International Journal of Security and Its Applications
Vol. 10, No. 4 (2016), pp.289-302
http://dx.doi.org/10.14257/ijsia.2016.10.4.27

Trust System Architecture for Securing GOOSE Communication in IEC 61850 Substation Network

Muhammad Talha Abdul Rashid, Salman Yussof and Yunus Yusoff

Center for Information and Network Security
College of Information Technology
Universiti Tenaga Nasional
Malaysia
muhammadtalhaf021@yahoo.com.my,
{salman, yunusy}@uniten.edu.my

Abstract

IEC 61850 is the standard for substation automation which enables substation equipment called Intelligent Electronic Devices (IEDs) to communicate with each other. The communication protocol used by the IEDs to communicate is called GOOSE. Unfortunately, there are security researchers who have identified a number of vulnerabilities in the GOOSE protocol and have demonstrated that these vulnerabilities can be exploited to perform security attacks on the IEC 61850 network. By itself, the IEC 61850 standard does not address security requirements needed in a critical infrastructure. Therefore, a security mechanism to better protect the IEC 61850 network needs to be implemented. In their paper, Coates et al. has proposed a Trust System for securing the TCP/IP communication of SCADA network. However, due to the focus on TCP/IP communication, the Trust System by Coates et al. cannot be directly utilized for the IEC 61850 network because the IEDs are using GOOSE protocol to communicate. This paper proposed a Trust System for securing GOOSE communication between IEDs in IEC 61850 network. The proposed Trust System contains the modules for firewall, format and pattern validation, priority level assignment, alerting, blocking, and event logging.

***Keywords**: Trust System, IEC 61850, GOOSE, Security Attacks, Substation Automation*

1. Introduction

IEC 61850 is an Ethernet-based standard for substation automation system communication. This standard was introduced in 2003 by International Electro-technical Commission's (IEC) Technical Committee 57 (TC57) [1]. All communication requirements and needs within the substation environment network are covered in this standard. There are fourteen sections inside IEC 61850 that is published between 2003 and 2005 [2]. Protocols defined on IEC 61850 are MMS (Manufacturing Message Specification) in section 8.1, GOOSE (Generic Object Oriented Substation Event) and SMV (Sampled Message Value) in sections 9.1 and 9.2.

IEDs (Intelligent Electronic Devices) inside an IEC 61850 substation have specific requirement such as fast communication, ensured delivery times, and multi-vendor interoperability. The IEC 61850 standard covers the requirement needed by IEDs by providing dependability, proficiency, adaptability and interoperability. IEDs can take advantage on the utilization on Ethernet communication for IEC 61850 GOOSE messages that ensures high-speed performance functions [1].

A typical electrical substation contains a number of IEDs and additionally a number of clients to access the IEDs. Validation and identification of gadgets and persons are

ISSN: 1738-9976 IJSIA

required in order to keep IEDs data and network in the substation secured. Dependable, adaptable, proficient and secure communication protocols are needed to offer both time-critical operation and secure communication in the substation network [1].

The IEC 61850 standard only provides the specification for communication between IEDs and clients within a substation network. However, it does not specify any security requirements that are important in any critical infrastructure. To address the security issues, another standard called IEC 62351 has been proposed. This standard provides security measurement, mechanism and protection for the IEC 61850 standard and some other standard [2]. Part 6 in IEC 62351 proposed security measures such as authentication for GOOSE protocol for real-time communication [2]. However, because of the strict time performance requirement of GOOSE messages, "security measures which affect transmission rates are not acceptable." (International Electrotechnical Commission 2007a, p.30). Therefore, the IEC 62351 standard does not propose any encryption for GOOSE messages.

There are security researchers who have identified security weaknesses in the GOOSE protocol and have demonstrated that these weaknesses can be exploited to launch security attacks on IEC 61850 network. Hoyos *et al*. proposed a malware attack that can capture, alter and re-inject GOOSE messages into the substation network [3]. Hong *et al*. demonstrated a modification attack that can be used to compromise an IED [4][5]. He has also demonstrated that it is possible to perform DoS attack on an IED by sending large number of GOOSE messages. Kush *et al*. has managed to perform a DoS called the GOOSE poisoning attack which would render genuine GOOSE messages to be out of date and in this way the valid GOOSE messages would not be able to be processed by the targeted IED [6].

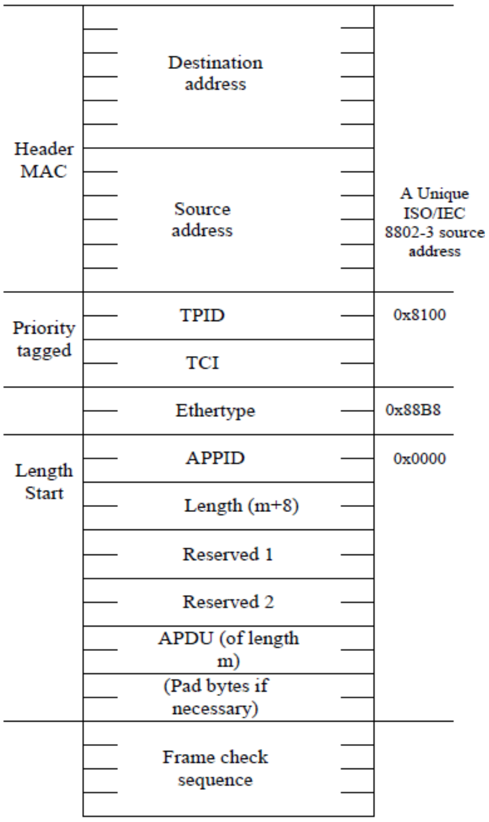
This paper proposes a Trust System architecture for securing to the IEC 61850 GOOSE communication in substation network, especially from the GOOSE-based security attacks that have been identified by researchers. The proposed Trust System is adopted from the Trust System that was originally proposed and defined by Coates *et al*. for SCADA network in a regional utility intranet [7]. This Trust System is based on best-of-breed utilization of standard IT system security components and IP protocols. The Trust System provides a nonproprietary system, system inside of systems, or computer program agents that connect to a current network, somewhat transparently, to perform the elements of relating information and recognizing risk levels for comparing events and status updates that indicate negative effects on utility services [7][8]. However, instead of using the Trust System to evaluate TCP/IP messages, the Trust System will evaluate the GOOSE messages used by IEDs in IEC 61850 substation to communicate.

