Revista ITECKNE - Universidad Santo Tomás, Seccional Bucaramanga, Colombia, Vol. 18 Nº 2 julio - diciembre de 2021

Estado del arte modelo óptimo de operación posterior a ataques intencionales considerando conmutación de los sistemas de transmisión

Theoretical framework about optimal model of operation after intentional attacks considering transmission system switching

Juan Carlos Toctaquiza-Vargas[1]; Diego Francisco Carrión-Galarza[2]

[1]Universidad Politécnica Salesiana, Quito, Ecuador, jtoctaquiza@est.ups.edu.ec
[2]Universidad Politécnica Salesiana, Quito, Ecuador, dcarrión@.ups.edu.ec

Fecha de recepción: 1 de marzo de 2021. Fecha de aprobación: 11 de mayo de 2021

Resumen- La presente investigación está enfocada en la operación óptima posterior a ataques intencionales considerados conmutación de los sistemas de transmisión. Los modelos aplicables para este proceso se enfocan en la aplicación de métodos de optimización binivel que son capaces de analizar dos posibles escenarios, con el fin de disminuir el tiempo de pérdida o salida de la demanda del sistema eléctrico. El principal objetivo de este trabajo está relacionado con mantener los requerimientos mínimos que permitan la operación del Sistema Eléctrico de Potencia, para esto se realizará el planteamiento de ecuaciones que permita establecer los modelos matemáticos ante ataques intencionales que deberá mantener el funcionamiento del Sistema Eléctrico y reaccionar ante contingencias a través de la Conmutación Óptima de Líneas de Transmisión.

Palabras clave- Vulnerabilidad de sistemas de potencia; conmutación de líneas de transmisión; optimización; seguridad redes eléctricas; ataque intencional; conmutación óptima de líneas de transmisión; análisis de contingencias.

Abstract- This research is focused on the optimal operation after intentional attacks considering switching of transmission systems. The applicable models for this process focus on the application of bi-level optimization methods that are capable of analyzing two possible scenarios in order to reduce the time of loss or departure from the demand of the electricity system. The main objective of this work is related to maintaining the minimum requirements that allow the operation of the Electric Power System. For this, equations will be used to help establish the mathematical models in the event of intentional attacks. The operation of the Electric System should hold and react in the event of contingencies through the Optimal Switching of Transmission Lines.

Keywords- Power system vulnerability; transmission line switching; optimization; electrical network security; intentional attack; optimal transmission switching; contingency analysis.

Citar este artículo como: J.C. Toctaquiza-Vargas, D.F. Carrión-Galarza, Estado del arte modelo óptimo de operación posterior a ataques intencionales considerando conmutación de los sistemas de transmisión. *ITECKNE*, 18 (2), 2021 pp. 121 - 131 DOI: https://doi.org/10.15332/iteckne.v18i1.2559

1. INTRODUCCIÓN

La gestión de los sistemas eléctricos de potencia - SEP ha cambiado en los últimos tiempos con la implementación de redes inteligentes, que se caracterizan por tener modernas tecnologías de comunicación [1] procesamiento de señales y control; permitiendo monitorear las redes eléctricas sin esfuerzo y en áreas amplias [2] La ubicación y el tamaño de las subestaciones primarias PS son los movimientos estratégicos en la planificación de los sistemas de distribución. Aunque las subestaciones representan una minoría de los costos del sistema, definen el carácter general del sistema de distribución [3].

La conmutación óptima de líneas de transmisión OTS permite al operador tomar decisiones importantes frente a la presencia de contingencias N-1 en los sistemas eléctricos de potencia, que satisface los requisitos de viabilidad, estabilidad y fiabilidad del disyuntor CB necesarios para la implementación práctica [4]. En los últimos años han aumentado las investigaciones de la OTS que demuestran un aumento de las restricciones consideradas como la confiabilidad, las pérdidas, la congestión y la estabilidad [5] Hay que considerar que la topología se modifica luego de una contingencia y debe ser capaz de sobre ponerse ante otra posible perturbación en el SEP que puede ser a través de un disparo de línea o la variación en la generación [6].

En el trabajo de [7] se presentan dos algoritmos que permiten obtener información sobre cargabilidad en líneas, ángulos de voltaje en barras y el despacho económico - DE. En el algoritmo uno se indica la metodología para el despacho óptimo de generación mediante flujos óptimos de potencia DC, FOPDC. El modelo minimiza los costos de generación bajo restricciones de límite de flujo de potencia por líneas, límites de generación y balance de potencia. El algoritmo dos analiza el impacto de acciones de conmutación sobre el SEP bajo condiciones de contingencia N-1, el cual se basa en la aplicación de OTS con FOPDC.

Los autores de [8] presentan un modelo de optimización que se construye estableciendo un costo mínimo de operación del sistema y un margen de seguridad estático máximo como objetivo. La conmutación óptima de la transmisión como herramienta de gestión de la congestión para cambiar la topología de red que, a su vez, conduciría a una mayor eficiencia en el mercado de la electricidad [9]. En el trabajo presentado por [10], el modelo de optimización se formula como un programa de cono de segundo orden entero mixto MISOCP, mientras que el modelo de flujo de potencia de CA, las complejas restricciones de restauración del sistema de energía y los procesos cambiantes de los estados disponibles de componentes se consideran sintéticamente para hacer el modelo más realista.

Las líneas de transmisión son esenciales en un SEP [11] y actualmente forman parte de un amplio estudio [12], principalmente en líneas de gran capacidad de energía y a largas distancias en las que la probabilidad de emergencias inesperadas como sobrecarga y bajo voltaje aumenta el riesgo de fallas y pueden ser objetos de ataques intencionales. Los autores en [13] contribuyen principalmente con el método de conmutación correctiva como una medida de control de línea en lugar de una parte de la programación del día antes de hacer frente a emergencias inesperadas del sistema eléctrico como pueden ser sobrecarga y bajo voltaje. Establece el modelo de optimización multi-objetivo que incorpora seis objetivos contradictorios que abarcan los aspectos de la economía, la seguridad y la fiabilidad. Recomiendan que para establecer planes de operación frente a emergencias y contrarrestar posibles perturbaciones en el sistema eléctrico haya un control de línea con enfoque multitérmico de elaboración de esquemas.

Algunos autores proponen modelos de optimización en cuyos modelos está formulada una programación lineal de enteros mixtos MILP y la aplicación descomposición de Bender [14]. En [15] se utiliza un modelo de combinación de dos medidas, que son: Compromiso Unitario UC y Conmutación de Transmisión; (TS) para limitar la corriente de cortocircuito SCC. Los autores dedujeron una expresión explícita para la correlación entre la impedancia nodal y los estados de línea, utilizando la metodología de inversión de matriz y la técnica de linealización.

