Security of Process Bus in Digital Substation

by

Ramya Karnati

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science
(Computer and Information Science)
in the University of Michigan-Dearborn
2020

Master's Thesis Committee:

Assistant Professor Junho Hong, Co-Chair
Associate Professor David Yoon, Co-Chair
Assistant Professor Jaerock Kwon

Acknowledgements

To begin I would like to acknowledge my parents, for their love and support throughout my life. They have always made me priority and encouraged me to put forth my best effort in whatever endeavor I pursue. My parents take great pride in my education and career achievements, so I would like to dedicate this work to them. Next I would like to acknowledge the guidance that Dr. Junho Hong has provided throughout the thesis process. From the very beginning he has been open to my ideas and provided helpful insight for this project. He has also worked around my schedule in order to accommodate my needs. Thank you to Dr. Junho Hong for helping me throughout the entirety of this project I would like to express my gratitude to committee members Dr. David Yoon and Dr. Jareock Kwon for their insight and constructive feedback on the project. Finally, I would like to recognize the department of Computer and Information Science and Electrical and Computer Engineering for accepting me into the program and allowing me to pursue my interests in cyber security

Table of Contents

List of Figures

List of Tables

Abstract

Cyber security attacks in substations have been a issue for a very long time [1]. It is necessary to secure the communication between devices in substation automation system. Generally, Substation Automation Systems uses Intelligent Electronic devices (IED) for monitoring, control and protection of substation. In the past, single purpose and mostly hard-wire interconnected devices were safety and control devices. More and more features have been built into multi-function intelligent electronic devices (IEDs) over time. The need for contact between the devices in the scheme has increased by increasing the number of functions per unit. The lack of wide-ranging knowledge of data communication technologies, protocols, remote access and risks to cybersecurity would improve the prospects for cyber-initiated events. Enabling support for authentication and authorization, auditability and logging as well as product and system hardening are critical features for safeguarding electric power grids and power networks.

The introduction of a centralized account management system in the substation automation system is a simple solution for adding and removing users who have or are deprived of access. For utilities that have to stick to laws, this is a big advantage. The security logging mechanisms are a must in the case of intrusion prevention, finding unexpected use patterns and for safety forensics. It has to be precise, readily distributed and easily gathered [2]. Adopting new solutions for substations. These systems are following standards and trends, as of which one of them is in particular Ethernet and TCP/IP based communication protocols. The substation automation multicast messages are Generic Object Driven Substation Event (GOOSE) and Sampled Measured Value (SMV), Manufacturing Message Specification (MMS). The two recent standards published to protect the systems are IEC 61850 and IEC 62351. The mainstream development for substation automation is IEC61850. It provides an integrated solution for ensuring communication in substation automation between intelligent electronic devices (IED). On the one side, these standard mandates that GOOSE and SV messages must be used by the RSA cryptosystem to provide source authenticity.

This report provides a realistic consideration and review of the implementation in a substation automation system of a stable sampled measured value (SeSV) message. IEC Working Group 15 of Technical Committee 57 released IEC62351 on protection for IEC61850 profiles because of the lack of security features in the standard. However, the use of IEC62351 standards-based SV authentication methods is still not integrated and computational capabilities and performance are not validated and checked with commercial-grade devices. Therefore this report demonstrates the performance of SeSV allowed security feature packets transmitted between security and control devices by appending the extended IEC61850 packets to a message authentication code (MAC). A prototype implementation on a low-cost embedded commodity device has shown that with negligible time delay, the MAC-enabled SV message can completely protect the process bus communication in the digital substation.

Chapter 1: Introduction

Power substations are the critical juncture of an interconnected grid that transfer energy in long distance. Many substations are still operated with conventional monitoring and control schemes through hardwired cables and serial communication protocols [3]. The Ethernet-based communication brought many advantages, e.g., standardized system modeling and communication between different vendors. Furthermore, the use of standards based engineering brought many benefits to the power utilities. For instance, IEC61850 based engineering can (1) reduce the cost of configuration, installation, and commissioning, (2) enhance the multi-vendor interoperability, (3) increase the long-term stability, and (4) reduce the impact on the existing utility automation systems by upgrading the device capabilities through changing the communication stack in the system. This would only require to change the communication stack of the product when new revision of IEC61850 standard can become available [4]–[8].

Sampled value (SV) is a layer-2 protocol that is defined in IEC 61850-9, and it contains measurements, e.g., three-phase currents and voltages with neutral values [9], [10]. Two types of SV messages are defined in IEC 61850-9-2 LE, e.g., 80 samples per cycle for protection and 256 samples per cycle for measurement [11]. In the IEC61850 based digital substation, a merging unit (MU) is the device where SV is published, and it is also connected to circuit breakers via hardwired for control and status monitoring. Once a protective intelligent electronic device (IED) receives SV from MU, it calculates the protection functions, e.g., distance and time overcurrent protection. Then it will send a trip signal to MU for opening the circuit breaker (CB). Therefore, the digital substation has a high penetration of information and communication technology (ICT), and cyberinfrastructures have been widely deployed for monitoring, control, and operation, e.g., IEC61850 based system models and communications [12]. As a result, the number of cyber-attacks on substations is increasing, and it becomes a major threat that may cause damages to the substation [13]. Monitoring-control attacks (MCA) are highly stealthy as they are difficult to detect. Substation communication protocols are crucial for the operation. Its data integrity shall not be fabricated or modified by others [14]. However, its security features

are not included in IEC61850 standard since (1) the need for high speed performance in SV, e.g., publishing 4,800 samples per second in a 60-Hz system, (2) limited performance of the processor in IEDs and (3) cybersecurity was not a major concern when IEC61850 was published. Due to the lack of security establishment in IEC61850 standard, IEC Working Group (WG) 15 of Technical Committee (TC) 57 published IEC62351 on security for IEC61850 profiles [15]. One of the main objectives of IEC62351 standard is to develop cyber security features for SV message since the multicast scheme has potential cyber vulnerabilities, e.g., group center trust and group access control. Due to the limited processing power of IED, most encryption schemes or other security features are not applicable for the SV (it may delay the protection function). Therefore, IEC 62351-6 Ed.1 standard could be enhanced with an authentication scheme with the 1024 bit Rivest Shamir-Adleman (RSA) digital signature for SV [15].

Based on the recommendation from IEC 62351-6 Ed.1, different types of hardware and cryptography algorithms, e.g., RSA with 1024 and 512 keys, have been tested for generic object-oriented substation events (GOOSE) message; however, test results cannot meet the performance requirements using the state-of-art hardware as of 2010 [16], [17]. In order to find better performance algorithms, authors of [18] investigated the elliptic curve digital signature algorithm (ECDSA) and proved that ECDSA is faster than RSA and required lower computational power. Then IEC62351-6:2020 Ed.2 standard will be released to recommend a more realistic and better performance authentication scheme with a digital signature using the hash-based message authentication code (HMAC) or Galois message authentication code (GMAC) for SV [19]. The flexible and plug-and-play security filter with GMAC and HMAC has been proposed and tested to secure the GOOSE communication for protection and control devices in a digital substation. The authors showed that the proposed GMAC based security filter could meet the transmission time requirement of GOOSE (i.e., 3 msec) [20]. The reference [21] provides a review of IEC62351 security mechanisms for IEC61850 based messages that include GOOSE, R-GOOSE, SV, R-SV and MMS. However, it is still not common to apply the GMAC and HMAC to SV (i.e., IEC 61850-9-2LE), and need more research for a practical consideration for implementation, and also performance tests.

Practically, this report shows the implementation and performance analysis of IEC62351 Ed.2 schemes for secure SV (SeSV) by modifying the structure of the SV protocol data unit (PDU). Different MAC algorithms, e.g., HMAC and GMAC, with different sizes of private keys

are tested and validated. A hardware-in-the-loop (HIL) testbed with different hardware and software platform has been designed and implemented in a laboratory environment. The main contributions of this report are (1) implementation of different MAC algorithms as per IEC62351-6:2020 to secure SV message, (2) SV intrusion detection algorithms when the preshared key is compromised and used by attacker, (3) laboratory based SV message related cyber attacks, impact analysis, and mitigations using HIL, (4) recommendations from performance and feasibility analysis of SeSV. In the remainder of this report, Chapter 4 describes the potential cyber threats and existing vulnerabilities of the substation automation system. Chapter 5 explains the message authentication code (MAC) algorithms recommended by IEC62351-6:2020 standard. The implementation methods of cybersecurity features for SV have been proposed in Chapter 6. Chapter 6 provides the hardware-in-the-loop testbed and Chapter 7 provides test results using HIL testbed of the proposed methods and algorithms. Conclusions and recommendations for future work are given in Chapter 8.

Chapter 2: Cyber Security of Substation

2.1. Substation Automation System

The main basic element of the Substation Automation System (SAS) is Supervisory Control and Data Acquisition (SCADA). In combination with the ability to issue control commands to circuit breakers, SCADA is used to collect asset tracking data and equipment status information. Automation may also be supported by SCADA, such as automatic control logic, sequence switching, and interlocking [22]. Substation collects and sends metering information, equipment status information, to the Substation Control Room, and can also claim control commands obtained from the control room. Both security & control operations and SCADA control operations occur at the level of a substation bay. Protection operations need to be extremely efficient and have fast operating speeds. Protection operations include circuit breaker trip commands and circuit breaker reclose orders. SCADA operations are essential for normal operations, such as data retrieval, data monitoring, data flow management, and equipment control required for routine operations and maintenance. Relays are owned by Protection and Control, Remote Terminal Units (RTUs) are operated by SCADA.

A substation automation system's equipment may be organized into three categories, e.g. the station level, bay level and operation level. A user-interface framework with databases, servers, workstations, and engineering facilities is installed at the station level. At the bay level, the safety and control (P&C) IEDs and phasor measuring unit (PMU) are mounted. The sensors, CT, VT, circuit breaker (CB) and merging unit (MU) are process level equipment's. Substation automation facilities, e.g., GOOSE, SMV and MMS, use IEC 61850 related protocols. For sending tripping signals from IEDs to circuit breakers, GOOSE is used. The calculated voltage and current values sampled are transmitted from a MU to an IED. A number of devices are GPS-synchronized. For tracking, control and reporting between the user-interface framework and IEDs, the Manufacturing Message Specification (MMS) is used.

Figure 1: shows the layout of the bay level substation where Substation Bay controllers, protective relays and Phasor Measurement Units (PMUs) collect data from the switch gear in the substation in the Relay Space. The process bus is used between primary system equipment (process level) and bay level devices (such as protective relays) to communicate sampled values, equipment status and equipment controls. And then the collected data is transmitted over the station bus to the Substation control room.

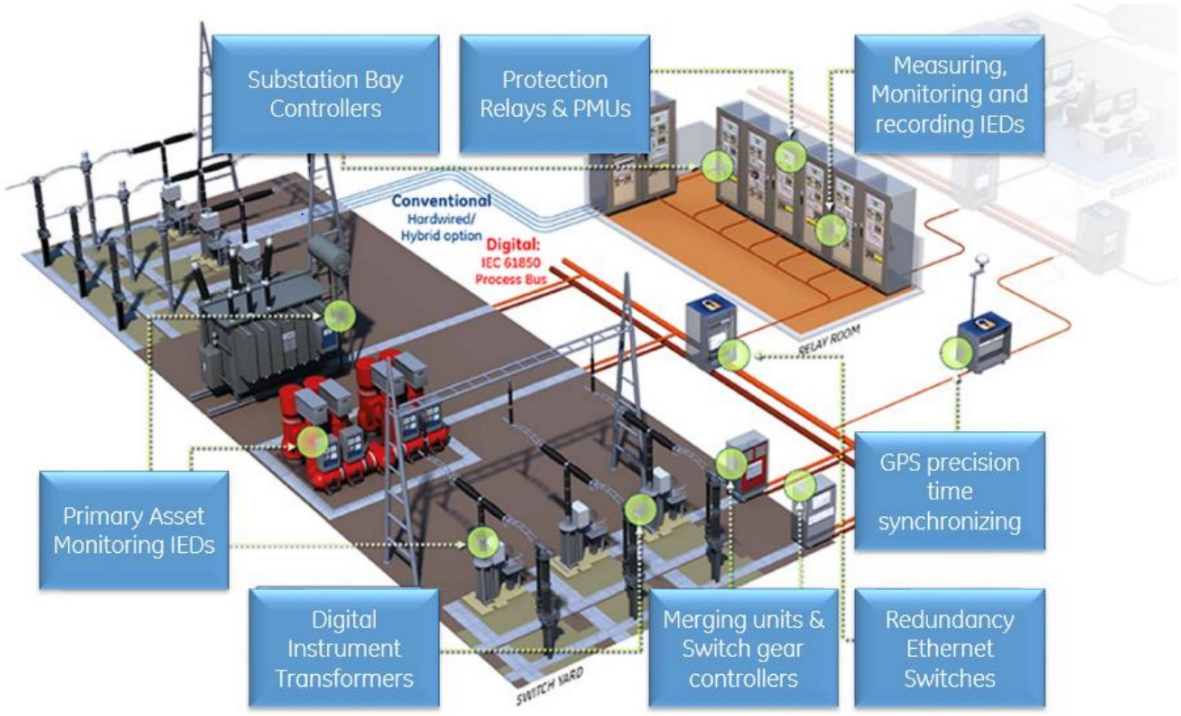

Figure 1: Substation automation bay level

Figure 2: depicts how to control and trace substation data by linking a substation control room to the relay room. All substation data is sent to the Energy Management System (EMS) or Distribution Management System (DMS), which ensures that the power system operates cost-effectively and efficiently. SCADA systems are based on communication, and hundreds of different SCADA protocols have been developed over time to allow data to be exchanged between devices. The most common protocol in use is DNP in North America. Standard models of IEC 61850 provide standard ways of representing data and standard ways of making data accessible.

