**Sistema seguro de mensajería de emergencia MQTT para redes C-V2X basado en IoT**

PALOS ANGULO, Francisco Antonio†\*, RUIZ IBARRA, Erica Cecilia.

*Instituto tecnológico de sonora.*

[*International Identification of Science - Technology and Innovation*](http://www.ecorfan.org/servicios/ID-Researcher.pdf)

**Resumen**

En la actualidad en México las zonas urbanas siguen careciendo de infraestructura para comunicar a la población a través de tecnologías de telecomunicación, este uno de los principales problemas que enfrentan los servicios de emergencia por parte de las autoridades. El sistema propuesto ha sido pensado para lograr la mayor cobertura en tramos carreteros y así poder satisfacer las demandas de emergencia por parte de los ciudadanos para así conseguir una respuesta eficiente sin perder la seguridad de los mensajes de esta índole bajo condiciones de baja intensidad de señal y poder evitar potenciales ataques procedente del mensaje en sí. El presente trabajo de investigación desarrolla un sistema basado en IoT el cual brinda un medio seguro de comunicación en tiempo real de mensajes cifrados bajo el algoritmo AES 128, obtenido por medio de implementación de hardware, a través del protocolo MQTT bajo un sistema C-V2X, dicha implementación es orientada en escenarios experimentales donde la intensidad de señal puede generar perdidas de comunicación.

**Introducción**

Durante las últimas dos décadas, la industria automotriz ha sido el semillero de la innovación tecnológica como resultado de los avances significativos en las tecnologías de computación, comunicación y almacenamiento. La red Ad-Hoc de vehículos (VANET) es una de las aplicaciones más atraídas de internet de las cosas que está creciendo rápidamente desde que su oferta de seguridad mejoró. VANET es un tipo de red emergente que facilita la comunicación entre vehículos en carretera. Esta aplicación es uno de los elementos importantes en los sistemas de transporte inteligente (ITSs) (Eze et al., 2016).

El automóvil totalmente conectado estará compuesto por un ecosistema de tecnologías conectadas que le permitirán transferir y procesar grandes cantidades de datos mientras viaja a alta velocidad. En los próximos años, la mayoría de los vehículos estarán equipados con un dispositivo inalámbrico a bordo (OBU: On-Board Units por sus siglas en inglés), Sistema de Posicionamiento Global (GPS: Global Positioning System por sus siglas en inglés), Registrador de datos de eventos (EDR: Event Data Recorder por sus siglas en inglés) y sensores (radar). Estos equipos se utilizan para detectar la congestión y el estado del tráfico. Entonces ellos automáticamente tomarán las acciones apropiadas en el vehículo y transmitirán esta información a través de Vehículo a Vehículo (V2V) o Vehículo a Infraestructura (V2I) dentro de la red vehicular (Hasrouny, n.d.).

VANET tiene como objetivo garantizar una conducción segura mejorando el flujo del tráfico y, por lo tanto, reducir significativamente accidentes automovilísticos. Este último se resuelve proporcionando la información adecuada al conductor o al vehículo. Además, cualquier alteración de esta información en tiempo real puede provocar una falla del sistema que afecte a la seguridad de las personas en la carretera. Para garantizar el buen funcionamiento del sistema, es imperativo asegurar esta información, lo que la convierte en una de las principales prioridades para la investigación.

**Redes inalámbricas**

La red inalámbrica que mayor cobertura tiene para establecer comunicación bidireccional, es la red de tecnología celular, sin embargo, al menos en México las cifras del reporte muestran que a escala nacional, Telcel brinda 82.2% de cobertura garantizada en 2G, 86% en 3G y 77.7% en 4G, le sigue AT&T México, con 68.8% en 3G y 71.8% en 4G, mientras que Telefónica Movistar cuenta con 53.3% en 3G y 45.8% en 4G. 82 % del territorio mexicano tiene el servicio de 2G por medio del proveedor Telcel. (*CIAPEM 2021 – Comité de Informática de La Administración Pública Estatal y Municipal A.C.*, n.d.)

Al observar los mapas oficiales de las compañías proveedoras de servicio de telecomunicaciones celulares se puede notar que se manifiesta mayor concentración en zona urbana con múltiples nodos, mientras que las zonas de no cobertura están comprendidas a través de zonas aisladas y tramos carreteros, siendo en estos tramos un potencial problema si se manifiestan accidentes o eventos de emergencia.

Según el Sistema Nacional de Seguridad Pública (INSP) (*Instituto Nacional de Salud Pública*, n.d.), anualmente se registran hasta 24 mil decesos por accidentes automovilísticos, siendo éstos la quinta causa de muerte en la población en general y la primera entre jóvenes (*Luto Carretero: Los Accidentes Viales Más Trágicos Del 2021 - Infobae*, n.d.). No solo accidentes automovilísticos se pueden presentar en zonas aisladas, sino también incendios forestales, alteración de la carretera ya sea pista congelada o resbaladiza, colapso de un puente, derrumbe de un cerro etc. Pueden ocasionarse un sin fin de eventos de índole de emergencia o alerta, de los cuales es conveniente conocer oportunamente su ocurrencia y ubicación.

