ISSN 0798 1015

REVISTA ESPACIOS

Vol. 41 (Nº 07) Año 2020. Pág. 27

Metodologías de evaluación del riesgo en ciberseguridad aplicadas a sistemas SCADA para compañías eléctricas

Methodologies for cyber security risk assessment applied to SCADA systems for power companies

ROSAS BELLO, Wilmar Andrés 1; MEDINA BECERRA, Fabián Andrés 2 y MESA LARA, Jairo Alonso 3

Recibido: 20/11/2019 • Aprobado: 20/02/2020 • Publicado 05/03/2020

Contenido

1. Introducción
2. Metodología
3. Resultados
4. Conclusiones
Referencias bibliográficas

RESUMEN:
El presente artículo de revisión pretende identificar las principales metodologías de evaluación del riesgo en seguridad aplicadas a sistemas SCADA enfocado a infraestructura crítica, en este caso a compañías eléctricas. De esta forma, se tomaran como prioridad aquellos documentos en los cuales las metodologías sean experimentales preferiblemente con resultados aceptables y aquellas con planteamientos adecuados en los que se espera la implementación y pruebas con buenos resultados.
Palabras clave: Ciberseguridad, SCADA (Control por Supervisión y Adquisición de datos), amenazas, vulnerabilidades

ABSTRACT:
This review article aims to identify the main security risk assessment methodologies applied to SCADA systems focused on critical infrastructure, in this case to electricity companies. In this way, priority will be taken to those documents in which the methodologies are experimental, preferably with acceptable results and those with adequate approaches in which implementation and tests with good results are expected.
Keywords: Cybersecurity, SCADA (Control for Supervision and Data Acquisition), threaths, vulnerabilities

1. Introducción

En la actualidad, la ciberseguridad se ha transformado en un concepto estándar entre las empresas; puesto que la informática es una herramienta de uso habitual en los negocios, y como la información es susceptible a fluctuaciones hace falta tomar medidas de seguridad a niveles de riesgo altos.

El término de ciberseguridad, se le conoce como la seguridad de la tecnología de la información, puesto que engloba un gran número de técnicas y métodos para proteger los sistemas, así como otros dispositivos o las redes de comunicación. Gracias a las herramientas disponibles hoy en día, los sistemas podrán estar más protegidos de los ataques informáticos, hackeos, cualquier robo de datos o identidad. De acuerdo con lo anterior, es importante que para dotar un sistema con las mejores medidas en seguridad, se tenga en cuenta cómo va evolucionando este concepto y siempre estar a la vanguardia para conocer a la perfección las nuevas herramientas que van

apareciendo con el fin de evitar las múltiples amenazas que van surgiendo con el uso de la tecnología.

Por lo tanto, la ciberseguridad tiene como foco la protección de la información digital que "vive" en los sistemas interconectados. En consecuencia, está comprendida dentro de la seguridad de la información.

"Seguridad apunta a una condición ideal, ya que no existe la certeza de que se pueden evitar todos los peligros. Su propósito es reducir el riesgo hasta un nivel aceptable para los interesados" (Mendoza, 2015).

Según Nicholas R. RodoÞle **(**2019) los sistemas de infraestructura crítica basados en SCADA dependen de tecnologías basadas en TI, lo que permite a las empresas de servicios públicos proporcionar infraestructura y servicios esenciales a la sociedad; debido a la dependencia de las infraestructuras críticas en los sistemas basados en TI, los ciberataques que alguna vez se usaron contra los sistemas de TI tradicionales ahora son capaces de atacar la infraestructura crítica . Como resultado, la seguridad cibernética para la infraestructura crítica es una preocupación para los proveedores de servicios públicos. Los servicios de infraestructura crítica incluyen transporte, tratamiento de agua, generación de energía y fabricación. En el pasado, los investigadores se han centrado en ataques aislados en sistemas de control, o en varios tipos de ataques a protocolos de comunicación. Alternativamente, investigaciones anteriores clasificaron los ataques basados en tres partes: hardware, redes y software, lo que proporcionó a la investigación de ciberseguridad un panorama de ataques más amplio.

Los números de incidentes relacionados con sistemas SCADA también crecen de manera constante. Además, un extenso estudio del actual estado de seguridad cibernética de los sistemas SCADA basados en un conjunto de entrevistas con un gran número de expertos confirmó que las amenazas cibernéticas en los sistemas SCADA están aumentando y se encuentran en expansión.

El objetivo del siguiente trabajo consiste en analizar las diferentes metodologías propuesta**s** por diferentes autores, en las cuales, se reconozca el desarrollo metodológico de la ciberseguridad en infraestructura crítica aplicado a sistemas SCADA, de igual forma que se identifiquen las tendencias, las limitaciones y la calidad en la implementación de las metodologías existentes.

2. Metodología

El presente trabajo tiene un enfoque cualitativo, dado que pretende hacer un análisis reflexivo basado en la revisión documental sobre algunas metodologías implementadas en la evaluación del riesgo en ciberseguridad aplicadas a sistemas SCADA para compañías eléctricas.

Dichas metodologías se resumen en los siguientes artículos:

Tabla 1
Lista de los métodos de evaluación del riesgo para los sistemas SCADA ordenados por número de citaciones. (Fuente**:** autores)

No	Referencias	Año	Título del método	País	Citas
4	(Leandros A, Jianmin, & Tiago J, 2016)	2016	Combinando métodos de conjunto y métricas de redes sociales para mejorar la precisión de OCSVM en la detección de intrusos en sistemas SCADA	Portugal	38
6	(Van, Quoc, & Yvon, 2016)	2016	Enfoque SCADA como servicio para la interoperabilidad de plataformas de micro redes.	Francia	33
12	(Shitharth & Prince, 2017)	2017	Un algoritmo mejorado basado en la optimización para la detección de intrusos en la red SCADA	India	20

