Article **Journal Information Technology**
December, 2022 Vol.9 No.28 7-16

Secure MQTT emergency messaging system for C-V2X networks based on IoT

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

ID 1st Author: *Francisco Antonio, Palos-Angulo* / **ORC ID**: 0000-0002-4766-8644, **CVU CONACYT ID**: 1076458

ID 1st Co-author: *Erica Cecilia, Ruiz-Ibarra* / **ORC ID**: 0000-0002-7020-4960, **CVU CONACYT ID**: 86862

DOI: 10.35429/JIT.2022.28.9.7.16 Received: August 10, 2022; Accepted December 30, 2022

Abstract

Currently in Mexico in some road sections, there are still areas of non-coverage where the infrastructure does not supply communication alerts or dangerous situations to the population through telecommunication technologies, this is one of the problems faced by emergency services by the authorities. Given this scenario, the present project develops a system based on IoT that provides a secure means of real-time communication of messages under the AES 128 algorithm, obtained through hardware implementation, through the MQTT protocol under a C-V2X system, which is oriented for experimental scenarios where the intensity of the signal can generate communication losses. The proposed system has been designed to achieve greater coverage on road sections and meet emergency demands by citizens with the least possible delay, without compromising the security of messages of this nature under conditions of low signal intensity and avoiding possible attacks.

VANET, AES128, MQTT, ESP32, C-V2X, IoT

Resumen

En la actualidad en México en algunos tramos carreteros siguen existiendo zonas de no cobertura donde la infraestructura no abastece para comunicar a la población de alertas o situaciones de peligro a través de tecnologías de telecomunicación, éste es uno de los principales problemas que enfrentan los servicios de emergencia por parte de las autoridades. Ante este escenario el presente proyecto desarrolla un sistema basado en IoT que 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, la cual está orientada para escenarios experimentales donde la intensidad de señal puede generar pérdidas de comunicación. El sistema propuesto ha sido pensado para lograr mayor cobertura en tramos carreteros y satisfacer las demandas de emergencia por parte de los ciudadanos con el menor retardo posible, sin comprometer la seguridad de los mensajes de esta índole bajo condiciones de baja intensidad de señal y evitar potenciales ataques.

VANET, AES128, MQTT, ESP32, C-V2X, IoT

Citation: PALOS-ANGULO, Francisco Antonio & RUIZ-IBARRA, Erica Cecilia. Secure MQTT emergency messaging system for C-V2X networks based on IoT. Journal Information Technology. 2022. 9-28: 7-16

† Researcher contributing as first author.

I. Introduction

During the last two decades, the automotive industry has been the hotbed of technological innovation as a result of significant advances in computing, communication and storage technologies. Vehicle Ad-Hoc Network (VANET) is one of the most attracted applications of internet of things that is growing rapidly since its security offering improved. VANET is an emerging type of network that facilitates communication between vehicles on the road. This application is one of the most important elements in intelligent transportation systems (ITSs) (Eze et al., 2016).

The fully connected car will be composed of an ecosystem of connected technologies that will enable it to transfer and process large amounts of data while traveling at high speed. In the coming years, most vehicles will be equipped with an On-Board Units (OBU), Global Positioning System (GPS), Event Data Recorder (EDR), and sensors (radar) (Eze et al., 2016). These devices are used to detect congestion and traffic status. Then they will automatically take appropriate actions on the vehicle and transmit this information through Vehicle-to-Vehicle (V2V) or Vehicle-to-Infrastructure (V2I) within the vehicular network.

VANET aims to ensure safe driving by improving traffic flow and thereby significantly reducing car accidents. The latter is solved by providing the appropriate information to the driver or vehicle. Moreover, any alteration of this information in real time may cause a system failure affecting the safety of people on the road. To ensure the proper functioning of the system, it is imperative to secure this information, which makes it one of the top priorities for research.

