CEA Comité Español de Automática

XLVI JORNADAS AUTOMÁTICA CARTAGENA 2025

UNIVERSIDADE DA CORUÑA

Jornadas de Automática

Adquisición de tráfico de red en demostrador de subestación eléctrica

Baltuille, Pablo[a], Santos, Jose Miguel[a], Pérez, Daniel[a], Alonso, Serafín[a], Fuertes, Juan José[a,*], Domínguez, Manuel[a,*]

[a]*Grupo de Investigación SUPPRESS, Escuela de Ingenierías, Universidad de León, Campus de Vegazana, León, 24007, España*

https://suppress.unileon.es

To cite this article: Baltuille, Pablo, Santos, Jose Miguel, Pérez, Daniel, Alonso, Serafín, Fuertes, Juan José, Domínguez, Manuel. 2025. Acquisition of network traffic at electrical substation demonstrator. Jornadas de Automática, 46. https://doi.org/10.17979/ja-cea.2025.46.12126

Resumen

En este artículo se presenta una metodología orientada a la adquisición de conjuntos de datos de tráfico de red, tanto normal como anómalo, en sistemas de automatización y control de subestaciones eléctricas digitales. El enfoque se centra en los protocolos comúnmente utilizados en estas plataformas –IEC61850 GOOSE, MMS y SV, PTP, IEC60870-5-104 y SNTP– y se desarrolla en un entorno controlado con dispositivos representativos, como un controlador de bahía, relés de protección, sistema SCADA, etc. Sobre esta infraestructura se ejecuta un conjunto de experiencias planificadas que reproducen el funcionamiento normal de una subestación y se introducen ataques específicos para analizar su impacto. Finalmente, los datos recopilados se analizan mediante la extracción y selección de características y se organizan en flujos de datos útiles para el posterior entrenamiento de modelos.

Palabras clave: Subestaciones eléctricas, Ciberseguridad, Detección de anomalías, IEC61850, IEC60870

Acquisition of network traffic at electrical substation demonstrator

Abstract

This article presents a methodology oriented to the acquisition of network traffic data sets, both normal and anomalous, in digital electrical substation automation and control systems. The approach focuses on the protocols commonly used in these platforms–IEC61850 GOOSE, MMS and SV, PTP, IEC60870-5-104 and SNTP–and is developed in a controlled environment with representative devices, such as a bay controller, protection relays, SCADA system, etc. A set of planned experiments that reproduce the normal operation of a substation are run on this infrastructure and specific attacks are introduced to analyze their impact. Finally, the collected data is analyzed by feature extraction and selection and organized into data streams useful for subsequent model training.

Keywords: Electrical substations, Cybersecurity, Anomaly detection, IEC 61850, IEC 60870

1. Introducción

En los últimos años, el proceso de digitalización en el sector energético y del transporte ha transformado los sistemas de automatización y control. Las subestaciones eléctricas, esenciales para el funcionamiento de redes ferroviarias, han evolucionado desde entornos aislados hacia sistemas ciberfísicos interconectados, donde diferentes dispositivos se comunican entre sí siguiendo estándares tales como IEC 61850 o IEC 60870. Esta transición ha mejorado varios aspectos de configuración, monitorización remota, y capacidad de respuesta.

Sin embargo, también ha introducido vulnerabilidades derivadas del uso de nuevas tecnologías, la convergencia entre las redes IT/OT y la creciente exposición a ciberamenazas. Este hecho resulta más estratégico en infraestructuras críticas donde un incidente puede tener consecuencias graves de seguridad (Gaspar et al., 2023). Concretamente en el sector energético, las subestaciones constituyen uno de los objetivos

*Autores para correspondencia: jj.fuertes@unileon.es, mdom@unileon.es

con mayor número de incidentes.

En este contexto, resulta fundamental disponer de metodologías que permitan simular, observar y analizar el comportamiento de estos sistemas tanto en condiciones normales como ante posibles escenarios de ataque. Sin embargo, el estudio de estas situaciones en entornos reales está limitado por consideraciones de seguridad, lo que dificulta la obtención de datos fiables para su posterior estudio. El presente trabajo aborda esta necesidad utilizando un demostrador que reproduce un sistema de automatización de una subestación eléctrica de tracción, incorporando dispositivos reales y comunicaciones basadas en los estándares IEC 61850 e IEC 60870. Con el objeto de completar las comunicaciones, el demostrador ha sido ampliado con mecanismos de sincronización temporal y de simulación de protocolos como *Sampled Values* (SV), *Precision Time Protocol* (PTP) y *Simple Network Time Protocol* (SNTP), asegurando la precisión y coherencia entre los eventos que se produzcan en el sistema.

A partir de esta infraestructura se desarrolla una metodología para la adquisición de dos conjuntos de datos diferenciados: uno correspondiente a tráfico normal y otro constituido por tráfico anómalo, resultado de ataques diseñados específicamente para comprometer los protocolos utilizados. La inclusión de ataques como denegación de servicio (*Denial of Service*, DoS), *Man-in-the-Middle* (MitM) o ataque de reinyección (*Replay*) resulta clave para simular escenarios verosímiles y estudiar el comportamiento del sistema ante amenazas

El resto del artículo se estructura del siguiente modo: en el apartado 2 se revisan trabajos relacionados con tráfico en redes industriales; en el apartado 3 se detalla el banco de pruebas utilizado, incluyendo la configuración del armario y las comunicaciones establecidas; el apartado 4 describe la metodología empleada para la generación y análisis de tráfico; en el apartado 5 se presentan los resultados experimentales; y en el apartado 6 se exponen las conclusiones y futuras líneas de trabajo.