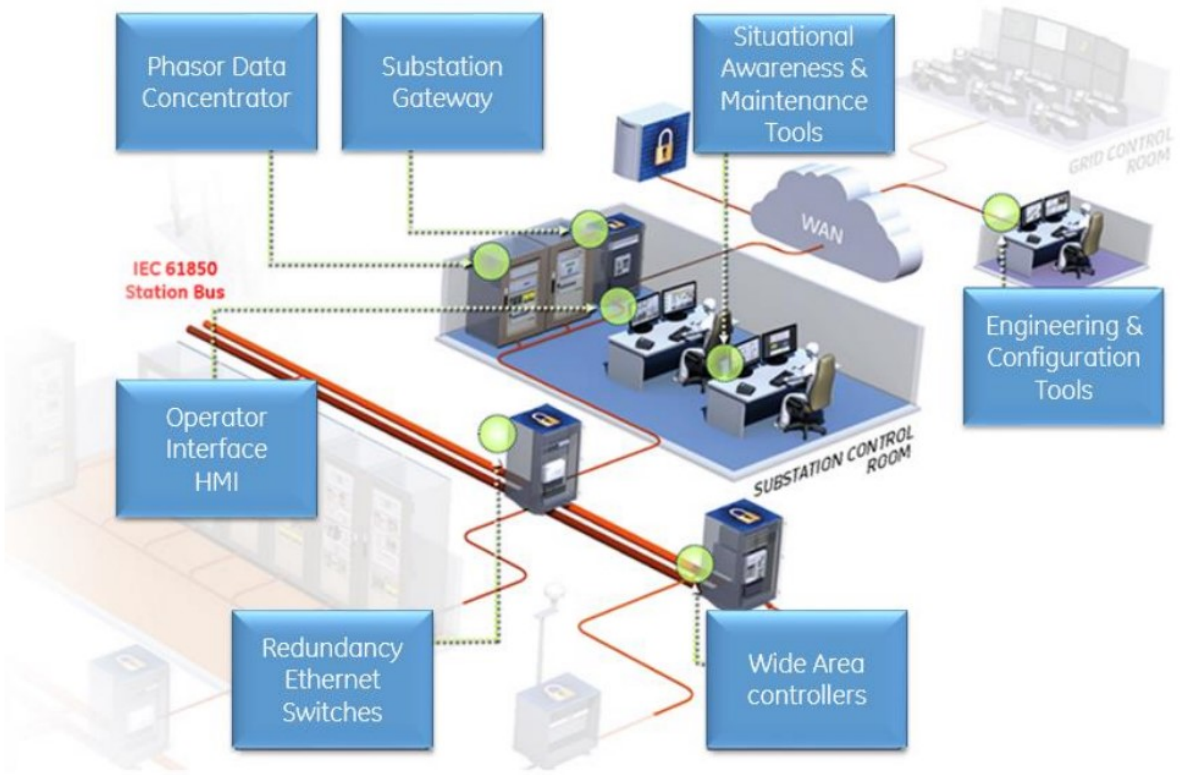

Figure 2: Substation automation station level

2.2. Substation Automation System and Vulnerabilities

IEC TC 57 has released IEC 61850 specifications for the design of the automation of electric substations. (1) interoperability, (2) simpler configuration, and (3) long-term reliability are the key objectives of substation automation standards. Interoperability helps substations to handle different vendors' intelligent electronic devices (IEDs). Data can be exchanged and general device properties retained by IEDs from various manufacturers. Using IEC 61850-based protocols, a simplified configuration modified hardwired connections (from current transformer (CT) and voltage transformer (VT) to safety relays) to Ethernet-based communication. It also greatly decreases engineering efforts and costs. ICT's changing period is much quicker than that of the functions of the power substation. Long-term reliability means that updating ICTs does not cause the entire substation system to be re-engineered. Potential cyber security vulnerabilities in the automation network of substations, as shown in Figure 3:

A1: Compromise user-interface

A2: Interrupt time synchronization

A3: Compromise station level communication bus

A4: Gain access to bay level devices

A5: Change protective device settings

A6: Capture and modify GOOSE message

A7: Compromise process level communication bus

A8: Generate fabricated analog values (SV)

A9: Compromise firewall and gain access to substation

As an effective cyber-attack can cause major damage to the power grid, it is important to protect the substation automation ICT against cyber intrusions. The A2 cyber-attack, for

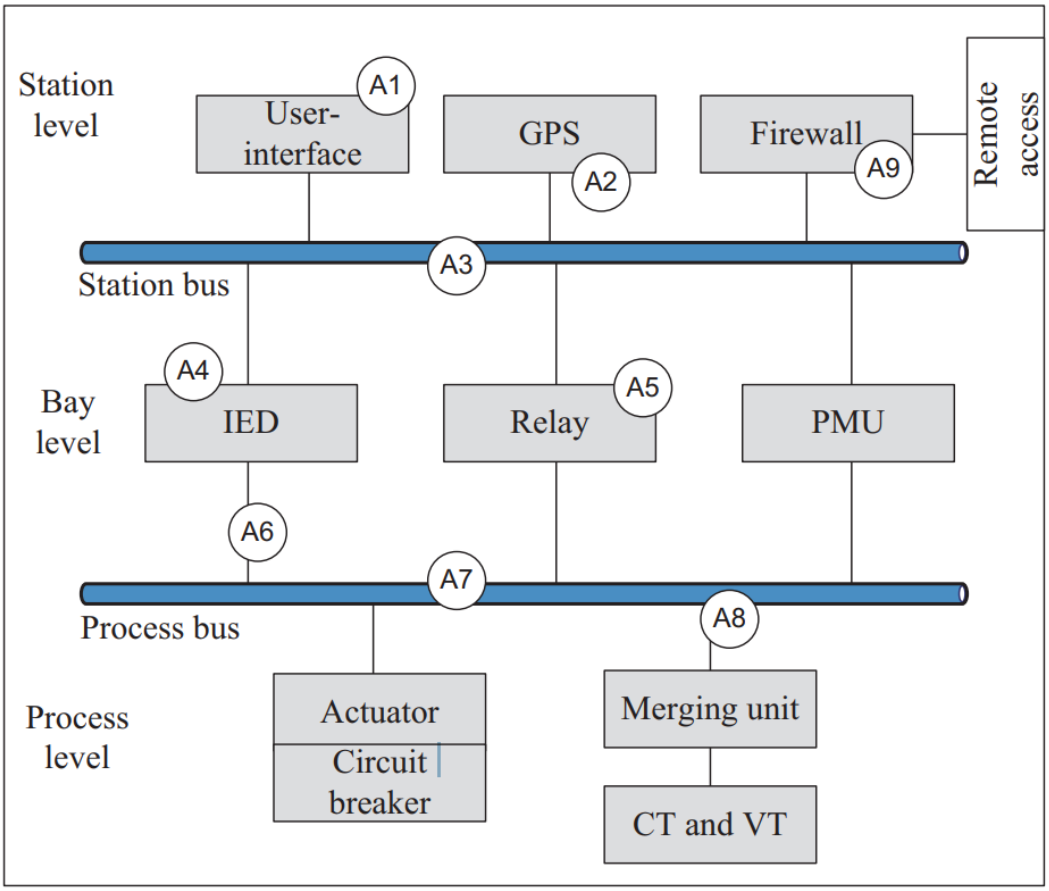

Figure 3: Potential cyber threats in a substation automation system

example, will interrupt time synchronization in the ICT network of the substation, and the operator(s) will lose the availability of communications from the substation.

2.3. Security Issues Faced in Substation Automation System

Stuxnet attack, considered to be one of the most advanced attacks to date [23]. Stuxnet's penultimate goal is to change the file system and change the system setting and status of the target devices to control field devices, taking advantage of OS and programmable logic controller (PLC) software vulnerabilities. It was possible to gain access by installing malware on the computers inside the SCADA system. Similar attack vectors (the attack vector means a route by which intruders gain access to a device in order to achieve an attack purpose, leveraging the vulnerabilities of the system) can be used to gain access to the substation based on IEC 61850 by any advanced intruders.

The GOOSE message communication system, which is one of the most important vulnerabilities in the IEC 61850 protocol, is concerned in most studies. The transmission of false GOOSE messages to Intelligent Electronic Devices (IED) controlling primary field devices may have the same impact as the Stuxnet attack. Spoofing or injection of false GOOSE messages can cause IED file system modifications or status settings to change eventually disrupting primary field device operations. With the goal of achieving Denial of Service (DoS), intruders may also flood GOOSE messages into IEDs. As long as the purpose of security monitoring is to identify and report suspicious behaviors, a monitoring system can detect such critical attacks once they take place in the system. Seven security standards for industrial control systems (ICS) were introduced by the International Society of Automation (ISA), which cover overall aspects of safety requirements and are also well suited to SCADA systems. These ISA specifications are close to traditional security requirements for the IT network, but in the SCADA/ICS system they are more specialized. Access Control, Usage Control, Data Privacy, Data Confidentiality, Limit Data Flow, Timely Event Response, and Network Resource Availability are the seven security criteria. Access control, referred to in the ISA document as identification and authentication control, means checking the identity of users (humans, software processes, devices) who request access prior to the activation of communication. The goal is to prevent selected devices or data from being illegitimately (unauthenticated) accessed. Use control means imposing an authenticated user's delegated privileges to perform the requested action on the device and controlling the privilege use. This is aimed at preventing unauthorized access to the computers or data selected. Data integrity means preventing unauthorized data exploitation, and data

confidentiality means preventing unauthorized disclosure of information in the data archive and communication networks. Limited data flow means the recognition of the necessary limitations of the information flow and hence the strictly controlled configuration of the communication paths used to deliver information. Time-to-event response means responding to a breach of security by notifying, monitoring and taking prompt corrective measures. Finally, the availability of network resources is intended to guarantee the system's availability against failure or denial of critical services. In the SCADA method, availability has the highest priority of these seven criteria, since the ultimate aim of attackers is to interrupt normal activity. Such specifications are not mutually exclusive. For example, because system availability can be triggered by false message injection or deliberate message overflow, system availability is closely related to authentication of the user (or device) and integrity of the data. The network separation strategy is directly linked to the minimal flow of data and partly linked to the regulation of access. The task of the Communication Message Protection Strategy is to verify the authenticity of the content of the messages and the valid message originators

2.4. Integration IEDs with Security Systems

Utilities must bear in mind that no industry can eradicate risk entirely when determining security strategies against current threats facing the energy sector

2.4.1. User Authentication and Authorization

All users of IEDs in the critical infrastructure need identification and authentication. At login, most of the IEDs implement local authentication. These local accounts should be created on the IED and updated to their default passwords. These accounts have to be allocated to unique roles if the IED supports role-based access. Because each IED needs to be reconfigured when accounts or passwords are changed, local authentication is difficult to handle. Central authentication allows management of identities and passwords. Role-Based Access Control (RBAC) for enterprise-wide use in power systems is specified by the IEC 62351-8 specification.

With respect to power structures, this standard defines requirements for identifying roles, task assignments and role-to-right mapping. It also offers a mandatory list of role-to-right mappings that can be used in their IED configurations by utilities. It allows utilities to check the consistency of all user accounts, user account classes, user function categories, and related privileges once every 15 calendar months. The privilege analysis is to ensure that minimum

privilege access is delegated to each user, and utilities can enforce this by exercising role-based access control. Specific system roles (operator, engineer, observer, administrator, etc. should be defined first and then group access rights to the roles and delegate users to those roles. Role-based access permissions remove the need for individual user accounts to conduct the privilege check.