The wireless network that has the greatest coverage to establish bidirectional communication is the cellular technology network, however, at least in Mexico the report figures show that on a national scale, Telcel provides 82.2% of guaranteed coverage in 2G, 86% in 3G and 77.7% in 4G, followed by AT&T Mexico, with 68.8% in 3G and 71.8% in 4G, while Telefónica Movistar has 53.3% in 3G and 45.8% in 4G. 82% of the Mexican territory has 2G service through Telcel. (CIAPEM - Comité de Informática de La Administración Pública Estatal y Municipal A.C., n.d).

2021 When observing the official maps of the cellular telecommunications service providers, it can be seen that there is a greater concentration in urban areas with multiple nodes, while the areas of non-coverage are comprised of isolated areas and road stretches, where there is a potential problem if accidents or emergency events occur.

According to the National Public Safety System (INSP) *(Instituto Nacional de Salud Pública, 2022*), up to 24 thousand deaths are registered annually due to automobile accidents, being the fifth cause of death in the general population and the first among young people (Luto Carretero: Los Accidentes Viales Más Trágicos Del 2021 - Infobae, n.d. 2021). Not only automobile accidents can occur in isolated areas, but also forest fires, road alterations such as frozen or slippery roads, collapse of a bridge, collapse of a hill, etc. An endless number of emergency or warning events can occur, of which it is convenient to know their occurrence and location in a timely manner.

VANET still has challenges ahead, a lot of work has been done to solve them and even more on security issues. The security messages are transmitted through an open wireless connection, which makes it easier to interfere and intervene than a wired network, it is vulnerable to various types of security attacks such as spoofing, modification, identity disclosure, *Sybil* attacks and so on. In VANET, although it is necessary to propagate emergency messages due to the occurrence of events in isolated areas, it is also dangerous to expose this information to malicious entities, or people who can abuse this essential information for drivers and users, as well as for official entities such as: police department, fire department, emergency medical services, civil protection, etc. Vehicles move fast (US: 70mph or 112 kph).

As a result, a VANET system needs to handle an environment where nodes within the network move at high speeds potentially entering and exiting the network very quickly (Shrestha *et al.*, 2018). Given this scenario the following questions arise.

ISSN: 2410-4000

How to provide confidentiality to messages, what security method is suitable for VANET requirements during the exchange of information between vehicles, what level of encryption is suitable when transmitting information between the vehicle to any entity of interest under a messaging protocol without having a delay affecting in unstable cellular signal areas?

In this sense, the contribution of our proposal is the development of an IoT system as a secure means of real-time communication of encrypted messages in VANET, in emergency scenarios, using the AES 128 algorithm and the MQTT protocol under a C-V2X architecture. The system is implemented in hardware, using ESP32 modules, and validated in low RSSI scenarios.

This paper is organized as follows: it consists of four sections, introduction, state of the art, method, results and conclusions.

II. State of the art

The messaging of information is what is going to determine the action by the authorities depending on the content of the message, therefore, how to be executed this action is fundamental. There are different related works regarding this problematic, (Nadezda, 2017) focuses on driving assistance applications and makes an exhaustive analysis based on simulations in his proposal. With the objective of evaluating MQTT and CoAP under different scenarios, (R. Tomar et al., 2020) builds an IoT architecture which is implemented in an ESP32 using MQTT messaging, in which different metrics of interest are obtained as results, among them the information sent and the time it takes, (Hussein & Shujaa, 2020), likewise uses the same messaging protocol to send encrypted messages in response of medical ambulance services. On the other hand, (R. and P. M. and S. H. G. Tomar, 2017) proposes an architecture that takes advantage of MQTT features such as quality of service, points out the null need for VANET infrastructure. In summary, what these papers have in common is how to employ MQTT as *multi-cast* messaging for the purpose of dispelling messages of an emergency or alert nature.

Security

MQTT has several security options in terms of authentication, authorization and data confidentiality. For authentication, it provides a simple authentication scheme through username and password fields in the login packet that a client can use to connect the intermediary, although authentication credentials are sent in plain text and some form of encryption must be used (Katsikeas *et al*., 2017).

