GESTIÓN Y CIBERSEGURIDAD PARA MICRORREDES ELÉCTRICAS RESIDENCIALES

Elvis Eduardo Gaona García
David Gustavo Rosero Bernal
Eduardo Alirio Mojica Nava
César Leonardo Trujillo Rodríguez
Nelson Leonardo Díaz Aldana

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Doctorado en Ingeniería
UNIVERSIDAD DISTRITAL "FRANCISCO JOSÉ DE CALDAS"

Elvis Eduardo Gaona García

Profesor Titular Universidad Distrital Francisco José de Caldas, Ingeniero Electrónico, Especialista en Telecomunicaciones Móviles, Magíster en Ciencias de la Información y las Comunicaciones y Doctor en Ingeniería, Director del Grupo de Investigación en Telecomunicaciones de la Universidad Distrital – GITUD.

David Gustavo Rosero Bernal

Empresario, catedrático, estudiante Doctorado en Ingeniería de la Universidad Distrital Francisco José de Caldas. Ingeniero Electrónico, Magíster en Ingeniería Electrónica y de Computadores, Magíster en Administración de Empresas, Investigador del Laboratorio de Investigación en Fuentes Alternativas de Energía - LIFAE.

Eduardo Alirio Mojica Nava

Profesor Asociado, Universidad Nacional de Colombia, Sede Bogotá.
Ingeniero Electrónico, Magíster en Ingeniería Electrónica y Computadores, Doctor en Automatización e Informática Industrial.

César Leonardo Trujillo Rodríguez

Profesor Titular Universidad Distrital Francisco José de Caldas, Ingeniero Electrónico, Magister en Ingeniería Eléctrica y Doctor en Ingeniería Electrónica, Investigador del Laboratorio de Investigación en Fuentes Alternativas de Energía – LIFAE.

Nelson Leonardo Diaz Aldana

Profesor Asociado, Facultad de Ingeniería, Universidad Distrital Francisco José de Cladas. Magister en Ingeniería Automatización Industrial y Doctor en Tecnologías Energéticas, Director del Laboratorio de Investigación en Fuentes Alternativas de Energía – LIFAE.

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Doctorado en Ingeniería
UNIVERSIDAD DISTRITAL "FRANCISCO JOSÉ DE CALDAS"

GESTIÓN Y CIBERSEGURIDAD PARA MICRORREDES ELÉCTRICAS RESIDENCIALES

Elvis Eduardo Gaona García
David Gustavo Rosero Bernal
Eduardo Alirio Mojica Nava
César Leonardo Trujillo Rodríguez
Nelson Leonardo Díaz Aldana

Gestión y ciberseguridad para microrredes eléctricas residenciales / Elvis Eduardo Gaona García ... [et al.]. -- 1a. ed. -- Bogotá : Universidad Distrital Francisco José de Caldas, 2020.

128 páginas ; 24 cm. -- (Doctorado en Ingeniería).

Incluye resumen en inglés. – Contiene referencias bibliográficas.

ISBN 978-958-787-228-6 (impreso) -- 978-958-787-229-3 (digital)

1. Redes eléctricas 2. Sistemas eléctricos 3. Distribución de energía eléctrica I. Gaona García, Elvis Eduardo II. Serie

CDD: 621.3192 ed. 23 CO-BoBN- a1057504

ISBN Impreso: 978-958-787-228-6
ISBN Digital: 978-958-787-229-3

Primera edición: octubre de 2020.

Corrección de estilo y diseño gráfico:
Amadgraf Impresores Ltda.
Impresión:
Amadgraf Impresores Ltda.

Doctorado en Ingeniería
Carrera 7 # 40B-53
Bogotá
Correo electrónico: investigacion.doctoradoing@udistrital.edu.co

Hecho el depósito legal.

Impreso y hecho en Colombia
Printed and made in Colombia.

Resumen

Las microrredes eléctricas han permitido la integración de recursos energéticos distribuidos con características diferentes y que se encuentren ubicados en un área específica, buscando garantizar el suministro de energía a una carga determinada. Esto ha permitido no solo que se permitan dar soluciones energéticas a comunidades apartadas en zonas no interconectadas a la red eléctrica convencional mediante el uso de fuentes de energías renovables y no convencionales. También, ha significado un cambio en el paradigma de como los usuarios convencionales de energía interactúan con los sistemas de generación y transmisión de energía convencionales. Esto, aprovechando las potencialidades de la Generación Distribuida (GD) y su integración mediante pequeñas microrredes, buscando garantizar su consumo energético reduciendo la dependencia de la red eléctrica.

Lo anterior sumado a un creciente interés por reducir el impacto de los sistemas convencionales de generación basados en combustibles fósiles en el medio ambiente, ha impulsado el uso de fuentes de energía renovables con menor impacto ambiental como la energía solar fotovoltaica o eólica dentro de usuarios residenciales. En este contexto surgen las microrredes residenciales o domiciliarias como una alternativa que permita reducir la dependencia energética de la red convencional, buscando ade-

más un beneficio en la reducción de las erogaciones mensuales, con menor impacto ambiental.

Por lo tanto, en una microrred residencial se debe garantizar la interacción confiable de sistemas de generación de energía con características de generación heterogénea y altamente variable con cargas de diferente naturaleza, principalmente electrónicas, las cuales deben estar disponibles para satisfacer los perfiles y necesidades de consumo de los habitantes del hogar. Para desarrollar esta tarea, se recurre a los sistemas de gestión de energía los cuales son responsables de coordinar y administrar todos los recursos energéticos y cargas, mediante un esquema de priorización de las mismas, dentro de la microrred residencial, de tal forma que se garantice la disponibilidad energética que los usuarios requieren para suplir sus necesidades básicas, soportados en sistemas de comunicaciones confiables entre las diferentes unidades distribuidas y el sistema de gestión de energía. Dentro de la estructura de gestión, se encuentra la capa cibernética de la microrred, basada en un sistema de comunicaciones en la cual se intercambian consignas de control para los diferentes generadores y cargas, así como información sobre perfiles y preferencias de consumo y generación.

Debido a la gran cantidad de información y complejidad en el manejo de esta, los sistemas de generación de energía en microrredes residenciales se ha venido soportando en tecnologías emergentes, pero ya bien posicionadas, como el Internet de las cosas (IoT por sus siglas en inglés), infraestructura de medición avanzada o incluso la computación en la nube buscando optimizar el manejo de información y una gestión energética más eficiente que responda a las necesidades de los usuarios.

Sin embargo, el uso de nuevas tecnologías soportadas en sistemas de comunicaciones significa un gran riesgo en el manejo de información y la confiabilidad de la microrred debido a su interacción con el sistema de gestión de energía. En este caso no solo se puede comprometer la estabilidad del sistema eléctrico. También, puede estar comprometida información sensible de los usuarios como preferencias de consumo, tiempos de

permanencia en el hogar, etc. que puede ser adquirida externamente sin consentimiento de los usuarios.

Por lo anteriormente descrito se plantea la necesidad de abordar la ciberseguridad de las microrredes eléctricas como temática principal de este libro. En el documento se abordan las características generales para un sistema de gestión de energía en microrredes residenciales y se explora la vulnerabilidad de sus sistemas de comunicaciones para finalizar con una exploración de estrategias y arquitecturas que garanticen la ciberseguridad de las microrredes domiciliarias.

Palabras Clave

Ciberseguridad, Microrredes Residenciales, Sistema de Gestión de Energía,

Abstract

Electrical microgrids have enabled the integration of distributed energy resources with different generation characteristics, but located locally into a well-defined area. The microgrids look for ensuring the energy supply for a specific load based on local energy resources. This fact has allowed not only the possibility of supply energy to remote communities, not interconnected to the utility grid, by means of the integration of renewable energy sources. Also, the microgrid concept has become a change in the paradigm of how electricity users interact with the conventional energy grid. All this is possible by taking advantage of the potentiality of heterogeneous distributed generators and their integration within microgrids, looking always ensuring the local consumption based on local resources while reducing the dependence of the utility grid.

Given the above points, and in addition to an increasingly growing concern for reducing the impact of conventional energy sources based on fossil fuels in the environment, those facts have driven the use of renewable energy sources with the minimum environmental impact such as photovoltaic panels and wind turbine generators within the household domine. In this context, the residential microgrid concept emerges as an alternative for reducing the dependence from the utility grid, loo-

king for an effective reduction on the energy bill, with a minimum environmental impact.

Therefore, in a residential microgrid, it is necessary to ensure proper interaction between heterogeneous and highly variable energy resources with loads of several different characteristics, mainly electronic loads, which should be available to satisfy the requirements of the household owners. To perform this important task, energy management systems are required for coordinating and managing all the distributed energy resources and loads within the residential microgrid, in such a way that reliability of the local energy system is ensured. To do this, the energy management system is supported on dedicated communication channels enabling the communication between the distributed energy resources and loads with the management units. The communication channel enables the definition of set points and control commands for the different loads and distributed generators, also allows the energy management system to receive information about loads and consumption profiles in order to define the proper control and coordination action. This layer in the management structure is commonly known as the cybernetic layer.

Due to the large amount of information and complexity in the management of this amount of information, energy generation systems in residential microgrids have been supported in emerging technologies, but already well positioned, such as the Internet of things, advanced measurement infrastructure, or even cloud computing looking for a faster an enhaced information processing and more efficient energy management that responds to user needs.

However, the use of new technologies supported in communications systems means a great risk in the management of information and the reliability of the microgrid, due to its interaction with the energy management system. In this case, not only the stability of the electrical system can be compromised. Also, sensitive user information such as consumption preferences, residence time at home, etc. may be compromised, manipu-

lated or obtained from undesired entities. Since, the information can be acquired externally without the consent of the users.

Based on the above, the need to address the cybersecurity of electric micro networks as the main theme of this book is raised. The document addresses the general characteristics for an energy management system in residential microgrids and explores the vulnerability of its communications systems. At the end, an exploration of strategies and architectures that guarantee the cybersecurity of residential microgrids are explored.

Key Words

Cybersecurity, Energy Management System, Residential Microgrids, Communication systems.

Tabla de Contenido

Capítulo 3

Capítulo 4

Capítulo 5

Capítulo 6

Listado de Figuras

Listado de abreviaturas y símbolos

AI	Inteligencia artificial
ABP	Activación por personalización
AC	Autoridad de certificación
AES	Estándar de encriptación avanzada
AMI	Infraestructura de medición avanzada
ANN	Redes neuronales artificiales
AES	Estándar de encriptación avanzado
BOT	Mejor tiempo de operación
CA	Agente de control
CIA	Confidencialidad, integridad, disponibilidad
CS	Ciberseguridad
CNN	Redes neuronales convolucionales
DES	Estándar de encriptación de datos
DDoS	Denegación de servicio distribuido
DG	Generación distribuida
DNN	Redes neuronales profundas
DoS	Denegación de servicio
IDEA	Algoritmo de encriptación de datos internacional
EES	Sistema de almacenamiento de energía
EMS	Sistema de gestión de energía
GW	Puerta de enlace

GP	Proceso gaussiano
GP	Proceso gaussiano
HEMS	Sistema de administración de energía residencial
HoMeS	Sistema de gestión de energía al hogar con almacenamiento
HVAC	Sistema de calefacción, ventilación y aire acondicionado
iBMS	Administración de baterías inteligente
IEC	Comisión electrotécnica internacional
IP	Fase inicialización
IOT	Internet de las cosas
ISO	Interconexión de sistemas abiertos
KDF	Llave de función de derivación
LoRa	Red de amplio rango
MA	Agente microrred
MAS	Sistema multiagente
MILP	Modelo de programación lineal de entero mixto
MGCC	Control central de la microrred
MAC	Control de acceso al medio
MitM	Hombre en el medio
NIST	Instituto Nacional de Estándares
OSI	Organización internacional para la estandarización
OTAA	Activación en el aire
PAR	Consumo pico a promedio
PSEMS	Sistema de energía inteligente y persuasivo
PCC	Punto de conexión común
RBESS	Sistema de almacenamiento de baterías residenciales
RES	Fuentes de energía renovable
RF	Radiofrecuencia
RNG	Generador de números aleatorio
RNN	Redes neuronales recurrentes
SF	Factor de ensanchamiento
SG	Red inteligente
SHA	Agente de vivienda inteligente
SNR	Relación señal a ruido
TDES	Estándar de cifrado de datos triple
UDP	Protocolo de datagrama de usuario

UIT	Unión internacional de telecomunicaciones
UTM	Gestión unificada de amenazas
WAN	Red de área amplia

Introducción

Las microrredes eléctricas permiten la integración de recursos energéticos disponibles localmente y con características de generación heterogéneas coordinados y gestionados de tal forma que aseguren el suministro de energía a una carga determinada [1]. En este sentido, el concepto de administración de energía toma un papel determinante dentro de la operación de una microrred, permitiendo, entre otras muchas funcionalidades, la integración de fuentes de energía renovables y de sistemas de almacenamiento de energía los cuales permiten entre otras cosas mejorar tres (03) condiciones críticas del sistema eléctrico como lo son: calidad de potencia, confiabilidad y eficiencia. Lo anterior, en adición al marcado interés en las cargas DC, ha moderado la discusión acerca de los sistemas de distribución DC versus los AC. De hecho, se ha desarrollado investigación considerable teniendo en cuenta los sistemas de distribución DC y su eventual aplicación al sector domiciliario. El desarrollo continuo y el incremento en la utilización de dispositivos inteligentes en los hogares revelan un futuro prometedor de los hogares inteligentes que se integran al internet de las cosas (IoT - por sus sigla en inglés: internet of things), donde los sistemas de potencia eléctricos domiciliarios trabajan en colaboración con dispositivos inteligentes para integrar sistemas de energía más autónomos, sustentables y limpios [2].

En este sentido, al considerar la optimización de la energía a nivel residencial, todo apunta al concepto de IoT, bajo el cual, todos los dispositivos dentro de un hogar serán capaces de interactuar entre ellos y sus usuarios para optimizar el consumo de energía y garantizar el confort de los usuarios. Para esto, cada dispositivo eléctrico electrónico podrá comunicarse y suministrar información al usuario o al sistema de administración de energía (EMS) el cual tomará decisiones de manejo de cargas de acuerdo a criterios de optimización predefinidos y a los requerimientos particulares del usuario. Al reunir y monitorear los patrones de consumo, se hace más fácil ajustarse a la oferta y la demanda del sistema energético, en particular, cuando se cuenta con fuentes de generación no determinísticas como por ejemplo, solar fotovoltaica o eólicas. Los usuarios estarán al tanto de su consumo y podrán ajustar su comportamiento de manera adecuada [3], de hecho, el EMS podría reducir el desperdicio de energía resultante de los malos hábitos de consumo de los usuarios y decidir la mejor hora de trabajo de ciertos dispositivos dependiendo del precio y de la disponibilidad de energía [4]. La Figura 1.1 ilustra el concepto de IoT para aplicaciones residenciales.

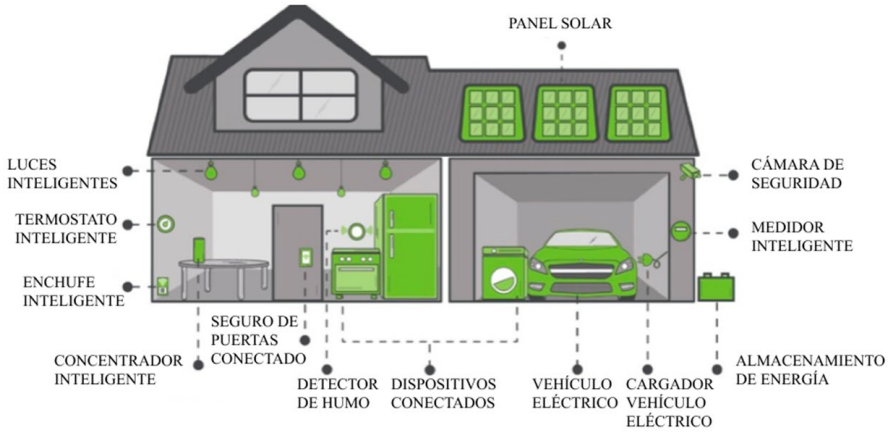

Figura 1.1 Concepto IoT para aplicaciones residenciales [5]

Una gran cantidad de investigaciones hoy en día, se centran en la evaluación de la vulnerabilidad de los dispositivos del sistema en la red eléctrica; sin embargo, el incluir con éxito los equipos de cómputo y los sistemas integrados de una red eléctrica, es sólo el primer paso para un ataque exi-

toso. Para modificar de manera predecible los componentes físicos de una red eléctrica (por ejemplo, manipulando estratégicamente generadores o cargas), los atacantes deben comprender cómo funcionan sus sistemas de control.

Los defensores que aprovechan sólo los mecanismos de seguridad de la información para proteger su red eléctrica tendrán un éxito limitado contra los atacantes sofisticados. Para desarrollar una estrategia de seguridad de defensa en profundidad, los defensores deben incorporar modelos de control de la red eléctrica para comprender las vulnerabilidades y la fragilidad del sistema que están tratando de proteger (por ejemplo, no todos los dispositivos comprometidos pueden conducir un sistema a un estado inseguro) así como diseñar algoritmos de control resistentes al ataque que puedan sobrevivir a un compromiso parcial del sistema.

Para facilitar la integración de la ingeniería de control con la seguridad adecuada, se presenta el papel de los sistemas de control para la red eléctrica, se muestra cómo modelar la vulnerabilidad del sistema de control observando los estados físicos afectados y ofrecemos sugerencias de diseño para resistir los ataques. El objetivo de la red eléctrica es generar y luego entregar suficiente energía eléctrica para satisfacer la demanda del consumidor. En general, se puede dividir la red eléctrica en tres partes principales: generación, transmisión y distribución.

Las funcionalidades de la nueva red eléctrica no solo crean beneficios, sino que inevitablemente introducen riesgos relacionados a la intromisión, divulgación y manipulación no autorizada de la información. Por estos motivos se incluye en la Smart Grid una línea de investigación dedicada a la seguridad de la información y las comunicaciones, conocida como ciberseguridad (CyberSecurity, CS), en donde se abordan los temas relacionados a las políticas de seguridad contemplados por el Instituto Nacional de Estándares (NIST – por sus siglas en inglés : National Institute of Standards). La CS es el área encargada de la seguridad de la información aplicada al sector eléctrico, convirtiéndose en pieza fundamental para la integración del sistema de generación, transporte y distribución de energía con una in-

fraestructura de comunicaciones que tenga implementados los objetivos CIA (Confidentiality, Integrity, Availability) de CS [6], [7].

Los incidentes y amenazas de ciberseguridad son un hecho cotidiano. Durante varios años consecutivos, este tema ha estado en la parte superior de la creciente lista de problemas que mantienen despiertos a los líderes de la industria energética. Al mismo tiempo, los avances tecnológicos y las expectativas de los clientes están impulsando a las empresas eléctricas a ser cada vez más digitales e interconectadas con redes más allá de su control directo. Ya es ampliamente considerado que todos los países necesitan tomar medidas defensivas mucho más serias para proteger la infraestructura eléctrica y, por lo tanto, nuestra seguridad física y económica [8]. ¿Son las microrredes una posible solución y las empresas de servicios públicos deben tomar la iniciativa para desarrollarlas como contramedidas de ciberataques? Una cuestión que se trata en el presente libro y que lleva a explorar las posibles contramedidas ante ciberataques.

Recientemente hubo informes sobre un ataque cibernético dirigido a la ciudad de Nueva Orleans, EE.UU. Todos los sistemas informáticos del gobierno se apagaron para mitigar los daños e investigar el incidente. En [9], se encuentra información sobre las amenazas cibernéticas a la red eléctrica de los EE. UU. Se estima que se han instalado 200,000 implantes de malware en la infraestructura crítica de los EE.UU., Y sorprendentemente, no parece haber habido ninguna resolución formal o incluso una investigación. Por otro lado, un ataque cibernético en 2015 en la red ucraniana causó un corte de energía durante seis horas y dejó a aproximadamente 225,000 personas sin electricidad. El ataque de malware BlackEnergy infectó la red de una empresa de servicios públicos a través del correo electrónico de phishing, luego recolectó las credenciales necesarias para obtener acceso a la operación del sistema SCADA, el atacante luego abrió interruptores para desconectar más de 30 subestaciones [10]. Más recientemente, se informó un evento cibernético dentro de la red eléctrica en los Estados Unidos en 2019 [11]. Estos eventos cibernéticos en Ucrania y en pequeñas empresas de servicios públicos de EE.UU. Pueden ser una indicación de los

preparativos adversos, lo que aumenta su disposición a realizar ataques a gran escala, si es necesario, en un momento estratégico.

Una posibilidad que es un poco más práctica que una red completamente redundante es la instalación de microrredes de respaldo altamente seguras para proteger la infraestructura crítica y los sistemas de contramedidas contra las amenazas cibernéticas. El ejército de EE. UU. ha demostrado tales tácticas en varias bases durante un período de años en un programa llamado demostración de infraestructura de energía inteligente para la confiabilidad y seguridad de la energía (SPIDERS) [12]. Diseñado para abordar tanto la demostración como la transferencia de tecnología, el programa utilizó proyectos de microrredes para proteger los activos críticos de la pérdida de energía debido a los ataques cibernéticos, sostener operaciones críticas durante cortes de energía prolongados y documentar el uso de energía distribuida y recursos de conservación como parte de la solución.

Las empresas de servicios públicos pueden argumentar correctamente que la conexión de las microrredes a sus sistemas podría ser parte del problema de la ciber-vulnerabilidad tanto como parte de la solución. Lo mismo puede decirse de cualquier dispositivo protegido de forma inadecuada que esté conectado a la red, ya sea un inversor inteligente, reconectador u otro equipo electrónico. Es por eso que la ciberseguridad es un problema para cada parte de la red y todos los dispositivos conectados a ella, en particular los sistemas destinados a mejorar la protección cibernética o proporcionar respaldo. La industria de microrredes proporciona una respuesta para esta preocupación.

Las microrredes ofrecen resistencia a los sistemas de red a través de la diversificación con múltiples fuentes de energía descentralizadas: arquitectura segmentada que permite que las microrredes funcionen con otras microrredes, con la red principal o de forma independiente; y frecuentemente, construidas en fuentes de energía redundantes dentro de microrredes individuales. Las microrredes de ciberseguridad se basan en esta

diversificación con mecanismos de respaldo a prueba de fallas integrados en los sistemas de control de microrredes para evitar que una intrusión corrompa la red. Las microrredes diseñadas para respaldar la infraestructura crítica e implementar contramedidas cibernéticas parecen ser soluciones prácticas para reforzar la seguridad. Todos los servicios públicos, los desarrolladores de microrredes y los expertos en ciberseguridad tienen experiencia para ayudar en la identificación de medidas de respaldo de microrred que podrían proporcionar niveles adicionales de seguridad para clientes individuales y toda la red.

El documento está organizado de la siguiente manera: en el capítulo 2 se hace mención al control y gestión para microrredes DC domiciliarias, en el capítulo 3 se ilustran las técnicas y tecnologías emergentes para la gestión de microrredes domiciliarias, en el capítulo 4 se describen las vulnerabilidades en las microrredes, en el capítulo 5 se muestran las definiciones y la arquitectura de referencia de la ciberseguridad, en el capítulo 6 se describen los tipos de ataques en las pruebas de vulnerabilidad y finalmente el capítulo 7 se relacionan las conclusiones.

Capítulo 2

Control y gestión para microrredes DC domiciliarias

Con base con los datos suministrados por el banco mundial cerca del 22% de la población rural del mundo no cuenta con acceso al sistema eléctrico domiciliario [13]. Bajo esta consideración, este tipo de población es más vulnerable a problemas relacionados con temas de salubridad y factores asociados con cambios climáticos. Al tener en cuenta esta situación, los países en desarrollo enfrentan dificultades y costos de implementación elevados cuando tratan de expandir el sistema eléctrico a zonas rurales y remotas. Tal condición favorece el desarrollo de sistema de energía modulares, en particular, las microrredes. Estas redes son flexibles e integran de manera eficiente sus recursos contribuyendo de manera sustentable al desarrollo de la industria eléctrica.

