS components to communicate in a standard way. Its objective is to develop a communication infrastructure that can seamlessly connect different equipment from different vendors without any issues. In this regard, IEC 61850 has emerged as a promising solution for power utility automation domain since it proposes an object-oriented approach for information modeling of different components of the power system [19].

The object-oriented modeling approach helps in organizing data, configuring objects and making them consistent and interoperable. There is a consensus among research and industry stakeholders that IEC 61850 will emerge as the communication standard of the future smart grid [20,21]. The research focuses on extending IEC 61850 to model new components such as electric vehicles (EVs) [22], smart meters [23], different protection schemes [24], and fault current limiters [25]. Building on this trend, a standardized model needs to be developed for EMS controllers in microgrids.

This paper presents a standardized communication modeling of an EMS that is developed for a real microgrid. Individual components are developed with logical devices (LDs) and logical nodes (LNs). These individual models are combined to develop overall EMS modeling. Furthermore, data objects (DOs) are designated mapped to variables that are monitored in the microgrid. Generic object-oriented substation event (GOOSE) and manufacturing message specification (MMS) messages are configured to exchange information between microgrid components and the EMS controller. Further, the IEC 62351 cybersecurity considerations for securing these IEC 61850 GOOSE and MMS messages are implemented and results are demonstrated.

The rest of the paper is organized as follows: Section 2 shows the operation principles of the EMS controller that is modeled. Section 3 details the standard communication models that are developed and shows message exchanges for different scenarios. Section 4 discuss the implementation of IEC 62351 cybersecurity considerations for GOOSE and MMS messages. Section 5 gives future research directions and draws the conclusions.

2. Microgrid EMS Operation Principles

In this paper, a microgrid EMS controller for an off-grid island located in Southeast Asia is considered [11]. In this scenario, ample solar potential is envisioned. As shown in Figure 1, said microgrid consists of a diesel generator, photovoltaic (PV) system, battery system, and loads. The diesel generator operates in grid-forming mode and stipulates voltage and frequency. PV and battery systems are utilized to maximize renewable energy use. It is observed that for 250 kW of aggregated load, there is excess installed capacity; 225 kW diesel generator, 50 kW PV system and 100 kW battery system.

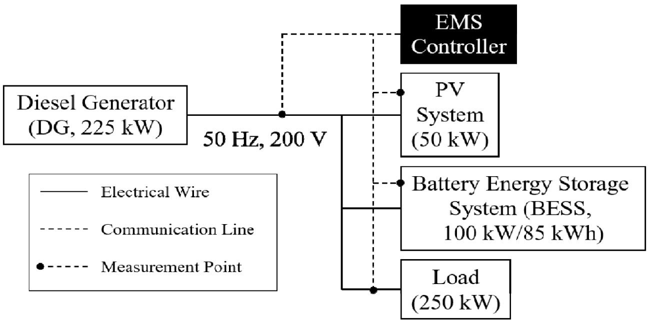


Figure 1. Microgrid configuration.

The EMS in question implements two main functions:

Function 1: Diesel Generator Output Control

In this function, generator outputs and the load values are monitored. PV or BESS are instructed to meet some of the demand so that the diesel generator's output does not exceed its upper boundary. Currently, there are 4 units in the diesel generator plant, and it is desired to use only 1 of them. That is to say, when the demand rises and another diesel generator unit needs to be fired, the EMS controller meets this demand from PV and BESS to avoid this. Furthermore, the increase in the microgrid's demand value can be compensated with the functionality. In this fashion, PV or BESS will be utilized to meet the increase in demand, instead of new diesel generators.

There is a certain lower boundary for the output of diesel generator so that it can successfully set local voltage and frequency. Inverters, utilized for PV and BESS, mostly need a reference point to follow. Smart inverters, which can help with grid forming, will be investigated in future work [10].

Function 2: Frequency Control

In this function frequency at the terminals of the diesel generator is monitored. In case of a swing, BESS is triggered to suppress the variation in the frequency value. Since the frequency control requires a much quicker and reliable response, EMS instructs the BESS to charge or discharge. In an ideal situation, if there is a frequency drop, the preferred step is to increase the generation from the PV system. However, this depends on the current solar radiation, power output of PV, and its ability to pick up EMS's instruction quickly. In order to ensure the desired operation, BESS is prioritized as such events have larger impacts in off-grid systems [26].

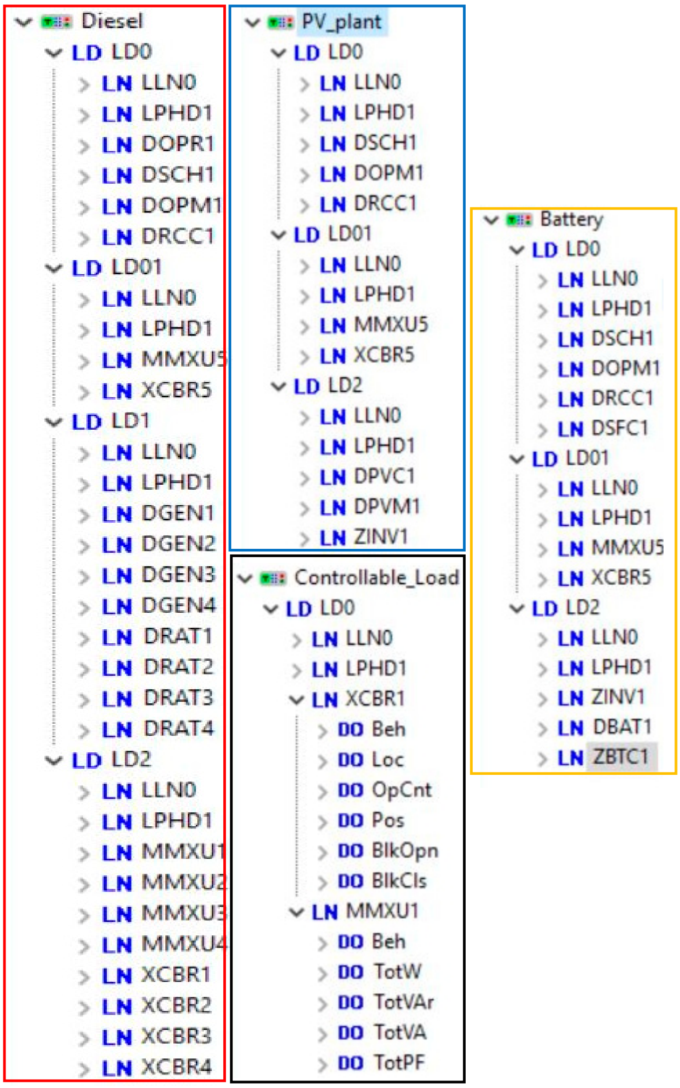
3. EMS Modeling with IEC61850

Communication models of these four components of the microgrid are developed with LDs and LNs of IEC 61850. The diesel generator model has four LDs. *LD0* represents operation modes with *DOPR1*, schedules with *DSCH1*, and related information with *DOPM1 and DRCC1*. *LD0* is included in all models, i.e., diesel generator, PV, load and BESS and used for similar purposes. *LD01* models physical connection with *XCBR5* and measurement devices with *MMXU5*. EMS contacts *MMXU5* to acquire any measurement data and instructs *XCBR5* to connect or disconnect to the microgrid. *LD01* is used for all models except the load model where *XCBR and MMXU* LNs are included individually. For the diesel generator, *LD1* represents four different units included inside the plant while *LD2* represents individual connection and measurement values of these individual units. *DGEN1-4* models each diesel unit's control parameters while *DRAT1-4* includes information about rated values of the generators.

LD2 in PV and BESS model energy generation and storage characteristics of these devices. For PV, it models PV module with *DPVC1* and *DPVM1*, inverter with *ZINV*. As for BESS, it models battery with *DBAT1* (for rated value information), inverter with *ZINV1*, and battery controller with *ZBTC1*.

