

ANÁLISIS DE LA GESTIÓN EN LAS REDES VEHICULARES

Lic. José Antonio León Martínez¹

¹ Centro de Estudios de Telecomunicaciones e Informática (CETI), Empresa de Telecomunicaciones de Cuba SA (ETECSA), Universidad Tecnológica de La Habana. “José Antonio Echevarría”, CUJAE, Ave 114 #11901 e/ Ciclovía y Rotonda, Marianao, La Habana, Cuba

¹e-mail: josea.leon@etecsa.cu

RESUMEN

Las redes vehiculares sobresalen por la capacidad y el potencial que brindan para el control del tráfico, la seguridad vial, la eficiencia en el tráfico y las comunicaciones V2V y V2I, pero también presentan muchos desafíos. Las características de su infraestructura heterogénea y su integración con otras tecnologías de redes la hacen vulnerables y difícil de gestionar. En este artículo se propone un análisis de la gestión en la red vehicular haciendo una revisión de la literatura existente que abarca los diferentes paradigmas asociados a la forma de gestión en este tipo de redes. Para lograr este objetivo se propone primeramente una descripción general de las redes vehiculares, llamadas comúnmente VANET (Vehicle Ad-hoc Network). Se hace del análisis de los diferentes desafíos que se tienen en las redes vehiculares y a partir de estos se identifican las soluciones y los diferentes enfoques para lograr una gestión eficiente en las redes VANET. Por último, se mencionan algunos temas de seguridad por la importancia que tiene en este contexto y además por ser uno de los problemas que más se presentan en esta tecnología. Los resultados muestran un recorrido por las distintas formas de gestión de la red vehicular que sirve de referencia a profesionales para el conocimiento de este tema. El trabajo demuestra que la gestión de VANET aplicando tecnologías avanzadas como la Inteligencia artificial (AI Artificial Intelligence) y la computación en el borde (Edge Computing) se hace más fácil.

PALABRAS CLAVES: V2V, V2I, VANET, gestión

ANALYSIS OF MANAGEMENT IN VEHICLE NETWORK

ABSTRACT

Vehicular networks stand out for their capacity and potential for traffic control, road safety, traffic efficiency, and V2V and V2I communications, but they also present many challenges. The characteristics of their heterogeneous infrastructure and their integration with other network technologies make them vulnerable and difficult to manage. This article proposes an analysis of vehicular network management by reviewing the existing literature that covers the different paradigms associated with the management method in this type of network. To achieve this objective, a general description of vehicular networks, commonly known as VANETs (Vehicle Ad-hoc Networks), is first proposed. The different challenges faced by vehicular networks are analyzed, and from these, solutions and different approaches for achieving efficient management in VANETs are identified. Finally, some security issues are mentioned due to their importance in this context and also because they are one of the most common problems in this technology. The results provide an overview of the different forms of vehicle network management, serving as a reference for professionals in their understanding of this topic. The work demonstrates that VANET management is becoming easier by applying advanced technologies such as Artificial Intelligence (AI) and Edge Computing.

INDEX TERMS: V2V, V2I, VANET, management

1. INTRODUCCIÓN

Las redes vehiculares ad-hoc (VANET, Vehicle Ad-hoc Network) representan un pilar fundamental en el desarrollo de sistemas de transporte inteligente (ITS). Estas redes permiten la comunicación entre vehículos (V2V) y entre vehículos e infraestructura (V2I), facilitando aplicaciones críticas como la prevención de accidentes, la gestión del tráfico y la entrega de servicios multimedia en movimiento.

A diferencia de las redes MANET (Mobile Ad-hoc Networks), las VANET enfrentan desafíos únicos debido a la alta movilidad de los nodos, la dinámica topológica cambiante y los estrictos requisitos de latencia y seguridad. Por ello, una gestión eficiente de estas redes es esencial para garantizar su escalabilidad, confiabilidad y rendimiento en entornos reales.

En este artículo, exploraremos los principales aspectos de la gestión de redes VANET, incluyendo protocolos de enrutamiento, estrategias para optimizar el uso de recursos y algunos tipos de ataques que son comunes en este tipo de redes. Además, analizaremos los desafíos actuales y las tendencias futuras que podrían impulsar la adopción masiva de esta tecnología en las smart cities del mañana. Para este estudio se realiza una revisión sistemática de la literatura existente y se exponen los conceptos fundamentales y los avances que se han alcanzado en este contexto tecnológico. El uso de diversas tecnologías inalámbricas en ambientes vehiculares ha sido objeto de estudio desde la década de 1970. Existen algunos proyectos e investigaciones sobresalientes al respecto. Uno de los proyectos pioneros fue el Sistema Integral Automovilístico de Control de Tráfico (CACCS, Comprehensive Automobile Traffic Control System) desarrollado por el Ministerio de Industria y Comercio Internacional (MITI, Ministry of International Trade and Industry) de Japón en 1973, cuyo objetivo fue reducir la congestión del tráfico vehicular y disminuir el número de accidentes de tránsito [1].

En 1986 surge PROMETHEUS (Programme for European Traffic with Highest Efficiency and Unprecedented Safety) constituida por 19 países de Europa, que impulsó la investigación en comunicaciones móviles inalámbricas con la propuesta Prometheus SRMRN (Short-Range Mobile Radio Network). En la década de 1990, el concepto de VANET tomó relevancia en la comunidad científica en informática y telecomunicaciones; la disponibilidad de sistemas de posicionamiento global (GPS, Global Positioning System) y dispositivos inalámbricos de bajo costo favoreció el avance de las redes vehiculares. Surgieron proyectos como PATH (California Partners for Advanced Traffic and Highways), ASV (Advanced Safety Vehicle) y PROMOTE CHAUFFEUR (Europa) que conformaron un framework en distintas áreas de las redes vehiculares tales como: estándares para las comunicaciones vehiculares, arquitectura y diseño de la red, protocolos de enrutamiento, desarrollo de aplicaciones y aspectos de seguridad.

2. DESCRIPCION GENERAL DE LA RED

Las redes vehiculares ad-hoc (VANET) se pueden clasificar como un subconjunto de MANET (Mobile Ad-hoc Network) donde los nodos de comunicación son vehículos, ver Fig. 1. Sin embargo, ciertas características de VANET, como la alta movilidad, la gran extensión geográfica y la diversidad de aplicaciones, no permiten utilizar los protocolos u arquitecturas que se han diseñado especialmente para MANET [2].

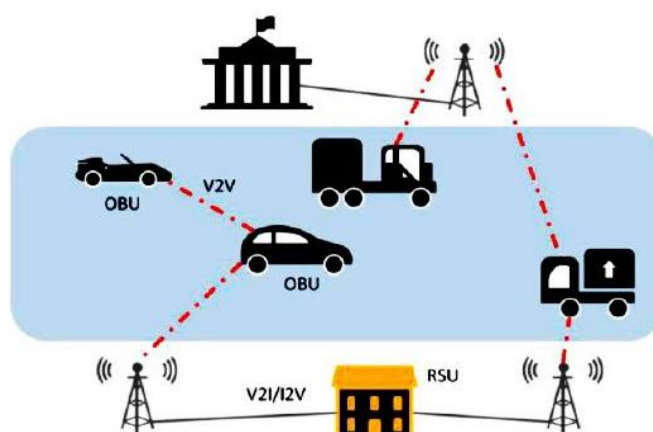


Figura 1: Arquitectura general de VANET [2].