VANET todavía tiene desafíos por delante, mucho se ha trabajado para resolverlos y aún más en temas de seguridad. Los mensajes de seguridad se transmiten a través de una conexión abierta de medio inalámbrico por lo cual es más fácil de interferir y de intervenir que una red alámbrica, es vulnerable a diversos tipos de ataques de seguridad como suplantación, modificación, divulgación de identidad, ataques Sybil y así sucesivamente.

En VANET, a pesar de que es necesario propagar los mensajes emergencia por la ocurrencia de eventos en zonas aisladas, también resulta peligroso exponer esta información a entes maliciosas, o personas que puedan hacer abuso de esta información imprescindible para los conductores y usuarios, así como también para entidades oficiales como lo son: departamento de policía, bomberos, servicios médicos de emergencia, protección civil etc. Los vehículos se mueven rápidamente (EE. UU: 70mph o 112 kph). Como resultado, un sistema VANET necesita manejar un entorno donde los nodos dentro de la red se muevan a altas velocidades potencialmente ingresando y saliendo de la red muy rápidamente (Shrestha et al., 2018).

En este escenario ¿Cómo brindar confidencialidad a los mensajes?, ¿Qué método de seguridad es el adecuado para los requerimientos de VANET durante el intercambio de información entre vehículos? ¿Qué nivel de cifrado es el idóneo al transmitir información entre el vehículo a cualquier entidad de interés bajo un protocolo de mensajería sin tener un retraso que afecte en zonas inestables de señal celular?

Analizar el desempeño de los algoritmos de cifrado de mensajes X, Y y Z en ambientes con baja calidad de señal, mediante la implementación de estos en módulos ESP32, con la finalidad de determinar cuál de ellos brinda mayor integridad al mensaje para escenarios VANET.

**Objetivo**

Desarrollar una comparación de algoritmos de cifrado en aplicaciones VANET mediante una arquitectura compuesta por protocolos ya existentes, con la finalidad de establecer una comunicación segura a través de internet aun cuando los vehículos se encuentren en zonas de baja intensidad de señal y garantizar la integridad de los mensajes transmitidos.

Generar un esquema de seguridad bajo una arquitectura compuesta con tecnologías y sistemas existentes, con la cual vehículos puedan establecer una comunicación segura a través de internet aún en zonas de poca cobertura dando integridad a los mensajes transmitidos a través de un protocolo de mensajería con funcionalidades adecuadas a VANET.

* Desarrollar un sistema seguro que brinde confidencialidad a los mensajes a transmitir a partir de implementación en hardware a través de un ESP32.
* Bajo el sistema C-V2X establecer la comunicación entre vehículo e internet a través del protocolo de mensajería MQTT.
* Garantizar la transmisión y recepción de los mensajes seguros entre V2V, V2I y otras unidades.
* Lograr un tiempo de respuesta eficiente, sin alejarse de los requisitos que demandan los eventos de emergencia.

**Contribución**

La contribución de este trabajo es brindar un método seguro de transmisión de mensajes en automóviles de índole de emergencia.

La contribución de este trabajo se obtiene través de un análisis de cómo se comporta este sistema bajo la implementación en el módulo ESP32, mediante este análisis indicar la conducta sobre las métricas que se presentan en los resultados procedentes de la experimentación en un tramo carretero.

**Organización**

Este trabajo consiste en cuatro secciones, introducción, estado del arte, método, resultados y conclusiones

**Estado del arte**

La mensajería de la información es lo que va a determinar el actuar por parte de las autoridades dependiendo del contenido del mensaje, por lo tanto, el cómo ser ejecutada esta acción es fundamental, existen diferentes trabajos relacionados con respecto a esta problemática, (Nadezda, 2017) se enfoca en aplicaciones de asistencia de manejo y hace un análisis exhaustivo en base a simulaciones en su propuesta. Con el objetivo de evaluar MQTT y CoAP bajo diferentes escenarios, (R. Tomar et al., 2020)construye una arquitectura IoT donde implementa en un ESP32 utilizando mensajería MQTT donde tiene como resultados diferentes métricas de interés, entre ellas la información mandada y el tiempo que demora, (Hussein & Shujaa, 2020), de igual manera utiliza el mismo protocolo de mensajería para mandar mensajes cifrados en respuesta de servicios médicos de ambulancia.(R. and P. M. and S. H. G. Tomar, 2017) propone una arquitectura en la cual se aprovechan las características de MQTT como la calidad de servicio, señala la nula necesidad de infraestructura VANET. En resumen, lo que tienen en común estos artículos es la manera de emplear MQTT como mensajería *multi-cast* con el propósito de disipar los mensajes de índole de emergencia o alerta.

