Seguridad cibernética en las redes eléctricas inteligentes

Amenazas y desafíos

Y. Sáez[1], E. Collado[2]
[1]Universidad Tecnológica de Panamá, [2]Texas A&M University
yessica.saez@utp.ac.pa, edwin.collado@tamu.edu

Resumen: *la red eléctrica inteligente, mejor conocida como Smart Grid, promete aumentar la capacidad, fiabilidad y eficiencia de la red eléctrica actual a través de la participación de los consumidores y la convergencia de la tecnología de la información con la red eléctrica existente. Sin embargo, esta integración crea una nueva serie de puntos vulnerables causados por intrusión cibernética y corrupción, que pueden conducir a efectos físicos devastadores y grandes pérdidas económicas. El objetivo de este trabajo es documentar y proporcionar una visión general sobre los principales requerimientos de seguridad cibernética, los posibles tipos de ataques, y los desafíos que enfrentan las redes eléctricas inteligentes. Además, se proponen estrategias y tecnologías que podrían ayudar a reducir o mitigar la ejecución de ataques exitosos en las mismas.*

Palabras claves: *Smart Grid, red eléctrica inteligente, seguridad cibernética, amenazas, vulnerabilidades, ataques cibernéticos.*

Title: *Cyber security of the Smart Grid: Threats and Challenges*

Abstract: *the intelligent power grid, better known as Smart Grid, promises to improve the capacity, reliability and efficiency of existing electricity grid through the participation of consumers and the convergence of information technology with the current electricity grid. However, this integration creates a new set of vulnerabilities caused by cyber intrusion and corruption that can lead to devastating physical effects and economic losses. The main objective of this work is to document and to provide an overview of the main requirements of cyber security, the possible types of attacks, and the challenges that the intelligent power grids faces. In addition, strategies and technologies that could help reduce or mitigate the execution of attacks on these networks are proposed.*

Key words: *Smart Grid, intelligent power grid, cyber security, threats, vulnerabilities, cyber attacks.*

Tipo de artículo: original
Fecha de recepción: 13 de julio de 2016
Fecha de aceptación: 16 de noviembre de 2016

1. Introducción

Actualmente la distribución de energía eléctrica se realiza a través de un sistema en su mayoría mecánico, con un uso modesto de sensores, con una mínima comunicación y con muy poco control electrónico para monitorear y controlar dispositivos de la red. Dado el rápido incremento en el consumo de energía y la complejidad de la infraestructura del sistema eléctrico, la industria energética ha iniciado la búsqueda de una solución que permita mejorar el rendimiento de la red eléctrica actual, con el objetivo de servir eficientemente al alto número de consumidores esperados en el futuro. En años recientes, se ha escuchado hablar sobre la red eléctrica inteligente o "Smart grid" como una solución prometedora a este problema. Este término ha sido utilizado ampliamente en muchos aspectos, por lo que su definición es considerablemente dinámica. Energía y Sociedad define la "Smart Grid" como "una red que integra de manera inteligente las acciones de los usuarios que se encuentran conectados a ella – generadores, consumidores y aquellos que son ambas cosas a la vez–, con el fin de conseguir un suministro eléctrico eficiente, seguro y sostenible" [1]. En otras palabras, la red eléctrica inteligente permitirá la optimización de generación y almacenamiento, transporte, distribución, y el consumo de energía, lo que asegurará la fiabilidad, la conservación de la energía y la mitigación de los impactos ambientales y económicos.

La figura 1 ilustra la arquitectura general de la red eléctrica inteligente basada en el modelo conceptual del Instituto Nacional de Normas y Tecnología de los Estados Unidos (NIST) [2]. Este tipo de redes eléctricas prometen aumentar la capacidad, fiabilidad y eficiencia a través de la participación de los consumidores y la convergencia de la tecnología de la información y comunicaciones con la red eléctrica existente. Sin embargo, esta integración crea una nueva serie de puntos vulnerables causados por intrusión cibernética y corrupción que pueden conducir a efectos físicos devastadores y grandes pérdidas económicas. De hecho, una acción maliciosa en una parte de la infraestructura de la red eléctrica podría crear caos en el mercado eléctrico y efectos globales rápidamente, por el hecho de que la misma provee interconexión con otras infraestructuras críticas como lo son el transporte, las telecomunicaciones, la salud pública, banca y finanza, suministro de agua, servicios de seguridad, entre otros.

