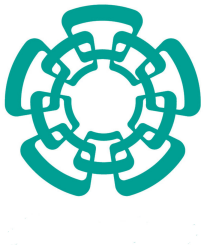

Centro de Investigación y de Estudios Avanzados
del Instituto Politécnico Nacional

Unidad Cinvestav Tamaulipas

Plataforma móvil para evaluación de esquemas de diseminación de mensajes en VANETs mediante dispositivos móviles inteligentes

Tesis que presenta:

Carlos Alfredo Leyva Vázquez

Para obtener el grado de:

Maestro en Ciencias en Ingeniería y Tecnologías Computacionales

Dr. Hiram Galeana Zapién, Director
Dr. Javier Rubio Loyola, Co-Director

Cd. Victoria, Tamaulipas, México. Octubre, 2017

Esta investigación fue parcialmente financiada por el proyecto SALUD-2014-C01-233836 del Fondo Sectorial de Investigación en Salud y Seguridad Social (FOSISS).

La tesis presentada por Carlos Alfredo Leyva Vázquez fue aprobada por:

_____

Dr. Miguel Morales Sandoval

Dr. Edwyn Javier Aldana Bobadilla

Dr. Hiram Galeana Zapién, Director

Dr. Javier Rubio Loyola, Co-Director

Cd. Victoria, Tamaulipas, México., 20 de Octubre de 2017

A mis padres, por todo su apoyo en cada etapa de mi vida.

Agradecimientos

- Agradezco al CINVESTAV-Tamaulipas por la oportunidad de permitirme realizar mis estudios de posgrado.
- También agradezco a todo el personal docente de la institución que a lo largo del periodo de cátedras han sido de gran importancia en mi formación académica.
- Particularmente agradezco a los Drs. Hiram Galeana Zapién, Alejandro Galaviz Mosqueda, Javier Rubio Loyola y Miguel Morales Sandoval por el apoyo en lo personal y académico que me han brindado desde mi llegada a la institución.
- Agradezco a mis compañeros por el apoyo y experiencias vividas a lo largo de nuestra estancia en la institución.
- También agradezco al personal administrativo y manual del CINVESTAV-Tamaulipas por las facilidades que me brindaron durante mi estancia.
- Agradezco también a CONACyT por el apoyo económico proveido que me permitió concentrarme en mis estudios.

Índice General

Índice de Figuras

Índice de Tablas

Índice de Algoritmos

Resumen

Plataforma móvil para evaluación de esquemas de diseminación de mensajes en VANETs mediante dispositivos móviles inteligentes

por

Carlos Alfredo Leyva Vázquez
Unidad Cinvestav Tamaulipas
Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, 2017
Dr. Hiram Galeana Zapién, Director
Dr. Javier Rubio Loyola, Co-Director

Las redes vehiculares ad-hoc (VANETs) son una tecnología de comunicación que permite efectuar transmisiones entre vehículos para intercambiar información de contexto, la cual puede ser utilizada por aplicaciones de tránsito vehicular o de entretenimiento. Un requerimiento clave de las VANETs consiste en garantizar la diseminación eficiente y segura de mensajes desde un nodo origen hacia una zona de relevancia, lo cual se realiza mediante la implementación de protocolos de la capa de red. Para el diseño de protocolos de diseminación de mensajes, la comunidad científica se ha apoyado mayormente en software de simulación, el cual, de manera general modela las condiciones del canal de comunicación, rangos de cobertura, etc. Sin embargo, el modelado de las características del entorno limita el estudio y análisis de los protocolos de diseminación de mensajes en condiciones normales de operación con las características físicas del entorno. Por lo anterior, es necesario contar con una herramienta que permita validar protocolos de diseminación en escenarios reales. En vista de lo anterior, en este trabajo de tesis se presenta el diseño e implementación de una plataforma móvil para la validación de esquemas de diseminación de mensajes en VANETs. La plataforma consta de tres características principales para el despliegue y análisis de las funcionalidades requeridas por

un protocolo de diseminación broadcast basado en ubicación: a) adquisición y procesamiento de información de ubicación, lo cual se logra incorporando un receptor GPS conectado vía Bluetooth a los dispositivos móviles para mejorar la precisión de los protocolos; b) gestión de paquetes, lo cual se habilita mediante la incorporación de políticas de agregación, así como de un esquema de seguridad para garantizar la validez de los nodos en la VANET mediante firmas digitales; c) comunicación inalámbrica, con lo cual se habilita la creación, conexión, y transmisión de mensajes entre nodos de una red ad-hoc. Esta plataforma ha sido validada con ayuda de dispositivos móviles inteligentes con un protocolo de diseminación de mensajes basado en ubicación. A diferencia de otros trabajos donde se analiza el comportamiento de protocolos de diseminación de mensajes mediante simulación, en este trabajo de tesis se ha hecho en análisis del protocolo mediante experimentación realizada en escenarios reales, cuantificando su rendimiento en términos de pérdida de paquetes y retardo en las transmisiones. Mediante la experimentación se ha comprobado que es posible mejorar el desempeño de un protocolo de diseminación basado en ubicación mediante un receptor GPS externo de altas prestaciones, con lo cual se abre la posibilidad de analizar características prácticas de los protocolos de diseminación de mensajes basados en ubicación que serían solamente estimadas en un análisis bajo entornos de simulación. De igual manera, se abre la posibilidad de analizar y diseñar nuevos protocolos de diseminación de mensajes basados en ubicación previo a su implementación y despliegue.

Abstract

Mobile platform for evaluation of message dissemination schemes in VANETs using intelligent mobile devices

by

Carlos Alfredo Leyva Vázquez
CINVESTAV-Tamaulipas
Center for Research and Advanced Studies of the National Polytechnic Institute, 2017
Dr. Hiram Galeana Zapién, Advisor
Dr. Javier Rubio Loyola, Co-Advisor

Vehicular Ad-hoc Networks (VANETs) is a communication technology that enables transmissions between vehicles to exchange context information, which in turn can be used by vehicular traffic or entertainment applications. A key requirement of VANET technology is to guarantee efficient and safe dissemination of messages from a node source to a zone of relevance, which is achieved by implementing network layer protocols. The design of dissemination protocols has been traditionally addressed by means of simulation tools, which in general terms, model the communication channel conditions, coverage ranges, etc. However, modeling these features limits the study and analysis of the dissemination protocols in operating conditions, with the physical features of the real environment. Considering the above, this thesis presents the design and implementation of a mobile platform for the validation of message dissemination schemes in VANETs. The platform consists of three main features for the deployment and analysis of the functionalities required by a location-based message dissemination protocol: a) acquisition and processing of location information, which is assessed by incorporating a GPS receiver connected via Bluetooth to mobile devices in order to improve the accuracy of the protocols; b) packet management, which is enabled by incorporating aggregation

policies, as well as a security scheme to guarantee the validity of nodes in the VANET through digital signatures; c) wireless communication, which is used to enable the creation, connection, and transmission of messages between nodes of an ad-hoc network. Our platform has been validated with the use of intelligent mobile devices, considering a message dissemination protocol. Contrary to traditional tools aimed at analyzing dissemination protocols through simulation, in this thesis, dissemination protocols are analyzed in real scenarios, measuring their performance in terms of packet loss and transmission delay. In addition, we have analyzed the performance of dissemination protocols making use of an external GPS sensor. With experimental validations, we demonstrate that it is possible to increase the performance of location-based dissemination protocols by using more accurate GPS sensors. This makes our platform a potential candidate to analyze practical characteristics of dissemination protocols that actually would be very difficult to analyze with traditional simulation tools. All in all, our platform makes it possible to analyze and to design novel dissemination protocols based on location prior to their implementation and deployment.

Nomenclatura

ITS	Intelligent Transportation Systems
VANET	Vehicular Ad-Hoc Network
MANET	Mobile Ad-Hoc Network
OBU	Onboard Unit
RSU	Roadside Unit
V2V	Vehicle-To-Vehicle
V2I	Vehicle-To-Infrastructure
V2P	Vehicle-To-Pedestrian
GPS	Global Positioning System
DSRC	Dedicated Short Range Communication
WAVE	Wireless Access in Vehicular Environments
MAC	Medium Access Control
OFDM	Orthogonal Frequency-Division Multiple Access
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
PKC	Public Key Cryptography
TA	Trusted Authority
PKI	Public Key Infrastructure
CA	Certification Authority
IBE	Identity-Based Encryption
CLS	Certificateless Signature Scheme
API	Application Programming Interface
ZOR	Zone of Relevance
ZOF	Zone of Forwarding
POI	Point of Interest
P2P	Peer-To-Peer
IP	Internet Protocol
RTT	Round Trip Time

1 Introducción

En este capítulo se exponen los antecedentes, motivación y objetivos del presente trabajo de tesis. Asimismo, se detallan las etapas de la metodología empleada en la investigación y se describe la organización del documento.

1.1 Antecedentes y motivación

En la actualidad, el aumento en la demanda de transporte terrestre está ocasionando en ciudades altos niveles de congestión de tráfico, lo cual implica un mayor impacto ambiental. Asimismo, esta situación hace evidente la ineficiencia de la infraestructura de transporte actual en términos de tiempos de traslado y cantidad de accidentes, que se prevé continué empeorando debido al crecimiento poblacional y de la urbanización. Ante este panorama, en años recientes se ha propuesto el concepto de sistemas de transporte inteligente (ITS, por sus siglas en inglés) con el propósito de mejorar sustancialmente la operación y eficiencia de los sistemas de transporte terrestre actuales. Los ITS son un conjunto de tecnologías de información y de comunicación que posibilitan el

intercambio de información entre los vehículos de forma autónoma. Aunque dicha información se enfoca principalmente en el intercambio de mensajes de alerta sobre diversas condiciones viales (por ejemplo, accidentes, puntos de congestión, etc.), también se vislumbra el despliegue de otros servicios orientados a compartir contenido multimedia o *streaming* a los pasajeros o conductores de los vehículos (por ejemplo, información sobre el pronóstico del clima) [2]. Se espera que los ITS permitan hacer más eficientes [1], seguros [2] y sostenibles [3] los medios de transporte en dos escenarios principalmente: a) entornos urbanos, caracterizados por una alta densidad vehicular, y b) entornos rurales como autopistas o carreteras, donde el dinamismo de la red es un reto aún abierto en la literatura debido a la alta movilidad de los nodos, donde los protocolos existentes para MANETs no son del todo aplicacbles. En función del tipo de escenario a considerar, existen diferentes paradigmas de comunicación: a) vehículo a vehículo (V2V, por sus siglas en inglés), b) vehículo a infraestructura (V2I, por sus siglas en inglés), c) vehículo a peatón (V2P, por sus siglas en inglés). Adicionalmente se plantea el paradigma V2X, para la inclusión de nuevos enfoques.

Para el desarrollo de los ITS la comunidad científica y la industria automotriz han identificado a las redes vehiculares ad-hoc (VANET, por sus siglas en inglés) como la tecnología de comunicación inalámbrica que permitirá la diseminación eficiente de la información entre vehículos. Una VANET es un tipo particular de red ad-hoc móvil (MANET, por sus siglas en inglés), cuyos nodos (vehículos) disponen de una entidad de cómputo, comunicación y almacenamiento denominado unidad a bordo (OBU, por sus siglas en inglés), que actúa como receptor/transmisor para la diseminación de mensajes de alerta, así como sensores de proximidad, de ubicación, entre otros [3, 4, 5, 6]. Estas redes son capaces de soportar las aplicaciones pretendidas en los ITS, cuyo despliegue se prevé contribuya en la coordinación entre los vehículos para brindar información oportuna que favorezca la toma de decisiones ante percances en la vía de tránsito, así como mejorar la experiencia de los conductores y

[1] Optimización del flujo vehicular, rutas, paso de vehículos en intersecciones, asistencia con semáforos inteligentes, entre otros.

[2] Seguridad para los datos transmitidos. Servicios a garantizar: confidencialidad, integridad y disponibilidad

[3] Tecnología verde. Reducción de emisiones contaminantes mediante uso eficiente de combustible.

usuarios de vehículos en general [7].

La diseminación de mensajes en las VANETs representa un reto debido a las condiciones de movilidad y limitaciones en rango de cobertura, lo que demanda el diseño de algoritmos de contención para la reserva del canal y esquemas de diseminación que consideren la propagación de mensajes a nodos fuera del alcance del emisor original. En la comunidad científica se han propuesto protocolos de comunicación para mejorar el rendimiento de la red, con la implementación de técnicas para disminuir el número de nodos que transmiten en determinado momento y brindar soporte a diferentes servicios y aplicaciones [8]. En este sentido, el paradigma de comunicación V2V ha sido propuesto como uno de los enfoques clave para el despliegue de las VANETs. En este paradigma, los vehículos comparten información recolectada por sus sensores mediante comunicación inalámbrica operando en la banda de frecuencia de 5 GHz bajo un modo ad-hoc. Este modo de operación resulta idóneo debido a que no requiere de una infraestructura para realizar conexiones y transmisiones. Asimismo, este paradigma se puede emplear para establecer conectividad entre vehículos y dispositivos móviles de usuarios peatonales (V2P).

El diseño y validación de protocolos de diseminación en VANETs normalmente se realiza mediante simulación por computadora. Es decir, el desarrollo de software de simulación que permita evaluar protocolos de diseminación en diversas capas de una VANET, como es el caso de control de acceso al medio, encaminamiento, etc. Para ello, en los escenarios de simulación se implementan las características representativas de la propagación en el medio inalámbrico mediante modelos empíricos que caracterizan la atenuación de la señal entre nodos móviles. Asimismo, es común que en el diseño de un software de simulación se tomen en cuenta suposiciones que permitan simplificar la implementación de un escenario particular. Si bien la simulación por computadora permite el diseño de nuevos protocolos para VANETs, existe la necesidad de realizar la validación de los mismos en experimentación a fin de obtener métricas de rendimiento (retardo, pérdidas de paquetes, tasa de transmisión, etc) en condiciones de propagación del canal reales.

Sin embargo, la experimentación en escenarios reales representa un reto debido a la falta de una

estandarización en la fabricación de OBUs, lo que puede ocasionar que éstas queden obsoletas en poco tiempo, afectando la búsqueda de interoperabilidad entre diferentes prototipos. Por esto resulta poco factible su adquisición para efectos de investigación en algunos grupos de trabajo. Ante ello, se ha propuesto en la literatura el uso de dispositivos móviles inteligentes para las tareas de transmisión y recepción en distintos escenarios [9, 10, 11, 12]. Esto permitiría formar *test beds*[4] para validar esquemas de diseminación en entornos realistas que además puedan ser dotados de características adicionales como servicios de seguridad y mejores prestaciones en la obtención de la ubicación de los nodos mediante el sistema de posicionamiento global (GPS), pues las capacidades de conectividad, sensado y cómputo de los teléfonos móviles actuales lo permiten.

Los trabajos encontrados en la literatura que utilizan dispositivos móviles para la diseminación de mensajes se enfocan en comunicaciones simples, en su mayoría, de un solo salto (*single-hop*), sin considerar la inclusión de protocolos de diseminación ni la provisión de servicios de seguridad en las transmisiones. Esta última característica es importante debido a que los escenarios de VANET requieren que se garanticen los servicios de seguridad informática debido a las repercusiones que la propagación de mensajes de alerta falsos representa, pudiendo resultar en efectos contrarios a los deseados e incluso provocar accidentes. A fin de preservar la autenticación de los nodos, confidencialidad de los datos y otros servicios de seguridad, es necesario implementar mecanismos que den certeza a los usuarios de que la información que se propaga por la red sea confiable o al menos provenga de un vehículo válido. Estos requerimientos de seguridad han sido considerados por el estándar IEEE 1609.2, el cual recomienda la implementación de un esquema de firma digital y verificación bajo el uso de llaves respaldadas por certificados digitales. Sin embargo, han surgido alternativas ante ciertas características que presentan oportunidad de mejora.

La obtención de la ubicación de los nodos de la red es una tarea clave en los esquemas de diseminación basados en localización, los cuales requieren la mayor precisión posible en tales

[4]Plataforma para experimentación de módulos de un sistema mediante un framework para validar el funcionamiento del módulo.

lecturas. Esto, aunado a las condiciones de movilidad en las VANETs, demanda además una frecuencia alta en la actualización de las lecturas de ubicación de los nodos [13]. La realización de pruebas experimentales puede permitir analizar en condiciones reales el rendimiento de protocolos de diseminación que aporte una retroalimentación para el diseño y desarrollo de los mismos, considerando los valores observados en métricas para escenarios reales. Esto puede (eventualmente) contribuir a la aceleración del despliegue de VANETs en el ámbito de investigación e industria [14].

1.2 Planteamiento del problema

Si bien la factibilidad del uso de teléfonos móviles inteligentes ha sido probada para experimentaciones en el escenario descrito de las comunicaciones vehiculares, a la fecha no ha sido propuesta **una plataforma para teléfonos móviles inteligentes que integre de manera unificada funcionalidades requeridas en una VANET para la diseminación de mensajes**. Tal es el caso de una **frecuencia alta de muestreo de la información de ubicación** de los dispositivos (lo cual es uno de los aspectos ampliamente usados en los criterios de diseminación), así como la incorporación en un entorno real de **servicios de seguridad orientados a preservar la autenticación de los nodos** (en el caso de aplicaciones para envío de mensajes de alerta).

1.3 Objetivos

1.3.1 Objetivo general

Obtener una plataforma para la implementación y evaluación del rendimiento de protocolos de diseminación de mensajes en VANETs con soporte de servicios de integridad de mensajes y autenticación de nodos.

1.3.2 Objetivos específicos

1. Desarrollar una aplicación móvil que permita evaluar el desempeño de protocolos de diseminación de mensajes mediante métricas de retardo y pérdida de paquetes.

2. Incrementar la granularidad del sensado de ubicación en la plataforma móvil para la diseminación de mensajes en VANETs.

3. Cuantificar el impacto de mecanismos de seguridad para proveer servicios de autenticación de nodos e integridad de mensajes en la plataforma propuesta.

1.4 Metodología

A fin de alcanzar los objetivos planteados, se han definido las siguientes etapas que dividen las actividades de diseño, desarrollo y experimentación para la plataforma propuesta.

Etapa 1. Definición del esquema para la diseminación de mensajes y desarrollo inicial.

En esta etapa se han considerado los aspectos clave de los tres componentes a integrar en la plataforma (diseminación de mensajes, integración de sensor GPS externo y esquema de seguridad), identificando los requerimientos de entrada a los módulos, flujo de información en la plataforma y los resultados a mostrar en la interfaz con el usuario o a almacenar en archivos para su futuro análisis. Lo anterior con la finalidad de establecer los mecanismos a implementar y desarrollar en la plataforma.

- Análisis preliminar de diseminación de mensajes en VANETs.
    - Analizar los trabajos más relevantes con respecto a esquemas de diseminación de mensajes validados en entornos reales.
    - Definir los escenarios en que actúan los protocolos de diseminación de mensajes.
    - Definir métricas y criterios para la evaluación de la plataforma.

- Identificar los esquemas de seguridad aplicables a VANETs e implementación inicial.
    - Analizar los mecanismos de seguridad que ofrecen mejores prestaciones de infraestructura y carga en la red.
    - Definir escenarios de ataque factibles para prevenir mediante la integración de mecanismos de seguridad en la plataforma.
    - Seleccionar e implementar el esquema de seguridad.
- Desarrollar el módulo de gestión de ubicación.
    - Definir diagrama de clases para la implementación del módulo.
    - Integrar sensor GPS externo a la plataforma inicial.
    - Definir campos referentes a ubicación en el paquete a transmitir.

Etapa 2. Desarrollo e integración de los módulos de la plataforma.

El objetivo de esta etapa es la obtención de los módulos que conforman la plataforma de acuerdo a los requerimientos establecidos en la primera etapa, finalizando con la integración de todos los módulos para obtener la plataforma final.

- Desarrollar el módulo de comunicación.
- Analizar el estado del arte sobre protocolos de diseminación e identificar características comunes entre los protocolos basados en ubicación de los nodos.
- Integrar los módulos desarrollados en la plataforma.

Etapa 3. Validación de la plataforma mediante pruebas en escenarios reales. [5]

[5] Experimentación en escenarios reales: conjunto de pruebas de transmisión de mensajes en un ambiente del mundo real (no simulado), expuesto a los efectos del canal de comunicación inalámbrico.

En esta etapa se considera la realización de pruebas pertinentes a fin de evaluar el rendimiento de la plataforma con todos sus elementos contemplados, se establecen los escenarios sobre los que se realiza experimentación y se analizan los resultados obtenidos.

- Validar el flujo de trabajo en la plataforma mediante pruebas sintéticas locales.
- Evaluar el funcionamiento de la plataforma en diferentes escenarios controlados.
- Evaluar los mecanismos de seguridad implementados.
- Validar las bondades de la integración de un módulo GPS externo con respecto al sensor nativo.
- Analizar los resultados obtenidos identificando el impacto de la integración de las características adicionales al proceso de comunicación.

1.5 Estructura del documento

En el siguiente capítulo se presentan los conceptos clave del trabajo realizado. En el Capítulo 3 se analizan los trabajos relacionados con este proyecto de tesis. Por su parte, el Capítulo 4 concentra las características de la plataforma implementadas según la metodología empleada para cumplir con los objetivos presentados previamente. En el Capítulo 5 se describe la metodología de experimentación y los resultados obtenidos. Finalmente, en el Capítulo 6 se presentan las conclusiones del trabajo y las actividades que se prevé puedan complementar el trabajo presentado.

