Hindawi
Security and Communication Networks
Volume 2019, Article ID 9682189, 16 pages
https://doi.org/10.1155/2019/9682189

Research Article

Analyzing Reliability of the Communication for Secure and Highly Available GOOSE-Based Logic Selectivity

Peyman Jafary,[1] **Antti Supponen**,[1] **Mikko Salmenperä**,[2] **and Sami Repo**[1]

[1] *Laboratory of Electrical Energy Engineering, Tampere University of Technology, 33720, Tampere, Finland*
[2] *Laboratory of Automation and Hydraulics, Tampere University of Technology, 33720, Tampere, Finland*

Correspondence should be addressed to Peyman Jafary; peyman.jafary@tut.fi

Received 6 July 2018; Accepted 24 March 2019; Published 2 May 2019

Guest Editor: Jin Wei

Copyright © 2019 Peyman Jafary et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In an electrical distribution network, Logic Selectivity significantly reduces both the number and duration of outages. Generic Object-Oriented Substation Events (GOOSE) have a key role in the decision-making process of substation protection devices using GOOSE-based Logic Selectivity. GOOSE messages are exchanged between remote protection devices over the communication network. Secured communication with low latency and high reliability is therefore required in order to ensure reliable operation as well as meeting real-time requirement of the Logic Selectivity application. There is thus a need to evaluate feasibility of the selected communication network technology for Logic Selectivity use cases. This paper analyzes reliability of cellular 4G/LTE Internet for GOOSE communication in a Logic Selectivity application. For this purpose, experimental lab set-ups are introduced for different configurations: ordinary GOOSE communication, secured GOOSE communication by IPsec in Transport mode, and redundant GOOSE communication using the IEC 62439-3 Parallel Redundancy Protocol. In each configuration, the GOOSE retransmissions are recorded for a period of three days and the average GOOSE transmission time is measured. Furthermore, the measured data is classified into histograms and a probability value for communication reliability, based on the transmission time, is calculated. The statistical analysis shows that 4G Internet satisfies the real-time and reliability requirements for secure and highly available GOOSE-based Logic Selectivity.

1. Introduction

Smart grid distribution automation employs various methods for Medium Voltage (MV) fault management in order to supply uninterrupted power to the clients and improve the reliability of the distribution network. One method is Logic Selectivity [1, 2], which operates by distributing intelligence over Intelligent Electronic Devices (IEDs) distributed between the electrical substations. Logic Selectivity can be implemented in an interoperable manner by applying a standardized data model [3, 4] for describing the electrical functions. In addition, standard communication services, such as GOOSE [5], are used for exchanging messages between the scattered substation IEDs. Communication on top of Internet Protocol (IP) is the latest trend for intersubstation communication for IEDs. IP-based communication is challenging for the OSI model (ISO/IEC 7498-1) layer-2 GOOSE messages. This challenge can be overcome by utilizing data networking techniques between substations, such as tunneling and encapsulation [6, 7].

Intersubstation communication must be secured to protect GOOSE messages against cyber-security attacks [8]. GOOSE messages can also be duplicated (redundancy) in order to enhance data availability in the case of failure. Applying security and redundancy protocols imposes additional processing and transmission delays on GOOSE communications, which could affect Logic Selectivity timing requirements. Therefore, high-performance communication technology (capable of transmitting secured GOOSE messages between substations in real time) is required for implementing secure and highly available GOOSE-based Logic Selectivity. Nowadays, 4G Long-Term Evolution (LTE) cellular technology is being considered as a potential [9] technology for data transmission between electrical substations in smart grid automation applications.

In [1], the authors analyzed both functional and nonfunctional characteristics of standardized GOOSE-based Logic Selectivity in which protection, control, and monitoring functions were modelled [10] according to the IEC61850 standard. Moreover, Layer-2 Tunneling Protocol version 3 (L2TPv3) [11] over IPsec [12] was proposed for secure GOOSE communication over 4G/LTE.

This paper is an extension of the work originally presented by authors in [1]. This paper discusses the role of GOOSE in the functional performance of Logic Selectivity and focuses on the structure of GOOSE messages, pattern of the retransmission times, and communication over 4G/LTE. This communication causes some delay to GOOSE exchanges between IEDs. This delay must be shorter than the real-time requirement for Logic Selectivity to ensure selective operation of the protection IEDs. The reliability of the communication is analyzed by introducing lab set-ups for measuring GOOSE transmission times in different scenarios: GOOSE over L2TPv3 over IP, GOOSE over L2TPv3 over IPsec, and extended-GOOSE with Parallel Redundancy Protocol (PRP) [13] over L2TPv3 over IP/IPsec.

The goal is to measure GOOSE transmission times in the above-mentioned scenarios and investigate the reliability of the 4G/LTE Internet for the successful application of Logic Selectivity. The measured data is statistically analyzed to determine the probability that the real-time communication requirement is fulfilled. The data is analyzed with a statistical histogram classification in MATLAB. From this statistical classification, we obtain information about how the transmission time of GOOSE messages has behaved during the measurement periods. This information is equated to the behavior of transmission times in a fault scenario. Thus, we can then analyze the probability of correct Logic Selectivity, assuming that in a fault scenario the transmission time would behave as it did in the laboratory measurements. Section 2, below, explains GOOSE-based Logic Selectivity. The experimental lab set-ups for measuring GOOSE transmission times are presented in Section 3. After that, Section 4 discusses statistical analysis of the data. Finally, Sections 5 and 6 present the discussion and conclusions.

2. GOOSE-Based Logic Selectivity

In MV fault management, fault isolation and supply restoration can be managed in a centralized architecture either via Distribution Management System (DMS) intelligence [14] or by distributing the intelligence over dispersed IEDs that share an intelligent algorithm. An example of distributed algorithm is GOOSE-based Logic Selectivity algorithm [1] explained below.

2.1. Algorithm Description. Algorithm applies data that are modeled with respect to [10] IEC61850 standard. Algorithm includes three [1] stages: fault isolation by opening the closest Circuit Breaker (CB) to the fault, further reduction of the faulty area by opening the closest Switch (SW) to the fault, and supply restoration by reclosing the opened CB. The details of the algorithm and the applied IEC61850 data are described in [1, 10]. Figure 1 shows the algorithm flowchart.

The algorithm considers different parameters relating to the direction of the power flow, the present trend of substituting switches by breakers along MV feeders, the location of the substation in the distribution network, fault detection, and fault passage information. The location of each substation IED along the distribution feeder is important for the algorithm. All upstream substation IEDs should be configured to subscribe to the GOOSE blocking messages [1] published from the downstream substation IEDs. In the algorithm, the IEDs are also classified based on their control function: an IED that controls the CB is called a CB IED and an IED that controls the attached SW is known as a SW IED. If an IED controls both the CB and the SW, it is treated as both a CB IED and a SW IED.

There are four time values in the algorithm: the T_{cb}, T_{sw}, fast reclosing (R1), and slow reclosing (R2) times. In a fault condition, the algorithm is triggered in the IEDs that subsequently issue control (open/close) command in accordance with the mentioned time values, as indicated in Figure 2.

T_{cb} is the time for fault isolation by the CB IED, while T_{sw} is the time needed by the SW IED to further reduce the faulty section. There are also two reclosing times: R1 for handling temporary faults and R2 for handling permanent ones.

2.2. Algorithm Functional Performance Evaluation. The algorithm is assessed by experimenting with a hardware-in-the-loop [15] simulation in which the electrical distribution network is simulated in Real Time Digital Simulator (RTDS) [16] and the actual IEDs are externally connected to the RTDS, as shown in Figure 3.

Figure 3 shows that the simulated network consists of one Primary Substation (PS) and three Secondary Substations (SS1, SS2, and SS3). The power flow direction is from the upstream substation (PS) towards the downstream substations (SSs). In the simulated network, all the CBs and SWs are normally closed except for CB1, which is normally open. These CBs/SWs are controlled by the attached IEDs.

All the substations are equipped with real IEDs that are externally connected to RTDS as explained in [1]. These IEDs receive network measurement values (current and voltage) from RTDS, and they can control (open/close) their respective CBs and/or SWs. The IEDs are prototypes from Schneider Electric and support the intelligence required for executing the Logic Selectivity algorithm that is embedded into the IEDs. In the algorithm, IED1 is a CB IED, while IED3 and IED4 are SW IEDs. IED2 functions as both a SW IED and a CB IED. While preparing the set-up, all the upstream IEDs are configured to subscribe to the published GOOSE from the downstream IEDs. This is required by the algorithm and achieved by activating the proposed [10] IEC 61850 Logical Nodes designed for this purpose. In addition, the IEDs are connected to the Router (Cisco 892) and 4G modems (Cisco 819) in order to create GOOSE communication over the Internet via an L2TPv3 tunnel.

In order to evaluate the algorithm's performance, the IEDs' protection operations are validated during a MV fault

