

MECANISMO DE SEGURIDAD ORIENTADO A MENSAJERÍA CIFRADA V2V BASADA EN MQTT

**TESIS**

QUE PARA OBTENER EL TÍTULO DE

**MAESTRIA EN CIENCIAS DE LA INGENIERIA**

PRESENTA

**Francisco Antonio Palos Angulo**

CIUDAD OBREGÓN, SONORA

AGOSTO DE 2022

**AGRADECIMIENTOS**

**ÍNDICE GENERAL**

[RESUMEN 2](#_Toc97042811)

[CAPÍTULO I. INTRODUCCIÓN 3](#_Toc97042812)

[1. Antecedentes 3](#_Toc97042813)

[2. 1.2 Planteamiento del problema 5](#_Toc97042814)

[3. 1.3 Objetivo 6](#_Toc97042815)

[4. 1.5 Justificación 7](#_Toc97042816)

[1.6 Delimitaciones 8](#_Toc97042817)

[1.7 Limitaciones 9](#_Toc97042818)

[CAPÍTULO II. ESTADO DEL ARTE 10](#_Toc97042819)

[2.1 Características y restricciones de VANET 11](#_Toc97042820)

[2.2.1 Características importantes en redes y comunicaciones 11](#_Toc97042821)

[2.2.2 Características de VANET relevantes para vehículos y conductores 12](#_Toc97042822)

[1. 13](#_Toc97042823)

[2. 2.2 Ciberseguridad 13](#_Toc97042824)

[2.1. 2.2.1Pilares de la seguridad 13](#_Toc97042825)

[2.2. 2.1.2 Ataques y vulnerabilidades 13](#_Toc97042826)

[3. 2.3 Protocolos de internet de las cosas 14](#_Toc97042827)

[4. Ataques () 15](#_Toc97042828)

[5. METODOS (inteligencia artificial, algoritmos) 15](#_Toc97042829)

[6. Cifrado (meto lo de encriptado ligero) 15](#_Toc97042830)

[7. Algoritmos de ruteo 15](#_Toc97042831)

[8. Protocolo MQTT 15](#_Toc97042832)

[8.1. Protocolos de comunicación 20](#_Toc97042833)

[CAPÍTULO III. MÉTODO 22](#_Toc97042834)

[CAPÍTULO V. RESULATDOS. 22](#_Toc97042835)

[CAPÍTULO VI. CONCLUSIÓN 22](#_Toc97042836)

[BIBLIOGRAFÍA 22](#_Toc97042837)

**LISTA DE FIGURAS**

**LISTA DE TABLAS**

RESUMEN

# INTRODUCCIÓN

En este capítulo se presenta la propuesta de investigación. Inicialmente se describen los antecedentes de la investigación, puntualizando el contexto donde se presenta el problema; se define claramente el problema a afrontar, así como el objetivo propuesto. Posteriormente, se justifica el desarrollo del proyecto, indicando los beneficios del mismo. Por último, se establece el alcance y las limitantes de la investigación.

## Antecedentes

Durante los últimos 10 años, la industria automotriz ha atravesado un período de inmensa agitación. Los modelos de negocio tradicionales, las cadenas de suministro y los actores del mercado establecidos se ven desafiados por una ola de nuevos participantes que están sacudiendo el mercado. Este trastorno ha sido causado por varias tendencias que afectan a la industria, incluida la aparición de vehículos autónomos, el crecimiento de la movilidad compartida y la electrificación de la red de vehículos. Si bien cada uno de estos ha jugado un papel importante en desestabilizar el mercado, la mayor disrupción probablemente se pueda atribuir a otra tendencia: la tecnología conectiva. Ya sea completa o semiautónoma, híbrida o eléctrica, compartida o personal, se espera que la conectividad sea la característica definitoria del "automóvil del futuro" [1].

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 [2].

Algunas compañías automotrices ya están interesadas en integrar “VANET-ENABLE” a sus vehículos y han proporcionado financiación para mejorar la investigación. *Ford* planea lanzar vehículos capaces de comunicarse con cualquier otro dispositivo en el área, mientras que “*Applied Information”* planea implementar productos de infraestructura de tráfico dentro de los EE. UU. para que los vehículos con estas capacidades puedan beneficiarse de los servicios VANET [3]. Ford no está solo en estas aspiraciones, ya que General Motors ya ha instalado algunos dispositivos V2V en sus Cadillac y Toyota tiene planes de hacer lo mismo para todos sus vehículos en 2024 [4].

VANET (Vehicular Ad hoc Network) se ha convertido en una de las más prometedoras y de desarrollo más rápido de las redes móviles ad-hoc (MANET: Mobile Ad-hoc Network) incluyendo vehículos inteligentes, unidades de carretera (RSU: *Road side unit* por sus siglas en inglés) y unidades a bordo (**OBU**: *On-Board Units* por sus siglas en inglés) que se comunican a través de redes inalámbricas volátiles. La investigación actual en la industria de los vehículos y las innovaciones en medios de transmisión junto con las notables administraciones de portabilidad multimodal aceleraron los ITS (“Intelligent Transport Systems”) centrales, de los cuales VANET aumentó considerablemente la atención.

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.

La seguridad es un tema importante en las VANET, como resultado del efecto que las amenazas y vulnerabilidades pueden tener en la conducta y la satisfacción personal del conductor. La seguridad es dar la condición de estar libre de peligro o amenaza; también se puede definir mediante un conjunto de medidas que se consideran seguras o protegidas [2]. La seguridad implica protección, así como las medidas tomadas para estar seguro o protegido. Por ejemplo, para proporcionar la seguridad adecuada para un desfile, los funcionarios de la ciudad a menudo contratan guardias adicionales. En VANET, es fundamental protegerse contra las actividades de uso indebido y definir con precisión la arquitectura de seguridad porque es una comunicación inalámbrica que es más difícil de proteger. La seguridad y el nivel garantizado de implementación afecta la seguridad de las personas.[5]

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.