2. Estado del arte

La adquisición de datos en infraestructuras reales es difícil de obtener tanto por su confidencialidad como por los riesgos de interrupción. Sin embargo, existen enfoques que reproducen comportamientos con sistemas reales en entornos controlados (Conti et al., 2021) lo que permite obtener conjuntos de datos fiables. También se pueden producir datos sintéticos a través de simulaciones y considerar enfoques híbridos donde entornos simulados complementen las funcionalidades de equipos reales (Gaspar et al., 2023). Aunque existen algunos ejemplos de datos públicos, como EPIC (Adepu et al., 2019) o *PowerDuck* (Zemanek et al., 2022), son necesarios trabajos adicionales que amplíen la representación del funcionamiento industrial de los protocolos y su comportamiento ante diferentes ataques.

El estándar IEC 61850 ha sido ampliamente adoptado en subestaciones por su capacidad para estructurar comunicaciones entre dispositivos de protección y control. Dentro de este estándar, los protocolos GOOSE, MMS y SV han sido objeto de estudio (Aftab et al., 2020), así como también el impacto que diferentes tipos de ataques (Elgargouri and Elmusrati, 2017) producen en este tipo de redes (Roomi et al., 2023). En concreto, trabajos como (Kush et al., 2014) o (Tasmi et al., 2024) estudian e identifican vulnerabilidades en el protocolo GOOSE y proponen ataques para su explotación. Otros autores amplían ese estudio también a los efectos de ataques contra MMS (Pärssinen et al., 2022) o SV (Hussain et al., 2023), así como posibles medidas de mitigación (Manzoor et al., 2024).

Respecto al protocolo IEC60870-5-104, utilizado en redes de supervisión, se han realizado investigaciones como (Radoglou-Grammatikis et al., 2019), la cual se encuentra relacionada con la emulación de ataques sobre subestaciones simuladas con objeto de comprobar los riesgos que suponen sobre la red, o también el análisis del impacto de ataques concretos (Arifin et al., 2021). Otros autores, como (Teryak et al., 2023), se centran en los escenarios de ataque existentes y desarrollan un escenario propio para entrenar algoritmos de *machine learning*.

En lo referido al protocolo PTP, hay una variedad de artículos en los que se analizan los principales ataques contra este protocolo, por ejemplo en (Alghamdi and Schukat, 2020a,b; Akbarzadeh et al., 2023) donde se investigan APT (*Advanced Persistent Threats*), como el ataque *Delay* (*Delay Attack*), para lograr una pérdida de sincronización y examinar sus consecuencias (Ullmann and Vögeler, 2009). En el caso de SNTP, los trabajos exploran las implicaciones de ataques contra el protocolo, por ejemplo el estudio de una suplantación de identidad *Spoofing* (Mahlous, 2024) o denegación de servicio (DoS) (Malhotra et al., 2015), donde se compromete la disponibilidad de un servicio; y variantes como distribuidos DDoS (Rudman and Irwin, 2015) producidos a gran escala por varios equipos infectados previamente, o DRDoS donde los paquetes se redirigen divididos al objetivo con un factor de amplificación (Sassani et al., 2016).

Aunque existen estudios que abordan individualmente la seguridad de cada protocolo o la detección de ataques específicos, son escasos los trabajos que integran en un mismo entorno la generación de tráfico real, la simulación de ataques y la captura de datos etiquetados. En este trabajo se abordan estos aspectos mediante un demostrador físico que reproduce el funcionamiento de una subestación eléctrica de tracción, incorporando dispositivos reales, protocolos industriales y mecanismos de sincronización temporal.

3. Banco de pruebas

El banco de pruebas utilizado en este artículo consiste en un armario de control para un sistema eléctrico bifásico de tracción, orientado al transporte ferroviario (Baltuille et al., 2024). A continuación, se detalla la estructura del armario, las funcionalidades de simulación y sincronización incorporadas y el mecanismo de captura del tráfico de red mediante sondas especializadas.

3.1. Armario de control de subestación de tracción

El armario reproduce el funcionamiento de una subestación eléctrica de tracción equipada con dos líneas de alimentación eléctrica: la línea A, como principal y la línea B, como respaldo. La selección de la línea activa, así como su conmutación en caso de fallo, se realiza mediante cinco interruptores

(KA, K0, K1, KB y K2). El sistema incorpora una funcionalidad automática (*Automatic Transfer Scheme*, ATS) que permite transferir la carga a la línea alternativa ante una interrupción en el suministro, mejorando la disponibilidad del sistema. En la Figura 1 se presenta un esquema eléctrico del armario, incluyendo los sistemas de protección y control encargados de gestionar los interruptores.