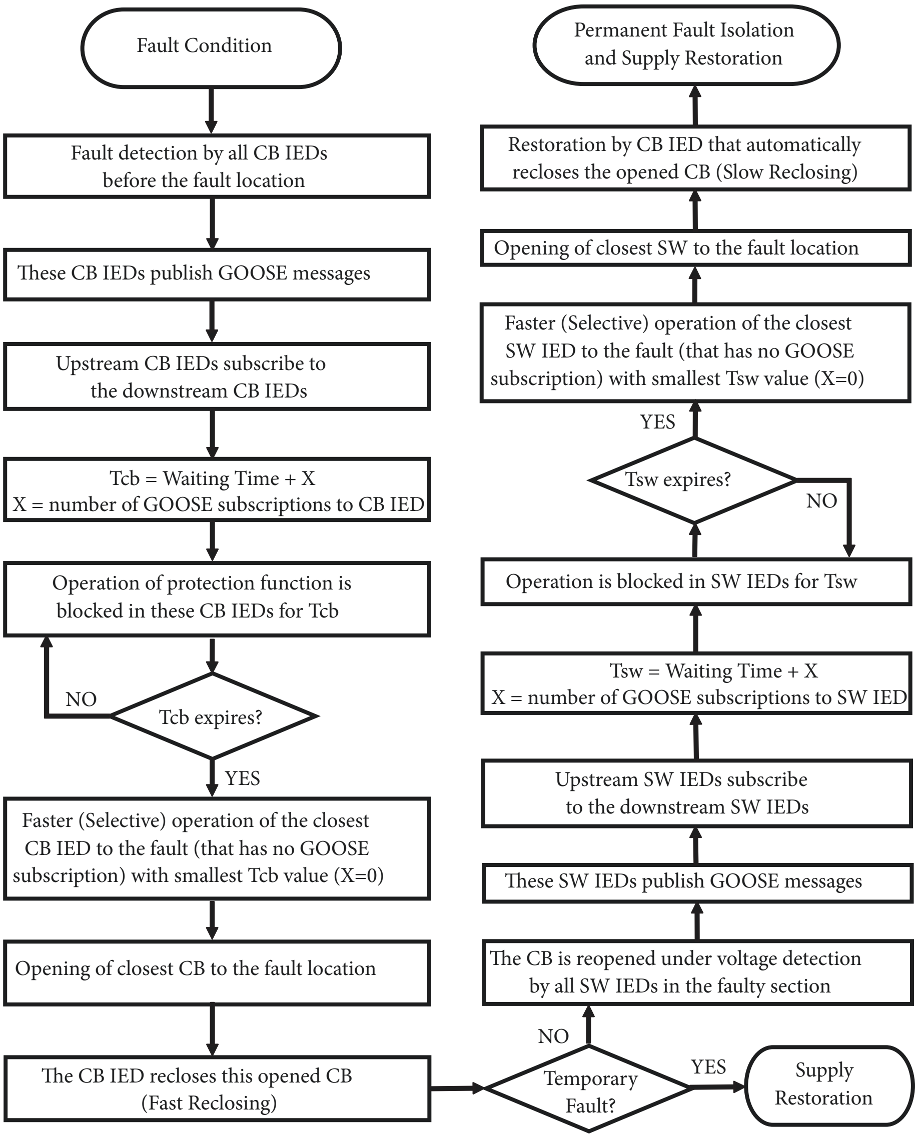

Fault Condition
Fault detection by all CB IEDs before the fault location
These CB IEDs publish GOOSE messages
Upstream CB IEDs subscribe to the downstream CB IEDs
Tcb = Waiting Time + X
X = number of GOOSE subscriptions to CB IED
Operation of protection function is blocked in these CB IEDs for Tcb
NO
Tcb expires?
YES
Faster (Selective) operation of the closest CB IED to the fault (that has no GOOSE subscription) with smallest Tcb value (X=0)
Opening of closest CB to the fault location
The CB IED recloses this opened CB (Fast Reclosing)
Temporary Fault?
YES
Supply Restoration
NO
The CB is reopened under voltage detection by all SW IEDs in the faulty section
These SW IEDs publish GOOSE messages
Upstream SW IEDs subscribe to the downstream SW IEDs
Tsw = Waiting Time + X
X = number of GOOSE subscriptions to SW IED
Operation is blocked in SW IEDs for Tsw
Tsw expires?
NO
YES
Faster (Selective) operation of the closest SW IED to the fault (that has no GOOSE subscription) with smallest Tsw value (X=0)
Opening of closest SW to the fault location
Restoration by CB IED that automatically recloses the opened CB (Slow Reclosing)
Permanent Fault Isolation and Supply Restoration

Figure 1: GOOSE-based Logic Selectivity algorithm.

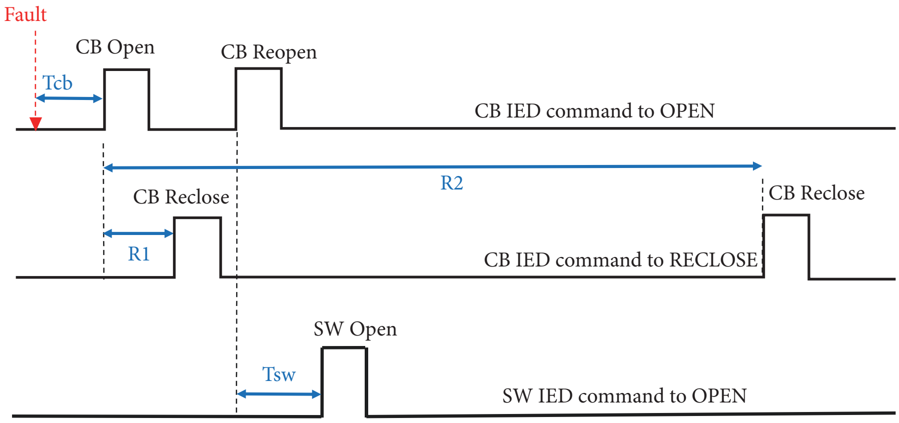


Figure 2: Algorithm time values and IEDs control commands.

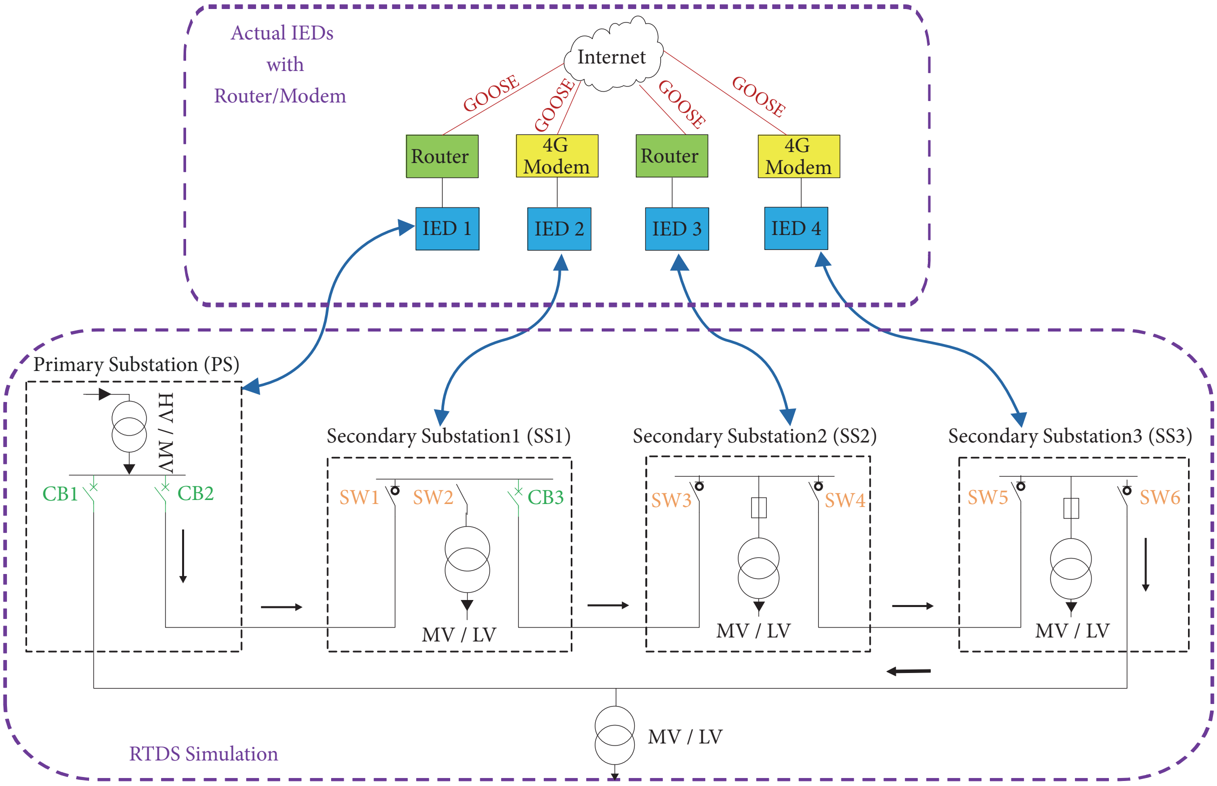


FIGURE 3: Hardware-in-loop simulation of GOOSE-based Logic Selectivity.

condition in the simulated network. Therefore, the fault simulation logic is also designed in the RTDS.

The fault logic is capable of simulating different MV faults (Phase/Phase-Phase/Three-Phase short circuit overcurrent) and different fault types (temporary and permanent) at diverse locations in the simulated model.

The simulated network in RTDS is monitored in real time by RSCAD software [16]. In RSCAD, three items are selected for real-time monitoring: the open/close commands that the RTDS receives from the attached IEDs, the status of the simulated CBs/SWs, and the electrical current value flowing in the simulated network. The algorithm's performance is evaluated by starting the fault simulation and investigating the above-mentioned items in real time. Figure 4 illustrates one example in which the algorithm's performance is assessed in the simulated electrical network for a permanent (5-second duration) three-phase short-circuit overcurrent fault between SS2 and SS3.

In Figure 4, the fault simulation is started (step1) in RSCAD. The IEDs before the fault location detect the fault current and publish GOOSE blocking messages. The first stage of the algorithm is accomplished by the CB IEDs opening the nearest CB to the fault location, that is, CB3. This is opened (step2) by tripping its attached CB IED2. The fast reclosing time (R1=300 ms) and slow reclosing (R2=30 sec) have been configured for the CB IEDs. In this test, the opened CB3 is reclosed (step3) by CB IED2 after fast reclosing time has elapsed. CB3 is commanded to reopen (step4), since the fault is permanent (5 sec duration). Then, the second stage of the algorithm comes into operation by SW IED3 that isolates the faulty section by opening (step5) the nearest SW to the fault location, that is, SW4. Finally, CB3 is commanded to reclose after passing the slow reclosing time and supply is restored. This last step is not shown in Figure 4 because Time Axis shows real-time values up to 3 seconds.