## Planteamiento del problema

**El estado actual de 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.

**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 [6].

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) [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 o alerta, eventos los cuales resultan convenientes hacer saber de su existencia y ubicación.

Sin embargo, así como de igual manera es necesario propagar los mensajes de índole descrita anteriormente, de igual manera 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.[3]

En este contexto. ¿Cómo brindar integridad a los mensajes?, ¿Se puede logar tener un método de seguridad bajo las características de VANET sin perder eficiencia en el intercambio de información? ¿Qué nivel de cifrado es 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?

## Objetivo

### Objetivo general

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 aun en zonas de poca cobertura dando integridad a los mensajes transmitidos a través de un protocolo de mensajería con funcionalidades adecuadas a VANET.

### Objetivos específicos

* Desarrollar un esquema de seguridad que brinde integridad, confidencialidad y autenticación en los mensajes a transmitir.
* 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 eventos de emergencia necesiten.

## Hipótesis

Dado a la naturaleza ligera del protocolo de mensajería MQTT se espera cumplir con un cifrado robusto en el mejor de los casos y en el peor escenario que pueda manejar un algoritmo de cifrado ligero. También se pronostica que el tiempo de transmisión/ recepción no se aleje mucho de lo que la necesidad de la emergencia nos permite.

## Justificación

Dado la naturaleza de la red ad-hoc en donde VANET se desempeña, se está en constante volatilidad en cuanto ruteo de comunicación, así como también un constante cambio de dispositivos a comunicar, al siempre estar buscando la ruta más rápida para establecer comunicación, entonces hay menos tiempo para reacción o procesamiento de métodos de seguridad.



Figura . Mapa cobertura 4G (LTE) TELCEL sector noroeste de México [6].



Figura . Mapa cobertura 4G (LTE) TELCEL sector noroeste de México [6].

Al tener zonas denominadas por las compañías proveedoras de servicio como zonas de no garantía, es decir: zonas donde la conexión a internet mediante 3G o 4G no son estables, estos puntos se presentan a través de tramos carreteros como se ve en las anteriores dos figuras, la carretera internacional México 15 siendo de las más importantes del país se puede apreciar que sufre problemas de incomunicación, sea carretera internacional o no el peligro es inminente para los conductores, se corre el riesgo de perder comunicación paulatinamente a medida que se aleja de la infraestructura, sin mencionar zonas de puntos muertos de señal en carretera.

El método empleado en este proyecto, tendrá un impacto directo en la seguridad de los conductores bajo escenarios de señal inestable o zonas de no garantía. El tiempo que transcurre al salir de un nodo de infraestructura a otro podrá ser determinante, ya que, dependiendo de la velocidad del conductor, así como se aleja paulatinamente del nodo, puede llegar a un punto muerto donde la conexión se pierde por completo, de igual manera al entrar a la cobertura del nodo más cercano donde la señal empieza de menos a más. En estos dos periodos si no se garantiza una comunicación segura pueden subyacer diferentes consecuencias: como lo son tiempos de respuesta de parte de las autoridades o del conductor, esto con la misión de prevenir o actuar en lo ocurrido, así como también la exposición de información potencialmente peligrosa dado a la naturaleza de estos escenarios en manos de una entidad maliciosa que se aproveche de la carencia de autenticidad, integridad y confidencialidad, se puede interceptar la información en el medio vulnerable donde la amenaza puede escalar aún más.

## Delimitaciones

El proyecto cubre la parte de comunicación entre vehículo e internet, esto es considerando que la información que se establezca una vez en la nube, puede transmitirse a diferentes puntos o establecer un enlace *multicast* o *broadcast*.

Parámetros como procesamiento, tiempos de respuesta, consumo de recursos, calidad de la señal recibida, es objeto de estudio solo en la parte del dispositivo embebido, ya que se considera que el hardware que involucran estos procesos estará dentro del OBU del vehículo.

## 1.7 Limitaciones

* Tiempo limitado a agosto 2022.
* No se consideran experimentaciones con datos simulados o emplear algún paquete de simulación.
* La implementación experimental solo cubre ciertas zonas de interés en un tramo carretero.
* La velocidad del vehículo no se tendrá a consideración de manera analítica, ya que este parámetro no lo podemos controlar.

# ESTADO DEL ARTE

El estado del arte para la presente tesis se divide en cuatro subsecciones, ya que hay varias metodologías y tecnologías involucradas en temas de seguridad en VANET: i) Ciberseguridad: se analizan varios trabajos a través de sus esquemas, tipos de implementación, ataques, vulnerabilidades, ii) técnicas de manejo de mensajería: se estudian varios métodos a través de su tipo de implementación ya sea *Machine Learning* o diferentes algoritmos, herramientas de simulación y métricas reportadas, iii) Protocolos de comunicación: se analizan diferentes protocolos para aplicaciones con red “*ad-hoc*”.iv) algoritmos de cifrado: se analizan diferentes algoritmos de encriptación con aplicación en VANET o de campo relacionado, mecanismos para su utilización, v) Características y restricciones de VANET: se analizan diferentes puntos que conforman el entorno VANET así como también restricciones físicas que se tienen que contemplar.

Debes explicar como está estructurado el capítulo en el mismo orden que lo presentas, traes un desorden solo copy and paste, nada de análisis y críticas al estado del arte.

## VANET

En este punto se definen los conceptos y características que intervienen en el tema, así como también diferentes implicaciones

Una red ad-hoc vehicular, habitualmente referida por su acrónimo en inglés VANET, es un tipo de red de comunicación que utiliza a los vehículos como nodos de la red

* Red ad-hoc:
  + MANET: (*Mobile Ad-hoc Networks*) are temporarily established, self-organized, and maintained networks used for communication from source to the destination node
    - VANET: Vehicular ad-hoc Networks:

### Arquitectura VANET

VANET tiene un poco de acceso a la infraestructura de red y ofrece múltiples servicios. La Figura 1. Muestra los modos de comunicación vehículo a vehículo (V2V), vehículo a infraestructura (V2I) o híbrido. En V2V, los medios de comunicación utilizados se caracterizan por una latencia corta y una alta velocidad de transmisión. Esta arquitectura se utiliza en diferentes escenarios de emisión de alertas (frenado de emergencia, colisión, desaceleración, etc.) o conducción cooperativa. En V2I, la red vehicular tiene en cuenta las aplicaciones que utilizan los puntos de infraestructura RSUs que multiplican los servicios a través de portales de internet en común [9].