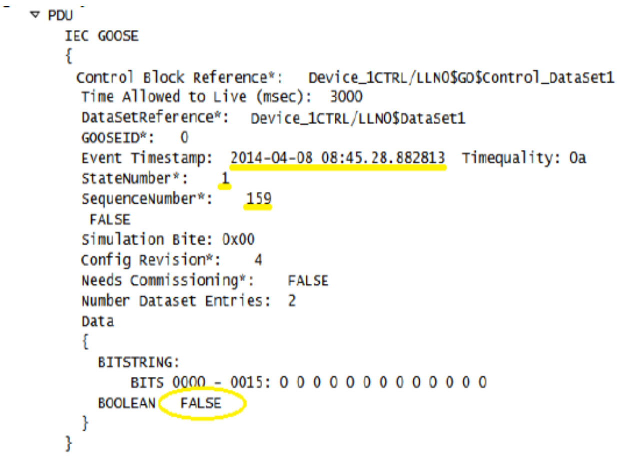
The rest of the paper is organized as follows. Section 2 provides an overview of the GOOSE protocol. Section 3 describes on the Trust System that has been proposed for SCADA network. Section 4 describes the security attacks that can be performed on IEC 61850 network by exploiting the GOOSE protocol. Section 5 presents the proposed Trust System model to be used for securing GOOSE communication in IEC 61850 substation network. Lastly, Section 6 concludes the paper.

2. IEC 61850 GOOSE Protocol

The main goal of the GOOSE protocol is to provide a fast and reliable mechanism that permits the exchange of information between two or more IEDs over IEEE 802.3 networks. To trade these datagrams, IEC 61850-8-1 describes a communication based on a publish/subscribe model, where the messages is created and send from one IED (the publisher) to a group of destination IEDs (the subscribers) at the same time in a single transmission from single source [5].

GOOSE is not the same as other protocol utilized in substation automation because it uses three layers in Open Systems Interconnection (OSI) model stack, *i.e*., physical, data link, and application layer, for the real-time requirement. This GOOSE scheme utilizes the Media Access Control (MAC) address. GOOSE messages permit a sending IED, a publisher, to multicast user-configurable state information to receiving IEDs, known as subscribers. GOOSE is an unacknowledged connectionless communication protocol, in that, the subscribers do not send acknowledgement to the publisher. The GOOSE services use as a re-transmission plan to improve communication speed and dependability.





```
- ▽ PDU -
     IEC GOOSE
     {
       Control Block Reference*:   Device_1CTRL/LLNO$GO$Control_DataSet1
        Time Allowed to Live (msec):  3000
        DataSetReference*:  Device_1CTRL/LLNO$DataSet1
        GOOSEID*:   0
        Event Timestamp:  2014-04-08 08:45.28.882813  Timequality: 0a
        StateNumber*:    1
        SequenceNumber*:    159
         FALSE
        Simulation Bite: 0x00
        Config Revision*:    4
        Needs Commissioning*:    FALSE
        Number Dataset Entries:  2
        Data
        {
          BITSTRING:
              BITS 0000 - 0015: 0 0 0 0 0 0 0 0 0 0 0 0 0
          BOOLEAN    FALSE
        }
     }
```

Figure 2. GOOSE APDU Fields [9]

Figure 1 and 2 show fields inside a GOOSE message. The trust system proposed in this paper will need to evaluate a number of these fields, namely the destination and source

MAC address, and Ether-type inside the GOOSE message frame, while T (time-stamp), stNum (State Number), sqNum (Sequence Number) and Data are inside GOOSE APDU (Application Protocol Data Unit) [9].

The destination field is related to an Ethernet MAC multicast address. IEC 61850 has been assigned Ethernet addresses that begin with the three first octets (01-0C-CD). The fourth octet should be 01 for GOOSE protocol. The last two octets of the six are utilized as individual locations for every GOOSE message. The source address is a unicast MAC address. The Ether-type for a GOOSE message type is defined 0x88B8. T is the "time-stamp" field at which the number in the stNum was incremented. StNum field is a counter that increment every time a GOOSE message that has been generated as a result from event change in the substation. SqNum field is a counter that increased in increment order to retransmitted GOOSE messages [3]. Finally, the data field contains the information about the GOOSE message in Boolean values.