Incidentes recientes, incluyendo ataques cibernéticos [3], demuestran que la infraestructura del sistema eléctrico está alcanzando un nivel de complejidad e interconexión que lo hace particularmente vulnerable a interrupciones de energía [4], [5]. Esto ha generado una preocupación razonable que ha conducido a cuestionamientos acerca de la seguridad en los sistemas eléctricos.

Dado que la investigación sobre seguridad cibernética de la red eléctrica inteligente se encuentra aún en su fase inicial de desarrollo, el objetivo de este trabajo es arrojar luces sobre posibles futuras direcciones de investigación para la seguridad de dicha red. Específicamente, este trabajo busca proporcionar una visión general sobre las principales amenazas cibernéticas y ataques que pueden afectar la seguridad y el rendimiento de la red eléctrica inteligente. El resto de este trabajo está organizado de la siguiente manera: la Sección 2 describe la seguridad cibernética en forma general, la Sección 3 discute los objetivos y requerimientos necesarios para asegurar las redes eléctricas inteligentes, la Sección 4 resume los principales ataques cibernéticos presentes en estas redes, la Sección 5 analiza los principales desafíos cibernéticos que enfrenta la industria energética, y finalmente la Sección 6 provee conclusiones y recomendaciones que pueden ser de gran utilidad en el diseño