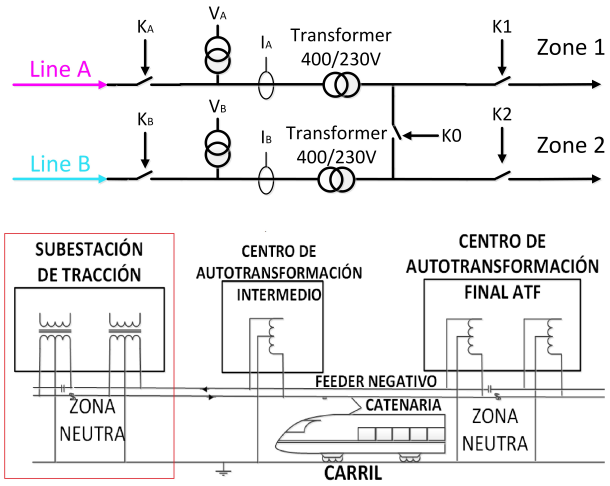

Figura 1: Esquema de líneas del armario de control de la subestación

3.2. *Simulación de tráfico SV y sincronización temporal*

Dado que no todos los equipos de protección y control disponen de forma nativa del protocolo SV, se ha optado por simular el tráfico asociado a dicho protocolo, cuya adopción es cada vez más común en los diseños de subestaciones. Para ello, se han desplegado dos máquinas virtuales que actúan como publicador y suscriptor, utilizando la biblioteca *libiec61850* para generar tráfico SV en condiciones controladas. La Figura 2 muestra el esquema de conexiones de los equipos del armario en las redes de control y supervisión. En la zona izquierda de la red de control (representada en azul) se indican las máquinas responsables de la generación del tráfico SV simulado.

Además, se han incorporado mecanismos de sincronización temporal en ambas redes del sistema. En la red de supervisión, se ha desplegado un servidor PTP mediante la implementación *ptpd2*, una versión de código abierto del protocolo IEEE 1588, con el objeto de alcanzar una sincronización precisa entre dispositivos. Adicionalmente, se ha configurado un servidor SNTP tanto en la red de control como en la de supervisión, con el fin de proporcionar una sincronización básica de todos los dispositivos, incluyendo aquellos que no son compatibles con PTP. La combinación de estas soluciones permite una correlación temporal precisa entre los paquetes capturados por las sondas y los eventos que ocurran en el sistema, lo cual mejora la calidad del análisis y la fiabilidad de los resultados.

3.3. *Arquitectura de sondas*

Para analizar detalladamente las comunicaciones del sistema, se han desplegado dos sondas en ubicaciones estratégicas de la red del armario. Cada sonda ha sido configurada con reglas específicas de filtrado y detección, adaptadas a los protocolos presentes en su segmento de red correspondiente.

La primera sonda se encuentra instalada en la red de supervisión, entre la pasarela (*gateway*) y uno de los switches del anillo redundante de dicha red. Esta ubicación (ver Figura 2) permite capturar el tráfico entrante conforme al protocolo IEC 60870-5-104, así como los eventos intercambiados por el SCADA.

La segunda sonda está ubicada entre la pasarela, el controlador de bahía y uno de los switches del anillo de la red de control. Desde esta posición es posible capturar tráfico generado bajo al estándar IEC 61850, incluyendo mensajes MMS entre la pasarela y otros dispositivos, tramas GOOSE emitidas por los relés de protección, y mensajes SV utilizados para la transmisión de medidas de tensión y corriente digitalizadas. Asimismo, se considera la detección del tráfico de sincronización horaria mediante los protocolos PTP y SNTP, fundamentales para garantizar la precisión temporal en la operación de la red.

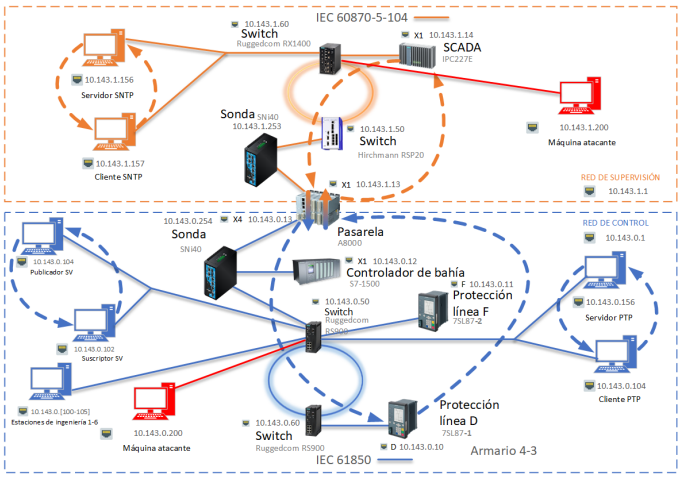

Figura 2: Esquema de las redes de control y supervisión

4. Metodología

La adquisición del tráfico de red se estructura en la captura de tráfico normal y de tráfico anómalo, en función de si las comunicaciones representan un funcionamiento habitual o están afectadas por ataques. La metodología planteada para la monitorización y el análisis del tráfico de red se organiza en tres fases:

1. **Generación de tráfico**: Se planifican operaciones específicas en el sistema (por ejemplo, una secuencia de operaciones de maniobra desde el SCADA), provocando una secuencia de eventos que generan tráfico de red. En condiciones normales, se producen tramas de los protocolos IEC 60870-5-104 y SNTP en la red de supervisión, y MMS, GOOSE, SV y PTP en la red de control. En el caso de tráfico anómalo, se ejecutan ataques definidos sobre los protocolos seleccionados.
2. **Captura del tráfico**: Las sondas desplegadas en ambas redes monitorizan y registran los paquetes generados durante las pruebas. A través de sus interfaces web,

es posible visualizar detalles como el tipo de protocolo, la dirección de origen y destino, o la hora de detección. Asimismo, los paquetes se pueden exportar para su análisis posterior.