7	(Massimo & Michał Chora´s, 2017)	2017	Plataforma de simulación para seguridad cibernética y análisis de vulnerabilidad de infraestructuras críticas	Polonia	14
11	(Lily & Po, 2019)	2019	Asegurar las operaciones en el sistema de control industrial basado en la plataforma SCADA-IoT utilizando un conjunto de redes de creencias profundas.	Australia	11
3	(Dong, Huaqun, Jianying, Luying, & Jun, 2018)	2018	SCADAWall: un modelo de firewall habilitado para CPI para la seguridad SCADA	Indonesia	8
1	(Pavel, Valery, evich, Irina Sergeevna, & Aleksey, 2014)	2014	Análisis, clasificación y métodos de detección de ataques a través de redes inalámbricas de sensores en sistemas SCADA	Rusia	7
8	**(**C, Kianoosh G, M, Sunitha, & S.S, 2018).	2018	Esquema clave de pre-distribución con soporte de licencia conjunta para sistemas SCADA	USA	6
5	(Tarek & Latifa, 2017)	2017	Implementación práctica de seguridad incondicional para el protocolo IEC 60780-5-101 SCADA	Algeria	5
9	(kumar, Mohanapriya, & Kalaiselvi, 2014)	2014	Desarrollo de un sistema SCADA resistente a los ataques y seguro utilizando WSN, MANET e Internet	India	5
10	(Lily & Po, 2019)	2019	Análisis de vulnerabilidad de la dinámica en cascada en redes inteligentes bajo ataques de redistribución de carga	China	2
2	(Meir, 2019)	2019	Detección de ciberataques en sistemas SCADA utilizando técnicas de reconocimiento de patrones temporales.	Israel	1

En cuanto al proceso metodológico a realizar se definirá para la construcción del artículo de revisión las siguientes preguntas de investigación:

¿Cuáles son las más destacadas vulnerabilidades de los sistemas SCADA aplicados a infraestructura crítica? ¿Cuáles son las amenazas comúnmente encontradas en sistemas SCADA?

¿Cuáles son las metodologías adecuadas para implementar en compañías eléctricas, teniendo en cuenta las vulnerabilidades? ¿Qué carencias y posibilidades de mejora tiene las actuales metodologías?

2.1. Desarrollo del tema

METODO 1: Análisis, clasificación y métodos de detección de ataques a través de redes inalámbricas de sensores en sistemas SCADA

El objetivo de esta investigación, consiste en analizar el problema al detectar ataques en WSN (redes inalámbricas de sensores) de sistemas SCADA. Como resultado de estudios analíticos, los autores desarrollaron una clasificación de ataques externos en redes de sensores y efectuaron la descripción detallada de los impactos en el ataque de componentes de los sistemas SCADA de acuerdo con las direcciones seleccionadas de estos. Se revisaron los métodos de detección de intrusiones en redes inalámbricas de sensores de sistemas SCADA y funciones de WIDS (intrusión inalámbrica sistemas de detección). Donde se evidencian factores antropogénicos en las amenazas de seguridad interna.

La eficacia de resolver problemas de seguridad de la información de los sistemas APCS y SCADA depende principalmente de la protección de la transmisión de datos a tecnologías aplicadas en el entorno del transporte de componentes (Pavel, Valery, Evich, Irina Sergeevna, & Aleksey, 2014)

Para concluir el estudio, se encontró que a pesar del número de posibles ataques a redes inalámbricas de sensores y sistemas SCADA, los más peligrosos son las amenazas antropogénicas internas a la seguridad de la información, que incluirían acciones no intencionales del personal que crean las condiciones propicias para ataques externos de piratas informáticos, ignorar intencionalmente los requisitos de seguridad de la información por parte del personal que sirve al sistema SCADA y la falta de calificación del personal en el campo de las tecnologías de la información y la implementación de métodos de seguridad de la información.

METODO 2: Detección de ciberataques en sistemas SCADA utilizando técnicas de reconocimiento de patrones temporales.

En el presente artículo, se proponen técnicas de detección de ciberataques basadas en el reconocimiento de patrones temporales. Los métodos de reconocimiento de patrones temporales no solo buscan anomalías en los datos transferidos por los componentes SCADA a través de la red, sino que también buscan anomalías que pueden ocurrir al usar incorrectamente comandos legítimos, de modo que los intervalos de tiempo no autorizados e incorrectos entre ellos pueden paralizar el sistema. Específicamente, lo que propone el autor son dos algoritmos basados en modelos ocultos de Markov (HMM), una poderosa herramienta estadística que permite modelar un sistema y hacer predicciones sobre su estado futuro basándose únicamente en su estado actual. Las particularidades deben extraerse para el modelo de aprendizaje, y se formulan varios métodos de extracción de características que tienen en cuenta el orden de las operaciones y el tiempo entre ellas. El siguiente algoritmo consiste en redes neuronales artificiales (ANN) que pueden lograr un aprendizaje no supervisado basado en el enfoque ANN. Se Evaluaron los algoritmos en datos SCADA reales y simulados con cinco métodos de extracción de características diferentes; en cada método, los algoritmos consideran diferentes aspectos de los datos sin procesar los cuales consisten en (1) vector de función, (2) tiempo desde la última operación, (3) tiempo desde la última operación similar, (4) una combinación del código de función y el tiempo desde la última operación, y (5) una combinación de código de función y el tiempo desde la última operación similar.

Los resultados demostraron que los métodos de reconocimiento de patrones temporales, especialmente aquellos basados en la extracción de características de tiempo, pueden detectar ataques cibernéticos, incluidos aquellos que involucran funciones legítimas, que en la literatura se reconocen como difíciles de detectar. (Meir, 2019)

Para concluir el estudio, específicamente se demostró que el método de extracción de características es más simple, que solo considera el tiempo de duración entre las funciones posteriores, el cual produce el modelo más preciso. Este hallazgo puede explicarse por el tipo de ataque abordado en este documento. El orden de las operaciones permanece estable, pero el tiempo de duración entre las operaciones cambia; se cree que los algoritmos pueden ser una buena solución para detectar ataques en sistemas SCADA, particularmente a la luz del hecho de que los sistemas SCADA tienden a ser menos dinámicos que los sistemas de TI.