Authorization in MQTT can be achieved using an access control list (ACL) on the *broker* side. The ACL contains permissions for users or system processes to grant access to objects, as well as allowed operations on particular objects. MQTT ACL contains all username and password pairs and topics that a client has publish and/or subscribe access to. Enhanced authorization features can be implemented in the broker in the form of add-ons or in the form of an additional web service. More sophisticated access control schemes can also be integrated into MQTT (Fysarakis et al., 2014), (Fysarakis *et al*., 2018). As for the confidentiality of MQTT messages, this can be achieved at the application layer by using payload encryption. For this encryption, any of the available encryption algorithms or authenticated encryption can be used, provided that there is support for the target devices.

IoT development hardware is viable for VANET applications, however, the implementation of encryption algorithms is one of the tasks that compromise the resources of the embedded hardware on the card itself, along with the task of establishing physical connection to the medium to be transmitted. Due to the work performed by these tasks it is important to consider the resources, for this we have different works where encryption algorithms are implemented in different development cards, (Singh *et al*., 2015) works with a SMQTT concept employing a key/text-encryption based encryption based on KP/AP-ABE attributes, using lightweight elliptic curve encryption, the implementation was done in *Raspberry pi*. In (Katsikeas *et al*., 2017) the authors conclude that authenticated payload cipher with AES-OCB is the most suitable for industrial applications, it was implemented on Zolertia Z1.

ISSN: 2410-4000

Meanwhile, in (De Santis *et al*., 2017) the authors propose an optimized implementation of ChaCha20 for ARM Cortex-M4 processors, performance evaluation shows that ChaCha20-Poly1305 ciphers are promising candidates for securing emerging IoT applications with low speed and space constraints. In (Sadio et al., 2019) similarly handles the ChaCha20-Poly1305 algorithm implemented on an Arduino one.

III. Methodology

Next, Figure 1 presents the methodological route followed for the development of the project, which is described in detail.

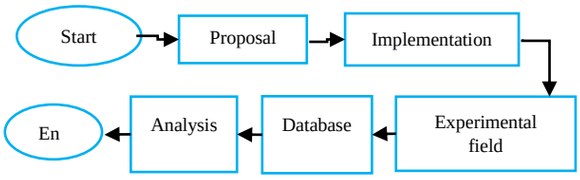


Figure 1 General diagram of the methodology used
Source: Own Elaboration

First, through an exhaustive bibliographic research on surveys of the main challenges in VANETS and a review of the state of the art, the project proposal was proposed, thus identifying the main VANET architectures and emerging technologies capable of supporting encryption algorithms.

The technologies to be used in the implementation are based on the proposal. Subsequently, the proposed system was implemented in hardware using ESP32 and GPS and GSM modules.

The system tests were performed by first evaluating the operation of the embedded system locally, then the complete IoT system was validated, implementing different services on the server to establish communication between client and server.

Finally, tests were performed in a real scenario, measuring the performance of the system in the road section from Cd. Obregón to Mochis, in order to evaluate the system with different RSSI. Finally, the results obtained during the tests are analyzed and the project is documented.

IV. Development

A. Proposed architecture

In this work, an IoT system is proposed to establish a secure and real-time communication of encrypted messages for VANET in emergency scenarios, which integrates three technologies as shown in Figure 2.

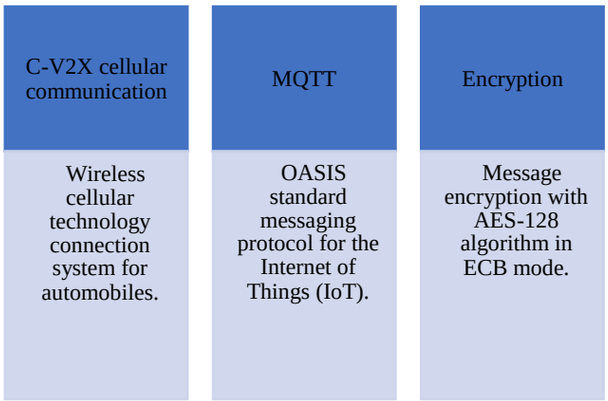


Figure 2 Main stages of the proposed architecture
Source: Own Elaboration

– CV2X is used to transmit emergency messages to the corresponding entity (such as police, ambulance, fire department, etc.) and then propagate the message to potentially affected vehicles, in order to cover areas with low signal strength (low RSSI). The vehicles are considered to be covered by the 2G GSM cellular network as it has the longest range. In addition, it is important to mention that the message requirements will depend on the type of emergency. That is to say, within the message payload, the alert message varies, where it can symbolize any type of emergency alert, from an object on the road to an accident requiring immediate intervention.

