International Interdisciplinary Congress on Renewable Energies, Industrial Maintenance, Mechatronics and Informatics
Booklets

RENIECYT 1702902 CONACYT

RENIECYT - LATINDEX - Research Gate - DULCINEA - CLASE - Sudoc - HISPANA - SHERPA UNIVERSIA - Google Scholar DOI - REDIB - Mendeley - DIALNET - ROAD - ORCID

Title: MQTT secure emergency messaging system for IoT-based C-V2X networks

Authors: PALOS-ANGULO, Francisco Antonio and RUIZ-IBARRA, Erica Cecilia

Editorial label ECORFAN: 607-8695
BCIERMMI Control Number: 2022-01
BCIERMMI Classification (2022): 261022-0001

Pages: 18
RNA: 03-2010-032610115700-14

ECORFAN-México, S.C.
143 – 50 Itzopan Street
La Florida, Ecatepec Municipality
Mexico State, 55120 Zipcode
Phone: +52 1 55 6159 2296
Skype: ecorfan-mexico.s.c.
E-mail: contacto@ecorfan.org
Facebook: ECORFAN-México S. C.
Twitter: @EcorfanC

www.ecorfan.org

Holdings
Mexico Colombia Guatemala
Bolivia Cameroon Democratic
Spain El Salvador Republic
Ecuador Taiwan of Congo
Peru Paraguay Nicaragua

Introducción

- Las redes vehiculares ad-hoc (VANET) han recibido una atención significativa tanto de las comunidades académicas como industriales.
- VANET es una clase particular de Red Móvil Ad Hoc (MANET) en la que los nodos móviles son vehículos.
- MANET: Mobile Ad-hoc Network
- VANET: Vehicular Ad-hoc Network
- Compañías que incursionan en desarrollo de VANET: Ford, Toyota y GM.

Composición futura de vehículos

- Dispositivos a equipar:
  - **OBU:** Unidad a bordo (*On-Board Units*).
  - **GPS:** Sistema de Posicionamiento Global (*Global Positioning System*).
  - **EDR**: Registrador de datos de eventos (*Event Data Recorder* p).
  - **Sensores**: (radar).

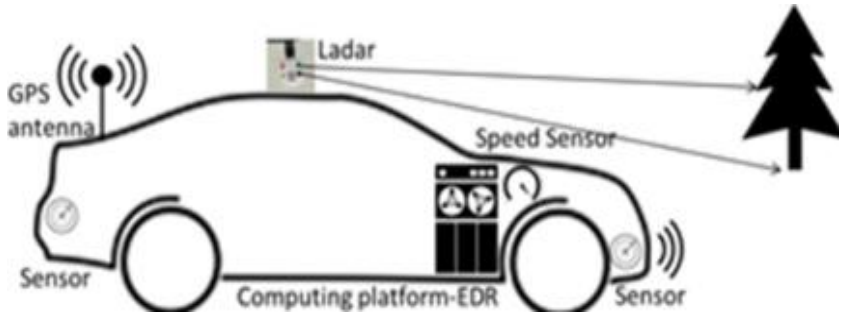

Figura 1. Elementos que conforman un vehículo en VANET.

Arquitectura VANET

- AU (Aplication)

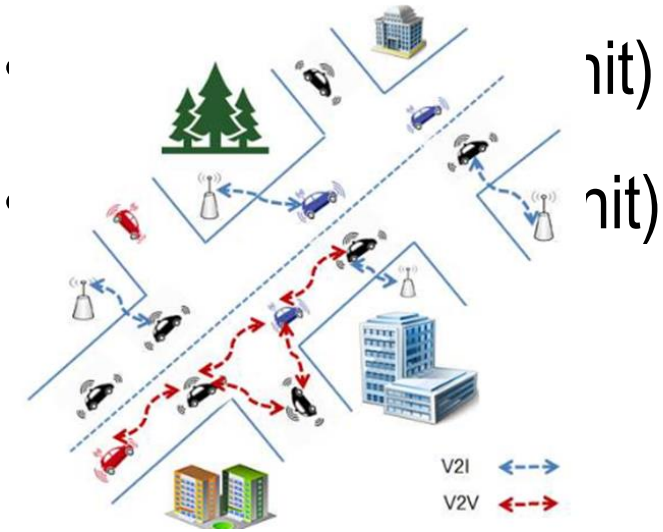

Figura 2. Arquitectura VANET.

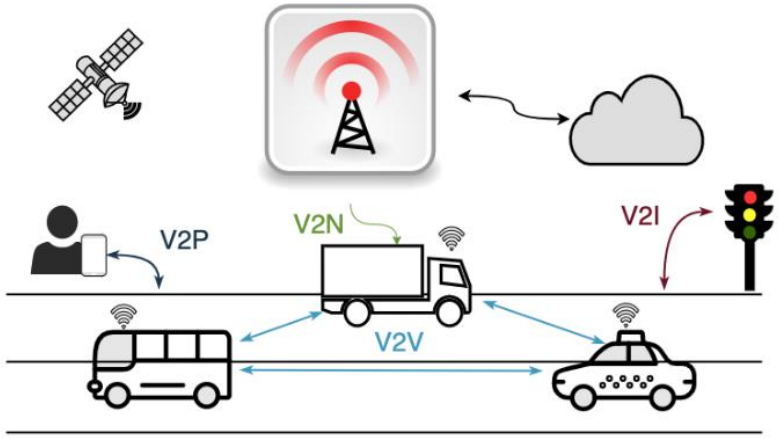

Figura 3. Patrones de comunicación.