2

Marco Teórico

En este capítulo se presenta el marco teórico relacionado con la presente tesis, el cual se enfoca en los fundamentos y aspectos generales de las VANETs y los diferentes enfoques de seguridad recomendados para este tipo de redes. Finalmente, se introduce la idea del uso de dispositivos móviles para realizar experimentos de comunicaciones referente a VANETs.

2.1 Redes vehiculares ad-hoc (VANETs)

Una VANET es una red inalámbrica cuyos nodos son entidades presentes en las vialidades (vehículos, peatones e infraestructura de acceso a Internet) y cuentan con transceptores (dispositivos electrónicos que cuentan con la habilidad de transmisión y recepción conjuntamente) para el intercambio de mensajes con el objetivo de mejorar la seguridad y comodidad de los pasajeros y eficiencia vial. El tipo de información a compartir puede provenir de alertas retransmitidas por otros nodos o bien información de contexto del vehículo extraída de los sensores integrados [3, 4, 5, 6]. Se distinguen de otras redes ad-hoc (aquellas que no dependen de una infraestructura preexistente)

por su arquitectura de red híbrida (ad-hoc y celular), características del movimiento de sus nodos y escenarios de aplicación [15]. Los componentes de una VANET son ilustrados en la Figura 2.1, en ella se identifican además los paradigmas de comunicación que se presentan en virtud de los componentes involucrados.

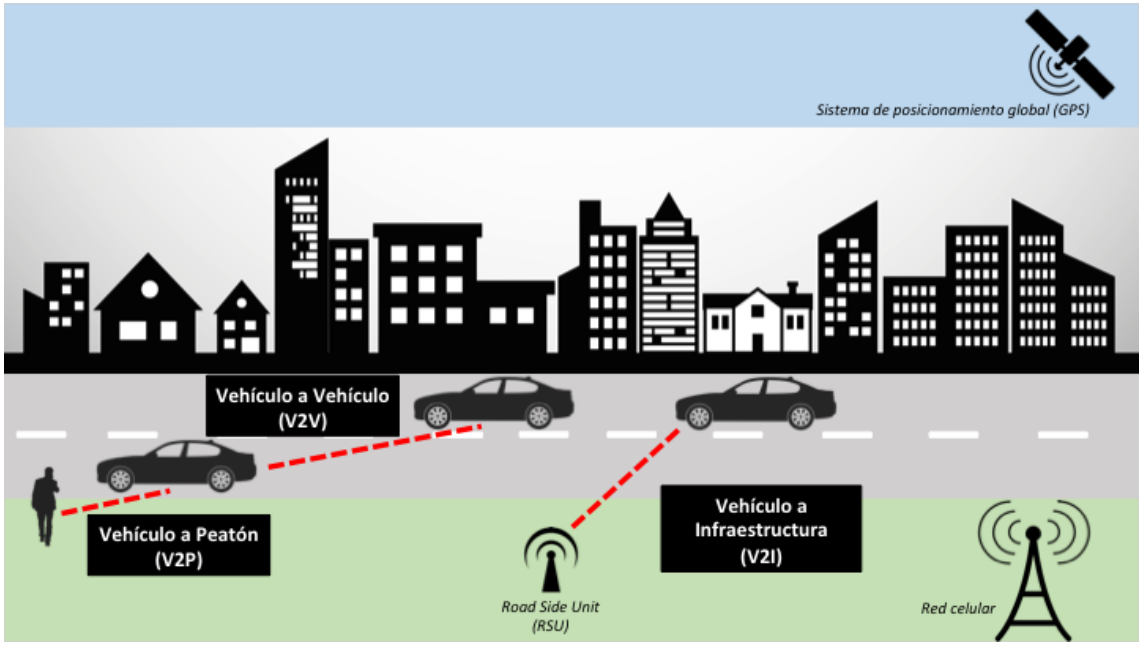

Figura 2.1: Entidades participantes y paradigmas de comunicación en una VANET [1].

2.1.1 Conceptos fundamentales

El intercambio de mensajes entre los nodos de una VANET se lleva a cabo bajo diferentes paradigmas, los cuales varían según las entidades participantes en dicho proceso de comunicación, como se describe en el siguiente listado. De acuerdo a lo descrito anteriormente, en las VANETs el intercambio de información entre los vehículos puede realizarse mediante tres diferentes tipos de paradigmas de comunicación.

- Comunicación vehículo a vehículo (V2V). En este paradigma de comunicación, la diseminación de mensajes se efectúa directamente entre los vehículos participantes en una VANET. Dicha

comunicación se efectúa a través de la interfaz inalámbrica que opera en la banda de frecuencia dedicada de comunicaciones de corto alcance (DSRC, por sus siglas en inglés).

- Comunicación vehículo a infraestructura (V2I). Este paradigma considera el uso de puntos de acceso colocados en las vialidades (RSU, por sus siglas en inglés) para la diseminación de mensajes entre vehículos. Específicamente, la comunicación se establece a través de los RSUs que actúan como *gateways* para la conectividad hacia Internet.

- Vehículo a Peatón (V2P). En este paradigma se asume que los vehículos puedan establecer comunicación hacia dispositivos móviles inteligentes que porten los usuarios peatonales en un entorno urbano. A diferencia del paradigma V2V, en este caso las condiciones de movilidad son reducidas y la transferencia de mensajes es esporádica orientado principalmente a la emisión de alertas en los dispositivos móviles de usuarios peatonales para informar de la proximidad de coches en los cruces de avenidas.

Los paradigmas V2V y V2P comparten el mismo reto, es decir la diseminación de mensajes de manera eficiente, en términos del número de nodos destino alcanzados, en un ambiente inalámbrico haciendo uso de tecnologías de corto alcance [16]. En este contexto, existen requerimientos generales en los diferentes niveles de la arquitectura de una VANET que es necesario considerar para el desarrollo de nuevos protocolos y algoritmos en dichos paradigmas de comunicación. Éstos se detallan a continuación en términos de la capa del modelo OSI en la que se presentan [17].

- Capa física. El diseño de protocolos en la capa física debe considerar factores como la variabilidad de la señal en tiempo y frecuencia en el canal inalámbrico, los cuales son aspectos inherentes al canal inalámbrico en las VANETs. De acuerdo al estándar IEEE 802.11p, en la capa física se hace uso del acceso múltiple por división de portadoras ortogonales (OFDM, por sus siglas en inglés) en el rango de la banda de frecuencia de 5 GHz.

- Capa de acceso al medio. La capa de control de acceso al medio (MAC, por sus siglas en inglés)

debe proveer un acceso al canal de manera confiable, justa y eficiente. Los protocolos MAC deben considerar los diferentes tipos de aplicaciones para las que se efectúan transmisiones. Por ejemplo, mensajes referentes a aplicaciones de seguridad vial deben ser enviados rápidamente y con tasas de error muy bajas. Con esto surge la necesidad de un reparto eficiente del medio, lo cual es uno de los retos principales en VANETs debido a la alta movilidad de sus nodos y las fluctuaciones de las condiciones del canal de comunicación y la topología de de red. Los protocolos MAC para VANETs deben lidiar con el problema de la terminal oculta [18] que se presenta en escenarios donde los vehículos forman grandes filas causando un decremento en la transferencia de información.

- Capa de red. Esta capa define principalmente protocolos de enrutamiento para establecer caminos confiables entre emisor y receptor. Las redes vehiculares soportan diferentes enfoques de comunicación, los cuales pueden ser categorizados en tres grupos: comunicación *unicast*, comunicación *multicast/geocast* y comunicación *broadcast*. En el primero, el objetivo principal es efectuar la comunicación de un nodo origen hasta un nodo objetivo en la red vía comunicación inalámbrica multi-salto. En el segundo grupo, el objetivo es efectuar comunicaciones de un nodo origen a un grupo de nodos destino. La familia de protocolos *Geocast* es una forma particular de *multicasting*, donde las comunicaciones son destinadas a un grupo de nodos que se encuentran dentro de una zona geográfica. En el tercer grupo, la principal característica es transmitir los mensajes desde un nodo emisor hacia el resto de los nodos en la red a la vez. Los nodos que reciben un mensaje, lo retransmiten a su vez, para que éste llegue a otros que se encuentren fuera del rango de cobertura del emisor original.

- Capas de transporte. En VANETs, muchas aplicaciones *unicast* requieren un servicio similar al dado por TCP, es decir, confiable y ordenado. Sin embargo, TCP presenta un rendimiento deficiente en las VANETs [19], por lo que se han desarrollado soluciones como el protocolo de transporte vehicular [20] y el protocolo de transporte de control móvil [21] (VTP y MCTP,

respectivamente, por sus siglas en inglés), destinados a aplicaciones que requieren enrutamiento *unicast*. Sin embargo, en aplicaciones previstas en ITS es necesario establecer una comunicación *multicast*, lo cual implica un reto debido a que en dichos protocolos los nodos no informan el estado de su conexión (disponible, conectado, entre otros).

- Capas de aplicación. En esta capa, los protocolos deben minimizar el retardo punto a punto, el cual es importante al transmitir mensajes de emergencia o seguridad vial cuyos requisitos de latencia se encuentran en el orden de milisegundos.

Como se ha indicado, no basta un enfoque *unicast* para las aplicaciones previstas para VANETs, debido a que el tipo de mensajes que transmiten pueden ser de interés para un grupo de vehículos dentro de una zona geográfica; o bien, para todos los que conforman la red. De acuerdo a estos criterios, se presentan transmisiones de salto único (*single-hop*) y multi-salto (*multi-hop*) para llevar un mensaje al nodo o zona destino. En este contexto, el diseño de protocolos de diseminación de multi-salto es un área de investigación activa durante más de una década. El protocolo de diseminación más simple es el que opera mediante la inundación de mensajes en la red. En este caso, cada nodo que recibe un mensaje por primera vez lo retransmite sin tomar en cuenta ninguna restricción. Sin embargo, debido a que las VANET emplean un mecanismo de control de acceso medio (MAC), la inundación de mensajes puede generar fácilmente el problema de tormenta de diseminación (BSP, por sus siglas en inglés) [22]. En dicho problema el rendimiento de la red se degrada debido al gran número (innecesario) de retransmisiones y colisiones redundantes. Este es el caso del estándar IEEE 802.11p34, que actualmente es la opción más destacada para permitir la comunicación en VANETs utilizando el acceso múltiple por detección de portadora y prevención de colisiones (CSMA/CA, por sus siglas en inglés) en la capa MAC.

2.1.2 Aplicaciones en las VANETs

Las aplicaciones en VANETs tienen como objetivo evitar el riesgo de accidentes vehiculares mediante la distribución de información notificando sobre incidentes y obstáculos (seguridad vial), optimizar el flujo de vehículos reduciendo el tiempo de traslado y evitando embotellamientos (manejo y eficiencia de tráfico), además de proveer información sobre el área al pasajero y ofrecer servicios de entretenimiento (comodidad e info-entretenimiento) [23]. A continuación se describen brevemente algunos de los tipos de aplicaciones encontrados en la literatura.

- **Info-entretenimiento**: Aplicaciones cuyo objetivo es mejorar la comodidad del pasajero de un vehículo. Esto incluye: localización de puntos de interés (POI), información del tráfico o clima actual y comunicaciones interactivas. Todo tipo de aplicaciones que puedan ejecutarse sobre el *stack* TCP/IP pueden entrar en este grupo, por ejemplo: juegos en línea y mensajería instantánea.

- **Seguridad vial**: Su principal objetivo es evitar accidentes en las vías de tránsito. Se dividen en tres clases: asistencia (navegación, prevención cooperativa de choques y cambio de carril), información (límite de velocidad permitida, notificación sobre zona escolar) y alertas (choques, obstáculos, condiciones del camino). Estas aplicaciones normalmente demandan comunicación directa (V2V) debido a su naturaleza sensible a retardos [24]. Ejemplos de estas aplicaciones son TrafficView [25] y StreetSmart [26], que informan a los conductores, a través de comunicaciones entre vehículos, sobre las condiciones de tráfico en las cercanías y más adelante en su dirección. Con [27] se busca la formación de flotas de vehículos para evitar cambiar de carril y ajustar la velocidad, permitiendo viajar de manera cercana y segura. El ahorro de combustible a través de la reducción de la aerodinámica de un vehículo cuando la distancia entre éste y otro sea corta, es lo que se busca en [28].

- **Servicios de pago:** Aplicaciones que permiten efectuar pago de cuotas en casetas de cobro a

lo largo de las autopistas. Permiten que estas operaciones se efectúen sin necesidad de detener el vehículo, evitando tiempo de espera en filas.

- **Servicios basados en ubicación:** Hacen uso del GPS para localizar hoteles, tiendas, restaurantes, gasolineras, etc.

2.1.3 Protocolos de diseminación de mensajes en VANETs

Un protocolo de diseminación en las VANETs es un conjunto de criterios que determinan la manera en que se efectúa el intercambio de mensajes entre los vehículos de la red. Estos protocolos implementan diferentes características para cumplir con los requerimientos de las aplicaciones, así como los requerimientos en las diferentes capas de la arquitectura de una VANET. La Tabla 2.1 presenta las características deseables de los protocolos con base en los requerimientos de las aplicaciones previamente descritas [29]. En ella se observan cinco de los requerimientos más comunes para los diferentes tipos de aplicaciones, el diseño de un protocolo de diseminación de mensajes considera dar solución a uno o más de estos requerimientos, por ejemplo, los protocolos orientados a las aplicaciones para a envío de mensajes de alerta consideran los requerimientos de baja latencia y alta confiabilidad.

Si bien los requerimientos para un protocolo de diseminación de mensajes pueden ser divididos en las cinco categorías de la Tabla anterior, existen protocolos que implementan características híbridas o pertenecientes a diferentes enfoques. Por ejemplo, se han desarrollado protocolos que implementan la división por segmentos de la vialidad o el escenario en que aplican, mientras que conservan mecanismos para lograr una baja latencia y también alcanzar una confiabilidad aceptable en las transmisiones. En la Sección 3.1.4 se detalla un poco más sobre estos protocolos, en particular para aquellos que utilizan un criterio de transmisión *broadcast*.

Requerimientos	Descripción	Características
Baja latencia	Bajo retardo punto a punto; compromiso de tiempo real	Enrutamiento o inundación basado en malla
		Baja contención o reservación de recursos del canal
		Priorización de paquetes
Alta confiabilidad	Entrega de información altamente probable	Retransmisión de paquetes
		Recursos del canal dedicados o de baja contención
Alto escalamiento	Capacidad para mantener requerimientos de servicio en diferentes densidades vehiculares	Eliminación, filtrado y priorización de paquetes adaptativa
		Técnicas de clustering
Alcance bien definido	Soporta envío de mensajes selectivo basado en trayectoria, región, proximidad o identificación	Dirección, zona, ubicación incluída en los paquetes transmitidos
Servicios de membresía	Provee servicios de membresía grupales para estructuras grupales persistentes	Algoritmo de registro centralizado o distribuido
		Detección de desafiliación de miembros

Tabla 2.1: Características de los protocolos deseables para las aplicaciones.

2.2 Mecanismos de seguridad

Jeremy Blum y Azim Eskandarian [30] presentan una importante pregunta: Una red inalámbrica de vehículos inteligentes puede hacer más seguro y rápido el viajar en carretera. Pero ¿pueden los *hackers* usar el sistema para provocar accidentes?. Con esta pregunta señalan la importancia que los fabricantes de vehículos y desarrolladores de soluciones en el ámbito de VANETs deben dar a la seguridad informática aplicada en este ámbito. La seguridad en VANETs es crucial porque afecta la vida de las personas. Por ello, información vital sobre vehículos y conductores no debe ser accesada, modificada o eliminada por un atacante. Además, se debe ser capaz de determinar la responsabilidad de los conductores, mientras se mantiene su privacidad. A continuación se definen los servicios de seguridad que deben ser garantizados en una VANET [31].

- **Confidencialidad**: Consiste en mantener un mensaje secreto para aquellos que no estén autorizados para conocerlo.

- **Autenticación**: Se refiere a verificar la identidad del usuario que actúa como emisor o receptor de un mensaje o que intenta acceder a un recurso del sistema. Este servicio se puede garantizar guardando información acerca de los usuarios y solicitándole a cada uno ingresar datos acordados como conocidos entre ambas partes (usuario y sistema). Sólo si los datos presentados por el usuario son correctos, se le permite realizar la acción deseada.

- **Control de acceso**: Ser capaz de identificar qué usuario ha realizado determinada acción hacia un recurso del sistema. Esto se logra indicando los permisos o privilegios que los usuarios de la red tienen asignados.

- **Integridad**: Asegurar que un mensaje no ha sido modificado durante su transmisión o almacenamiento. Se logra mediante la obtención de un resumen representativo del mensaje original, el cual puede ser generado nuevamente por el receptor para confirmar que el mensaje recibido arroja el mismo resumen que el original.

- **No repudio**: Asegurar que un usuario que ha participado en alguna actividad no pueda negar dicha participación. Se logra manteniendo un registro de actividades en el sistema. Además, en un esquema de firma/verificación, se confirma la participación del firmante.

- **Disponibilidad**: Garantizar que los recursos del sistema estén en tiempo y forma habilitados para ser usados por uno o varios usuarios. Esto debe incluir estrategias de administración de gestión de riegos y planes de contingencia (cuando el evento de riesgo ocurre).

2.2.1 Clasificación de ataques

Los principales ataques a la seguridad de una VANET se pueden clasificar de la siguiente manera:

Ataques que buscan comprometer el servicio de disponibilidad:

- ***Denegación de servicio***: Consiste en inhabilitar la red introduciendo intencionalmente tráfico innecesario.
- ***Interferencia***: Similar a Denegación de servicio, pero a nivel de capa física. Consiste en enviar una señal para interrumpir el canal de comunicación.

Ataques que buscan comprometer el servicio de autenticación:

- ***Usurpación***: Consiste en tomar la identidad de otro nodo de la red con fines maliciosos. Pudiendo realizar acciones negativas que comprometan al nodo usurpado.
- ***Ataque Sybil***: Se presenta cuando una entidad maliciosa utiliza múltiples identidades a la vez.

Ataques que buscan comprometer el servicio de integridad:

- ***Manipulación de mensajes***: Crear, modificar o eliminar información de manera no autorizada.
- ***Modificación de mensajes broadcast***: El atacante trata de fabricar e inyectar mensajes de alerta de seguridad falsos en la red.

Respecto a la veracidad de los mensajes transmitidos, existen tres métodos que buscan garantizar la confiabilidad de la información recibida:

- Método de umbral: La veracidad de un mensaje es establecida sabiendo que mensajes con el mismo contenido han sido enviados por distintas fuentes. Si el número de fuentes identificadas está por encima de un umbral establecido, el mensaje se considera confiable.
- Métodos basados en confianza y en reputación: Un mensaje se considera confiable si el nodo emisor tiene buena reputación ante el sistema.

En las siguientes subsecciones se describen los esquemas de seguridad más importantes, destacando sus bondades e inconvenientes y la solución que ofrecen los esquemas siguientes para solventar esas necesidades. Se presentan ambos enfoques típicos de criptografía (simétrica y asimétrica), así como el esquema recomendado por el estándar IEEE 1609.2 para seguridad en VANETs y las alternativas a ese enfoque.

2.2.2 Criptografía de llave privada (llaves simétricas)

Es una solución a los problemas de confidencialidad e integridad. Se basa en el manejo de una llave privada que ambas partes de una comunicación poseen para cifrar y descifrar los mensajes transmitidos entre ellos. Esta llave debe ser acordada y configurada por ambas partes previo a la comunicación.

El proceso de cifrado consiste en generar un mensaje que no sea interpretable por un usuario ajeno o no autorizado a la comunicación en trato. Dado el mensaje original y la llave privada, mediante una serie de operaciones básicas a nivel de bits se transforma un mensaje legible en uno ilegible. Este mensaje es entonces transmitido al destinatario, teniendo la seguridad de que ningún usuario que no disponga de la llave privada podrá conocer el mensaje en claro. Una vez recibido el mensaje cifrado, el receptor utiliza la llave privada para realizar el proceso inverso al cifrado (descifrado) con la finalidad de obtener de vuelta el mensaje original.

El inconveniente con este enfoque de seguridad recae en el manejo de las llaves privadas, ya que si un atacante logra obtenerla, podría tener acceso a toda la información manejada, comprometiendo todo el sistema.

2.2.3 Criptografía de llave pública (llaves asimétricas)

Ante el problema del manejo de llaves en criptografía de llave privada, surge esta alternativa que consiste en la utilización de dos llaves: una privada y una pública. Ambas llaves están relacionadas y

con ellas se pueden realizar operaciones complementarias. Previo a iniciar el proceso de comunicación seguro, un usuario (emisor) que desea transmitir un mensaje a otro (receptor), le solicita a éste su llave pública y el receptor se la envía. El proceso de cifrado se lleva a cabo en el emisor, utilizando la llave pública del receptor. Una vez generado el mensaje cifrado, se le transmite al receptor, quien utiliza su llave privada para descifrar el mensaje original.

Este enfoque facilita la distribución de llaves entre los usuarios del sistema, debido a que pueden libremente transmitir sus respectivas llaves públicas sin temor a que un atacante pueda interpretar un mensaje destinado a ellos, ya que el atacante necesita de la llave privada para el descifrado. El enfoque de seguridad de llave pública por sí solo, tiene la incertidumbre de, al solicitar la llave pública del receptor, saber si realmente se esté tratando del nodo deseado. Si un atacante intercepta el mensaje de solicitud de llave pública y hace que no llegue a su destino (el nodo receptor), podría actuar como si él lo fuera, enviándole su llave pública al solicitante, haciéndole creer que él es el nodo pretendido.