Si bien las redes eléctricas de alto voltaje cubren grandes áreas geográficas, estas se vuelven difíciles de proteger por su complejidad y se vuelven vulnerables a cualquier ataque intencional [16]. La vulnerabilidad de los sistemas de energía a los cortes deliberados podría evaluarse mediante la metodología bien establecida de análisis de seguridad en las redes eléctricas. Sin embargo, en el nuevo contexto en el que entran en juego los agentes destructivos, la evaluación de la seguridad de las redes eléctricas debe examinar no solo las contingencias típicas asociadas con los fracasos aleatorios, sino también un conjunto adicional de interrupciones causadas por los atacantes cibernéticos. La implantación de sistemas de gestión de energía en las empresas eléctricas ha dado lugar a una mejora de la conciencia situacional en los sistemas de energía. Sin embargo, se introducen problemas adicionales de seguridad cibernética en operaciones en tiempo real. Desde entonces, se han dedicado investigaciones sustanciales a la viabilidad y formulación de ataques ciberfísicos coordinados contra sistemas de energía [17].

Con la integración de la infraestructura cibernética en redes inteligentes se forma una superficie de ataque ampliada y caracterizada por la intensificación de la complejidad, la heterogeneidad y el número de recursos. Esto se evidencia en la frecuencia, complejidad y gravedad de los ciberataques que van dirigidos hacia varias funciones operativas de las redes eléctricas como puede ser el control automático de la generación (AGC), la estimación del estado (SE) y los sistemas de gestión de energía (EMS) [18]. Las posibles formas de poder enfrentar un ataque intencional que pongan en riesgo la atención de la demanda de un sistema eléctrico, los cuales incluyen el ajuste de la generación, el

desprendimiento de la carga y la correcta conmutación de las líneas de transmisión.

La información que entregan los autores [2] se basa en resultados obtenidos en las afectaciones provocadas por los ciberataques en diferentes países que no solo afectan la operatividad del sistema; existen casos en los que la infraestructura sufrió daños considerables y en otros casos se identificó el robo de energía pese a contar con una medición AMI, lo cual genera pérdidas millonarias a las compañías eléctricas a nivel mundial. Por lo tanto, la caracterización, el modelado y la evaluación de la vulnerabilidad cibernética de la red eléctrica y el diseño de soluciones para proteger el sistema eléctrico frente a los adversarios cibernéticos son esenciales.

Existen algunos autores que presentan diferentes métodos de solución ante el problema de ataques intencionales. Los autores en [19] proponen un sistema denominado multi-agente que es capaz de evaluar la vulnerabilidad del sistema de energía, supervisar los errores ocultos de los dispositivos de protección y proporcionar acciones de control para evitar problemas catastróficos y secuencias en cascada de eventos.

De manera parecida, pero con un análisis en la vulnerabilidad del sistema eléctrico los autores en [20] determinan que para hacer frente a los peligros de tener daños en las infraestructuras del sistema eléctrico, ya sea por desastres naturales o ataques intencionales, se deben considerar nuevos enfoques para analizar la seguridad de los componentes críticos del sistema. La solución que presenta este trabajo se trata en la aplicación de la optimización multi-objetivo que propone un enfoque de resolver el problema de encontrar soluciones para modelos matemáticos que tienen múltiples funciones objetivas con múltiples criterios de optimización.

En [17] los autores se han dedicado a realizar investigaciones sustanciales a la viabilidad y formulación de ataques ciberfísicos coordinados contra sistemas de energía; en el mismo detalla que un ataque se produce por la inyección de datos falsos (FDIA por sus siglas en inglés) contra los esquemas de acción correctiva que pueden conducir a cortes de energía. Identifica también que el ciberataque, conocido también como un ataque físico cibernético, implica manipulación de datos en concentradores de datos de fasores. Los autores proponen la aplicación de un proceso Semi-Markov que puede incorporar distribuciones de probabilidad exponencial y no-exponencial para capturar la naturaleza de los ataques reales.

Los análisis que aportan los trabajos de investigación de [21], [22] expresan el problema de la amenaza de un ataque intencional como un problema máximo - mínimo, en el que el terrorista maximiza la carga derramada mientras el operador del sistema lo minimiza. Este importante resultado permite el desarrollo de soluciones de programación matemática a este complejo problema. El método heurístico propuesto se parece al método de descomposición de Benders; la solución satisfacía la viabilidad, según aseveraron los autores, el nivel de interrupción de la carga encontrado a través de la estrategia más destructiva no era óptimo.

El método máximo - mínimo planteado en [21], [23] explica que el problema de amenaza terrorista se pudo resolver transformando las expresiones no lineales existentes en restricciones lineales. Al sustituir el problema de minimización interno por el problema máximo - mínimo se convirtió en un problema máximo - máximo; maximización de un solo nivel que se resolvió aplicando la descomposición de Benders y la programación lineal de enteros mixtos MILP.

Por otro lado, en [24] se presenta un novedoso esquema clave de pre-distribución para mitigar la gravedad de los ciberataques en los sistemas SCADA en el que se garantiza una comunicación segura entre los dispositivos SCADA mediante la propuesta de una matriz que admite operaciones de unión de dispositivos, permisos de dispositivo y actualizaciones claves con bajo costo de comunicación.

En [18] se presenta la teoría de sistemas enfocados en la seguridad en tiempo real de los sistemas eléctricos en cuyo alcance se define dos partes principales: Análisis de contingencia CA y Supervisión del sistema. Los enfoques teóricos del sistema ya consideran los aspectos físicos con más detalle que los enfoques criptográficos y de seguridad tradicionales. Estos enfoques modelan los comportamientos maliciosos como errores de componentes, entradas externas o ruidos, analizan sus efectos en el sistema y diseñan algoritmos de detección o contramedidas a los ataques.

El trabajo de investigación de [25] aborda el análisis de vulnerabilidad de la red eléctrica bajo amenaza terrorista. Este problema se formula como un programa binivel no lineal de enteros mixtos. En la optimización de nivel superior, el agente terrorista maximiza el daño causado en el sistema de energía, que se mide en términos del nivel de pérdida de carga del sistema. Por otro lado, en la optimización de nivel inferior, el operador del sistema minimiza el daño mediante un funcionamiento óptimo del sistema de potencia. La característica de modelado distintiva presentada en este documento es que, entre las diferentes acciones correctivas disponibles, el operador del sistema tiene la capacidad de modificar la topología de la red. Debido a su no convexidad y no linealidad, el problema de programación de dos niveles resultante no se puede transformar de manera equivalente en un problema de optimización estándar de un nivel. Por tal motivo el autor propone un nuevo enfoque basado en la descomposición de Benders dentro de un marco de reinicio.