3. **Análisis de los datos capturados**: Los paquetes registrados son analizados con herramientas específicas de inspección de tráfico. Esto permite examinar en detalle la estructura interna de los mensajes, los valores transmitidos y la lógica de operación de los dispositivos implicados.

4.1. Adquisición de tráfico normal

En el entorno de laboratorio, se identificaron dos tipos principales de tráfico en las redes de control y supervisión: el tráfico cíclico, generado de manera periódica entre dispositivos para mantener la sincronización de variables, actualizar estados o realizar comprobaciones; y el tráfico asociado a eventos, que se activa ante determinadas acciones de operación. Ambos tipos de tráfico coexisten en condiciones normales, siendo el primero constante incluso sin intervención del operador.

Las experiencias consideradas incluyeron, entre otras, la ejecución de maniobras desde el sistema SCADA, como el cierre del interruptor KA, simulaciones de condiciones de interbloqueo lógico, maniobras coordinadas como el cierre de los interruptores KA y K1 y pruebas con fallos de subtensión: uno sin función ATS, que generó paquetes MMS y reportes sin maniobras automáticas; y dos con ATS activado (en la línea A y otro en la línea B) que desencadenaron el cierre automático de interruptores, acompañados por ráfagas de mensajes GOOSE y actualizaciones MMS. También se simuló un intento de cierre del interruptor KB con el KA ya cerrado, provocando respuestas de denegación por interbloqueo lógico.

Con el objeto de generar un conjunto de datos de comportamiento normal, se aplicó la metodología mencionada de tres fases diferenciadas. En la primera, se diseñó un archivo de planificación donde se describían el conjunto de experiencias de generación de tráfico de red junto con su temporización. Posteriormente, se realiza la captura del tráfico mediante las dos sondas independientes, conectadas respectivamente a las redes de control y supervisión del armario. La sonda de la red de control registra los paquetes de los protocolos IEC 61850 (GOOSE, MMS, SV) y PTP, mientras que la sonda de la red de supervisión registra eventos de IEC 60870-5-104 y SNTP.

Finalmente, se analizan los flujos de tráfico para extraer un conjunto de características, tanto comunes (estampa de tiempo, direcciones IP y MAC, puertos de origen y destino) como específicas de cada protocolo, tales como *InvokeID* en MMS o *smpCnt* en SV, así como campos que identifican las acciones transportadas, como *TypeID* en IEC 60870-5-104 o *confirmedServiceRequest* en MMS. Además, se aplica un filtrado para conservar sólo aquellas características con al menos un valor no nulo y se añaden etiquetas a los eventos para indicar que pertenece a estas experiencias de generación de tráfico.

4.2. Secuencia de ataques para tráfico anómalo

Para la generación del conjunto de datos correspondiente a tráfico anómalo, se ha diseñado un conjunto de ataques dirigidos contra los protocolos de las redes de control (IEC61850 y PTP) y de supervisión (IEC60870-5-104 y SNTP), tal como se muestran en la Tabla 1. Los ataques se han creado desde dos máquinas virtuales, una en cada red, simulando un escenario realista en el que dichos equipos han sido previamente comprometidos por un atacante con acceso interno al sistema.

Tabla 1: Ataques generados para tráfico anómalo.

Ataque	IEC61850	PTP	IEC60870-5-104	SNTP
Delay		X		X
DoS	X	X	X	X
Drop packets		X		X
Fuzzing	X			
MitM	X		X	
Flooding	X		X	
Poisoning	X			
Replay	X		X	

A continuación, se describen los tipos de ataques considerados:

- ***Denial of Service (DoS)***: Consiste en saturar el funcionamiento de un dispositivo enviando un volumen elevado de paquetes. En un caso serían paquetes de tipo TCP SYN contra el controlador de bahía y uno de los relés de protección (en el protocolo IEC61850) o contra la pasarela (en IEC60870-5-104). En el caso de los protocolos PTP y SNTP, este ataque se realiza mediante el envío de paquetes de tipo UDP malformados al servidor PTP, o mediante el envío de consultas de tipo *monlist* contra el servidor SNTP.

- ***Man-in-the-Middle (MitM)***: En primer lugar realiza un ataque de tipo *Spoofing ARP* para que las comunicaciones entre los dispositivos de interés circulen a través de la máquina atacante. En segundo lugar, intercepta un paquete, modifica el valor de uno de uno de sus campos y lo reenvía al dispositivo de destino. Funciona de forma similar, tanto en el protocolo IEC61850 como en el protocolo IEC60870-5-104.