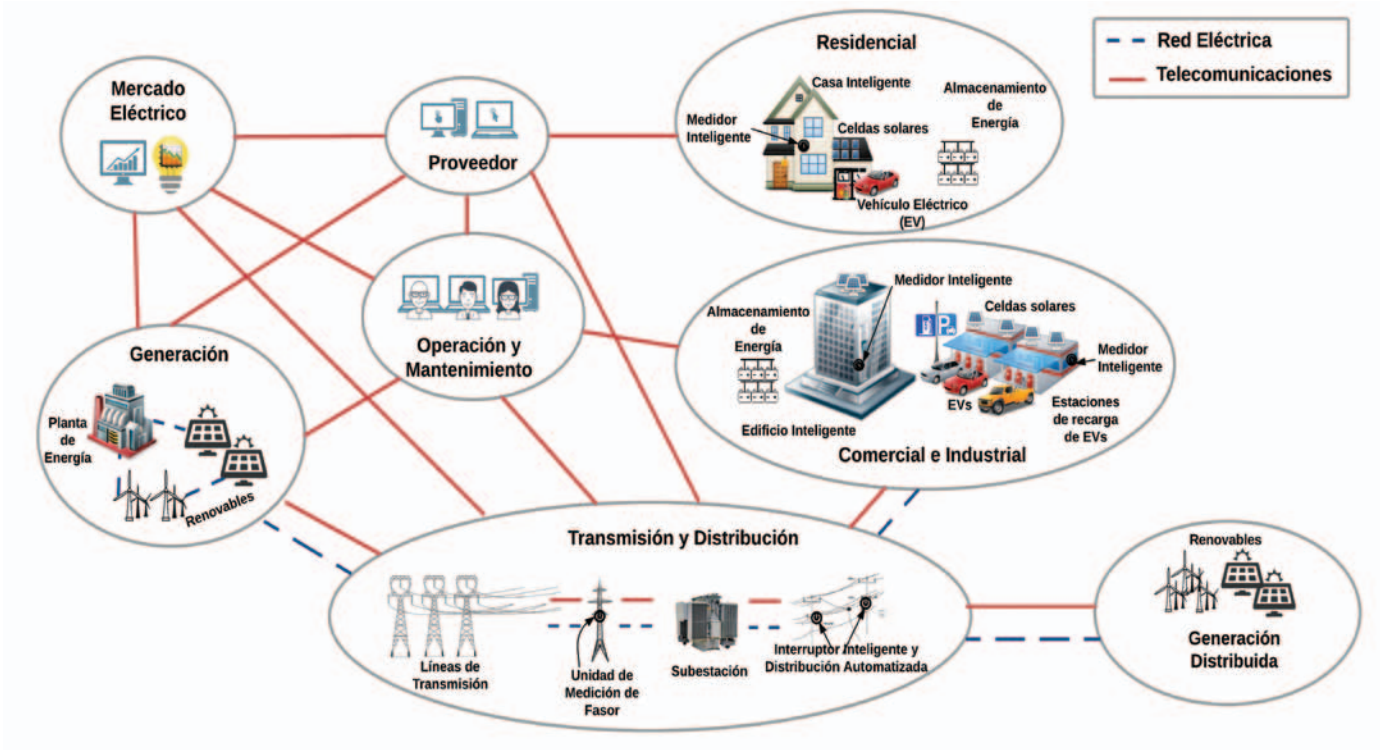

Figura 1. Arquitectura general de la red eléctrica inteligente (Creada por Sáez y Collado, adaptada de [2]).

de soluciones y estrategias de defensa para mejorar la seguridad cibernética en los sistemas informáticos y de comunicación de las redes eléctricas inteligentes.

2. Seguridad cibernética en las redes eléctricas inteligentes

La infraestructura cibernética de las redes eléctricas inteligentes incluye los sistemas y servicios de información electrónica y de comunicación y la información contenida en los mismos. Dichos sistemas y servicios están compuestos por el *hardware* y *software* utilizado para procesar (acceder, crear, modificar y destruir), almacenar y transmitir (intercambiar y distribuir) información [6]. Los ataques a la infraestructura cibernética, pueden causar fallas operacionales y de sincronización que afectarían componentes críticos, lo cual puede interrumpir el suministro de energía y causar pérdidas económicas. Por esto, es indispensable involucrar la seguridad cibernética en el proceso de diseño de la red eléctrica inteligente [7].

La incorporación de nuevas tecnologías a la red eléctrica actual aumenta la complejidad de la misma y con ello, aumenta también el número de riesgos. Por ejemplo, los nuevos nodos en la red eléctrica generan nuevos puntos de entrada que los agresores podrían explotar. Además, nuevas amenazas a sistemas de computadoras aparecen día a día debido al rápido incremento de herramientas de "hacking" sofisticadas, por lo tanto, cualquier enlace de telecomunicaciones dentro de la red eléctrica representa una vía potencialmente insegura en la operación de la misma.

Aunque que la destrucción física directa de generadores, subestaciones, y líneas de energía puede ser la estrategia más obvia para causar apagones, otras actividades que ponen en peligro el funcionamiento de los sensores, dispositivos de comunicación y sistemas de control mediante la suplantación de identidad o el envío de comandos incorrectos a los centros de control, también podrían interrumpir el sistema, causar apagones, y en algunos casos producir daños físicos a componentes críticos del sistema. Además, la digitalización de la red eléctrica habilita la posibilidad de ataques remotos. Por ejemplo, la implementación de la infraestructura de medición avanzada o "Advance Metering Infraestructure" (AMI) [8], [9], ampliamente considerada como uno de los primeros pasos en la digitalización de los sistemas de control de la red eléctrica, genera nuevas amenazas a la red, tales como: la fabricación de las lecturas del medidor de energía, manipulación de los costos de energía, el envío de señales de control falsas y códigos maliciosos.

Como consecuencia, la seguridad cibernética es una prioridad clave y debe incluirse en todas las etapas o fases del ciclo de vida del desarrollo de las redes eléctricas inteligentes, desde la fase de diseño, hasta las fases de implementación y mantenimiento. La planeación e implementación de estrategias de seguridad cibernética puede reducir las probabilidades de ataques exitosos y minimizar los impactos de aquellos que logran ejecutarse.

3. Objetivos y requerimientos de seguridad en las redes eléctricas inteligentes

La fiabilidad de las redes eléctricas inteligentes se basa en la confianza, la seguridad y la disponibilidad del control de los sistemas

de aplicación de comunicaciones [10]. Antes de seleccionar e implementar medidas y soluciones de seguridad cibernética que garanticen un funcionamiento seguro y fiable, es esencial entender cuáles son los objetivos y requisitos de seguridad de la red eléctrica.

A continuación, se describen los principales objetivos y requerimientos de seguridad para la red eléctrica inteligente [11].