2.5 Communication Protocols

A communication protocol specifies a set of rules for the sharing of data between two or more parties engaged in communication [24]. Protocols have been developed based on the particular specifications of that application to fulfill different purposes. Information on substations is collected via communication protocols, physical communication, and other technologies for substations. Protocols include DNP3, MODBUS, proprietary, IEC 61850

2.5.1 The IEC 61850 Standard

IEC 61850 is an international standard that specifies communication protocols at electrical substations for intelligent electronic devices [25]. It is part of the Technical Committee 57 reference architecture for electrical power systems of the International Electrotechnical Commission (IEC). It is possible to map the abstract data models specified in IEC 61850 to a number of protocols. MMS (Manufacturing Message Specification), GOOSE (Generic Object Oriented Substation Event), SMV (Sampled Measured Values) are the latest mappings. Using high-speed switched Ethernet, these protocols can run over TCP/IP networks or substation LANs to obtain the necessary response times below four milliseconds for protective relaying.

The Manufacturing Message Specification (MMS) is an international standard (ISO 9506) dealing with messaging systems for the transmission between networked devices or computer applications of real-time process data and supervisory control information.

Generic Object Oriented Substation Events (GOOSE) is a managed model process in which every data format (status, value) is grouped together into a data set and transmitted within 4 milliseconds of time.

Sampled Values (SV) protocol is a publisher and subscriber communication. This protocol is used in an Ethernet substation for information exchange between Merging Units and IEDs (IED-Intelligent Electronic Device).

IEC 61850 has been broken down into ten distinct parts. The first five provide detail on the principles and philosophy of the criteria. Furthermore, the other sections are divided into several sections that contain service information, data mapping, Abstract Communication Service Interface (ACSI), Substation Configuration Description Language (SCL), MMS and testing. The most important sections are parts seven and eight. Each system manufacturer, a communication network partner based on IEC 61850, has to adapt its products to the definitions and specifications set out in the standard. A client-server model follows the relationship between IEDs, but both functions may behave as such. The local Ethernet network connects with IEDs.

2.5.2. Major Benefits of IEC 61850

In converting between the communications protocols that could be used, a multi-manufacturer SAS has always faced difficulties. Thus, to include the following, a universal protocol may be used:

(1) Interoperability. Interoperability. It allows smooth multivendor system communication, easier setup, higher reliability, and more security. Other protocols can be used for SA, but none of them support interoperability between IEDs, such as IEC 61850, IEC 60870-5-101, Modbus, and Modbus plus, for example.

(2) Versatility. Flexibility. The norm supports various facilities with distinct criteria for performance.

(3) SCL Settings. According to user requirements, IEC 61850 uses Substation Configuration Terminology to define the entire substation system and each device in the network in a structured way [6]. It describes a collection of abstract data and object models for that.

(4) Lower cost for installation. By greatly lowering wiring costs, Ethernet connections based on OSI-7 are used.

2.5.3. Communication Protocols of IEC 61850

IEC 61850 uses and splits the OSI-7-layer stack into three classes for communication: Manufacturing Messaging Requirements, TCP/IP, and Sampled Value (SV) transfer. MMS is a standard that is international (ISO9506). It was chosen by IEC 61850 because it supports the complicated naming scheme and facilities of the standard. Due to its model of Virtual Manufacturing Device (VMD), it is especially chosen. Not only this but MMS also enables IEDs to operate simultaneously as clients and servers. With the VMD model, MMS describes contact

messages sent between IEDs. The VMD model describes the objects a server contains, the resources that can be used by the client, and the actions of the server when requests are sent by the client.

To include remote control communication services and smart metering, the MMS can be slightly changed. Not just that, but to support the mapping of IEC 61850 abstract objects, it can also provide the necessary complex information models. In addition, since it supports both TCP/IP and OSI communication profiles, MMS is able to provide workability.

Seven types of messages exist and they are mapped into various stacks of communication. Time-critical messages (i.e., they must be transmitted within 4 milliseconds) such as messages from GOOSE (Generic Object Oriented Substation Event) and SV messages used to transfer raw calculated data values (types 1 and 4) are mapped directly to Ethernet, minimizing overhead and thus processing time. Medium-speed messages, low-speed messages, file transfer functionality, and access control command messages (types 2, 3, and 5) are mapped to the MMS protocol running over the TCP/IP stack. Time synchronization messages (type 6) are transmitted using UDP/IP to all IEDs in a substation.

2.5.4. Security for IEC 61850

For analog measurements, IEDs used hardwired analog inputs from the instrument transformers and used hardwired digital IO as the discrete input/output channels. Many modern IEDs support voltage and current input in the digital format of Sampled Value (SV) streams transmitted as Ethernet packets on the Process Bus with the introduction of substation automation technologies, especially IEC 61850, and also support discrete control command or event input/output in the digital format of Generic Object Oriented Substation Event (GOOSE) messages transmitted The new IEC 61850 SV and GOOSE are distributed on communication buses as unencrypted Ethernet packets with a well-documented data structure in order to ensure interoperability. The IED input and output packets can be sniffed, decoded and even faked by an opponent linked to the substation buses, thereby exploiting the security and control mechanism.

2.5.5. IEC 62351 Overview

While the first sections of IEC 62351 (International Electrotechnical Commission (IEC) (2010b)) were published as early as 2007, more recent sections of IEC 62351 (International

Electrotechnical Commission (IEC) (2010b)) were published in 2010, with some sections still in progress and an estimated stabilization date of around 2015 [26]. The standard addresses information protection for control operations of power systems, and the ultimate aim is to protect the confidentiality, credibility, availability and non-repudiation characteristics of a device, primarily through the implementation of authentication mechanisms. The norm is divided into ten separate sections that cover various regions. In the following we give a brief overview of the different parts of the standard.

IEC 62351-1:

The first section provides a general overview of the standard IEC 62351, outlining the purpose of the standard as well as a brief introduction of the various chapters. It also offers general safety information, a list of security threats (both inadvertent and intentional, e.g. equipment failures, cyber hackers, etc.), as well as an overview of potential countermeasures to security. The section also briefly explains topics such as, among other items, risk assessments, key management and security processes.

IEC 62351-2:

The second part of the IEC 62351 standard explains glossary terms such as Access Control, Data Security, etc.

IEC 62351-3:

The third part of IEC 62351 discusses the protection of TCP/IP-based protocols used in the electricity delivery domain for automation systems. For TCP/IP-based protocols, it explicitly prescribes the use of Transport Layer Security (TLS) with X.509 certificates. The aim is to ensure the authenticity and integrity of the transport layer data as well as, optionally, confidentiality through the use of TLS encryption mechanisms. Threats such as man-in-the middle attacks and replay attacks are often countered with the use of TLS. This aspect of the specification also includes shared certificate authentication (i.e., client and server both have a certificate), and prescribes the algorithms to be used and certain minimum key lengths, as well as how certificate revocation can be treated.

IEC 62351-4:

Protection for profiles such as Manufacturing Message Specification (MMS) used in other IEC specifications is discussed in this section of the IEC 62351 standard. IEC 62351-4 describes how to use X.509 certificates to authenticate applications, and the standard describes

how to use TLS as a layer for safe connections between TCP and the ISO Transport Service using another TCP port. The TLS cipher suites, which must be supported, are further specified.

IEC 62351-5:

Security for protocols defines the fifth component of the IEC 62351 standard. Such protocols are message-based, and thus authentication must be performed on a per-message basis. In addition, the often restricted processing power available in the affected devices must take into account any safety mechanisms. Since keys used for authentication and/or encryption should be updated on a regular basis, this section also proposes mechanisms that allow remote updating of keys on a computer.

IEC 62351-6:

Protection for protocols specified in the related standard IEC 61850 is discussed in Part 6 of the IEC 62351 standard. The requirements described in IEC 62351-4 shall apply in respect of protocols in IEC 61850 using TCP/IP and MMS. In addition, this section proposes an extension to the IEC 61850 GOOSE and SMV PDUs (Protocol Data Unit), adding to the PDU an area containing information related to protection. The object of the extension is to authenticate a PDU by containing a signed PDU hash. This section of the specification also introduces Substation Configuration Language (SCL) extensions that allow certificate definitions to be used in the configuration.

IEC 62351-7:

The infrastructure of power systems makes heavy use of interconnected information systems for operations management. The Basic Network Management Protocol (SNMP) Part 7 of the IEC 62351 standard defines the data object models to be used that are unique to power systems, and this information system infrastructure also needs to be safely controlled.

IEC 62351-8:

The IEC 62351 specification in Part 8 specifies system-wide role-based access control for the infrastructure of power systems. It addresses various access types, such as direct and remote access, as well as human user access and device agent automated access. This section proposes three separate access token formats for transport roles, namely X.509 extension ID certificates, X.509 attribute certificates, and software certificates.

IEC 62351-9:

This section of the standard has not yet been released but is intended to address the management of the certificate and / or key.

IEC 62351-10:

The general guidelines for the security architecture of power systems are given in Part 10 of the IEC 62351 standard. This provides a summary of the security measures that can be applied to power systems, as well as guidance on system design on how to organize the power systems' communication infrastructure.

2.5.6. Assessing IEC 62351

Introduction of the security concerns This section provides the security of the power systems, an overview of the various threats to the system and the related security specifications capable of mitigating those threats. The enumeration is very complete, ranging from inadvertent threats such as natural disasters to malicious threats such as disgruntled workers, hackers and industrial espionage. The safety criteria are also very specific and are cross-referenced by the standard with the required safety countermeasures (although not all countermeasures are part of the actual standard). Activities such as risk assessments or security policies are often listed, as are the security challenges in power system operations, where availability is far more critical than confidentiality.

Chapter 3: Security of Sampled Values

3.1. Substation Automation Features

A substation automation system (SAS) consists of hardware and software platforms with control and monitor process that are connected through communication networks.
The main functional parts of SAS are as follows [27]:

- Human Machine Interface (HMI) with process database.
- Separate gateway for remote supervisory control via SCADA.
- Master clock (e.g. GPS receiver)
- Collection of the relevant data concerning the substation and distribution of the data where needed.
- Data exchange between the different system components via serial bus.
- Bay and station level devices for control, monitoring and protection.
- Bay-oriented local control panels with mimic diagram.

Control mode selection

The operation is usually performed via the local HMI as soon as the operator receives operation access at bay level. The local HMI is directed during normal operation and enables all switching devices to operate safely through the bay control IED.
Local mode

The item must first be chosen for the HMI. The selection will not be possible in the event of blocking or interlocking conditions and an appropriate alarm announcement will take place. If a selection is true, the location indicator indicates the possible direction and presses the appropriate ON or OFF button to close or open the corresponding object. Operation control from other locations (e.g. REMOTE) in this operating mode is not feasible. REMOTE MODE A higher level (station level) is provided to the control authority in this mode and the installation can only be controlled remotely. In this operating mode, monitoring of the process from the lower levels is not possible.

Emergency mode

The location indication shall be made directly from the circuit breaker of the primary equipment. In order to close or open the circuit breaker, the selection push button and either the ON or OFF push button must be pushed simultaneously on the imitation board. Service control from other locations (e.g., from REMOTE) in this operating mode is not feasible.

SCADA

SCADA (Supervisory Control and Data Acquisition) is a remote monitoring and control system that operates through communication channels with coded signals (usually using one 'communication channel per remote station'). Through adding the use of coded signals over communication channels, the control system can be combined with a data acquisition system to collect information about the status of the remote equipment for display or recording functions. It is a form of system of industrial control (ICS). Computer-based systems that monitor and control industrial processes that occur in the real world are industrial control systems.

Historically, SCADA systems differentiate themselves by being large-scale processes that can require several substations and large distances from other ICS systems. Popular Components of a Device

A SCADA system has the following subsystems:

- Remote Terminal Unit (RTU)
- Telemetry system
- Data Acquisition Server
- Human Machine Interface
- A supervisory system, gathering data on the process and sending commands to the SCADA system.
- Communication infrastructure connecting the supervisory system to the remote terminal units

IED (Intelligent Electronics Devices)

An Intelligent Electronic Device (IED) is a concept used in the electrical power field to describe power system equipment microprocessor-based controllers, such as circuit breakers, transformers, and capacitor banks. IEDs collect data from sensors and power equipment, and if they detect voltage, current, or frequency disturbances, or raise/lower voltage levels in order to maintain the desired level, they may issue control commands, such as tripping circuit breakers.

Popular IED types include protective relaying devices, controls for On Load Tap Changer, circuit breaker controllers, switches for capacitor banks, recloser controllers, voltage regulators, etc.

An IED refers microprocessor equipped device that can perform a dynamic range of functions that include analog/digital conversion, protection scheme, and reporting system status. MU IED converts analog currents and voltages signal to digital, and then sends sampled digital information to protection and control (P&C) IED using SV message.