**Seguridad**

MQTT cuenta con varias opciones de seguridad en términos de autenticación, autorización y confidencialidad de datos. Para la autenticación, proporciona un esquema de autenticación simple a través de campos de nombre de usuario y contraseña en el paquete de inicio de conexión que un cliente puede usar para conectar el intermediario, aunque las credenciales de autenticación se envían en texto sin formato y se debe usar alguna forma de cifrado (Katsikeas et al., 2017) .

La autorización en MQTT se puede lograr utilizando una lista de control de acceso (ACL) en el lado del *broker*. La ACL contiene permisos para que los usuarios o los procesos del sistema otorguen acceso a los objetos, así como las operaciones permitidas en objetos determinados. MQTT ACL contiene todos los pares de nombres de usuario y contraseñas y los temas que un cliente tiene acceso de publicación y/o suscripción. Las características de autorización mejoradas se pueden implementar en el corredor con la forma de complementos o con la forma de un servicio web adicional. También se pueden integrar esquemas de control de acceso más sofisticados en MQTT (Fysarakis et al., 2018),(Fysarakis et al., 2014). En cuanto a la confidencialidad de los mensajes MQTT, esto se puede lograr en la capa de aplicación mediante el uso de cifrado de carga útil. Para este cifrado, se puede utilizar cualquiera de los algoritmos de cifrado o cifrado autenticado disponibles, siempre que haya soporte para los dispositivos de destino.

El hardware de desarrollo de IoT es viable para aplicaciones VANET, sin embargo, la implementación de algoritmos de cifrado es una de las tareas que comprometen los recursos del hardware embebido en la tarjeta en sí, junto con la tarea de establecer conexión física con el medio a transmitir, debido al trabajo que desempeñan estas tareas es importante considerar los recursos, para ello se tienen diferentes trabajos donde se implementan algoritmos de cifrado en diferentes tarjetas de desarrollo, (Singh et al., 2015) trabaja con un concepto SMQTT empleando un cifrado basado en clave/texto-cifrado basado en atributos KP/AP-ABE utilizando cifrado ligero de curvas elípticas, la implementación se hizo en *Raspberrypi*. (Katsikeas et al., 2017). Trabajo donde autores concluyen que el cifrado autenticado de carga útil con AES-OCB es el más adecuado para aplicaciones industriales, se implementó en Zolertia Z1.(de Santis et al., 2017) los autores proponen una implementación optimizada de ChaCha20 para procesadores ARM Cortex-M4, la evaluación del desempeño muestra que los cifrados ChaCha20-Poly1305 son candidatos prometedores para asegurar las aplicaciones emergentes de IoT con poca velocidad y restricciones espacio. (Sadio et al., 2019) de igual manera maneja el algoritmo ChaCha20-Poly1305 implementado en un Arduino uno.

**Metodología**



Figura 1. Diagrama general de metodología empleada.

Mediante una investigación teórica exhaustiva sobre los temas relacionados, se realiza un análisis del problema propuesto a resolver donde el estado del arte de los temas involucrados son base para el desarrollo del proyecto, posterior se hace una evaluación sobre la implementación teniendo en cuenta las delimitaciones y limitaciones presentes para poder así presentar una propuesta donde se presentan las diferentes tecnologías evaluadas en la investigación del estado del arte logrando proponer una arquitectura fundamentada. Las pruebas y simulaciones se dan de manera local al principio para lograr una implementación en el sistema embebido a utilizar en conjunto con el hardware necesario para recibir la información y transmitirla, de lado del servidor también se requiere una implementación de diferentes servicios para que el sistema logre la comunicación entre cliente y servidor. Si los resultados son los esperados se procede realizar la implementación que llevará a cabo la experimentación en el tramo carretero designado, por ultimo se validan los resultados obtenidos para realizar su análisis y llegar a una conclusión.

**Propuesta**

* Los mensajes de emergencia tipo broadcast convenientes que pueden ser emitidos por conductores, así como también entidades como policía, ambulancia, departamento de bomberos que necesiten extender sus servicios fuera de zona urbana o viceversa, estarán bajo la cobertura de la tecnología 2G GSM por ser la de mayor alcance. Si pasa algo en zona rural y la información necesita ser comunicada inmediatamente a zonas urbanas lo cual tiene la misma importancia.
* MQTT es un protocolo de mensajería estándar OASIS para el Internet de las cosas (IoT). Está diseñado como un transporte de mensajería de publicación/ suscripción extremadamente ligera que es ideal para conectar dispositivos remotos con una huella de código pequeña y un ancho de banda de red mínimo. MQTT hoy en día se utiliza en una amplia variedad de industrias, como la automoción, la fabricación, las telecomunicaciones, el petróleo y el gas, etc.
* El método de cifrado se concentra para darle confidencialidad a los mensajes emitidos por MQTT. Con el propósito de ocultar información sensible como las coordenadas de posicionamiento global del vehículo.

