UNA REVISIÓN A LA CIBER SEGURIDAD EN REDES ELÉCTRICAS INTELIGENTES

A REVIEW OF CYBER SECURITY ON SMART GRIDS

Juan Carlos Olivares Rojas
Tecnológico Nacional de México / IT de Morelia, México
juan.or@morelia.tecnm.mx

Enrique Reyes Archundia
Tecnológico Nacional de México / IT de Morelia, México
enrique.ra@morelia.tecnm.mx

José Antonio Gutiérrez Gnecchi
Tecnológico Nacional de México / IT de Morelia, México
jose.gg3@morelia.tecnm.mx

Ismael Molina Moreno
Tecnológico Nacional de México / IT de Morelia, México
Ismael.mm@morelia.tecnm.mx

Jaime Cerda Jacobo
Universidad Michoacana de San Nicolás de Hidalgo, México
jcerda@umich.mx

Recepción: 21/marzo/2020 **Aceptación:** 27/abril/2020

Resumen

La Transformación Digital a través de las Tecnologías de las Cuarta Revolución Industrial han incidido de buena forma en prácticamente todas las actividades humanas y la red eléctrica no es la excepción. La Red Eléctrica es la responsable de brindar energía eléctrica a todos los procesos humanos y vivir sin ella es prácticamente imposible. La inclusión de tecnologías de información y operación (IT y OT) a la red eléctrica le han dado cierta "inteligencia" para brindar nuevos servicios a los usuarios finales y a las empresas eléctricas, tales como: medición de consumo y facturación en tiempo casi real, cortes y reconexiones de forma automática, monitoreo de la calidad de la energía, programas de respuestas a la demanda, detección de falla, entre otras. A pesar de estas nuevas ventajas, el uso de IT y OT conlleva varias ventajas, entre las más importantes: los costos, el gran volumen de

datos generados y sobre todo la seguridad de la información en todos los procesos de la red eléctrica inteligente. Este trabajo presenta una revisión al estado del arte actual respecto al tema de ciberseguridad en las redes eléctricas inteligentes de la siguiente manera: en la sección de Introducción se muestra los conceptos básicos de ciber seguridad en redes eléctricas inteligentes. En el capítulo de métodos se muestras los trabajos relacionados que pretenden dar solución a la problemática planteada. En la sección de resultados se realiza una tabla comparativa entre los principales trabajos. Posteriormente se discuten los resultados y se llegan a conclusiones.

Palabras Clave: Cadena de Bloques, Ciber Seguridad, Red Eléctrica Inteligente.

Abstract

The Digital Transformation through the Technologies of the Fourth Industrial Revolution has had a good impact on practically all human activities, and the electricity grid is no exception. The Grid is responsible for providing electrical energy to all human processes, and living without it is practically impossible. The inclusion of information and operation technologies (IT and OT) to the electricity grid have given it some "intelligence" to provide new services to end-users and utilities, such as consumption measurement and billing in near real-time, cuts and reconnections automatically, monitoring of power quality, demand response programs, fault detection, among others. Despite these new advantages, the use of IT and OT has several advantages, among the most important: costs, the large volume of data generated, and above all, the security of information in all the processes of the Smart Grid. This work presents a review of the current state of the art regarding the topic of cybersecurity in Smart Grid as follows: the Introduction section shows the basic concepts of cybersecurity in smart power grids. In the chapter on methods, the related works that aim to solve the problem posed are shown. In the results section, a comparative table is made between the main works. Later the results are discussed, and conclusions are reached.

***Keywords*:** *Blockchain, Cyber Security, Smart Grid.*

1. Introducción

Con la incorporación de las tecnologías de la información y las telecomunicaciones (TIC) a las redes eléctricas, se han desarrollado esquemas de comunicación bidireccional que optimizan el transporte y consumo de energía eléctrica y otorgan un grado de inteligencia a la red [Montoya-Mendoza, 2016]. Por otro lado, la incorporación de la generación por recursos renovables en distintos puntos de la red eléctrica incrementa la complejidad en el manejo de la transmisión y distribución de la energía, razón por la cual se ha ido incorporando a las redes tradicionales el concepto de Redes Eléctricas Inteligentes (REI) que entre sus características permiten una comunicación bidireccional entre diferentes elementos de la red eléctrica, haciendo más eficiente la operación de esta.

