REDES VANETS (VEHICULAR AD-HOC NETWORKS)

CARLOS ALBERTO GIRALDO LIPEDA T00012965
BERNARDO JOSE HERRERA PEREZ T00014522

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍAS
PROGRAMA DE INGENIERÍA DE SISTEMAS
CARTAGENA D.T Y C.
2010

REDES VANETS (VEHICULAR AD-HOC NETWORKS)

CARLOS ALBERTO GIRALDO LIPEDA T00012965
BERNARDO JOSE HERRERA PEREZ T00014522

Monografía

Docente ISAAC ZUÑIGA SILGADO
Ingeniero de Sistemas

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍAS
PROGRAMA DE INGENIERÍA DE SISTEMAS
CARTAGENA D.T Y C.
2010

ARTICULO 105

La Universidad Tecnológica de Bolívar, se reserva el derecho de propiedad intelectual de todos los trabajos de grado aprobados, y no se pueden ser explotados comercialmente sin autorización.

DEDICATORIA

Gracias a Dios por haberme concedido la oportunidad de culminar mis estudios de Ingeniería de Sistemas, por darme fortaleza y mucha sabiduría a lo largo del camino.

Agradezco a:

Mi Padre y a mi madre por el trabajo que realizaron día a día para brindarme las facilidades y tener la oportunidad de forjarme en una carrera la cual cursé con mucho orgullo.

A mis compañeros y amigos, que han sido testigos del proceso, de la preparación y del esfuerzo para culminar mis estudios

Así mismo, agradezco a nuestro tutor Isaac Zúñiga Silgado y la UTB por su apoyo brindado y por su asesoramiento, que ha hecho posible la culminación de nuestra monografía.

CARLOS ALBERTO GIRALDO LIPEDA

DEDICATORIA

Gracias a dios por no abandonarme y protegerme en todo momento, por guiarme por el sendero del bien, por darme todas las fortalezas, por darme la paciencia y por darme la oportunidad de ser un profesional.

Le agradezco a mis padres a los cuales les quiero dedicar esta monografía porque de no ser por ellos no estaría en esta etapa de mi vida, gracias a ustedes por brindarme la oportunidad de tener una formación académica, gracias por el amor, el apoyo y la confianza que tuvieron en mí, con todo mi corazón y es por ustedes que hoy soy lo que siempre he querido ser.

A mis amigos, especialmente Carlos mi compañero de Monografía, a mis compañeros de la universidad, a todos aquellos que han sido testigos del proceso, de la preparación y del esfuerzo para realizar esta monografía

Y por último quisiera agradecer a los docentes y tutores de la Universidad Tecnológica de Bolívar por la paciencia, tolerancia y compresión que tuvieron conmigo en este proceso de formación.

Gracias a todos por esperar junto a mí este día los quiero a todos con todo mi corazón.

BERNARDO JOSE HERRERA PÉREZ

AUTORIZACIÓN

Cartagena de Indias D.T. y C.

Nosotros CARLOS ALBERTO GIRALDO LIPEDA, con cédula de ciudadanía 73.009.119 de Cartagena y BERNARDO JOSE HERRERA PÉREZ con cédula de ciudadanía 1.047.366.751. Autorizamos a la Universidad Tecnológica de Bolívar para hacer uso de nuestro trabajo de grado y publicarlo en el catálogo online de la biblioteca.

Cordialmente,

CARLOS A. GIRALDO LIPEDA	BERNARDO J. HERRERA PÉREZ
CC.73.009.119 de Cartagena	CC. 1.047.366.751 de Cartagena

Cartagena de Indias D.T. y C.

Señores
COMITÉ DE FACULTAD DE INGENIERÍA DE SISTEMAS
Universidad Tecnológica de Bolívar
Ciudad

Estimados Señores.

De la manera más cordial nos permitimos presentar a su consideración y aprobación el trabajo de grado titulado “Diseño e implementación de Redes VANETS”. Elaborado por CARLOS ALBERTO GIRALDO LIPEDA y BERNARDO JOSE HERRERA PÉREZ.

Esperamos que el presente trabajo se ajuste a las expectativas y criterios de la Universidad para los trabajos de grado.

Cordialmente,

CARLOS A. GIRALDO LIPEDA	BERNARDO J. HERRERA PÉREZ
CC. 73.009.119 de Cartagena	CC. 1.047.366.751 De Cartagena

INTRODUCCIÓN

Actualmente las redes inalámbricas espontáneas sin dependencia de ninguna infraestructura como son las redes Ad-hoc, se encuentran en plena investigación y desarrollo a causa de su infinidad de posibles nuevas aplicaciones.

Una VANET o Vehicular Ad-Hoc Network, como su propio nombre indica, se trata de una red Ad-hoc donde sus nodos se corresponden con vehículos, concretamente estamos hablando de una red del tipo MANET (Mobile Ad-Hoc Network), es decir, una red ad-hoc móvil dónde sus nodos formarán dicha red en pleno movimiento con las dificultades que conllevará esto.

Estas redes vehiculares, presentan una serie de retos tecnológicos muy importantes debido al hecho de no tener infraestructura de red. Las funciones de autenticación, configuración, descubrimiento de servicios y provisión que tradicionalmente las llevan a cabo las operadoras, se tienen que llevar de forma distribuida entre los diferentes nodos de la red (los vehículos y sus equipos embarcados).

Debido a que la topología de red de las redes VANETS son variables, esto conlleva a que los nodos pueden moverse arbitrariamente, aunque generalmente lo hagan siguiendo ciertos patrones de movimiento, por ejemplo siguiendo las trayectorias de una vía, debido a esto la red se puede subdividir en varias y producir importantes pérdidas de paquetes. Son necesarios mecanismos que detecten estas circunstancias y minimicen estos efectos.

Son muchos los beneficios que se logran gracias a las redes VANETS, que sirven de soporte para una gran multitud de servicios en carretera. Estos servicios se clasifican en los siguientes tipos:

Servicios para la seguridad vial

Servicios para la administración

Servicios el entretenimiento

Servicios de utilidad

Actualmente en las redes VANETS se presentan varios tipos de problemas, más que todo vamos a dar a conocer dos puntos que para nosotros son cruciales el diseño e implementación y los problemas basados con la seguridad de las mismas. De igual forma, también palparemos los casos de aplicación de las redes VANETS en la vida real y sus grandes beneficios.

TÍTULO

Diseño e Implementación de Redes VANETS.

AREA DE INVESTIGACIÓN:

Redes Inalámbricas

COBERTURA DE INVESTIGACIÓN.

Institucional

CAMPO DE INVESTIGACIÓN

Personal Académico (Estudiantes y Profesores) IES (Instituciones de Educación Superior).

BREVE DESCRIPCIÓN DEL PROBLEMA.

Las redes VANETS presentan una serie de retos tecnológicos muy importantes debido al hecho de no tener infraestructura de red. Las funciones de autenticación, configuración, descubrimientos de servicios y provisión que tradicionalmente llevan a cabo las operadoras.

Debido a que la topología de red de las redes VANETS son variables, esto conlleva a que los nodos pueden moverse arbitrariamente, aunque generalmente lo hagan siguiendo ciertos patrones de movimiento, por ejemplo siguiendo las trayectorias de una vía, debido a esto la red se puede subdividir en varias y producir importantes pérdidas de paquetes. Son necesarios mecanismos que detecten estas circunstancias y minimicen estos efectos.

Actualmente en las redes VANETS se presentan varios tipos de problemas, más que todo vamos a dar a conocer dos puntos que para nosotros son cruciales el diseño e implementación y los problemas basados con la seguridad de las mismas.

OBJETIVOS

OBJETIVO GENERAL

Dar a conocer el estado actual de las VANETS a nivel nacional e internacional: Pasado, Presente y Futuro.

OBJETIVOS ESPECÍFICOS

- Aspectos básicos de las redes VANETS.
- Identificar los servicios, beneficios y desventajas propias de las VANETS.
- Factores que influyen en los aspectos actuales relacionados con:
  - ✓ El diseño e implementación: Tecnologías de hardware y software, y algoritmos de enrutamiento.
  - ✓ La seguridad informática: mecanismos utilizados para el control de la integridad de la información y el control de acceso.
- Dar a conocer la implementación de casos de VANETS en Colombia, Latinoamérica, USA, Europa y Asia, entre otros: Cobertura, Usos/Aplicación, Problemas que han tenido, Problemas que pueden tener

JUSTIFICACIÓN

Existe la necesidad de crear un documento que vaya dirigido a la comunidad estudiantil, profesores y todas aquellas personas que estén interesados en este tema. No podemos negar que hoy en día las redes inalámbricas espontáneas compuestas por terminales móviles sin dependencia de ninguna infraestructura están marcando el camino hacia una nueva generación de redes; así ha sido posible que hayan surgido nuevos servicios y prestaciones aplicables a diferentes campos o escenarios dónde hasta hace unos pocos años no era posible ofrecer tal conectividad. En este entorno es dónde encontramos las VANETS (Vehicular Ad-Hoc1 Networks), redes formadas entre los diferentes vehículos de un escenario determinado con la finalidad de intercambiar información para aumentar el confort y la seguridad de sus tripulantes. Aunque en la actualidad en nuestro entorno son muy pocos los recursos bibliográficos sobre redes VANETS, por eso queremos desarrollar este documento, para que les sirva de guía a todos los estudiantes, docentes y demás personas que quieran ampliar y difundir su conocimiento sobre este tema, ya que hasta la fecha de hoy son muy pocos los documentos en los cuales podemos obtener información clara y precisa sobre las redes VANETS.

TIPO DE INVESTIGACIÓN

La presente investigación es de tipo descriptiva, detallando el diseño, implementación y la seguridad acerca de las redes VANETS.

RECURSOS

Los recursos son documentos electrónicos tales como publicaciones, documentos técnicos y presentaciones hechas por los investigadores. Así como libros físicos, periódicos y archivos de prensa. Además de equipos de cómputo

AUTORES Y DIRECTOR

De la manera más cordial nos permitimos presentar el trabajo de Grado Titulado "Redes VANETS: Diseño, Implementación y aspectos de Seguridad". Elaborado por:

CARLOS ALBERTO GIRALDO LIPEDA y BERNARDO JOSE HERRERA PEREZ. Cuyo director de Monografía será el Ingeniero ISAAC ZUÑIGA SILGADO

RESUMEN

En muy pocos años, el campo de las redes AD-HOC ha tenido una rápida expansión visible en la proliferación de dispositivos inalámbricos de bajo costo como ordenadores portátiles, asistentes personales digitales, (PDAs), teléfonos móviles, entre otros.

Las redes AD HOC están formadas por dos o más dispositivos que son capaces de comunicarse entre sí sin la necesidad de recurrir a una infraestructura de red preexistente, con lo cual no son requeridas estaciones base ni cables ni routers fijos. Dichas redes pueden estar constituidas por grupos de terminales móviles independientes y basados en radio enlaces, aunque también cabría la posibilidad de que alguno de estos dispositivos estuviera conectado a un sistema celular o a una red fija.

Las AD-HOC se caracterizan por tener topologías dinámicas, donde los nodos se mueven libremente de manera arbitraria y en un tiempo impredecible y pueden estar constituidas por enlaces unidireccionales (comunicación en un único sentido) o bidireccionales (comunicación en ambos sentidos).

Dentro de este tipo de redes encontramos las redes MANETS (*Mobile Ad hoc NETwork*). Como su propio nombre indica la característica principal de una MANET es la movilidad de los nodos, estos pueden cambiar de posición rápidamente. La necesidad de crear redes de forma rápida en lugares sin infraestructura suele implicar que los nodos exploren el área y, en algunos casos, se deban unir para alcanzar un objetivo.
Este tipo de redes contienen un gran número de características como lo son: Ausencia de infraestructura, Topología dinámica, Ancho de banda limitado, Variación en la capacidad de los enlaces y los nodos, Conservación de la energía, escalabilidad, Falta de seguridad, Encaminamiento multisalto, Entorno imprevisible, Comportamiento de los terminales.

Pero a continuación haremos énfasis en el tema de mayor importancia en nuestro trabajo, hacemos referencia a las redes VANETS (Vehicular Ad-Hoc Network).
Se trata de una red ad-hoc donde sus nodos se corresponderían a vehículos (carros, camiones, autobuses entre otros.); en este caso, cabría la posibilidad de que dichos nodos formaran la red en pleno movimiento (por ejemplo mientras se circula por una autopista), por tanto, nodos que se mueven de forma arbitraria y que se comunican entre ellos (vehicle-to-vehicle), pudiendo tener también un

equipo fijo próximo que formara parte de la red y que también dotará a dicha red de una conexión.

Infraestructura de una Red VANETS

La infraestructura de una red VANETS se encuentra delimitada por:

- Unidades Carretera (RSU)
- Beacon
- UMTS. Universal Mobile Telecommunications System
- WIMAX
- Terrestrial Broadcast
- GSM
- RIFD
- GPS
- OBU
- Central Station

Uno de los componentes más importantes en la infraestructura de una red vanets es la estación central. Que es la encargada de administrar y operar una o varias carreteras de la red VANET, así como de dar soporte a los conductores y encargarse del mantenimiento de los dispositivos así como de los costos operativos de una red VANET.

Características de las Redes VANETS

Características	**Descripción**
Autonomía	Cada Terminal es un nodo autónomo con capacidad de procesado de la información y de encaminamiento de información proveniente de otros nodos de la misma red.
la topología de red es variable	Debido a que los nodos pueden moverse de forma arbitraria, aunque generalmente lo hagan siguiendo ciertos patrones de movimiento
Control distribuido de la red	Debido a la ausencia de infraestructura para el control de la red, este se realiza de forma distribuida

	en cada nodo
Encaminamiento	Es necesario que cada nodo por separado y todos en su conjunto sean capaces de proporcionar un mecanismo dinámico de encaminamiento.
Capacidad variable de los enlaces	Esta característica se produce en todas las comunicaciones inalámbricas.

En este tipo de redes, las principales áreas de aplicación son: la seguridad activa, servicios públicos, mejoras de conducción y negocios y entretenimiento móvil.

Los servicios de las redes VANETS están dirigidos a varios agentes como son el conductor, los ocupantes del vehículo, la administración de la red, las empresas.

Estos servicios se dividen en:

- servicios para la seguridad vial
- los servicios para la administración de las redes
- los servicios para el entretenimiento
- los servicios de utilidad.

Beneficios de las Redes VANETS

Los Beneficios de las redes VANETS a la comunidad son muy importantes dado que están empeñados en disminuir los accidentes de tráfico que son una de las primeras causas de muerte en el mundo. Encontramos beneficios en la Salud, mejora en el flujo de Transito, mejora el movimiento de las mercancías, incremento en la calidad de vida, entre otras.

Desventajas de las Redes VANETS

La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes VANETS. Este tipo de redes por el momento deben considerarse inseguras. Cualquiera podría estar escuchando la información transmitida. Y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos). En este caso es posible rastrear los movimientos de un cierto usuario, lo cual implica conocimiento de los hábitos privados de dicho usuario. Garantizar la privacidad de los usuarios a veces entra en conflicto con los requisitos de seguridad.

Las Interferencias. Las redes VANETS están expuestas actualmente a esto, ya que los automóviles se mueven a grandes velocidades y en su andar se puede diferir la señal con cualquier obstáculo. Los costos son una desventaja ya que implica un gasto el equipar la infraestructura de una red VANET con los siguientes elementos: las unidades a bordo, las unidades de carretera, el centro de control, los costos de comunicación y los costos de los proveedores de servicios.

Diseño de las Redes VANETS

El diseño de redes VANETS cuenta con los siguientes aspectos:

- protocolos eficientes para el enrutamiento,
- optimización de los protocolos broadcasting,
- localización optima de las estaciones a lo largo de la carretera y cálculo de rutas óptimas para vehículos en caso de accidentes.

Tecnologías de Software

Las tecnologías de software de las VANETS se dividen en simuladores de tráfico y simuladores de redes.

Simuladores de tráfico:

- GROOVESIM,
- CARISMA
- SUMO.

Entre los simuladores de redes tenemos el *NS2*.

Tecnologías de Hardware

Las tecnologías de hardware en las redes VANETS son aquellos dispositivos que permiten la comunicación, el soporte, la prestación de servicios.
Estos dispositivos son:

- CAN
- GPS
- VANETPC
- SYSTEM MONITOR
- POSITIONING PC

Algoritmos de Enrutamiento

Los algoritmos de enrutamiento se clasifican en:

Algoritmo	**Característica**
Algoritmos basados en el alcance	se dividen en 2 familias de protocolos, los unicast y los multicast
Algoritmos basados en el descubrimiento de rutas	se dividen en 3: los proactivos, los reactivos y los híbridos
basados en el algoritmo que implementan	Hay de 2 tipos los basados en el algoritmo estado de enlace (Dijkstra) y los basados en el algoritmo vector distancia (Bellman-Ford).

Mecanismos para el Control de la Integridad de la Información

Mecanismos	**Características**
PKI (Public Key Infraestructure)	Es una técnica que habilita el seguro intercambio de información, se logra a través del uso de una clave pública y privada que es generada a través de una entidad certificadora (CA)
DRP (Distributed Revocation Protocol)	Cada evaluador puede almacenar información acerca de acusaciones de privacidad y enviar los mensajes de acusación a los que son inculpados.
SEGURIDAD PARA MAC	se basa en que las unidades a bordo poseen una base de datos que contiene los componentes para firmar y verificar cada mensaje

Tipos de Ataques

Los ataques a las redes VANETS se clasifican en

- Falsificación de la información
- Manipulación de la información del sensor

- Denegación del servicio y falsificación de la identidad.

Mecanismos Para el Control De Acceso

Los mecanismos para el control de acceso están destinados para contrarrestar la mayoría de los ataques a las VANETS, aquí encontramos:

- **Control de Acceso:** que consiste en la autenticación de los usuarios de red para poder acceder a la red y sus servicios, en las redes inalámbricas se debe elegir un mecanismo de control de acceso distribuido para la red, basado en certificados digitales y autoridades certificadoras.
- **Cifrado y Gestión de Claves**: el empleo de técnicas de cifrado y de firmas digitales requiere del uso de claves criptográficas, se debe disponer de un mecanismo seguro para la gestión de claves. Para ello se dividen las VANETS en 2 esquemas: uno en el cual las claves se gestionan de forma autónoma y el otro esquema es que una entidad externa de confianza para la gestión de las claves.

Casos de Implementación de las Redes VANETS

Los casos de implementación de redes VANETS en la vida real tenemos: CVIS y CARTORRENT.