3.2. SMV (Sampled Measured Values)

SMV is a technique used to transfer measured samples between IED devices from sensor systems, such as CTs, VTs or digital I/O sharing. The lower layers of the ISO/OSI model use Ethernet multicast functionality and serial line unicast communication. The OSI reference model defines the definition of each communication layer, networking profiles, application (A-Profile) and transport profiles in detail (T-Profile). A-Profile is the collection of requirements and agreements dealing with the first three model layers of the ISO guide. The remaining four layers are in T-Profile shape. In accordance with the IEC 61850 standard, facilities are mapped into four separate combinations of A-Profile and T-Profile:

- Client/server model
- GOOSE/GSE control
- GSSE services
- Time synchronization

SV message provides a multicast mechanism for communicating data between one or more IEDs over an Ethernet network. In this case, MU IED becomes a publisher and P&C IEDs will be subscribers. The layer 2 (data link) of the OSI model is used to map SV message data, and the payload datagram is shown in Figure 4. The SV packet frame has the following fields:

1) Destination address: The first three octets are assigned by IEEE with 01-0C-CD whereas the fourth octet will be 04 for multicast sampled values.

2) Source address: The address of the publisher.

3) VLAN priority tag: Priority tagging according to IEEE 802.1Q.

4) Ethertype: SV Ethertype is set to 88-BA.

5) APPID: Application identifier.

6) Length: The total number of bytes in the SV message.

7) Reserved 1: Reserved for future standardization.

8) Reserved 2: Reserved for future standardization.

9) APDU: Application protocol data unit (APDU) that contains SV data structure.

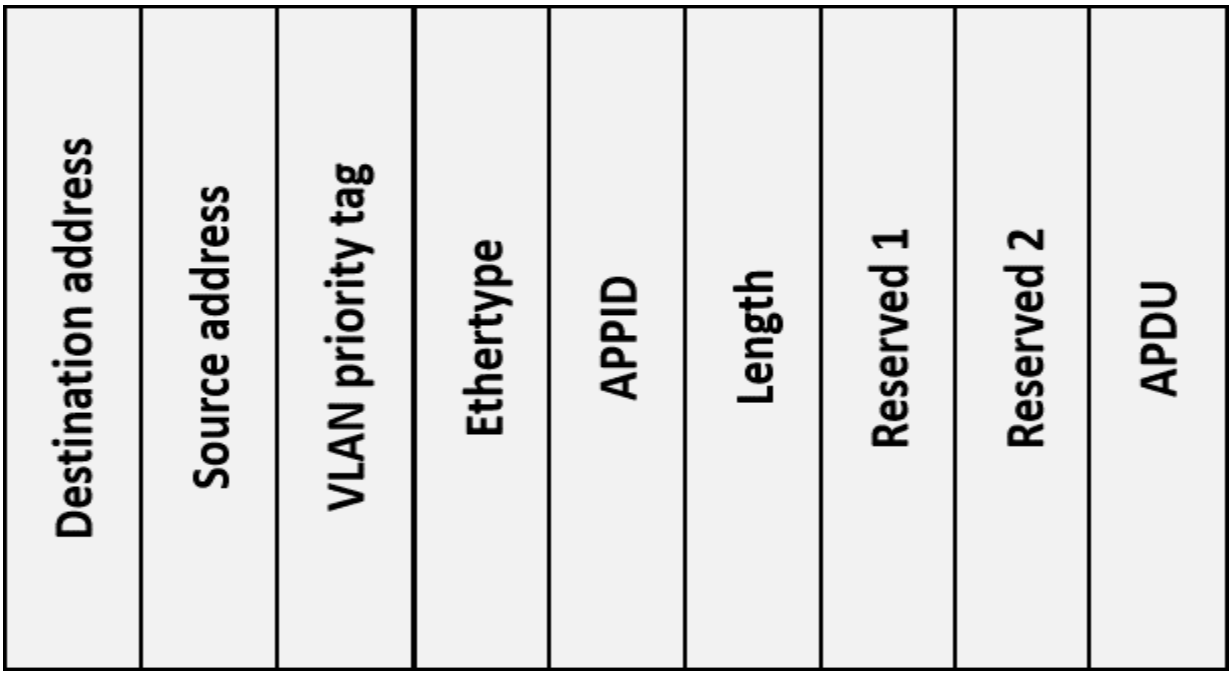

Figure 4: SV packet frame

The SV buffer is encoded as the APDU that contains information to be distributed in the process bus network, as described in Figure 5. The APDU of SV packet has the following fields:

1) svID: Should be a system-wide unique identification.

2) smpCnt: This will be incremented each time a new sampling value is taken. The counter shall be set to zero if the sampling is synchronised by clock signal and the synchronising signal occurs.

3) ConfRef: Value from the MSVCB.

4) RefrTm: Contains the refresh time of the SV buffer.

5) smpSynch: Synchronised by an external clock signal.

6) seqData: List of data values related to the data set definition.

Subscriber of protective IED receives this SV packet and decode the necessary information. For instance, smpCnt is used for the synchronization between multiple SV streams.

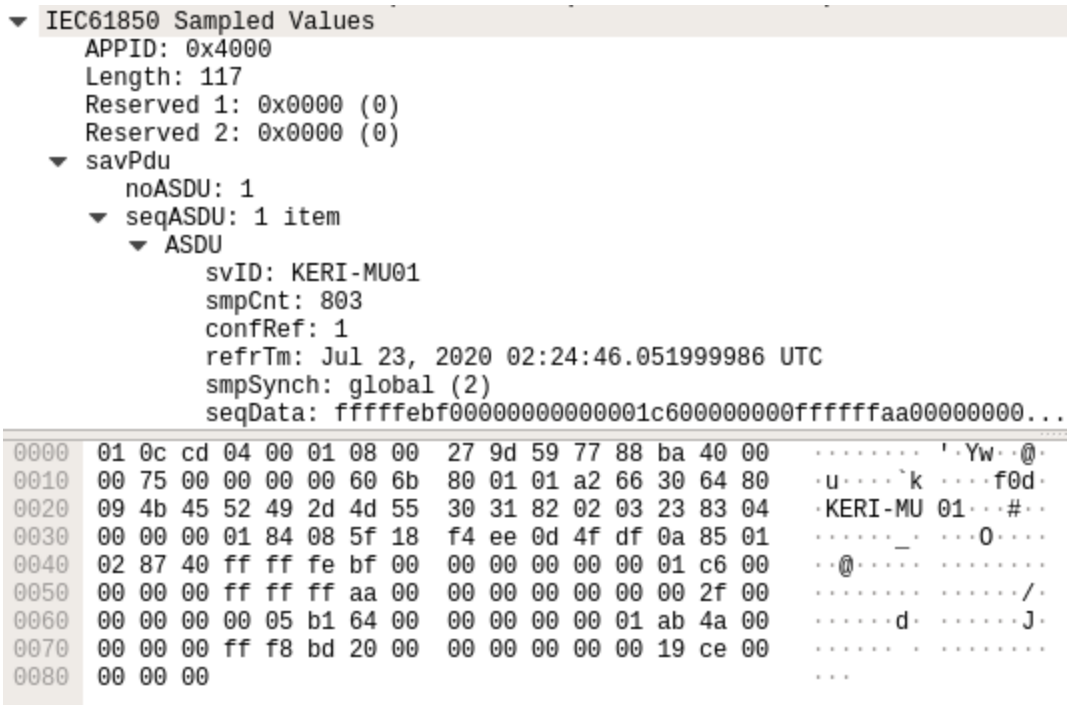

Figure 5: APDU of SV packet (no security features)

3.3. Potential Threats and Vulnerabilities

Typically, most of the high voltage substations are un-manned due to the nature of the power transmission system (located in wide-spread and remote sites). Furthermore, sub stations communicate with a control center (for monitor and control) through gateways and wide area networks, so they are not isolated. Therefore, remote access functionality that operators or engineers can have access to the substations is crucial [28]. The main problem of the remote access point is that remote access points may not be installed with adequate security features, e.g., misconfigured firewall, weak combination of password and its policy. Successful electronic intrusion to substation can be initiated in multiple ways, e.g., malware infection and gaining credential of remote access. An adversary may infect the laptop who has access to the substation communication network or gain remote login credentials using social engineering [29]. When attackers gain access, they could compromise either or both the station equipment (P&C relays, remote terminal units or user-interfaces) or communication protocols; One could gain access to the process bus network once the bay-level equipment is compromised.

Due to the characteristics of the SV protocol, such as, plain text message and multicast at the data link layer, it exposes all data information in the communication network. If someone or

device has access to the process bus, they can analyze the semantics of the SV message. Then they can find useful information that can be used for future cyber attacks. For instance, SV contains three-phase currents and voltages value. Modification of current measurements to 20 times the original value may trigger the protection scheme at the P&C IEDs. Another way to compromise the SV message and disrupt the regular operation of the substation system is to exploit the vulnerabilities of the processing process of the subscriber. More details will be discussed in the next Section.

3.4. Attacks upon Sampled Values

(1) Replay Attack: A replay attack can be initiated by playing back older SV packets that contain fault currents and voltages, which are critical information to pass on. In order to achieve the replay attack, attackers need to gain access to the monitoring port of process bus Ethernet switch, and capture the critical status of SV messages. The expected impact of a successful attack is to open the circuit breakers by triggering the protection functions of the SV subscriber (P&C IED).

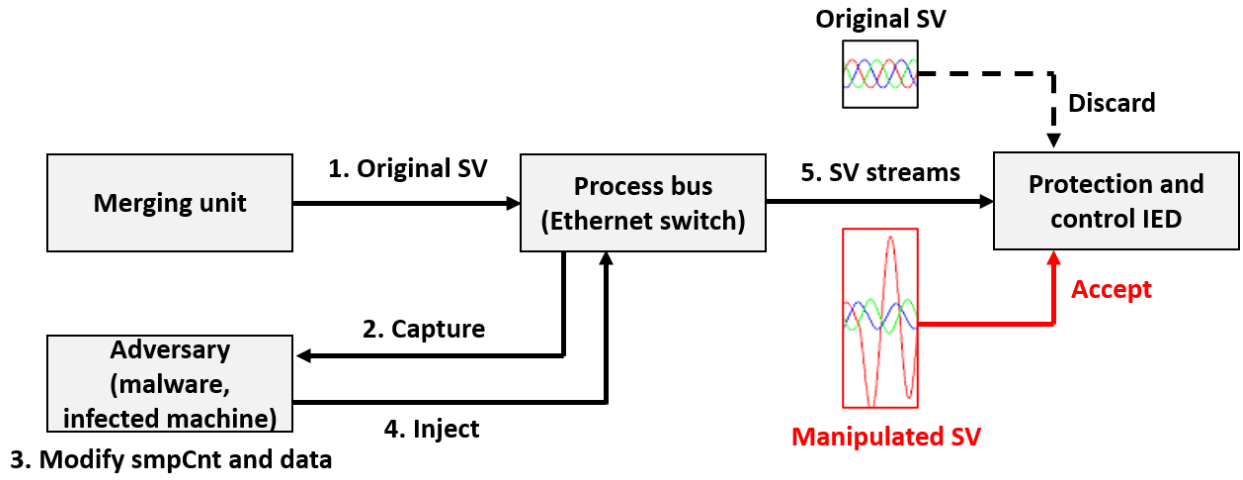

Figure 6: An example of spoofing attacks for SV messages

(2) Spoofing with a False Data Injection: The main objective of spoofing false SV data injection attacks is to capture, modify, and inject the original message with abnormal information [30]. After capture the original SV message, an adversary can manipulate the smpCnt and seqData. So the SV subscriber (P&C IED) will discard the original SV but subscribe to the compromised SV messages as illustrated in Figure 6. By modification of time synchronization information smpCnt and measurements seqData as shown in Table 1, the adversary can manipulate the normal

operation of SV subscribers. The increased smpCnt of manipulated SV packet will be accepted by the SV subscriber first, and then the lower number of smpCnt contained original SV packet will be dropped by SV subscriber. This is because SV subscriber programmed to receive the latest smpCnt contained SV packets for the synchronization. The injected increased I_1 and decreased V_1 data will trigger the protection function of P&C IED, and attackers can open the connected circuit breakers as described in Table 1.

(3) Flooding Attack: Availability is one of the keys to the normal operation in a substation. When a fault happened at the transmission line, if the fault current and voltage information cannot be reached to the P&C IED, backup protection will be initiated with unwanted outage areas. Attackers could identify the semantics of original SV messages in the process bus network. Then they can reproduce the lots of SV messages with the maximum size of Ethernet packets. This attack will disrupt the normal SV subscriber function of P&C IEDs, and they cannot process the protection functions due to the limited computational power.