2.2.4 Esquema basado en infraestructura (PKI)

Para subsanar las deficiencias del enfoque anterior, se requiere de una infraestructura (PKI, por sus siglas en inglés) basada en la integración de una entidad reguladora denominada autoridad confiable (TA) que asegure a los usuarios que la llave pública que reciben sea realmente del nodo con que se desea iniciar el proceso de comunicación segura. Este enfoque basa su funcionamiento en el uso de certificados digitales que son expedidos por la TA, los cuales son un conjunto de información formado por la llave pública de la entidad a certificar, información de identificación de la entidad a identificar, firma digital de la TA que certifica, vigencia, entre otros datos. Los certificados digitales dan certeza y validez del propietario de una llave pública. De hecho, el emisor solicita esta llave pública directamente a la TA y no al receptor.

El inconveniente con este enfoque es el manejo de los certificados digitales, ya que su utilización involucra transmisiones adicionales entre los nodos y la TA en procesos de validación de certificados

y revocación de los mismos (tienen un periodo de vida; expiran). Todo el proceso que involucra el uso de certificados representa una carga adicional en la red y un mayor uso de recursos.

2.2.5 Esquemas basados en identidad

Las implicaciones del uso de certificados generan la necesidad de contar con mecanismos que garanticen la misma seguridad sobre la identidad del nodo al que se le solicita la llave pública. Por ello, surge el enfoque de cifrado basado en identidad (IBE, por sus siglas en inglés), el cual fundamenta su operación en la utilización del valor de identidad (ID) que cada nodo de la red posee. Un nodo emisor no requiere solicitar la llave pública del receptor, sino que él mismo la puede generar utilizando el ID del receptor. Una vez generada se debe enviar a la TA (llamada PKG en este enfoque) para que ésta genere la llave privada correspondiente.

Se utiliza la llave pública del receptor para cifrar el mensaje y éste se transmite al receptor. Para descifrar el mensaje se requiere de la llave privada correspondiente, por lo que el receptor la solicita a la PKG. Sin embargo, en este enfoque se presenta un nuevo problema, ya que la PKG se encarga de generar las llaves privadas de todos los nodos participantes y lo más importante: almacena dichas llaves privadas, ya que deben estar disponibles para cuando el receptor del mensaje cifrado la solicite. Esto representa un riesgo debido a que una gran responsabilidad recae en la PKG y la hace blanco de ataques.

Ante esta situación se propone el enfoque de cifrado sin certificados (CLE, por sus siglas en inglés), el cual le resta responsabilidad a la autoridad confiable (PKG, en enfoque IBE y KGC, en CLE, por sus siglas en inglés) debido a que ya no se encarga de generar y almacenar las llaves privadas de los nodos, sino solo parte de ellas (llaves privadas parciales).

2.3 Sistemas de sensado con teléfonos móviles

En la actualidad, los teléfonos inteligentes están integrados con un conjunto de sensores embebidos potentes y de bajo costo, como acelerómetros brújulas dijitales, giroscopios, GPS, micrófono y cámaras, además permiten el desarrollo de aplicaciones y programación de tareas en general. Los procesadores equipados en los móviles actuales cuentan generalmente con 8 núcleos, alcanzando una frecuencia de reloj de hasta 2.3 GHz. Por su parte, los transceptores integrados en estos dispositivos integran la tecnología Wi-Fi bajo los protocolos 802.11 a/b/g/n/ac y *Wi-Fi Direct*, brindando diferentes alternativas y compatibilidad para la implementación de soluciones de comunicación que satisfagan los requerimientos de este tipo de redes. Esto favorece el surgimiento de aplicaciones de sensado a escala personal, grupal y comunitaria. Estos dispositivos pueden revolucionar sectores económicos, incluyendo negocios, salud, redes sociales, monitoreo del ambiente y transporte [32]. El sector de transporte a nivel global tiene como principal preocupación la gestión de tráfico y seguridad vial. Sistemas de sensado con teléfonos móviles como el proyecto *MIT VTrack* [33] o el proyecto *Mobile Millennium* [34] están siendo usados para proveer información del tráfico a gran escala utilizando teléfonos móviles que facilitan servicios como la estimación precisa del tiempo de viaje para mejorar la planeación de traslados diarios.

Las posibilidades que los teléfonos móviles ofrecían para la programación de aplicaciones, particularmente para plataformas populares como teléfonos basados en Symbian, carecían de interfaces bien definidas y confiables para accesar a sensores de bajo nivel y no eran adecuadas para tareas de procesamiento como rutinas de procesamiento de señales, o realizar inferencias computacionalmente costosas debido a los recursos del dispositivo. Los primeros teléfonos dotados con sensores (previo a 2007) como el Nokia N80 incluían un acelerómetro, pero no había APIs para acceder a las señales del sensor. Esto ha cambiado significativamente, ya que la mayoría de los móviles en el mercado son programables por desarrolladores externos y ofrecen SDKs, APIs y herramientas de software.

Las tareas de sensado son abordadas en aplicaciones modernas, principalmente por aquellas que utilizan la ubicación del dispositivo para mejorar la experiencia del usuario, basadas en el contexto, es decir, características propias del dispositivo (recursos de energía) y del usuario (actividades, entorno, preferencias, ubicación, etc.). En este sentido, el sensado de la ubicación del dispositivo y su contexto enfocado al desarrollo de aplicaciones ha sido impulsado por parte de las plataformas de desarrollo para el sistema operativo Android, donde se pueden encontrar plantillas base orientadas a trabajar con mapas de la ciudad y facilitando la interacción con el usuario. Sin embargo, en una VANET, las comunicaciones pueden tomar lugar repetidamente en periodos muy cortos de tiempo (ráfaga) y dado que en muchas ocasiones (dependiendo el esquema de diseminación adoptado) se requiere incluir la ubicación del vehículo que emite el mensaje, se requiere de una frecuencia de adquisición de la ubicación que concuerde con estos cortos periodos de tiempo. Este requerimiento es la motivación para la integración de un módulo sensor de ubicación ajeno al dispositivo móvil, el cual sea capaz de solventar esta necesidad.

2.4 Resumen

En este capítulo se han descrito las entidades y paradigmas de comunicación que conforman una VANET. Las entidades son todas aquellas presentes en las vialidades, que participan en las transmisiones. Mientras que los vehículos y peatones representan los elementos fundamentales de una VANET, otras entidades como RSU, antenas de acceso a la red celular y satélites, representan elementos complementarios, que estarán presentes en redes más robustas. Las entidades que formen la red también definen los paradigmas de comunicación que se presentan en una VANET en particular. Además, existe una gran variedad de aplicaciones, las cuales, según su clasificación, buscan satisfacer aspectos de seguridad vial o info-entretenimiento. Por su parte, los esquemas de seguridad buscan garantizar los servicios más susceptibles ante una gran variedad de ataques. Ante esto, el estándar IEEE 1609.2 recomienda el uso de esquemas basados en certificados para el aseguramiento de llaves

públicas utilizadas para cifrado y firma de mensajes. Sin embargo, ante el costo del manejo de tales certificados, han surgido alternativas basadas en identidad para evitar el uso de certificados. Finalmente, las características de los dispositivos móviles inteligentes actuales, sugieren que a nivel de cómputo, capacidades de comunicación y de sensado, es posible diseñar soluciones que consideren todo lo mencioando en este capítulo utilizando estos dispositivos.

3

Estado del arte

En este capítulo se presenta el estado del arte relacionado con el problema de investigación definido en la tesis. En particular, se analizan protocolos de diseminación más importantes en términos de los principios fundamentales. Asimismo, se hace una revisión de trabajos que proponen prototipos de validación de dichos protocolos. Finalmente, brevemente se discuten los esquemas de seguridad recomendados por el estándar IEEE 1609.2 para VANETs.

3.1 Clasificación de protocolos de diseminación de mensajes en VANETs

Las VANETs permiten que cada nodo comparta información de su contexto (ubicación, velocidad, etc.) a otros vehículos lejanos situados en zonas de relevancia (ZOR, por sus siglas en inglés) mediante la retransmisión de los mensajes en nodos intermedios entre el origen y el destino. Específicamente, debido a que la ZOR se limita comúnmente a cientos de metros (en función del rango de transmisión

de los nodos), es necesario el uso de los protocolos de diseminación para realizar la retransmisión de los mensajes a través de múltiples saltos. Estos protocolos operan en la capa de red y, dependiendo del nodo responsable de tomar la decisión de la retransmisión, éstos se agrupan generalmente en orientados al receptor y orientados al transmisor. En cualquier caso, el objetivo de los protocolos de diseminación es garantizar la diseminación eficiente de los mensajes entre nodos de la VANET, es decir, sin incurrir en retransmisiones redundantes innecesarias que sobrecarguen la VANET. Debido a los retos relacionados con el acceso al canal inalámbrico y la escasez de recursos de éste, existen problemas abiertos en la literatura para la diseminación eficiente de mensajes en VANETs de forma que se garanticen los niveles de calidad de servicio (retardo, pérdida de paquetes) requeridos por las aplicaciones.

Los protocolos de diseminación basados en ubicación son una familia de protocolos que tienen la característica común de hacer uso de la información geográfica de los nodos en la VANET para realizar la toma de decisión de diseminación o retransmisión. Además, el interés de los mensajes en VANETs, particularmente para el caso de aplicaciones de seguridad vial, es generalmente por regiones o zonas (ZOR), por lo que la diseminación de mensajes en estos casos se lleva a cabo mediante transmisiones *broadcast*. Respecto a esto, en trabajos encontrados en la literatura, este enfoque de comunicación es complementado mediante la utilización de la localización de los nodos para la reducción de transmisiones múltiples, seleccionando los nodos idóneos (con base en su distancia al emisor) para realizar esta tarea. Por ello, la plataforma desarrollada en este trabajo de tesis tiene como objetivo dar soporte y validar protocolos de diseminación *broadcast* que hacen uso de la ubicación de los nodos de la red. A continuación se describen los protocolos de diseminación que hacen uso del GPS para la toma de decisiones en transmisión y retransmisión de mensajes.

3.1.1 Protocolos basados en ubicación

En este tipo de protocolos las comunicaciones se llevan a cabo utilizando la localización geográfica de los nodos además de su dirección de red. La ubicación de los nodos que toman parte en la

comunicación entre los nodos vecinos es publicada mediante *beacons* transmitidos en intervalos regulares de tiempo [14]. Estos protocolos requieren asistencia del sistema GPS para las decisiones de enrutamiento, las cuales se basan únicamente en la ubicación del nodo destino incluida en la cabecera del paquete transmitido y la ubicación del nodo vecino al emisor, es decir, utilizan la ubicación para determinar el siguientes nodos retransmisores cuando la distancia al destino excede el rango de cobertura del emisor. Este tipo de protocolos es útil pues no se requiere que la ruta global entre emisor y receptor sea calculada ni mantenida [35]. Ejemplos de este tipo de protocolos son: *Algoritmo de efecto de enrutamiento por distancia para movilidad (DREAM, por sus siglas en inglés)* y *Enrutamiento avaro sin estado de perímetro (GPSR, por sus siglas en inglés)*. Entre las principales bondades de estos protocolos está el hecho de que proveen buen rendimiento en escenarios de autopista donde los vehículos se mueven rápidamente y los caminos tienen pocas obstrucciones y que tienen el menor overhead de procesamiento. Mientras que los inconvenientes que presentan están relacionados al requerimiento del GPS para su funcionamiento, ya que en ciertos sitios éste presenta mala o nula recepción de la señal satelital.

3.1.2 Protocolos basados en agrupamiento

El elemento principal de este tipo de protocolos es la formación de grupos (*clusters*) con vehículos que comparten características similares como velocidad, dirección, ubicación, entre otras. Las comunicaciones dentro de un mismo *cluster* (intra-*cluster*) se realizan a través de conexiones directas, mientras que las comunicaciones entre nodos de diferentes *clusters* (inter-*cluster*) requieren que un nodo dentro del *cluster* (denominado *cluster head*) se encargue de dicho proceso. Ejemplos de esta técnica de enrutamiento son: *Agrupamiento para red de comunicación inter vehicular abierta (COIN, por sus siglas en inglés)* y *Algoritmo de enrutamiento basado en ubicación con inundación basada en cluster (LORA_CBF, por sus siglas en inglés)*. Este tipo de protocolos tienen alta escalabilidad para redes grandes debido a la generación de una red virtual para diseminar mensajes a otros *clusters* por parte de los *cluster heads*. Sin embargo, los problemas que se presentan son en

los retardos y *overhead* en la red incrementados debido a esa misma operación de los *cúster heads*.

3.1.3 Protocolos basados en zonas

Bajo esta técnica se pretende que las transmisiones de un nodo emisor sean destinadas a todos los nodos dentro de una región geográfica especificada (ZOR). Los vehículos fuera de la ZOR no son alertados con esas transmisiones, de esta manera se reduce el overhead de la red. Algunos de los protocolos geocast son: geocast inter-vehicular (IVG, por sus siglas en inglés) [36], que es orientado al envío de mensajes de alerta basándose en un algoritmo de tiempo de diferimiento y designación de retardo dinámico completamente distribuido. Además utilizan el GPS para diseminar a áreas de interés. Otro trabajo es el protocolo geocast robusto distribuido (DRG, por sus siglas en inglés) [37], el cual define los términos de ZOR y zona de retransmisión (ZOF, por sus siglas en inglés). Así como el protocolo de enrutamiento geocast basado en dirección para diseminación de consultas en VANET (DG-CastoR, por sus siglas en inglés), el cual se basa en la estimación de disponibilidad de enlaces. Busca estimar los nodos vecinos que tendrán la misma trayectoria en la vía de tránsito.

3.1.4 Protocolos *broadcast*

Esta familia de protocolos se basan en la inundación de la red con los paquetes transmitidos. Generalmente este enfoque se utiliza para paquetes con mensajes de alerta (seguridad vial) ya que interesa que dichos mensajes lleguen a múltiples destinatarios, no exclusivamente a uno. Se han desarrollado variedad de protocolos, como *Protocolo broadcast vehicular distribuido (DV-CAST, por sus siglas en inglés)*, *Protocolo de transmisión broadcast consciente de la ubicación (POCA, por sus siglas en inglés)* y *Protocolo broadcast consciente de la densidad (DECA, por sus siglas en inglés)*. Las bondades de esta familia de protocolos son: la simplicidad de implementación, debido a que no se preocupa por encontrar rutas para transmitir los mensajes, sino que se transmite a todos. Además se garantiza que el mensaje transmitido eventualmente llegará al resto de los nodos en la red. Sin

embargo, con el uso de transmisiones broadcast decae el desempeño conforme el número de nodos incrementa, ya que se genera congestión en la red cuando todos los nodos transmiten.

Si bien este enfoque es uno de los idóneos para utilizar cuando se trata de transmitir mensajes de interés común en la red, es importante dar solución a la problemática de las múltiples transmisiones (repetidas) y sus repercusiones en la red. Por ello han surgido variedad de trabajos ofreciendo solución, incluso para diferentes escenarios, donde las variantes son la densidad vehicular y la velocidad a la que viajan los vehículos. De manera general, los escenarios donde la densidad vehicular es alta, favorecen la propagación de los mensajes a todos los nodos de la red, ofreciendo mayores potenciales nodos retransmisores. Sin embargo, es el escenario donde puede presentarse mayor cantidad de transmisiones innecesarias (repetidas) y donde más se observa una congestión de tráfico en la red.

La problemática en el escenario de baja densidad vehicular ha sido abordada por proyectos como [7], donde se diseña un protocolo para el envío de mensajes de alerta. Este aporte se basa en la solución a los tres principales condicionantes del rendimiento en las comunicaciones vía broadcast: tormenta de broadcast, interferencia y el problema de la terminal oculta. Ante el problema de la tormenta de broadcast, proponen un segmentado (con cálculos de distancia asistidos por la ubicación de los nodos y puntos de referencia) de la vía de tránsito, donde cada segmento de tamaño N tiene un nodo (auto) designado como responsable de transmitir los mensajes a todos los nodos su segmento, de esta manera se va propagando el mensaje sin la necesidad de sobrecargar el canal. Un nodo responsable de un segmento, designa el representante del siguiente segmento identificando aquel que se encuentre a la máxima distancia con respecto a él.

Como solución al problema de la interferencia y de los nodos ocultos, se propone un mecanismo de asignar bloques separados de tiempo multi-salto a los mensajes de alerta. Esto se logra emulando el mecanismo RTS-CTS, por medio de mensajes que le aseguran a un nodo el disponer del canal por un bloque de tiempo. Además implementan un mecanismo de confirmación de recepción (ACK) que se envía al final de cada bloque de tiempo.

Para la realización de pruebas utilizan un entorno simulado, donde comparan el rendimiento de

su propuesta contra el de dos proyectos más: *DV-CAST* y *Smart Broadcast*. En las pruebas se varía la densidad de los vehículos en una autopista y se observan métricas como retardo punto a punto y tasa de recepción, entre otras. Los resultados de la experimentación muestran ventaja en rendimiento con respecto a los demás, principalmente debido al diseño del protocolo que se centra en utilizar la cantidad necesaria de recursos para evitar retardos y congestión, entre otros problemas. Sin embargo, el hecho de utilizar un simulador para la realización de pruebas genera interés sobre el comportamiento presentado en un entorno real.

Por su parte, para escenarios con alta densidad vehicular también se han desarrollado trabajos como el presentado en [38], donde se presentan las funcionalidades que luego fueron adoptadas en [7] respecto al uso de segmentos para dividir el espacio del escenario (entorno urbano) y emular el mecanismo RTS-CTS para disminuir la cantidad de mensajes emitidos de manera innecesaria por la red. En este proyecto no consideran el mecanismo de confirmación de recepción (ACK) al final de cada transmisión, sin embargo aquí, debido a las características del escenario a trabajar, presentan solución al problema de las intersecciones, donde han colocado un repetidor en cada una de ellas y es quien se encarga de retransmitir los mensajes hacia los cuatro puntos (calles) en que se divide el área.

Las pruebas de funcionamiento se han realizado de igual manera bajo un simulador, donde se observa el comportamiento presentado por el algoritmo en condiciones geográficas con una y cuatro intersecciones. Los resultados obtenidos muestran un eficiente uso del ancho de banda de la red, mostrando porcentajes positivos en las métricas utilizadas.

Estos diferentes tipos de protocolos descritos tienen como característica común el uso de la ubicación geográfica para asistir en cálculos de distancias o criterios de transmisión. Además, los últimos dos trabajos descritos implementan características de protocolos también presentados previamente, como la formación de *clusters* y selección de *cluster heads*. Adicionalmente ofrecen solución a problemáticas inherentes al tipo de comunicación y entornos para los que son diseñados, como la densidad vehicular variante. Sin embargo, se trata de pruebas en simulador, por lo que

	GPS	Escenario	Pros	Cons
Basados en ubicación	Sí	Urbano/Autopista	Escalabilidad alta	Decae con interferencia en GPS
Basados en *cluster*	Sí	Urbano	Escalabilidad alta	Retardos y overhead incrementa debido a selección de *cluster* heads
Geocast	Sí	Autopista	Reduce overhead	Tiempo de respuesta elevado debido a desconexiones
Broadcast	Sí (multi-hop)	Autopista	Simplicidad de implementación y alta tasa de recepción	Escalabilidad baja

Tabla 3.1: Características principales de los protocolos de diseminación de mensajes en VANETs.

un entorno de pruebas real sigue siendo atractivo para la verificación del comportamiento de estos protocolos.

En la Tabla 3.1 se presenta un resumen de las características principales de los protocolos de diseminación presentados. En ella se observa que el principio de funcionamiento de todos estos esquemas es la utilización de la ubicación de los nodos y que su implementación es favorable dependiendo el tipo de escenario. De manera general, los protocolos que realizan transmisiones con nodos seleccionados para esta tarea, reducen el overhead y logran escalar de mejor manera conforme la red crece. Por otro lado, protocolos que no tratan estas consideraciones, tienen baja complejidad de implementación, a cambio de ser utilizables en escenarios poco congestionados.

3.2 Validación de protocolos de diseminación de mensajes en VANETs

Una característica común en los trabajos realizados en el tema que abordan los protocolos de diseminación de mensajes es el uso de simuladores para la realización de pruebas, esto abre un campo de acción muy importante para analizar el comportamiento que se podría observar fuera de un entorno simulado. En esta subsección se exponen los trabajos que se enfocan en la realización de pruebas de diseminación de mensajes en escenarios reales.

En 2012, A. Amoroso *et al.* [39] realizan una experimentación con 2 laptops, 2 antenas Wi-Fi

(802.11 b/g), un dispositivo GPS y 4 vehículos transitando por algunos caminos y autopistas. Dos de ellos encontrados en los extremos y dos viajando entre éstos, pudiendo variar su posición relativa. El envío de mensajes se realiza cuando el nodo frontal envía un mensaje de alerta por broadcast y cada nodo que va recibiendo ese mensaje, lo retransmite de igual manera. La métrica utilizada para evaluar el comportamiento de la red es el número de saltos que el mensaje logra dar antes de perderse, variando la distancia recorrida en cada salto. Obteniendo mayor número de saltos en distancias bajas.