3.1 Objetivos de seguridad

La seguridad en las redes eléctricas inteligentes definitivamente implica la protección y seguridad de la información. Los criterios de protección de la información generalmente se especifican en políticas tales como la disponibilidad, integridad y confidencialidad. NIST ha definido estas políticas de seguridad de la siguiente manera [2]-[11]:

- Disponibilidad: garantizar el acceso y utilización oportuna y confiable de la información. Esta es una de las tareas más importantes de las redes eléctricas inteligentes, puesto que una pérdida de disponibilidad representa la interrupción del acceso y uso de la información, lo cual podría debilitar la gestión y entrega de energía.
- Integridad: asegurar que la información no sea alterada de manera no autorizada. Esta política protege contra la modificación y destrucción inapropiada de la información, asegurando de esta manera el no repudio y la autenticidad de la misma.
- Confidencialidad: preservar la restricción de acceso y divulgación de la información. Esta política aborda la protección de la propiedad de la información asegurando que información sensible no sea divulgada a personas, entidades o procesos no autorizados.

3.2 Requerimientos de seguridad

Como se ha mencionado anteriormente, los requisitos generales para un alto nivel de seguridad son disponibilidad, integridad y confidencialidad. No obstante, adicionalmente a dichos objetivos, el NIST [11] también recomienda ciertos requisitos de seguridad específicos para la red eléctrica inteligente, los cuales abarcan tanto la seguridad cibernética como la seguridad física. Como este artículo está enfocado en la seguridad de los sistemas informáticos y de redes de comunicación, a continuación, se presentan algunos de los requisitos de seguridad cibernética más importantes para la red eléctrica inteligente basados en el estudio desarrollado en [11].

- **Privacidad:** a medida que la red eléctrica inteligente llega a los hogares y negocios, los clientes participan cada vez más en la gestión de su energía. Por lo tanto, la privacidad de la información se ha convertido en una preocupación cada vez grande. Los medidores inteligentes [8], [9] y el manejo de carga en las redes eléctricas inteligentes involucran la utilización de patrones de uso de electricidad que podrían revelar información privada [12], [13]. Por ejemplo, usuarios maliciosos podrían utilizar patrones de consumo para determinar no solamente cuánta energía se utiliza en una residencia o edificio, sino también para saber si los consumidores se encuentran o no en los mismos y así poder ejecutar ataques. También, los delincuentes podrían utilizar la información de estos patrones para perjudicar a consumidores específicos (robo de identidad). Como resultado, varias preocupaciones sobre privacidad deben ser abordadas. Afortunadamente, las tecnologías relacionadas con privacidad están muy bien desarrolladas y las soluciones de privacidad específicas necesarias dependerán del tipo de recurso de comunicación protegido [14].
- **Detección de ataques y respuesta rápida a incidentes:** la red eléctrica inteligente es una red de comunicación que comprende una gran cobertura. Por lo tanto, resulta prácticamente imposible proteger cada nodo de la red. Como resultado, es recomendable realizar consistentemente verificaciones de perfiles, pruebas y comparaciones para monitorear el estado del tráfico de la red con

Tabla 1. Ataques maliciosos a la red eléctrica inteligente

Según amenaza	Objetivo de seguridad afectado	¿Activo o pasivo?	Ejemplos
Intercepción (cuando personal no autorizado obtiene acceso a datos, dispositivos o componentes del entorno cibernético)	Confidencialidad	Pasivo (por lo general no puede ser detectado pero puede ser prevenido con criptografía)	Denegación de servicios (o "DoS, Denial of service"), espionaje, monitoreo de tráfico de datos
Modificación (cuando se obtiene acceso y se realizan modificaciones a datos, dispositivos o componentes del entorno cibernético de forma deliberada e ilegal)	Integridad	Activo (puede ser detectado con criptografía)	Modificación de señales de control, modificación de datos de sensores, modificación de información (por ejemplo utilización de energía)
Interrupción (cuando datos, dispositivos o componentes del entorno cibernético son destruidos o convertidos en no disponibles con el objetivo de retrasar, bloquear o perjudicar la comunicación en la red inteligente)	Disponibilidad	Activo (puede ser detectado, pero por lo general no se previene)	Eliminación de enrutamiento, interferencia de enlaces de comunicaciones, modificación de software para evitar ejecución precisa, borrado de datos
Fabricación (cuando personal no autorizado inserta objetos (por ejemplo datos o componentes) falsos en el sistema.	Autenticidad	Activo (puede ser detectado con criptografía)	Ataques por saturación, inserción de señales de control falsas, inserción de transacciones financieras falsas con fines de lucro

• Fuente: Adaptado de [14], [18]

la finalidad de detectar e identificar incidentes anormales debido a ataques. Los autores en [11], proporcionan recomendaciones relacionadas a la respuesta a incidentes, incluyendo políticas y procedimientos para la supervisión de respuesta a incidentes, manipulación, elaboración de informes, pruebas, capacitación, recuperación y reconstitución de los sistemas de información de redes inteligentes.