2.3. Role of GOOSE. GOOSE blocking messages affect decision-making in the algorithm by blocking the operation of any upstream IEDs during a fault condition. In the example described in Figure 4 (fault between SS2 and SS3), both CB IED1 and CB IED2 detect the fault current and start publishing GOOSE blocking messages. They wait until they have passed T_{cb} before issuing the open (trip) command. In the T_{cb} formula, the Waiting Time is constant (ex. 100 ms) and the number of GOOSE subscriptions to each CB IED determines the X value (ex. 50 ms for every subscription). In our simulation (Figure 3), the upstream CB IED is CB IED1. This is configured to subscribe to the GOOSE messages published from CB IED2, which is the only CB IED that is downstream from it in the network. Therefore, CB IED1 has a T_{cb} value containing the Waiting Time plus the time for one GOOSE subscription (e.g., 100 ms+1∗50 ms). However, CB IED2 is the nearest downstream CB IED in the network, and there are no more CB IEDs after that. Therefore, no GOOSE subscription needs be configured for CB IED2, in addition to which, and it has a smaller T_{cb} value (e.g., 100 ms+0∗50 ms). As a result, CB IED2 selectively issues a trip command before CB IED1, and the first stage of the algorithm

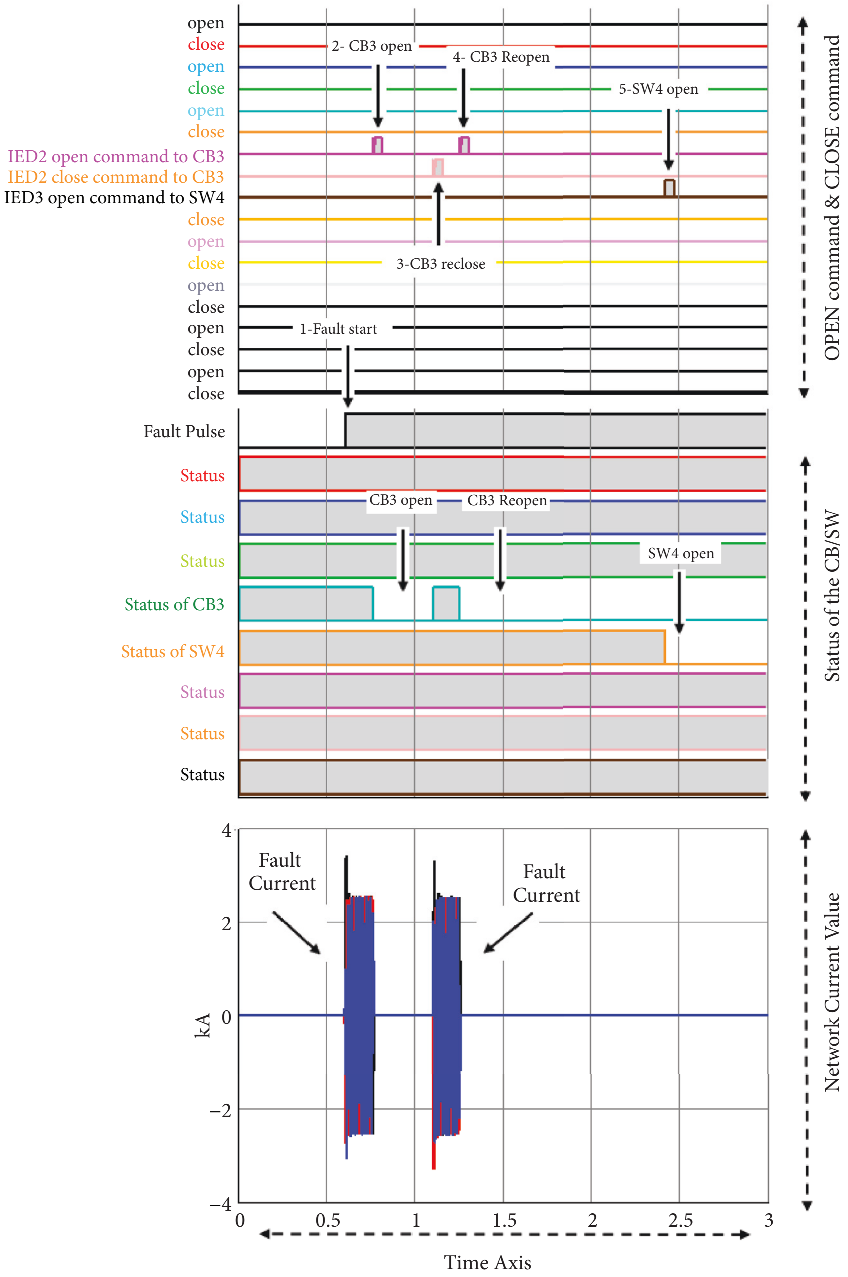


FIGURE 4: Real-time monitoring for the permanent fault between SS2 and SS3.

is thus accomplished. It is the same idea for T_{sw} in the second stage of the algorithm, but the SW IEDs (in this example SW IED2 and SW IED3) publish GOOSE blocking messages after a fault passage indication (instead of fault detection) along with under-voltage detection. It should be noted that protection operation in the upstream IED is blocked only if the published GOOSE from the downstream IED is received during the Waiting Time. Due to the importance of GOOSE messages in the algorithm, their structure and content are explained below.

The latest standard for distribution network automation is IEC 61850. This standard provides interoperability by defining hierarchical data model (IEC61850-7-1) and abstract communication services (IEC61850-7-2) for data exchange. One service is Publish/Subscribe, which is used by GOOSE (IEC61850-8-1) for event multicast and fast data exchange via data mapping to the ISO/IEC8802-3 Ethertypes. GOOSE messages are OSI model (ISO/IEC7498-1) layer 2 messages that are used for exchanging time-critical protection/interlocking data between the protection IEDs across an Ethernet LAN.

Figure 5 shows the different sections of a GOOSE message. These are defined in [5] and analyzed in detail in [17], so they are only briefly described here. The Ethernet header includes the Source and Destination addresses. The Source address is MAC (Media Access Control) address

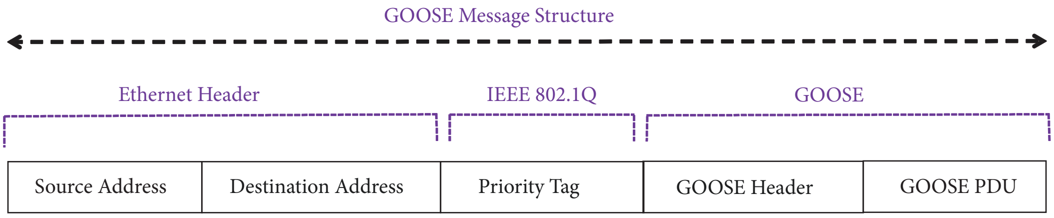


Figure 5: Structure of the GOOSE in Ethernet frame.

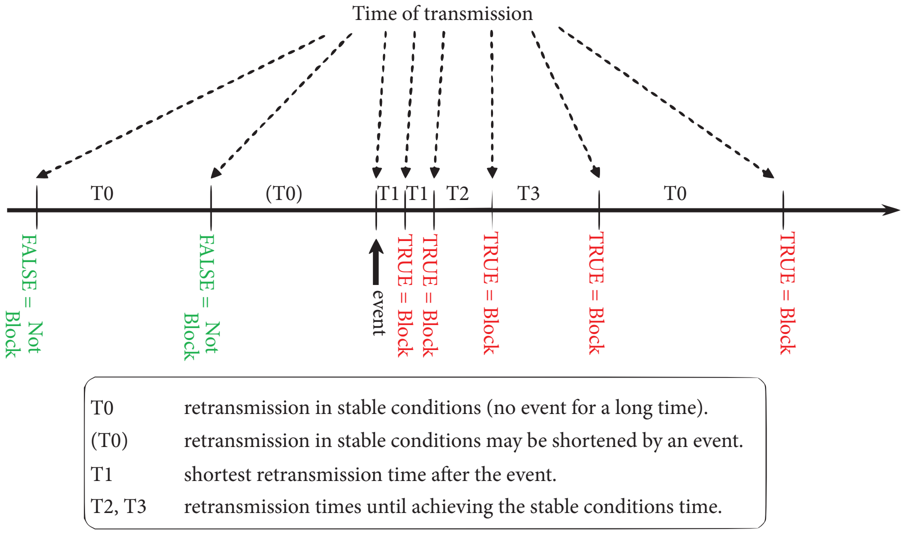

Time of transmission
T0
(T0)
T1
T1
T2
T3
T0
FALSE = Not Block
FALSE = Not Block
event
TRUE = Block
TRUE = Block
TRUE = Block
TRUE = Block
TRUE = Block
T0 retransmission in stable conditions (no event for a long time).
(T0) retransmission in stable conditions may be shortened by an event.
T1 shortest retransmission time after the event.
T2, T3 retransmission times until achieving the stable conditions time.

Figure 6: Times pattern for GOOSE messages retransmission [5].

of the IED, while the Destination address is the multicast address (01-0C-CD-01-xx-xx) defined by IEC 61850 [5] and reserved for GOOSE communication. The Priority Tag contains IEEE 802.1Q data (Tag Protocol Identifier and Tag Control Information), whose purpose is to logically separate and prioritize GOOSE traffic in the network. The GOOSE Header section includes information about the application identifier (APPID), which is a unique number that identifies the purpose of the particular data and provides information about its length. The GOOSE PDU (Protocol Data Unit) contains the data payload of the message as well as several labels relating to the timestamp, max response time, data change indication, retransmission, and so forth. This paper pays particular attention to two of these labels, the Sequence Number (SqNum) and the State Number (StNum). SqNum is an integer number that is incremented for each GOOSE transmission. StNum is an integer number that is incremented only if the data payload of the GOOSE message has changed.

In order to enhance reliability, IEC 61850 standard also proposes retransmission of GOOSE messages (with the same data payload but an incremental SqNum) in accordance with the specific pattern for time of transmission, as depicted in Figure 6.

The IEDs retransmit GOOSE in accordance with the stated strategy in Figure 6. These retransmission times are described for the IEDs in our test set-up during normal condition (no fault in the simulated network) and during fault conditions.

As discussed earlier, all the upstream IEDs (in Figure 3) are configured to subscribe to the GOOSE blocking messages published by the downstream IEDs. During a normal condition, all the IEDs periodically (within the T0 period) publish GOOSE blocking messages with a Boolean payload of FALSE that actually signifies not block-protection-operation for the recipient (subscribed) IEDs. In these GOOSE messages, only SqNum is incremented for each retransmission; StNum is not changed, since the payload has not changed. GOOSE messages are retransmitted at intervals of T0 until the occurrence of an event (i.e., starting fault in the simulated network and detecting fault current by the IEDs that run the algorithm). This shortens the T0 duration and a GOOSE message with new values (Boolean payload, SqNum, and also StNum) is generated immediately. During a fault condition, the IEDs publish GOOSE blocking messages with the Boolean payload of TRUE, which means block-protection-operation for the subscribed IEDs. These messages are retransmitted more frequently with shorter periods (T1, T2, and T3) until they reach T0.