Tipos de patrones de comunicación

1. *Vehicle ToVehicle (V2V).*
2. *Vehicle To Infrastructure (V2I).*
3. *Vehicle ToPedestrian (V2P).*
4. *Vehicle To Network (V2N).*

Por lo general, Vehicle To Everything (V2X) se utiliza para referirse a los cuatro tipos de comunicaciones

Características VANET

Redes y comunicaciones

- **Red ilimitada y escalable**: VANET se puede implementar para una o varias ciudades, incluso para países.

-**Comunicación inalámbrica**: La conexión de los nodos y su intercambio de datos se realizan a través de canales inalámbricos. Esto requiere una comunicación más segura.

-**Alta movilidad y topología de red que cambia rápidamente**: los nodos se mueven a alta velocidad y de manera aleatoria, lo que hace que sea más difícil predecir su posición y la topología de la red.

Vehículos y conductores

-**Alta capacidad de procesamiento y energía suficiente**: los nodos VANET no tienen problemas de energía y recursos de computación.

-**Mejor protección física**: los nodos VANET están físicamente mejor protegidos. Es más difícil comprometerlos físicamente.

-**Tiempo y posición conocidos**: La mayoría de los vehículos están equipados con GPS porque muchas aplicaciones dependen de la posición y la dirección geográfica o el área.

Seguridad

En VANET, la seguridad debe de **garantizar** que en el **intercambio de mensajes no haya** inyecciones o **alteraciones** por los atacantes. También, la fiabilidad de los conductores es esencial para informar el estado del tráfico correctamente sin ninguna limitación o complicación en tiempo.

Exclusivamente los desafíos de seguridad surgen con las características que VANET trae, abordar los desafíos de seguridad traen varias limitaciones.

Escenarios de emergencia

- Según el Sistema Nacional de Seguridad Pública (INSP) [7], 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 [8].
- 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.

Metodología

Se presenta la ruta metodológica que se siguió para el desarrollo del proyecto

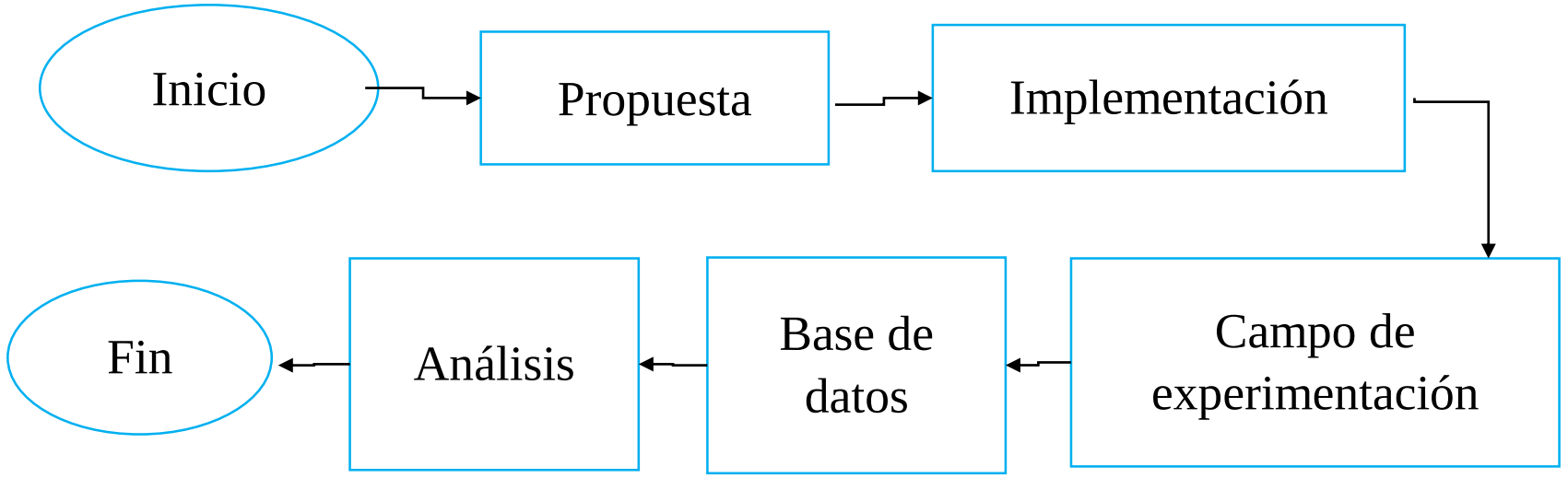

Figura 4. Diagrama general de metodología empleada.

Desarrollo

- **Arquitectura propuesta**

Comunicación celular C-V2X	MQTT	Cifrado
Sistema de conexión inalámbrica de tecnología celular para automóviles.	Protocolo de mensajería estándar OASIS para internet de las cosas (IoT).	Cifrado de mensajes con algoritmo AES-128 en modo ECB.