Any event that happens in the substation can cause IEDs to transmit a GOOSE message. The same message is retransmitted multiple times with increasing delay and with increments in sqNum until the following new event occurred, which requires the stNum to be incremented. The sqNum is reset to '0' when the stNum is changed. In any case, the particular time of re-transmission (interval) is not specified in the IEC 61850 standard. Therefore, distinctive vendors' GOOSE re-transmission times may differ. Since GOOSE is a multicast protocol utilizing the data link layer, there is no logical address and flow control functionality. Consequently, there is no authentication implemented for the message.

3. Trust System for SCADA Network

The Trust System proposed by Coates *et al*. is a communication security device, which is combined together with firewall and intrusion detection abilities, designed for use with strict real-time requirements network systems [8]. The concept of this proposed trust system is to take common standalone security products (*i.e*., firewalls, IDSs, router ACLs, *etc*.) in the IT security community and incorporate them in one package that is designed to address the security issues of SCADA and other power system requirements [7].

The Trust System operation involves several steps. The first step is to capture status messages or instructions from nodes inside the network. After the Trust System captures the status message, it then assigns the right data types (*e.g*., network, operational, financial data) to each of the message that contains good and verified data elements (*e.g*., values, files). Next it figures out whether the recipient is approved to read all of the message's data types. If not, it clears out the parts of the messages that the receiver is not authorized to read before sending it to the receiver. Finally, data elements that are legitimate are sent to database systems that can be used for company intranet display and to an archiving system to be used for future analysis [7].

3.1. Trust System Components

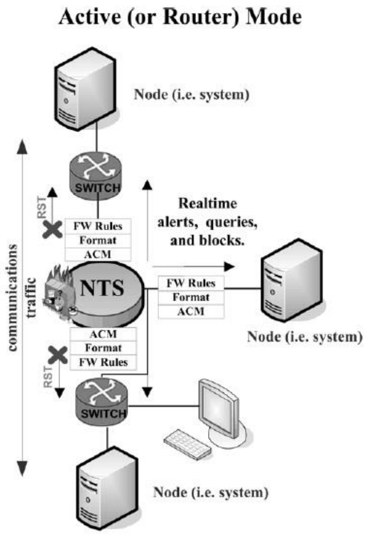


Figure 3. Trust System Active Mode [3]

Figure 3 shows the trust system in active (or router) mode. All of the communication traffic will be going through this enhanced router labelled Network Trust System (NTS) in the Figure 3 above. The component in trust system is separated into firewall rules and format module, access control matrix (ACM), suspicious event handler (SEH), and an outgoing message handling. The following sub-sections explain these components in more detail.

3.1.1. Firewall Rules Module: Firewall rules check: These rules filter one by one the incoming packets based on the combination of source/destination IP, message type allowed, protocol, source and destination port numbers, and trust system interface. Firewall rules scorekeeper (FWR-SK) will keep track of this information with a score, where a score '0' is for pass and score '1' is for fail, in which case the packet will be discarded by the firewall.

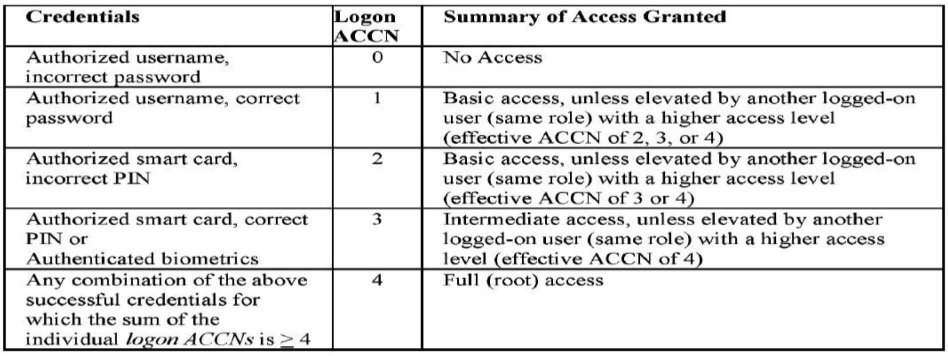
Encryption check: All messages transmitted between systems on the SCADA network should employ encryption, for example, network-layer IPSec. The arriving messages are decrypted by the trust system using its own private key together with the sender's public key.

3.1.2. Format Module: Input Validation and Format Checks: This module is different from the standard firewall module because it also investigates the packet's header size, contents, and application data. The trust system uses the following format rules to check and analyze the packets: - a) Compare between message length to the expected length. b) Compare between content and values to expected values/ranges. c) Compare between message source_IP to logged_on_IP of the system name. d) Compare between message source_IP to logged_on_IP of the username (if message was initiated by user instead of other system). Like the firewall rules check, a format scorekeeper (FOR_SK) keeps tracks whether the packet passes or fails this check. This information is then sent together with FWR-SK to the access control matrix (ACM).

Data Tagging: Tag is utilized by the ACM for access control and can likewise be utilized for data archiving, so that later access by users and systems can be verified with a trust system ACM's for approval. The tag for data element and other metadata parameters can likewise be transported along with the data (or file) when it is copied, pasted, modified, and attached to e-mails.