En este sentido, la red inteligente se ha concebido como una evolución de los sistemas eléctricos de potencia, debido al incremento de la generación de energía utilizando recursos renovables, pero con la encomienda de mejorar la eficiencia, la confiabilidad y la seguridad de la red existente [Gungor, 2011].

Dentro del Programa de Redes Eléctricas Inteligentes (PREI) 2017-2031 de la SENER y en las cuales participan la Comisión Federal de Electricidad (CFE), el Centro Nacional de Control de Energía (CENACE) y la Comisión Reguladora de Energía (CRE), se estipula que el objetivo principal es el uso de información digital y tecnología de control para mejorar la estabilidad, seguridad y eficiencia de la Red Nacional de Transmisión y de las Redes Generales de Distribución [SENER, 2017].

Tradicionalmente la seguridad en redes eléctricas inteligentes se ha enfocado en la seguridad física de las personas debido a consideraciones como altos voltajes y corrientes que pueden ocasionar pérdida de vidas humanas. Sin embargo, este uso de las Tecnologías de Información y Comunicaciones (TICs) en las redes eléctricas también las hacen más vulnerables a incidentes de ciber seguridad tales como: alteración de la información (tampering) reportada de los medidores inteligentes a los sistemas de facturación para un menor consumo y por ende pérdidas económicas para las empresas eléctricas, cortes y reconexiones no autorizados, apagones en diversas zonas, entre otros.

Por ejemplo, se estima que el nivel de pérdidas no técnicas (robo de energía, capturas incorrectas, falsificación de las lecturas, medición incorrecta del medidor, entre otras) representa el 13.38% por lo que lograr tener un mecanismo más seguro de medición inteligente es una necesidad. El error de precisión de un medidor inteligente oscila alrededor del 2% si es análogo y 0.5% si es digital [SENER 2017]. Además, el PREI estipula otras premisas entre las que destaca la ciber seguridad de todos los sistemas. En este sentido, se considera a los medidores inteligentes como el primer punto de ataque, por lo que tener mecanismos de seguridad es una necesidad, dado que la REI es una infraestructura crítica de seguridad nacional.

Debido a que la REI es muy extensa, este trabajo se centra en una de sus principales aplicaciones: Los Sistemas de Medición Inteligente (SMI), los cuales permiten tener lecturas de las mediciones en tiempo real sin necesidad de capturistas y menos propensas a errores humanos, a su vez se pueden hacer cortes y reconexiones de forma automática; así como conocer en tiempo real el consumo energético utilizado y su costo entre otras virtudes.

La ciber seguridad se ha tratado desde hace ya algunos años, pero en el campo de las redes eléctricas y los sistemas de medición inteligentes es relativamente reciente, existiendo aún muchas oportunidades de mejora.

La ciber seguridad es un concepto que se define a partir de los Sistemas Ciberfísicos en donde dichos sistemas, no solo están compuestos por elementos de hardware y software, sino que también incluyen al mundo físico en general: incluyendo personas, seres vivos y cosas, entre otros [Habibzadeh, et al., 2017].

La seguridad de la información se presenta a través de un análisis de riesgo de los activos que posean. La ciber seguridad se compone de la evaluación de amenazas (factores externos) que crean ataques, los cuales a su vez explotan vulnerabilidades (debilidades, factores internos) que tienen un impacto sobre las organizaciones y/o personas. Para poder mitigarlos (dado que por definición la ciber seguridad se maneja como una probabilidad en intervalos cerrados de 0 a 100 y por ende no se pueden eliminar) se utilizan contramedidas o controles.

La Ciber Seguridad tiene tres componentes fundamentales: Confidencialidad, Integridad y Disponibilidad (CIA por sus siglas en inglés) [ISO 2020].

Algunos tipos de ataques comunes en los sistemas de medición inteligentes como:

- Husmear (Eavesdropping) y difamación: Ambos afectan la Confidencialidad.
- Modificación de mensajes (tampering): Afecta la Integridad.
- Interferencia Inalámbrica/ Sabotaje: Afectan a la Disponibilidad.

