BENÉMERITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN

Estudio de una VANET para aplicaciones en ciudades inteligentes

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

PRESENTA:

MARIANA HERRERA MEJÍA

ASESORES DE TESIS:

M.C. EDNA ILIANA TAMARIZ FLOREZ (FCC)

Dr. RICHARD TORREALBA MELÉNDEZ (FCE)

PUEBLA, PUE. OCTUBRE 2019

DEDICATORIAS

Dedico esta tesis a mis padres quienes me apoyaron todo el tiempo y a mi hermana que siempre estuvo en las noches de desvelo.

A mis compañeros de clase quienes fueron un gran apoyo emocional durante el tiempo en que hice mis estudios y me acompañaron desde el inicio de la carrera.

A Cristian quien me apoyó y alentó para continuar, cuando parecía que me iba a rendir.

A mis maestros quienes nunca desistieron al enseñarme, aun sin importar que muchas veces parecía no mostrar interés en clase, a ellos que continuaron depositando su esperanza en mí.

A los sinodales quienes estudiaron mi tesis y la aprobaron.

A todos los que me apoyaron para escribir y concluir esta tesis.

Para ellos es esta dedicatoria, pues es a ellos a quienes se las debo por su apoyo incondicional.

AGRADECIMIENTOS

A mis asesores, la M.C Edna Iliana Tamariz Flores y al Dr. Richard Torrealba Meléndez por su apoyo y tiempo dedicado a este proyecto de tesis.

Al laboratorio de Caracterización de Sistemas Basados en Microondas FCE-BUAP por permitirme realizar la parte inicial de las simulaciones de mi tesis.

A la Facultad de Ciencias de la Computación por su excelente formación profesional y por gestar un ambiente propicio para el aprendizaje continuo. Por último, agradezco a mi alma mater, la Benemérita Universidad Autónoma de Puebla, por haberme brindado todas las facilidades para mi desarrollo profesional.

Índice

Índice de Figuras

Índice de Tablas

Capítulo 1. Introducción

1.1 Introducción

El concepto de ciudad inteligente (*smart city*) se ha adoptado recientemente debido al crecimiento en las ciudades. Existen dos enfoques principales en los que se basa: el enfoque orientado a la tecnología y a las TICs (Tecnologías de la Información y Comunicación). Específicamente, existen estrategias en la ciudad inteligente que se enfocan en la eficiencia y avances en la infraestructura como el transporte. Por lo tanto, se llama "ciudad inteligente" debido a la magnitud de las TICs y la integración de los datos en los sistemas urbanos.

En la cuestión de transporte, los vehículos llegarán a ser una parte integral de la era moderna de las comunicaciones que promete proporcionar conectividad ubicua, transmisiones ultra-confiables y de baja latencia. Las principales preocupaciones en los estándares de comunicación vehicular actuales, como el IEEE 802.11p, son la falta de baja latencia y transmisiones altamente confiables de comunicaciones periódicas. El estándar existente ha mostrado poca escalabilidad y falta de servicio garantizado en la implementación de redes a gran escala.

La red vehicular ad hoc, VANET por sus siglas en inglés, es una red de vehículos (referidos como nodos) y es una clase de red móvil ad hoc (MANET). Los vehículos se comunican usando la técnica de comunicación corta a distancia (DSRC). Esta red soporta comunicaciones vehículo a vehículo (V2V) y vehículo a infraestructura (V2I) para proporcionar la seguridad y confort a los usuarios por medio de mensajes de tipo difusión o *broadcasting*.

Los servicios de seguridad incluyen evitar la colisión de paquetes por la intersección entre vehículos, advertencias de accidentes de vehículos y advertencias sobre las condiciones de las carreteras.

Para ello, las tecnologías de red inalámbricas se utilizan comúnmente para establecer infraestructuras del Internet de las Cosas (IoT) y en la ciudad inteligente. En una arquitectura de red inalámbrica, la transmisión es en corto alcance y existen mecanismos de autoorganización que llegan a ser útiles e importantes para organizar automáticamente y conectar los nodos para formar la infraestructura inalámbrica. En este caso, el Protocolo de Enrutamiento IPv6 (RPL) para redes de baja potencia y pérdidas (*Low-Power and Lossy Networks*, LLNs) es un ejemplo.

De esta manera, el estándar 6LoWPAN (*IPv6 over Low-Power Wireless Personal Area Networks*) integra infraestructuras basadas en IP y WSNs (*Wireless Sensor Networks*) especificando la manera en que los paquetes IPv6 se enrutan en redes limitadas tales como las redes basadas en el estándar IEEE 802.15.4.

Por lo anterior, la presente propuesta de proyecto se enfoca en el estudio de una VANET en ciudades inteligentes a través del estándar IEEE 802.15.4 a 2.4 GHz. El trabajo se centra en una simulación en el sistema operativo Contiki, realizando la comunicación sólo entre vehículos por medio del estándar 6LoWPAN. A través de los mensajes enviados advirtiendo un choque, se revisará el problema del movimiento en la red y la velocidad.

1.2 Antecedentes del Proyecto.

Con la llegada de nuevas tecnologías inalámbricas se han desarrollado más y más avances para las aplicaciones, debido a que los eventos en la vida real se transforman en datos los cuales pueden ser procesados, guardados y ser utilizados posteriormente o en tiempo real para diferentes propósitos, esto con la ayuda de los nodos con sensores en una WSN.

Las aplicaciones basadas en una VANET son versátiles cuando se consideran en un contexto del ambiente urbano. Existen muchas aplicaciones de comunicación vehicular hoy en día, donde se puede revisar el estado de tránsito de los caminos a un destino específico, marcando diferentes rutas.

Pero debido a las características propias de la red, la actualización de los datos puede demorar y aún más en casos de desastres.

El incremento en la cantidad de vehículos en las ciudades origina embotellamientos. Por tal razón existe la necesidad en ambientes urbanos gestionar y monitorear el tráfico para tomar decisiones, anticipar problemas y coordinar los recursos para una operación eficiente.

Esto dio origen a plantear la propuesta del estudio de una VANET para la seguridad y protección de los ciudadanos mediante el intercambio de mensajes de advertencia entre vehículos. Esta propuesta marca una red inalámbrica basada en 3 nodos para la advertencia de un choque. Un primer nodo móvil enviará un mensaje de advertencia de que existe un choque; un segundo nodo móvil lo recibirá y esperará a un tercer nodo para enviarle la información. De esta manera el usuario tomará sus medidas de seguridad como el cambio de ruta, disminución de velocidad, etc.

1.3 Objetivos Generales y Específicos del Proyecto.

OBJETIVO GENERAL

Realizar una simulación de una VANET en una arquitectura vehículo a vehículo (V2V) para comprender las características de esta red.

Objetivos Específicos

- Estudio del Sistema Operativo Contiki y del simulador Cooja para realizar la simulación de la VANET V2V.
- Establecer el algoritmo que permita el intercambio de mensajes de alerta en una red ad hoc móvil.
- Establecer las características de una VANET simulando un choque entre vehículos en una carretera.

1.4 Infraestructura.

Con respecto al hardware, este proyecto sólo requirió de una máquina con los recursos necesarios para la instalación del sistema operativo Contiki, ya que el trabajo se centra sólo en las simulaciones.

1.5 Estado del Campo o del Arte.

Existen investigaciones sobre la comunicación vehicular que están siendo discutidas. A continuación, se presentan las más importantes:

Pressas A., et al. [1], presentan un ambiente de simulación con vehículos conectados utilizando la librería OMNeT++ y las comunicaciones entre vehículos con base en el estándar IEEE 802.11p. El propósito de este trabajo es establecer una conectividad mediante vehículos y la tecnología de red.

Xia Y., et al. [2], proponen un semáforo inteligente y un protocolo de enrutamiento GTLQR (*Queue Aware Routing Protocol*) para solucionar un problema complejo en una VANET, como lo es la movilidad de los nodos y el constante cambio en la topología de red.

Lin D., at al. [3], proponen una solución de enrutamiento que transmite mensajes en una VANET a través de una arquitectura auto organizada basada en zonas en movimiento en la que se utiliza la comunicación de vehículo a vehículo para facilitar la difusión de la información.

Wang J., et al. [4], implementan un modelo de ciudad inteligente basado en redes de detección vehicular (VSN) para evaluar aplicaciones inteligentes en servicios públicos y gestión de flujo urbano basado en comunicaciones V2V e V2I para la prevención de embotellamientos.

Por otro lado, 6LoWPAN trabaja con paquetes IPv6 sobre el estándar IEEE 802.15.4 basado en redes de aplicaciones las cuales requieren conectividad inalámbrica a tasas muy bajas para dispositivos como los requeridos en una ciudad inteligente. Sin embargo, los trabajos mencionados anteriormente no

especificaron el uso de 6LoWPAN/IEEE 802.15.4. Muchas investigaciones presentan la integración de los protocolos 6LoWPAN e IEEE 802.15.4 basados en una arquitectura de infraestructura para aplicaciones vehiculares del IoT [5] [6], como el que se presenta a continuación.

Tian B., et al. [7], proponen modificar el protocolo RPL para una VANET-WSN, considerando el manejo de la seguridad que los vehículos recolectan mediante un estado del mensaje desde los sensores instalados a lo largo del camino en una arquitectura de infraestructura.

De acuerdo con el estado del arte que se presenta, la red que se quiere simular en este trabajo de tesis no es nuevo, en algunos trabajos ya realizan la evaluación de una VANET o de los protocolos 6LoWPAN/IEEE802.15.4 pero por separado. En este trabajo se quiere considerar además del estudio de una VANET con los protocolos antes mencionados, introducir al manejo del S.O. Contiki para considerar como trabajo futuro una implementación.

El presente trabajo se encuentra organizado en seis capítulos los cuales se detallan a continuación: el Capítulo 2 presenta las redes vehiculares ad hoc (VANET), las arquitecturas que tienen y cómo se compone una red; en el Capítulo 3 se describe el modelo 6LoWPAN como propuesta de herramienta para la simulación de redes vehiculares. Por otro lado, los escenarios de simulación se explican en el Capítulo 4 y así, los resultados arrojados por el simulador se muestran en el Capítulo 5, terminando esta tesis con la conclusiones y trabajo a futuro en el Capítulo 6.

Capítulo 2. Redes vehiculares Ad-Hoc (VANET)

2.1. Introducción

El estilo de vida actual donde se está en constante movimiento ha logrado que las personas busquen medios para transportarse de manera segura y eficaz. Esto conlleva a un incremento gradual de los automóviles sobre la ciudad, por ende, la presencia de constantes accidentes vehiculares.

Con la finalidad de mejorar la seguridad de sus clientes, la industria automotriz se ha basado en las Tecnologías de la Información y la Comunicación (TICs) para proveer al conductor de asistencia, seguridad e información respecto al tráfico [8]**.** Es así como surge el concepto de VANET y todo el proceso que conlleva en lograr que una serie de automóviles logren mantenerse interconectados y transmitiendo información sobre su entorno constantemente.

En este segundo capítulo se abordan los fundamentos principales de una red vehicular Ad-hoc, desde las características principales, los retos a los que se enfrentan, los tipos de arquitecturas que existen, además de los protocolos y estándares que permiten el óptimo funcionamiento de la red.

2.2. Ciudad Inteligente

El significativo crecimiento de la población a través de los últimos años ha orillado a que se generen problemas de infraestructura y servicios para los ciudadanos. Es por ello por lo que las TICs han participado en el desarrollo de una solución respecto al problema planteado a través del uso de redes. El concepto inteligente se relaciona con la ciudadanía inteligente, la economía, la vida y la organización para mejorar la comodidad de la vida con la gestión de los recursos naturales y la ayuda del gobierno. Una ciudad inteligente o *smart city* ofrece soluciones de redes inteligentes que ayudan a organizar la vida diaria [9].

Una ciudad inteligente ofrece diferentes instalaciones basadas en cada objetivo. Algunas son los siguientes.

- Red Inteligente. Un ejemplo general es el marco eléctrico que reúne y distribuye recursos. Una red inteligente es un sistema que asocia a las personas con la tecnología y los sistemas naturales.
- Medidores inteligentes. Está diseñado para proporcionar beneficios al cliente y a la empresa. Los principales componentes utilizados en las ciudades inteligentes son estos medidores, la infraestructura y los dispositivos de control. Se utilizan para calcular el uso de electricidad a través del cual la compañía puede generar facturas y monitorear dispositivos inteligentes.
- Casa inteligente. La casa inteligente sigue las órdenes del propietario relacionadas con la seguridad y la tranquilidad. Los componentes utilizados en el hogar inteligente son móviles, de escritorio e Internet.
- Agua inteligente. Define una variedad de técnicas y sistemas que ayudan a reducir el uso del agua. El manejo inadecuado del uso del agua creará situaciones no constructivas. Necesitamos definir sistemas inteligentes para preservar este recurso natural al:

  1. Conservar el agua ambiental.
  2. Analizar y dar respuesta a los datos para obtener una mayor eficiencia de uso con la ayuda del gobierno.
  3. Controlar los residuos tóxicos y fortalecer la capacidad de respuesta ante situaciones urgentes.
- Smart Health. Ofrece soluciones para el cuidado de la salud con el apoyo de hospitales y redes para mejorar la efectividad del manejo inteligente de pacientes en asociación con farmacias para proporcionar medicamentos rápidamente. Acceso de red a departamentos de desastres que ayudan a proporcionar emergencias médicas mediante el intercambio de información crítica.
- Sistema de transporte inteligente (ITS). Utiliza una técnica de red reciente para resolver problemas en diferentes formas de transporte [9].

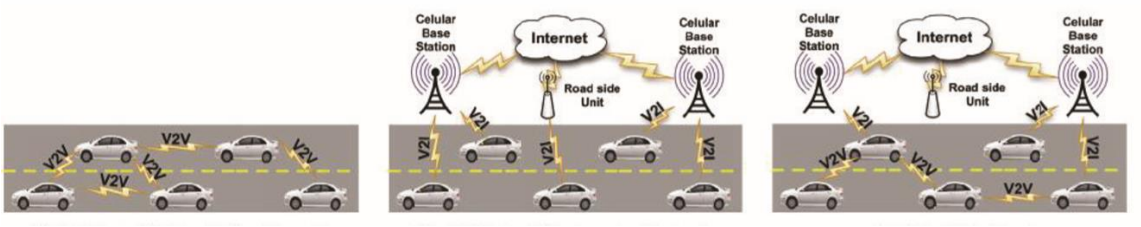
2.3. VANET

Las comunicaciones inalámbricas vehiculares han recibido una atención significativa en los últimos años debido a sus características únicas que las distinguen de las redes móviles ad-hoc (MANET), incluido su rápido ajuste a los cambios de topología y su alta movilidad, lo que les permite formar una red altamente dinámica.

La red vehicular ad-hoc (VANET) es una tecnología que utiliza automóviles en movimiento como nodos para crear una red móvil [10]**.** Este concepto ha tomado un papel de suma importancia en el ámbito de ciudades inteligentes, con la finalidad de aumentar la seguridad entre automovilistas.

Al realizar la implementación de una red ad-hoc es necesario tomar en cuenta ciertas características específicas como la movilidad, el cambio constante, el intercambio de información entre vehículos y el tamaño ilimitado de la red. Además de esto, cada vehículo debe ser implementado por un dispositivo VANET para formar una red ad-hoc y transmitir mensajes en la red. El principal inconveniente de las VANET es la inestabilidad de la red, lo que reduce su eficiencia [11].

La eficacia del sistema de advertencia de colisión en los autos se ha mejorado al permitir la comunicación cruzada entre la cercanía de los vehículos, para que la red pueda comunicar paquetes o información relevante de choque entre ellos. Para el mantenimiento de los nodos y de la ruta es necesario descubrir la ruta por medio de la difusión de mensajes, lo cual es el principal desafío de las VANET debido al comportamiento dinámico de los vehículos [8].