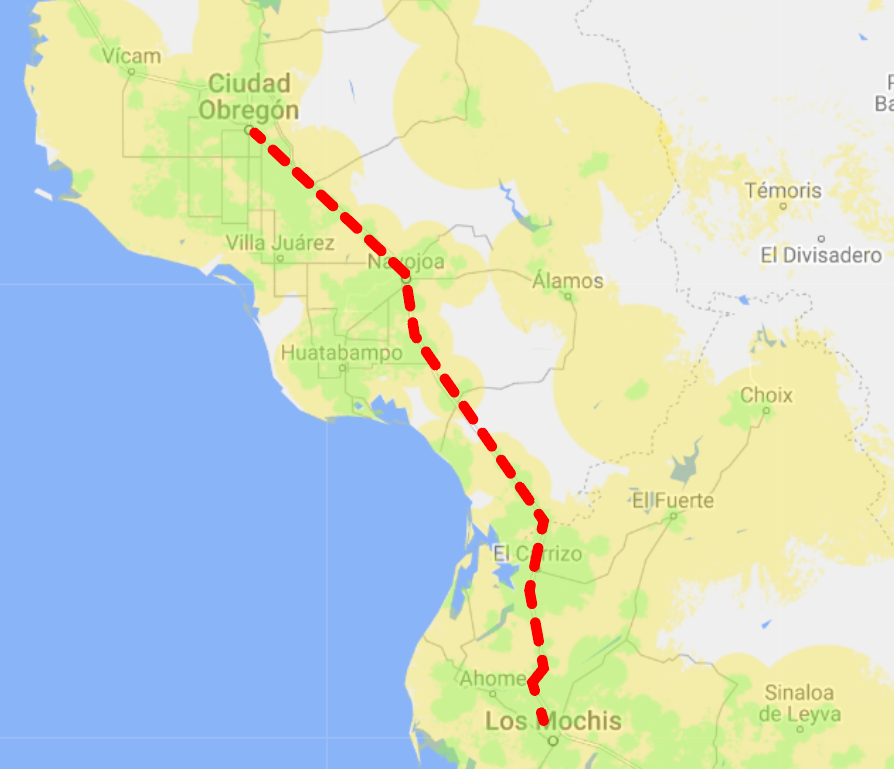


Figura 2. Campo de experimentación.

La experimentación da lugar a un tramo carretero estratégico donde se pueden manifestar valores de intensidad de señal de cualquier magnitud, en la Figura 2 (*Mapa de Cobertura - Corporativo | Mundo Telcel*, n.d.) Se muestra el mapa de cobertura 2G, denominado por la empresa perteneciente como zonas amarillas donde no se da garantía de comunicación y zonas verdes de garantía determinadas por la infraestructura.

Las métricas de interés de este proyecto se concentran en valores de retardo, el cual se monitoriza desde la publicación del mensaje emitida por el sistema embebido hasta el servidor, otras de las métricas es el *throughput* (relación entre información mandada e información recibida), los errores de los paquetes no son de menor importancia. Estos estos valores son objeto de análisis y a su vez indicadores de un correcto funcionamiento.

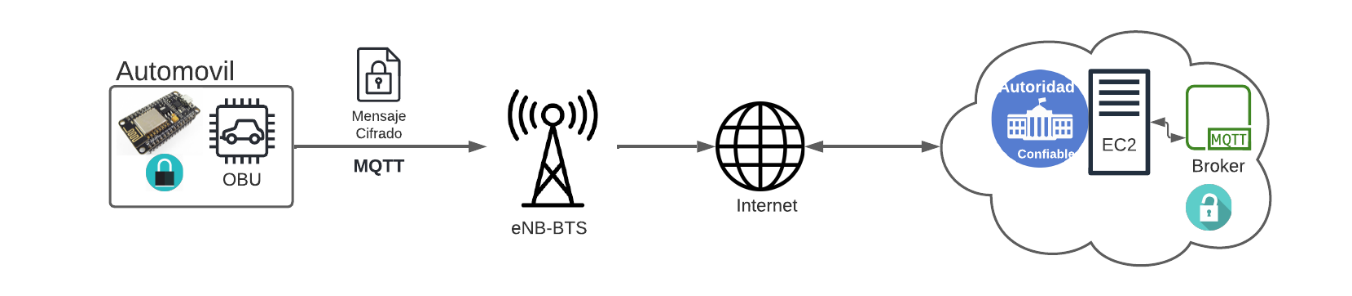


Figura 3. Arquitectura general.