Figura 5. Etapas principales de la arquitectura propuesta.

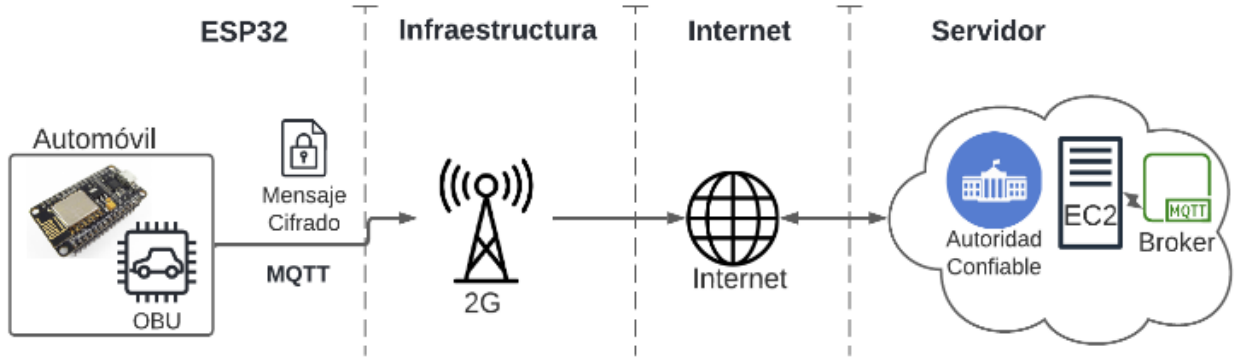

Figura 6. Arquitectura general.

Recursos

OBU	
ESP32 (CP210x)	El módulo ESP32 Wi-Fi/Bluetooth, Dos núcleos. http://esp32.net/)
Módulo Sim800L GSM V2	Módulo SIM800L v2.0 es un dispositivo GSM y GPRS de 4 bandas para enviar y recibir mensajes SMS y llamadas, o 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.

Tabla 1. Recursos del OBU.

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 2. Recursos del servidor.

Implementación del sistema

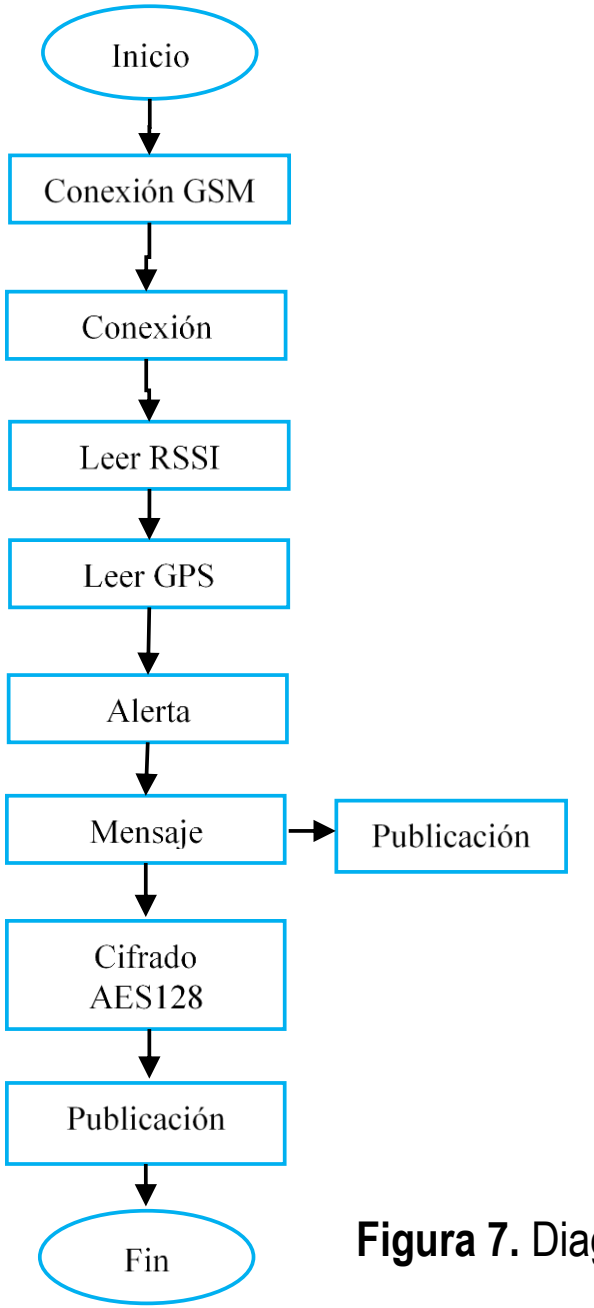

Figura 7. Diagrama lógico ESP32.