- *CVIS (Cooperative Vehicle Infraestructure Systems)*, la demostración al público de CVIS en Estocolmo (Suecia) fue el del *Public Road Tour*, en donde los visitantes podrían estar en uno de los 2 vehículos y disfrutar de los servicios y las aplicaciones. Las tecnologías mostradas fueron de comunicación, soporte a plataformas y mejorado del posicionamiento, con un total de 80-90 horas donde aproximadamente 400 personas pudieron disfrutar de los beneficios de esta demostración. Entre las aplicaciones CVIS más importantes tenemos: tecnología de comunicación, tecnología de posicionamiento, control de acceso, conducción segura.
- *CARTORRENT*, compartir el contenido utilizando el modelo P2P es muy popular en una red VANET. La limitada transmisión, la alta movilidad de los nodos hacen que los vehículos cooperen unos a otros para obtener información. Se han equipado 2 vehículos con un portátil cada uno que contiene 2 tarjetas inalámbricas, una de las tarjetas es la responsable por la comunicación y la otra es la responsable por la comunicación de los vehículos hacia los puntos de acceso. Cuando un vehículo recibe informes y solicita piezas de un archivo al punto de acceso, al mismo tiempo el vehículo recibe informes de piezas de otros vehículos.

CONTENIDO

Páginas.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

1. REDES VANETS (VEHICULAR AD-HOC NETWORKS)

Actualmente las redes inalámbricas espontáneas sin dependencia de ninguna infraestructura como son las redes ad-hoc, se encuentran en plena Investigación y desarrollo debido a su infinidad de posibles nuevas aplicaciones.

1.1 HISTORIA DE LAS REDES AD-HOC

En muy pocos años, el campo de las redes AD HOC ha tenido una rápida expansión visible en la proliferación de dispositivos inalámbricos de bajo costo como ordenadores portátiles, asistentes personales digitales, (PDAs), teléfonos móviles, entre otros.

A comienzos de los años 70 un trabajo pionero en radio de la Universidad de Hawái introduce el primer sistema que usa el medio de la radio para la transmisión de información, conocido ampliamente como ALOHA, fue desarrollado por Abramson y Kuo.

El trabajo realizado en Hawái llevó al desarrollo de una arquitectura distribuida consistente en una red de difusión de radio con mínimo control central llamada PARNET bajo el sponsor de DARPA en 1972.

El proyecto ayudó a establecer el concepto de redes móviles AD HOC. PARNET permitía la comunicación directa entre usuarios móviles sobre grandes áreas geográficas, ancho de banda compartido y protección contra los efectos de múltiples caminos. Los rápidos avances de la tecnología de la radio en los años 70 provocó la aparición de múltiples sistemas de comunicación móvil como teléfonos celulares e inalámbricos, sistemas de radio búsqueda, satélites móviles, entre otros.

Posteriormente, DARPA desarrolló el proyecto SURAN (*Survivable Radio Networks*) en 1983 que trata las tareas de escalabilidad de la red, la seguridad, la capacidad de proceso y gestión de energía. Se dedicaron esfuerzos para desarrollar dispositivos de bajo coste y con poco gasto de energía que pudieran soportar los avanzados protocolos de encaminamiento, escalar a miles de nodos las redes y dar soporte para ataques a la seguridad

El resultado fue la aparición de la tecnología conocida como LPR (*Low-cost Packet Radio*) en 1987. A mitad de los 90 se produce un nuevo avance con la llegada de tarjetas de radio 802.11 para ordenadores personales y portátiles. En dos artículos se propone por primera vez la idea de una colección de *hosts* móviles con una infraestructura mínima, y la IEEE (*Institute of Electrical and Electronic Engineers*) acuña el término de “redes ad hoc”.

Durante el mismo tiempo, el Departamento de Defensa de Estados Unidos continuaba trabajando con proyectos como el GloMo (*Global Mobile Information Systems*) o el NTDR (*Near term Digital Radio*). El objetivo del GloMo era permitir la conectividad multimedia de tipo *Ehernet*, en cualquier momento y en cualquier lugar, entre los dispositivos inalámbricos. NTDR son protocolos que se basan en dos componentes: agrupamiento y encaminamiento. Los algoritmos de agrupamiento organizan dinámicamente una red en líderes de grupo y miembros de grupo. Los líderes forman la columna vertebral de la red y los miembros se comunican entre sí a través de dicha columna. NTDR inicialmente fue un prototipo para la Armada de los Estados Unidos y en la actualidad algunos países lo utilizan como base para otros protocolos.

La definición de estándares como IEEE 802.11 provocó el rápido crecimiento de las redes móviles en campos no sólo militares, sino también en el mundo comercial. **[1][2]**

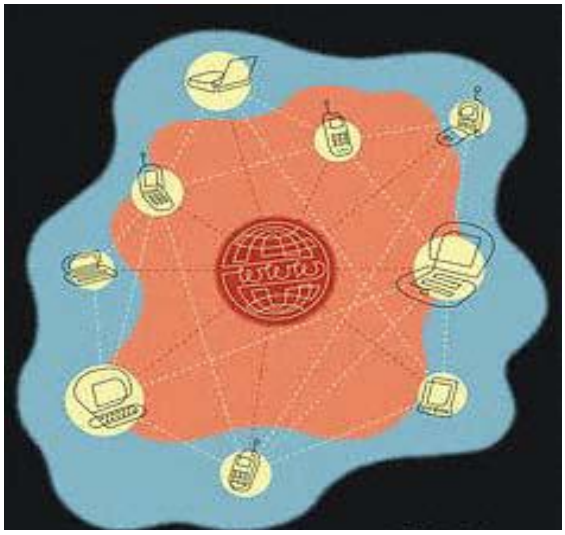
1.2 ¿QUÉ SON LAS REDES AD-HOC?

Puede definirse una red AD HOC como aquella que establece una comunicación espontánea entre terminales fijos y móviles o sólo móviles, siempre y cuando exista la posibilidad física de lograrlo.

Las redes AD HOC están formadas por dos o más dispositivos que son capaces de comunicarse entre sí sin la necesidad de recurrir a una infraestructura de red preexistente, con lo cual no son requeridas estaciones base ni cables ni routers fijos. Dichas redes pueden estar constituidas por grupos de terminales móviles independientes y basados en radio enlaces, aunque también cabría la posibilidad de que alguno de estos dispositivos estuviera conectado a un sistema celular o a una red fija.

Las redes AD HOC son adaptativas y están habilitadas para configurarse a sí mismas, prescindiéndose de la intervención de un administrador del sistema. En la práctica, las redes ad hoc podrían disponer desde decenas hasta centenares de nodos de comunicaciones capaces de cubrir alcances radio de 30 a 100 metros en interiores y de 100 hasta 300 metros en exteriores.

Figura 1. Red AD HOC



En las redes AD HOC es posible que dos nodos inalámbricos se puedan comunicar entre sí, incluso cuando se hallan fuera de su alcance radio, gracias a la presencia de nodos intermedios que actuarán como routers y reenviarán los paquetes de datos de la fuente al destino. Una red donde la comunicación entre dos estaciones se consigue mediante el reenvío de datos a través de otros nodos intermedios, recibe el nombre de red inalámbrica multisalto.

Las redes AD HOC se caracterizan por tener topologías dinámicas, donde los nodos se mueven libremente de manera arbitraria y en un tiempo impredecible y pueden estar constituidas por enlaces unidireccionales (comunicación en un único sentido) o bidireccionales (comunicación en ambos sentidos). En una red AD HOC se pueden realizar tareas de encaminamiento con el fin de optimizar la calidad de servicio. Las redes ad hoc presentan restricciones de ancho de banda motivadas

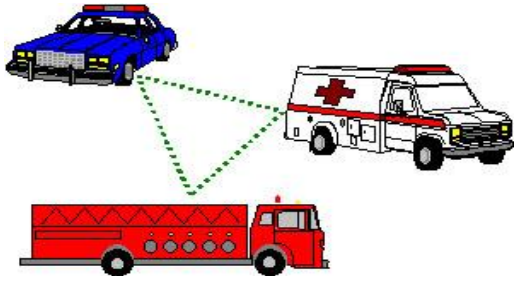
por la capacidad variable de sus enlaces inalámbricos y, como consecuencia, en muchas ocasiones se produce congestión. De hecho, el throughput de las comunicaciones inalámbricas es mucho menor que la tasa máxima de transmisión radio debido a causas tales como la contienda en el acceso múltiple, fading, ruido y condiciones de interferencia.

Este tipo de redes presentan muchos inconvenientes, mas en el ámbito de la calidad. Si proporcionar calidad de servicio en una red IP fija tiene sus complicaciones, conseguir ofrecer calidad de servicio en una red ad hoc se convierte en un reto tan extremadamente difícil como atrayente. En una red AD HOC resulta particularmente complicado proporcionar una cierta calidad de servicio porque tanto la topología como capacidad de los enlaces varían dinámicamente. Además, en los entornos inalámbricos la existencia de fading provoca que las tasas de pérdidas de paquetes y las variaciones de retardo sean mucho mayores y variables en comparación con las redes fijas.

Por todos estos motivos, se ha llegado a cuestionar si resulta viable proporcionar calidad de servicio a una red con estas características; no obstante, se han realizado y se están dedicando muchos esfuerzos para conseguirlo; prestigiosos investigadores de todo el planeta se hallan actualmente entregados a este propósito. En un principio, la investigación en el campo de las redes AD HOC se centró fundamentalmente en desarrollar redes aisladas e independientes, que pudieran desempeñar su labor en determinados escenarios destacados:

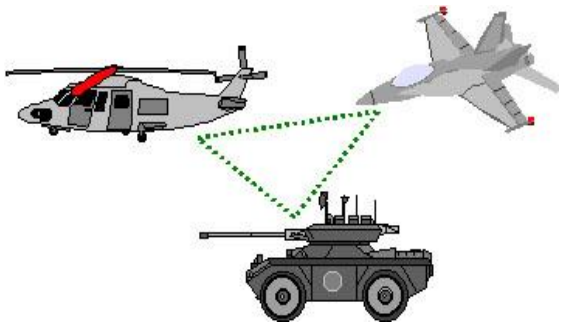
- Redes en catástrofes naturales (huracanes, inundaciones, terremotos, incendios, etc.), es decir, en zonas que carecen de infraestructura.

Figura 2. Aplicación de red AD HOC



- Redes en operaciones militares en zonas donde tampoco haya infraestructura

Figura 3. Aplicación de red AD HOC en operaciones militares



- Redes en áreas remotas o muy escasamente pobladas, donde no salga a cuenta instalar redes con infraestructura. **[2]**

1.3 ¿QUÉ ES UNA RED MANETS?

Una red MANET (*Mobile Ad hoc NETwork*) es un conjunto de nodos móviles que se comunican entre sí a través de enlaces inalámbricos (*wireless*). Al contrario de las redes convencionales, una red MANET no necesita la existencia de una infraestructura previa ya que cada nodo se apoya en los demás para conseguir comunicarse con otro creando la llamada comunicación multisalto.

Como su propio nombre indica la característica principal de una MANET es la movilidad de los nodos, que pueden cambiar de posición rápidamente. La necesidad de crear redes de forma rápida en lugares sin infraestructura suele implicar que los nodos exploren el área y, en algunos casos, se deban unir para conseguir un objetivo. El tipo de movilidad que desarrollen los nodos puede tener una influencia a la hora de escoger el protocolo de encaminamiento que aumente el rendimiento de la red. Otro de los aspectos importantes en la redes ad hoc es la llamada auto organización La idea Principal se basa en la coordinación y colaboración de todos los nodos de la red para conseguir un mismo objetivo. Se

han propuesto varios métodos de auto organización para redes en general y para redes ad hoc en particular. La autoconfiguración puede desglosarse en las siguientes capacidades:

- **Auto-reparación**: mecanismos que permitan detectar, localizar y reparar automáticamente los fallos siendo capaces de distinguir la causa del error. Por ejemplo, sobrecarga o mal funcionamiento.

- **Auto-configuración**: métodos de generación de configuraciones adecuadas en función de la situación actual dependiendo de las circunstancias ambientales. Por ejemplo, conectividad o parámetros de calidad de servicio.

- **Auto-gestión**: capacidad de mantener dispositivos o redes dependiendo de los parámetros actuales del sistema.

- **Adaptación**: adecuación a los cambios de las condiciones ambientales. Por ejemplo, cambio en el número de nodos vecinos.

A continuación se presentan características de las redes móviles AD HOC.

- **Ausencia de infraestructura**. Al contrario que las redes convencionales que cuentan con la existencia de elementos físicos, las redes móviles se forman autónomamente.

- **Topología dinámica**. Los nodos se pueden mover arbitrariamente haciendo que algunos enlaces se destruyan y otros se creen cuando un nodo se acerque a otros que antes tenía fuera de su alcance.

- **Ancho de banda limitado**. En la mayoría de las ocasiones será menor que el de una conexión cableada, afectado además por las interferencias de las señales electromagnéticas.

- **Variación en la capacidad de los enlaces y los nodos**. Los nodos pueden disponer de varias interfaces de radio que difieren entre sí en capacidad de transmisión/recepción y en la banda de frecuencia en la que

trabajan. Esta característica complica el desarrollo de los protocolos de encaminamiento en gran medida.

- **Conservación de energía**. Algunos o todos los nodos de una MANET son alimentados por una batería y no tienen posibilidad de recargarla. Para estos nodos, el criterio más importante a la hora de diseñar sistemas y protocolos será la optimización de la conservación de energía.

- **Escalabilidad**. En muchas aplicaciones las redes ad hoc pueden llegar a tener miles de nodos lo que conlleva dificultad en tareas como direccionamiento, encaminamiento, gestión de localización, gestión de configuración, interoperabilidad, seguridad, etc.

- **Falta de seguridad**. La seguridad juega un papel importante en las redes ad hoc dado el carácter vulnerable de los enlaces inalámbricos que se forman. Los protocolos de encaminamiento deben proporcionar una comunicación segura. Existen áreas de investigación en este sentido que sugieren incluir datos de sensores externos e información geográfica y topográfica en el propio algoritmo de encaminamiento.

- **Encaminamiento multisalto**. Los nodos actúan como *routers* para retransmitir los paquetes que se intercambian nodos cuyo alcance no permite una comunicación directa.

- **Entorno imprevisible**. Las redes ad hoc pueden darse en terrenos en los que las situaciones no son las más óptimas debido a condiciones peligrosas o desconocidas. Pueden darse casos donde los nodos se destruyan, se estropeen o comiencen a producir fallos.
- **Comportamiento de los terminales**. Uno de las principales claves para que una MANET tenga un funcionamiento adecuado es la confianza que cada nodo tiene que tener sobre los demás. Sin esta confianza sería imposible crear un protocolo de encaminamiento ya que la información debe transmitirse por varios nodos intermedios. Normalmente, los protocolos de encaminamiento que descubren los terminales intermedios se basan en las respuestas que dan los nodos sobre el coste de la comunicación. Existen nodos maliciosos que podrían intencionadamente

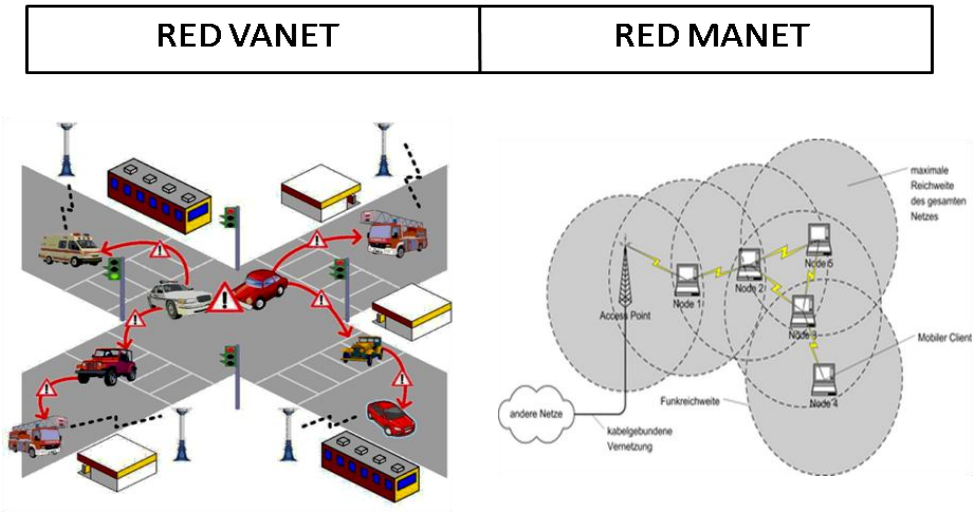
informar de forma incorrecta sobre los costes con la finalidad de recibir todos los paquetes, poder manipularlos, alterarlos o incluso eliminarlos. **[2]**

1.4 ¿QUÉ ES UNA RED VANET?

Una VANET o Vehicular Ad-Hoc Network, como su propio nombre indica, se trata de una red ad-hoc donde sus nodos se corresponderían a vehículos (carros, camiones, autobuses entre otros.); en este caso, cabría la posibilidad de que dichos nodos formaran la red en pleno movimiento (por ejemplo mientras se circula por una autopista), por tanto, nodos que se mueven de forma arbitraria y que se comunican entre ellos (vehicle-to-vehicle), pudiendo tener también un equipo fijo próximo que formara parte de la red y que también dotará a dicha red de una conexión.

1.5 VANETS vs. MANETS

Figura 4. Red Vanet vs Red Manet



- **Topología:** en una red MANET los nodos se mueven arbitrariamente, por lo tanto, la topología de la red que suele ser multihop puede cambiar rápidamente y al azar, a veces impredecible, y puede estar compuesta de enlaces bidireccionales y unidireccionales. En una red VANET los nodos

pueden moverse de forma arbitraria, aunque generalmente lo hagan siguiendo ciertos patrones de movimiento, por ejemplo siguiendo las trayectorias de una autopista. Debido a esto, la red se puede subdividir en varias y producir importantes pérdidas de paquetes. Son necesarios mecanismos que detecten estas circunstancias y minimicen sus efectos.

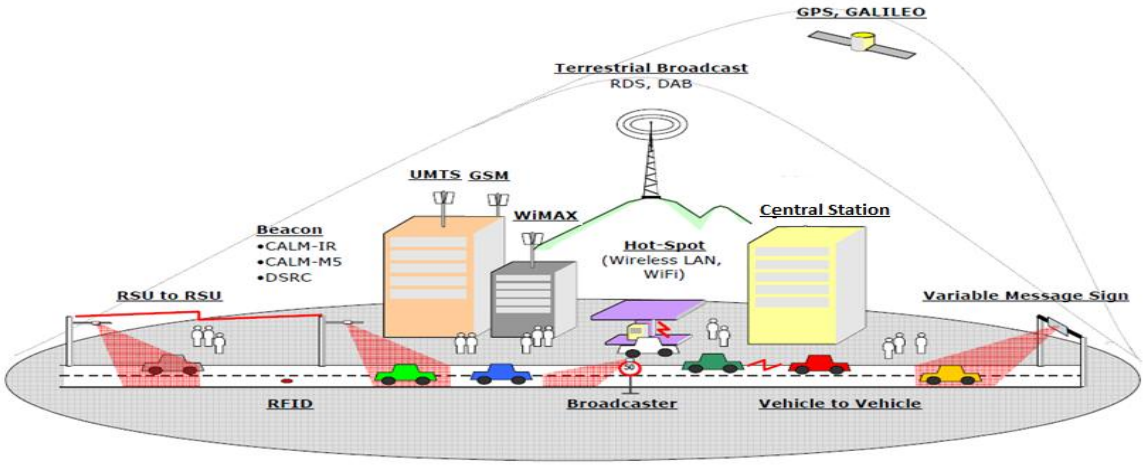
- **Consumo de energía:** algunos o todos los nodos en una red MANET pueden necesitar baterías para su funcionamiento, ejemplo: Portátiles, PDA, Celulares. Por eso uno del criterio más importante para el diseño de sistemas para redes MANETS es el de la conservación de energía. En el caso de las redes VANETS no se consideran restricciones en cuanto a la potencia consumida dado que son vehículos cuya batería tiene un tiempo de vida muy prolongado y que se va recargando en el camino.