(4) High smpCnt Attack: If SV subscriber continuously receives the highest number of smpCnt contained SV message, they will drop all other normal SV packets. By this cyber-attack, the adversary could disrupt the normal SV processing operation in the substation. This will disrupt the normal monitoring on the measurement function of SV subscribers.

Table 1: Parameters of original and SV packets

Parameter	Original SV	Manipulated SV
smpCnt	N	N+10
ConfRef	1	1
RefrTm	7/18/2020 13:12	7/18/2020 13:12
smpSynch	2	2
seqData	$I_1, I_2, I_3, V_1, V_2, V_3$	I_1 x $20, I_2, I_3, V_1/20, V_2, V_3$

Chapter 4: Message Authentication Code

In the world of open computing and communications, having a way to verify the integrity of data transmitted over or stored in an insecure medium is a prime necessity. Usually, "message authentication codes" are mechanisms that include such integrity checks based on a secret key (MAC). In order to verify information exchanged between these parties, message authentication codes are usually used between two parties that share a secret key.

A message authentication code (MAC) is known as a signed security tag, and it is used to authenticate a plaintext communication message. The MAC can be generated from the original message, and it contains a short length of security information for confirming the integrity of the transferred message from the sender [31]. Therefore, the receiver can identify whether the message is not manipulated by the adversary. Typically both the sender and the receiver should possess a shared secret key to detect any changes to the original message content. However, generating MAC from the message context will require computational power and time, and this is a crucial problem for the real-time operation of the substation automation system. For instance, power system protection applications (e.g., distance and overcurrent protection functions) in P&C IEDs need to receive 4,800 SV packets per second in the 60-Hz power system (i.e., 0.208 [msec] packet interval as shown in Table 2), and SV has to arrive within 3 [msec] as defined in IEC61850 [32]. Hence, SV message needs to have a higher priority than other input data, and encryption algorithms are not recommended due to the increased computational time and limited processing resources of the IEDs. In other words, the MAC should be calculated and encoded within appropriate time windows at the sender, and the receiver should decode and compare the MACs faster than the time interval between packets.

4.1. Galois Message Authentication Code (GMAC)

Galois/Counter Mode (GCM) has been widely adopted because of its efficiency and performance. It has a combined structure from CTR (refer as a counter) mode and message

authentication code. GCM uses GHASH function for the message authentication code. Due to its fast throughput rate, it has known for the appropriate cryptography method that can be used for the high speed communication channels with low-cost commodity hardware. GCM can be used for only generating authentication code by ignoring the encryption process using CTR mode. So GMAC is an authentication-only variant of the GCM. Any length of initialization vectors can be

Table 2: SV message sending profile

	Protection	Measurement
Sample/cycle	80	256
Samples/package	1	8
Package/cycle	4,000(50 Hz)	1,600 (50 Hz)
	4,800(60 Hz)	1.920 (60 Hz)
Time interval between packets	250 µsec (50 Hz)	625 µsec (50 Hz)
	208 µsec (60 Hz)	520 µsec (60 Hz)

used and accepted by GMAC. GMAC can support parallel processing, so the speed of encoding and decoding could be faster than other algorithms.

Blocks are numbered sequentially, as in usual counter mode, and then this block number is combined with an initialization vector (IV) and encrypted with a block cipher E, usually AES. To generate the ciphertext, the product of this encryption is then XORed with the plaintext. This is basically a stream cipher, like all counter modes, and so it is important that each stream that is encrypted uses a different IV [33].

4.2. Hash Message Authentication Code (HMAC)

HMAC is based on hash functions and it can guarantee the integrity and authentication of the message. It is a hash-based cryptography function, and any cryptographic hash function could be used in the calculation of an HMAC. The advantages of HMAC could be (1) short and fixed length of the tag, (2) avoiding the duplication, and (3) hide the original message. Due to the characteristics of collision resistance and one-way function, calculating the same inputs from the generated HMAC tags is almost impossible. For the estimation and checking of the message

authentication values, HMAC often uses a hidden key [34]. The primary objectives behind this construction are

* To use usable hash functions, without modifications. Hash features that work well in software, in particular, and for which code is freely and widely accessible.
* To retain the original hash function output without incurring major degradation.
* In an easy way to use and handle keys.
* Based on rational assumptions on the underlying hash function, to provide a well understood cryptographic study of the strength of the authentication mechanism.
* To allow the underlying hash function to be quickly substituted in the event that faster or safer hash functions are identified or needed.

Chapter 5: SV with MAC

This report developed and implemented GMAC and HMAC PDU extensions to original SV packets. In order to integrate MAC algorithms, new cybersecurity functions, i.e., secure SV (SeSV), are introduced in the existing open-source code library [35]. It secures SV message communication by applying the MAC algorithms with preshared keys between publishers and subscribers. Note that the key distribution algorithms and methods for MAC, e.g., Group Domain of Interpretation (GDOI), will be discussed in future research. The SeSV functions are written in C language and combined with OpenSSL library. Figure 7: describes the implemented extended SV PDU that contains authentication value for cybersecurity. The reserved 1 and 2 fields need to be calculated. Reserved 1 refers to the length of the extension. Reserved 2 indicates the 16-bit CRC that is computed using the first 8 bytes of the SV PDU. The authentication value frame has the following fields:

1) Version: Extension protocol version number.
2) Time of current key: Time information of the current key.
3) Time of next key: Indication of the number of minutes
prior to the new key being placed into service. A negative value is reserved to indicate that no new key has been scheduled to be placed into service.
4) Initialization vector: An initialization value for the MAC or encryption algorithm.
5) Key ID: Assigned by the key distribution center (KDC) as a reference.
6) MAC value: The calculated MAC value for the authentication/integrity of the messages.

Both additional features in extended PDU and the authentication values are considered to generate the SeSV frame. The following Section shows more details of generating MAC during the communication process in the digital substation environment

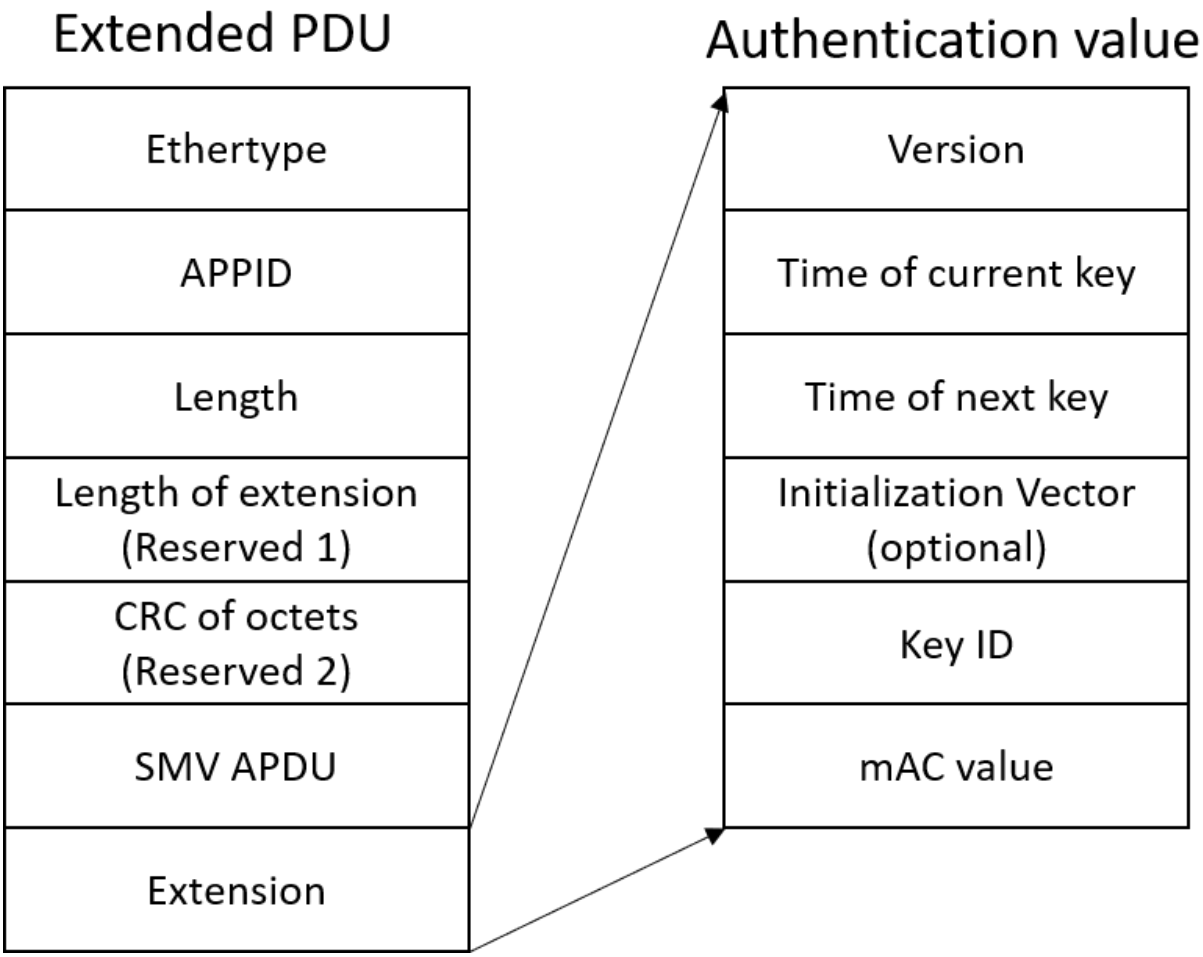

Figure 7: Extended PDU for SV.

5.1. MAC for Publisher and Subscriber

In order to secure the SV messages from the merging unit (publisher) to the P&C IED (subscriber), MAC algorithms (GMAC and HMAC) are applied. The overall authentication process of the proposed MAC scheme is shown in Fig. 8. Table 3 describes more details of the proposed SeSV. The SeSV engine generates original SV PDU, SV_{ori}^{t} using three phase currents $I_{a,b,c}^{t}$, voltages $V_{a,b,c}^{t}$ and time information (Time). The publisher and subscriber share the same shared symmetric key, Key(K). The publisher will generate an extension field SV text1 using MAC algorithms together with the key and the original SV PDU. Then the extension is appended to the original SV PDU, and the SeSV SV_{SeSV}^{t} will be published into the process bus network.

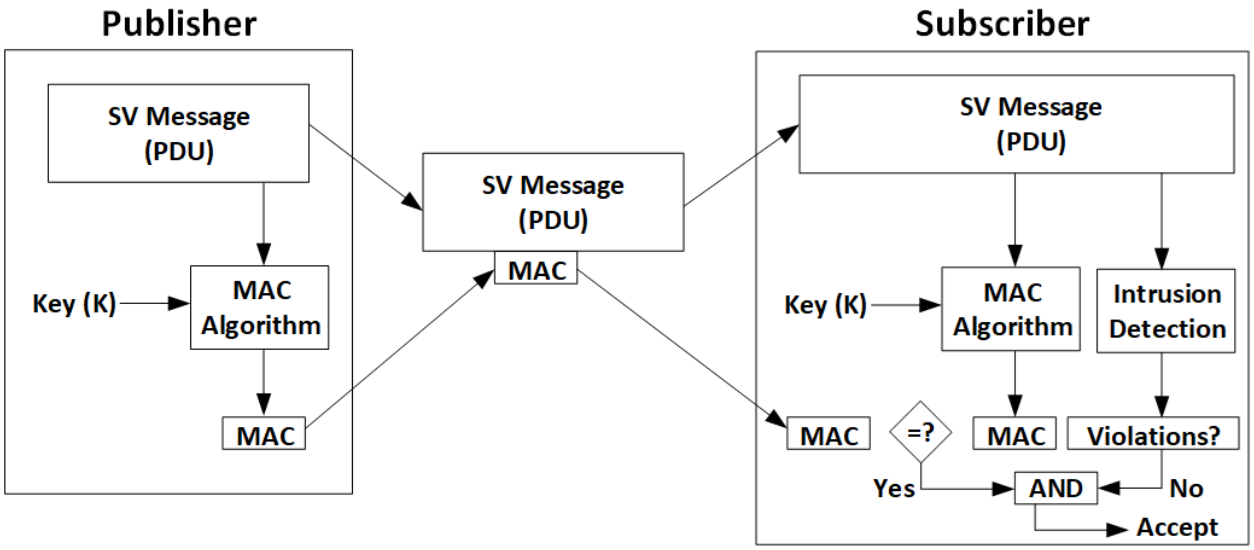

Figure 8: Proposed SeSV MAC integration for publisher and subscriber

Once the subscriber receives the packet with the MAC tag, it will calculate the MAC tag again using the pre-shared symmetric key, Key(K). If the calculated MAC tag and delivered MAC tag are matched, the delivered SeSV message is verified and checked the integrity of the SV message. More details are illustrated in Table 4 Once the subscriber captures all incoming packets , $C^{t}_{pkt,p}$ in the process bus, it will filter the SeSV packets. Then the parsed SeSV data is saved in the security buffer. New MAC SV^{t}_{ext2} is calculated from the delivered SeSV using the same key. If they match, the subscribed SeSV will be processed for the next "AND" logic as shown in Figure 8. If attackers gain access or finish the reverse engineering to get the symmetric key, they can execute the cyberattacks that mentioned in Chapter 3. In order to check such an attack, the intrusion detection module has been proposed for the SV subscriber. The semantics of SV messages can be used to check abnormal behaviors of SeSV. Step 4 detects a lost SV packet or replay attack by checking the SV counter number (SmpCnt, SV^{t}_{cnt}). SmpCnt will be incremented each time SV is published and will be reset to zero every second via pulse per second (PPS) signal. If attackers have the same symmetric key, they can generate the abnormal SV packet. This cannot be detected by the MAC algorithm since the delivered and calculated MAC will be the same. However, the injection of fabricated SV packets can be detected by Step 4-(b). This method will monitor the SV destination MAC address SV^{t}_{dst}, svID SV^{t}_{sid}, and APPID SV^{t}_{aid} on every packet. For instance, if more than N numbers of identical SV packets have

the same SV counter number SV_{cnt}^{t} within short range of time window, this will not be an error but a SV injecting attack. Step 4-(c) shows SmpCnt SV_{cnt}^{t} violation.