Por otra parte, existen otras vulnerabilidades en la REI [Islam, et al., 2019] como por ejemplo:

- Falta de expertos en temas de ciber seguridad en la REI, dado que la mayoría de los expertos son del campo de ingeniería eléctrica y la gente de TIC está más en los procesos de información que en los procesos operativos
- La ciber seguridad de diversos componentes eléctricos está en valores predeterminados; por ejemplo, nombre de usuarios y contraseñas sin modificar, contraseñas poco robustas, entre otras.
- Hasta hace poco se invertía poco dinero en ciber seguridad en el área de las redes eléctricas.

Algunas amenazas de la REI son [Gunduz, Das, 2020]:

- Al ser una infraestructura crítica para los gobiernos de todo el mundo (dado que su ausencia paraliza las actividades prioritarias de cualquier país), está altamente expuesta a ciber criminales que desean paralizar los sistemas eléctricos de potencia.
- Por otra parte, los usuarios finales tienden a falsificar las lecturas de su medición para pagar menos
- Algunos usuarios se roban la energía sin pagar al colgarse de la red sin sistemas de medición, lo cual se traduce en grandes pérdidas para las empresas eléctricas.

Algunos ejemplos del impacto que produce la falta de ausencia de ciber seguridad en REI son [Amleh, et al., 2020]:

- Los apagones producidos por usuarios mal intencionados provocan pérdidas cuantiosas en las empresas eléctricas

- La desconexión del servicio eléctrico por desastres naturales en algunas zonas produce pérdidas económicas millonarias.
- La falta de verificación de medidores de energía eléctrica ocasiona que haya mayor probabilidad de los usuarios finales a falsificar su consumo/producción de energía eléctrica.

Para salvaguardar la CIA en REI existen diversos mecanismos, unos de los enfoques más sonados en la actualidad son las cadenas de bloque (Blockchain). Cuando se habla de cadenas de bloques, más del 90% de las ocasiones se asocia con lo que es el bitcoin (una moneda electrónica cifrada –criptomoneda- de par a par y de fuente abierta). En realidad, es más que eso. Así, una cadena de bloques es un mecanismo seguro de almacenamiento de datos, que es compartido y distribuido por muchas computadoras [Perera, 2020].

A pesar de sus enormes ventajas, los blockchain presentan algunas desventajas [Di Silvestre, 2020]:

- Construida para bajos volúmenes de transacciones.
- No es recomendable para un solo participante.
- No es un remplazo para la replicación de base de datos.
- No es un remplazo para el procesamiento de las transacciones (se guarda solo el resultado).
- Es una tecnología naciente (frontera).
- Tiene un consumo energético bastante elevado debido al alto procesamiento.
- Los costos de implementación de la infraestructura son elevados.
- Hay poca compatibilidad entre distintos mecanismos.

Algunos autores consideran la tecnología de la cadena de bloques como otra revolución en el área de las TICs como en su momento fue el Internet.

El presente trabajo muestra un estudio de los principales trabajos sobre el tópico de ciber seguridad en REI en vías de cubrir los principales retos de amenazas y vulnerabilidades en la REI. El propósito es servir de referencia base para posteriores estudios de ciber seguridad en REI y en otros contextos como el Internet de las

cosas. Los autores de este artículo creen que esquemas combinados de diversos mecanismos de ciber seguridad pueden prever mayor protección, particularmente las técnicas de blockchain son mecanismos novedosos y seguros para la REI.

2. Métodos

Los primeros acercamientos en el estudio de mecanismos y esquemas de ciber seguridad en redes eléctricas y particularmente de medidores inteligentes se dieron a partir de 2007 y es a partir de 2011 que han tomado más relevancia, en donde los últimos tres años ha crecido significativamente.

A continuación, se muestra una revisión exhaustiva de manera generalizada de la literatura de los distintos trabajos existentes más sobresalientes que atacan la problemática de la ciber seguridad en los SMI. Para ello, se seleccionaron los trabajos de los últimos años que mostraban una técnica diferente y que era el más citado en dicha área. Con los trabajos listados en la siguiente sección se concentran los resultados para posteriormente ser discutidos.

Uno de los enfoques con lo que se ha tratado de resolver el problema de Ciber Seguridad es caracterizando los distintitos tipos de ataques que pueden ocurrir y brindando una solución específica. Por ejemplo, en [Skopik, 2012] se presenta un trabajo para la protección de la privacidad en la recolección de datos de medidores inteligentes utilizando cifrado de datos homomórficos.