- **Seguridad:** los mecanismos de seguridad de las redes VANETS son más complejos dado que está en peligro la vida del conductor y de los pasajeros. Problemas tales como la falsificación de identidad, denegación del servicio, manipulación de la información son muy graves y pueden hacer mucho daño a la seguridad de las redes VANETS. En las redes MANETS la seguridad se centra en el control de acceso para evitar que personas no autorizadas accedan a redes privadas inalámbricas. Como ventaja, el carácter descentralizado de control de redes MANETS prevé un fortalecimiento adicional en contra de los puntos únicos de fallo de enfoques más centralizado.

- **Particionamientos de la red:** debido a las grandes distancias que puede cubrir una red vehicular, es normal que una VANET sufra de frecuentes fragmentaciones en los grupos de vehículos. Caso contrario en las redes MANETS ya que las distancias que cubren las redes son muy pequeñas comparadas a las de las redes VANETS y por esto los grupos estarán más compactos, por ejemplo: una biblioteca, un lobby de un hotel, etc. **[3]**

1.6 INFRAESTRUCTURA DE UNA RED VANET

Figura 5. Infraestructura de una red Vanet



- **Unidades de Carretera (RSU):** actúan como intermediarios de comunicación entre las redes VANETS y las estaciones centrales, proporcionando a los vehículos a acceder a otro tipo de servicios, no relacionados con el tráfico. Los principales restos de esta tecnología serán: la integración de las RSU en las infraestructuras con total interoperabilidad en las redes y en los sistemas de tráfico, el despliegue de una arquitectura distribuida, flexible y fiable que sean capaces de recoger, almacenar y procesar los datos de los vehículos y su entorno, optimización en las comunicaciones mediante mejoras en los procedimientos para agilizar el descubrimiento y el acceso a los servicios. A largo plazo se prevé una evolución hacia un nuevo modelo integral de infraestructuras basadas en nodos inteligentes, de bajo coste distribuido a lo largo de la red.

- **Beacon:**
  - ✓ **CALM-M5:** es un estándar desarrollado lo más cercano posible a una onda supe conjunta, tiene en cuenta las normas internacionales en cuanto a los requerimientos multimedia. Se trabaja en el spectro global de los 5.9 GHZ

- ✓ **CALM-1R:** le agrega capacidades radiantes a las comunicaciones, y tomara la mayor parte del pesado trabajo de carga.

- ❖ **UMTS. Universal Mobile Telecommunications System:** es una de las tecnologías usadas por los móviles de tercera generación, sucesora de GSM, sus 3 grandes características son: las capacidades multimedia, una velocidad de acceso a internet elevada, la cual permite transmitir audio y video en tiempo real y una transmisión de voz con calidad igual a las de las redes telefónicas.

- ❖ **WIMAX:** Es el asíncrono de Worldwide Interoperability for Microware Access, es un sistema pensado para proporcionar servicios triple play, de voz, video y datos con una calidad de servicios independiente de si se opera en banda ancha regulada. Es la solución más económica y efectiva para suministrar banda ancha a escala universal.

- ❖ **Terrestrial Broadcast**

  - ✓ **RDS:** es un protocolo de comunicación que permite enviar pequeñas cantidades de datos digitales, con la señal emisora de radio FM. Se utiliza en Europa y Latinoamérica.
  - ✓ **DAB:** es un estándar de emisión de radio digital desarrollado por EUREKA, el DAB está diseñado para receptores como portátiles para la difusión de audio y mediante satélites, la cual permite introducir datos.

- ❖ **GSM:** Sistema Global para las Comunicaciones Móviles, es un sistema estándar para la comunicación mediante teléfonos móviles que incorporan la tecnología digital, por ello cualquier cliente de GSM puede conectarse a través de su teléfono con su computador y puede enviar y recibir mensajes de correo electrónico, faxes, navegar por internet y utilizar otras funciones digitales de transmisión de datos incluyendo el SMS.

- ❖ **Central Station:** es la encargada de administrar y operar una o varias carreteras de la red VANET, así como de dar soporte a los conductores y encargarse del mantenimiento de los dispositivos así como de los costos operativos de una red VANET.

- **RFID:** Es una ayuda al sistema GPS, su función es la de aumentar la precisión del sistema GPS para tener una posición más exacta de la persona, entidad que se quiera localizar.

- **GPS:** Es un sistema de posicionamiento global que permite determinar la ubicación de un vehículo, persona u objeto en todo el mundo con una precisión de metros. El GPS funciona mediante 27 satélites en órbita sobre la tierra a 20.000 KM de distancia. Cuando se desea determinar la posición de un vehículo, el GPS utiliza como mínimo 3 satélites de la red, de los que recibe las señales indicando su posición, con base a esta señal el GPS utiliza la triangulación que consiste en determinar la distancia de cada satélite con respecto al punto de medición.

- **OBU:** Son dispositivos que implementan las protocolos de comunicación y los algoritmos. El aumento progresivo de servicios y tecnologías en la OBU suponen que las investigaciones apunten hacia la capacidad de configuración de hardware para dar soporte a nuevos estándares de comunicación, de forma que los nuevos servicios puedan implementarse en módulos creados previamente. La capacidad de computación avanza hacia la segmentación de actividades, como en las operaciones de red por un lado y las comunicaciones más la interfaz de usuario por otro lado. Gracias al aumento en la capacidad de los nuevos procesadores, esto facilitara la implementación de modelos de comunicación e interacción más avanzadas y potentes. **[4]**

1.7 CARACTERÍSTICAS DE LAS REDES VANETS

Veamos a continuación el conjunto de características principales de estas redes:

- **Autonomía**. Cada Terminal es un nodo autónomo con capacidad de procesado de la información y de encaminamiento de información proveniente de otros nodos de la misma red. Gracias a esto el funcionamiento de la red no depende de ninguna infraestructura previa siendo así más tolerante a fallos del sistema.

- **Control distribuido de la red**. Debido a la ausencia de infraestructura para el control de la red, este se realiza de forma distribuida en cada nodo.

- **Encaminamiento.** Es necesario que cada nodo por separado y todos en su conjunto sean capaces de proporcionar un mecanismo dinámico de encaminamiento. Este encaminamiento multihop se basa en las capacidades de cada nodo. Los protocolos de encaminamiento clásicos no sirven en este contexto ya que no están preparados para estas variaciones de topología, puede que no converjan. Actualmente se están desarrollando multitud de algoritmos de encaminamiento para solucionar el problema. Más adelante detallaremos los más importantes en otra sección.

- **Topología de red variable**. En una VANET los nodos pueden moverse de forma arbitraria, aunque generalmente lo hagan siguiendo ciertos patrones de movimiento, por ejemplo siguiendo las trayectorias de una autopista. Debido a esto, la red se puede subdividir en varias y producir importantes pérdidas de paquetes. Son necesarios mecanismos que detecten estas circunstancias y minimicen sus efectos.

- **Capacidad variable de los enlaces.** Esta característica se produce en todas las comunicaciones inalámbricas, es intrínseca al medio de transmisión pero sus efectos se agravan más en las MANETS. Esto se debe a que cada nodo actúa como router y la información atraviesa múltiples enlaces inalámbricos. **[5]**

1.8 PRINCIPALES ÁREAS DE APLICACIÓN DE LAS VANETS

- **Seguridad activa:** la seguridad es uno de los temas primordiales en el desarrollo de tecnología automotriz, razón por la que este grupo de aplicaciones de las VANET es el de mayor interés. Su objetivo es hacer más segura la conducción de vehículos mediante la comunicación oportuna de señales de advertencia sobre una posible colisión, una velocidad excesiva de arribo a una curva, fallas en las condiciones del vehículo (frenos, luces, tren motriz, etc.). Estas aplicaciones pueden emplearse, incluso, para permitir que el vehículo intente de forma automática evitar el

accidente o para que reaccione de la mejor manera, en caso de que éste sea inevitable.

- **Servicios públicos:** ejemplos sobresalientes de este tipo de aplicaciones es el apoyo que pueden obtener los vehículos de emergencia (ambulancias, policía y cuerpos de rescate) mediante “sirenas virtuales”, anunciadas con anticipación a los demás vehículos. El conductor puede, así mismo, ser advertido sobre una potencial infracción al reglamento de tránsito, por ejemplo, al entrar a una zona con límite de velocidad inferior a la actual o al anunciar vuelta en una zona no autorizada, etc.

- **Mejoras de conducción:** este tipo de aplicaciones pueden emplearse para que los vehículos avisen un cambio en sus condiciones de movimiento (reducción o incremento de velocidad, cambio de carril, etc.) o su localización a los otros vehículos cercanos; también es posible recabar información de la infraestructura vial sobre la velocidad óptima de llegada a un semáforo para coincidir con la fase verde, zonas de embotellamiento o la disponibilidad de lugares de estacionamiento o permitir el diagnóstico remoto del vehículo, etc.

- **Negocios y entretenimiento móvil:** en este grupo se encuentran aplicaciones para facilitar la realización de transacciones durante el viaje, como pueden ser el pago de cuotas de peaje, descarga de contenidos multimedia, reservaciones, entre otros. **[6]**

2. SERVICIOS, BENEFICIOS Y DESVENTAJAS DE LAS REDES VANETS

2.1 SERVICIOS DE LAS REDES VANETS

Los servicios de las redes VANETS están dirigidos a varios agentes como son el conductor, los ocupantes del vehículo, la administración de la red, las empresas. Los servicios de las redes VANETS se dividen en 4 segmentos: los servicios para la seguridad vial, los servicios para la administración de las redes, los servicios para el entretenimiento y los servicios de utilidad.

2.1.1 Servicios para la Seguridad Vial

Son los más importantes dado que su objetivo es el de salvar vidas disminuyendo el número de accidentes en la carretera. En este sentido la comisión europea está haciendo un esfuerzo importante en la investigación, desarrollo e implementación de este tipo de servicios con el fin de que sean implementados lo más pronto posible.

Figura 6. Servicios seguridad vial

Los Servicios para la seguridad vial son:

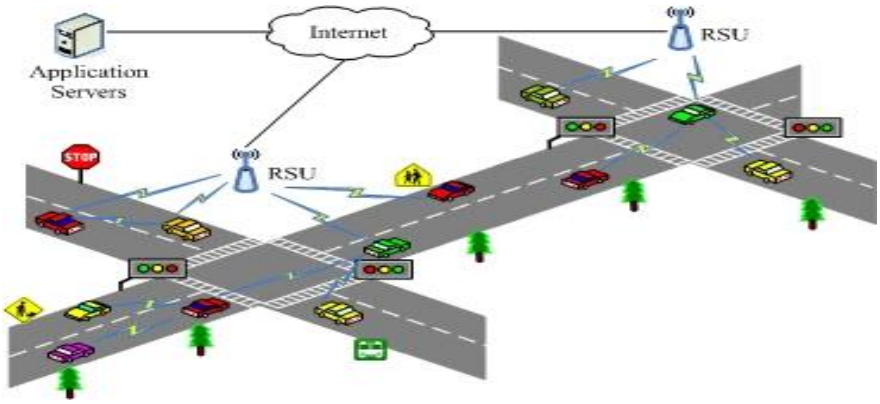
- **Mecanismos Anti-Colisión:** sirve para detectar posibles obstáculos en la vía. la funcionalidad principal consiste en el aviso de señales acústicas al conductor donde se le avisa la presencia de un vehículo. para un correcto despliegue de este servicio será necesario de una instalación en los automóviles de los usuarios donde especifique la posición, la trayectoria y la velocidad de cada vehículo y un mecanismo de escucha que permita recibir la información enviada por el resto de los vehículos y la carretera.

- **Aviso de Peligro:** la funcionalidad principal de este servicio es de detectar eventos peligrosos y luego comunicarlos a los vehículos que transitan la red. Consta de una serie de sensores que detectan el peligro y avisan a los usuarios con una breve descripción del problema que se presenta. Por ejemplo: cuando se produce un atasco en un cierto punto de la carretera donde están circulando los autos. también se puede necesitar el envió de un Geocast si se presenta otro problema en la vía, por lo tanto es necesario que los vehículos soporten el protocolo geocast para que no sobrecarguen la red con los mensajes enviados por broadcast.

- **ECALL:** este servicio consiste fundamentalmente en una llamada desde el vehículo a un número de emergencia en caso de accidente. Este servicio es una regularización de la unión europea y se espera que sea implementado completamente en el 2010. En caso de un accidente el automóvil trasmite una llamada de urgencia al centro de recepción de llamadas más adecuado y envía al mismo tiempo los datos del vehículo, principalmente la localización. El interés principal de este servicio es el de alertar de manera inmediata los servicios de urgencias, lo que permitirá reducir considerablemente el tiempo de espera y recibir la ayuda lo más pronto posible. **[3][7]**

2.1.2 Servicios para la administración

Figura 7. Servicios para la administración



- **Identificación de vehículos y obtención de información:** este servicio aportara una forma ágil y segura la información de los vehículos sin necesidad de detenerlos para ello será necesario una ley que permita que cada vehículo disponga de la información necesaria en formato electrónico y se trasmita automáticamente siempre y cuando un dispositivo debidamente autorizado lo requiera. Por ejemplo: cuando los policías están buscando vehículos sospechosos, con este servicio tendrán un mayor control de la carretera dado que recibirán la información de cada vehículo de una forma más ágil. Este servicio facilitara el control de las autoridades para que todos los servicios que transiten por las vías tengan la documentación necesaria (permiso de circulación, seguro, etc.). Cuando se detecte una infracción el servicio podrá trasmitir la denuncia de forma automática y tendrá asociado la identificación del conductor.

- **Detección de infracciones:** este servicio permitirá monitorear los parámetros de conducción de los vehículos. Los elementos de la infraestructura podrán obtener información sobre datos sensibles que pueden ocasionar peligro en las vías como: las velocidades excesivas, los tiempos de conducción sin parar, las infracciones en semáforos y stops y el tránsito por zonas prohibidas, entre otras. Todo aquello gracias al sistema de posicionamiento y las comunicaciones. **[7]**

2.1.3 Servicios para el entretenimiento

- **Acceso a internet desde los vehículos:** este servicio facilitara el acceso internet desde pantallas táctiles dentro de los vehículos. Este servicio suplirá las necesidades de comunicación del resto de los ocupantes del vehículo. los usuarios podrán acceder a toda la red, en donde podrán reservar hoteles, descargar contenidos entre otros. Una funcionalidad del acceso a internet es la descarga y reproducción de contenidos multimedia, debido a su gran adaptación se prevé que a corto plazo los vehículos dispongan de los medios para reproducir dicho contenido. Para ofrecer estos servicios el sistema de comunicaciones deberá ser capaz de acceder a internet a través de la red VANET o mediante la tecnología celular. La navegación y la descarga del correo electrónico no presentan grandes requisitos en términos de retardo y ancho de banda, mientras que para el envió de contenido multimedia se necesita de una buena calidad del servicio.

- **Envió de publicidad:** se puede desplegar un servicio mediante el cual los equipos de la infraestructura envíen publicidad, relacionada con los servicios de la vía. Los usuarios podrán configurar sus equipos para aceptar o rechazar este tipo de publicidad también los usuarios podrán crear un perfil modificable dinámicamente de forma que al circular por la autopista aceptaran avisos publicitarios de restaurantes, gasolineras, parqueaderos, centros de diversión. **[3]**

2.1.4 Servicios de utilidad

Figura 8. Servicios de utilidad

- **Calculo óptimo de las rutas:** este servicio puede ser usado desde el propio vehículo o como desde cualquier punto conectado a internet, se puede ofrecer como un servicio Web en donde informa permanentemente el estado de las carreteras en tiempo real. Se espera de que a largo plazo todos los vehículos podrán disponer de este sistema dado que facilitara la los conductores prever futuros atascos.

- **Tele diagnostico y ayuda online en caso de avería:** este servicio es liderado por las directivas de la comisión europea para liberar los manuales de reparación de los vehículos por parte de los fabricantes. Gracias a dicha liberación se podrán desplegar funciones como:

  - ✓ Consulta del manual electrónico por parte del conductor desde el vehículo
  - ✓ Consulta del manual por parte de las empresas de asistencia en carreteras
  - ✓ Consulta de un sistema experto en caso de averías

- ✓ Tele diagnostico: esta utilidad permite de forma remota valorar el grado de avería y facilitar la solución al conductor, ejemplo las instrucciones en caso de avería, el envió de la grúa.

- ❖ **Acceso automático en los peajes:** hoy en día se producen muchos problemas de retenciones en las autopistas y vías de pago que se producen en los tramos del peaje. Un servicio que gestione esto de forma automática y evitase a los conductores el parar en estas zonas ahorraría tiempo a los usuarios y reduciría el coste a la empresa gestora de la vía, dicho servicio consistiría en un mecanismo mediante el cual los vehículos puedan asociar su equipo a un medidor estándar de pago, tipo tarjeta crédito, esto permitirá el cargo automático del peaje sin necesidad de detener el vehículo. este sistema aportara mejoras a los sistemas tradicionales de pago en peajes ya que por un lado aumenta la distancia de comunicación y permite atravesar el peaje a mayores velocidades que las actuales. La seguridad de este servicio debe estar garantizada para evitar posibles ataques y el uso fraudulento de las tarjetas de pago de los usuarios.

- ❖ **Búsqueda y reserva de estacionamiento:** en los países desarrollados muchos de los parqueaderos públicos ya disponen de un mecanismo que informa a los vehículos entrantes de la localización de las plazas libres. Este servicio de búsqueda y reserva de estacionamiento es una extensión del servicio utilizado en los parqueaderos de forma que los usuarios desde el propio vehículo y en ruta puedan comunicarse con el parqueadero destino, notificarle la hora de llegada y reservar una de las plazas, por su parte el sistema de parqueadero aceptara la petición, facturara el cargo e indicara al usuario como llegar hasta su plaza.