(a) Red Ad-Hoc Vehículo a vehículo *(b) Red Vehículo a Infraestructura* *(c) Arquitectura Híbrida*

Figura 2.1. Arquitecturas VANET [8]

En la Figura 2.1 se muestra los tres tipos de arquitectura VANET que se maneja entre automóviles y el equipo de red para su funcionamiento. A continuación, se describen estas arquitecturas en la Tabla I.

Tabla I. Descripción de arquitecturas en una VANET.

Arquitectura	Descripción
Vehículo a Vehículo (V2V)	En este tipo de arquitectura existe comunicación directa entre automóviles sin depender de una infraestructura. Es comúnmente implementado para aplicaciones de seguridad.
Vehículo a Infraestructura (V2I)	Este tipo, se utiliza principalmente para aplicaciones como la recopilación de información y datos para comunicarse con la infraestructura en la carretera
Hibrido	Dependiendo de la distancia, el vehículo puede comunicarse entre el vehículo y la infraestructura de la carretera con el modo de salto único o salto múltiple [1].

2.4 Comunicación en una VANET

Debido al rápido cambio de la topología de la red provocado por una gran cantidad de automóviles, los mensajes de difusión o *broadcasting* en la VANET producen una gran cantidad de colisiones entre paquetes de información provocado por la transmisión simultánea de mensajes. Esto es llamado tormenta de transmisión, por lo que el *broadcasting* es incapaz de garantizar el éxito de la transmisión sin los paquetes de confirmación (ACK). Para solucionar estos inconvenientes unicast es una mejor opción ya que existe un mecanismo de transmisión y confirmación desde el destino al nodo de origen [12].

La arquitectura VANET se compone de tres dominios:

- Dominio en el vehículo. Está compuesto de una o múltiples unidades a bordo (OBU), avanzados sensores de asistencia al conductor (ADAS) como cámaras, sensores de proximidad, sensores de motor, radares y actuadores como el freno y el volante. La comunicación entre estos sistemas suele ser cableada, basada en el bus de la red de área del controlador (CAN) y en las comunicaciones de la línea de alimentación vehicular (VPLC).
- Red ad-hoc. Está compuesta por vehículos equipados con OBU y unidades de infraestructura (RSU). Una OBU puede verse como un nodo móvil en una red ad hoc y las RSU corresponden a un nodo estático. Las comunicaciones para V2V y V2I se basan en la pila de comunicaciones dedicadas de corto alcance (DSRC / 802.11p).
- Modo infraestructura. Se refiere a las RSU conectadas a Internet a través de alguna puerta de enlace. La existencia de estas RSU u otros hostpots ubicados fuera de la red de carreteras es lo que hace que las ciudades inteligentes estén conectadas [1].

Las OBU del vehículo pueden conectarse a Internet a través de las comunicaciones V2I como se observa en la Figura 2.2. En ausencia de RSU o puntos de acceso, las OBU también pueden comunicarse entre sí y con Internet mediante el uso de redes de radio celulares (3G, 4G, LTE-V).

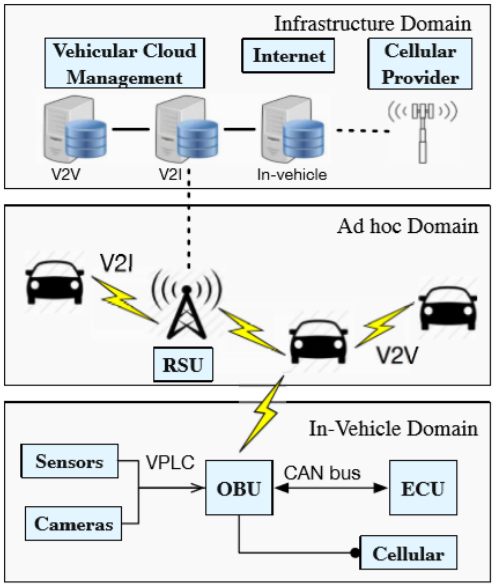


Figura 2.2. Arquitectura del sistema de vehículos conectados [12].

Las VANET proporcionan dos pilas de protocolos: el Protocolo de Internet estándar (IPv6) y el Protocolo de mensajes cortos (WSMP) de WAVE, diseñado para un funcionamiento optimizado en el entorno WAVE.

2.4.1 WAVE (Wireless Access for Vehicular Environments)

Un sistema de acceso inalámbrico en entornos vehiculares es un sistema de comunicación por radio destinado a brindar servicios de transporte sin problemas e interoperables. Estos servicios incluyen aquellos reconocidos por la arquitectura de los Sistemas Inteligentes de Transporte Nacional (ITS) de EE. UU., y muchos otros contemplados por las industrias de infraestructura automotriz y de transporte en todo el mundo, como las comunicaciones entre vehículos e infraestructura y las comunicaciones entre vehículos [13].

Los WAVE distinguen dos clases de canales de radio: un solo canal de control (CCH) y varios canales de servicio (SCH). De forma predeterminada, los

dispositivos con WAVE operan en el canal de control que está reservado para mensajes cortos, de alta prioridad, de control de la aplicación y del sistema.

2.4.1.1 WAVE Short Message Protocol (WSMP)

El protocolo de mensajes cortos funciona para el intercambio rápido de mensajes en un entorno de frecuencia de radio (RF) que varía rápidamente, donde la baja latencia también puede ser un objetivo importante.

Los mensajes cortos de WAVE (WSM) pueden enviarse en cualquier canal. El tráfico IP solo está permitido en SCHs. WSMP permite que las aplicaciones controlen directamente las características físicas, por ejemplo, el número de canal y la potencia del transmisor, que se utilizan para transmitir los mensajes. Una aplicación de envío también debe proporcionar la dirección MAC del dispositivo de destino, incluida la posibilidad de una dirección de transmisión. Los WSM se envían a la aplicación correcta en un destino según el Identificador del Proveedor de Servicios (PSID). Los WSM están diseñados para consumir una capacidad de canal mínima, por lo que se permiten tanto en el CCH como en los SCH.

2.4.2. Estándares involucrados

Las redes WAVE manejan estándares de acceso inalámbrico con funciones particulares para cada capa. En la Figura 2.3 se muestra una jerarquización de estos estándares.

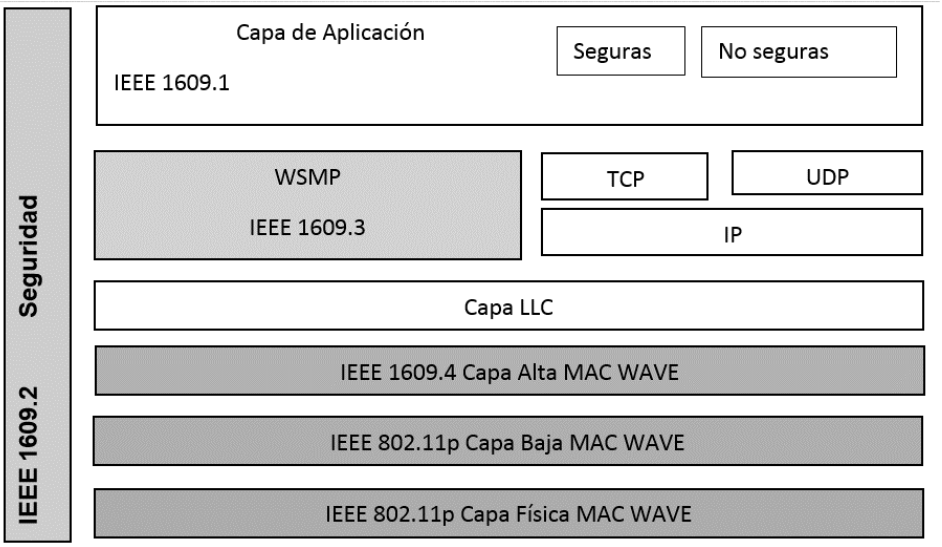


Figura 2.3. Estándares en WAVE

El estándar IEEE 1609 se componen por normas utilizadas en el modelo de comunicación, la estructura de gestión, mecanismos de seguridad y el acceso físico para las comunicaciones en el entorno de las redes WAVE. A continuación, en la Tabla ll se describe con mayor detalle el funcionamiento en cada capa:

Tabla II. Estándar IEEE 1609. [13]

Estándar	Capa
1609.1	Capa superior. Describe los servicios e interfaces, incluidos los mecanismos de protección de seguridad y privacidad.
1609.2	Servicios de seguridad. Especifica una gama de servicios de seguridad para su uso en el entorno WAVE (*Wireless Access in Vehicular Environments*).
1609.3	Capa de red. Define los servicios, que operan en la red y las capas de transporte, en apoyo de la conectividad inalámbrica entre dispositivos basados en vehículos, y entre dispositivos fijos en la vía pública y dispositivos basados en vehículos que utilizan el modo WAVE de 5.9 GHz.
1609.4	Capa inferior. Describe operaciones de radio inalámbricas multicanal que utilizan el IEEE P802.11p, el modo WAVE, el control de acceso al medio y las capas físicas, incluido el funcionamiento del canal de control y los temporizadores de intervalo del canal de servicio, los parámetros para el acceso prioritario, el cambio de canal y Enrutamiento, servicios de gestión y primitivas diseñadas para operaciones multicanal.

Las VANET se centran en la intercomunicación a un corto alcance, con arquitecturas tipo V2V y V2I, como se mencionó anteriormente. Esto con la finalidad de interconectarse cuando cualquier automóvil se una o abandone las regiones de la red. Es posible desarrollar aplicaciones que permitan optimizar los

trayectos en carretera gracias al estándar EEE802.11p, el cual define las capas físicas y de control de acceso al medio, permitiendo las comunicaciones vehiculares en el rango de 5.85-5.925 GHz [11].

El estándar 802.11p define la modalidad de interconexión entre estaciones en áreas limitadas utilizando la radiofrecuencia como medio de transmisión; constituye uno de los estándares de mayor interés para la evolución de las tecnologías de interconexión en áreas locales. En el año 1997 fue lanzada la primera versión y a pesar de que actualmente se encuentra obsoleta, ha marcado un principio para una tecnología con mucho futuro [11]. Inicialmente este estándar fue pensado para redes locales inalámbricas de corto alcance, sin embargo, ha surgido la necesidad de comunicar dispositivos portátiles a velocidad de transmisión elevada.

Otro de los estándares que se ven involucrados en el desarrollo de estas redes, es el IEEE 802.15.4, el cual va enfocado en proporcionar un marco y los niveles más bajos para redes de bajo costo y bajo consumo. Solo proporciona las capas MAC y PHY, dejando que las capas superiores se desarrollen de acuerdo con las necesidades del mercado [14].

Los requisitos principales para el desarrollo de una red vehicular son la comunicación ubicua de bajo costo y baja velocidad entre dispositivos. No pretende competir con los sistemas orientados al usuario final más comúnmente utilizados, como IEEE 802.11, donde los costos no son tan críticos y se demandan velocidades más altas. El concepto de IEEE 802.15.4 es proporcionar comunicaciones a distancias de hasta 10 metros y con velocidades de transferencia de datos máximas de 250 kbps.

El tamaño máximo de una trama MAC 802.15.4 es de 127 bytes. Una trama MAC tiene un campo fijo de 5 bytes, y el tamaño del campo de dirección varía de 4 a 20 bytes dependiendo del propósito. El IEEE 802.15.4 permite usar un algoritmo de encriptación usando claves simétricas. Consumirá hasta 21 bytes al transmitir información de cifrado. Para resumir, un nodo 802.15.4 puede transferir datos con tamaño de carga útil que va de 81 a 102 octetos [13].

2.5. Aplicaciones de una VANET en Ciudades Inteligentes.

La VANET es un tipo de red que ha recibido un gran interés en los últimos años por parte de investigadores, organismos de normalización y desarrolladores, ya que tiene el potencial de mejorar la seguridad vial, mejorar el tráfico y la eficiencia de los viajes, así como hacer el transporte más conveniente y cómodo tanto para los conductores como para los pasajeros [12]**.**

Construir ciudades inteligentes se ha convertido en un objetivo fundamental para mejorar la gestión de los flujos urbanos que dependen de las TICs. Inicialmente toda la atención estaba centrada en la implementación de carreteras más seguras y eficientes. Sin embargo, el avance en las tecnologías inalámbricas y su aplicación en los automóviles hace posible utilizar el Sistema de Transporte Inteligente (ITS). Los objetivos de ITS se muestran a continuación:

- Proteger y salvar el medio ambiente.
- Mejorar la seguridad vial.
- Incrementar la efectividad en el sistema de transporte.
- Para reducir el tiempo de viaje.
- Para reducir los gastos de viaje.

Las redes VANET tienen como función principal monitorear y controlar el tráfico vehicular utilizando el concepto de comunicación V2V y V2I. Enviando mensajes críticos en tiempo real a los vehículos que vienen entre distintos carriles y con esto orientarlos para tomar una ruta alternativa evitando la congestión del tráfico. Si utilizamos los beneficios de VANET en la ciudad inteligente, la información en tiempo real relacionada con la congestión del tráfico se puede brindar a los dispositivos inteligentes de las personas, con la finalidad de que puedan organizar sus trayectorias desde casa [13].

Algunas de las aplicaciones que se pueden implementar gracias a las redes VANET se describen a continuación.

2.5.1. Seguridad vial.

Las VANET tienen como propósito el estar constantemente monitoreando y recolectando información respecto a la carretera con la finalidad de prevenir algún tipo de percance. Funcionan como base para el estudio de técnicas a implementar en redes vehiculares, agrupadas en:

- Prevención de colisiones: La RSU detecta el riesgo de una colisión entre dos autos y advierte a los conductores mediante la OBU.
- Notificación de señalética: Tiene la finalidad de advertir a los conductores respecto a señales viales, así como brindar constantemente asistencia durante el recorrido.
- Gestión de incidentes: Son utilizadas ante un accidente de tránsito.

2.5.2. Eficiencia de tráfico.

Con la finalidad de mejorar las condiciones del flujo de tránsito mediante la gestión de los vehículos en la vía y las condiciones de esta. Estas aplicaciones se dividen en dos subcategorías:

- Gestión del tráfico: Resguardan información respecto al flujo vehicular y controlan desde las RSU hasta semáforos y cobro de peajes.
- Monitoreo del tráfico: A través de aplicaciones donde los usuarios pueden monitorear vehículos y condiciones de las carreteas, así, en caso de imperfecciones se les notifica a las autoridades como a otros conductores.

2.5.3. Información y entretenimiento.

Van enfocadas en proporcionar servicios de entretenimiento e información de interés a los conductores como se observa en la Figura 2.4. Estas se agrupan en:

- Entretenimiento: A través de estas aplicaciones los conductores pueden tener acceso a internet, jugar en línea, mirar contenidos

multimedia, entra otras. Esto ya sea con el uso de RSU o con puntos de acceso Wi-Fi.

- Información del contexto: Muestran información respecto a sitios de interés, locales, centros de atracciones, basándose en la localización.