- **Continuidad de operaciones:** un sistema de información de redes eléctricas inteligentes debe tener la capacidad de continuar o reanudar las operaciones en caso de interrupción de su funcionamiento normal. El trabajo presentado en [11] introduce un conjunto de recomendaciones sobre políticas y procedimientos de funciones y responsabilidades, centros de almacenamiento alternativos, métodos alternativos de mando y control, centros de control alternativos, recuperación y reconstitución y respuesta a prueba de fallas, entre otra información referente a la continuidad de las operaciones de la red eléctrica inteligente.
- **Identificación, autenticación y control de acceso:** las redes eléctricas inteligentes están conformadas de millones de dispositivos electrónicos y sistemas de información inteligentes. Por tanto, la identificación y autenticación deben ser procedimientos clave para verificar la identidad de un usuario o dispositivo y un prerrequisito para obtener acceso a recursos en el sistema de información de la red eléctrica inteligente. El enfoque de este control de acceso es asegurar que los recursos solo sean accedidos por personal apropiado y debidamente identificado. Para lograr esto, cada nodo en la red debe tener al menos funciones criptográficas básicas para realizar autenticaciones y encripción de datos.
- **Auditoría y responsabilidad:** las auditorías periódicas se utilizan para detectar brechas en los servicios de seguridad a través del examen de los registros del sistema de información de redes inteligentes. El registro es necesario para la detección de anomalías, así como el análisis forense. Con la convergencia de los sistemas eléctricos tradicionales y la tecnología de la información, el análisis correcto de la información de eventos (por ejemplo, interrupción del servicio eléctrico) es necesario con el fin de entender lo que ocurrió durante el evento.

4. Ataques a la red eléctrica inteligente

Un ataque cibernético se refiere a una acción no deseada realizada a la infraestructura y sistema de información y comunicación, explotando una vulnerabilidad en la misma [7]. En las redes de comunicación, los ataques a la seguridad pueden provenir tanto de usuarios egoístas que violan protocolos de seguridad con el objetivo de obtener más recursos de la red que aquellos usuarios legítimos [15], así como también de usuarios maliciosos cuyo objetivo es adquirir, modificar o alterar ilegalmente la información de la red [16]. Aunque ambos tipos de usuarios causan problemas de seguridad en las redes de comunicación, los usuarios maliciosos resultan ser de mayor preocupación en las redes eléctricas inteligentes debido a la cantidad de dispositivos de computación electrónicos utilizados para monitorear y controlar la red [11], [16].

En forma general, los ataques a los sistemas de comunicaciones se pueden clasificar en activos y pasivos [17], [18]. Los ataques activos intentan alterar los recursos del sistema y afectar la operación del mismo, mientras que los pasivos solo buscan conocer o escuchar información del sistema, pero sin afectar los recursos del mismo. Enumerar todos los posibles tipos de ataques a la red eléctrica inteligente resulta impráctico debido a su complejidad y larga escala. Sin embargo, este documento se enfoca en los ataques maliciosos, los cuales pueden ser clasificados según su amenaza, resaltando el impacto que tienen a los objetivos de seguridad [16], como se observa en la tabla 1.

5. Desafíos de la seguridad cibernética

Los sistemas de control utilizados en la red eléctrica fueron originalmente diseñados y desarrollados para trabajar de forma independiente de la red de comunicaciones. Eventualmente, estos sistemas han sido conectados a través de sistemas de comunicación sin tomar en cuenta los mecanismos necesarios para hacerlos seguros. Por tanto, uno de los desafíos que enfrentan las redes eléctricas inteligentes es el análisis y desarrollo de mecanismos y protocolos de seguridad apropiados para proteger tanto el dominio de los sistemas eléctricos como el dominio de los sistemas de comunicación y tecnología de información. Estos mecanismos deben brindar un balance de protección entre la parte física y cibernética.