2.4. Communication Requirements. GOOSE messages are often exchanged across a substation LAN in Horizontal Communication [18] between local IEDs at the substation Bay-level. However, GOOSE communication between remote

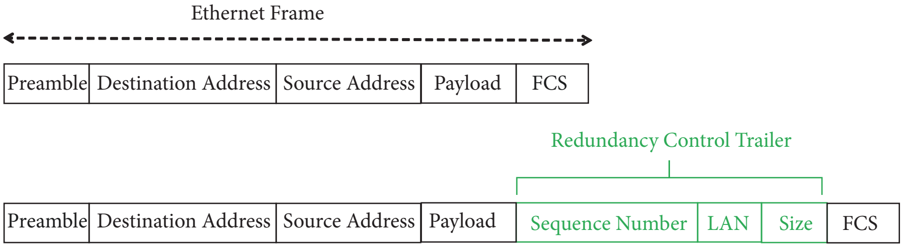


Figure 7: Ethernet frame extended by Redundancy Control Trailer (RCT).

IEDs is also required for emerging smart grid applications, such as GOOSE-based Logic Selectivity in which GOOSE should be exchanged between IEDs at remote substations. Therefore, a communication network between the substations is required. Internet-based communication is the latest trend in substation remote communication. However, such communication requires careful attention in terms of cyber-security and network determinism in order to ensure authentic and real-time functioning of the GOOSE-based Logic Selectivity. In [1], the authors analyzed these communication requirements with respect to the PICARD model [19], which addresses both cyber-security and automation requirements. Integrity and confidentiality were identified as the cyber-security requirements, while Alarm (hard real time, i.e., GOOSE must be exchanged strictly during Waiting Time) was identified as the automation requirement.

In [1], L2TPv3 over IPsec in Transport mode [20] was proposed to satisfy integrity and confidentiality requirements. In addition, the Alarm requirement was analyzed to some extent by measuring the communication characteristics. This paper looks further into Alarm requirement by applying statistical methods to analyze the measured delay in GOOSE communications in different scenarios. The paper also analyzes GOOSE exchanges in an IEC62439-3 PRP [13] network in order to increase the availability of the GOOSE messages for Logic Selectivity.

The IEC 62439-3 PRP is an Ethernet redundancy protocol that operates on layer 2 (Data Link layer) of the OSI model (ISO/IEC7498-1) and provides redundancy with zero recovery time. The PRP-enabled device duplicates the Ethernet frames and simultaneously sends two identical frames from two discrete Ethernet interfaces to two separate LANs: PRP A and PRP B. This redundant transmission is managed by the Link Redundancy Entity (LRE) [21] protocol, which duplicates each data frame.

Since the data frames are duplicated, a mechanism is required for handling the duplicated frames on the receiver side. There are two [22] mechanisms for handling these duplicates: Duplicate Accept and Duplicate Discard. In the Duplicate Accept mechanism, the receiver delivers both the original frames to the higher layer protocol and it is the task of the upper layer protocol to handle the duplicates. In the Duplicate Discard method, LRE appends Redundancy Control Trailer (RCT) [22] to the original Ethernet frame and these extended frames are sent to both LANs. The RCT section is placed between the data payload and the Frame Check Sequence (FCS) of the Ethernet frame. The RCT section contains three fields: Sequence Number, LAN identifier, and Size, as shown in Figure 7.

In the Duplicate Discard mechanism, the RCT is used for duplicate handling. In the RCT sections of the Ethernet pairs, the Sequence Number and Size fields have the same values. The only field with a different value is the LAN identifier, which has a value of either A or B, relating to PRP A and PRP B, respectively. In this method, the LRE performs duplicate filtering at the Data Link layer, so only one data frame is delivered to the upper layer. Accordingly, duplicate handling is transparent to the higher layer protocols such as GOOSE.

The Duplicate Discard mechanism is generally the preferred [22] method because it delivers only one data frame to upper layer protocol and consequently offloads the application processor. The Duplicate Discard mechanism also improves PRP network supervision, which is a further advantage over the Duplicate Accept method.

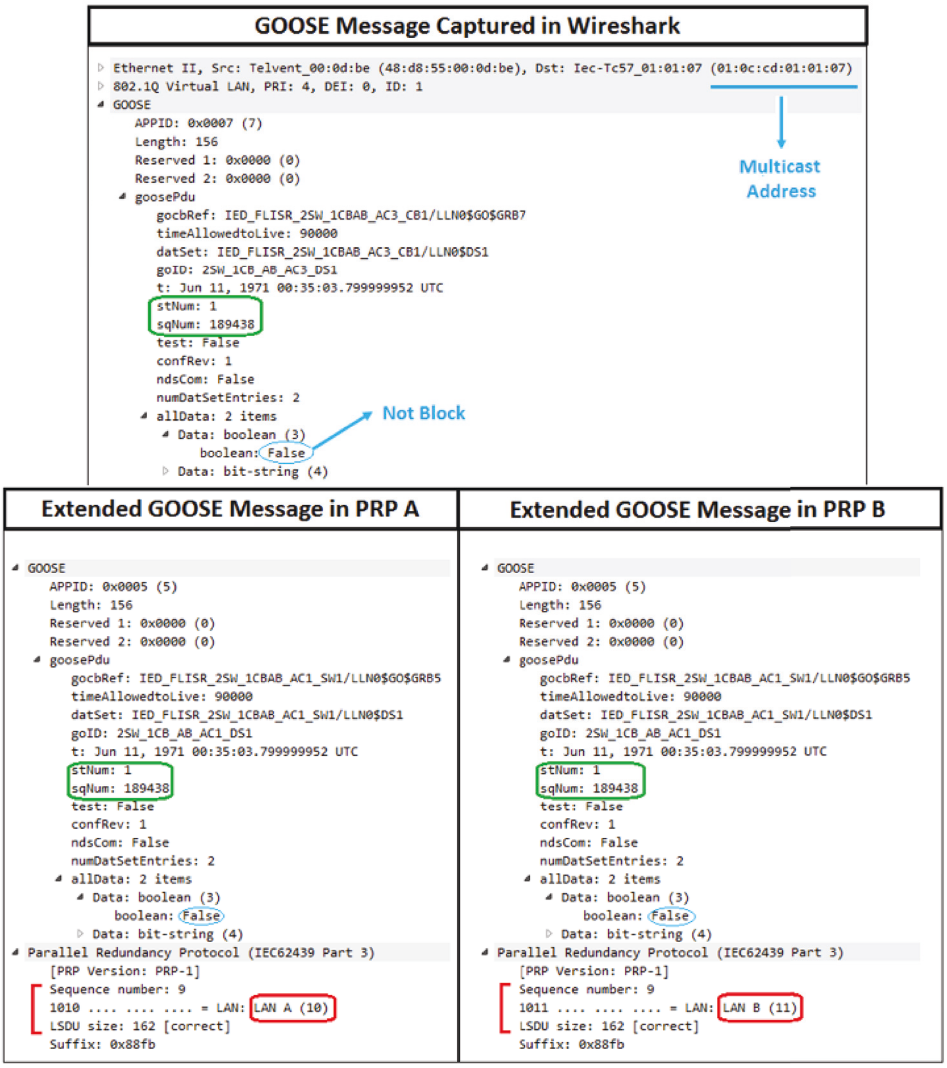
In GOOSE-based Logic Selectivity, the PRP in the Duplicate Discard mode can be used to create redundancy for the GOOSE blocking messages and increase data availability. Figure 8 is an example of one GOOSE blocking message in both its original format and in its extended format within the PRP networks, that is, PRP A and PRP B. These messages (Figure 8) were captured in the Wireshark software, which is the network packet analyzer software tool.

3. GOOSE Transmission Time Measurement

Section 2.3 stated that the upstream substation IEDs block their protection function operation only if they receive GOOSE blocking messages from the downstream substation IEDs during the Waiting Time defined in the Logic Selectivity algorithm. Therefore, any GOOSE transmission delay must be smaller than the Waiting Time. The goal of this section is to introduce the experimental lab set-ups used for measuring GOOSE transmission delay over 4G/LTE cellular communication in different scenarios: with/without cyber-security by IPsec protocol and with/without redundancy by IEC 62439-3 PRP.

3.1. GOOSE over L2TPv3 over IP/IPsec.

In [1], L2TPv3 tunnel was proposed for communication (tunneling) of the layer-2 multicast GOOSE messages over 4G/LTE Internet. L2TPv3 protocol can be carried either over User Datagram Protocol (UDP) or directly over IP/IPsec. In our case, the latter (L2TPv3 over IP/IPsec) was selected in order to minimize the



GOOSE Message Captured in Wireshark

```
▷ Ethernet II, Src: Telvent_00:0d:be (48:d8:55:00:0d:be), Dst: Iec-Tc57_01:01:07 (01:0c:cd:01:01:07)
▷ 802.1Q Virtual LAN, PRI: 4, DEI: 0, ID: 1
◢ GOOSE
    APPID: 0x0007 (7)
    Length: 156
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  ◢ goosePdu
      gocbRef: IED_FLISR_2SW_1CBAB_AC3_CB1/LLN0$GO$GRB7
      timeAllowedtoLive: 90000
      datSet: IED_FLISR_2SW_1CBAB_AC3_CB1/LLN0$DS1
      goID: 2SW_1CB_AB_AC3_DS1
      t: Jun 11, 1971 00:35:03.799999952 UTC
      stNum: 1
      sqNum: 189438
      test: False
      confRev: 1
      ndsCom: False
      numDatSetEntries: 2
    ◢ allData: 2 items
      ◢ Data: boolean (3)
          boolean: False
      ▷ Data: bit-string (4)
```

Extended GOOSE Message in PRP A

```
◢ GOOSE
    APPID: 0x0005 (5)
    Length: 156
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  ◢ goosePdu
      gocbRef: IED_FLISR_2SW_1CBAB_AC1_SW1/LLN0$GO$GRB5
      timeAllowedtoLive: 90000
      datSet: IED_FLISR_2SW_1CBAB_AC1_SW1/LLN0$DS1
      goID: 2SW_1CB_AB_AC1_DS1
      t: Jun 11, 1971 00:35:03.799999952 UTC
      stNum: 1
      sqNum: 189438
      test: False
      confRev: 1
      ndsCom: False
      numDatSetEntries: 2
    ◢ allData: 2 items
      ◢ Data: boolean (3)
          boolean: False
      ▷ Data: bit-string (4)
◢ Parallel Redundancy Protocol (IEC62439 Part 3)
    [PRP Version: PRP-1]
    Sequence number: 9
    1010 .... .... .... = LAN: LAN A (10)
    LSDU size: 162 [correct]
    Suffix: 0x88fb
```

Extended GOOSE Message in PRP B

```
◢ GOOSE
    APPID: 0x0005 (5)
    Length: 156
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  ◢ goosePdu
      gocbRef: IED_FLISR_2SW_1CBAB_AC1_SW1/LLN0$GO$GRB5
      timeAllowedtoLive: 90000
      datSet: IED_FLISR_2SW_1CBAB_AC1_SW1/LLN0$DS1
      goID: 2SW_1CB_AB_AC1_DS1
      t: Jun 11, 1971 00:35:03.799999952 UTC
      stNum: 1
      sqNum: 189438
      test: False
      confRev: 1
      ndsCom: False
      numDatSetEntries: 2
    ◢ allData: 2 items
      ◢ Data: boolean (3)
          boolean: False
      ▷ Data: bit-string (4)
◢ Parallel Redundancy Protocol (IEC62439 Part 3)
    [PRP Version: PRP-1]
    Sequence number: 9
    1011 .... .... .... = LAN: LAN B (11)
    LSDU size: 162 [correct]
    Suffix: 0x88fb
```

Figure 8: GOOSE blocking message in original and extended formats.

communication overhead bits that are added to the original GOOSE messages.

