IEC 61850 Network Cybersecurity: Mitigating GOOSE Message Vulnerabilities

Mauricio Gadelha da Silveira and Paulo Henrique Franco
Schweitzer Engineering Laboratories, Inc.

Presented at the
6th Annual PAC World Americas Conference
Raleigh, North Carolina
August 20–22, 2019

IEC 61850 Network Cybersecurity: Mitigating GOOSE Message Vulnerabilities

Mauricio Gadelha da Silveira and Paulo Henrique Franco, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—The IEC 61850 standard defines the organization and communication of protection, automation, and control information over Ethernet networks in a power substation. This makes the security and reliability of the electric power system directly dependent on the security and reliability of the communications network. The communications network is a conduit for malicious attacks in a substation that can cause material and operational damage. This paper explores security weaknesses in the Generic Object-Oriented Substation Event (GOOSE) protocol and how to mitigate them using managed switches and software-defined networking (SDN).**

I. Introduction

Until recently, electric power substations operated their control and protection schemes through proprietary control cables, contact sets, and communications protocols [1]. Information was communicated using hardwired, point-to-point connections. However, the potential benefits of Ethernet communications technology and substation automation have led to standardization that allows the exchange of information among equipment from different manufacturers. The IEC 61850 standard defines how data are organized to give them semantic meaning and how information is transmitted and processed. The standard defines a client-server communications model that is implemented with the Manufacturing Message Specification (MMS) protocol, and it defines a publisher-subscriber communications model that is implemented with Generic Object-Oriented Substation Event (GOOSE) and Sampled Value (SV) protocols. MMS is used to communicate information between intelligent electronic devices (IEDs) and supervisory control and data acquisition (SCADA), while GOOSE and SV are used to communicate information between IEDs.

GOOSE is a Layer 2 protocol, i.e., messages are transported over Ethernet, and it is described in IEC 61850-8-1 [2]. The need for high-speed performance in GOOSE and the limited processing power in IEDs has led to implementations that do not include security mechanisms such as publisher authentication and message encryption. Attack techniques such as GOOSE saturation and GOOSE frame manipulation exploit this open implementation, which can be used to degrade the operation of a substation or cause misoperation. The GOOSE saturation technique is used to flood the network with GOOSE messages that are identical to the ones transmitted by a publisher, thus making it difficult to properly process messages sent by the true publisher. The GOOSE frame manipulation technique operates by changing values in the GOOSE message, which may cause the subscriber to discard subsequent messages from the true publisher or cause the subscriber to fail.

These attack techniques take advantage of security gaps that exist in the GOOSE protocol, but they can be prevented with proper network engineering in the substation. Best practices in network configuration can be used to mitigate these and other forms of attacks in substations.

This paper is based on [3] and is expanded to include new mitigation technologies, practices, strategies, and defense-in-depth mechanisms, including using virtual local-area networks (VLANs), blocking ports that are not in use, and employing network management technologies such as software-defined networking (SDN).

II. IEC 61850 Background Review

A. IEC 61850

A substation automation system (SAS) is a system composed of IEDs connected through a communications network, and its function is to control and monitor processes in a substation. IEC 61850 [4] provides guidance for an SAS by defining object-oriented models for IED data and the services associated with the objects, as well as the communications interface used to transfer information between devices [5].

IEC 61850 allows logical and physical information flow between functions in the same device or on different devices in a local-area network (LAN), enabling communications among several levels of process and function (see Fig. 1).

For example, a grouping of protection and control functions (F1 or F2) is referred to as a logical device (LD), and an individual function is a logical node (LN) [6]. One function may be physically connected (PC) (i.e., functions are performed in separate devices) or logically connected (LC) (i.e., functions are performed on the same device) to another function.

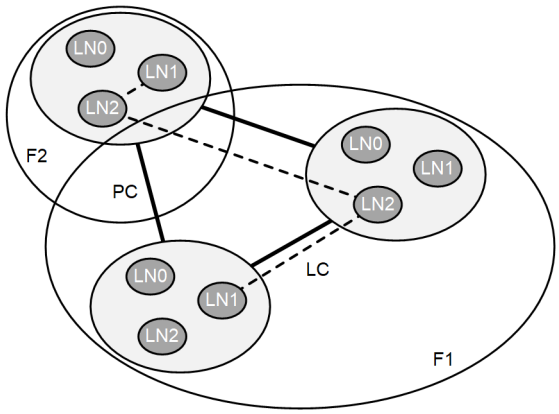

Fig. 1. Functions, Logical Devices, Logical Nodes, and Connections

The IEC 61850 protocol stack is shown in Fig. 2. It contains different types of messages mapped in different layers of the Open System Interface (OSI) model.

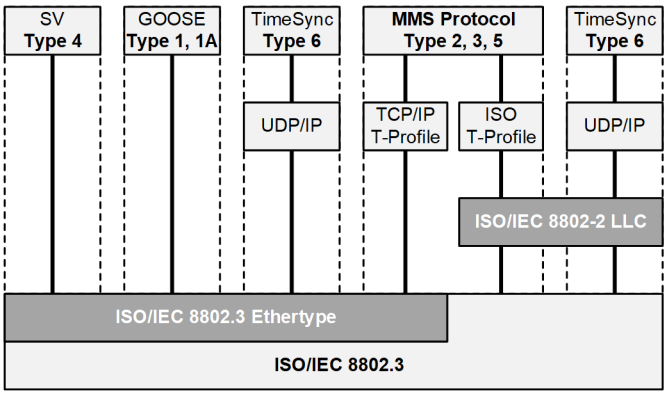

Fig. 2. IEC 61850 Protocol Stacks

Different types of messages have different functions. The SV protocol is used to exchange messages containing samples of electrical quantities [7]. The MMS protocol [8] connects communications centers and gateways through a client-server connection with the IEDs inside the substation. The GOOSE protocol [9] is used to exchange information between IEDs such as TRIP and LATCH.

