NODE-BASED ANALYSIS OF GOOSE COMMUNICATIONS IN IEC61850 SUBSTATIONS

J. Chuang[1], C.-H. Lin[2], and R. Wright[3]

[1]Moxa Inc., Taiwan; [2]Moxa Europe GmbH, Germany; [3]RJ Connect, RSA

ABSTRACT

The GOOSE communication protocol is used to protect critical operations in IEC 61850 substations. The protocol is based on a publisher-subscriber model and a retransmission mechanism that repeats the messages at regular intervals in a predefined manner. Because GOOSE is a connectionless communication model, the IEC 61850-5 standard has defined the key performance expectation as the delivery of messages with minimum latency, which is typically in the millisecond range. Ethernet technologies like packet multicast and VLAN are used to control the overall network load and improve the transmission performance in Intelligent Electronic Devices (IEDs). The current substations use so-called host-based approach to monitor the GOOSE communications end-to-end. In this paper, we examine a complementary approach and propose a node-based GOOSE communication analysis method using Ethernet switches, which can be integrated into a Power SCADA system or NMS to show the flow of each and every GOOSE message in a substation network.

HOST-BASED ANALYSIS OF GOOSE MESSAGES

A host-based approach utilizes a computer in the substation network to record and analyze the end-to-end transmission of GOOSE messages in the system.

The growing size of substation networks and the increasing deployment of GOOSE-based inter-substation communication solutions present additional challenges to monitoring and debugging of GOOSE communication issues. Some of the challenges include:

Pinpointing the source of a problem is a challenge: Substation networks work like black boxes, which makes identifying the source of a problem a challenge. Once an issue in the transmission of GOOSE packets between the IEDs is identified, the first step is to understand if the failure point is in the IEDs or somewhere in the network.

Most substation engineers cannot troubleshoot networking issues: Network analysis typically requires in-depth networking expertise, which includes knowledge of VLANs and multicast transmission.

Analyzing GOOSE communication issues requires modifications in a substation network and the IEDs deployed: As a complementary approach to the traditional host-based approach, a node-based approach can leverage the monitoring capabilities of Ethernet switches (nodes) to analyze the GOOSE traffic in a substation network.

NODE-BASED ANALYSIS OF GOOSE MESSAGES

The node-based analysis of GOOSE messages involves using Ethernet switches in the substation network to inspect the GOOSE packets and continuously monitoring their behavior. Certain functions and capabilities will have to be developed in the switches before they can be used to monitor the GOOSE messages that are being transmitted in the network and send alerts to the Power SCADA system for further action. The Ethernet switches should constantly monitor the timeAllowedtoLive (TATL) value and the state of each GOOSE message transmitted through the network to ascertain if the GOOSE message has timed out or if the message is tampered with, and then send alerts to the Power SCADA in the system identifying the type of issue.

Time Allowed to Live

In an unstable network, the GOOSE messages transmitted in the network can be influenced by noise, traffic, or human error, resulting in the packets not being received within a certain time frame. In the IEC 61850-8-1 standard [1], a timeAllowedtoLive (TATL) value is defined for each GOOSE message, which is the maximum validity period for a GOOSE message. Figure 1 shows the structure of a GOOSE protocol data unit (PDU). If a critical GOOSE message, such as a trip signal, is not received within the TATL period set for the message, the receiver (e.g., an IED) will assume that the message is lost resulting in the system not swapping to a backup circuit.

```
IECGoosePdu ::= SEQUENCE {
        gocbRef             [0]   IMPLICIT VISIBLE-STRING,
        timeAllowedtoLive   [1]   IMPLICIT INTEGER,
        datSet              [2]   IMPLICIT VISIBLE-STRING,
        goID                [3]   IMPLICIT VISIBLE-STRING OPTIONAL,
        T                   [4]   IMPLICIT UtcTime,
        stNum               [5]   IMPLICIT INTEGER,
        sqNum               [6]   IMPLICIT INTEGER,
        simulation          [7]   IMPLICIT BOOLEAN DEFAULT FALSE,
        confRev             [8]   IMPLICIT INTEGER,
        ndsCom              [9]   IMPLICIT BOOLEAN DEFAULT FALSE,
        numDatSetEntries    [10]  IMPLICIT INTEGER,
        allData             [11]  IMPLICIT SEQUENCE OF Data,
        }
```

FIGURE 1: GOOSE PDU showing the TATL parameter

Setting the correct TATL value for a GOOSE message is a complex topic that is not covered in this paper. However, a GOOSE message in a network might not reach the recipient IED if the TATL value is too restrictive or the flow of GOOSE traffic through an Ethernet network is restricted. There are already several papers published on the correct configuration of the TATL values for GOOSE messages. In this paper, we discuss the flow of GOOSE messages through the Ethernet network. For the purpose of this paper, we assume that the TATL values of GOOSE messages are set correctly.