Las microrredes domiciliarias pueden ser consideradas como el elemento fundamental de una microrred a gran escala o un grupo de microrredes pero funcionando a niveles reducidos de potencia. De igual manera que las microrredes, las microrredes domiciliarias integran fuentes de

energía renovables tales como sistemas fotovoltaicos, generadores de viento y sistemas de almacenamiento de energía con el objetivo satisfacer la demanda de la carga con la generación disponible de tal forma que se obtenga la confiabilidad del sistema. A partir de esta consideración, se genera un nuevo reto, la administración de energía que tiene que implementarse para satisfacer la demanda con respecto a la limitada cantidad de energía disponible sin que se comprometa la mínima calidad de vida teniendo en cuenta la intermitencia natural de la radiación solar [14]. Por lo tanto, el sistema de administración de energía que se considera el control y gestión de microrredes eléctricas domiciliarias es una parte integral de este tipo de aplicaciones.

Este capítulo se organiza de la siguiente manera: La sección 2.1 contempla los ahorros potenciales de la utilización de la corriente eléctrica en aplicaciones residenciales. Las técnicas de administración de energía para microrredes DC residenciales se abordan en la sección 2.2. La sección 2.3 aborda el diseño y la implementación de sistema de administración de energía para una residencia inteligente. La optimización de agendamiento en un sistema de administración de energía, las consideraciones de un sistema multiagente y el internet de las cosas se describen en las secciones 2.4, 2.5 y 2.6 respectivamente. Finalmente, en la secciones 2.7 y 2.8 se hace una discusión del capítulo y se presentan las conclusiones del capítulo.

2.1 Ahorros de energía potenciales al utilizar corriente directa para aplicaciones residenciales

El concepto de microrred busca facilitar la integración de los RES y de los ESS al nivel de consumo para reducir la dependencia del sistema de la red eléctrica principal. Adicionalmente, una microrred tiende a mejorar la eficiencia del sistema de distribución acercando la generación al consumo, en efecto, pérdidas adicionales se pueden evitar al utilizar tensiones DC para la distribución eléctrica.

Los sistemas de distribución que se basan en arquitecturas DC no tienen cargas de potencia reactivas y la resistencia equivalente en el conduc-

tor tiende a ser ligeramente menor; intrínsecamente, los sistemas se vuelven más simples y más eficientes [15]. La mejora en la eficiencia se logra al minimizar el número de etapas de conversión cuando se conecta dispositivos de base DC. Además, un sistema de distribución DC es una interfaz más natural entre la mayoría de dispositivos DC, pues se evitan etapas de conversión no necesarias en los convertidores de potencia, que da como resultado una reducción de pérdidas significativas, así como simplicidad y reducción de costo.

2.2 Técnicas de administración de energía para microrredes DC residenciales

La combinación de un panel fotovoltaico con un sistema de soporte de baterías es una selección popular alrededor del mundo para satisfacer la demanda de energía eléctrica en las unidades residenciales [16]. Muy frecuentemente hay un reto interesante en la administración de dicha energía, el cual se centra en el hecho de dimensionar las cargas, con el fin de seguir el estado de carga de las baterías, de acuerdo a la naturaleza intermitente del recurso solar, sin afectar la calidad de vida del usuario [17]. Por lo tanto, el sistema de administración de energía residencial (HEMS) es una parte integral de las microrredes eléctricas residenciales DC.

Varias técnicas de EMS para sistemas fotovoltaicos en microrredes DC se encuentran disponibles en la literatura, a continuación, se citan algunos de los más relevantes. Un sistema de administración de energía inteligente y persuasivo (PSEMS - por sus siglas en inglés: Persuasive Smart Energy Management System) conveniente para residentes con ingresos medios y bajos en países en desarrollo se analiza en [18]. La técnica propuesta detalla el consumo de carga diario de una residencia y sus preferencias con respecto al perfil de carga. A diferencia de PSEMS, un HEMS que minimiza la demanda de energía pico y mejora la eficiencia general del sistema incorporando unidades de almacenamiento de energía se detalla en [19]. Un sistema multi-agente que asegura las cargas críticas y mantiene la integridad del sistema y la estabilidad en un ambiente de microrred basado en paneles fotovoltaicos se investigó en [20]. Una arquitectura estratégica

para administración de energía en una microrred que asocia un panel fotovoltaico a un generador de potencia activa se detalla en [21]. Por otra parte, una estrategia de administración de energía de carga óptima para un sistema aislado compuesto por paneles fotovoltaicos y baterías se detalla en [22]. En este artículo se describe la clasificación de carga para el sistema empleando métodos de optimización tradicionales como el método de variable lenta y el método de función penalizante para obtener una curva de carga óptima que permita controlar la carga y reducir el tamaño de las baterías y los ciclos que rigen la carga y descarga de las mismas.

Un sistema fotovoltaico aislado que satisface las necesidades energéticas de viviendas residenciales se discute en [23]. El sistema tiene cinco modos de operación definidos y un control de supervisión que define la selección del modo apropiado del sistema a cualquier hora del día para administrar el flujo de energía entre los paneles fotovoltaicos, las baterías y la carga. Desviándose de la administración de energía convencional los autores de [24] incorporan técnicas de inteligencia artificial tales como el control de lógica difusa para la administración de energía de un sistema híbrido aislado que incluye paneles solares, generadores eólicos y baterías de combustible. Los autores demostraron que el controlador difuso era capaz de ejecutar de manera adecuada las diferentes condiciones operacionales trabajando en todas las condiciones posibles de potencia de entrada proveniente de varias fuentes para satisfacer la demanda local.

2.3 Diseño e implementación de un sistema de administración de energía para una residencia inteligente

En algunos países la presencia de altas cargas en horas pico ha originado fallas en el suministro de energía eléctrica. Por lo tanto, la eficiencia en la generación de energía no es lo único relevante para un país y se debe considerar, paralelamente, el patrón de consumo de energía eficiente. Bajo esta perspectiva, se hace necesario incrementar la atención sobre la importancia de dar al consumidor final el acceso a la información de su consumo de energía. Las aplicaciones móviles jugarán un papel importante en la interacción entre la máquina y el hombre. La conexión inteligente

habilita al usuario para operar un dispositivo y monitorear su consumo de energía incluso desde una ubicación remota. Estudios demuestran que al tener acceso a este tipo de información le ayuda al cliente a reducir su consumo de energía en valores cercanos al 15% [25].

El sistema de administración de energía residencial es una tecnología que reduce y administra el consumo de energía en la residencia, de hecho, la realimentación del consumo de energía a los usuarios es efectiva para reducir el consumo total de la misma. Un HEMS típico muestra únicamente el consumo de energía de toda la residencia y de los dispositivos disponibles [26]. Debido al incremento de consumo de energía y el agotamiento de los recursos naturales, muchas políticas de energía y proyectos de investigación y desarrollo están en progreso en varios países. Sin embargo, la mayoría de ellos están empezando sin mayor desarrollo comercial. Es importante, por lo tanto, especializarse en el consumo de energía residencial y proponer un esquema simple y efectivo para reducir el desperdicio de energía en los hogares [27].

Una solución interesante se muestra en [25]. En este trabajo se presenta una aplicación que controla y monitorea de manera remota el consumo de energía que ha sido desarrollado de manera conveniente para la administración automática de energía de los dispositivos eléctricos y electrónicos disponible en los hogares. Como particularidades de esta propuesta, se destaca que no necesita una ubicación particular, es de bajo costo, consumo y tamaño. La solución consiste de tres (03) módulos: el módulo esencial, el módulo PLC y el módulo de detección. Esto le permite al usuario tener una conexión de internet remota a una aplicación de potencia embebida que monitorea y controla los dispositivos eléctricos. Esto se logra, calculando los niveles de tensión de la batería, del panel solar y de las turbinas de viento, cuyos valores se presentan en la pantalla LCD y se cargan a la página web utilizando protocolos SPI [28] y Ethernet [29]. Para controlar la carga, se utiliza un módulo Bluetooth que recibe los comandos de la aplicación del dispositivo celular y las envía a un microcontrolador para encender y apagar la carga. Un medidor de energía se utiliza para medir el número de unidades consumidas por la carga así como su factor de

potencia. Estas medidas se envían al servidor a través de protocolos tales como ZIGBEE [30] para su respectiva gestión.

2.4 Optimización de agendamiento en un sistema EMS

El sistema de administración de energía de un sistema distribuido es un objetivo y un tópico interdisciplinario. Puede ser implementado de manera centralizada o descentralizada [31], presentando ventajas y desventajas de cualquier manera. De acuerdo con el tipo de sistema especial, sea este comercial, residencial o militar, el sistema EMS centralizado puede diseñarse para no controlar ni supervisar el sistema total sino para reunir la información de administración, optimizar y despachar de manera experta y lograr un funcionamiento eficiente y económico. Sin embargo, la utilización de un sistema centralizado tiene una desventaja, la falla de una unidad central puede causar la caída de todo el sistema. En la administración descentralizada, se introduce el sistema multi-agente [32] que incluye un agente de base de datos, un agente monitor de fecha, un agente operador, un agente de acceso al DER y un agente de planificación. De la misma manera que en el sistema centralizado, se presenta un problema: la coordinación de energía y tensión en la red distribuida.

Recientemente, y comparándolo con la disminución de la producción eléctrica tradicional, la estrategia de lograr un balance en el sistema de distribución entre la demanda y el suministro se logra al ajustar la demanda. Un programa de respuesta a la demanda debe enfocarse a cambiar la utilización de las horas picos a las horas no pico y ser más flexible y adaptarse para responder a la generación distribuida variable presente en los paneles fotovoltaicos y en la generación eólica, el almacenamiento de las baterías y los vehículos eléctricos. En los sistemas residenciales DC, los componentes pueden lograr una respuesta a la demanda con la utilización de EMS centralizados.

Una aproximación interesante de lo discutido se presenta en [33], donde el problema de optimización se formula para minimizar el costo to-

tal de operación con el objetivo de mejorar la eficiencia del sistema en el contexto de precio en tiempo real. En el sistema de potencia, cada componente se modela de acuerdo con la formulación de costo, adicionalmente, la respuesta del sistema a la demanda con base en la información de precio en tiempo real se puede lograr. La Figura 2 1 presenta la estructura de potencia y del sistema de administración de energía de una microrred residencial DC.

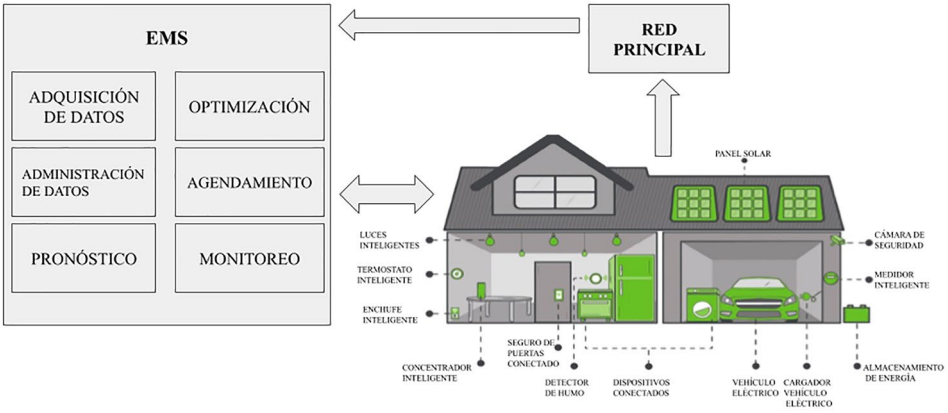

Figura 2.1 Estructura del sistema de administración de energía DC [33]

La optimización del proceso se lleva a cabo en el sistema experto del EMS centralizado que consiste de un controlador central al que se le suministra la información relevante por parte de los diferentes elementos del sistema y es responsable de:

- ***Recolectar y administrar la información local:*** datos de carga, generación de potencia y datos de los medidores inteligentes.

- ***Pronosticar la información del DER:*** carga, potencia del aerogenerador y de los paneles fotovoltaicos.

- ***Informar el estado de red principal:*** precio de la electricidad en tiempo real, información de la respuesta a la demanda.

- ***Monitorear el sistema completo:*** estado de carga del ESS, seguridad y restricciones de confiabilidad del sistema residencial DC.

- ***Sistema experto:*** algoritmos de optimización para varias funciones objetivo, restricciones y límites de operacionales de las unidades.

- Las variables de salida del EMS son los valores de referencia del sistema de control de cada DER.

2.5 Sistemas multi-agente para microrredes DC residenciales

Las microrredes DC se tornan en un concepto prometedor de redes de distribución eléctricas debido a que muchos generadores de potencia renovables distribuidos y tecnologías de almacenamiento de energía son fuentes DC. Muchos dispositivos eléctricos, tales como los cargadores de vehículos eléctricos, vehículos eléctricos híbridos, sistemas de iluminación a base de diodos y centros de datos, utilizan energía DC. Una microrred DC residencial que contenga uno o más unidades residenciales, puede mejorar la confiabilidad, eficiencia energética y seguridad de la red de distribución futura [34]. La inclusión de sistemas multi-agente [35] (MAS - por sus siglas en inglés: Multiagent System) es una aproximación relativamente reciente para la administración de energía de sistemas complejos que puede ser usada para desarrollar una estrategia de control de una microrred DC residencial [36]. Muchos artículos proponen la utilización del MAS para resolver los problemas de la respuesta a la demanda interna [37], respuesta a la demanda externa [34] y la operación en modo isla de las microrredes residenciales [20]. Recientemente, un modelo de residencia inteligente con base en un sistema multi-agente ha sido considerado para evaluar las características de las casas inteligentes, tales como generación de energía, almacenamiento e intercambio de electricidad [20], [38].

El MAS considera un agente de control (CA - por sus siglas en inglés: Control Agent) y varios agentes de residencia inteligentes (SHA - por sus

siglas en inglés: Smart Home Agents). Los SHA y CA toman decisiones de manera autónoma utilizando las funciones de utilidad de disponibles y emplean los algoritmos de mejor tiempo operacional (BOT - por sus siglas en inglés: Best Operational Time) para vehículos eléctricos y otras cargas de potencia relativamente altas. El algoritmo BOT utiliza las observaciones de corriente de los agentes y predice las condiciones futuras del ambiente para agendar óptimamente esas cargas y evitar los horarios de demanda pico y de precios de electricidad elevados. Por lo tanto, el MAS no solo minimiza los costos de electricidad de las residencias inteligentes, sino que adicionalmente previene las sobrecargas de los transformadores de estado sólido, en el caso que sean estos los que se estén empleando producto de la masificación de los mismos para este tipo de aplicaciones, durante la operación. Incluso juega un rol importante para el control autónomo de una residencia inteligente dado que, básicamente, los usuarios residenciales no tienen tiempo o no son lo bastante proactivos para ejecutar de manera óptima el control manual de la gestión de la energía.

En particular el CA es encargado de:

- Determinar el modo de operación de la microrred DC residencial: modo compra, modo venta o modo isla.
- Monitorear las señales de precio de la electricidad.
- Monitorear y controlar la demanda de energía de la microrred de tal manera que el transformador de estado sólido no se sobrecargue.
- Recibir la señal de demanda de emergencia del operador de la red distribuida.
- Controlar la energía suministrada a la microrred en el modo de compra.
- Controlar la potencia AC vendida en el modo de venta.
- Detectar fallos de la red externa y desconectarse de la red principal cuando estos se detecten.
- Detectar la recuperación de red principal e informar a todos los SHA el estado de recuperación. El CA enviará en mensaje de cambio de modo, información del precio de la electricidad y señales a todos los SHA.

De manera paralela, el SHA se comporta como un propietario y es responsable de:

- Suministrar a los usuarios la información de tiempo real de las entidades disponibles en la residencia.

- Reunir la información de precio de la electricidad y señales que provienen del CA.

- Monitorear y controlar el consumo de electricidad modificando las cargas controlables de acuerdo con un conjunto particular de requerimientos.

- Suministrar y almacenar la electricidad de la residencia.

- Le permite al usuario controlar el estado de las cargas basado en sus prioridades y tiempos definidos.

2.6 El IoT en hogares más sustentables y eficientes

La aplicación del concepto de IoT puede producir ahorros de energía significativos. El IoT en el hogar puede ser implementado al conectar varios dispositivos inteligentes a un EMS central con capacidades de toma de decisión. Al comenzar la interacción con los dispositivos en la rutina diaria, el EMS puede detectar la presencia de personas, aprender de sus hábitos y actuar consecuentemente para optimizar la energía que se consume en la vivienda [39]. El proceso de aprendizaje puede cubrir una cantidad considerable de variables, tales como:

- La ubicación de la gente en la vivienda.
- La hora de salida o llegada a la vivienda.
- La hora en que se cocina, se limpia o se duerme.
- La duración de la ducha y la temperatura del agua al tomar la ducha.

Como resultado del análisis de las costumbres, el EMS puede ahorrar energía al corregir malos hábitos, tales como, apagar las luces encendidas en habitaciones desocupadas, desconectar el sistema de calefacción si las ventanas o las puertas están abiertas, habilitar el encendido de dispositivos como lavavajillas y lavadoras con base en el precio de la electricidad o disponibilidad de energía si hay un RES instalado en la vivienda [2]. Todo esto, por medio de la utilización de diversos productos comercialmente disponibles entre los que tenemos, interruptores, tomas de energía y luminarias led inteligentes, y toda clase de sensores, cámaras y actuadores, que permiten activar o desactivar diversos dispositivos de manera remota.

2.7 Discusión del capítulo

Los objetivos fundamentales de las estrategias HEMS son la administración óptima de la energía y el control de las unidades residenciales para minimizar el costo de la electricidad y reducir los picos de carga de la microrred. Generalmente, el modelado y la definición de las estrategias de control de una residencia inteligente bajo un ambiente IoT se desarrollan con base en la información de carga de los hogares y los modelos de las unidades residenciales.

La integración de muchos campos heterogéneos en el mismo sistema no es fácil, y muchos retos deben ser superados antes de efectuar la implementación. De hecho, la falta de estandarización para sistemas DC y de códigos para aplicaciones de IoT sería uno de los problemas principales para desarrollar dichos sistemas [40]. De igual manera, se pueden citar los siguientes retos [25] asociados al caso de IoT:

- ***Conectividad:*** Pocos estándares de comunicaciones se usan en la actualidad: Bluetooth, Wi-Fi, ZigBee. Se necesitan nuevos protocolos de comunicaciones de fuente abierta.

- ***Consumo:*** Los dispositivos utilizados en estas aplicaciones funcionan con baterías que deberían estar en uso por años. Se debería utilizar dispositivos que generen energía a partir de vibraciones, luz o calor.

- ***Seguridad:*** Los dispositivos utilizados en la integración deben incorporar tecnologías de seguridad físicas para que el acceso no autorizado a la información personal no sea posible.

- ***Falta de infraestructura:*** Se necesita de una infraestructura común de software y hardware para reducir los costos de desarrollo y potencializar la creación de dispositivos IoT compatibles.

Teniendo en cuenta los sistemas de distribución DC podemos considerar los siguientes desafíos en aplicaciones residenciales:

- ***Seguridad y protección:*** La utilización de RES y ESS hace que el flujo de potencia sea bidireccional a través de las líneas de distribución. Por lo tanto, se necesita nuevos esquemas para detectar y aislar fallas y secciones sin desconectar todo el sistema.

- ***Falta de productos comerciales:*** Es fácil notar que hay pocos productos comerciales listos para utilizar tensiones DC. Por lo tanto, se necesita hacer pequeñas modificaciones en los dispositivos para incorporarlos al sistema.

2.8 Conclusiones del capítulo

Considerando las particularidades de las fuentes de generación basadas en recursos energéticos renovables variables, el sistema de gestión de energía debe basarse sobre plataformas y técnicas de control robustas que extraiga la potencia máxima de los paneles fotovoltaicos y de los aerogeneradores y mantenga un buen balance entre los ciclos de carga y descarga de las baterías. Adicionalmente, el EMS debe ser capaz de garantizar la regulación del a tensión en el bus DC, el estado de carga óptimo de las baterías, la limitación en la potencia suministrada por las baterías y protección del sistema.

Aunque muchos esquemas EMS han sido propuestos para lograr el ajuste del sistema con respecto a la demanda de energía, no se presenta un mayor detalle sobre el cómo llevar los sistemas de gestión conceptualmente definidos a una implementación real. En este sentido se debe avanzar en prototipos y aplicaciones hardware y software que permitan la comercialización e implementación de los sistemas de gestión.

Para lograr un sistema de energía sustentable, el foco no debería limitarse a generación de energía. La distribución de energía debe hacerse de manera eficiente y el desperdicio debería ser minimizado. En el futuro cercano, los sistemas de gestión energía, sustentables y basados en recursos energéticos renovables serán la tendencia buscando entre otras cosas cumplir con los objetivos de desarrollo sostenible y una regulación del consumo de energía hasta en un 60% de acuerdo a la norma ISO 50001 "Sistema de Gestión Integral de la Energía". Para lograr estos objetivos no hay duda que los sistemas de producción de energía deben cambiarse y no deben depender de petróleo, gas o carbón. Sin embargo, más que focalizarse en abastecer la demanda de energía con nuevas fuentes, se debe pensar en reducirla. La implementación de tecnologías DC para obtener distribución energética eficiente junto con plataformas inteligentes para optimizar recursos y reducir el desperdicio de energía, debe ser el objetivo al que se deben orientar las investigaciones.

Capítulo 3

Técnicas y tecnologías emergentes para la gestión de microrredes domiciliarias

La manera de organizar la generación, el almacenamiento y la gestión de la energía eléctrica desde la perspectiva de las energías renovables, así como, la parametrización de las características de consumo de energía de comunidades con acceso limitado a la oferta eléctrica interconectada, ha tomado mayor relevancia durante los últimos años debido primordialmente a la exigencia que define el bienestar social del presente siglo. De manera complementaria al aumento de la demanda, otros factores exigen la mejora y la actualización de la infraestructura de la red eléctrica y su apertura a otras tecnologías que satisfagan las necesidades de los usuarios finales. Precisamente, el marcado interés en las fuentes de energía renovables, la evolución persistente de las tecnologías de almacenamiento de energía, la masificación de las microredes domiciliarias, la contínua investigación en los sistemas de gestión de las micro redes y la generalización de las tecnologías y herramientas disponibles en diferentes ambientes de cómputo, motivan el desarrollo de este capítulo.

Las tareas que están enlazadas a la operación de las microrredes domiciliarias como la integración fluctuante de un número considerable de dispositivos y objetos heterogéneos cuyas características de movilidad y distribución son particulares sobre diversas áreas geográficas, las necesidades de soporte en tiempo real y requerimientos de capacidades de procesamiento y almacenamiento extensivo de información y la consideración de protección a aplicaciones críticas, aunada al manejo de técnicas de optimización avanzadas, puede llevarse a cabo mediante técnicas y tecnologías emergentes autónomas y escalables que sigan lo definido para el control y gestión de microrredes [41].

El presente capítulo se divide en tres secciones. La sección 3.1 presenta las distintas técnicas de administración para microrredes residenciales. Incluimos en esta sección los avances más relevantes que el grupo de investigación ha obtenido a partir de la aplicación de técnicas de aprendizaje profundo en el sistema de administración de energía. Finalmente, las secciones 3.2 y 3.3, presentan la discusión y las conclusiones del capítulo.

3.1 Técnicas de administración de energía para microrredes AC residenciales

Avances tecnológicos recientes en términos de comunicaciones en dos direcciones, infraestructura de medición avanzada (AMI, por sus siglas en inglés Advanced Metering Infrastructure)[42], fuentes de energía distribuidas y la construcción de instalaciones automáticas han contribuido al desarrollo de dispositivos para hogares inteligentes. De hecho, hay ejemplos de casas modernas que son capaces de generar y consumir energía. Este tipo de sistemas se consideran en la literatura como microrredes residenciales [43].