Los nodos en las redes VANET consisten en vehículos equipados con unidades de a bordo (OBU OnBoard Unit) y unidades fijas en carretera (RSU Road Side Units), remitirse a la Tabala 1. Cada vehículo en movimiento y las RSU correspondientes forman simultáneamente una red auto organizada temporal.

Tabla 1: Resumen de los principales componentes de la red VANET [2].

Nombre	Tipo	Función
Vehículo	Unidad	Los vehículos están equipados con GPS (Sistema de Posicionamiento Global), RFID (Identificación por Radiofrecuencia), RADAR para posicionamiento,
OBU	Unidad	Un dispositivo de comunicación instalado en el vehículo permite comunicaciones DSRC (comunicación dedicada de corto alcance) con otras OBU o RSU
RSU	Unidad	Una unidad de comunicación que se encuentra al costado de la carretera y sirve como puerta de enlace entre las OBU y la infraestructura de comunicación
V2V	Comunicación	Los vehículos se envían y reciben mensajes entre sí
V2I	Comunicación	Los vehículos pueden conectarse a la infraestructura para algunos servicios
V2P	Comunicación	Los vehículos envían y reciben mensajes hacia y desde los peatones que caminan por la calle.

En conjunto, las comunicaciones V2V y V2I se conocen como V2X (Fig. 2), sus principales características se describen a continuación [3]:

- Topología variable: Debido a las altas velocidades y al continuo desplazamiento de los automóviles la topología de la red es altamente variable.
- Red sin infraestructura fija: En las comunicaciones V2V la arquitectura de la red es ad hoc y no existe una autoridad central que administre los nodos.
- Red frecuentemente desconectada: La topología dinámica de la red ocasiona desconexiones frecuentes de los nodos; el enlace entre los vehículos puede perderse fácilmente ocasionando la pérdida de paquetes en la comunicación.
- Nodos auto configurables: No existe un coordinador para las comunicaciones, por lo que los nodos deben auto organizarse y auto administrarse.
- Suministro de energía ilimitado: Los nodos no tienen restricciones en el consumo de energía, dado que la batería de los vehículos proporciona una cantidad suficiente para la operación de la OBU.
- Aspectos de radio comunicación: La radio comunicación en las VANET es compleja debido a diferentes factores: interrupción frecuente del radioenlace, condiciones desfavorables para la propagación de la señal (atenuación y reflexión) e interferencia con otros enlaces.

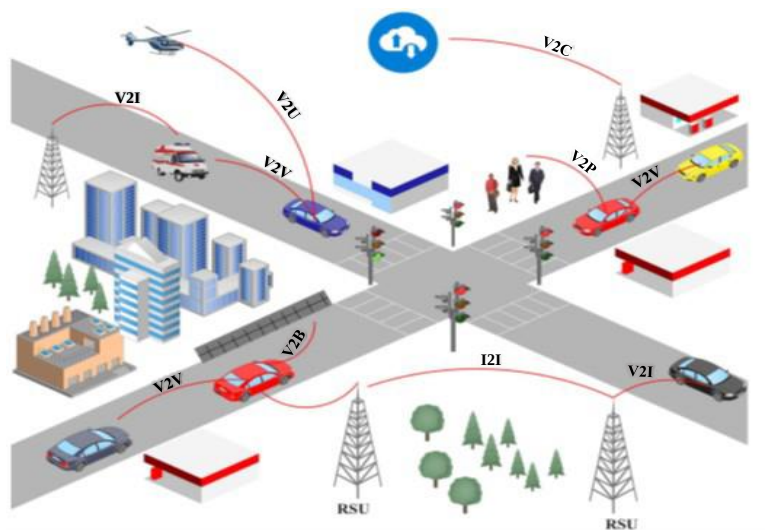


Figura 2: Comunicaciones V2X en ambientes vehiculares [4].

Las redes de acceso inalámbricas estándar que conviven con las redes VANET son:

- Las redes de servicio de corto alcance dedicado (DSRC Dedicated short-range communications) para intercambio inalámbrico directo de datos de V2X.
- Las redes WI-FI, VLC (Visible Light Communication) para servicios en lugares de cobertura deficiente.
- Las redes móviles LTE y 5G siendo esta última la más representativa, además pueden coexistir otros tipos de conexiones como bluetooth, satélite, WIMAX, Zigbee y mmWave.

Protocolos de encaminamiento en redes VANET

En las redes Ad-hoc la movilidad de los nodos, la inestabilidad de las topologías, y la ausencia de una infraestructura de centralización hacen obsoletos los protocolos que se usan en redes fijas. En redes VANET, los protocolos de encaminamiento deben ser capaces de funcionar de manera automática y distribuida [5].

Los protocolos de encaminamiento se pueden clasificar a partir de tres tipos fundamentales:

- El alcance.
- El modo de descubrimiento de rutas.
- Tipo de algoritmo que implementan (vector de distancias, estado de enlace).

Según el alcance:

- Protocolo Broadcast: El broadcasting consiste en mandar tráfico desde un nodo origen a todos los nodos presentes en la red usando la técnica de múltiples saltos.
- Protocolo Unicast: En el campo de la tecnología de redes, el unicast se utiliza para establecer una conexión directa punto a punto entre el emisor y el receptor.
- Protocolo Geocast: Los protocolos geocast son protocolos multicast donde los grupos están organizados en función de la posición geográfica de los nodos de la red. Se usan protocolos geocast cuando se desea mandar un mensaje a un grupo de vehículos de una determinada zona, para anunciar por ejemplo la presencia de un peligro en la carretera.

Según el modo de descubrimiento de rutas:

- Protocolos proactivos: Tienen la ventaja de un menor retardo end-to-end porque las rutas están disponibles al momento de querer establecer una conexión. La mayor desventaja es la generación de un gran tráfico para mantener las tablas actualizadas, presentando problemas de escalabilidad en redes de mayor tamaño.
- Protocolos reactivos: Las rutas son buscadas únicamente cuando se presenta la necesidad, el proceso de descubrimiento de ruta lo inicia el nodo origen, si encuentra una ruta hacia el nodo destino deseado mantendrá la transmisión hasta que el destino deja de ser accesible.
- Protocolos híbridos: Combinan los méritos de estos dos tipos de protocolos, además, solucionan sus limitaciones. Los protocolos de enrutamiento de paquetes más populares en redes convencionales se clasifican principalmente como de estado de enlace y de vector distancia.

En la Tabla 2 se muestran los protocolos más representativos atendiendo a la clasificación antes citada:

Tabla 2: Características de los protocolos [5].