METODO 3: SCADAWall: un modelo de firewall habilitado para CPI para la seguridad SCADA

Según (Dong, Huaqun, Jianying, Luying, & Jun, 2018) muchos cortafuegos han estado ampliando sus capacidades de seguridad para admitir los sistemas de control de supervisión y adquisición de

datos (SCADA) o para proteger las operaciones dentro del control de procesos industriales. Un firewall SCADA generalmente necesita inspeccionar más profundamente la carga útil para comprender exactamente qué aplicaciones industriales detalladas se están ejecutando.

Sin embargo, las características de seguridad en los firewalls SCADA tradicionales tienen inconvenientes en dos aspectos principales. Primero, un firewall SCADA tradicional de inspección profunda de paquetes (DPI) solo inspecciona parcialmente el contenido de una carga útil. Los paquetes especialmente diseñados que llevan una carga maliciosa pueden explotar, este inconveniente puede evitar la inspección del firewall. En segundo lugar, los firewalls SCADA existentes tienen poca capacidad para proteger los protocolos industriales patentados.

En el presente documento, se propone un nuevo modelo de firewall SCADA llamado SCADAWall que tiene como objetivo inspeccionar los comandos SCADA y evitar ataques más inteligentes a través de tres algoritmos detallados. Este modelo funciona con una tecnología de inspección integral de paquetes (CPI). SCADAWall también incluye un nuevo Algoritmo de Extensión de Protocolos Industriales Propietarios (PIPEA) para extender las capacidades a la protección de protocolos industriales patentados, y un Algoritmo de Detección de Fuera de Secuencia (OSDA) para detectar anormalidades dentro de las operaciones industriales. Se ha comparado las características de seguridad con dos firewalls comerciales SCADA, que incluyen FW1 (dispositivo de seguridad de xenón Belden Tofino) (Byres, Eric. (2012) seguridad de Tofino) y FW2 (dispositivo Checkpoint 1200R) (dispositivo resistente Checkpoint 1200R). Ambos están diseñados para proteger múltiples protocolos industriales estandarizados a través de la tecnología DPI. Este trabajo también muestra que SCADAWall puede mitigar efectivamente esos inconvenientes sin sacrificar el requisito de baja latencia del sistema SCADA.

Para concluir el estudio se encontró que los resultados de evaluación del desempeño, muestran que el prototipo de CPI puede mantener la comunicación en tiempo real sin sacrificar el desempeño de la red. En el trabajo futuro, SCADAWall tiene el potencial de lograr más características de seguridad, como prevenir estados críticos o anomalías debido a preocupaciones de seguridad.

METODO 4: Combinando métodos de conjunto y métricas de redes sociales para mejorar la precisión de OCSVM en la detección de intrusos en sistemas SCADA.

De acuerdo con (Leandros A, Jianmin, & Tiago J, 2016) los sistemas SCADA son grandes, complejos e incorporan un número creciente de componentes ampliamente distribuidos. La presencia de un mecanismo de detección de intrusos en tiempo real, que puede hacer frente a diferentes tipos de ataques, es de gran importancia para defender un sistema contra los ciberataques.

Este mecanismo de defensa debe ser distribuido, barato y sobre todo preciso, puesto que las falsas alarmas positivas o los errores con respecto al origen de la intrusión significan costos severos para el sistema. Recientemente se propuso un mecanismo de detección integrado, a saber, IT-OCSVM, que se distribuye en una red SCADA como parte de un sistema de detección de intrusos distribuidos (DIDS), que proporciona datos precisos sobre el origen y el momento de una intrusión.

En este documento se analiza la arquitectura del mecanismo de detección integrado y se realizan simulaciones extensas basadas en ciberataques reales en un pequeño banco de pruebas SCADA para evaluar el rendimiento del mecanismo propuesto.

Se concluye que el mecanismo de detección, que se ejecuta de forma distribuida, se puede utilizar en grandes redes SCADA sin modificaciones adicionales. La combinación de métricas de análisis de redes sociales con técnicas de clasificación de aprendizaje automático mejora el rendimiento del mecanismo de detección y la precisión para todos los escenarios de simulación investigados.

METODO 5: Implementación práctica de seguridad incondicional para el protocolo IEC 60780-5-101 SCADA

Los sistemas SCADA se utilizan en la infraestructura crítica para monitorear y controlar procesos industriales vitales. Los firewalls tradicionales, los mecanismos de autenticación y los algoritmos y protocolos criptográficos son inadecuados para proteger los sistemas SCADA y los procesos industriales subyacentes de los ataques cibernéticos.

Este artículo describe un enfoque novedoso para proporcionar un alto nivel de seguridad para el protocolo IEC 60870-5-101, un protocolo de comunicaciones SCADA abierto no enrutable utilizado en la industria de la energía eléctrica. El enfoque propuesto incorpora una capa secreta entre las capas físicas y de enlace de la arquitectura de rendimiento mejorada del protocolo IEC 60870-5-

101. La capa secreta es una implementación de la noción de Shannon de un sistema incondicionalmente seguro en el que se aprovecha la autenticidad, integridad y confidencialidad de la transmisión de datos SCADA.

Los resultados experimentales que utilizan un banco de pruebas de control industrial confirman que el enfoque propuesto satisface las restricciones temporales impuestas a los sistemas SCADA utilizados en subestaciones eléctricas. (Tarek & Latifa, 2017)

Para proporcionar un alto nivel de secreto a IEC-60870-5-101 basado en comunicaciones del sistema SCADA, esta investigación introduce una capa secreta entre la capa física y la capa de enlace de datos. En la capa secreta, las tramas de longitud variable se cifran para ocultar toda la información transmitida. Este enfoque garantiza la autenticidad del equipo y la integridad de los datos, y protege el sistema de ataques pasivos, así como de ataques de modificación y fabricación, como ataques de búsqueda de fuerza bruta, ataques de repetición, ataques antropogénicos en el medio y falsos ataques al servidor. Además, para garantizar un funcionamiento fluido del sistema SCADA con un alto nivel de seguridad, el enfoque no realiza ajustes en la capa física ni realiza cambios importantes en el tamaño óptimo del marco y las estructuras de la unidad de datos del servicio de aplicaciones.