De igual manera que en las microrredes DC residenciales, en las microrredes AC residenciales el HEMS juega un papel crítico en la optimización de energía de una residencia inteligente debido a que actúa como un sistema experto que sirve al residente dentro de la unidad residencial. Sin embargo, en la literatura, el HEMS en microrredes AC ha sido más investigado

que su contraparte DC, pues su aplicación y conveniencia con base en la instalación de dispositivos y equipos AC ha tenido mayor difusión [44]. Los autores en [45] proponen un modelo HEMS para agendar de manera óptima la operación de los dispositivos disponibles en la residencia bajo precio de electricidad en tiempo real. En [46] se controla de manera óptima un sistema de almacenamiento de baterías residenciales (RBESS por sus siglas en inglés, Residential Battery Energy Storage System) y los dispositivos de la residencia con la energía disponible en un panel fotovoltaico de techo. En [47], una arquitectura para la regulación de carga se propone para minimizar el costo de operación residencial. En [48], se diseña un HEMS para programar dinámicamente los dispositivos en cada vivienda con base en el pronóstico y reporte de la demanda de energía de toda la comunidad. El trabajo presentado en [49] se basa en un mecanismo de actualización de carga/descarga del RBESS soportado en reglas que no produce necesariamente una solución óptima sobre un horizonte de tiempo finito y no considera la demanda flexible de los dispositivos residenciales. En [50] se estudió la programación coordinada de un sistema de calefacción, ventilación y aire acondicionado (HVAC por sus siglas en inglés, Heating, Ventilating and Air Conditioning) combinado con un vehículo eléctrico. En [51] se propone un modelo de programación de dispositivos sujeto a una estructura tarifaria combinada de precio en tiempo real y tasas de tendencia. La propuesta de [51], [52] es un esquema de optimización para calentadores de agua solares que permita minimizar el consumo pico de potencia de una unidad residencial. En [53] se desarrolla un HEMS con tecnología vehículo a hogar (V2H por sus siglas en inglés, Vehicle to Home) y energía solar residencial.

En general, en las investigaciones asociadas al EMS, los autores proponen una arquitectura de optimización distribuida para dar respuesta a la demanda de energía que se basa en la optimización de costo donde cada usuario considerado en el modelo recibe información en respuesta a la variación de los precios de la electricidad. En la programación de operación de los dispositivos se utiliza generalmente algoritmos iterativos que minimizan el costo de operación con base a técnicas de administración de demanda y uso eficiente de energía. Estos algoritmos permiten habilitar los equipos de tal manera que se reduzca el gasto monetario del consumidor

considerando las variaciones del precio de la energía y las incertidumbres en el tiempo de operación de los dispositivos y la generación de energía renovable. A continuación, se presentan algunos de los modelos y arquitecturas, que, a la fecha, impactan de manera innovadora el concepto de control y gestión de una microrred AC domiciliaria.

3.1.1 Actualización de técnicas de optimización del EMS

Una aproximación interesante se observa en [54], donde se propone una programación óptima con un día de antelación de la operación de la batería utilizando una técnica de optimización con programación lineal. El flujo de trabajo del proceso de optimización se presenta en la Figura 3.1.

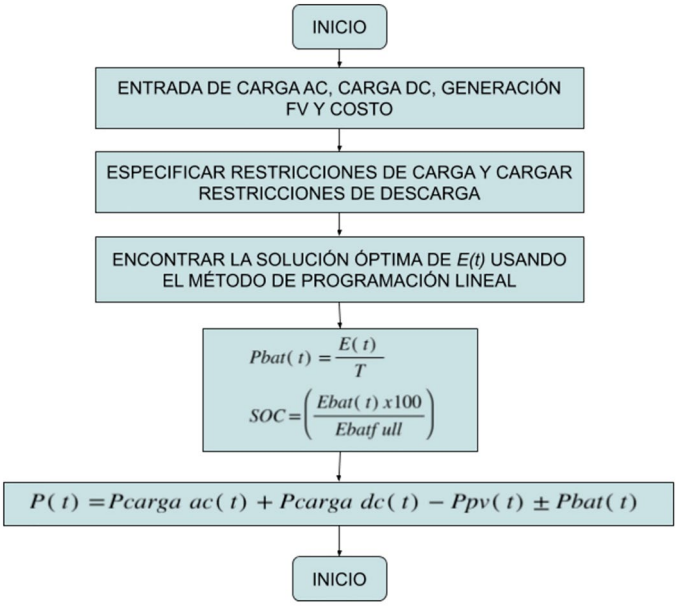

Figura 3.1 Flujo de trabajo del proceso de optimización, basado en [54]

Para la programación óptima de la operación de la batería, se tiene que incluir la información pronosticada de carga, de generación fotovoltaica y de precio de la electricidad. Con base en las funciones objetivo, se genera una solución óptima para la carga de la batería y para la tasa de descarga soportada en el pronóstico. Se debe tener en cuenta que un día

se divide en 12 espacios de tiempo y para cada uno se debe determinar la tasa de carga y descarga óptima. Con la programación de batería óptima, el costo asociado al intercambio de energía con la red principal se puede minimizar. De manera complementaria, cuando la generación excede la demanda, la carga es asumida por las fuentes de energía renovables y el sobrante de energía se vende a la red principal, en caso contrario, cuando la disponibilidad de energía en el bus DC no es suficiente para satisfacer la carga, el déficit de energía será suministrado por la red principal.

En [55] se considera una residencia que tiene múltiples dispositivos inteligentes con diferentes parámetros. Los habitantes tienen su propia microrred que consiste de un panel solar y una turbina eólica que se conecta con la red principal, con un vehículo eléctrico y con almacenamiento estático. Se considera para el problema de agendamiento un modelo de programación lineal de entero mixto (MILP por sus siglas en inglés, Mixed Integer Linear Programming) que permita coordinar los dispositivos de la residencia y la carga / descarga del vehículo eléctrico de acuerdo con la generación eléctrica de la microrred y la tarifa de electricidad. Los resultados de la investigación muestran que la energía disponible en el vehículo eléctrico y en los sistemas de almacenamiento estáticos contribuyen considerablemente en la minimización del costo de la electricidad y en la relación de consumo pico a promedio (PAR por sus siglas en inglés, Peak to Average Ratio) en aquellas horas cuando la demanda es alta o la microrred tiene una generación de energía mínima. El esquema MILP es capaz de programar los dispositivos inteligentes y el vehículo eléctrico de acuerdo con la generación de electricidad de la microrred a partir de sus señales de control.

La administración de la demanda y el programa de respuesta a la demanda se evalúan en [56]. Estos conceptos forman parte de la investigación en redes inteligentes en la que se incentiva al consumidor a cambiar su carga en horas de alto consumo a horas de bajo consumo para reducir sus costos de electricidad, incrementar la comodidad del usuario y asegurar el balance adecuado de la energía a través de un modelo que busca minimizar tres elementos: el consumo de energía, el costo del consumo

de la energía y el costo de la generación de energía. Los resultados de la investigación muestran que el modelo propuesto y el algoritmo utilizado para balancear el consumo de energía permiten reducir considerablemente tanto el costo de consumo de energía como el costo de su generación.

En comparación con las soluciones tradicionales, una arquitectura controlada por datos se ilustra en [57]. Este tipo de solución es más flexible, confiable y su implementación es más económica. La contribución del sistema de administración de energía propuesto se resume en cuatro puntos. El primero, la función de costo objetivo se aproxima en línea a través de un proceso Gaussiano (GP por sus siglas en inglés, Gaussian Process) por lo que no necesita considerar funciones objetivo conocidas ni precisas. Segundo, todas las incertidumbres pertinentes asociadas con la carga y energía producida por los generadores distribuidos son consideradas en el modelo. Tercero, el modelo controlado por datos se propone para encontrar el extremo de la función objetivo la cual no tiene una expresión definida, sin embargo, la función puede obtenerse a través de la observación en diferentes puntos. Y finalmente, el EMS propuesto utiliza información global para optimizar el costo en cada tiempo de manera independiente. La función objetivo también puede actualizarse en cada tiempo de acuerdo con las muestras de observaciones obtenidas. Esto permite que el EMS en línea sea capaz de lograr el objetivo de optimización de largo plazo para adaptarse a los cambios producidos en las funciones objetivo. La Figura 3.2 muestra la estrategia de administración de energía propuesta en [57].

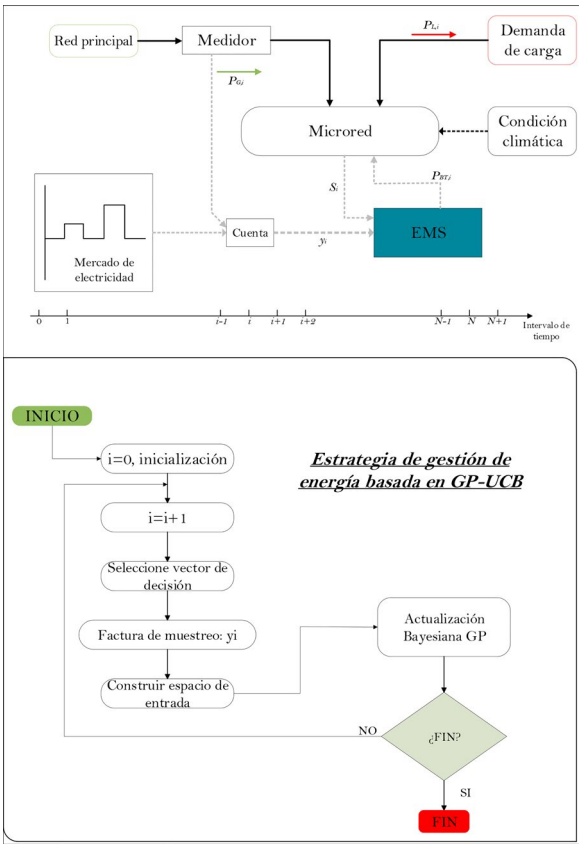

Figura 3.2 Estrategia de administración de energía propuesta, basada en [57]

La generación de energía de las unidades de generación distribuida en la microrred depende de las condiciones ambientales que se caracterizan por tener alta incertidumbre y aleatoriedad. El EMS monitorea los estados de operación interna de la microrred y toma decisiones óptimas para mantener la cuenta de la electricidad al mínimo y lograr el balance de energía y el nivel de almacenamiento de energía adecuado en la microrred. La estrategia del EMS sigue el algoritmo óptimo Bayesiano que tiene en cuenta predicción previa y actualización posterior. Esta solución disponible en línea puede aproximar y aprender funciones objetivo utilizando un GP y observaciones en tiempo real. De igual manera, puede resolver el problema de optimización de una microrred en un modelo libre y controlado por información, que, de cierta manera, es una aproximación prometedora para la optimización en línea.

En [58] se presenta una aproximación de teoría de juegos para el EMS de residencia distribuida con almacenamiento (HoMeS por sus siglas en inglés, Home Energy Management System with Storage). Los autores utilizan un juego Stackelberg de múltiple-líder múltiple-seguidor para decidir las estrategias de la microrred, maximizar su rentabilidad, utilizar de manera adecuada la energía generada como las estrategias de los clientes. Es decir, para satisfacer sus necesidades de energía maximizando su beneficio individual. Con base en la energía almacenada remanente, cada consumidor decide sobre la energía necesaria para sus dispositivos, esta cantidad se convierte en la mínima cantidad de energía de este cliente, y la socializa dentro de la coalición. Al recibir esta información las microrredes deciden la mínima cantidad de energía a ser generada y el mínimo precio por unidad de energía, este precio se socializa dentro de la coalición. En este momento, cada cliente decide la cantidad de energía que quiere solicitar, incluyendo la cantidad de energía para almacenamiento y futuro uso. Cada microrred decide el precio por unidad de energía con base en la cantidad de energía solicitada por medio de una aproximación no-cooperativa.

Las contribuciones del trabajo en [58] se pueden resumir en los siguientes puntos. Inicialmente, los autores presentan un modelo HoMeS para consumo de energía en tiempo real en la presencia de instalaciones de almacenamiento y varías microrredes en la coalición. Luego, por medio de la aproximación de teoría de juegos de múltiple-líder múltiple seguidor, se evalúan las estrategias óptimas de las microrredes utilizando un juego cooperativo - fase inicial del juego propuesto - y las estrategias de los clientes utilizando un juego no cooperativo - siguiente fase del juego propuesto. Finalmente, se presentan tres algoritmos diferentes: El primer algoritmo es utilizado en la fase de inicialización (IP por sus siglas en inglés, Initialization Phase) de las microrredes para determinar la cantidad mínima de energía a ser generada. El segundo algoritmo es usado por los clientes para decidir la cantidad de energía solicitada con base en el precio de energía de tiempo real. En el algoritmo final que se propone, las microrredes deciden el precio por unidad de energía en tiempo real, dependiendo de la cantidad total de energía solicitada.

Con la metodología propuesta, los autores muestran cómo el sistema de administración de energía distribuido en la presencia de almacenamiento puede hacerse obteniendo un valor óptimo de la energía solicitada por los clientes, mientras se considera la demanda de energía total del sistema. Por otra parte, se asegura la rentabilidad de las microrredes pues el precio óptimo seleccionado por cada microred es menor comparado con el que se utiliza un EMS tradicional.

3.1.2 Aplicación de lógica difusa en el EMS

En esta sección se presenta una serie de investigaciones que incorporan lógica difusa en el EMS teniendo como principal resultado una alta penetración en la energía renovable lo que trae consigo más rentabilidad para los usuarios finales.

En [59] se propone una estructura de comunidad de energía inteligente consistente de usuarios de residencias inteligentes, usuarios sin residencias inteligentes y una unidad de generación de energía centralizada que busca facilitar la distribución de energía entre los vecinos. El diagrama esquemático de la estructura de la comunidad que comparte energía se muestra en la Figura 3.3

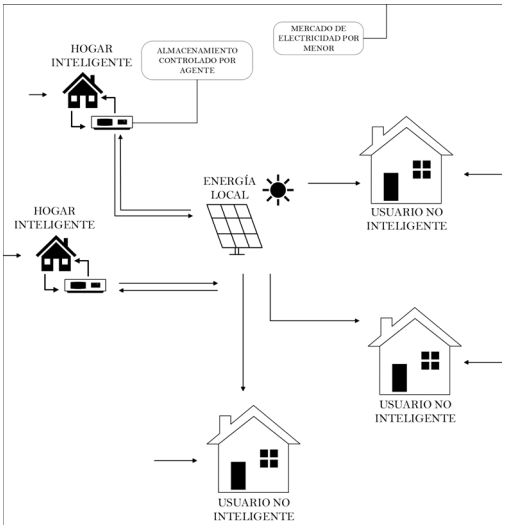

Figura 3 3. Estructura de la comunidad que comparte energía, basado en [59]

El modelo de comunidad propuesto permite a los vecinos negociar el exceso de energía para maximizar la utilización de energía renovable. Adicionalmente, se incluye un mecanismo de determinación de precio que se basa en la relación demanda vs exceso. Para facilitar las decisiones de negociación, los autores proponen un algoritmo de aprendizaje Q difuso, el cual es un algoritmo de modelo libre, que a través de lógica difusa puede obtener variables continuas de un conjunto difuso discreto. La efectividad de la estructura de comunidad propuesta y del algoritmo utilizado se evalúa a través de una serie de análisis numérico bajo diferentes escenarios que se puede resumir de la siguiente manera: Primero, el mecanismo de determinación de precios propuesto para la generación de energía mantiene el precio entre los niveles determinados para la generación y precio de mercado, permitiendo reducir los costos de energía e incrementar la rentabilidad de los generadores-consumidores. Segundo, el algoritmo de aprendizaje Q difuso puede ser aplicado para tareas continuas y recurrentes, tales como la negociación de energía en la comunidad, lo que hace posible entrenar constantemente los agentes inteligentes y mejorar la eficiencia de las estrategias y decisiones del EMS sin la necesidad de un modelamiento complicado y tedioso de la comunidad. Finalmente, este modelo de comunidad permite la negociación punto a punto de energía. Esto se logra por que los usuarios en la comunidad pueden adquirir energía de la unidad de generación local con precios más bajos y los usuarios con residencias inteligentes pueden vender su energía adicional a la unidad de generación para generar una entrada extra, permitiendo que los usuarios puedan participar en el mercado de energía, influenciando en los precios de la energía y logrando beneficios con la asistencia de equipo de control y almacenamiento inteligente.

En [60] se presenta un sistema de administración de baterías inteligente (iBMS por sus siglas en inglés, Intelligent Battery Management System) utilizado en una microrred residencial que trabaja en modo conectado a la red y en modo isla. La microrred utilizada está compuesta de un generador fotovoltaico, un sistema de baterías y un grupo residencial pequeño que se ubica en una zona caribeña con una radiación solar promedio de 1000 W/m2 con gran intermitencia debido al movimiento de las nubes y

la alta probabilidad de siniestros debido al clima. El iBMS considera un controlador difuso para los modos de operación en modo isla y en modo conectado a la red y las reglas se definen de acuerdo al comportamiento de consumo de las personas que habitan las residencias, la intermitencia de la energía disponible en el panel fotovoltaico, el estado de carga de la batería y la energía contratada de la red principal. Un ejemplo de las funciones de asociación definidas para el sistema de administración de energía de una microrred trabajando en modo isla, se muestra en la Figura 3.4

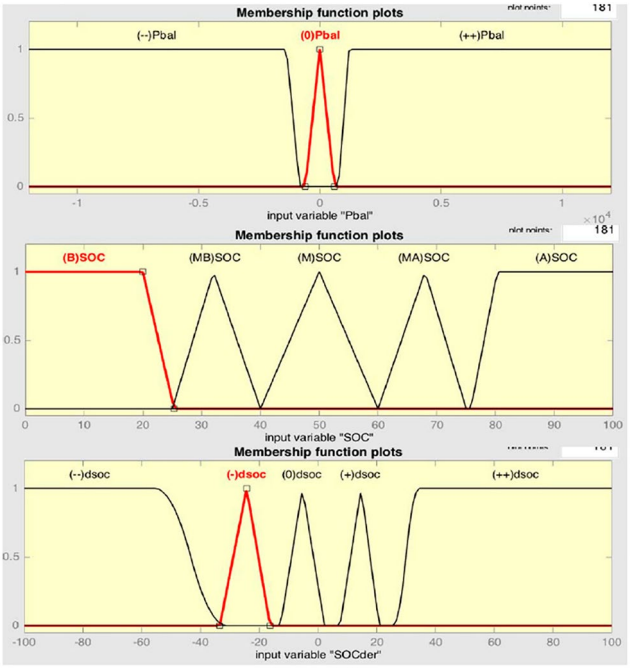

Figura 3.4 Funciones de asociación de entrada [60].

El diseño del controlador tiene tres entradas: la energía total manejada por el sistema, el estado de carga de la batería y tasa de carga o descarga de la batería. A partir de estas entradas se generan tres funciones de membresía. La primera función de membresía representa el flujo de potencia de la microrred cuando se desconecta de la red principal (Pbal). El punto en el cuál la potencia consumida por los hogares es igual a la potencia producida por los paneles fotovoltaicos y la batería se representa

como (0)Pbal. De manera similar, la condición cuando la potencia de la carga es mayor a la potencia producida se representa como (++)Pbal, de lo contrario, la condición cuando la potencia de la carga es menor que la potencia producida se representa como (--)Pbal. La segunda función de membresía define el estado de carga de la batería (SOC) a partir de cinco niveles: bajo, medio-bajo, medio, medio-alto y alto. Finalmente, la tercera función de membresía representa la tasa de carga o descarga de la batería (SOCder). A partir de un nivel neutral (0 dsoc) se puede pasar a niveles de carga y descarga bajos (+dsoc y -dsoc) y a niveles altos (++dsoc y --dsoc).

El resultado de la simulación del controlador fuzzy en modo isla, es una función de respuesta a la demanda que le dará al sistema de administración de energía de la batería, una manera de mantener la operación sustentable de la microrred por un periodo considerable de tiempo, que depende principalmente de las reglas definidas por los propietarios de la solución.

De igual manera el iBMS considera dos bloques de respuesta a la demanda utilizando cargas eléctricas no críticas disponibles en las residencias. El objetivo principal del iBMS es suministrar energía eléctrica a las residencias utilizando la energía disponible sin generar alteraciones a la red principal cuando la microrred está trabajando en modo red, y de igual manera, mantener el estado de carga de la batería en su máximo posible.

3.1.3 Aplicación de IoT - Cómputo FOG en el EMS

La integración del IoT con una microrred domiciliaria tiene en cuenta la instalación de sensores inteligentes, medidores inteligentes, conmutadores y válvulas controlables, enlaces de comunicaciones, puntos de acceso entre otros. El flujo de datos provenientes de los dispositivos y de los medidores inteligentes se almacena en la capa física y se envía a capas superiores para asegurar un control central apropiado. Por lo tanto, una forma razonable de integrar IoT con una microrred es reorganizar las funciones originales del controlador central de la microrred (MGCC por sus siglas en inglés, Microgrid Central Controller) de acuerdo con las capacidades IoT

activadas [61]. Por lo tanto, se propone una teoría de control jerárquico mejorada para facilitar la integración como se muestra en la Figura 3.5

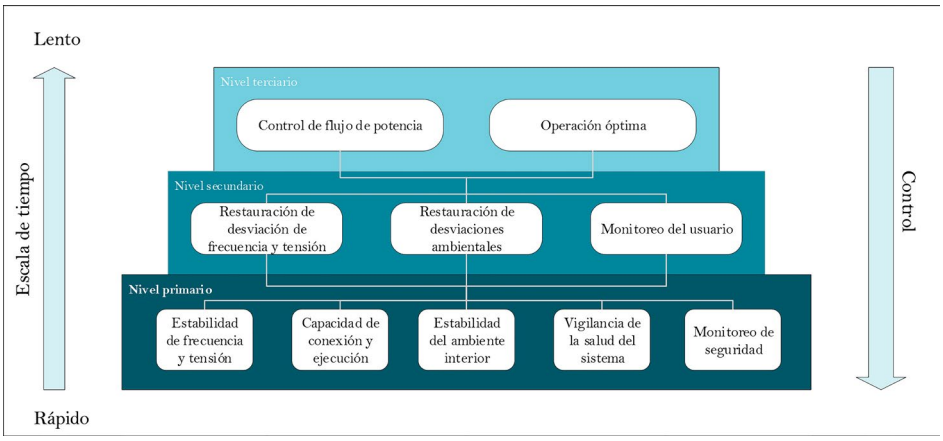

Figura 3.5 Estructura de control jerárquico de una MG

La integración en el nivel primario se asocia con la conexión de los dispositivos inteligentes a través de diferentes protocolos de comunicaciones. Durante la última década, diferentes entes de estandarización han hecho esfuerzos significativos para suministrar soluciones completas en diferentes dominios manejados por aplicaciones entre las que se considera sistemas de producción industrial, residencias inteligentes y soluciones de edificios inteligentes, generando el desarrollo de diferentes estructuras de información intermedias y protocolos. A continuación, y teniendo en cuenta que los objetivos de la integración del IoT con las microrredes de nivel residencial es mejorar la experiencia de los usuarios, el nivel de confort y eficiencia para controladores de temperatura, humedad, ventilación e iluminación pueden ser incluidos en el control secundario original del MGCC. Finalmente, el nivel de confort, pronóstico del tiempo, hábitos de los residentes y precio de la electricidad en tiempo real, se necesitan considerar para lograr la operación óptima global de la microrred domiciliaria y obtener mejoras en la eficiencia y ahorros en los costos de operación. El control terciario debe considerar una lista de escenarios completa en la que los pesos de confort y perspectiva económica puedan variar para lograr una

operación óptima global en cada escenario específico de acuerdo con la información prevista y el precio de la electricidad en tiempo real.

Es claro que el IoT se ha convertido en el nuevo paradigma para conectar dispositivos inteligentes y auto-configurables en una plataforma de red global y dinámica. Incluso, los servicios de cómputo en la nube, suministran a los clientes la infraestructura, plataforma, software y sensores de red como servicios que garantizar tener la confiabilidad y desempeño acordados en contratos de niveles de servicio que se tornan esenciales para la plataforma de administración de energía. Sin embargo, la perspectiva de centralización del control a través de cómputo en la nube genera cierta desconfianza porque podría poner en riesgo el funcionamiento de dispositivos utilizados para sensar, comunicar, calcular y actuar de manera predefinida en el sistema de administración de energía como resultado de los incrementos en el tiempo de respuesta y latencia presente en este tipo de tecnología. Por lo tanto, se introduce el concepto de cómputo FOG (niebla en inglés) para moderar algunos de los problemas anteriormente mencionados.