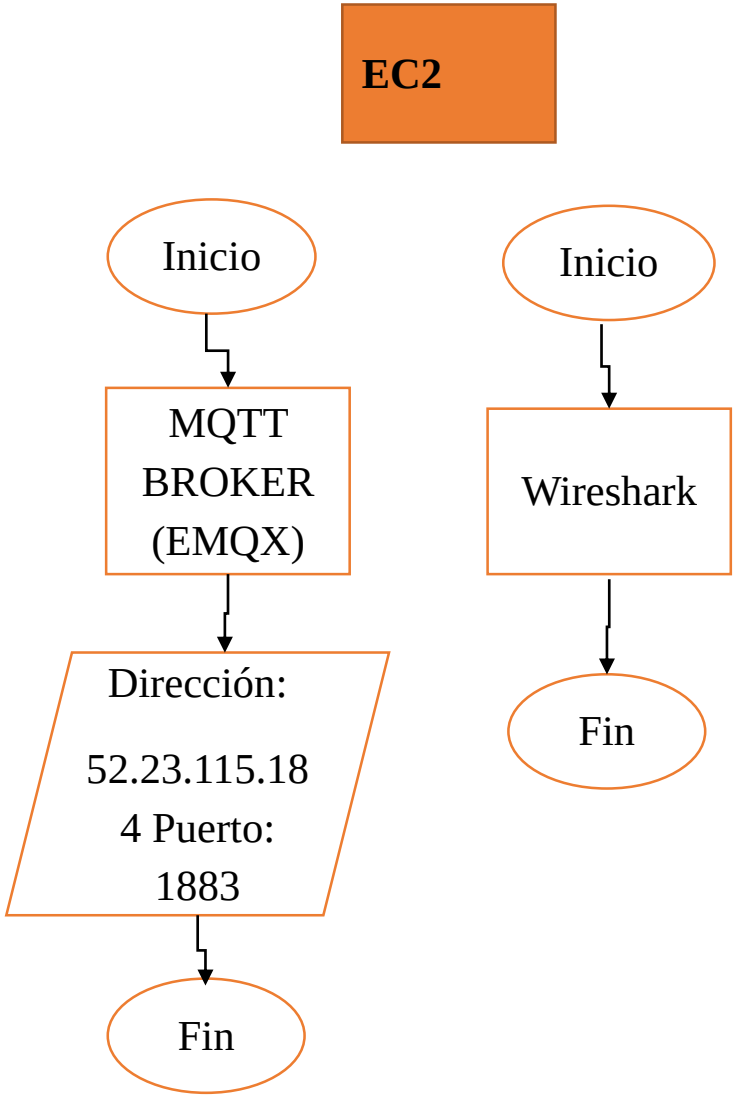

Figura 8. Procesos ejecutados por servidor

Resultados

Figura 9. Campo de experimentación.

Fuente: (*Mapa de Cobertura - Corporativo | Mundo Telcel*, 2022)

Cifrado

Se implementó de manera independiente el algoritmo AES-128 en modo de bloques ECB para probar el comportamiento del dispositivo embebido. El algoritmo de cifrado con una llave privada de 16 bytes y una carga útil de igual dimensión se obtuvo un tiempo promedio de 30.5ms.

RSSI durante el recorrido

Se recorrieron 266 Km con una duración de 3h 12min aproximadamente, tiempo el cual el ESP32 se mantuvo en funcionamiento y periodo en el cual se monitorizaba el tráfico de la red del servidor.
Durante la experimentación se obtuvieron los siguientes valores de RSSI mostrados en la Figura 8 por el módulo SIM800L haciendo referencia los valores tabulados en la Tabla III de (AT+CSQ – Signal Quality | M2MSupport.Net, n.d. 2022).

Valor	RSSI dBm	Condición	Valor	RSSI dBm	Condición
2	-109	*Marginal*	17	-79	*Good*
3	-107	*Marginal*	18	-77	*Good*
4	-105	*Marginal*	19	-75	*Good*
5	-103	*Marginal*	20	-73	*Excellent*
6	-101	*Marginal*	21	-71	*Excellent*
7	-99	*Marginal*	22	-69	*Excellent*
8	-97	*Marginal*	23	-67	*Excellent*
9	-95	*Marginal*	24	-65	*Excellent*
10	-93	*OK*	25	-63	*Excellent*
11	-91	*OK*	26	-61	*Excellent*
12	-89	*OK*	27	-59	*Excellent*
13	-87	*OK*	28	-57	*Excellent*
14	-85	*OK*	29	-55	*Excellent*
15	-83	*Good*	30	-53	*Excellent*
16	-81	*Good*			

Tabla 3. Valores de RSSI a través de comandos AT por el módulo GSM.

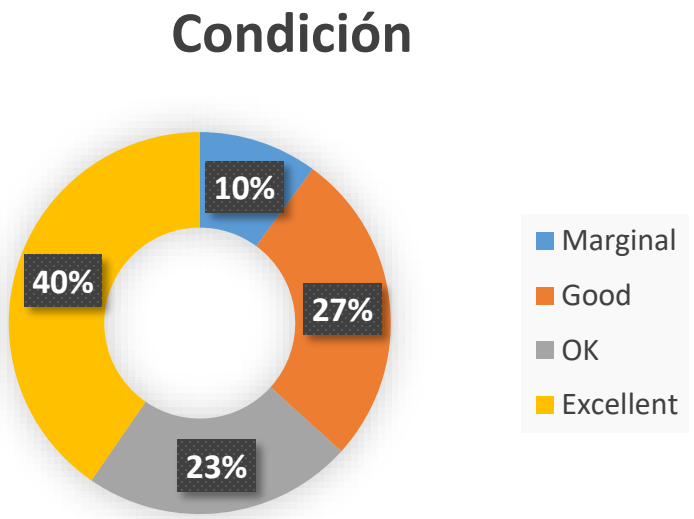

Gráfico 1. Valores de RSSI.