Se concluye mediante los resultados experimentales, donde se utilizaron un banco de pruebas de control industrial que la solución IEC 60870-5-101 propuestas, satisface las restricciones temporales impuestas a los sistemas SCADA utilizados en subestaciones eléctricas. Específicamente, la solución no afecta las operaciones en tiempo real, especialmente cuando la implementación está bien optimizada.

METODO 6: Enfoque SCADA como servicio para la interoperabilidad de plataformas de micro redes.

Según (Van, Quoc, & Yvon, 2016), en el contexto del desarrollo de redes inteligentes, este documento considera el problema de la interoperabilidad de las plataformas de micro redes, particularmente entre las instituciones de investigación. Se introducen varios niveles de interoperabilidad con los requisitos respectivos. El objetivo principal del documento es proponer una arquitectura SCADA privada basada en la nube híbrida adecuada satisfaciendo diversas necesidades en el marco de la interoperabilidad de las plataformas de micro red mientras se mantienen las condiciones de restricción de seguridad.

La interoperabilidad entre las micro-redes permitirá a las instituciones de investigación intercambiar información significativa, obtener acceso al grupo de recursos compartidos y eventualmente, local o remotamente tomar prestada la infraestructura asociada para actividades de investigación.

El modelo de entrega de PaaS permite a los usuarios implementar las aplicaciones, pero no les permite a los usuarios obtener el control total de la infraestructura subyacente ni acceder a datos restringidos. El modelo de entrega SaaS, en otro nivel superior de seguridad, permite a los usuarios utilizar las aplicaciones que se ejecutan en la infraestructura, a través de una interfaz de cliente, como un navegador web. El operador, sin embargo, tiene control total sobre la infraestructura.

Para con concluir, en el contexto de un fuerte desarrollo en la red inteligente, este documento considera el problema de la interoperabilidad de las plataformas de micro red, particularmente entre las infraestructuras de investigación e industriales. Como cada vez hay más proyectos y plataformas SG, la necesidad de colaboración e intercambio de información entre las instituciones de investigación e industriales aparece de forma natural. Conduce a la necesidad de interoperabilidad entre sus infraestructuras, especialmente las plataformas de micro-red.

METODO 7: Plataforma de simulación para seguridad cibernética y análisis de vulnerabilidad de infraestructuras críticas

De acuerdo con (Massimo & Michał Chora´s, 2017) los progresivos avances en la tecnología de la información y la comunicación han prestado infraestructuras críticas modernas para volverse cada vez más complejas e interconectadas, y en continua evolución. La creciente interrelación compleja entre estos sistemas críticos crea nuevas vulnerabilidades de seguridad, que pueden ser explotadas por usuarios malintencionados para comprometer datos sensibles y otros sistemas también muy lejos de la zona de impacto.

En escenarios reales de delitos cibernéticos, los adversarios usan un conjunto de vulnerabilidades para entrar en una red. Esto también se expresa como un "encadenamiento de vulnerabilidad", que es una técnica muy importante adaptada en el proceso de violación de la seguridad de los

sistemas de TI. En este documento, se considera un caso de uso hipotético (aunque realista, en desarrollo), donde se hace uso los resultados del escenario de pruebas de penetración para proporcionar un análisis detallado del riesgo de seguridad cibernética. Esta idea amplía la investigación previa con respecto a la implementación en el entorno habilitado para HLA.

Para concluir se ha presentado una plataforma de simulación de ciberseguridad para respaldar el análisis de vulnerabilidades de sistemas críticos. En particular, se adaptó una solución basada en HLA para la simulación híbrida compleja y distribuida. A La solución propuesta se puede utilizar para realizar pruebas de penetración y análisis de seguridad de aplicaciones de red complejas a gran escala, en particular para infraestructuras críticas, como redes de energía complejas.

METODO 8: Esquema clave de pre-distribución con soporte de licencia conjunta para sistemas SCADA

De acuerdo con el presente artículo, los sistemas de control de supervisión y adquisición de datos (SCADA) se utilizan en las principales industrias para lograr mayores niveles de eficiencia, seguridad y calidad. Debido a los ataques de seguridad masivos, asegurar dichos sistemas es un problema crítico. Para asegurar las comunicaciones de los sistemas SCADA, se observa que los esquemas clave de pre-distribución son más adecuados.

En este documento, se propone un esquema de pre-distribución de claves basado en matriz para sistemas SCADA. El esquema admite operaciones de actualización de combinación, salida y clave del dispositivo con un menor costo de comunicación. Además, el esquema de distribución previo clave propuesto admite la transmisión segura, la transmisión múltiple y las comunicaciones unicast entre los sistemas SCADA.

En este enfoque, las claves secretas no se transmiten a través de la red para manejar las operaciones, como la actualización de claves, unirse y salir. Alternativamente, cada dispositivo calcula localmente las claves requeridas, una vez que se implementan en la red. Sin embargo, en estas situaciones en las que el dispositivo compromete o admite el secreto de reenvío, las claves auxiliares y de grupo se cifran y se envían a los dispositivos requeridos. (C, Kianoosh G, M, Sunitha, & S.S, 2018).

El esquema propuesto utiliza una matriz para abordar los desafíos clave de pre-distribución. La matriz está diseñada de tal manera que ofrece un llavero para los dispositivos en la red, los nuevos dispositivos pueden unirse a la red sin modificar la matriz existente. Después de realizar operaciones de unión y salida, los cambios en la matriz se pueden rastrear de manera efectiva, lo que ayuda al KDC a identificar los dispositivos recién unidos, los dispositivos desalojados y el número total de dispositivos en cualquier grupo.

El uso de la propiedad de multiplicación escalar en la matriz permite la función de actualización clave. En las operaciones de unión y actualización de claves, nuestra intención es calcular localmente las claves requeridas y reducir las posibilidades de exposición de claves secretas.