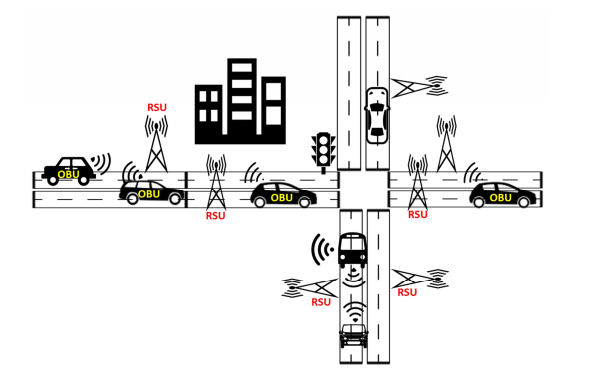


Figura . Elementos que componen una arquitectura VANET

En la figura anterior se ilustra la interacción entre los diferentes elementos los cuales son: RSU, OBU. Estos elementos logran la comunicación vehículo a vehículo en donde OBU es el protagonista, así como también se logra la comunicación vehículo a infraestructura donde RSU Y OBU comparten información.

### Características importantes en redes y comunicaciones

Para establecer comunicación entre unidades, es necesario generar una red, para lograr esto se deben considerar diferentes características, ya que no es igual establecer una red orientada a sensores, a establecer una red inalámbrica donde los las unidades crean nodos en movimiento. Por lo tanto, en aplicación VANET se consideran las siguientes características.

* **Red ilimitada y escalable**: VANET se puede implementar para una o varias ciudades, incluso para países. Esto requiere cooperación y gestión para los requisitos de seguridad.
* **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. Esto mejora la privacidad del nodo y causa desconexión frecuente, volatilidad y la imposibilidad de *Handshake* es decir establecer un intercambio de información.

Bajo estas limitaciones, debe respetarse el retraso en la difusión de la alerta. Se necesita un buen rendimiento de retardo mediante el uso de un algoritmo criptográfico rápido o mediante la autenticación de entidades y la entrega de mensajes a tiempo. Para ello, la priorización de los paquetes de datos y el control de la congestión es de mayor importancia; los datos relacionados con la seguridad y la eficiencia del tráfico deben ser más rápidos que los demás. [9,10].

### Características de VANET relevantes para vehículos y conductores

El vehículo es la entidad donde se llevan a cabo los procesos de información que el conductor o usuario le adjudique, pero esta entidad debe de cumplir con ciertas tareas las cuales contemplan entornos físicos y al mismo tiempo manejar parámetros confidenciales. Contemplando lo anterior mencionado se consideran las siguientes características.

* **Alta potencia de procesamiento y energía suficiente**: los nodos VANET no tienen problemas de energía y recursos de computación. Su fuente de potencia se da en forma de baterías y alta capacidad de cálculo para ejecutar cálculos criptográficos complejos.
* **Mejor protección física**: los nodos VANET están físicamente mejor protegidos. Es más difícil comprometerlos físicamente. Esto reduce el efecto de los ataques a la infraestructura.
* **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. Se utiliza un GPS a prueba de manipulaciones para la localización segura para proteger la ubicación de los nodos contra los atacantes.
* **Infraestructura de aplicación de la ley existente**: A través de los agentes de la ley, pueden atrapar al adversario que atacó el sistema.
* **Registro central con mantenimiento e inspección periódicos**: Los vehículos están registrados ante la Autoridad Central (CA) y tienen una identificación única (matricula de circulación vehicular). Los vehículos se mantienen periódicamente para actualizaciones de *firmware* y *software*. En PKC (*Public Key Cryptography*), el mantenimiento es para actualizar certificados y claves y para obtener CRL (*Certificate Revocation List*) nueva.

Brevemente, la red vehicular es una interacción entre el comportamiento y la cooperación de los conductores, la red y la infraestructura. Cualquier solución de seguridad potencial debe encontrar un compromiso para involucrar a todas las partes dentro de ella.

### **Avances en el estado del arte**.

En esta sección se abordan los diferentes avances en cuanto a VANET en general. Los principales avances que se tienen son en cuanto estandarizaciones estipulados en la IEEE, estándares en la capa física (señales de medio inalámbrico), esquemas de funcionamiento, etc.

#### Estándares

|  |  |  |
| --- | --- | --- |
| Referencia | Técnica | Resultados |
|  |  |  |

Aquí presentar DSRC y sus limitaciones

## Ciberseguridad orientada a VANET.

La ciberseguridad es un tema fundamental, ya que la seguridad que se desarrolla en este proyecto gira en torno a la ciberseguridad ya que el prefijo “ciber” se concentra en proteger la red, datos e información, aunque existen muchas definiciones al respecto y conceptos muy similares como por ejemplo seguridad informática, sin embargo todos tienen el mismo objetivo: preocuparse por tener entendimiento acerca de posibles amenazas de seguridad, vulnerabilidades de sistema y riesgos de seguridad, para así poder dar respuesta a lo anterior mencionado [12]. Por lo tanto, en relación a los tópicos que intervienen en este proyecto es adecuado establecer la ciberseguridad como las actividades necesarias para proteger las redes y los sistemas de información, los usuarios de dichos sistemas, y otras personas afectadas por ciber amenazas[13].

### Pilares de la seguridad

En seguridad, hay cuatro aspectos básicos que deben considerarse: confidencialidad, autenticación, integridad y no repudio, que se describen a continuación.