En [40], los autores utilizan tres tipos de dispositivos: smartphones, tablets y laptops, se basan en dos estándares: 802.11a y 802.11g y usan vehículos para preparar un escenario de pruebas. Realizan experimentos estáticos donde miden la intensidad de la señal radio (RSSI, por sus siglas en inglés) detectada a ciertos puntos separados por la misma distancia a lo largo del trayecto del escenario, esto con la finalidad de obtener el rango de cobertura máximo aceptable de los dispositivos. También realizan un segundo experimento, en él se analizan aspectos de calidad de servicio de la red: retardo extremo a extremo (E2ED, por sus siglas en inglés), porcentaje de paquetes entregados (PDR, por sus siglas en inglés) y la frecuencia con la que se envían los datos (TDR, por sus siglas en inglés). Este proyecto presenta una experimentación más amplia, al utilizar diferentes dispositivos y analizar diferentes distancias y parámetros del escenario. A pesar de esto, los experimentos pueden ser ampliados para abarcar mayor variedad de escenarios, como aquellos donde se efectuén transmisiones multi-salto.

Un caso más de experimentación con dispositivos móviles se presenta en [41], donde los autores proponen un sistema para la diseminación de mensajes en tiempo real en VANETs utilizando el sistema operativo Android. Para el desarrollo de su aplicación habilitan el modo ad-hoc (inhabilitada por defecto) y utilizan dispositivos HTC One y Nexus 5 para la experimentación. Los casos de prueba abordados consisten en colocar cada móvil dentro de un vehículo y ubicarlos a diferentes distancias, yendo desde los 40 hasta los 120 metros. Las pruebas consisten en el envío de mensajes de un móvil a otro, observando la tasa de recepción de paquetes (PRR, por sus siglas en inglés). Los resultados

Proyecto	Alcance	Dispositivos utilizados	Escenario	Métricas	Observaciones
[39]	Multi-Hop	Receptor GPS Laptops Antenas Wi-Fi Vehículos	Móvil	Número de saltos	Longitud del circuito: 19 km Saltos: 12.5
[40]	Single-Hop	Vehículos Tabletas Teléfonos inteligentes	Estático	E2ED PDR TDR	Distancias: 25-150 m PDR: 100-10 % E2ED: 2.2 - 1042 ms
[41]	Single-Hop	Teléfonos inteligentes	Estático	PRR	Distancias: 40-120 m PRR: 55-5

Tabla 3.2: Proyectos con experimentación en escenarios reales.

mostrados expresan que a medida que la distancia entre los dispositivos incrementa, la tasa de recepción disminuye, un efecto esperado en este tipo de medios inalámbricos. Sin embargo, las tasas de recepción registradas se encuentran por debajo del 60 % para el caso de 40 metros de separación, mientras que a los 120 metros, la tasa es casi nula.

En la Tabla 3.2 se encuentra un resumen de los trabajos que realizan experimentación en escenarios reales controlados de VANETs. En ella se presentan los escenarios, dispositivos empleados, métricas y observaciones sobre la experimentación realizada en tales proyectos.

3.3 Mecanismos de seguridad en VANETs

Como se menciona en el Capítulo 1, los mecanismos de seguridad aplicables en VANETs son dictaminados por el estándar para el acceso inalámbrico en ambientes vehiculares (WAVE) IEEE 1609.2, donde se establece el uso de criptografía de llave pública (PKC), mediante el uso de infraestructura (PKI) debido a la garantía que ofrece en cuanto al servicio de autenticación de nodos en la red, esto mediante el uso de firmas y certificados digitales. A continuación se presenta una explicación de la necesidad del uso de estos enfoques y una descripción del funcionamiento de estos mecanismos recomendados por el estándar IEEE 1609.2 [42].

En cualquier escenario donde se utilice criptografía de llave pública, el emisor utiliza la llave pública

del receptor para cifrar el mensaje y lo envía al destinatario. Cuando el mensaje llega al destino, se descifra mediante (exclusivamente) la llave privada del receptor, esto garantiza la confidencialidad de la comunicación. El problema con este escenario se presenta cuando el emisor solicita la llave pública del destinatario, pues no está seguro si la llave que le sea otorgada efectivamente sea la del destinatario deseado, es decir, un atacante puede tomar acción en este punto y hacerse pasar por otro usuario. Como solución al problema anterior aparecen los certificados digitales, los cuales ofrecen autenticación de los nodos. Para su implementación se requiere de una autoridad certificadora (CA), las cuales asocian llaves públicas con los identificadores únicos de los nodos y expiden los certificados digitales. Éstos certificados contienen información de la versión, número de serie, identificador del algoritmo, editor, validez, algoritmo de llave pública, llave privada, entre otros. Además, la CA almacena todas las llaves públicas de los nodos que acceden a ella como entidad confiable.

En una PKI, sin embargo, se requiere de algunas entidades para su implementación completa, además algunos aspectos importantes no son cubiertos en su totalidad por tal enfoque, tal es el caso de la revocación de certificados, donde la distribución de las listas con los certificados marcados como revocados resulta no escalable debido al número creciente de nodos en la red. Adicionalmente, la autenticación se vuelve un problema dado que los nodos emiten mensajes periódicos (beacons) cada 300 ms (según el estándar para DSRC), pudiendo resultar en un número excesivo de mensajes recibidos volviendo complicado el proceso de revisión en cuanto al tiempo de respuesta para la verificación, llegando a ser no realizable.

Ante las características mejorables que ofrece el protocolo para seguridad en VANETs surgen esquemas como alternativas, tal es el caso del cifrado basado en identidad (IBE) [43]. En este esquema, la llave pública de un usuario es información única acerca de la identidad del mismo (por ejemplo la placa del vehículo), esta información se encuentra disponible para los miembros de la red mediante una autoridad central, esto significa que un emisor que tiene acceso a los parámetros públicos del sistema puede cifrar un mensaje usando tal llave pública. El receptor obtiene su llave para el descifrado de la autoridad central, la cual debe ser confiable pues es la que genera las llaves

privadas para todos los nodos de la red.

Los sistemas basados en identidad permiten a cualquier nodo de la red generar una llave pública a partir del valor de identidad de otro nodo de la red. Una tercera entidad llamada generador de llave privada (PKG), genera la llave privada correspondiente. Para operar, dicha PKG publica una llave pública maestra y resguarda la llave privada maestra correspondiente. Conociendo la llave pública maestra y el valor de identidad del nodo con que se desea comunicar, un emisor puede generar una llave pública con la cual puede contactar a la PKG para que ésta, usando la llave privada maestra, genere una llave privada para el identificador de identidad. Los nodos pueden cifrar mensajes o verificar firmas sin la necesidad de la distribución previa de llaves entre los participantes. Lo anterior resulta conveniente en escenarios donde la distribución previa de llaves sea inviable. Por otro lado, para el descifrado o firma de mensajes, el usuario autorizado debe contactar a la PKG para obtener la llave privada apropiada. Un aspecto importante a considerar en este enfoque es que la PKG debe ser altamente confiable, debido a su importante rol en este esquema, pues es capaz de generar la llave privada de todos los nodos en la red.

Entre las ventajas que este esquema ofrece, se encuentra el hecho de que si existe un número finito de nodos, luego de que se les han otorgado las llaves a todos ellos, la entidad PKG puede ser omitida. Lo anterior debido a que el sistema asume que, una vez emitidas las llaves, éstas serán siempre válidas (ya que este sistema en su versión básica carece de revocación de llaves). Además, debido a que las llaves públicas son derivadas de identificadores, IBE elimina la necesidad de una infraestructura de distribución de llaves. La autenticidad de la llave pública es garantizada siempre y cuando el transporte de las llaves privadas al usuario correspondiente se mantenga seguro (autenticidad, integridad y confidencialidad). IBE ofrece además características que tienen que ver con la posibilidad de codificar información adicional al identificador. Por ejemplo, un emisor puede especificar la fecha de expiración para un mensaje y éste añade la fecha a la identidad real del receptor. Cuando el receptor contacta a la PKG para recibir la llave privada para esta llave pública, la PKG puede evaluar la fecha indicada y rechazar la operación si ésta ha expirado. De manera

general, la ventaja más marcada de este esquema sobre el basado en certificados digitales es el hecho de no necesitar obtener la llave pública del receptor antes de poder cifrar un mensaje para éste, ya que ésta puede ser generada por el emisor. Esto sin embargo, es posible a cambio del inconveniente de tener una autoridad central capaz de descifrar todos los mensajes en la red, ya que almacena las llaves privadas de los miembros participantes, lo cual implica tener que garantizar la seguridad de dicha entidad [44, 45].

Ante el problema del almacén de llaves privadas en la PKG, surge el enfoque de criptografía de llave pública sin certificados (CL-PKC), definido por Al-Riyami *et al.* [46]. Este esquema utiliza de igual manera una entidad confiable, denominada central de generación de llaves (KGC, por sus siglas en inglés). Sin embargo, la KGC no tiene acceso a las llaves privadas, como en el caso de la PKG, sino que a partir de un identificador (ID) genera y otorga llaves privadas parciales a los participantes del esquema. Cada nodo participante puede entonces generar su propio par de llaves (pública y privada) a partir de la llave privada parcial otorgada por la KGC y otros valores secretos y parámetros públicos del esquema. Una vez generado el par de llaves, los nodos pueden realizar las operaciones de cifrado, descifrado, firma y verificación de firma.

Con la revisión y análisis de los esquemas de seguridad descritos se ha generado un artículo científico, donde se presenta una comparativa cualitativa entre ellos [47]. Este artículo fue presentado en el Tercer Congreso Nacional de Ingeniería (CONNAI) 2016 en la Universidad Politécnica de Victoria.

3.4 Resumen

En esta sección se han presentado algunos de los enfoques para diseminación de mensajes en VANETs, los cuales se concentran en protocolos que utilizan la información de ubicación de los nodos para la toma de decisiones al transmitir dichos mensajes. Mientras las diferencias entre ellos se presentan en la manera en que organizan la red (*cluster*, ZOR) y la manera en que mantienen

(o no) la información acerca de los nodos cercanos (vecindario), las similitudes de éstos protocolos principalmente son relacionadas a la manera en que realizan sus transmisiones (más de un nodo destino interesado) y el uso de la ubicación de los nodos. Se han descrito algunos trabajos que proponen soluciones que consideran los inconvenientes de las transmisiones *broadcast* y la disminución de nodos transmisores. De igual manera se han discutido trabajos que realizan experimentación para esquemas de comunicación simple en escenarios reales, utilizando dispositivos móviles, demostrando su factibilidad de uso. Finalmente, se fundamenta la alternativa del uso de los esquemas basados en identidad ante las condiciones que presentan aquellos que utilizan certificados digitales en el contexto de la seguridad en VANETs.

4

Diseño y desarrollo de la plataforma

En este capítulo se exponen las funcionalidades requeridas en la plataforma, su diseño, modelado y características desarrolladas. Se detallan los procesos involucrados en su flujo de trabajo, así como las técnicas y esquemas implementados.

4.1 Definición de requerimientos

A fin de diseñar la plataforma móvil prevista en la presente tesis para realización de pruebas de transmisión de mensajes, a continuación se definen diversos requerimientos relacionados a la administración de comunicaciones, mecanismos de seguridad, recolección de estadísticas, entre otros.

- Administración de la VANET sin la intervención de una entidad gestora: La plataforma debe permitir la realización de pruebas de diseminación de mensajes entre nodos participantes en la VANET sin la intervención de una infraestructura. Esto involucra que nuevos nodos deben ser capaces de identificar la VANET existente y establecer la comunicación. Asimismo, la

plataforma debe permitir la creación de una VANET para el caso del primer nodo a incorporar a la misma.

- Transmisión de mensajes entre los nodos de la VANET. La característica más importante para el funcionamiento de una VANET es la diseminación de mensajes utilizando un protocolo. Para este caso, es necesario incluir en la plataforma un repositorio para almacenar los diferentes criterios considerados en protocolos de diseminación. Además, es necesario disponer de un formato pre-establecido de mensajes.

- Almacenamiento de información de los mensajes enviados/recibidos en la VANET para la generación de estadísticas. Este requerimiento es necesario para almacenar los registros de mensajes transmitidos y recibidos por un nodo. Esto permitirá calcular fuera de línea las métricas de rendimiento de un protocolo de diseminación particular en términos de tasa de paquetes perdidos, tiempo de transmisión, etc.

- Implementación de características de esquemas de diseminación de mensajes que consideren la ubicación de los nodos en la VANET. Como se ha mencionado, este trabajo se concentra en la implementación de esquemas de diseminación *broadcast* que hacen uso de la información que provee el GPS. En este sentido, se debe dar soporte al manejo de información de localización de los nodos en ambos roles (emisor y receptor), esto implica operaciones como el cálculo de distancias.

- Implementación de un esquema de seguridad para garantizar el servicio de autenticación de los nodos en la VANET. La plataforma debe incorporar un esquema de seguridad que permita comprobar que un mensaje recibido ha sido enviado por un nodo válido en la VANET.

- Implementación de una técnica de agregación de mensajes. La plataforma debe ofrecer características adicionales respecto a la generación y transmisión de mensajes que puedan ser utilizadas cuando el tiempo de respuesta para las aplicaciones así lo permita y se requiera

dar importancia al ahorro de energía.

4.2 Descripción de la plataforma

En el presente trabajo se propone una plataforma para la implementación de un prototipo de VANET que considera un diseño modular que facilite la integración de implementaciones externas de protocolos de diseminación o esquemas de seguridad que requieran ser validados. En este sentido, se ha implementado un protocolo de diseminación y un esquema de seguridad, éstos son descritos en subsecciones posteriores. Además, se incorpora un receptor de GPS externo con mayores prestaciones de granularidad (frecuencia de actualización de lecturas) en la obtención de la ubicación comparado con el sensor nativo de los dispositivos móviles utilizados para la experimentación. Con esto se brinda mayor precisión a los protocolos de diseminación que consideran la ubicación de los nodos.

Los requerimientos de la solución son atendidos mediante la modularización de una plataforma que realiza las tareas de cada etapa de la configuración y experimentación de manera aislada, desarrollando las tareas en los módulos correspondientes. De esta manera, se facilita el reemplazo del módulo de protocolo de diseminación por parte de un usuario externo que desee validar su implementación sobre la plataforma, siempre y cuando sea parte de la familia de protocolos *broadcast* que incluyen la información de ubicación en las transmisiones. En la Figura 4.1 se muestra de manera general la estructura de la solución propuesta considerando el flujo de emisión y recepción de mensajes.[1] Como se aprecia en esta figura, los componentes de la plataforma se ubican en diferentes capas, la primera de ellas es la interfaz de configuración, donde el usuario indica las características a considerar en la sesión de pruebas. La capa de gestión de paquetes modela los roles que toma cada nodo (cliente y servidor), con las características de creación, manipulación, envío y recepción de paquetes. La capa de interacción con sensores permite la obtención de la ubicación a través de los sensores nativo y/o externo. La última capa representa las tareas de envío y recepción de mensajes a través de la

[1] El diagrama UML de despliegue para la estructura de la solución se encuentra en el Anexo A de este documento.

interfaz inalámbrica del dispositivo, además de los criterios que considera el protocolo de diseminación empleado.

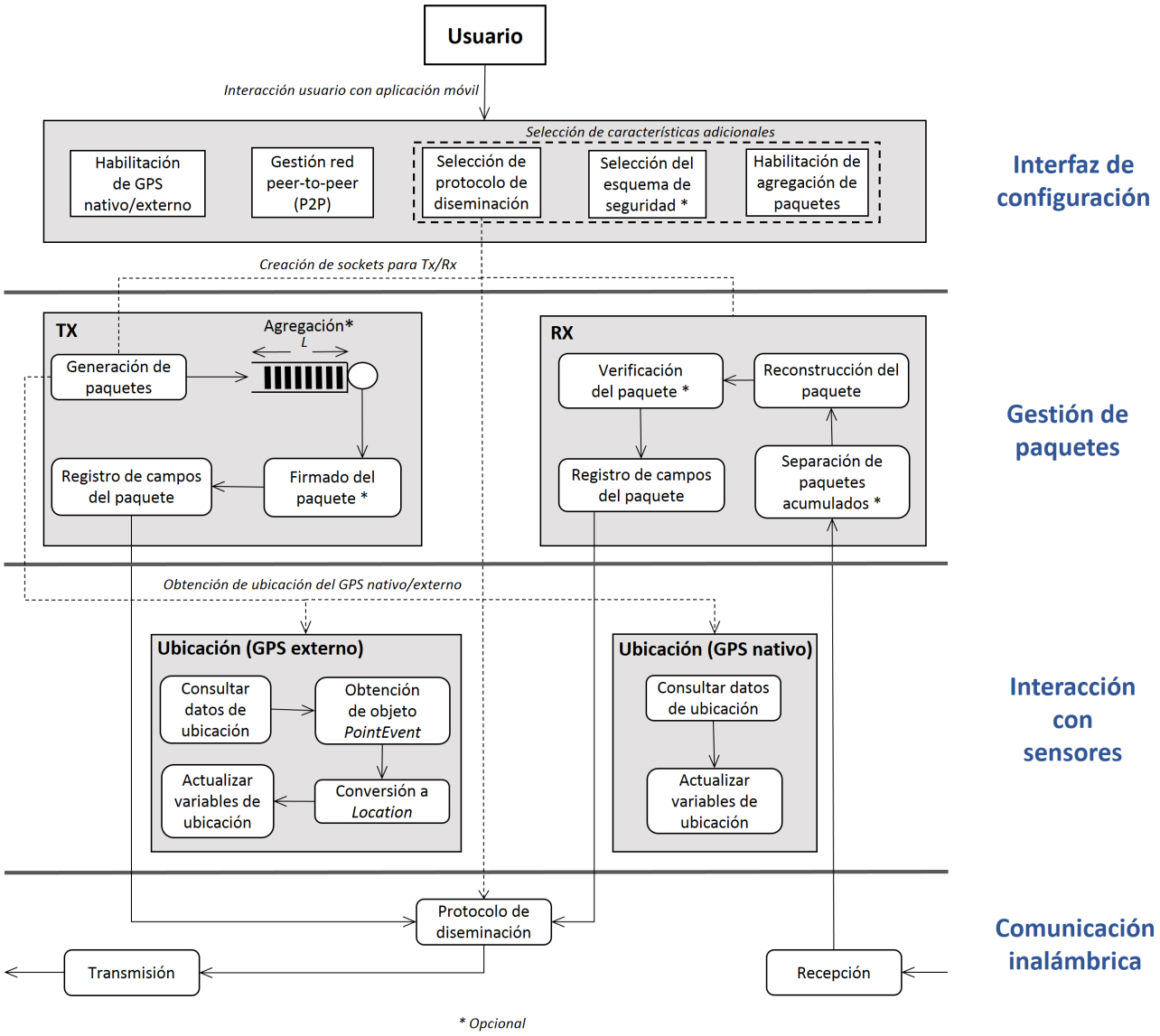

Figura 4.1: Diagrama de bloques de la plataforma para diseminación de mensajes.

En los siguientes apartados se detallan las funcionalidades de la plataforma presentadas en la Figura 4.1. También se presentan los mecanismos considerados para brindar seguridad (esquema de firmas digitales) y alternativas para la transmisión de los mensajes en la plataforma (agregación de paquetes generados).

4.2.1 Interfaz de configuración

Este bloque se trata de la pantalla principal de la plataforma, con la que el usuario interactúa indicando los parámetros a considerar en la sesión de prueba. Las opciones de configuración de la plataforma se explican a continuación.

4.2.1.1. Selección de proveedor de ubicación

La plataforma de pruebas el uso de un sensor GPS externo, el cual se conecta mediante *Bluetooth* y actualiza las lecturas de ubicación para disponerlas al resto de los módulos de la plataforma. El receptor GPS debe ser vinculado al dispositivo móvil de manera manual por el usuario. Una vez vinculado, la plataforma lo reconoce como disponible y puede hacer uso de los elementos básicos de la API de Android para realizar el proceso de vinculación y toma de lecturas en segundo plano. Asimismo, el usuario puede optar por seleccionar el GPS nativo del dispositivo móvil como proveedor de ubicación del protocolo de diseminación que se desee validar.

4.2.1.2. Gestión de red Wi-Fi Peer-to-peer (P2P)

Como se menciona en subsecciones anteriores, los requerimientos de conectividad para una VANET incluyen la creación, descubrimiento y conexión a una red sin intervención de una entidad gestora. Bajo la API de Android, estos requerimientos se cumplen utilizando la clase *WifiP2pManager* que retorna un canal que conecta la plataforma con el *framework* Wi-Fi P2P. La interacción entre las clases que participan en este proceso se presenta en las Figuras 4.2 y 4.3. Entre estas interacciones, se tiene el manejo de las notificaciones de los métodos por defecto de *WifiP2pManager*, las cuales son administradas por un *BroadcastReceiver* que debe ser registrado. Este *receiver* notifica sobre eventos como cambio de estado de la conexión, nuevos dispositivos disponibles y desconexiones. El término *servicio* en este contexto se refiere a la información del dispositivo (dirección MAC, dirección IP, rol que desempeña, etc.) y es la base para el descubrimiento y conexión a otros dispositivos.