EMS contacts *ZINV* if any specific information or instruction is to be sent to inverters of PV or BESS. BESS includes a battery and EMS can retrieve related information from *DBAT1* and change its settings in *ZBTC1*. The load model includes two separate LNs for connection and measurement, i.e., *XCBR1* and *MMXU1*, respectively. This model can be used for multiple loads. In other words, it does not necessarily model aggregate load. EMS only considers load-shedding by instructing *XCBR1* to disconnect from the microgrid. Sophisticated demand side management schemes are not implemented. Therefore, detailed real, reactive, apparent power, and power factor measurements are included in the model. These are stored inside *MMXU1* LN, namely in *TotW*, *TotVAr*, *TotVA*, *TotPF* data objects.

EMS is an intelligent electronic device (IED) that is connected to these components as shown in Figure 1 and uses the communication mapping detailed in Figure 2. In order to test the operation and validate message exchanges, different scenarios are run, and the operation is observed. Due to lack of space, detailed message captures are only given for results of Function 2. Nevertheless, Table 1 summarizes all the operation details of these functions. It illustrates the different functions, the components involved, specific action taken, and the types of IEC 61850 messages used.



- Diesel
  - LD LD0
    - LN LLN0
    - LN LPHD1
    - LN DOPR1
    - LN DSCH1
    - LN DOPM1
    - LN DRCC1
  - LD LD01
    - LN LLN0
    - LN LPHD1
    - LN MMXU5
    - LN XCBR5
  - LD LD1
    - LN LLN0
    - LN LPHD1
    - LN DGEN1
    - LN DGEN2
    - LN DGEN3
    - LN DGEN4
    - LN DRAT1
    - LN DRAT2
    - LN DRAT3
    - LN DRAT4
  - LD LD2
    - LN LLN0
    - LN LPHD1
    - LN MMXU1
    - LN MMXU2
    - LN MMXU3
    - LN MMXU4
    - LN XCBR1
    - LN XCBR2
    - LN XCBR3
    - LN XCBR4

- PV_plant
  - LD LD0
    - LN LLN0
    - LN LPHD1
    - LN DSCH1
    - LN DOPM1
    - LN DRCC1
  - LD LD01
    - LN LLN0
    - LN LPHD1
    - LN MMXU5
    - LN XCBR5
  - LD LD2
    - LN LLN0
    - LN LPHD1
    - LN DPVC1
    - LN DPVM1
    - LN ZINV1

- Controllable_Load
  - LD LD0
    - LN LLN0
    - LN LPHD1
    - LN XCBR1
      - DO Beh
      - DO Loc
      - DO OpCnt
      - DO Pos
      - DO BlkOpn
      - DO BlkCls
    - LN MMXU1
      - DO Beh
      - DO TotW
      - DO TotVAr
      - DO TotVA
      - DO TotPF

- Battery
  - LD LD0
    - LN LLN0
    - LN LPHD1
    - LN DSCH1
    - LN DOPM1
    - LN DRCC1
    - LN DSFC1
  - LD LD01
    - LN LLN0
    - LN LPHD1
    - LN MMXU5
    - LN XCBR5
  - LD LD2
    - LN LLN0
    - LN LPHD1
    - LN ZINV1
    - LN DBAT1
    - LN ZBTC1

Figure 2. IEC 61850 modeling of the diesel generator, photovoltaic (PV), battery energy storage system (BESS), and load.

Table 1. IEC 61850 models and message types used for different ems functions.

Function	Direction	Action Taken	Type
Function 1 Supply Demand Control	PV-> EMS	PV sends its operating mode and current P generation to EMS	MMS
	Diesel-> EMS	Diesel gen-set sends its nominal, max and min generation points to EMS	MMS
	EMS-> BESS	BESS is instructed to start charging/discharging	GOOSE
	EMS-> PV	If action taken by BESS is not sufficient, PV is instructed to curtail its generation	GOOSE
	EMS->Diesel	Checking how many units are online	MMS
Function 2 Frequency Control	Diesel-> EMS	Diesel gen-set sends its nominal, max and min generation points to EMS	MMS
	EMS-> BESS	Battery is instructed to operate in frequency support mode	GOOSE
	EMS-> BESS	Verifying operating conditions of BESS	MMS
	EMS->Diesel	Checking how many units are online	MMS

3.1. Function 1: Diesel Generator Output Control Tests (Load Decrease)

The load value is set, initially, to 160 kW. PV output is at its limit, 50 kW, and the remaining 110 kW is sourced by the diesel generator. PV operating mode and its limit are reported as follows:

EMS_controller → PV_plant.DOPM $ OpModConW $ SPC $ "true" 1

EMS_controller → PV_plant.DRCC $ OutWSet $ APC $ 50.

The lower boundary of the generator is set as 100 kW inside *DOPR* LN while current operating mode and generation values are reported in *DOPM* and *DRCC*:

EMS_controller → Diesel.DOPR $ ECPNomWRtg $ ASG $ 110, 100, 140 (nominal, min & max output in kWs)

EMS_controller → Diesel.DOPM $ OpModConW $ SPC $ "true" 1

EMS_controller → Diesel.DRCC $ OutWSet $ APC $ 110 (110 kW power supplied by Diesel).

In reality, this is a very high value, but the purpose is to see how EMS controller reacts. At $t = 1$ sec, the load is decreased from 160 to 100 kW. Without any EMS controller, this drop is reflected on the diesel generator's output while PV and BESS stay the same. This causes the diesel generator's output to go beyond its lower limit.

There are two ways to solve this. The EMS controller can instruct BESS to start charging so that the diesel generator's output is higher than the lower limit. This command is relayed from EMS to BESS via *ZBTC* LN.

EMS_controller → Battery.ZBTC $ BatChaSt $ ENG $ '2' (Battery charging operational mode).

If the BESS is already charged, or the drop-in diesel generator's output is very high, the EMS controller can instruct PV to curtail its generation. It is important to note that if the load decrease was larger, this option would not be sufficient on its own. In that case, a combination of the above is required. This "if" statement and the resultant curtailment instruction are performed by EMS as follows:

If Battery.ZBAT $ BatVHi $ SPS $ = '1' Then (i.e. battery is fully charged)

EMS_controller → PV_plant. DRCC $ OutWSet $ APC $ 5 (90% curtailed power).

3.2. Function 1: Supply–Demand Control Tests (Load Increase)

Initially, load was set to 140 kW. The PV generator provides no power, and the entire demand is met by the diesel generator, i.e., 140 kW. The upper limit of the diesel generator is set to be 140 kW. Of available units, only unit 1 is operating under these conditions. These settings and operating values are mapped to communication models as follows:

EMS_controller → Diesel.DOPR $ ECPNomWRtg $ ASG $ 110, 100, 140 (nominal, min and max output in kWs)

EMS_controller → Diesel.DOPM $ OpModConW $ SPC $ "true" 1

EMS_controller → Diesel.DRCC $ OutWSet $ APC $ 140

EMS_controller → Diesel.DGEN1 $ GnOpSt $ 2 (operating)

EMS_controller → Diesel.DGEN2 $ GnOpSt $ 1 (Not operating)

EMS_controller → Diesel.DGEN3 $ GnOpSt $ 1 (Not operating)

EMS_controller → Diesel.DGEN4 $ GnOpSt $ 1 (Not operating).