Protocolo	Alcance	Esquema	Información geográfica
Blind Flooding	Broadcast	---	No
MPR	Broadcast	---	No
NES	Broadcast	---	No
CDS	Broadcast	---	No
DSDV	Unicast	Proactivo	No
DSR	Unicast	Reactivo	No
AODV	Unicast	Reactivo	No
LAR	Unicast	Proactivo	Si
TORA	Unicast	Reactivo	No
ZRP	Unicast	Híbrido	No
FSR	Unicast	Proactivo	No
OLSR	Unicast	Proactivo	No
LBM	Geocast	Proactivo	Si
GeoTORA	Geocast	Reactivo	Si
GeoGRID	Geocast	Reactivo	Si
GAMER	Geocast	Proactivo	Si

A continuación, se caracterizan los principales protocolos relacionados anteriormente en la Tabla No.2:

En lo que se refiere a los protocolos broadcast el protocolo más simple a la recepción de un mensaje es el Blind-Flooding, un nodo lo reenvía a todos sus vecinos. También de esta clasificación tenemos el MPR (Multi-Point Relay Flooding) que consiste en elegir un conjunto de nodos vecinos que cubre el acceso a los nodos distantes de 2 saltos. Está el NES (Neighbor Elimination Scheme), en él un nodo que recibe un mensaje de broadcast no retransmite directamente, sino que espera un tiempo aleatorio para ver si otro nodo manda la información. Por último CDS (Connected Dominating Sets), cuya la idea es organizar los nodos de la VANETs en una jerarquía. Se hace una clasificación de los nodos en dos categorías: los nodos dominantes y los nodos pasivos.

De los protocolos unicast se destacan Destination-sequenced Distance-Vector Routing (DSDV) que su principal objetivo es evitar los problemas de bucles en la actualización de las tablas de encaminamiento. El protocolo Dynamic Source Routing (DSR) que se compone de dos mecanismos: el descubrimiento y el mantenimiento de rutas. Los mecanismos permiten a un nodo origen descubrir y mantener las rutas hacia un nodo destino cuando se necesita

mandar tráfico en la red ad-hoc. Se basa en una técnica de source routing, cuyo fin es determinar la mejor ruta completa hacia un destino.

Otro protocolo de esta clasificación es Ad-hoc On-Demand Distance-Vector Routing (AODV), se construye sobre el protocolo DSDV analizado previamente. La idea es mejorar DSDV minimizando el número de paquetes broadcast requeridos para crear rutas, ya que, al ser bajo demanda, los nodos que están en el camino no tienen que participar en el intercambio de tablas ni mantener la ruta. Location Aided Routing (LAR) es un protocolo proactivo que introduce la idea de enrutamiento geográfico para disminuir la sobrecarga en el descubrimiento de rutas. Temporally-Ordered Routing Algorithm (TORA) propuesto para mejorar las prestaciones en redes altamente dinámicas. La idea básica es la generación de mensajes de control del protocolo en un pequeño conjunto de nodos cerca de la localización de un cambio topológico.

El protocolo Zone Routing Protocol (ZRP), clasificado como unicast, donde todos los nodos mantienen proactivamente las rutas dentro de una zona local conocida como zona de encaminamiento (IARP). Sin embargo, a nivel global ZRP emplea mecanismos reactivos (IERP) para encaminar los paquetes entre las áreas locales por lo que se clasifica como híbrido. El protocolo Fisheye State Protocol (FSR) es un mecanismo mediante el cual se captura con detalle los pixeles que se encuentran cerca del punto focal. El detalle disminuye a medida que se aumenta la distancia al punto focal. Por último, el protocolo Optimized Link State Routing (OLSR) es una optimización directa del algoritmo de estados de enlace adaptado a los requisitos específicos de una WLAN con alta movilidad.

Es importante mencionar el protocolo multicast MAODV que es la extensión multicast de AODV, conocida también como Multicast AODV. Lo que se pretende construir son árboles multicast bidireccionales compartidos que conecten múltiples fuentes y destinos para cada grupo multicast.

Los protocolos geocast son un caso particular de los multicast pero es interesante detallar algunos de ellos debido al hecho de que son muy usados en redes VANETs. Entre los más empleados tenemos al Location Based Multicast (LBM), orientado a la transmisión de datos que se basa en el protocolo unicast LAR expuesto anteriormente. También está el LBM, este se basa en un flooding tradicional salvo que los nodos tienen que decidir si retransmiten o no a los demás nodos según dos esquemas: LBM box y LBM step. Otro ejemplo es GEOTORA, como su propio nombre lo indica deriva directamente del algoritmo unicast TORA. Se construyó de la siguiente manera: se modificó TORA para hacer un protocolo anycast, modificando este protocolo anycast se consiguió un protocolo multicast.

El protocolo GEOGRID es un protocolo geocast derivado del unicast GRID. Al igual que GRID, GEOGRID realiza una partición del área geográfica que ocupa la red en celdas de dos dimensiones. Por último, el protocolo Geocast Adaptive Mesh Environment for Routing (GAMER) que se basa en la idea de crear rutas redundantes desde el origen hacia una zona geocast.

3. LA GESTIÓN DE LAS REDES VEHICULARES

Las comunicaciones V2X en las redes VANET presentan muchas características que la hacen difícil para el monitoreo y la gestión de detención de fallos, problemas de seguridad, control del tráfico, entre otras. Esto plantea algunos desafíos que hay que tener en cuenta [6].

Topología ad hoc dinámica y movilidad de nodos

La topología de red altamente dinámica debido a la densidad y movilidad de los nodos móviles es uno de los problemas más desafiantes que se deben superar en las redes vehiculares. Como la topología de la red cambia constantemente con el tiempo, un administrador de red no puede planificar la topología a priori. Por lo tanto, nuevos nodos pueden unirse o salir de la red en cualquier momento, cambiando no solo la topología de la red sino también la densidad de nodos. Tales cambios pueden causar varios problemas relacionados con el descubrimiento de rutas, lo que lleva a rutas y estructuras subóptimas. Esta situación da como resultado un enorme desperdicio de recursos. Una posible solución que reduce el impacto de la topología altamente dinámica y minimiza los efectos de tales problemas es diseñar metodologías de gestión de movilidad. El método se encargará de las rutas de red y actualizaciones de estructura con el objetivo de reflejar el estado actual de la topología de la red, permitiendo así servicios de alta velocidad y sin interrupciones para redes vehiculares. Sin embargo, los protocolos de movilidad presentan limitaciones de rendimiento, por ejemplo la latencia, en escenarios altamente dinámicos y las metodologías ineficientes pueden dar como resultado no solo un gran desperdicio de recursos sino también rutas subóptimas.

Limitaciones de ancho de banda y recursos

Debido a la velocidad de los nodos móviles y a la naturaleza de los canales inalámbricos, el ancho de banda de las comunicaciones puede ser mucho menor en las redes vehiculares. Por el contrario, la tasa de pérdida de paquetes tiende a ser mayor en comparación con la Internet tradicional. Para agravar aún más este problema, las redes vehiculares también se caracterizan por una corta duración de ompletos a los administradores de red, ayudándolos a crear medidas para mejorar el rendimiento general de la red. Además, esto puede permitir que se investiguen problemas de rendimiento, como el consumo innecesario de ancho de banda.

Gestión de la movilidadcontacto. Tal condición en el volumen de datos que se pueden transferir en cada oportunidad de contacto, impone serias limitaciones para las aplicaciones de intercambio multimedia propuestas.

