SImulación de comunicación segura entre un servidor y estaciones de carga de vehiculos electricos en una SMART GRID

Jesus Ortiz Sandoval
Universidad Técnica Federico Santa María
Valparaíso, Chile

Resumen

Uno de los principales problemas que existen en la implementacion de sistemas de carga electrica es la movilidad en la comunicaciòn entre el cliente y la empresa prestadora del servicio. En la litertura actual se encuentran diversos estudios referentes a las diferentes arquitecturas, tecnologias y equipos que se pueden instalar en un sistema de carga de vehiculos electricos, pero solo algunos alcanzan a introducirse en el area de la seguridad en la comunicación, pero se encuentra una deficiencia en el analisis de algoritmos de encriptacion. En el siguiente proyecto se plantea un análisis del impacto de la configuración de una comunicación segura para el desarrollo de las transacciones en un sistema de vehículos eléctricos, evaluando el tipo de algoritmo de encriptación y el tamaño de la llave, se despliega una simulacion completa de un servicio de comunicaciòn con una red de equipos en el software GNS3 encontrando el tamaño de llave necesario para generar una comunicación en tiempo real soft.

1. INTRODUCCIÓN

Con la introduccion de las nuevas tecnologias en el area de la ingenieria electrica y las ciudades inteligentes se definen el concepto de Smart grid donde el suministro electrico deja de ser constante, y aparecen diferentes elementos como medidores inteligentes, vehiculos electricos, sistemas de generaciòn propios lo que convierten al sistema electrico en un proceso dinamico.

Una de las principales implementaciones de esta tecnología está relacionada con la estabilización de la carga en la red que puede verse afectada por la inclusión de vehículos eléctricos con los picos de energía que ocurren en el momento de la carga.

La implementacion en la vida real del concepto tiene muchos desafios inherentes a infraestructura, generacion y comunicaciòn de los elementos del sistema.

Para encontrar la mejor solucion se estudian las diferentes arquitecturas que se pueden implementar en los sistemas de distribución de energía (DAS), evaluando las topologías, los costos y, sobre todo, permitiendo una transición rápida y efectiva.

Cuando se implementa este tipo de proyectos en la vida real se tiene que tener varios aspectos fundamentales en cuenta. Uno de ellos es la seguridad en la comunicaciòn realizada entre el host y el servidor, ya que la infromaciòn que se comparte entre los equipos no puede ser en ningun momento alterada. Es importante determinar un dimensionamiento de un sistema de encriptaciòn de la comunicación que permita mantener los tiempos de comunicación en vida real sin comprometer la capacidad de transmision, evaluando la carga y los tiempos que representan de conexiòn, procesamiento y espera desde el lado del servidor.

El siguiente informe se divide en busqued del estado del arte, luego un enfoque del problema a discutir, el modelado del sistema de encriptación y autenticación, la simulación de los servicios, para terminar con las conclusiones del proyecto.

2. ESTADO DEL ARTE

X. He et al, analizan cómo se automatiza la generación de datos de entrada en programas para simular sistemas de distribución eléctrica. Este tipo de programas nos permite analizar voltaje, armónicos, comportamientos anormales, y eso puede ser de gran ayuda para aumentar y evaluar diferentes arquitecturas de distribución en nodos inteligentes.[1]

Es importante enfocar la tecnologia a implementar con la realidad actual, y la metodologia adecuada para hacer simulaciones que incluyan las particularidades del entorno.
F. Li et al, concluye el alto rendimiento de la arquitectura de comunicaciones en un sistema de distribución de electricidad orientado a países en desarrollo, esto es muy interesante y Chile actualmente por el grupo de 20 paises desarrollados (G20) es consideró un país en vías de desarrollo. Este trabajo evalua elementos, como la calidad de servicio (QoS) y el impacto de micro grilla en el tipo de arquitectura de comunicaciones que se debe elegir. [2]