Finalmente, el autor [26] utiliza un modelo de interrupción de cascada de flujo de potencia realista para simular el comportamiento del sistema, donde el atacante puede usar el Q-learning para mejorar el daño del ataque de topología secuencial hacia errores del sistema con menos esfuerzos de ataque. Los estudios de caso basados en tres

sistemas de pruebas IEEE han demostrado la capacidad de aprendizaje y la eficacia del análisis de vulnerabilidad basado en Q-learning. Desde la perspectiva de un defensor/operador de cuadrícula, el análisis de vulnerabilidades basado en Q-learning puede identificar componentes críticos en un esquema de ataque secuencial potencial. El autor enfatiza que el Q-learning también da una señal de advertencia de que la información de estado topológico del sistema podría utilizarse para concebir esquemas de ataque desastrosos. Estos conocimientos serán útiles para mejorar el conocimiento de la situación de la red inteligente contra los ciberataques.

Con base en las referencias citadas se espera que la principal contribución de este trabajo sea presentar una literatura científica sobre investigaciones relacionadas con modelos de operación posterior a ataques intencionales, considerando conmutación de los sistemas de transmisión.

De manera general se presenta la siguiente pregunta de investigación: ¿Es posible plantear un modelo de operación posterior a contingencias intencionales que considere la conmutación de los sistemas de transmisión?

El documento tiene la siguiente organización: la sección 1, trata la bibliografía encontrada de diferentes autores que relaciona la investigación de este documento; la sección 2, revisa modelos matemáticos aplicados ante una amenaza terrorista; la sección 3, presenta la descripción de la conmutación óptima de líneas de transmisión; la sección 4, presenta el análisis genérico comparativo con diversas tendencias de investigación.

2. MODELOS MATEMÁTICOS APLICADOS ANTE AMENAZAS TERRORISTAS

Las expresiones matemáticas que se detallan a continuación fueron desarrolladas en [16], por tal razón se menciona el detalle expuesto por el autor.

	Nomenclatura
A. índices	
j	Índice de generador
l	Índice de líneas de transmisión
n	Índice de barras
B. Conjuntos	
J	Conjunto de índices de generadores
L	Conjunto de índices de líneas de transmisión
N	Conjunto de índices de barras
C. Constantes	
A_{nl}	Elemento de la matriz de incidencia de la red que es igual a 1 si la barra es la barra emisora de la línea; si la barra es la barra receptora de la línea y 0 en caso contrario
P_n^d	Demanda de la barra n en megavatios
P_l^f	Capacidad de flujo de energía de la línea l en megavatios
P_j^g	Capacidad del generador j en megavatios
δ_n	Límites de los ángulos de fase (radianes)
$\emptyset^{spec}$	Nivel más bajo de caída de carga total especificado por el terrorista en megavatios
D. Variables	
ΔP^d	Vector de cargas nodales en megavatios
v_l	Variable 0/1 que es igual a 0 si la línea se destruye o de lo contrario es igual a 1
μ_l	Multiplicador de Lagrange asociado con la ecuación que relaciona flujo de potencia y ángulos de fase para la línea
λ_n	Multiplicador de Lagrange asociado con la ecuación de balance de potencia en la barra
$\underline{W_1}$	Multiplicador de Lagrange asociado con el límite superior del flujo de potencia de la línea l
$\overline{W_1}$	Multiplicador de Lagrange asociado con el límite inferior del flujo de potencia de la línea l
$\underline{\theta_j}$	Multiplicador de Lagrange asociado con el límite inferior del flujo de potencia del generador j
$\overline{\theta_j}$	Multiplicador de Lagrange asociado con el límite superior del flujo de potencia del generador j
$\underline{\alpha_n}$	Multiplicador de Lagrange asociado con el límite inferior de la caída de carga en la barra n
$\overline{\alpha_n}$	Multiplicador de Lagrange asociado con el límite superior de la caída de carga en la barra n

2.1 Formulación Binivel general del problema de amenaza terrorista

Una forma general del problema de amenaza terrorista se puede plantear como el siguiente programa binivel [16].

F.O.:

$$\underbrace{\max}_{x} c^{\circ}(x, y^{*}) \qquad (1)$$

Sujeto a

$$f^{\circ}(x, y^{*}) \geq 0 \qquad (2)$$

$$y^{*} = \arg\left\{\underbrace{\min}_{y} c^{i}(x, y)\right\} \qquad (3)$$

Sujeto a

$$f^{i}(x, y) \geq 0 \qquad (4)$$

El problema binivel indicado anteriormente consiste en una optimización externa, donde las ecuaciones (1) y (2) están relacionadas con el terrorista y una optimización interna como se indica en las ecuaciones siguientes (3) y (4), las cuales están asociados con el operador del sistema. Como se puede observar, los exponentes de las ecuaciones (1) y (2) "o" indican "exterior"; los exponentes de las ecuaciones (3) y (4) "i" indican "interior".

De las ecuaciones descritas anteriormente, el terrorista controla el vector de las variables "x" que representan las variables de estado binario 0/1, que relaciona la condición de atención a los componentes del sistema para su revisión. Las variables de decisión están adaptadas por "y" "y*" pueden ser controladas por el operador del sistema, generalmente son variables del SEP, ángulo (δ) potencia gererada (P^g) potencia de flujo $(8P^f)$ y variación en la demada ΔP^d.

La función objetivo de la optimización externa $c^\circ(x,y)$ se maximiza sobre x en la ecuación (1), la cual está sujeta a un conjunto de funciones restringidas $f^\circ(x,y)$, dependiendo de las variables de nivel interno y externo de (2) y sujeto a la optimización interna, en la que la función objetivo $c^i(x,y)$ posiblemente diferente, se minimiza en y como se muestra en la ecuación (3) que está sujeta a $f^i(x,y)$ con x, como se muestra en la ecuación (4).

La formulación del problema máximo - mínimo, propuesta en los artículos de investigación [16] y [21]transmission lines, generators, transformers, es un caso particular de las ecuaciones (1) y (4). Igualando la función objetivo $c^\circ(x,y) = c^i(x,y)$ externas e internas, respectivamente, y con f° siendo una función únicamente de las variables x de nivel externo.

El programa binivel en donde se considera un problema específico de amenaza terrorista, en el que el terrorista minimiza el número de componentes del sistema de energía, que deben ser destruidos para causar un nivel de pérdida de carga mayor o igual a una cantidad específica. El objetivo principal del operador del sistema es justamente minimizar la pérdida de carga y aplicar los planes de contingencia N-1, en el menor tiempo posible para mantener el funcionamiento continuo del sistema [27]. Se debe considerar que la amenaza terrorista puede afectar la estabilidad, la regulación primaria y la potencia reactiva del sistema.

Los componentes vulnerables que se pueden identificar en un sistema eléctrico de potencia SEP, frente a un ataque terrorista son generadores, subestaciones, barras, líneas, transformadores y banco de capacitores - reactores. Las líneas de transmisión son los componentes desprotegidos y representan un objetivo relativamente fácil para cualquier ataque intencional [8].