- ***Packet Flooding***: Este ataque envía de forma continuada una gran cantidad de paquetes malformados del protocolo IEC60870-5-104 para inundar la red de supervisión; o un gran volumen de paquetes malformados de los protocolos GOOSE o TCP para inundar la red de control.

- ***Poisoning***: Se crea un paquete del protocolo GOOSE con una orden errónea y se envía al dispositivo de destino para que éste la ejecute.

- ***Delay***: Este ataque realiza en primer lugar un ataque de tipo *ARP Spoofing* para situarse en la red de comunicaciones entre el cliente y el servidor (tanto PTP como SNTP). Después, intercepta los paquetes procedentes del servidor y los retiene durante 3 segundos para después reenviarlos al cliente y provocar un fallo de sincronización.

- ***Dropping Packets***: De forma similar al ataque *Delay*, este ataque realiza el ataque *ARP Spoofing* para interceptar los paquetes y después los elimina. De esta for-

ma, el cliente (tanto PTP como SNTP) no recibe ningún paquete del servidor durante la ejecución de este ataque.

- ***Replay***: A través de este ataque se intercepta un paquete (de los protocolos MMS y GOOSE o del protocolo IEC60870-5-104) que contenga una orden relacionada con alguna de las pruebas controladas anteriores y se reenvía de forma continuada al destino, de forma que éste ignore el resto de órdenes que se le envíen.

- ***Fuzzing***: Realiza una serie de pruebas mediante el envío de una gran cantidad de paquetes de tipo TCP contra el controlador de bahía.

Siguiendo la metodología descrita previamente, se modifica el archivo de planificación en la primera fase para incluir la ejecución de los ataques contra los diferentes protocolos, junto con su temporización. En la segunda fase, el tráfico generado durante la secuencia de eventos y ataques se captura a través de las sondas desplegadas en ambas redes. La ejecución de los ataques se lleva a cabo de forma controlada, asegurando que las sondas registren los eventos maliciosos generados.

Finalmente, en la tercera fase se realiza un análisis del conjunto generado. De forma similar a la generación del conjunto de datos de tráfico normal, se extraen y se seleccionan las características relevantes; y se asigna una etiqueta a cada evento en la que se indica la experiencia a la que pertenece.

5. Resultados experimentales

Como resultado de la aplicación de la metodología descrita, se ha generado un conjunto de datos correspondiente a tráfico normal, obtenido a partir de pruebas controladas que reproducen distintas condiciones operativas de una subestación de tracción. El tráfico capturado a través de las sondas ha permitido construir flujos etiquetados con eventos característicos de los protocolos implementados, lo que sienta las bases para su posterior análisis y validación.

```
frame.time ip.src ip.dst eth.src eth.dst tcp.srcport tcp.dstport udp.srcport udp.dstport goose.appid goose.length
SIPROTEC2Application/LLN0$DataSet_Salud SIPROTEC2Application/LLN0$GO$Control_DataSet 3000 SIPROTEC2/Application/LL
 SIPROTEC2Ln1/LLN0$DataSet_disparos SIPROTEC2Ln1/LLN0$GO$Control_DataSet 3000 SIPROTEC2/Ln1_59Overvoltage1/LLN0/Co
SIPROTEC2UD2/LLN0$DataSet SIPROTEC2UD2/LLN0$GO$Control_DataSet 3000 SIPROTEC2/UD2/LLN0/Control_DataSet "Jan 27, 20
08 102                                1   9643 4     1    1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1 A8000HEALTH,A8000
 51008                                 1  9643   4   1                  18 1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1
59 102                                 1   23276 5      1   1 SIPROTEC1CB1 CSWI1$CO$Pos$Oper        3 43 0   1 2
 54859
 54859                                  1  23276   5     1                 1
08 102                                  1   9644 5      1   1 A8000CBKD CSWI1$CO$Pos$Oper        3 534 0   1 2,3,
SIPROTEC1CB1/LLN0$DataSet_interruptores SIPROTEC1CB1/LLN0$GO$Control_DataSet 3000 SIPROTEC1/CB1/LLN0/Control_DataS
 51008                                  1  9644   5     1                 1
SIPROTEC2CB1/LLN0$DataSet_Interruptores SIPROTEC2CB1/LLN0$GO$Control_DataSet 3000 SIPROTEC2/CB1/LLN0/Control_DataS
SIPROTEC1CB1/LLN0$DataSet_interruptores SIPROTEC1CB1/LLN0$GO$Control_DataSet 3000 SIPROTEC1/CB1/LLN0/Control_DataS
SIPROTEC1UD1/LLN0$DataSet SIPROTEC1UD1/LLN0$GO$Control_DataSet 3000 SIPROTEC1/UD1/LLN0/Control_DataSet "Jan 31, 20
x4000 60 0 1 1 1 1 svpub_over 421 1 0 442f4b6b44143a4d679c941e34395800
SIPROTEC1CB1/LLN0$DataSet_interruptores SIPROTEC1CB1/LLN0$GO$Control_DataSet 3000 SIPROTEC1/CB1/LLN0/Control_DataS
SIPROTEC1UD1/LLN0$DataSet SIPROTEC1UD1/LLN0$GO$Control_DataSet 3000 SIPROTEC1/UD1/LLN0/Control_DataSet "Jan 31, 20
SIPROTEC1CB1/LLN0$DataSet_interruptores SIPROTEC1CB1/LLN0$GO$Control_DataSet 3000 SIPROTEC1/CB1/LLN0/Control_DataS
SIPROTEC1UD1/LLN0$DataSet SIPROTEC1UD1/LLN0$GO$Control_DataSet 3000 SIPROTEC1/UD1/LLN0/Control_DataSet "Jan 31, 20
 54860                                  1   0  1     RPT           129  9 1,1,1,1,1,1,1,1,1  3,4,17  1  0   10
 54859                                  1   0  1     RPT           240  9 1,1,1,1,1,1,1,1,1  3,4,17  1  0   10
 54859                                  1   0  1      1 SIPROTEC1CB1 CSWI1$CO$Pos$Oper        3 43  1 1  3,2,5,
SIPROTEC1CB1/LLN0$DataSet_interruptores SIPROTEC1CB1/LLN0$GO$Control_DataSet 3000 SIPROTEC1/CB1/LLN0/Control_DataS
SIPROTEC1UD1/LLN0$DataSet SIPROTEC1UD1/LLN0$GO$Control_DataSet 3000 SIPROTEC1/UD1/LLN0/Control_DataSet "Jan 31, 20
08 102                                1   9645 4     1    1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1 A8000HEALTH,A8000
```