Un factor clave par el desarrollo de ciudades inteligentes y limpias es la introduccion de la electricidad como combustible para el sistema de transporte, pero su implementacion representa un desafio al tener niveles dinamicos de carga en la distribucion electrica de la ciudad. Z. Zhang et al, proponen algunos métodos de optimización par la carga de celdas de bateria de vehiculos electricos, y la comunicación en el sistema para realizar la inclusión de vehículos eléctricos en la red (V2G) [3]

Y. Kwon et al, analizan la configuración de los sistemas eléctricos, las novedades que se pueden implementar para enfocarse en los sistemas de comunicación y poder hacer una evaluación de los resultados referentes a paquetes enviados en transmisiones seguras, estos sistemas deben elegirse tomando como referencia la eficiencia y estabilidad del sistema [4]
Estos trabajos abordan en conjunto los sistemas electricos y de comunicaciones en carga de vehiculos electricos, en este proyecto se desea implementar comunicaciones segura, y ver el impacto de este servicio en el servidor y su escalabilidad en la implementación.

3. PROBLEMA Y MARCO TEORICO

Esta área del conocimiento actualmente desarrolla muchos trabajos de investigación, referentes a tecnologías, arquitecturas, protocolos, distribución, etc. Pero también es relevante los estudios que se están haciendo para llevar a cabo una correcta distribución de esta tecnología referente a lo que son los sistemas de seguridad en la red. Es importante determinar que lo que se desea es un sistema que no afecte la estabilidad del sistema, que permita tener una eficiencia en la comunicación y que asegure la integridad de la información en las transacciones, se desea implementar un sistema de autenticación y encriptamiento AES (Advanced Encription Standard) con diferente tamaño de clave, además de diseñar el envió de un hash en cada transacción al usuario y a la empresa fuente del servicio , y medir cuanto es el incremento de latencia, y si se mantiene en niveles adecuados de eficiencia de prestación del servicio. Aunque la seguridad es elemento de estudio desde hace tiempo, en este proyecto se desea es medir el impacto de la implementacion de un servidor que provea el servicio de comunicación segura.

3.1 EPON diseño y simulación

Tabla 1. Perdidas asociadas con cada elemento de la red [5]

Componente	**Atenuación**	Perdida insertada
Fiber	0.4 dB/Km	N/A
Connector	0.2 dB	N/A
Splitter 1x2	N/A	(5%-95%) (0.4dB -11dB)
Splitter 1x4	N/A	(25%-25%-25%-25%)(6dB-6dB-6dB-6dB-)

Utilizando un sistema basado en el protocolo Ethernet industrial junto con una red PON (red óptica pasiva), se tiene un OTL (Optical trannsmisor layer) que es un transmisor óptico, cableado de fibra óptica, divisores de fibra óptica y unidades de recepción óptica de la ONU como se muestra en la figura 1. Para diseñar la red, primero se realiza el modelado de la red tomando como referencia la tabla 1 con los valores asociados con la atenuación de los componentes y la pérdida de señal insertada en los divisores.

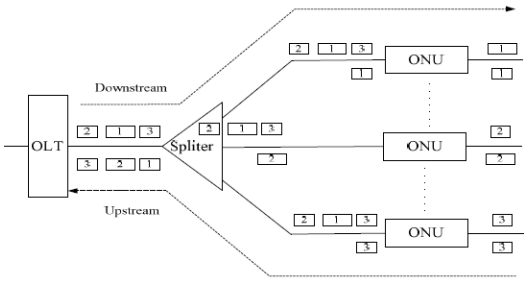

Figure 1. Arquitectura EPON [1]

Para poder realizar el modelado correcto, primero analizamos los tipos de arquitectura que se pueden implementar, lo que se desea en este caso es resolver uno de los principales problemas que ocurren en la transición de la red de distribucion normal a una red inteligente, son costos de implementación e infraestructura, para tal caso debemos aprovechar la misma arquitectura de distribución eléctrica, tomando para tal caso la infraestructura tipo bus como podemos analizar en la figura 2.