El cómputo FOG mueve el alcance del cómputo en nube hacia el límite de la red y crea una estructura de control intermedia descentralizada. Es una plataforma que suministra a la IoT las capacidades de pre-procesamiento de información que satisface las necesidades de baja latencia [62] y proporciona a los dispositivos las capacidades de ejecución, interoperabilidad e interactividad que les facilitan transferir y procesar la información generada en los tiempos de respuesta adecuados. Para el diseño de la plataforma FOG se debe considerar de manera adecuada la integración de los componentes de hardware, software y las arquitecturas de comunicación, tal como se aprecia en la Figura 3.6

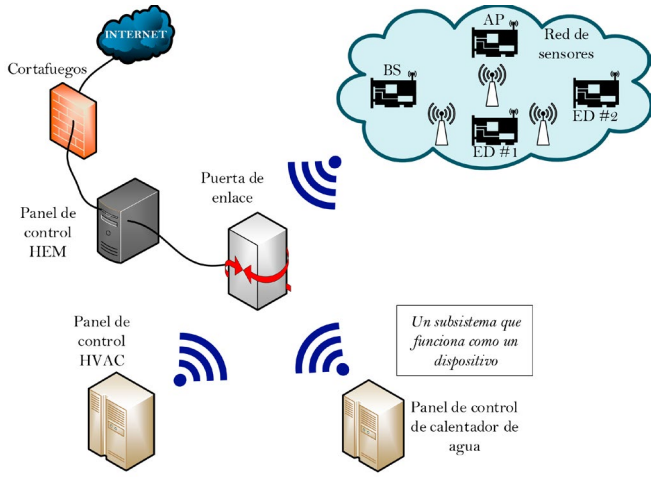

Figura 3.6 Arquitectura FOG para una microrred domiciliaria [50].

De acuerdo a lo presentado en [62], la implementación sobre una plataforma de cómputo FOG suministra la flexibilidad, interoperabilidad, conectividad, privacidad de información y características de tiempo real necesarias para el sistema de administración de energía. Adicionalmente, la utilización de software/hardware de fuente abierta y la posibilidad de integrarla de manera personalizada, le proporciona al usuario la capacidad de controlarla como un servicio.

3.1.4 Aplicación de IoT - Cómputo cloud en el EMS

Los sistemas de cómputo en la nube suministran capacidad de almacenamiento de información escalable, infraestructura de cómputo rápido y capacidades de alta compatibilidad de software que se pueden adaptar a las necesidades de usuarios y aplicaciones.

Una aplicación interesante para el sistema de administración de energía en microrredes domiciliarias utilizando capacidades de cómputo en la nube se aprecia en [63] al proponer un sistema multi-agente con base en esta tecnología. El MAS consiste de agentes de la microrred (MA por sus siglas en inglés, Microgrid Agents) y agentes de residencias inteligentes

(SHA por sus siglas en inglés, Smart Home Agents). Los SHAs toman decisiones de manera autónoma al utilizar funciones de sus opciones disponibles y los algoritmos de mejor tiempo operacional aplicados a vehículos eléctricos y otras cargas de alta potencia controlables para evitar los tiempos de demanda pico o de precios de electricidad elevados. Por lo tanto, el MAS no solo minimizará los costos de electricidad de las residencias inteligentes, sino que también previene la sobre-carga del sistema de almacenamiento de energía. El MAS se implementa en un sistema de cómputo en la nube, y los dispositivos IoT se utilizan para comunicación en tiempo real entre las residencias inteligentes y la nube a través de internet. De esta manera, la plataforma MAS con base en la nube posibilita la comunicación con los agentes de manera razonable y en tiempo real para facilitar el control de las microrredes residenciales tal y como se muestra en la Figura 3.7

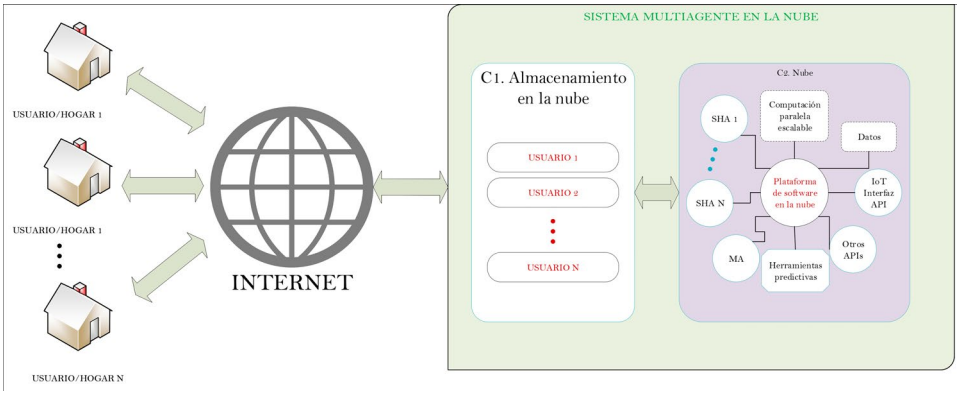

Figura 3.7 Plataforma cloud para MAS

Los resultados del artículo muestran que el MAS propuesto no solo aplica los cambios de carga y los ajusta de manera adecuada cuando la respuesta de demanda interna se lo solicita, sino que lo hace también a partir de las solicitudes de demanda externa. Por lo tanto, el MAS propuesto con base en la nube puede mejorar el desempeño de las microrredes domiciliarias en términos de minimización de picos de carga, ahorrando los costos de la electricidad del hogar e incrementando la eficiencia de la utilización de la batería de la residencia.

3.1.5 Sistema de administración de energía de una microrred basado en aprendizaje profundo (deep learning)

En esta sección se presentan los avances que el grupo de investigación LIFAE (Laboratorio de Investigación de Fuentes Alternativas de Energía) de la Universidad Distrital Francisco José de Caldas ha obtenido con la aplicación de métodos de aprendizaje profundo en el sistema de administración de energía de un grupo de microrredes.

3.1.5.1 Métodos basados en aprendizaje profundo

Generalmente, los métodos basados en aprendizaje profundo que se utilizan para la administración y pronóstico de energía son: las redes neuronales artificiales (ANN por sus siglas en inglés, Artificial Neural Networks), las redes neuronales profundas (DNN por sus siglas en inglés, Deep Neural Networks), las redes neuronales convolucionales (CNN por sus siglas en inglés, Convolutional Neural Networks) y las redes neuronales recurrentes (RNN por sus siglas en inglés, Recurrent Neural Networks) [64].

Una ANN se diseña con base en el mecanismo de trabajo del sistema nervioso humano [65]. Este sistema aprende a implementar una tarea al considerar únicamente ejemplos sin ser programado con reglas específicas. Una ANN se fundamenta en una colección de nodos o unidades que se llaman neuronas a través de las cuales se lleva a cabo la comunicación. Una arquitectura simple de una ANN se muestra en la Figura 3 8. En el modelo presentado, una neurona recibe una entrada y produce una salida a partir de su función interna de activación. La salida de algunas neuronas es la entrada a otras neuronas lo que produce un gráfico de pesos dirigido. Las funciones internas de activación, así como, los pesos que calculan la activación se alteran a través de un proceso conocido como aprendizaje, el cual se controla a través de parámetros como el número de capas ocultas, la tasa de aprendizaje y el número máximo de iteraciones. El modelo de entrenamiento ANN utiliza los datos históricos para entrenarse y hacer una predicción con base en la nueva información de entrada.

Las DNN pertenecen a la familia de las ANN. Se generan a través de múltiples capas ocultas entre las capas de entrada y salida [66]. Una comparación entre las DNN y las ANN se presenta en la Figura 3.8. La DNN procesa la entrada a través de manipulación matemática para producir la salida, independientemente de si la relación entre la información es lineal o no lineal. La red se entrena utilizando un conjunto de entrenamiento que resulta en el cálculo de probabilidad de cada salida. Una DNN contiene más capas que otras redes, tal y como se muestra en la Figura 3.8.

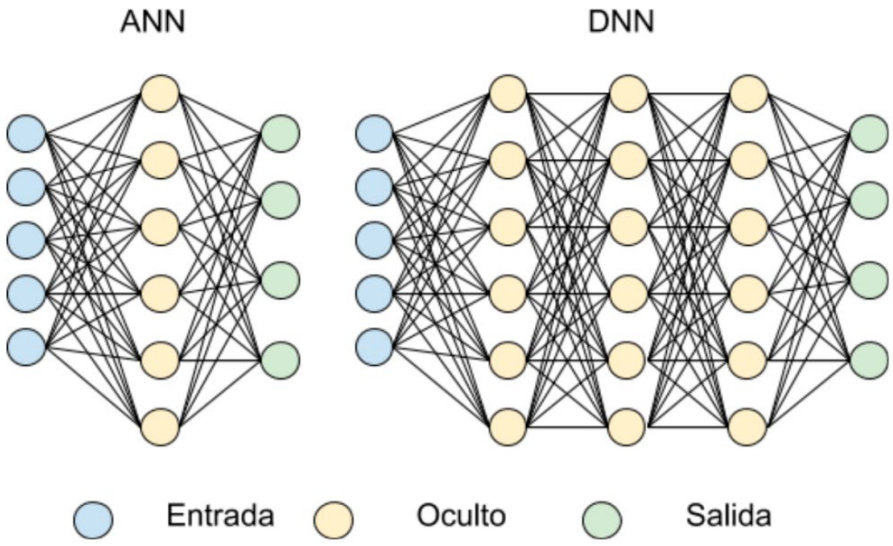

Figura 3.8 Arquitecturas típicas de redes neurales artificiales (ANN) y redes neurales profundas (DNN). Fuente: [64]

Las CNN se conocen también como ANN de espacio invariante y se inspiran en proceso biológicos en los cuales las neuronas están completamente conectadas unas a otras [67]. La principal diferencia con otras redes neuronales es que las CNN utilizan una serie de diferentes tipos de capas ocultas, es decir, capa convolucional, capa de alisado, capa de deserción, capa de agrupamiento, capa completamente conectada, capas de normalización, etc. La entrada y la salida de las capas ocultas se enmascaran por medio de una función de activación. Esta función, generalmente, involucra un método de propagación regresiva para producir un peso más preciso.

Paralelamente, la capa convolucional en las CNN se utiliza para des-escalar la información de entrada de tal manera que se facilite el proceso, sin modificar la información.

Finalmente, las RNN son una clase especial de las ANN que son desarrolladas para un proceso secuencial de información [68]. Usualmente, las redes convencionales suministran entrenamiento a cada muestra de manera independiente; sin embargo, este tipo de entrenamiento independiente no es suficiente, en especial, para datos que exhiben una relación temporal. Las RNN ofrecen una solución a este problema al tomar las entradas de manera secuencial, poseer conexiones de re-alimentación para ejecutar procesamiento temporal y utilizar capas ocultas como memoria para el almacenamiento de información secuencial. Es importante mencionar que las RNN utilizan los mismos parámetros (U, V, W en la Figura 3.9) para cada capa, en vez de utilizar diferentes parámetros para cada capa, como lo hacen las DNN. En la Figura 3 9 se presenta a la RNN desplegada en una red completa, es decir, si la RNN es utilizada para hacer una predicción basada en una secuencia de los últimos seis (06) datos de entrada, la red deberá ser desplegada en seis capas. En los cálculos de RNN, xt, ot y st muestran la entrada, salida y el estado oculto en el tiempo t, respectivamente.

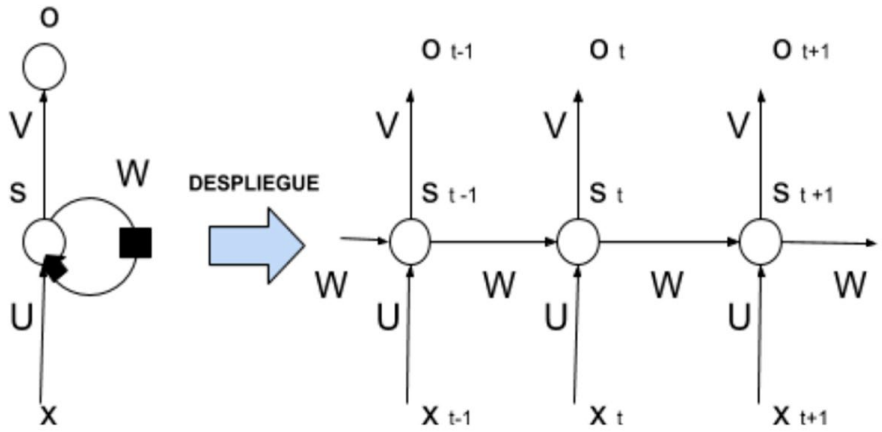

Figura 3.9 Ejemplo de una arquitectura RNN. Fuente: [69]

3.1.5.2 Asociación al sistema de administración de energía

Al considerar la intermitencia de la generación de energía de los recursos renovables y el comportamiento del consumo de los usuarios de una microrred o de un grupo de microrredes se hace necesario el pronóstico preciso de estos aspectos para obtener una administración de energía eficiente. El trabajo desarrollado por el grupo de investigación se ha focalizado en tres (03) aspectos: Pronóstico de generación de energía, pronóstico del consumo de energía y automatización del sistema de administración de energía a partir de soluciones disponibles en la nube.

En la actualidad, se dispone de una gran cantidad de información que hace posible el desarrollo de modelos de pronóstico bastante precisos. Sin embargo, el reto consiste en definir flujos de trabajo para el análisis de datos que permitan convertir toda la información de baja calidad en información procesable. Una aproximación interesante se ha trabajado en [70]. En el documento se define un flujo de trabajo que tiene en cuenta cuatro pasos:

1. Importar datos de diferentes fuentes, tales como, archivos, bases de datos y hojas de datos.

2. Limpiar la información por medio de la eliminación de valores atípicos y ruido, y combinar los conjuntos de datos.

3. Desarrollar un modelo predictivo preciso con base en la combinación de datos utilizando técnicas adecuadas de aprendizaje profundo.

4. Desplegar el modelo como una aplicación en un ambiente de producción.

Para el desarrollo de la investigación se está utilizando cuatro herramientas: Matlab [71], Simulink [72], Opal-RT [73] y Amazon AWS [74]. Matlab y Simulink se utilizan para modelar el sistema de administración de energía de una microrred y expandirlo a la integración de un sistema de administración de energía de un grupo de microrredes. La definición

del modelo incluye el flujo de trabajo que permita el análisis de datos para el pronóstico de la generación y consumo de energía. Adicionalmente, se proyecta definir una aplicación que permita seleccionar cualquier microrred del grupo para desplegar una imagen de la carga y la generación de energía pasada, y pronosticar una carga y generación futura. Esta información puede ser utilizada para comprender el efecto de factores como la irradiancia, la velocidad del viento, la ubicación y el estado del tiempo en el consumo de energía, y facilitar la administración de la misma, es decir, determinar cuanta energía se debe generar o en su defecto adquirir.

La plataforma de simulación de elementos eléctricos complejos Opal-RT se utiliza para emular en tiempo real el desempeño del modelo del grupo de microrredes en términos de generación de datos y seguimiento al sistema de administración de energía. La incorporación de los datos en la caracterización del comportamiento de generación y consumo de energía permite obtener un pronóstico más preciso, de tal manera, que el sistema de administración de energía pueda tomar decisiones más acertadas con respecto a la negociación de excesos o faltantes de energía.

Finalmente, se utiliza el servicio de almacenamiento simple de Amazon (Amazon S3 [75]) para garantizar el acceso y registro de los archivos que se utilizan por los modelos y los algoritmos de pronóstico bajo condiciones adecuadas de escalabilidad, disponibilidad de datos, seguridad y rendimiento.

3.1.5.2.1 Pronóstico de generación y consumo de energía

El sistema de administración de energía en el sector residencial o comercial juega un rol importante en el mejoramiento de la escalabilidad y confiabilidad de la red. Cuando hogares inteligentes se integran con dispositivos de generación de energía como las turbinas eólicas y los paneles solares, es necesario predecir la generación de energía a partir de estas fuentes para llevar a cabo una administración de energía eficiente. La generación de energía de estas fuentes puede pronosticarse teniendo líneas de tiempo definidas: un día, diez horas, dos horas, una hora, etc. y de cierta

manera aproximarse al tiempo real. El impacto de las diferentes condiciones del clima como la nubosidad, la irradiancia, la velocidad del viento, la humedad, etc. pueden facilitar el pronóstico de la generación de energía de una microrred particular o de un grupo de microrredes - incluso, se puede tomar como punto de partida el pronóstico de la generación con base en las condiciones de una temporada particular, siempre y cuando, se tenga acceso a los datos que la definen. La Figura 3.10, muestra el pronóstico de generación de una zona de interés con base en las condiciones ambientales presentadas a principio del año 2016.

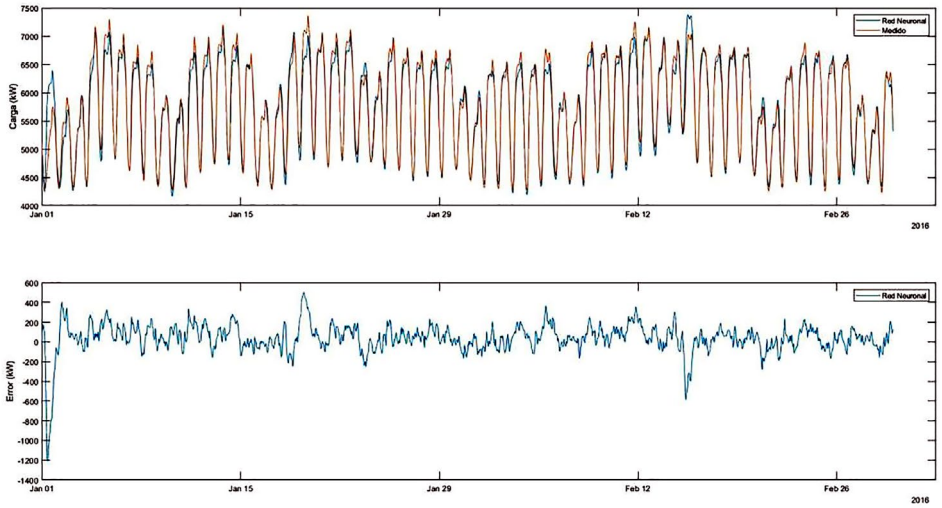

Figura 3.10 Ejemplo de pronóstico de generación teniendo en cuenta los datos disponibles en www.datos.gov.co. Fuente: Propia

Al tener disponible el pronóstico de generación de energía de una microrred se puede verificar que el consumo de energía es menor que la capacidad de generación total instalada. Si por el contrario, no se puede satisfacer la demanda de energía al trabajar al 100% la capacidad de los generadores, no será posible satisfacer la demanda sin importar como se operan las fuentes de generación. En este caso el sistema de administración de energía debería estar en capacidad de negociar la adquisición de electricidad de otra microrred o de la red principal, lo cual sería una opción relativamente costosa. Bajo esta perspectiva, se podría seleccionar un ob-

jetivo de generación ligeramente superior al resultado del pronóstico para generar una protección contra la variabilidad en el sistema y las imprecisiones del modelo (Ver Figura 3.11).

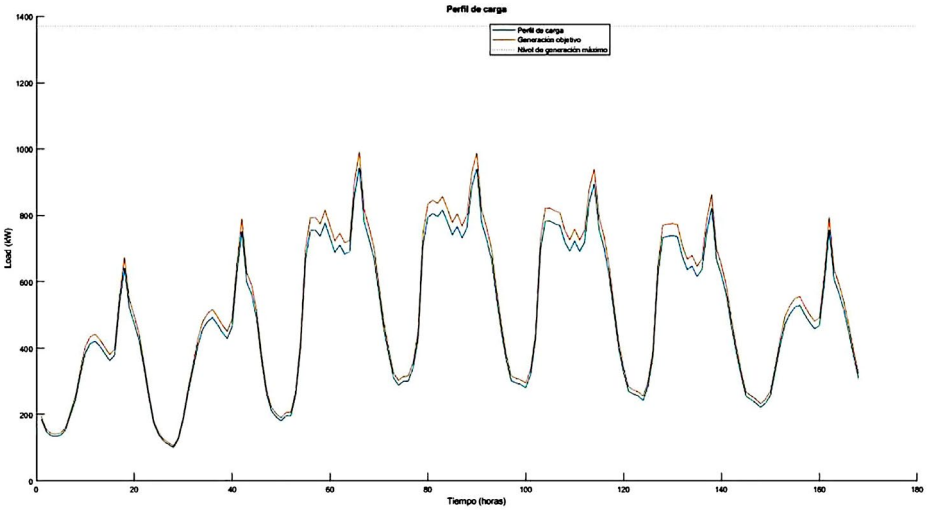

Figura 3.11 Ejemplo de ajuste de generación con base en el pronóstico de consumo Fuente: Propia

3.1.5.2.2 Automatización del sistema de administración de energía a partir de soluciones disponibles en la nube

El cloud computing presenta una serie importante de beneficios que impactan la flexibilidad y la competitividad de las microrredes. En esta investigación se resaltan dos en particular. El primero es la escalabilidad de las aplicaciones. Este beneficio favorece la inversión de capital pues únicamente se paga por lo que se utiliza, se disminuye el impacto económico de una posible recuperación ante un desastre y se elimina la necesidad de preocuparse de la actualización permanente de los servidores ya que esto se considera dentro del servicio contratado. Adicionalmente, los servicios en la nube son soluciones relativamente amigables con el ambiente, únicamente se utiliza lo que se necesita y la capacidad del servidor se adapta a la fluctuación de la nube. El segundo beneficio es el incremento de la auto-

nomía de las aplicaciones que resulta del trabajo colaborativo bajo condiciones de seguridad adecuadas y la inclusión constante de herramientas de inteligencia artificial que facilitan condiciones de trabajo remoto que en la actualidad es una tendencia y un requerimiento.

La Figura 3.12 muestra una arquitectura preliminar de la implementación del sistema de administración de energía de las microrredes a partir de soluciones disponibles en la nube en particular Amazon EC2 [76] y Matlab Production Server [77].

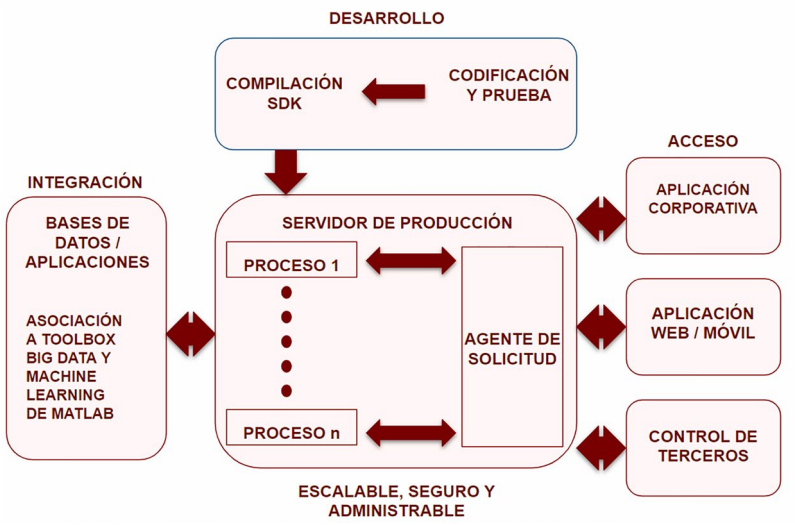

Figura 3.12 Arquitectura aplicada. Fuente: Propia

La arquitectura aplicada en el desarrollo de la solución se divide en cuatro (04) secciones desplegadas en la nube: Acceso a la información, desarrollo de las aplicaciones, integración con herramientas de aprendizaje profundo e integración con un servidor escalable. La integración adecuada de las secciones mencionas permite cumplir con el objetivo propuesto para la investigación: definir e implementar una arquitectura soportada en la nube que permita la gestión escalable del sistema de administración de energía para un grupo de micro redes.

3.2 Discusión del capítulo

Los sistemas de energía eléctrica convencional están atravesando por una transformación radical debido al incremento de la demanda a nivel mundial y la urgencia de reducir las emisiones de carbono. Ambos objetivos pueden llevarse a cabo al incorporar más generación renovable en la red principal e incluir tecnologías de comunicaciones e información innovadoras.

La implementación de microrredes en los procesos de las ciudades inteligentes a través de los recursos renovables, generación eficiente, mediciones inteligentes y cargas óptimas aumenta la capacidad de la plataforma con costo adicional mínimo [78]. Las microrredes facilitan operaciones claves numerosas, tales como: resiliencia, generación distribuida, uso eficiente de los recursos y dependencia, que últimamente definen la utilización y negociación de electricidad.