La evaluación de desempeño muestra que el esquema propuesto satisface los requisitos de desempeño del sistema SCADA. El resultado de las pruebas de protocolo verifica la efectividad del esquema propuesto. Comparamos nuestro esquema propuesto con los existentes para resaltar sus beneficios.

Para concluir la matriz propuesta admite operaciones de unión de dispositivos, abandono de dispositivos y actualización clave con un bajo costo de comunicación. El esquema permite comunicaciones seguras por pares, funciones de difusión y multidifusión. Las claves secretas no se transfieren a través de la red para manejar operaciones como la actualización de claves, unirse y salir, y así mitigar los ataques de exposición clave. Si el adversario es capaz de capturar todos los datos de comunicación entre los dispositivos, no podrá comprometer los dispositivos ni calcular la clave secreta utilizada para cifrar los mensajes. El análisis de seguridad de los protocolos de unión y abandono propuestos, la prueba de protocolos utilizando la herramienta Scyther y la comparación del esquema propuesto con los esquemas de pre-distribución y gestión de claves existentes resaltan la eficiencia del esquema propuesto.

METODO 9: Desarrollo de un sistema SCADA resistente a los ataques y seguro utilizando WSN, MANET e Internet.

Según (kumar, Mohanapriya, & Kalaiselvi, 2014) algunos de los sistemas comunes SCADA (Control de supervisión y adquisición de datos) involucran sistemas de distribución de energía y agua. En este documento, se considera el sistema SCADA de distribución de energía que comprende varias subestaciones. Se propone un marco seguro que combina el sistema de control de energía con redes inalámbricas de sensores (WSN), redes móviles ad hoc (MANET) e Internet,

proporcionando prevención de anomalías y gestión de estado. Los ataques SCADA ocurren en los estimadores de estado de los sistemas de energía que se utilizan para enrutar los flujos de energía y detectar dispositivos defectuosos. Los estimadores están ubicados en el centro de control SCADA, que es un área sensible y las mediciones deben transmitirse a través de un canal de comunicación seguro.

La resistencia al ataque del sistema SCADA se mejora al aumentar la dureza y la complejidad del problema del ataque.

El impacto de ataque de la subestación es una métrica que relaciona el recuento en el que un atacante obtiene acceso a una subestación y realiza un ataque sigiloso. Menor es el impacto del ataque, mayor sería la protección del sistema SCADA. El impacto de ataque normalizado máximo se evalúa con respecto a cuatro recuentos variables, a saber, rutas únicas alteradas, rutas múltiples, RTU autenticadas a prueba de manipulaciones y RTU autenticadas a prueba de manipulaciones.

En conclusión las infraestructuras críticas (CI) como los sistemas SCADA son importantes debido a su enorme área de cobertura a nivel nacional. Una falla o ataque a estos sistemas da como resultado cambios drásticos en la distribución del servicio.

Estos efectos también pueden ser graves o en cascada y provocar la interrupción de otros servicios esenciales. El sistema SCADA resistente a los ataques y seguridad (ARS) se evalúa contra las técnicas existentes como NAMDIA (Mitigación de ataques de integridad de datos basada en la red), Retrofit IDS (Sistema de detección de intrusiones) y CSBF (Filtro crítico basado en estado) para mejorar el ataque-resistencia y seguridad de los sistemas SCADA. Se encuentra que el rendimiento del sistema ARS SCADA es bueno en comparación con los métodos existentes en términos de impacto y latencia de ataque normalizados máximos.

METODO 10: Análisis de vulnerabilidad de la dinámica en cascada en redes inteligentes bajo ataques de redistribución de carga

Las redes inteligentes integran la ingeniería de sistemas de energía con tecnología de información y comunicación para formar un sistema complejo. En este estudio, se propone un marco para modelar la red inteligente como redes complejas interdependientes e investigar las vulnerabilidades de las topologías sujetas a ataques dirigidos. (Lily & Po, 2019)

Basado en las características particulares de los sistemas de energía, los componentes requieren alcanzar un equilibrio de poder a través de la redistribución o desprendimiento de cargas en cada ataque. En comparación con la eliminación aleatoria y la eliminación de bloques, la efectividad de la estrategia propuesta se validó en el bus IEEE 39 y en la red troncal provincial real. A partir del análisis de los resultados experimentales, encontramos que la vulnerabilidad de la topología está estrechamente relacionada con los tipos y ubicaciones de nodos críticos.

Las vulnerabilidades y limitaciones de los parámetros de configuración. Con base en el análisis estadístico de las propiedades complejas de la red, los sistemas de energía se pueden modelar como redes aleatorias o de mundo pequeño, mientras que las redes de comunicación se pueden modelar como redes sin escala. Desde una perspectiva compleja de la teoría del sistema, las redes dependen de varias propiedades topológicas vulnerables, como la distribución de grados, la longitud promedio de la ruta y la eficiencia. Basado en las características topológicas y sistemáticas de las redes inteligentes, los ataques a nodos críticos aceleran rápidamente la dinámica en cascada, lo que resulta en daños devastadores.

En comparación con los métodos existentes, las principales contribuciones de este estudio son los siguientes:

(1) Las redes inteligentes se modelan como gráficos híbridos interdependientes con enlaces de soporte de múltiples a múltiples, en términos del complejo sistema y de la teoría de la percolación.

(2) La dinámica en cascada se desencadena por ataques secuenciales de nodos críticos según la estrategia de inyección de datos falsos.

Según el análisis del método, los diferentes tipos de nodos afectan la topología en diversos niveles. Podemos concluir tres tipos de nodos según sus influencias. En primer lugar, el nodo raíz en forma de árbol con una gran cantidad de nodos es el tipo más vulnerable, que es el objetivo de ataque principal. Es el tipo más crítico y vulnerable en la topología, y se le debe proporcionar una protección mejorada. El nodo raíz en forma de línea larga es un caso especial del nodo raíz en forma de árbol. En segundo lugar, el nodo ubicado en la posición crítica en un solo bucle puede no tener muchas conexiones.