**Confidencialidad**: es el servicio que permite mantener la información en secreto, de tal manera que sólo los usuarios autorizados puedan manipularla, utilizando técnicas de cifrado y codificación de datos; dichos usuarios pueden ser personas, procesos, programas, etc.

**Autenticación**: este servicio confirma que alguien es quien dice serlo, utilizando por ejemplo biométricas (huellas dactilares, retina, voz, etc.), certificados digitales o Códigos de Autenticación de Mensajes (MAC).

**Integridad**: en este servicio, se asegura que la información transmitida no ha sido modificada por un tercero, utilizando generalmente firmas digitales, lo que implica una función hash aplicada al mensaje, donde el currículum generado se envía a lo largo del mensaje original.

**No repudio:** el servicio ofrece una prueba de que, en el lado emisor, la información ha sido entregada, y recibida, respectivamente.

### Ataques y vulnerabilidades en VANET

El principal problema de seguridad es cómo hacer que los canales de comunicación V2V y V2I sean seguros. Un buen enfoque para la seguridad debe proporcionar servicios de alta calidad en términos de disponibilidad, confidencialidad, autenticación, integridad y no repudio [14]. Privacidad: Privacidad significa que solo las personas dedicadas en VANET deben tener derecho a acceder y controlar la información del vehículo. Confianza: En VANET, la gestión de la confianza se ocupa de cómo un vehículo puede confiar en otros vehículos y los mensajes recibidos

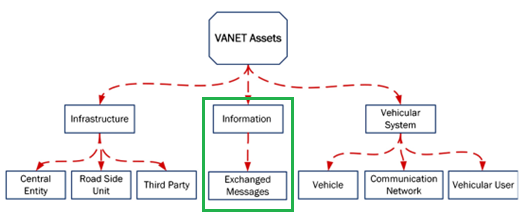


Figura . Activos en arquitectura VANET.

La información que se transmite/recibe es el principal activo a brindarle seguridad como lo vemos en la figura anterior marcada con verde, este se va a dar a través del intercambio de mensajes V2X. Sin embargo la infraestructura y el sistema vehicular son los dos puntos de trayectoria de la información.

Características únicas como la alta movilidad y volatilidad que tiene VANET lo han hecho vulnerable a varios tipos de ataques externos e internos. Estos ataques han causado tres preocupaciones principales en el diseño de seguridad en VANET: seguridad, privacidad, confianza [15].

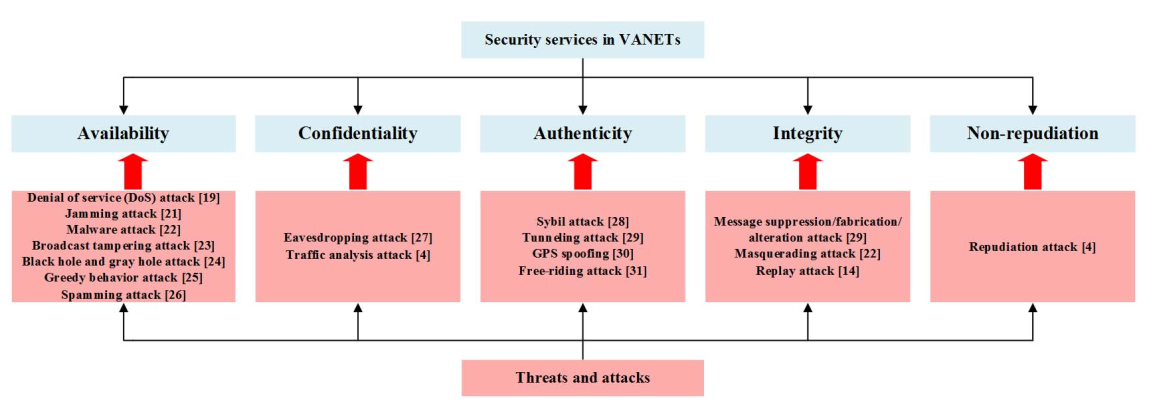


Figura . Servicios de seguridad en VANETs.

Proteger VANET de los ataques de vehículos maliciosos debido a la naturaleza dinámica de la formación de la red. Algunos de estos ataques pueden ser llevados a cabo por nodos dentro de la red (es decir, nodos que ya han sido autorizados para ser miembros de VANET); Otros ataques pueden ser llevados a cabo por vehículos que no pertenecen al VANET. Entre los tipos de ataques existentes más comunes:

* Suplantación de mensajes
* Reproducción de mensajes
* Integridad de mensajes
* Suplantación de identidad,
* Denegación de servicio (DoS)
* Seguimiento de movimiento

De los ataques más importantes a considerar en este proyecto es el de integridad, suplantación, reproducción de mensajes y manipulación de difusión.

## Protocolos de interés.

Haciendo referencia al modelo OSI y al modelo que emplea el internet moderno: TCP/IP, conceptos relacionados a VANET donde ya se ha dado un extenso seguimiento y su uso ha madurado, como lo es internet de las cosas donde se puede aprovechar las características que lo conforman: distribución masiva de mensajes, cobertura de red extensa, alta generación de nodos de comunicación, entre otras.

### Protocolos utilizados en internet de las cosas

Los protocolos de IoT se pueden dividir en cuatro categorías básicas que son: aplicación, descubrimiento de servicios, infraestructura y otros protocolos influyentes [14]. La Tabla i muestra los protocolos estándar de IoT más destacables:

Protocolo de aplicación restringida (CoAP): Este protocolo tiene como objetivo permitir que los dispositivos pequeños con baja potencia, computación y capacidades de comunicación compartan y conmuten entre sí. Transporte de telemetría de cola de mensajes (MQTT): MQTT utiliza el patrón de publicación-suscripción para proporcionar flexibilidad y simplicidad de transición. Consta de tres componentes básicos, suscriptor, editor y corredor.

