Cyber security threats to IEC 61850 based transmission line protection schemes and what we can do to stop them

Alexander Apostolov

OMICRON electronics, USA

1 INTRODUCTION

The IEC 61850 standard has been used for more than 15 years in different substation protection, automation and control schemes. Even that it was designed for use in substation protection, automation and control systems, it was also applied for many transmission line accelerated protection schemes, such as permissive overreaching, permissive underreaching or directional comparison schemes. The use of the standard GOOSE communications to exchange messages between multifunctional protection relays at both ends of the transmission line exposes the protection scheme to cyber security attacks. This is a concern for protection specialists and that is why the industry is looking at ways to improve the cyber security of the protection system. To better understand the cyber security threats on transmission line protection schemes using GOOSE messages we need to look at what these communications are based on and what possible threats are out there.

2 GOOSE COMMUNICATIONS

High-speed peer-to-peer communications in IEC 61850 based protection and control systems use a specific method designed to meet a variety of requirements. It is very important that the concept of the Generic Substation Event (GSE) model is not based on commands, but on the sending indication by a function that a specific substation event has occurred. It is designed to support reliable high-speed communications between different devices or applications and allows the replacement of hard-wired signals between devices with communication messages exchange while improving the functionality of the protection, automation and control system.

The model includes several features that can be used to improve the reliability, availability and security of the system. At the same time the proper use of these features in vendors' implementation will allow the reduction in maintenance and increase in the flexibility of the system. To understand the reasons for these benefits, we need to look into some of the details of the Generic Substation Event model.

The GSE method can be considered as a mechanism for reporting by a logical device. The achievement of speed performance, availability and reliability depends on the implementation in any specific device.

The generic substation event model is used to exchange the values of a collection of Data Attributes defined as a Data Set. Edition 2 of the standard defines **GOOSE** (Generic Object Oriented Substation Event) that supports the exchange of a wide range data types organized in a data set. The information exchange is based on a publisher/subscriber mechanism.

The publisher writes the values in a transmission buffer at the sending side and multicasts them over the substation local area network to the different subscribers – clients or servers.

The data in the published GOOSE messages is a collection of values of data attributes defined as members of a data set. The receiver reads the values from a local buffer at the receiving side. A GSE control class in the publisher is used to control the process. If the value of at least one of the DataAttributes has changed, the transmission buffer of the Publisher is updated with the local service "publish" and the values are transmitted with a GOOSE message.

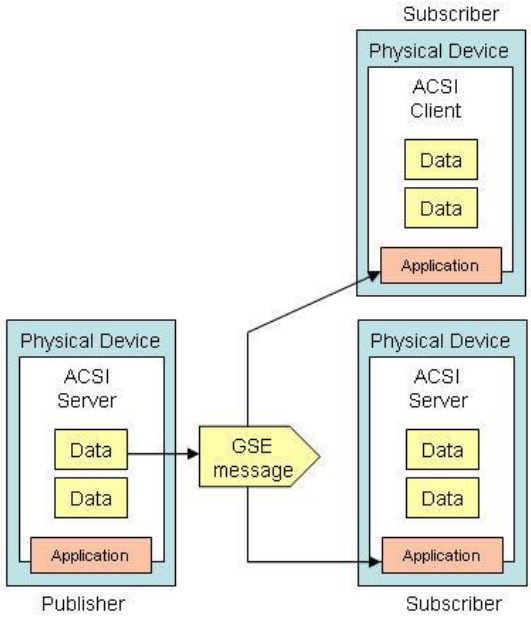

Fig. 1 Publisher/Subscriber mechanism

The publisher/subscriber mechanism allows the source IED to reach multiple receiving IEDs thus significantly improving the efficiency of the communications interface.
Since the GOOSE messages replace hard-wired signals used for protection and control applications IEC 61850 introduces mechanisms that ensure the delivery of the required information.
Once a new value of a data attributed has resulted in the multicasting of a new GOOSE message, the repetition mechanism ensures that the message is sent with a changing time interval between the repeated messages until a new change event occurs.