Table 3: Algorithm for Publisher

SeSV_Publisher (SV PDU)
Step 1: Generate SV PDU without security,
$SV_{ori}^{t} \leftarrow [V_{a,b,c}^{t}, I_{a,b,c}^{t}, \text{Time}]$
Step 2: Generate extension field,
$SV_{ext1}^{t} \leftarrow \text{MAC}[\text{Key (K)}, SV_{ori}^{t}]$
Step 3: Appending the extension to the original SV PDU,
$SV_{SeSV}^{t} \leftarrow [SV_{ori}^{t}, SV_{ext1}^{t}]$
Step 4: Publish to the process bus

Table 4: Algorithm for Subscriber

SeSV_Subscriber (SV PDU)
Step1: Capture and filter the SeSV packet, $C_{pkt,p}^{t}[SV_{SeSV}^{t}]$
Step2: Generated extension field using the delivered SeSV,
$SV_{ext2}^{t} \leftarrow \text{MAC}[\text{Key (K)}, SV_{SeSV}^{t}[SV_{ori}^{t}, SV_{ext1}^{t}]]$
Step3: Compare SV_{ext1}^{t} and SV_{ext2}^{t}
a. If $SV_{ext1}^{t} = SV_{ext2}^{t}$, go to step 4
b. If $SV_{ext1}^{t} \neq SV_{ext2}^{t}$, go to step 7
Step4: Check the semantics of each SV message as follows
a. If $SV_{cnt}^{t}+1 = SV_{cnt}^{t+1}$
b. If $N_{same}^{sv,T}$ > N number of same packets,
$[SV_{dst}^{t}, SV_{aid}^{t}, SV_{cnt}^{t}] = [SV_{dst}^{t+1}, SV_{aid}^{t+1}, SV_{cnt}^{t+1}]$
c. $SV_{cnt}^{t}+N < SV_{cnt}^{t}$
Step5: If [3(b) OR 4(a,b,c)] = true, go to Step7 otherwise go to Step6
Step6: Accept the SeSV packet
Step7: Drop the SeSV packet and issue an alarm

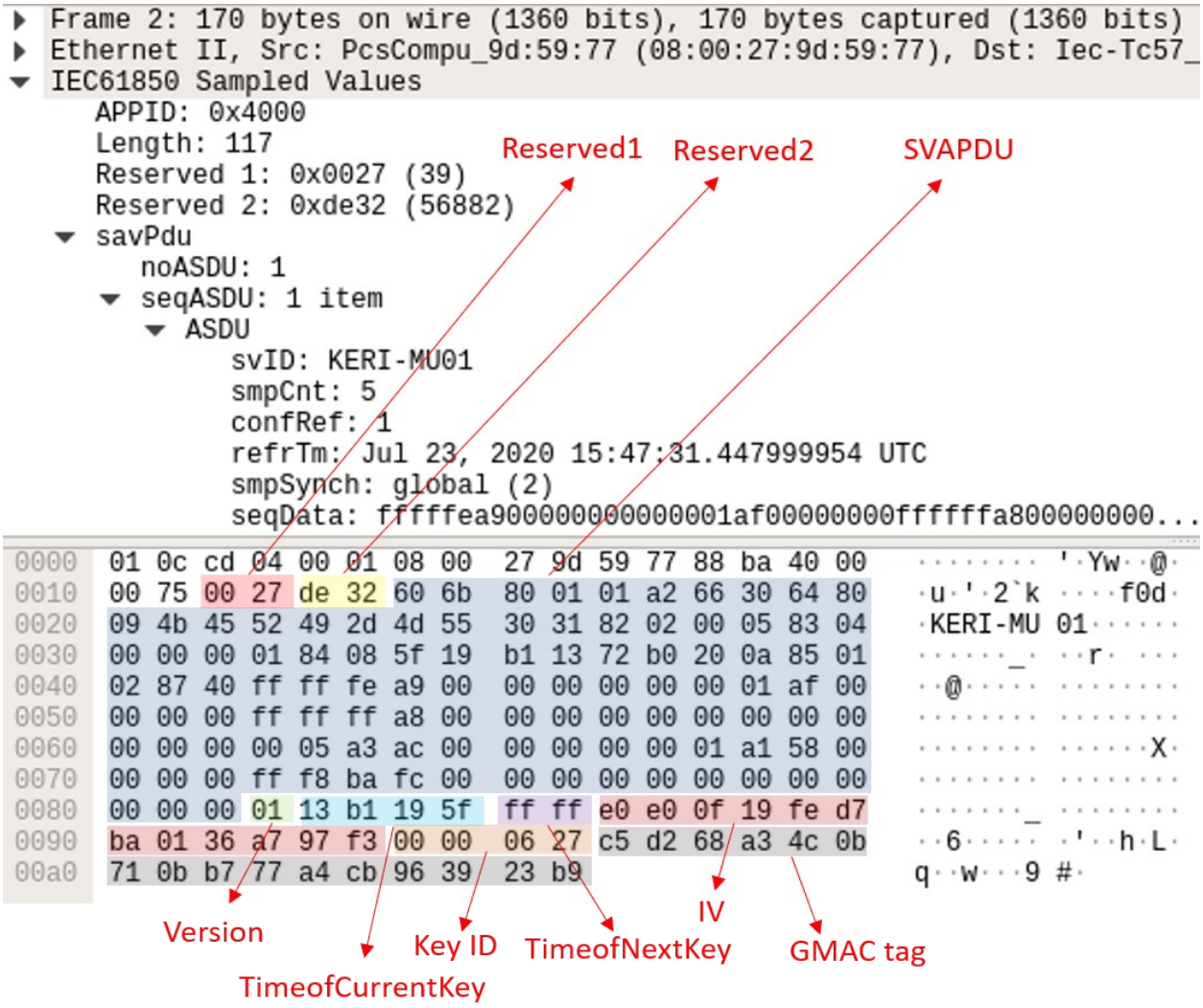

Figure 9: Captured SV packet with AES-GMAC.

If there are more than N number of lost SV packets, this will be regarded as “high SmpCnt attack.” Once a violation is detected in Step 4, the P&C IED will drop all SeSV packets and send an alarm to operators.

5.2. GMAC for SV

Figure 9: shows the captured SeSV packet with AES-GMAC algorithm. It contains all the relative authentication values of SV PDU that is described in Figure 8: The Reserved 1 field shows the 39 bytes of GMAC extension that is appended to the original SV packet whereas the Reserved 2 value indicates the 16-bit CRC calculation. The length of the generated GMAC tag is 16 bytes.

5.3. HMAC for SV

Similarly, Figure 10. shows the captured SeSV packet with AES HMAC algorithm. It also contains all the relative authentication values of SV PDU that is described in Figure 8. One of the main differences between GMAC and HMAC tags is the IV field that is needed for GMAC calculation but not for the HMAC.

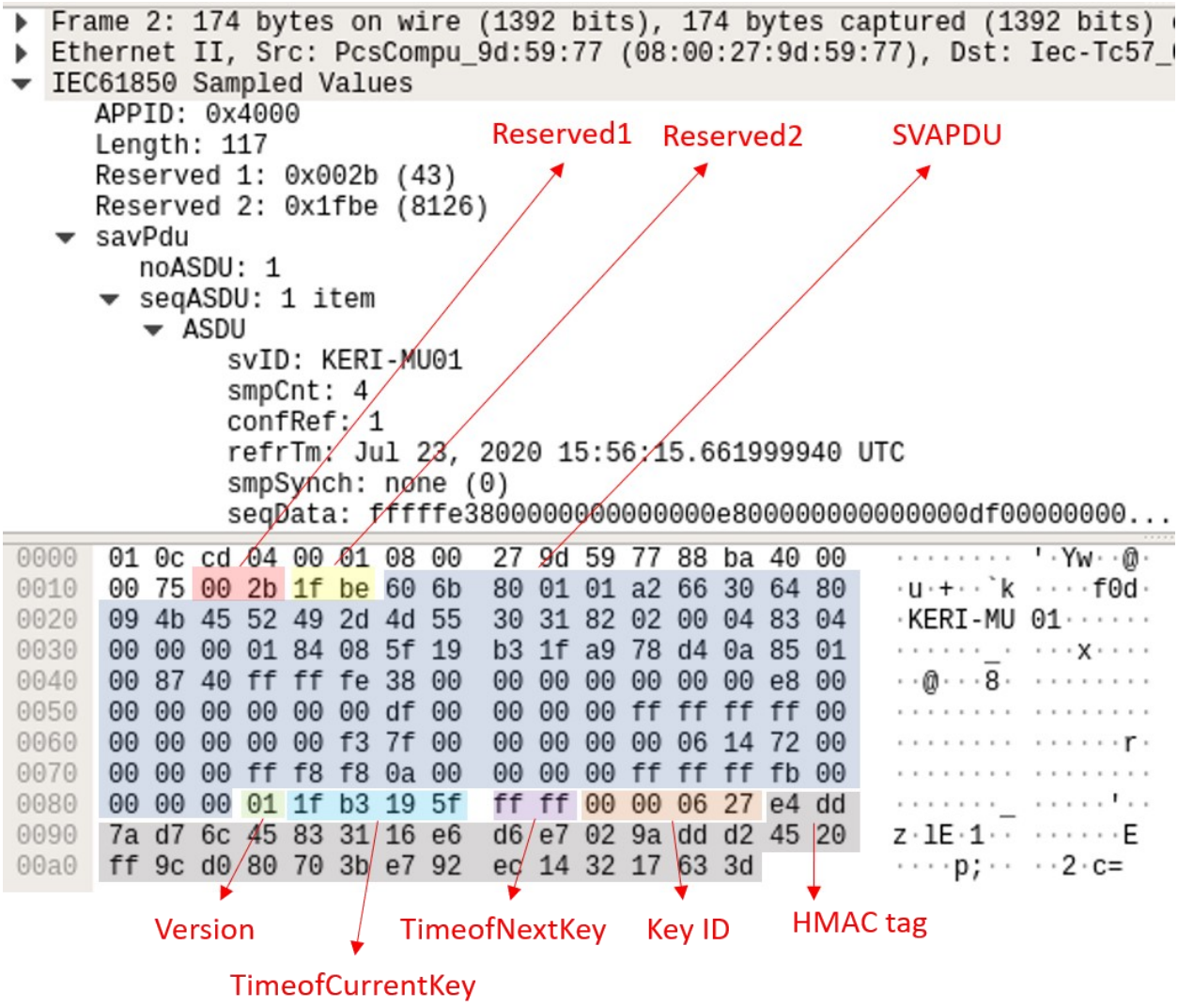

Figure 10: Captured SV packet with HMAC-SHA

Chapter 6: Hardware-In-The-Loop (HIL) TestBed

To validate the proposed algorithms in a more realistic environment, a time-domain

Table 5: Performance evaluation of GMAC for SV

Platform	Algorithms	Packet size (Bytes)	Average processing time(μsec)		
			Publisher MAC	Subscriber	
				MAC	Comp.
Intel Core i5	AES-GMAC-128	170	6.392	6.402	1.021
	AES-GMAC-192	170	6.458	6.453	1.025
	AES-GMAC-256	170	6.505	6.509	1.026
ARM Cortex-A9	AES-GMAC-128	170	34.613	34.619	1.284
	AES-GMAC-192	170	34.849	34.884	1.345
	AES-GMAC-256	170	34.935	34.897	1.234

electromagnetic transient power system simulation model has been developed using MATLAB Simulink Simscape Power Systems and extracted the simulated currents and voltages as input for the merging unit. The power system model used for the HIL simulation is shown in Figure 11: The model is created for a representative high voltage 500 kV substation and includes a number of controllable loads system. Additionally, a medium voltage network is also modeled with a distribution grid connected to the 230 kV side. A total of 2 embedded devices (ARM Cortex-A9) are implemented for IEC61850 based merging unit and P&C IED with the proposed SeSV functions, respectively. A key requirement of the demonstration is that the proposed SeSV must not delay existing protection system's capability to detect and protect against faults in the system. It was confirmed in the lab set up that the distributed cybersecurity functions performed dependably in blocking simulated cyber-attacks with timing performance that did not compromise the relays' protection times.