Para promover e incitar el desarrollo de nuevas aplicaciones y servicios, se deben emplear enfoques de gestión nuevos y diferentes para las comunicaciones, los datos y la gestión de recursos en entornos vehiculares. Se pueden proponer algunos enfoques para monitorear las condiciones de la red que proporcionen informes y estadísticas c

Las operaciones de gestión de movilidad de red son responsables de gestionar y mantener la conectividad a Internet entre grupos de nodos móviles, con el objetivo de lograr un rendimiento óptimo de la red. Las propuestas de gestión de movilidad para redes vehiculares deben diseñarse teniendo en cuenta los requisitos específicos de las redes vehiculares: comunicaciones entre vehículos (V2V) y entre vehículos y algún tipo de infraestructura en la carretera (V2I). Con base en estos dos tipos de comunicaciones, se puede definir una taxonomía para los enfoques de movilidad. En las comunicaciones V2V, la mayoría de los esquemas de gestión de movilidad se centran en el descubrimiento y mantenimiento de rutas, lo que implica topologías altamente dinámicas, ubicación y problemas de transferencia. Por otro lado, los esquemas propuestos relacionados con la movilidad en las comunicaciones V2I implican problemas de host y red, como la optimización de rutas y la integración con VANET. La mayoría de ellos consideran algunos protocolos de gestión de movilidad de Internet (por ejemplo, Mobile IPv4 y Mobile IPv6). Sin embargo, la implementación común de estos protocolos introduce una alta latencia de transferencia y aumenta la cantidad de pérdida de datos.

Gestión del tráfico

Se espera que el diseño e implementación de soluciones de gestión del tráfico mejoren los flujos de tráfico, lo que ayudará a detectar y reducir los atascos y los accidentes. Con la optimización del flujo, también es posible reducir el consumo de recursos y las emisiones de los vehículos. Por lo general, la gestión del tráfico se logra teniendo en cuenta el funcionamiento de los protocolos de enrutamiento y cómo estos gestionan los datos.

Con base en estas dos características, los esquemas para abordar la gestión del tráfico se pueden clasificar en una taxonomía considerando dos actividades principales: predicción y optimización. Para permitir el proceso de predicción, la información del tráfico vial debe recopilarse utilizando algún tipo de metodología. Las metodologías predictivas pueden recopilar datos utilizando modelos analíticos, sensores fijos, teléfonos o dispositivos móviles (por ejemplo, teléfonos inteligentes) combinados con receptores GPS. Después del proceso de predicción, la información recopilada debe evaluarse mediante una metodología de control de ruta o control de señales de tráfico para implementar una estrategia de optimización del tráfico. Los vehículos conducidos por humanos pueden luego usar esta información para reducir la congestión vial.

Gestión de comunicaciones, datos y recursos

Con el creciente interés en las redes vehiculares y la madurez de los protocolos de enrutamiento para redes inalámbricas, se han propuesto redes ad hoc, aplicaciones y servicios innovadores. Sin embargo, para diseñar aplicaciones eficientes se deben tener en cuenta las características particulares de este tipo de redes. Por ejemplo, el posicionamiento y la conectividad de los nodos, la intermitencia y equidad de las comunicaciones, la latencia y las limitaciones de recursos pueden tener un impacto significativo en el rendimiento de la red. Además, el creciente número de tecnologías disponibles para los vehículos hace que la comunicación y la gestión de recursos sean dos de los principales problemas que deben resolverse cuando se trata de redes vehiculares. Para superar algunas de estas limitaciones, se deben diseñar nuevas metodologías que sean capaces de manejar la gestión y el seguimiento de la

comunicación, los recursos y los datos. En este apartado se detallan las propuestas más importantes para cada funcionalidad.

En el contexto de las redes VANET, la gestión de red puede abordarse de diferentes enfoques, dependiendo de los requisitos de la aplicación, la infraestructura disponible y los objetivos de rendimiento, estos enfoques se describen a continuación [7]:

- Gestión centralizada (basada en infraestructura): Utiliza elementos centralizados como RSUs (Roadside Units) o servidores para coordinar comunicaciones, seguridad y distribución de datos. Este tipo de gestión es ideal para áreas urbanas con infraestructura preexistente, por ejemplo, priorización de mensajes de emergencia mediante RSUs.
- Gestión descentralizada (ad-hoc/V2V): Los vehículos se auto organizan sin dependencia de infraestructura, comunicándose directamente (V2V). Permite robustez en zonas remotas o sin cobertura de RSUs. Por ejemplo, protocolos de enrutamiento reactivos como AODV (Ad-Hoc On-Demand Distance Vector).
- Gestión híbrida: Combina V2V (Vehicle-to-Vehicle) y V2I (Vehicle-to-Infrastructure), aprovechando RSUs cuando están disponibles y usando redes ad-hoc en su ausencia, esto balancea eficiencia y cobertura. Por ejemplo, disseminación de información de tráfico mediante RSUs y retransmisión entre vehículos.
- Gestión basada en clusters: Los vehículos forman grupos con un "cabecilla de cluster" que gestiona la comunicación interna y externa, esto permite reducir la sobrecarga de mensajes en redes densas. Por ejemplo, algoritmos de elección de cabecilla basados en movilidad o recursos.
- Gestión asistida por la nube [8]: Integra servicios en la nube para procesamiento masivo de datos, almacenamiento y análisis, esto facilita aplicaciones como navegación predictiva o gestión del tráfico en tiempo real. Por ejemplo, plataformas cloud para procesar datos de sensores vehiculares.
- Gestión basada en SDN (Software-Defined Networking) [9] [10]: Separa el plano de control (centralizado) del plano de datos (vehículos/RSUs), esto permite flexibilidad y adaptación dinámica a cambios en la red. Por ejemplo, control centralizado de políticas de seguridad y enrutamiento.
- Gestión geográfica o posicional: Usa la ubicación de los vehículos para decisiones de enrutamiento o difusión de mensajes, es eficaz para aplicaciones como alertas de colisión en intersecciones. Por ejemplo, protocolos como GPSR (Greedy Perimeter Stateless Routing).

Partiendo de estos enfoques se pueden determinar algunas áreas de oportunidad que se pueden estudiar más a profundidad, se mencionan algunas a continuación:

- Gestión de movilidad y enrutamiento: Se pueden aplicar técnicas de predicción de movilidad vehicular como los modelos de tráfico y el ML (Machine Learning).
- Gestión de recursos: Uso de las bandas 5G/6G y V2X para la asignación dinámica de recursos y la optimización de recursos con el uso de Edge y Fog computing.
- Seguridad y privacidad: Estudio de otros métodos de autenticación descentralizada, detección de intrusos basada en IA y técnicas de preservación de privacidad, por ejemplo, pseudonimización.
- Gestión de la energía: Optimización del consumo en vehículos eléctricos (V2G, Grid-aware routing).

Existen tecnologías habilitadoras para desarrollar estos aspectos; para las comunicaciones inalámbricas los estándares DSRC (Dedicated Short-Range Communications), C-V2X, 5G/6G, el uso de la computación distribuida con Edge/fog computing para procesamiento en tiempo real y Offloading de tareas a infraestructura (RSUs, cloud) y por último la inteligencia artificial y analítica de datos.