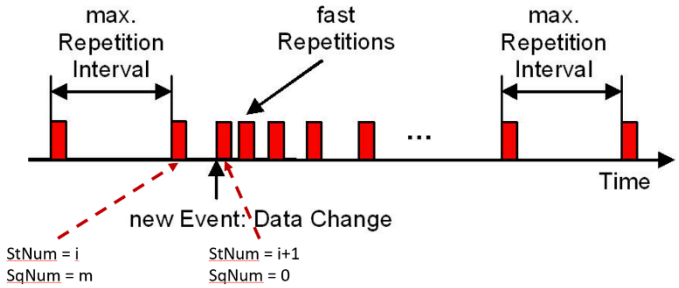

Fig. 2 GOOSE repetition mechanism

As shown in Figure 2, at the beginning after a change the interval is very short – a few milliseconds, which later increases until it reaches a value of a few seconds. This method achieves several important tasks:

- Ensures that a loss of a single message is not going to affect the functionality of the system
- Allows any new device to inform all subscribing devices about its state
- Allows any new device to learn the state of all publishing devices it subscribes to

The GOOSE messages contain information that allows the receiving devices to know not only that a status has changed, but also the time of the last status change. The repetition mechanism can be used as a heartbeat that allows the continuous monitoring of the communications interface – something that is not possible in conventional hard-wired systems.

As already mentioned, the content of the GOOSE message allows the receiving devices to perform processing of the data in order to execute required actions. Some of the data in the GOOSE message that help perform the functions described earlier are:

- T – the time stamp representing the time at which the attribute StNum was incremented.
- StNum indicates the current state number - a counter that increments every time a GOOSE message (including a changed value) has been sent for the first time. The initial value is 1.
- SqNum is the sequence number – the value of a counter that increments each time a GOOSE message with the same values has been sent. The initial value is 0.
- Simulation is a parameter that indicates that the GOOSE message is used for test purposes (if the value is TRUE) and that the values of the message have been issued by a simulation unit and shall not be used for operational purposes. The GOOSE subscriber will report the value of the simulated message to its application instead of the real message depending on the setting of the receiving IED.

The state number and the sequence number can be used to detect intrusion, thus allowing significant improvement in the cyber security of the system without the need for encryption or other cyber security methods.

3 CYBER SECURITY THREATS

Communications are one of the greatest developments of the 20th and 21st centuries, but like everything else in life there are positives and negatives. The positives are that they allow us to implement accelerated protection schemes that improve the performance of the protection systems and the stability of the electric power grid. The drawback, especially when we are not using point to point connections but are going over wide area networks is that communications become the target of cyber security attacks. That is why there are certain requirements that are imposed on communication systems in order to deal with the cyber security threats. These are requirements can be summarized as:

- Confidentiality meaning ensuring that there is no unauthorized access to information
- Integrity meaning that there is no unauthorized modification or theft of information
- Availability meaning dealing with denial of service attacks or prevention of unauthorized access
- Non-repudiation which means accountability and denial of action that took place or claim of action that did not take place

So cyber security protection needs to ensure that these requirements are met by the communication systems. In this paper we are not going to discuss threats such as unauthorized access to IED configuration tools that can allow a hacker to change settings or direct access to an IED that can have a similar impact. The focus is on the direct communications interface between the protection IEDs and what an intruder can do when using IEC 61850 GOOSE messages and how we can prevent undesired tripping of transmission lines by an intruder. We still need to look at the possible threats sources that may have an impact on the communications interface between the protection devices.

The following are some of the threats sources that may have such an impact:

- Low skilled intruders who enjoy getting unauthorized access to utility information systems
- Well-intentioned employees who make inadvertent errors due to inadequate training or poor judgment
- Employees with criminal intent
- Disgruntled employees or ex-employees who cause damage
- High skilled intruders - individuals and organizations directed against the utility
- High skilled terrorists

Low skilled intruders do not represent significant threat to the protection systems because even if they are able to get access to the communications network and copy and manipulate some of the messages that they can see the probability that they will be able to make changes that are not going to be detected be the intrusion detection systems they will not be leading to the tripping of the transmission line.

The dangerous cases are the remaining ones from the list above, because we can assume that skilled intruders are familiar with the standard and they understand the content of the message and the data types of the data

objects or attributes in the data set and they can manipulate them in such a way that will not prevent the detection of the intrusion, but may lead to an undesired tripping before the intrusion is detected. This is what is being discussed in the next section of the paper.