- ❖ **Información y alerta de estaciones de gasolina:** a través de este servicio los usuarios podrán pedirle al sistema información acerca de las estaciones de gasolina, como las que se encuentran más cerca, las empresas prestadoras del servicio, los precios de los tipos de combustibles. para esto las estaciones de gasolina deberán entregar información y se comprometerán a tenerla actualizada a todo momento. a largo plazo una extensión de este servicio será la integración de sensores que informan de la cantidad de combustible restante en el automóvil y la ruta programada a la estación de gasolina más cercana. **[3][7]**

2.2 BENEFICIOS DE LAS REDES VANETS

Los Beneficios de las redes VANETS a la comunidad son muy importantes dado que están empeñados en disminuir los accidentes de tráfico que son una de las primeras causas de muerte en el mundo. Las redes VANETS mejoran la calidad de viajar de las personas ya que les permite seleccionar las rutas con información actualizada en tiempo real, notifica a los conductores sobre accidentes en la carretera, presta servicios de utilidad, seguridad y entrenamiento a los ocupantes de los vehículos, reducen el consumo de combustibles y los gases de efecto invernadero cuando dirigen los vehículos a sus destinos y esto evita que se desperdicie el combustible y así reducir las emisiones de $C0_2$. También hay beneficios para los administradores ya que permite utilizar plenamente la red de una carretera dado que puede controlar el flujo de vehículos basado en la monitorización y detección de congestiones en la vía, permite reconfigurar dinámicamente un segmento del tráfico a una determinada dirección. Los Beneficios de las redes VANETS pueden ser de varios tipos:

- **Salud:** dado que reduce los accidentes de tráfico ya que son una de las causas principales de muerte en el mundo

- **Mejora el flujo de Trafico**

  - ✓ Posee una Mejor gestión del tráfico y la velocidad de los conductores.
  - ✓ Alivia la congestión del tráfico.

- **Mejora las decisiones de viajar por parte del conductor**

  - ✓ Posee avanzadas herramientas de planificación de viaje.
  - ✓ Sistemas avanzados de asistencia al conductor.
  - ✓ Información de los viajes disponibles en vehículos particulares y públicos, en las paradas de autobuses, en las terminales, en el hogar y en la oficina.
  - ✓ es un apoyo a conductores de la tercera edad y a conductores sin experiencia.

- **Mejor protección y seguridad**

  - ✓ Mejora la gestión de accidentes.
  - ✓ Sistemas de prevención de accidentes.
  - ✓ Control y seguimiento a vehículos de transporte público.
  - ✓ Mejor vigilancia a los medios de transporte.

- **Reducción del consumo de combustible y de las emisiones contaminantes**

  - ✓ Reducción en las demoras para los transportistas en los puestos de control.
  - ✓ Planificación de los viajes para reducir el tiempo optimizando las rutas.
  - ✓ Vigilancia en la carretera del medio ambiente.

- **Mejora el movimiento de las mercancías**

  - ✓ Mejora de extremo a extremo la gestión de mercancías.
  - ✓ Posee una mejor gestión de la logística.

- **Aumento de la productividad económica**
  - ✓ Proporciona una mayor capacidad de transportar carga y promover el comercio.
  - ✓ Mejora la eficiencia operativa.
  - ✓ Ahorra millones de dólares en tiempo perdido.
  - ✓ Puede contribuir al desarrollo de infraestructuras.
  - ✓ Control y seguimiento a vehículos de transporte público.
  - ✓ Mejor vigilancia a los medios de transporte.

- **Incrementa la calidad de vida**

  - ✓ Mayor acceso a los servicios de transporte para todos los viajeros
  - ✓ Un mejor confort, comodidad y mayor seguridad
  - ✓ el despliegue de la infraestructura de comunicaciones. **[8]**

2.3 DESVENTAJAS DE LAS REDES VANETS

La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes VANETS. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red. Sin embargo, en una red inalámbrica (VANETS) desplegada un tercero podría acceder a la red, bastaría con que estuviese en un lugar próximo. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior.

Este tipo de redes por el momento deben considerarse inseguras. Cualquiera podría estar escuchando la información transmitida. Y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos). Las mismas precauciones que tenemos para enviar datos a través de Internet deben tenerse también para este tipo de redes.

Una de las principales debilidades en las redes VANETS es la seguridad, más que todo hacemos referencia a La privacidad. En redes ad-hoc es una meta complicada de conseguir. En este tipo de redes los usuarios finales requieren servicios y envían información personal (e.g. identificadores, preferencias, entre otros.) a través de nodos que actúan normalmente como enrutadores y ocasionalmente como proveedores de servicios. Estos nodos no son de confianza y pueden comprometer la privacidad de los usuarios, analizando la información que estos reenvían a terceras personas.

Este comportamiento permite a los intrusos acumular información de diversas fuentes e inferir información importante sobre un usuario específico. En redes móviles o VANETS, este problema es incluso mayor. En este caso es posible rastrear los movimientos de un cierto usuario, lo cual implica conocimiento de los hábitos privados de dicho usuario. Garantizar la privacidad de los usuarios a veces entra en conflicto con los requisitos de seguridad. Por ejemplo, un sistema que ofrece servicios requiere que los usuarios se autentifiquen para asegurar el correcto pago por dichos servicios. Otro ejemplo ocurre cuando un cierto usuario se comporta de forma inadecuada en la red. El sistema debe ser capaz de identificar a dicho usuario para poder tomar medidas contra él. Las medidas que adoptemos para regular estas situaciones pueden afectar la privacidad de los usuarios. Los autores proponen que todos los nodos que participan en la red se

registren. Esta solución viola por completo las normas de privacidad. Los autores presentan un protocolo que permite a los nodos de una VANETS reconocerse cuando se encuentran de nuevo. Este esquema proporciona autenticación segura contra atacantes pasivos. El problema es que permite a los usuarios cambiar libremente su identidad.

Las Interferencias. Las redes VANETS están expuestas actualmente a esto, ya que los automóviles se mueven a grandes velocidades y en su andar se puede diferir la señal con cualquier obstáculo.

Al igual que los teléfonos celulares, Internet puede ser tentador y puede distraer a los usuarios de la carretera. Comprobación de mensajes de correo electrónico, navegar por la web o incluso ver los vídeos de YouTube pueden absorber los conductores y provocar accidentes.

Del mismo modo, mientras que los conductores pueden tener la oportunidad de hacer el trabajo mientras está de viaje, también pueden aprovechar esta oportunidad para participar en otras tareas de ocio, como la VOIP con la familia, ver noticias destacadas o escuchar.

Aunque aún quedan años, VANET es una tecnología que podría incrementar significativamente la productividad durante los tiempos que suelen ser improductivos. Sin embargo, para lograr esto, los usuarios VANET primero deben vencer las tentaciones y distracciones pausadas que proporciona Internet.

Otra debilidad de este tipo de redes es que el desarrollo actual es muy lento y se ven muy pocos avances en este sentido.

Los costos son una desventaja ya que implica un gasto el equipar la infraestructura de una red VANET con los siguientes elementos: las unidades a bordo, las unidades de carretera, el centro de control, los costos de comunicación y los costos de los proveedores de servicios. Uno de los mayores costos está en la instalación de las unidades de carretera y la configuración y mantenimiento de un centro de control, para ello se han dividido los costos en 2 tipos:

- **Costos para la compra e instalación de equipos:**
  - ✓ Los costos de la infraestructura física están determinados por los costos de los dispositivos tecnológicos que necesita la red VANET
  - ✓ Los costos de instalación para las unidades de carretera, los equipos en la estación central y los costos de instalación de dispositivos en los automóviles.

- **Costos operativos:**

  - ✓ Contratación, tomar en cuenta cuantos operadores y administradores son requeridos para la red VANET
  - ✓ Alojamiento, tomar en cuenta el espacio de oficina para los operadores, administradores y los equipos de la estación central.
  - ✓ Mantenimiento, en general los costos de mantenimiento y los costos de renovación de equipos.
  - ✓ Costos de comunicación
  - ✓ Costos del uso de servicios públicos

Tabla 1. Costo de implementación de una Red Vanet

Costo Implementación redes VANETS		Costos dispositivos del automóvil	
Dispositivo	**Costo**	**Dispositivo**	**Costo**
Unidad de carretera (RSU)(10)	**$5,000,000**	**Radares (Delantero, Trasero)**	**$2,000,000.00**
Beacon		**Equipo de comunicación**	**$600,000.00**
UMTS base station(10)	**$10,000,000**	**Unidad a bordo (OBU)**	**$300,000**
WIMAX Service(Anual)	**$2,000,000**	**Interfaz Grafica**	**$1,000,000**
Transmisión Terrestre	**$2,500,000**	**Sistema GPS**	**$600,000.00**
GPS service (Anual)	**$800,000**	**Grabadora de Datos**	**$700,000.00**
GSM service	**$2,000,000**		
Equipos de computación	**$80,000,000**	**Total Vehículo**	**$5,200,000.00**
Personal (anual)	**$180,000,000**		
Mantenimiento(anual)	**$5,000,000**		
Total Implementación	**287.300.000**		

2.3.1 ¿Qué se está haciendo para eliminar las desventajas de las VANETS?

Para disminuir el costo de los equipos, el consorcio CVIS (Cooperative Vehicle Infraestructure Systems) dice que actualmente los dispositivos para las redes VANETS son muy caros, pero a medida que se aumenta la escala de producción de dichos dispositivos, los precios bajaran. Las tecnologías cooperativas seguirán la evolución de los precios típicos de las tecnologías de información donde normalmente una caída de 25-30% en el precio puede ser visto como una duplicación del volumen. Se estiman que los costos de mantenimiento serán comparables con los costos de mantenimiento de los controladores de tráfico actuales. Para reducir los costos también se tienen que pensar en materiales menos costosos y que sean de igual resistencia en la elaboración de los dispositivos tanto para los automóviles, las carreteras y las estaciones centrales.
La seguridad en las redes inalámbricas es muy vulnerable, para ello el grupo CVIS toma esta desventaja de las redes inalámbricas como la principal prioridad a tratar en el tema de las redes VANETS. La seguridad es un prerrequisito para el correcto funcionamiento para hacer de los sistemas cooperativos seguros. El total de amenazas en todos los niveles de arquitectura (en las redes, sistema, niveles de aplicación) y las amenazas generales (errores en el sistema, negligencia, intrusión al sistema, etc.) dentro de los sistemas cooperativos, son analizadas para tomar las posibles contramedidas. A fin de habilitar las comunicaciones seguras así como de proteger la privacidad, un administrador de identidades es el responsable por el almacenamiento y el arrendamiento de pseudónimos para las aplicaciones cliente, la infraestructura del administrador de identidades ha sido investigada por el proyecto SeveCom. CVIS se ha enfocado específicamente en las prioridades de seguridad (Framework de autenticación y autorización para las aplicaciones). El grupo de trabajo *eSecurity* está cooperando con el artículo 29 de la comisión de trabajo Europea en la elaboración de un código de práctica para manejar las fallas de seguridad para la telemática de vehículos y los sistemas cooperativos. **[9]**
Los trabajos de investigación:

- **IEEE:** *Enhancing the Security of Local Danger Warnings in VANETs - A Simulative Analysis of Voting Schemes*. Ostermaier, Benedikt, Dotzer,
- **ACM:** *Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification*. Tim Leinmüller, Elmar Schoch
- **CVIS:** *"eSecurity" In-vehicle communication, Cooperative Systems: Workshop on Security and Privacy IssuES.* Emilio Dávila Gonzalez,

3. FACTORES QUE INFLUYEN EN LOS ASPECTOS ACTUALES RELACIONADOS CON: EL DISEÑO E IMPLEMENTACIÓN Y LA SEGURIDAD INFORMÁTICA

3.1 DISEÑO DE REDES VANETS

Actualmente existe una importante línea de investigación dedicada a estudiar el diseño y las posibilidades de una red ad hoc formada por vehículos "VANET", este tipo de redes permite el intercambio de información entre los usuarios que se encuentran en los vehículos así como el intercambio desde y hacia los proveedores de servicios que tienen estaciones colocadas a lo largo de las autopistas.

Entre las aplicaciones de las redes VANETS se encuentra la posibilidad de realizar estimaciones meteorológicas precisas gracias a los sensores situados en los vehículos que envían información permanentemente a las centrales meteorológicas y contribuyen a la mejora de la seguridad vial. Las aplicaciones destinadas a mejorar la seguridad vial tienen un interés social para reducir las dramáticas cifras de muertos que ocasionan los accidentes de tráfico. Gracias a las VANETS es posible alertar a los vehículos cercanos de un accidente para que así los conductores tomen las medidas con la suficiente antelación, del mismo modo el conductor puede cambiar su ruta para evitar una congestión.

En cuanto a las oportunidades de diseño inteligente, las redes VANETS son relativamente recientes y aunque poseemos un conocimiento previo existente sobre las redes inalámbricas y la telefonía móvil que permite que los diseños noveles funcionen, es necesario dedicarles considerables recursos en investigación para hacer de la tecnología de las redes VANETS más barata, eficaz, eficiente y asequible para la población mundial. Los aspectos claves para un diseño inteligente de las redes VANETS son:

- ✓ Protocolos eficientes para el enrutamiento de los paquetes de datos
- ✓ Optimización de los protocolos de broadcasting
- ✓ Optimización del uso de energía en los dispositivos móviles
- ✓ Localización optima de las estaciones a lo largo de la autopista
- ✓ Calculo de rutas óptimas para vehículos en caso de accidentes o congestión. **[10]**

3.2 TECNOLOGÍAS DE HARDWARE Y SOFTWARE PARA EL DISEÑO E IMPLEMENTACIÓN

3.2.1 Concepto de modelo de movilidad.

Uno de los grandes retos de las VANETS es el campo de su simulación para su estudio y desarrollo debido a su propia naturaleza. Hemos de tener en cuenta que nos será muy difícil acercarnos a la generación de modelos de movilidad realistas, ya que nos encontramos en un escenario donde los nodos existentes se moverán de forma arbitraria y cada uno de ellos de forma distinta, sus enlaces irán cambiando de estado a lo largo del tiempo dependiendo del entorno.

Para poder simular un comportamiento necesitamos un simulador que nos permita definir el comportamiento de los nodos. Movimiento, condiciones entre otros. con un simulador de redes, que nos servirá para evaluar los datos generados por el simulador de tráfico y simular la comunicación Wireless que nos definirá las características de propagación del medio radio, acceso al medio, enrutamiento, errores, seguridad entre otros. A este método conjunto de simulación se le denomina, simulación híbrida.

3.2.2 Tecnologías de Software

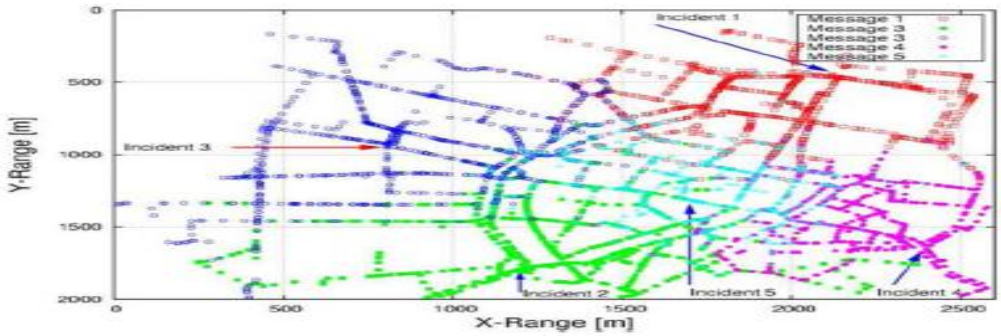
3.2.3 Simuladores de tráfico

Vamos a describir algunos de los simuladores de tráfico de entornos VANET mas utilizados y aceptados; comentar que la razón por la que hemos escogido éstos frente a otras opciones viene dada por la inclinación por parte de la mayoría de investigadores que se han dedicado a evaluar los diferentes simuladores de tráfico para estos entornos; estos simuladores de tráfico son GrooveSim, Carisma y SUMO.

- **GrooveSim.** La finalidad de este simulador de tráfico híbrido es la de ofrecer un modelo de movilidad en un escenario topográfico real a través de mapas digitales. Los desarrolladores del mismo afirman que Groove Simulator es capaz de simular comunicaciones vehicle-to-vehicle en movimiento donde intervengan miles de ellos, obteniendo logs para el registro de los datos de la simulación (pequeños informes donde se

registran los datos referentes a la simulación realizada). Uno de los aspectos a comentar es que GrooveSim se trata de un programa propietario y no gratuito. **[7]**

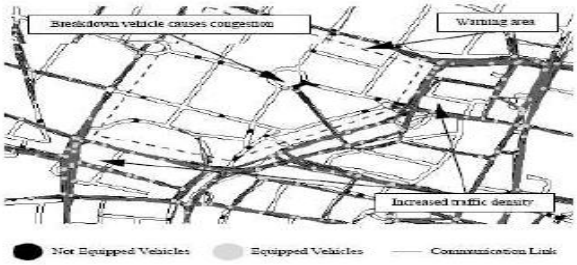
Figura 9. Captura del simulador GrooveSim



- **CARISMA.** En este caso estamos ante un simulador, que como el anterior, realiza las simulaciones en un entorno topográfico real tratándose también de un simulador híbrido.

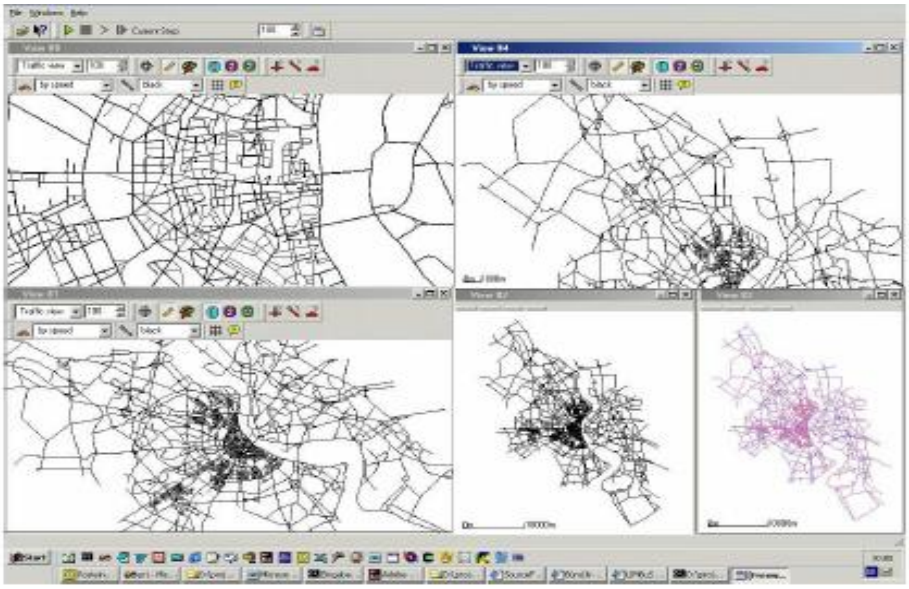
  Las principales características de CARISMA o Context-Aware Reflective middleware System for Mobile Applications son la posibilidad de emular escenarios que abarquen unos cientos o unos pocos miles de vehículos, solamente soporta dos carriles por carretera, cada calle posee la misma capacidad y prioridad de tráfico, supone que los edificios existentes están ubicados a lo largo de la calle, actualización de la posición de los vehículos cada segundo durante la simulación, evaluación y asignación de diferentes mecanismos de enrutamiento…entre otros. Sin duda un herramienta muy potente a tener en cuenta. De igual manera que en el caso anterior, Carisma también es un programa propietario y no gratuito. **[7]**

Figura 10. Captura simulador Carisma



- **SUMO.** Una de las grandes ventajas de SUMO o Simulation of Urban Mobility es que se trata de un simulador de VANETS de código abierto y gratuito desarrollado por la DLR o *Deutsche Gesellschaft für Luft und Raumfahrt*, es decir, el centro aeroespacial nacional alemán. Se trata de un simulador que permite definir entornos de movilidad reales gracias a la utilización de mapas digitales, ofrece la posibilidad de utilizar diferentes tipos de vehículos, carreteras que cambian en cuanto a su composición (carriles, velocidad, prioridades… entre otros.) y un amplio abanico de posibilidades e integración con otros simuladores debido a que es código abierto.