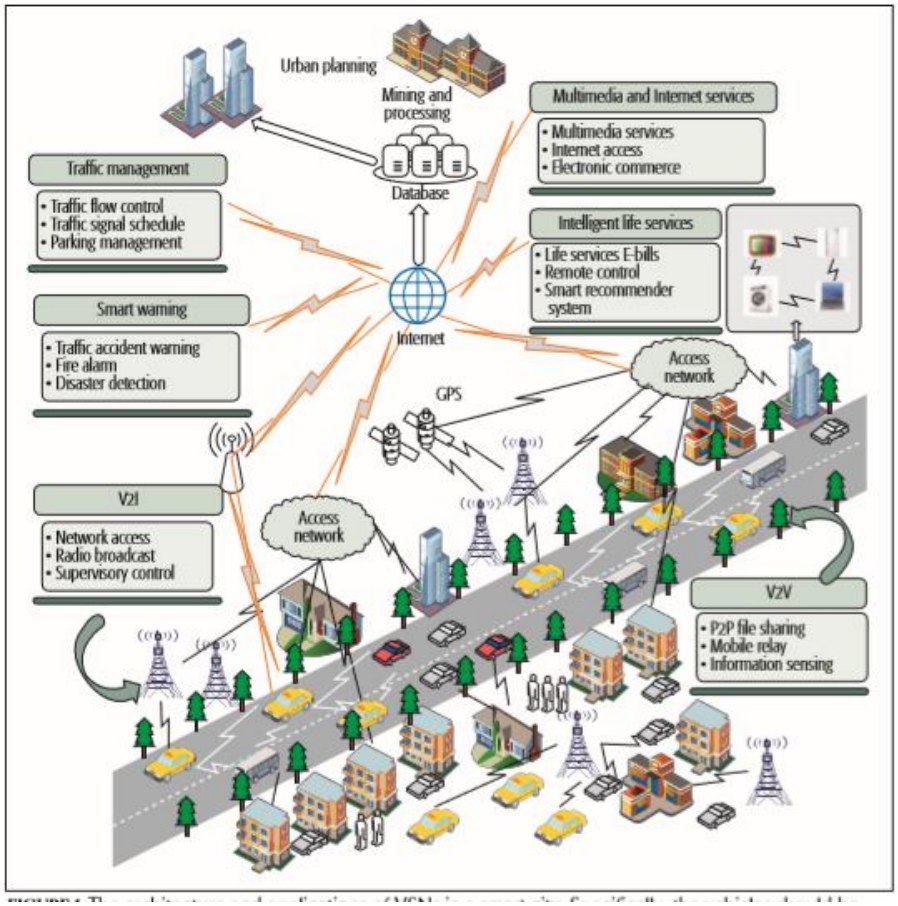


Figura 2.4. Arquitecturas [4]

2.6. Conclusiones del capítulo 2.

Las redes vehiculares ad-hoc (VANET) tienen un futuro prometedor en el ámbito de ciudades inteligentes, con objetivos muy claros a cubrir y un campo de estudio suficientemente amplio, como lo es el proporcionar seguridad y aumentar el rendimiento de los automóviles. Sin embargo, esto también conlleva el reto primordial con el que se enfrenta, el cual es que se trabaja con redes en constante movimiento y por ende provoca cierta inconsistencia al arrojar los datos en el momento de que se pierde la conectividad, así como el tamaño

ilimitado de la red. Estos obstáculos han alentado el desarrollo de protocolos con rutinas eficientes, además de la interacción constante entre distintos estándares.

Capítulo 3. 6LoWPAN para Redes Vehiculares.

3.1. Introducción

Internet y algunas otras redes basadas en TCP/IP han ofrecido soporte para aplicaciones como el envío de archivos, correo electrónico además de accesos remotos, sin embargo, en la actualidad, con la creciente demanda de estar conectado de manera constante en las diferentes redes, principalmente en la World Wide Web (www), ha puesto en jaque la funcionalidad a futuro del protocolo IPv4.

Este capítulo presenta al protocolo Ipv6 y el enfoque por el cual se está apostando al incremento en el uso de nuevas tecnologías. En este tema se presenta, además el tema de las redes de baja potencia de área personal también conocidas como LoWPAN, de esta manera se explica el modelo para redes de área personal utilizando el protocolo IPV6, denominado 6LoWPAN. Adicionalmente, se presenta el S.O. Contiki con la herramienta de simulador que proporciona, llamada COOJA, los cuales trabajan para este tipo de redes.

3.2. IPv6

Para definir que un entorno se encuentra interconectado, este debe permitir el tráfico en tiempo real, esquemas flexibles de control de congestión y características de seguridad. Ninguno de estos requisitos se cumple fácilmente con la IP existente [15]. Los usuarios de Internet en todo el mundo han aumentado de manera exponencial cada año con el uso de nuevos dispositivos, lo que genera escasez en los recursos de direcciones. IPv4 usa el identificador de 32 bits, de modo que hay 4.3 mil millones de identificadores numéricamente, pero la asignación de direcciones basada en clases permite solo 0.5 o 1 mil millones de espacio de direcciones [16], la cual no es adecuada para el crecimiento exponencial de las redes.

A partir de esta problemática, fue clara la necesidad de un nuevo protocolo IP, ya que el protocolo IPv4 se volvió muy complejo por el hecho de que los protocolos adicionales deben instalarse con IPv4 para que los dispositivos que usan IP logren funcionar correctamente y se adapten a aplicaciones más avanzadas con la finalidad de que los países no presenten dificultades al conectarse a las redes.

El nuevo protocolo de Internet IPv6, anteriormente denominado protocolo de Internet de próxima generación se propuso a partir de la década de 1990 como un sucesor de IPv4 y se publicó como RFC 1752.2. Más adelante, el protocolo IPv6 se estandariza en RFC 1883, que eventualmente se vuelve obsoleto por RFC 2460.3 [16].

En julio de 1994, se comenzó a trabajar en la creación del nuevo protocolo, que finalmente se publicaría como IPv6 en 1998. Las características clave introducidas por IPv6 fueron:

- Formato de encabezado simplificado
- Capacidad de direccionamiento expandida
- Compatibilidad mejorada para extensiones y opciones
- Etiquetado de flujo
- Capacidades de autenticación y privacidad [17]

Otra de las características importantes en este protocolo es que mientras que el IPv4 requiere de algunos otros protocolos definidos independientemente para su funcionamiento, IPv6 ya cuenta con estas funciones dentro de sí mismo.

A pesar de que IPv6 ya se ha implementado, varios expertos han dudado de su uso y creen que los protocolos NAT, *Application Level Gateway* (ALG) y DHCP ayudarán a IPv4 a resolver el problema de escasez de direcciones resultante de la dirección de 32 bits [16].

3.2.1. Arquitectura de IPV6

A pesar de que IPv4 ha logrado satisfacer las necesidades de los usuarios hasta la actualidad, IPv6 tiene varias ventajas como sucesor del protocolo IP que es necesario mencionar. En la Tabla lll se muestran las características del protocolo de nueva generación con sus respectivas justificaciones.

Tabla III. Características de IPv6 [16].

Característica	Explicación
Capacidad de direccionamiento expandido	El tamaño de la dirección IPv6 es de 128 bits de longitud y cuatro veces más que la longitud de la dirección de IPv4. Esta mayor longitud permite varias características deseables como: • La delegación jerárquica y la gestión del espacio de direccionamiento, • El número prácticamente ilimitado de asignación de direcciones a dispositivos de Internet • La configuración automática de dispositivos de Internet.
Formato de encabezado simplificado	El tamaño del encabezado IPv4 varía de 20 bytes a 20 más la longitud del campo de opción, pero el campo de opción es muy variable para saber dónde comenzará el campo de datos. Algunos campos en el Encabezado de IPv4 se eliminan o se mueven al Encabezado de opción para simplificar y reducir el costo de procesamiento común de los paquetes en IPv6.
Auto configuración	El dispositivo habilitado para IPv6 puede configurarse dinámicamente cuando se conecta. Cuando un dispositivo IPv6 se inicia, configura automáticamente su dirección de enlace local con varias direcciones de multidifusión y obtiene o construye su dirección IP global.
Proporcionar calidad de servicio	Las etiquetas de flujo son etiquetas predefinidas para clasificar los paquetes de datos para liquidar las solicitudes de calidad de los compañeros que se comunican. El campo Tipo de servicio (ToS) en formato de encabezado IPv4 se define para el propósito similar. Sin embargo, la mayoría de los enrutadores IPv4 no admiten este campo.
Seguridad Integrada	Para la seguridad de la red en IPv4, se diseña IPsec. Es ampliamente utilizado para la red privada virtual (VPN). Sin embargo, su soporte es opcional en IPv4. IPsec es obligatorio en IPv6.
Movilidad mejorada	La optimización de ruta es posible en el IPv6 móvil. Los mecanismos de autenticación para

	el nodo móvil se proporcionan en el proceso de optimización de ruta.

Algunos campos del encabezado de IPv4 se eliminan por completo y se vuelven obsoletos, se mueven a los encabezados de extensión o se asignan con diferentes nombres de campo con funciones ligeramente modificadas. Además, el campo “etiqueta de flujo” con longitud de 20 bits como recientemente se ha introducido en IPv6 aún se está desarrollando.

3.2.2. Estructura de la dirección IPv6

La dirección de IPv6 se representa por el sistema hexadecimal que utiliza para identificar de forma única una interfaz de red y lograr el envío de paquetes entre hosts. Estas direcciones tienen algunas características como la posibilidad de configuración automática aun cuando los enrutadores no estén habilitados, además del desacoplamiento entre el ID de host y la dirección de red, y que estas direcciones se calculan desde la capa MAC. Una de las diferencias entre IPv4 e IPv6 es el espacio de direcciones, ya que en lugar de utilizar 4 octetos como IPv4, IPv6 utiliza 128 bits agrupados en hextetos que, de acuerdo con esto resultan 8 hextetos, mostrando un total de 32 valores hexadecimales. En la Tabla IV se muestran estas diferencias.

Tabla IV. Diferencias entre IPv4 e IPv6.

Característica	IPv4	IPv6
Tamaño de dirección	32-bit	128-bit
Formato de dirección	Decimal	Hexadecimal
Separación de valores	Un punto (.)	Dos puntos (:)
Número de direcciones	2^{32}	2^{128}
Agrupación de bits	4 octetos	8 hextetos
Cantidad de números en la dirección.	4 números decimales	32 números hexadecimales
Máscara de subred	Sí	No
Dirección de broadcast	Sí	No

Las longitudes de las ID individuales que conforman la estructura de una dirección IPv6 se basan en la regla **pi = 3.14**, que significa **3 hextetos** para el Global ID, **1 hexteto** para el ID de subred y **4 hextetos** para el ID de interfaz. A

continuación, se presenta en la Figura 3.1 la estructura de Ipv6 y se explica cada uno de estos IDs.

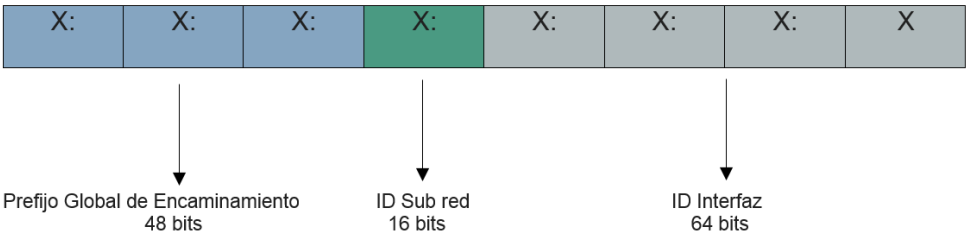


Figura 3.1 Estructura de la dirección IPv6

ID del Prefijo de Enrutamiento Global-48 bits. Es la porción de prefijo o de red y se utiliza para identificar direcciones especiales o rango de direcciones asignadas a un sitio.

IPv6 al no utilizar una dirección de máscara de subred, se basa en la duración de prefijo que indica la porción de red mediante la notación **/Prefijo**. Esta duración puede ir de 0 a 128 pero la duración típica es de /64.

ID de Subred-16 bits. Este ID también se conoce como agregador de nivel de sitio (SLA) y es utilizado para identificar un enlace dentro de un sitio.

ID de interfaz-64 bits. Este ID identifica una interfaz en un enlace, el cual es único. El ID se construye a partir de una identificación MAC de 48 bits expandiéndola al identificador único extendido de 64 bits (EUI). El proceso que se sigue para obtener este ID se muestra en la Figura 3.2:

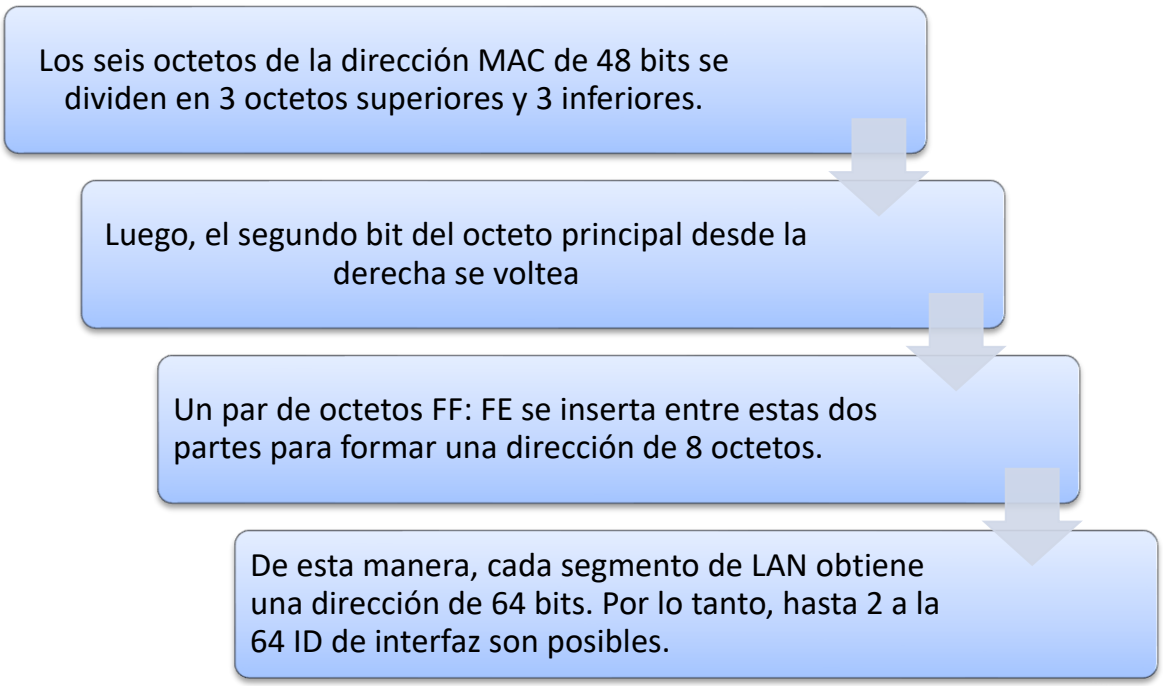


Figura 3.2 Formación de una dirección EUI a partir de la dirección MAC [18].

Ahora bien, como ejemplo se muestra en la Figura 3.3 el proceso que se mencionó anteriormente:

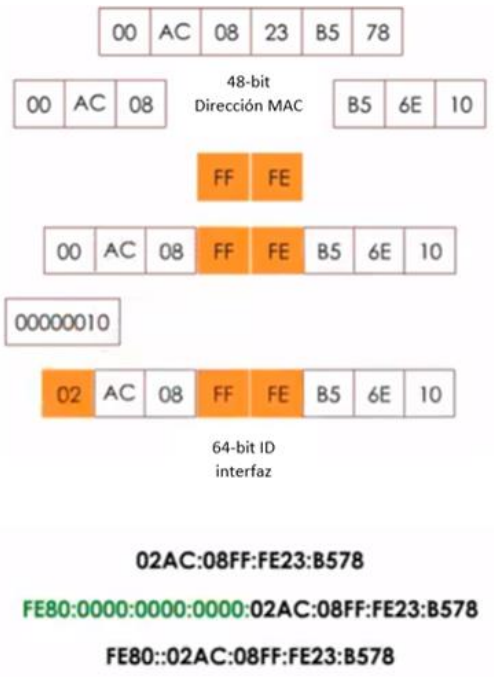


Figura 3.3. Ejemplo del Proceso EUI 64.