Por otro lado, existe una gran variedad de tecnologías de comunicaciones utilizados en las redes eléctricas inteligentes: líneas telefónicas, fibra óptica, conexión inalámbrica, entre otras [19]. Cada una de estas tecnologías cuenta con mecanismos y estándares de seguridad propios, lo cual dificulta el desarrollo de un sistema de defensa uniforme. Por tanto, uno de los grandes retos que enfrenta la seguridad cibernética es desarrollar estrategias viables, suficientemente escalables, compatibles y adecuadas para ser implementadas en toda la red.

Los requerimientos de temporización para el envío de mensajes en las redes eléctricas inteligentes dependen del dominio (generación, mercado eléctrico, proveedor, operación y mantenimiento, transmisión y distribución, y consumidor) en que nos encontremos [16]. Consecuentemente, otro desafío práctico que afrontan los diseñadores de seguridad es que las soluciones de seguridad no solo deben proteger el intercambio de información, sino que también deben cumplir con los requisitos de comunicación y procesamiento de datos.

Hoy en día los operadores humanos son quienes en última instancia toman las decisiones y las acciones que controlan las operaciones del sistema. Por tanto, otro de los desafíos a los que se enfrenta la seguridad cibernética consiste en considerar factores como la fiabilidad de los operadores dentro de los centros de control y la posibilidad de que códigos inseguros o señales de control erróneas hayan sido generados o insertados en el sistema, ya que un suceso de estos podría tener consecuencias catastróficas. Por ejemplo, en septiembre de 2003, Italia y algunas partes de Suiza enfrentaron lo que se conoce como su mayor interrupción en el suministro de energía, el cual afectó a 56 millones de personas en total, resultando en enormes pérdidas financieras [2]. Dicho incidente ocurrió a causa de dificultades técnicas causadas por error humano y la comunicación ineficaz dentro de los operadores de la red eléctrica. Otro gran apagón debido al error humano reportado en [2], se produjo en Europa del

Oeste en noviembre del 2006, donde la comunicación insuficiente fue también un tema importante detrás de este incidente.

6. Discusión

La seguridad cibernética es uno de los principales retos de la transformación de las redes eléctricas. La misma debe ser construida como parte de su diseño, es decir, no debe incorporarse como una idea de último momento. Por lo tanto, identificar los posibles problemas que afectan la confidencialidad, integridad y disponibilidad del flujo de información en el sistema de la red eléctrica inteligente es indispensable al momento de investigar cuáles son las mejores prácticas de seguridad de la información que deben ser aplicadas a las redes y en qué medida pueden aplicarse.

En este caso, debido a que una sola medida de seguridad no puede contrarrestar todo tipo de amenaza en la red eléctrica inteligente, la estrategia de defensa a profundidad o seguridad en capas, es decir, la combinación estratégica de múltiples tecnologías de seguridad en cada capa del sistema de computación (por ejemplo en los sistemas de operaciones, base de datos, aplicaciones, redes, etc.), es una de las estrategias de defensa más recomendadas [14], [19]. Esta estrategia ayudaría a reducir riesgos de acceso sin autorización al sistema de comunicaciones y la infraestructura de tecnologías de la información, debido a fallas en una técnica de seguridad en particular. Igualmente, reduciría el riesgo y la probabilidad de ataques al incrementar el costo y complejidad para comprometer el sistema, en comparación con utilizar un solo mecanismo de seguridad. Algunas de las tecnologías de seguridad que deben ser consideradas dentro de esta estrategia son los firewalls, sistema de detección de intrusiones, antivirus, verificación de identidad a través de mecanismos de autenticación (incluyendo criptografía , firma de datos), uso de claves para protección contra *malware* en sistemas embebidos y sistemas de propósito general.

Además, tal como se menciona en [14], la arquitectura lógica de seguridad en las redes eléctricas inteligentes conlleva un constante proceso de cambio, debido a que de igual forma en que la tecnología evoluciona, también evolucionan las amenazas. Por lo tanto, es recomendable realizar evaluaciones de vulnerabilidades, por lo menos una vez al año, para asegurar que las herramientas y técnicas de seguridad estén acordes con las necesidades.