In reality, this may not be a very high value, but the purpose is to see how the EMS controller reacts. At t = 1 s, the load is increased from 140 to 190 kW. Without any EMS controller, this increase is reflected on the diesel generator's output and it exceeds its upper limit. This means additional units of diesel generators need to be turned on to meet this demand (i.e., by setting *Diesel.DGEN2 $ GnOpSt* to 2). Since PV generation is not dispatchable, in this case, the only solution is to instruct BESS to discharge. BESS immediately starts discharging and gradually increases the amount of provided energy. This ramp rate is totally dependent on the battery characteristics and can be improved by using batteries with high discharge speeds. In parallel, DG output decreases below the upper limit.

3.3. Function 2: Frequency Control Tests

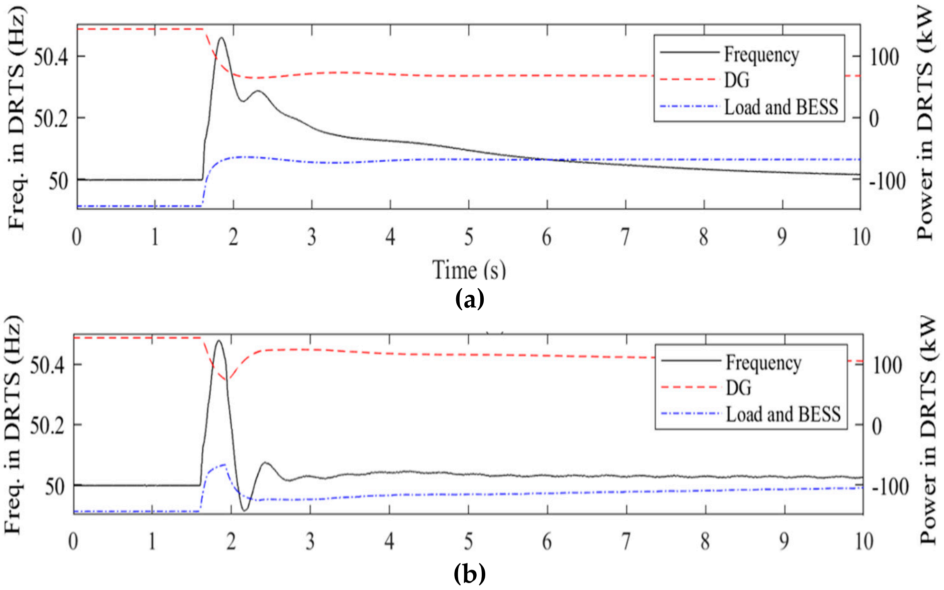
Initially, load was set to 150 kW. The PV generator provides no power, the entire demand is met by the diesel generator and the frequency is 50 Hz. At t = 1.6 s, load is reduced from 150 to 70 kW. Figure 3a,b show results with and without the EMS controller, respectively [11]. It can be observed that frequency swing without the EMS controller is much larger than that of with EMS controller.

The EMS controller compares the lower limit of the diesel generator with its current measured value. If the latter is lower, then it instructs battery to operate in frequency response mode. These are performed as follows:

If Diesel.DRCC$OutWSet < Diesel.DOPR $ ECPNomWRtg (min)

Then EMS_controller → Battery.DSFC $ HzAct $ SPC $ '1' (1- activate frequency control mechanism).

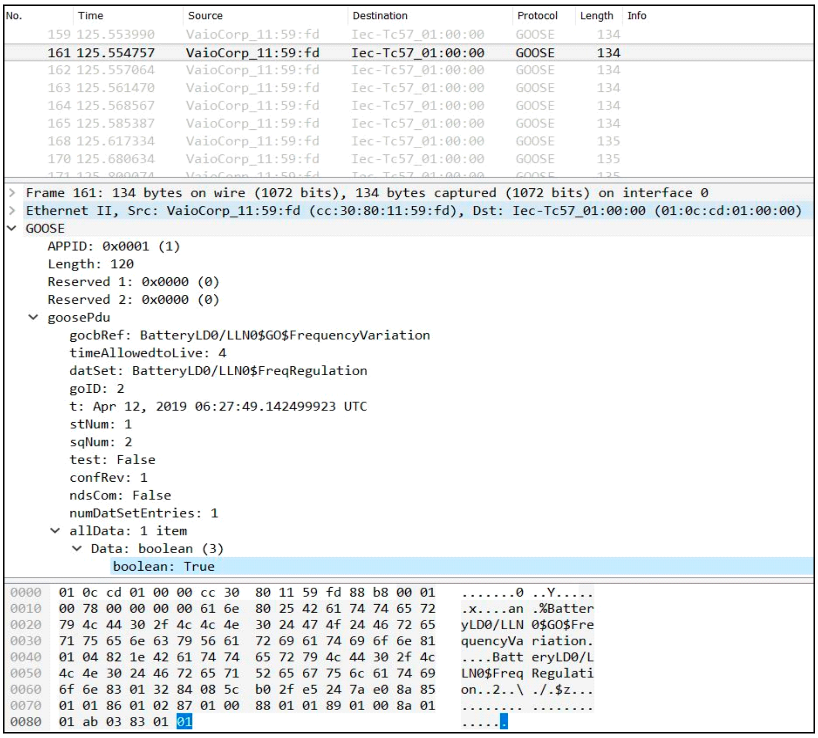
This command is relayed to BESS via GOOSE message, as this is an event-based operation. Figure 4 shows Wireshark capture of the message sent by EMS to BESS to commence frequency support.



(a)

(b)

Figure 3. Frequency control function test results: (**a**) without energy management system (EMS); (**b**) with frequency control function in EMS.