– MQTT is used as an IoT-oriented messaging protocol, which is designed as an extremely lightweight publish/subscribe messaging transport, ideal for connecting remote devices with a small code footprint and minimal network bandwidth. Such a protocol is intended to efficiently send messages to monitor vehicle location and possible emergency alert, while securing the message with payload encryption.

ISSN: 2410-4000

- Finally, an encryption method is used to give confidentiality to the messages emitted by MQTT, with the purpose of hiding sensitive information such as the global positioning coordinates of the vehicle. Some features of AES (Al-Mashhadani & Shujaa, 2022):
- It is used in messaging applications such as *Signal* and *Whatsapp*, computing platforms such as VeraCrypt, and other commonly used technologies.
- The AES algorithm is trusted as a standard by the U.S. government as well as many institutions.
- AES is the most widely used and popular today.
- In terms of cyber security, AES is the most widely accepted encryption standard in the world.
- Figure 3 describes the proposed system architecture, which integrates the technologies described above in addition to the server. A detailed description of each of its component elements follows.

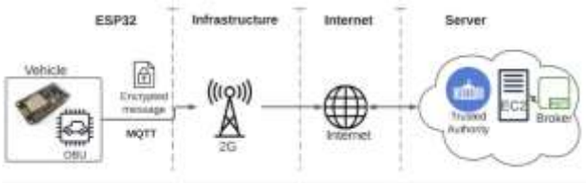


Figure 3 General architecture
Source: Own Elaboration

- ESP32: The first block refers to the identity of the car, which is equipped by the OBU unit with the characteristics of Table 1. This is the point where the information starts by obtaining the RSSI and GPS information from their respective modules, to be processed and published by the MQTT protocol once encrypted.
- Infrastructure: the second block is made up of the structure that refers to the RSU in a VANET environment, it depends on the existing infrastructure provided in this project by TELCEL, which achieves the connection to the Internet.
- Internet: the third block is the integration of the internet network in both points of the system (Device - Server) establishing the TCP-IP protocol with which MQTT works.
- Server: established by IaaS service with the characteristics of Table 2, subscribed to the corresponding topics of MQTT, when the information arrives at this point, thanks to the cloud computing features, the possibilities regarding the management of the received information increase conveniently, whether you want to do broadcasting message or send to specific points depending on the issued alert and its needs.

OBU	
ESP32 (CP210x)	ESP32 Wi-Fi/Bluetooth module, Two cores. *http://esp32.net/)*
Sim800L GSM Module V2	SIM800L v2.0 module is a GSM and GPRS 4-band device for sending and receiving SMS messages and calls, or having mobile data network and internet via GPRS.
Neo6mv2 GPS module	This GPS module has an integrated antenna and EEPROM, is highly accurate and very simple to use.

Table 1 OBU Resources
Source: Own Elaboration

EC2 AWS (Iaas) Server		
Hardware	Processor	Intel Xeon ES-2676 2.4GHz
		64Gb
	RAM	2 Gb
Software	Operating system	Ubuntu Server 18.04 LTS

Table 2 Server resources
Source: Own Elaboration

B. System Implementation

The following is a description of how the system was implemented in the ESP32 module and the MQTT server, as well as a detailed explanation of the processes programmed in these modules (Figure 4 and 5).