Due to the low transmission latency required by GOOSE messages (as defined by IEC 61850-5 [10]), they are mapped directly to Layer 2 of the OSI model, which avoids the overhead of higher network abstraction levels. Mapping in the OSI layers determines the dynamics of transmission and composition of the frames of a message.

B. GOOSE Messages

GOOSE messages provide a mechanism for exchanging information between one or more IEDs over an IEEE 802.3 network. GOOSE messages are transmitted through multicast and are distributed through a publisher-subscriber configuration, where one IED (publisher) is responsible for creating messages that are delivered to a group of IEDs (subscribers). GOOSE message information is mapped to the data link layer of the OSI model and follows the payload datagram shown in Fig. 3.

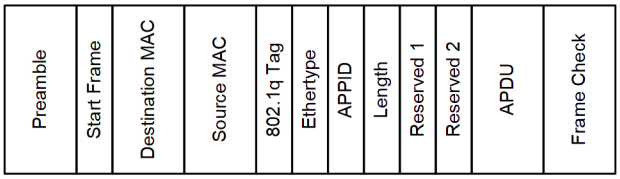

Fig. 3. GOOSE Frame

The GOOSE datagram has the following 12 fields:

- The **Preamble** and **Start Frame** fields are identical to the first two fields of the Ethernet frame.
- The **Destination MAC** field corresponds to the multicast address. IEC 61850 defines a range for message addresses that start with the first three octets 01-0C-CD. The fourth octet represents the datagram type: 01 for GOOSE, 02 for GSSE, or 04 for SV. The fifth and sixth octets define the individual message address.
- The **Source MAC** field defines the address of the publishing device.
- The **IEEE 802.1Q Tag** field (VLAN priority tagging) defines the message selection and separation mechanism.
- The GOOSE **Ethertype** field is set to 88 B8.
- The **APPID** field identifies the frame.
- The **Length** field indicates the total number of bytes in the message.
- The first bit of the **Reserved 1** field indicates if the device is in simulation mode.
- The **Reserved 2** field is reserved for future standardization.
- The last fields are the Application Protocol Data Unit (**APDU**) and **Frame Check** sequence.

The payload is allocated to the APDU that contains information to be shared by the system. The data contained in the APDU are coded according to Abstract Syntax Notation One/Basic Encoding Rule (ASN.1/BER). ASN.1 describes the data structure, and BER describes the format of the bits on the wire. Fig. 4 shows how the information contained in the APDU is divided.

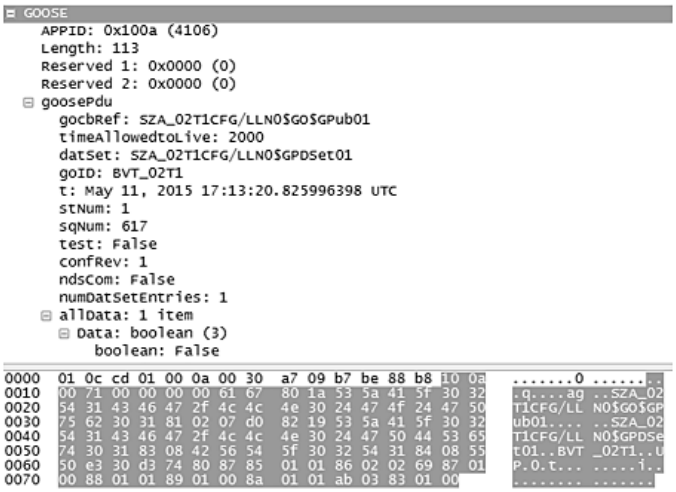

Fig. 4. GOOSE APDU

The APDU described in IEC 61850-8-1, Appendix A is a sequence of the following 12 parameters that carry information to subscriber IEDs:

- **gocbRef**: Reference to the GOOSE control block associated with the publication.
- **timeAllowedtoLive**: The maximum wait time before the next retransmission.
- **datSet**: Reference to the data set being published in the GOOSE message.
- **goID**: GOOSE message identification.
- **t**: Time at which the last state change was detected.
- **stNum**: State Number; GOOSE message transmission variation counter.

- **sqNum**: Sequence Number; GOOSE message counter.
- **test**: Indicates whether the message is in a test.
- **confRev**: Counter; increases with each change in the data set configuration.
- **ndsCom**: Needs Commissioning; indicates whether the GOOSE control block configuration is incomplete or incorrect.
- **numDatSetEntries**: Number of elements (FCDAs) within the data set.
- **allData**: Contains all data information within the data set.

Publisher IEDs encode the information contained in the data set and create an envelope that follows the ASN.1/BER standard. Subscriber IEDs receive this packet and use the information in the gocbRef, datSet, goID, confRev, and numDatSetEntries parameters to validate and process messages. After message validation, the information in the data set is used to process the IED logic.

C. *Dynamic GOOSE Message Transmission*

The performance requirements of GOOSE are described in IEC 61850-5 as types 1 and 1A. Type 1 GOOSE typically contains binary content but may carry analog quantities as well. Type 1A GOOSE carries critical messages in a substation. Performance requirement Class P1 requires a transmission time on the order of 10 milliseconds, and Class P2/P3 requires transmission times of 3 milliseconds.

The publisher IED encodes a new event in the data set and transmits it to the receivers through a multicast connection. Message propagation, defined in IEC 61850-8-1, has a message retransmission dynamic as shown in Fig. 5.