4 INTRUSION DETECTION

Based on the understanding of the GOOSE message design it is possible to implement an intrusion detection mechanism in the subscribing multifunctional IEDs.
It will require analysis of the following data in each message:

- State number
- Sequence number
- Values of data attributes in the GOOSE data set
- Time between consecutive GOOSE messages

The expected behavior of the GOOSE message publisher is that any time when a value of a data attribute in the GOOSE data set changes the following should happen:

- The state number should be incremented by 1
- The sequence number should be reset to 0
- The values of the attributes in the data set should be updated
- The repetition mechanism should be reset to the initial fast repetition values

Any deviation from the above behavior can be used as an indication of possible intrusion.
For example, if there is:

- new state number that is out of order
- new sequence number that is out of order
- new value of a data attribute without a change in the state number

However, if we have the case of a very skillful intruder which is an IEC 61850 expert and is able to penetrate the defense system, get the state number from the repeated messages and publish a GOOSE message with the correct state number and sequence number of zero, this will be a valid message that may lead to a protection operation if a meaningful value of a data attribute is in the data set.

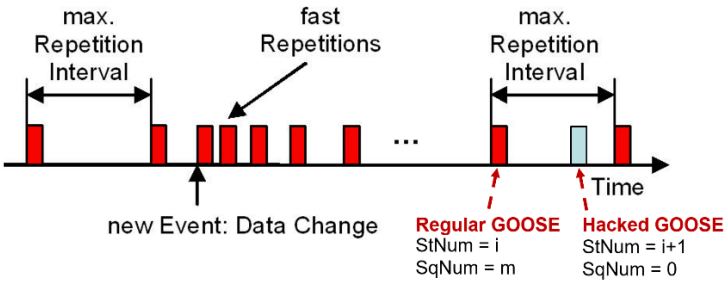

Fig. 3 Hacked GOOSE message

This intrusion will be immediately detected when the next message from the publishers in the substation protection and control systems is received, however this may be too late, depending on the time of receiving of the hacked message within the repetition interval.
What might be helpful in this case is the fact that if the intruder is just monitoring the messages on the communications it is not clear what specific piece of data a data attribute in the GOOSE data set represents. So the intruder might have to try changing values of different attributes that he expects might lead to a protection operation and that is why it is very important that the intrusion is detected as quickly as possible and proper measures are taken to mitigate it.

The most dangerous case is when the intruder has been able to get access to the IED configuration description information about the content of the GOOSE datasets. If this has happened, then the intruder will know exactly which data attribute value to change in order to cause the maximum damage possible.
This is when we need to turn to what I call "functional security", relying on our knowledge of the behavior of the electric power system and protection IEDs under specific fault conditions.

5 IEC 61850 BASED TRANSMISSION LINE PROTECTION

Conventional distance protection does not provide instantaneous tripping for all faults on the protected transmission line. Communications based accelerated schemes allow considerable improvement in the overall fault clearing time for any fault within the zone of protection, while at the same time they do not have the high-speed communication requirements that line differential protection has. This is due to the fact that in these schemes a signaling channel is used to transmit simple ON/OFF data (from a local protection device). This provides additional information to the remote end protection device that can be used to accelerate in-zone fault clearance or prevent operation for external faults. These teleprotection schemes can be grouped into three main operation modes. In each mode, the decision to send a command is made by a local protective relay operation:
In **Intertripping**, (direct or transfer tripping) applications, the command is not supervised at the receiving end by any protection function and simply causes a breaker trip operation. Since no checking of the received signal is performed, it is absolutely essential that any noise on the signaling channel isn't seen as being a valid signal. In other words, an inter-tripping channel must be very secure.
In **Permissive** applications, tripping is only permitted when the command coincides with a protection operation at the receiving end. Since this applies a second, independent check before tripping, the signaling channel for permissive schemes does not have to be as secure as for Inter-tripping channels.
In **Blocking** applications, tripping is only permitted when no signal is received, but a protection operation has occurred. In other words, when a command is transmitted, the receiving end device is blocked from operating even if a protection operation occurs. Since the signal is used to prevent tripping, it is clear that a signal is received whenever possible and as quickly as possible. In other words, a blocking channel must be fast and dependable.
The protection function that sends the permissive or blocking signal to the remote end determines the type of scheme used. If this is a distance element, we usually talk about Permissive Underreaching or Overreaching schemes, or Blocking schemes. If a directional element is used to initiate the transmission of a signal to the remote end of the protected line - we have Directional Comparison schemes. A directional comparison schemes can be Permissive or Blocking, with directional elements initiating the signal transmission and providing the supervision at the receiving end.
Permissive schemes tend to be more secure than blocking schemes because forward directional decisions must be made at both ends of the line before tripping is allowed. Failure of the signaling channel will not result in unwanted tripping, because no signal is going to be received and the relay does not trip based on a forward directional detection only.
The challenge for the implementation of accelerated transmission line protection schemes is that they require a communications channel which, if it is a dedicated one, will require additional costs.
IEC 61850 GOOSE messages are a technology that can help us achieve these goals without significant additional expenses and can be used with different technologies.