Principales componentes involucrados en la gestión de redes VANET [11]:

Manuscrito recibido: 05-05-2025, aceptado: 17-08-2025

Sitio web: <http://revistatelematica.cujae.edu.cu/index.php/tele>

- **Arquitectura de la Red Vehicular:** Se basa en una arquitectura que incluye: Vehículos (V2V, Vehicle-to-Vehicle), Infraestructura (V2I, Vehicle-to-Infrastructure), por ejemplo, semáforos, postes de control o estaciones base y otro elemento de la arquitectura es la nube y servidores centralizados.
- **Gestión de la Comunicación:** Esto incluye protocolos de enrutamiento específicos para VANETs, como AODV (Ad-Hoc On-Demand Distance Vector) o GPSR (Greedy Perimeter Stateless Routing), para garantizar que los mensajes lleguen a su destino de manera eficiente. También se incluye la calidad del Servicio (QoS Quality of Service) priorizando el tráfico crítico (por ejemplo, mensajes de emergencia) sobre otros tipos de datos. Asimismo, el control de congestión es parte de la gestión de la comunicación, se implementan mecanismos para evitar la saturación de la red, especialmente en áreas con alta densidad de vehículos.
- **Seguridad y Privacidad:** Esto incluye la autenticación de la identidad de los nodos (vehículos o infraestructura) para evitar ataques. Incluye el cifrado de los datos transmitidos para garantizar la privacidad y la detección de intrusos mediante sistemas para identificar y mitigar comportamientos maliciosos en la red).
- **Gestión de Movilidad:** Incluye el seguimiento de la ubicación con el uso de sistemas GPS y tecnologías como el Geocasting para enviar mensajes a zonas geográficas específicas. También la predicción de rutas (Anticipación de los movimientos de los vehículos para optimizar la comunicación) y handover entre celdas (Transición suave entre diferentes puntos de acceso, por ejemplo, entre estaciones base).
- **Gestión de Recursos:** Se basa en la asignación de canales (Uso eficiente del espectro radioeléctrico, especialmente en entornos con alta densidad de vehículos) y energía (Optimización del consumo de energía en los dispositivos de comunicación, especialmente en vehículos eléctricos o híbridos).
- **Aplicaciones y Servicios:** Esto incluye: Seguridad vial (Alertas en tiempo real sobre accidentes, condiciones climáticas adversas o congestión), entretenimiento y conectividad (Servicios de internet y multimedia para los pasajeros) y gestión del tráfico (Optimización del flujo vehicular mediante la coordinación con semáforos y sistemas de control).
- **Desafíos en la Gestión de VANET:** Incluye alta movilidad (Los vehículos se mueven rápidamente, lo que dificulta el mantenimiento de conexiones estables), escalabilidad (La red debe manejar un gran número de vehículos en áreas urbanas densas), interoperabilidad (Compatibilidad entre diferentes fabricantes y tecnologías) y latencia (Garantizar que los mensajes críticos lleguen en tiempo real).

Dependiendo de los objetivos, tecnologías y arquitecturas utilizadas la gestión se puede enfocar además con diferentes alternativas como se muestra en la Tabla 3 [12]:

Tabla 3: Alternativas para redes VANET basada en objetivos, tecnologías y arquitecturas [12]

Tipos de redes	Ventajas	Casos de uso
Redes celulares vehiculares (C-V2X Cellular vehicle-to-everything)	Más cobertura y fiabilidad, baja latencia, escalabilidad	Comunicación en tiempo real para evitar colisiones y para gestión de tráfico
Redes basadas en infraestructuras (Infrastructure-Centric-Network)	Control centralizado de red, gestión de tráfico y monitoreo vial.	Semáforos inteligentes, detección de incidentes en la vía.
Redes híbridas	Flexibilidad, redundancia y fiabilidad en las comunicaciones	V2V en áreas donde la cobertura celular es deficiente

Redes de sensores vehiculares (Vehicle-Sensor-Network)	Monitoreo ambiental o diagnóstico de vehículos	Detención de condiciones climáticas adversas, diagnóstico de fallas en vehículos
Redes basadas en computación en la nube (Cloud-Based Vehicle Networks)	Escalabilidad para manejar grandes volúmenes de datos (Big Data, IA, etc)	Optimización de rutas en tiempo real, análisis de patrones de tráfico.
Redes de computación en el borde (Edge Computing for Vehicle Network)	Reduce latencia, disminuye carga en la red central	Procesamiento de imágenes para detección de peatones, evitar colisiones
Redes de comunicación por satélite	Cobertura global, útil para zonas rurales de difícil acceso	Monitoreo de flotas en áreas remotas, asistencia a emergencias
Redes de comunicación por luz visible (VLC-Visible Ligth Communication)	Alta velocidad de transmisión no requiere espectro radioelectrico adicional	Comunicación en intersecciones, transmisión de datos en túneles
Redes de comunicación por radio definida por software (SDR-Software Defined Radio)	Flexibilidad para operar en entornos y tecnologías heterogéneos, se actualiza por software	Integración de VANET con redes celulares o satelitales

Ejemplos de gestión de desempeño en redes vehiculares

La gestión del desempeño en redes vehiculares busca optimizar la eficiencia, confiabilidad y calidad de los servicios en tiempo real. Aquí algunos puntos clave [13]:

Optimización de la Latencia en Comunicaciones V2X

Garantizar respuestas ultra-rápidas para evitar accidentes o congestiones. Para ello se utilizan las tecnologías Edge computing (procesamiento en el borde de la red), protocolos de baja latencia (IEEE 802.11p). Ejemplos en vehículos autónomos, priorizan la comunicación de emergencia como frenado automático sobre otros datos.

Gestión de Congestión en Redes Denso-Vehiculares

Evitar saturación en zonas con alta densidad de vehículos como centros urbanos. Las tecnologías que se emplea son Balanceo de carga dinámico y redes 5G con network slicing. Como ejemplo se puede mencionar que en Tokio, se usan algoritmos para distribuir la carga de datos entre torres celulares y RSUs (Roadside Units).

Calidad de Servicio (QoS) para Aplicaciones Críticas

Priorizar tráfico crítico (por ejemplo, emergencias) sobre aplicaciones no esenciales (por ejemplo, entretenimiento). Las tecnologías empleadas son SDN (Software-Defined Networking), políticas de QoS basadas en IA (Inteligencia Artificial). Un ejemplo de esto son las ambulancias conectadas que reciben ancho de banda preferencial para coordinar rutas con semáforos.

Mantenimiento Predictivo de Infraestructura

Monitorear el estado de RSUs y sensores para prevenir fallos. Las tecnologías empleadas son Machine Learning para anomalías, IoT para auto-diagnóstico. Como ejemplo se puede mencionar que en California, sensores en semáforos predicen fallos eléctricos usando análisis de vibraciones.

Eficiencia Energética en Vehículos Eléctricos

Optimizar rutas y consumo de energía en flotas de vehículos eléctricos. Las tecnologías empleadas son los algoritmos de optimización y la telemetría en tiempo real. Un ejemplo de este tipo de gestión es en Tesla, se utiliza redes vehiculares para recomendar estaciones de carga según tráfico y demanda.

Resolución de Interferencias en Comunicaciones

Mitigar interferencias entre señales V2V, Wi-Fi y 5G en entornos urbanos. Las tecnologías empleadas son MIMO (Multiple-Input Multiple-Output) y espectro dinámico. Un ejemplo es en Alemania, se usan técnicas de beamforming para direccionar señales y evitar colisiones.