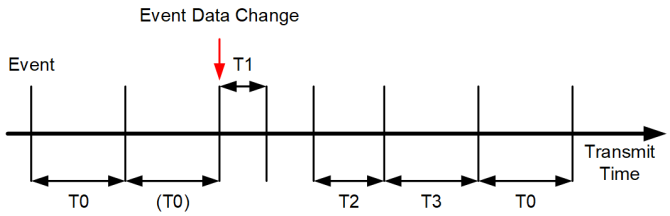

Fig. 5. GOOSE Message Transmission Mechanism

Events are generated in the local application of an IED and trigger GOOSE messages if the data are in the GOOSE data set. If no event occurs, the messages are retransmitted periodically at the steady-state interval T0. The occurrence of an event triggers the fast-transmission mechanism of the GOOSE message. The time T0 represents the transition from the steady-state to the fast-retransmission regime.

When an event occurs, the data are transmitted as soon as possible. Time T1 is the time between the occurrence of the event and retransmission. The times T2 and T3 are associated with the retransmission of messages until steady-state operation. The retransmission curve before steady-state operation varies depending on the IED manufacturer. At each retransmission of messages by the publisher, sqNum is incremented, and timeAllowedtoLive informs the subscriber of the maximum interval within which to expect the next message. If an event occurs, stNum is incremented.

D. *GOOSE Receive State Machine*

The details of GOOSE message processing by the subscriber is specific to the implementation manufacturer. Fig. 6 shows an implementation example from IEC 62351-6.

```
1:  Actual <- Store message StNum;
2:     IF Previous ≠ Actual THEN
3:          IF Actual < Previous AND No TTL time-out THEN
4:               Discard GOOSE message;
5:          END
6:          delta_t <- Previous_Timestamp - Actual_Timestamp
7:          IF |delta_t| > 2 minimum wait time THEN
8:               Discard GOOSE message;
9:          END
10:         ELSE
11:              Process GOOSE message;
12:         END
13:    END
14:    ELSE
15:         Discard GOOSE message;
16:    END
```

Fig. 6. GOOSE Receive Algorithm

The IED subscriber, upon receiving the GOOSE message, performs checks before processing the information contained in the message APDU. The IED starts processing by storing the value of the current stNum parameter.

Line 2 in Fig. 6 checks the difference between the parameters, stNum of the current message, and stNum of the last message; if the information is equal, it is processed and Line 15 discards the GOOSE message.

Line 3 in Fig. 6 uses the lowest operator for the parameter comparison between the actual stNum and the stNum of the previous message. The check is performed because the increment of the stNum parameter is increasing for each retransmission. If the message is not valid (TTL timeout) or the stNum information does not satisfy the condition of the lesser operator, the message is discarded.

Line 6 in Fig. 6 calculates the time variation between two subsequent messages. The comparison is made with a parameter equal to two times the minimum waiting time of the message; if the time is longer than this, the message is discarded. This prevents late messages with a valid TTL from being processed.

Lines 10 and 11 in Fig. 6 represent the positive result of message scavenging scans; if all conditions are met, the GOOSE message is processed successfully.

E. *GOOSE Message Vulnerability*

A successful cyber attack depends on three things: motivation, vector, and technique. An attack can be motivated by political interests, assessing the vulnerability of a system, or financial interests. Vectors are the paths of access to a computer or a network. Attack techniques can vary according to network architecture, message structure, and message transmission dynamics.

Network access can be obtained through malware installed on a Universal Serial Bus (USB) device, infected equipment, a malicious person with access to the substation network, or a hacker capable of penetrating the network from a distance. The program or malware does not have to have direct access to publisher and subscriber equipment; however, it must have the

ability to analyze, identify, and reproduce GOOSE messages. The level of vulnerability is considered low only for isolated LANs without external communication; however, the current situation of substations, where information is shared with operations centers through gateways and shared communications links, is not intrinsically isolated. The lack of proper network configuration and security during the design and commissioning phase of a communications network is another vector that can be used for exploiting GOOSE messages.

Due to the nature of the GOOSE protocol, attacks can be made using several techniques capable of exploiting vulnerabilities in the data link layer: VLAN hopping, media access control (MAC) flood attack, and spoofing attack [11]. The consequences of a cyber attack in a substation can cause irreversible damage. The malfunction of the data network can cause incorrect operation of protection and control schemes and improper performance of primary equipment such as circuit breakers and disconnectors.

GOOSE and SV message types are defined as plaintext messages. There are link-level safety mechanisms described in IEC 62351, Part 6; however, they are not useful because of the time delay that they add in the transmission of messages [12]. Embedded latency through cryptography and message authentication is the main barrier to link-level implementation. IEC 62351 defines the methods for low-power computing, but they are not enough to meet the performance requirements of IEC 61850-5.

Another way that attackers can exploit the vulnerabilities of GOOSE is through the processing logic in the receiving device. The processing logic defines how the device handles a valid old message, a fake but valid message, or an invalid message, and how these messages affect the burden on the device. GOOSE messages carry important information. They convey close and TRIP signals that are critical for the operation of a substation. The next section further explores some of the known vulnerabilities of the GOOSE protocol.

III. GOOSE Message Cyber Attacks

A. Possible Forms of Attack

The purpose of this section is to discuss the behavior of a malicious GOOSE message capable of interfering with the traffic between a publisher and a subscriber and how to detect, trace, and prevent this vulnerability. Malicious GOOSE messages can operate in two different ways: the malicious message can prevent the subscriber from processing the original message, or it can influence a decision by modifying the values of the original message but preserving the semantics. The following section uses the GOOSE flood attack technique as an example scenario.

B. GOOSE Flood Attack

In a flood attack, the malware, after inspecting the network and finding a GOOSE message, floods the network with GOOSE packets with the same semantics as the Ethernet header, but the APDU is modified and filled with padding bytes until they reach the maximum size of the Ethernet packet of 1,522 bytes. The intent of the attack is to compromise IED processing and impair message traffic.