5.1. GOOSE over MPLS

The GOOSE message was designed for peer-to-peer substation communications and because of that it uses a three-layer stack and MAC multicast. This is not suitable for messages that need to be sent over a wide area network. For that reason, we need additional features to support GOOSE transmission over wide area networks.

MPLS networks became the focus of evaluation and deployment in power utilities. The Multiprotocol Label Switching (MPLS) is a packet-forwarding technology which uses labels in order to make data forwarding decisions. The Layer 3 header analysis is done just once (when the packet enters the MPLS domain). Label inspection drives subsequent packet forwarding.
In the traditional 7 layer OSI model Layer 2 covers protocols like Ethernet which can carry IP packets, but only over simple LANs or point-to-point WANs while Layer 3 covers Internet-wide addressing and routing using IP protocols. MPLS sits between these traditional layers, providing additional features for the transport of data across the network. Because of that MPLS is sometimes called a "Layer 2.5 networking protocol".
This technology allows the engineering of paths between substations that can transport layer 2 traffic through the WAN, thus effectively extending the LAN into the remote substation. IEDs communicating via GOOSE can exchange information with remote device just as if they were connected to the same local network.

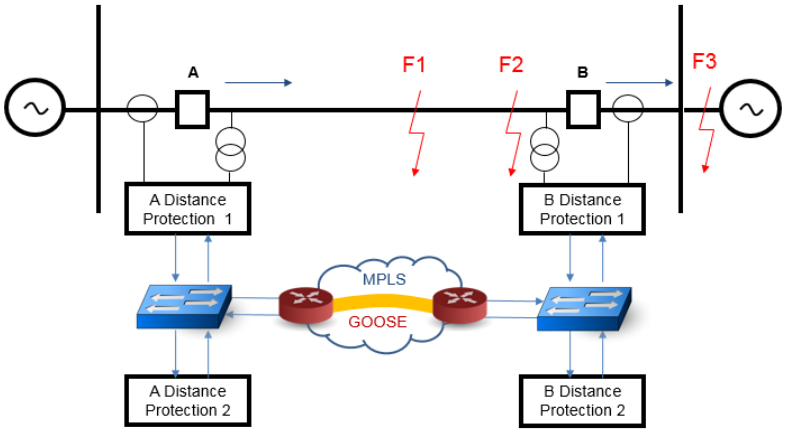

Fig. 4 GOOSE over MPLS

5.2. R-GOOSE

The technical report IEC 61850 90-5 Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118 is the document that also defined the methods for transmitting GOOSE messages over wide area networks based on IP solutions. This report selected UDP/IP as the option to transmit data over large distances. The GOOSE messages based on this technology became known as Routable GOOSE of R-GOOSE.
The Internet Protocol (IP) is a Layer 3 protocol. The Network layer adds the concept of routing above the Data Link layer. When data arrives at the Network layer, the source and destination addresses contained inside each frame are examined to determine if the data has reached its final destination. If that is true, this Layer 3 formats the data into packets delivered up to the Transport layer. The IP allows the routing of data packets (IP packets) between different networks over any distance.
The User Datagram Protocol (UDP) is a Transport Layer 4 network protocol. While TCP (Transmission Control Protocol) is a connection-oriented protocol that requires first to establish communications between a client and a server, UDP is connectionless, which makes it more suitable for GOOSE communications.
To ensure the security of the R-GOOSE messages the technical report IEC 61850 90-5 specifies a mandatory mechanism to provide the needed end-to-end cryptographic integrity using the definitions from IEC 62351-6.