3.2.3 Tipos de direcciones

Con el IPv6 una interfaz puede tener varias direcciones. Los tres ámbitos son especialmente importantes porque están definidos para todos los tipos de direcciones [19]. Estas direcciones se clasifican en:

Unicast. Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado solo a la interfaz identificada con esta dirección. Es el equivalente a las direcciones IPv4 actuales. En la Tabla V se presentan los tipos de direcciones unicast con sus características [18].

Tabla V. Direcciones IPv6 unicast.

Direcciones IPv6 unicast	Características	Dirección IPv6
Unicast global	Son similares a las direcciones IPv4 públicas porque son globalmente única y enrutables en Internet.	2000::/3 a 3FFF::/48
Link-local	Establecen comunicación con otros dispositivos que pertenecen al mismo enlace local. Están limitadas a un único enlace por lo que no pueden enrutarse más allá de este enlace. Toda interfaz la tiene.	Rango FE80::/10 a FEBF::/10
Loopback	Es utilizada para que los hosts se envíen paquetes a sí mismos, por lo que no se puede asignar a una interfaz. Tienen la misma función que en IPv4 127.0.0.1	::1/128 o ::1
Dirección sin especificar	Esta dirección no se puede asignar a una interfaz ya que se utiliza como dirección de origen.	::/128 o ::
Local única	Estas direcciones solo realizan conectividad entre dispositivos que se encuentran dentro de un sitio. Son similares a las direcciones IPv4 privadas.	Rango FC00:/7 a FDFF::/7

Anycast. Una dirección anycast IPv6 es una dirección que se asigna a más de una interfaz de red, con la propiedad de que, si un paquete se envía a una dirección anycast, este se enruta a la interfaz más cercana que tenga dicha dirección de acuerdo con las métricas de los protocolos de enrutamiento.

Las direcciones anycast son asignadas de acuerdo con el espacio de direcciones unicast, utilizando cualquiera de los formatos definidos para direcciones unicast. De esta forma, las direcciones anycast no se pueden

distinguir sintácticamente de las unicast. Cuando una dirección unicast se asigna a más de una interfaz, ésta se convierte en una dirección anycast y los nodos donde esta dirección es asignada deben configurarse explícitamente para que sepan que es una dirección anycast.

Multicast. Una dirección multicast IPv6 es un identificador para un grupo de interfaces. Una interfaz puede pertenecer a cualquier número de grupos multicast. Las direcciones IPv6 multicast tienen el prefijo FFxx::/8.

3.2.4 Reglas de compresión

Para expresar la dirección IPv6 de longitud de 128 bits en cadenas de texto, existen tres formatos; formato nativo, formato comprimido y formato mixto. Al igual que la notación de 'dirección / prefijo' en IPv4, estos tres formatos se pueden escribir con notación de prefijo. Por ejemplo, 1111: 2222: 3333: 0: 0: 0: ABCD: 5678 es posible. **No es necesario escribir 0 inicial o 0s sucesivos en cada campo de direcciones** como se verá a continuación [16].

- **Formato sin compresión de dirección IPv6 (habitual)**

Este formato llamado también como formato nativo está compuesto de los ocho campos de 4 valores hexadecimales separados por dos puntos. En la Tabla VI se muestran algunos ejemplos de direcciones en su modo nativo.

Tabla VI. Formato nativo IPv6.

Direcciones en formato nativo de IPv6
0000:0000:0000:0000:0000:0000:0000:0000
0000:0000:0000:0000:0000:0000:0000:0001
1111:2222:3333:0000:0000:0000:1234:5678
FE80:0000:0000:0000:0000:0000:0000:0001
3FFE:0B00:0C18:0001:0000:1234:AB34:0002

- **Formato comprimido**

Es normal que en IPv6 existan grandes cadenas de ceros dentro de una dirección. En estos casos se han establecido algunas reglas para suprimir los valores consecutivos ante dos situaciones: cadenas sucesivas de ceros y cadenas con ceros al inicio.

- *Cadenas sucesivas de ceros*

Cuando se presentan de uno a múltiples campos de ceros, es legal representar estos como ceros ó :: (doble dos puntos). Sin embargo, es permitido usarlo una sola vez en la escritura de la dirección. A continuación, en la Tabla Vll se muestran algunas direcciones comprimidas con base en esta regla:

Tabla Vll. Formato comprimido 1.

Formato Nativo	Formato Comprimido
0000:0000:0000:0000:0000:0000:0000:0000	::
0000:0000:0000:0000:0000:0000:0000:0001	::0001
1111:2222:3333:**0000:0000:0000**:1234:5678	1111:2222:3333::1234:5678
FE80:**0000:0000:0000:0000:0000:0000**:0001	FE80::0001
3FFE:0B00:0C18:0001:**0000**:1234:AB34:0002	3FFE:0B00:0C18:0001::1234:AB34:0002

- *Cadenas con ceros al inicio*

Este método se aplica para cada uno de los campos hexadecimales que tienen uno o más ceros al inicio. Esto quiere decir que, **si hay uno o más ceros al inicio de cada campo, estos pueden ser suprimidos. Sin embargo, si cada caracter del campo es cero se puede que al menos uno de estos se debe mantener**. En la Tabla Vlll se explican algunos ejemplos empleando este mecanismo.

Tabla VIII. Formato comprimido 2.

Formato Nativo	Formato Comprimido
0000:0000:0000:0000:0000:0000:0000:0203:**0**253:**00**21:**000**3	0:0:0:0:0:0:203:253:21:3 ó ::203:253:21:3
0000:0000:0000:0000:0000:FF00:CE7B:1F01	0:0:0:0:0:FF00:CE7B:1F01 ó ::FF00:CE7B:1F01

- **Formato mixto**

La dirección IPv6 mixta se genera de la siguiente manera: x: x: x: x: x: x: x: a.b.c.d, donde x indica cuatro dígitos hexadecimales y a.b.c.d es la dirección IPv4. Este tipo de dirección permite que un nodo en una red pública IPv4 obtenga conectividad IPv6 sin el soporte de un enrutador o sin ningún cambio en la topología de la red a la que pertenece. El formato de dirección comprimido también se puede aplicar para el formato de dirección mixta [16].

Tabla IX, Formato Mixto

Formato Nativo	Formato Comprimido
0:0:0:0:FFFF:192.1.56.10	:: FFFF:192.1.56.10
FE80:0:0:0:0:0:0:129.141.52.38	FE80::129.141.52.38
0:0:0:0:0:0:FFFF:203.253.21.3	::FFFF:203.253.21.3

3.3. Redes LoWPAN

Las redes inalámbricas de área personal de baja potencia (Low Power Wireless Personal Area Networks) representan el futuro de dispositivos integrados en el mundo diario, abarcando áreas de interés desde la medicina hasta la agricultura y obviamente en el ámbito de las telecomunicaciones donde la necesidad de mantenerse conectado al Internet es muy alta sin decir, fundamentales.

Para el desarrollo de aplicaciones basadas en el IoT las redes inalámbricas de área personal WPANs (Wireless Personal Area Networks) deben contar con la capacidad de recolectar información, además de ser escalables y funcionales para lograr su integración con la reciente arquitectura de Internet. Este tipo de redes abarcan dispositivos que cumplen con el estándar

IEEE 802.15.4 y trabajan juntos para conectar el entorno físico a las aplicaciones del mundo real.

Los dispositivos IEEE 802.15.4 se caracterizan por su corto alcance, baja velocidad de bits, bajo consumo y bajo costo. Muchos de los dispositivos que utilizan radios IEEE 802.15.4 tendrán limitaciones en su potencia de cálculo, memoria y disponibilidad de energía [20]. El grupo de trabajo IEEE 802.15.4 se fundó en diciembre de 2000 y se dedica a definir un tipo de tecnología de acceso a redes inalámbricas portátil de bajo costo para dispositivos fijos / móviles. En la Figura 3.4 se muestra la arquitectura de las redes LoWPAN, como se observa, el estándar IEEE 802.15.4 abarca únicamente las capas inferiores Física y de Enlace (PHY y MAC respectivamente).

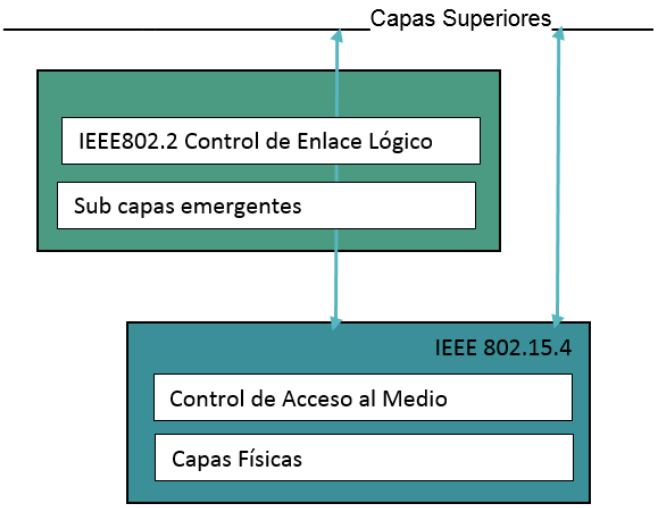


Figura 3.4. Arquitectura Redes Inalámbricas Personales [21].

3.4. IPv6 sobre LoWPAN

En general, las redes de sensores tienen ciertas limitaciones con la capacidad de la red, ya que el IEEE 802.15.4 solo prescribió el estándar de PHY y MAC. Sin embargo, al incluir el estándar IPv6 se logra que los paquetes se transmitan bajo la red 6LoWPAN. Este estándar fue establecido formalmente por IETF para instituir el estándar LR-WPAN (Low-Rate WPAN) basado en IPv6, el propósito de este grupo es introducir IPv6 en LR-WPAN que toma IEEE 802.15. 4 como su estándar básico de capa inferior [21]. 6LoWPAN es una capa de adaptación IPv6

estandarizada por IETF que permite la conexión IP a través de redes de baja potencia y con pérdidas. La extensión de IP a LoWPAN se enfrenta a desafíos diferentes a los de la red tradicional [21]. El propósito es crear un conjunto de encabezados que permitan direcciones IPv6 con grandes encabezados y que se compriman en más pequeños desde 40 bytes hasta 11 bytes de longitud.

La interoperabilidad entre IPv6 y la red LoWPAN se debe a los enrutadores de frontera con soporte de 6LoWPAN. Dentro de la red 6LoWPAN, los enrutadores o los hosts no necesitan trabajar con todos los formatos de encabezado de IPv6 o UDP.

3.4.1. Pila de protocolos

La pila de protocolos de 6LoWPAN se conforma por seis capas en las que cada una cuenta con su respectivo protocolo adaptado para dispositivos de bajo consumo. Como se puede observar en la Figura 3.5, para implementar la conexión perfecta de la capa MAC y la capa de red, el grupo de trabajo IETF de 6LoWPAN sugirió que se agregue una capa de adaptación entre la capa MAC y la capa de red para lograr la compresión del encabezado, la fragmentación, el reensamblaje y el reenvío de la ruta de malla [21].

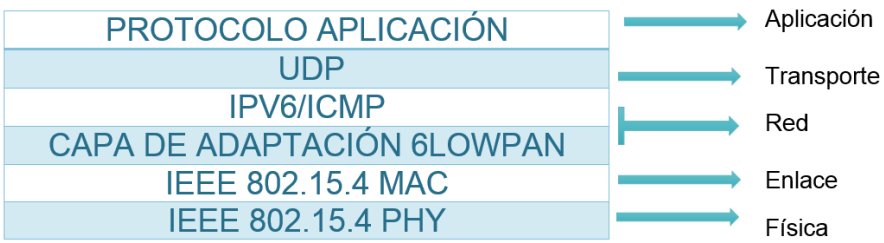


Figura 3.5. Pila de protocolos del modelo 6LoWPAN.

La capa de adaptación tiene como funciones principales las siguientes:

1. Compresión del encabezado TCP/IP.
2. Fragmentación y reensamblado de paquetes.
3. Enrutamiento.

En la Tabla X se muestran algunos factores a considerar en la arquitectura de IP sobre IEEE 802.15.4 para cada capa:

Tabla X. Factores considerados en el modelo 6LoWPAN [18].

CARACTERÍSTICA	EXPLICACIÓN
Diseño de cabecera	En una red IP estándar, un encabezado de paquete IP es de 40 bytes, mientras que IEEE 802.15.4 admite una MTU (Unidad Máxima de Transferencia) de 127 bytes.
Fragmentación de paquetes	El requisito de interoperabilidad implica que la longitud del paquete entrante de la red IP a menudo puede ser muy grande. Los enlaces IPv6 pueden admitir hasta 1280 bytes.
Enrutamiento de la capa de enlace	Un solo nodo basado en IEEE 802.15.4 puede tener múltiples radios. El origen, el destino o ambos pueden usar direcciones cortas de 16 bits o direcciones largas de EUI (Identificador Único Extendido) de 64 bits.
Enrutamiento de la capa IP	IEEE 802.15.4 es compatible con múltiples radios, por lo que puede utilizar cualquiera de las radios disponibles en un solo salto.
6LoWPAN impacto en la energía	La implementación de IP sobre IEEE 802.15.4 pone ciertos costos indirectos esenciales. La optimización de los gastos generales resulta un desafío.

Es útil mencionar que la capa de transporte del modelo 6LoWPAN no proporciona conexión TCP, en su lugar utiliza UDP como medio de transporte. En cierto sentido, 6LoWPAN puede verse como una capa de adaptación para manejar el enrutamiento, la fragmentación y el reensamblaje sobre la capa MAC IEEE 802.15.4 [18].

3.4.2. Compresión, Fragmentación y Reensamblado

La tecnología inalámbrica de baja potencia admite el direccionamiento de la capa de enlace. A partir de ahí surge la necesidad de mapeo entre el direccionamiento de la capa de enlace y el direccionamiento de la capa de red, que se logra mediante la compresión.

A continuación, se mencionan algunos puntos importantes al realizar la compresión de encabezados:

- Los nodos forman parte de una subred IPv6 con direcciones MAC únicas.
- El prefijo global es conocido por todos los nodos en la red, mientras que el prefijo local está vinculado mediante un formato de compresión de encabezado.
- Solo se puede usar el encabezado comprimido para el prefijo local.
- Las direcciones de multidifusión también se comprimen.
- El esquema de compresión se basa en el concepto de encabezados apilados.
- El encabezado comprimido se encapsula dentro de la carga útil de la trama MC del estándar 802.15.4 [18].

3.4.3 Enrutamiento

El enrutamiento por lo general tiene lugar en la capa de red, sin embargo, con el modelo 6LoWPAN y gracias a la capa de adaptación como se observa en la Figura 3.6, el enrutamiento se puede llevar a cabo ya sea en la capa de enlace (*mesh-under*) o en la de red (*route-over*).

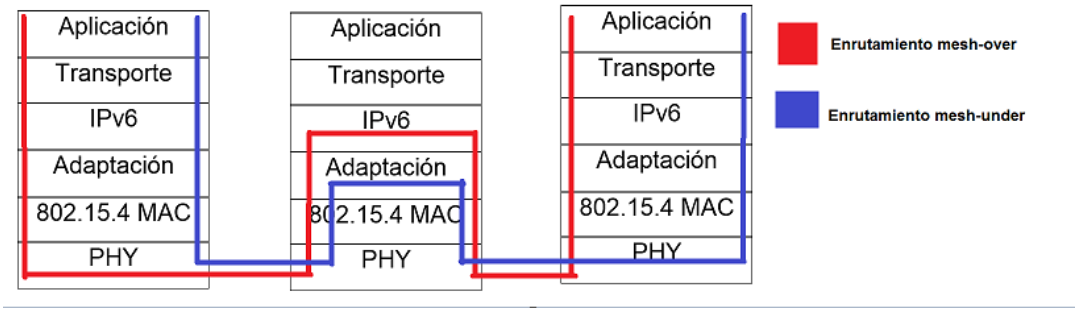


Figura 3.6. Enrutamiento en redes 6LoWPAN.