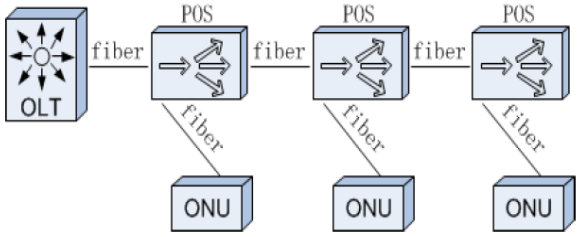

Figura 2. Arquitectura tipo BUS EPON [1]

Para este proyecto se toma como referencia un hipotético sistema de carga de vehículos eléctricos implementado en la Universidad Técnica Federico Santa María, con referencia únicamente al alimentador 1 de la línea que tiene 11 unidades de carga, la idea principal de este diseño es que si el funcionamiento correcto del modelo y la simulación puede proceder a una implementación adecuada. En la figura 3 se puede ver el diagrama general de la arquitectura EPON propuesta, y la sección que se va a estudiar.

Tomando como referencia el trabajo realizado por (Ahmed y Kim, 2019), evaluaremos su comportamiento, pero con una métrica diferente a la evaluada en el documento en cuestión. Dado que nos enfocamos en crear un servicio de comunicación encriptado como un proceso crítico y se desea analizar el impacto de este servicio en la latencia de los dispositivos que pertenecen a la red inteligente y qué sucede con la latencia en el momento en que se establece la comunicación entre el vehiculo y el servidor, cuando se establece la comunicación para enviar ID de usuario, carga, estado de bateria y recibir un hash por la operación.

Una vez implementada la arquitectura se hacen mediciones de latencias, con distancias fija de 10 metros entre estacion, lo que encontramos es que la latencia al estar conectados en una arquitectura estrella es la misma.

Tabla 2. Resultados con arquitectura funcionando entre estacion y equipos de la red

	1-3 estaciones	4-10 estaciones	>10 estaciones
Charger 3-1-20	42 ms	42 ms	42 ms
Charger 3-1-18	40 ms	40 ms	40 ms
Charger 3-1-17	47 ms	47 ms	47 ms
Charger 3-1-16	36 ms	36 ms	36 ms
Charger 6-1-5	38 ms	38 ms	38 ms
Charger 5-1	22 ms	22 ms	22 ms
Charger 6-1-15	36ms	36ms	36ms
Charger 4-1-7	34 ms	34 ms	34 ms

3.2 Autenticación y cifrado

Es importante determinar que en un sistema adecuado de autenticación y cifrado de información entre un host y un usuario se tiene que cumplir con integridad de la información que se va a compartir, disponibilidad de los datos, y no repudio de la transacción.

Con estos preceptos claros, nosotros vamos a estudiar dos métodos de autenticación que serán implementados en paralelo con diferentes tamaños de clave, para analizar que ambos cumplan con los requisitos expuestos, además de ver cuál es el impacto en los resultados alcanzados en la simulación sin sistema de seguridad que se observan en la tabla 2.

4. METODOLOGIA PROPUESTA

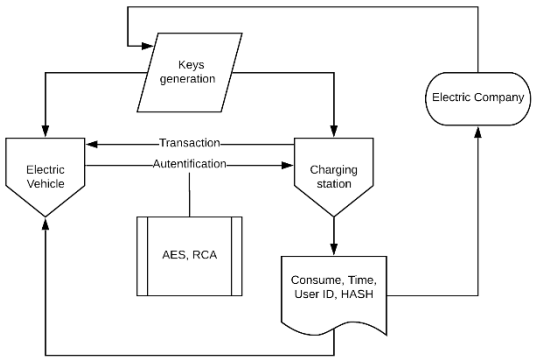

Figura 3. Metodologìa de desarrollo propuesta.