Escalabilidad en entornos de tráfico dinámico

Adaptar la red a cambios abruptos (por ejemplo, eventos masivos, accidentes). Para ello se emplean las tecnologías de redes ad-hoc vehiculares (VANETs) y el escalado automático en la nube. Un ejemplo es durante el Super Bowl en EE.UU., se despliegan RSUs temporales para manejar el tráfico extra.

Gestión de Seguridad sin Comprometer el Rendimiento [14]:

Implementar cifrado y autenticación sin sobrecargar la red. Las tecnologías empleadas son la criptografía ligera (Lightweight Cryptography) y los certificados digitales. Un ejemplo es el estándar IEEE 1609.2, para cifrar mensajes V2V con bajo overhead computacional.

Monitoreo de Rendimiento en Tiempo Real

Dashboards para operadores de tráfico que muestran métricas clave (ejemplo, latencia, pérdida de paquetes). Las tecnologías empleadas son Prometheus/Grafana y los análisis de flujos. Un ejemplo es en Barcelona, el sistema Sentilo integra datos de sensores y redes para análisis en vivo.

Adaptación a Condiciones Climáticas

Ajustar parámetros de red en lluvia, nieve o niebla. Las tecnologías empleadas son sensores ambientales y redes auto-ajustables. Un ejemplo es que en Suecia, las RSUs aumentan la potencia de señal en invierno para contrarrestar interferencias.

En Europa y Asia estos indicadores de desempeño ya se cumplen en soluciones implementadas en Smart Cities para la gestión vehicular. Se puede mencionar a la ciudad de Amsterdam (Países bajos) con la plataforma Connected Transport que utilizan SDN (Software Defined Networking) para garantizar óptima calidad del servicio, además redes mesh vehiculares para adaptarse a los cambios de la densidad del tráfico y la tecnología Blockchain para autenticación segura. También se puede mencionar la ciudad de Helsinki (Finlandia) donde se implementa la movilidad como servicio (MaaS), para optimizar el tráfico existe una integración de buses, bicicletas y vehículos autónomos en una sola plataforma que se denomina Whim App. Asimismo, para garantizar la eficiencia energética existen rutas optimizadas para reducir consumo en vehículos eléctricos [15] [16].

Por último, se pueden mencionar dos ejemplos en China, la solución en la ciudad del cerebro Hangzhou (City Brain by Alibaba Cloud) que implementa una solución para reducción de la congestión sobre IA y Big Data para análisis de tráfico en tiempo real, ajustando semáforos y rutas. La ciudad de Shanghai presenta un proyecto 5G+V2X con HUAWEI que garantiza baja latencia con redes 5G Ultra-Reliable Low Latency Communication (URLLC) para comunicación vehículo-infraestructura con una latencia menor de 10ms. Además, en la ciudad se implementa seguridad mejorada mediante criptografía cuántica en comunicaciones V2V y uso de redes neuronales para predecir congestión y reconfigurar rutas [17] [18] [19] [20].

Europa y China están liderando la optimización de redes vehiculares en Smart Cities pero con enfoques diferentes:

- Europa prioriza descentralización (Edge computing) y seguridad (Blockchain).
- China apuesta por 5G + IA masiva y eficiencia energética radical.

4. SEGURIDAD Y ESTÁNDARES EN LA REDES VEHICULARES

En las redes vehiculares (VANET) se pueden producir distintos tipos de ataques que pueden dañar la disponibilidad, la autenticación y la confidencialidad en la red, a continuación, se mencionan algunos de estos [21] [22]:

- Ataque DDoS: En los ataques DoS (denegación de servicio), los atacantes inundan la red VANET con un alto número de mensajes ficticios o alterados en un intento de bloquear los canales de comunicación y consumen una gran cantidad de potencia informática de otros nodos (Disponibilidad).
- Ataque de agujero de gusano: Un atacante en una VANET tiene la capacidad de tunelizar paquetes transmitidos en un área a otra (Disponibilidad).
- Ataque de suplantación de GPS: Un ataque de suplantación de identidad, también conocido como ataque de túnel, engaña a los receptores GPS de la zona para que piense que sus coordenadas son diferentes a donde están realmente (Disponibilidad).
- Sybil Attack: Se producirá un error judicial si el atacante inicia el ataque de Sybil creando varios vehículos virtuales en la carretera que tienen toda la misma identificación. Incluso el atacante puede transmitir algunas comunicaciones falsas utilizando vehículos virtuales para promover sus actividades (Autenticación).
- Suplantación de nodo: Un atacante puede asumir una identidad diferente y hacerse pasar por el verdadero remitente del mensaje en un ataque de suplantación de nodo (Autenticación).
- Ataque de distorsión de la confianza: Los nuevos ataques VANET pueden utilizar mecanismos de gestión de confianza, se puede engañar a los nodos para que acepten estimaciones inexactas de la fiabilidad de otros nodos manipulando el cálculo de la confianza (Autenticación).
- Violación de la privacidad: Los atacantes en VANET generalmente vinculan los datos de ubicación e identificación recopilados por el vehículo, comprometiendo así la privacidad de los usuarios (Confidencialidad).
- Ataque social: En este ataque, el atacante distrae la atención de los conductores e influye en sus comportamientos de conducción y procesos de toma de decisiones enviándoles mensajes poco éticos.

Estándares para redes vehiculares (IEEE 802.11p, 1609)

La demanda de movilidad, de cobertura geográfica y el alto grado de variabilidad de las redes vehiculares son factores determinantes en la elección de los protocolos y de los estándares adecuados para la comunicación V2X. En el año 1999 la Comisión Federal de Comunicaciones de Estados Unidos (FCC, Federal Communications Commission) asignó 75 MHz de ancho de banda en la frecuencia 5,9 GHz para los servicios del sistema inteligente de transporte denominado DSRC (Dedicated Short-Range Communication) [23] [24].

Posteriormente, en el año 2002 la Sociedad Americana de Transporte Inteligente (ITSA, Intelligent Transportation Society of America) recomendó la adopción de un único estándar para la capa física y para la capa de acceso al medio (MAC, Medium Access Control) propio de las VANET. En consecuencia, en el año 2004 se consolidó el grupo de trabajo IEEE TFP (Task Force p) con el objetivo de especificar una arquitectura de comunicación para entornos vehiculares, basada en la tecnología inalámbrica para redes de área local IEEE 802.11, denominada IEEE 802.11p. Más adelante, el grupo de trabajo IEEE 1609 desarrolló un conjunto de especificaciones de las capas de red, transporte y aplicación para las comunicaciones vehiculares.

Los estándares IEEE 802.11p e IEEE 1609 definen el acceso inalámbrico en ambientes vehiculares, este conjunto de protocolos se denomina WAVE (Wireless Access in the Vehicular Environment). WAVE proporciona una arquitectura para las comunicaciones V2X, destinada al uso aplicaciones de seguridad y eficiencia vial. La Fig. 3 muestra la pila de protocolos de la arquitectura WAVE siguiendo el modelo de referencia OSI.