En el tipo de enrutamiento de malla (*mesh-under*) el reenvío se realiza desde la capa de enlace haciendo uso de los encabezados 6LoWPAN. Para enviar el paquete al destino, se utiliza la dirección corta EUI de 64 o 16 bits [18]. En la Figura 3.7 se menciona de manera general como se realiza este tipo de enrutamiento:

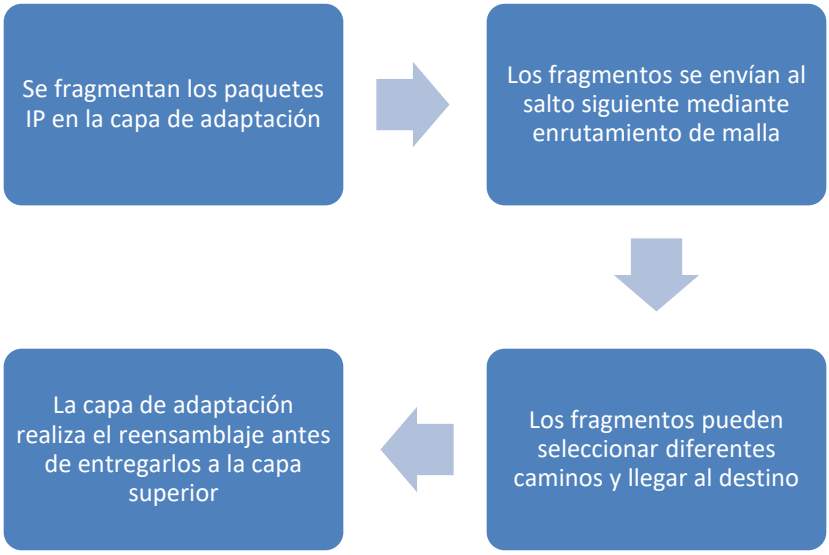


Figura 3.7. Enrutamiento "*mesh-under*".

Ahora, las decisiones de enrutamiento "mesh-over" se realizan en la capa de red. Cada salto de capa de enlace es también un salto de IP. La capa de red utiliza el encabezado IP encapsulado para tomar una decisión sobre el enrutamiento [18].

Existen algoritmos de enrutamiento de estado de enlace, en los cuales se mantienen las rutas a través del crecimiento de ámbito. Por otro lado, los algoritmos de enrutamiento basados en vectores de distancia constantemente realizan actualizaciones de enrutamiento para propagarlas. Ambos enfoques no son adecuados para redes con pérdidas de ancho de banda bajo.

3.4.4 Protocolo de aplicación restringida (CoAP)

Al ser un trabajo basado en redes de baja potencia existe la necesidad de que el servicio de transporte en la capa de red cumpla con los requisitos de longitud mínima en sus mensajes, es por lo que el Protocolo de Aplicación Restringido (CoAP) está diseñado para cumplir con varios requisitos que se originan en una red limitada. Aunque es muy parecido a HTTP, CoAP tiene un bajo riesgo respecto a fiabilidad y seguridad, además de permitir la multidifusión.

A diferencia de HTTP que hace uso de TCP como servicio de transporte, CoAP utiliza UDP con los métodos REST, GET, POST, PUT y URI como HTTP

con la finalidad de hacerlo más fiable, además, emplea un mecanismo de retransmisión y proporciona enlaces UDP para la confiabilidad y el soporte de multidifusión logrando que sea un protocolo REST (Transferencia de Estado Representacional) eficiente y limpio.

El protocolo REST admite cuatro tipos diferentes de mensajes:

1. **Confirmación**: requiere un acuse de recibo.

2. **No confirmable**: no requiere ningún reconocimiento.

3. **Reconocimiento**: reconoce un mensaje.

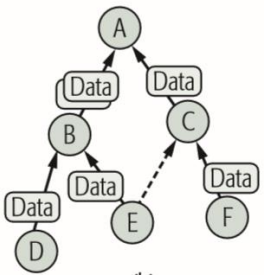
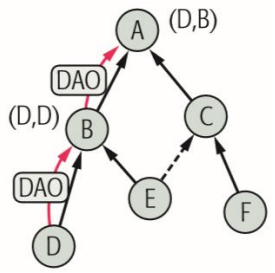
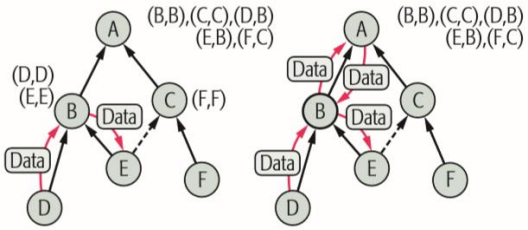
4. **Restablecer**: indica que se ha recibido un mensaje configurable pero falta el contexto [18].

3.5. Protocolo de Enrutamiento para Redes de Baja Potencia y Pérdida, RPL

El Protocolo de Enrutamiento IPv6 para Redes de Baja Potencia y Pérdida RPL es un algoritmo basado en vector de distancia con los objetivos de diseño detallados en una serie de RFC [18] diseñados para WSN a gran escala estandarizado por la IETF en 2011. RPL se ha vuelto rápidamente en el protocolo de enrutamiento para IoT para dispositivos que utilizan IEEE 802.15.4 en sus capas MAC y PHY.

El protocolo admite tres tipos diferentes de tráfico: punto a punto (tráfico entre nodos), punto a multipunto (tráfico hacia abajo) y multipunto a punto (tráfico hacia arriba a la raíz). El concepto principal de RPL es que los nodos pueden autoorganizarse formando una topología de árbol con una raíz en la parte superior [22]. En la tabla XI se explica con mayor detalle las aplicaciones de cada tipo de comunicación:

Tabla XI. Enrutamiento con RPL [23].

Multipunto a Punto	Punto a Punto	Punto a Multipunto
Requerida por los dispositivos con capacidades de detección, que normalmente monitorean el ambiente mediante la adquisición periódica de muestras de cantidades físicas y las envían a una unidad central.	Sirve como una alternativa a un controlador centralizado que recopila datos y emite comandos, los dispositivos pueden cooperar entre sí de manera descentralizada al confiar en la comunicación punto a punto.	Se requiere para enviar consultas a los sensores o, cuando está presente un bucle de control, para enviar comandos de actuación.
		

RPL crea una topología de enrutamiento en forma de un grafo acíclico orientado hacia el destino (DODAG): un grafo dirigido sin ciclos, orientado hacia un nodo raíz, como un router de frontera (border router). Por defecto, cada nodo tendrá varias rutas definidas como padres hacia la raíz; pero se usa una ruta elegida para reenviar paquetes de datos hacia la raíz, mientras que los otras se mantienen como rutas de respaldo. Este esquema, se denomina comunicación multipunto a punto en RPL. Una vez creada la topología esta se mantiene a través de paquetes de control llamados objetos de información DODAG (DIO). Cabe mencionar que los DIO se anunciarán más rápidamente cuando la red sea inestable, mientras que cuando la red sea estable llevarán un ritmo más lento [23].

Por otro lado, hay métricas de enlace que pueden ser utilizados por OF (Función de Objetivo) para definir el padre preferido basadas en la confiabilidad de enlace, demora y energía, entre otras. OF utiliza ETX (Recuento de

Transmisión Esperado), que representa la confiabilidad del enlace, para comparar a los padres en la lista de padres y obtener el "padre preferido" que se puede configurar como ruta predeterminada para la dirección ascendente [7].

Para admitir el patrón de tráfico dual desde la raíz a los dispositivos, llamado comunicación punto a multipunto en RPL, el estándar requiere mensajes de control adicionales y estado de enrutamiento. Específicamente, cada nodo en la red debe anunciarse como un posible destino a la raíz mediante el envío de paquetes de control del objeto de anuncio de destino (DAO) [23].

RPL define dos modos de operación: *almacenamiento y no almacenamiento*. En el modo de almacenamiento, cada nodo establece una tabla que contendrá todas las asignaciones entre los destinos posibles a acceder desde su sub-DODAG además de sus respectivos nodos del siguiente salto. Por otro lado, en el modo de no almacenamiento, la raíz es el único nodo que mantiene información de enrutamiento.

En cuestiones de movimiento con RPL, se afirma que las aplicaciones industriales requieren el soporte de nodos ubicados en vehículos o máquinas que se mueven a velocidades de hasta 35 km/h y que los dispositivos no deben actuar como enrutadores mientras están en movimiento [23].

3.6. 6LoWPAN para la VANET

Uno de los desafíos más importantes a cubrir en una VANET, es la posición geográfica, la cual es altamente requerida por la disponibilidad de receptores de sistemas de localización eficientes. Es por eso que, diversas aplicaciones y servicios vehiculares solo serán posibles desarrollar con IPv6. La razón es que está considerada como la tecnología más apropiada para admitir la comunicación en VANET gracias a su espacio de direcciones ampliado, soporte de movilidad mejorado, facilidad de configuración y seguridad integrada [24].

Por otro lado, una herramienta más que hará posible el desarrollo de estas redes es el RPL ya que es flexible y tiene especificaciones especiales, como el soporte de muchos nodos de baja potencia y pérdida, diferentes tráficos

y autocorrección. De esta manera, el RPL personalizado podría ser adecuado para vehículos conectados [25].

En la Figura 3.8 se muestra gráficamente cómo se realiza el direccionamiento IP entre dos carriles de automóviles y las estructuras viales.

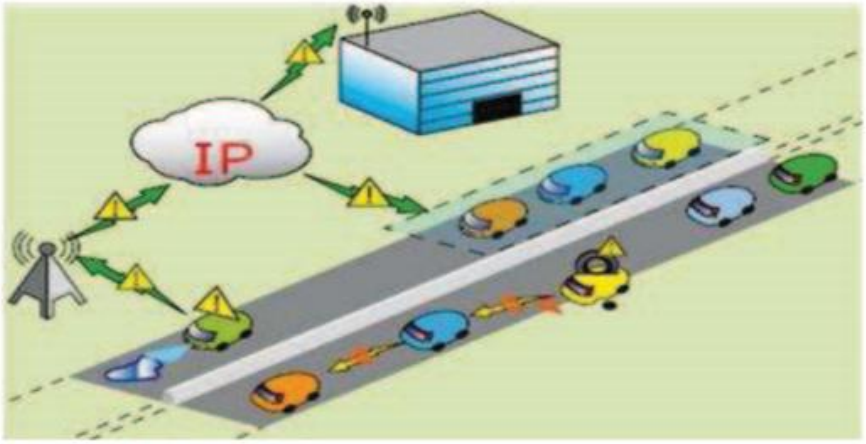


Figura 3.8. Direccionamiento de vehículos [24]

Con base en esta observación, la integración de la información geográfica en IPv6 es uno de los desafíos de investigación más importantes. Los organismos de normalización se ocuparon del enrutamiento geográfico y también de IPv6 para VANET por separado, como el Consorcio de Comunicación Auto-Automóvil (C2C-CC), ETSI TC ITS y la CALMA ISO [24].

Usar 6LoWPAN genera un impacto reducido en la demora y el rendimiento gracias a los mecanismos de compresión existentes. Pero también señalan cierta ineficacia en la detección de movimiento utilizada.

3.7. Sistema Operativo Contiki

Existen hoy en día muchos sistemas operativos tales como Contiki, TinyOS, RiOT, OpenWSN, Nano-RK entre otros que soportan el protocolo 6LoWPAN. El entorno utilizado para realizar las simulaciones de red en este proyecto de tesis es el sistema operativo basado en Linux, Contiki, el cual fue implementado por un grupo de desarrolladores liderado por Adam Dunkels del Instituto Sueco de Ciencias de la Computación [26].

Como características se puede mencionar que está escrito en el lenguaje de programación C, además de ser un sistema portable y tener la capacidad de ser multitarea para sistemas integrados en red con eficiencia de memoria y redes de sensores inalámbricos, además de proporcionar la comunicación IP en IPv6. Contiki consiste en un núcleo controlado por eventos, encima del cual los programas de aplicación se pueden cargar y descargar dinámicamente en tiempo de ejecución [26].

Contiki proporciona abstracciones de hardware que encapsulan la complejidad del hardware. Este enfoque hace que Contiki funcione con varios hardware, incluidos MCU y módulos de radio. Contiki también proporciona bibliotecas generales para detección, activación y comunicación [27].

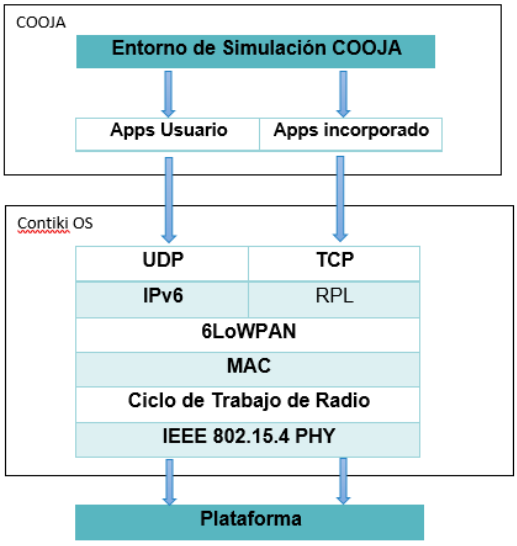


Figura 3.9. Arquitectura general de Contiki S.O.

Como se puede observar en la Figura 3.10, la ROM del sistema se encarga de los módulos estáticos como el Kernel, el cargador de programas, el tiempo de ejecución de programas y el servicio de comunicación, además de que todos los programas generados por el usuario se cargarán en el módulo “programa cargado”. Por otro lado, únicamente el Kernel y el servicio de comunicación serán usados por la memoria RAM.

Contiki usa un compilador GCC para compilar archivos de código fuente en C Desarrollamos aplicaciones Contiki escritas en archivos *.c. Una vez compilados, obtenemos el archivo binario. Básicamente, convierte la aplicación de la sintaxis del programa C a un archivo binario nativo para un destino de hardware específico [27]. La Figura 3.10 ejemplifica mejor el flujo de programación en el sistema:

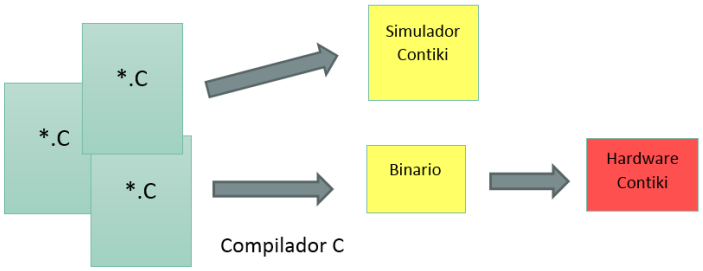


Figura 3.10. Flujo de programación de Contiki [26]

En este trabajo es importante mencionar que se propuso utilizar Contiki OS debido a que contiene dos pilas de comunicaciones: uIP y Rime. uIP posee una pequeña compatibilidad con la pila TCP/IP que hace posible que Contiki se pueda comunicar sobre Internet. Rime es una pila de comunicación ligera diseñada para radios de baja potencia. Aunque el *driver* que viene por defecto es el de RIME, para este trabajo nos basamos en el código de ejemplo de la pila uIP *simple-udp-rpl* porque no se puede utilizar RIME y 6LoWPAN en la capa de adaptación al mismo tiempo, pero sí es importante indicar que la pila uIP hace uso de RIME solo para proporcionar una API tipo socket para uso de aplicaciones llamadas proto-sockets.