While L2TPv3 over IP communication has no cybersecurity measures, L2TPv3 over IPsec communication contains Encapsulating Security Payload (ESP) [20] security mechanisms that provide integrity, confidentiality, and authentication for GOOSE communication between substations. Figure 9 shows the structure of the GOOSE messages transmitting in both unsecured (L2TPv3 over IP) and secured (L2TPv3 over IPsec) tunnels.

The GOOSE exchange in the L2TPv3 tunnel involves a transmission delay caused by the added communication overheads as well as a communication network delay. Figure 10 introduces the lab set-up for GOOSE transmission in unsecured and secured tunnels.

In Figure 10, the IEDs publish GOOSE messages in accordance with the strategy (T0 in stable condition) indicated in Figure 6. The IEDs are attached to the Router/4G Modem that supports the L2TPv3 protocol and creates Internet communication for the GOOSE blocking messages.

SENSOR is a PC with several Ethernet network interface cards and Wireshark software. In SENSOR, Ethernet port 1 is connected to the router mirror port and Ethernet port 2 is connected to 4G Modem mirror port. The mirror ports monitor network traffic and provide GOOSE traffic for Wireshark software, which records this traffic on both Ethernet ports simultaneously. We recorded GOOSE traffic for a period of three days in two configurations: L2TPv3 over IP and L2TPv3 over IPsec. Thus, two sets of Wireshark files were recorded.

These Wireshark files are used as the references for measuring GOOSE transmission delay and for other statistical analyses. The GOOSE content of the each file is exported from Wireshark and saved as a CSV (Comma Separated Values) file. Transmission delay can be measured by calculating the time difference between two GOOSE messages with similar

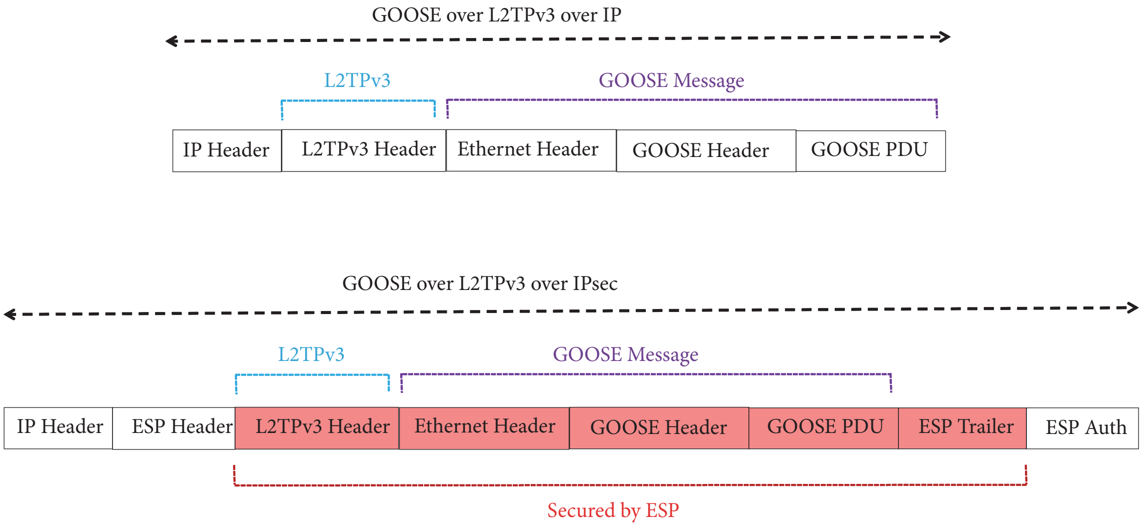


Figure 9: GOOSE message over L2TPv3 over IP/IPsec.

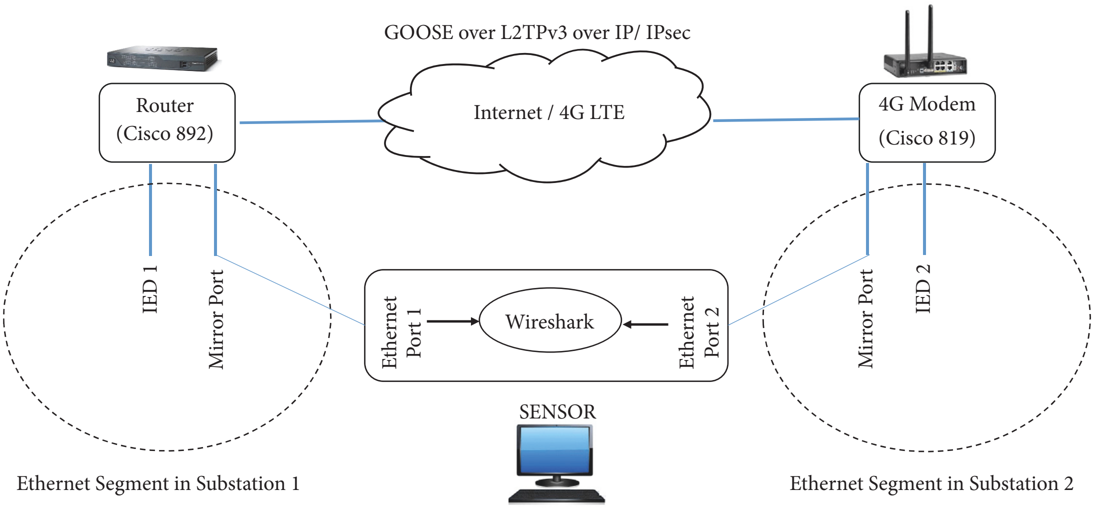


Figure 10: Lab set-up for measuring GOOSE transmission time.

data (StNum, SqNum, and Boolean value) but different Ethernet port numbers. Figure 11 shows an example of how the transmission time for one GOOSE message is calculated.

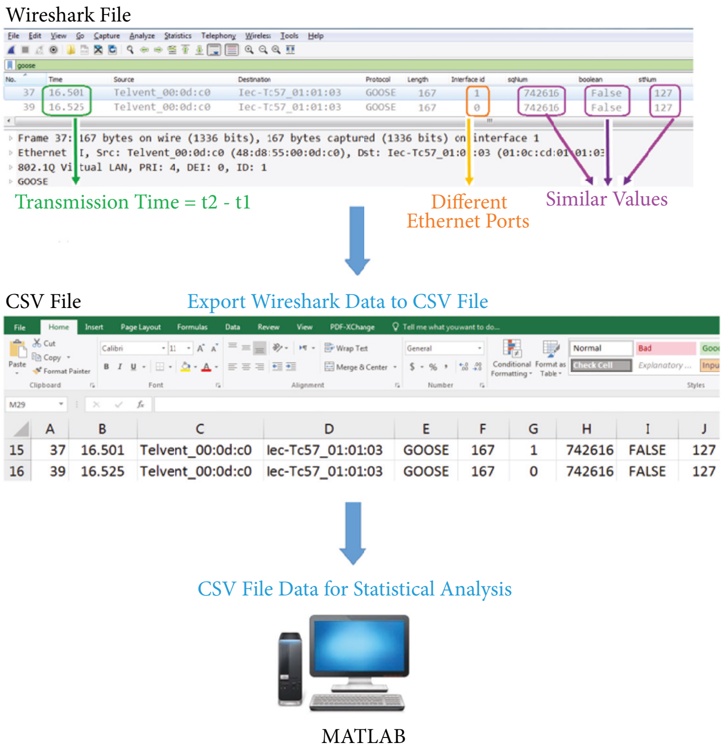
The transmission time calculation and other statistical analyses of the CSV files were carried out in MATLAB environment, as will be explained in Section 4.

3.2. Extended-GOOSE over L2TPv3 over IP/IPsec. Section 2.4 explained that GOOSE messages can be extended with RCT and sent in PRP networks. In our tests, the IEDs have no built-in support for IEC 62439-3 PRP. Thus, additional PRP devices were required in order to create extended-GOOSE. Figure 12 presents the lab set-up for creating extended-GOOSE messages transmitting in both unsecured and secured tunnels.

Extended-GOOSE messages are created by using PRP Ethernet switch (ABB AFS660) that contains both normal and PRP Ethernet ports. The normal Ethernet port of switch receives the original GOOSE from the IED, appends the RCT, and sends two extended-GOOSE messages to the PRP A and PRP B Ethernet ports, whose formats were shown earlier in Figure 8.

The PRP Ethernet ports (PRP A and PRP B) are connected to the respective router/4G modem that exchanges extended-GOOSE over the 4G/LTE Internet. Figure 13 shows the structure of the extended-GOOSE messages exchanged between the Router and 4G Modem in unsecured and secured tunnels.