The Role of Ethernet Switches in a Node-Based Analysis

Ethernet switches are key components of the node-based analysis of GOOSE messages in a substation network. All switches in a substation network will inspect each and every GOOSE packet that is multicast through the network. The GOOSE packets are continuously monitored and information such as their status (health, timeout, or tampered) along with the name of the subscriber IED and the incoming port on the switch are recorded in a monitoring table. A GOOSE-enabled switch in a substation network should be able to:

- Dynamically detect all GOOSE messages and store their packet information in a monitoring table
- Continuously update the table by monitoring the GOOSE messages for each retransmission and state change
- Detect failure points based on the values recorded in the monitoring table
  For example:
  - Timeout: A GOOSE message is received over TATL value
  - Tampered: A GOOSE message is sent from two different sources
- Communicate with the nodes in the network so that only the first node that identifies the issue sends an alert

All the switches in the network should be able to communicate with each other so that only the first node that encounters a problem (e.g. timeout) should send an alert message. If all nodes that encounter the issue send out alert messages, troubleshooting the issue will take considerable time and effort.

As illustrated in Figure 2 below, only the switch SW2 should send out an alert to the Power SCADA even though SW3 also encounters the same issue.

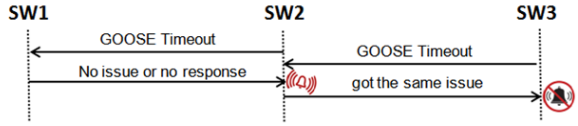

FIGURE 2: Smart alert mechanism in substation switches

The Role and Function of the Power SCADA in a Node-Based Analysis

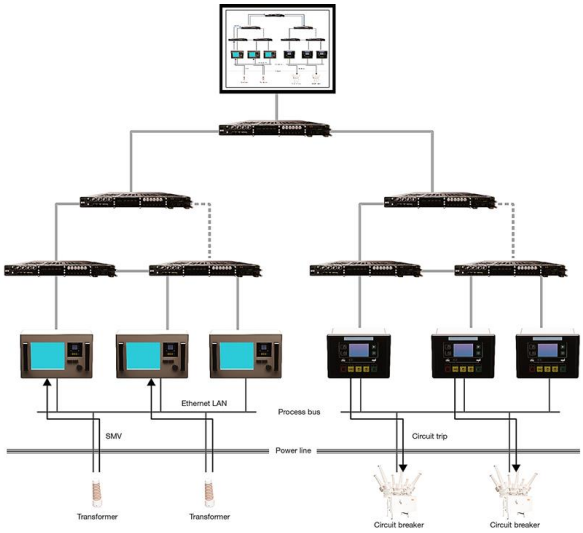

FIGURE 3: Power SCADA in node-based analysis of GOOSE traffic

The Power SCADA system in a substation control center receives alert messages from the Ethernet switches in the network and processes them. Before the Power SCADA system can process alerts from Ethernet nodes designed for monitoring GOOSE messages, it should be equipped with the following capabilities:

- Able to represent a network topology that can show each unique end-to-end path for GOOSE communication in a substation network
- Should be able to import the substation configuration description (SCD) file that identifies the publisher and subscriber IEDs for each GOOSE message

- Should be able to show the connection between IEDs and switches and be able to perform a system run of all GOOSE messages
- Receive GOOSE status information from a switch through MMS or SNMP
- Send user alerts when the status of a GOOSE message changes (i.e., from *health* to *timeout* or *tampered*)
- (Optional) Should be able to update the GOOSE monitoring table maintained by the switches based on the SCD so that each switch only monitors the GOOSE packets subscribed to by its IEDs

Typical Scenario 1: GOOSE Message Time Out

GOOSE messages, especially time-critical GOOSE messages, should be received by the subscribing IEDs within a specific time frame to ensure a reliable protection relay system in the substation network. A time-out scenario occurs when a GOOSE message does not arrive within a time equal to the TATL value of the GOOSE message. In other words, when a message arrives at the subscriber end at a time period that is greater than the TATL value, the message is marked as lost at the receiver end. The root cause for the time out could be an aging component in the network or an alteration in the packet information. An aging IED or switch in the system might send a weak signal, resulting in the receiver not being able to identify if a data bit has the value 0 or 1, leading to an incorrect message. When a GOOSE packet is altered due to noise in the network, the recipient will not be able to act on the message, which can lead to a time out. The switch that receives the GOOSE packet performs a cyclic redundancy check (CRC) on the packet. In the two time-out scenarios described earlier, the CRC checks will fail, indicating issues in the content of the GOOSE packets. The switch then send a time-out alert to the Power SCADA.