3.7.1. Simulador COOJA

Dentro del entorno Contiki se encuentra una herramienta llamada Cooja la cual es un simulador flexible basado en Java diseñado para la simulación de redes inalámbricas de sensores que corre en el sistema operativo Contiki [28]. Esta herramienta resulta muy útil para llevar un seguimiento gráfico en cada simulación, proporcionando los eventos de radio, la monitorización de las conexiones existentes para cada nodo, entre otras características por mencionar. Por ende, todo esto facilita el desarrollo de simulaciones y el análisis de funcionamiento para los protocolos utilizados en el presente trabajo.

3.8. Conclusiones del Capítulo 3

En este capítulo se analizaron los protocolos que sirven de base para el presente trabajo relacionado a las redes vehiculares. El protocolo IPv6 es el punto principal por el cual es posible llevar a cabo las simulaciones. Por otro lado, la definición de las redes LoWPAN y el RPL permitirá el análisis de las conexiones entre nodos para las simulaciones y así entender el algoritmo que se propondrá para la red.

Este trabajo se basará en direcciones Link-local y direcciones establecidas por uIP en Contiki ya que son creadas para comunicaciones en una subred local.

Capítulo 4. Escenario de las simulaciones

4.1. Introducción

Este capítulo se muestra con detalle cada componente que integra la simulación, desde la herramienta utilizada llamada Cooja que proporciona el S.O. Contiki, enfatizando cada punto de observación que ofrece el simulador, hasta los archivos generados para posibilitar que el trabajo desarrollado permita la movilidad.

La interfaz de la herramienta Cooja se explica con mayor detalle con la finalidad de que el lector ubique cada componente gráfico, así como las transferencias de paquetes que se llevan a cabo en cada caso de simulación realizada. Por otro lado, y de manera más formal se expone a través de un diagrama de flujo el funcionamiento del código desarrollado, el cual como se dijo en el capítulo 3 fue realizado bajo el lenguaje C, para lograr el objetivo de envío y recepción de información a través de una red VANET.

En adición, se muestran los criterios a seguir para definir la velocidad de los nodos que posteriormente se plasmaron en archivos .dat, que gracias a un plug-in fue posible agregar a las simulaciones para que estuvieran en constante movimiento y bajo distintas velocidades y distancias.

4.2. Entorno de trabajo

Contiki ofrece una herramienta muy útil para la realización de simulaciones de redes llamada Cooja. Dentro de ella, se ofrecen distintas opciones a agregar que permiten dar un seguimiento de las simulaciones desarrolladas. Por mencionar algunas, las más importantes y que en este trabajo se utilizó para mayor entendimiento de la interacción entre los motes que simulan los automóviles.

En la Figura 4.1 se observa del lado izquierdo una cuadrícula donde se diseña la red deseada agregando cada mote, basándose en un sistema de coordenadas (x,y). También hay otra ventana llamada "*Simulation control*" donde se inician y detienen las simulaciones, además de tener la posibilidad de ir por pasos y recargarla si llegan a haber modificaciones.

Además, cuenta con otra ventana dirigida a mostrar el archivo de movilidad que se usa, el tiempo medido en *ms* cuando comienzan a desplazarse los motes y el número de posiciones que están programadas.

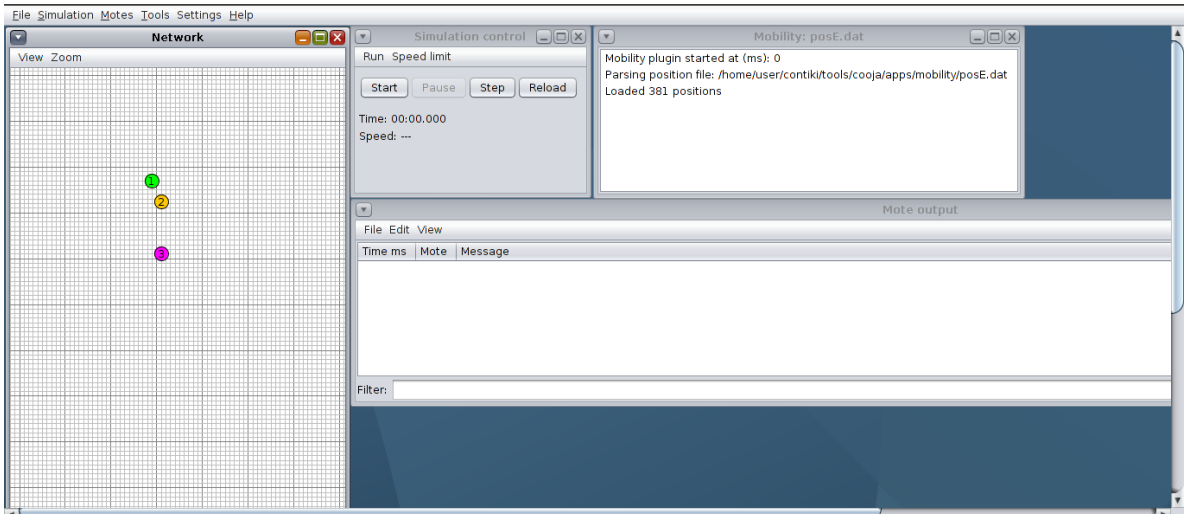


Figura 4.1. Entorno Cooja.

La ventana que se consideró más importante para el seguimiento de los resultados arrojados es la llamada "Mote output" (Figura 4.2.) donde se van desplegando cada paso del nodo desde la asignación de direcciones hasta el momento donde ya está enviando o recibiendo paquetes de información, se puede observar los tiempos en que ocurre cada conexión y el número de mote que realiza cierta actividad definido como mensaje.

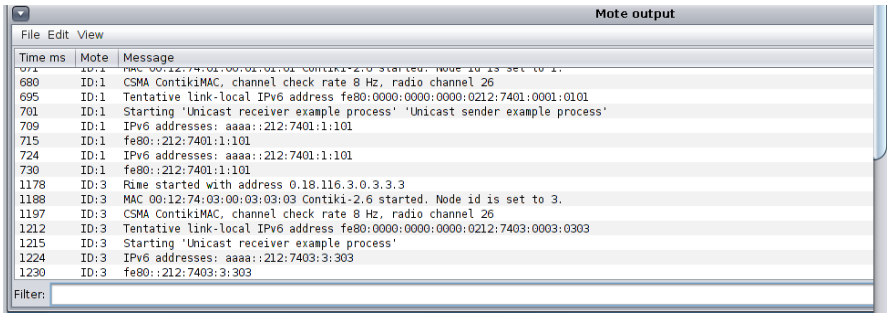


Figura 4.2. Salidas de motes

Cooja permite crear redes bajo los requerimientos establecidos por el usuario, por lo que ofrece distintos tipos de motes con características específicas. En las simulaciones desarrolladas, el mote con el que se trabajará es el llamado “SKY mote” ya que además de ser un módulo inalámbrico de muy baja potencia, está diseñado para el uso en redes de sensores bajo el estándar IEEE 802.15.4. Otra razón por la que se utilizó este módulo es la compatibilidad con el S.O. Contiki y la ventaja de trabajar bajo código abierto.

4.3. Estructura de la red móvil

La comunicación entre los vehículos representados por los nodos móviles es a través de una red Ad-hoc móvil o MANET, donde por defecto se asignan direcciones de enlace local a cada nodo, esto con la finalidad de que cada auto pueda mandar y recibir información. En la Tabla XII se muestran las direcciones que corresponden a cada nodo y su respectiva dirección IP.

Tabla XII. Direcciones IPv6 asignadas.

# de Nodo	Dirección de enlace local	Dirección IP
1	fe80::212:7401:1:101	aaaa::212:7401:1:101
2	fe80::212:7402:2:202	aaaa::212:7402:2:202
3	fe80::212:7403:3:303	aaaa::212:7403:3:303

Por otro lado, la Figura 4.3 muestra gráficamente como se pretende que interactúen los automóviles en distintos carriles. El contexto en el cual se realizaron los experimentos fue donde el nodo 2 es el primero en detectar un accidente, el usuario hace que se almacene el dato comportándose como Transmisor en la red hasta que otro auto receptor ingrese a su área de servicio, como el caso del nodo 1, y le transmita el aviso de prevención. Posteriormente, el nodo 1 guarda la información, siendo ahora un transmisor, hasta encontrarse con el nodo 3 y enviarle el aviso de prevención. En la imagen se muestra la interacción V2V.

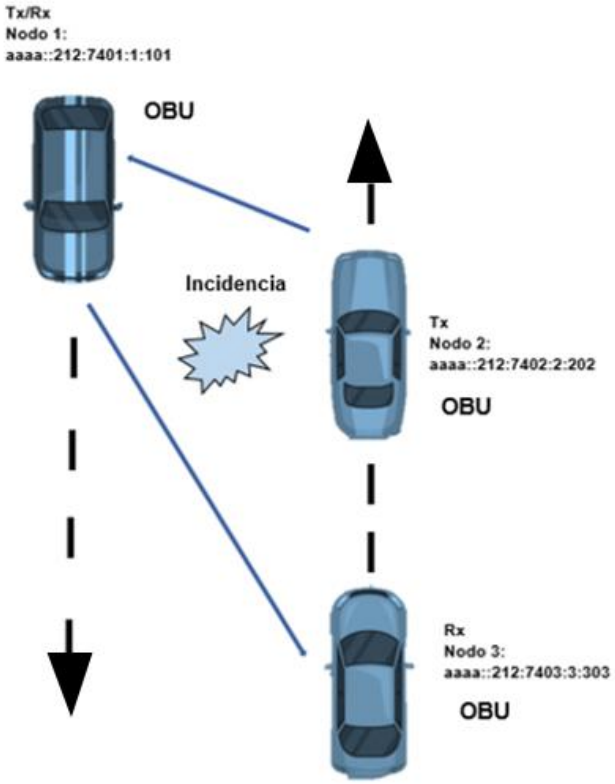


Figura 4.3. Estructura de comunicación entre nodos.

4.4. Diagrama de Flujo

La comunicación establecida entre los dispositivos se realiza a través del estándar IEEE 802.15.4, el cual especifica velocidades de 250 kbps en la banda de 2.4 GHz, de 20 kbps en la banda de 868 MHz y de 40 kbps en la banda de 915 MHz, en donde se trabajó solo en la banda de 2.4 GHz. Además, el estándar accede al canal utilizando el mecanismo CSMA/CA en redes PAN con la señal Beacon habilitada y deshabilitada.

Por otro lado, el estándar 6LoWPAN no requiere de la señal Beacon habilitada y no usa CSMA/CA ranurado, por tal razón la pila de este estándar se diferencía de la pila de protocolos de Contiki OS en que este último agrega la capa RDC, que en conjunto con la técnica de acceso al medio CSMA/CA indican cuando se transmite o no un paquete. Por último, los paquetes IPv6 se transmiten solicitando reconocimiento (ACK).

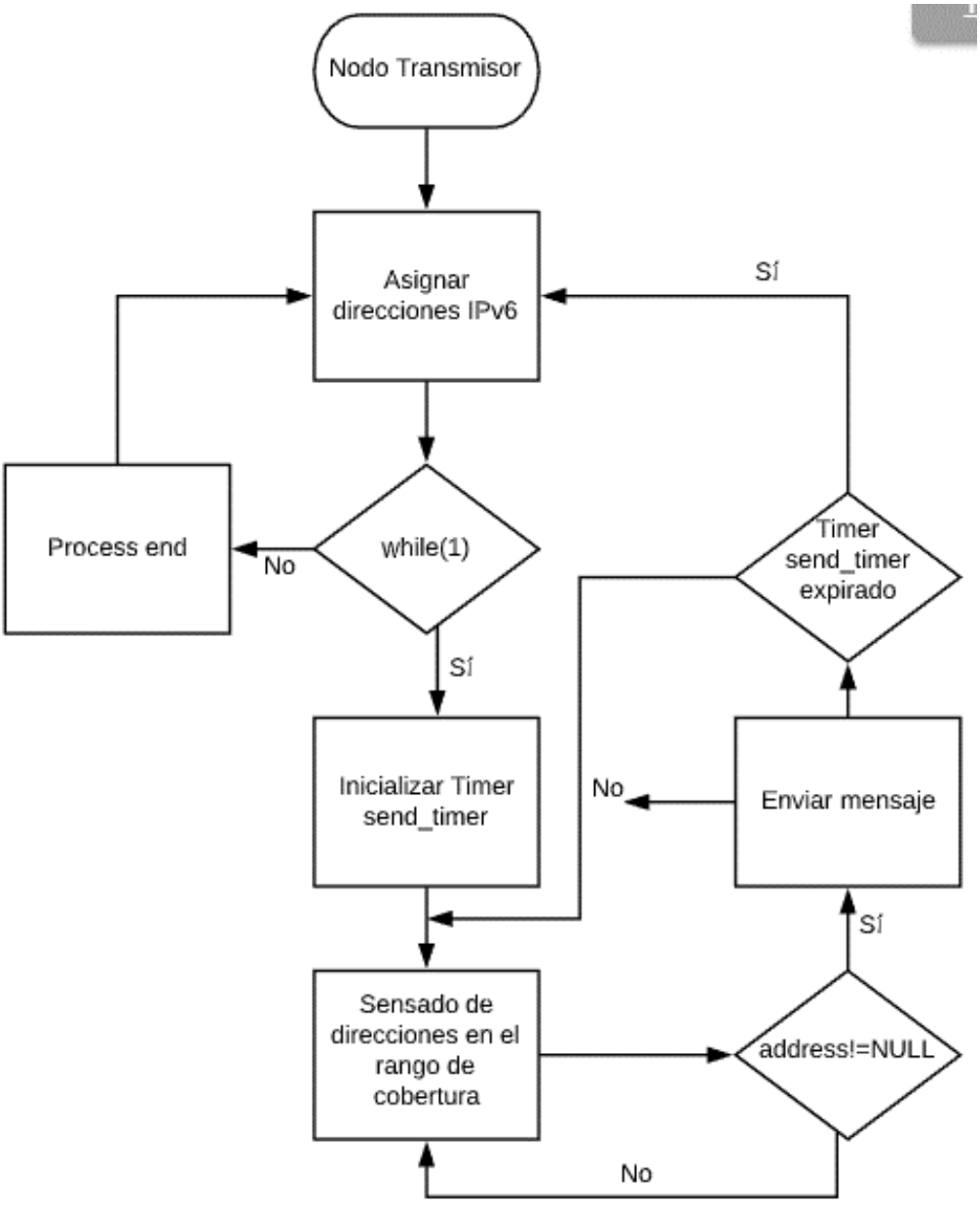
De acuerdo con lo anterior, fue necesario elaborar un diagrama de flujo para cada rol que puede tomar un automóvil en el ámbito vial, es decir, un diagrama para el caso donde un auto es transmisor y otro donde actúe como receptor.

La imagen 4.4 muestra con mayor detalle el proceso por el cual ambos casos cubren cada capa de la pila de protocolos para una red vehicular. Como se puede ver, este proceso comienza con la inicialización de la pila de protocolos RIME mencionada en el capítulo 3, continúa con las asignaciones de direcciones físicas para posteriormente inicializar el protocolo CSMA/CA (Acceso Múltiple con Detección de Portadora/ con prevención de colisiones), el cual tiene la finalidad de que un nodo verifique la ausencia de tráfico antes de transmitir en un medio compartido. Después de esto, se asignan a cada mote direcciones de enlace local para IPv6. Nótese que este flujo es el mismo tanto para un nodo transmisor o receptor.