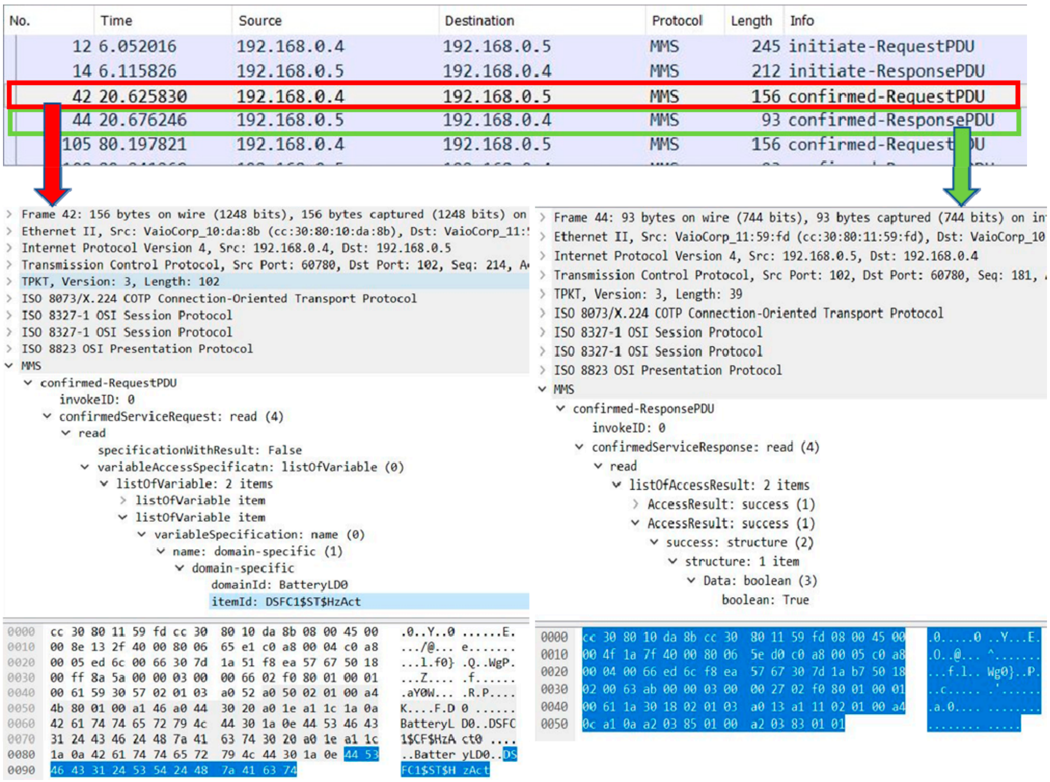


```
No.   Time          Source               Destination           Protocol  Length  Info
  159 125.553990    VaioCorp_11:59:fd    Iec-Tc57_01:00:00     GOOSE       134
  161 125.554757    VaioCorp_11:59:fd    Iec-Tc57_01:00:00     GOOSE       134
  162 125.557064    VaioCorp_11:59:fd    Iec-Tc57_01:00:00     GOOSE       134
  163 125.561470    VaioCorp_11:59:fd    Iec-Tc57_01:00:00     GOOSE       134
  164 125.568567    VaioCorp_11:59:fd    Iec-Tc57_01:00:00     GOOSE       134
  165 125.585387    VaioCorp_11:59:fd    Iec-Tc57_01:00:00     GOOSE       134
  168 125.617334    VaioCorp_11:59:fd    Iec-Tc57_01:00:00     GOOSE       135
  170 125.680634    VaioCorp_11:59:fd    Iec-Tc57_01:00:00     GOOSE       135

> Frame 161: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
> Ethernet II, Src: VaioCorp_11:59:fd (cc:30:80:11:59:fd), Dst: Iec-Tc57_01:00:00 (01:0c:cd:01:00:00)
v GOOSE
    APPID: 0x0001 (1)
    Length: 120
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  v goosePdu
      gocbRef: BatteryLD0/LLN0$GO$FrequencyVariation
      timeAllowedtoLive: 4
      datSet: BatteryLD0/LLN0$FreqRegulation
      goID: 2
      t: Apr 12, 2019 06:27:49.142499923 UTC
      stNum: 1
      sqNum: 2
      test: False
      confRev: 1
      ndsCom: False
      numDatSetEntries: 1
    v allData: 1 item
      v Data: boolean (3)
          boolean: True

0000  01 0c cd 01 00 00 cc 30  80 11 59 fd 88 b8 00 01   .......0 ..Y.....
0010  00 78 00 00 00 00 61 6e  80 25 42 61 74 74 65 72   .x....an .%Batter
0020  79 4c 44 30 2f 4c 4c 4e  30 24 47 4f 24 46 72 65   yLD0/LLN 0$GO$Fre
0030  71 75 65 6e 63 79 56 61  72 69 61 74 69 6f 6e 81   quencyVa riation.
0040  01 04 82 1e 42 61 74 74  65 72 79 4c 44 30 2f 4c   ....Batt eryLD0/L
0050  4c 4e 30 24 46 72 65 71  52 65 67 75 6c 61 74 69   LN0$Freq Regulati
0060  6f 6e 83 01 32 84 08 5c  b0 2f e5 24 7a e0 8a 85   on..2..\ ./.$z...
0070  01 01 86 01 02 87 01 00  88 01 01 89 01 00 8a 01   ........ ........
0080  01 ab 03 83 01 01                                  ......
```

Figure 4. GOOSE message sent by EMS to BESS for frequency support.

At any time, EMS can inquire about the operating mode of BESS via MMS messages. Figure 5 shows the information request sent by EMS (IP address 192.168.0.4) to BESS (IP address 192.168.0.5) and the response sent back. As shown, the request MMS has "Battery.LD0.DSFC$ST HzAct" while the response MMS shows "True (1)". This confirms the BESS is operating in frequency support mode.

EMS and other communication models are emulated using IEC 61850 software tools in a local area network (LAN). As shown in Figure 6, EMS can connect to any of these IEDs, example shows diesel and BESS, to read and set the parameters. This ensures necessary parameters are read for decision making and others are set as required by the EMS logic. As shown, EMS instructs diesel IED to connect to the network and start injection power while BESS is instructed to activate its HzAct mode, i.e., frequency support mode.



```
No.   Time        Source        Destination   Protocol  Length  Info
   12 6.052016    192.168.0.4   192.168.0.5   MMS          245  initiate-RequestPDU
   14 6.115826    192.168.0.5   192.168.0.4   MMS          212  initiate-ResponsePDU
   42 20.625830   192.168.0.4   192.168.0.5   MMS          156  confirmed-RequestPDU
   44 20.676246   192.168.0.5   192.168.0.4   MMS           93  confirmed-ResponsePDU
  105 80.197821   192.168.0.4   192.168.0.5   MMS          156  confirmed-Request DU
```

```
> Frame 42: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits) on
> Ethernet II, Src: VaioCorp_10:da:8b (cc:30:80:10:da:8b), Dst: VaioCorp_11:!
> Internet Protocol Version 4, Src: 192.168.0.4, Dst: 192.168.0.5
> Transmission Control Protocol, Src Port: 60780, Dst Port: 102, Seq: 214, A
> TPKT, Version: 3, Length: 102
> ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
> ISO 8327-1 OSI Session Protocol
> ISO 8327-1 OSI Session Protocol
> ISO 8823 OSI Presentation Protocol
v MMS
  v confirmed-RequestPDU
      invokeID: 0
    v confirmedServiceRequest: read (4)
      v read
          specificationWithResult: False
        v variableAccessSpecificatn: listOfVariable (0)
          v listOfVariable: 2 items
            > listOfVariable item
            v listOfVariable item
              v variableSpecification: name (0)
                v name: domain-specific (1)
                  v domain-specific
                      domainId: BatteryLD0
                      itemId: DSFC1$ST$HzAct

0000  cc 30 80 11 59 fd cc 30  80 10 da 8b 08 00 45 00   .0..Y..0 ......E.
0010  00 8e 13 2f 40 00 80 06  65 e1 c0 a8 00 04 c0 a8   .../@... e.......
0020  00 05 ed 6c 00 66 30 7d  1a 51 f8 ea 57 67 50 18   ...l.f0} .Q..WgP.
0030  00 ff 8a 5a 00 00 03 00  00 66 02 f0 80 01 00 01   ...Z.... .f......
0040  00 61 59 30 57 02 01 03  a0 52 a0 50 02 01 00 a4   .aY0W... .R.P....
0050  4b 80 01 00 a1 46 a0 44  30 20 a0 1e a1 1c 1a 0a   K....F.D 0 ......
0060  42 61 74 74 65 72 79 4c  44 30 1a 0e 44 53 46 43   BatteryL D0..DSFC
0070  31 24 43 46 24 48 7a 41  63 74 30 20 a0 1e a1 1c   1$CF$HzA ct0 ....
0080  1a 0a 42 61 74 74 65 72  79 4c 44 30 1a 0e 44 53   ..Batter yLD0..DS
0090  46 43 31 24 53 54 24 48  7a 41 63 74               FC1$ST$H zAct
```

```
> Frame 44: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on in
> Ethernet II, Src: VaioCorp_11:59:fd (cc:30:80:11:59:fd), Dst: VaioCorp_10
> Internet Protocol Version 4, Src: 192.168.0.5, Dst: 192.168.0.4
> Transmission Control Protocol, Src Port: 102, Dst Port: 60780, Seq: 181,
> TPKT, Version: 3, Length: 39
> ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
> ISO 8327-1 OSI Session Protocol
> ISO 8327-1 OSI Session Protocol
> ISO 8823 OSI Presentation Protocol
v MMS
  v confirmed-ResponsePDU
      invokeID: 0
    v confirmedServiceResponse: read (4)
      v read
        v listOfAccessResult: 2 items
          > AccessResult: success (1)
          v AccessResult: success (1)
            v success: structure (2)
              v structure: 1 item
                v Data: boolean (3)
                    boolean: True

0000  cc 30 80 10 da 8b cc 30  80 11 59 fd 08 00 45 00   .0.....0 ..Y...E.
0010  00 4f 1a 7f 40 00 80 06  5e d0 c0 a8 00 05 c0 a8   .O..@... ^.......
0020  00 04 00 66 ed 6c f8 ea  57 67 30 7d 1a b7 50 18   ...f.l.. Wg0}..P.
0030  02 00 63 ab 00 00 03 00  00 27 02 f0 80 01 00 01   ..c..... .'......
0040  00 61 1a 30 18 02 01 03  a0 13 a1 11 02 01 00 a4   .a.0.... ........
0050  0c a1 0a a2 03 85 01 00  a2 03 83 01 01            ........ .....
```

Figure 5. MMS messages showing information request by EMS and BESS's response.