The extended-GOOSE transmission delay is calculated in the same way as was explained for normal GOOSE transmissions in the previous subsection. In SENSOR, two sets of Wireshark files (L2TPv3 over IP and L2TPv3 IPsec) are also recorded for this experimental set-up. However, in this set-up, Ethernet ports of SENSOR are connected to the normal Ethernet ports in the PRP switches, instead of the mirror ports in the Router/4G Modem. This was done in


Wireshark File
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
goose
Transmission Time = t2 - t1
Different
Ethernet Ports
Similar Values
CSV File
Export Wireshark Data to CSV File
File Home Insert Page Layout Formulas Data Review View PDF-XChange Tell me what youwant to do...
Cut
Copy
Format Painter
Paste
Clipboard
Calibri
11
Font
Wrap Text
Merge & Center
Alignment
General
Number
Conditional Formatting
Format as Table
Normal
Bad
Good
Check Cell
Explanatory ...
Input
Styles
M29
CSV File Data for Statistical Analysis
MATLAB

```
No.   Time     Source              Destination          Protocol  Length  Interface id  sqNum   boolean  stNum
  37  16.501   Telvent_00:0d:c0    Iec-Tc57_01:01:03    GOOSE     167     1             742616  False    127
  39  16.525   Telvent_00:0d:c0    Iec-Tc57_01:01:03    GOOSE     167     0             742616  False    127

Frame 37: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface 1
Ethernet II, Src: Telvent_00:0d:c0 (48:d8:55:00:0d:c0), Dst: Iec-Tc57_01:01:03 (01:0c:cd:01:01:03)
802.1Q Virtual LAN, PRI: 4, DEI: 0, ID: 1
GOOSE
```

	A	B	C	D	E	F	G	H	I	J
15	37	16.501	Telvent_00:0d:c0	Iec-Tc57_01:01:03	GOOSE	167	1	742616	FALSE	127
16	39	16.525	Telvent_00:0d:c0	Iec-Tc57_01:01:03	GOOSE	167	0	742616	FALSE	127

Figure 11: Exporting data from Wireshark to CSV file for statistical analysis.

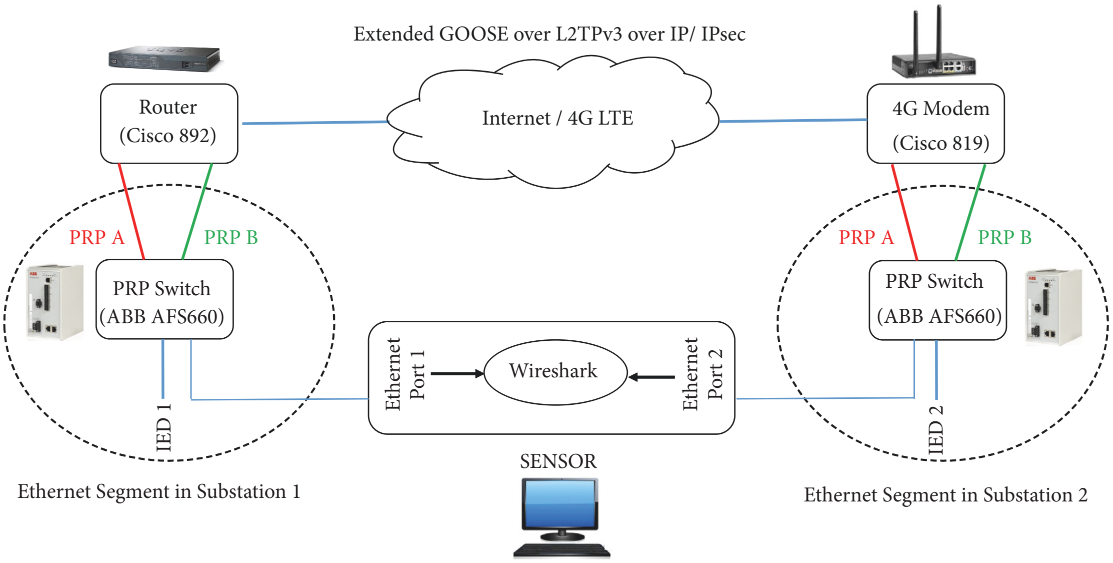


Figure 12: Lab set-up for measuring extended-GOOSE transmission time.

order to measure the end-to-end GOOSE communication delay. The Wireshark files were also recorded over three days for this experiment. These Wireshark files are also saved as CSV files, which can be used for calculating extended-GOOSE transmission delay as well as for further statistical analysis that will be explained in Section 4.

In case of extended-GOOSE, data availability can be further enhanced by duplicating the communication channel in order to maximize network availability. This requires an additional router/4G modem in each substation in which PRP A and PRP B connect to two separate routers/4G modems, as shown in Figure 14.

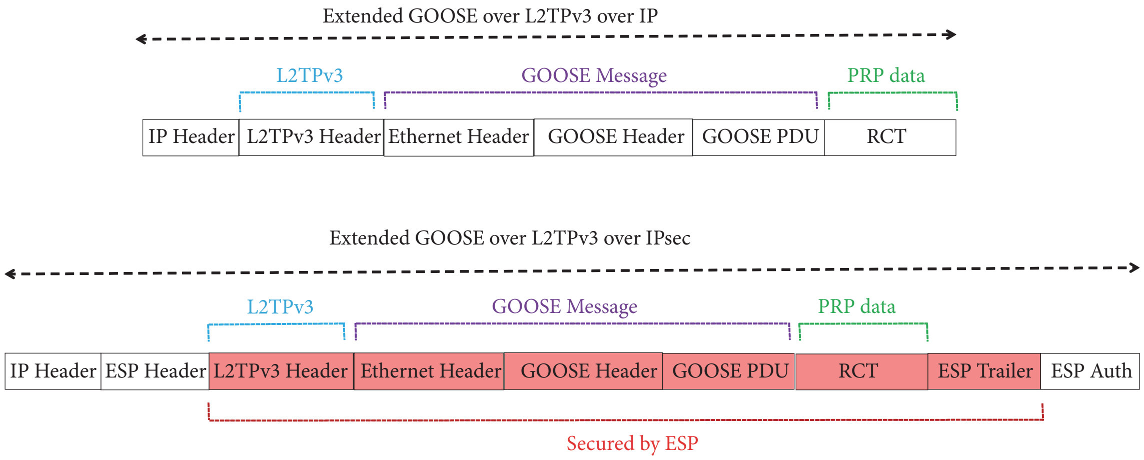


Figure 13: Extended-GOOSE message over L2TPv3 over IP/IPsec.

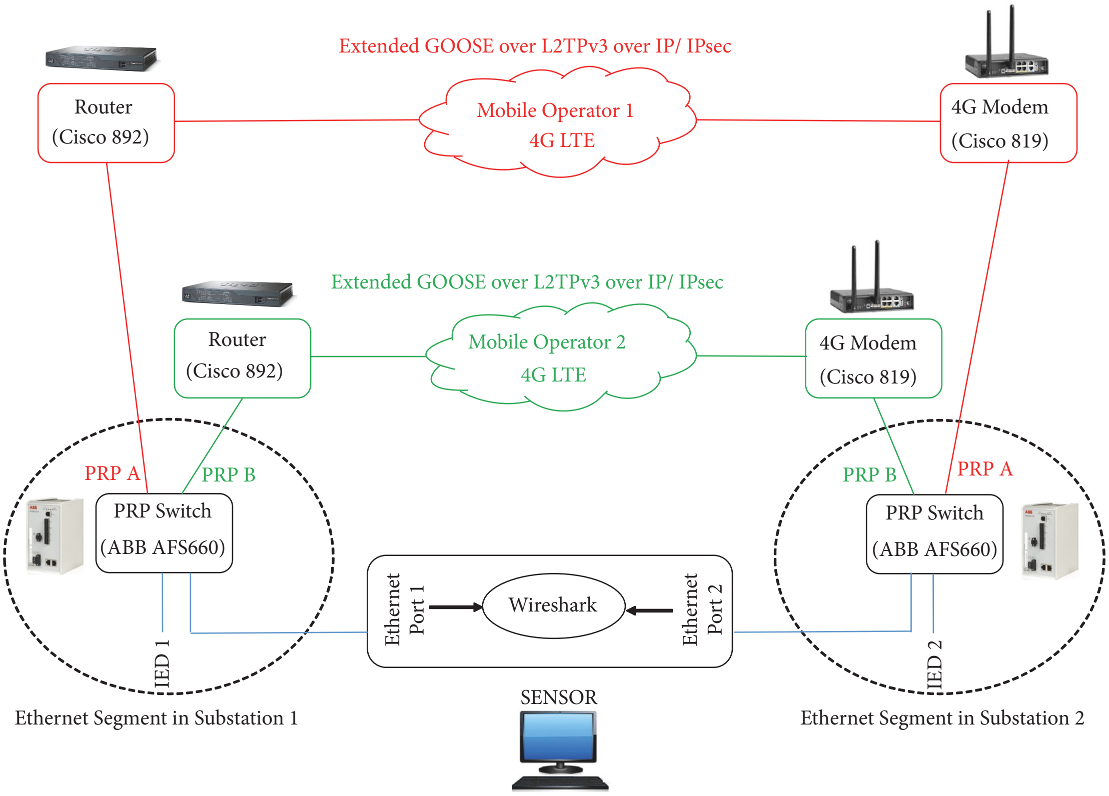


Figure 14: Lab set-up for measuring duplicated extended-GOOSE transmission time.

The depicted lab set-up (Figure 14) is applied to extended-GOOSE transmissions while using two separate communication networks. In SENSOR, again two sets (with and without security) of files are recorded for about three days. This results in two new CSV files that will be used for the duplicated extended-GOOSE transmission delay calculation and other statistical analyses that are explained in the following Section.

4. Statistical Analysis of the Measured Data

This section discusses the statistical analysis of the data recorded over three days, saved as CSV files, and used in a MATLAB computing environment. A total of six CSV files were created corresponding to the lab set-ups described in the previous Section, that is, Figures 10, 12, and 14. Each lab set-up provides two CSV files: one file for the unsecured GOOSE

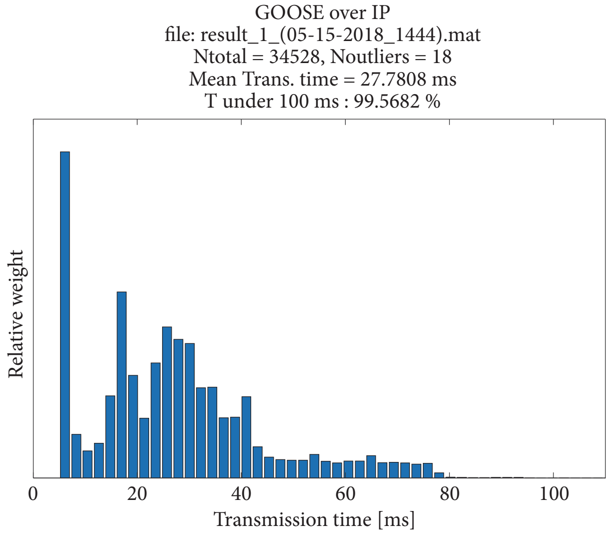


FIGURE 15: Histogram of transmission times in GOOSE over IP.