En la figura 4 encontramos nuestra propuesta de desarrollo de proyecto, utilizando la misma simulación para la arquitectura EPON lo que vamos a realizar es la implementación de este sistema de autenticación y cifrado, entre el servidor que se encarga de la administración de las estaciones de carga, y los vehículos que llegan a hacer su respectiva transacción, en primer lugar, vamos a correr dos experimentos diferentes con los sistemas de encriptación AES y RSA, la generación de la llave estará a cargo del servidor central, por cada transacción vamos a crear un ticket que debe contener la información de consumo, tiempo, ID del usuario y un HASH que le será entregada al usuario y será almacenado en el servidor para verificar la integridad de las transacciones. En el momento que se esté desplegando el sistema y que se estén llevando a cabo transacciones, se ejecutaran las mismas pruebas de latencia, para ver si este sistema tiene algún impacto en la calidad de la comunicación, así como aleatoriamente se elegirán HASH para verificar la integridad de algunas transacciones realizadas.

5. RESULTADOS

Tabla 3. Resultados de tiempos de latencia entre estaciones de la red EPON y el servidor que aloja el servicio de cmounicación segura.

LATENCIA	
ESTACION	**SERVIDOR**
EV1	1.0106 ms
EV2	1.0088 ms
EV13	3.8738 ms
EV15	3.2172 ms
EV20	4.2 ms
EV22	3.3624 ms
EV24	3.8118 ms
EV25	7.2036 ms
EV26	5.116 ms
EV27	4.8322 ms
EV32	5.2814 ms
EV33	5.1567 ms
EV35	5.757 ms

El escenario de simulacion es encuentra en la figura 4, donde se realiza la estructuracion de una red EPON de sistemas de vehiculos electricos dividida en tres secciones. En la tabla 3 se muestran los resultados de latencia desde varios equipos elegidos al azar hacia el servidor donde se aloja el servicio de encriptamiento corriendo con todos los servicios configurados para establecer la comunicación segura, que tiene los siguientes elementos:

- Apache 2 servidor Web
- Servidor DNS usando BIND9
- Servidor FTP usando BIND9
- Generación de claves mediante OpenSSL

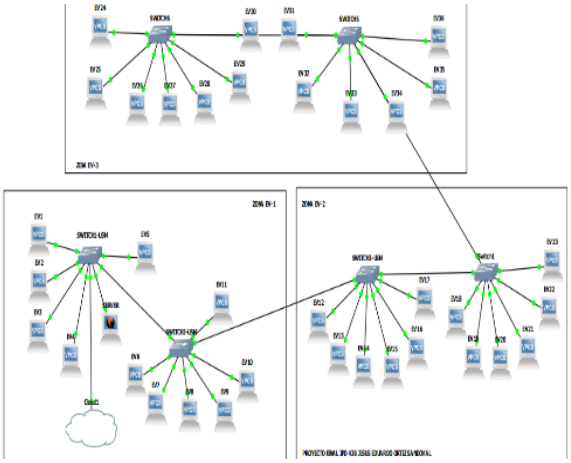

Figura 4. Diseño de propuesta de EV en USM

En la figura 5 encontramos la implementación que se hizo de las 3 zonas de carga de vehículos eléctricos en una topología mixta, utilizando bus en la conexión en los switches y una conexión en estrella alrededor de el para los cargadores, con la conexión de un servidor principal en la Zona 1 de la configuración, utilizamos VPC. (Virtual PC), usando el servidor de registro y asignacion de IP (Protocolo de internet) dinamico (DHCP) que provee la configuración cloud con router externo, además que se remplazaban en algunas estaciones por Lubuntu para hacer las pruebas de conexión con los servicios instalados.