Figura 3: Extracto del patrón de los flujos de tráfico de red generados a partir del conjunto de datos de tráfico normal.

En la Figura 3 se muestra un extracto representativo del archivo que contiene algunas tramas de los primeros flujos de tráfico generados a partir del conjunto de datos de tráfico normal. Se pueden observar estructuras periódicas y campos que permiten identificar relaciones específicas entre los dispositivos propios del funcionamiento normal del sistema. La trama que se encuentra resaltada dentro de la figura corresponde a la ejecución de evento 1 (cierre de un interruptor).

Respecto al conjunto de datos de tráfico anómalo, se diseñaron y ejecutaron un conjunto de ataques dirigidos a los protocolos de interés de la red de control (IEC61850 y PTP) y de supervisión (IEC60870-5-104 y SNTP). Aunque la realización de ataques se encuentra aún en desarrollo, se ha podido aplicar la metodología propuesta para ejecutar y estudiar una muestra que incluye ataques dirigidos contra los protocolos GOOSE, PTP y SNTP.

La ejecución controlada de estos ataques ha permitido observar determinados patrones relacionados con el comportamiento del tráfico en la red. Por ejemplo, la Figura 4 muestra el efecto de la ejecución de un ataque tipo *Replay* sobre el protocolo GOOSE. En condiciones normales, el tráfico de paquetes del protocolo GOOSE se realiza desde dos dispositivos hacia un conjunto de direcciones MAC de forma regular en el tiempo. Sin embargo, durante la ejecución del ataque, el paquete interceptado (el cual se encuentra resaltado en color rojo) es reenviado continuamente (véase el flujo de paquetes que se encuentran debajo de la línea discontinua), manteniendo inalteradas las direcciones de origen y destino. Este cambio de patrón en el tráfico del protocolo GOOSE denota una posible anomalía debida a la ejecución de un ataque. Las pruebas realizadas han mostrado unos patrones de comportamiento anómalo, tanto en el número de paquetes enviados como en la ausencia de cambios en los orígenes y destinatarios de los mismos, así como en su tamaño.

```
5.424751    SiemensEnerg_03:2f:86    IecTc57_01:00:04    GOOSE    228
5.552885    SiemensEnerg_03:2f:86    IecTc57_01:00:05    GOOSE    171
7.210059    SiemensEnerg_03:2f:92    IecTc57_01:00:00    GOOSE    201
7.210880    SiemensEnerg_03:2f:92    IecTc57_01:00:01    GOOSE    195
7.223067    SiemensEnerg_03:2f:92    IecTc57_01:00:03    GOOSE    212
7.317362    SiemensEnerg_03:2f:92    IecTc57_01:00:06    GOOSE    171
7.385047    SiemensEnerg_03:2f:86    IecTc57_01:00:02    GOOSE    195
7.425562    SiemensEnerg_03:2f:86    IecTc57_01:00:04    GOOSE    228
7.561149    SiemensEnerg_03:2f:86    IecTc57_01:00:05    GOOSE    171
9.211149    SiemensEnerg_03:2f:92    IecTc57_01:00:00    GOOSE    201
9.212010    SiemensEnerg_03:2f:92    IecTc57_01:00:01    GOOSE    195
9.223928    SiemensEnerg_03:2f:92    IecTc57_01:00:03    GOOSE    212
9.317695    SiemensEnerg_03:2f:92    IecTc57_01:00:06    GOOSE    171
9.384739    SiemensEnerg_03:2f:86    IecTc57_01:00:02    GOOSE    195
9.425866    SiemensEnerg_03:2f:86    IecTc57_01:00:04    GOOSE    228
9.553216    SiemensEnerg_03:2f:86    IecTc57_01:00:05    GOOSE    171
10.212886   SiemensEnerg_03:2f:86    IecTc57_01:00:02    GOOSE    195
10.248783   SiemensEnerg_03:2f:86    IecTc57_01:00:02    GOOSE    195
10.280869   SiemensEnerg_03:2f:86    IecTc57_01:00:02    GOOSE    195
10.316839   SiemensEnerg_03:2f:86    IecTc57_01:00:02    GOOSE    195
10.348383   SiemensEnerg_03:2f:86    IecTc57_01:00:02    GOOSE    195
10.384776   SiemensEnerg_03:2f:86    IecTc57_01:00:02    GOOSE    195
10.416698   SiemensEnerg_03:2f:86    IecTc57_01:00:02    GOOSE    195
10.458156   SiemensEnerg_03:2f:86    IecTc57_01:00:02    GOOSE    195
10.492670   SiemensEnerg_03:2f:86    IecTc57_01:00:02    GOOSE    195
10.532651   SiemensEnerg_03:2f:86    IecTc57_01:00:02    GOOSE    195
10.564404   SiemensEnerg_03:2f:86    IecTc57_01:00:02    GOOSE    195
10.596333   SiemensEnerg_03:2f:86    IecTc57_01:00:02    GOOSE    195
10.628438   SiemensEnerg_03:2f:86    IecTc57_01:00:02    GOOSE    195
```