La formulación binivel o dos niveles para ataques intencionales se plantea como se detalla a continuación:

F.O.:

$$\underbrace{\max}_{v} \sum_{l \in L} vl \qquad (5)$$

Sujeto a

$$\sum_{n \in N} \Delta P_n^{d*} \geq \emptyset^{spec} \qquad (6)$$

$$\Delta P^{d*} = \arg\left\{ \underbrace{\min}_{\delta, P^g, P^f, \Delta P^d} \sum_{n \in N} \Delta P_n^d \right\} \qquad (7)$$

Sujeto a

$$P_l^f = v_l \frac{1}{x_l} \sum_{n \in N} A_{nl} \delta_n, \forall l \in L \quad (\mu_l) \qquad (8)$$

$$\sum_{j \in J_n} P_j^g - \sum_{l \in L} A_{nl} P_l^f + \Delta P_n^d = P_n^d, \forall n \in N \quad (\lambda_n) \qquad (9)$$

P

$$-\overline{P}_l^f \leq P_l^f \leq \overline{P}_l^f, \quad \forall n \in N \quad (\underline{W}_1, \overline{W}_1) \qquad (10)$$

$$P_{-j}^g \leq P_j^g \leq \overline{P}_j^g, \quad \forall j \in J \quad (\theta_j, \overline{\theta}_j) \qquad (11)$$

$$0 \leq \Delta P_n^d \leq P_n^d, \quad \forall n \in N \quad (\alpha_n, \overline{\alpha}_n) \qquad (12)$$

Donde los multiplicadores de Lagrange asociados con las restricciones de las ecuaciones (8) - (12) en el problema de optimización interna están entre paréntesis.

En las ecuaciones (5) - (12) establece una instancia de la formulación general de dos niveles (1) - (4) con diferentes funciones objetivas de nivel externo e interno $c^\circ(x,y) \neq c^i(x,y)$ y con f° siendo una función de las variables de nivel interno. Las ecuaciones de optimización del nivel externo se definen en las ecuaciones (5) y (6). En tanto las ecuaciones (7) - (12) representan el problema del nivel interno. El terrorista toma el control del vector 0/1 de variables v, donde v_l es igual a 0 si la línea l es destruida o en caso contrario es igual a 1 si está en condiciones de servicio. Las variables de decisión controlada por el operador del sistema son, $\delta, P^g, P^f, y \Delta P^d$.

La ecuación (5) describe el objetivo del terrorista que es maximizar el número de líneas no atacadas o de forma equivalente, minimizar el número de líneas atacadas. De esta forma el terrorista busca que la pérdida total de la carga sea mayor o igual al nivel previamente esperado, según el modelo planteado en la ecuación (6). Las restricciones mostradas en la ecuación (6) no se pueden modelar en una formulación de máximo - mínimo. Por otro lado, el operador del sistema tiene un objetivo diferente como se plantea en la ecuación (7) que es minimizar la pérdida total de la carga bajo la combinación de líneas destruidas elegidas por el terrorista.

Las restricciones de la ecuación (8) representan los flujos de línea en términos de los ángulos de fase nodal y las variables de nivel exterior. Considerando que si la línea se destruye, el flujo de energía se establece en 0 mediante (8). Las restricciones de la ecuación (9) formulan las ecuaciones de balance de potencia nodal, mientras que las restricciones de la ecuación (10) enuncian los límites de capacidad de flujo de línea. Para finalizar las restricciones de las ecuaciones (11) y (12) establecen los límites de generación y pérdida de carga respectivamente. En referencia a los límites de generación tienen en cuenta las reservas de rotación rápida

y los límites de velocidad de rampa que se supone han sido calculados previamente por el operador del sistema.

Además de su complejidad intrínseca debido a los dos niveles de optimización, el problema (5) - (12) es una programación de entero mixto lineal (que contiene variables continuas y binarias) cuyos trabajos se relacionan en [2], [6], [11], [14]–[16], [28] y programación de enteros mixtos no lineal debido al producto de las variables [9] v_l y δ_n en (8). Sin embargo, como se describe a continuación, aprovechando el hecho de que el problema de optimización interna es lineal para un vector dado, el problema (5) - (12) se puede transformar en un problema S-MILP equivalente.

2.2 Defensa contra ataques de repetición

En este ejemplo los autores [18] consideran la defensa contra el ataque de repetición, donde un adversario registra una secuencia de mediciones del sensor y reproduce la secuencia después. Los ataques de repetición son ataques cibernéticos que rompen la integridad o más precisamente la frescura de los datos de medición. En este ataque a la integridad del sistema, claramente concebido y operado en el ámbito cibernético, explotó cuatro vulnerabilidades de día cero para romper las infraestructuras cibernéticas y permaneció sin descubrir durante varios meses después de su lanzamiento. Por lo tanto, un enfoque cibernético puro para reproducir ataques puede no ser capaz de reaccionar lo suficientemente rápido antes de que el sistema se dañe. En este trabajo se presenta el resumen del concepto de autenticación física y una metodología que puede detectar este tipo de ataques independientemente del tipo de ataque utilizado para obtener acceso al sistema de control.

Para lograr una mayor generalidad, el método se presenta para un sistema de control genérico. Se supone que los sensores están monitoreando un sistema con la siguiente dinámica de estado:

F.O.:

$$X_{k+1} = F_{X_k} + Bu_k + W_k \qquad (13)$$

Donde $x_k \in R^n$ es el vector de variables de estado en el momento, $W_k \in R^n$ es el ruido del proceso en el momento, k, y x_0 es el estado inicial. Se asume que W_k, x_k son variables aleatorias gaussianas independientes, $x_0 \sim N(\overline{x_0}, \Sigma)$, $W_k \backsim N(0, Q)$.

Para cada período de muestreo k la verdadera ecuación de medición de los sensores se puede escribir como:

F.O.:

$$Z_k = Hx_k + v_k \qquad (14)$$

Donde $z_k \in R^n$ es una colección de todas las mediciones de los sensores en el tiempo k y $v_k \sim N(0, R)$ es el ruido de medición independiente de x_0 y w_k.