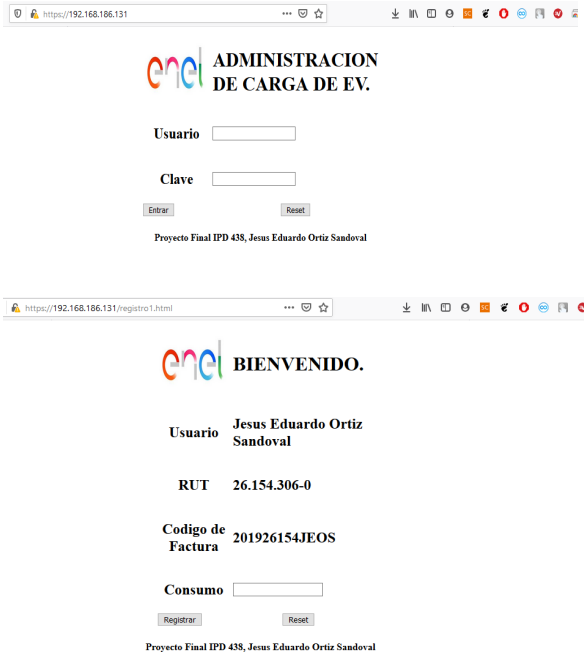

Figura 5. Página web para realizar las transacciones

Luego el primer servicio que configuramos es el servidor Apache2 para almacenar la página web que construimos básicamente en HTML junto con SQL para almacenar la información. En este servidor es donde se instalan las llaves de autenticación utilizando AES con diferentes tamaño de llave que es la evaluación que se realiza de capacidad del servidor.

Para el servicio de el certificado se instala también un servicio OpenSSL para poder generar las llaves que generan la comunicación segura entre el usuario y el servidor, cabe la pena resaltar que este proceso debe ser automático,. Se realiza la simulacion para poder ver la pagina que se esta accediendo y poder estar seguros de que al momento de automatizar todo el procesos efectivamente funciona como debe ser.

Para garantizar que el certificado cumple con las especificaciones del algoritmo en el momento

que se realiza la comunicación podemos dar clic en el candado que indica la comunicación segura y ver la información del certificado y de las llaves que fueron generadas para encriptar la comunicación, en la figura 7 podemos observar la información con la que se generaron las llaves.

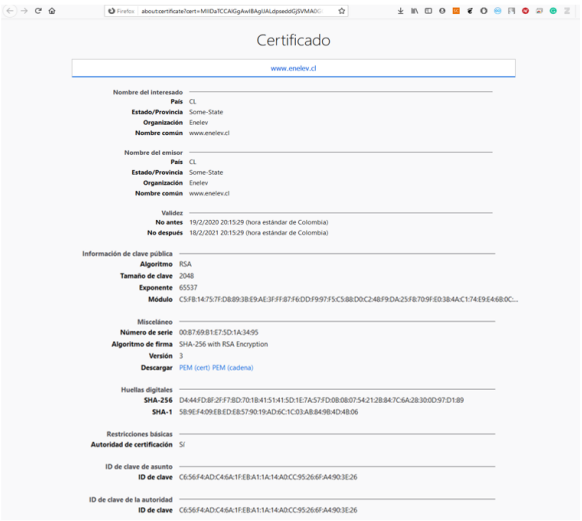

Figura 6. Certificado usando OpenSSL con tamaño de clave de 2048 bytes.

Con todo el sistema desplegado diseñamos la forma de evaluar el servidor y acercarnos a encontrar los resultados de este proyecto, obviamente no es relevante medir el ping desde los PC hasta el servidor, por que ellos solo miden el tiempo de respuesta lo que era necesario era poder medir los tiempos que se generaban al ingresar al sistema, tiempos de conexión y de espera, para este fin encontramos que el servidor Apache2 trae una herramienta llamada Apache Bench, con esta herramienta el procedimiento a realizar es cargar los certificados OpenSSl con diferente tamaño de llave, se reinicia el servidor Apache2 y realizar la medición del servidor, en las figura 8 y 9 encontramos el resultado de la medición del servidor, las llaves que se generan son de tamaño 2048 y 4096 utilizando algoritmo AES.