Por otra parte, en [He, et al., 2017] se muestra un trabajo en donde a través de técnicas de aprendizaje profundo se puede tratar de predecir en tiempo real si un paquete en redes eléctricas inteligentes es falso. Los ataques de inyección de paquetes falsos son uno de los tipos de amenazas más estudiados hoy en día en los sistemas de medición inteligente.

Uno de los temas más estudiados con respecto a Ciber Seguridad en Medidores inteligentes tiene que ver con la protección de la privacidad de los datos de consumo. [Foreman, et al., 2017] describen una arquitectura de agregación para la reducción de datos y asegurar privacidad en la infraestructura de medición avanzada (AMI, por sus siglas en inglés). El esquema de agregadores (intermediarios) es un esquema de solución utilizando en problemas de la REI.

Algunos autores se han enfocado en garantizar la confidencialidad de la información en los medidores inteligentes, por ejemplo, en [Barka, 2016] se muestra una arquitectura para proveer seguridad en los datos de los sistemas de medición inteligentes usando control de acceso basado en roles.

Los estudios más recientes en ciber seguridad se centran en Sistemas de Detección y Prevención de Intrusos y en la REI no es la excepción. Por ejemplo, en [Faisal, 2015] se presenta un estudio de factibilidad para implementar un sistema de detección de intrusos capaz de interpretar flujos de datos de consumo energético en tiempo real.

Otro trabajo enfocado en la detección de intrusos se muestra en [Molazem, et al., 2015] en donde se implementa un Sistema de Detección de Intrusos para Sistemas Embebidos de Memoria Limitada. De manera generalizada los mecanismos de cadenas de bloque se han utilizado principalmente para el manejo de monedas digitales seguras (criptomonedas). En los últimos años, las aplicaciones para garantizar seguridad en diversas áreas del conocimiento como medicina, sistemas de votación electrónica, cadena de suministro, entre otras, han empezado a aparecer. Por ejemplo, en [Dorri, et al., 2017] se muestra una implementación de cadenas de bloque para dispositivos de Internet de las Cosas en el Hogar.

Hasta el momento, no se han encontrado en la literatura implementaciones de cadenas de bloques que vayan enfocadas en garantizar seguridad en las transacciones de consumo en sistemas de medición inteligente. Sin embargo, existen muchos trabajos relacionados como en [Tanaka, et al., 2017], [Mihaylov, 2014] y [Mihaylov, 2016] en donde se muestran propuestas de implementación de cadenas de bloques para el intercambio de energía en REI a través del uso de criptomonedas específicas.

3. Resultados

La Tabla 1 resume la comparativa de los trabajos más sobresalientes para garantizar la ciber seguridad en SMI. Se muestra cada trabajando comparando la técnica utilizada, así como si cubre los criterios CIA y describe características específicas de cada trabajo.

Tabla 1 Estado del arte de ciber seguridad en Sistemas de Medición Inteligente

Trabajo	Técnica	Confidencialidad	Integridad	Disponibilidad	Otro
[Skopik, 2012]	Cifrado homomórfico	Parcial	Sí	No	Privacidad
[He, et al., 2017]	Aprendizaje Profundo	Sí	Sí	No	Pruebas de inyección de paquetes falsos
[Foreman, et al., 2017]	Agregadores	No	No	No	Privacidad y reducción de datos
[Barka, 2016]	Acceso Basado en Roles (RBAC)	Sí	No	No	Servidores de la Empresa
[Faisal, 2015]	IDS	Sí	Sí	Sí	Minería de streaming de datos
[Molazem, et al., 2015]	IDS	Sí	Sí	Sí	Limitación memoria 16 GB
[Dorri, et al., 2017]	Blockchain	Sí	Sí	Sí	Privacidad Implementación HAN
[Tanaka, et al., 2017] [Mihaylov, 2014] [Mihaylov, 2016]	Blockchain	Sí	Sí	Sí	Privacidad Intercambio de Energía Uso de criptomonedas

4. Discusión

Como puede observarse, existen diversos mecanismos que permiten garantizar ciber seguridad en la REI y en los Sistemas de Medición Inteligente.