La madurez e incremento de la disponibilidad de la energía renovable está moviendo la generación de energía más cerca de donde se necesita, lo que ha permitido el desarrollo de las microrredes residenciales: redes de energía de pequeña escala que operan de manera independiente o en conjunto con la red principal. En la actualidad, las microrredes residenciales podrían tomar provecho de los desarrollos tecnológicos más avanzados para mejorar sus características incluyendo cómputo en la nube, cómputo FOG, IoT, dispositivos inteligentes, cómputo de última tecnología y sistemas inteligentes. Sin embargo, para lograr esto se necesita superar varios obstáculos y retos que incluyen estrategias de control complejas y participación de los consumidores.

Las tendencias mencionadas en este capítulo abren la oportunidad para la integración de la inteligencia artificial (AI por sus siglas en inglés, Artificial Intelligence) al sistema de administración de energía. La implementación de AI puede hacer uso de las nuevas infraestructuras de cómputo y

del alto volumen de conjunto de datos para desarrollar y entrenar modelos AI y desplegarlos en las microrredes particularmente en las microrredes domiciliarias.

3.3 Conclusiones del capítulo

La descentralización de la generación de energía requiere capacidades de cómputo local, aunque no necesitan ser tan poderosos como los sistemas predictivos centrales. Sin embargo, los nodos de cómputo deben ser capaces de ejecutar modelos de optimización predeterminados y filtrar y comprender señales locales para pasar señales necesarias al controlador central de la microrred.

El cómputo actual soporta despliegue eficiente de sistemas de cómputo FOG y cloud ejecutando procesamiento de información cerca de las fuentes de información, por ejemplo, dentro de la microrred o cerca de los límites de la misma. Adicionalmente, el despliegue de capacidades de inteligencia artificial permite el muestreo de datos a intervalos mucho más altos que las estructuras típicas mejorando el rango de 15 a 60 minutos y disminuyéndolas a menos de un minuto, superando las limitaciones de la congestión de la red de datos, almacenamiento y cómputo por fuera de línea.

La inclusión de diversas tecnologías de última tendencia en el sistema de administración de energía de las microrredes eléctricas domiciliarias hace que el sistema sea capaz de reaccionar de manera adecuada para ejecutar análisis y generar modelos con base en la información recolectada. De esta manera, el sistema completo se vuelve autónomo y efectivo en base a costo, mientras que otros requerimientos como el ancho de banda y conectividad se minimizan.

La rápida expansión del cómputo en la nube hace que los servidores locales se vuelvan obsoletos y permite el procesamiento remoto de una gran cantidad de información. El cómputo FOG es una requerimiento necesario para soportar el cómputo en la nube, puesto que reduce el ancho

de banda requerido, lo que es clave para acceder las infraestructura de cómputo en la nube.

La inclusión de nuevas tecnologías de la información y las telecomunicaciones y la descentralización de la información y sistemas de gestión traen retos adicionales en cuanto a la confiabilidad y vulnerabilidad de la información que se comparte entre las unidades distribuidas o incluso con la unidad de gestión centralizada.

Capítulo 4

Vulnerabilidades en microrredes

La red eléctrica tiene múltiples objetivos de control [79]; los más relevantes son la seguridad (prevención de accidentes y protección de equipos), la confiabilidad del servicio eléctrico a los clientes y la optimización del mercado eléctrico. La seguridad y la protección están garantizadas por relés e interruptores automáticos que reaccionan a fallas locales. Por ejemplo, en las líneas de transmisión y distribución se produce una falla cuando una de las líneas hace contacto con otra línea o con "tierra" (por ejemplo, un árbol). Este contacto genera una corriente tan grande que puede provocar incendios o electrocución, dañar el equipo o reducir la tensión de la línea, lo que afecta la calidad de la electricidad entregada. Los interruptores automáticos son mecanismos de protección comunes que se activan cuando la corriente que fluye a través de ellos excede un cierto límite. Del mismo modo, los generadores tienen relés de protección que evitan que se conecten a la red eléctrica si están fuera de fase.

El capítulo se divide en diferentes secciones relacionados con la vulnerabilidad en las microrredes. En la sección 4.1 se establecen las relaciones entre la estabilidad y los mecanismos de protección, los nuevos desafíos

de control en la red inteligente en la sección 4.2. El control resiliente en la sección 4.3 y 4.4, las estrategias de control contra ataques cibernéticos en la sección 4.6 plantea alternativas para lidiar con los problemas de vulnerabilidad. Finalmente se presenta un análisis de la vulnerabilidad en la infraestructura de la red en las secciones 48 y 4.9, finalmente las conclusiones en la sección 4.9.

4.1 Estabilidad y mecanismos de protección

Los relés de protección y los controles primarios son responsables de mantener la estabilidad del sistema y prevenir daños y otros accidentes en escalas de tiempo cortas. Cuando estos sistemas no logran evitar daños, se lleva a cabo una serie de procedimientos de respuesta de emergencia del centro de control, generalmente mediados por un operador humano.

En los sistemas de control, la estabilidad del sistema se define como la capacidad para mantener un valor de referencia deseado (por ejemplo, 60 Hz) bajo perturbaciones. Por lo tanto, la estabilidad del sistema de energía es la capacidad de un sistema de energía eléctrica para recuperar el equilibrio operativo después de una perturbación física. Las definiciones de estabilidad difieren según el tipo de perturbación y las variables a analizar, como la estabilidad de la señal pequeña, la estabilidad transitoria y el colapso de la tensión. Además del análisis de estabilidad, la seguridad de la ingeniería energética se refiere a la capacidad de un sistema para soportar perturbaciones repentinas o fallas en los componentes del sistema. Está relacionado con la capacidad de evitar fallas en cascada y pérdida de carga no controlada.

El análisis de contingencia estudia las consecuencias de posibles fallas, como una falla línea-tierra o una falla línea-línea, fallas de generación y la desconexión de cualquier elemento sin falla. En particular, el criterio N-1 para el análisis de contingencias, considera el fallo de un elemento y la posibilidad de poder seguir operando aceptablemente.

Los estados operativos de un sistema se pueden clasificar en normal, alerta, emergencia y colapso, como se muestra en la Figura 4.1. En el estado normal, todos los parámetros del sistema están dentro de los rangos aceptables. Los cambios significativos en el sistema, como un gran aumento de carga y condiciones climáticas extremas, pueden hacer que el sistema sea vulnerable y entre en un estado de alerta. En un estado de alerta, el sistema es estable, pero ciertos eventos pueden llevarlo a un estado de inestabilidad. Con acciones correctivas inmediatas, el sistema puede restablecerse a su funcionamiento normal; sin embargo, contingencias adicionales pueden conducir a un estado de emergencia. En estados de emergencia, el sistema viola algunas restricciones operativas, pero puede restaurarse; sin embargo, las contingencias severas pueden conducir a estados inestables que conducen al colapso. Finalmente, en un estado colapsado, el sistema es inestable y es necesaria la pérdida de generación, deslastre de carga o aislamiento del sistema para evitar fallas en cascada.

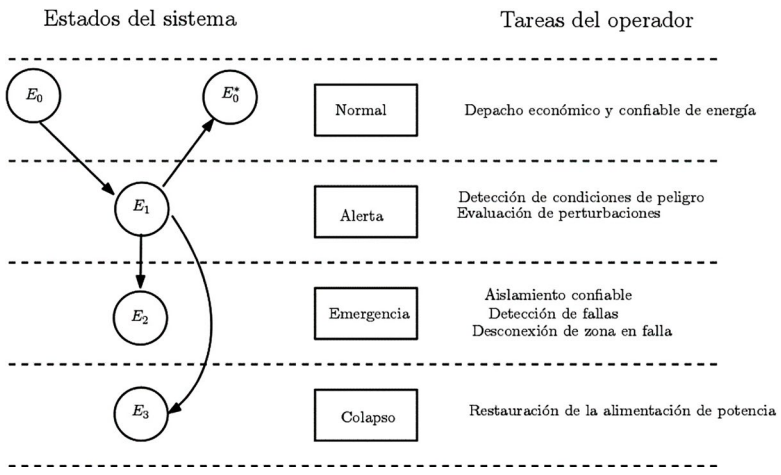

Figura 4.1 Estados del sistema y tareas del operador

Los modelos actuales de evaluación de seguridad tratan los estados de falla como el resultado de causas naturales y no están preparados para reaccionar a ataques intencionales, que no son aleatorios y pueden involucrar la falla simultánea de varios componentes tácticamente importantes.

4.2 La red inteligente: nuevos desafíos de control

La red inteligente se refiere a los múltiples esfuerzos en todo el mundo para modernizar las antiguas infraestructuras de la red eléctrica con nuevas tecnologías, lo que permite un sistema automatizado en red más inteligente. El objetivo de una red inteligente es entregar energía con mayor eficiencia, confiabilidad y seguridad y proporcionar más transparencia y opciones para consumidores de electricidad.

Las principales iniciativas asociadas con la red inteligente son la infraestructura de medición avanzada (AMI – por sus siglas en inglés: Advance Meter Infrastructure), la respuesta a la demanda, las microrredes, la automatización de la distribución, los recursos energéticos distribuidos y la integración de vehículos eléctricos híbridos. Cada una de estas iniciativas tiene nuevos requisitos de sistema de control desafiantes.

Los sistemas AMI utilizan medidores inteligentes que proporcionan comunicaciones bidireccionales entre la empresa de servicios públicos y el consumidor, reduciendo la necesidad de leer los medidores en el sitio y brindando una gama de nuevas capacidades a las empresas de servicios públicos, que incluyen monitoreo de consumo de electricidad, detección de interrupción automática, desconexión remota y restauración automática de energía.

4.3 Hacia un control resiliente

Como se ha descrito, las redes eléctricas tienen varios mecanismos de protección para evitar accidentes, daños y apagones, y como primera línea de defensa, pueden hacer que los ataques sean más difíciles de ejecutarse. Sin embargo, estos mecanismos de protección fueron diseñados para fallas accidentales y no están garantizados para prevenir acciones de atacantes estratégicos. Por ejemplo, el ataque Aurora muestra cómo los adversarios pueden evitar las medidas de protección para conectar un generador fuera de sincronización con un sistema energizado mediante la explotación de supuestas fallas benignas de los algoritmos de filtrado [85].

Además, la inyección de datos falsos de los algoritmos de estimación de estado muestra cómo los atacantes pueden eludir las pruebas de detección de anomalías tradicionales centrándose en identificar errores de medición del sensor. Las protecciones contra estos ataques requieren investigación sobre cómo extender la seguridad tradicional y los sistemas de control tolerantes a fallas a los sistemas de control resistentes al ataque.

4.4 Control de frecuencia resiliente

La estabilidad y el rendimiento de una red eléctrica pueden verse afectados si un canal de comunicación del sensor o de la señal de control se retrasa o bloquea con un ataque de denegación de servicio (Denial of Service: DoS). Al observar la dinámica del sistema, se determina que cualquier retraso en la señal de control de más de dos segundos produce un control de frecuencia inestable. El muestreo y los retrasos entre el control central y los generadores aumentan el tiempo de estabilización del sistema (el tiempo que tarda un sistema en volver a su punto estable) hasta un punto en el que el sistema ya no es estable.

Ante esta vulnerabilidad potencial, los operadores deben considerar los casos en que los atacantes pueden causar retrasos o caídas de paquetes. Uno de los mayores problemas de seguridad es que el tiempo de ataque puede ser ilimitado; por lo tanto, los sistemas de control deben sobrevivir incluso a los peores ataques posibles que pueden enviar retrasos arbitrarios o ataques DoS.

Para lograr algoritmos de control de frecuencia resilientes, se propone un algoritmo de control secundario descentralizado que permite a un grupo de generadores y cargas lograr la sincronización de frecuencia con retrasos arbitrarios y pérdidas de paquetes. Largas demoras o ataques DoS aún impactan significativamente el sistema, causando oscilaciones y disparando interruptores automáticos; sin embargo, los resultados garantizan que todos los nodos de la red eventualmente convergerán a la misma frecuencia. Por lo tanto, el sistema es estable [80].

Los costos adicionales para implementar este algoritmo resiliente en comparación con la solución centralizada incluye la necesidad de una infraestructura de comunicación donde todos los buses puedan compartir su frecuencia con todos los generadores del sistema (y no solo con un controlador centralizado) y dispositivos de almacenamiento que puedan absorber energía.

Como trabajo futuro, se planea estudiar la cantidad de tiempo que un sistema necesita para la convergencia, que es una cantidad más práctica para los operadores del sistema que una promesa de que el sistema eventualmente convergerá sin importar cuánto tiempo tome. Después de todo, se puede lograr estabilidad teóricamente, pero una gran desviación o corriente disparará los interruptores de protección y podría causar otros efectos no deseados. Modelar la interacción de los mecanismos de protección con la física del sistema es uno de los principales desafíos para crear una base de control resiliente en la red eléctrica [80].

4.5 Respuesta a la Demanda elástica con precios en tiempo real

Por el momento, el control de frecuencia en la red eléctrica es un enfoque de seguimiento de carga en el que los centros de control ajustan la potencia del generador en respuesta a los cambios en la carga causados por los consumidores. Para aumentar la eficiencia, múltiples esfuerzos continuos están tratando de controlar la energía consumida por los clientes de la red eléctrica, así como controlar la energía inyectada a la red. En su forma básica, los programas de respuesta a la demanda son un problema de control en el que la señal de control permite incentivos (por ejemplo, fijación de precios en tiempo real) o el control de carga directa reduce el consumo de electricidad de los consumidores durante las horas pico, desplazándolo a las horas de menor actividad. Por ejemplo, la utilidad controla directamente los puntos de ajuste del aire acondicionado de los consumidores [81].

Recientemente se ha explorado la seguridad de los algoritmos de respuesta a la demanda con precios de electricidad en tiempo real [81]. Se consideró a un atacante que comprometió una parte de los canales de comunicación utilizados para enviar información de precios a los consumidores y luego estudió los efectos de retrasar los cambios de precios y aumentar los precios de la electricidad. Estos modelos adversos paramétricos: retrasos o escalar la señal real en lugar de dar a los atacantes arbitrarios control de ello, son beneficiosos porque permiten mantener el análisis matemático manejable; sin embargo, limitando los adversarios de esta manera limitan el modelado realista.

Para estudiar atacantes que no están sujetos a estas restricciones, se permiten cambios arbitrarios en la señal de precios. Se modela este ataque genérico como una perturbación que puede modificar arbitrariamente la información de precios para la parte de los consumidores y mostrar cómo diseñar algoritmos de control resistentes para este problema. Las funciones de sensibilidad se han utilizado ampliamente para analizar el impacto de perturbaciones externas o cambios de parámetros en la salida de un sistema de retroalimentación. En la teoría de sistemas y control, la retroalimentación puede atenuar o amplificar las perturbaciones; por lo tanto, al usar la representación de frecuencia de un sistema, se puede obtener la función de sensibilidad y observar la respuesta del sistema a una perturbación de una frecuencia específica [81].

De acuerdo con la función de sensibilidad, los efectos sobre la diferencia entre la potencia suministrada y la consumida se amplifican en casi todas las frecuencias y todos los parámetros de control. Por otro lado, los ataques propuestos tienen frecuencias cercanas a cero (o al consumo de referencia) y, por lo tanto, no se amplificarán. Por ejemplo, si la frecuencia de ataque es cero, no habrá cambios en el error de oferta-demanda.

Los ataques diseñados para identificar las frecuencias amplificadas a partir de la función de sensibilidad tendrán un mayor impacto en el sistema que los ataques de demora o escala con la misma cantidad de desviación máxima de la señal de referencia. Además de caracterizar los efectos de

ataques más generales, la teoría de control puede ayudar a definir algoritmos más resilientes [82]. El área de control robusto ofrece una gran cantidad de trabajos en el diseño de controladores que identifican problemas y se reconfiguran para minimizar los impactos de estas perturbaciones. En particular, dado que se conocen los modelos físicos del sistema, se puede identificar cuándo los comandos de control no tienen el resultado esperado y luego estimar el error diseñando un "observador" (estimador de estado) para el sistema. Una vez que se estima la modificación de la señal de fijación de precios del atacante, se puede compensar la acción de control basada en esta estimación y, además, cambiar el comando de control y el parámetro basado en la función de sensibilidad para minimizar los efectos del ataque. Esta sería una posible solución temporal, mientras que los analistas de seguridad identifican los canales de comunicación comprometidos y revocan cualquier credencial o dispositivo utilizado en el ataque [82].

Si bien aplicar una teoría de control robusta a este problema puede minimizar el impacto de los ataques, no puede eliminarlos. La principal diferencia entre un control robusto y seguro es que, en este último, un atacante estratégico puede aprender sobre la estrategia de detección y respuesta y diseñar un ataque que evite la detección o active la respuesta automática de una manera que el diseñador no anticipó.

Para mejorar el análisis de los mecanismos de detección de ataques, el análisis se centrará en los atacantes que pueden evadir la detección, y luego se estudiará el peor ataque posible que el sistema no detecta. Este tipo de análisis es un paso hacia la diferenciación entre control robusto y control seguro, pero se necesitará más investigación que explique las diferencias entre fallas aleatorias y ataques estratégicos contra los sistemas de control.

4.6 Estrategias de control contra ataques cibernéticos

La ciberseguridad en sistemas eléctricos de potencia se puede definir como el conjunto de herramientas, políticas, conceptos de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de una organización y los usuarios. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada. La ciber-seguridad garantiza que se alcancen y mantengas las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes. Las propiedades de seguridad incluyen, entre otras, las siguientes: Disponibilidad, Integridad y Confidencialidad [82].

4.6.1 Control Jerárquico Optimizado bajo Ataque

Una microrred controlada de forma distribuida puede ser propensa a los ciber-ataques. Esto se puede hacer a través de un controlador o actuador inversor, y los ataques a través de un enlace de comunicación. Los ataques pueden ser repelidos incluyendo un término de ganancia variable en el control secundario de frecuencia, para microrredes AC, que incluye factores de confiabilidad como el factor de confianza relacionado con la información medida en cada inversor y el factor de confianza relacionado con la confiabilidad de los datos recibidos de los otros inversores. Estos factores utilizan una medida de distancia a través de una norma euclidiana dada por el error entre la frecuencia medida y la frecuencia de referencia, en comparación con un valor umbral ya definido.

Las ganancias dinámicas se incluyen directamente sobre el control secundario de cada inversor. Sin embargo, esos factores no consideran la disponibilidad de potencia de cada uno, y no existe un criterio de optimización para derogar el ataque cibernético sin saturar algunos de los inver-

sores. Estas referencias óptimas no solo garantizan que el ciber-ataque se repele, sino que también mantienen la señal dentro de los límites permitidos por el sistema [82].

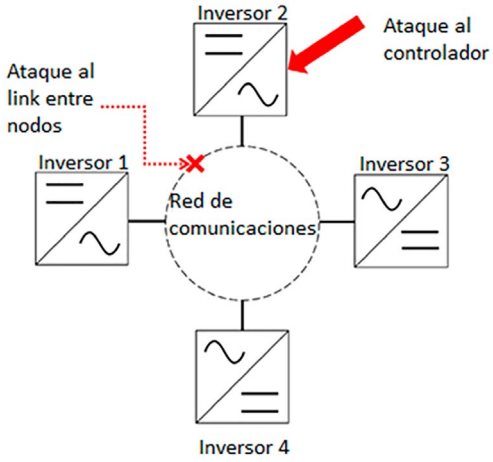

Figura 4.2 Configuración de una microrred bajo ataque [82].

Un control distribuido recopila datos de los vecinos a través de un sistema de comunicación local, porque es más susceptible a los ataques cibernéticos. Según la Figura 4 2, los ataques se pueden clasificar como ataques a controladores locales y ataques a los enlaces de comunicaciones entre nodos.

4.7 Vulnerabilidades en la infraestructura inalámbrica de la red

En los enlaces inalámbricos, al permitirse el acceso a las instalaciones donde están alojados los dispositivos de comunicación como, por ejemplo, la ubicación física de las puertas de enlace (Gateway), existe la posibilidad de manipular los parámetros de los enlaces de comunicación. Dichos cambios pueden causar el uso excesivo de la batería de los dispositivos [83]. Incluso si se desea, se puede llegar a cortar la comunicación existente entre los nodos y el gateway, este punto es muy importante, porque un gateway dentro de una red de comunicación inalámbrica, por ejemplo, LoRaWAN, fácilmente puede estar comunicando a cientos de nodos con la aplicación

al mismo tiempo y tal ruptura en la línea puede estar generando una pérdida masiva de información [84].

Otro ejemplo con respecto a la seguridad dentro de las instalaciones físicas en donde se encuentran los dispositivos, es el servidor de red, ya que es éste es quien posee toda la información requerida para determinar las claves tanto de red como de aplicación de todos los nodos conectados a la red de comunicación [85].

Es importante tener en cuenta que la ubicación física de los dispositivos centrales no siempre puede ser un secreto para los atacantes, ya que puede darse la posibilidad de determinar la localización física del gateway con ayuda de la captura del tráfico de la red [85]. Dado que los parámetros de configuración para la transmisión de los paquetes dependen hasta cierto punto del lugar geográfico en donde se ubique el gateway, debido a que diferentes regiones tienen parámetros de configuración diferentes dentro de las especificaciones del estándar inalámbrico, de esta forma es posible determinar el lugar general en donde se ubica el dispositivo y así poder explotar las vulnerabilidades anteriormente mencionadas.

También, es realmente importante la debida y adecuada protección contra intrusiones no autorizadas de los nodos, porque al violar la estructura física de los nodos, se puede llegar a tener conocimiento de las llaves utilizadas para la encripción de los datos enviados al servidor, y por consiguiente se pueden capturar los mensajes enviados y desencriptarlos para su posterior uso durante el tiempo de actividad del nodo. Este punto es realmente significativo cuando se activa el dispositivo por medio de la activación por personalización (ABP – por sus siglas en inglés: Activation By Personalization), debido a que este método conecta directamente el nodo a la red sin requerir de una solicitud de unión con su respectiva respuesta. La dirección del dispositivo (DevAddr), la llave de sesión de red (NwkSKey), y la llave de sesión de aplicación (AppSKey) [86] son guardadas directamente en el nodo y el conocimiento de los anteriores datos mencionados por un individuo malicioso lleva a un gran riesgo de la seguridad de la red [84].

4.8 Vulnerabilidades de conexión

En la infraestructura de red, la conexión entre el Gateway y los nodos terminales se realizan de forma inalámbrica y la conexión entre el gateway y el servidor de la aplicación preferiblemente se realiza de forma cableada. Las diferentes fallas de seguridad se presentan en su mayoría en el primer segmento de la conexión, debido a que la flexibilidad del enlace de comunicación inalámbrica le permite a un atacante tener un acceso al medio sin restricciones por parte de los operadores para evitar fugas de información o intrusiones no permitidas cuando se hace uso de este método para transportar los datos, vulnerando la integridad de los datos.

Por ejemplo, una vulnerabilidad expuesta en [84], menciona que dependiendo de la distancia a la que se encuentren los nodos con respecto a la puerta de enlace o los parámetros con las que son configurados los mensajes a transmitir, pueden existir casos en los que existan enlaces cuyo tiempo de duración de la transmisión sea más largo de lo usual, con lo cual, se puede llegar a realizar una fácil interceptación de paquetes e incluso se pueden llegar a corromper los paquetes transmitidos antes de que alcancen el gateway.

Otra de las vulnerabilidades que se pueden presentar en una red LoRaWAN, es la debilidad del protocolo específicamente al uso de valores previamente capturados de frame counter, ya que según [87], el reuso de valores frame counter con la misma llave de sesión y la misma dirección de dispositivo no se previene adecuadamente en la especificación. Esta vulnerabilidad podría aplicar tanto para una red cuyos nodos se hayan activado por medio de ABP o por medio de la activación en el aire (OTAA – por sus siglas en inglés : Over The Air Activation). Cuando se activa un nodo por medio de ABP la vulnerabilidad se presenta al reiniciar el dispositivo o cuando se desborda el contador, mientras que al activar el nodo por medio de OTAA, se generaría una falla solamente al presentarse un desbordamiento del contador cuando se encuentra dentro de una sesión.