En el registro de un servicio el objetivo es manifestar la intención de un nodo (vehículo) de formar parte de la red. Se inicializa el servicio con la información del nodo, quedando disponible para que otros nodos puedan identificarlo. En la operación de descubrimiento, un nodo escanea el canal de comunicación en busca de servicios registrados y publicados por otros nodos. En particular, en esta operación se asigna un *Listener* para conocer cuando se hayan descubierto nuevos servicios y se extrae su nombre/identificador, para luego mostrarlo al usuario en un listado. Finalmente, puede seleccionarse un nodo de los listados para iniciar la conexión (*peer-to-peer*), iniciando así la red. Durante este proceso se gestionan los roles que tomará cada nodo (sólo existe un propietario del grupo y el resto toman el rol de cliente), así como la asignación de direcciones IP y la configuración de los *sockets* cliente y servidor del nodo.

4.2.1.3. Selección de características adicionales

La pantalla de configuración concluye con la selección del protocolo de diseminación a validar (con criterios de envío/retransmisión que son considerados previo a la transmisión, como se observa en la capa de comunicación inalámbrica), la indicación para que las transmisiones sean aseguradas o no, así como la habilitación de la técnica de agregación de paquetes. Estas funcionalidades son opcionales y basta con indicar en las casillas correspondientes cuáles de ellas se han de utilizar.

4.2.2 Gestión de paquetes

Para la realización de una prueba de validación con un protocolo de diseminación, es necesario disponer de los medios para generar adecuadamente los paquetes incluidos en los mensajes. En este sentido, en este bloque se encuentran las funciones de generación de paquetes, acumulación y firma de los mismos (si así se indica en la configuración inicial), concluyendo el flujo de trabajo con el guardado de los campos de los paquetes generados y la transmisión de los mismos. La lógica general de este bloque es la división de tareas de acuerdo a los roles que cumple cada nodo: emisor y receptor.

Los paquetes generados en la plataforma constan de 8 campos: (a) identificador, etiqueta única

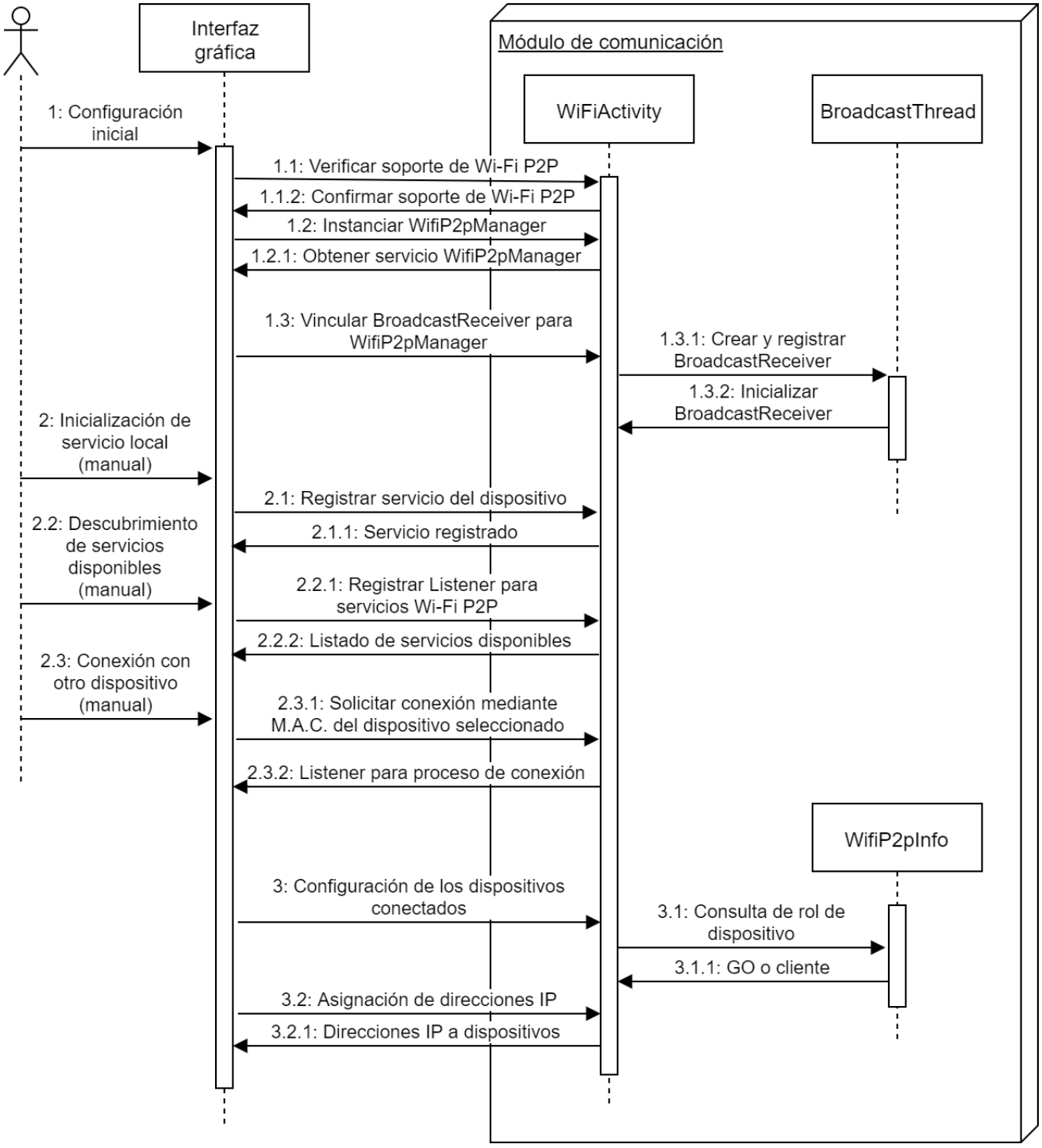

Figura 4.2: Diagrama de secuencia de la gestión de conexiones bajo Wi-Fi P2P (parte 1).

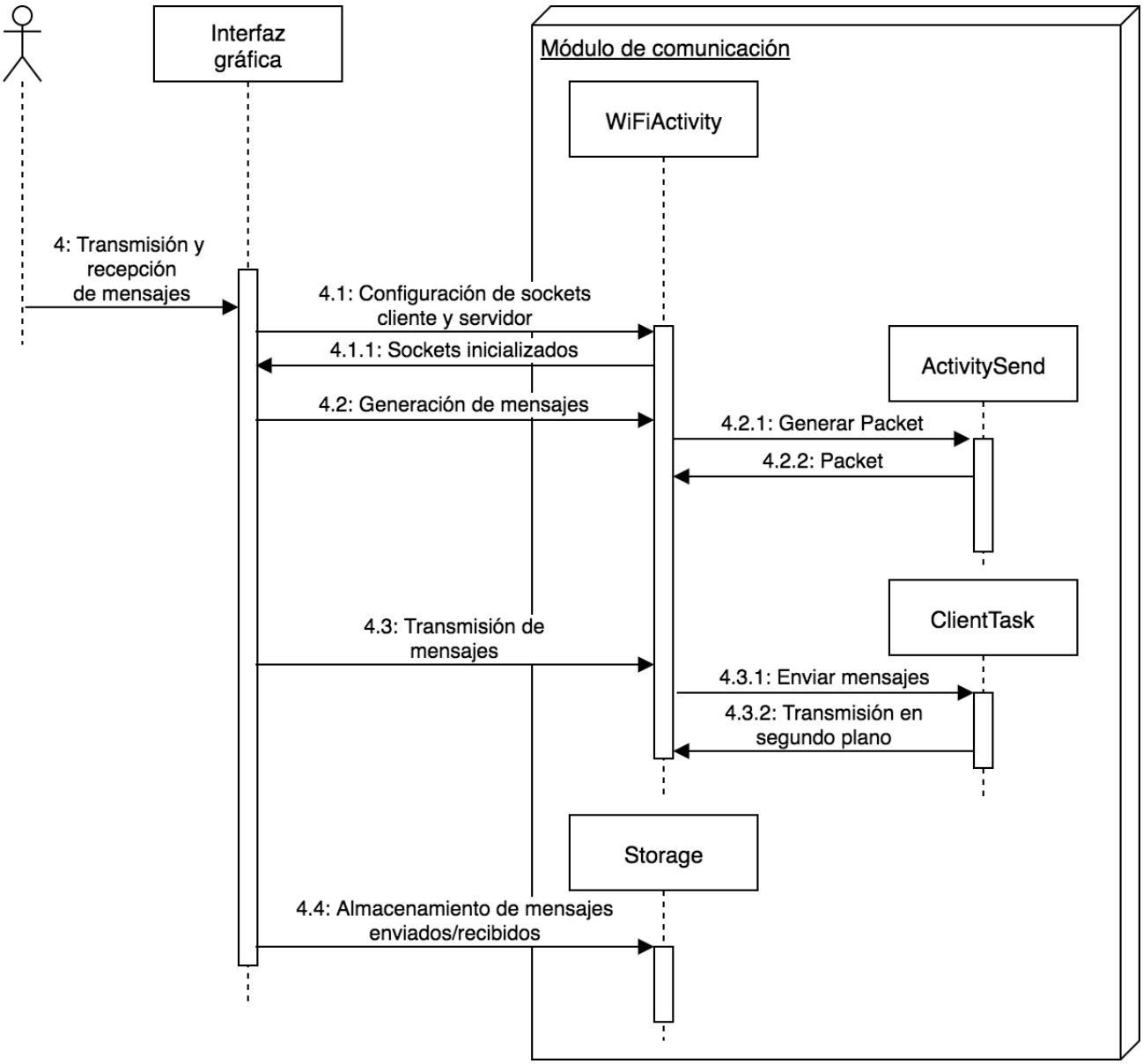

Figura 4.3: Diagrama de secuencia de la gestión de conexiones bajo Wi-Fi P2P (parte 2).

para cada paquete generado, (b) tipo de mensaje, que identifica si se trata de un mensaje de alerta, de control o de confirmación, (c) dirección MAC del dispositivo, que identifica la tarjeta de red del nodo, (d) dirección IP del dispositivo, que permite identificar cada nodo ante la red, (e) fecha y hora de emisión, utilizada para el cálculo del tiempo transcurrido entre emisión y recepción, (f) latitud, (g) longitud y (h) velocidad del nodo, utilizados para el cálculo de distancia y consideraciones de los

protocolos de diseminación. La Tabla 4.1 muestra el tamaño de cada campo en la carga útil total.

Campo	Tipo de dato	Tamaño (bytes)
ID paquete	String	7
ID mensaje	Char	2
Dirección MAC	String	17
Dirección IP	byte[]	4
Fecha y hora	String	23
Latitud	Double	8
Longitud	Double	8
Velocidad	Double	8
Seguridad	Char	2
Total		79

Tabla 4.1: Campos del paquete generado en la plataforma en el formato sin seguridad (carga útil).

Cabe destacar que con la finalidad de garantizar la unicidad de los paquetes se genera su identificador utilizando los últimos tres octetos de la dirección MAC del dispositivo y el tiempo del sistema en nanosegundos. Ambos datos son concatenados y resumidos con una función *hash* y se toman los primeros siete caracteres de ese resumen *hash*, como se ilustra en la Figura 4.4.

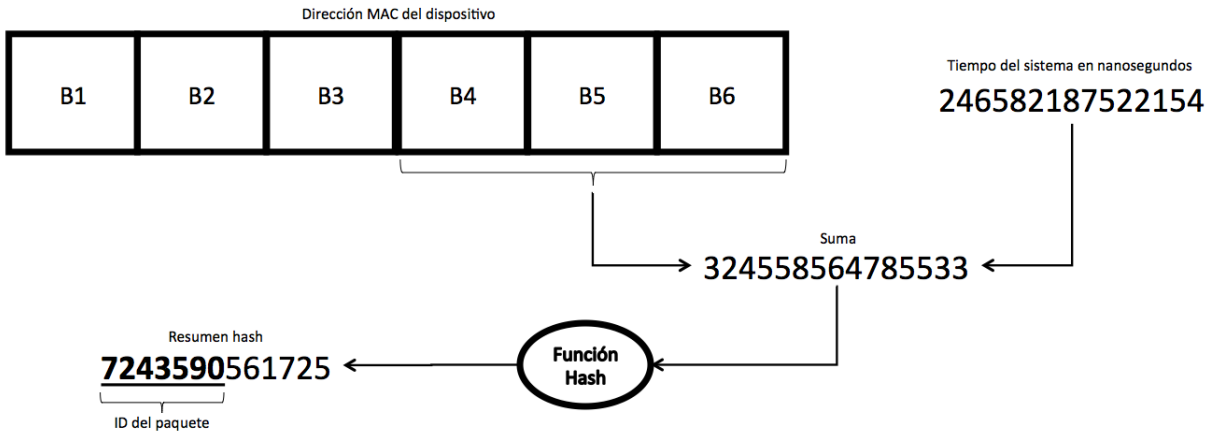

Figura 4.4: Proceso de generación del identificador del paquete a transmitir.

Al resto de los campos del paquete se les asigna el valor de variables ya manejadas hasta este punto del proceso, por lo que basta con obtener los bytes que representan dichas variables para

Algoritmo 1 Generación del identificador del paquete
Entrada: MAC : Dirección MAC del dispositivo
Salida: ID_pkt : Identificador del paquete
1: $macPart[] = MAC.split(" : ")$
2: $macLastThree = macPart[3] + macPart[4] + macPart[5]$
3: $time = System.nanoTime()$
4: $hash = (macLastThree + time).hashCode()$
5: **Devolver** $|hash|.substring(0, 7)$

finalmente concatenar los ocho campos en un arreglo de bytes con un tamaño total de 87 bytes. El último campo del paquete indica si éste ha sido asegurado o no con una firma digital, esto se explica en las siguientes subsecciones.

4.2.3 Esquema de seguridad

Una vez generado un paquete con el proceso anterior, el resultante es denominado carga útil y debe ser asegurado (firmado). Se ha seleccionado el esquema *CLS*, propuesto por A. Malip *et al.* (2014) [48] para este proceso. Este esquema implementa un mecanismo de firma sin certificados basado en operaciones con elementos pertenecientes a grupos cíclicos formados a partir de los parámetros que conforman una curva elíptica.

Para la implementación del esquema CLS se ha utilizado la biblioteca JPBC [49], así como el módulo de generación de llave pública y los archivos con los parámetros de curvas elípticas definidos por el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) de la API DET-ABE, desarrollada por M. Morales y A. Díaz [50].

El esquema CLS indica la generación de las llaves necesarias para las operaciones de firma y verificación en una etapa fuera de línea. Esta tarea involucra dos procesos: la configuración de la TA, donde se generan los parámetros públicos y privados del esquema (Algoritmo 2), y el registro de los nodos que formarán parte del esquema, este proceso incluye operaciones tanto en la TA (Algoritmo 3) como en el nodo que se está registrando (Algoritmo 4). Los parámetros públicos son generados y distribuidos por la autoridad confiable, mientras que en una etapa en línea son utilizadas para

efectuar las operaciones mencionadas. La Figura 4.5 ilustra ambas etapas propuestas en el esquema de seguridad y los elementos involucrados en éstas.

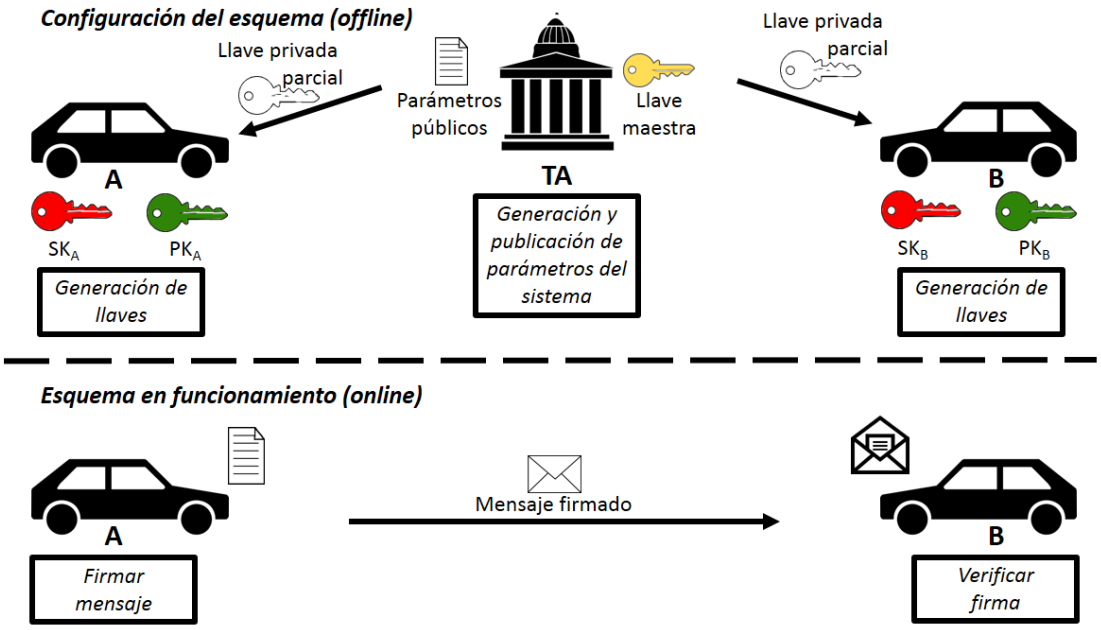

Figura 4.5: Diagrama general de funcionamiento del esquema de seguridad sin certificados digitales.

Algoritmo 2 Configuración de la Autoridad Confiable

Entrada: 1^k: Nivel de seguridad
Salida: *params* : Set

1: G_1 : Grupo aditivo de orden q
2: G_2 : Grupo multiplicativo de orden q
3: e : Emparejamiento bilineal G_1 x $G_1 \rightarrow G_2$
4: H_1, H_2, H_3 : Función *hash* que mapea de $\{0,1\}^*$ a G_1
5: s : Entero $\in Z_q^*$ (Llave privada maestra)
6: P : Elemento $\in G_1$ (Generador de G_1)
7: $P_0 = s \cdot P$: Multiplicación escalar (Llave pública maestra)
8: H_4 : Función *hash* que mapea de $\{0,1\}^*$ a G_1
9: **Devolver** $params = (G_1, G_2, e, q, P, P_0, H_1, H_2, H_3, H_4)$

A continuación se describen los procesos realizados por el esquema de seguridad en la etapa en línea.

Obtención de parámetros públicos del esquema:

Algoritmo 3 Registro de un nodo en la Autoridad Confiable
Entrada: ID_V : Identificador único del nodo
Salida: x_V : Llave privada parcial del nodo
1: $Q_V = H_1(ID_V)$: Resumen *hash* del identificador del nodo
2: $x_V = sQ_V$: — (Llave privada parcial del nodo)
3: **Devolver** x_V

Algoritmo 4 Generación de llaves en el nodo
Entrada: x_V : Llave privada parcial del nodo
Salida: (sk_V, pk_V) : Par de llaves (privada y pública) del nodo
1: y_V : Entero $\in Z_q^*$ (Valor secreto)
2: $sk_V = (x_v, y_V)$: Tupla (Llave privada del nodo)
3: $pk_V = y_V P$: (Llave pública del nodo)
4: **Devolver** (sk_V, pk_V)

Fuera de línea se pre-cargan en el dispositivo móvil los archivos generados por la entidad confiable del esquema de seguridad: parámetros públicos (nivel de seguridad, tipo de curva elíptica, generador y llave pública maestra) y llave privada parcial del nodo. En este proceso se accede a dichos archivos y a partir de ellos se generan los elementos necesarios para el esquema. Se realiza primero un emparejamiento con los datos obtenidos de los parámetros públicos y se asignan los grupos y componentes del esquema $(G1, \mathbb{Z}_r, P, P_0)$. Dichos componentes quedan disponibles para el resto de las funciones que las utilizarán para las operaciones básicas y emparejamientos.

Firma del paquete:

Los componentes que han sido inicializados en el proceso anterior, ahora son utilizados para el firmado del paquete. Con ellos se generan los elementos utilizados en la operación de firma (*u, U, P, ppkV, IDv, yv, pkV, M*), donde *M* es el resumen *hash* del mensaje a firmar (en este caso la carga útil). Este proceso se lleva a cabo en el lado del emisor, dentro del proceso de transmisión de un paquete. El Algoritmo 5 presenta las operaciones realizadas para la generación de la firma de un mensaje.

Algoritmo 5 Firma de mensaje

Entrada: ID_V : Identificador único del nodo
sk_V : Llave privada del nodo
pk_V : Llave pública del nodo
M : Resumen *hash* del mensaje a firmar
Salida: θ_V : Firma del nodo para el mensaje
1: u : Entero $\in Z_q^*$
2: $U = u \cdot P$: Multiplicación escalar
3: $v = x_V + u \cdot H_2(M, ID_V, pk_V, U) + y_V \cdot H_3(M, ID_V, pk_V)$
4: **Devolver** $\theta_V = (U, v)$ Tupla

Como se observa en la línea 3 del Algoritmo 5, se integran los bytes de los elementos *M, IDv, pkV y U* y se calcula su resumen *hash*. Lo mismo se realiza para integrar los bytes de los elementos *M, IDv y pkV* y calculando su resumen *hash*. Se realizan multiplicaciones y sumas entre los elementos calculados. Finalmente, se toman los bytes de los elementos U, v, pkV y IDv son concatenados a un arreglo (*overhead* de seguridad) con un tamaño de 420 bytes para a su vez añadirlo a la carga útil existente. De esta manera se tiene el paquete completo y listo para ser transmitido.