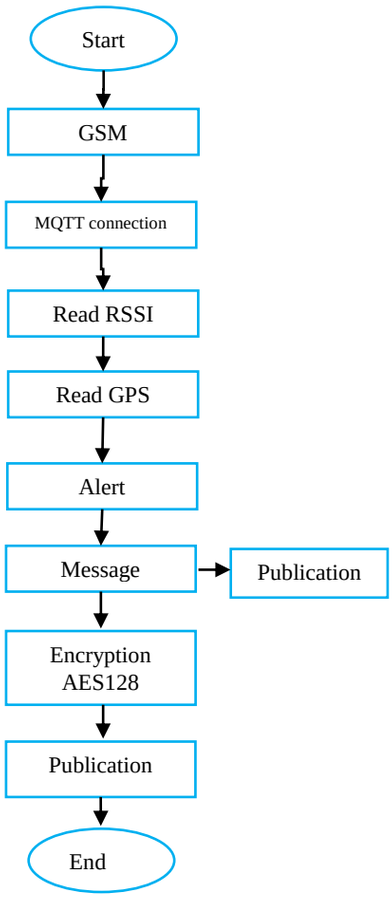


Figure 4 ESP32 logic diagram
Source: Own Elaboration

Algorithm in ESP32

First the embedded device configurations are initialized, as for MQTT it is given its connection credentials with the server and in turn the SIM800L unit is configured with its corresponding libraries. The GPS information is read through functions and the GSM module reads the RSSI through AT commands. Once this information is ready, the structure of the unencrypted message is formed (example: *RSSI:22,lat:27.321077,lon:-09.721893,Alert:1*), a bus for the message payload of 40 bytes is given, once the message is published under the mentioned topic. The encryption is done in four parts where each one is a separate variable (this is done in order to take advantage of the 16 native bytes of the algorithm) and they are put together to make a single publication requiring a bus of 129 bytes to send the complete encrypted message. Once the last process is done, the system enters a return cycle towards the reading of the values until the publication of the encrypted message.

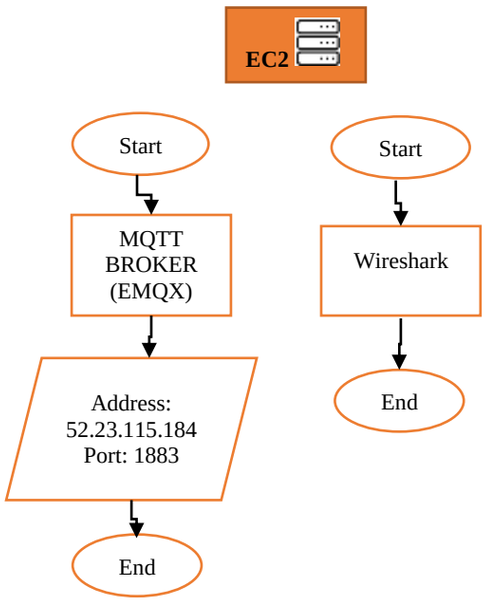


Figure 5 Processes executed per server
Source: Own Elaboration

Server: The server is in charge of three tasks:

1. Establish the broker.
2. Sniffing with the wireshark tool during the experimentation period to perform the analysis with the collected information.

To manipulate the hardware and software of the server, the SSH protocol is used, and also the FTP protocol to download the analysis data sheet.

VI. Results

The experimentation is carried out in a strategic road section where signal strength values of any magnitude can be shown. Figure 6 (*Coverage Map - Corporate | Telcel World, 2022*) shows the 2G coverage map, denominated by the company as yellow zones where there is no guarantee of communication and green zones of guarantee determined by the infrastructure.

As performance metrics of the proposed system, the throughput known as the ratio between transmitted information and received information; and packet errors are used.

ISSN: 2410-4000

Figure 6 Experimental field
Source: (Coverage Map - Corporate | Telcel World, 2022)

Encryption

The AES-128 algorithm was implemented independently in ECB block mode to test the behavior of the embedded device.

The encryption algorithm with a 16-byte private key and a payload of the same size resulted in an average time of 30.5ms.

Measurement tool for communication.

To obtain the communication metrics, sniffing was done with the protocol analysis tool Wireshark, which was seated inside the server and intercepted the communication packets via MQTT published by the ESP32 during the experimentation period.