Figura 11. Captura simulador Sumo



Una de las limitaciones de SUMO frente a CARISMA, es el hecho de que éste calcula las rutas de los vehículos antes de realizar la simulación, cosa que dificulta la evaluación de la comunicación vehicle-to-vehicle afectada por variaciones en el comportamiento de los mismos durante la propia simulación, Herramientas para la simulación de VANETS 11 es decir, que nos será más difícil evaluar a tiempo real la comunicación entre vehículos frente a una variación provocada de su comportamiento de una forma repentina (aceleración, cambio de ruta, frenada …entre otros.) ya que con SUMO se tiene que prever todo esto antes de hacer la propia simulación. **[7]**

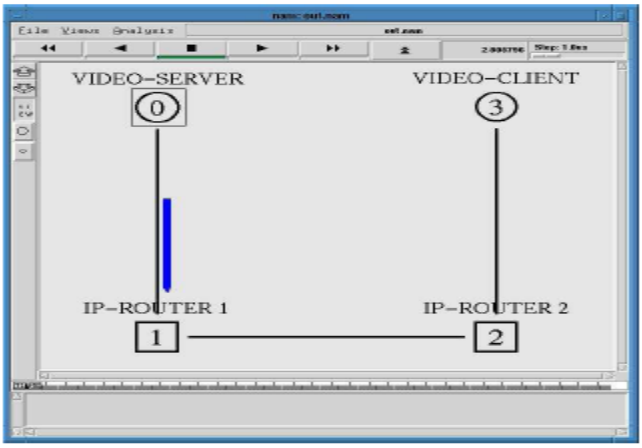
3.2.4 Simulador de redes.

Nuestro simulador de redes será el encargado de emular el entorno Wireless en nuestro modelo de movilidad, para ello hemos de exigir a éste una serie de prestaciones para su ejecución. Todos los que se han aventurado a la simulación de VANETS coinciden que el simulador que cumple con las exigencias es NS2 o Network Simulator 2.

- **NS2.** Network Simulator 2 es uno de los simuladores más ampliamente aceptados en la comunidad científica [10], además da la posibilidad de ser utilizado en conjunción con otros programas, como un simulador de tráfico (CARISMA o SUMO por ejemplo).

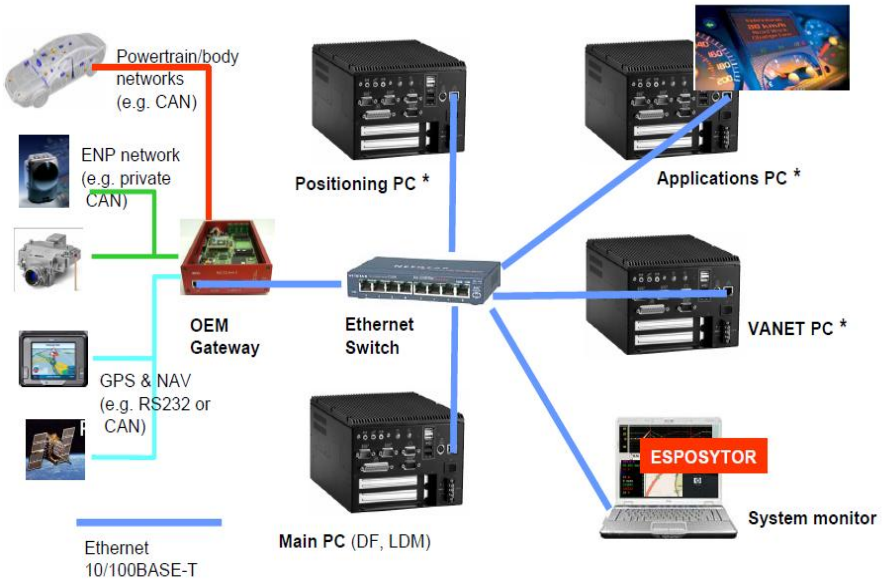
  NS2 implementa diferentes escenarios Wireless, diferentes modelos de propagación, implementación del protocolo de acceso al medio IEEE 802.11, tiene en cuenta los efectos de rebotes de la señal, como le pasa a esta por ejemplo en la carretera en una comunicación entre dos vehículos…entre otros. En definitiva, estos aspectos hacen a este simulador más que apto para su utilización en este campo. **[7]**

Figura 12. Captura NS2



3.3 Tecnologías de Hardware

Figura 13. Tecnologías de hardware



- ✓ **CAN:** Controller Area Network, es estándar usado en los vehículos que permite a los microcontroladores y otros dispositivos comunicarse unos a otros sin ningún computador central. CAN es un protocolo basado en mensajes, diseñado específicamente para aplicaciones vehiculares, pero también es usado en otras áreas como la automatización industrial y equipos médicos.

- ✓ **ENP network:** es una construcción de redes por una empresa para interconectar varios sitios de una misma compañía, ejemplo: sitios de producción, oficinas, tiendas, etc. En orden de compartir recursos computacionales alrededor de la red.

- ✓ **GPS:** es un sistema global de navegación por satélite que permite determinar en todo el mundo la posición de un objeto, una persona, un vehículo, etc. Con una precisión de centímetros. El GPS funciona mediante 32 satélites en la órbita sobre el globo a 20.00 km, con trayectorias sincronizadas para cubrir toda la trayectoria de la tierra. Para determinar la posición, se utilizan 3 satélites de la red, de los que se recibe señales que indican la identificación y la hora del reloj de cada satélite. Con base en estas señales, dispositivo sincroniza el reloj del GPS y calcula el tiempo que se tarda en llegar las señales al equipo y mide la distancia al satélite mediante una triangulación. Conocidas las distancias se determina la posición relativa respecto a los 3 satélites. Conociendo además las coordenadas de cada uno de los satélites, se obtiene la posición absoluta del punto de medición.

- ✓ **Ethernet 10/100BASE-T:** es un estándar de transmisión de datos para redes de área local. Ethernet define las características de cableado señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI. El estándar 10/100Base-T utiliza dos cables trenzados y alcanza una velocidad de 100 mbps.

- ✓ **Ethernet Switch:** es un dispositivo de lógica de interconexión de redes de computadoras que opera en la capa 2 del modelo OSI. Su función es la de interconectar dos o más segmentos de red, de manera similar a los bridges. Pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas de red. Los switches se utilizan cuando se desea

conectar múltiples redes, funcionándolas en una sola. Al igual que los bridges, dado que funcionan como un filtro en la red, mejorando el rendimiento y la seguridad de las LANs.

- ✓ **System Monitor:** es un sistema hardware-software usado para monitorear los recursos y el rendimiento en un sistema de computadora. Estos sistemas de monitoreo pueden seguir el rastro a los recursos del sistema, tales como la frecuencia y el uso de la CPU, la cantidad de memoria RAM disponible, también pueden mostrar información como la cantidad de espacio disponible en uno o más discos duros, las temperaturas de la CPU y otros componentes importantes. También la información de la red, como el sistema de direcciones IP, la taza de descarga y subida de archivos entre otros.

- ✓ **OEM Gateway:** es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red destino. El Gateway es normalmente un equipo informático configurado para dotar a las máquinas de un área local conectadas al de un acceso hacia una red exterior, usando operaciones de traducción de direcciones IP.

- ✓ **Positioning PC, VANET PC, Application PC:** serán incorporados en una Computadora basada en un algoritmo de complejidad. Esta computadora será capaz de realizar las tareas de la prestación de servicios de la VANET, la posición de los automóviles en la carretera y la distribución y ejecución de aplicaciones para la red vehicular. **[11]**

3.4 ALGORITMOS DE ENRUTAMIENTO

En estos últimos años las investigaciones acerca de los algoritmos de enrutamiento en las redes ad-hoc se ha incrementado, la movilidad de los nodos, la inestabilidad de las topologías y la ausencia de una infraestructura de centralización hacen obsoletos a los protocolos que se usan en redes fijas. En las redes ad-hoc los algoritmos de enrutamiento deben funcionar de forma automática y distribuida. Los algoritmos de enrutamiento que utilizan las redes VANETS se clasifican de la siguiente manera:

3.4.1 Algoritmos Basados en el alcance.

Se dividen en dos familias de protocolos los unicast y los multicast. Los protocolos unicast son los que envían información de un único destino a un único receptor, los protocolos multicast consisten en enviar información simultáneamente a múltiples destinos, antes del envió de la información, se deben establecerse una serie de parámetros para poder recibir la información, para ello es necesario unirse a un grupo “multicast”, este grupo tiene asociado una dirección. Por ejemplo en IPV4 se reservan las direcciones tipo D para el multicast. Los protocolos multicast se dividen en 3 protocolos que son el broadcast, el geocast y el anycast. El protocolo broadcast es aquel que manda información a todos los nodos dentro de su alcance, por lo tanto no es necesario haberse unido al grupo multicast previamente. El protocolo anycast envía información a un único destinatario, pero uno cualquiera no especificado. El protocolo geocast es aquel que envía tráfico a un grupo de receptores situados en la misma zona geográfica, este protocolo es usado en las redes MANETS. **[3]**

- **Protocolos Broadcast:** el broadcasting consiste en enviar tráfico desde un nodo origen a todos los nodos presentes en la red usando la técnica de múltiples saltos. Hay 4 tipos de protocolos broadcasting:

  - **Blind Flooding:** es el más simple dado que a la recepción de un mensaje, un nodo lo reenvía a todos sus vecinos, la optimización que presenta este protocolo es que cada nodo recuerda los paquetes flooding que ha recibido y si le vuelven a llegar no los retransmite evitando así duplicidades**.**

- **Multi-Point Relay Flooding (MPR):** consiste en elegir un grupo de nodos vecinos que cubren el acceso a los nodos distantes de 2 saltos. Esta mejora permite dividir por 2 el número de mensajes de control**.**

- **Neighbor Elimination Scheme (NES):** consiste en que un nodo recibe un mensaje de broadcast y no retransmite directamente si no que espera un tiempo aleatorio para ver si algún otro nodo envía la información. En este caso los nodos escuchan los mensajes y apuntan a que los nodos han enviado la información a otros. Después del tiempo de espera, el nodo envía el tráfico a los vecinos que no han sido informados por otros nodos.

- **Connected Dominating Sets (CDS):** consiste en organizar todos los nodos de la VANETS en una jerarquía. Se hace una clasificación de los nodos en 2 categorías: los nodos dominantes y los nodos pasivos. Los nodos dominantes son elegidos de manera que cubran la totalidad de la red en sus retransmisiones. Para construir la jerarquía dentro de la red, se asigna una prioridad a cada nodo, Un nodo es pasivo si dentro de sus vecinos directos hay un nodo dominante, si no existe el nodo dominante entonces el nodo se vuelve dominante. La asignación de prioridades a los nodos usa algoritmos matemáticos complejos. En la recepción de un mensaje broadcast, un nodo retransmite ese mensaje solo si se trata de un nodo dominante. **[3]**

- **Protocolos Unicast**

  - ✓ **Destination-Sequenced Distance Vector (DSDV):** el objetivo de este protocolo es evitar los problemas de bucles en la actualización de las tablas, para ello añade un nuevo campo a las tablas que es el número de secuencia que permite distinguir entre una tabla antigua y una nueva. Este protocolo utiliza el algoritmo de “vector distancias”, esto significa que mantiene las tablas con todos sus destinos accesibles junto con el siguiente salto, la métrica y el número de secuencia de la entrada en la tabla. Las tablas se envían en modo broadcast de forma periódica o cuando ocurre un cambio significativo de la topología de red. Una ruta es considerada mejor que otra si tiene un número de secuencia mayor. El problema de este protocolo

es que genera una elevada sobrecarga de control debido a los mensajes que envía permanentemente.

- ✓ **Dynamic Source Routing: s**e compone de 2 mecanismos: el descubrimiento y el mantenimiento de rutas que permiten a un nodo origen descubrir y mantener las rutas hacia un nodo destino cuando se necesita enviar tráfico en la red. Este protocolo es basado en la técnica de “Source Routing”, para determinar la mejor ruta completa hacia un destino. El nodo origen inunda la red con una trama de exploración, al recibir una copia de la trama cada nodo se agrega en la cabecera de la trama y actualiza sus tablas con la información contenida en la trama.

- ✓ **Location Aided Routing (LAR):** es un protocolo que introduce la idea del enrutamiento geográfico para disminuir la sobrecarga en el descubrimiento de rutas. La información geográfica es obtenida a partir de sistemas GPS, lo que limita el espacio de búsqueda y contribuye a una disminución de la cantidad de mensajes en la red y por lo tanto un incremento del rendimiento de la red. El protocolo LAR utiliza el mecanismo de descubrimiento de rutas del protocolo DSDV, la diferencia radica en que los mensajes no se envían a todos los vecinos, si no que a partir de la información geográfica, se consigue una inundación controlada de la red.

- ✓ **Temporally Ordered Routing Algorithm (TORA):** Es un protocolo basado en el concepto de “Links Reversal”. La idea de este protocolo es la generación de mensajes de control del protocolo en un pequeño conjunto de nodos cerca de la localización de un cambio topológico. El protocolo desarrolla funciones básicas, la creación de rutas, el mantenimiento y su eliminación. La creación de rutas corresponde la selección de la métrica para establecer un DAG (Directed Acyclic Graph) hacia el destino. El DAG consiste en asignar una dirección a los enlaces basada en las alturas relativas de los nodos vecinos, el nodo origen tiene la altura mayor y el nodo destino tiene la altura menor. El mantenimiento se refiere al hecho de adaptar la estructura de enrutamiento en respuestas a los cambios

topológicos de la red. Cuando un enlace no está disponible el DAG se rompe y es necesario una reparación de la ruta para restablecerlo. La fase de eliminación de rutas involucra un broadcast para eliminar las rutas que no contienen la ruta hacia un destino. El protocolo TORA elimina las rutas inválidas, busca una nueva alternativa para un destino y construye otra ruta.

- ✓ **AODV (Ad-hoc On Demand Distance Vector Routing):** el algoritmo AODV proporciona rutas libres de bucles aun cuando están reparando rutas dañadas, debido a que este algoritmo no requiere anuncios periódicos de enrutamiento globales, la demanda de toda el ancho de banda disponible es menor de aquellos protocolos que necesitan de dichos anuncios. Sin embargo este algoritmo mantiene la mayoría de las ventajas básicas de los mecanismos de enrutamiento del vector distancia. Los nodos no tienen que descubrir y mantener una ruta para otro nodo hasta que los 2 nodos necesiten comunicarse, a menos que uno de los nodos este ofreciendo un servicio como intermediario de una estación de trasmisión para mantener conectividad con otros nodos. Las tablas de enrutamiento de los nodos dentro del vecindario está organizada para optimizar el tiempo de respuesta para los movimientos locales y proporciona una respuesta rápida de tiempo para las solicitudes de establecimiento de nuevas rutas. **[3]**

- ❖ **Protocolos Geocast**

  - ✓ **Location Based Multicast:** es un protocolo orientado hacia la transmisión de datos que se basa en el protocolo unicast LAR. El protocolo LBM se basa en un flooding tradicional salvo que los nodos tienen que decidir si retransmiten o no a los demás nodos según los siguientes 2 esquemas:

    - **LBM Box:** en este caso un nodo a la recepción de un paquete Geocast retransmite a los nodos que se encuentran en la zona de forwarding, si no se encuentran reenvía el paquete.

- **LBM Step:** este esquema usa otra forma para determinar la zona de forwarding. Ejemplo: Si ***A*** recibe un paquete Geocast de un nodo ***B***, ***A*** retransmite el paquete si está más cerca del centro de la zona Geocast que de **B** por lo menos una distancia ***X***.

.

- ✓ **GEOTORA:** Este protocolo se deriva del protocolo unicast TORA, Se construyo modificando el protocolo TORA en Anycast y luego modificando el protocolo en Multicast. En el protocolo TORA se asigna un DAG para cada nodo de la red, en cambio en el protocolo GEOTORA se mantiene un único DAG para todo el grupo Geocast, logrando así que cualquiera de los nodos presentes en la zona Geocast sea destino, para ello primero el protocolo realiza un Anycast hacia un nodo de la zona Geocast. En la recepción de un paquete Anycast, el nodo se encarga de retransmitir en modo flooding a todos los nodos de su zona Geocast.

- ✓ **GAMER:** "Geocast Adaptative Mesh Environment for Routing" Es un protocolo Geocast que se basa en la idea de crear rutas redundantes desde el origen hacia una zona Geocast. Esta idea provino de constatar que solo una ruta hacia la zona Geocast es frágil sobre todo en un entorno de movilidad muy alta, como lo es el entorno vehicular. Por eso este protocolo propone rutas redundantes basadas en mallas hacia una zona Geocast. El protocolo GAMER se adapta de forma dinámica a la topología de red cambiando el tamaño de la zona de forwarding, lo que cambia la densidad de las mallas en tiempo real. Como consecuencia cuando los nodos son de movilidad alta una malla densa se crea y cuando hay movilidad baja, la malla se hace menos densa. El protocolo GAMER puede elegir en 3 esquemas diferentes que son: el CONE, CORRIDOR y FLOOD.**[3]**

3.4.2 Algoritmos Basados en el descubrimiento de rutas

Los protocolos basados en el descubrimiento de rutas se dividen en 3, los proactivos, los reactivos y los híbridos. Los protocolos proactivos son aquellos que intentan tener una independencia permanente de las necesidades de enrutamiento. Se busca tener actualizadas las tablas de enrutamiento a través del envió de mensajes de forma periódica, esto indica una respuesta rápida ante las solicitudes de ruta, sin embargo esto crea una sobrecarga importante de la red con los mensajes de control. Los protocolos reactivos son los que obtienen información del enrutamiento solo cuando es necesario, son protocolos de baja dependencia y solo buscan la ruta hacia un destino en el momento en el que se quiere mandar la información a dicho destino, obviamente la sobrecarga en la red es mucho menor, sin embargo los retardos al establecimiento de las comunicaciones son mayores. Los protocolos híbridos son los que combinan los protocolos proactivos y los reactivos, utilizando el protocolo proactivos para los nodos cercanos y utilizando los protocolos reactivos para los nodos más alejados. **[3]**

3.4.3 Basados en el tipo de algoritmo que implementan

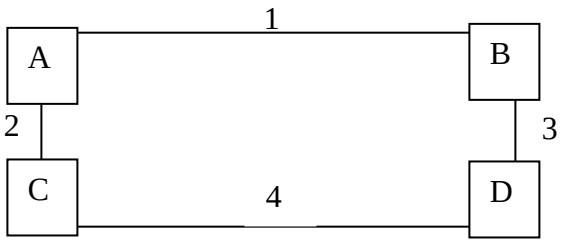
Los hay de 2 tipos los basados en el algoritmo de “estado de enlace” (Dijkstra) y los basados en el algoritmo de “vector distancia” (Bellman-Ford)**.** Los basados en el algoritmo de vector distancia, cada nodo mantiene una tabla de enrutamiento así:

Tabla 2. Tabla de enrutamiento

Desde A hasta	Enlace	Distancia
A	Local	0
B	1	1
C	2	3
D	2	5

Periódicamente cada nodo pasa su tabla a sus nodos vecino, así que con información recibida cada nodo calcula su tabla. Los protocolos basados en el estado de enlace son aquellos en donde todos mantienen una tabla del mapa completo de la red.