**ESP32**: Toma la identidad de OBU, este es el punto donde la información parte obteniendo la información de RSSI y GPS de sus respectivos módulos, para esta ser procesada y publicada por el protocolo MQTT una vez cifrada. **Infraestructura:** se tiene dependencia sobre la infraestructura existente brindada en este proyecto por TELCEL, la cual logra la conexión hacia **Internet**: red por la corre MQTT, y a su vez esta conectada el ultimo elemento de la arquitectura. **Servidor:** establecido por servicio de IaaS, suscrito a los tópicos correspondientes de MQTT, cuando la información llega este punto, gracias a las prestaciones de *cloud computing,* las posibilidades en cuanto el manejo de la información recibida aumentan convenientemente, ya sea que se quiera hacer mensaje *broadcasting* o mandar convenientemente a puntos específicos dependiendo de la alerta emitida y sus necesidades.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Tabla I. Recursos del OBU   |  |  | | --- | --- | | **OBU** | | | ESP32 (CP210x) | El módulo ESP32 Wi-Fi/Bluetooth, Dos nucleos. *http://esp32.net/)* | | Modulo Sim800L Gsm V2 | Modulo SIM800L v2.0 es un dispositivo GSM y GPRS de 4 bandas para enviar y recibir mensajes SMS y llamadas ó bien tener red de datos móviles e internet mediante GPRS. | | Módulo Gps Neo6mv2 | Este módulo GPS posee antena y EEPROM integradas, presenta una gran precisión y su uso es muy simple. | | |  |  |  | | --- | --- | --- | | Servidor (*Iaas*) EC2 AWS | | | | **Hardware** | Procesador | Intel Xeon ES-2676 2.4GHz | |  | SSD | 64Gb | |  | Ram | 2 Gb | | **Software** | Sistema operativo | Ubuntu Server 18.04 LTS |   Tabla II. Recursos del servidor. |

**Desarrollo**

|  |  |
| --- | --- |
| Figura 4. Diagrama lógico ESP32 | Figura 5. Procesos ejecutados por servidor |

**Esp32**: Primero se inicialan las configuraciones, en cuanto a MQTT se le otorgan sus credenciales de conexión con el servidor y a su vez se configura la unidad SIM800L, con sus librerías correspondientes. A través de funciones se lee la información GPS y a su vez el módulo GSM por comandos AT lee el RSSI, una vez lista esta información se procede a hacer la estructura del mensaje no cifrado (ejemplo: RSSI:22,lat:27.321077,lon:-109.721893,Alert:1), se le otorga un bus para la carga útil del mensaje de 40 bytes, una vez logrado el mensaje se publica bajo el tópico mencionado.

El cifrado se hace en cuatro partes donde cada una es una variable por separado (esto se hace con el objetivo de aprovechar los 16 bytes nativos del algoritmo) y se juntan para hacer una sola publicación necesitando un bus de 129 bytes para mandar el mensaje cifrado completo. Una vez echo el ultimo proceso el sistema pasa a ciclarse desde la lectura de los valores hasta la publicación del mensaje cifrado.

**Servidor**: El servidor se encarga de tres tareas:

1. Establecer el bróker.
2. Suscribirse a los tópicos donde el ESP32 publica para escuchar los mensajes.
3. Hacer *sniffing* con la herramienta *wireshark* en el periodo de experimentación para hacer el análisis con la información recopilada.

Para manipular el hardware y software del servidor se hace uso del protocolo SSH, y también del protocolo FTP para descargar la hoja de datos del análisis.

**Resultados**

Se implementaron diferentes algoritmos de manera independiente en el ESP32, para hacer contraste con el que se usa en este proyecto.

Figura 6. Grafica de resultados en algoritmos de cifrado.

El algoritmo AES-128 con una llave privada de 16bytes y una carga útil de igual dimensión se obtuvo un tiempo promedio de 30.5ms.

Para hacer obtener las métricas de comunicaciones se hizo *sniffing* con laherramienta de análisis de protocolos *Wireshark,* la cual seasentó dentro del servidor e interceptó los paquetes de comunicación mediante MQTT publicados por el ESP32 durante el periodo de experimentación.

Se mostró el un correcto funcionamiento del protocolo de mensajería sobre la red donde se estableció la dirección ip 172.31.16.41 por el ISP y el nodo de destino 38.65.160.139 el cual tiene la dirección publica 52.23.115.184.



Figura 7. Análisis de trafico en la red del servidor.

Se establecieron dos tópicos MQTT con QoS(0), “msj\_seguro” y “msj\_no\_seguro”. El primer tópico se da con el propósito de obtener la información sin cifrado por cuestiones de monitoreo ya que este proyecto no cubre la parte de descifrado.