RSSI during the run

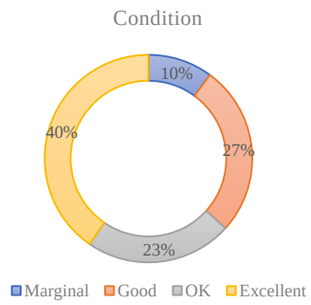
A distance of 266 km was covered with a duration of approximately 3h 12min, during which time the ESP32 was in operation and during which time the network traffic of the server was monitored.

During the experimentation, the following RSSI values were obtained, shown in Figure 8, for the SIM800L module, referring to the values tabulated in Table 3 of (AT+CSQ - Signal Quality | M2MSupport.Net, n.d. 2022).

Value	RSSI dBm	Condition	Value	RSSI dBm	*Condition*
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			

Table 3 RSSI values through AT commands by GSM module
Source: (AT+CSQ - Signal Quality | M2MSupport.Net, n.d.)

The minimum RSSI value recorded with which it was possible to send the message is four (Marginal), the maximum value obtained was 30 (Excellent), giving an average of 18 over the entire route.



Graph 1 RSSI values
Source: Own Elaboration

The signal with which the GSM module operated was of excellent quality in most of the route, on the other hand, marginal RSSI values where the module was able to transmit information occurred less frequently, the other conditions: "OK" and "Good" were presented in a similar way Figure 9 in which 1836 rows of data are recorded. The route began its journey from the exit of the city of Obregon Sonora, to the beginning of the square of the city of Los Mochis Sinaloa. The GPS information depended on the GSM module to be transmitted, while this module is with established link to the internet, the periods of time in which the GSM does not establish connection were present in the route since it depended on the infrastructure of the cellular connection service provider in this case TELCEL under its 2G signal emitters.

ISSN: 2410-4000

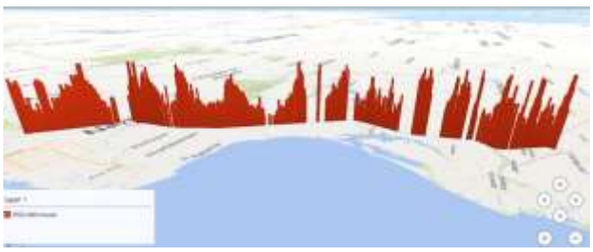


Figure 7 Map drawn by the information received from the GPS module
Source: Own Elaboration

Two MQTT topics were established with QoS(0), "msj_secure" and "msj_not_secure". The first topic is given with the purpose of obtaining the information without encryption for monitoring purposes since this project does not cover the decryption part (Figure 10).

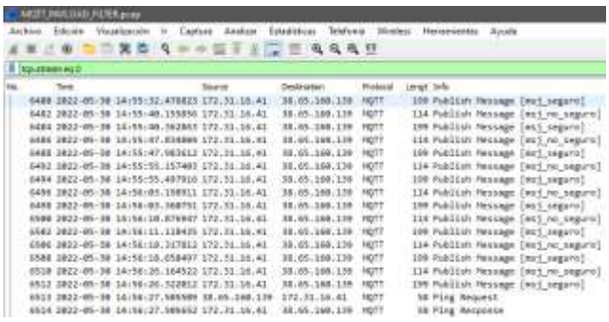


Figure 8 Server network traffic analysis.
Source: Own Elaboration

Two patterns are identified in the graph in Figure 11, where the information packets arrive at two over seconds, and where they arrive at four over seconds, this is because the data is sent by two topics, in the "msj_no_secure" one there is a 40-byte bus to send the plain text with the unencrypted information, while in "msj_secure" the bus is 129 bytes where the encrypted information travels.

Also in the lower ridges we can see the operation of the keep alive, a method belonging to the MQTT protocol to identify the existence of connection with the client. These two patterns mentioned above denote a behavior where the transmitted packets use a minimum of bandwidth in the communication despite a constant update of the data.