Tabla 3. Mapa completo de red



Desde A hasta	Hasta	Enlace	Distancia
A	B	1	1
A	C	2	1
B	A	1	1
B	D	3	1
C	A	2	1
C	D	4	1
D	B	3	1
D	C	4	1

Periódicamente cada nodo envía el estado del enlace a los demás nodos vecinos. Por ejemplo: el nodo A envía <B,1,1> <C,2,1>. Los mensajes recorren la red en todos los enlaces salientes. La recepción de una tabla de número de secuencia X tiene 3 posibilidades:

1) Si X es superior al número actual del mapa, se actualiza la tabla y se reenvía.

2) Si X es inferior al número actual del mapa, se manda el mapa actual por el enlace de llegada del mensaje.

3) Si X es igual al número de mapa, no se hace nada.

Con las tablas obtenidas, cada nodo aplica el algoritmo de Dijkstra para calcular las rutas óptimas. **[3]**

3.5 ATAQUES A LAS REDES VANETS

Podemos clasificar los ataques dependiendo su objetivo. Los ataques en que sus víctimas son una pequeña área de nodos se llaman ataques locales. Los ataques que afectan una gran área de nodos se llaman ataques extendidos. Por supuesto que un ataque extendido es más dañino para todo el sistema de seguridad, para ello se trata de un ataque local no aumente y se convierta en un ataque extendido. Pero no en todos los casos el área víctima del ataque no puede ser la misma área donde los nodos maliciosos están. En esta situación los adversarios podrán atacar desde largas distancias, este tipo de adversarios tienen más opción de convencer a los conductores con información falsa. Pero estos adversarios tendrán mayor éxito en convencer a conductores locales que a otros que se encuentran en otras aéreas dado que los conductores que se encuentran en otras aéreas reciben la información de los otros conductores cercanos y esto hará que estos ataques fallen.

El resultado de un ataque normalmente tiene 3 posibilidades: el éxito, el detectar pero no corregir y el detectar y corregir. La situación más favorable para un adversario es que la víctima este aislada y rodeada de nodos maliciosos. Este es uno de los casos más raros y la víctima no tiene más opción de que aceptar los mensajes falsos. La situación menos favorable para el adversario es que se hayan detectado que algunos nodos son maliciosos pero dado la poca información el nodo bueno no pueda corregir la falsa información. La peor situación para los adversarios es que no solo es detectado los nodos maliciosos si no que la información ha sido corregida dado que la víctima está rodeada de suficientes nodos buenos. **[12]**

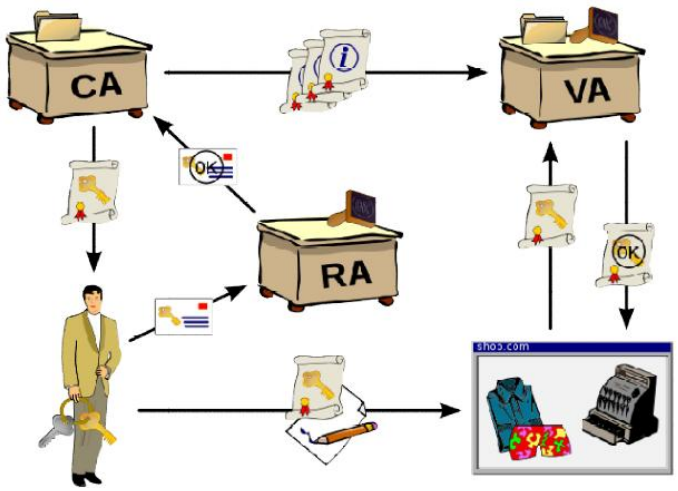
En general los ataques de las redes VANETS se clasifican por:

- ✓ **Falsificación de la información**
- ✓ **Manipulación de la información del sensor**
- ✓ **Denegación del servicio**
- ✓ **Falsificación de identidad**

3.6 MECANISMOS UTILIZADOS PARA EL CONTROL DE LA INTEGRIDAD DE LA INFORMACIÓN Y EL CONTROL DE ACCESO

3.6.1 PKI (Public Key Infrastructure)

Figura 14. Técnica PKI



Puede ser descrita como una técnica que habilita el seguro intercambio de información para los usuarios de una red. Esto es logrado a través del uso de una clave pública y privada que es generada e intercambiada a través de un certificado de autoridad. El PKI es un acuerdo que une las claves públicas con la identidad de los usuarios a través de un certificado de autoridad (CA). El certificado de autoridad identifica a los usuarios individualmente, para lograr esto, cada usuario debe estar registrado individualmente con un certificado de autoridad, después del registro, el certificado de autoridad agrega al usuario a una lista, y luego se actualiza la lista de identidades de usuarios que tienen asignadas claves públicas.

El certificado de autoridad también tendrá otra lista de usuarios que les han sido revocados la certificación. El PKI es usado porque asume el uso de la criptografía de clave pública, que es el método más común en internet para la autenticación de mensajes de remitente o la encriptación de un mensaje. El PKI posee una ventaja sobre la creación compartida para el cifrado y descifrado de datos, la tradicional clave compartida puede ser robada por un hacker o un intruso, luego esta persona será capaz de descifrar los datos utilizando la clave compartida que él puede

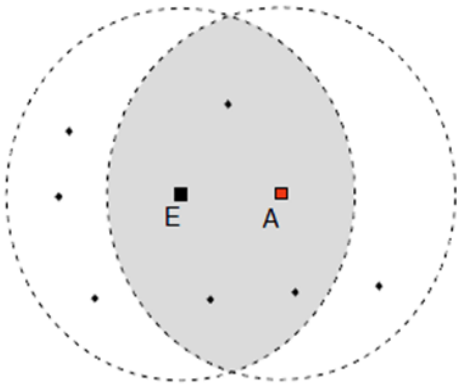
tener. Usando PKI se previene este problema ya que ambas partes poseen claves públicas diferentes. Las ventajas de PKI sobre otras técnicas de encriptación es que PKI permite a dos usuarios de la red autenticarse uno al otro para el envió de datos cifrados sin un contacto previo.

Por lo tanto no se necesita una clave para el intercambio de datos, pero esto puede ser una desventaja ya que es muy peligroso en todos los medios, ya que no se puede garantizar que la red es completamente segura. Otra ventaja es la lógica flexible y fácil detrás de la infraestructura PKI, para firmar un mensaje, el remitente cifra el mensaje con su clave privada, el receptor descifra el mensaje con la clave pública del remitente y si el mensaje es lo que se espera que el receptor sepa que fue enviado por el remitente. Para cifrar algo, el remitente cifra el mensaje con la clave pública del receptor. Luego solo el receptor puede descifrar el mensaje usando su clave privada. **[13]**

3.6.2 DRP (Distributed Revocation Protocol)

El protocolo DRP fue escogido debido a su naturaleza ad-hoc, lo que hace la verificación una manera simple e interesante. La idea inicial es de aplicar una técnica y herramienta de verificación semiautomática, como el modelo inspector de seguridad. La idea del DRP es que cada agente (evaluador) pueda almacenar información acerca de acusaciones o violaciones de privacidad y enviar mensajes de acusación a los agentes (acusados) que son inculpados de mal comportamiento.

Figura 15. Técnica DRP



Para que la votación tenga significado, solo los agentes en el barrio acusado deben tenerse en cuenta. Un barrio es un conjunto de agentes en el rango del evaluador y el acusado. Un agente solo puede recibir mensajes de otros agentes que están en su rango. Los votos de los agentes que están fuera del rango del acusado, no deben tenerse en cuenta. Al final si la mayoría de agentes reporta al acusado, este es reportado a un certificado de autoridad.

La figura muestra que solo los agentes en el rango del evaluador (E) y el acusado (A), son considerados vecinos del evaluador y el acusado, desde sus puntos de vista. El protocolo DRP posee varias características:

- ✓ Cada vehículo posee un reloj y un dispositivo GPS, para tener presente la ubicación y el tiempo. Cada vehículo posee un conjunto de claves seguras, estas son pares de claves publicas que son emitidas por una autoridad de certificación, estas son usadas para firmar los mensajes.

- ✓ Cada clave tiene un periodo de validez contenida en el certificado, la valides de los periodos de las claves de seguridad coinciden cuando en algún momento dado un vehículo posee un importante número de claves validas.

- ✓ Las claves son anónimas, solo la autoridad certificadora puede deducir si dos claves pertenecen al mismo vehículo.

- ✓ Las claves son almacenadas en un TPD (Tamper Proof Device) Dispositivos a prueba de manipulaciones, el TPD prohíbe al dueño del vehículo recuperar las claves. El TPD podrá sin embargo firmar ningún mensaje que solicite una clave de su elección.

- ✓ Un mensaje seguro contiene, un timestamp y la localización del remitente, el mensaje es firmado por una clave segura e incluye el certificado. Con esto cada vehículo que reciba un mensaje seguro, podrá determinar si el mensaje fue enviado por un usuario legítimo.
- ✓ La clave segura que es usada para firmar los mensajes es cambiada cada 2 minutos para asegurar la anonimidad del vehículo. **[14]**

Las desventajas del DRP son: falsas acusaciones a otros agentes y cuando un agente recibe los mensajes firmados, no puede deducir si esas claves pertenecen al mismo agente.

3.6.3 Protocolo de seguridad MAC para VANETS

Este protocolo puede proveer comunicaciones seguras, mientras garantiza la fiabilidad y los requisitos de rendimiento en aplicaciones DSRC relacionadas con la seguridad. DSRC (Dedicated Short Range Communications) es una tecnología clave que para aplicaciones y servicios de las redes VANETS.

Tabla 4. Ilustración de comunicaciones para seguridad en redes Vanets

Aplicaciones	Prioridad	Latencia	Trafico Red	Rango Mensaje
Seguridad Critica	Clase 1	100	Eventual	300m
Advertencia Seguridad	Clase 2	100	Periódico	50-300m
Cobro de peaje electronic	Clase 3	50	Eventual	15m
Acceso internet	Clase 4	500	Eventual	300m
Grupo comunicaciones	Clase 4	500	Eventual	300m
Servicio búsqueda rutas	Clase 4	500	Eventual	300m

La seguridad de las redes VANETS requiere de autenticación e integridad de mensajes, no repudiación de mensajes, entidad de autenticación, control de acceso, mensajes confidenciales, disponibilidad, privacidad, anonimidad y una identificación fiable para las aplicaciones seguras de clase 1 y clase 2 que se ven en la tabla. Para los mensajes no seguros como los de la clase 3 y clase 4, estos tienen diferentes requerimientos de los de clase 1 y clase 2. Se puede asumir que los otros mecanismos de seguridad se ocuparan de los requerimientos de seguridad de los mensajes tipo clase 3 clase 4.

Podemos asumir que cada unidad a bordo de los vehículos tiene una base de datos segura, que almacena todos los componentes criptográficos usados para firmar y verificar cada mensaje. Cada vehículo tiene que tener un certificado valido que usualmente es expedido por una autoridad certificadora (CA). El protocolo PKI sea utilizado para la emisión de certificados por una autoridad certificadora. Para la privacidad de un vehículo, como la identidad y la ruta, un conjunto de claves anónimas pueden ser usadas para firmar cada mensaje que se cambiara periódicamente. Estas claves pueden ser recargadas en la base de datos segura

de la unidad a bordo (OBU) para un largo periodo de tiempo. Por ejemplo licencia de matricula por un año, hasta el año siguiente. Cada clave es certificada por el emisor de una autoridad certificadora, y tiene un corto periodo de vida. En caso de accidente, las autoridades pueden acceder a la identidad real del vehículo usando un ELP (Electronic License Plate), esto también puede ayudar a la no-repudiación en caso de accidentes. **[15]**

Los atacantes no pueden alterar tanto el mensaje, como el timestamp, debido a la firma digital y desde que ninguna otra unidad a bordo conoce la clave privada del remitente, ninguna otra unidad a bordo puede alterar el contenido del paquete. El certificado del remitente es incluido en el paquete, de modo que los otros vehículos pueden extraer la clave pública del remitente y verificar si comprobar la regularidad de cada mensaje. Una vez que una unidad a bordo recibe un mensaje, esta compara el hash del mensaje y si los dos hash son iguales, el mensaje es verificado. En otro caso el mensaje es falso y será ignorado.

3.7 CONTROL DE ACCESO

Como en las redes tradicionales, las VANETS necesitan un mecanismo que controle el acceso tanto a la red como a los servicios que provee. Las consecuencias de un ataque en el cual un intruso tendría acceso a los servicios de la red pueden ser catastróficas ya en las VANETS los nodos asumen tareas de gestión y de encaminamiento al no tener una unidad de centralización. Un intruso podría desviar el tráfico durante el encaminamiento o tener acceso a claves de identificación.

En la capa de red, es necesario garantizar que ningún nodo no autorizado se una a la red bien para recibir información o para encaminarla. Así mismo a nivel de aplicación también es imprescindible asegurarse que elementos sin autorización no acceden a servicios, por ejemplo al servicio de gestión de claves.

El control de acceso consiste generalmente en la autenticación de los usuarios de la red. Es decir para acceder a la red y a sus servicios, un usuario debe identificarse de forma univoca y la red lo autentica como autorizado para el acceso. En ciertas redes ad hoc los servicios se encuentran centralizados mientras que en otras están distribuidos, este hecho hace necesario el uso de

diferentes mecanismos de control de acceso. Si elegimos un mecanismo de control de acceso distribuido para la red, será necesario un control de acceso basado en certificados digitales y autoridades certificadoras. En otros esquemas con servicios centralizados se requiere una autentificación basada en usuario y contraseña. Es muy útil hacer un estudio previo de las necesidades de seguridad de la red a desplegar, de esta forma, se podrían adecuar los mecanismos de control de acceso a la red. **[3][15]**

3.7.1 Sistema de detección de intrusos

El control de acceso consiste en una primera línea de defensa para impedir el acceso a la red a intrusos. Los sistemas de detección de intrusos (SDI) forman una segunda línea de protección muy importante. Existen varias propuestas de SDI para VANETS, veamos las más interesantes:

En el documento "*Intrusion detection in wireless ad-hoc net- Works*" los autores proponen una arquitectura distribuida y cooperativa para la detección de intrusos. En este sistema, cada nodo ejecuta un agente SDI que monitoriza las actividades locales al nodo. Si el SDI detecta una intrusión a partir de las trazas locales inicia un procedimiento de respuesta. Si se detecta una anomalía pero que no hay evidencias formales de la intrusión se usa un protocolo cooperativo con los vecinos para determinar si la intrusión tuvo lugar o no.

En el documento "*Intrusion detection using mobileagents in wireless ad-hoc networks*", se propone un sistema distribuido basado en tecnología de agentes móviles. Un agente móvil se define como una entidad software autónomo, ligero y dinámicamente actualizable que atraviesa la red y se ejecuta sobre ciertos nodos. Este método es especialmente apropiado en el caso de las VANETS, donde los recursos como el ancho de banda de los enlaces o la capacidad de los nodos pueden ser limitados. Las diferentes funciones del SDI se distribuyen entre diferentes tipos de agentes de forma que la carga introducida por el SDI se reparte de forma eficiente entre los nodos de la red.

En cualquier caso, el empleo de técnicas de SDI depende siempre de la aplicación y del escenario concreto sobre el cual se ejecuta.

La desventaja de este sistema es la sobrecarga que pueden introducir estos mecanismos, en términos de transmisión sobre el medio inalámbrico, de procesamiento y almacenamiento en los nodos, su uso puede resultar justificable únicamente en aplicaciones con fuertes requisitos de seguridad y en aquellas en las que los dispositivos involucrados dispongan de suficiente capacidad y autonomía como para que el SDI no imponga limitaciones intolerables para las prestaciones de los servicios finales ofrecidos al usuario. **[3]**

3.7.2 Seguridad en el encaminamiento

Los nodos en una VANETS actúan como routers, participando en el protocolo de encaminamiento para descubrir y mantener rutas hacia otros nodos de la red. En las redes tradicionales, los routers son administrados por operadores de confianza pero eso deja de ser cierto en las VANETS donde cada nodo que se une a la red participa en la toma de decisiones.

La desventaja de la seguridad en el encaminamiento radica en que si resultado del algoritmo del encaminamiento es manipulado, el funcionamiento normal de la VANET puede verse seriamente afectado. Por este motivo la seguridad en el encaminamiento es de primera importancia para la seguridad global del Sistema. La investigación para proporcionar protocolos de encaminamiento seguros sigue hoy en día, ya se han propuesto algunos esquemas. Se ha definido un conjunto de técnicas para diseñar algoritmos de encaminamiento ad-hoc resistentes a intrusiones, este conjunto se llama TIARA. Varios protocolos se basan en las técnicas TIARA como por ejemplo SRP o ARIADNE.

SRP proporciona información segura y autenticada a cada par de nodos que desea establecer una comunicación. El establecimiento se hará bajo una asociación de seguridad entre el nodo que inicia la comunicación y el nodo destino.
ARIADNE usa un proceso de criptografía simétrica que permite asegurar la integridad y la autenticación en las comunicaciones del protocolo. **[3]**

3.8 CIFRADO Y GESTIÓN DE CLAVES

El empleo de técnicas de cifrado y de firmas digitales como mecanismo de seguridad requiere el uso de claves criptográficas, que serán compartidos por todos los nodos. Por lo tanto, se debe disponer de un mecanismo seguro para la gestión de claves. Se puede dividir las VANETS en dos grupos: el auto organizado que se gestionan de forma autónoma y las VANETS que hacen uso de una entidad externa de confianza para la gestión de claves.

En esquemas de VANETS pura, sin red de respaldo, es más apropiado usar un esquema de gestión de clave que no depende de ninguna entidad externa. En cambio, si se dispone de una red de respaldo, se puede optar por esquemas de tipos centralizados. Las soluciones las más populares son:

Para una red VANET pura:

- ✓ Gestión de claves en cadena de certificados.
- ✓ Gestión de clave basada en movilidad.

Para una red VANET hibrida:

- ✓ Autoridades de certificación distribuidas.
- ✓ Gestión paralela de claves. **[3]**

3.8.1 Gestión de claves en cadena de certificados

Cada nodo genera su certificado, se distribuye y se almacena en cada nodo de la red. Si un nodo deja de fiarse de otro modo, se puede pedir una renovación del certificado. Del mismo modo, si un nodo sospecha que su clave privada ha sido comprometida, puede revocar su propio certificado y generar otra clave privada. Aquí la desventaja es que algunos nodos maliciosos podrán generar certificados falsos y distribuirlos por toda la red.

