Retos de seguridad en redes inteligentes

Las redes inteligentes de distribución eléctrica tienen potencial para generar grandes beneficios económicos y ambientales. Sin embargo, también constituyen un ambiente en el que emergen múltiples retos para garantizar la seguridad de la información que se maneja.

Sandra Julieta Rueda Rodríguez

Las redes inteligentes de distribución de energía eléctrica, llamadas Smart Grids en inglés, recolectan y registran información en diversos puntos de su infraestructura y, con base en los datos recopilados, toman decisiones para mejorar la eficiencia de los mecanismos de distribución. Incluso, podrían reducir la pérdida de energía y el costo de producción y distribución, beneficiando al medio ambiente y a los consumidores.

Considerando las ventajas que ofrecen las redes inteligentes, los gobiernos y los operadores de energía, varios países ya han puesto en marcha planes para la instalación y desarrollo de sus redes. En la Unión Europea las diferentes iniciativas en el área están encaminadas a la integración de las redes de distribución de los diferentes países de la Unión [4], a actualizar la infraestructura y extender el número de clientes de la red [9]. La iniciativa gubernamental en los Estados Unidos está encaminada a actualizar la infraestructura e integrar los diversos consumidores a la red [2]. En cuanto a nuestros vecinos de América del Sur, los gobiernos de Brasil y Chile cuentan con sendos planes para apoyar el desarrollo de sus redes inteligentes. Finalmente, en Colombia la iniciativa en el desarrollo de redes inteligentes está liderada por diferentes empresas del sector eléctrico y universidades que adelantan diversos proyectos en tecnología de redes inteligentes.

Aunque los expertos en el área de distribución de energía creen firmemente en las ventajas del desarrollo de la tecnología de redes inteligentes, los expertos en seguridad informática han llamado la atención sobre algunos riesgos de seguridad que emergen, riesgos que se relacionan con el servicio mismo, así como con la privacidad de los usuarios.

Infraestructura de las Redes Inteligentes.

La columna vertebral de una red inteligente es una red de datos que recopila información sobre consumo constantemente y la comunica a un punto de control para que allí se tomen

decisiones que mejoren las condiciones de distribución.

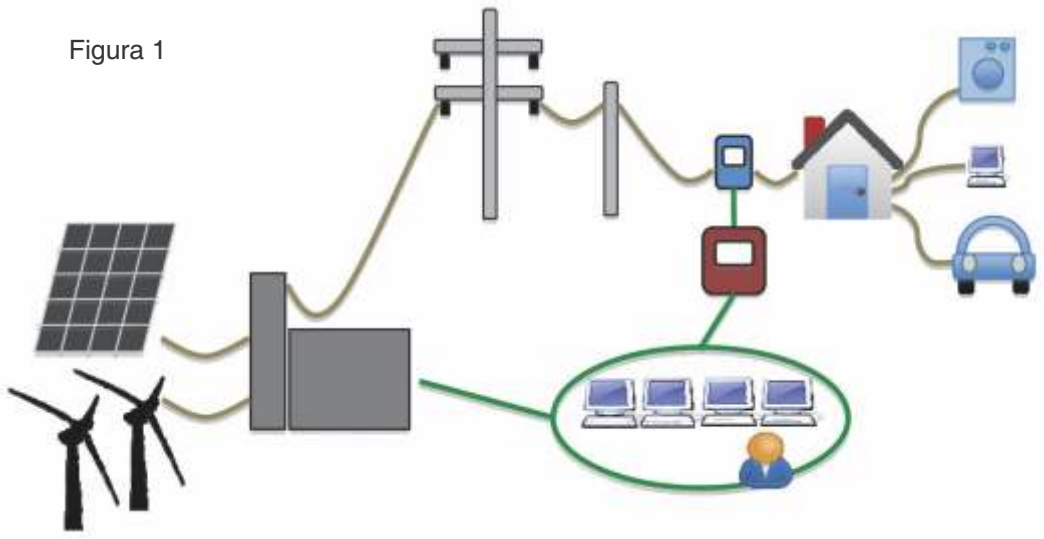
Una red inteligente tiene dos partes, una red de distribución y una red de datos. La red de distribución de energía está compuesta por las líneas de distribución y las fuentes tradicionales de generación de energía, como las hidroeléctricas. Además, tiene la capacidad de integrar la red de generación y distribución fuentes alternativas de energía, como páneles solares y granjas de viento.