Protocolo extensible de mensajería y presencia (XMPP): es una comunicación en tiempo real y se utiliza para llamadas multimedia. Es compatible con un protocolo de mensajería abierto, seguro, libre de spam y descentralizado. *Advanced Message Queue Protocol* (AMQP) es un protocolo de capa de aplicación estándar abierto para IoT que se centra en entornos orientados a mensajes. Su soporte de comunicación confiable a través de la entrega de mensajes garantiza primitivas que incluyen como máximo: una vez, al menos una vez y exactamente una entrega.[15]

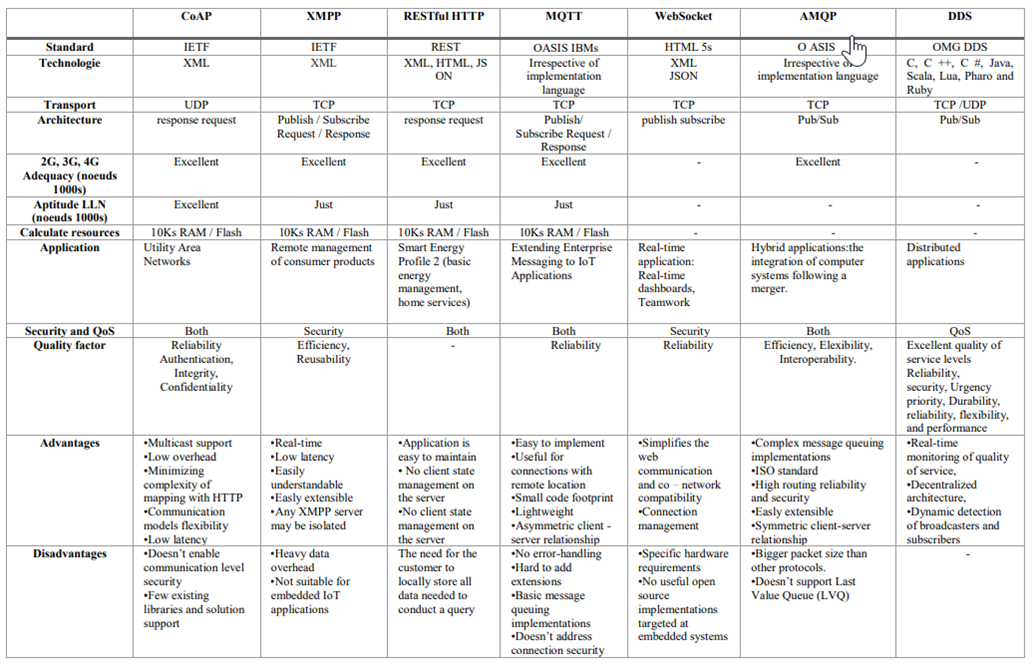
Tabla . Protocolos estándar para internet de las cosas

|  |  |  |
| --- | --- | --- |
| Protocolo de aplicación | CoAP DDS  AMQP    MQTT  MQTT –SN  XMPP  HTTP REST | |
| Descubrimiento de servicio | MDNS DNS-SD | |
| Protocolo  de  infraestructura | Protocolo de enrutamiento | RPL |
| Capa de Red | IPV4/IPV6 |
| Capa de enlace | IEEE 802 .15 .4 |
| Capa física (dispositivo) | LTE-A EPC global IEEE 802 15.4 Z-wave |
| Capa influyente | IEEE 1888.3. IPSec IEEE 1905.1 | |

En la Tabla i se muestran diferentes tipos de protocolos organizados mediante capas, en la capa de aplicación tenemos las más comunes que se utilizan en internet de las cosas, en los protocolos de infraestructura se sitúan estandarizaciones típicas en redes inalámbricas subyacentes a IEE 802.p.

#### Protocolos en la capa de aplicación

Es el séptimo nivel del modelo OSI y el cuarto de la pila TCP/IP. Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos. La capa de aplicación es utilizada por el software del usuario final, como los navegadores web y los clientes de correo electrónico. Proporciona protocolos que permiten al software enviar y recibir información y presentar datos significativos a los usuarios.



En esta tabla, se comparan los existentes protocolos en la capa de aplicación IoT que se utilizan para conectar dispositivos, pero también el usuario en aplicaciones a Internet. Cada protocolo de aplicación de IoT tiene sus propias ventajas y desventajas. Como ahora mencionado, la selección del protocolo de aplicación es completamente dependiendo de la aplicación. Comenzando con Criterios de Transporte entre ellos, se identifica a CoAP y DNS como los únicos que se ejecuta sobre UDP, lo que lo convierte en el más ligero los otros protocolos usan TCP. Arquitectura de publicación/suscripción que utilizado por *WebSocket*, AMQP y DDS es más adecuado para el IoT que solicitud/respuesta de CoAP y RESTful HTTP, otros protocolos mencionados utilizan ambos tipos de arquitectura, los protocolos que brindan seguridad y QoS son CoAP, RESTful HTTP, AMQT, MQTT [16].

## CV2-X

¿Porque CV2X? tiene mayor cobertura y mejor en casos de mensajes broadcast

Tanto para DSRC como para CV2-X comparten similitudes gracias su red de área inalámbrica, esta naturaleza de red implica una vulnerabilidad considerable y de aquí se desglosan los siguientes ciber ataques posibles.

**Packet Sniffing**

Las redes están diseñadas para facilitar y acelerar el tráfico de información. Para lograr este objetivo, la información se envía en paquetes a través de redes cableadas e inalámbricas. Debido a la naturaleza de las redes inalámbricas, estos paquetes se envían a través del aire. Como resultado, es muy fácil capturarlos.

Una gran cantidad de tráfico se envía a través de redes inalámbricas, como RTP, SNMP o HTTP. La característica común de estos es el hecho de que están en texto plano. Lo que significa que uno puede leerlos fácilmente con la ayuda de herramientas de acceso gratuito como Wireshark. Como resultado, alguien con intenciones maliciosas puede simplemente robar sus contraseñas e información confidencial similar.