3.8.2 Gestión de claves basada en la movilidad

Se basa en un esquema de distribución peer-to-peer de las claves de los nodos basada en la movilidad de cada nodo. Se transmite una clave a un nodo según la movilidad que tiene en un momento para que este nodo distribuya las claves a los nodos a su alcance. Se rompe así la necesidad de tener una entidad externa para compartir las claves. **[3]**

3.8.3 Autoridades de certificación distribuidas

Se basa en una entidad externa de certificación que se encarga de distribuir las claves a los nodos de la red. La desventaja de este sistema es que si alguna persona logra tener el control de esta entidad, puede comprometer los mecanismos de certificación y así distribuir certificados falsos a todos los nodos de la red. Se puede distribuir los certificados de forma parcial o total.

En un mecanismo de distribución parcial de los certificados se elige un subconjunto de nodos llamados servidores a los cuales se transmiten las claves. Esos nodos deben disponer de una clave privada y una clave pública para que la entidad externa les pueda identificar de forma univoca. Cada uno de los servidores genera una firma parcial utilizando su clave privada que es enviada a un combinado, que puede ser cualquier servidor. El combinado reconstruye así la firma digital. En un mecanismo de distribución total de los certificados, la clave se distribuye a todos los nodos de la red y requiere que un nodo use la entidad externa para contactar con cualquier vecino. No es necesario el concepto de combinado ya que será el propio nodo quien reconstruye la firma digital del grupo. **[3]**

3.8.4 Gestión paralela de claves

Esta alternativa descrita en "*Composite Key Management for Ad- hoc Networks*", se basa en una distribución parcial de los certificados por parte de una entidad externa y de un mecanismo de cadenas de certificados. La propuesta es conocida como Composite Key Management. La entidad externa distribuye el certificado a nodos servidores y luego tiene lugar el mecanismo de cadenas de certificados. **[3]**

4. CASOS DE IMPLEMENTACIÓN DE REDES VANETS EN LA VIDA REAL.

4.1 CVIS (COOPERATIVE VEHICLE INFRASTRUCTURE SYSTEMS)

La demostración al público de CVIS en Estocolmo (Suecia) fue el de "*Public Road Tour*" en donde los visitantes podrían estar en uno de los vehículos y disfrutar una demostración de 30 minutos de las ocho aplicaciones CVIS y cuatro demostraciones tecnológicas. La aplicación mostrada fue elegida cuidadosamente para subrayar los beneficios de los sistemas cooperativos en soporte de: uso eficiente de la infraestructura existente, seguridad, cambios intermodales, redes sociales y anuncios locales.

Figura 16. Demostración de la gira de vía pública en Estocolmo

Las cuatro tecnologías demostradas fueron: tecnológicas de comunicación, soporte abierto de plataformas y el mejorado del posicionamiento. Todos los visitantes recibieron un volante del *Public Road Tour* que contiene un mapa de la gira y una corta descripción de cada demostración así como información para contactar a las compañías. Con un total de 80-90 horas en donde aproximadamente 400 personas pudieron disfrutar los beneficios del *Public Road Tour*, para la próxima demostración un mayor número de automóviles estarán disponibles. Después de la demostración de CVIS se les entrego a los participantes un formulario de preguntas acerca de las ventajas de las tecnologías CVIS. **[16]**

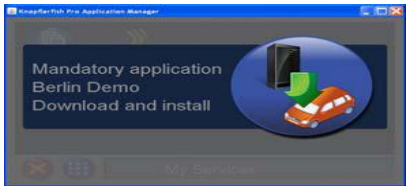
4.2 APLICACIONES CVIS

- **Tecnología de comunicación**: uno de los puntos clave de CVIS es la entrega sin fallas entre la variedad de canales de comunicación usados para los sistemas cooperativos. El sistema se cambia fácilmente entre el rango corto, el rango medio que es usado para sistemas integrados de transporte y el 3G que es usado para el internet y la comunicación.

Figura 17. Canales activos de comunicación

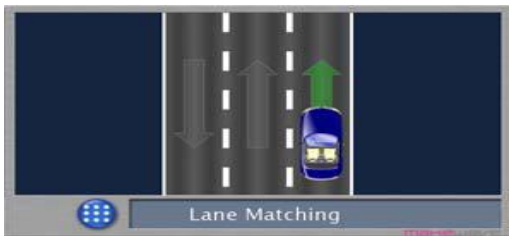
- **Plataforma de servicios abierta:** la naturaleza abierta de la plataforma CVIS habilita fácilmente la descarga automática de aplicaciones. Nuevos servicios se pueden agregar dinámicamente a la plataforma del automóvil durante el recorrido. El escenario de Estocolmo incluye una unidad de anuncios en la vía para una aplicación CVIS Live! Luego la aplicación CVIS Live! Es descargada por un centro anfitrión del host que está localizado en un servidor en Holanda.

Figura 18. Disponibilidad para descargar una aplicación.



- **Tecnología de Posicionamiento:** la mejora del posicionamiento desarrollado dentro de CVIS crea oportunidades para la eficiencia del camino. La mejora del posicionamiento provee un gran paso adelante comparado con las tecnologías actuales

Figura 19. Emparejamiento con el carril



- **Cobro en la Vía:** es una aplicación que permite los peajes mediante cercas geográficas. La naturaleza cooperativa de CVIS se muestra añadiendo una variedad de servicios de tráfico. Esta parte del *Public Road Tour* muestra la información y las tarifas en esta parte del camino, calculado por la oficina del peaje que

está en contacto directo con la aplicación del automóvil. **[16]**

Figura 20. Cobro de los servicios en la vía

- **Horario del tren:** esta aplicación ofrece a los conductores el estacionar los vehículos en una estación de tren. El horario actual del tren es enviado al automóvil por una unidad de carretera en la estación. La tabla de tiempo se presenta dinámicamente al conductor generando un aviso por el siguiente tren apropiado. La aplicación maneja modalidad múltiple proviniendo información acerca de la disponibilidad de aéreas de parqueo locales.

Figura 21. Programación del tren

- **Control de acceso:** esta aplicación demuestra el concepto de la movilidad sostenible mediante la generación de zonas seguras (color verde). La evitación de accidentes se basa en la limitación de túneles o puentes dependiendo de las características del vehículo y la carga. El vehículo recibe un anuncio cuando se aproxima a una zona controlada, ejemplo la ciudad de Estocolmo. Cuando se entra a una zona sensible, ejemplo una zona libre de camiones, se aplican las reglas que coincidan con la especificación del vehículo, si el vehículo cumple las reglas, se le concede el acceso por esa vía, si no se le niega.

Figura 22. Control de acceso

- **Mejora Conciencia del conductor:** cuando un vehículo se encuentra en sentido contrario, la aplicación se encarga de enviar un mensaje de alerta a los demás conductores en la vía. También envía una advertencia al control de tráfico central, este control puede informar inmediatamente a los vehículos que están en la ruta del peligro que produce antes de que puedan ver al automóvil.

Figura 23. Mensaje de alerta

- **Afluencia servicios de aplicación:** para disminuir el tráfico y los correspondientes atascos, la aplicación sugiere mediante invitaciones a los pasajeros para que suban al mismo automóvil, siempre y cuando vayan al casi todos al mismo destino. Esta aplicación ayuda al ahorro de gasolina y crea oportunidades de conocer gente nueva. **[16]**

Figura 24. Afluencia de servicios

- **Narrowcasting:** durante la jornada, puede ser útil ser informado acerca de varios servicios en la carretera, si son por suscripción o si son gratis. Durante el viaje, el sistema evalúa las opciones de gasolina del automóvil. La información acerca de la gasolina del automóvil es presentada al conductor mediante una narración, alguna preferencia personal acerca del tipo de estación de gasolina no es establecida debido a las políticas de las compañías de hidrocarburos.

Figura 25. Servicios en la vía

- **Conducción segura:** el sistema del automóvil permite la información de seguridad dinámica para el automóvil. Durante la jornada los invitados experimentaran dos ejemplos de esta aplicación de seguridad. Primero una advertencia basada en el tiempo para estudiantes es enviada al automóvil, puede ser en la mañana o en la tarde, cuando los niños entran o salen del colegio. Segundo una advertencia para cruses peligrosos más adelante, permitiendo al conductor reducir la velocidad. La comunicación entre la unidad de carreteras y los dispositivos de manos pueden ofrecer posibilidades para advertir a personas solo cuando están de hecho alrededor.

Figura 26. Precaución

- **Administración de flota:** esta aplicación reserva un avanzado espacio de parqueo para camiones en el destino o a lo largo de la carretera para la descarga de mercancías. En adición para ahorrar tiempo y millas en la búsqueda de un espacio para estacionar. En esta aplicación un vehículo de reparto puede hacer una reservación automáticamente por medio de un operador de flotas. Un sistema de reserva central procesa la reservación e informa al vehículo del lugar de parqueo. Si es necesario debido a demoras de tráfico, una actualización de tiempo o de lugar de parqueo será sugerida por el sistema.**[16]**

4.3 CARTORRENT

Compartir el contenido utilizando el modelo P2P ha sido más significativamente popular en una red vehicular ad hoc (VANET). La pequeña ventana de transmisión de un vehículo hacia un punto de acceso, la alta movilidad de los vehículos y la conectividad intermitente y de poca duración de hacia un punto de acceso, esto proviene a los vehículos incentivos para cooperar con otros para obtener información desde la internet. Estas características de las VANETS, naturalmente estipulan el uso de un modelo P2P cooperativo relacionado a una aplicación de contenido compartido como es “CarTorrent”. Se ha implementado la aplicación CarTorrent y se ha desarrollado en una VANET real. Se han hecho pruebas para afirmar la flexibilidad de una aplicación de archivos compartidos P2P.

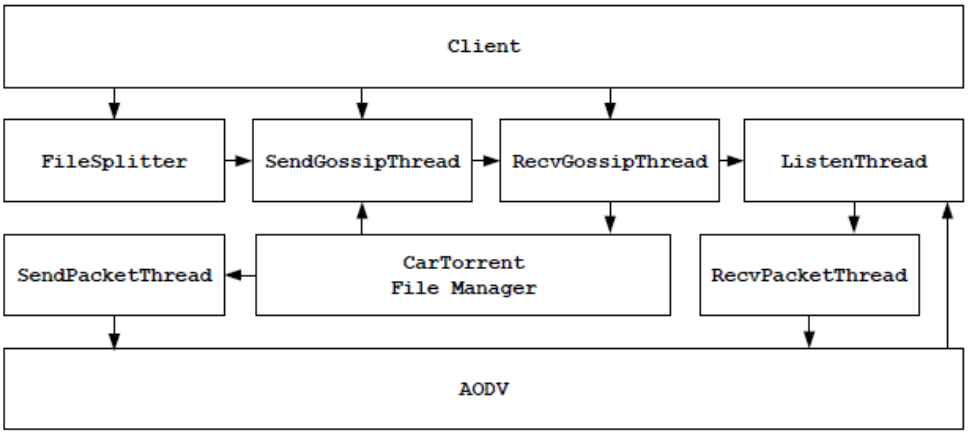
Los requerimientos de una navegación segura han propulsado el desarrollo y la implementación de las VANETS. Más allá de la navegación segura, nuevos tipos de aplicaciones tales como “Oficina sobre ruedas” y “Entretenimiento en autos”. Si las personas quieren descargar no solo música, si no tráileres de películas mientras manejan, pero también la información acerca de la localización de hoteles, las personas pueden descargar los archivos desde puntos de acceso que se encuentran en la carretera, que proveen la conexión a internet. El modelo convencional cliente-servidor en las redes VANETS, por las siguientes razones: primero dado la alta movilidad de los nodos, el tiempo de contacto actual a un punto de acceso es corto. Segundo en entornos reales la fuerza de la señal inalámbrica está dado por la distancia, entre más cerca este de la señal, mas fuerte será, si la distancia incrementa entre el vehículo y el punto de acceso, esto conlleva a un error de envió de paquetes dado que en algún momento se perderá la señal con el vehículo. Tercero no es practico instalar puntos de acceso en la carretera cada 300 metros, ni tampoco detenerse en la mitad del camino para descargar un archivo. Para manejar efectivamente esta situación, se utiliza la aplicación de archivos compartidos P2P, para los usuarios que están fuera del rango de un punto de acceso, puedan descargar los archivos a partir de otros nodos.

En un archivo P2P, como “BitTorrent”, el archivo es divido en partes iguales, y los nodos con las partes del archivo pueden intercambiar todo lo que esté disponible formando una red superpuesta. Esto no solo evita la sobrecarga a un servidor, sino que también incrementa la disponibilidad de las partes, acelerando el proceso de descarga. **[17]**

4.4 ARQUITECTURA CARTORRENT

La correcta progresión del compartimiento cooperativo P2P ha llevado el concepto de CarTorrent, como un protocolo múltiple que explota la naturaleza broadcast del medio inalámbrico y de la proximidad de los nodos, por el uso de un mecanismo informativo y una estrategia de selección novedosa.

Figura 27. Progresión del comportamiento cooperativo



- **File Manager:** cada archivo es manejado por el "CarTorrent File Manager", es el responsable por el rastreo y el estado de cada pieza de un archivo. Mantiene una lista de los nodos con sus respectivas piezas. Esta información es actualizada cada vez que una pieza de un archivo es descargada. La lista de los nodos también es actualizada cada vez que un cliente recibe un informe.

- **SendGossipThread:** es el responsable por él envió de informes periódicamente. Hay 2 tipos de informes. El primero es del nodo mismo, el segundo es de una cola donde los informes de los otros nodos se mantienen. Los informes son enviados con diferentes frecuencias basados en parámetros probabilísticos en el programa inicial del nodo. Los informes que son de interés del nodo son enviados con una alta prioridad usando una alta frecuencia. La prioridad es determinada si el nodo está interesado en el archivo que ha sido informado por otros nodos.

- **RecieveGossipThread:** es el responsable por el recibimiento de informes. El hilo desbloquea cuando recibe un informe. El informe es descartado si el informe es sobre el mismo nodo. Si el informe no es descartado, entonces es enviado al "CarTorrent File Manager" para un futuro procesamiento y

luego es mantenido en una cola de informes que serán enviados por el SendGossipThread.

- **SendPacketThread:** es el responsable por él envió de periódico de peticiones. Una petición para un archivo en particular es detener la descarga cuando el cliente haya descargado todas las piezas del archivo.

- **ListenThread y ReceivePacketThread:** cuando la aplicación CarTorrent inicia, el componente ListenThread es creado para las conexiones entrantes. Cada conexión entrante es luego manejada por el componente RecievePacketThread, para un futuro procesamiento. Al mismo tiempo el sistema crea 3 hilos RecievePacketThreads que procesaran las conexiones entrantes. Si el número de las conexiones entrantes es mayor que 3, habrá una demora en el procesamiento de las otras peticiones. Existen 2 tipos de paquetes entrantes. **[17]**

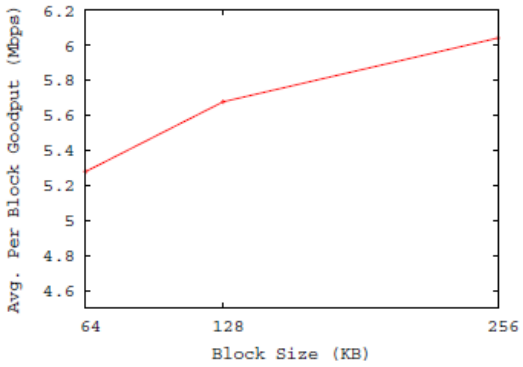
4.5 ESCENARIO APLICACIÓN CARTORRENT

Se han equipado 2 vehículos con un portátil que contiene 2 tarjetas inalámbricas 802.11b. Una de las tarjetas es la responsable por la comunicación de los vehículos en el modo ad hoc. La otra tarjeta es la responsable por la comunicación entre los vehículos y los puntos de acceso. Cuando un vehículo se aproxima a un punto de acceso, este recibe informes y solicita las piezas al punto de acceso, después de un tiempo el punto de acceso obtendrá las peticiones y enviara las piezas solicitadas. Al mismo tiempo, el vehículo recibe informes y solicitudes de piezas de otros nodos en otra interface. Desde que CarTorrent usa hilos para el recibimiento entrante de informes, dado que tiene la capacidad de tener en cuenta informes simultáneos tanto para solicitar alguna pieza al punto de acceso o para la petición de alguna pieza por parte de otro nodo. Las solicitudes son firmadas por el autor, esto permite al sistema identificar a que usuario se debe enviar las distintas piezas. Para evitar la interferencia entre 2 interfaces de tarjetas, se pone una tarjeta en el canal 1 y la otra se coloca en el canal 11. Se usa TCP como un protocolo de transporte, se ha especificado un tiempo de espera de 0.65 segundos para evitar el atascamiento para que así el componente “RecievePacketThread” pueda servir continuamente las peticiones entrantes. **[17]**

4.6 PRUEBAS CARTORRENT EN LA VIDA REAL

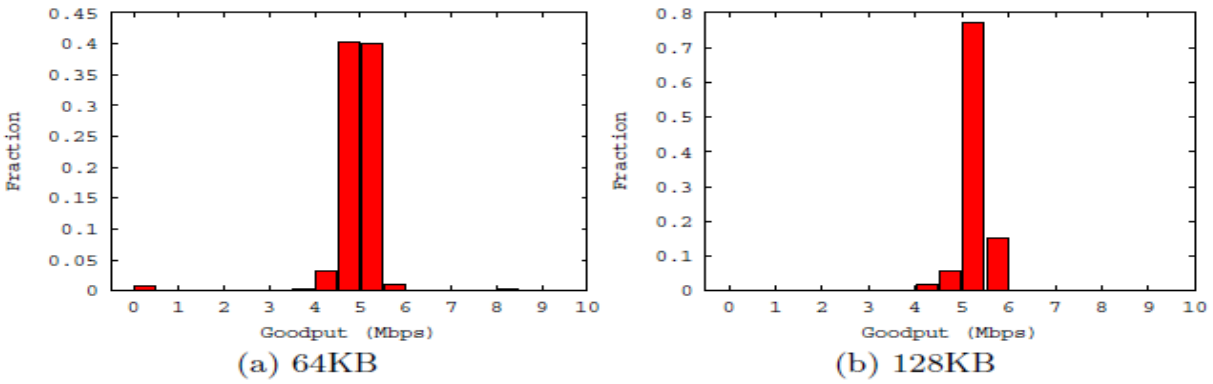
4.6.1 Estacionamiento

Figura 28. Muestra de pieza promedio por pieza



La figura muestra la pieza promedio de los tamaños de las piezas de 64 KB, 128KB y 256KB. Dado que las piezas son enviadas usando el protocolo TCP que toma tiempo para configurar, es más eficiente enviar piezas de gran tamaño, sin embargo el incremento del promedio por pieza decrece dado que las grandes piezas son más susceptibles a retransmisión en redes móviles. Por otra parte dado el tamaño del buffer del remitente y el receptor, las piezas de gran tamaño están sujetas a la fragmentación y a más procesamiento. Para dichas piezas que fallan al ser transmitidas en el rango de los nodos o del punto de acceso, estas son descartadas después de la desconexión. **[17]**

Figura 29. Distribución de rendimiento por pieza en un escenario de parqueadero



4.6.2 Carretera

Figura 30. Calidad de las líneas

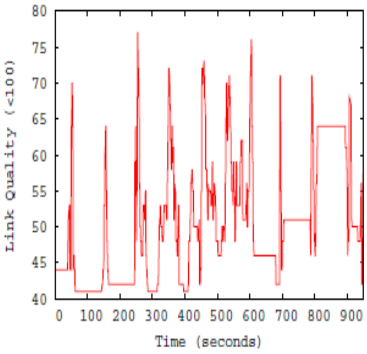


Figura 29 (a). Muestra la calidad de las líneas entre nodos en un entorno ad hoc.