- La ruta inicio su recorrido desde la salida de la ciudad Obregón Sonora, hasta los inicios del cuadro de la ciudad de Los Mochis Sinaloa.
- La información del GPS dependía del módulo GSM para ser transmitida, mientras que este módulo esté con enlace establecido a internet
- Se registran 1836 filas de datos

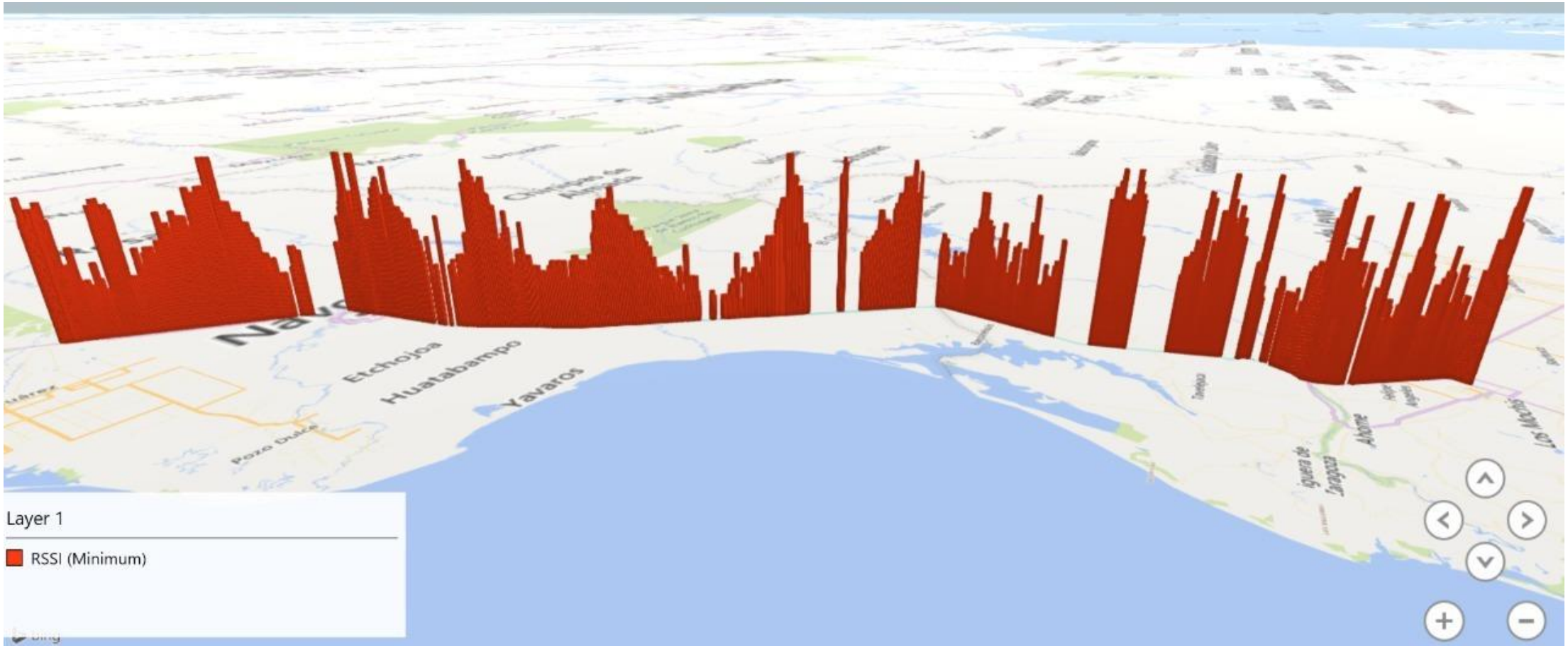

Figura 10. Mapa trazado por la información recibida del módulo GPS.