Si desea proteger su red inalámbrica contra la detección de paquetes, debe invertir en soluciones de cifrado.

## MQTT

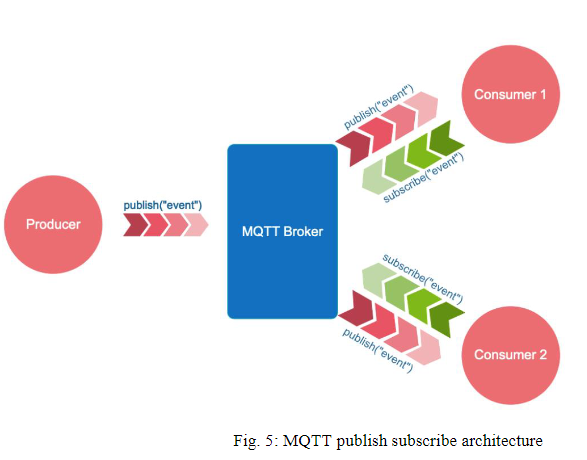
ttp://mqtt.org/. Hacer referencia a [5]

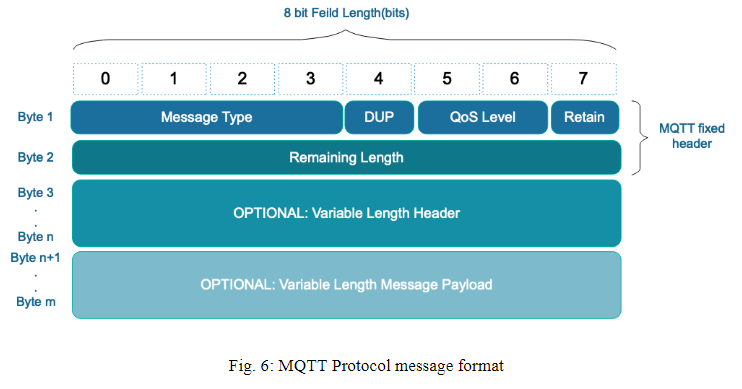
“What is Pub/Sub Messaging?” [Online]. Available: <https://aws.amazon.com/pub-sub-messaging/> [20]

¿Que es MQTT?

Message Queue Telemetry Transport or MQTT[5]for short is an ISO standard for networking, i.e. ISO/IEC PRF 20922[5], introduced by IBM (1999) and later on standardized by OASIS (2013). MQTT is a lightweight networking protocol based on a publish-subscribe model[20]. It aims to connect applications and networks in a comparatively faster manner as compared to the standard TCP/IP protocol

?Como funciona?





Ventajas?

Desventajas

### Seguridad en MQTT

MQTT se basa en el protocolo de transporte TCP. De forma predeterminada, las conexiones TCP no utilizan una comunicación cifrada.

*Transport Layer Security* (TLS) y *Secure Sockets Layer* (SSL) proporcionan un canal de comunicación seguro entre un cliente y un servidor. En esencia, TLS y SSL son protocolos criptográficos que utilizan un mecanismo de apretón de manos para negociar varios parámetros para crear una conexión segura entre el cliente y el servidor. Una vez completado el protocolo de enlace, se establece una comunicación cifrada entre el cliente y el servidor y ningún atacante puede espiar ninguna parte de la comunicación.

**TLS (*Transport Layer Security*)**

Para cifrar toda la comunicación MQTT, muchos agentes MQTT permiten el uso de TLS en lugar de TCP simple. El puerto 8883 está estandarizado para una conexión MQTT segura. El nombre estandarizado en IANA es "*secure-mqtt*". El puerto 8883 está reservado exclusivamente para MQTT a través de TLS.

* Desventajas de TLS:
  + Hay un inconveniente en el uso de MQTT sobre TLS: la seguridad tiene un costo en términos de uso de CPU y sobrecarga de comunicación. Si bien el uso adicional de la CPU suele ser insignificante en el “broker”, puede ser un problema para dispositivos muy restringidos que no están diseñados para tareas de computación intensiva. Técnicas como la reanudación de la sesión pueden mejorar drásticamente el rendimiento de TLS.

Si TLS se implementa correctamente en el lado del cliente y el servidor, se asegura de que ningún espía pueda interceptar la comunicación y se obtiene esa capa adicional de seguridad que es importante para la autenticación y autorización a nivel de aplicación.

**Certificados de autoridades certificadas**

Los certificados de CAs(*Certificated Autority*) de confianza valen el dinero extra que cuestan. Los certificados auto firmados no funcionan bien con muchas implementaciones de TLS y, a menudo, conducen a un código descuidado. Por ejemplo, código que no valida certificados y abre la puerta a ataques *Man-In-The-Middle*. Si su agente MQTT es público, un certificado de confianza es imprescindible. Si utiliza MQTT a través de *websockets*, los certificados auto firmados no son óptimos. La mayoría de los navegadores web modernos no permiten conexiones *websocket* a recursos con certificados que no son de confianza [17].

**Resumen**

El cliente MQTT puede autenticar el agente mediante certificados SSL enviados desde el servidor. La autorización en MQTT se utiliza para restringir el acceso a los recursos del intermediario en función de la información proporcionada por el cliente. Para verificar la integridad de los datos, se puede utilizar una función hash. TLS puede proporcionar tales algoritmos. Para la confidencialidad de los mensajes MQTT, se puede utilizar algoritmo de cifrado. Sin embargo, estos algoritmos deben ser ligeros y requieren soporte al cliente.

Además de TLS, es de considerar otros mecanismos de seguridad, como el cifrado de la carga útil, las verificaciones de firma de la carga útil (*Payload*) y los mecanismos de autorización.

## Análisis de trabajo relacionado

Al integrar diferentes elementos en este proyecto donde se genera una selección de varias propuestas, sistemas, esquemas, protocolos, estándares. En esta sección se hace un análisis de los diferentes trabajos actuales.