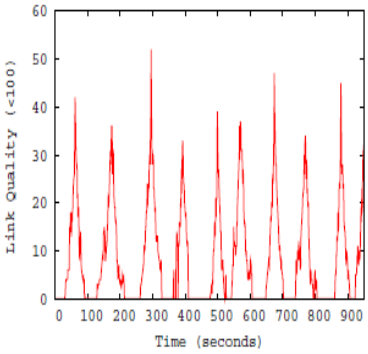


Figura 29 (b). Muestra la calidad de las líneas entre nodos en una infraestructura con Access point.

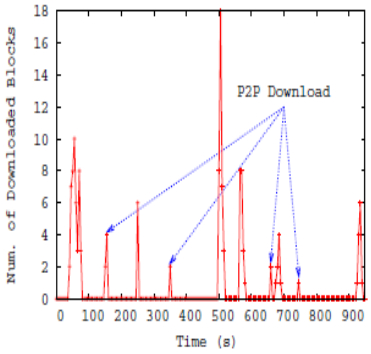


Figura 29 (c). Muestra la distribución de las piezas descargadas sobre el tiempo.

Las figuras 29(a), 29(b) y 29(c) muestran la relación entre la calidad del enlace y el número de piezas descargadas en uno de los 2 automóviles. Las descargas P2P están indicadas en la figura 29(c) por 4 flechas que denotan 4 diferentes periodos de tiempo. Debido que el espacio es constante, solo se presentan resultados de un solo automóvil, los resultados sobre otros autos son muy similares. En períodos de 40s-70s y de 520s-600s, no hubo piezas descargadas por parte del nodo hacia el punto de acceso. Esto refleja el modo de diseñar la estrategia de selección de piezas. En un periodo de 790s-810s y de 890s-910s, la calidad del enlace entre los nodos fue buena, pero no hubo alguna actividad de descarga, se asumió que el nodo no tuvo piezas que el otro nodo quiso. Desde que los 2 nodos tuvieron la exacta cantidad de piezas, el intercambio de piezas no tuvo lugar.

En el periodo de 920s-950s las piezas fueron todas descargadas del punto de acceso. El efecto de la configuración de tiempo TCP se vio en el periodo 480s-520s, a pesar de la excelente conexión entre el punto de acceso y el nodo, la descarga empezó hasta los 510s, el comienzo retardado indico la asociación entre el punto de acceso y la configuración del tiempo TCP. Hubo 2 periodos misteriosos entre los 300s y los 400s, durante estos 2 periodos la calidad del enlace entre el punto de acceso y el nodo fue alta, pero sin embargo no hubo alguna actividad de descarga, se comparó los mismos periodos con las otras piezas descargadas de los nodos y la razón fue el “efecto captura” de otro nodo pidiendo por piezas causo un numero de procesos que causo una saturación en el punto de acceso. Luego cuando el punto de acceso estuvo listo para recibir esas peticiones, el nodo ya se encontraba fuera de su rango. Para ello se planea

modificar la estrategia de selección de piezas para que los nodos descarguen unos a otros en el rango del punto de acceso. También se desea incrementar el número de procesos que un punto de acceso pueda recibir para que no quede saturado. **[17]**

5. CONCLUSIÓNES

En muy pocos años, el campo de las redes AD HOC ha tenido una rápida expansión visible en la proliferación de dispositivos inalámbricos de bajo costo como ordenadores portátiles, asistentes personales digitales, (PDAs), teléfonos móviles, entre otros.

Las redes AD HOC son adaptativas y están habilitadas para configurarse a sí mismas, prescindiéndose de la intervención de un administrador del sistema. En la práctica, las redes ad hoc podrían disponer desde decenas hasta centenares de nodos de comunicaciones capaces de cubrir alcances radio de 30 a 100 metros en interiores y de 100 hasta 300 metros en exteriores.

Dentro de este gran conjunto podemos encontrar las redes MANETS que Como su propio nombre indica la característica principal de una MANET es la movilidad de los nodos, que pueden cambiar de posición rápidamente. La necesidad de crear redes de forma rápida en lugares sin infraestructura suele implicar que los nodos exploren el área y, en algunos casos, se deban unir para conseguir un objetivo.

Fue necesario explicar este tipo de redes para hacer mejor énfasis en nuestro trabajo de grado el cual hace referencia a las redes VANETS que como su propio nombre indica, se trata de una red ad-hoc donde sus nodos se corresponden a vehículos (carros, camiones, autobuses entre otros.). Realizamos un cuadro comparativo donde ilustramos ciertas diferencias que existen entre las redes VANETS y las redes MANETS que de nominamos Manets vs Vanets. Aquí encontramos y tocamos aspectos importantes sobre lo que son: la topología, consumo de energía, seguridad, particionamientos de red entre otros.

Las redes VANETS tienen unas características muy importantes que a su vez las hacen muy especiales como por ejemplo notamos que son redes autónomas donde Cada Terminal es un nodo autónomo con capacidad de procesado de la información y de encaminamiento de información proveniente de otros nodos de la misma red. El control de dicha red es distribuido, Debido a la ausencia de infraestructura para el control de la red. La topología de red es variable, En una VANET los nodos pueden moverse de forma arbitraria, aunque generalmente lo hagan siguiendo ciertos patrones de movimiento. Como por ejemplo siguiendo las trayectorias de una carretera. Aquí empezamos a tocar el tema de la infraestructura de las redes VANETS que están conformadas por Unidades de Carretera (RSU), Beacon UMTS. Universal Mobile Telecommunications System, WIMAX, Terrestrial Broadcast, GSM, WIFI, RFID, GPS entre otros.

Las redes VANETS tienen sus principales áreas de aplicación, tales como la seguridad activa, servicios públicos, mejoras en la conducción, negocios y entretenimiento móvil. En cuanto a Los servicios de las redes VANETS, estos están dirigidos a varios agentes como son el conductor, los ocupantes del vehículo, la administración de la red, las empresas. Los servicios de las redes VANETS se dividen en 4 segmentos: los servicios para la seguridad vial, los servicios para la administración de las redes, los servicios para el entretenimiento y los servicios de utilidad.

En nuestro trabajo también planteamos las ventajas Los Beneficios de las redes VANETS pueden ser de varios tipos: Salud, Mejora el flujo de Tráfico, Mejora las decisiones de viajar por parte del conductor, Mejora el movimiento de las mercancías, Incrementa la calidad de vida, entre otros. Una de las principales debilidades en las redes VANETS es la seguridad, más que todo hacemos referencia a La privacidad. En redes ad-hoc es una meta complicada de conseguir. En este tipo de redes los usuarios finales requieren servicios y envían información personal (e.g. identificadores, preferencias, entre otros.) a través de nodos que actúan normalmente como enrutadores y ocasionalmente como proveedores de servicios. Además de los problemas de seguridad debemos sumarle los problemas relacionados con los costos. Ya que es una cifra muy elevada al momento de querer implementarla.

Las tecnologías de software se dividen en simuladores de tráfico y simuladores de redes, en la monografía se describió algunos de los simuladores de trafico de entornos VANET más utilizados y aceptados tales como: GrooveSim, Carisma y SUMO. El simulador de redes será el encargado de emular un entorno inalámbrico en nuestro modelo de movilidad, todas las personas que se han aventurado a la simulación de VANETS coinciden que el simulador cumple que cumple con todas exigencias es el NS2. En esta investigación se describió las tecnologías de hardware que son dispositivos que están en el automóvil, en la carretera y en las estaciones centrales, dichos dispositivos permiten la comunicación, el uso de servicios y aplicaciones que necesitan los usuarios de las redes VANETS, entre las tecnologías de hardware más importantes están: CAN, GPS.

En los últimos años las investigaciones acerca de los algoritmos de enrutamiento en las redes ad-hoc se ha incrementado, factores tales como la movilidad de los nodos, la inestabilidad de las topologías y la ausencia de una infraestructura hacen obsoletos a los protocolos que se usan en redes fijas. En las redes VANET los algoritmos deben utilizarse de manera automática y distribuida. En la investigación se describió las clases de algoritmos de enrutamiento: los algoritmos basados en el alcance, los algoritmos basados en el descubrimiento de rutas y basados en el tipo de algoritmo que implementan.

Asegurar la comunicación VANET es un tema serio y crucial ya que de no hacerlo retrasaría el despliegue de esta tecnología en el camino. Todos los conductores quieren asegurarse de que su identidad sea preservada en el intercambio de mensajes con otros conductores o entidades. Por otro lado los gobiernos quieren garantizar que el despliegue de una red VANET no cause más accidentes debido a las fallas de seguridad. En esta investigación se describieron los mecanismos para la integridad de la información que son el PKI, el protocolo de seguridad DRP y el protocolo de seguridad MAC. En esta investigación se describió los mecanismos para el control de acceso: sistemas de detección de intrusos y seguridad en el encaminamiento. También se describió técnicas de cifrado y gestión de claves: gestión de claves en cadenas de certificados, basada en la movilidad, gestión paralela distribuida y autoridades de certificación. En la investigación se describieron 2 casos de implementación de redes VANETS en la vida real, el primer caso fue el del grupo CVIS que consistían en 2 VANES equipadas con sensores y múltiples aplicaciones que fueron mostradas al público en Estocolmo (Suecia). El 2 caso fue de CARTORRENT en donde las piezas de archivos son compartidas por los automóviles y las unidades de carretera, este tuvo 2 escenarios: el del parqueadero y el escenario de la carretera.

6. RECOMENDACIONES

- Hacer un seguimiento a los consorcios a nivel mundial como CVIS, SAFESTPOT, donde se desarrollan las principales tecnologías de hardware y software sobre las redes VANETS

- Hacer un seguimiento a las actividades regulatorias y normativas en el entorno vehicular. Para asegurar el correcto funcionamiento de una red VANET se deben conocer de mano las implicaciones normativas a nivel mundial

- Los dispositivos tecnológicos que necesita una red VANET no son baratos debido a la alta tecnología que estos necesitan, se deben buscar dispositivos al alcance de los países subdesarrollados

- Se debe tener en cuenta que el desarrollo de una red VANET puede tardar años debido a los altos costos de los dispositivos y los problemas de seguridad en las redes inalámbricas ya que ningún gobierno quiero implementar un sistema que cause más víctimas de las que actual mente causa el sistema vehicular actual.

- Los simuladores son una gran herramienta para las universidades ya que permite definir entornos de movilidad real gracias a la utilización de mapas digitales, algunos son de software libre y otros son de pago pero su costo es muy inferior al costo de realizar una prueba real.

BIBLIOGRAFÍA

[1] Cristian Crespo Cintas. Integración de Protocolos de Acceso Avanzados en Redes WLAN IEEE 802.11. Ingeniería Técnica de Telecomunicación, especialidad Sistemas de Telecomunicación http://upcommons.upc.edu/pfc/bitstream/2099.1/5112/1/memoria.pdf [online] [*Citado el 2 de Octubre del 2010*]

[2] José Ignacio Ruiz Núñez, Alicia Triviño, Luis Javier García. Configuración DHCP en redes MANET subordinadas. Universidad Compútense de Madrid. Madrid. 2008.
http://eprints.ucm.es/10066/1/José_Ignacio_Ruiz_Núñez.pdf [online]
[*Citado el 26 de Agosto del 2010*]

[3] Helene Domenec, y José María Peña, Estudio comparativo de protocolos de encaminamiento en redes VANETS. Universidad politécnica de Madrid facultad de informática, Junio 2008
oa.upm.es/1444/1/PFC_HELENE_DOUMENEC.pdf [online]
[*Citado el 4 de Marzo del 2010*]

[4] Frank Kargl. Vehicular Communications and VANETS. ULM University. Alemania
http://events.ccc.de/congress/2006/Fahrplan/attachments/1216-vanet.pdf
[*online] [Citado el 21 de Julio 2010*]

[5] Iván Lequerica Roca, Ismael Cortázar Múgica. Rendimiento de VANETS en escenarios de uso realistas. Telefónica Investigación y desarrollo. España.
http://www.tid.es/netvehicles/media/papers07/VANETs.pdf [online]
[*Citado el 26 de Julio 2010*]

[6] R. Soto C. Centro de integración para la industria automotriz y aeronáutica de sonora, A. C. CIIAAS.
http://ciiaas.org/pdf/meses/20%20abr%2009/CIIAAS.20.04.2009.pdf [online]
[*Citado el 2 de Agosto 2010*]

[7] Raúl Santos Leiva. Simulación de VANETS. Universidad politécnica de Cataluña, Noviembre 2007.
https://upcommons.upc.edu/pfc/bitstream/2099.1/4485/1/santos.pdf [online]
[*Citado el 4 de Junio 2010*]

[8] Mitretek Systems. Intelligent Transportation Systems Benefits, Costs and Lessons Learned
http://ntl.bts.gov/lib/jpodocs/repts_te/14073_files/14073.pdf [online]
[*Citado el 29 de Abril 2010*]

[9] Paul Komptner. The new Cooperative Era. Cooperative Vehicle Infraestructure Systems. 2010
http://www.cvisproject.org/download/ERT_CVIS_FinalProject_Bro_06_WEB.pdf [online] [*Citado el 9 de Junio 2010*]

[10] http://diricom.lcc.uma.es/diricom/diricom-es/VANETs-es.html , Diseño Inteligente de Redes Vehiculares (VANETS) [online]
[*Citado el 4 de Septiembre 2010*]

[11] Cristopher Brown, Robert Bosch GmbH, Vehicle as Sensors for Cooperative Systems. BOSCH. Alemania
http://www.cvisproject.org/download/Presentations/Aalborg07/SS07/SS07_Bosch-Zott.pdf [online] [Citado el 1 de Agosto 2010]

[12] Antonios Stampoulis y Zheng Chai. A Survey of Security in Vehicular Networks
zoo.cs.yale.edu/~ams257/projects/wireless-survey.pdf [online]
[*Citado el 29 de Mayo 2010*]

[13] Souhail Guennouni. A study of Security Requirements for Vehicular Ad hoc Networks (VANET) Communication.
http://www.cs.odu.edu/~gpd/msprojects/sguennou.0/Final_Report.pdf
[online] [*Citado el 10 de Mayo 2010*]

[14] Marcin Poturalski. Verification of a VANET protocol IC-29 miniproject
secowinetcourse.epfl.ch/previous/0506/ReportPoturalski.pdf [online]
[*Citado el 12 de Mayo 2010*]

[15] Yi Qian, Kejie Lu y Nader Moayeri. A SECURE VANET MAC PROTOCOL FOR DSRC APPLICATIONS. National Institute of Standards and Technology y Department of Electrical and Computer Engineering University of Puerto Rico
w3.antd.nist.gov/pubs/Yi-Paper1.pdf [online]
[*Citado el 18 de Mayo 2010*]

[16] Cooperative Vehicle Infraestructure System (CVIS). Public Road Tour. http://www.cvisproject.org/download/WorldCongressPage/chapter_2.pdf [online] [*Citado el 24 de Mayo 2010*]

[17] Kevin C. Lee, Seung-Hoon Lee, Ryan Cheung, Uichin Lee, Mario Gerla. First Experience with CarTorrent in a Real Vehicular Ad Hoc Network Testbed. University of California, Los Angeles. http://www.cs.ucla.edu/~shlee/papers/cartorrent.pdf [online] [*Citado el 30 de Mayo 2010*]

GLOSARIO

Ancho de banda: *e*s la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bits por segundo (BPS), kilobits por segundo (KBPS), o megabits por segundo (MBPS).

Anycast: es una forma de direccionamiento en la que la información es enrutada al mejor destino desde el punto de vista de la topología de la red.

Bluetooth: es una especificación industrial para Redes Inalámbricas de Área Personal que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2,4 GHz

Broadcast: es la transmisión de un paquete que será recibido por todos los dispositivos en una red.

Criptografía: es un conjunto de procedimientos para cifrar los mensajes, de forma que si son interceptados no se pueda saber ni modificar su contenido.

Diffie Hellman: es un protocolo criptográfico que permite a 2 partes que no han tenido contacto alguno para establecerse conjuntamente con una clave secreta compartida a través de un canal de comunicación inseguro.

Dispositivos E/S: es la colección de interfaces que usan las distintas unidades funcionales de un sistema de procesamiento de información para comunicarse unas con otras, o las señales enviadas a través de esas interfaces.

Geocast*:* refiere a la entrega de la información a un grupo de destinaciones en la red identificado por sus localizaciones geográficas. Es una forma especializada de multicast utilizado por alguno protocolos de la encaminamiento para redes ad hoc móviles

IEEE 802.11: define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana.

INVANET: usan el protocolo IEEE 802.11 WIFI y WIMAX IEEE 802.16 para la comunicación fácil y eficaz entre los vehículos de movilidad dinámica. Medidas eficaces, como los medios de comunicación entre los vehículos se puede activar y los métodos para el seguimiento de vehículos automotores.

IPV4: es la versión 4 del Protocolo IP (Internet Protocol) versión anterior de IPv6. Ésta fue la primera versión del protocolo que se implementó extensamente, y forma la base de Internet.

MANET: es una colección de nodos móviles autónomos que se comunican entre sí mediante enlaces wireless, dónde no existe una infraestructura de red fija y la administración se realiza de forma descentralizada.

Multicast*:* es Modo de difusión de información en vivo que permite que ésta pueda ser recibida por múltiples nodos de la red y por lo tanto por múltiples usuarios.

Multihop: es cuando las redes inalámbricas utilizan dos o más saltos inalámbricos para transmitir información desde un origen a un destino.

Peer-to-peer (P2P): es una red de computadoras en la que todos o algunos aspectos de ésta funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

Red ad-hoc: es aquella (especialmente inalámbrica) en la que no hay un nodo central, sino que todos los ordenadores están en igualdad de condiciones.

Retardo*:* es el tiempo de procesamiento de cada elementos de red llámese switches, routers, firewalls, servidores y clientes.

Voip: *es* un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes, en lugar de enviarla en forma digital o analógica, a través de circuitos utilizables sólo para telefonía como una compañía telefónica convencional

WIMAX: *e*s una tecnología dentro de las conocidas como tecnologías de última milla, también conocidas como bucle local que permite la recepción de datos por microondas y retransmisión por ondas de radio.

Youtube: es un sitio electrónico en el cual los usuarios pueden subir y compartir vídeos.

Zigbee: es el nombre de la especificación de un conjunto de protocolos de alto nivel de comunicación inalámbrica para su utilización con radios digitales de bajo consumo, basada en el estándar IEEE 802.15.4 de redes inalámbricas de área personal