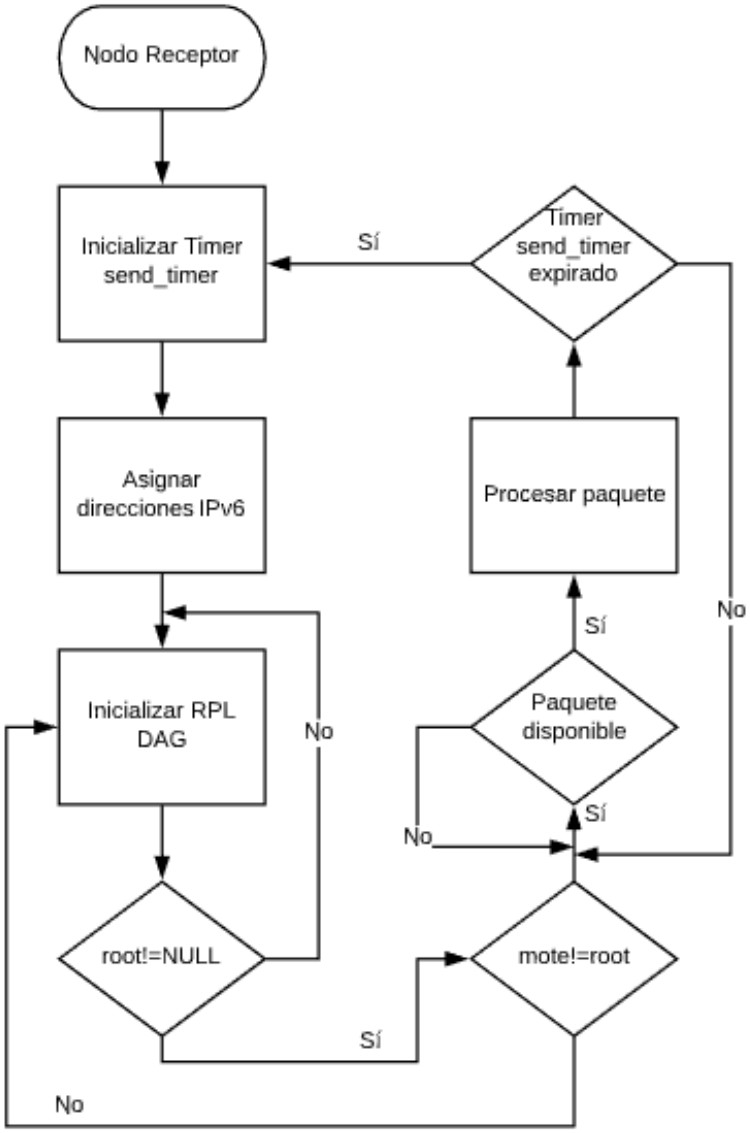
Ahora, en la figura 4.4 a) el nodo transmisor a partir de los procesos previos ya mencionados trabaja bajo UDP al ser un protocolo sin conexión y sin reconocimiento, este se encarga de mandar paquetes a los nodos más cercanos

y que estos reciban un mensaje de confirmación, en caso de no encontrar nodos cercanos va a repetir el proceso de envío hasta que encuentre un receptor, sin embargo, se propone que en la implementación el vehículo lleve un contador de kilometraje el cual al recorrer 5km después de la incidencia detenga el proceso de envío de mensajes.

Por otro lado, para el caso del nodo receptor, la imagen 4.4 b) incluye el proceso de la creación de un grafo dirigido, esto con el propósito de que el protocolo RPL pueda comenzar a buscar la ruta óptima y las conexiones entre motes sean más estables. El receptor se mantendrá en modo sleep hasta que entre en el rango de cobertura de algún dispositivo y de esta forma activar el modo de “Esperar envío de paquetes”.



a) Diagrama para un nodo transmisor



b) Diagrama para un nodo receptor

Figura 4.4. Diagrama de flujo de simulación para la VANET.

4.5. Escenarios para la movilidad

Tomando en cuenta lo mencionado en el capítulo 3 respecto a la velocidad recomendada para el óptimo funcionamiento del RPL, se crearon archivos con extensión .dat que permiten la movilidad en la simulación. En estos, se especifican los parámetros que requiere cada nodo, como lo son el tiempo inicial, el final y las posiciones en las que se van desplazando los nodos en cierto rango de tiempo, basado en un sistema de coordenadas (x,y).

Para definir el desplazamiento de cada nodo respecto al tiempo se tomó en cuenta una cuadrícula donde cada cuadro representa 10 metros de distancia, esto fue definido al basarse en el kilometraje apropiado mencionado en la sección 3.5 del capítulo 3. Además, al realizar los respectivos cálculos, se obtiene que recorrer 35 km/h es aproximadamente proporcional a 10 m/s. En la Figura 4.5 se explica de manera más gráfica que, por cada segundo transcurrido, el automóvil se va a desplazar 10 m. Ahora bien, estos datos fueron introducidos en el archivo .dat.

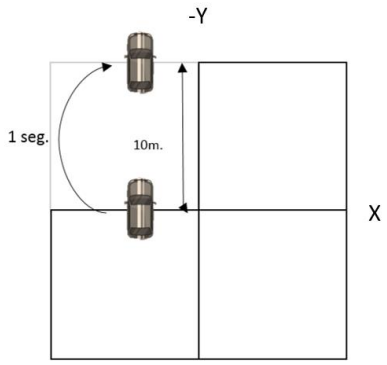


Figura 4.5. Desplazamiento de nodos simulando velocidad a 35 km/h.

Para verificar lo mencionado con anterioridad, se llevó a cabo dos casos de simulación con diferente velocidad y un tercer caso con nodos estáticos para observar las diferencias entre ellos. El primer caso es donde la velocidad se duplica a 70 km/h o bien, a aproximadamente 20 m/s, esto con la hipótesis de que el enrutamiento entre nodos será aún más inestable. De igual manera, la Figura 4.6 representa lo explica.

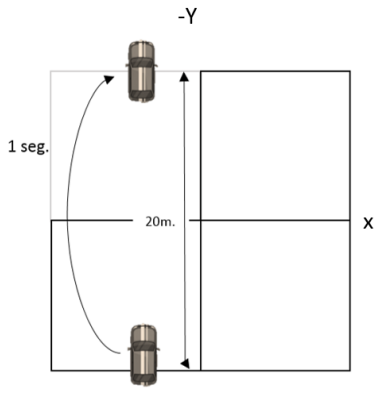


Figura 4.6. Desplazamiento de nodos simulando velocidad a 70 km/h.

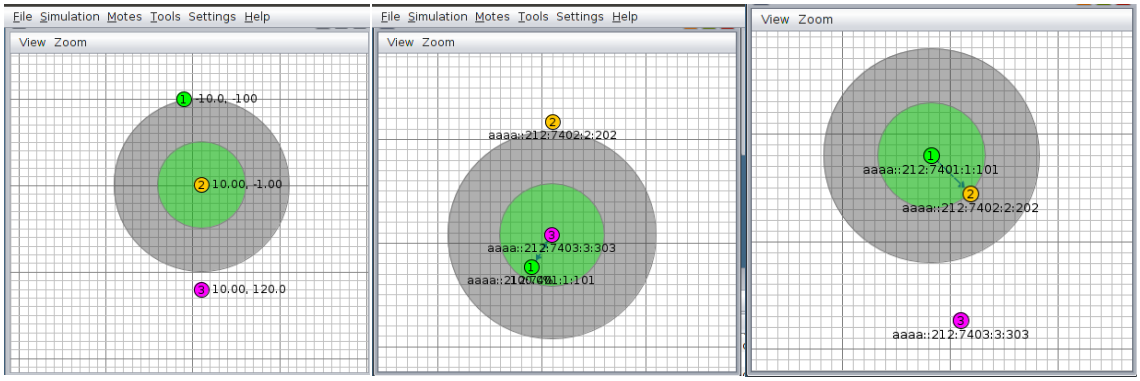
4.6. Conclusiones del capítulo 4

En este capítulo se mostró con mayor detalle las características que se tomaron en cuenta para el desarrollo de las simulaciones, cómo se busca que interactúen los nodos a través de la red vehicular gracias a los diagramas de flujo que se realizaron y las consideraciones que se tuvieron al fijar velocidades a partir del promedio mencionado de 35 km/h, todo esto con la finalidad de que el escenario inicial tenga los fundamentos correctos y la simulación sea lo más exacta posible en sus resultados.

Capítulo 5. Resultados

5.1 Introducción

En este capítulo se mostrarán con base en la premisa de que, al ser una red en constante movimiento, las conexiones sufrirán de pérdidas de conexión y que por ende la pérdida de paquetes es inevitable. De esta manera, se buscó monitorear estas pérdidas para hacer un promedio de los paquetes recibidos en cada caso. La figura 5.1 a) muestra las posiciones iniciales entre cada mote y el radio de reconocimiento en la red, mientras que en el inciso b) se visualiza el intercambio de información entre nodos una vez que ambos se encuentran en la zona de cobertura al 100%.



a) Posiciones iniciales. b) Comunicación entre nodos 1 y 3. c) Comunicación entre nodos 1 y 2.

Figura 5.1. Posiciones iniciales y comunicación entre nodos

Enfocándose en la herramienta de salida de los motes mostrada en la Figura 5.2, muestra el desglose de información como la inicialización de todos los protocolos de la pila RIME, desde el tiempo de **515 ms** para cada uno de los motes.

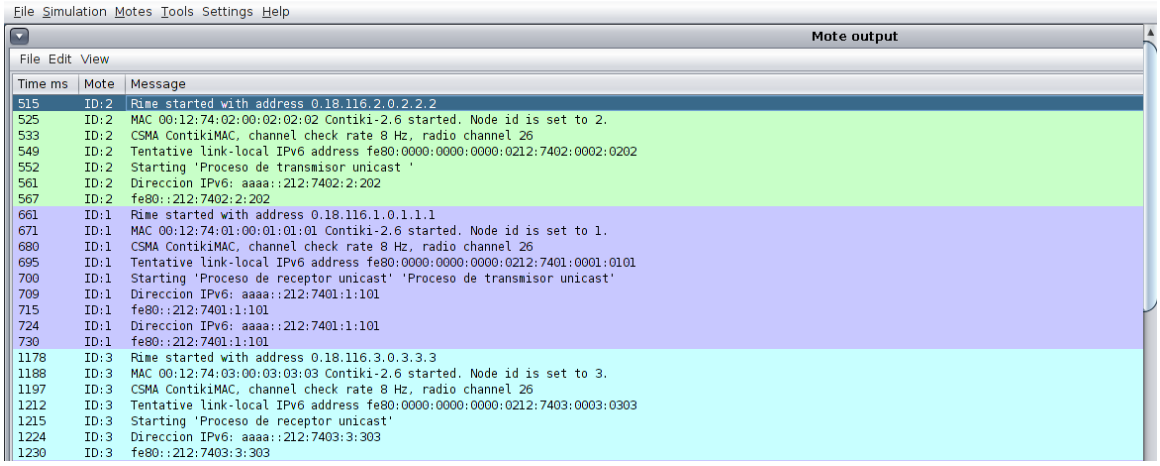


Figura 5.2. Inicialización de protocolos.

5.2 VANET con velocidad a 35 km/h

Las simulaciones realizadas bajo esta velocidad presentan resultados los cuales se muestran en la Figura 5.3, donde se observa que es hasta el tiempo de **513248 ms** cuando el nodo 2 comienza con el envío de paquetes dirigiéndose hacia el nodo 1 lo hace por duplicado porque la velocidad lo permite. El nodo 1 estando en modo receptor, acepta el mensaje de acuerdo con el tiempo 540888 ms que es el último mensaje que le envió el nodo 2 y envía sólo una confirmación en el tiempo **540942 ms** que corresponde al número de Mensaje 3.

Posteriormente, el nodo 1 pasa a ser transmisor del aviso del choque y comienza a enviar mensajes en el momento en que detecta al nodo 3 en su área de cobertura en el tiempo de **5550355 ms,** y el nodo 3 confirma la recepción hasta el mensaje número 7 en el tiempo de **624834 ms**.

```
513248    ID:2   Choque detectado, envia a :aaaa::212:7401:1:101
540888    ID:2   Choque detectado, envia a :aaaa::212:7401:1:101
540942    ID:1   Informacion recibida desde : aaaa::212:7402:2:202 'Mensaje 3'
550355    ID:1   Choque detectado, envia a : aaaa::212:7403:3:303
624785    ID:1   Choque detectado, envia a : aaaa::212:7403:3:303
624834    ID:3   Informacion recibida desde : aaaa::212:7401:1:101 'Mensaje 7'
```

Figura 5.3. Simulación a velocidad 35 km/h aproximadamente.

En la Tabla XIII se muestran de forma simplificada los tiempos en el que los nodos realizaron el envío y recepción de paquetes, así como los respectivos mensajes que les corresponden a cada uno.

Tabla XIII. Tiempo de envío para cada nodo a una velocidad de 35 km/h.

Tiempo (ms)	Nodo ID	Mensaje
540888	ID:2	Choque detectado, envía a: aaaa::212:7401:1:101
540942	ID:1	Información recibida desde: aaaa::212:7402:2:202 Mensaje 3
624785	ID:1	Choque detectado, envía a: aaaa::212:7403:3:303
624834	ID:3	Información recibida desde: aaaa::212:7401:1:101 Mensaje 7

5.3 VANET con velocidad a 70 km/h

Los resultados para este segundo caso arrojaron que el primer envío de paquetes fue en el tiempo de **453913 ms** por parte del nodo 2 hacia el nodo 1 siendo este el receptor del mensaje, pero sucede que no el nodo 1 no puede recibir inmediatamente mensaje por lo que se imprime el mensaje de **"Servicio no encontrado"**. Posteriormente hasta el tiempo **540888 ms** el nodo 2 envía el mensaje al nodo 1 y este nodo 1 envía un mensaje de recibido. Ahora el nodo 1 siendo el transmisor del mensaje envía el aviso en tiempo **550355 ms** al nodo 3. Se observó que, con esta velocidad la inconsistencia es aún mayor ya que no había una conexión constante en la red, por lo que no se realizó ninguna confirmación de recepción de paquetes por parte del nodo 3.

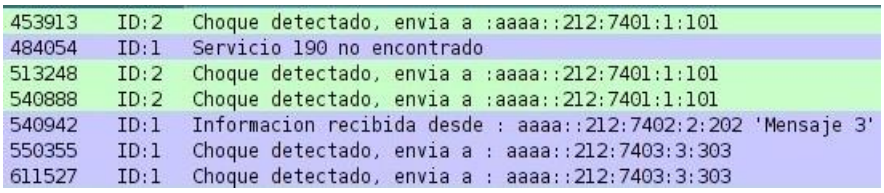


Figura 5.4. Simulación a velocidad 70 km/h aproximadamente.

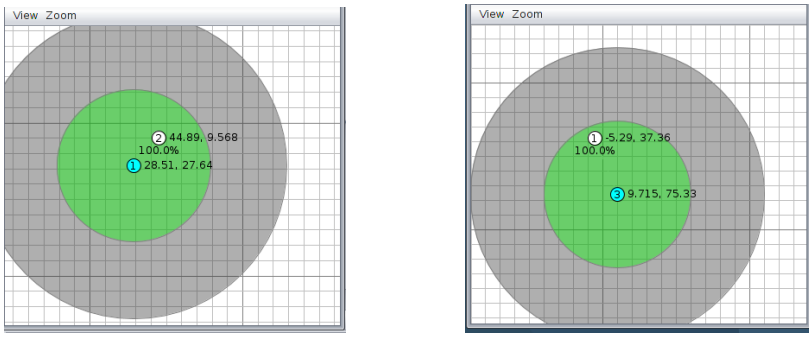
Por otro lado, la Tabla XIV muestra igualmente los tiempos de forma simplificada en el que los nodos interactuaron.

Tabla XIV. Tiempo de envío para cada nodo a una velocidad de 70 km/h.