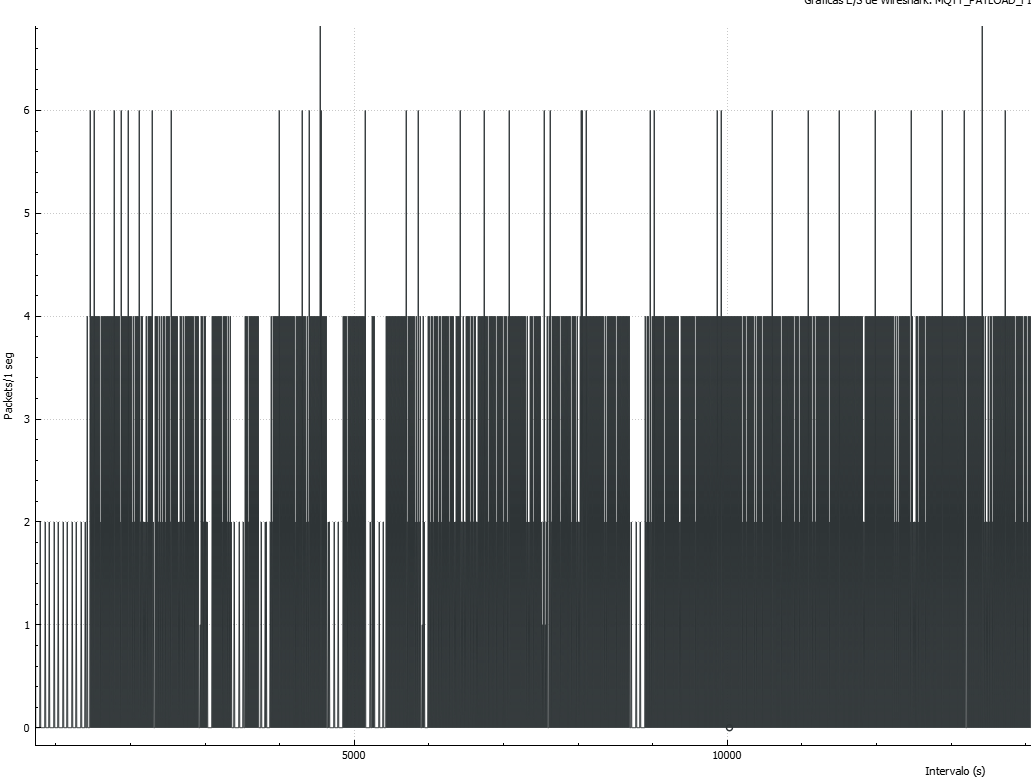


Figura 8. Estadística de entrada-salida.

Se identifican dos patrones en gráfica, donde los paquetes de información llegan a dos sobre segundo, y donde llegan a cuatro sobre segundo, esto es porque los datos se mandan por dos tópicos, en el de “msj\_no\_seguro” se tiene un bus de 40 bytes para mandar el texto plano con la información sin cifrado, a su vez en “msj\_seguro” el bus es 129 bytes donde viaja la información cifrada. También en las crestas mas bajas se puede ver el funcionamiento del *keep alive,* método perteneciente al protocolo MQTT para identificar la existencia de conexión con el cliente.



Figura 9. Analisis de paquetes recibidos-transmitidos.

Con la herramienta Endpoints, el ESP32 con dirección 172.31.16.41 y el servidor con 172.31.16.41. Se registraron 3,886 paquetes transmitidos por el ESP32 y 3,328 paquetes recibidos por parte del servidor, lo que un *troughtput* de 85.64%.

Durante la experimentación se obtuvieron los siguientes valores de RSSI.

Tabla III. Valores de RSSI

|  |  |
| --- | --- |
| RSSI magnitud | |
| Min | x |
| Max | x |
| Promedio | x |

En el transcurso de la experimentación se registró un RSSI marginal del 20%, decente del 40% bueno del 30% y excelente del 10%.

Ponerle las etiquetas.

**Ruta recorrida**

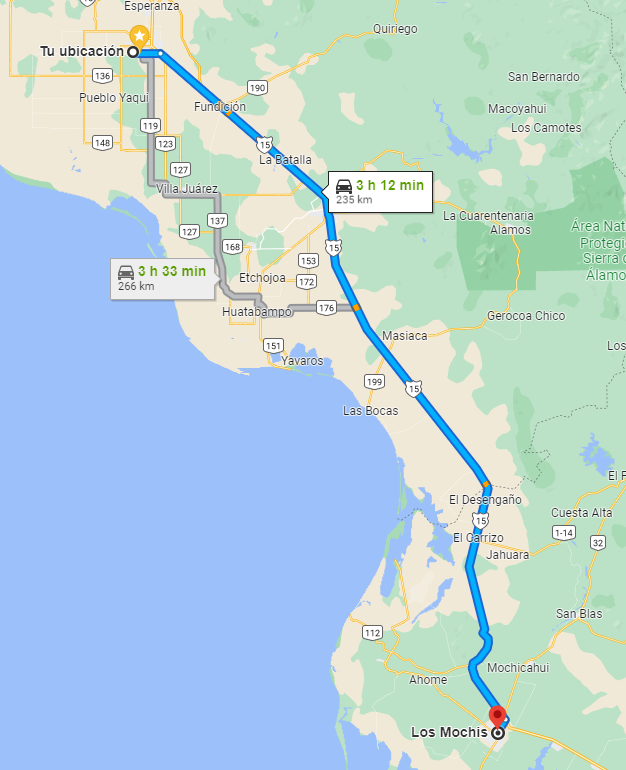


Figura 10. Mapa de ruta recorrida.