3.1.3. Access Control Matrix (ACM) – Logon Security: Initial Network Logon Control: Logon ACCN (Access Credentials Control Number) represents a reliability of a logon credentials, effective ACCN is the total summation between trust level for the user (or system) and the logon ACCN, and logon IP is the source IP address from which the logon occurred. The values of logon ACCN, effective ACCN, and logon IP are initially at value zero until a user or system signed onto the network. After a logon has been authorized, the logon IP, logon ACCN, and effective ACCN are updated in the ACM. If the user signed off from the network, the values are reset to zero. Based on this, the trust system can know the users that are signed on and from which area. Trust system uses the results either successful or failed credentials, given by the logon server, to compute the logon ACCN, utilizing the characteristic outlined in Table 1 below.

Table 1. Example LOGON ACCNs Assigned Based [3]



Credentials	Logon ACCN	Summary of Access Granted
Authorized username, incorrect password	0	No Access
Authorized username, correct password	1	Basic access, unless elevated by another logged-on user (same role) with a higher access level (effective ACCN of 2, 3, or 4)
Authorized smart card, incorrect PIN	2	Basic access, unless elevated by another logged-on user (same role) with a higher access level (effective ACCN of 3 or 4)
Authorized smart card, correct PIN or Authenticated biometrics	3	Intermediate access, unless elevated by another logged-on user (same role) with a higher access level (effective ACCN of 4)
Any combination of the above successful credentials for which the sum of the individual *logon ACCNs* is ≥ 4	4	Full (root) access

Work Schedule Restricted Access: The trust system can also determine each logon attempts whether it is against a normal work routine. This enables the trust system to detect abnormal activities, for example, an employee coming in after working hours with the intention to attempt something malicious.

Simultaneous Logon Control: On the off chance that a user, as of now already logged on at one IP address, attempted again to logon from a second IP address, then the trust system need to check its simultaneous_logon_limit parameter to guarantee that the highest possible number of simultaneous logons for single user would not be violated before issuing a logon_approved message.

3.1.4. Access Control Matrix (ACM): Distributed Access Control Matrices: the system/nodes are only approved to send/receive some types of message to/from particular other systems, and just on interfaces that corresponding to their routing tables. In this trust system by [7], it is assumed that local ACMs at every node send an update to the network-level ACM on the SCADA network trust system every time the node authenticates an upgrade to its own particular ACM.

Standard Access Levels: a nodal ACM maintains the entries for all users who are authorized to access the node and all systems approved to communicate with it. Most access level in the trust system is defined as a standard, in this case the Trust System uses the Standard Access Levels Table (SALT) inside the trust system. SALT contains an authorized access operations based on the user's (or system's) role and ACCN. For example, a user with access level 4 can do read and execute operation on SCADA code and logs, but the user cannot edit them.

Message Sanitization: when a recipient is approved to get a message type, but is only permitted to access a subset of the data element contained in the message, the trust system can perform a process called sanitization to the message before sending it. In this sanitization process, the trust system can check and compare the access level of every data element type of every single label in the message, and the caveat (*i.e*. company-sensitive, no vendors) of the data element types, with its ACM. Even an e-mail attachment could be filtered by this sanitization process to look for files that are not approved for the recipient to download.

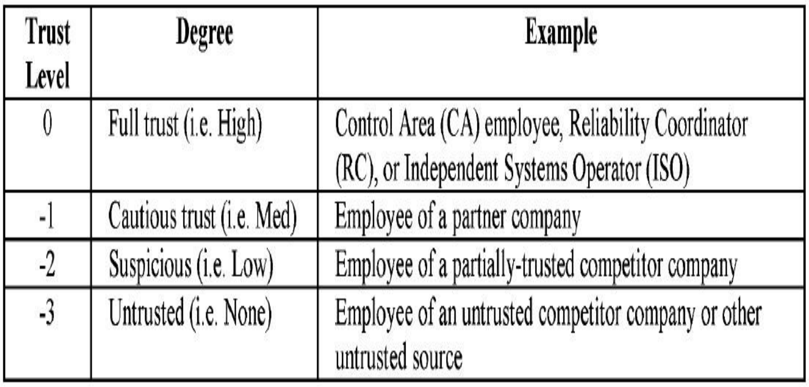
Access Violation Attempts: when a user tries an access operation, the requested data type to access and the access operation on that data type is checked against the ACM for the single person role and EACCN. If the user that requested for the access operation is not approved, the attempt is denied and the system starts up a suspicious event.

ACM Scorekeeper: this scorekeeper (ACM-SK) keeps track of failed logon, simultaneous logon, and failure of an access operation. All of the collected scorekeepers are sent to the Suspicious Event Handler (SEH) module.

3.2. Trust Levels

A trust level of 0 indicates that it is good and trust level of -1 to -3 indicate that something fishy has happened which causes the trust system to start monitoring further traffic from a specific source with higher suspicion. Trust level that is low will also decrease the ACCN level, and because of this, the access level of the user/system is affected. Table 2 below show the trust level from 0 to -3.

Table 2. Example of Trust Levels [3]



Trust Level	Degree	Example
0	Full trust (i.e. High)	Control Area (CA) employee, Reliability Coordinator (RC), or Independent Systems Operator (ISO)
-1	Cautious trust (i.e. Med)	Employee of a partner company
-2	Suspicious (i.e. Low)	Employee of a partially-trusted competitor company
-3	Untrusted (i.e. None)	Employee of an untrusted competitor company or other untrusted source

This trust system proposed by [7] is designed for the SCADA network between companies in a regional utility intranet. This security mechanism mainly authenticates messages from the point of access control or logon credentials and access privilege. The messages that are used for simulation in this trust system are IPv6-based TCP and UDP protocols. UDP was use for non-real-time updates and trust system inquiry, to reduce network congestion [7]. On the other hand, TCP was used for urgent emergency traffic and real-time or almost real-time traffic that either requires reliability or would be implemented as TCP by its manufacturer [7]. The trust system proposed by [7] operates on the TCP and UDP traffic transmitted in SCADA network. However, it does not provide any security defense mechanism for IEC 61850 GOOSE communication.