**Implementaciones en VANET de CV2-X.**

Se presentan trabajos en el estado del arte relacionados a VANET en un ámbito general, con el objetivo de analizar el área donde desempeñan la problemática y observar las limitantes, así como también la cobertura del proyecto, que metodologías abordan y que resultados tienen.

Tabla ii. Estado del arte en aplicaciones VANET en general

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ref. | Método | Problema que abordan | Contribución | Resultados |
| [18] | Propuesta analítica CV2-X bajo diferentes escenarios, utilizando el protocolo MQTT. | Colisión de vehículos, prevención de accidentes en peatones. | Análisis exhaustivo en base a simulaciones en su propuesta. Con el objetivo de evaluar MQTT y CoAP bajo diferentes escenarios. | Tiempos de medición en diferentes QoS que brinda MQTT, donde se muestra la diferencia considerable de tiempos en la que interactúa QoS0 y Qos2. |
| [19] | Presentan una arquitectura con IaaS (AWS) para establecer enlace punto a punto con el dispositivo NODEMCU V3. | Mensajes *multicast* y servicio de emergencia. | Una aproximación a lo que es mensajería de índole de emergencia propagada a modo multicasting. | Tiempos de transmisión de un solo mensaje a varios dispositivos, tamaño de la información transmitida, numero de paquetes. Consideraron parámetros de GPS. |
| [20] |  |  |  |  |
|  |  |  |  |  |

**Análisis de trabajos relacionados en VANET.**

La seguridad que abordan estas aproximaciones se da solo en cuanto al objetivo general de la problemática en sí, ya que los servicios de emergencia y servicios de prevención tienen en objetivo el resguardo e integridad física del usuario. Sin embargo, estos trabajos solo implementan el protocolo MQTT sin preocuparse por la seguridad en los mensajes sin mencionar que no aprovecharon las ventajas y la compatibilidad de MQTT con mecanismos de cifrado como lo son TLS/SSL que son básicas en la capa de aplicación. Solo estudian el comportamiento del protocolo en eventos multicas o broadcast y atribuyen los resultados positivos a la flexibilidad del mensaje en desempeño a la necesidad de su problemática.

Como resultado; queda en evidencia que el protocolo es justificablemente utilizado en problemáticas con naturaleza de emergencia, es decir: que requiere una difusión hacia varios puntos con eficiencia.

Considered the communication for collision avoidance over 4G/LTE*. S. Kato, M. Hiltunen, K. Joshi and R. Schlichting, “Enabling Vehicular Safety Applications over LTE Networks,” in International Conference on Connected Vehicles and Expo (ICCVE), Las Vegas, NV, USA.* 2013.

Communications for emergency vehicle applications over 5G networks were presented in

*I. Farris, A. Orsino, L. Militano, M. Nitti, G. Araniti, L. Atzori and A. Iera, “Federations of Connected Things for Delay-sensivibe IoT Services in 5G Environments,” in IEEE ICC SAC Symposium Internet of Things, Paris, 2017*

Communications for emergency vehicle applications over 5G networks were presented in [92].

**Seguridad en MQTT**

|  |  |  |  |
| --- | --- | --- | --- |
| Ref. | Método | Contribución | Resultados |
| [21] | Esquema de seguridad SMQTT y SMQTT-SN con cifrado basado en clave/texto-cifrado basado en atributos (KP/CP-ABE) utilizando criptografía ligera de curvas elípticas. | Los autores dan un análisis de seguridad de su esquema propuesto y muestran que sus protocolos son seguros bajo varios ataques. | Presentan resultados de tiempos de respuesta en diferentes atributos, es decir el tamaño de la carga útil que va desde 1 a 10 atributos.  Procesos medidos: Tiempos promedios de la generación de llave, cifrado, descifrado. También midieron el uso del CPU en los procesos. |
| [22] | Despliegue seguro de MQTT para dominio industrial.  Un nodo restringido, Zolertia Z1, se utiliza para el rendimiento evaluación. | Los autores concluyen que el cifrado autenticado de carga útil con AES-OCB es el más adecuado para aplicaciones industriales. | Compararon el cifrado con: AES, AES-OCB y LLSec, todos con dimensión de tamaño útil en bytes (16-64), esto en referencia a tiempo.  Compararon la memoria ocupada en la ROM y RAM en kB de parte del sensor y actuador, esto con los algoritmos anteriormente mencionados. |
| [23] | Esquema de seguridad con algoritmo chacha20-poly1305 AEAD para aplicaciones ligeras de IoT. 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 | Tabla comparativa donde predominan los experimentos con ARMC CORTEX M4, se considera el proceso de cifrado y de MAC, diferentes dimensiones de la carga útil y parámetros para medir el algoritmo en sí, sin considerar tiempos, solo ciclos de procesamiento. |
| [24] | Esquema de seguridad ligero para el protocolo MQTT/MQTT-SN basado en chacha20-poly1305 AEAD.  La implementación del cliente MQTT-SN y el uso del cliente MQTT usan diferentes bibliotecas de Arduino existentes. Se desarrollo en dos dispositivos: Arduino uno y ESP8266 | La evaluación del rendimiento muestra que la seguridad propuesta es adecuada para nodos restringidos en términos de uso de CPU y memoria. | Tiempos de encriptado/desencriptado en base a la carga útil desde 8 a 64 bytes  Memoria ocupada en la ROM y RAM en bytes. |

**Contrastar que hacen los demás y que no**

**Desglozar la parte técnica de las antenas, limites de la red, en que.**

**Que parámetros necesita 4g para establecer una.**

**Análisis**.

Todos los esquemas se relacionan en que cifran la carga útil usando el protocolo MQTT, la mayoría emplea métodos de medición de rendimiento en relación a tiempo y los resultados no pasan más de los dos segundos, algunos contemplan la seguridad TSL y lo que mas interesa es como se comportan en los dispositivos clientes o que hacen “Edge computing”, se utilizaron diferentes placas de desarrollo, sin embargo, todas compartían todas eran de índole de bajo consumo.