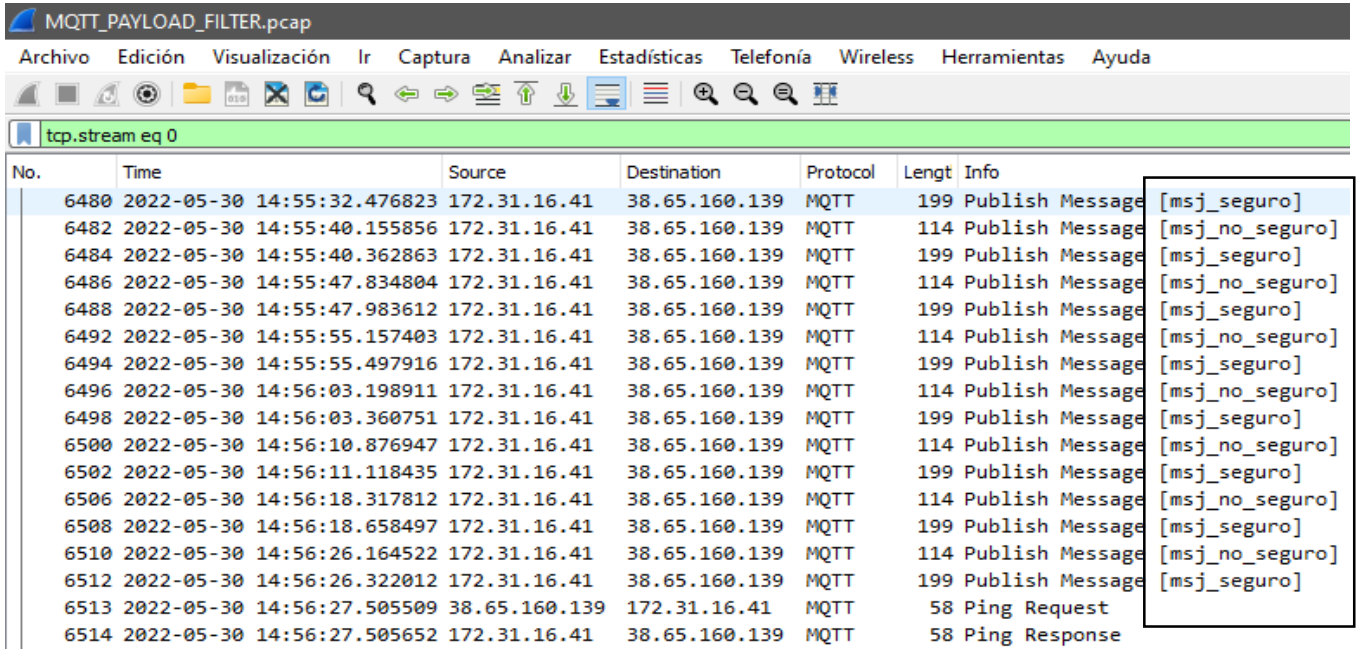

Figura 11. Análisis de tráfico en la red del servidor.

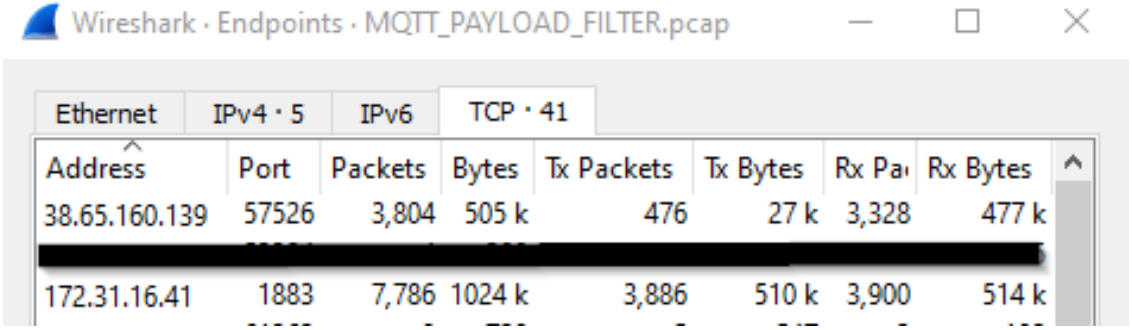

Figura 12. Análisis de paquetes recibidos-transmitidos

Tiempos

Máximo tiempo de no comunicación.