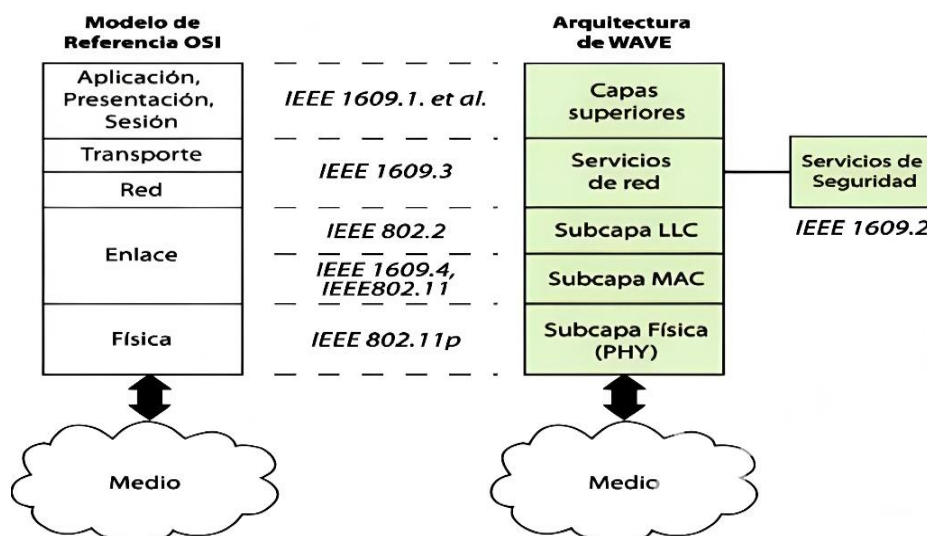


Figura 3: Estándares pertenecientes al modelo WAVE

IEEE 802.11p

El estándar IEEE 802.11p define las características de la capa física y MAC necesarias para operar en un ambiente vehicular:

- Capa física (PHY): Al igual que el protocolo IEEE 802.11a, el estándar IEEE 802.11p utiliza la transmisión multiportadora OFDM (Orthogonal Frequency Division Multiplexing).
- Capa MAC: El propósito de la capa MAC es establecer los mecanismos de acceso al canal de comunicación, de manera que unos conjuntos de estaciones puedan compartir eficientemente el medio inalámbrico. El estándar IEEE 802.11p define el uso de CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) para las comunicaciones V2X. La capa MAC también considera aspectos de la transmisión como la probabilidad de recepción de paquetes, el tiempo de acceso al canal, el control de congestión y la priorización de los mensajes.
- Operación multicanal: Una de las funciones de la capa MAC consiste en la priorización de los mensajes generados por aplicaciones de seguridad (sensibles a retardos elevados). Con el propósito de coordinar los diferentes tipos de mensajes, el estándar IEEE 802.11p establece un esquema de acceso al canal mejorado (EDCA, Enhanced Distributed Channel Access), EDCA especifica cuatro categorías de acceso, cada una asociada a un canal independiente y con una prioridad diferente. En la arquitectura de comunicación V2X se establecen dos tipos de canal: canal de control y el canal de servicio.

El estándar IEEE 1609

La familia de estándares IEEE 1609 define los aspectos de operación y gestión de la capa de red, de transporte y de aplicación de la arquitectura WAVE. A continuación, se describe brevemente cada estándar:

- IEEE 1609.0: Define la arquitectura general de WAVE, el modelo de la comunicación, los mecanismos de acceso al medio inalámbrico en ambientes vehiculares, la estructura general de los componentes como OBUs, RSUs e interfaces WAVE (IEEE, 2007a).
- IEEE 1609.4: Describe la operación multicanal (SCH y CCH) que debe implementar 802.11p, incluyendo los parámetros para la priorización de mensajes, temporizadores, conmutación del canal y primitivas diseñadas para el funcionamiento multicanal, se recomienda al lector referirse al estándar (IEEE, 2006a).
- IEEE 1609.3: Describe los servicios de la capa de red para entornos vehiculares, especifica las funciones de

- enrutamiento y direccionamiento basados en el nivel 3 del modelo de referencia OSI y de los protocolos IP, UDP y TCP, se recomienda al lector referirse al estándar (IEEE, 2007b).
- IEEE 1609.2: Especifica los servicios de seguridad en los sistemas WAVE, define los formatos de los mensajes y su procesamiento, se recomienda al lector referirse al estándar (IEEE, 2006b).
 - IEEE 1609.1: Describe el administrador de recursos (RM, Resource Manager) en los sistemas WAVE, que permite a una unidad a bordo (OBU) con capacidad de cómputo limitada ejecutar procesos de manera remota, se recomienda al lector referirse al estándar (IEEE, 2006c).
 - IEEE 802.2: Especifica la capa lógica de control (LLC, Logical Link Control) (IEEE, 1998; Kenney, 2009).

CONCLUSIONES

Las VANET han surgido como uno de los campos de investigación más apasionantes dentro de los sistemas de transporte inteligentes, proporcionando así información de seguridad y comodidad para los conductores. Sin embargo, las VANET son especialmente vulnerables a una variedad de amenazas a la seguridad, incluidos los ataques maliciosos y la distribución de información no fiable, que puede tener graves consecuencias, como los accidentes de tráfico. En el trabajo de investigación se ha realizado un recorrido por las distintas formas de gestión de estas redes para mostrar cuánto se ha logrado en investigaciones enfocadas a esta tecnología. Se ha demostrado cómo las actuales tecnologías como por ejemplo la inteligencia artificial, la computación en el borde, la red definida por software y otras que se mencionan, han servido para lograr una mejor gestión y más eficiente de las VANET.

RECONOCIMIENTOS

El autor de este artículo agradece a la profesora Dra. Caridad Arias Calderón por brindar todos los conocimientos adquiridos sobre la gestión de las redes de telecomunicaciones como base para este trabajo de investigación.