Para concluir, las redes inteligentes es un sistema complejo interdependiente entre una red eléctrica y red de comunicación. Es vulnerable a los objetivos de los ciberataques, particularmente el ataque de inyección de datos falsos que puede dañar el objetivo deseado y desencadenar LR sin sospechar. La teoría de redes complejas se ha introducido para estudiar la complejidad de la topología y los efectos de las fallas en cascada. De acuerdo con la estrategia de ataque, el ataque secuencial basado en la importancia del nodo y la ubicación colapsa todo el sistema de energía paso a paso. Durante este proceso en cascada, la eliminación de diferentes tipos de nodos daña la topología en diversos niveles de destrucción.

METODO 11: Asegurar las operaciones en el sistema de control industrial basado en la plataforma SCADA-IoT utilizando un conjunto de redes de creencias profundas.

Otro de los métodos que se analizaron consiste en la plataforma de Internet (IoT) se usa cada vez más en las industrias modernas. Miles de millones de dispositivos son capacidades de detección inteligente como PLCs, actuadores, dispositivos electrónicos inteligentes (IED) de sistemas de control industrial (ICS) y control de supervisión y red de adquisición de datos (SCADA) están conectados a través de la plataforma IoT. La plataforma IoT (Internet de las cosas) ha facilitado a las industrias modernas un monitoreo y control eficiente de los sistemas físicos (hardware y maquinarias) que resulta en una adquisición inteligente de datos, procesamiento y administración de negocios altamente productiva y rentable. Inicialmente, estos dispositivos se han implementado sin ningún problema de seguridad, puesto que se ejecutarán en redes aisladas. (Shamsul, John, Mohammed, & Ahmad, 2018)

Por lo tanto, los dispositivos de una red SCADA se enfrentan a una amenaza significativa de ataques maliciosos a través de las vulnerabilidades de la red corporativa o los dispositivos utilizados en SCADA.

De acuerdo con los autores, la arquitectura propuesta para ICS se ha verificado utilizando datos de red SCADA reales. Los resultados experimentales muestran que el sistema de detección basado en conjuntos supera a los motores de detección de ataques existentes.

Un atacante modifica el paquete de manera que oculta los estados reales de los dispositivos y los sistemas físicos. Esto se puede hacer de muchas maneras, incluido el envío de la misma lectura del sensor a la MTU para engañar al operador sobre una situación real del sistema físico. Los otros tipos pueden ser una simulación del sistema para una condición de falla y estimar las mediciones para una situación de falla. Luego modifica las lecturas en el paquete con el valor estimado para inducir al operador a error sucedió Esto requiere un conocimiento completo del sistema que se puede lograr mediante un ataque de reconocimiento.

Como conclusión se analiza que las industrias modernas utilizan tremendamente la plataforma IoT y conectan numerosos sensores inteligentes, IED (compatibilidad de IoT de banda estrecha) con su red SCADA para un control centralizado y una mejor gestión en conjunto con la computación en la nube. Esto no solo mejora la optimización de la producción para superar los desafíos de la situación dinámica del mercado, sino que también ayuda a monitorear y responder a la situación de seguridad de una manera mejorada. Los dispositivos archivados de los sistemas de control industrial (ICS), PLC, IED y protocolos relacionados se diseñaron inicialmente para operar en redes aisladas en las que se ignoraban los problemas relacionados con la seguridad y las amenazas. Sin embargo, su integración con la plataforma IoT e Internet expone a los ICS a importantes amenazas de seguridad.

METODO 12: Un algoritmo mejorado basado en la optimización para la detección de intrusos en la red SCADA

De acuerdo con (Shitharth & Prince, 2017) identificar y detectar intrusiones en un SCADA es una tarea crítica y exigente en los últimos días. Para este propósito, se desarrollan varios sistemas de detección de intrusiones (IDS) en los trabajos existentes. Sin embargo, tiene algunos inconvenientes, que incluyen altas tasas de falsos positivos y falsos negativos, no puede detectar la fecha cifrada y solo es compatible para detectar las intrusiones externas.

En este documento se proponen técnicas de optimización de búsqueda (IWP-CSO) y de red neuronal basada en la arquitectura neuronal jerárquica (HNA-NN). La intención principal de este documento es detectar y clasificar las intrusiones en una red SCADA basada en la optimización. Al principio, en la red de entrada se proporciona un conjunto de datos, donde se ordenan los atributos y se inicializan los clústeres. Luego, las características se optimizan para seleccionar los mejores atributos utilizando el algoritmo IWP-CSO propuesto. Finalmente, las intrusiones en una red se clasifican empleando el algoritmo HNA-AA propuesto. Los resultados experimentales

evalúan el rendimiento del sistema propuesto en términos de sensibilidad, especificidad, precisión, recuerdo, exactitud y tasa de detección falsa.

En este trabajo, hay más cantidad de atributos que se utilizan para formar la estructura SCADA. Por lo tanto, es necesario identificar si los atributos están agrupados o no. Si está agrupado, se pueden obtener resultados precisos; de lo contrario, conduce a la tasa de clasificación errónea. Para encontrar las variaciones entre las etiquetas normales y de ataque, la función de costo se estima en función del conjunto de características. Además, la probabilidad de partículas se estima a partir del valor del peso. Entonces, el valor de aptitud se calcula para encontrar el rango de probabilidad de ataque y no ataque.

Para concluir este artículo presenta un algoritmo IWP-CSO y HNA-NN mejorado para detectar las intrusiones en una red SCADA. La principal contribución de los documentos es aplicar el marco de optimización adecuado con la combinación de búsqueda y red neuronal para reducir la dimensión de las características que mejorarán la precisión de manera efectiva. Luego, los mejores atributos seleccionados se clasifican utilizando la técnica de clasificación HNA-NN, que predice la etiqueta del atacante y el no atacante.

3. Resultados

3.1. Discusión

De acuerdo con la información recopilada y los análisis de los diferentes métodos, se puede argumentar, que todas las investigaciones efectuadas por los diferentes estudios buscan como principal objetivo, determinar que el método aplicado en diversas situaciones es el indicado para la seguridad de datos informáticos y que adicionalmente fortalecen a los sistemas SCADA.