Verificación de firma:

Cuando se trata del receptor, al recibir un paquete que ha sido generado aplicando el esquema de seguridad, es necesario validar la firma que acompaña a la carga útil. Para ello, se realiza el proceso de obtención de parámetros públicos del esquema. Luego, se calcula el resumen *hash* del identificador (*IDv*) del nodo firmante. Se generan los elementos principales para realizar la verificación (*Qv, U, v, IDv, pkV*). Se concatenan los bytes de los elementos *M, IDv, pkV y U* y se calcula su resumen *hash*. Lo mismo se realiza para los elementos *M, IDv y pkV*. Posteriormente se realizan emparejamientos bilineales y multiplicaciones escalares entre los elementos calculados. La verificación es exitosa si se comprueba la igualdad expresada en la línea 2 del Algoritmo 6.

Con la firma de mensajes y su verificación, se asegura que el nodo firmante es válido ante el sistema, ya que para efectuar la operación de firma ha tenido que pasar por el proceso fuera de línea en el que se registra ante la TA y ésta le otorga su llave privada parcial y los parámetros públicos del

Algoritmo 6 Verificación de firma

Entrada: M : Resumen *hash* del mensaje firmado recibido
$\theta_V = (U, v)$: Firma del emisor
ID_V : Identificador único del nodo emisor
pk_V : Llave pública del emisor

1: $Q_V = H_1(ID_V)$
2: **Si** $e(v, P) = e(Q_V, P)e(H_2(M, ID_V, pk_V, U), U)e(H_3(M, ID_V, pk_V), pk_V)$ **Entonces**
3: **Devolver** Firma válida
4: **Si no**
5: **Devolver** Firma no válida
6: **Fin Si**

sistema. Uno de estos parámetros (P), es utilizado en las operaciones de firma y verificación, por lo que si la validación es exitosa, implica que el nodo firmante también es válido. Sin embargo, puede presentarse el caso en que un nodo, a pesar de ser válido, tome conductas maliciosas, modificando mensajes emitidos por otros nodos antes de llegar a su destino, por ejemplo. Ante este posible ataque a la seguridad, el esquema CLS propone un sistema de reputación el cual consiste en el envío de mensajes de retroalimentación por parte de los nodos que han recibido un mensaje hacia el servidor de reputación, valorando su experiencia con el nodo emisor de la alerta. El servidor de reputación mantiene actualizados las puntuaciones de reputación de cada nodo, de manera que, cuando un nodo alcanza una reputación baja, significa que ha transmitido información no verídica, pudiendo proceder a su revocación del sistema. Este sistema de reputación, sin embargo, no ha sido implementado en la plataforma debido a la infraestructura requerida para su funcionamiento (servidor de reputación y suficientes nodos en la red). No obstante, la implementación base para este esquema permite que éste pueda ser completado cuando se cuente con la infraestructura adecuada.

4.2.4 Técnica de agregación de paquetes

Debido al tamaño y tiempo de procesamiento que el esquema de seguridad representa, las comunicaciones tienen un impacto importante en relación a la proporción de los paquetes generados con criterios de seguridad. Mientras que apenas 87 bytes son información útil para el esquema de

comunicación (cerca del 20 % del tamaño total del paquete), el resto es información únicamente para el esquema de seguridad (80 %). Esto es una proporción poco deseable para el esquema de comunicación, por lo que se ha propuesto como alternativa el uso de una técnica de agregación que permita el ajuste de las proporciones de los paquetes en las pruebas de diseminación en VANETs con dispositivos móviles. Dicha técnica consiste en acumular paquetes generados sin transmitirlos inmediatamente, sino hasta alcanzar un número L de paquetes acumulados (indicado en la interfaz de configuración). De esta manera, se tiene un compromiso en relación al ahorro de recursos de red y energía del dispositivo ante el tiempo de respuesta para las aplicaciones. La siguiente figura ilustra el objetivo de la técnica de agregación de paquetes.

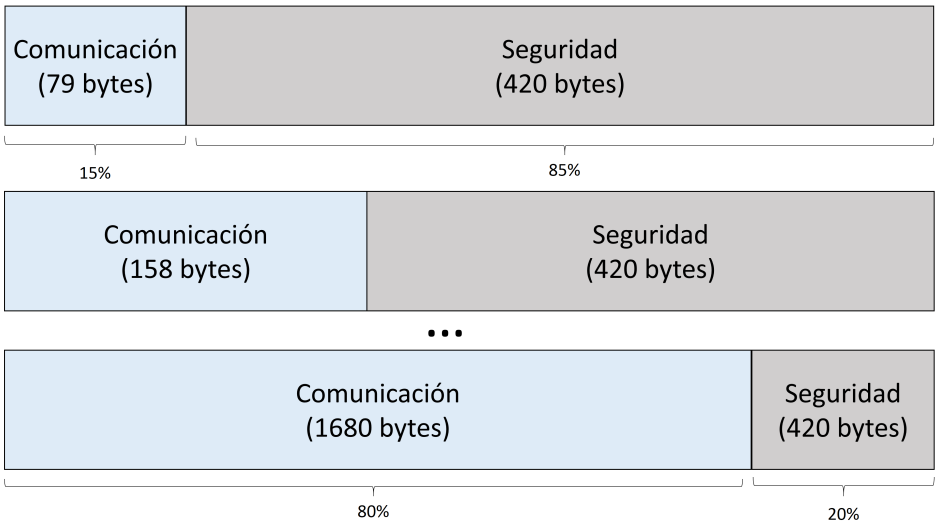

Figura 4.6: Funcionamiento de la técnica de agregación de paquetes.

Cabe mencionar, que la frecuencia con la que los paquetes son generados está dictaminada por el intervalo que se indica por el usuario en la interfaz de configuración de la prueba, por lo que el tiempo de espera en la acumulación de paquetes está definido por ese mismo intervalo y el número de paquetes a agregar. Además, el uso de esta técnica está sujeto al tipo de aplicación al que vaya destinado el esquema de diseminación a validar, ya que algunas de ellas serán sensibles al tiempo de respuesta de las comunicaciones, el cual se ve incrementado con el uso de esta técnica. Sin embargo,

otro compromiso que se presenta es el ahorro de energía del dispositivo debido a la frecuencia con la que se realizan las transmisiones salientes en la interfaz Wi-Fi, siendo menos el consumo cuando se utiliza esta técnica de agregación.

4.2.5 Registro de campos del paquete

Sin importar si se trata de un caso de transmisiones con o sin seguridad, una vez que se transmite o recibe un paquete correctamente (firma verificada, en el caso de seguridad), se guarda un registro de los campos de la carga útil. Este registro involucra obtener el directorio principal de almacenamiento en el dispositivo para crear un archivo que contendrá los datos de cada paquete que forme parte de la misma prueba. Se crea una instancia de *OutputStreamWriter* para gestionar el archivo a generar y una para *BufferedWriter* para escribir sobre el archivo de salida. Se obtiene cadena de texto con los campos de la carga útil del objeto que modela el paquete en la plataforma. Finalizando con la escritura de la cadena de texto y el tiempo invertido en la firma y verificación del paquete. El archivo resultante queda disponible para su análisis estadístico de manera *offline* al término de una sesión de prueba.

4.2.6 Interacción con sensores

Este bloque trata la interacción con el módulo *hardware* GPS del dispositivo móvil para la obtención de la ubicación y la interacción vía *Bluetooth* con el sensor GPS externo.

Como se ha indicado en la subsección *4.2.1.1*, el receptor GPS que ha sido vinculado al dispositivo en trato se comunica vía *Bluetooth* para después poder utilizar los elementos de la API de Android. Dichos elementos son:

- **Métodos**: Funciones definidas en las clases, encargadas de conectar, actualizar, escanear, desconectar, entre otras actividades con otros dispositivos o interacción con otras clases.

- ***Listeners***: Objetos que permiten notificaciones de las llamadas a los métodos de las clases. Cuando se llama a uno de estos métodos, se le asigna el Listener que se desea atienda a los resultados de la ejecución del método.

- ***Intents***: Notifican sobre eventos específicos detectados por el *framework* de Android, por ejemplo, un dispositivo disponible, conectado, desconectado, un evento de una clase se ha presentado, etcétera.

Las actualizaciones de ubicación del receptor GPS externo, manejadas a partir de su identificador universal (UUID, por sus siglas en inglés) ya conocido, son procesadas por la plataforma, teniendo que ser convertidas del formato origen, establecido por la asociación de electrónicos de la marina nacional (NMEA, por sus siglas en inglés) de Estados Unidos a coordenadas geográficas (latitud, longitud) para después mantenerlas disponibles para el resto de los módulos. En la Figura 4.7 se ilustra el flujo de procesos en la plataforma para la interacción con el sensor GPS externo.

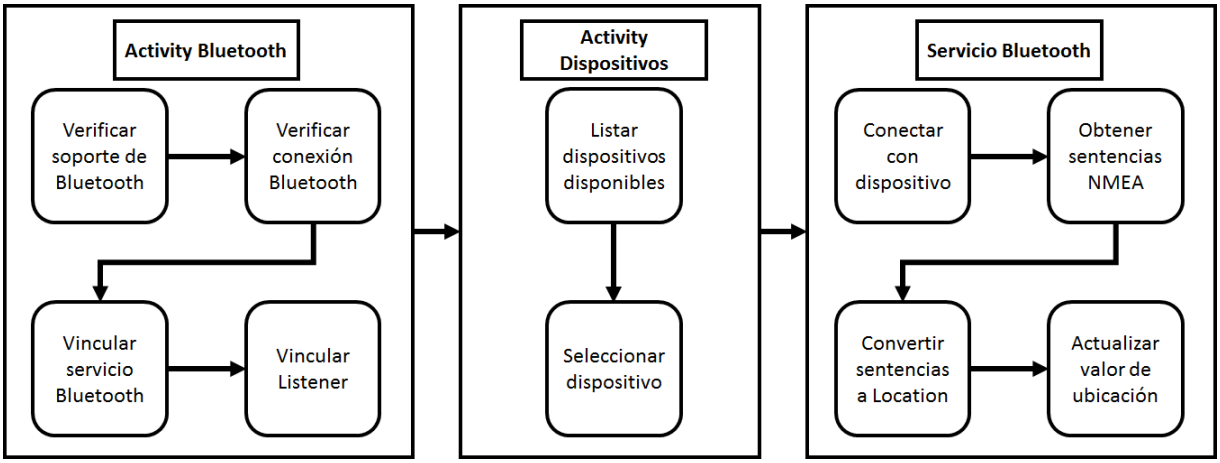

Figura 4.7: Flujo de actividades en la integración del sensor GPS externo a la plataforma vía Bluetooth.

Por otra parte, la habilitación de lecturas del sensor GPS nativo se realiza mediante la invocación a la clase *Location Manager* de la API de Android, cuyo método *getLastKnownLocation* devuelve un objeto *Location* con la información de la lectura de ubicación. Se invoca el método

requestLocationUpdates de la clase *Location Manager* para iniciar el proceso de adquisición de lecturas y se vincula un *Listener* para actualizar los valores de latitud, longitud y velocidad cada que se presente un cambio en los mismos.

4.2.7 Comunicación inalámbrica

Este bloque modela la salida y entrada de paquetes por la interfaz Wi-Fi, con la característica de la implementación de un protocolo de diseminación. Cuando se ha seleccionado un protocolo en la interfaz de configuración, se asume que dicho protocolo ha sido desarrollado e integrado a la plataforma e interactúa con las características que ofrece la misma. Para este trabajo de tesis, se ha destinado la plataforma para la validación de protocolos basados en ubicación. Más detalles sobre la validación de protocolos de diseminación en la sección 5.6.1.

4.2.8 Extracción de estadísticas

En una etapa fuera de línea, habiendo terminado la sesión de pruebas, el archivo almacenado mediante el proceso de registro de campos, es analizado con un *script* realizado en *Matlab*. En particular, en cada dispositivo se obtienen dos archivos por cada sesión de pruebas, correspondientes a los paquetes transmitidos y recibidos, respectivamente. En la Figura 4.8 se muestra el contenido de los archivos generados.

En la experimentación se efectúan transmisiones de mensajes de un nodo a otro(s). Las métricas observadas son: retardo promedio (Ecuación 4.1) desde la emisión de un mensaje hasta su recepción, para el total de paquetes emitidos en la sesión, y la pérdida de paquetes (Ecuación 4.2) en dicha sesión.

$$D = \frac{\sum_{i=1}^{N} T_{rec}^{i} - T_{env}^{i} - T_{firma}^{i}}{N} \tag{4.1}$$

Donde:

ID paquete	ID Mensaje	MAC origen	IP origen	Timestamp envío	Latitud	Longitud	Velocidad	Tiempo de firma
1570612	A	8a:30:8a:da:38:33	192.168.49.1	2017-08-18 03:55:20:299	23.72097588	-99.07728577	0	0
2051988	A	8a:30:8a:da:38:33	192.168.49.1	2017-08-18 03:55:25:298	23.72097588	-99.07730103	0	0
1846130	A	8a:30:8a:da:38:33	192.168.49.1	2017-08-18 03:55:30:299	23.72097588	-99.07730865	0	0
1000584	A	8a:30:8a:da:38:33	192.168.49.1	2017-08-18 03:55:35:299	23.72094345	-99.07740021	0	0
6969938	A	8a:30:8a:da:38:33	192.168.49.1	2017-08-18 03:55:40:298	23.72094345	-99.07740021	0	0

Registro de paquetes transmitidos

ID paquete	ID Mensaje	MAC origen	IP origen	Timestamp envío	Latitud	Longitud	Velocidad	Tiempo de verificación	Timestamp recepción
1570612	A	8a:30:8a:da:38:33	192.168.49.1	2017-08-18 03:55:20:299	23.72097588	-99.07728577	0	0	2017-08-18 03:55:19:625
2051988	A	8a:30:8a:da:38:33	192.168.49.1	2017-08-18 03:55:25:298	23.72097588	-99.07730103	0	0	2017-08-18 03:55:24:564
1846130	A	8a:30:8a:da:38:33	192.168.49.1	2017-08-18 03:55:30:299	23.72097588	-99.07730865	0	0	2017-08-18 03:55:29:582
1656338	A	8a:30:8a:da:38:33	192.168.49.1	2017-08-18 03:55:45:298	23.72094345	-99.07740021	0	0	2017-08-18 03:55:44:692
8694377	A	8a:30:8a:da:38:33	192.168.49.1	2017-08-18 03:55:55:298	23.72094154	-99.07740021	0	0	2017-08-18 03:55:54:566

Registro de paquetes recibidos

Figura 4.8: Fragmento de los rchivos generados en cada nodo con la información de los campos en los paquetes.

D representa el retardo promedio en las transmisiones,

T^i_{rec} representa el *timestamp* de recepción del paquete i,

T^i_{env} representa el *timestamp* de envío del paquete i,

T^i_{firma} representa el tiempo invertido en la generación de la firma del paquete i y

N representa el número total de paquetes transmitidos.

$$PL = \frac{P_{env} - P_{rec}}{P_{env}} \tag{4.2}$$

Donde:

PL representa la pérdida de paquetes en una sesión de pruebas,

P_{env} representa el número de paquetes enviados, y

P_{rec} representa el número de paquetes recibidos.

4.3 Resumen

En este capítulo se ha presentado el diseño de la plataforma, presentando su separación por capas considerando su flujo e interacción y se han descrito sus características esenciales, como la integración del sensor GPS externo y la gestión de la red P2P mediante la API de Android, así como la generación de paquetes, su composición y el registro de sus campos para la obtención de estadísticas. De igual manera se han descrito las características adicionales al esquema de comunicación, como el aseguramiento de los mensajes con el esquema de firma CLS, el cual basa su funcionamiento en el uso de emparejamientos bilineales con elementos obtenidos de parámetros de curvas elípticas, así como la técnica de agregación de paquetes cuyo objetivo es la reducción del número de transmisiones, disminuyendo la carga en la red y consumo de energía, a cambio de un incremento en el tiempo de respuesta de las aplicaciones.

5

Experimentación y resultados

En este capítulo se describe la metodología de experimentación realizada con la finalidad de validar la plataforma y sus módulos, detallando escenarios y configuraciones para las sesiones de prueba. Se presentan además los resultados obtenidos con dicha experimentación y se discuten las observaciones en cada caso.

5.1 Infraestructura utilizada

Para la experimentación con la plataforma se han utilizado dos tabletas Samsung Galaxy Note 10.1 (GT-N8010), además de un teléfono Samsung Galaxy Grand Prime (SM-G531H). Adicionalmente, se ha utilizado una *laptop* Lenovo Thinkpad Edge 14 para la configuración del esquema CLS, actuando como TA en la fase fuera de línea del esquema. Para la obtención de la ubicación se han utilizado tres receptores GPS externos *GPS Lap Timer* de la marca Qstarz Racing, con una frecuencia de actualización de 1 hasta 10 Hz. Para la experimentación descrita posteriormente, se ha utilizado la frecuencia de 10 Hz en los receptores GPS externos. En particular, para las pruebas realizadas se

ha vinculado un receptor GPS externo a cada dispositivo móvil. En la Tabla 5.1 se muestran las características de los dispositivos empleados en la experimentación de la plataforma.

Módulos	Samsung Galaxy Note 10.1	Samsung Galaxy Grand Prime	Lenovo Thinkpad Edge 14
Procesamiento	Quad-Core 1.4 Ghz ARM Cortex-A9	Quad-core 1.2 GHz Cortex-A53	Intel Core i5 M540 4 núcleos (2.53 GHz)
Memoria	2 GB RAM LPDDR2	1 GB RAM LPDDR2	4 GB RAM DDR3
Comunicaciones	Wi-Fi 802.11 a/b/g/n	Wi-Fi 802.11 a/b/g/n	Wi-Fi 802.11 b/g/n

Tabla 5.1: Características de los dispositivos empleados en la experimentación.

5.2 Descripción de la experimentación realizada

La experimentación se ha dividido en cuatro casos distintos. En el primero de ellos se busca la validación de la plataforma a nivel general, es decir, verificar que los módulos realizan sus funciones adecuadamente, lo cual se comprueba cuando las transmisiones y recepciones de mensajes se efectúan normalmente. En esta prueba, además, se ha explorado el impacto del utilizar diferentes intervalos de tiempo entre transmisiones.

En el segundo caso se realiza un análisis de las transmisiones con la finalidad de cuantificar el impacto del esquema de seguridad, con las implicaciones que representa (aumento de tamaño de los paquetes y tiempo de procesamiento para firma y verificación).

El tercer caso se enfoca en el análisis de la implentación de la técnica de agregación de paquetes, las adecuaciones al formato de los paquetes para su soporte, el impacto que genera sobre el tráfico en la red y el impacto sobre el tiempo de procesamiento en las operaciones del esquema de seguridad.

Por último, se ha evaluado la plataforma a diferentes distancias para observar la variación del retardo y pérdida de paquetes en diferentes escenarios (con y sin seguridad). Además, se ha implementado y validado un protocolo de diseminación, se obtienen los valores para las métricas observadas por sus autores y se utilizan ambos receptores GPS (externo y nativo) para observar su

impacto sobre el funcionamiento del protocolo.

En las siguientes secciones se describen los casos mencionados.

5.3 Validación de la plataforma

Para la validación del funcionamiento de la plataforma implementada se ha realizado experimentación con las dos tabletas separadas por una distancia determinada, transmitiendo un mensaje cada determinado tiempo hasta alcanzar el número de paquetes indicado en la interfaz de configuración. Estos valores de distancia e intervalos de transmisión son indicados más adelante, cuando se describa cada experimentación.

La experimentación contempla una fase previa en la que una computadora portátil actúa como la entidad confiable del esquema de seguridad CLS. Ésta se encarga de la generación de los parámetros públicos y las llaves privadas parciales de los nodos. Una vez generados, estos componentes son guardados en el almacenamiento de las tabletas emisor y receptor. Cabe mencionar que el proceso de hacer llegar estos datos a los nodos se asume que sucede bajo un canal de comunicación seguro [48]. Al iniciar la plataforma en las tabletas, éstas generan su par de llaves (pública y privada) a partir de los parámetros pre-cargados en sus tarjetas de memoria.

Como se ha mencionado, en la interfaz de configuración de pruebas el usuario indica la cantidad de paquetes a transmitir, el intervalo de generación de paquetes y si se trata de una prueba con o sin seguridad. En todas las pruebas, las tabletas se encuentran colocadas a una altura de aproximadamente 70 centímetros sobre el suelo y con el reverso hacia la otra tableta para obtener la mejor recepción de la señal. Además, en cada sesión de pruebas se colocan los dispositivos separados por cierta distancia (10, 20, 50 y 100 metros, por ejemplo). En la Figura 5.1 se ilustra lo anterior.