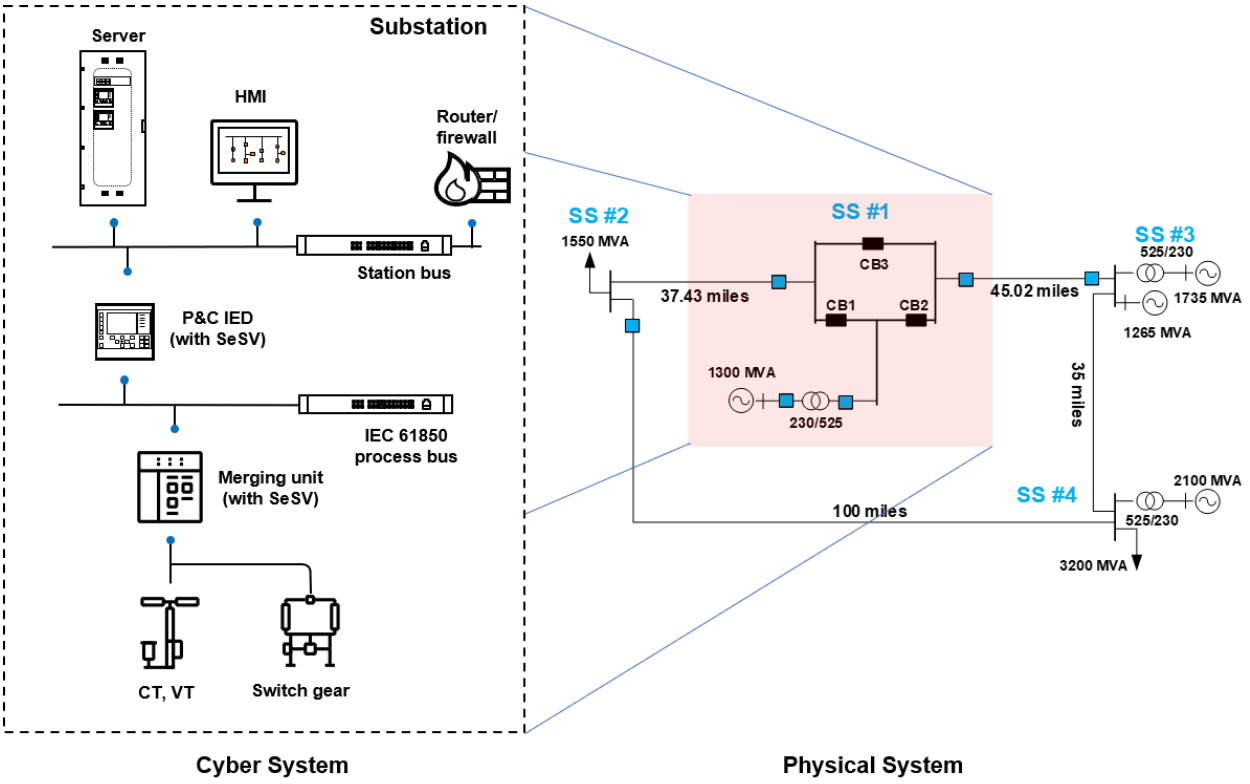

Figure 11: HIL Testbed

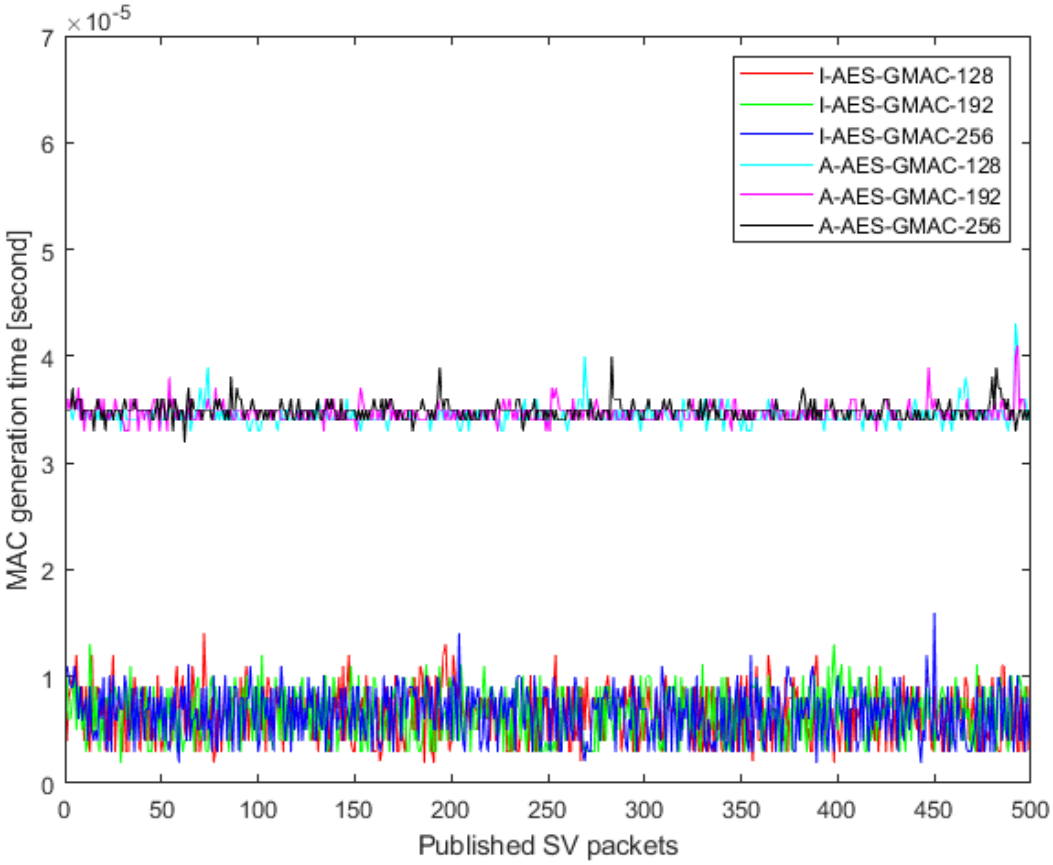

Figure 12: GMAC generation time (I: Intel Core i5, A: ARM Cortex-A9)

Chapter 7: Case Study

7.1. Case Study 1

Table 6: Performance evaluation of HMAC for SV

Platform	Algorithms	Packet size (Bytes)	Average processing time(µsec)		
			Publisher MAC	Subscriber	
				MAC	Comp.
Intel Core i5	HMAC-SHA256-128	158	17.080	17.455	1.034
	HMAC-SHA256	174	17.933	17.930	1.061
	HMAC-SHA512	190	19.579	19.577	1.026
ARM Cortex-A9	HMAC-SHA256-128	158	96.212	96.250	1.134
	HMAC-SHA256	174	96.188	96.189	1.149
	HMAC-SHA512	190	172.815	173.224	1.127

Performance of MAC Algorithms Table 5 shows the results of the performance test using the different GMAC algorithms and hardware for the proposed SeSV. The GMAC encoding times at both publisher and subscriber and comparison times are calculated to check the average SeSV processing time. Due to the diverse of the microprocessors in the merging unit and P&C IEDs, one high performance and the other low processor have been chosen.

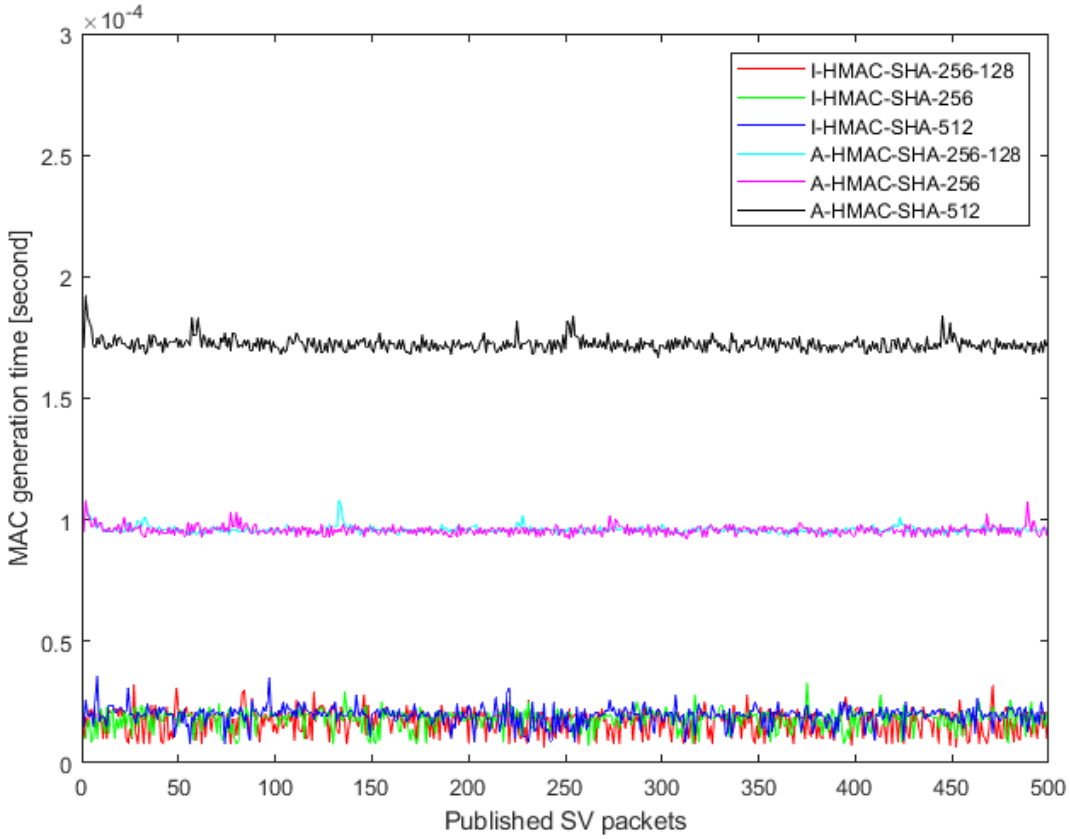

Figure 13: HMAC generation time (I: Intel Core i5, A: ARM Cortex-A9)

The results show that AES-GMAC-128 algorithm has the most top processing performance, whereas AES-GMAC-256 has the most inferior performance. By considering the SV packet intervals as described in Table 2, even AES-GMAC 256 can be used for the ARM core implemented device. Figure 12: illustrates the overall results of different MAC algorithms with different hardware during 500 times of test cases. Compare to the GMAC algorithms, HMAC showed much higher computational times to calculate the MAC tag as shown in Table 6 and Figure 13. Even though HMAC-SHA512 shows the highest average computational time, it is still faster than the lowest SV interval time (208 µsec). One interesting observation from the

experiments is that HMAC algorithms showed a similar performance using Intel CPU; however, it showed different performance using the ARM core processor as described in Figure 13.

7.2. Case Study 2: SV Attack Without MAC

The four different types of cyber-attacks have been used for the case study of SV attacks as shown in Table 7. Once an adversary gains access to the process bus of the digital substation, they could monitor the SV packets and analyze the semantics of SV PDU. After finish the analysis of SV streams, they could initiate the four different types of SV attacks. For instance, they injected the malicious SV packets that contain fault currents and voltages, and the P&C IED will subscribe to the manipulated SV packet as illustrated in Figure 14. The fault currents information of SV will initiate the overcurrent function of IED, and then the IED will send trip GOOSE messages back to the merging unit. The circuit breakers that are connected to the merging unit will be opened and attackers successfully finished the cyber-attacks. In this scenario, the proposed SeSV has not been implemented in the merging unit and P&C IED. So the results show that the impacts of the successful attacks are critical.