C. High stNum GOOSE Attack

In a stNum attack, after finding a GOOSE message, the malware sends a single message with the maximum value of stNum. The intention is for the subscriber IED to discard subsequent messages if the receiving algorithm is based on IEC 62351 [13].

D. Semantic Spoofing GOOSE Attack

A semantic spoofing attack focuses on reproducing the scope of an original message but with a message that contains false information. After analyzing the network and finding a GOOSE message, the malware checks and manipulates the Boolean or analog information of the APDU. The malware also simulates message transition mechanics by incrementing stNum and zeroing sqNum. The intent is to mislead the IED through a false message.

E. GOOSE Replay Attack

A replay attack uses post-traffic injection in the network through an open port. The open port could be a non-configured switch port or a testing port with access to all the network traffic. The replay attack operates by playing back an older GOOSE substation event, such as a feeder fault, and injecting signals to manipulate the behavior of subscriber devices.

IV. Attack Methodology Example: GOOSE Flood Attack

A. Test Scenario

This test scenario consists of two IEDs, a managed switch, and a computer with two network cards for invader simulation and data measurement. The three devices are connected to the switch ports through network cables, as shown in Fig. 7. The switch is configured transparently without any rules or port blocking. The IEDs typically operate with a network card capable of supporting a bandwidth of 100 Mbps.

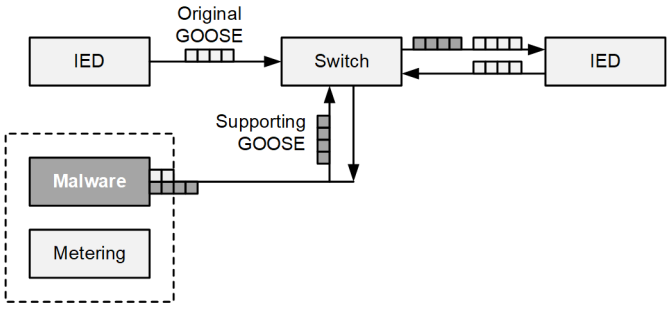

Fig. 7. Test Scenario

The IEDs are configured using a ping-pong architecture. The transmitting IED publishes Boolean information on the network. Upon receiving the information, the IED subscriber returns the response to the network. The IED transmitter does not sign the message of the IED subscriber. The configuration parameters of the IED GOOSE message header is listed in Table I. MAC addresses are uniquely configured for each IED while the VLAN ID (VID) is configured to be the same for both

IEDs. The steady-state retransmission time is one second, and the transmission time after a state change is four milliseconds. Wireshark software [14] is used to collect published packets on the network.

TABLE I
PARAMETERS OF IED GOOSE MESSAGES

Parameter	IED 1	IED 2
MAC Address	01-0C-CD-01-00-13	01-0C-CD-01-00-14
APP ID	0x1013	0x1014
VID	0x001	0x001
VLAN PRIORITY	4	4
Configuration Revision	1	1
Minimum Time (ms)	4	4
Maximum Time (ms)	1000	1000

B. Communications Network Profile Before the Attack

The profile of GOOSE messages prior to the attack is logged and graphed in Fig. 8 and Fig. 9. The GOOSE data Boolean information from the transmitter and receiver are represented by the dots in the plot. The recorder starts with the transmitter IED sending the Boolean data with the false value and the receiver following the information and publishing it to the network with a small delay. The transition from false to true is driven by the transmitter IED and is followed by the receiver IED.

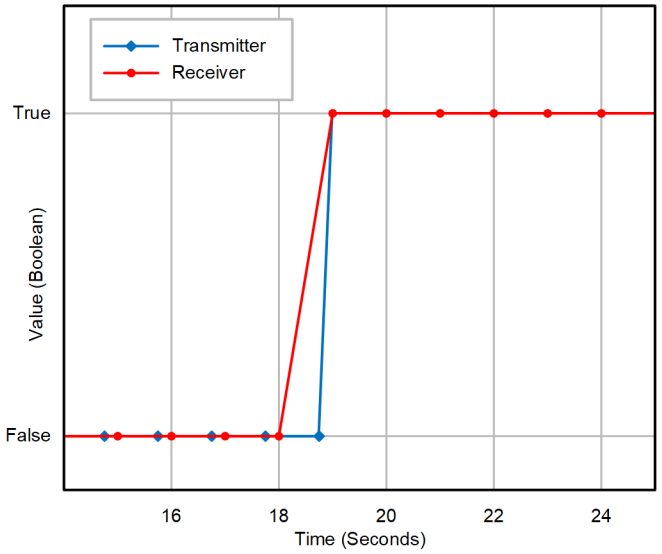

Fig. 8. Healthy GOOSE Communications Profile: Transmitter and Receiver

Fig. 9 shows the bandwidth usage during the transition from a false state to a true state. During steady-state operation, the bandwidth used by the network is approximately 2 Kbps for a data set containing one binary and quality bits. During a state transition (false to true) the bandwidth reaches a peak of 9 Kbps due to the transmission mechanism of GOOSE messages. The increase in the bandwidth is due to the retransmission rate of the GOOSE message after an event to ensure delivery. However, the network profile before the attack is very stable, only using 0.01 percent of its total capacity.