4. IEC 61850 GOOSE-based Security Attacks

As mentioned earlier in the introduction section, there are security researchers who have demonstrated that the vulnerabilities in GOOSE protocol can be exploited to launch security attacks on IEC 61850 substation automation network. The following sub-sections further elaborate the GOOSE-based attacks that have been carried out by the security researchers.

4.1. Attacks

4.1.1. GOOSE Modification Attacks: The first GOOSE modification attack is based on malware attack by Hoyos *et al*. This malware is based on automated script that changes the following fields in the GOOSE packet: state number (stNum), sequence number (sqNum) and the Boolean values inside GOOSE message structure. The script will reset the stNum and sqNum automatically to zero and for the Boolean values, if the value is true the script overwrites it to a false value and the vice versa [3].

After the script has successfully modified the GOOSE packet, the packet is injected back into the network. The cloned packet will enter in the middle of a GOOSE communication and this will make the GOOSE messages communicated and transmitted out of sequence. The field devices (*i.e*. the IEDs) did not produce any error or alert that the message is out of sequence [10].

The second modification attack is proposed by Hong *et al*. that relies on modification the sequence number (sgNum) and state number (stNum), time, and the binary data value [5]. GOOSE sqNum and stNum modification attack is done by capturing the GOOSE packet and change the sqNum or stNum value and send the packets back into the transmission [10]. The result from this attack will make circuit breaker to issues a warning in the substation [4][5]. GOOSE timestamp modification attack done by modification the transfer time to make it greater than the recommended GOOSE transfer time specified as 4ms. The result from this attack are the same as the stNum and sqNum modification attack. Final modification attack is on the binary data value inside the GOOSE packet. The value is change from false to true or vice versa. The result from this modification attack is that it can cause a circuit breaker to open without proper authorization.

4.1.2. GOOSE DoS Attacks: Hong *et al*. demonstrated a GOOSE DoS attack which is are done by injecting a number of GOOSE packets that are greater than the number of packets allowed within the time threshold for GOOSE packet transmission. This may cause to targeted IED to lose availability and stop responding to other requests [4][5].

Another GOOSE DoS attack is the GOOSE poisoning attack proposed by [6]. This attack has three separate variants. The variants are high status number attack, high rate flooding attack, and semantic attack. In high status number attack, the attacker sends a single spoofed GOOSE packet with a very high status number from the attacker to a legitimate GOOSE receiver. In high rate flooding attack, the attacker sends multiple number of spoofed GOOSE packets, with incrementing status number. The spoofed GOOSE packets will eventually carry a status number higher than the one expected by the GOOSE receiver. The final variant is the semantic attack and it is divided into two phases. In the first phase, the attacker will monitor the network traffic to determine the status number in the GOOSE packet currently transmitted and to figure out the rate of status number change. In the second phase, the attacker will spoof GOOSE packets with a higher rate than the normal rate of status number change. The result from this second phase is it will prevent the real GOOSE message from being processed by GOOSE receiver [10].

4.1.3. GOOSE Replay Attack: The GOOSE replay attack was demonstrated by [4][5]. The attack is done by capturing the packets transmitted between IEDs with the intention to retrasnmitted the same captured packets without alteration in order to achieve a specific result as intended by the original message [10]. The results from this replay attack can cause a circuit breaker to open without authorization [4][5].

4.2. Consequences of Security Attacks

The GOOSE packet malware may cause unauthorized changes in the field inside GOOSE messages which could cause problems such as automation breakdown, circuit breaker to perform incorrect operation, bypassing interlocks and even damaging the field devices physically. In the event that the attack compromises a bus bar or differential protection, more than one distribution or transmission circuit could also be affected [10].

The GOOSE manipulation attack will allow the attacker to gain control and operate circuit breakers without authorization. Attacks that can affect the transmission time such as the attack that affect the packet generation and receive time and the high rate flooding attack will give a significant decline in performance for GOOSE communication inside the substation [10].

5. Trust System for Securing GOOSE Communication

Since the security researchers have shown that the GOOSE protocol can be exploited to launch security attacks, it became clearer that the GOOSE protocol needs to be protected by a security mechanism, such as the trust system proposed by [3]. A Trust System for GOOSE communication is a security device that is a switch, with firewall and intrusion detection abilities to detect GOOSE security attacks, specifically designed to operate within the real-time requirement for GOOSE communication inside substation network. The benefits from this trust system for GOOSE communication is that the security system can give a comprehensive and all in one package of IT security solution (*i.e.*, firewall, intrusion detection, alert or blocking handler, *etc.*) to counter GOOSE security threats. This trust system will also provide defense in layered or defense in depth technology by thoroughly checking and preventing from the GOOSE security threats explained in Section 4.