Tabla 2
Resumen de los métodos de evaluación del riesgo

Referencias	Dominio	Objetivo	Evaluación
(Pavel, Valery, evich, Irina Sergeevna, & Aleksey, 2014)	Sensores inalambricos	El objetivo de esta investigación, consiste en analizar el problema al detectar ataques en WSN (redes inalámbricas de sensores) de sistemas SCADA.	No
(Meir, 2019)	técnicas de detección de ciberataques basadas en el reconocimiento de patrones temporales	Lo que propone el autor son dos algoritmos basados en modelos ocultos de Markov (HMM)	Se Evaluaron los algoritmos en datos SCADA reales y simulados con cinco métodos de extracción de características diferentes; en cada método,
(Dong, Huaqun, Jianying, Luying, & Jun, 2018)	modelo de firewall habilitado para CPI	Objetivo inspeccionar los comandos SCADA y evitar ataques más inteligentes a través de tres algoritmos detallados.	Se encontró que los resultados de evaluación del desempeño, muestran que el prototipo de CPI puede mantener la comunicación en tiempo real sin sacrificar el desempeño de la red. En el trabajo futuro, SCADAWall tiene el potencial de lograr más características de seguridad, como prevenir estados críticos o anomalías debido a preocupaciones de seguridad.

(Leandros A, Jianmin, & Tiago J, 2016)	Redes sociales	Se analiza la arquitectura del mecanismo de detección integrado y se realizan simulaciones extensas basadas en ciberataques reales en un pequeño banco de pruebas SCADA para evaluar el rendimiento del mecanismo propuesto.	El mecanismo de detección, que se ejecuta de forma distribuida, se puede utilizar en grandes redes SCADA sin modificaciones adicionales.
(Tarek & Latifa, 2017)	Sub-estaciones eléctricas	Un enfoque novedoso para proporcionar un alto nivel de seguridad para el protocolo IEC 60870-5-101,	Mediante los resultados experimentales, donde se utilizaron un banco de pruebas de control industrial que la solución IEC 60870-5-101 propuestas, satisface las restricciones temporales impuestas a los sistemas SCADA utilizados en subestaciones eléctricas.
(Van, Quoc, & Yvon, 2016)	interoperabilidad de las plataformas de micro redes	El objetivo principal del documento es proponer una arquitectura SCADA privada basada en la nube híbrida adecuada satisfaciendo diversas necesidades en el marco de la interoperabilidad de las plataformas de micro red mientras se mantienen las condiciones de restricción de seguridad.	En particular, se adaptó una solución basada en HLA para la simulación híbrida compleja y distribuida.
(Massimo & Michał Chora´s, 2017)	Seguridad cibernética	En este documento, se ha presentado una plataforma de simulación de ciberseguridad para respaldar el análisis de vulnerabilidades de sistemas críticos.	No se efectuó
(C, Kianoosh G, M, Sunitha, & S.S, 2018).	Principales industrias para lograr mayores niveles de eficiencia, seguridad y calidad.	En este documento, proponemos un esquema de pre-distribución de claves basado en matriz para sistemas SCADA.	La evaluación de desempeño muestra que el esquema propuesto satisface los requisitos de desempeño del sistema SCADA. El resultado de las pruebas de protocolo verifica la efectividad del esquema propuesto. Comparamos nuestro esquema propuesto con los existentes para resaltar sus beneficios.

(kumar, Mohanapriya, & Kalaiselvi, 2014)	Distribución de energía que comprende varias subestaciones.	Los ataques SCADA ocurren en los estimadores de estado de los sistemas de energía que se utilizan para enrutar los flujos de energía y detectar dispositivos defectuosos.	Se encuentra que el rendimiento del sistema ARS SCADA es bueno en comparación con los métodos existentes en términos de impacto y latencia de ataque normalizados máximos.
(Lily & Po, 2019)	redes inteligentes bajo ataques de redistribución de carga	Se propone un marco para modelar la red inteligente como redes complejas interdependientes e investigar las vulnerabilidades de topología sujetas a ataques dirigidos.	De acuerdo con la estrategia de ataque, en la evaluación del ataque secuencial basado en la importancia del nodo y la ubicación colapsa todo el sistema de energía paso a paso.
(Shamsul, John, Mohammed, & Ahmad, 2018)	dispositivos con capacidades de detección inteligente	Asegurar las operaciones en el sistema de control industrial basado en la plataforma SCADA-IoT utilizando un conjunto de redes de creencias profundas.	Los resultados experimentales muestran que el sistema de detección basado en conjuntos supera a los motores de detección de ataques existentes.
(Shitharth & Prince, 2017)	Algoritmo mejorado	La intención principal de este documento es detectar y clasificar las intrusiones en una red SCADA basada en la optimización.	Los resultados experimentales evalúan el rendimiento del sistema propuesto en términos de sensibilidad, especificidad, precisión, recuerdo, exactitud, Jaccard, dados y tasa de detección falsa.

Fuente, autores

Las vulnerabilidades más destacadas, según diversos autores hacen referencia a infiltraciones de intrusos por diversos medios, a través de explotación de vulnerabilidades de software que prevalecen en los sistemas SCADA. Además, son principales problemas para la arquitectura y para las propiedades topológicas de los sistemas el sabotaje, incluyendo la interrupción de los servicios o la posibilidad de desencadenar situaciones peligrosas dentro del sistema.

Se plantea que los métodos adecuados para implementar en compañías eléctricas, teniendo en cuenta las vulnerabilidades son aquellas cuyos patrones temporales sean aquellos basados en la extracción de características de tiempo; de igual forma la metodología que involucra al IEC 60870-5-101 satisface las restricciones temporales impuestas a los sistemas SCADA utilizados en subestaciones eléctricas, esta tecnología no afecta las operaciones en tiempo real.

Las principales carencias de las metodologías estudiadas se resumen en la dependencia de las plataformas y servicios basados en la internet, sin que exista la suficiente tecnología para detectar los riesgos y amenazas latentes que van surgiendo a medida que avanza la tecnología, muchas metodologías se basan en protocolos los cuales deben ser evaluados y puestos a investigación para su implementación por ende no trabajan en tiempo real y su aplicabilidad es muy limitada.