Modo ECB: 00:08:09

Tiempo de respuesta del MODULO GSM = **20908** milisegundos

Paquete	AES CBC
1	163
2	4254
3	4254
4	4262
Total	12933

Tabla 4. Tiempos de ejecución del algoritmo en micro segundos

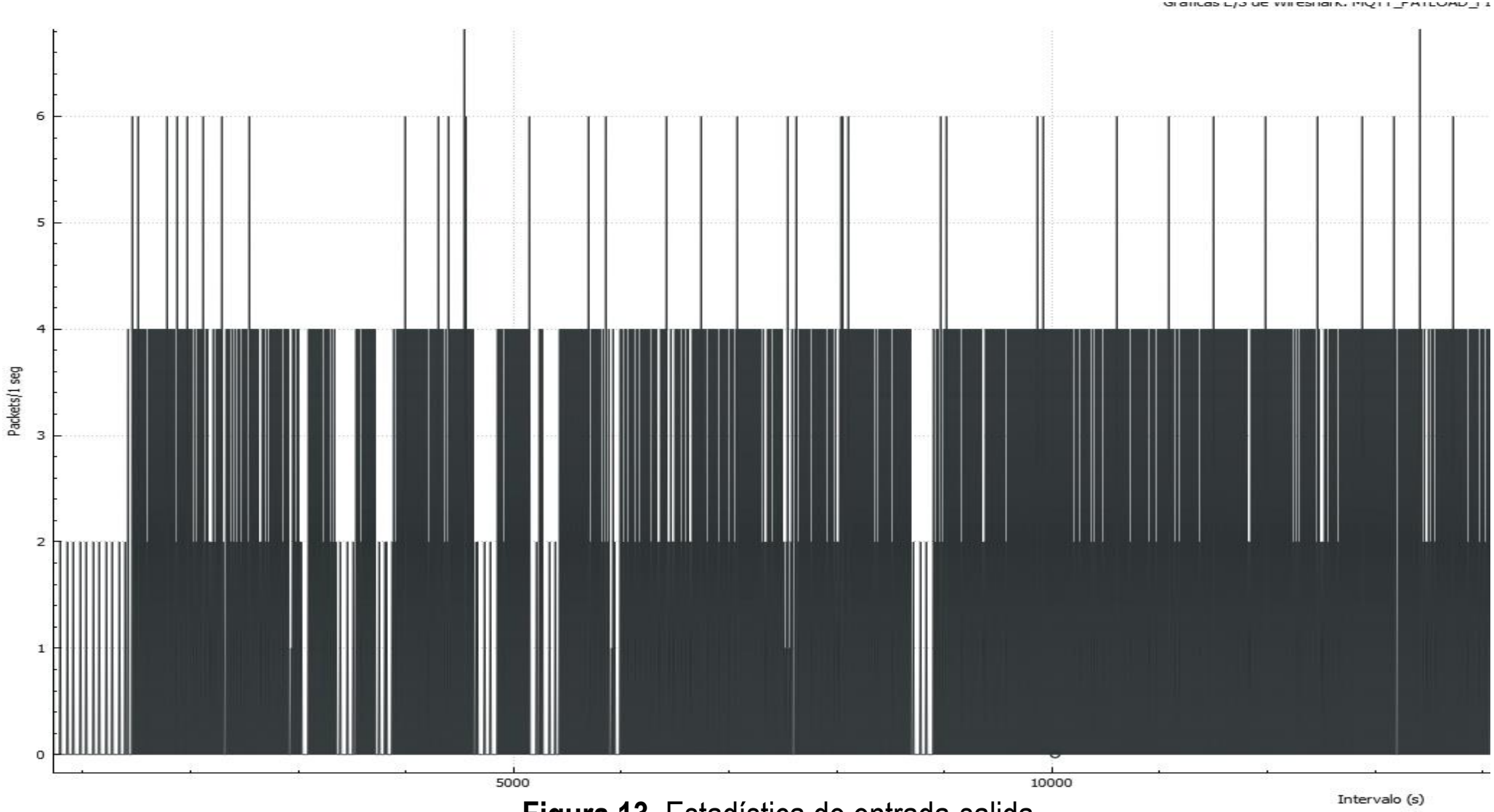

Figura 13. Estadística de entrada-salida.

Uso de recursos

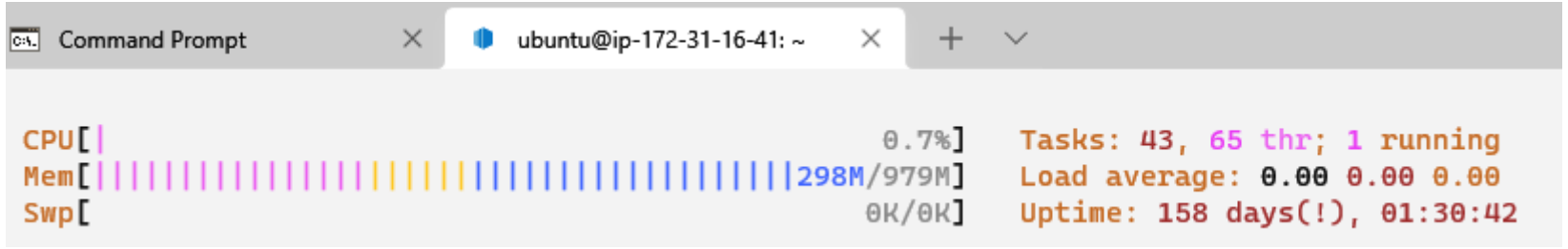

Figura 14. Hardware en uso por el servidor EC2.

```
Advanced Memory Usage is available via "PlatformIO Home > Project Inspect"
RAM:   [          ]   4.4% (used 14428 bytes from 327680 bytes)
Flash: [==        ]  21.6% (used 283626 bytes from 1310720 bytes)
```

Figura 15. Recursos consumidos por el ESP32.