La red de datos está integrada por medidores inteligentes, recolectores y centrales de datos. Los medidores inteligentes, conocidos en inglés como Smart meters, son dispositivos electrónicos con hardware de capacidad limitada, instalados en los puntos de consumo para medir y registrar uso de energía. Las características de hardware de un medidor inteligente varían dependiendo de la empresa que lo fabrica; algunos de los medidores disponibles actualmente en el mercado tienen procesadores de 32 bits con velocidades que varían entre 50 y 100 MHz, aproximadamente 256KB de memoria RAM, 512KB de memoria flash y un mecanismo para transmisión y recepción inalámbrica de datos. Además de enviar información, el medidor puede recibir y ejecutar comandos.

Los medidores se comunican periódicamente con un recolector, un dispositivo que recibe y almacena los datos de un área geográfica relativamente pequeña, un barrio, por ejemplo. Los recolectores a su vez se comunican, en uno o varios pasos, con la central de datos del operador de distribución de energía. La Figura 1 presenta el esquema de una red inteligente.

Figura 1. Esquema de la infraestructura de una red inteligente. La red está integrada por una red de generación y distribución de energía y una red de datos. La red de datos cuenta con medidores inteligentes (dispositivo azul en la figura) en los puntos de consumo, que miden y registran el uso de energía de forma continua. Los medidores envían la información a un punto de recolección (dispositivo rojo en la figura) que almacena información de varios medidores y luego la envía a la central de manejo de datos del operador de distribución de energía (anillo verde en la figura). La central toma decisiones para optimizar la distribución.

Figura 1



La “inteligencia” de la red se basa en su capacidad para medir el consumo en múltiples puntos de la infraestructura y reaccionar de acuerdo con la información recolectada. Los puntos en los que se toman medidas son diversos, por ejemplo, hogares, edificios, centros comerciales y fábricas. La reacción de la red también puede variar, por ejemplo, la red puede reenrutar recursos para cumplir con una demanda alta en horas pico, en un área determinada o puede reducir la producción en ciertos puntos cuando la demanda es baja.

Un operador de distribución también puede usar la información recolectada para crear modelos de distribución que incorporen mecanismos de resistencia y recuperación a fallas, optimicen la distribución e integren a la red, de forma coordinada, fuentes diversas de generación de energía. Los modelos también pueden predecir la demanda durante ciertos periodos de tiempo, lo que le permite a la red hacer algunos ajustes en su capacidad de distribución de forma proactiva. Además, pueden detectar los puntos en los que es necesario mejorar la infraestructura (crecer) porque la demanda se acerca mucho o ha llegado al límite de la capacidad de distribución.

Un usuario también puede usar sus propias medidas, las que se toman con un medidor inteligente a la entrada de su casa, para tomar decisiones que lo beneficien. Por ejemplo, si un operador de distribución establece tarifas altas para horas pico, un usuario puede ajustar su consumo durante estas horas y reducir costos.

Riesgos de Seguridad

Los beneficios económicos y ambientales de las redes inteligentes son evidentes y los expertos en el área de transmisión y distribución de energía creen firmemente en las ventajas de esta tecnología. Sin embargo, los expertos en seguridad informática resaltan los retos que emergen en este ambiente y trabajan en el desarrollo de mecanismos de protección.

Manipulación de la información. De acuerdo con investigadores en los Estados Unidos, los medidores inteligentes son un objetivo muy atractivo para los adversarios. Si los medidores son comprometidos, los adversarios pueden montar ataques remotos a gran escala con consecuencias como manipulación masiva de información, fraude y denegación del servicio [6]. De hecho, investigadores en ese país desarrollaron un gusano de prueba que se podía propagar entre medidores inteligentes para mostrar de forma conceptual que el riesgo es real [3]. Sin las medidas de seguridad apropiadas, los adversarios pueden atacar, además de los medidores inteligentes, la información transmitida entre los medidores y los recolectores.

Seguridad de la infraestructura. La manipulación de información y del servicio no es el único objetivo que puede atraer a los adversarios. El año pasado diversos medios publicaron detalles técnicos de Stuxnet, un gusano cuyo propósito era atacar un conjunto definido de sistemas de control industrial, conocidos en inglés como Supervisory Control and Data Acquisitionsystems, SCADA. Los investigadores de Symantec señalan que el gusano se valía de varias vulnerabilidades, incluyendo una vulnerabilidad desconocida hasta el momento (zero-dayexploit) para ingresar a un sistema y propagarse, además incorporaba técnicas sofisticadas para evadir programas antivirus. Una vez el gusano entraba en un sistema, era capaz de reprogramarlo ocasionando daño físico a algunos componentes [8]. Stuxnet demuestra que un programa malicioso puede ocasionar daño físico a algunos elementos del mundo real. Aunque los expertos en programas maliciosos están de acuerdo

en que Stuxnet es sumamente sofisticado y seguramente no se produzca un programa malicioso de calidad semejante con frecuencia, el riesgo es real, un gusano con las características de Stuxnet podría alterar o dañar componentes físicos de una red inteligente.