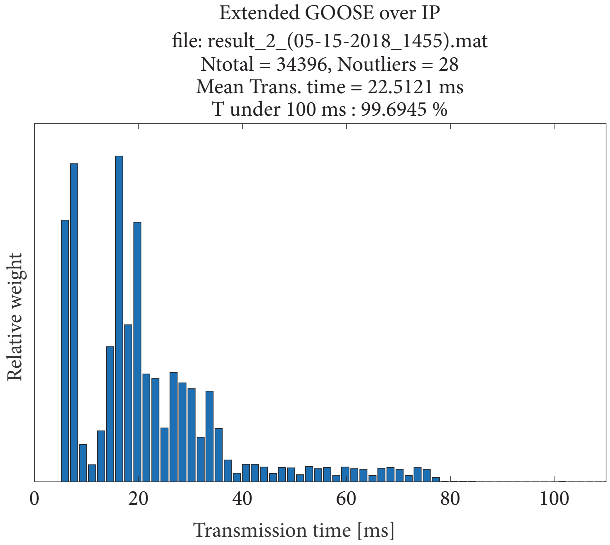


FIGURE 16: Histogram of transmission times in extended-GOOSE over IP.

transmissions (L2TPv3 over plain IP) and one file for the secure GOOSE transmissions (L2TPv3 over IPsec).

The aims are to calculate the average GOOSE transmission delay and the probability of communication reliability in each configuration. This is accomplished by programming the logic in MATLAB, which reads the CSV file of each configuration. Then, it calculates the GOOSE transmission delay by comparing the timestamps of each unique GOOSE message in the recorded CSV file. The mean value of the transmission delay is calculated for the recorded GOOSE messages. Finally, the probability of communication reliability is analyzed by counting the number of GOOSE messages that do not fill the reliability requirement and comparing this number with the total number of GOOSE messages sent during the recording period.

The GOOSE messages that do not appear on both interfaces of the Wireshark recording are regarded as lost messages or outliers. In addition, those GOOSE messages whose transmission time was longer than 300 ms are also regarded as outliers. The results of these MATLAB analyses are shown in Figures 15–20. Each figure contains the topic that indicates the respective lab set-up, total number of recorded GOOSE messages in the three-day period, the number of outliers, the mean value of the GOOSE transmission times, and the calculated percentage for the measured transmission times that are under the limit, that is, Waiting Time (100 ms).

Figures 15–20 present the observed distribution of the transmission times in our measured data from the experimental lab set-ups. In case of GOOSE over IP/IPsec, the delay in copying GOOSE messages to the mirror ports has also been added to the transmission times.

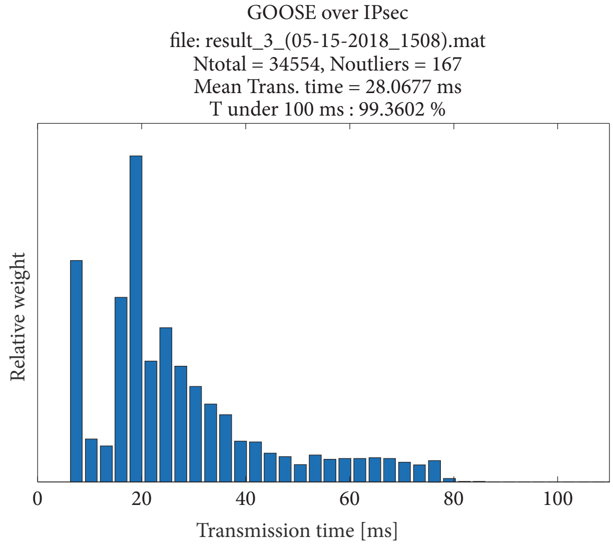


Figure 17: Histogram of transmission times in GOOSE over IPsec.

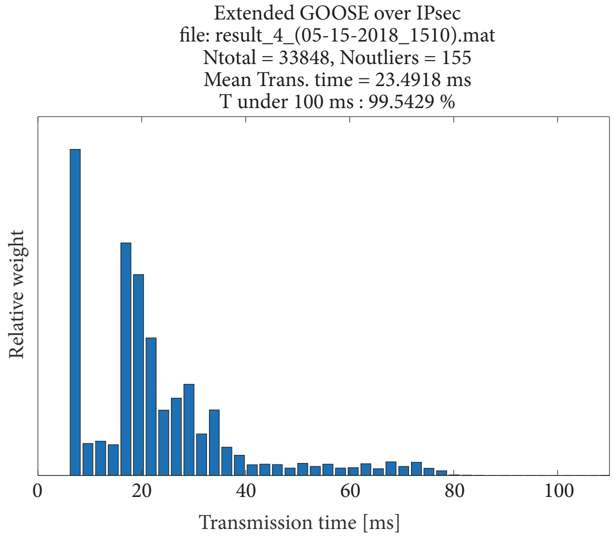


Figure 18: Histogram of transmission times in extended-GOOSE over IPsec.

As can be seen from Figures 15–20, the underlying statistical behavior of the transmission times does not seem to fit any standard probability distribution function. From statistical analysis point of view, any future work should focus on finding out the parameters of the underlying statistical mechanism so that a forecast model for the GOOSE transmission times can be created.

5. Discussion

In the GOOSE-based Logic Selectivity algorithm, T_{cb} and T_{sw} have key roles in the selective operation of the protection IEDs. These values make the operation times of the upstream IEDs greater than those of the downstream IEDs because of the value of X, as is shown in Figure 21.

Every upstream IED subscribes to the GOOSE published by its corresponding downstream IED. In each IED, the T_{cb} and T_{sw} timers are triggered after the event which is fault detection for T_{cb} and fault passage and under-voltage detection for T_{sw}. The Waiting Time is a constant value but X is variable. Thus, T_{cb} and T_{sw} are functions of the X variable in each IED. The number of GOOSE subscriptions to each IED determines the value of X and, consequently, T_{cb} and T_{sw} for each IED. The number of GOOSE subscriptions depends on the location of the IED in the electrical network. The upstream IED subscribes to the published GOOSE from both the intermediate and downstream IEDs. As a result, the upstream IED has the largest value for X. The downstream IED has zero GOOSE subscriptions because there is no IED after that. This results in X being equal to zero and minimum

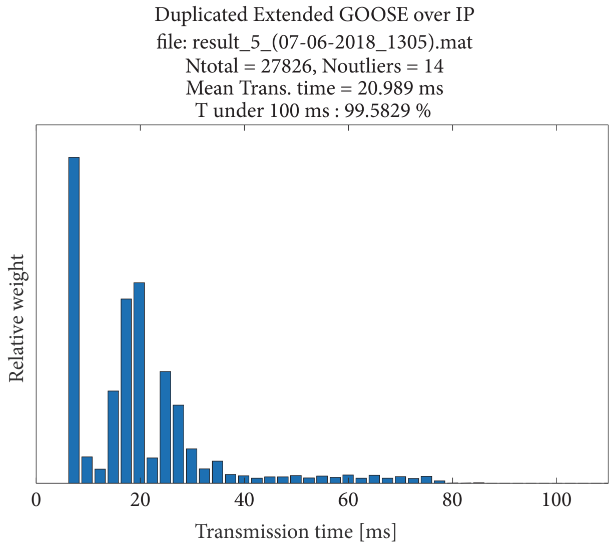


Figure 19: Histogram of transmission times in duplicated extended-GOOSE over IP.

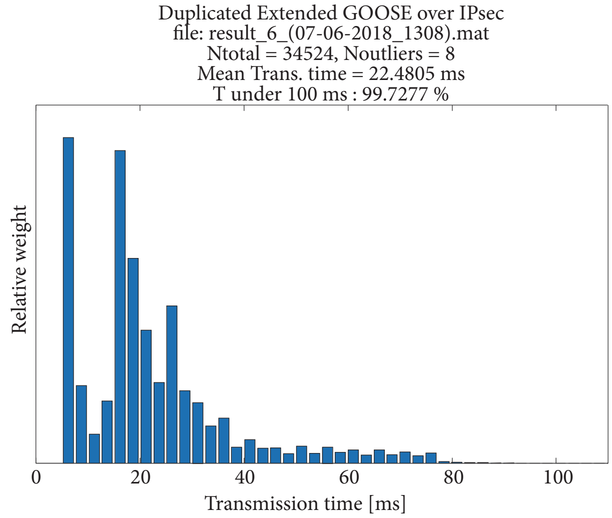


Figure 20: Histogram of transmission times in duplicated extended-GOOSE over IPsec.

values for T_{cb} and T_{sw}. In fact, the value of the X variable provides selective operation of IEDs. The idea behind the X variable is that each upstream IED allows time for its downstream IED to either clear the fault (in case of T_{cb}) or reduce the faulty section (in case of T_{sw}).

The important point here is that the subscription of each upstream IED to the GOOSE published by its downstream IEDs must occur within the Waiting Time. In other words, after passing the Waiting Time, every upstream IED waits for an additional X value (i.e., it delays sending its trip signal) only if it has received the expected GOOSE blocking messages from its downstream IED. If an upstream IED receives a GOOSE blocking message during the Waiting Time, then the IED blocks its protection operation for the additional time, X, and subsequently increases its Tcb and T_{sw} values. Otherwise, T_{cb} and T_{sw} values are not increased in the upstream IED and both the upstream and downstream IEDs will have the same T_{cb}/T_{sw} values (Waiting Time + 0) and will thus operate simultaneously after they have passed the Waiting Time. In this case, the algorithm operation is not selective.