Tabla 4. Evaluación del servidor usando Apache Bench

Tamaño Llave	Conexión	Procesamiento	Espera
AES 2048	5 ms	24 ms	7 ms
AES 4096	221 ms	12 ms	47 ms

6. CONCLUSIONES

Aunque el trabajo se planteó originalmente como un estudio de seguridad en sistemas de grilla inteligente, debido al poco tiempo a la complejidad de realizar simulaciones a profundidad de sistemas completos solo pudimos estudiar el impacto de un espacio de comunicación segura bajo una pagina web donde se intercambia la información y se genera el reporte de la transacción que es almacenado en el servidor.

Este trabajo de estudio de sistemas seguros utilizando certificado OPENSSL, nos permite establecer cuanto es el costo en tiempo de escoger diferente tamaño de llaves para el intercambio de información, teniendo en cuenta las capacidades del servidor elegido para poder mantener tiempos real time soft.

Debido a las limitaciones de configuraciones que entrega CISCO en su software de análisis de redes PACKET TRACER no se pudo desarrollar el proyecto como se planteo en un comienzo debido a que el servidor no permitía la configuración adecuada de los sistemas que iban a ser necesario para la evaluación del impacto de la seguridad en los sistemas eléctricos inteligentes, esto se debe a que Packet Tracer no maneja sistemas operativos reales Ubuntu, Windows, etc, si no maneja un OS básico sin ninguna posibilidad de hacer configuraciones de instalación de llaves, paquetes, servicios o tampoco permitir la comunicación con el exterior mediante una maquina virtual, con todo lo que se encontró se tuvo que determinar que el software GNS3 es necesario para realizar el proyecto, pues tiene la escalabilidad necesaria para la implementación del proyecto, no se puede desconocer que Packet Tracer es bueno para analizar la arquitectura o topología de la red, pero este tipo de simulación no se puede evaluar en este programa.

Es interesante la forma en la que se puede configurar todo tipo de servicios en una máquina virtual pequeña Lubuntu. Se pudo desplegar un servidor Apache2, DNS, FTP además de que se instalo el servicio OpenSSL, para generar las llaves de encriptación usando AES con diferentes tamaños de claves que fueron herramienta para la evaluación del servidor en sus tiempos de ejecución.

6.1 Trabajos futuros

Se pueden diseñar otras pruebas con otro tipos de encriptacion como 3DES que podría ser evaluados no solo con latencia del sistema, tambien se puede evaluar la disponibilidad para determinar si en algun momento, cuando haya ataques el servidor ve afectado su rendimiento por esta situación.

Aunque en el servidor se desplego el algoritmo en JavaScript para generar un hash con string usando MD5 y que permita generar la seguridad en cada transacción solo hizo falta la implementación con Php para mostrar en el servidor y conectarlo con SQL, se recomienda hacer mediciones del servicio en conjunto con esta funcionalidad para ver el impacto de la generación de Hash.

7. BIBLIOGRAFIA

[1] X. He, M. O. Pun, and C. C. J. Kuo, “Secure and efficient cryptosystem for smart grid using homomorphic encryption,” 2012 IEEE PES Innov. Smart Grid Technol. ISGT 2012, 2012, doi: 10.1109/ISGT.2012.6175676.

[2] F. Li, B. Luo, and P. Liu, “Secure Information Aggregation for Smart Grids Using Homomorphic Encryption,” pp. 327–332, 2010, doi: 10.1109/smartgrid.2010.5622064.

[3] Z. Zhang, K. T. Chau, C. Qiu, and C. Liu, “Energy encryption for wireless power transfer,” IEEE Trans. Power Electron., vol. 30, no. 9, pp. 5237–5246, 2015, doi: 10.1109/TPEL.2014.2363686.

[4] J. H. Im, H. Y. Kwon, S. Y. Jeon, and M. K. Lee, “Privacy-preserving electricity billing system using functional encryption†,” Energies, vol. 12, no. 7, pp. 1–15, 2019, doi: 10.3390/en12071237.

[5] M. A. Ahmed and Young-Chon Kim, “System Architecture based on IoT for Smart Campus Parking Lots” International conference on Computer Applications & Information Security, ICCAIS'2019. 01-03 May, 2019.