Privacidad del usuario. Aunque la información que los medidores inteligentes registran para cada usuario se recolecta y procesa con dos objetivos claros, calcular la factura de consumo y optimizar la distribución, esta información puede ser usada con fines diferentes. Quienes trabajan en el área de seguridad informática seguramente están acostumbrados a encontrar situaciones en las que un sistema que se diseña con un propósito especial, termina siendo usado para un propósito totalmente diferente.

En el caso de las redes inteligentes, la información de consumo describe el comportamiento del usuario o de los usuarios a quienes pertenece [7]. A partir de esta información es posible obtener información privada, como el número aproximado de personas que viven en un hogar, la hora a la que salen, la hora a la que regresan y en algunos casos, la lista de electrodomésticos instalados.

En cierta forma, este problema no es exclusivo de las redes inteligentes. A comienzos de este año el Supervisor Europeo de Protección de Datos, la entidad de la Unión Europea para la protección de datos, pidió a Google un tiempo para revisar su nueva política de seguridad y las consecuencias que ella podría traer para los ciudadanos de la Unión. La nueva política de Google explica la intención de recolectar y procesar los datos de los usuarios para prestar un mejor servicio. Estos datos incluyen información que el usuario facilita por voluntad propia, al registrarse por ejemplo, así como información que Google deduce a partir del acceso a uno de sus servicios, por ejemplo información del dispositivo, ubicación física y cookies que Google comparte con sus socios de negocios.

Desde un punto de vista técnico, la situación de Google y de las redes inteligentes es la misma: una organización recopila información que describe con cierto detalle el comportamiento de sus usuarios. El objetivo es prestar un mejor servicio, pero la información puede ser usada con fines diferentes por la entidad que almacena la información o por terceros maliciosos que la obtienen de forma ilícita.

Preparación para la llegada de las redes inteligentes

En la Unión Europea y los Estados Unidos los planes para el desarrollo de la tecnología de redes inteligentes ya están en marcha. En Colombia la empresa privada, algunos operadores y las universidades lideran el desarrollo. Lo cierto es que el gobierno, los operadores de distribución y los usuarios deben prepararse para la llegada de esta tecnología.

Políticas. El uso y expansión de Internet como soporte a diversas tareas del quehacer diario ha llevado a los gobiernos a estudiar el desarrollo de leyes para la protección de los datos personales de sus ciudadanos. La Unión Europea, por ejemplo, cuenta con la directiva de protección de datos, la cual establece límites sobre los datos personales que una entidad puede recolectar y cómo los puede procesar. El Gobierno de los Estados Unidos define ciertos lineamientos, pero prefiere que los proveedores de servicios y los usuarios se autoregulen porque aunque sus ciudadanos creen firmemente en su derecho a la privacidad, principios fundamentales de su constitución protegen el libre flujo de información. [1]

En Colombia, la Corte Constitucional recientemente "avaló gran parte del texto de la futura ley de protección de datos personales" [5], la cual dicta disposiciones para la protección de los datos personales en Colombia. De acuerdo con el texto del proyecto de ley, un dato personal es cualquier información vinculada o que pueda asociarse con una o varias personas naturales determinadas o determinables. La ley establece que la información sujeta a tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. La definición de dato personal parece aplicar de forma natural a la información que pueda ser recopilada por una red inteligente en los hogares y negocios de los ciudadanos Colombianos, para luego ser procesada con la intención de ofrecer un mejor servicio.

El Gran Hermano. En la novela 1984 de George Orwell, el gran hermano vigila constantemente a las personas e intenta controlar todas sus acciones y pensamientos. Si bien la tecnología de redes inteligentes de distribución tiene el potencial de generar beneficios económicos y ambientales, hay quienes se preocupan por la información que pone en las manos de los operadores de distribución de energía y de las organizaciones que tendrían acceso "legal" a tal información. Sin embargo, deberíamos reconocer que hoy en día ya hemos entregado "voluntariamente" una gran cantidad de información acerca de nosotros mismos. Usamos a diario teléfonos celulares, buscadores, redes sociales y servicios web que recopilan nuestra información y construyen un perfil para ofrecer un mejor servicio. Las redes inteligentes solamente generarían una porción adicional de información.