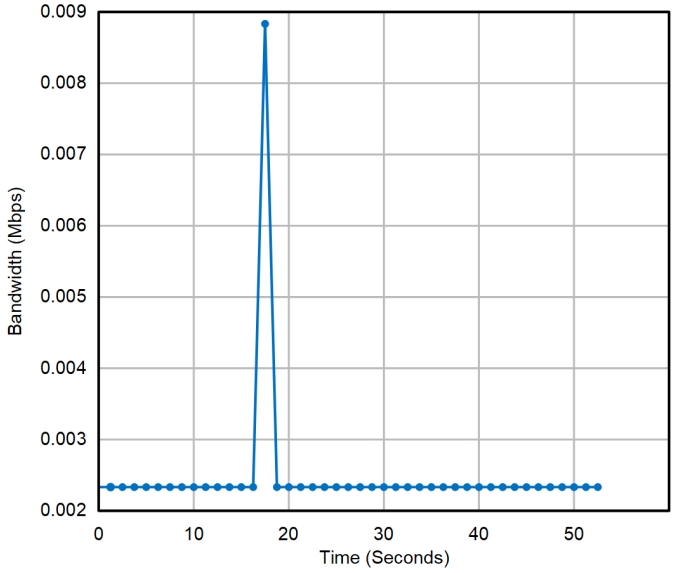

Fig. 9. Bandwidth Recorded During an Event Change

C. GOOSE Flood Attack: 40 Percent of Bandwidth

The experiment analyzes the performance of the IED subscriber during a condition of heavy, unwanted GOOSE traffic. The malware generates frames with manipulated data so as not to interfere with the IED logic decisions. Fig. 10 shows the GOOSE APDU of messages generated by the malware. The Boolean information in the allData attribute is replaced by bit-strings and filled with a null-value until it reaches a value close to the maximum transmission capacity of the Ethernet frame (1,522 bytes). The unwanted GOOSE messages are sent at a rate interval of approximately 400 microseconds.

```
▷ Frame 9310: 1488 bytes on wire (11904 bits), 1488 bytes
  captured (11904 bits) on interface 0
▷ Ethernet II, Src: Schweitz_0b:06:be (00:30:a7:0b:06:be),
  Dst: Iec-Tc57_01:00:13 (01:0c:cd:01:00:13)
◢ GOOSE
    APPID: 0x1013 (4115)
    Length: 132
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  ◢ goosePdu
      gocbRef: A0401U_005_ICD_1CFG/LLN0$GO$GooseDSet15
      timeAllowedtoLive: 2000
      datSet: A0401U_005_ICD_1CFG/LLN0$DSet15
      goID: Sub1Bay1
      t: Jul  6, 2016 18:03:52.332397460 UTC
      stNum: 1234
      sqNum: 0
      test: False
      confRev: 1
      ndsCom: False
      numDatSetEntries: 1
    ◢ allData: 1 item
      ◢ Data: bit-string (4)
          Padding: 1
          bit-string: <MISSING>
```

Fig. 10. APDU Generated by Malware

Fig. 11 shows the data set Boolean information profile over time before and during the GOOSE attack. IEDs are publishing GOOSE messages with true Boolean values, and the attack begins at between 10 and 20 seconds.

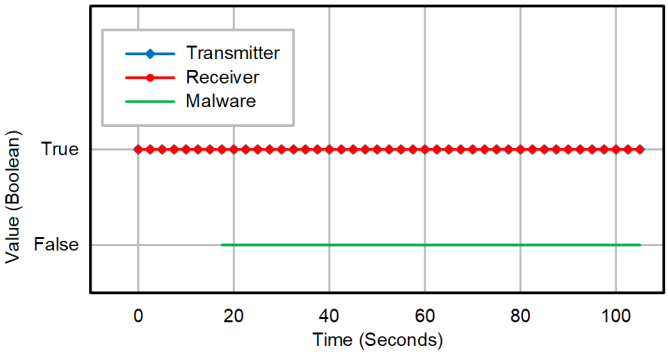

Fig. 11. GOOSE Flood Attack: 40 Percent of Bandwidth

Fig. 12 shows the transmitter and receiver GOOSE messages at between 40 and 45 seconds during the GOOSE flood attack. It can be observed that the sqNum value is incremented correctly and the maximum transmission time is steady at a rate of one second. Therefore, there is no degradation in the IED GOOSE transmitter and receiver mechanism.

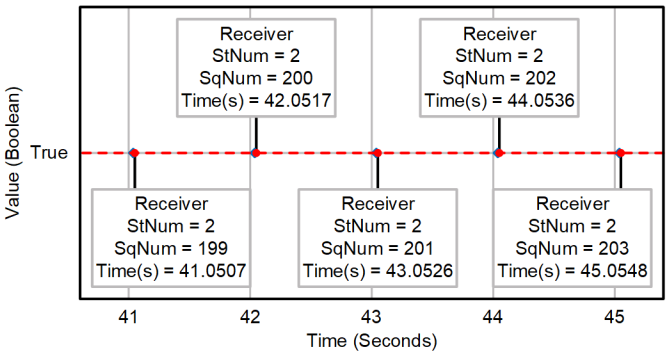

Fig. 12. GOOSE Flood Attack: 40 Percent of Bandwidth

Fig. 13 shows the bandwidth at the start of the attack, reaching 40 Mbps, or 40 percent of total network capacity.

D. GOOSE Flood Attack: 85 Percent of Bandwidth

The experiment continues with the increase of the malware transmission data rate until it reaches 85 percent of the network capacity. Fig. 14 shows the data set Boolean information profile over time for traffic at 85 Mbps. IEDs are publishing GOOSE messages with true values, and the figure clearly shows some missing packets in the transmission and reception of the GOOSE messages at between 2 and 5 seconds and at between 12 and 15 seconds.

Fig. 15 shows that the parameter stNum remains constant in both packets, indicating that it belongs to the same order of variation. sqNum increased by one over a range of one second; however, the transmitted message is not recorded for five seconds. Also, the packet sqNum values for the receiver jump from sqNum = 700 to sqNum = 703; this result is due to the effects of packet loss caused by network saturation.