4. Cybersecurity Considerations for Microgrid Communication

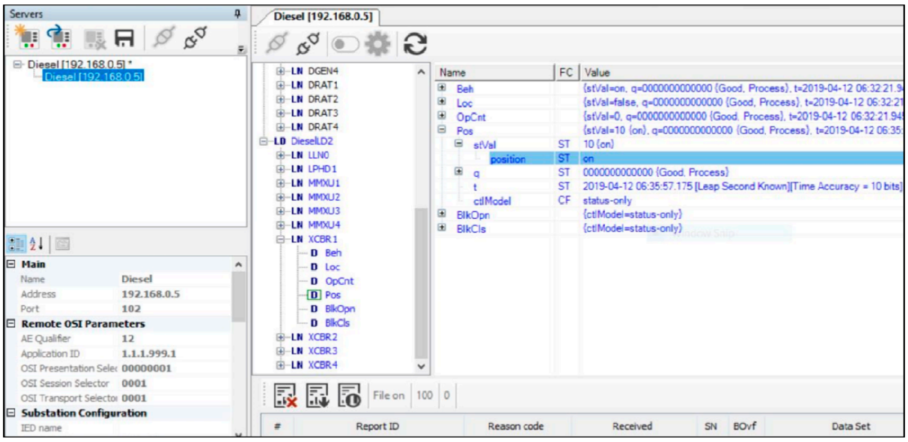
The IEC 61850 message exchanges for realizing the microgrid energy management functions are described in the previous section. These messages carry critical and sensitive information such as dispatch instructions or control commands for energy management operation. If any of these messages are tampered or modified, this would have an adverse impact on microgrid energy management operation. Further, it may lead to severe consequences. Hence, all the message exchanges must be protected against any potential attack.

In this regard, IEC 62351 standard series has recommended security guidelines for safeguarding IEC 61850 messages [27]. From Table 1, it is clear that GOOSE and MMS messages are employed for realizing the energy management function. Hence, the GOOSE and MMS messages must be protected against any potential cyberattacks.

4.1. Security Considerations for GOOSE Message

IEC 62351-1 considers authenticity and integrity as the security requirements for GOOSE messages. To achieve this, IEC 62351-6 recommends appending the GOOSE messages with an authentical value. The authentication value is generated by digitally signing a message authentication code (MAC) using *RSASA-PKCS1-v1_5*. The MAC is generated by computing a hash value of GOOSE *APDU* using the SHA256 algorithm. This digitally signed authentication value is added as extension field to the GOOSE message as shown in Figure 7. The format of this extension field is shown in Figure 8.

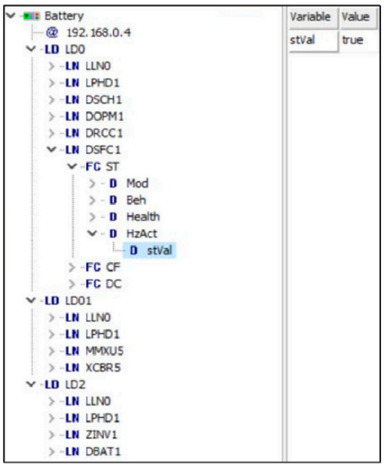
Diesel Control IED



Main
Name Diesel
Address 192.168.0.5
Port 102
Remote OSI Parameters
AE Qualifier 12
Application ID 1.1.1.999.1
OSI Presentation Selec 00000001
OSI Session Selector 0001
OSI Transport Selecto 0001
Substation Configuration
IED name

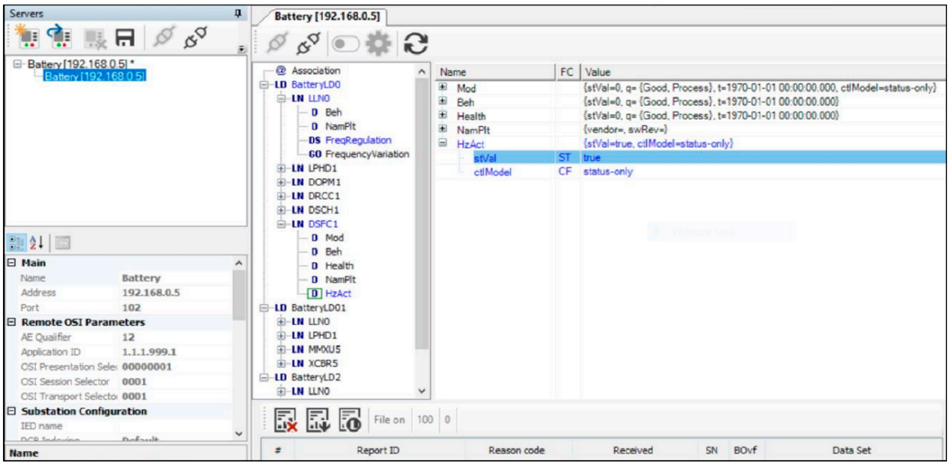
Name	FC	Value
Beh		{stVal=on, q=0000000000000 (Good, Process), t=2019-04-12 06:32:21.9
Loc		{stVal=false, q=0000000000000 (Good, Process), t=2019-04-12 06:32:21
OpCnt		{stVal=0, q=0000000000000 (Good, Process), t=2019-04-12 06:32:21.94
Pos		{stVal=10 (on), q=0000000000000 (Good, Process), t=2019-04-12 06:35
stVal	ST	10 (on)
position	ST	on
q	ST	0000000000000 (Good, Process)
t	ST	2019-04-12 06:35:57.175 [Leap Second Known][Time Accuracy = 10 bits]
ctlModel	CF	status-only
BlkOpn		{ctlModel=status-only}
BlkCls		{ctlModel=status-only}

EMS Controller



Variable	Value
stVal	true

BESS Control IED



Main
Name Battery
Address 192.168.0.5
Port 102
Remote OSI Parameters
AE Qualifier 12
Application ID 1.1.1.999.1
OSI Presentation Selec 00000001
OSI Session Selector 0001
OSI Transport Selecto 0001
Substation Configuration
IED name
DCB Indexing Default
Name

Name	FC	Value
Mod		{stVal=0, q= (Good, Process), t=1970-01-01 00:00:00.000, ctlModel=status-only}
Beh		{stVal=0, q= (Good, Process), t=1970-01-01 00:00:00.000}
Health		{stVal=0, q= (Good, Process), t=1970-01-01 00:00:00.000}
NamPlt		{vendor=, swRev=}
HzAct		{stVal=true, ctlModel=status-only}
stVal	ST	true
ctlModel	CF	status-only

Figure 6. EMS controller console with the diesel generator Intelligent Electronic Device (IED) and BESS IED.

At the publisher IED, all the GOOSE messages are appended with digitally signed authentication values. At the subscriber IED, after receiving the GOOSE message, it decrypts the digitally signed authentication value and also computes a new hash value for the received GOOSE *APDU*. Now, the computed hash value is compared with the decrypted authentication value. If these values match, then the received GOOSE message is authentic. If the values do not match, the GOOSE message is discarded as it not authentic.