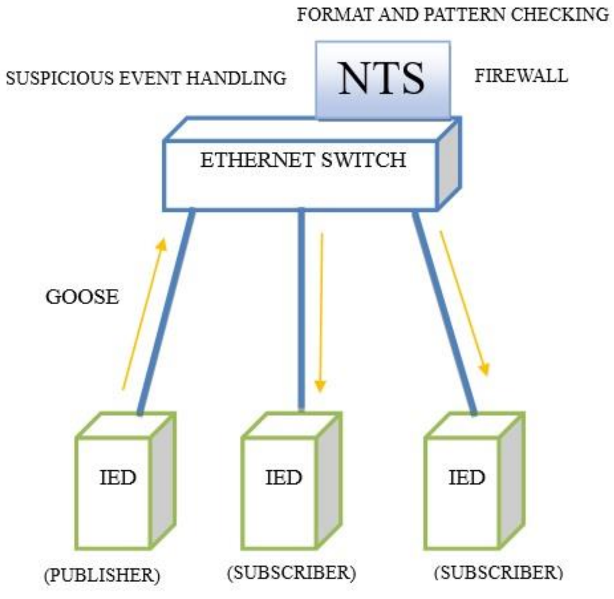


Figure 4. Trust System Architecture for GOOSE

Figure 4 shows how and where the trust system will be implemented inside the IEC 61850 substation network. This trust system is included inside a switch as an enhancement in order to monitor GOOSE communication between publisher and subscriber IEDs. These trust system architecture contains components that can validate whether the GOOSE packet is legitimate or is part of a malicious attacks. The components are firewall, format or pattern checking, priority assigning, and suspicious event handler (SEH). These components are further explained in the following sub-sections.

5.1. Firewall Rules

The trust system is set to recognize a signature for authorized traffic. Functionalities of these rules are to filter incoming GOOSE packet on the combination of source/destination MAC address pairs, the Ether-type for GOOSE message, and the trust system interface that is accepting the packet. The MAC address in the GOOSE packet needs to be same as IEDs MAC address defined inside the trust system and the Ether-type for GOOSE needs to be ‘0x88B8’. If the rules detected a difference in MAC address and Ether-type in the GOOSE packet, the pass and fail parameters, known as labels, are updated in the GOOSE firewall rules scorekeeper (GFWR-SK) with a score value of 0 for pass or 1 for fail. The GOOSE packet that fails the firewall rules checking may be discarded.

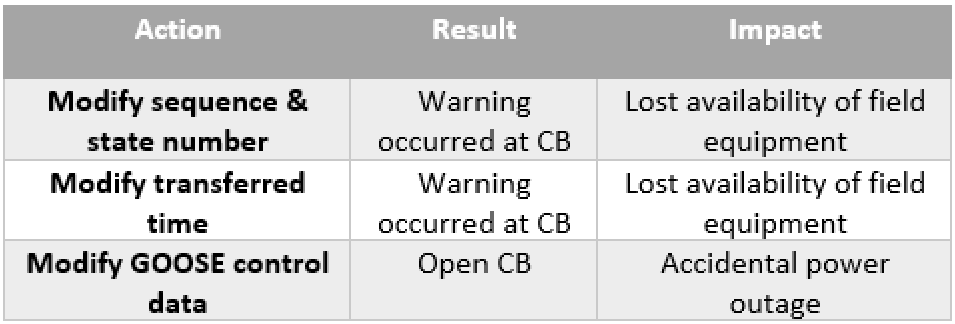
5.2. Format and Pattern Checker

This component has three separate GOOSE fields checking mechanism for a malicious packet. The fields are, status number (stNum) and sequence number (sqNum), Timestamp and Boolean data field. The following sub-sections describe the three GOOSE field checking mechanisms.

5.2.1. stNum and sqNum: stNum Check: The trust system reads the stNum field and compares it to the stNum value of the previous packet based on the following rules. The first rule is that the value for stNum cannot be (2^{23} - 1) because the previous value is not (2^{23} - 2) as this value was used by [8] for high status number attack. The second rule is that the value cannot be 5800 because the previous value is not 5799 and this value was used by [8] as a starting status number for high rate flooding attack. This checking mechanism is used for preventing the GOOSE poisoned attack described in [8].

sqNum Check: If the GOOSE packet passed the above stNum check then the sqNum field will be checked next to see whether it is in the correct sequence. The rule checks if a captured GOOSE messages sqNum is not set to zero after the stNum is changed or the sqNum itself is out of sequence. This can detect the GOOSE packet malware attack done by [7] and GOOSE manipulation attack by [5] and [6].0

Table 3. GOOSE Attack Results [5]



Action	Result	Impact
Modify sequence & state number	Warning occurred at CB	Lost availability of field equipment
Modify transferred time	Warning occurred at CB	Lost availability of field equipment
Modify GOOSE control data	Open CB	Accidental power outage

stNum and sqNum Scorekeeper (STSQ-SK): If the GOOSE message does not pass the rules, the pass and fail parameter, known as label, are updated in the stNum and sqNum

Scorekeeper that contains name, value, and score (0 = passed or 1 = failed). At this point, if one of the stNum or sqNum checks failed, the GOOSE packet is assigned with score value of 1. Table 3 shows the result and impact based on modification of the sequence and state number that can trigger a warning alert on the circuit breaker inside the substation. The scorekeeper will record the value of 1 if this unauthorized modification of stNum and sqNum occurred.