Suponemos que un atacante registra una secuencia de mediciones desde el tiempo T_0 hasta el tiempo $T_0 + T - 1$ y la reproduce desde el tiempo $T_0 + T$ hasta el tiempo $T_0 + 2T - 1$, donde $T_0 \geq 0$, $T \geq 1$. Como resultado, las mediciones dañadas que Z_k^a recibió por el operador del sistema son:

F.O.:

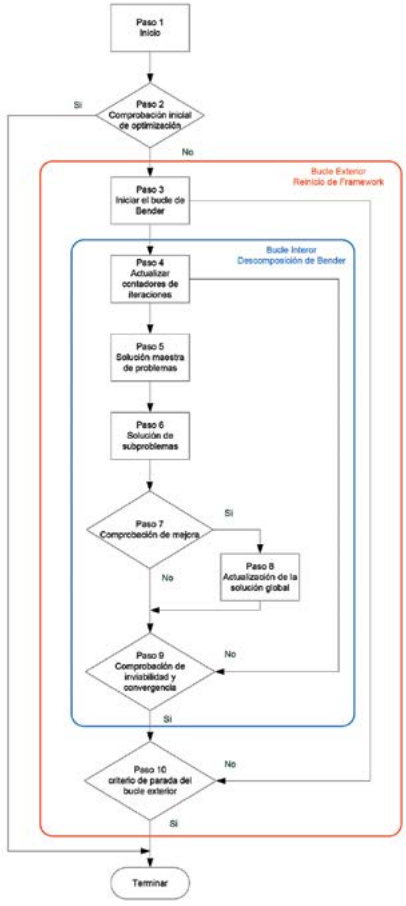
$$Z_k^a \begin{cases} Z_k, & 0 \leq k \leq T_0 + T - 1 \\ Z_k - T, & T_0 + T \leq k \leq T_0 + 2T - 1 \end{cases} \qquad (15)$$

El objetivo es diseñar un estimador, un controlador y un detector de tal forma que: el sistema es estable cuando no hay ningún ataque de repetición; el detector puede detectar el ataque de repetición con una alta probabilidad.

2.3 Descomposición de Benders en conmutación de líneas de transmisión

La metodología propuesta, en lo sucesivo denominada Conmutación de línea de descomposición BDLS de Benders, se muestra en la Fig. 1.

Fig. 1. METODOLOGÍA PROPUESTA CONTRA ATAQUES INTENCIONALES



Fuente Los autores.

3. CONMUTACIÓN DE LÍNEAS DE TRANSMISIÓN

La conmutación de líneas de transmisión se puede definir como un método de control para problemas, tales como situaciones de sobretensión o bajo voltaje, sobrecargas de línea, pérdida o reducción de costos, mejora de la seguridad del sistema. En la práctica se requiere satisfacer la demanda de manera eficiente, optimizando la red a través del control de los disyuntores de línea de transmisión, además de la salida del generador.

La investigación de [11], [29], [30] en referencia a la conmutación de líneas de transmisión, conlleva al uso del modelo de conmutación óptima de transmisión (OTS por sus siglas en inglés) esta literatura presentada por los autores recomienda que la OTS podría aumentar la eficiencia económica del despacho del sistema de energía. Adicionalmente hacen un alcance en la capacidad de conmutación de línea de transmisión para reducir el costo de envío, optimizado el costo a través de una formulación de enteros mixtos.

3.1 Modelo de conmutación óptima de transmisión OTS

Nomenclatura	
n	Número de generadores
k	Línea de transmisión
i	Número de barra
N	Conjunto de índices de barras
C_n	Costo de operación de un generador
D_b	Demanda eléctrica
Y_k	Susceptancia eléctrica de la línea de transmisión
$F_k^{\max}$	Máxima tasa de la línea de transmisión
$G_n^{\max}$	Generación máxima
$G_n^{\min}$	Generación mínima
θ_a	Ángulo de origen de la barra
θ_b	Ángulo de destino de la barra
$Z^{\max}$	Número máximo de líneas conmutadas
Z^k	Estado de la línea (0 fuera de servicio; 1 en servicio)
g_n	Potencia del generador
f_k	Flujo de potencia transmitido por la línea
$\underline{P}$	Variable para optimizar
M_k	Valor máximo de potencia de las líneas

Este modelo está basado en la programación de entero mixto (MIP) basado en un problema tradicional de flujo de potencia óptimo. El objetivo del modelo de optimización es minimizar el costo de generación de energía durante un lapso de tiempo sujeto a suministrar la carga en ese tiempo. El modelo presentado está dado en [11]:

F.O.:

$$Min, P_1 = \sum_n C_n * g_n \qquad (16)$$

Sujeto a

$$\sum_{n\in n_b} g_n + \sum_{k\in \emptyset_b^+} f_k - \sum_{k\in \emptyset_b^-} f_k = D_b \forall b \qquad (17)$$

$$-(1-Z_k)M_k \le Y_k(\theta_{a_k} - \theta_{b_k}) \le (1-Z_k)M_k \forall k \qquad (18)$$

$$-F_k^{\max} Z_k \le f_k \le F_k^{\max} Z_k \quad \forall k \qquad (19)$$

$$G_n^{\min} \le g_n \le G_n^{\max} \forall n \qquad (20)$$

$$-\Theta_k^{\max} \le \theta_{a_k} - \theta_{b_k} \le \Theta_k^{\max} \forall k \qquad (21)$$

El método de programación entero mixto puede ser complicado de resolver en un sistema eléctrico de potencia, especialmente cuando el número de líneas de transmisión es elevado. En [11] se propone modelo aproximado de optimización en sistemas de transmisión, a continuación, se propone para resolver la dificultad de cálculo del problema.

F.O.:

$$\sum_k (1-Z_k) = Z^{\max} \qquad (22)$$

La función objetivo (16) minimiza los costos totales de generación de electricidad. Las restricciones (17) aseguran que la energía que fluye hacia cada bus sea igual a la energía que fluye hacia afuera de cada bus. La relación física entre los ángulos de voltaje de los buses conectados y el flujo de potencia en las líneas de conexión se representa mediante restricciones (18). Los límites térmicos de las líneas se respetan mediante restricciones (19) y las capacidades de los generadores están aseguradas por restricciones (20). Los límites de las diferencias de ángulo de fase de los buses conectados se imponen mediante restricciones (21). El estado de la variable binaria Z_k indica que la línea k está en servicio $Z_k = 1$ o fuera de servicio $Z_k = 0$. Los lados izquierdo y derecho de las restricciones (19) se multiplican por variables binarias Z_k para garantizar que no haya flujo de energía en las líneas que están fuera de servicio. Si una línea está en servicio $Z_k = 1$ entonces la desigualdad (18) será equivalente a la igualdad $f_k = Y_k(\theta_{a_k} - \theta_{b_k})$. Por otro lado, si una línea no está en servicio $Z_k = 0$, entonces la desigualdad (18) será independiente de la variable de flujo de potencia f_k, pero incluirá el parámetro disyuntivo M_k.

Al establecer el valor de este parámetro en un número suficientemente grande, las restricciones de desigualdad (18) serán redundantes cuando la línea correspondiente se ponga fuera de servicio.

4. ANÁLISIS DE CONTINGENCIAS EN EL SISTEMA ELÉCTRICO DE TRANSMISIÓN

Una contingencia se presenta cuando un componente del SEP sale de servicio. La importancia de analizar las contingencias permite verificar si nuestro sistema tiene la capacidad de soportar y mantener su operación en el SEP bajo condiciones mínimas de operación.

La presencia de contingencias en el sistema eléctrico de transmisión se debe principalmente por las condiciones climáticas, accidentes intencionales o naturales o por la operación errónea desde el centro de control, afectando el normal funcionamiento de las líneas de transmisión.