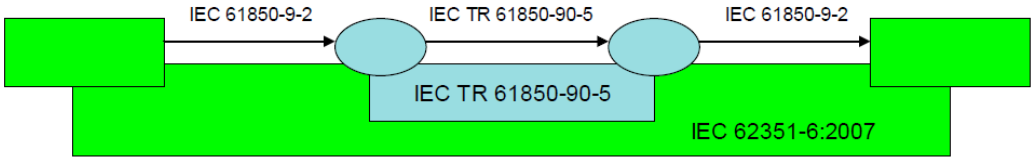

Fig. 5 End-to-end cryptographic integrity

5.3. FUNCTIONAL SECURITY

The use of wide-area GOOSE for permissive schemes is better from a cyber-security point of view because even if a hacker is able to penetrate the communications link and send a permissive GOOSE, the receiving end is not going to trip if it does not see a fault itself. We can define this as “functional security”, because the tripping of the local breaker is not activated simply based on the received GOOSE message but is functionally supervised in the POTT trip logic by the start of the Zone 2 distance element represented by a PDIS logical node.

The case is more complicated for direct transfer trip (DTT) schemes. In principle they do not require local supervision and because of that may lead to a tripping of a breaker when a hacked GOOSE message is received. This can be improved if there is redundancy in the data that is included in the GOOSE data set - for example if the DTT data objects is in the same data set with a different data object indicating the operation of a protection element (maybe breaker failure protection) that resulted in the DTT. It will be more difficult for the attacker to modify both pieces of data that have functional relationship without knowing the specific structure of the data set. This way the subscribing device can check if both the DTT and the protection element changed states at the same time, it will use that as the functional security criteria to allow or block the tripping of the breaker.

The worst case scenario is if the intruder knows the structure of the data set so he can manipulate related data attributes that may lead to the tripping of a circuit breaker. This is when the functional security should include same logic that relies on a good understanding of what might be the reason to issue the direct transfer trip. In most cases this is done for a busbar fault and breaker failure to clear it. The local breaker failure function then sends the DTT signal to the remote end to clear the fault. But if there is a busbar fault at the remote substation it should be seen buy the zone 2 of the local distance protection. So when the IED receives the DDT message it will check if there is a zone 2 start on that transmission line and if there isn't this will mean that this may not be a valid DTT message. But any such logic needs to be developed based on good understanding of the protection schemes at both ends of the line and detailed analysis of the expected behavior during a variety of fault conditions.

6 TESTING

The implementation of the functional security capability requires proper testing to verify that it is operating as expected under different electric power system conditions.

The test system needs to be capable of simulating normal power flow, as well as short circuit fault conditions to verify that the transmission line protection scheme will operate when a short circuit fault occurs without the additional time delay based on the received GOOSE message from the remote end of the line. However, it should also demonstrate that there will be no breaker trip when a GOOSE message indicating the operation of a protection function at the remote end has been received is the result of attacker interference. This will require during the tests a message with a correct state and sequence number to be sent over the communication interface to the receiving protection device to verify the performance of the redundant data based functional security mechanism. We need to have the ability as part of the test to simulate messages that in some cases will have the redundant data change simultaneously in order to indicate correct operation or do

not change simultaneously, which will be used as intrusion detection and for blocking the tripping of the breaker.

7 CONCLUSIONS

The availability of specific features in the GOOSE publishing mechanisms allow for the development of intrusion detection methods that can be implemented in the subscribing IEDs. Additional end-to-end security is implemented in R- GOOSE based on IEC 62351-6. The intrusion detection is based on the monitoring of state and sequence numbers, as well as data attribute value changes.
Using good understanding of the protection system of the transmission line and its operation during different fault conditions can be used to implement a mechanism of “functional security” that will prevent the undesired ttripping of the transmission line even if an intruder has been able to successfully avoid the cyber security protection mechanisms.

REFERENCES

[1] IEC TR 61850-90-5:2012 Communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118

[2] IEC 62351-6:2020 Power systems management and associated information exchange – Data and communications security - Part 6: Security for IEC 61850