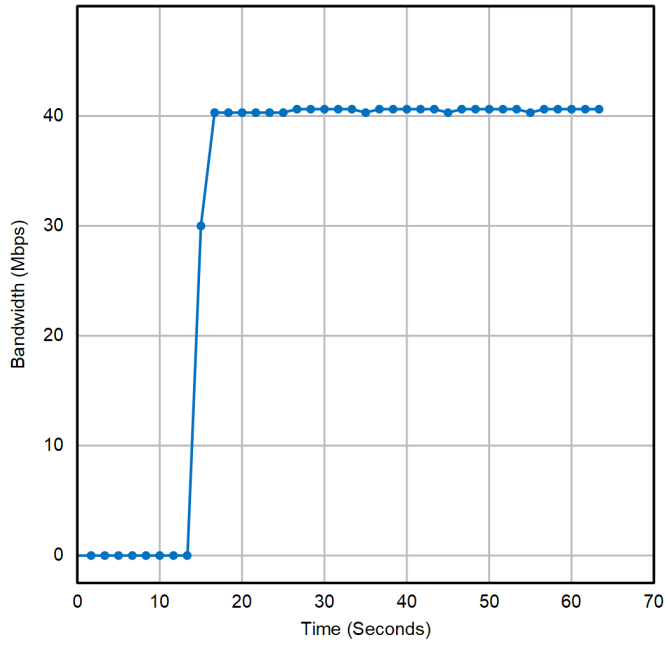

Fig. 13. Bandwidth Recorded During GOOSE Flood Attack: 40 Mbps

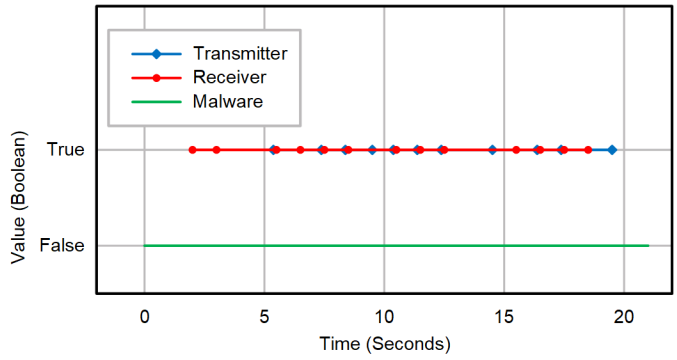

Fig. 14. GOOSE Flood Attack: 85 Percent of Bandwidth

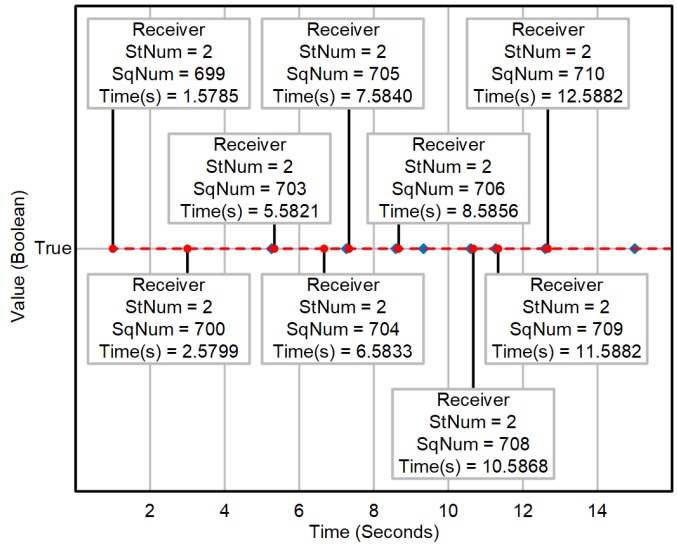

Fig. 15. GOOSE Flood Attack: 85 Percent of Bandwidth

```
SubsID1
--------------------------------------------------------------------------------
Ctrl Ref: A0401U_005_ICD_1CFG/LLN0$GO$GooseDSet15
AppID   : 4115
From    : 07/01/2016 09:08:41.764  To: 07/01/2016 09:14:15.594

Accumulated downtime duration                    : 0000:04:37:532
Maximum downtime duration                        : 0000:04:37:532
Date & time maximum downtime began               : 07/01/2016 09:09:38.062
Number of messages received out-of-sequence (OOS)  : 41199
Number of time-to-live (TTL) violations detected   : 0
Number of messages incorrectly encoded or corrupted: 40922
Number of messages lost due to receive overflow    : 890169
Calculated max. sequential messages lost due to OOS: 1231
Calculated number of messages lost due to OOS      : 342218

#   Date        Time          Duration        Failure
1   07/01/2016  09:14:15.321  0000:00:00:272  MESSAGE CORRUPTED
2   07/01/2016  09:14:15.321  0000:00:00:000  OUT OF SEQUENCE
3   07/01/2016  09:14:14.321  0000:00:01:000  MESSAGE CORRUPTED
4   07/01/2016  09:14:14.321  0000:00:00:000  OUT OF SEQUENCE
5   07/01/2016  09:14:13.321  0000:00:00:999  MESSAGE CORRUPTED
6   07/01/2016  09:14:13.320  0000:00:00:001  OUT OF SEQUENCE
7   07/01/2016  09:14:12.319  0000:00:01:000  MESSAGE CORRUPTED
8   07/01/2016  09:14:12.319  0000:00:00:000  OUT OF SEQUENCE
```

Fig. 16. Subscriber IED Response After GOOSE Flood Attack

Fig. 16 shows the GOOSE log report provided by the receiver IED after the cyber attack. The log shows excessive loss of packets due to a buffer overflow caused by the malware packet injection. It also shows the recorded date and time and the cause of GOOSE packet discards. The information log demonstrates the harm to the application caused by network saturation.

V. Cybersecurity for Power Substations

Modern substations provide resources to facilitate and improve the implementation of functions that use the communications network. When implemented correctly, these resources provide reliability and efficiency; however, if implemented in the wrong way, with gaps in security, they can create vulnerabilities that facilitate attacks and failures in the automation system, reducing the reliability and efficiency of the installation [15].