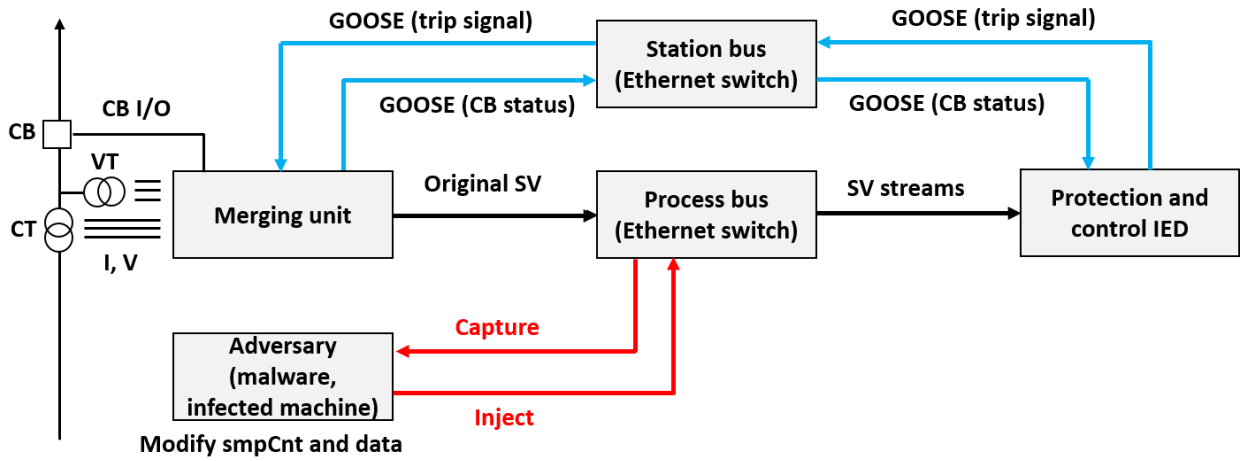

Figure 14: Communication diagram for the case study.

7.3. Case Study 3: SV Packet Injection Attack with MAC

The proposed SeSV structures are implemented in this case study scenarios. As explained in Chapter 5, the MAC algorithms of SeSV detects the four types of cyber attacks including the preshared key based attack. Without the IDS module in SeSV subscriber, an SV injection attack using the same preshared key cannot be detected at the subscriber. The results show that the IDS module can bridge the gaps of the MAC based algorithms.

Table 7: Results of SV attacks

	Without SeSV		With SeSV	
Attack type	Attack result	Impact	Attack result	Impact
SV replay attack	Success	Open CB	Fail	Alarm issued
Spoofing attack	Success	Open CB	Fail	Alarm issued
SV flood attack	Success	P&C IED Comm. error	Fail	Alarm issued
High smpCnt attack	Success	Drop lots of SV packets	Fail	Alarm issued
Preshared key attack	N/A	N/A	Fail	Alarm issued

7.4. Case Study 4: Time Delay for Protection

Cybersecurity functions must not interrupt the existing protection functions of P&C IED. Any delays or interruptions of the normal operation of P&C IED during the power system fault may damage or disrupt the life of expensive substation equipment, e.g., transformer. Therefore, the total time delay has been measured to validate the performance of the proposed SeSV that includes delays in the merging unit t_{MU}, process bus Ethernet switch t_{SWp} delay in P&C IED t_{PI} to calculate the protection algorithm, SV communication delay t_{SV} GOOSE communication delay t_{GS}, and station bus Ethernet delay t_{SWs} as shown in Eq. 1.

$$t_{total} = t_{PI} + t_{SWs} + t_{SWp} + t_{MU} + t_{SV} + t_{GS} \quad (1)$$

The merging unit starts to measure the time when a fault occurred at a transmission line, and then calculate the total time delay when MU receives trip GOOSE signal from the P&C IED. The simulated protection function is the instantaneous overcurrent function with root mean squared (RMS) calculation in the P&C IED. Table 8 shows the results of the total protection time delay

Table 8: Total protection time delay using SeSV

Platform	Algorithm	The total protection time delay (msec)
Intel Core i5	AES-GMAC-128	1.377
	AES-GMAC-192	1.361
	AES-GMAC-256	1.379
	HMAC-SHA-256-128	1.384
	HMAC-SHA-256	1.387
	HMAC-SHA-512	1.386
ARM Cortex-A9	AES-GMAC-128	3.198
	AES-GMAC-192	3.159
	AES-GMAC-256	3.146
	HMAC-SHA-256-128	3.195
	HMAC-SHA-256	3.194
	HMAC-SHA-512	3.199

from the fault to receiving a trip signal. Since the implemented HIL system only focused on the necessary functions, e.g., SeSV, GOOSE, and overcurrent protection, the actual implementation in the commercial IED may have more delays (subscribe multiple SV messages). The highest total delay to use ARM Cortex-A9 processor is when HMAC is chosen for the authentication algorithm, and this can be used for the applications with a total of 3.2 [msec] delay.

Chapter 8: Conclusion

The increased numbers of cyber-physical attacks on power grid applications show that the need for improving security measures of the existing industrial communication protocols, e.g., SV message of IEC61850-9-2LE. Although IEC62351- 6:2020 recommended to use GMAC and HMAC as cybersecurity mitigation to check the integrity of SV, practical considerations and performance tests to apply the MAC algorithms are not shown. Furthermore, the compromised symmetric key between publisher and subscriber may expose other security vulnerabilities and cyber threats. This report proposed a SeSV framework to handle the above-mentioned problems using HIL testbed. The performance of the proposed SeSV has been evaluated and validated with different types of GMAC and HMAC algorithms and hardware platforms. The results of SeSV framework show promising and meeting the performance requirements of IEC61850. This can be implemented on existing IEDs in digital substations. Future work includes (1) interoperability issues between different products should be addressed, (2) performance evaluation of multiple SV streams, as well as (3) key distributed algorithms can be established.

References

[1] J. Hong, “Cybersecurity of substation automation systems”. PhD thesis, Washington State University, 2014.

[2] R. Falk and Steffen, “Security Considerations for Multicast Communication in Power Systems,” *International Journal on Advances in Security*, vol 6 no 3 & 4, 2013.

[3] D. C. Elizondo, J. de La Ree, A. G. Phadke, and S. Horowitz, “Hidden failures in protection systems and their impact on wide-area disturbances,” in 2001 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No.01CH37194), vol. 2, 2001, pp. 710–714.

[4] G. N. Ericsson, “Cyber security and power system communication –essential parts of a smart grid infrastructure,” *IEEE Trans. Power Del*., vol. 25, no. 3, pp. 1501–1507, Jul. 2010.

[5] C. Brunner, "IEC 61850 for power system communication," 2008 IEEE/PES Transmission and Distribution Conference and Exposition, Chicago, IL, 2008, pp. 1-6.

[6] D. M. E. Ingram, P. Schaub, R. R. Taylor, and D. A. Campbell, “System level tests of transformer differential protection using an IEC61850 process bus,” *IEEE Trans. Power Del*., vol. 29, no. 3, pp. 1382–1389, Jun. 2014.

[7] L. Zhu, D. Shi, and P. Wang, “IEC61850-based information model and configuration description of communication network in substation automation*,” IEEE Trans. Power Del.*, vol. 29, no. 1, pp. 97–107, Feb.2014.

[8] Q. Huang, S. Jing, J. Li, D. Cai, J. Wu, and W. Zhen, “Smart substation: State of the art and future development,” *IEEE Trans. Power Del*., vol. 32, no. 2, pp. 1098–1105, April 2017.

[9] S. Kariyawasam, A. D. Rajapakse, and N. Perera, “Investigation of using IEC61850-sampled values for implementing a transient-based protection scheme for series-compensated transmission lines,” *IEEE Trans. Power Del*., vol. 33, no. 1, pp. 93–101, Feb. 2018.

[10] R. Wojtowicz, R. Kowalik, and D. D. Rasolomampionona, “Next generation of power system protection automation—virtualization of protection systems,” *IEEE Trans. Power Del*., vol. 33, no. 4, pp. 2002–2010, Aug.2018.

[11] J. Hong and C. Liu, “Intelligent electronic devices with collaborative intrusion detection systems,” *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 271–281, Jan. 20

[12] I. Lim and T. S. Sidhu, “Design of a backup ied for IEC61850-based substation,” *IEEE Trans. Power Del*., vol. 28, no. 4, pp. 2048–2055, Oct.2013.

[13] J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, “Cyber-attack resilient distance protection and circuit breaker control for digital substations,” *IEEE Trans. Ind*. Informat., vol. 15, no. 7, pp.4332–4341, July 2019.

[14] Y. Yang, H. Xu, L. Gao, Y. Yuan, K. McLaughlin, and S. Sezer, “Multidimensional intrusion detection system for IEC61850-based scada networks,” *IEEE Trans. Power Del*., vol. 32, no. 2, pp. 1068–1078, April 2017.

[15] “Power systems management and associated information exchange - data and communication security,” in Part 6, Security for IEC 61850, 2007, IEC62351-6:2007.

[16] F. Hohlbaum, M. Braendle, and F. Alvarez, “Cyber security practical considerations for implementing IEC62351,” in PAC World Conf., Dublin, Ireland, Jun. 2010.

[17] M. Strobel, N. Wiedermann, and C. Eckert, “Novel weaknesses in IEC62351 protected smart grid control systems,” in 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm), 2016, pp. 266–270.

[18] T. T. Tesfay and J. Le Boudec, “Experimental comparison of multicast authentication for wide area monitoring systems,” *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 94–4404, Sept. 2018.

[19] “Power systems management and associated information exchange - data and communication security,” in Part 6, Security for IEC61850, IEC62351-6:2020 PRV, 2020.

[20] D. Ishchenko and R. Nuqui, “Secure communication of intelligent electronic devices in digital substations,” in 2018 IEEE/PES Transmission and Distribution Conference and Exposition (T D), 2018, pp. 1–5.

[21] S. M. S. Hussain, T. S. Ustun, and A. Kalam, “A review of IEC62351 security mechanisms for IEC61850 message exchanges,” *IEEE Trans.Ind. Informat*., vol. 16, no. 9, pp. 5643–5654, Sept. 2020.

[22] J. Hong, C. Liu and M. Govindarasu, “Detection of cyber intrusions using network-based multicast messages for substation automation,” ISGT 2014, Washington, DC, 2014, pp. 1-5, doi: 10.1109/ISGT.2014.6816375.

[23] P. E. Weerathunga and A. Cioraca, "Securing IEDs against cyber threats in critical substation automation and industrial control systems," 2017 70th Annual Conference for Protective Relay Engineers (CPRE), College Station, TX, 2017, pp. 1-20, doi: 10.1109/CPRE.2017.8090048.

[24] S. Mohagheghi, J. Stoupis and Z. Wang, "Communication protocols and networks for power systems-current status and future trends," 2009 IEEE/PES Power Systems Conference and Exposition, Seattle, WA, 2009, pp. 1-9, doi: 10.1109/PSCE.2009.4840174.

[25] Khaled, Omar, et al. "Analysis of secure TCP/IP profile in 61850 based substation automation system for smart grids." International Journal of Distributed Sensor Networks, vol. 2016, 2016. Accessed 14 Dec. 2020.

[26] S. Obermeier, S. R. Schlegel, J. Schneider, “Assessing the Security of IEC 62351,” 3rd International Symposium for ICS and SCADA Cyber Security Research, pp. 11-19, September 2015.

[27] T. V. Arun, L. Lathesh, A. R. Suhas, “Substation Automation system,” International Journal of Scientific & Engineering Research, vol. 7, Issue 5, May 2016.

[28] J. Wang, G. Constante, C. Moya, and J. Hong, “Semantic analysis framework for protecting the power grid against monitoring-control attacks,” IET Cyber-Physical Systems: Theory Applications, vol. 5, no. 1, pp. 119–126, March 2020.

[29] Y. Zhang, L. Wang, Y. Xiang, and C. Ten, “Inclusion of scada cyber vulnerability in power system reliability assessment considering optimal resources allocation,” *IEEE Trans. Power* Syst., vol. 31, no. 6, pp. 4379–4394, Nov. 2016.

[30] H. Smith and H. Morrison, Ethical Hacking: A Comprehensive Beginner’s Guide to Learn and Master Ethical Hacking, comprehensive ed. CreateSpace Independent Publishing Platform, North Charleston, SC, Jun. 21, 2018.

[31] S. M. S. Hussain, S. M. Farooq, and T. S. Ustun, “Analysis and implementation of message authentication code (MAC) algorithms for GOOSE message security,” IEEE Access, vol. 7, pp. 80980–80984, June 2019.

[32] “Consolidated version, communication networks and systems for power utility automation,” in Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC8802-3, 2020, IEC61850-9-2:2020 CSV.

[33] M. Dworkin, “Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC,” NIST Special Publication 800-38D.

[34] H. Krawczyk, M. Bellare and R. Canetti, “HMAC: Keyed-Hashing for Message Authentication,” IETF RFC 2104.

[35] “Open-source libraries for IEC61850,” Available at: http://libiec61850.com/, May 2020