Figura 4: Extracto del patrón del ataque *Replay* contra el protocolo GOOSE.

6. Conclusiones

En este artículo se presenta una metodología para el estudio de escenarios de ciberseguridad mediante un demostrador de los sistemas de automatización y control de una subestación eléctrica de tracción ferroviaria. La propuesta se basa en la generación de tráfico de red en un entorno controlado, tanto en condiciones normales de operación como ante situaciones anómalas provocadas por ciberataques. Para ello, se han incluido en el demostrador simuladores que complementen los protocolos estudiados y la ejecución de los ataques.

Para la generación de un conjunto de datos de tráfico normal, se diseñaron y ejecutaron pruebas controladas que simulan el funcionamiento típico de la subestación, enviando eventos a través de la red del sistema. Se registró este tráfico agrupándolo en flujos y extrayendo características relevantes de cada protocolo. Posteriormente, se definieron y ejecutaron ataques dirigidos a los principales protocolos de la subestación, lo que permitió generar un conjunto inicial de datos de tráfico anómalo. Aunque este conjunto se encuentra en fase de desarrollo, los ensayos realizados de ataques sobre GOOSE, PTP y SNTP han permitido identificar patrones distintivos y avanzar en la construcción de métodos de experimentación reproducibles y útiles.

Como línea futura de trabajo, se plantea ampliar el conjunto de ataques ejecutados sobre el sistema y utilizar estos datos para entrenar y evaluar modelos de detección de anomalías, clasificar incidentes de ciberseguridad y aplicar mecanismos de mitigación de amenazas en entornos industriales críticos.

Agradecimientos

Este trabajo ha sido realizado dentro del Proyecto Estratégico del Instituto Nacional de Ciberseguridad, S.A. (INCIBE) " Investigación en Ciberseguridad Industrial en los Sistemas de Automatización y Control de las Subestaciones de Tracción", perteneciente a la convocatoria de Proyectos Estratégicos INCIBE (2020-2023) y financiado por la Unión Europea NextGeneration – EU, en el Plan de Recuperación, Transformación y Resiliencia, a través de INCIBE.

Referencias

Adepu, S., Kandasamy, N. K., Mathur, A., 2019. Epic: An electric power testbed for research and training in cyber physical systems security. In: Computer Security: ESORICS 2018 International Workshops, CyberICPS 2018 and SECPRE 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers 2. Springer, pp. 37–52.

Aftab, M. A., Hussain, S. S., Ali, I., Ustun, T. S., 2020. Iec 61850 based substation automation system: A survey. International Journal of Electrical Power & Energy Systems 120, 106008.

Akbarzadeh, A., Erdodi, L., Houmb, S. H., Soltvedt, T. G., Muggerud, H. K., 2023. Attacking iec 61850 substations by targeting the ptp protocol. Electronics 12 (12).
URL: https://www.mdpi.com/2079-9292/12/12/2596
DOI: 10.3390/electronics12122596

Alghamdi, W., Schukat, M., 2020a. Cyber attacks on precision time protocol networks—a case study. Electronics 9 (9).
URL: https://www.mdpi.com/2079-9292/9/9/1398
DOI: 10.3390/electronics9091398

Alghamdi, W., Schukat, M., 2020b. Practical implementation of apts on ptp time synchronisation networks. In: 2020 31st Irish Signals and Systems Conference (ISSC). pp. 1–5.
DOI: 10.1109/ISSC49989.2020.9180157

Arifin, M. A. S., Stiawan, D., Susanto, Rejito, J., Idris, M. Y., Budiarto, R., 2021. Denial of service attacks detection on scada network iec 60870-5-104 using machine learning. In: 2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI). pp. 228–232.
DOI: 10.23919/EECSI53397.2021.9624255

Baltuille, P., Morán, A., Alonso, S., Prada, M. A., Fuertes, J. J., Domínguez, M., 2024. Design of a testbed for network traffic analysis in iec 61850-based traction substations. Jornadas de Automática 45.
URL: https://doi.org/10.17979/ja-cea.2024.45.10920
DOI: 10.17979/ja-cea.2024.45.10920

Conti, M., Donadel, D., Turrin, F., 2021. A survey on industrial control system testbeds and datasets for security research. IEEE Communications Surveys & Tutorials 23 (4), 2248–2294.