Se recorrieron 266km con una duración de 3h 12min aproximadamente, tiempo el cual el ESP32 se mantuvo en funcionamiento y periodo en el cual se monitorizaba el trafico de la red del servidor.

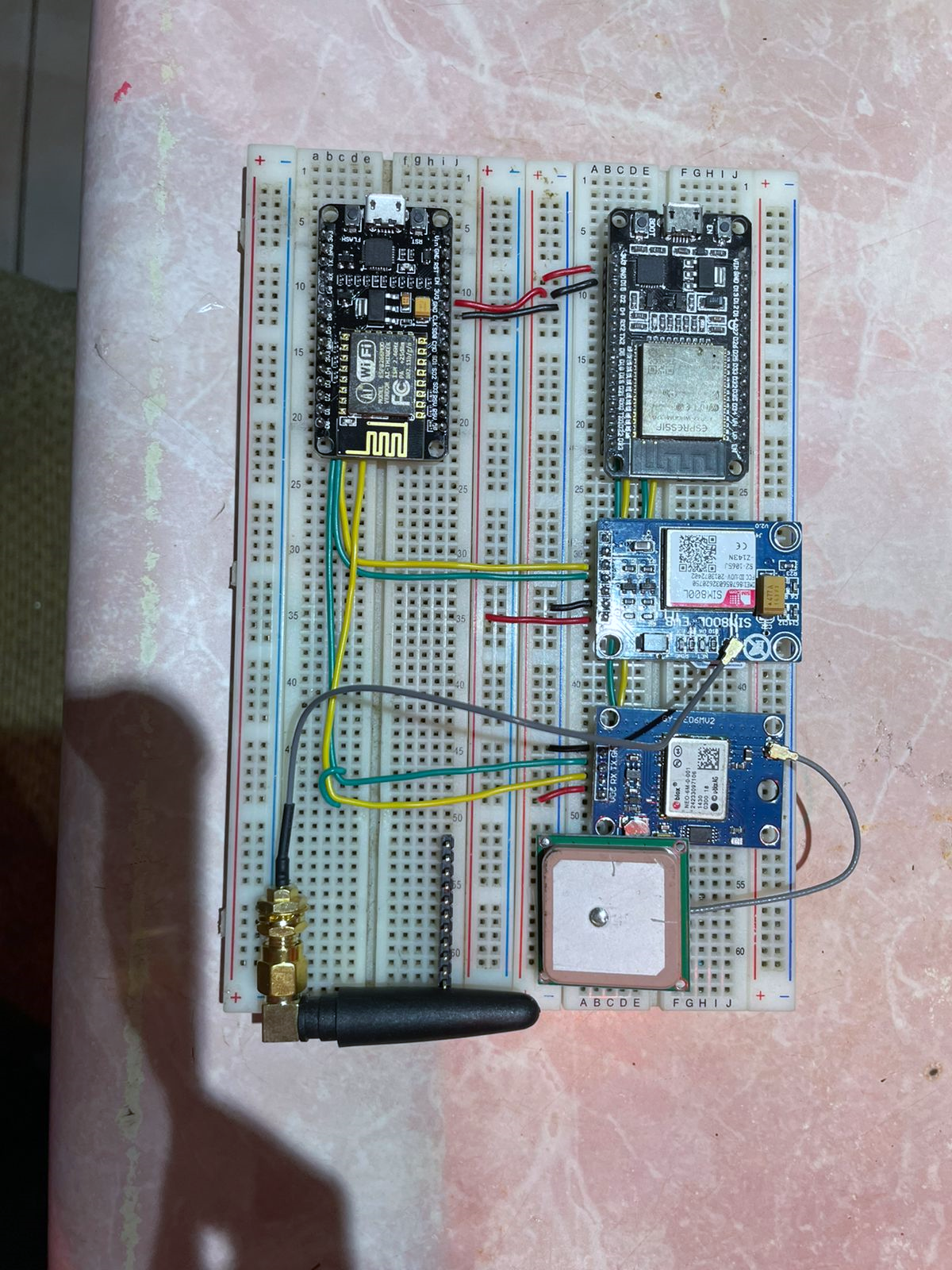
****

Figura 11. Prototipo de hardware experimental.