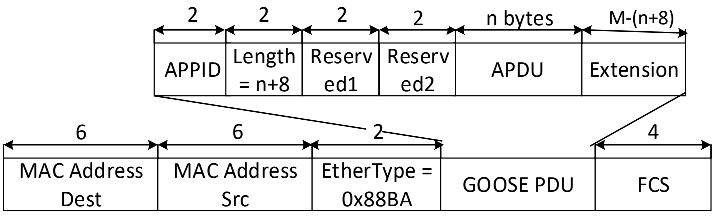


Figure 7. Extended GOOSE message with security field appended.

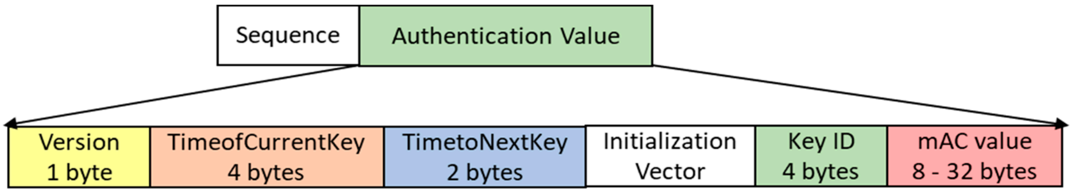


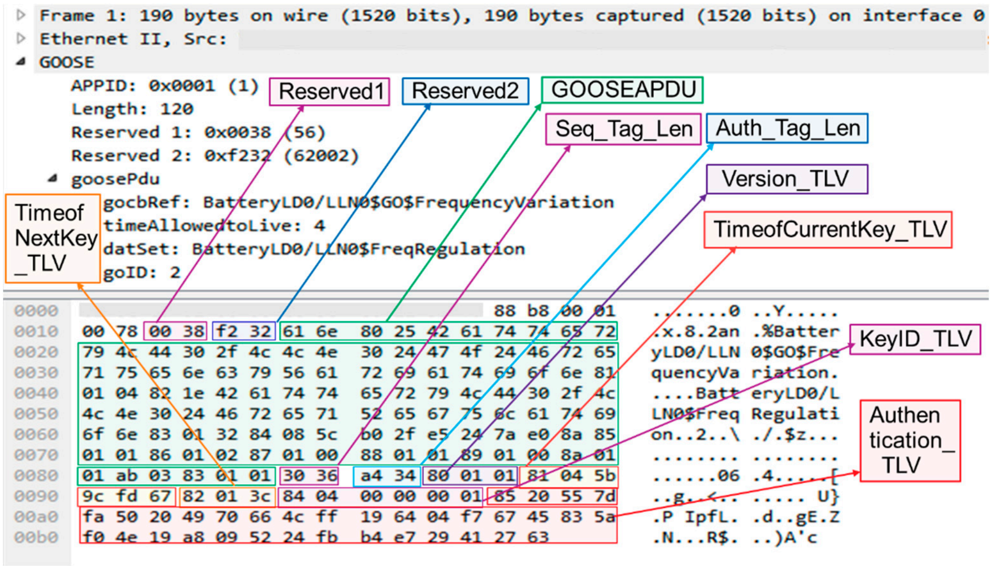
Figure 8. Format of extension field.

Previous studies reported that the RSA-based digital signatures for generating authentication values require high processing times, hence cannot be applied to GOOSE messages which has very stringent timing requirements of 3 ms (including computational and communication delays) [28]. Hence, in literature, elliptic curve digital signature algorithm (ECDSA)-based digital signatures were proposed, which resulted in comparatively lower computational times but still not enough for GOOSE requirements. Recently, hashed message authentication code (HMAC)-based algorithms have been proposed as an alternate solution to secure the GOOSE messages [29]. HMAC-based algorithms resulted is very low computational times, well below the 3 ms, which do not affect the performance of the GOOSE messages. In this paper, HMAC algorithms are utilized to secure the GOOSE messages. The size of the extension field for different digital signatures and HMAC variants is shown in Table 2.

Table 2. Different security extensions for GOOSE messages.

S.No	Security Extension	Extension Value (in bytes)
1	RSASSA-PKCS1-v1_5	128
2	Elliptic curve digital signature algorithm (ECDSA)	48
3	HMAC-SHA256-80	10
4	HMAC-SHA256-128	16
5	HMAC-SHA256-256	32
6	AES-GMAC-64	8
7	AES-GMAC-128	16

IEC 61850 GOOSE message exchanges for implementing functions discussed in Section 3, also shown, in Table 1 are secured by adding HMAC-based authentication values. The GOOSE message, shown in Figure 4, published by EMS to activate frequency mode operation in BESS is secured appending the HMAC-based authentication value as shown in Figure 9. Similarly, all the GOOSE messages published are secured by appending the authentication values.



```
▷ Frame 1: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits) on interface 0
▷ Ethernet II, Src: [redacted]
◢ GOOSE
    APPID: 0x0001 (1)
    Length: 120
    Reserved 1: 0x0038 (56)
    Reserved 2: 0xf232 (62002)
  ◢ goosePdu
      gocbRef: BatteryLD0/LLN0$GO$FrequencyVariation
      timeAllowedtoLive: 4
      datSet: BatteryLD0/LLN0$FreqRegulation
      goID: 2

0000  [redacted]                             88 b8 00 01   .......0 ..Y.....
0010  00 78 00 38 f2 32 61 6e  80 25 42 61 74 74 65 72   .x.8.2an .%Batter
0020  79 4c 44 30 2f 4c 4c 4e  30 24 47 4f 24 46 72 65   yLD0/LLN 0$GO$Fre
0030  71 75 65 6e 63 79 56 61  72 69 61 74 69 6f 6e 81   quencyVa riation.
0040  01 04 82 1e 42 61 74 74  65 72 79 4c 44 30 2f 4c   ....Batt eryLD0/L
0050  4c 4e 30 24 46 72 65 71  52 65 67 75 6c 61 74 69   LN0$Freq Regulati
0060  6f 6e 83 01 32 84 08 5c  b0 2f e5 24 7a e0 8a 85   on..2..\ ./.$z...
0070  01 01 86 01 02 87 01 00  88 01 01 89 01 00 8a 01   ........ ........
0080  01 ab 03 83 01 01 30 36  a4 34 80 01 01 81 04 5b   ......06 .4.....[
0090  9c fd 67 82 01 3c 84 04  00 00 00 01 85 20 55 7d   ..g..<.. ..... U}
00a0  fa 50 20 49 70 66 4c ff  19 64 04 f7 67 45 83 5a   .P IpfL. .d..gE.Z
00b0  f0 4e 19 a8 09 52 24 fb  b4 e7 29 41 27 63         .N...R$. ..)A'c
```

Figure 9. Secure Generic object-oriented substation event (GOOSE) message with hashed message authentication code (HMAC) extension.

4.2. Security Considerations for MMS Messages

IEC 62351-4 recommends transport layer security (TLS) defined by the RFC 5246 for securing the IEC 61850 MMS messages. Through TLS mechanism, a secure session is established between client and server before exchanging any data. TLS defines a cipher suite which is a set of cryptographic algorithms for peer authentication, key exchange, encryption, and message authentication for establishing a secure session.

Figure 10 illustrates the message exchanges between a client and server for establishing a TLS session. The client and server initially exchange certificates (X.509 format) and verify each other. The node authenticity is confirmed by the certificate exchange mechanism. Also, through the certificate exchange, the public keys of both client and server are exchanged.