5.2.2. Time: Timestamp Check: The GOOSE message is forwarded from the stNum and sqNum Module to this time module to check if it violates the time rules for GOOSE message. GOOSE transfer time requirement is 4ms. Therefore, the rule is that the difference between the generated time and receive time cannot be greater than the 4ms transfer time.

Time Threshold Check: For this section the trust system will check if the number of captured GOOSE packet within predefined time is greater than the predefined threshold for number of GOOSE packets within the predefined time or there is no captured GOOSE packet within the predefined time. For example, let's say that a sender transmits 1000 GOOSE packets per second. This number of packets is too large and this fits the signature of a GOOSE manipulation attack described by [5] and [6]. The checking mechanism proposed here will be able to detect and prevent this kind of attack.

Time Module Scorekeeper (TM-SK): This TM-SK functions similar to the STSQ-SK. It tracks the pass/fail value of the label and this label are then forwarded along with the STSQ-SK to the Data checking module. Table 3 shows that if modification on the transfer time occurred, this action will also trigger a warning on circuit breaker in substation. The scorekeeper will be changed to 1 when this modification action occurred.

5.2.3. Data: Data Integrity Check: In this module the trust system checks if the GOOSE indicator that contains the binary control value is changed from false to true or vice versa. According to IEC 61580 standard, when the binary control value is changed, the stNum of the GOOSE message also needs to be changed to the next number in sequence and the sqNum needs to be reset to zero. This mechanism will check whether this standard is violated. Data checking mechanism is for detecting and blocking against the GOOSE packet malware attack described in [7] and GOOSE manipulation attack described in [5] and [6].

Data Scorekeeper (D-SK): D-SK also functions the same as STSQ-SK and TM-SK and all three labels are forwarded together to the next step to assign level of priorities. Based on Table 3, modification on GOOSE data or GOOSE control data can be critically severe as it can cause a circuit breaker to open and close without authorized permission and this can lead to accidental blackout in the region covered by the substation. The scorekeeper value will be changed to 1 if the modification on GOOSE control data occurred.

5.3. Priority Assigning Level

The priority level is assigned based on the scorekeeper violation indicator in the Format and Pattern Checker. The level for the new trust system for GOOSE can be divided into three levels. Level '0' represents a GOOSE message that never contains any kind of threat at all, level '-1' is for an attack that can affect the GOOSE communication performance based on time or the GOOSE messages is out of sequence, and level '-2' is point id for an attack that can manipulate the control data value inside the GOOSE message and can cause severe catastrophe. Table 4 below shows which violation will be assigned which priority level to determine the action that will be taken in the suspicious event handler (SEH) component.\

Table 4. Priority Levels

Level	Degree	Content
0	High Trust	This level indication is for good GOOSE packet with no violation have been detected and passed all of the scorekeeper.
-1	Low Trust (Suspicious)	This level is for GOOSE packet that have stNum and sqNum violated, or time violation or both. This can be track by identifying STSQ-SK and TM-SK score. Both need the score to be 1 or just only STSQ-SK or TM-SK.
-2	Untrusted	This level of priority is for GOOSE packet that have data violation only or "data and out of sequence stNum sqNum" or "data and time violation" or the last one is all the violation together. This determined by STSQ-SK, TM-SK and D-SK.

5.4. Suspicious Event Handler (SEH)

The SEH uses the priority level to determine whether to generate a security alert or to block the packet source. The lowest priority level is used to generate an alert while the highest priority will generate a blocking function. The action to be taken for each priority level is described below.

Level 0: Pass through the trust system.

Level -1: For this priority level the alert to an operator will be generated immediately. This level of priority will also generate an Alert Event ID (AEID) and the tracking number in this AEID will increment if the handler finds similar level of priority and similar type of violation in subsequent packets. The tracker serves as a reference point for gathering similar packets that may be part of a larger event that is going to happen.

Level -2: This last and lowest priority level allows the trust system to deny or block the source MAC address because this priority level is used as a sign that GOOSE control data manipulation attack is happening and the risk from this attack is high as it can lead to an accidental power outage.

6. Conclusion

GOOSE communication inside a substation network is vulnerable to attack as demonstrated by security researchers. The attacks are performed by exploiting the content of fields in the GOOSE message to cause an unauthorized event in the substation. The trust system proposed by [3] is for the SCADA network between regional utility intranet and it will provide a security mechanism that complies with the strict real-time operation requirements for the SCADA network. This paper proposed a trust system to be implemented for securing IEC 61850 GOOSE communication. This trust system for GOOSE communication will provide all in one security features such as firewall and intrusion detection system and give more comprehensive security protection for GOOSE communication.

References

[1] A. Elgargouri, R. Virrankoski, and M Elmusrati, "IEC 61850 Based Smart Grid Security", 2015 IEEE International Conference on Industrial Technology (ICIT), Seville, Spain, **(2015)** March 17-19.

[2] F. Hohlbaum, M. Braendle, and F. Alvarez, "Cyber Security Practical considerations for implementing IEC 62351", PACWorld 2010, **(2010)**.

[3] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure", 2012 IEEE Globecom Workshops (GC Wkshps), Anaheim, California, United States of America, **(2012)** December 3-7.

[4] J. Hong, C.-C. Liu, and M. Govindarasu, “Integrated Anomaly Detection for cyber security of the substations”, 2014 IEEE PES General Meeting | Conference & Exposition, National Harbor, MD, **(2014)** July 27-31.