**Conclusión**

Se desarrolló un sistema seguro que otorgó confidencialidad a los mensajes con índole de emergencia en vehículos bajo un sistema C-V2X se estableció la comunicación entre vehículo e internet a través del protocolo de mensajería MQTT por el ESP32. De esta manera se garantiza la transmisión y recepción de los mensajes entre V2V, V2I y otras unidades. Se logro un tiempo de respuesta eficiente, sin alejarse de los requisitos que demandan los eventos de emergencia. Aunque AES-128 en su modo ECB no es recomendable usar dado que resultan patrones evidentes en los mensajes, queda a trabajo futuro la mejora en cuanto a su estructura y modo de operación, así como también el esquema de seguridad para otorgar otros pilares de la seguridad informática.

**Referencias**

*CIAPEM 2021 – Comité de Informática de la Administración Pública Estatal y Municipal A.C.* (n.d.). Retrieved March 9, 2022, from https://ciapem.org/

de Santis, F., Schauer, A., & Sigl, G. (2017). ChaCha20-Poly1305 authenticated encryption for high-speed embedded IoT applications. *Proceedings of the 2017 Design, Automation and Test in Europe, DATE 2017*, 692–697. https://doi.org/10.23919/DATE.2017.7927078

Eze, E. C., Zhang, S. J., Liu, E. J., & Eze, J. C. (2016). Advances in vehicular ad-hoc networks (VANETs): Challenges and road-map for future development. *International Journal of Automation and Computing 2016 13:1*, *13*(1), 1–18. https://doi.org/10.1007/S11633-015-0913-Y

Fysarakis, K., Papaefstathiou, I., Manifavas, C., Rantos, K., & Sultatos, O. (2014). Policy-based access control for DPWS-enabled ubiquitous devices. *Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA)*, 1–8. https://doi.org/10.1109/ETFA.2014.7005233

Fysarakis, K., Soultatos, O., Manifavas, C., Papaefstathiou, I., & Askoxylakis, I. (2018). XSACd—Cross-domain resource sharing &amp; access control for smart environments. *Future Generation Computer Systems*, *80*, 572–582. https://doi.org/10.1016/j.future.2016.05.023

Hasrouny, H. (n.d.). *Trust management and security solutions for vehicular networks*. https://tel.archives-ouvertes.fr/tel-01892393

Hussein, N. A., & Shujaa, M. I. (2020). Secure vehicle to vehicle voice chat based MQTT and coap internet of things protocol. *Indonesian Journal of Electrical Engineering and Computer Science*, *19*(1), 526–534. https://doi.org/10.11591/ijeecs.v19.i1.pp526-534

*Instituto Nacional de Salud Pública*. (n.d.). Retrieved March 9, 2022, from https://www.insp.mx/

Katsikeas, S., Fysarakis, K., Miaoudakis, A., van Bemten, A., Askoxylakis, I., Papaefstathiou, I., & Plemenos, A. (2017). Lightweight & secure industrial IoT communications via the MQ telemetry transport protocol. *Proceedings - IEEE Symposium on Computers and Communications*, *0*, 1193–1200. https://doi.org/10.1109/ISCC.2017.8024687

*Luto carretero: los accidentes viales más trágicos del 2021 - Infobae*. (n.d.). Retrieved March 9, 2022, from https://www.infobae.com/america/mexico/2021/12/27/luto-carretero-los-accidentes-viales-mas-tragicos-del-2021/

*Mapa de Cobertura - Corporativo | Mundo Telcel*. (n.d.). Retrieved June 2, 2022, from https://www.telcel.com/mundo\_telcel/quienes-somos/corporativo/mapas-cobertura

Nadezda, Y. (2017). *A Safe Intelligent Driver Assistance System in V2X Communication Environments based on IoT*.

Sadio, O., Ngom, I., & Lishou, C. (2019). Lightweight Security Scheme for MQTT/MQTT-SN Protocol. *2019 6th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2019*, 119–123. https://doi.org/10.1109/IOTSMS48152.2019.8939177

Shrestha, R., Bajracharya, R., & Nam, S. Y. (2018). Challenges of Future VANET and Cloud-Based Approaches. In *Wireless Communications and Mobile Computing* (Vol. 2018). Hindawi Limited. https://doi.org/10.1155/2018/5603518

Singh, M., Rajan, M. A., Shivraj, V. L., & Balamuralidhar, P. (2015). Secure MQTT for Internet of Things (IoT). *Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*, 746–751. https://doi.org/10.1109/CSNT.2015.16

Tomar, R. and P. M. and S. H. G. (2017). A novel approach to multicast in VANET using MQTT. *Ada User J*, 231–235.

Tomar, R., Sastry, H. G., & Prateek, M. (2020). A V2I BASED APPROACH TO MULTICAST IN VEHICULAR NETWORKS. *Malaysian Journal of Computer Science*, *2020*(Special Issue 1), 93–107. https://doi.org/10.22452/mjcs.sp2020no1.7