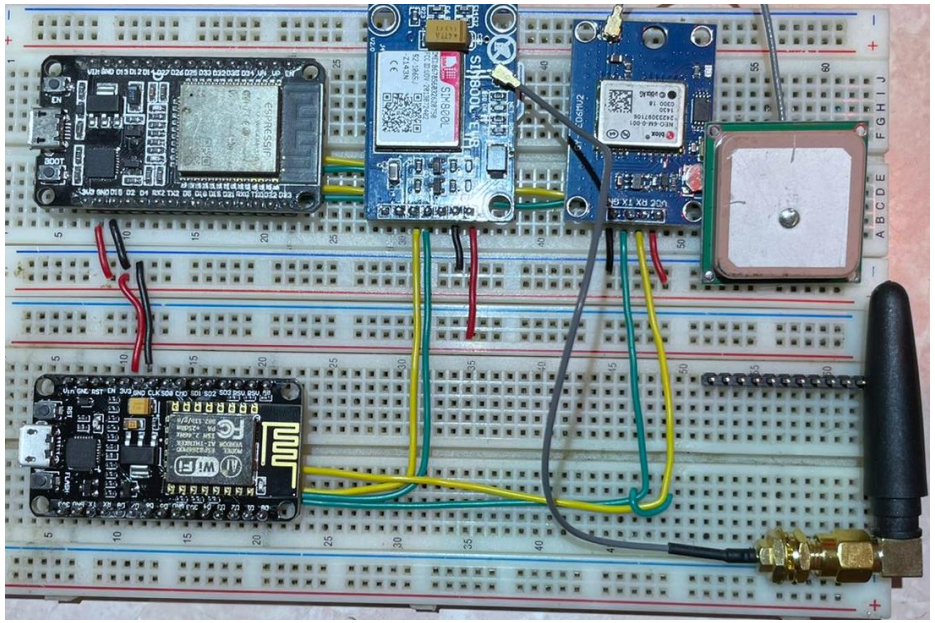

Figura 16. Prototipo de hardware experimental.

Figura 17. Prototipo en ejecución 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 logró un tiempo de respuesta eficiente, sin alejarse de los requisitos que demandan los eventos de emergencia además gracias a MQTT se demostró un mínimo uso de ancho de banda sobre el medio de comunicación.
    - El módulo GSM logró establecer comunicación estable en un amplio rango de valores aún en condiciones de bajo nivel de RSSI e incluso nivel nulo, esto se presentó en toda la ruta evaluada.
    - Aunque AES-128 en su modo ECB no es recomendable usar dado que resultan patrones evidentes en los mensajes, queda como trabajo futuro mejorar 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

[1]M. Luther Mfenjou, A. Adamou Abba Ari, W. Abdou, and F. ois Spies, “Sustainable Computing: Informatics and Systems Methodology and trends for an intelligent transport system in developing countries,” *Sustainable Computing: Informatics and Systems*, vol. 19, pp. 96–111, 2018, doi: 10.1016/j.suscom.2018.08.002.

[2]H. Hasrouny, “Trust management and security solutions for vehicular networks.” [Online]. Available: https://tel.archives-ouvertes.fr/tel-01892393

[3]R. Shrestha, R. Bajracharya, and S. Y. Nam, “Challenges of Future VANET and Cloud-Based Approaches,” *Wireless Communications and Mobile Computing*, vol. 2018. Hindawi Limited, 2018. doi: 10.1155/2018/5603518.

[4]M. Lee and T. Atkison, “VANET applications: Past, present, and future,” *Vehicular Communications*, vol. 28, Apr. 2021, doi: 10.1016/j.vehcom.2020.100310.

[5]L. Xie, Y. Ding, H. Yang, and X. Wang, “Blockchain-based secure and trustworthy internet of things in SDN-enabled 5G-VANETs,” *IEEE Access*, vol. 7, pp. 56656–56666, 2019, doi: 10.1109/ACCESS.2019.2913682.

[6]“CIAPEM 2021 – Comité de Informática de la Administración Pública Estatal y Municipal A.C.” https://ciapem.org/ (accessed Mar. 09, 2022).

[7]“Instituto Nacional de Salud Pública.” https://www.insp.mx/ (accessed Mar. 09, 2022).

[8]“Luto carretero: los accidentes viales más trágicos del 2021 - Infobae.” https://www.infobae.com/america/mexico/2021/12/27/luto-carretero-los-accidentes-viales-mas-tragicos-del-2021/ (accessed Mar. 09, 2022).

[9]H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, “VANet security challenges and solutions: A survey,” *Vehicular Communications*, vol. 7, pp. 7–20, Jan. 2017, doi: 10.1016/J.VEHCOM.2017.01.002.

[10]B. Mokhtar and M. Azab, “Survey on Security Issues in Vehicular Ad Hoc Networks,” *Alexandria Engineering Journal*, vol. 54, no. 4, pp. 1115–1126, Dec. 2015, doi: 10.1016/J.AEJ.2015.07.011.

[11]G. Karagiannis *et al.*, “Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions,” *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4, pp. 584–616, Dec. 2011, doi: 10.1109/SURV.2011.061411.00019.

[12]A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, “Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review,” *Computers in Industry*, vol. 137, p. 103614, May 2022, doi: 10.1016/J.COMPIND.2022.103614.

[13]C. Kohler, “The EU Cybersecurity Act and European standards: an introduction to the role of European standardization,” *International Cybersecurity Law Review 2020 1:1*, vol. 1, no. 1, pp. 7–12, Sep. 2020, doi: 10.1365/S43439-020-00008-1.

[14]A. Karim Mohamed Ibrahim, R. A. Rashid, A. H. F. A. Hamid, M. Adib Sarijari, and M. A. Baharudin, “Lightweight IoT middleware for rapid application development,” *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 17, no. 3, pp. 1385–1392, 2019, doi: 10.12928/TELKOMNIKA.V17I3.11793.

ECORFAN®