Por otro lado, otra falla respecto al uso de un contador definido como DevNonce, el cual es un número secuencial que permite mantener la integridad y la autenticidad, adicionalmente, permite evitar duplicados en los mensajes al momento de realizar el procedimiento de unión de un dispositivo a la red. La falla mencionada se relaciona con el reúso de los valores del DevNonce, debido a que dentro del protocolo un único valor de DevNonce debería usarse cada vez que se genere una petición de unión, sin embargo, no se posee un seguimiento adecuado para los valores usados en procedimientos de unión previos, por lo que sería posible generar y hacer uso de un valor de DevNonce anteriormente utilizado [87], además dentro del servidor de red no se especifica la cantidad de valores de DevNonce que deben ser almacenados para cada dispositivo, sin contar con que dentro del protocolo se menciona de manera muy breve y de manera poco detallada la forma en la que el servidor de red debe manejar el mensaje transmitido en caso de que use un DevNonce previamente usado en un requerimiento de unión [88].

Al igual que con la trama, se podría hacer uso de los procedimientos utilizados por un nodo al momento de unirse a la red, como pueden ser los mensajes join-request y join-accept. En el caso del join-request, sería posible causar que se sature el contador de peticiones de join-request al repetir el mismo mensaje de join-request varias veces, causando que el contador se reinicie y permita un reúso de valores en donde las claves de sesión usadas previamente pueden ser derivadas y usadas nuevamente [87]. Por el otro lado, para el mensaje de join-accept parece faltar un mecanismo que evite los ataques de replay ya que a diferencia del mensaje de join-request en donde se ha introducido el DevNonce, no existe tal protección en el join-accept por lo que el nodo no rechazaría un join-accept enviado desde un gateway malicioso debido a que no puede distinguir si el mensaje provino de una fuente real o una falsa, en otras palabras, es posible realizar un ataque de sustitución [88] sin que se presente mucha resistencia por parte del sistema. Esta vulnerabilidad probablemente se deba a que un nodo con recursos limitados es incapaz de rastrear muchos valores de verifica-

ción, sin embargo, esto impide que se asocie correctamente el mensaje de join-accept con el respectivo mensaje join-request que lo desencadenó [87].

Las respuestas de acknowledgments (ACK) se configuran en la red para la aplicación verifique que un mensaje enviado, se ha recibido correctamente. Sin embargo, estos mensajes abren las puertas de otra vulnerabilidad que se puede notar en el protocolo como es la falta de asociación del ACK con los datos, debido a que no se puede identificar el ACK con el dato del nodo que ha disparado dicho mensaje [87].

Igualmente no solo existen vulnerabilidades entre la conexión de los dispositivos finales y el gateway, sino que también se pueden explotar vulnerabilidades presentes entre el servidor de red y servidor de la aplicación como puede ser la vulnerabilidad que existe al verificar el protocolo que se utiliza para el envío y desencripción de los datos entre éstos dos servidores, esta debilidad se da porque los cálculos de desencripción para los datos de la aplicación se llevan a cabo en el servidor de red, esta acción deja sin proteger la integridad de los datos de la aplicación, ya que se transportan dichos datos desde el servidor de red al servidor de la aplicación desencriptados.

Otra falencia en esa parte de la conexión de la red es que posibilita realizar modificaciones precisas en los datos de la aplicación porque el cifrado de los datos de la aplicación implica una operación XOR con un bloque secreto y de la forma en que el protocolo realiza el procedimiento se conservan las posiciones de los bits [87].

Algo más para tener en cuenta es que la AppSKey se utiliza para cifrar los datos de la aplicación entre el dispositivo final y la aplicación. Sin embargo, esta clave se deriva de la AppKey y el AppNonce. Dado que el servidor de red también conoce el AppKey, el servidor de red también puede generar el AppSKey y descifrar los datos de la aplicación [85].

4.9 Conclusiones del Capítulo

El capítulo aborda las diferentes consideraciones en términos de seguridad que se deben tener presente al momento de realizar un despliegue de la infraestructura de comunicaciones que soporta el AMI, identificando los segmentos vulnerables en la red de comunicaciones. Desde la teoría de control robusta se pueden minimizar el impacto de los ataques que se presenten en el sistema eléctrico, perfeccionando algoritmos de control de frecuencias resilientes desde el punto de vista del control secundario descentralizado, sin embargo, no pueden eliminarse estos ataques.

Desde la infraestructura de telecomunicaciones, se han explorado el uso de dispositivos inalámbricos de gran alcance y bajo consumo han facilitado el despliegue de aplicaciones basados en el IoT para diversas aplicaciones, siendo una de ellas la medición a distancia aplicado al sector eléctrico. Sin embargo, poco se ha trabajado en uno de los puntos más vulnerables de los dipositivos inalámbricos recientes como lo es la seguridad. Para esto se requiere analizar las vulnerabilidades que se presentan al momento de utilizar estas tecnologías y las contramedidas necesarias para mitigar el riesgo.

Capítulo 5

Mecanismos de seguridad

La ciberseguridad como contramedida a los diferentes ataques generados en los sistemas eléctricos recientemente han integrado algoritmos criptográficos empleados tanto en dispositivos físicos (hardware) como en niveles superiores de las aplicaciones, buscando mantener la confidencialidad y la integridad de los datos de tarificación, gestión y transaccionales en el sector energético.

El capítulo se divide en tres secciones: en la sección 5.1 relacionan los pilares de la seguridad, la sección 5.2 los mecanismos de seguridad con algoritmos HASH y de clave simétrica. Finalmente se presentan las conclusiones en la sección 5.3.

5.1 Pilares de la seguridad

5.1.1 Confidencialidad

Otro término con el que se le conoce a la confidencialidad es el de privacidad. La confidencialidad protege los datos de la manipulación de

personas o sistemas no autorizados; el objetivo principal de los ataques, es la información personal de los clientes, el consumo y la facturación, por lo que sólo las partes involucradas deberían ser las autorizadas de leer el contenido [89].

El objetivo de la confidencialidad es prevenir la divulgación no autorizada de la información sobre la organización [90]. A nivel de microrredes, la seguridad involucra a las redes AMI. Dado que los mensajes enviados no son críticos en tiempo, la disponibilidad es menos importante que la integridad y la confidencialidad. De esta manera, las soluciones de seguridad en la red para AMI se enfocan principalmente en proveer integridad y confidencialidad. Los métodos utilizados para garantizar la confidencialidad incluyen el cifrado de datos, la autenticación y el control de acceso.

5.1.2 Integridad

La integridad es la encargada de detectar la modificación o destrucción no deseada de la información. Este objetivo incluye mecanismos de defensa contra la inserción de mensajes no permitidos, el reenvió de mensajes reutilizados y el retardo de los mensajes en la red. La integridad garantiza que el contenido del mensaje no ha sido alterado entre el emisor y receptor, ya que los datos experimentan varias operaciones como captura, almacenamiento, recuperación, actualización y transferencia. Las entidades autorizadas deben mantener inalterados los datos durante todas estas operaciones. Si el contenido es modificado, entonces los participantes de la comunicación deben notificarse [89].

El objetivo de la integridad es evitar modificaciones no autorizadas de la información [90]. Los métodos utilizados para garantizar la integridad de los datos incluyen funciones criptográficas HASH, las comprobaciones de validación de datos, las comprobaciones de consistencia de los datos y los controles de acceso. En la integridad se requiere detectar la modificación o destrucción no deseada de la información. Este objetivo incluye mecanismos de defensa contra la inserción de mensajes no permitidos, el reenvío de mensajes reutilizados y el retardo de los mensajes en la red. Por

último, objetivo está la confidencialidad, que protege los datos de la manipulación de personas o sistemas no autorizados; el objetivo principal de los ataques es obtener la información personal de los clientes, el consumo y la facturación.

5.1.3 Disponibilidad

El objetivo de la disponibilidad es evitar interrupciones en los recursos y servicios de información. Algunos métodos empleados para garantizar la disponibilidad involucran copias de seguridad, redundancia en el sistema, mayor recuperabilidad del sistema, mantenimiento del equipo, sistemas operativos y software actualizados y planes de contingencia para recuperación ante eventos no planificados.

La disponibilidad de los datos es el principio que se utiliza para describir la necesidad de mantener utilizables los sistemas y servicios de información en todo momento. Para ser capaz de enviar mensaje entre emisor y receptor, una red debe estar disponible. Si una red está libre de forma limitada esto tendrá impactos negativos en la posibilidad de transmitir el mensaje [89]. Los ataques cibernéticos y las fallas en el sistema pueden impedir el acceso a los sistemas y servicios de información.

Uno de los factores más importantes en las redes de energía eléctrica es la disponibilidad, por lo tanto, la extensión de la red también es uno de los objetivos más importantes del cybersecurity [91]. Este objetivo permite el acceso oportuno y confiable al uso de los recursos en el momento que lo desee, es decir, que la red debe estar en capacidad de prevenir que personas no autorizadas impidan el acceso y bloqueen la red a otras que si lo están. La disponibilidad de la información está ligada a ciertos límites de tiempo, por ejemplo en sistemas críticos en tiempo real, la latencia máxima estimada es de 4ms [7].

A nivel de microrredes, la seguridad involucra a las redes AMI. Dado que los mensajes enviados no son críticos en tiempo, la disponibilidad es menos importante que la integridad y la confidencialidad. De esta manera,

las soluciones de seguridad en la red para AMI se enfocan principalmente en proveer integridad y confidencialidad, aprovechando las soluciones existentes para las redes de sensores y el internet [92]–[94].

Adicionalmente, los dispositivos finales, como los medidores residenciales y los ubicados en campo, tienen limitaciones en hardware como: baja capacidad de procesamiento, bajo almacenamiento en memoria, bajas tasas de transmisión, bajo throughput y protocolos de corto alcance [95].

Como solución a estas problemáticas inmersas en el proceso de medición de energía, se cuenta con la instalación de medidores inteligentes que están en la capacidad de entregar en tiempo real información actualizada y detallada sobre su consumo de energía, tal como lo menciona enel codensa - emgesa en su página web , sin embargo, no basta con la sola instalación de estos medidores inteligentes, pues como lo menciona la Superintendencia de Industria y Comercio (SIC) en su boletín tecnológico: medición y gestión inteligente de consumo eléctrico, " De igual manera, dada la vulnerabilidad de los sistemas eléctricos y la privacidad de los datos, resultaría necesario recurrir a los avances en el campo de ciberseguridad" [96].

El proceso de instalación e implementación de medidores inteligentes de consumo de energía eléctrica en Colombia ya se encuentra en desarrollo, sin embargo, para la mitigación del fraude no basta con la instalación de medidores inteligentes, sino que además es necesario hacer uso de herramientas informáticas que permitan garantizar la seguridad de la información que viaja a través de la red de medidores inteligentes mitigando las vulnerabilidades que puedan existir.

Es posible que la instalación de redes de medición inteligente o denominadas también redes inteligentes continúe evolucionando de manera exponencial en el país, lo cual podrá atribuir a la generación de mediciones más exactas y por ende a un mejor uso de la energía puesto que, "Uno de los principales objetivos de la red inteligente es que los usuarios finales tengan información sobre sus consumos y dispongan de herramientas

que favorezcan el control eficiente de sus cargas, generando así eficiencia energética" [97], sin embargo, no basta con tener mediciones inteligentes, sino que existe la necesidad de mitigar el fraude y garantizar seguridad e integridad de los datos que viajan a través de dichas redes, de no tomar medidas en el asunto es posible que se generen ataques de diferentes tipos poniendo en riesgo información sensible de los clientes o consumidores finales.

5.2 Criptografía

Las funciones criptográficas aportan seguridad al canal de comunicaciones empleado en la transferencia de datos entre los nodos. A través del uso de estos algoritmos se previenen diversos ataques del tipo pasivo y activo. En la implementación de CS en SG, se deben permitir o aprobar el uso de funciones criptográficas o de seguridad (HASH, números pseudoaleatorios, encriptación, etc,) por el NIST.

En general, existen tres tipos de algoritmos aprobados por el NIST [98], estos algoritmos han sido sometidos a intensivos análisis de seguridad antes de aprobarlos para su uso en CS. Los algoritmos criptográficos están divididos en tres grandes familias: algoritmos HASH, algoritmos de clave simétrica y algoritmos de clave asimétrica.

5.2.1 Algoritmos HASH

Los algoritmos criptográficos HASH o funciones HASH no utilizan una clave para su operación natural, su función principal es generar una cadena de caracteres más corta a la cadena de entrada, con las características de ser una función en un único sentido. Las funciones HASH son utilizadas para:

- Proporcionar autenticidad e integridad de la información a través de códigos de autenticación de mensajes (MAC)

- Comprimir mensajes y crear firmas digitales.

- Como función para derivar claves criptográficas (Key Derivation Function, KDF)

- Generar números aleatorios (Random Number Generators, RNG)

5.2.2 Algoritmos de clave simétrica

Se les llama encriptación simétrica o de llave privada por el uso compartido de una misma clave que el emisor utiliza para cifrar la información y el receptor para descifrarla. Transforman la información siendo computacionalmente muy difícil conocer su valor anterior sin conocer la clave secreta. Su uso se hace para:

- Proveer confidencialidad a un canal de comunicaciones

- Proporcionar autenticidad e integridad de la información a través de códigos de autenticación de mensajes (MAC)

- El establecimiento de claves.

En la Figura 5-1 se muestra que con la existencia de una única clave (secreta) que deben compartir emisor y receptor. Con la misma clave se cifra y se descifra por lo que la seguridad reside en mantener dicha clave en secreto [99].

En este tipo de criptografía, la seguridad se garantiza principalmente por dos factores, la robustez del algoritmo implementado y la longitud de clave utilizada, la robustez del algoritmo permite que el criptoanálisis sea inservible al momento de violar la seguridad en el canal de información, cuando los métodos de criptoanálisis son insuficientes para revelar la información, la clave entra a desempeñar un papel fundamental ante posibles ataques denominados "por fuerza bruta" los cuáles consisten en intentar obtener la clave a través de probar las posibles combinaciones de la clave por medio de herramientas computacionales, la longitud de la clave determinará la seguridad del sistema, en la actualidad, los principales

algoritmos de cifrado utilizan claves de por lo menos 128 bits, lo cual implica que hay 2128 posibles combinaciones, es decir, 3.403*1038 diferentes combinaciones, lo que garantiza la seguridad de la información por mucho tiempo para los recursos computacionales existentes hoy en día.

La criptografía simétrica implementa dos técnicas básicas utilizadas en la criptología, que se conocen como confusión y difusión propuestas por el matemático e ingeniero electrónico estadounidense Claude Elwood Shannon que se emplean a través de la sustitución y la transposición.

Los cifrados por sustitución aplican el principio de la confusión propuesta por Shannon, que consiste en sustituir caracteres del texto en claro, por otros caracteres del mismo alfabeto o de otros alfabetos. Por su parte, los cifrados por transposición aplican el principio de la dispersión también propuesto por Shannon y que tiene como acción la permutación de los caracteres del texto en claro.

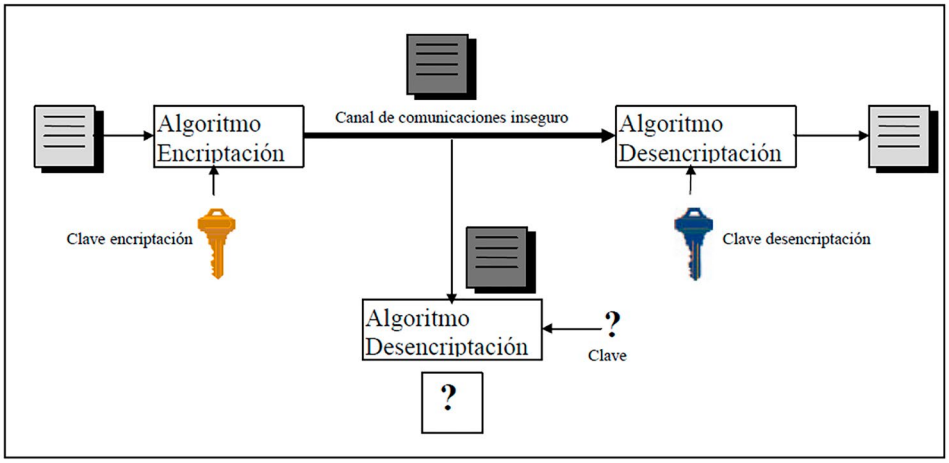

Figura 5.1 Esquema de la criptografía simétrica o de clave secreta [100]

5.2.2.1 Principales algoritmos simétricos o de clave secreta

5.2.2.1.1 DES (Data Encryption Standard)

El algoritmo de cifrado aplica permutaciones y sucesiones de manera consecutiva al texto en claro, este algoritmo utiliza una clave simétrica de 64 bits, de los cuales los primeros 54 bits se utilizan para el proceso de cifrado, los 8 bits restantes de la clave se utilizan para procesos de detección de errores, por lo cual la clave efectiva que utiliza DES es de 54 bits. En la actualidad este algoritmo ya no es un estándar seguro debido a que hoy en día se puede vulnerar este algoritmo por tres métodos de criptoanálisis: Criptoanálisis Diferencial, Criptoanálisis Lineal y ataque por fuerza bruta.

5.2.2.1.2 3DES (Triple Data Encryption Standard)

Como su nombre lo indica, este algoritmo consiste en aplicar las mismas funciones que DES pero en tres ocasiones, utiliza una longitud de clave de 128 bits, que se divide a su vez en dos claves de 64 bits; 3DES aumenta de manera considerable la seguridad con respecto a DES pero consume recursos computacionales significativos a diferencia de DES, existe otra variante de este tipo de algoritmos aunque no es muy conocida por su alto consumo de recursos computacionales conocido como DES-EDE3, se utiliza una longitud de clave de 192 bits que se divide en tres claves, con este algoritmo se consigue mayor robustez.

5.2.2.1.3 RC5 (Rivest Cipher 5)

Este tipo de algoritmo se caracteriza por tener la capacidad de variar la longitud de clave, el número de iteraciones y los bloques de información, se aplican operación XOR a los bloques de información que pueden ser de 32,64 o 128 bits, la seguridad de este algoritmo aumenta con relación a la cantidad de iteraciones que se realicen.

5.2.2.1.4 IDEA (International Data Encriptión Algorithm)

Utiliza una clave de longitud de 128 bits que se aplica a bloques de datos de 64 bits, IDEA combina operaciones de matemática modular y operaciones lógicas de la OR exclusiva, debido a longitud de clave los ataques por fuerza bruta se hacen ineficientes y se considera un algoritmo bastante seguro para muchas aplicaciones.

5.2.2.1.5 BLOWFISH

Este algoritmo utiliza longitud de bloque de 64 bits, con longitudes de clave variable que por lo general son de 32, 64 y 128 bits aunque tiene la posibilidad de implementar claves de hasta 448 bits, realiza un total de 16 iteraciones utilizando operaciones de matemática modular y OR exclusiva, la principal ventaja de este algoritmo es que es de uso libre en todo el mundo.

5.2.2.1.6 AES (Advanced Encryption Standard)

Este algoritmo utiliza longitud de clave variable que puede ser de 128, 192 o 256 bits, la longitud de los bloques es de 128 bits, la cantidad de iteraciones o rondas que utiliza depende de la longitud de clave utilizada en el algoritmo, utiliza en su mayoría cálculos realizados en estructuras de campos finitos. Este algoritmo es un estándar de cifrado adoptado por el gobierno de los Estados Unidos a partir del 2001 luego de ser el algoritmo ganador en un concurso organizado por el NIST en 1997.

5.2.2.2 Algoritmos de clave asimétrica

Los algoritmos asimétricos conocidos también como algoritmos de clave pública incluyen el manejo de dos tipos de claves, llave pública y llave privada, en este esquema se genera una llave pública a partir de la llave privada que se comparte con los demás usuarios. La información se cifra con

la llave pública y solo quien posea la clave privada asociada puede descifrar la información, la llave pública puede conocerse por cualquier entidad, pero ésta no debe revelar de ninguna forma información acerca de la clave privada. Estos algoritmos son usados comúnmente para:

- Proveer confidencialidad a un canal de comunicaciones
- Comprobar firmas digitales
- Establecer las claves secretas entre dos entidades
- Como RNG

Las desventajas de usar este esquema de encriptación están ligadas a los tiempos necesarios para procesar la información, debido a que las claves para estos sistemas son de mayor tamaño que las de un esquema simétrico, donde el texto cifrado es siempre de mayor tamaño que el texto plano, ocasionando que se envíe menos información que en un esquema de cifrado simétrico; requiriendo mayor tiempo para procesar la información y más recursos en el canal de comunicaciones. Estas desventajas, sumado a los requerimientos de la microrred, hacen que se descarte el uso de los algoritmos asimétricos en el esquema de seguridad, adicionalmente los algoritmos simétricos están aprobados por el NIST para su uso en SG [101], incluyen AES y TDES para cifrado simétrico y los algoritmos basados en funciones HASH (SHA) para autenticación y generación de claves.

Capítulo 6

Vulnerabilidad de la red inalambrica

La forma de evidenciar las vulnerabilidades que se presentan en un sistema de comunicaciones que opera en una microrred residencial es realizando ataques controlados a la red de prueba. Para esto se van a realizar ataques a una red inalámbrica, donde sus trasmisores funcionan con el estándar LoRaWAN (v1.0 y v1.1) desplegada en una topología en estrella para los dispositivos de la red AMI conectados a los dispositivos de la microrred, centralizando sus datos en un gateway.

Los posibles ataques para validar las vulnerabilidades de mayor relevancia en la red LoRaWAN son los ataques de: eavesdropping, jamming, replay, bit flipping, ACK spoofing, Man in the middle y el de denegación de servicios DoS.

El capítulo contempla siete posibles ataques a implementar como lo son: eavesdropping, jamming, replay, bit flipping, ACK spoofing, Man in

the middle y el de denegación de servicios DoS. Finalmente se presentan las conclusiones en la sección 6.8.

6.1 Ataque de Eavesdropping

La interceptación (eavesdropping) es un ataque pasivo de difícil detección mientras se lleva a cabo, donde el atacante realiza dos acciones: escuchar (sniffing) y grabar (capturing) comprometiendo la privacidad de la red; en este proceso los datos permanecen intactos, esto no significa que los datos capturados puedan leerse o entenderse [85]. Este ataque pasa de pasivo a convertirse en activo cuando el atacante hace uso de esta información, causando problemas de privacidad por ejemplo al utilizar el estándar LoRaWAN [89].

6.1.1 Descripción del ataque

En una red LoRaWAN, el ataque lo puede realizar cualquier miembro con acceso a la red, aunque el nodo malicioso no necesariamente debe ser un miembro activo dentro de la misma red. La zona más vulnerable para este tipo de ataque está entre los nodos y el gateway. La mayoría del tráfico que puede obtenerse (sniffed) en la red LoRaWAN esta encriptada, por lo tanto, se requieren acciones adicionales para acceder a los datos reales transmitidos. Utilizando un dispositivo (sniffer) que escuche las señales de radio transmitidas, las visualice o represente como paquetes de datos de red, y las guarde para su posterior análisis este ataque se convierte en un ataque activo.

Una forma de mitigar este ataque es codificar toda la trama enviada, esto debido a que la visualización de los datos no encriptados le permite al atacante tener información útil para identificar la conformación de la trama enviada y la ubicación de los datos en la misma.

6.2 Ataque de Jamming

El ataque de interferencia (Jamming) es un ataque que se realiza mediante la emisión de energía electromagnética al receptor víctima y pueden tener como objetivo diferentes capas del modelo OSI:

- Interferencia de la capa física, donde el atacante envía cualquier señal de banda ancha con una relación señal-ruido (SNR) más alta que la víctima.

- Interferencia de la capa MAC, donde el atacante sólo interviene partes específicas del mensaje (por ejemplo, el CRC32, o el mensaje firmas), asegurándose que el paquete es desechado por el destinatario, este ataque tiene como finalidad interrumpir o alterar las transmisiones de radio.