REFERENCIAS

- [1] A.K.Singh, R. Kumar y S.Rathore, "Evolution of VANETs: From Early Prototypes to Modern Deployments and Future Trends", IEEE Communications Surveys & Tutorials, vol.26, No.1, pp450-489, Enero 2024, doi: 10.1109/COMST.2023.3309876.
- [2] H. Che, Y. Duan, C. Li, y L. Yu, "On trust management in vehicular ad hoc networks: A comprehensive review", Frontiers, vol. 1, n.º 995233, pp. 1-29, Octubre de 2022.
- [3] E. Abdelkreem, Sh. Hussein, A. Tamam, "Feature engineering impact on position falsification attacks detection", International Journal of Information Security, Springer vol. 23, pp. 1939–1961, 2024.
- [4] N. H. Hussein, Ch. T. Yaw, S. P. Koh, S. K. Tiong, K. H. Chong "A Comprehensive Survey on Vehicular Networking: Communications, Applications, Challenges, and Upcoming Research Directions", IEEE Access, vol. 10, No. 1109, pp. 86127-86180, Agosto 2022.
- [5] J. M. Garcia Campos, "Evaluación de Protocolos de Encaminamiento Para Redes Vehiculares (VANET)", Proyecto Fin de Carrera Ingeniería de Telecomunicación, Universidad de Sevilla, España, 2014.
- [6] J. A. F. F. Dias, J. J. P. C. Rodrigues, V. N. G. J. Soares, J. M. L. P. Caldeira, V. Korotaev, y M. L. Proença Jr, "Network Management and Monitoring Solutions for Vehicular Networks: A Survey", Electronics, vol. 9, n.º 853, pp. 1-32, mayo 2020.
- [7] C. Zhang, H. Lu, J. Wang, "Deep Reinforcement Learning for Vehicular Network Resource Allocation", ACM SIGCOMM Workshop on Networked AI Systems, 2023.
- [8] Y. Dai, D. Xu, S. Maharjan, and Y. Zhang, "Artificial Intelligence Empowered Edge Computing and Caching for Internet of Vehicles", IEEE Wireless Communications, vol. 26, no. 3, pp. 12–18, Junio 2019.
- [9] J. Guerrero-Ibáñez, "SDN-Based Architecture for Improving VANET Performance", IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 4, pp. 2315-2328, 2021.
- [10] A. K. Singh, B. Gupta, Y. Kumar, "Intelligent Traffic Management in VANETs Using Machine Learning and SDN", IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 5, pp. 4567-4578, mayo 2022.
- [11] G. Karagiannis et al., "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions", IEEE communications surveys & tutorials, vol. F, n.º 4, pp. 584-616, Julio 2011.
- [12] T. Nguyen, D. Kim, and S. Park, "5G NR-V2X for Next-Generation Vehicle Network Management: Challenges and Solutions," IEEE Communications Magazine, vol. 61, no. 4, pp. 88-94, Apr. 2023.

- [13] A. Festag, "5G-VANET: A Collaborative Architecture for Reliable and Low-Latency Vehicular Communications", IEEE Communications Magazine, vol. 59, no. 3, pp. 78-84, 2021.
- [14] K. Zhang, "Blockchain-Based Secure Data Management in VANETs", IEEE Internet of Things Journal, vol. 7, no. 8, pp. 7234-7245, 2020.
- [15] L. van den Berg, "Secure V2X Communication Using Blockchain in Amsterdam's Smart Mobility Framework," IEEE Vehicular Technology Conference (VTC-Spring), pp. 1–6, Abril 2022, doi:10.1109/VTC2022-Spring54318.2022.9860602.
- [16] K. Nykänen et al., "MaaS Integration for Energy-Efficient Urban Mobility: The Whim App in Helsinki," IEEE Intelligent Transportation Systems Magazine, vol. 14, no. 3, pp. 102–115, Julio. 2022, doi:10.1109/MITS.2021.3084567
- [17] Y. Zhang et al., "AI-Powered Traffic Optimization in Hangzhou: A Case Study of Alibaba's City Brain," IEEE Access, vol. 9, pp. 148521–148535, octubre 2021, doi:10.1109/ACCESS.2021.3123456.
- [18] J. Li et al., "Real-Time Edge AI for Urban Traffic Management: Lessons from Hangzhou," IEEE Transactions on Sustainable Computing, vol. 6, no. 4, pp. 789–802, diciembre 2021, doi:10.1109/TSUSC.2021.3098765
- [19] Q. Chen et al., "Ultra-Low Latency 5G-V2X Networks for Dynamic Traffic Environments: Shanghai's Pilot," IEEE Communications Magazine, vol. 60, no. 8, pp. 45–51, agosto 2022, doi:10.1109/MCOM.2022.9845123
- [20] X. Liu et al., "Quantum-Resistant Security Protocols for Vehicular Networks in Shanghai's Smart City," IEEE Transactions on Quantum Engineering, vol. 3, pp. 1–12, 2022, doi:10.1109/TQE.2022.3208761.
- [21] H. Yang, X. Liu, y F. Zhao, "Blockchain-Secured Decentralized Management for Vehicular Edge Computing," IEEE Access, vol. 12, pp. 23456-23470, enero 2024.
- [22] M. Singh, S. Kim, "Blockchain-Based Secure Communication in VANETs", IEEE Access, vol. 7, pp. 58266–58280, 2019.
- [23] A. GONZALEZ MARIÑO, F. FONS, y J. M. MORENO AROSTEGUI, "The Future Roadmap of In-Vehicle Network Processing: A HW-Centric (R-)evolution", IEEE Access, vol. 10, pp. 69223-69249, 2022.
- [24] M. S. Al-kahtani, "A Comprehensive Survey on VANETs: Challenges, Architectures, and Future Directions", IEEE Access, vol. 8, pp. 121652-121683, 2020.
- [25] R. Souza, "A Mobility-Aware Routing Protocol for VANETs in Urban Scenarios", IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 6600-6613, 2020.
- [26] A. K. Singh, R. Kumar, and S. Verma, "Enhanced Traffic Management in VANETs Using Machine Learning-Based Routing," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 5, pp. 5123-5135, mayo 2023.
- [27] R. Gupta, S. Patel, and E. Johnson, "AI-Driven Dynamic Fleet Management in Smart Cities," IEEE Access, vol. 11, pp. 45672-45685, 2023.
- [28] J. Zhang, L. Wang, Y. Chen, y M. Li, "A Dynamic Clustering-Based Resource Management Scheme for Vehicular Networks," IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 2, pp. 1234-1245, febrero 2024.
- [29] K. Patel, R. Kumar, y S. Sharma, "SDN-Enabled Adaptive Routing Protocol for Efficient Vehicular Network Management," IEEE Internet of Things Journal, vol. 11, no. 4, pp. 5678-5692, marzo 2024.
- [30] A. Gupta, P. Singh, y T. Nguyen, "Machine Learning-Based Traffic Prediction for QoS Optimization in 5G-V2X Networks," IEEE Vehicular Technology Conference (VTC2024-Spring), pp. 1-6, junio 2024
- [31] M. Alvi, B. Khan, y C. Reyes-Munoz, "Hybrid V2I/V2V Communication for Emergency Message Dissemination in Urban VANETs," IEEE Communications Letters, vol. 28, no. 3, pp. 789-793, marzo 2024.

SOBRE LOS AUTORES

Lic. José Antonio León Martínez graduado de Licenciatura en Ciencias de la Computación en la Universidad de La Habana, actualmente trabaja en la Empresa de Telecomunicaciones de Cuba ETECSA, es profesor Asistente en la Facultad de Telecomunicaciones y Electrónica de la Universidad Tecnológica José Antonio Echevarría de La Habana. Código ORCID 0009-0007-3847-7735

CONFLICTO DE INTERESES

No existen conflictos de intereses.

CONTRIBUCIONES DE LOS AUTORES

- Autor 1: Preparación, creación y desarrollo del artículo, revisión y adecuación de cada una de las versiones, contribución a la idea y organización del artículo, propuesta del tema de investigación y aprobación de la versión

Manuscrito recibido: 05-05-2025, aceptado: 17-08-2025

Sitio web: <http://revistatelematica.cujae.edu.cu/index.php/tele>

final.

Esta revista provee acceso libre inmediato a su contenido bajo el principio de hacer disponible gratuitamente investigación al público. Los contenidos de la revista se distribuyen bajo una licencia Creative Commons Attribution-NonCommercial 4.0 Unported License. Se permite la copia y distribución de sus manuscritos por cualquier medio, siempre que mantenga el reconocimiento de sus autores y no se haga uso comercial de las obras.