**Establecimiento de tiempos efectivos.**

Según la comunicación dedicada a onda corta (DSRC: poner el significado en ingles por sus siglas en inglés), cada vehículo transmite periódicamente mensajes de seguridad cada 100-300 milisegundos sobre la carretera, advertencias de seguridad y condiciones de tráfico [8, 9].

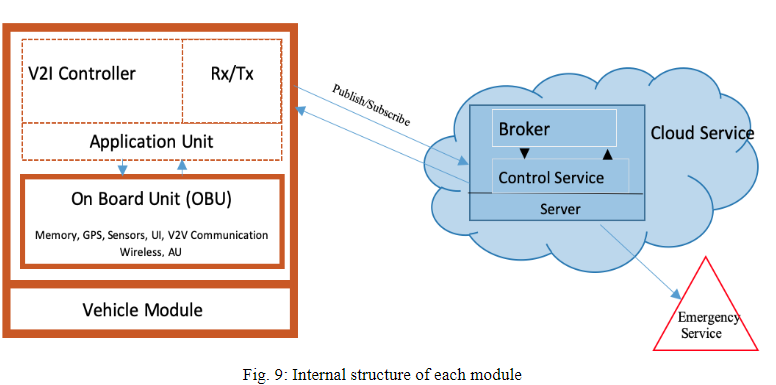
Bajo el concepto internet de las cosas se cuenta con un análisis maduro en diferentes aplicaciones como por ejemplo aplicaciones de Salud, Monitorización de calidad de aire, o en aplicaciones industriales donde la supervisión de algún proceso se tiene que dar. Para estas aplicaciones ya se tienen estimadas frecuencias de actualización, retraso tolerable, velocidad de conexión. En aplicaciones de emergencia y respuesta en tiempo real y diagnósticos remotos se tienen las siguientes especificaciones [25].

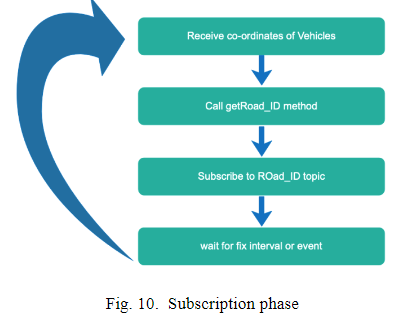
* Tolerancia a retraso: Baja, orden de segundos.
* Frecuencia de actualización: Requiere comunicación de emergencia red ad-hoc.
* Velocidad de transmisión: Alta.

En conclusión es buena idea mantener los menores tiempos de respuesta menores al minuto.

# MÉTODO

~~En esta sección se presenta la metodología aplicada para desarrollar una propuesta de arquitectura IoT para 5G. Se presentan los sujetos de estudio, se describe de manera general el procedimiento utilizado, así como los materiales y herramientas empleadas.~~





Organizarlos en fases

# RESULAT

# DOS.

En este capítulo se tienen los resultados obtenidos a través de las diferentes etapas del desarrollo para lograr una arquitectura funcional de internet de las cosas. Se presentan los

# CONCLUSIÓN

BIBLIOGRAFÍA

[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.

[15] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, “IoT Middleware: A Survey on Issues and Enabling Technologies,” *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 1–20, Feb. 2017, doi: 10.1109/JIOT.2016.2615180.

[16] S. Elhadi, “Comparative study of IoT protocols.” [Online]. Available: https://ssrn.com/abstract=3186315

[17] “HiveMQ Introduction :: HiveMQ Documentation.” https://www.hivemq.com/docs/hivemq/4.7/user-guide/introduction.html (accessed Mar. 08, 2022).

[18] Y. Nadezda, “A Safe Intelligent Driver Assistance System in V2X Communication Environments based on IoT,” 2017.

[19] R. Tomar, H. G. Sastry, and M. Prateek, “A V2I BASED APPROACH TO MULTICAST IN VEHICULAR NETWORKS,” *Malaysian Journal of Computer Science*, vol. 2020, no. Special Issue 1, pp. 93–107, Nov. 2020, doi: 10.22452/mjcs.sp2020no1.7.

[20] N. A. Hussein and M. I. Shujaa, “Secure vehicle to vehicle voice chat based MQTT and coap internet of things protocol,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 1, pp. 526–534, 2020, doi: 10.11591/ijeecs.v19.i1.pp526-534.

[21] L. Bisne and M. Parmar, “Composite secure MQTT for Internet of Things using ABE and dynamic S-box AES,” *2017 Innovations in Power and Advanced Computing Technologies, i-PACT 2017*, vol. 2017-January, pp. 1–5, 2017, doi: 10.1109/IPACT.2017.8245126.

[22] S. Katsikeas *et al.*, “Lightweight & secure industrial IoT communications via the MQ telemetry transport protocol,” *Proceedings - IEEE Symposium on Computers and Communications*, vol. 0, pp. 1193–1200, Sep. 2017, doi: 10.1109/ISCC.2017.8024687.

[23] F. de Santis, A. Schauer, and G. Sigl, “ChaCha20-Poly1305 authenticated encryption for high-speed embedded IoT applications,” *Proceedings of the 2017 Design, Automation and Test in Europe, DATE 2017*, pp. 692–697, May 2017, doi: 10.23919/DATE.2017.7927078.

[24] O. Sadio, I. Ngom, and C. Lishou, “Lightweight Security Scheme for MQTT/MQTT-SN Protocol,” *2019 6th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2019*, pp. 119–123, Oct. 2019, doi: 10.1109/IOTSMS48152.2019.8939177.

[25] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, “A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges,” *IEEE Access*, vol. 6. Institute of Electrical and Electronics Engineers Inc., pp. 3619–3647, Dec. 02, 2017. doi: 10.1109/ACCESS.2017.2779844.