6.2.1 Vulnerabilidades del estándar

El estándar LoRaWAN no se basa ni en la detección de canales ni en la sincronización de tiempo para evitar colisiones, su principal defensa contra colisiones es la baja velocidad de transmisión de datos de los dispositivos finales en la red. Éstas colisiones no siempre terminan en pérdida de paquetes, al presentarse transmisiones simultáneas de paquetes a la misma frecuencia y con el mismo factor de ensanchamiento (SF - por sus siglas en inglés : Spread Factor), se puede generar interferencia mutua [103]. Esta vulnerabilidad en la capa física de LoRa permite a los atacantes emplear dispositivos que no son demasiado sofisticados o especializados para realizar un ataque de jamming en redes LoRa, mediante el envío de mensajes LoRa a una frecuencia determinada que eliminen todas las transmisiones en esa frecuencia. En la figura 6-1 se clasifica las interferencias en dos categorías de acuerdo con su capacidad de detectar el medio: canal consciente y canal inconsciente.

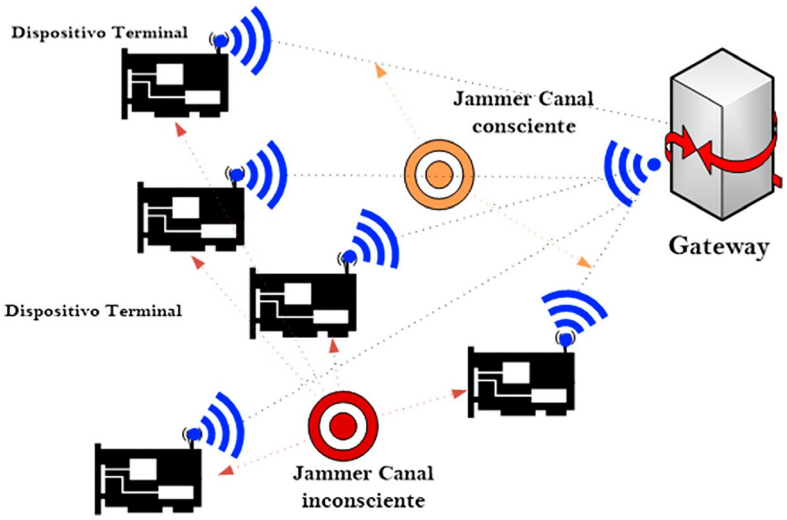

Figura 6.1 Ataque jamming

El jammer de canal inconsciente está a la escucha de una de las sub-bandas y una vez se detecta actividad en el canal, se envía un paquete en el mismo canal y SF. Mientras que el jammer de canal consciente en lugar de escuchar el canal, se transmite sobre los tres canales al tiempo de forma periódica un determinado nivel DC y selecciona un SF aleatorio cada vez que se envía un paquete.

En el ataque se utiliza jamming por ruido de banda parcial [104], introduciendo una señal interferente a una parte específica del espectro cubriendo solamente los canales usados, con el mismo SF del nodo. Al realizar esto, se busca que la transmisión del mensaje sea afectada de tal forma que el mensaje sea rechazado o en su defecto, se modifique la información que contiene.

La forma de mitigar el ataque es reduciendo las colisiones que se presentan en la red añadiendo canales para la transmisión de los mensajes dentro de la banda de frecuencias, también variar el SF entre el envío de los mensajes del nodo dificultando el ataque y evitando las interferencias entre nodos en una red a gran escala.

6.3 Ataque por Replay

El ataque de replay (reproducción), tiene como principio reproducir maliciosamente una transmisión válida. Normalmente se utiliza combinado con un ataque de denegación de servicio (DoS) y/o spoofing (suplantación de identidad). El atacante genera un spoofing del nodo, intercepta y repite la transmisión de datos válida a través de la red, después del ataque el servidor valida el mensaje proveniente de un nodo autenticado previamente en la red. Cuando el nodo suplantado intenta enviar un mensaje o conectarse nuevamente a la red, provoca una denegación de servicio en el servidor, debido a que los controles de seguridad de la red validan la existencia de un nodo con los datos de autenticación proveídos por el nodo legítimo.

Este ataque se basa en la captura previa al sniffing, donde el dispositivo malicioso captura las credenciales del nodo final.

Para el caso de la red LoRaWAN, la activación por ABP posee una vulnerabilidad crítica, debido a que las llaves son invariables y no requiere autenticación constante en la red, por lo tanto, para que un mensaje malicioso, sea aceptado por el servidor LoRaWAN debe cumplir los siguientes requisitos:

- Las claves de sesión son las mismas que las de un dispositivo final aceptado.

- El campo de DevAddr es el mismo que el de un dispositivo final aceptado.

- El valor del Counter es aceptable.

Cuando se realiza este ataque, el atacante puede elegir y reenviar los mensajes antes de un reinicio, y el servidor no puede determinar si estos mensajes son de la sesión actual o de una sesión anterior al reinicio de

la conexión. Adicionalmente, el protocolo no establece como debe usarse el fragmento "Counter" de la trama de forma segura.

En este ataque el contador debe reiniciarse, por lo que el atacante debe tener la capacidad de reestablecer los dispositivos finales y esperar hasta que el valor del contador del dispositivo final llegue a su máximo y luego reiniciar desde o para los dispositivos finales activados por OTAA. Mientras que en los dispositivos finales activados por ABP, el atacante también puede esperar hasta que el contador se desborde o reiniciar los dispositivos finales y su contador también se reinicie en o empleando menos tiempo que la activación por OTAA.

6.3.1 Representación del ataque

El ataque usa la información de sesiones de captura de datos previas, dichas sesiones de captura se realizan por medio de eavesdropping, para luego reenviarse en instantes de tiempo posteriores. Este ataque es generalmente usado para explotar las vulnerabilidades en la autenticación. En la figura 6.2 se muestra el diagrama de un ataque por replay, donde se identifica una combinación gateway y servidor malicioso enlazándose con el dispositivo terminal.

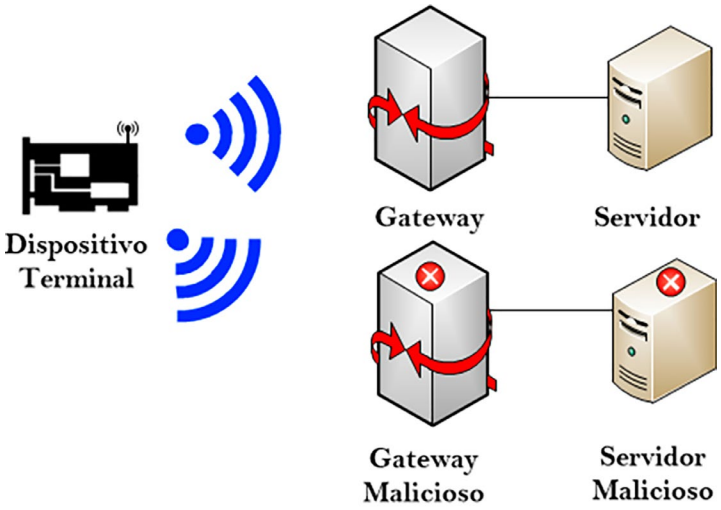

Figura 6.2 Ataque replay [89]

Este ataque se puede evitar utilizando una marca secuencial o marca de tiempo en las tramas de intercambio de datos entre los nodos y el gateway. Los servidores y routers pueden también almacenar mensajes repetidos y eliminarlos tras cierto número de repetidores, limitando el número de intentos que un atacante pueda realizar.

6.4 Ataque de Bit Flipping

El ataque Bit Flipping (inversión de bit) es un método que puede cambiar campos específicos en el texto cifrado sin decifrar el texto cifrado, y pretende probar la integridad del mensaje al cambiar un bit de la trama que se envía desde el servidor de red para verificar si el servidor de aplicación puede desencriptar apropiadamente el mensaje recibido o detectar que el mensaje proviene de una fuente no autorizada [89].

La integridad del mensaje se ve comprometida debido a que en el estándar LoRaWAN el mensaje se verifica nuevamente después de que pasa a través del servidor de red, por lo tanto, el mensaje se podría alterar durante el intercambio de información entre el servidor de red y el servidor de la aplicación. En la figura 6.3 se muestra el esquema del ataque bit flipping.

6.4.1 Descripción del ataque

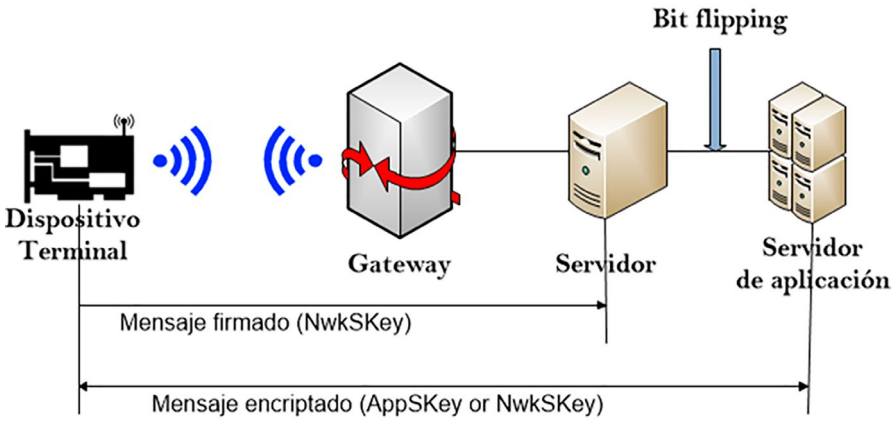

Figura 6.3 Ataque Bit Flipping

Este ataque es factible en modos de encriptación específicos, donde el texto plano tiene el mismo orden de bits con el texto cifrado. El atacante solo debe modular bits en las mismas posiciones del texto cifrado. Al enviar un mensaje sin encriptar (plaintext) y su respectiva llave de encripción (Keystream), se puede generar un mensaje cifrado (ciphertext). Por lo tanto, al enviar un mensaje el protocolo lo maneja de la siguiente forma:

plaintext XOR Keystream = ciphertext
ciphertext XOR Keystream = plaintext

Con lo anterior se puede notar que la posición de los bits del ciphertext es igual a la posición de los bits del plaintext, lo que significa que, si se cambia algún valor del ciphertext, se puede alterar el plaintext. Esto indica que no solo puede alterarse la información sino también los encabezados, la ruta y/o comandos dentro del mensaje [89]. Para llevar a cabo este ataque, se necesita tener acceso al servidor de red o que el atacante sea capaz de realizar un ataque de Man-in-the-Middle entre el servidor e red y el servidor de la aplicación para modificar la información.

De acuerdo con la intención del atacante es posible obtener diferentes resultados dependiendo de la parte del mensaje que se altera, por ejemplo, cuando se realiza el ataque sobre:

6.4.1.1 FrmPayload

Se puede lograr vulnerar la integridad de los datos que son enviados al servidor de la aplicación desde los nodos, provocando que dichos datos entrantes sean falsos.

6.4.1.2 Valor del FCount

Cuando el atacante cambia el valor del contador, puede causar que exista una falta de sincronismo de los valores del contador en la trama y el servidor de aplicación haciendo que se rechacen y se descarten los

mensajes entrantes al servidor de la aplicación. Si el atacante realiza este procedimiento iterativamente provoca un ataque de denegación de servicio (DoS).

6.4.1.3 DevAddr:

Cuando se cambia ese parámetro, el servidor asume que el mensaje proviene de otro nodo diferente [89].

La integridad de los datos se debe verificar una vez hayan pasado por el servidor o en el servidor de aplicaciones y no en el servidor de red. Otro método para evitar este tipo de ataque es cambiar aleatoriamente las posiciones de los campos de información en los dispositivos finales empleando técnicas complejas que permitan estos cambios en el texto cifrado.

6.5 Ataque de ACK Spoofing

Este ataque tiene como finalidad explotar las falencias del diseño que se presentan al hacer uso del mensaje opcional de ACK en el estándar LoRaWAN, a través de una suplantación de identidad del nodo o gateway, la cual permite que se haga uso del ”nombre” del dispositivo para reconocer como válidos los mensajes de ACK provenientes del atacante.

En este ataque la parte más vulnerable de la red es el gateway, debido a que es el puente entre la conexión a internet y el nodo por lo que se puede comprometer por medio de falsificación de UDP permitiendo introducir a la red LoRaWAN un gateway malicioso. Una gran falla del protocolo es que para un mensaje de uplink el ACK no indica el mensaje que se confirma, solamente confirma que el último mensaje es recibido. Entonces, el gateway malicioso podría guardar la confirmación enviada y usarla para futuros mensajes[89].

6.5.1 Descripción del ataque

En la Figura 6.5 se muestra la forma de realizar el ataque ACK spoofing, en donde el nodo final envía un mensaje M1 (uplink), cuando el servidor de aplicación recibe el mensaje de confirmación del gateway, en vez de enviar un mensaje de respuesta al nodo final (downlink), el gateway guarda dicho mensaje para un uso posterior. Debido a que el nodo final no recibe confirmación del gateway, retransmite el mensaje y después de un tiempo descarta ese mensaje (cree que se perdió o fue rechazado).

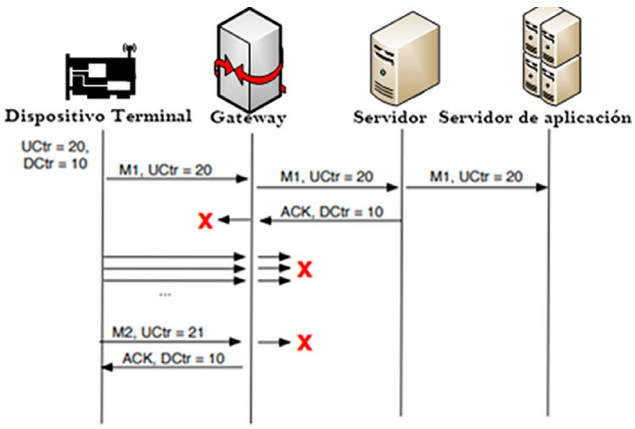

Figura 6.4 Ataque ACK spoofing [89]

El nodo final envía el siguiente mensaje M2 y el gateway malicioso utiliza el ACK anteriormente guardado para hacer creer al nodo que el mensaje ha sido enviado correctamente, sin embargo, este nunca llega al servidor de aplicación.

Existen diferentes formas de mitigar este tipo de ataques, iniciando con la restricción física al Gateway, emplear accesos remotos por SSH, enlaces con el servidor por TCP.

6.6 Ataque de Man in the Middle (MitM)

En el ataque de intermediario (Man in the Middle), el atacante se ubica entre el nodo origen y destino, con la capacidad de leer, insertar y

modificar los mensajes interceptados sin que ninguna de las partes se dé por enterado. Este tipo de ataque requiere una forma activa de eavesdropping, permitiendo el acceso a los datos que las dos partes de la red están intercambiando. Dado que la comunicación entre los nodos y el gateway se hace inalámbricamente, éste es el segmento más vulnerable para realizar este ataque a diferencia del segmento entre el servidor de red y el servidor de aplicación, donde su enlace es cableado en la mayoría de las veces.

6.6.1 Descripción del ataque

En la figura 6-5 se muestra el esquema del ataque MitM, donde el atacante se ubica entre el nodo y el gateway interceptando los mensajes antes de que lleguen al destino.

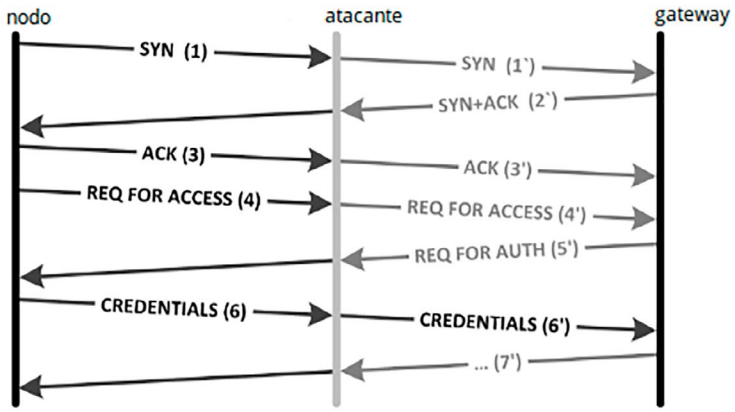

Figura 6.5 Ataque Man in the Middle

De esta forma el atacante intercepta todos los mensajes que van entre las dos víctimas e inyectar nuevos. Esto se realiza en dos pasos antes de que el mensaje complete un ciclo, el primero entre el nodo y el atacante y el segundo entre el atacante y el gateway, sin embargo, el nodo y el gateway piensan que tienen una comunicación directa entre ellos.

Existen diferentes formas de implementar estrategias de defensa contra estos ataques. MitM emplean técnicas de autenticación basadas en claves públicas, autenticación mutua fuerte, claves secretas, contraseñas.

La integridad de las claves públicas debe asegurarse de alguna manera, pero éstas no exigen ser secretas, mientras que las contraseñas y las claves de secreto compartido tienen el requerimiento adicional de la confidencialidad. Las claves públicas pueden verificarse por una autoridad de certificación (CA), cuya clave pública sea distribuida a través de un canal seguro (por ejemplo, integrada en el navegador web o en la instalación del sistema operativo).

La mayoría de la información que puede recolectarse en una red LoRaWAN está encriptada, requiriéndose acciones adicionales para obtener el acceso real a los datos, sin embargo, LoRaWAN emplea contadores como una medida para evitar este tipo de ataque [85].

6.7 Ataque Denial of Service (DoS)

La denegación de servicio (Denial of Service) consiste en evitar que usuarios legítimos puedan acceder a un servicio o recursos, mediante la sobrecarga de la red con consumo del ancho de banda durante un periodo de tiempo, proporcionando pérdida en la conectividad con la red. La degradación de la calidad del servicio la consiguen los atacantes solicitando múltiples peticiones saturando los recursos del sistema que aloja el servicio, siendo incapaces de atenderlos. Los ataques de denegación de servicio (DoS) amenazan la disponibilidad del sistema y evitan que los usuarios legítimos tengan acceso y usen sistemas de información cuando sea necesario.

En el ataque de DoS, solo una fuente realiza el ataque, siendo impráctico debido a que la capacidad de las infraestructuras ha aumentado con el tiempo, permitiendo una atender mayor cantidad de peticiones de forma simultánea. La evolución de este tipo de ataque es la denegación de servicio distribuidos (Distributed Denial of Service), los ataques DDoS utilizan un elevado número de dispositvos atacantes contra un objetivo al mismo tiempo, para esto se utilizan bots, sistemas infectados cuyo propietario muchas veces desconoce que sus dispositivos hacen parte de una red

maliciosa. Los tipos de agotamiento de recursos son los de recursos de red y el de CPU, memoria o disco usado en la aplicación.

6.7.1 Descripción del ataque

En una red LoRaWAN, el segmento vulnerable se encuentra entre el nodo final y el servidor, mediante el uso de mensajes del tipo join-accept se realiza este tipo de ataque, donde el gateway recibe tantas peticiones de acceso al servidor por parte del atacante, bloqueando la solicitud del nodo que quiere alcanzar dicho gateway. En la figura 6.6 se muestra el esquema general del ataque de DoS.

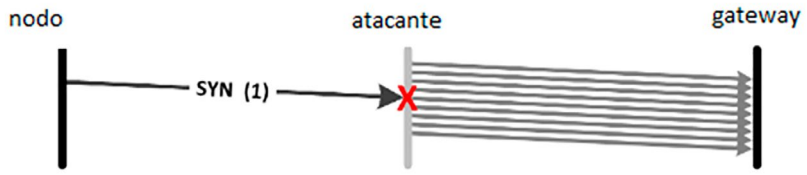

Figura 6.6 Ataque denegación de servicio DoS

La implementación de medidas preventivas para contrarrestar este tipo de ataques es imprescindible, ya que causan graves consecuencias en el sistema atacado ya que solo se identifica cuando el servicio ha dejado de funcionar. Para minimizar las consecuencias de este ataque se deben incorporar distintas medidas de seguridad, como proteger la red interna implementando un sistema de detección y prevención de intrusiones (IDS/IPS) que estén al tanto de las conexiones y genere alertas si detecta intentos de acceso no autorizados o mal uso de protocolos; utilizar un dispositivo o software con funcionalidad mixta, como un UTM que permite gestionar de manera unificada la mayoría de ciberamenazas que pueden afectar la red.

La redundancia permite duplicar el activo en más de un servidor y el balanceado de carga asignar la carga de trabajo asignado a un servidor u otro. Contar con más de un servidor reducirá la posibilidad de que se detengan debido a la sobrecarga. Además, aporta otras ventajas como la tolerancia a los fallos, esto es, si un servidor falla, el total del trabajo lo asumiría el otro servidor.

6.8 Conclusiones del capítulo

En este capítulo se abordaron las temáticas necesarias que permean aspectos importantes en el diseño, implementación y funcionamiento de las microrredes, buscando cumplir con los pilares de la seguridad.

El sistema de comunicaciones se compone por dos grandes áreas, la primera con la infraestructura de comunicaciones, donde se define la arquitectura y topología de red, los estándares y tecnologías para la transmisión de los datos y los protocolos de encaminamiento abarcando las capas físicas, de enlace, red y transporte del modelo de sistemas abiertos de interconexión (Open Systems Interconnection, OSI) de la organización internacional de estándares (International Organization for Standardization, ISO) [102]. La segunda área está compuesta por las aplicaciones de software, la estructura de almacenamiento y visualización de datos que permiten proporcionarle a los datos seguridad y servicios adicionales, abarcando las capas de presentación, sesión y aplicación de dicho modelo.

Las vulnerabilidades detectadas en el segmento inalámbrico como el alambrado, permiten identificar los puntos más débiles en términos de seguridad de la información al momento de emplear dispositivos de medición con transferencia de datos entre los dispositivos de una microrred y el punto de gestión para entornos residenciales. Generando una serie de medidas que permitan mitigar los riesgos de mantener una infraestructura de comunicaciones sin defensas a ataques que deben adoptarse en los protocolos de seguridad de las empresas encargadas de la comercialización de energía.

Conclusiones

La incorporación de nuevos recursos energéticos sumadas a las nuevas tendencias en el consumo de energía, derivados de los nuevos estándares de calidad de vida y confort en los consumidores residenciales, han generado nuevos requerimientos y cambios en los paradigmas de generación y consumo de energía. Esto sumado con los objetivos de desarrollo sostenible han impulsado el desarrollo de sistemas de gestión de energía para usuarios residenciales, los cuales ahora no solo serán vistos como consumidores sino como generadores de energía. Dentro de las estrategias de gestión de energía que se encuentran en la literatura se busca la maximización del uso del recurso energético disponible y la minización del consumo de energía de la red y así buscar su independencia energética. Sin embargo, aún se requiere trabajo adicional en cuanto a dispositivos y algoritmos que permitan una implementación en hogares.

En este sentido diferentes tecnologías emergentes como los dispositivos IoT y la computación en la nube permitirán la adquisición y manejo de una gran cantidad de datos que permitan identificar las preferencias de consumo de los usuarios residenciales y de esta forma plantear algoritmos de gestión que más personalizadas y a la medida de los usuarios.

Adicionalmente, la descentralización de la generación y la interoperación de diferentes microrredes residenciales requiere capacidades de cómputo local que deben ser capaces de ejecutar modelos de optimización predeterminados y filtrar y comprender señales locales para pasar señales necesarias al controlador central de la microrred y manejo de una gran cantidad de información.

El cómputo actual soporta despliegue eficiente de sistemas de cómputo FOG y cloud ejecutando procesamiento de información cerca de las fuentes de información, por ejemplo, dentro de la microrred o cerca de los límites de la misma. Adicionalmente, el despliegue de capacidades de inteligencia artificial permite el muestreo de datos a intervalos mucho más altos que las estructuras típicas mejorando el rango de 15 a 60 minutos y disminuyéndolas a menos de un minuto, superando las limitaciones de la congestión de la red de datos, almacenamiento y cómputo por fuera de línea.

La inclusión de diversas tecnologías de última tendencia en el sistema de administración de energía de las microrredes eléctricas domiciliarias hacen que el sistema sea capaz de reaccionar de manera adecuada para ejecutar análisis y generar modelos con base en la información recolectada. De esta manera, el sistema completo se vuelve autónomo y efectivo en base a costo, mientras que otros requerimientos como el ancho de banda y conectividad se minimizan.