La primer sesión de pruebas se ha realizado sin considerar el esquema de seguridad para observar el comportamiento de las transmisiones utilizando diferentes intervalos de transmisión. En este caso, el escenario de pruebas ha considerado una separación de 10 metros entre ambos nodos, un total

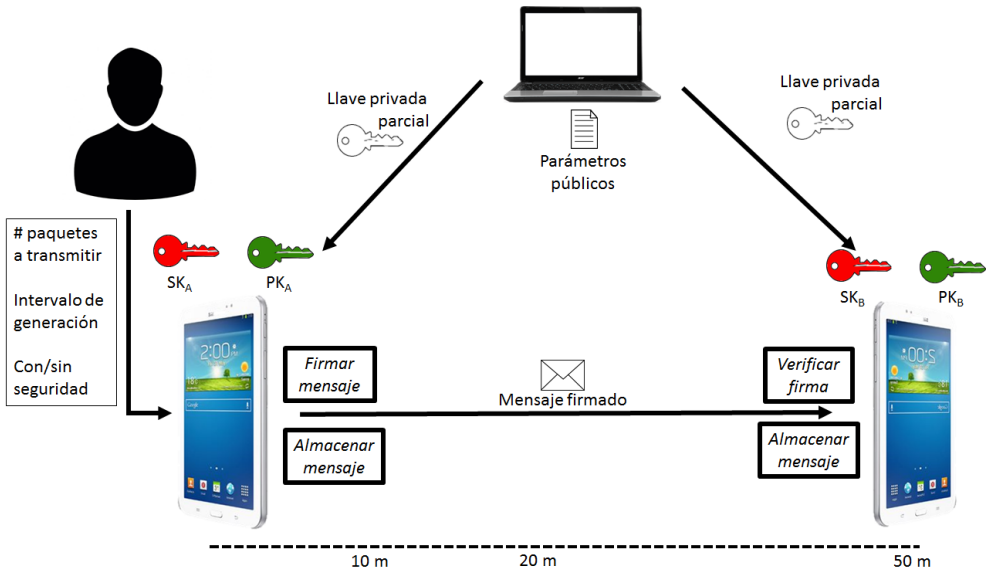

Figura 5.1: Escenario de pruebas realizadas.

de 3720 paquetes e intervalos de 5, 10 y 15 segundos. Se han efectuado transmisiones durante diez minutos, repitiendo este proceso 31 veces para validación estadística. Los resultados de esta experimentación se presentan en la Figura 5.2, donde se observa que el retardo no se ve afectado por el intervalo de transmisión utilizado. Por ello, se ha seleccionado el intervalo de 5 segundos para la realización de pruebas en adelante.

5.4 Análisis del impacto del esquema de seguridad

La plataforma implementa características para permitir la generación, transmisión y recepción de paquetes, los cuales pueden incluir campos con información de utilidad para el esquema de seguridad. En la subsección 5.4.1 se analiza el comportamiento de las transmisiones sin considerar el uso del esquema CLS. Por su parte, la subsección 5.4.2 incluye el análisis cuando los campos con información sobre la firma de los mensajes es incluido en los paquetes transmitidos.

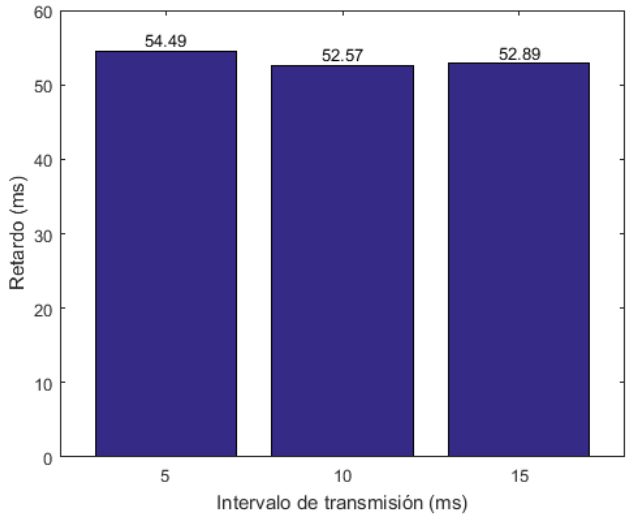

Figura 5.2: Retardo promedio en las transmisiones con distintos intervalos de transmisión a una distancia de 10 metros.

5.4.1 Comunicación sin seguridad

En este caso inicial, los paquetes son generados en la plataforma sin considerar campos del *overhead* atribuido a la información necesaria para el funcionamiento del esquema de seguridad. Esta composición para los paquetes es la considerada para el caso en que únicamente se comparten los identificadores del paquete y dispositivo, así como la información de ubicación del nodo emisor. En la Tabla 4.1 se ilustran los campos contenidos en los paquetes utilizados para este caso. Se observa un tamaño total de 79 bytes para los paquetes transmitidos.

Dado que la estructura de los paquetes utilizados es constante en tamaño, se puede calcular de manera analítica (sin necesidad de realizar experimentación en campo) la tasa de transmisión para diferentes intervalos entre las transmisiones. Esto se presenta en la Figura 5.3. En ella se observa una menor tasa a medida que el intervalo se fija en un valor mayor, esto debido a que entre menos frecuentes sean las transmisiones, menor será el flujo de datos por la red.

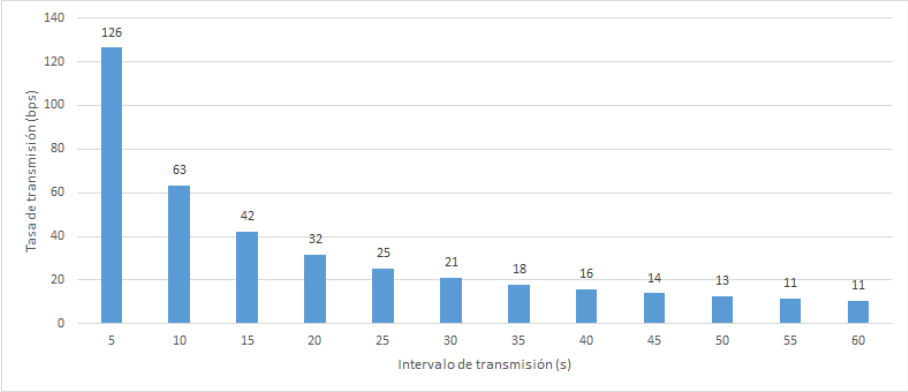

Figura 5.3: Tasa de transmisión a diferentes intervalos de tiempo.

5.4.2 Integración del overhead para el esquema de seguridad

La implementación del esquema de seguridad requiere de la inclusión de campos adicionales al paquete a transmitir, estos campos son los componentes de la firma digital sobre el mensaje que originalmente se genera para gestionar el esquema de comunicación, al cual denominamos carga útil (Tabla 4.1), así como la llave pública del vehículo que realiza dicha firma. En la Tabla 5.2 se muestra la estructura de los paquetes adaptada para gestionar el esquema de seguridad.

Campo	Descripción	Tipo de dato	Tamaño (bytes)
Carga útil	Campos de información del paquete	byte[]	79
U	Valor escalar obtenido por el esquema CLS	byte[]	128
v	Valor escalar obtenido por el esquema CLS	byte[]	128
pkV	Llave pública del nodo firmante	byte[]	128
IDv	Identificador del nodo firmante	byte[]	36
Total		499	

Tabla 5.2: Estructura del paquete generado en la plataforma incluyendo información para el esquema de seguridad CLE en su versión simétrica.

El tamaño de los componentes mostrados en la Tabla 5.2 cambia cuando se utiliza un enfoque asimétrico para los emparejamientos bilineales efectuados en el esquema de seguridad. En la Tabla 5.3 se muestra el tamaño para cada componente bajo dicho enfoque. Se puede apreciar que son valores inferiores a los presentados en el enfoque simétrico, ya que en este caso, el emparejamiento

se realiza con un elemento de cada grupo (G_1 *y* G_2), siendo de mayor tamaño elementos de G_2. Sin embargo, la versión asimétrica presenta una complejidad superior en sus operaciones, resultando en un tiempo de procesamiento elevado al integrar el esquema a la plataforma en Android, por lo tanto, se ha considerado el enfoque simétrico para la experimentación descrita en secciones siguientes.

Campo	Tipo de dato	Tamaño (bytes)
Carga útil	byte[]	79
U	byte[]	40
v	byte[]	80
pkV	byte[]	40
IDv	byte[]	36
Total		275

Tabla 5.3: Estructura del paquete generado en la plataforma incluyendo información para el esquema de seguridad CLE en su versión asimétrica.

El esquema de seguridad se basa en la generación y distribución de llaves en una etapa fuera de línea, mientras que en la etapa en línea se presentan únicamente operaciones de firma y verificación de mensajes. Este esquema trabaja sobre parámetros de una curva elíptica, además se realizan emparejamientos bilineales con elementos de los grupos definidos ($G_1 y G_2$) bajo un enfoque simétrico. En la Tabla 5.4 se muestra el tamaño de los elementos de cada grupo para los diferentes niveles de seguridad.

	Grupos		
Nivel de seguridad (bits)	G1	GT	Zr
80	128	128	36
112	256	256	40
128	512	512	56
192	768	768	64
256	1924	1924	96
	Tamaño de elementos (bytes)		

Tabla 5.4: Tamaño de los elementos involucrados en el esquema de seguridad basado en emparejamientos bilineales bajo el enfoque simétrico.

Con base en el tamaño total de los paquetes con la adición de los campos para seguridad, se presenta en la Figura 5.4 el análisis de la tasa de transmisión calculada de manera analítica para los diferentes intervalos de comunicación (utilizando un nivel de seguridad de 80 bits). En ella se puede observar una diferencia muy marcada al comparar este comportamiento con el que se presenta en las transmisiones sin consideraciones de seguridad. Esto introduce un segundo compromiso, esta vez para la tasa de transmisión y flujo de tráfico en la red contra el nivel de seguridad en el esquema de comunicaciones. Cabe mencionar que la solución empleada para la generación y verificación de las firmas digitales es basada en emparejamientos bilineales bajo un enfoque simétrico. Estos mecanismos pueden ser abordados desde un enfoque asimétrico, lo que reflejaría una disminución en el tamaño de los elementos involucrados en las operaciones de firma y verificación, disminuyendo también la tasa de transmisión y flujo en las transmisiones.

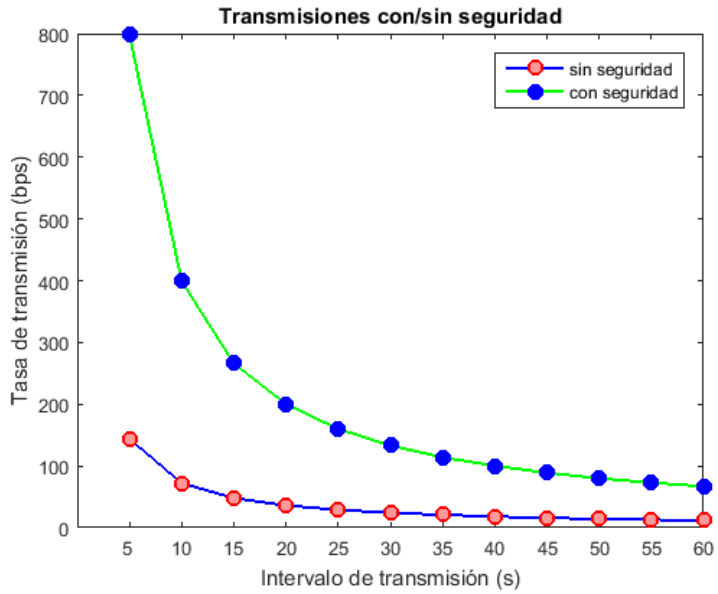

Figura 5.4: Tasa de transmisión a diferentes intervalos de tiempo considerando la inclusión de los campos para el esquema de seguridad (nivel de seguridad 80 bits).

En las Figura 5.5 se presentan las tasas de transmisión para los diferentes niveles de seguridad (tamaño de elementos en esquema de seguridad) en escala logarítmica. En ella se observa un incremento considerable conforme el nivel de seguridad aumenta. Este compromiso deberá

considerarse para la selección del nivel a utilizar para un tipo de prueba o integración futura, dependiendo del tipo de seguridad que la aplicación en trato demande, o bien, de la tolerancia al retardo en las transmisiones.

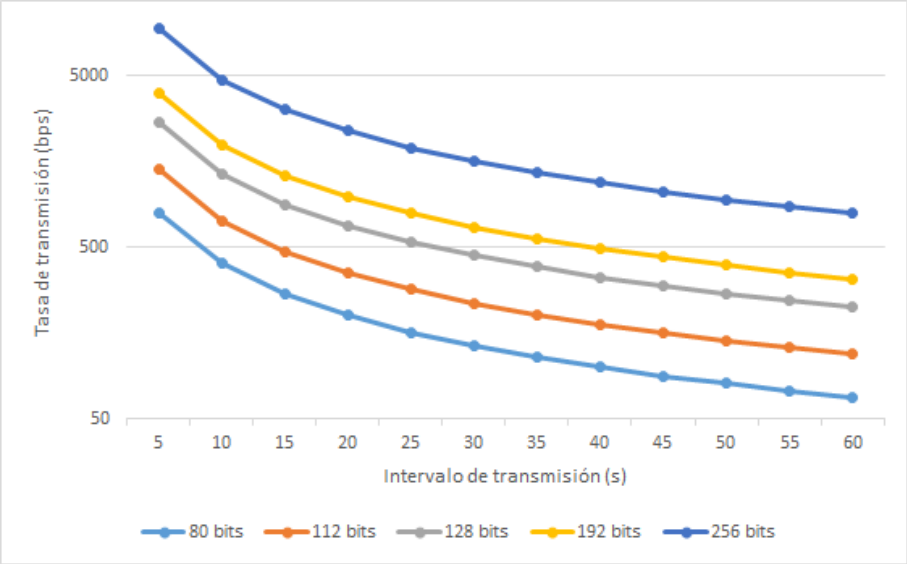

Figura 5.5: Tasa de transmisión a diferentes intervalos y niveles de seguridad (80, 112, 128, 192 y 256 bits).

5.4.3 Análisis de tiempo/espacio con la implementación del esquema de seguridad

Se han implementado dos enfoques para los emparejamientos bilineales del esquema de seguridad: simétrico y asimétrico. Las diferencias entre ellos se presentan en dos aspectos: el tamaño de los elementos que componen la firma (menor tamaño bajo el enfoque asimétrico) y el tiempo de procesamiento que toman las operaciones de firma y verificación (menor bajo el enfoque simétrico). Luego de las pruebas realizadas se han obtenido los valores de espacio y tiempo para los dos enfoques de seguridad. Mientras que los valores en espacio se mostraron en la Tabla 5.3, los tiempos de procesamiento se presentan en la Tabla 5.5.

Dada la naturaleza de las VANETs, en particular la movilidad de sus nodos (vehículos), se asume

	Tiempo para firma (ms)	Tiempo para verificación (ms)
Simétrico	1,302	3,309
Asimétrico	1,343	90,125

Tabla 5.5: Tiempo de procesamiento empleado bajo ambos enfoques de seguridad.

un corto periodo de vigencia para los mensajes transmitidos, por lo que el nivel de seguridad mínimo (80 bits) se ha seleccionado para el esquema de seguridad. Este esquema, presenta las dos operaciones principales utilizadas: firma y verificación de firma, las cuales involucran a su vez procesos para tratar con los valores manejados en las operaciones.

Con el objetivo de cuantificar el tiempo de procesamiento que cada operación implicada en el flujo global de la plataforma, se han realizado pruebas de generación y transmisión de paquetes. Se han obtenido los resultados que aparecen en la Tabla 5.6, para el caso del dispositivo generador/emisor de los mensajes y en la Tabla 5.7, cuando se trata del receptor. En estos resultados se observa que el proceso de generación de firma es prácticamente la única operación impactante en el emisor (99 % del tiempo de procesamiento), mientras que el resto de las operaciones tiene un tiempo de procesamiento casi despreciable (entre ellas incluida la operación de registro, que involucra escritura sobre un archivo). De manera similar, lo presentado en el dispositivo receptor, para el caso de la operación de verificación de firma.

	Construcción del mensaje	Conversión a bytes	Generación de firma	Registro de campos del mensaje	Salida a la interfaz	Cálculo de tiempos	Procesamiento total
Tiempo de procesamiento (ms)	1.56	2.16	1,514.43	4.43	0.83	0.75	1,524.16

Tabla 5.6: Tiempo de procesamiento para las operaciones de la arquitectura en la transmisión de mensajes (emisor).

Tras medir el tiempo de procesamiento empleado en las operaciones de ambas entidades participantes en la comunicación, se ha calculado el retardo promedio entre transmisión y recepción

	Reconstrucción del mensaje	Verificación de firma	Registro de campos del mensaje	Cálculo de tiempos	Procesamiento total
Tiempo de procesamiento (ms)	7.85	3,328.91	7.25	0.86	3,344.87

Tabla 5.7: Tiempo de procesamiento para las operaciones de la arquitectura en la recepción de mensajes (receptor).

de los mensajes. El retardo promedio calculado es de 62.63 ms. Por lo tanto, la suma de los retardos del emisor, receptor y transmisión, resulta en un tiempo total de procesamiento de 4,931.66 ms. En la Figura 5.6 se observa la diferencia del retardo que aportan los procedimientos de cada entidad y de transmisión al tiempo de procesamiento total de la arquitectura.

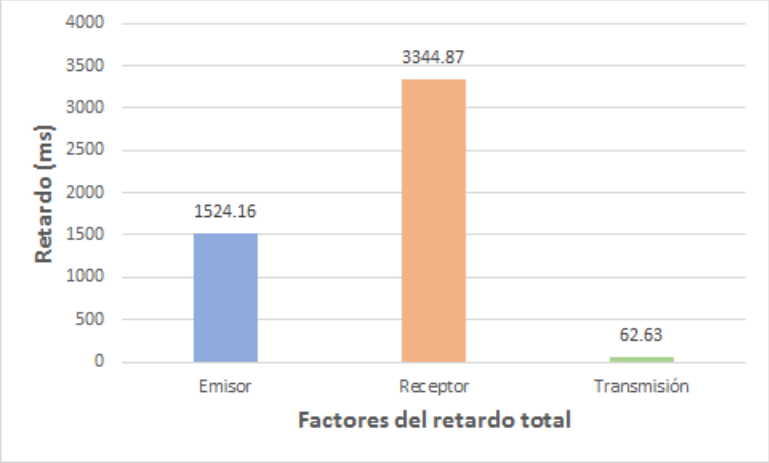

Figura 5.6: Tiempo de procesamiento empleado para los tres factores del retardo total.

5.5 Evaluación de técnica de agregación de paquetes

Como se explicó anteriormente, la técnica de agregación consiste en acumular paquetes generados y firmar el conjunto una vez alcanzado un número indicado de paquetes acumulados para entonces transmitir. En la Figura 5.7 se observa el impacto que tiene la utilización de esta técnica, en ella

se observa una gráfica con la tasa de transmisión (en escala logarítmica) de acuerdo al número de paquetes generados. Como se puede notar, se encuentra muy por encima el caso que no considera agregación, esto se atribuye a que los datos transmitidos en este caso, incluyen la firma del paquete en cada transmisión, a diferencia del enfoque con agregación.

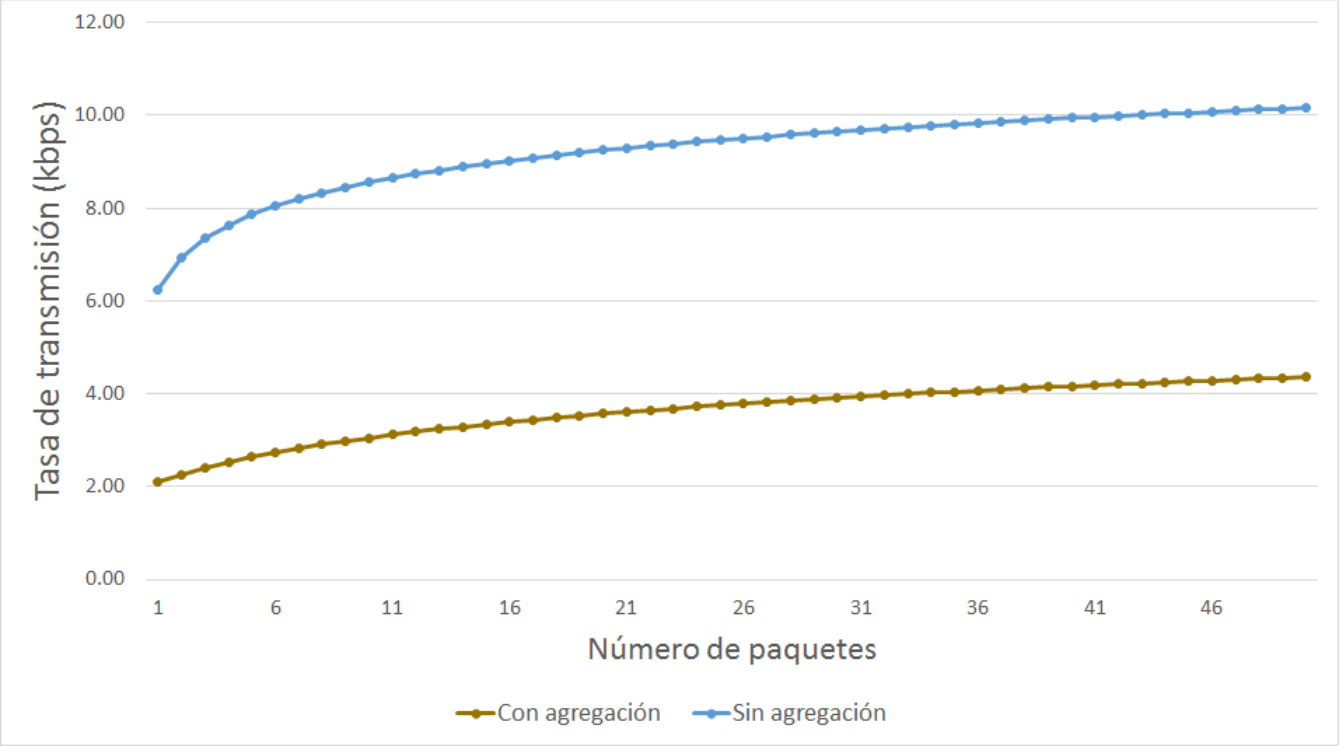

Figura 5.7: Comparativa de tasa de transmisión entre casos con y sin agregación.