4. Conclusiones

Los métodos analizados en ocasiones son una combinación de procesos industriales que se analizan en algunos casos en tiempo real, muchos de estos son técnicas muy complejas y como

resultado pueden ser dispendiosas para su aplicación inmediata.

No existe una forma exacta para mantener los sistemas asegurados, tampoco una normatividad, ni componentes tecnológicos que garanticen que no habrá problemas a futuro. Por esta razón se deben considerar cada uno de los factores internos (vulnerabilidades) y factores externos (amenazas o ataques) que pueden afectar la seguridad de una organización específica.

Debido a que los sistemas SCADA se utilizan en la infraestructura crítica para monitorear y controlar procesos industriales vitales se deben implementar tecnología que se actualice constantemente con el fin de mejorar la protección de dichos sistemas debido a que los mecanismos tradicionales de autenticación, los algoritmos y los protocolos criptográficos son inadecuados para proteger los sistemas SCADA y los procesos industriales subyacentes de los ataques cibernéticos.

En Colombia se podrían implementar estos sistemas debido a las ventajas que ya se han venido tratando, además, la inversión para este tipo de métodos no representaría una pérdida sino una inversión garantizando niveles óptimos de seguridad en infraestructuras criticas principalmente en plantas o compañías eléctricas.

Referencias bibliográficas

C, P. T., Kianoosh G, B., M, H. A., Sunitha, N., & S.S, I. (2018). Key pre-distribution scheme with join leave support for SCADA systems. *international journal of critical infrastructure protection*, 111-125.

Dong, L., Huaqun, G., Jianying, Z., Luying, Z., & Jun, W. W. (2018). SCADAWall: A CPI-enabled firewall model for SCADA security. *computers & security*, 134-154.

kumar, N. R., Mohanapriya, P., & Kalaiselvi, M. (2014). Development of an Attack-Resistant and Secure SCADA System using WSN,MANET, and Internet. *International Journal of Advanced Computer Research*, 627-633.

Leandros A, M., Jianmin, J., & Tiago J, C. (2016). Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems. *journal of information security and applications*, 1-12.

Lily, L., & Po, H. (2019). Vulnerability analysis of cascading dynamics in smart grids under load redistribution attacks. *Electrical Power and Energy Systems*, 182-190.

Massimo, F., & Michał Chora´s, R. K. (2017). Simulation Platform for Cyber-Security and Vulnerability Analysis of Critical Infrastructures. *Journal of Computational Science*, 1-26.

Meir, K. (2019). Cyber-Attack Detection in SCADA Systems using Temporal Pattern. *Computers & Security*, 1-13.

Mendoza, M. A. (16 de Junio de 2015). *welivesecurity.* Obtenido de https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

Nicholas R. RodoÞle, K. R. (2019). Extending the Cyber-Attack Landscape for SCADA-based Critical Infrastructure. *International Journal of Critical Infrastructure Protection*, 2-3.

Pavel, V. B., Valery, A., evich, K., Irina Sergeevna, N., & Aleksey, G. (2014). Analysis, classification and detection methods of attacks via wireless sensor networks in SCADA systems. *Life Science Journal*, 384-388.

Shamsul, H., John, Y., Mohammed, M. H., & Ahmad, A. (2018). Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks. *Applied Soft Computing*, 1-31.

Shitharth, & Prince, W. (2017). An enhanced optimization based algorithm for intrusion detection in SCADA network. *computers & s e c u r i t y*, 16-26.

Tarek, C., & Latifa, H. (2017). A practical implementation of unconditional security for the IEC 60780-5-101 SCADA protocol. *International Journal of Critical Infrastructure Protection*, 1-32.

Van, H. N., Quoc, T. T., & Yvon, B. (2016). SCADA as a service approach for interoperability of micro-grid. *Sustainable Energy, Grids and Networks*, 1-14.

United States Government Accountability Office, Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems, Report to Congressional Requesters, March 2004,http://www.gao.gov/new.items/d04354.pdf.

United Stateds Government Accountability Office (GAO), Department of Homeland Securitys (DHSs) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO-05-434 (Washington, D.C.: May, 2005).

Kevin S. Killourhy, Roy A. Maxion and Kymie M. C. Tan (2004),A Defense-Centric Taxonomy Based on Attack Manifestations, Proceedings of International Conference on Dependable Systems & Networks: Florence, Italy

Nicolas Falliere, Liam O Murchu, and Eric Chien, (2011) W32. Stuxnet Dossier , Symantec Security Response, Version 1.4, http://www.symantec.com/content/en/us/enterprise/media/security response/whitepapers/w32 stuxnet dossier.pdf

Network using ant colony clustering approach and unsupervised feature extraction, in: IEEE International Conference on Industrial Technology, 2005, ICIT 2005, IEEE, 2005, pp. 51–56.

Linda O., T. Vollmer, M. Manic, Neural (2009) network based intrusion detection system for critical infrastructures, in: International Joint Conference on Neural Networks, 2009, IJCNN, pp. 1827–1834.

Sneath P., Sokal R., et al. (1973) Numerical Taxonomy, The Principles and Practice of Numerical Classification.

Moore A., Hall J., Kreibich C., Harris E., Pratt I. (2003), Architecture of a network monitor, in: Passive & Active Measurement Workshop 2003, PAM2003, Citeseer, 2003.

---

1. Estudiante de Maestría en Tecnología Informática. Boyacá. Universidad Pedagógica y Tecnológica de Colombia. anros8626@gmail.com

2. Docente. Boyacá. Universidad Pedagógica y Tecnológica de Colombia. fabian.medina@uptc.edu.co

3. Docente. Boyacá. Universidad Pedagógica y Tecnológica de Colombia. jairo.mesa@uptc.edu.co

---

Revista ESPACIOS. ISSN 0798 1015
Vol. 41 (Nº 07) Año 2020

[Índice]