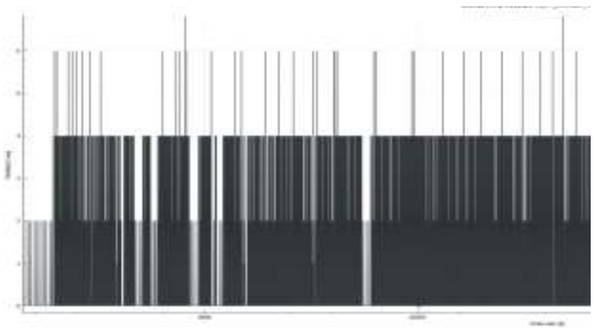


Figure 9 Input-output statistics
Source: Own Elaboration

With the *Endpoints* tool displayed in Figure 12, the ESP32 and the server with their respective IP addresses. There were 3,886 packets transmitted by the ESP32 and 3,328 packets received by the server, a *troughtput* of 85.64%.

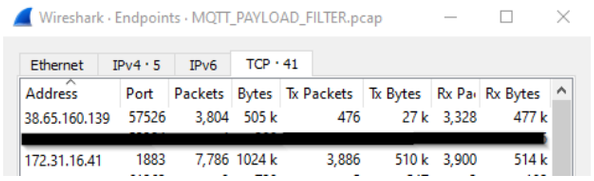


Figure 10 Received-transmitted packet analysis
Source: Own Elaboration

In the prototype model, the components or modules with their respective antennas that make up the embedded system are mounted on an experimental board (Figure 13).

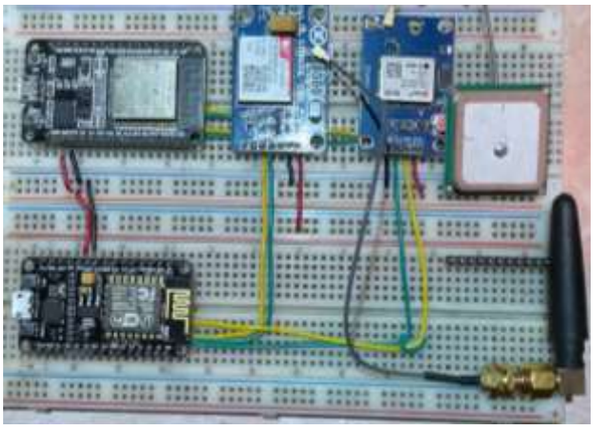


Figure 11 Experimental hardware prototype
Source: Own Elaboration

It is worth mentioning that the previous figure shows an ESP8266 board that was not used and was intended as a backup board.

Conclusion

A secure system was developed that granted confidentiality to messages with emergency nature in vehicles under a C-V2X system. The communication between vehicle and internet was established through the MQTT messaging protocol by the ESP32. This ensures the transmission and reception of messages between V2V, V2I and other units. An efficient response time was achieved, without deviating from the requirements demanded by emergency events. In addition, thanks to MQTT, a minimum use of bandwidth over the communication medium was demonstrated.

The GSM module was able to establish stable communication in a wide range of values even in conditions of low RSSI level and even null level, this was present in all the evaluated route. Although AES-128 in its ECB mode is not advisable to use since it results in evident patterns in the messages, it remains as future work to improve its structure and operation mode, as well as the security scheme to provide other pillars of computer security.

Funding

Funding: The present work has been funded by CONACYT. CVU: 1076458

References

Al-Mashhadani, M., & Shujaa, M. (2022). IoT Security Using AES Encryption Technology based ESP32 Platform. *International Arab Journal of Information Technology*, *19*(2), 214–223. https://doi.org/10.34028/iajit/19/2/8

AT+CSQ – Signal quality | M2MSupport.net. (n.d.). Retrieved June 13, 2022, from https://m2msupport.net/m2msupport/atcsq-signal-quality/

CIAPEM 2021 – Comité de Informática de la Administración Pública Estatal y Municipal A.C. (2021). 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., Soultatos, O., Manifavas, C., Papaefstathiou, I., & Askoxylakis, I. (2018). XSACd—Cross-domain resource sharing & access control for smart environments. *Future Generation Computer Systems*, *80*, 572–582. https://doi.org/10.1016/j.future.2016.05.023

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. (2022). 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. (2021). https://www.infobae.com/america/mexico/2021/12/27/luto-carretero-los-accidentes-viales-mas-tragicos-del-2021/

Mapa de Cobertura - Corporativo | Mundo Telcel. (2022). 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