Cumplir con los estándares de confiabilidad se vuelve un desafío, por tal motivo se vuelve necesario evaluar la confiablidad del sistema con base en los procedimientos para mitigar las fallas $N-1$. Los estudios realizados sobre este método en [5], [7], [9], [12], [27], [30] definen que la principal salida de los equipos del SEP se debe a fallas en el sistema.

El objetivo de los análisis de contingencias es conocer el estado del sistema eléctrico de potencia antes de que se produzca la falla y después de esta, con el propósito de mantener un procedimiento de operación al momento que ocurran. El caso más estudiado de una contingencia es el tipo $N-1$, la misma que se refiere a la capacidad que tiene el sistema eléctrico de potencia en actuar frente a la presencia de una falla y a la habilidad que tienen los generadores para estabilizar el sistema.

Los parámetros que permiten analizar la operación de las contingencias son la tasa de falla y la tasa de reparación, estos son puntos clave para el cálculo de los índices de confiabilidad. Se sabe que la confiabilidad de un sistema eléctrico de potencia se sustenta en la capacidad de soportar una falla y conocer el nivel de seguridad manteniendo protegido al SEP.

La tasa de falla TTF se conoce como el número de interrupciones del servicio en los equipos del SEP y se define en la siguiente ecuación:

$$TTF = MTTF * \ln(U) \qquad (23)$$

Donde:

$MTTF$ se conoce como el tiempo promedio entre fallas

U es la indisponibilidad anual de un equipo

La tasa de reparación TTR se conoce como el tiempo estimado en realizar la reparación del elemento en falla y se define en la siguiente ecuación:

$$TTR = MTTR * \ln(U) \qquad (24)$$

Donde:

$MTTF$ se conoce como el tiempo promedio de reparación

U es la indisponibilidad anual de un equipo.

Como se puede revisar la confiabilidad del Sistema Eléctrico de Potencia se establece por las fallas que ocurren durante un tiempo determinado y según los trabaos consultados se cuantifica en un tiempo promedio de cinco minutos, por lo tanto el SEP debe estabilizar sus parámetros de operación en este tiempo como máximo.

5. ANÁLISIS GENÉRICO COMPARATIVO

5.1 Tendencias de investigadores

El estado del arte de la presente investigación busca proporcionar la actual temática de la literatura científica sobre los modelos óptimos de operación posterior a ataques intencionales, considerando conmutación de los sistemas de transmisión. Para este trabajo se ha considerado detallar las restricciones del problema y la propuesta de solución enfocado en los trabajos realizados por otros autores con temas relacionados a lo investigado.

Se debe considerar que las investigaciones que se presentan en la Tabla I fueron consideradas como aportes importantes para iniciar esta investigación. No se descarta la posibilidad de ir mejorando cualquiera de los diversos métodos propuestos por los investigadores citados.

6. RECOPILACIÓN DE LA INFORMACIÓN

Durante la búsqueda de la información en las herramientas bibliométricas se identificaron 4.647 artículos en Web of Science; 6.590 artículos en Scopus; 2.866 artículos en IEEExplore y 22.100 artículos en Google Académico en un espacio de tiempo del 2000 hasta el 2021. La mayoría de artículos citados fueron filtrados y los estudios pertinentes se incluyeron en la revisión de este trabajo. La Tabla II muestra la síntesis de los parámetros de búsqueda en la recuperación de artículos.

Como se representa en la Fig. 2 ha habido un rápido desarrollo de publicaciones en el campo de la operación, optimización de los sistemas de transmisión a partir del 2000, el mismo que ha tenido un mayor aumento y la tendencia se mantiene hasta el 2020 con cerca de 700 publicaciones.

Existe una gran posibilidad de que en 2021 sigan publicándose más trabajos de investigación en referencia a los temas tratados en este trabajo académico como es la vulnerabilidad de sistemas eléctricos de potencia, conmutación óptima de líneas de transmisión, análisis de contingencias.

Tabla I.
TENDENCIAS DE INVESTIGADORES EN EL MODELO ÓPTIMO DE OPERACIÓN POSTERIOR A ATAQUES INTENCIONALES CONSIDERANDO CONMUTACIÓN DE LOS SISTEMAS DE TRANSMISIÓN

DATOS		RESTRICCIONES DEL PROBLEMA				PROPUESTAS PARA RESOLVER EL PROBLEMA				
Año de publicación	Investigador	Costo	Confiabilidad	Redes	Cobertura/Crecimiento/ Expansión	MINLP	MILP	GESTIÓN	Optimización	Algoritmos, Heurística o Metaheurística
2020	A. Bosisio [3]	X	X	X			X	X	X	X
2017	G. Huang, J. Wang, C. Chen, J. Qi, and C. Guo [1]		X		X			X	X	X
2005	J. M. Arroyo and F. D. Galiana [13]		X	X			X		X	X
2015	P. Dehghanian, Y. Wang, G. Gurrala, E. Moreno-Centeno, and M. Kezunovic [4]	X	X	X				X	X	X
2017	X. Xu, Y. Cao, H. Zhang, S. Ma, Y. Song, and D. Chen [10]	X	X	X	X	X			X	X
2008	E. B. Fisher, R. P. O'Neill, and M. C. Ferris [9]	X	X	X	X		X		X	X
2015	S. Dehghan and N. Amjady [5]	X		X	X	X	X	X	X	X
2011	C. M. Rocco, J. E. Ramirez-Marquez, D. E. Salazar, and C. Yajure [17]	X	X	X					X	X
2018	K. G. Boroojeni, M. Hadi Amini, N. R. Sunitha, and S. S. Iyengar[21]	X	X	X				X		X
2012	M. Khanabadi, H. Ghasemi, S. Member, and M. Doostizadeh [7]	X		X		X		X	X	X
2017	X. Wu, Z. Zhou, G. Liu, W. Qi, and Z. Xie [6]	X		X					X	X
2020	S. Basumallik, S. Eftekharnejad, and B. K. Johnson [14]		X	X						X
2019	J. Lin [12]	X	X	X	X		X	X	X	X
2018	J. Aghaei, A. Nikoobakht, M. Mardaneh, M. Shafie-khah, and J. P. S. Catalão [24]	X	X	X	X					X
2018	H. Zhang, G. Li, and H. Yuan [8]	X		X						X
2020	T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari, and P. Dehghanian [2]	X	X	X				X	X	X
2012	Y. Mo [15]	X		X				X		X
2009	J. Salmeron, K. Wood, and R. Baldick [11]		X						X	X
2010	A. Delgadillo, J. Arroyo, and N. Alguacil [22]			X				X	X	X
2016	J. Yan, S. Member, H. He, S. Member, X. Zhong, and Y. Tang [23]		X							X
2018	M. Jabarnejad [25]	X							X	
2013	Q. Wang, S. Member, J. Watson, and Y. Guan [26]	X	X				X		X	X

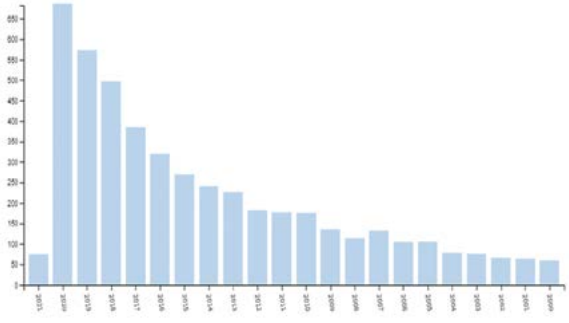
Fuente Los autores.