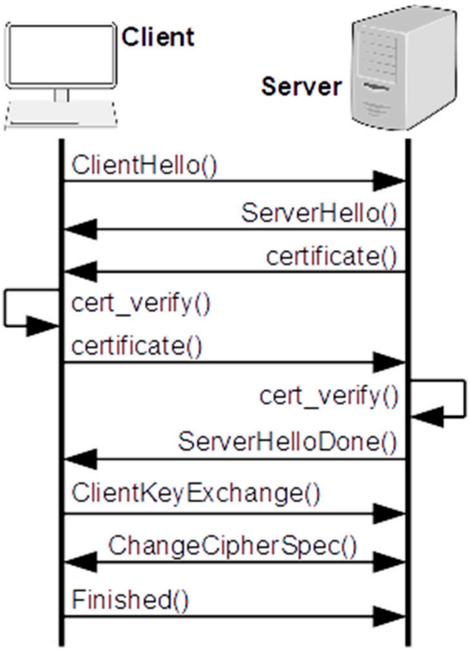
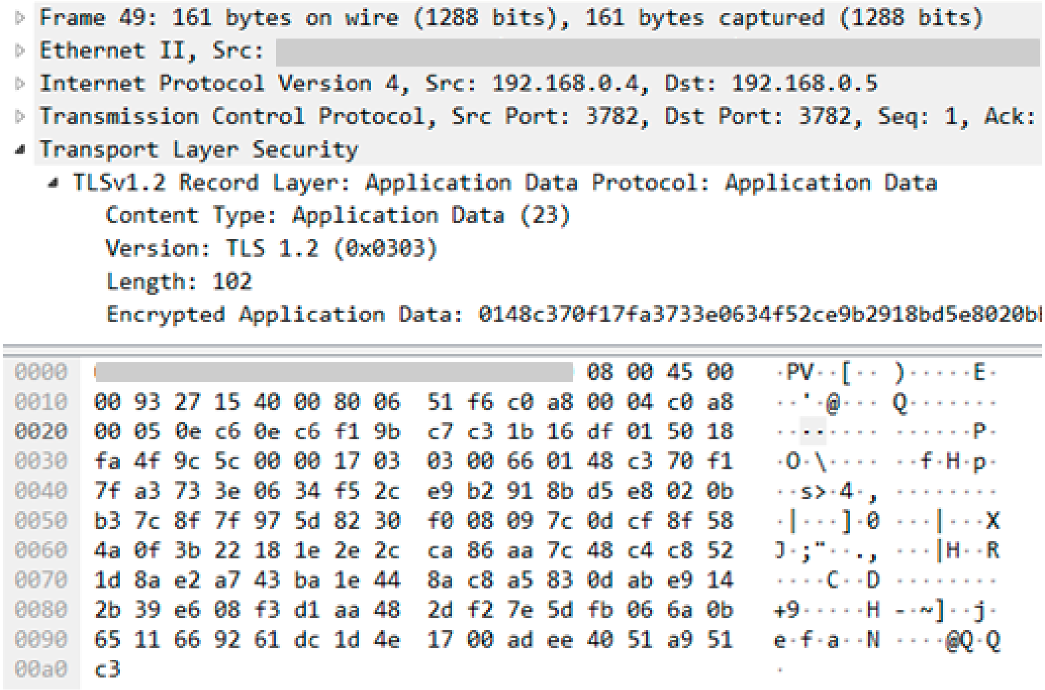


Figure 10. Message exchanges for transport layer security (TLS) establishment for client and server.

Once the certificates are exchanged, the client sends a secret key by using any key exchange algorithm such as Diffie–Hellman (DH). Using this secret key, the client and server negotiate changes in cipher suite. Once the cipher suite is finalized, further application message exchanges are encrypted with digital signatures according to the cipher suite algorithms. This encryption of the application message exchanges ensures confidentiality of the message exchanges.

IEC 62351-4 standard specifies the minimum cipher suite for securing MMS messages shall be TLS_DH_DSS_WITH_AES_256_SHA. This implies that the DH algorithm is used for establishing secret key, advanced encryption standard-256 (AES 256) is used for application data encryption and secure hash algorithm (SHA-256) algorithm is utilized for generating hash function. Further, IEC 62351-4 specifies uses of port 3782 in transport layer for establishing TLS sessions and exchanging MMS messages.

Using the above cipher suite, the IEC 61850 message exchanges described in Table 1 for realizing different EMS functions are secured. As an example, the IEC 61850 MMS request message shown in Figure 5 is secured by establishing a TLS session over port 3782 with the above cipher suite. Figure 11 shows the screenshot of TLS secure MMS request message request showing information request regarding the operating mode of BESS by EMS.



```
▷ Frame 49: 161 bytes on wire (1288 bits), 161 bytes captured (1288 bits)
▷ Ethernet II, Src: [redacted]
▷ Internet Protocol Version 4, Src: 192.168.0.4, Dst: 192.168.0.5
▷ Transmission Control Protocol, Src Port: 3782, Dst Port: 3782, Seq: 1, Ack:
◢ Transport Layer Security
  ◢ TLSv1.2 Record Layer: Application Data Protocol: Application Data
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 102
      Encrypted Application Data: 0148c370f17fa3733e0634f52ce9b2918bd5e8020b

0000  [redacted]              08 00 45 00   ·PV··[·· )·····E·
0010  00 93 27 15 40 00 80 06  51 f6 c0 a8 00 04 c0 a8   ··'·@··· Q·······
0020  00 05 0e c6 0e c6 f1 9b  c7 c3 1b 16 df 01 50 18   ········ ······P·
0030  fa 4f 9c 5c 00 00 17 03  03 00 66 01 48 c3 70 f1   ·O·\···· ··f·H·p·
0040  7f a3 73 3e 06 34 f5 2c  e9 b2 91 8b d5 e8 02 0b   ··s>·4·, ········
0050  b3 7c 8f 7f 97 5d 82 30  f0 08 09 7c 0d cf 8f 58   ·|···]·0 ···|···X
0060  4a 0f 3b 22 18 1e 2e 2c  ca 86 aa 7c 48 c4 c8 52   J·;"···., ···|H··R
0070  1d 8a e2 a7 43 ba 1e 44  8a c8 a5 83 0d ab e9 14   ····C··D ········
0080  2b 39 e6 08 f3 d1 aa 48  2d f2 7e 5d fb 06 6a 0b   +9·····H -·~]··j·
0090  65 11 66 92 61 dc 1d 4e  17 00 ad ee 40 51 a9 51   e·f·a··N ····@Q·Q
00a0  c3                                                 ·
```

Figure 11. Transport layer security (TLS) secured IEC 61850 MMS request showing information request by energy management system (EMS) to battery energy storage system (BESS).

5. Conclusions

Integration of intermittent renewable energy technologies in power systems, especially in microgrids, requires extensive monitoring and control. EMS controllers can be utilized for this purpose. Considering the variety of equipment that can be a part of the microgrid and the diversity of manufacturers, it is imperative that a standard communication infrastructure be developed. This ensures that the EMS can communicate with different devices in an interoperable way. IEC 61850 is poised to be the communication standard of future smart grids due to its object-oriented structure and data-transmission capacity.

In this paper, an IEC 61850-based communication model has been developed and implemented for a microgrid EMS. The developed IEC 61850 models were emulated and real-time message exchanges between different components of the microgrid for energy management are shown. The results validate the developed models and message mapping. The results from the emulation models are very useful before the actual deployment of the system in field. Furthermore, considering that sensitive operational data is exchanged in these messages, cybersecurity features have been implemented as per IEC 62351. Messages with and without security features are compared to highlight differences in tags and message size. Future work may focus on investigating the performance of the proposed IEC 61850-based communication for microgrid EMS for on real hardware system by including a real microgrid controller (such as SEL RTAC 3555) in conjunction with real time digital simulator (RTDS). Further, investigations on performance of the proposed system for different communication technologies that can be used in small islands with more diverse generation portfolio can be conducted.