Tiempo (ms)	Nodo ID	Mensaje
540888	ID:2	Choque detectado, envía a: aaaa::212:7401:1:101
540942	ID:1	Información recibida desde: aaaa::212:7402:2:202 Mensaje 3
550355	ID:1	Choque detectado, envía a: aaaa::212:7403:3:303
N/A	ID:3	----

5.4 VANET sin movimiento

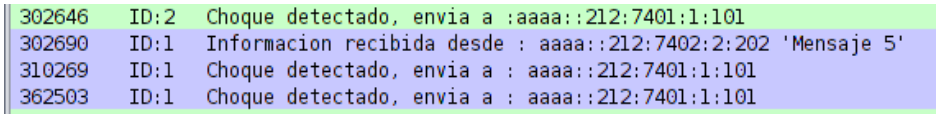
Finalmente, se realizó un caso “ideal” donde el envío y recepción de información es completamente instantáneo, es decir, cuando la red es estática y no hay pérdida de conexión entre nodos. Para esta simulación se colocaron los tres nodos en una posición aleatoria de manera que todos estuvieran dentro de su rango de cobertura con la finalidad de observar la velocidad con la que se hace el envío de paquetes en una red donde el movimiento no fuera un factor. Lamentablemente usando este tipo de simulación, el objetivo principal no es satisfactorio, ya que este se basa en las redes móviles, por lo que este ejemplo solo es para demostrar que el trabajo planteado tiene como obstáculo y propósito la misma variable, la velocidad y el tiempo de reconocimiento. En la figura 5.6. se muestra cómo se realizó este caso, para ello se realizaron las simulaciones por separado, es decir, una simulación donde interactúe el nodo dos con el uno y otra donde interactúen el nodo uno con el tres, con la finalidad de que se mostrara que la conexión en el envío de paquetes es prácticamente instantánea. Como se observa, la cobertura es del cien por ciento.



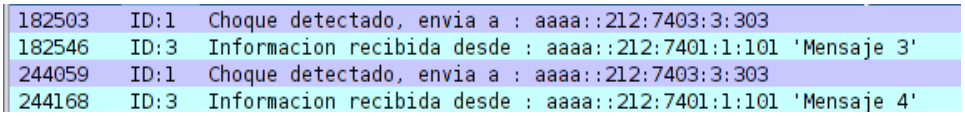
a) Escenario nodo 2 a 1 b) Escenario nodo 1 a 3

Figura 5.5. Escenario simulación sin movimiento

Por otro lado, en la Figura 5.7. se muestra que el primer mensaje enviado por el nodo 2 ocurre en el **302646 ms** y la respuesta del nodo 1 se da en el tiempo de **302690 ms**, claramente con muy poca diferencia de tiempo. Así bien, el nodo 1 envía su primer paquete en el **182503 ms**, mientras que la confirmación de recibido por parte del nodo 3 se da en el **182546 ms**, todo esto sin pérdida de paquetes porque se puede observar que la secuencia de mensajes se lleva a cabo sin saltos.



a) Salidas de mote 2 al mote 1



b) Salidas de mote 1 al mote 3

Figura 5.6. Simulación en modo estático

Tabla XV. Tiempo de envío para cada nodo en modo estático.

Tiempo (ms)	Nodo ID	Mensaje
891406	ID:2	Choque detectado, envía a: aaaa::212:7401:1:101
891442	ID:1	Información recibida desde: aaaa::212:7402:2:202 Mensaje 14
902644	ID:1	Choque detectado, envía a: aaaa::212:7403:3:303
902710	ID:3	Información recibida desde: aaaa::212:7401:1:101 Mensaje 15

5.5 Análisis de los resultados

En este apartado se presentará una comparación entre los tres casos presentados en cuanto a retardo en la transmisión, esto considerando desde el tiempo en que se inicia el proceso en la red, es decir la primera parte que corresponde del nodo 2 al nodo 1, siempre que este último reciba el mensaje. La segunda parte del proceso que va del nodo 1 al nodo 3. En la Tabla XVII se muestran el tiempo de los resultados arrojados en milisegundos.

Tabla XVI. Latencia entre nodos para cada simulación (ms).

Velocidad promedio de los nodos	Primera parte **ID:2 a ID:1**	Segunda parte **ID:1 a ID:3**
Km/h	**Retardo (ms)**	**Retardo (ms)**
35	54	49
70	54	N/A
Estático*	44	43

Como se puede observar de la Tabla IX, los retardos para las velocidades de 70 y 35 km/h en la primera parte coinciden, pero al pasar a la segunda parte, la velocidad de 70 km/h ocasiona que el nodo 3 no pueda confirmar si le llegó el aviso del accidente. Finalmente, en el caso estático se consideraron los mensajes 4 y 5 de la Figura 5.6 para la primera y segunda parte respectivamente, debido a que en los primeros mensajes se tenía un mayor retardo mientras se establecía el enlace.

5.6 Conclusiones del capítulo 5

Después de haber realizado distintas pruebas con el simulador tomando como referencia la velocidad entre nodos y observando como varían los resultados del tiempo de envío y recepción de paquetes cuando esta es mayor o menor, se concluye que efectivamente un factor muy importante en la implementación de redes móviles es la velocidad a la que van cada nodo, resulta un obstáculo al observar que de esto depende si la red mantiene una conexión constante o se vuelve inconsistente, además el hecho de que cada nodo al recibir un paquete deba pasar a través del ACK también resulta un problema para la robustez de la red. Sin embargo, a pesar de lo mencionado en la simulación donde los nodos iban a una velocidad aproximada de 35 Km/h se observó un tiempo de respuesta corto y sin tanta pérdida de información.

Capítulo 6. Conclusiones y trabajo a futuro.

El proyecto presentado se basó en el estudio de los fundamentos para las redes sensoriales inalámbricas, WSN, así como las de baja potencia LoWPAN en conjunto del protocolo IPv6. Esto con la finalidad de la realización de simulaciones en un entorno vehicular VANET, a través de herramientas y software diseñado para este tipo de proyectos y con ello realizar el estudio de los posibles inconvenientes al considerar llevar el trabajo a nivel de hardware como trabajo a futuro. Los puntos más importantes que se destacaron en este proyecto se mencionan a continuación:

- El primer punto realizado fue el estudio de los protocolos utilizados en el modelo 6LoWPAN, comprender la estructura de las direcciones utilizando IPv6 así como sus reglas de compresión. Por otro lado, fue de suma importancia el estudio del protocolo de enrutamiento para redes de baja potencia RPL.
- Una vez comprendidos los fundamentos se eligió al sistema operativo Contiki como mejor opción para la realización de las simulaciones a través de su herramienta COOJA, ya que la pila de protocolos de Contiki organiza los módulos de red en una pila que cubre todas las capas tradicionales del modelo OSI.
- Se adecuaron los programas de ejemplo de Contiki OS udp-client.c y udp-server.c tomando como base las librerías que marcaban para la creación de los enlaces de comunicación y así poder establecer el intercambio de mensajes de alerta primero en una red sin movimiento.
- Con base en el estudio del comportamiento de una VANET V2V, el mayor obstáculo con el que se trabajó fue el factor de la velocidad en los automóviles. Considerando que al ser una red ad-hoc móvil, la conexión entre módulos no resultaba constante, generando inconsistencias y pérdidas de paquetes de información provocando en este tipo de redes de bajo recursos enlaces muy inestables. Es por ello por lo que los

requerimientos para una red de sensores inalámbricos son muy distintos de las redes tradicionales y en este trabajo se comprobó que una velocidad de 35 Km este problema se vuelve mínimo.

- En este proyecto sólo se consideró un salto en movimiento, se observó que a medida que se abarcaba más distancia añadiendo más motes aumentaban las pérdidas y la latencia. Estas pérdidas y este aumento de latencia pueden ser ocasionados por la calidad del enlace inalámbrico.
- Dentro de las simulaciones se tuvo que considerar con cuidado el tiempo de ejecución ya que, al analizarla durante un largo lapso, los nodos se saturaban de información y la simulación se volvía mucho más inestable, ya que el simulador cuenta con un solo buffer para el envío y recepción de mensajes que complica la gestión de mensajes.

Finalmente se concluye que el modelo 6LoWPAN es de gran utilidad al proponer protocolos diseñados para redes con baja tasa de transmisión logrando que el mayor problema de la velocidad se vea reducido gracias a que el envío de paquetes se vuelve más ligero y aún en movimiento, los nodos logren realizar las conexiones.

Los resultados obtenidos tomando en cuenta todo lo mencionado lograron demostrar las hipótesis realizadas al inicio de todo el trabajo, las cuales consideraban que un automóvil que envía datos a una velocidad mayor es más probable que tenga pérdida de paquetes que un auto con velocidad media de 35 km o incluso menos. Las simulaciones realizadas utilizando una topología ad-hoc sirven de base para el posible desarrollo a nivel de hardware ya que al tener datos previos se pueden predecir problemas que puedan surgir al momento de la implementación.

Este proyecto puede resultar escalable y usable para cualquier tipo de automóvil en el exterior considerando limitantes como la velocidad permitida, el tráfico de fondo, fallos en el sensor, congestión en la red y la ocupación en la banda 2.4 GHz.

Finalmente, el trabajo fue aceptado y presentado como ponencia con el título “IPv6 como un Objeto de Aprendizaje para las Ciudades Inteligentes” en el

Tercer Workshop en Objetos de Aprendizaje 2019, celebrado el día 9 de agosto de 2019 en la FCC-BUAP.

Referencias

[1] A. Pressas, Z. Sheng, P. Fussey and D. Lund, Connected Vehicles in Smart Cities: Interworking from Inside Vehicles to Outside, 2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), London, 2016, pp. 1-3. doi: 10.1109/SAHCN.2016.7732976.

[2] Y. Xia, X. Qin, B. Liu and P. Zhang, A greedy traffic light and queue aware routing protocol for urban VANETs, in China Communications, vol. 15, no. 7, pp. 77-87, July 2018. doi: 10.1109/CC.2018.8424605.

[3] D. Lin, J. Kang, A. Squicciarini, Y. Wu, S. Gurung and O. Tonguz, MoZo: A Moving Zone Based Routing Protocol Using Pure V2V Communication in VANETs, in IEEE Transactions on Mobile Computing, vol. 16, no. 5, pp. 1357-1370, 1 May 2017. doi: 10.1109/TMC.2016.2592915.

[4] J. Wang, C. Jiang, K. Zhang, T. Q. S. Quek, Y. Ren and L. Hanzo, Vehicular Sensing Networks in a Smart City: Principles, Technologies and Applications, in IEEE Wireless Communications, vol. 25, no. 1, pp. 122-132, February 2018. doi: 10.1109/MWC.2017.1600275.

[5] M. Carignani, S. Ferrini, M. Petracca, M. Falcitelli and P. Pagano, A prototype bridge between automotive and the IoT, 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, 2015, pp. 12-17. doi: 10.1109/WF-IoT.2015.7389019.

[6] L. Virágg, J. Kovács and A. Edelmayer, Extension of the ITS Station Architecture to Low-Power Pervasive Sensor Networks, 2013 27th International Conference on Advanced Information Networking and Applications Workshops, Barcelona, 2013, pp. 1386-1391.

[7] B. Tian *et al*., Application of Modified RPL Under VANET-WSN Communication Architecture, 2013 International Conference on Computational and Information Sciences, Shiyang, 2013, pp. 1467-1470. doi: 10.1109/ICCIS.2013.387.

[8] P. Mutalik and V. C. Patil, "A survey on vehicular ad-hoc network [VANET's] protocols for improving safety in urban cities," 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon), Bangalore, 2017, pp. 840-845.

[9] C. M. Raut and S. R. Devane, "Intelligent transportation system for smartcity using VANET," 2017 International Conference on Communication and Signal Processing (ICCSP), Chennai, 2017, pp. 1602-1605.

[10] G. S. Khekare and A. V. Sakhare, "A smart city framework for intelligent traffic system using VANET," 2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), Kottayam, 2013, pp. 302-305.

[11] K. Eshteiwi, K. Ben Fredj, G. Kaddoum and F. Gagnon, "Performance analysis of peer-to-peer V2V wireless communications in the presence of interference," 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, 2017, pp. 1-6.

[12] Y. Xie, I. W. Ho and E. R. Magsino, "The Modeling and Cross-Layer Optimization of 802.11p VANET Unicast," in IEEE Access, vol. 6, pp. 171-186, 2018.

[13] IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture," in IEEE Std 1609.0-2013, vol., no., pp.1-78, 5 March 2014

[14] Keunsol Kim, Seung-Woo Lee, D. g. Park and Bhum Cheol Lee, "PTP interworking 802.15.4 using 6LoWPAN," 2009 11th International Conference on Advanced Communication Technology, Phoenix Park, 2009, pp. 873-876.

[15] W. Stallings, "IPv6: the new Internet protocol," in IEEE Communications Magazine, vol. 34, no. 7, pp. 96-108, July 1996. doi: 10.1109/35.526895

[16] Mun, Y., & Lee, H. (2010). Understanding IPv6. New York: Springer.

[17] G. Fairhurst, "IPv6 - The Network Protocol of the Future," 2008 4th Advanced Satellite Mobile Systems, Bologna, 2008, pp. 7-12. doi: 10.1109/ASMS.2008.7

[18] GHOSH, R. (2018). WIRELESS NETWORKING AND MOBILE DATA MANAGEMENT. [S.l.]: SPRINGER.

[19] Stockebrand, B. (2011). IPv6 in practice. Berlin: Springer.

[20] A. A. Hasbollah, S. H. S. Ariffin and M. I. A. Hamini, "Performance analysis for 6loWPAN IEEE 802.15.4 with IPv6 network," TENCON 2009 - 2009 IEEE Region 10 Conference, Singapore, 2009, pp. 1-5. doi: 10.1109/TENCON.2009.5396174

[21] X. Ma and W. Luo, "The Analysis of 6LowPAN Technology," 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Wuhan, 2008, pp. 963-966. doi: 10.1109/PACIIA.2008.72

[22] I. Wadhaj, I. Kristof, I. Romdhani and A. Al-Dubai, "Performance Evaluation of the RPL Protocol in Fixed and Mobile Sink Low-Power and Lossy-Networks," 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, 2015, pp. 1600-1605. doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.241

[23] O. Iova, P. Picco, T. Istomin and C. Kiraly, "RPL: The Routing Standard for the Internet of Things... Or Is It?," in IEEE Communications Magazine, vol. 54, no. 12, pp. 16-22, December 2016. doi: 10.1109/MCOM.2016.1600397CM

[24] Y. Khaled, M. Tsukada and T. Ernst, "Geographical information extension for IPv6: Application to VANET," 2009 9th International Conference on Intelligent Transport Systems Telecommunications, (ITST), Lille, 2009, pp. 304-308. doi: 10.1109/ITST.2009.5399339

[25] M. Alishahi and M. Majidpour, "Proposing a RPL based protocol for intelligent connected vehicles," 2014 International Conference on Connected Vehicles and Expo (ICCVE), Vienna, 2014, pp. 943-944. doi: 10.1109/ICCVE.2014.7297696

[26] T. Paul and G. S. Kumar, "Safe Contiki OS: Type and Memory Safety for Contiki OS," 2009 International Conference on Advances in Recent Technologies in Communication and Computing, Kottayam, Kerala, 2009, pp. 169-171. doi: 10.1109/ARTCom.2009.126

[27] Kurniawan, A. (2018). Practical Contiki-NG. Berkeley, CA: Apress.

[28] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne and T. Voigt, "Cross-Level Sensor Network Simulation with COOJA," Proceedings. 2006 31st IEEE Conference on Local Computer Networks, Tampa, FL, 2006, pp. 641-648. doi: 10.1109/LCN.2006.322172