Percepción de los Usuarios. Mientras los ciudadanos de la Unión Europea y los Estados Unidos consideran gran variedad de datos como datos personales y por tanto privados, los colombianos parecen tener una percepción diferente.

Como parte de un trabajo sobre privacidad de datos en Internet, los estudiantes del curso Seguridad de Aplicaciones Web del Departamento de Ingeniería de Sistemas y Computación de la Universidad de los Andes encuestaron a 140 personas con diferentes perfiles (edad, ocupación, manejo de tecnología). Aunque la muestra no es suficiente para sacar conclusiones sobre la percepción de la población en general, esta deja ver una tendencia. La mayoría de los encuestados dan gran importancia a la protección de datos bancarios (número de cuenta, tarjetas de crédito, etc.) y de su información en redes sociales (cuenta de usuario, fotos, lista de contactos, etc.). Sin embargo, un tercio de los encuestados (48/140) dice que sus hábitos de navegación son información pública y no necesitan ser protegidos. Esta percepción es extraña, considerando que los hábitos de navegación de una persona pueden revelar detalles de su vida privada.

Así como un tercio de los encuestados no considera que los hábitos de navegación son datos personales, es posible que algunos ciudadanos consideren que su perfil de consumo de energía es público y no necesita ser protegido. El gobierno, los operadores de distribución o las organizaciones de protección del consumidor deberán asumir la tarea de educar a los usuarios para defender su privacidad o al menos entender los riesgos.

Mecanismos de protección. Muchas industrias y universidades en diferentes países adelantan proyectos de investigación y desarrollo para mejorar la tecnología de las redes inteligentes. Tales proyectos incluyen, entre otros, diseños de medidores inteligentes con coproce-

sadores eficientes para cifrar y descifrar la información, tratando de mantener un consumo bajo de poder, desarrollo de herramientas que las empresas que manufacturan los medidores inteligentes pueden usar para adelantar evaluaciones de penetración de forma semiautomática y algoritmos para ajustar el perfil de consumo, de tal manera que resuma la información que el operador de distribución necesita, mientras elimina las características que revelan detalles del comportamiento del usuario.

Conclusión

Las redes inteligentes de distribución eléctrica están diseñadas para tomar decisiones, de forma proactiva, que mejoren la eficiencia de sus mecanismos de distribución. Los expertos en distribución y transmisión de energía están de acuerdo sobre los beneficios económicos, sociales y ambientales que las redes inteligentes pueden generar. Sin embargo, los expertos en seguridad informática llaman la atención sobre las políticas y mecanismos de seguridad necesarios de implementar para proteger la infraestructura y a los usuarios. La lección que nos queda es sencilla: la llegada de la tecnología de redes inteligentes está cerca y es ventajosa, simplemente debemos prepararnos de forma adecuada para manejar los problemas de seguridad que pueden surgir en este nuevo ambiente.

Referencias

[1] William Clinton, Albert Gore. A Frameworkfor Global Electronic Commerce,1997. http://www.w3.org/TR/NOTE-framework-970706#privacy, consultado en Abril 2012.

[2] US Energy Independence and Security Act. EISA, 2007.

[3] Recoverable Advanced Metering Infrastructure. Mike Davis. Black Hat, 2009.

[4] Grid+ Project. www.gridplus.eu, consultado en Abril 2012.

[5] Observatorio de Protección de Datos Personales en Colombia. www. habeas data.org.co, consultado en Abril 2012.

[6] Security and PrivacyChallenges in the Smart Grid. Patrick McDaniel y Stephen McLaughlin. Revista IEEE Seguridad y Privacidad (IEEE Security and Privacy), Mayo-Junio 2009.

[7]ProtectingConsumerPrivacyfrom Electric Load Monitoring. Stephen McLaughlin, Patrick McDaniel y William Aiello. Conferencia ACM en Seguridad de Computadores y Comunicaciones (Computer and Communications Security), Octubre 2011.

[8]Stuxnetworm hits industrial systems. Robert McMillan. www.computerworld.com, consultado en Abril 2012.

[9] Smart GridsEuropean Technology Platform (SmartGridsETP). www.smartgrids.eu, consultado en Abril 2012.

Sandra Julieta Rueda Rodríguez. *Profesora asistente, Departamento de Ingeniería de Sistemas y Computación, Universidad de Los Andes, Colombia. PhD en ComputerScience and Engineering de The Pennsylvania StateUniversity, Estados Unidos. Áreas de interés: seguridad de sistemas de software, modelos de control de acceso y verificación semiformal de políticas de seguridad.*