Accordingly, the IEDs make selective decisions by detecting the fault current (or fault passage and under-voltage) and also by receiving GOOSE blocking messages from the downstream IEDs during the Waiting Time. Hence, GOOSE exchange during Waiting Time is an important criterion that must be fulfilled for the GOOSE-based Logic Selectivity algorithm to work successfully. The value of the Waiting Time is determined by considering several factors such as the number of protection stages in the electrical network, the types of fault (ex. ANSI 50, ANSI 51 or ANSI 67N), the magnitude of the fault current, the thermal capability of the

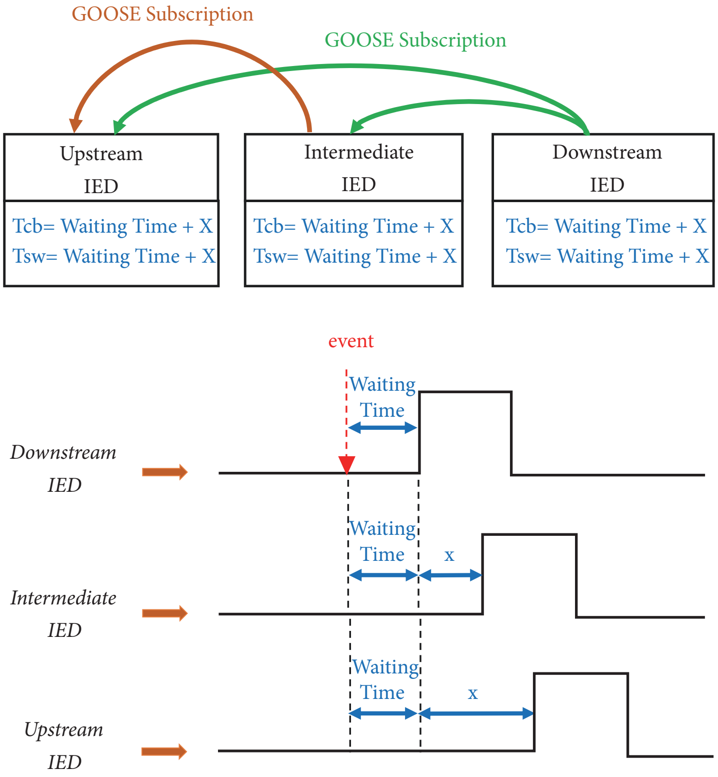


Figure 21: Time setting of IEDs for issuing trip commands.

line section, and the ability of the switching devices to tolerate the fault current.

The value of the Waiting Time is in the order of milliseconds. In our experiment, Waiting Time was selected to be 100 ms, which meant that selective operation of the algorithm required the IEDs to exchange the GOOSE blocking messages in less than 100 ms; that is, the GOOSE Internet communication delay had to be less than 100 ms. This highlights the importance of communication reliability, since this affects the protection function and the selective operation of the IEDs

The statistical analysis shows that, in the case of our laboratory set-ups, the transmission speed and reliability are sufficient for a real application. The risk of loss of selectivity due to communication failure is relatively low. Even at their worst, 99.4% of the communicated packages fulfilled the real-time requirement of Logic Selectivity. However, it is important to bear in mind that this number only represents the reliability of the transmissions in a laboratory set-up. In order to use the information obtained from the GOOSE transmission time in real-life applications, additional analyses are required. Most importantly, the cross-correlations of transmission times in the case of multiple communicating IEDs still require further measurement and analysis.

In addition, the allowable level of required reliability needs to be assessed case by case. In the context of this paper, we have identified that over 99% reliability in communication is considered “good enough.” In real-life applications, however, lower or higher values for reliability may be required. These requirements should be based on a risk analysis of the effects of loss-of-selectivity.

GOOSE-based Logic Selectivity is an efficient MV fault management method that provides rapid fault isolation and restoration of the power supply via dynamic reconfiguration of the IEDs communicating by GOOSE. Furthermore, GOOSE-based Logic Selectivity offers interoperability, high scalability (adding a new IED to the system only entails updating the subscription list of the upstream IEDs), and distributed control architecture, all of which meet the requirements of state-of-the-art smart grids approaches, such as decentralized [23] distribution automation. However, a reliable communication network is required for GOOSE exchange. In practice, time-based [1] Selectivity should also be designed as the back-up fault isolation solution in case of poor-quality communication or communication failure. The communication quality can be supervised by checking the arrival of GOOSE messages in the prescribed arrival period, T0, as was shown in Figure 6. IEDs can be programmed to switch their logic from GOOSE-based Logic Selectivity to time-based Selectivity if the GOOSE blocking messages are not periodically received during the T0 time interval. These periodic GOOSE messages can be regarded as the heartbeat of the system, and if they do not occur regularly within the predefined time period (T0), then this indicates communication failure or low service quality.

6. Conclusion

This experiment investigated the feasibility of using cellular 4G/LTE Internet for normal and extended-GOOSE communication in an unsecure/secure tunnel via one/duplicated communication channel. The communication reliability and latency were analyzed for the GOOSE retransmissions. In all the studied configurations, communication reliability was satisfactory and the average GOOSE transmission delay stayed well under the 100 ms upper limit set for our GOOSE-based Logic Selectivity application.

Although all the configurations meet the reliability and real-time requirements of our use cases, extended-GOOSE messages transmitting in secured tunnel/s by IPsec are the preferred configuration. This configuration not only enhances GOOSE availability but also protects GOOSE communication against cyber-security attacks. This leads to reliable and authentic operation of GOOSE-based Logic Selectivity and consequently dependable automation of an electrical distribution network.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] P. Jafary, O. Raipala, S. Repo et al., “Secure layer 2 tunneling over IP for GOOSE-based logic selectivity,” in *Proceedings of the 2017 IEEE International Conference on Industrial Technology (ICIT)*, pp. 609–614, IEEE, 2017.

[2] D. Pala, G. Proserpio, E. Bionda, S. Pugliese, and D. Della Giustina, “IEC CIM-61850 harmonization - The logic selectivity case,” in *Proceedings of the 16th International Conference on Environment and Electrical Engineering, EEEIC 2016*, pp. 1–15, IEEE, June 2016.

[3] T. Berry and L. Guise, “IEC61850 for distribution feeder automation,” in *Proceedings of the IET International Conference on Resilience of Transmission and Distribution Networks, RTDN 2015*, September 2015.

[4] A. Dede, D. D. Giustina, F. Franzoni, and A. and, “IEC 61850-based logic selectivity scheme for the MV distribution network,” in *Proceedings of the Applied Measurements for Power Systems Proceedings (AMPS)*, pp. 1–5, 2014.

[5] IEC 61850 standard, part 8-1, Communication networks and systems in substations, “Specific Communication Service Mapping (SCSM)-Mapping to MMS and to ISO/IEC 8802-3,” 1st edition, 2004.

[6] C. H. R. de Oliveira and A. P. Bowen, “Iec 61850 goose message over wan,” in *Proceedings of the International Conference on Wireless Networks (ICWN12)*, Las Vegas, Nevada, 2012.

[7] S. M. Blair, F. Coffele, C. D. Booth, B. De Valck, and D. Verhulst, “Demonstration and analysis of IP/MPLS communications for delivering power system protection solutions using IEEE C37. 94, IEC 61850 Sampled Values, and IEC 61850 GOOSE protocols,” 2014.

[8] W. Wang and Z. Lu, “Cyber security in the smart grid: survey and challenges,” *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[9] P. Ferrari, A. Flammini, M. Loda, S. Rinaldi, D. Pagnoncelli, and E. Ragaini, “First experimental characterization of LTE for automation of smart grid,” in *Proceedings of the 6th IEEE International Workshop on Applied Measurements for Power Systems, AMPS 2015*, IEEE, Germany, September 2015.

[10] A. A. Sotomayor, D. Della Giustina, G. Massa, A. Dedè, F. Ramos, and A. Barbato, “IEC 61850-based adaptive protection system for the MV distribution smart grid,” *Sustainable Energy, Grids and Networks*, 2017.

[11] Layer 2 Tunneling Protocol version 3, https://tools.ietf.org/html/rfc3931.

[12] Securing L2TP using IPsec, https://tools.ietf.org/html/rfc3193.

[13] IEC 62439-3, “Industrial communication networks - High availability automation networks,” in *Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)*, part 3, 3rd edition, 2016.

[14] P. Jafary, S. Repo, and H. Koivisto, “Security solutions for smart grid feeder automation data communication,” in *Proceedings of the 2016 IEEE International Conference on Industrial Technology, ICIT 2016*, pp. 551–557, IEEE, Taiwan, March 2016.

[15] V. Tuominen, H. Reponen, A. Kulmala, S. Lu, and S. Repo, “Real-time hardware- and software-in-the-loop simulation of decentralised distribution network control architecture,” *IET Generation, Transmission & Distribution*, 2017.

[16] Real-Time Digital Simulator, https://www.rtds.com/.

[17] C. Kriger, S. Behardien, and J.-C. Retonda-Modiya, “A detailed analysis of the GOOSE message structure in an IEC 61850 standard-based substation automation system,” *International Journal of Computers, Communications & Control*, vol. 8, no. 5, pp. 708–721, 2013.

[18] P. Jafary, S. Repo, J. Seppala, and H. Koivisto, “Security and reliability analysis of a use case in smart grid substation automation systems,” in *Proceedings of the 2017 IEEE International Conference on Industrial Technology, ICIT 2017*, pp. 615–620, IEEE, Canada, March 2017.

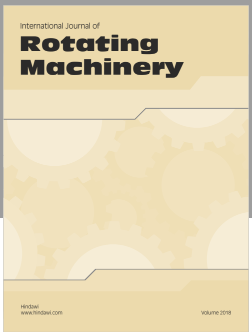
[19] J. Seppälä and M. Salmenperä, “Towards dependable automation,” in *Cyber Security: Analytics, Technology and Automation*, vol. 78, pp. 229–249, Springer, 2015.

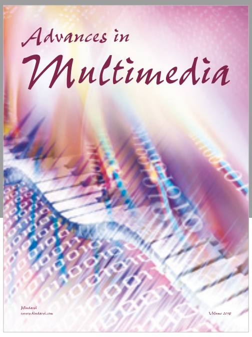
[20] Security for Internet Protocol. https://tools.ietf.org/html/rfc2401.

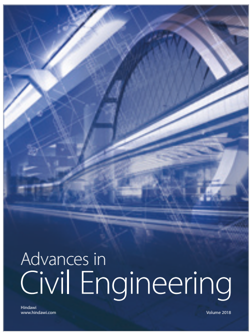
[21] H. Kirrmann, M. Hansson, and P. Müri, “IEC 62439 PRP: Bumpless recovery for highly available, hard real-time industrial networks,” in *Proceedings of the 12th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA 2007*, pp. 1396–1399, IEEE, Greece, 2007.

[22] H. Weibel, *Tutorial on Parallel Redundancy Protocol (PRP)*, Zurich University of Applied Sciences, 2011.

[23] S. Repo, F. Ponci, A. Dede et al., “Real-time distributed monitoring and control system of MV and LV distribution network with large-scale distributed energy resources,” in *Proceedings of the PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe, 2016)*, pp. 1–6, IEEE, 2016.







Hindawi

Submit your manuscripts at
www.hindawi.com