Elgargouri, A., Elmusrati, M., 2017. Analysis of cyber-attacks on iec 61850 networks. In: 2017 IEEE 11th International Conference on Application of Information and Communication Technologies (AICT). pp. 1–4.
DOI: 10.1109/ICAICT.2017.8686894

Gaspar, J., Cruz, T., Lam, C.-T., Simões, P., 2023. Smart substation communications and cybersecurity: A comprehensive survey. IEEE communications surveys & tutorials 25 (4), 2456–2493.
DOI: 10.1109/COMST.2023.3305468

Hussain, S. M. S., Aftab, M. A., Farooq, S. M., Ali, I., Ustun, T. S., Konstantinou, C., 2023. An effective security scheme for attacks on sample value messages in iec 61850 automated substations. IEEE Open Access Journal of Power and Energy 10, 304–315.
DOI: 10.1109/OAJPE.2023.3255790

Kush, N. S., Ahmed, E., Branagan, M., Foo, E., 2014. Poisoned goose: Exploiting the goose protocol. In: Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014)[Conferences in Research and Practice in Information Technology, Volume 149]. Australian Computer Society, pp. 17–22.

Mahlous, A. R., 2024. Quantitative risk analysis of network time protocol (ntp) spoofing attacks. IEEE Access 12, 164891–164910.
DOI: 10.1109/ACCESS.2024.3493759

Malhotra, A., Cohen, I. E., Brakke, E., Goldberg, S., 2015. Attacking the network time protocol. Cryptology ePrint Archive, Paper 2015/1020.
URL: https://eprint.iacr.org/2015/1020
DOI: 10.14722/ndss.2016.23090

Manzoor, F., Khattar, V., Liu, C.-C., Jin, M., 2024. Zero-day attack detection in digital substations using in-context learning. In: 2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). IEEE, pp. 220–225.

Pärssinen, J., Raussi, P., Noponen, S., Opas, M., Salonen, J., 2022. The digital forensics of cyber-attacks at electrical power grid substation. In: 2022 10th International Symposium on Digital Forensics and Security (ISDFS). pp. 1–6.
DOI: 10.1109/ISDFS55398.2022.9800831

Radoglou-Grammatikis, P., Sarigiannidis, P., Giannoulakis, I., Kafetzakis, E., Panaousis, E., 2019. Attacking iec-60870-5-104 scada systems. In: 2019 IEEE World Congress on Services (SERVICES). Vol. 2642-939X. pp. 41–46.
DOI: 10.1109/SERVICES.2019.00022

Roomi, M. M., Hussain, S. M. S., Mashima, D., Chang, E.-C., Ustun, T. S., 2023. Analysis of false data injection attacks against automated control for parallel generators in iec 61850-based smart grid systems. IEEE Systems Journal 17 (3), 4603–4614.
DOI: 10.1109/JSYST.2023.3236951

Rudman, L., Irwin, B., 2015. Characterization and analysis of ntp amplification based ddos attacks. In: 2015 Information Security for South Africa (ISSA). pp. 1–5.
DOI: 10.1109/ISSA.2015.7335069

Sassani, B. A., Abarro, C., Pitton, I., Young, C., Mehdipour, F., 2016. Analysis of ntp drdos attacks' performance effects and mitigation techniques. In: 2016 14th Annual Conference on Privacy, Security and Trust (PST). pp. 421–427.
DOI: 10.1109/PST.2016.7906966

Tasmi, Stiawan, D., Suprapto, B. Y., Setiawan, H., Arifin, M. A. S., 2024. Introduction to goose data communication attack traffic pattern in iec 61850. In: 2024 11th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI). pp. 256–261.
DOI: 10.1109/EECSI63442.2024.10776142

Teryak, H., Albaseer, A., Abdallah, M., Al-Kuwari, S., Qaraqe, M., 2023. Double-edged defense: Thwarting cyber attacks and adversarial machine learning in iec 60870-5-104 smart grids. IEEE Open Journal of the Industrial Electronics Society 4, 629–642.
DOI: 10.1109/OJIES.2023.3336234

Ullmann, M., Vögeler, M., 2009. Delay attacks — implication on ntp and ptp time synchronization. In: 2009 International Symposium on Precision Clock Synchronization for Measurement, Control and Communication. pp. 1–6.
DOI: 10.1109/ISPCS.2009.5340224

Zemanek, S., Hacker, I., Wolsing, K., Wagner, E., Henze, M., Serror, M., 2022. Powerduck: A goose data set of cyberattacks in substations. In: Proceedings of the 15th Workshop on Cyber Security Experimentation and Test. pp. 49–53.