7. Conclusiones

Finalmente, diversas interrogantes relacionadas a la seguridad cibernética de sistemas y componentes específicos de las redes eléctricas inteligentes requieren mayor discusión, específicamente en temas sobre cómo y cuánta privacidad puede ser soportada, por lo que se recomienda ampliar este tema en publicaciones futuras.

Referencias

[1] (2010) Sitio web Energía y Sociedad. [Online]. Disponible en: http://www.energiaysociedad.es/

[2] (2014) Página web smart grid en NIST. [Online]. Disponible en http://www.nist.gov/smartgrid/upload/NIST-SP-1108r3.pdf

[3] A. Anwar, A. Mahmood, Cyber security of smart grid infrastructure, Pathan, A. P-S.K.,The State of the Art in Intrusion Prevention and Detection, Boca Raton, Florida: CRC Press/Taylor & Francis Group, 2014.

[4] Albert, Réka, István Albert, and Gary L. Nakarado. "Structural vulnerability of the North American power grid." Physical review E 69.2 (2004): 025103.

[5] Arianos, Sergio, et al. "Power grid vulnerability: A complex network approach." Chaos: An Interdisciplinary Journal of Nonlinear Science 19.1 (2009): 013119.

[6] I. Ghansah, "Smart Grid cyber security potential threats, vulnerabilities and risks," California Energy Commission, PIER Energy-Related Environmental Research Program, Sacramento, CA, CEC-500-2012-047, 2009.

[7] T. Baumeister, "Literature review on smart grid cyber security", Technical Report, 2010, [online] Available: http://csdl.ics.hawaii.edu/techreports/10-11110-11.pdf

[8] Karnouskos, Stamatis, Orestis Terzidis, and Panagiotis Karnouskos. "An advanced metering infrastructure for future energy networks." New Technologies, Mobility and Security. Springer Netherlands, 2007. 597-606.

[9] Depuru, Soma Shekara Sreenadh Reddy, Lingfeng Wang, and Vijay Devabhaktuni. "Smart meters for power grid: Challenges, issues, advantages and status." Renewable and sustainable energy reviews 15.6 (2011): 2736-2742.

[10] C.M., Shipman, K.M. Hopkinson, and J. Lopez, "Con-Resistant Trust for Improved Reliability in a Smart-Grid Special Protection System," IEEE Transactions on Power Delivery, vol.30, Issue-1, pp.455–462, Sept. 2014.

[11] The Smart Grid Interoperability Panel - Cyber Security Working Group, "Guidelines for smart grid cyber security," NISTIR 7628, 2010.

[12] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures," in Proc. of IEEE SmartGridComm, 2010, pp. 232–237.

[13] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," IEEE Security & Privacy, vol. 7, Issue-3, pp. 75–77, May-June 2009.

[14] D. Yadav and A.R Mahajan, "Smart Grid Cyber Security and Risk Assessment: An Overview," International Journal of Science, Engineering and Technology Research (IJSETR), vol. 4, Issue-9, pp. 3078–3085, Sept. 2015.

[15] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux, "On selfish behavior in CSMA/CA networks," in Proc. of IEEE INFOCOM, 2005, pp. 2513–2524.

[16] W. Wang and Z. Lu. "Cyber security in the Smart Grid: Survey and challenges," The International Journal of Computer and Telecommunications Networking, vol. 57, Issue-5, pp. 1344–1371, April 2013.

[17] R. Shirey, Página web RFC 2828 Internet Security Glossary en IETF.[Online]. Disponible en https://www.ietf.org/rfc/rfc2828.txt

[18] D. Kundur, "A tour of information security," Texas A&M University, Info_Security_ Handout, pp. 13-23, 2012.

[19] N. Poveda, C. Medina y M. Zambrano, "Tecnologías de comunicación para redes de potencia inteligentes de media y alta tensión," Prisma Tecnológico, Vol. 5, no. 1, pp. 29–32, 2014.

[20] S. M. Amin and A. M. Giacomoni, "Smart grid- safe, secure, self- healing: Challenges and opportunities in power system security, re- siliency, privacy," IEEE Power Energy Mag., Vol. 10, no. 1, pp. 33–40, Jan./Feb. 2012.