Tabla II.
DETALLE DE PARÁMETROS DE BÚSQUEDA PARA LA RECUPERACIÓN DE ARTÍCULOS

Parámetros	Selección
Consulta de búsqueda	(((Power System Vulnerability) OR (Transmission Line Switching)) OR ((Optimization) AND (Intentional Attack)) OR ((Electrical Network Security) AND (Optimal Transmission Switching)) OR ((Intentional Attack) AND (Optimal Transmission Switching)) OR ((Binivel) AND (Power System Vulnerability)) OR ((Power System Vulnerability) AND (Bender Decomposition)))
Tipo de documento	Artículos
Espacio de tiempo	2000 - 2021
Índice de citas	SCIE - SSCI - ESCI
Lenguaje	Inglés
Países	China, Estados Unidos, Irán, Inglaterra, Suiza, Suecia, Países Bajos, Canadá, España, Australia, Corea del Sur, Brasil, Italia, Francia

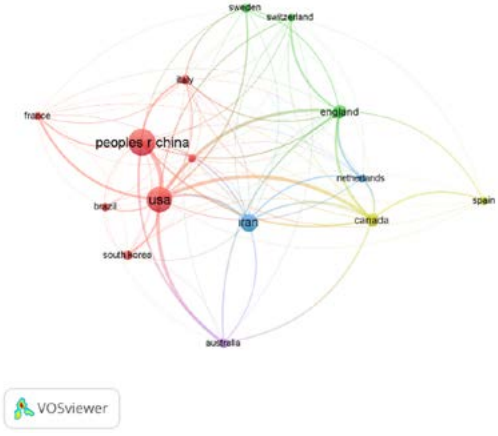
Fuente Los autores.

Fig. 2. NÚMERO DE PUBLICACIONES POR AÑO.
ESPACIO DE TIEMPO 2000 - 2021



Fuente Los autores.

Fig. 3. DETALLE DE AUTORES CON MAYORES PUBLICACIONES EN DIFERENTES PAÍSES



Fuente Los autores.

Los documentos revisados que comprendían el objetivo de este trabajo de investigación fueron posteriormente clasificados y analizados en términos de país. En la Fig. 3. DETALLE DE AUTORES CON MAYORES PUBLICACIONES EN DIFERENTES PAÍSES se pueden observar los países con más tendencia a la investigación que se lleva en este trabajo. Para este análisis se utilizó la herramienta Vosviewer.

El análisis bibliométrico de este estudio servirá para comprender mejor la base intelectual en el campo de los modelos de optimización posterior a ataques intencionales, considerando conmutación de los sistemas de transmisión.

7. CONCLUSIONES

Los resultados del análisis descriptivo muestran un rápido aumento en el número de publicaciones que conducen a un crecimiento general de la base intelectual al campo relacionado con esta investigación.

La importancia de planificar y mantener las redes eléctricas operativas y seguras sin alterar las condiciones óptimas de su funcionamiento se convierten en el principal reto de la ingeniería eléctrica. Con el desarrollo de la tecnología se ha logrado fortalecer este campo, pero a la vez nos deja la interrogante sobre el beneficio de la tecnología para afectar el funcionamiento óptimo del sistema eléctrico de potencia.

Aplicar conmutación óptima de transmisión en un sistema eléctrico de potencia beneficia el control y operación. Con la implementación de un modelo óptimo de operación al mismo, permitirá mejorar dicho control y reducir los tiempos de desconexiones que afectan técnica y económicamente a las empresas de suministro de energía. Por tal motivo, la implementación de un modelo que enfrente los peores escenarios ante un ataque intencional se hace necesario con el fin de evaluar, solucionar y proteger el sistema eléctrico frente a los adversarios cibernéticos.

La formulación binivel permite evaluar dos escenarios al momento de producirse un ataque intencional a través de la función objetivo de la optimización interna y externa. Dependerá de las variables para proceder al análisis del comportamiento luego del ataque. El propósito de resolución de estos problemas es identificar compontes de una red eléctrica permitirá crear mecanismos de defensa y estar preparados ante un posible ataque. Los resultados numéricos que se obtengan se convertirán en un instrumento útil para que el operador del sistema mitigue el impacto de interrupciones deliberadas.

8. REFERENCIAS

[1] G. Huang, J. Wang, C. Chen, J. Qi, and C. Guo, "Integration of Preventive and Emergency Responses for Power Grid Resilience Enhancement," IEEE Trans. Power Syst., vol. 32, no. 6, pp. 4451–4463, Nov. 2017. DOI: http://dx.doi.org/10.1109/TPWRS.2017.2685640

[2] T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari, and P. Dehghanian, "Electric Power Grid Resilience to Cyber

Adversaries: State of the Art," IEEE Access, vol. 8, pp. 87592–87608, 2020. DOI: https://doi.org/10.1109/access.2020.2993233

[3] A. Bosisio *et al.*, "A GIS-based approach for high-level distribution networks expansion planning in normal and contingency operation considering reliability," *Electr. Power Syst. Res.*, vol. 190, no. April 2020, p. 106684, Jan. 2021.

[4] P. Dehghanian, Y. Wang, G. Gurrala, E. Moreno-Centeno, and M. Kezunovic, "Flexible implementation of power system corrective topology control," *Electr. Power Syst. Res.*, vol. 128, pp. 79–89, Nov. 2015. DOI: http://doi.org/10.1016/j.epsr.2015.07.001

[5] D. Carrión, J. Palacios, M. Espinel, and J. W. González, "Transmission Expansion Planning Considering Grid Topology Changes and N-1 Contingencies Criteria," 2021, pp. 266–279.

[6] S. Dehghan and N. Amjady, "Robust Transmission and Energy Storage Expansion Planning in Wind Farm-Integrated Power Systems Considering Transmission Switching," *IEEE Trans. Sustain. Energy*, vol. 7, no. 2, pp. 765–774, Apr. 2016. DOI: http://dx.doi.org/10.1109/TSTE.2015.2497336

[7] S. Pinzón, D. Carrión, and E. Inga, "Optimal Transmission Switching Considering N-1 Contingencies on Power Transmission Lines," *IEEE Lat. Am. Trans.*, vol. 19, no. 4, pp. 534–541, 2021.