La rápida expansión del cómputo en la nube hace que los servidores locales se vuelvan obsoletos y permite el procesamiento remoto de una gran cantidad de información. El cómputo FOG es un requerimiento necesario para soportar el cómputo en la nube, puesto que reduce el ancho de banda requerido, lo que es clave para acceder la infraestructura de cómputo en la nube.

Sin embargo, la transmisión y manejo de una gran cantidad de información sobre la cual se deben garantizar los pilare básicos de seguridad; Confidencialidad, Integridad, Disponibilidad. El manejo de información por redes de comunicación generalmente inalámbricas le permite a un atacante tener

un acceso al medio de forma simple y sencilla, ya que la comunicación y el transporte de los datos se realiza por medio de ondas de radio transmitidas en el aire y es prácticamente imposible que se restrinja el acceso al medio por parte de los operadores para evitar fugas de información o intrusiones no permitidas cuando se hace uso de este método para transportar los datos, causando que se quebrante uno de los pilares de la seguridad de la información, el cual es la integridad de los datos.

Una contra medida admisible para la vulnerabilidad de confiabilidad que presentan las comunicaciones inalámbricas como las empleadas en el estándar LoRaWAN, es la encriptación de la trama completa, o como mínimo la parte del MACpayload, debido a que en esta sección se encuentran el contador, el puerto, la dirección del nodo y otros campos que contienen información del mensaje que puede ser utilizada por un ente malicioso. La mitigación de los ataques como el bit-flipping se pueden realizar haciendo una verificación de los datos en la aplicación final y el ataque de ACK Spoofing se recomienda añadir un firewall en la red para evitar intrusiones y malware que puedan comprometer al gateway.

Referencias

[1] C. L. Trujillo Rodriguez et al., "Generalidades de Microrredes Eléctricas," in Microrredes Eléctricas, 1st ed., Bogotá D.C.: Universidad Distrital, 2015, p. 178.

[2] E. Rodriguez-Diaz, J. C. Vasquez, and J. M. Guerrero, "Intelligent DC Homes in Future Sustainable Energy Systems: When efficiency and intelligence work together," IEEE Consumer Electronics Magazine, vol. 5, no. 1. pp. 74–80, 2016.

[3] K. Ehrhardt-Martinez, "Changing habits, lifestyles and choices: The behaviours that drive feedback-induced energy savings," pp. 2085–2094, 2011.

[4] B. T. Patterson, "DC, Come Home: DC Microgrids and the Birth of the Enernet," IEEE Power and Energy Magazine, vol. 10, no. 6. pp. 60–69, 2012.

[5] "How residential IOT can help shape a smart city." [Online]. Available:http://smartcity.lv/how-residential-iot-can-help-shape-a-smart-city/. [Accessed: 23-Mar-2020].

[6] E. E. Gaona-García, S. L. Martínez-Rojas, C. L. Trujillo Rodriguez, and E. A. Mojica-Nava, "Autenticated Encription of PMU Data," Tecnura, vol. 18, no. December, pp. 70–79, 2014.

[7] NITS, Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, vol. 1, no. August. National Institute of Standards and Technology, 2010.

[8] Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab, and Y. Al-Turki, "Networked Microgrids for Enhancing the Power System Resilience," Proceedings of the IEEE. 2017.

[9] J. Gao, Enhancing the Resilience of the Nation's Electricity System. 2017.

[10] J. E. Sullivan and D. Kamensky, "How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid," Electr. J., 2017.

[11] S. Mishra, K. Anderson, B. Miller, K. Boyer, and A. Warren, "Microgrid resilience: A holistic approach for assessing threats, identifying vulnerabilities, and designing corresponding mitigation strategies," Appl. Energy, 2020.

[12] J. Stamp, "The SPIDERS project - Smart Power Infrastructure Demonstration for Energy Reliability and Security at US military facilities," 2012.

[13] B. Mundial, "Acceso a la electricidad, sector rural (% de la población rural)," 2020. [Online]. Available: https://datos.bancomundial.org/indicador/EG.ELC.ACCS.RU.ZS. [Accessed: 01-Apr-2020].

[14] J. Sankar V.C., M. Raghunath, and M. G. Nair, "Optimal scheduling and energy management of a residential hybrid microgrid," in 2017 Innovations in Power and Advanced Computing Technologies (i-PACT), 2017, pp. 1–6.

[15] E. Rodriguez-Diaz, F. Chen, J. C. Vasquez, J. M. Guerrero, R. Burgos, and D. Boroyevich, "Voltage-Level Selection of Future Two-Level LVDC Distribution Grids: A Compromise Between Grid Compatibiliy, Safety, and Efficiency," IEEE Electrification Magazine, vol. 4, no. 2. pp. 20–28, 2016.

[16] N. Rajasekar, N. Bilakanti, and M. Miyatake, "Energy management technique for home micro grid system," TENCON 2017 - 2017 IEEE Region 10 Conference. 2017.

[17] A. S. O. Ogunjuyigbe, T. R. Ayodele, and O. E. Oladimeji, "Management of loads in residential buildings installed with PV system under intermittent solar irradiation using mixed integer linear programming," Energy and Buildings, vol. 130. pp. 253–271, 2016.

[18] A. S. O. Ogunjuyigbe, C. G. Monyei, and T. R. Ayodele, "Price based demand side management: A persuasive smart energy management system for low/medium income earners," Sustainable Cities and Society, vol. 17. pp. 80–94, 2015.

[19] S. H. Hong, M. Yu, and X. Huang, "A real-time demand response algorithm for heterogeneous devices in buildings and homes," Energy, vol. 80. pp. 123–132, 2015.

[20] M. Pipattanasomporn, H. Feroze, and S. Rahman, "Securing critical loads in a PV-based microgrid with a multi-agent system," Renew. Energy, vol. 39, no. 1, pp. 166–174, 2012.

[21] D. Lu and B. Francois, "Strategic framework of an energy management of a microgrid with a photovoltaic-based active generator," 2009 8th International Symposium on Advanced Electromechanical Motion Systems & Electric Drives Joint Symposium. 2009.

[22] V. Dash and P. Bajpai, "Power management control strategy for a stand-alone solar photovoltaic-fuel cell--battery hybrid system," Sustainable Energy Technologies and Assessments, vol. 9. pp. 68–80, 2015.

[23] J. Von Appen, Sizing and operation of residential photovoltaic systems in combination with battery storage systems and heat pumps. Kassel University Press, 2018.

[24] S. Saravanan and S. Thangavel, "Fuzzy logic controller based power management for a standalone solar/wind/fuel cell fed hybrid system," Journal of Renewable and Sustainable Energy, vol. 5, no. 5. p. 53147, 2013.

[25] J. Yamini and Y. Ratna Babu, "Design And implementation of smart home energy management system," 2016 International Conference on Communication and Electronics Systems (ICCES). 2016.

[26] Z. Xuhui, L. Na, K. Peihua, and L. Boyang, "Design of the Networked Electric Meter Based on GPRS," 2014 Fourth International Conference on Instrumentation and Measurement, Computer, Communication and Control. 2014.

[27] A. A. Adhau, N. M. Patel, A. T. Zaidy, S. L. Patil, and A. S. Deshpande, "Low cost electricity meter reading system using GSM," 2013 International Conference on Energy Efficient Technologies for Sustainability. 2013.

[28] K. P. Pandey and A. Upadhyay, "Design and implementation of SPI protocol," International Journal of Advance Engineering and Research Development, vol. 4, no. 12. 2017.

[29] A. Perez, "Ethernet Technology - Resource Management," IP, Ethernet and MPLS Networks. pp. 203–226, 2013.

[30] C. Wang, T. Jiang, and Q. Zhang, ZigBee\textregistered Network Protocols and Applications. CRC Press, 2016.

[31] L. Meng, E. R. Sanseverino, A. Luna, T. Dragicevic, J. C. Vasquez, and J. M. Guerrero, "Microgrid supervisory controllers and energy

management systems: A literature review," Renewable and Sustainable Energy Reviews, vol. 60. pp. 1263–1273, 2016.

[32] C. Dou, D. Yue, Q.-L. Han, and J. M. Guerrero, "Multi-Agent System-Based Event-Triggered Hybrid Control Scheme for Energy Internet," IEEE Access, vol. 5. pp. 3263–3272, 2017.

[33] J. Yue, Z. Hu, C. Li, J. C. Vasquez, and J. M. Guerrero, "Optimization scheduling in intelligent Energy Management System for the DC residential distribution system," 2017 IEEE Second International Conference on DC Microgrids (ICDCM). 2017.

[34] D. Martin, "Hardware-In-The-Loop for Power and Telecomunications Co-Simulation with Applications," 2014.

[35] A. Garro, M. Mühlhäuser, A. Tundis, M. Baldoni, and P. Torroni, "Intelligent Agents: Multi-Agent Systems," in Reference Module in Life Sciences, 2018.

[36] T. Kim, J. Yun, and W. Qiao, "A multiagent system for residential DC microgrids," 2015 IEEE Power & Energy Society General Meeting. 2015.

[37] R. Fazal, J. Solanki, and S. K. Solanki, "Demand response using multi-agent system," 2012 North American Power Symposium (NAPS). 2012.

[38] S. Kahrobaee, R. A. Rajabzadeh, L.-K. Soh, and S. Asgarpoor, "A Multiagent Modeling and Investigation of Smart Homes With Power Generation, Storage, and Trading Features," IEEE Transactions on Smart Grid, vol. 4, no. 2. pp. 659–668, 2013.

[39] E. R. Diaz, X. Su, M. Savaghebi, J. C. Vasquez, M. Han, and J. M. Guerrero, "Intelligent DC microgrid living laboratories - A Chinese-danish

cooperation project," in 2015 IEEE 1st International Conference on Direct Current Microgrids, ICDCM 2015, 2015.

[40] K. Palaniappan, S. Veerapeneni, R. Cuzner, and Y. Zhao, "Assessment of the feasibility of interconnected smart DC homes in a DC microgrid to reduce utility costs of low income households," 2017 IEEE Second International Conference on DC Microgrids (ICDCM). 2017.

[41] PE/T&D - Transmission and Distribution, "IEEE 2030.7-2017 - IEEE Standard for the Specification of Microgrid Controllers," 2017. [Online]. Available: https://standards.ieee.org/standard/2030_7-2017.html. [Accessed: 01-Apr-2020].

[42] E. E. Gaona Garcia, "Esquemas de trasmisión de datos en una Microrred a través de una Infraestructura de medición avanzada," Rev. UIS Ing., vol. 15, no. 2, pp. 85–92, Jan. 2017.

[43] E. Wood, "The Home Microgrid: Not Later. Now. - Microgrid Knowledge," Microgrid Knowledge. 2014.

[44] F. Luo, G. Ranzi, S. Wang, and Z. Y. Dong, "Hierarchical Energy Management System for Home Microgrids," IEEE Transactions on Smart Grid, vol. 10, no. 5. pp. 5536–5546, 2019.

[45] Z. Zhao, W. C. Lee, Y. Shin, and K.-B. Song, "An Optimal Power Scheduling Method for Demand Response in Home Energy Management System," IEEE Transactions on Smart Grid, vol. 4, no. 3. pp. 1391–1400, 2013.

[46] M. A. A. Pedrasa, T. D. Spooner, and I. F. MacGill, "Coordinated Scheduling of Residential Distributed Energy Resources to Optimize Smart Home Energy Services," IEEE Transactions on Smart Grid, vol. 1, no. 2. pp. 134–143, 2010.

[47] M. Rastegar, M. Fotuhi-Firuzabad, and F. Aminifar, "Load commitment in a smart home," Applied Energy, vol. 96. pp. 45–54, 2012.

[48] Y. Ozturk, D. Senthilkumar, S. Kumar, and G. Lee, "An Intelligent Home Energy Management System to Improve Demand Response," IEEE Transactions on Smart Grid, vol. 4, no. 2. pp. 694–701, 2013.

[49] Y. Iwafune, T. Ikegami, J. G. da Silva Fonseca, T. Oozeki, and K. Ogimoto, "Cooperative home energy management using batteries for a photovoltaic system considering the diversity of households," Energy Conversion and Management, vol. 96. pp. 322–329, 2015.

[50] D. T. Nguyen and L. B. Le, "Joint Optimization of Electric Vehicle and Home Energy Scheduling Considering User Comfort Preference," IEEE Transactions on Smart Grid, vol. 5, no. 1. pp. 188–199, 2014.

[51] A. H. Mohsenian-Rad and A. Leon-Garcia, "Optimal residential load control with price prediction in real-time electricity pricing environments," IEEE Trans. Smart Grid, vol. 1, no. 2, pp. 120–133, 2010.

[52] W.-T. Li, K. Thirugnanam, W. Tushar, C. Yuen, K. T. Chew, and S. Tai, "Improving the Operation of Solar Water Heating Systems in Green Buildings via Optimized Control Strategies," IEEE Transactions on Industrial Informatics, vol. 14, no. 4. pp. 1646–1655, 2018.

[53] F. Luo, G. Ranzi, W. Kong, Z. Y. Dong, and F. Wang, "Coordinated residential energy resource scheduling with vehicle-to-home and high photovoltaic penetrations," IET Renewable Power Generation, vol. 12, no. 6. pp. 625–632, 2018.

[54] V. C. J. Sankar, M. Raghunath, and M. G. Nair, "Optimal scheduling and energy management of a residential hybrid microgrid," in 2017 Innovations in Power and Advanced Computing Technologies (i-PACT), 2017, pp. 1–6.

[55] S. Aslam, N. Javaid, M. Asif, U. Iqbal, Z. Iqbal, and M. A. Sarwar, "A mixed integer linear programming based optimal home energy management scheme considering grid-connected microgrids," in 2018

14th International Wireless Communications Mobile Computing Conference (IWCMC), 2018, pp. 993–998.

[56] Z. Iqbal, N. Javaid, M. R. Khan, F. A. Khan, Z. A. Khan, and U. Qasim, "A Smart Home Energy Management Strategy Based on Demand Side Management," in 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), 2016, pp. 858–862.

[57] G. Dong and Z. Chen, "{Data-Driven} Energy Management in a Home Microgrid Based on Bayesian Optimal Algorithm," IEEE Trans. Ind. Inf., vol. 15, no. 2, pp. 869–877, 2019.

[58] A. Mondal, S. Misra, and M. S. Obaidat, "Distributed home energy management system with storage in smart grid using game theory," IEEE Syst. J., vol. 11, no. 3, pp. 1857–1866, 2015.

[59] S. Zhou, Z. Hu, W. Gu, M. Jiang, and X. Zhang, "Artificial intelligence based smart energy community management: A reinforcement learning approach," CSEE J. Power Energy Syst., vol. 5, no. 1, pp. 1–10, 2019.

[60] C. Lebrón and F. Andrade, "An intelligent battery management system based on fuzzy controller for home microgrid working in grid-connected and island mode," in 2016 IEEE ANDESCON, 2016, pp. 1–4.

[61] Y. Guan, J. C. Vasquez, and J. M. Guerrero, "An enhanced hierarchical control strategy for the Internet of Things-based home scale microgrid," in 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), 2017, pp. 51–56.

[62] M. A. Al Faruque and K. Vatanparvar, "Energy Management-as-a-Service Over Fog Computing Platform," IEEE Internet Things J., vol. 3, no. 2, pp. 161–169, 2016.

[63] J. Vagdoda, D. Makwana, A. Adhikaree, T. Faika, and T. Kim, "A Cloud-Based Multiagent System Platform for Residential Microgrids

Towards Smart Grid Community," in 2018 IEEE Power Energy Society General Meeting (PESGM), 2018, pp. 1–5.

[64] S. Aslam, H. Herodotou, N. Ayub, and S. M. Mohsin, "Deep Learning Based Techniques to Enhance the Performance of Microgrids: A Review," 2019 International Conference on Frontiers of Information Technology (FIT). 2019.

[65] M. H. Hassoun, Fundamentals of Artificial Neural Networks. MIT Press, 1995.

[66] J. Schmidhuber, "Deep learning in neural networks: an overview," Neural Netw., vol. 61, pp. 85–117, 2015.

[67] M. Matsugu, K. Mori, Y. Mitari, and Y. Kaneda, "Subject independent facial expression recognition with robust face detection using a convolutional neural network," Neural Networks, vol. 16, no. 5–6. pp. 555–559, 2003.

[68] C. H. Dagli, S. T. Kumara, and Y. C. Shin, "Intelligent engineering systems through artificial neural networks." Proceedings of the Artificial Neural Networks in Engineering (ANNIE '91), St. Louis, Missouri, USA, 1991.

[69] D. Britz, "Recurrent Neural Networks Tutorial." [Online]. Available: http://www.wildml.com/2015/09/recurrentneural-networks-tutorialpart- 1-introduction-to-rnns/. [Accessed: 22-Mar-2020].

[70] A. Deoras, "Electricity Load and Price Forecasting Webinar Case Study." [Online]. Available: https://www.mathworks.com/matlabcentral/fileexchange/28684-electricity-load-and-price-forecasting-webinar-case-study. [Accessed: 23-Mar-2020].

[71] "MATLAB - El lenguaje del cálculo técnico." [Online]. Available: https://la.mathworks.com/products/matlab.html. [Accessed: 23-Mar-2020].

[72] "Simulink - Simulación y diseño basado en modelos." [Online]. Available: https://la.mathworks.com/products/simulink.html. [Accessed: 23-Mar-2020].

[73] "Real-Time simulation | Real-Time Solutions | OPAL-RT," OPAL-RT. [Online]. Available: https://www.opal-rt.com/. [Accessed: 23-Mar-2020].

[74] "AWS | Cloud Computing - Servicios de informática en la nube," Amazon Web Services, Inc. [Online]. Available: https://aws.amazon.com/es/. [Accessed: 23-Mar-2020].

[75] "AWS | Almacenamiento de datos seguro en la nube (S3)," Amazon Web Services, Inc. [Online]. Available: https://aws.amazon.com/es/s3/. [Accessed: 23-Mar-2020].

[76] "AWS | Elastic compute cloud (EC2) de capacidad modificable en la nube," Amazon Web Services, Inc. [Online]. Available: https://aws.amazon.com/es/s3/. [Accessed: 23-Mar-2020].

[77] "MATLAB Production Server." [Online]. Available: https://la.mathworks.com/products/matlab-production-server.html. [Accessed: 23-Mar-2020].

[78] S. Khan, D. Paul, P. Momtahan, and M. Aloqaily, "Artificial intelligence framework for smart city microgrids: State of the art, challenges, and opportunities," in 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), 2018, pp. 283–288.

[79] E. A. Mojica-Nava, B. V. Toro Tovar, E. E. Gaona-García, and C. L. Trujillo Rodríguez, Control de microrredes eléctricas inteligentes. 2017.

[80] C. Barreto, J. Giraldo, A. A. Cardenas, E. Mojica-Nava, and N. Quijano, "Control Systems for the Power Grid and Their Resiliency to Attacks," IEEE Secur. Priv., vol. 12, no. 6, pp. 15–23, Nov. 2014.

[81] C. Barreto, A. A. Cárdenas, N. Quijano, and E. Mojica-Nava, "CPS," in Proceedings of the 30th Annual Computer Security Applications Conference on - ACSAC '14, 2014, pp. 136–145.

[82] V. Toro, E. D. Baron, and E. Mojica-Nava, "Optimized Hierarchical Control for an AC Microgrid Under Attack," Ingeniería, vol. 24, no. 1, pp. 64–82, Jan. 2019.

[83] B. Oniga, E. De Poorter, and A. Munteanu, "A secure LoRaWAN sensor network architecture," IEEE SENSORS, pp. 1–3, 2017.

[84] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes, "Exploring The Security Vulnerabilities of LoRa," 2017 3rd IEEE Int. Conf. Cybern., pp. 1–6, 2017.

[85] E. van Es, "LoRaWAN vulnerability analysis:(in) validation of possible vulnerabilities in the LoRaWAN protocol specification.," 2018.

[86] L. Alliance, "LoRaWAN TM 101." LoRa-Alliance.org, 2018.

[87] T. C. M. Dönmez and E. Nigussie, "Security of LoRaWAN v1.1 in Backward Compatibility Scenarios," Procedia Comput. Sci., vol. 134, pp. 51–58, 2018.

[88] S. Zulian, "Security threat analysis and countermeasures for LoRaWAN join procedure," 2016.

[89] X. Yang, "LoRaWAN: Vulnerability Analysis and Practical Exploitation," 2017.

[90] Isot. Excellence, "Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad," SGSI: Blog especializado en Sistemas de Gestión de Seguridad de la Información, 2018. [Online]. Available: https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/.

[91] S. Cruz-Duarte, P. A. Gaona-Garcia, and E. E. Gaona-Garcia, "Cybersecurity In Microgrids," in 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), 2018, pp. 7–12.

[92] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," Comput. Networks, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.

[93] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," IEEE Commun. Surv. Tutorials, vol. 14, no. 4, pp. 998–1010, 2012.

[94] J. Daemen and V. Rijmen, Efficient Implementation of Advanced Encryption Standard. Springer-Verlag, 2001.

[95] M. Kumar and A. Singhal, "Efficient implementation of advanced encryption standard (AES) for ARM based platforms," in 2012 1st International Conference on Recent Advances in Information Technology, RAIT-2012, 2012, pp. 23–27.

[96] P. Mojica G., S. Cuéllar, and C. Medina, "Medición y Gestión Inteligente de Consumo Eléctrico," 2016.

[97] H. Suleiman, I. Alqassem, A. Diabat, E. Arnautovic, and D. Svetinovic, "Integrated smart grid systems security threat model," Inf. Syst., vol. 53, pp. 147–160, Oct. 2015.

[98] Nist, N. S. Publication, and N. I. of S. and Technology, "NIST Special Publication 1108 NIST Framework and Roadmap for Smart Grid Interoperability Standards," Nist Spec. Publ., vol. 0, pp. 1–90, 2014.

[99] J. R. Aguirre, Seguridad Informática y Criptografía. 2006.

[100] J. Katz, Introduction to Modern Cryptography. Chapman and Hall/CRC, 2007.

[101] R. J. Easter and J. E. Bryson, "Annex A : Approved Security Functions for FIPS PUB 140-2 , Security Requirements for Cryptographic Modules," 2012. .

[102] E. E. Gaona-García, C. L. Trujillo Rodriguez, and H. E. Rojas Cubides, "Infraestructura de comunicaciones en microrredes eléctricas," Redes Ing., vol. 5, no. 2, pp. 28–38, 2014.

[103] E. Aras, N. Small, G. S. Ramachandran, S. Delbruel, W. Joosen, and D. Hughes, "Selective Jamming of LoRaWAN using Commodity Hardware," in Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, 2017, pp. 363–372.

[104] J. M. de la Garza, "RF Jamming," 2006.

Impreso en papel bond 90 gr.
en familia tipográfica Candara a 11,5 pts.

Amadgraf Impresores Ltda.
Bogotá, D.C., Colombia
Octubre de 2020.

OTROS TÍTULOS DE ESTA COLECCIÓN

RADIACIÓN-MATERIA: GEANT4 Hands On!

REDES NEURONALES CONVOLUCIONALES USANDO KERAS Y ACELERANDO CON GPU

GESTIÓN DE LA ENERGÍA: EL USUARIO DE ENERGÍA COMO PARTE ACTIVA DEL SISTEMA

DETECCIÓN Y CORRECCIÓN DE PROPAGACIONES ANÓMALAS EN RADARES METEREOLÓGICOS

INTRODUCCION A LA INVESTIGACIÓN SOBRE DESASTRES NATURALES Y CIUDADES INTELIGENTES

INVESTIGACIÓN EN INGENIERÍA FUNDAMENTADA EN LA GESTIÓN DEL CONOCIMIENTO

LOS RECURSOS DISTRIBUIDOS DE BIOENERGÍAEN COLOMBIA

ARQUITECTURAS DE RED NEURO-CONVOLUCIONAL PARA APLICACIONES DE ROBÓTICA ASISTENCIAL

En el presente libro se plantea la necesidad de abordar la ciberseguridad de las microrredes eléctricas como temática principal. En este documento se abordan las características generales para un sistema de gestión de energía en microrredes residenciales y se explora la vulnerabilidad de sus sistemas de comunicaciones, para finalizar con una exploración de estrategias y arquitecturas que garanticen la ciberseguridad de las microrredes domiciliarias.

ISBN 978-958-787-228-6

9 789587 872286