Physical access to power substations is typically managed through keys, locks, and fences to prevent unauthorized access to the facility. Access to modern substations is managed mostly through the communications network, so network access must be restricted.

By using security gateways and technologies such as VLANs and SDN, it is possible to restrict access and protect the integrity of substation data at all network levels.

Network engineering also makes it possible to direct the flow of data, ensuring the correct operation of the communications network during a contingency situation and avoiding overloads. By applying the right tools and best network practices, it is possible to create a safer, more reliable, and more secure network without compromising communications performance and applied embedded security protocols.

A. *Layer 2 Management Using IEEE 802.1Q Tags*

VLANs are used to partition and isolate networks at the data link layer of the OSI model and follow the IEEE 802.1Q standard [16].

Fig. 17 shows a schematic of message traffic managed by a switch. Using IEEE 802.1Q tags in Ethernet frames, it is possible to manage data flow through the data link layer of the OSI model.

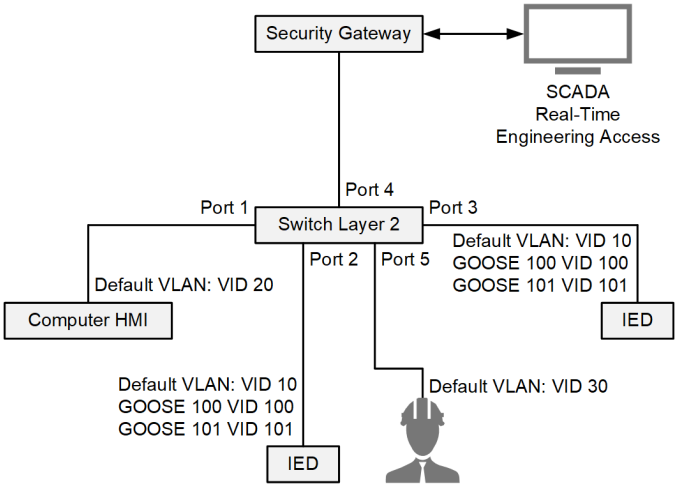

Fig. 17. Network Diagram Using VLANs

Table II shows the VLANs used in the application in Fig. 17. Access between VID 10, 20, and 30 is managed through the security gateway. A firewall manages the inspection of packets and access levels. Data flow with tags 10, 20, and 30 is directed to Port 4 and distributed to the necessary ports and SCADA system.

TABLE II
VLAN IDENTIFICATION

VID	VLAN Definition
10	IED LAN
20	SCADA LAN
30	Engineering Access
100	Message GOOSE 100
101	Message GOOSE 101

VLANs 100 and 101 are specific to GOOSE messages, and no security gateway routing is required. GOOSE messages travel exclusively through Ports 2 and 3. Only the necessary equipment shares the information; however, some types of attacks can disrupt the security of VLANs such as VLAN hopping attacks, where an attacker bypasses a Layer 2 restriction. An example of a VLAN hopping attack is the switched spoofing method.

The switched spoofing technique is where an attacker acts as a switch to create a trunk link to allow any VLAN packet to pass through the port. Switched spoofing can be prevented by using the correct switch configuration to stop dynamic trunk port negotiation.

Network management through VLANs makes it possible to isolate the communications network to the necessary equipment, making it difficult (but not impossible) for unauthorized users to access the network. It also optimizes the performance of the communications network once multicast traffic is divided.

B. Software-Defined Networking

SDN is a static network architecture based on lookup table technology. It secures and optimizes network performance by reducing bandwidth through flow control. SDN is an approach that uses open protocols, such as OpenFlow, that allow flow control on border devices such as switches [17].

SDN architecture has three levels: application, flow controller, and network infrastructure. Fig. 18 shows the interaction between the three levels. The application layer has three main functions: system operation, administration, and management (OAM).

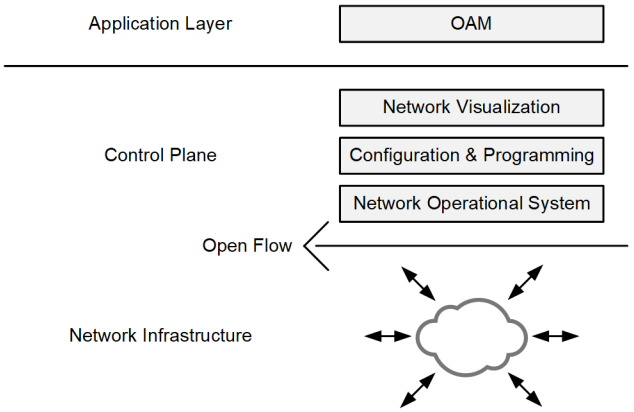

Fig. 18. SDN Architecture

The control plane is the central application that allows network visualization. It determines how the system handles packets. The network infrastructure level is where equipment receives instructions from the controller and directs packets to their respective destinations.

The SDN switch uses the rules that are configured by the controller and stored in the flow tables. The list of flow entries consists of pre-defined match field values and actions. The match field values can be any field from OSI Layer 1 to 4. For GOOSE messages, a match field value can be any information parameter from the Ethernet header such as the IEEE 802.1Q tag, the destination MAC address, or the incoming physical port.

The SDN switch (see Fig. 19) compares incoming entries with each entry in the flow table and searches for a valid rule. The packet is then sent to the action output, and the switch forwards the packet to the specified port or discards it.