El principal mecanismo de ciber seguridad continúa siendo las técnicas criptográficas que permiten el cifrado y descifrado de los datos utilizando enfoques simétricos o asimétricos. En general, dichas técnicas criptográficas están basadas en principios matemáticos que permiten un rápido cifrado de los datos, en los cuales para descifrar la información sin conocer la clave privada se requiere un esfuerzo computacional bastante grande que pudiese tardar muchos años en romperse. Particularmente, en REI difiere un poco su utilización, por ejemplo, en medidores inteligentes, así como otros Dispositivos Eléctricos Inteligentes (IED) se requiere de criptografía ligera dado que las capacidades de procesamiento y almacenamiento en sistemas embebidos y de Internet de las Cosas (IoT) son bastantes limitadas. Por otra parte, para aplicaciones de monitoreo de calidad de la energía como en las Unidades de Medición Fasorial (PMU) se requiere de algoritmos sumamente rápidos que permitan trabajar en tiempo real garantizando seguridad. A su vez las aplicaciones de facturación y manejo de relaciones con los clientes requieren de algoritmos criptográficos sumamente robustos que permitan guardar la información sensible de los clientes de forma muy segura.

Actualmente, las aplicaciones criptográficas van del manejo de firmas digitales para garantizar la autenticación de las partes, además del uso de certificados digitales

que permitan probar la identificación de las partes. El manejo de algoritmos de hash permite ayudar a la integridad de los datos siendo sumamente aplicado en los sistemas de medición inteligente.

Dado que la ciber seguridad es un tema que es imposible de garantizar al 100% existen diversas técnicas para tratar de mitigar los riesgos de la falta de ciber seguridad. Por ejemplo, el enfoque de Sistemas de Detección de Intrusos / Sistemas de Prevención de Intrusos (IDS/IPS, por sus siglas en inglés), es un esquema ampliamente utilizado hoy en día. Por ejemplo, el uso de firewalls permite garantizar la prevención de intrusos a través del uso de reglas de entrada y salida de las comunicaciones de las diversas aplicaciones de red. Un mejor enfoque es el uso de sistemas de detección de intrusos, el detalle de estos sistemas radica en los patrones y bases de conocimientos que permitan detectar un comportamiento anómalo como una intrusión a los sistemas, aunque cada vez es más usado debido a las diversas técnicas de Inteligencia Artificial (IA).

El uso de técnicas de IA para lograr ciber seguridad es cada vez más utilizado hoy en día, particularmente las técnicas de aprendizaje profundo permiten encontrar esquemas de aprendizaje ante diversos ciberataques.

A su vez el manejo de permisos y roles sigue siendo un tema de interés para la buena protección de los sistemas en REI, que, si es mezclado con técnicas de intermediarios y de diversas formas de organización como los agregadores, permiten un mejor esquema de ciber seguridad.

Finalmente, el uso de tecnologías de blockchain para garantizar ciber seguridad es cada vez más popular debido a que es un esquema que combina diversas técnicas de seguridad ya existentes como la criptografía hash, las firmas digitales y la redundancia de los datos de una forma muy ingeniosa para lograr transparencia e inmutabilidad de los datos.

5. Conclusiones

La REI es cada vez más utilizada por sus grandes ventajas comparada con la red eléctrica tradicional pero también presenta algunos retos, entre los cuales, uno de los más relevantes es la ciber seguridad.

El presente trabajo revisa diversos mecanismos para lograr ciber seguridad en la REI entre los que destacan técnicas criptográficas, IDS/IPS, así como cadena de bloques.

Aunque no existe un mecanismo único para lograr la ciber seguridad en REI, los autores de este trabajo creen que los mecanismos de cadena de bloque serán un disruptor de soluciones de ciber seguridad para la REI y otros dominios de aplicación de IoT.

A su vez, los autores de este trabajo proponen que los esquemas de ciber seguridad en REI deberán ser combinados entre sí para una mejor protección de los datos.

Agradecimientos

Este trabajo es parcialmente financiado por el Tecnológico Nacional de México bajo los proyectos 8000.20-P y 9002.20-P

6. Bibliografía y Referencias

[1] Amleh, N., et al., Impact of Smart Restoration and Energy Storage Systems on the Reliability of Electric Microgrid. Arab J Sci Eng 45, 1911–1925, 2020. https://doi.org/10.1007/s13369-019-04288-6.