[8] X. Wu, Z. Zhou, G. Liu, W. Qi, and Z. Xie, "Preventive Security-Constrained Optimal Power Flow Considering UPFC Control Modes," *Energies*, vol. 10, no. 8, p. 1199, Aug. 2017. DOI: https://doi.org/10.3390/en10081199

[9] M. Khanabadi, H. Ghasemi, and M. Doostizadeh, "Optimal Transmission Switching Considering Voltage Security and N-1 Contingency Analysis," *IEEE Trans. Power Syst.*, vol. 28, no. 1, pp. 542–550, Feb. 2013. DOI: http://dx.doi.org/10.1109/TPWRS.2012.2207464

[10] H. Zhang, G. Li, and H. Yuan, "Collaborative Optimization of Post-Disaster Damage Repair and Power System Operation," *Energies*, vol. 11, no. 10, p. 2611, Sep. 2018. DOI: http://dx.doi.org/10.3390/en11102611

[11] E. B. Fisher, R. P. O'Neill, and M. C. Ferris, "Optimal Transmission Switching," *IEEE Trans. Power Syst.*, vol. 23, no. 3, pp. 1346–1355, Aug. 2008.

[12] D. Carrion and J. W. Gonzalez, "Optimal PMU Location in Electrical Power Systems Under N-1 Contingency," in 2018 International Conference on Information Systems and Computer Science (INCISCOS), 2018, vol. 2018-Decem, no. 1, pp. 165–170.

[13] X. Xu, Y. Cao, H. Zhang, S. Ma, Y. Song, and D. Chen, "A Multi-Objective Optimization Approach for Corrective Switching of Transmission Systems in Emergency Scenarios," Energies, vol. 10, no. 8, p. 1204, Aug. 2017. DOI: https://doi.org/10.3390/en10081204

[14] J. Salmeron, K. Wood, and R. Baldick, "Worst-Case Interdiction Analysis of Large-Scale Electric Power Grids," *IEEE Trans. Power Syst.*, vol. 24, no. 1, pp. 96–104, Feb. 2009. DOI: 10.1109/TPWRS.2008.2004825 https://doi.org/

[15] J. Lin *et al.*, "Co-optimization of unit commitment and transmission switching with short-circuit current constraints," *Int. J. Electr. Power Energy Syst.*, vol. 110, no. February, pp. 309–317, Sep. 2019. DOI: https://doi.org/10.1109/TPWRS.2009.2037232

[16] J. M. Arroyo and F. D. Galiana, "On the Solution of the Bilevel Programming Formulation of the Terrorist Threat Problem," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 789–797, May 2005. DOI: https://doi.org/10.1109/TPWRS.2005.846198

[17] S. Basumallik, S. Eftekharnejad, and B. K. Johnson, "The impact of false data injection attacks against remedial action schemes," *Int. J. Electr. Power Energy Syst.*, vol. 123, no. April, p. 106225, Dec. 2020. DOI: https://doi.org/10.1016/j.ijepes.2020.106225

[18] Yilin Mo *et al.*, "Cyber–Physical Security of a Smart Grid Infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012. DOI: https://doi.org/10.1109/JPROC.2011.2161428

[19] C. C. Liu, J. Jung, G. T. Heydt, V. Vittal, and A. G. Phadke, "The strategic power infrastructure defense (SPID) system. A conceptual design," *IEEE Control Syst.*, vol. 20, no. 4, pp. 40–52, Aug. 2000. DOI: https://doi.org/10.1109/37.856178

[20] C. M. Rocco, J. E. Ramirez-Marquez, D. E. Salazar, and C. Yajure, "Assessing the Vulnerability of a Power System Through a Multiple Objective Contingency Screening Approach," *IEEE Trans. Reliab.*, vol. 60, no. 2, pp. 394–403, Jun. 2011. DOI: https://doi.org/10.1109/TR.2011.2135490

[21] J. (Naval P. S. Salmeron, K. (Naval P. S. Wood, and R. (University of T. at A. Baldick, "Optimizing Electric Grid Design Under Asymmetric Threat (II)," *Security*, no. December, p. 79, 2006.

[22] J. Salmeron, K. Wood, and R. Baldick, "Analysis of Electric Grid Security Under Terrorist Threat," *IEEE Trans. Power Syst.*, vol. 19, no. 2, pp. 905–912, May 2004. DOI: https://doi.org/10.1109/TPWRS.2004.825888

[23] R. Alvarez, J. (Naval P. S. Salmeron, and K. (Naval P. S. Wood, "*Interdicting Electrical Power Grids,*" Naval Postgraduate School, 2004.

[24] P. T. C., K. G. Boroojeni, M. Hadi Amini, N. R. Sunitha, and S. S. Iyengar, "Key pre-distribution scheme with join leave support for SCADA systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 24, pp. 111–125, Mar. 2019. DOI: https://doi.org/10.1016/j.ijcip.2018.10.011

[25] A. Delgadillo, J. M. Arroyo, and N. Alguacil, "Analysis of Electric Grid Interdiction With Line Switching," *IEEE Trans. Power Syst.*, vol. 25, no. 2, pp. 633–641, May 2010. DOI: https://doi.org/10.1109/TPWRS.2009.2032232

[26] J. Yan, H. He, X. Zhong, and Y. Tang, "Q-Learning-Based Vulnerability Analysis of Smart Grid Against Sequential Topology Attacks," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 1, pp. 200–210, Jan. 2017. DOI: https://doi.org/10.1109/TIFS.2016.2607701

[27] M. Sahraei-Ardakani, X. Li, P. Balasubramanian, K. W. Hedman, and M. Abdi-Khorsand, "Real-Time Contingency Analysis With Transmission Switching on Real Power System Data," *IEEE Trans. Power Syst.*, vol. 31, no. 3, pp. 2501–2502, May 2016. DOI: https://doi.org/10.1109/TPWRS.2015.2465140

[28] J. Aghaei, A. Nikoobakht, M. Mardaneh, M. Shafie-khah, and J. P. S. Catalão, "Transmission switching, demand response and energy storage systems in an innovative integrated scheme for managing the uncertainty of wind power generation," *Int. J. Electr. Power Energy Syst.*, vol. 98, no. August 2017, pp. 72–84, Jun. 2018. DOI: https://doi.org/10.1016/j.ijepes.2017.11.044

[29] M. Jabarnejad, "Approximate optimal transmission switching," *Electr. Power Syst. Res.*, vol. 161, pp. 1–7, Aug. 2018. DOI: https://doi.org/10.1016/j.epsr.2018.03.021

[30] Q. Wang, J. Watson, and Y. Guan, "Two-stage robust optimization for N-k contingency-constrained unit commitment," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2366–2375, Aug. 2013. DOI: https://doi.org/10.1109/TPWRS.2013.2244619