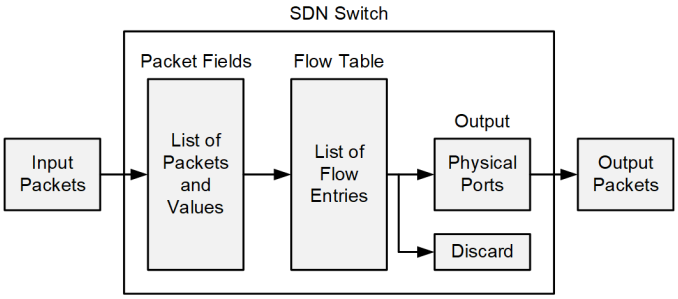

Fig. 19. Model SDN Switch

The first step to engineering a secure GOOSE network using SDN is defining all required GOOSE messages used in the application. Since the GOOSE message header information and the network topology is defined by the user, it is possible to use the incoming switch port and some fields from the Ethernet header to create a secure rule for the incoming GOOSE messages. Also, it is possible to restrict the flow of messages for a single output port to avoid the unnecessary spread of GOOSE message communications.

Once the SDN network has been engineered, the switch behaves as configured by the user, eliminating possible paths of intrusion and data network overload. If a malicious actor tries to spoof a packet, SDN prevents that packet from going forward and reports this activity to a centralized intrusion detection system (IDS).

VI. CONCLUSION

The IEC 61850 standard provides a model for electric power substation automation. GOOSE messages can be used to share blocking, TRIP, and closing signals for equipment in a substation. Due to high performance requirements, GOOSE messages are implemented in clear text, and authentication and security procedures are not native to the protocol implementation, which makes GOOSE messages more vulnerable. Attack techniques such as manipulation of Ethernet frames and network saturation can compromise the performance of equipment used in the protection and control system. Employing best practices for Ethernet network

configuration and new technologies such as SDN can minimize the risk of attacks and increase network performance.

The technique of network saturation explored in this paper shows how the multicast transmission dynamic can be used maliciously and negatively impact the performance of network-connected equipment. Once data capacity limits are reached, packet loss occurs for both transmitter and receiver equipment. When a network is compromised by an attack, packet delivery and minimum GOOSE message transmission times may no longer be guaranteed.

Networking best practices can be used to mitigate possible attacks and ensure the integrity of message exchange. The use of IEEE 802.1Q technology ensures network segregation at the data link layer by configuring switches and inserting tags into Ethernet frames. SDN networks are whitelisted by design. The static topology of SDN networks allows precise access and flow control at the network controller ports, thus preventing attacks on substations.

VII. References

[1] D. Dolezilek, D. Whitehead, and V. Skendzic, "Integration of IEC 61850 GSE and Sampled Values Services to Reduce Substation Wiring," proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.

[2] IEC 61850-8-1, Communication Networks and Systems in Substations – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3, 2004.

[3] M. Silveira and P. Franco, "Segurança Cibernética Em Redes IEC 61850: Como Mitigar Vulnerabilidades Das Mensagens GOOSE," proceedings of the Seminário Nacional de Produção e Transmissão de Energia Elétrica, Curitiba, Brazil, October 2017.

[4] IEC 61850-1, Communication Networks and Systems in Substations – Part 1: Introduction and Overview, 2003.

[5] C. Ozansoy, *Modelling and Object Oriented Implementation of IEC 61850: The New International Standard on Substation Communications and Automation*, Lambert Academic Publishing, 2010.

[6] IEC 61850-7-1, Communication Networks and Systems in Substations – Part 7-1: Basic Communication Structure for Substation and Feeder Equipment – Principles and Models, 2003.

[7] J. Konka, C. Arthur, F. Garcia, and R. Atkinson, "Traffic Generation of IEC 61850 Sampled Values," proceedings of the IEEE First International Workshop on Smart Grid Modeling and Simulation (SGMS), Brussels, Belgium, October 2011.

[8] R. O'Fallon, D. Klas, T. Tibbals, and S. Shah, "IEC 61850 MMS SCADA Network Optimization for IEDs," proceedings of the DistribuTECH Conference, San Diego, CA, February 2011.

[9] C. Kriger, S. Behardien, and J. 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 (IJCCC)*, Vol. 8, Issue 5, October 2013, pp. 708-721.

[10] IEC 61850-5, Communication Networks and Systems in Substation – Part 5: Communication Requirements for Functions and Device Models, 2003.

[11] Y. Bhaiji, "Understanding, Preventing, and Defending Against Layer 2 Attacks," proceedings of the Cisco Expo, Cairo, Egypt, January 2009.

[12] J. Hoyos, M. Dehus, and T. Brown, "Exploiting the GOOSE Protocol: A Practical Attack on Cyber-Infrastructure," proceedings of the IEEE Globecom Workshops, Anaheim, CA, December 2012.

[13] N. Kush, E. Ahmed, M. Branagan, and E. Foo, "Poisoned GOOSE: Exploiting the GOOSE Protocol," proceedings of the 12th Australasian Information Security Conference, Auckland, New Zealand, January 2014.

[14] "Wireshark," The Wireshark Foundation, Retrieved July 8, 2019. Available: https://www.wireshark.org/.

[15] C. Ewing, "Engineering Defense-in-Depth Cybersecurity for the Modern Substation," proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.

[16] IEEE 802.1Q – IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks, 2018.

[17] "ONF," Open Networking Foundation, Retrieved July 8, 2019. Available: https://www.opennetworking.org/.

VIII. Biographies

Mauricio Gadelha da Silveira is an electrical engineer with a BS earned from Sao Paulo State University in 2013. Since 2014, he has been with Schweitzer Engineering Laboratories, Inc., where he is currently a lead integration and automation engineer. His work includes power system modeling, cybersecurity assessment, and network design for critical infrastructure.

Paulo Henrique Franco graduated as an electrical engineer at the Electrical Engineer Department at Universidade Estadual Paulista in 2004. Since 2007, he has been working for Schweitzer Engineering Laboratories, Inc. He is currently an automation engineer, acting as a project technical lead.

© 2019 by Schweitzer Engineering Laboratories, Inc.
All rights reserved.
20190712 • TP6921-01