[5] J. Hong, C.-C. Liu, and M. Govindarasu, “Detection of Cyber Intrusions using Network-based Multicast Messages for Substation Automation”, 2014 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, United States of America, **(2014)** February 19-22.

[6] N. Kush, E. Ahmed, M. Branagan, and E. Foo, “Posisoned GOOSE: Exploiting the GOOSE Protocol”, AISC ’14 Proceedings of the Twelfth Australasian Information Security Conference, Auckland, New Zealand, **(2014)** January 20-23.

[7] G. M. Coates, K. M. Hopkinson, S. R. Graham, and S. H. Kurkowski, “Collaborative, trust-based security mechanisms for a regional utility intranet”, Power & Energy Society General Meeting, 2009. PES ’09. IEEE, Calgary, Alberta, Canada, **(2009)** July 26-30.

[8] G. M. Coates, K. M. Hopkinson, S. R. Graham, and S. H. Kurkowski, “A Trust System Architecture for SCADA Network Security”, IEEE Transactions on Power Delivery., vol. 25, no. 1, **(2009)**, pp. 158-169.

[9] C. Fernandes, S. Borkar, and J. Gohil, “Testing of GOOSE Protocol of IEC61850 Standard in Protection IED”, International Journal of Computer Applications., vol. 93, no. 16, **(2014)**, pp. 30-35.

[10] M. T. A. Rashid, S. Yussof, Y. Yusoff, and R. Ismail, “A Review of Security Attacks on IEC61850 Substation Automation System Network”, 2014 International Conference on Information Technology and Multimedia (ICIMU), Putrajaya, Malaysia, **(2014)** November 18-20.

[11] F. Cleveland, “IEC TC57 Security Standards for the Power System’s Information Infrastructure – Beyond Simple Encryption”, 2005/2006 IEEE PES Transmission and Distribution Conference and Exhibition, Dallas, Texas, United States of America, **(2006)** May 21-24.

[12] R. Tawde, A. Nivangune, and M. Sankhe, “Cyber Security in Smart Grid SCADA Automation Systems”, 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, **(2015)** March 19-20.

[13] H. Falk, “Securing IEC 61850”, 2008 IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, Pennsylvania, United States of America, **(2008)** July 20-24.

[14] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J.-C. Tan, “An Intrusion Detection System for IEC61850 Automated Substation”, IEEE Transaction on Power Delivery., vol. 25, no. 4, **(2010),** pp. 2376-2383.

[15] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J.-C. Tan, “Security Analysis and Auditing of IEC61850-Based Automated Substations”, IEEE Transaction on Power Delivery., vol. 25, no. 4, **(2010),** pp. 2346-2355.

[16] S. Fries, H. J. Hof, T. Dufaure, and M. G. Seewald, “Security for the Smart Grid – Enhancing IEC 62351 to Improve Security in Energy Automation Control”, International Journal on Advances in Security., vol. 3, no. 3 & 4, **(2010).**

[17] Y. Wang, D. Ruan, D. Gu, J. Gao, D. Liu, J. Xu, F. Chen, F. Dai, and J. Yang, “Analysis of Smart Grid Security Standards”, IEEE International Conference on Computer Science and Automation Engineering (CSAE), Shanghai, China, **(2011)** June 10-12.

[18] X. Lu, W. Wang, and J. Ma, “Authentication and Integrity in the Smart Grid: An Empirical Study in Substation Automation Systems”, International Journal of Distributed Sensor Networks., vol. 2012, **(2012).**

[19] M. Goraj, J. Gill, and S. Mann, “Recent Development in Standards and Industry Solutions for Cyber Security and Secure Remote Access to Electrical Substations”, 11th International Conference on Developments in Power Systems Protection, Birmingham, UK, **(2012)** April 23-26.

[20] W. Wang, and Z. Lu, “Cyber security in the Smart Grid: Survey and Challenges”, Computer Networks., vol. 57, no. 5, **(2013),** pp. 1344-1371.

Authors

Muhammad Talha, he is a postgraduate student pursuing Master of Information Technology, Universiti Tenaga Nasional, Malaysia. He received his Bachelor of Computer Science degree in System and Networking from Universiti Tenaga Nasional, Malaysia, in 2013. He has experience in working as a research assistant at the Univerisit Tenaga Nasional for two years and currently in this year working as a system developer for Zetro Services Sdn. Bhd. His research interests include network security, IT security and security for critical infrastructure.

Salman Yussof, he is an Associate Professor at the College of Information Technology, Universiti Tenaga Nasional, Malaysia. He received his Bachelor of Science degree and Masters of Science degree in Electrical and Computer Engineering from Carnegie Mellon University, USA, in 1999. In the same year, he was accepted as a faculty member at the College of Information Technology, Universiti Tenaga Nasional. While working as a faculty member, he pursued his PhD study in the same university and eventually received his PhD in 2010. His research interests include next generation Internet technologies, network security and security for critical infrastructure. He is a member of IEEE.

Yunus Yusoff, he is a Principal Lecturer at College of Information Technology, Universiti Tenaga Nasional, Malaysia. He received his Bachelor and Masters degrees from Pacific Lutheran University, Washington, USA. He received his PhD from Unviersiti Tenaga Nasional. He has more than 10 years of working experience in the industry (focusing in IT security in financial institution), prior to joining the education sector. His research interests include computer forensics, IT security policy & management and IT disaster recovery.