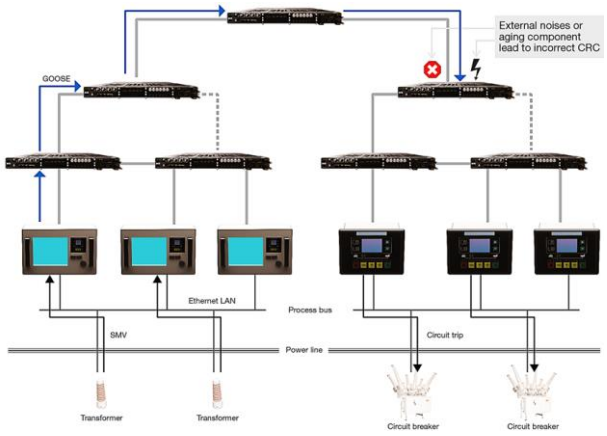

FIGURE 4: GOOSE message time-out scenarios

In the two time-out scenarios, we apply the node-based analysis as follows:

1. The Power SCADA in the substation maintains a detailed list of each and every Ethernet switch in the network with details such as:
    a. Information on each port and the IED connected to the port
    b. The TATL value of each GOOSE message
2. When the Power SCADA receives time-out alerts from network switches, it refers to the monitoring table to identify the GOOSE message.
3. The transmission path of the GOOSE message is traversed to identify the node of the timeout.
4. Once the faulty IED or network node is identified, corrective measures are implemented to fix the issue.

Typical Scenario 2: GOOSE Message Tampered

Power substations are among the public infrastructure companies that are routinely targeted by hackers, who can deploy various methods to listen in on the GOOSE packets transmitted through the substation network. They can then disrupt the transmission of information or even bring the entire network down by, for example, creating duplicate GOOSE messages with different states (0 and 1). On the other hand, a person from within the substation network (for example, a disgruntled employee or a former employee with access to the system) could also cause downtime in a substation network by disrupting the transmission of GOOSE packets or duplicating GOOSE packets. The node-based analysis that we recommend can help you quickly identify an issue of GOOSE package tampered and take corrective measures, such as isolating a part of the network, as follows:

1. The Power SCADA in the substation maintains a detailed list of each and every Ethernet switch in the network, with details such as:
    a. Information on each port and the IED connected to the port
    b. The publisher and subscriber IEDs for each GOOSE message
2. When the Power SCADA receives alert messages that indicate that the same GOOSE packet has been received from two ports, it checks the monitoring table to confirm the GOOSE message details.

3. The Power SCADA can quickly identify the duplicate GOOSE message and send an MMS to the network node.
4. Once the faulty network node is identified, corrective measures are implemented to fix the issue.

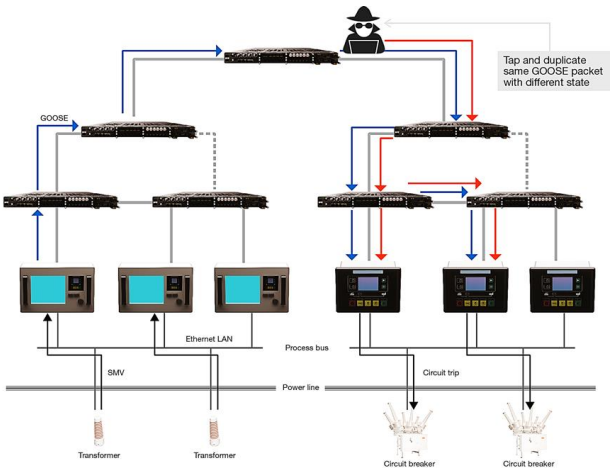

FIGURE 5: GOOSE message tampered scenario

CONCLUSION

In this paper, we present some recommendations and solutions for GOOSE packet monitoring in IEC 61850 substations and suggest ways to set up smart alert mechanisms to help identify traffic bottlenecks locally so that substation operators/owners can implement preventive maintenance measures.

Our recommendations/solutions include:

- Using Ethernet switches to form a node-based GOOSE packet detection mechanism
- Using Ethernet switches to analyze GOOSE traffic and proactively issue alerts to SCADA systems with information on the problematic node

Ethernet switch-based solutions significantly reduce the time required to troubleshoot network issues in a substation and help network administrators to quickly identify the cause of the problem, thereby reducing communication bottlenecks in an IEC 61850 substation.

Transmitting GOOSE messages through Ethernet networks can be complicated and hard to manage. However, knowing how to leverage Ethernet switches as local monitoring nodes can help substation owners/operators manage their substations more efficiently by providing them with a more complete and detailed view of their substation operation.

REFERENCE

1. IEC 61850-8-1:2011 Communication networks and systems for power utility automation, Part 8-1: Specific communication service mapping (SCSM) and Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3