[2] Barka, E., et al; Securing Smart Meters Data for AMI Using RBAC, 2016 11th Asia Joint Conference on Information Security. https://ieeexplore.ieee.org /document/7782051.

[3] Di Silvestre, M. L., et al., Blockchain for power systems: Current trends and future applications, Renewable and Sustainable Energy Reviews, Vol. 119, 2020. https://doi.org/10.1016/j.rser.2019.109585.

[4] Dorri, A., et al., Blockchain for IoT Security and Privacy: The Case Study of a Smart Home, 2nd IEEE PERCOM Workshop on Security Privacy and Trust in the Internet of Things 2017: https://ieeexplore.ieee.org/document /7917634.

[5] Gunduz, M. Z., and Das, R., Cyber-security on smart grid: Threats and potential solutions, Computer Networks, Vol. 169, 2020, https://doi.org/10.1016/j.comnet.2019.107094.

[6] Faisal, M. A., et al., Data-Stream-Based Intrusion Detection System for Advanced Metering Infrastructure in Smart Grid: A Feasibility Study, IEEE Systems Journal, Vol. 9, No. 1: https://ieeexplore.ieee.org/document/6720175.

[7] Foreman, J. C., et al.; Aggregation Architecture for Data Reduction and Privacy in Advanced Metering Infrastructure, 2017 IEEE PES Innovative Smart Grid Technologies Conference – Latin America (ISGT Latin America). Quito, Ecuador: https://ieeexplore.ieee.org/document/8126704.

[8] Gungor, V. C., et al., Smart grid technologies: Communication technologies and standards, IEEE Transactions on Industrial Informatics, vol. 7, no. 4, pp. 529–539, 2011: https://ieeexplore.ieee.org/document/6011696.

[9] Habibzadeh, H., et al., A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities, Sustainable Cities and Society, Vol. 50, 2019: https://doi.org/10.1016/j.scs.2019.101660.

[10] He, Y., et al., Real-Time Detection of False Data Injection Attacks in Smart Grid: A Dep Learning-Based Intelligent Mechanism, IEEE Transactions on Smart Grid, Vol. 8, No. 5. 2017: https://ieeexplore.ieee.org/document/7926429.

[11] Islam, S. N., et. al., Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures, in IEEE Transactions on Industrial Informatics, vol. 15, no. 12, pp. 6522-6530, 2019.

[12] ISO, Estándar ISO 27000, ISO, 2020: http://www.iso27000.es/.

[13] Molazem, F., et al., Flexible Intrusion Detection System for Memory-Constrained Embedded Systems, 2015 11th European Dependable Computing Conference: https://ieeexplore.ieee.org/document/7371950.

[14] Montoya-Mendoza, Y. A., et al., Estado del Arte de Smart Grid: Parte I, Revista Ingeniería al Día, Vol. 2, No. 1, pág. 87-107, 2016: http://revista.unisinu.edu.co/revista/index.php/ingenieriaaldia/article/view/54

[15] Mihaylov, M., et al., Boosting the Renewable Energy Economy with NRGcoin, 4th International Conference on ICT for Sustainability (ICT4S 2016). Atlantis Press. Pp. 229-230. https://dx.doi.org/10.2991/ict4s-16.2016.27.

[16] Mihaylov, M., et al., NRG-X-Change: a Novel Mechanism for Trading of Renewable Energy in Smart Grids, Department Sensing & Control.

[17] Perera, S., et al., Blockchain technology: Is it hype or real in the construction industry?,Journal of Industrial Information Integration, Vol. 17, 2020: https://doi.org/10.1016/j.jii.2020.100125.

[18] SENER, Programa de Redes Eléctricas Inteligentes. Secretaría de Energía, 2017: https://www.gob.mx/cms/uploads/attachment/file/250609/2017_Programa_ de_Redes_El_ctricas_Inteligentes.pdf

[19] Skopik, F., et al, Attack Vectors to Metering Data in Smart Grids under Security Constraints, 2012 IEEE 36th International Conference on Computer Software and Applications Workshops, 2012: https://ieeexplore.ieee.org/document/6341564.

[20] Tanaka, K., et al., Blockchain-based electricity trading with Digitalgrid router, 2017 IEEE International Conference on Consumer Electronics – Taiwan (ICCE-TW): https://ieeexplore.ieee.org/document/7991065.