Author Contributions: Conceptualization, T.S.U. and S.M.S.H.; methodology, T.S.U. and S.M.S.H.; validation, S.M.S.H., writing—T.S.U.; supervision and funding acquisition, T.S.U. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by This work was supported in part by Fukushima Prefecture's Reconstruction Grant, 2019.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hubble, A.H.; Ustun, T.S. Scaling renewable energy based microgrids in underserved communities: Latin America, South Asia, and Sub-Saharan Africa. In Proceedings of the 2016 IEEE PES PowerAfrica, Livingstone, Zambia, 28 June–3 July 2016; pp. 134–138.
2. Almeshqab, F.; Ustun, T.S. Lessons learned from rural electrification initiatives in developing countries: Insights for technical, social, financial and public policy aspects. *Renew. Sustain. Energy Rev.* **2019**, *102*, 35–53. [CrossRef]
3. International Energy Agency. *WEO-2017 Special Report: Energy Access Outlook, From Poverty to Prosperity*; IEA Publications (International Energy Agency): Paris, France, 2017.
4. Scott, A.; Diecker, J.; Harrison, K.; Miller, C.; Hogarth, J.R.; Wheeldon, S. *Accelerating Access to Electricity in Africa with Off-Grid Solar—Solar Market Systems*; Overseas Development Institute: London, OH, USA, 2016.
5. IRENA. *National Energy Roadmaps for Islands*; IRENA: Bonn, Germany, 2016.
6. Hubble, A.H.; Ustun, T.S. Composition, placement, and economics of rural microgrids for ensuring sustainable development. *Sustain. Energy Grids Netw.* **2018**, *13*, 1–18. [CrossRef]
7. Ustun, T.S.; Mekhilef, S. Design and implementation of static synchronous series compensator with a soft-switching H-bridge inverter with DSP-based synchronization control. *Int. Rev. Electr. Eng.* **2010**, *5*, 1347–1353.
8. Nadeem, F.; Hussain, S.M.S.; Tiwari, P.K.; Goswami, A.K.; Ustun, T.S. Comparative Review of Energy Storage Systems, Their Roles, and Impacts on Future Power Systems. *IEEE Access* **2019**, *7*, 4555–4585. [CrossRef]
9. *Nippon Koei Develops Storage Battery Control System for Controlling Power Frequency*; Nippon Koei Co. Ltd.: Tokyo, Japan, 2018; Available online: http://pdf.irpocket.com/C1954/VKXr/syDo/kNFH.pdf (accessed on 23 October 2019).
10. Aftab, M.A.; Hussain, S.M.S.; Ali, I.; Ustun, T.S. IEC 61850 and XMPP Communication Based Energy Management in Microgrids Considering Electric Vehicles. *IEEE Access* **2018**, *6*, 35657–35668. [CrossRef]
11. Kikusato, H.; Ustun, T.S.; Suzuki, M.; Sugahara, S.; Hashimoto, J.; Otani, K.; Shirakawa, K.; Yabuki, R.; Watanabe, K.; Shimizu, T. Integrated Power Hardware-in-the-Loop and Lab Testing for Microgrid Controller. In Proceedings of the 2019 IEEE Innovative Smart Grid Technologies—Asia (ISGT Asia), Chengdu, China, 21–24 May 2019.
12. Naz, A.; Javaid, N.; Rasheed, M.B.; Haseeb, A.; Alhussein, M.; Aurangzeb, K. Game Theoretical Energy Management with Storage Capacity Optimization and Photo-Voltaic Cell Generated Power Forecasting in Micro Grid. *Sustainability* **2019**, *11*, 2763. [CrossRef]
13. Barchi, G.; Pierro, M.; Moser, D. Predictive Energy Control Strategy for Peak Switch and Shifting Using BESS and PV Generation Applied to the Retail Sector. *Electronics* **2019**, *8*, 526. [CrossRef]

14. Al-Sakkaf, S.; Kassas, M.; Khalid, M.; Abido, M.A. An Energy Management System for Residential Autonomous DC Microgrid Using Optimized Fuzzy Logic Controller Considering Economic Dispatch. *Energies* **2019**, *12*, 1457. [CrossRef]
15. Roiné, L.; Therani, K.; Manjili, Y.S.; Jamshidi, M. Microgrid energy management system using fuzzy logic control. In Proceedings of the 2014 World Automation Congress (WAC), Waikoloa, HI, USA, 3–7 August 2014; pp. 462–467.
16. Li, B.; Zhang, P.; Li, X.; Cao, S. Distributed Absorption and Half-Search Approach for Economic Dispatch Problem in Smart Grids. *Energies* **2019**, *12*, 1527. [CrossRef]
17. Deng, W.; Pei, W.; Shen, Z.; Zhao, Z.; Qu, H. Adaptive Micro-Grid Operation Based on IEC 61850. *Energies* **2015**, *8*, 4455–4475. [CrossRef]
18. Byong-Kwan, Y.; Seung-Ho, Y.; Won-Yong, K.; Yu-Seok, J.; Byung-Moon, H.; Kwang-Soo, J. Communication Architecture of the IEC 61850-based Micro Grid System. *J. Electr. Eng. Technol.* **2011**, *6*, 605–612.
19. *Communication Networks and Systems for Power Utility Automation, IEC 61850, Ed.2.0. 2013*; CENELEC: Brussels, Belgium, 2014.
20. Ustun, T.S.; Ozansoy, C.; Zayegh, A. Simulation of communication infrastructure of a centralized microgrid protection system based on IEC 61850-7-420. In Proceedings of the IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Tainan, Taiwan, 5–8 November 2012; pp. 492–497.
21. Ali, I.; Hussain, S.M.S. Control and management of distribution system with integrated DERs via IEC 61850 based communication. *Eng. Sci. Technol.* **2017**, *20*, 956–964. [CrossRef]
22. Hussain, S.M.S.; Ustun, T.S.; Nsonga, P.; Ali, I. IEEE 1609 WAVE and IEC 61850 Standard Communication Based Integrated EV Charging Management in Smart Grids. *IEEE Trans. Veh. Technol.* **2018**, *67*, 7690–7697. [CrossRef]
23. Hussain, S.M.S.; Tak, A.; Ustun, T.S.; Ali, I. Communication Modeling of Solar Home System and Smart Meter in Smart Grids. *IEEE Access* **2018**, *6*, 16985–16996. [CrossRef]
24. Ustun, T.S.; Ozansoy, C.; Zayegh, A. Differential protection of microgrids with central protection unit support. In Proceedings of the IEEE 2013 Tencon—Spring, Sydney, Australia, 17–19 April 2013; pp. 15–19.
25. Ustun, T.S.; Ozansoy, C.; Zayegh, A. Extending IEC 61850-7-420 for distributed generators with fault current limiters. In Proceedings of the 2011 IEEE PES Innovative Smart Grid Technologies, Perth, WA, USA, 13–16 November 2011; pp. 1–8.
26. Keshan, H.; Thornburg, J.; Ustun, T.S. Comparison of lead-acid and lithium ion batteries for stationary storage in off-grid energy systems. In Proceedings of the 4th IET Clean Energy and Technology Conference, Kuala Lumpur, Malaysia, 14–15 November 2016; pp. 1–7.
27. Hussain, S.M.S.; Ustun, T.S.; Kalam, A. A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges. *IEEE Trans. Ind. Inform.* **2019**. [CrossRef]
28. Farooq, S.M.; Hussain, S.M.S.; Ustun, T.S. Performance Evaluation and Analysis of IEC 62351-6 Probabilistic Signature Scheme for Securing GOOSE Messages. *IEEE Access* **2019**, *7*, 32343–32351. [CrossRef]
29. Hussain, S.M.S.; Farooq, S.M.; Ustun, T.S. Analysis and Implementation of Message Authentication Code (MAC) Algorithms for GOOSE Message Security. *IEEE Access* **2019**, *7*, 80980–80984. [CrossRef]