Sin importar las combinaciones elegidas en base al compromiso entre nivel de seguridad y tasa de transmisión, las proporciones de la carga útil y *overhead* de los paquetes se conservan con mucho mayor peso en el *overhead*. Esto se traduce en múltiples transmisiones con un porcentaje poco significativo de información con utilidad para el esquema de comunicación, requiriendo sin embargo, mucho espacio en las comunicaciones para la gestión del esquema de seguridad. Ante esta situación se plantea el uso de un mecanismo de agregación de paquetes, esto es, en vez de generar un paquete cada determinado intervalo y transmitirlo, lo que se busca es acumular dichos paquetes generados y procediendo a su transmisión hasta alcanzado un tamaño que represente una proporción más

aceptable respecto al tamaño (fijo) necesario para el *overhead* de seguridad.

Para la implementación de esta alternativa de agregación, se necesita incluir en el paquete el número de cargas útiles que están incluidas en dicho paquete. Por ello, se ha añadido un campo al inicio de la estructura presentada en la Tabla 4.1, esta modificación ha sido considerada en la plataforma para la realización de experimentos, por lo que en cada prueba los paquetes generados tienen la estructura presentada en la Tabla 5.8 mostrada a continuación.

Campo	Tipo de dato	Tamaño (bytes)
# Aggr	int	4
Carga útil	byte[]	79
U	byte[]	128
v	byte[]	128
pkV	byte[]	128
IDv	byte[]	36
Total		503

Tabla 5.8: Estructura del paquete generado en la plataforma incluyendo información para el esquema de seguridad CLE en su versión asimétrica y adaptado para soporte a agregación de paquetes.

Se presenta entonces un tercer compromiso, en este caso entre la cantidad de paquetes agregados (que representa un aumento/disminución en el tráfico generado en la red y un ahorro de energía en el dispositivo) y el retardo en las transmisiones. Esto es: a mayor cantidad de paquetes agregados, menor tráfico de paquetes viajando por la red, pero mayor retardo en las comunicaciones. En la Figura 5.8 se presentan las tasas de transmisión para los diferentes niveles de seguridad conforme aumenta el número de paquetes agregados (L). En ella se observa el incremento en la tasa de transmisión con el comportamiento lineal esperado a medida que se agrega mayor cantidad de paquetes.

Cabe mencionar que el aumento en el tamaño de la carga útil con el uso de la técnica de agregación no repercute en el tiempo de procesamiento del esquema de seguridad. Esto ha sido comprobado con la realización de pruebas donde se han acumulado de 1 a 5 mensajes y se ha registrado el tiempo que toma realizar los procesos tal cual se tiene en las Tablas 5.6 y 5.7. Los resultados de esta experimentación se muestran en la Figura 5.9, donde se puede observar que el tiempo de

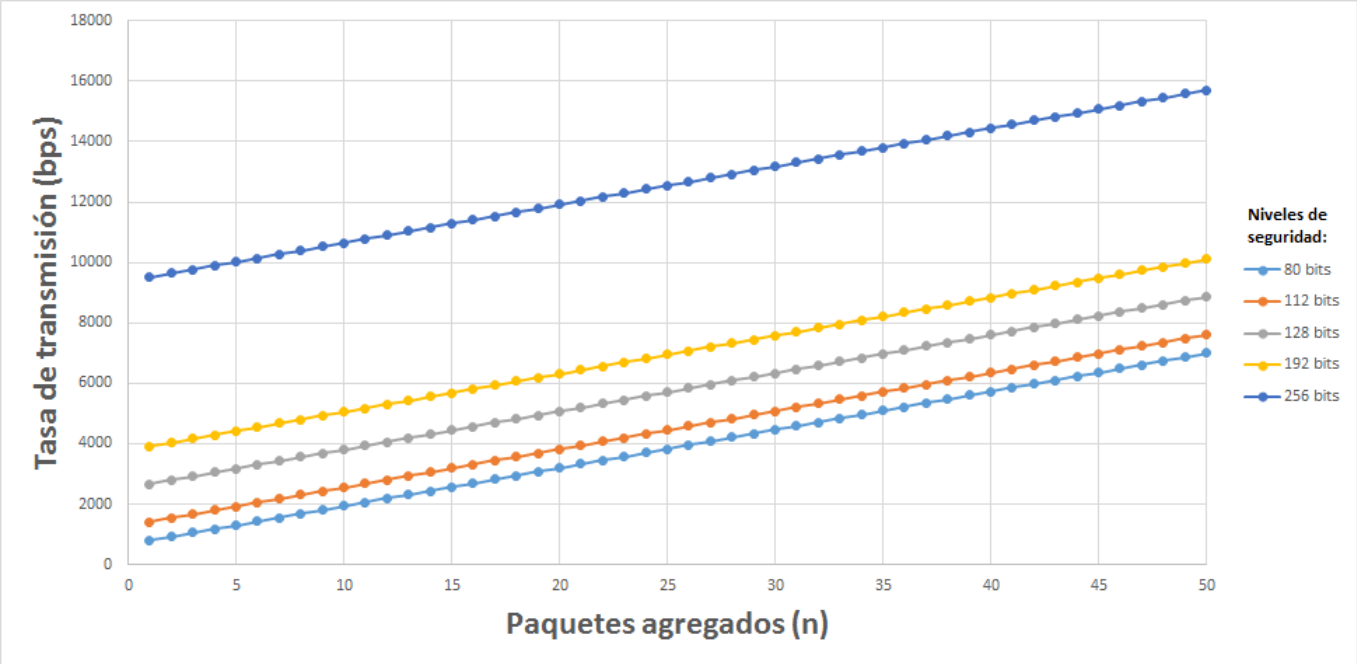

Figura 5.8: Tasa de transmisión para los diferentes niveles de seguridad conforme aumenta el número de paquetes agregados (n) en un intervalo de generación de paquetes (5 segundos).

procesamiento para las operaciones de firma y verificación no se ve afectado por el incremento en el tamaño de la carga útil que se firma/verifica. Esto se debe a que, en el esquema de seguridad, el mensaje representa al total de paquetes agregados. Se obtiene un resumen *hash* (de tamaño fijo) de dicho mensaje y es el que se utiliza en las operaciones de firma y verificación. Por lo tanto, sin importar cuántos paquetes hayan sido acumulados con la función de agregación, el resumen *hash* siempre mantiene el mismo tamaño.

5.6 Evaluación de protocolo de diseminación de mensajes con la plataforma

Se han realizado pruebas sin el esquema de seguridad para las transmisiones y otra sesión en la que sí se utiliza. El intervalo de transmisión se ha establecido en 5 segundos, mientras que el factor variante es la distancia (10, 20, 50 y 100 metros) de separación entre los nodos. Esta sesión de

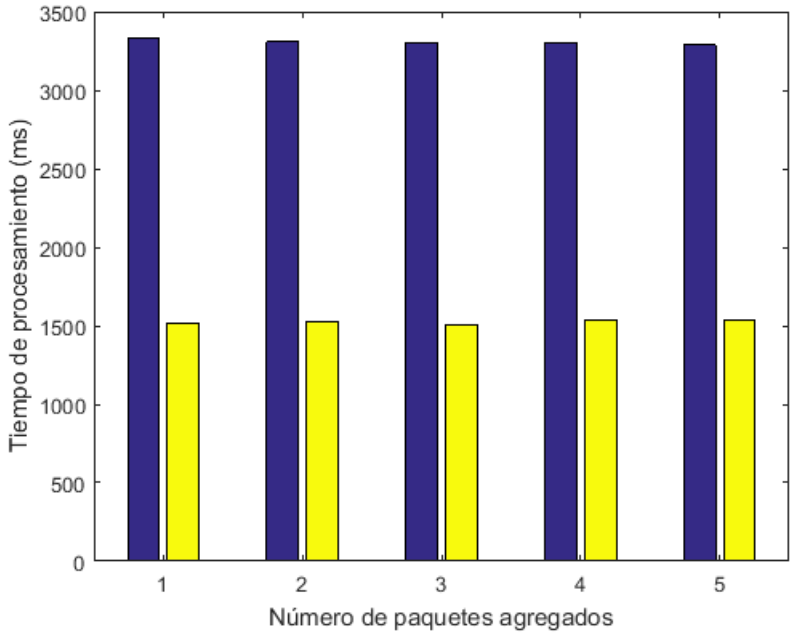

Figura 5.9: Tiempos de procesamiento para firma y verificación en casos con agregación de mensajes.

pruebas considera transmisiones (cada 5 segundos) durante diez minutos, efectuando 31 repeticiones, alcanzando un total de 3720 paquetes transmitidos por cada combinación distancia-aseguramiento. Cabe mencionar que debido a la falta de sincronización de los relojes de las tabletas utilizadas, para el cálculo del retardo se ha considerado el tiempo transcurrido desde la emisión de un paquete hasta la recepción de la confirmación de llegada de ese paquete de vuelta en el emisor (RTT).

En la Figura 5.10 se observa el retardo promedio en las transmisiones. El aumento del valor para esta métrica conforme la distancia de separación crece, es nuevamente un comportamiento esperado, ya que la señal requiere mayor tiempo de propagación para alcanzar esas distancias crecientes. Se observa además que en el caso de los paquetes transmitidos sin overhead de seguridad se tiene un retardo superior que cuando se utiliza el esquema de seguridad, esto se debe a que la tecnología Wi-Fi implementa de manera inherente un mecanismo de control de tráfico que emula el comportamiento de una cola de espera para la salida por la interfaz inalámbrica. Lo anterior significa que, a pesar de que el tamaño de los paquetes sin seguridad es menor, el mecanismo de control de tráfico les

da salida a la interfaz hasta haber alcanzada cierta cantidad mínima de bits a transmitir o bien, un tiempo máximo de espera. Los paquetes con overhead de seguridad son de mayor tamaño, por lo que alcanzan más rápidamente esa cantidad mínima de bits requerida y son enviados a la interfaz de salida primero. Esto resulta en retardos inferiores para el caso de transmisiones con overhead de seguridad. En estos experimentos, la desviación estándar del retardo en las transmisiones oscila entre 37.87 y 45.22 ms. Esta variación se debe al canal inalámbrico, donde las tasas de transmisión no son constantes y se presentan fenómenos que desvían la trayectoria de las transmisiones. Además, los tiempos de llegada de los paquetes transmitidos se ven afectados por la emisión de paquetes de confirmación de recepción (ACK), los cuales han sido necesarios para el cálculo del propio retardo (RTT).

En lo referente a la pérdida de paquetes, para el caso de transmisiones no aseguradas se presenta en la Figura 5.11, mientras que el caso con seguridad, en la Figura 5.12. En estas figuras se observa nuevamente un incremento, en la mayoría de los casos, conforme la distancia aumenta, lo cual es un efecto esperado. Sin embargo, el impacto del canal inalámbrico repercute en la pérdida de paquetes, que se ve acentuada en el caso sin seguridad.

El resumen de los resultados para retardo y pérdida de paquetes en la experimentación se presenta en la Tabla 5.9 para el caso sin seguridad y en la Tabla 5.10 para el caso con seguridad.

	Sin seguridad			
Distancia (m)	**RTT (ms)**	**Pérdida (%) Transmisión**	**Pérdida (%) Total**	**Pérdida (%) Retransmisión**
10	106.56	23.02	33.89	10.87
20	111.15	26.92	27.14	0.22
50	112.55	26.07	45.65	19.58
100	114.92	27.05	48.12	21.07

Tabla 5.9: Resultados de la experimentación al transmitir mensajes sin seguridad a diferentes distancias.

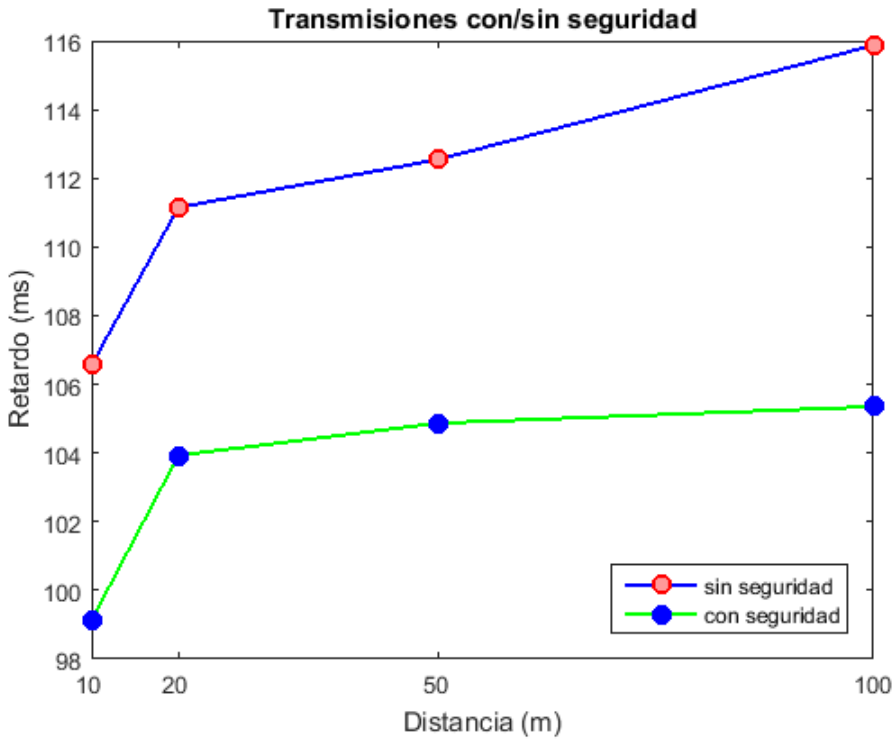

Figura 5.10: Retardo promedio en las transmisiones, con intervalo de transmisión de 5 segundos a diferentes distancias utilizando el esquema de seguridad sin certificados.

5.6.1 Validación del protocolo *Urban Multi-Hop Broadcast*

Uno de los principales objetivos de este trabajo es la utilización de la plataforma desarrollada para validar protocolos de diseminación. Como se ha puntualizado a lo largo de este documento, el alcance de la plataforma es la familia de protocolos basados en la ubicación de los nodos de la red. Como se ha presentado en la Sección 3.1, existen protocolos de diseminación *broadcast* que adoptan características de aquellos basados en localización (los nodos envían información con su ubicación). Por esta característica y por la simplicidad de implementación de los protocolos *broadcast*, se han analizado algunos de ellos con la finalidad de identificar sus principales características y seleccionar uno a implementar. Éstas se presentan en la Tabla 5.11, donde son presentadas como solución para cumplir con los objetivos en común de los protocolos de diseminación *broadcast*. Además, las funcionalidades de la plataforma hacen posible la implementación de tales características.

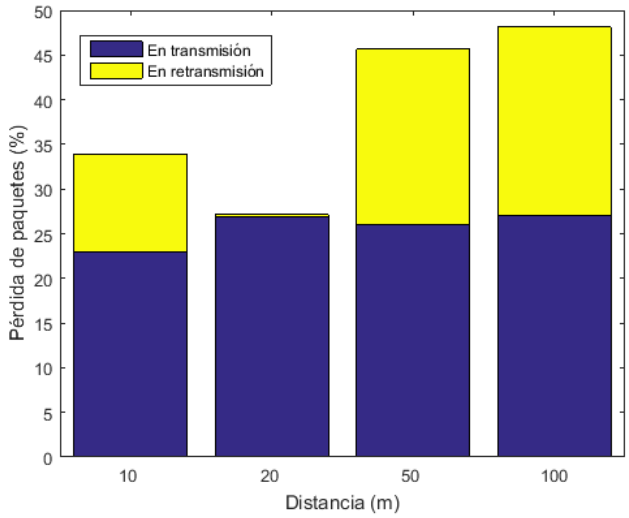

Figura 5.11: Pérdida de paquetes promedio en las transmisiones con intervalo de transmisión de 5 segundos a diferentes distancias sin utilizar el esquema de seguridad.

	Con seguridad			
Distancia (m)	**RTT (ms)**	**Pérdida (%) Transmisión**	**Pérdida (%) Total**	**Pérdida (%) Retransmisión**
10	99.13	5.75	29.08	23.33
20	103.93	19.37	39.46	20.09
50	104.87	10.63	33.77	23.14
100	105.35	13.31	45.10	31.79

Tabla 5.10: Resultados de la experimentación al transmitir mensajes con seguridad a diferentes distancias.

Se ha seleccionado e implementado el protocolo *broadcast* multi-salto urbano (UMB [38]), diseñado por *Korkmaz et al*. Las características implementadas de este protocolo son:

- **Selección de nodos retransmisores**

  Uno de los principales problemas en los protocolos de diseminación *broadcast*, específicamente con el método de inundación, es el uso irracional del canal de comunicación, lo cual provoca colisiones en las transmisiones y redundancia en los mensajes propagados, pues todos los nodos transmiten al mismo tiempo y transmiten la misma información en ocasiones. Por ello, antes de iniciar la transmisión de mensajes de alerta, el emisor envía una señal (RTB) a todos los nodos

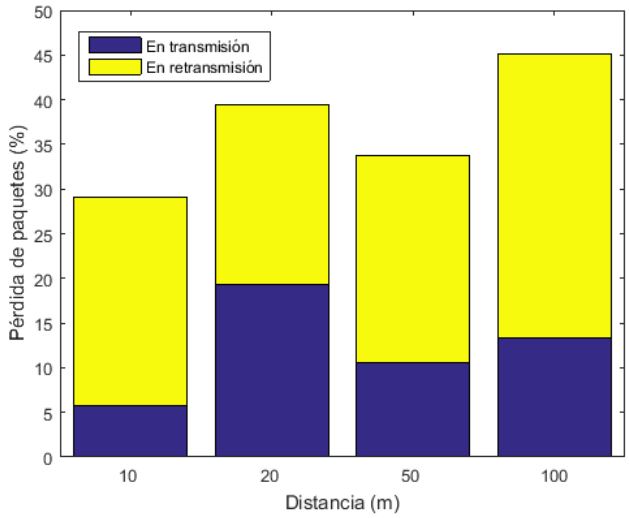

Figura 5.12: Pérdida de paquetes promedio en las transmisiones con intervalo de transmisión de 5 segundos a diferentes distancias utilizando el esquema de seguridad.

Objetivo	Solución	Soporte en la plataforma	Protocolos broadcast (GPS)
Evitar colisiones	Selección de nodos retransmisores	Sí	UMB [38] SB [51] TSM [7] PRP [52]
Uso del canal de comunicación	RTB/CTB	Sí	
Confiabilidad en las transmisiones	Paquetes ACK	Sí	

Tabla 5.11: Características de los protocolos de diseminación *broadcast* que utilizan la ubicación de los vehículos.

dentro de su rango de cobertura para manifestar su intención de transmitir. RTB incluye la ubicación del emisor. Cuando esta señal es recibida por otro nodo, éste (conociendo su propia ubicación) calcula la distancia hacia el emisor.

Posteriormente, el receptor emite una señal (*black burst*) que actúa como auxiliar en la reservación del canal. La distancia calculada anteriormente es utilizada para calcular la duración del *black burst*: a mayor distancia, mayor duración. Este procedimiento es efectuado por todos los nodos que recibieron el RTB. Al término de la emisión del *black burst*, el nodo sensa el canal; si éste se encuentra ocupado (aún se está transmitiendo el *black burst* de otro nodo),

termina su labor en esta sesión del proceso. De lo contrario, significa que éste ha sido el nodo que transmitió un *black burst* por más tiempo, siendo también el nodo más lejano al receptor. Cuando se cumple el segundo caso, dicho nodo procede emitiendo una señal (CTB), misma que, al ser recibida por el nodo emisor inicial, indica que se ha identificado el nodo retransmisor.

- **Proveer confiabilidad a las transmisiones**

  Una vez conocido el nodo que ha sido seleccionado como retransmisor, el emisor original procede a enviar los mensajes de alerta (por ejemplo) y únicamente el nodo retransmisor es el responsable de hacer llegar la información a nodos fuera del rango de cobertura del emisor. Cuando los nodos reciben los mensajes de alerta, emiten un mensaje de confirmación de recepción: ACK. De esta manera el emisor tiene certeza de que el mensaje ha sido recibido por el nodo destino.

La implementación de este protocolo en la plataforma es validada siguiendo la metodología presentada en la Figura 5.13. La experimentación se ha realizado con los mismos dispositivos previamente descritos (Sección 5.6). Se han considerado cuatro escenarios de prueba, variando el receptor GPS (nativo y externo) empleado y el tipo de transmisiones (con y sin seguridad) a un intervalo de 5 segundos. En estas pruebas no se ha considerado agregación de paquetes.

Se colocaron las tabletas Galaxy Note a 25 y 30 metros (denotados como nodo B y C, respectivamente) del teléfono Galaxy Grand Prime (nodo A). La experimentación consistió en el envío de mensajes desde el nodo A (emisor) hacia los nodos B y C (receptores). Las métricas utilizadas para analizar el desempeño se describen a continuación.

- Recepción exitosa: Relación entre el número de vehículos que conforman la red y el número de vehículos que recibieron los mensajes transmitidos.

- Velocidad de diseminación de los mensajes: Es calculada dividiendo la distancia que ha recorrido un paquete entre el retardo para llegar a ese punto.

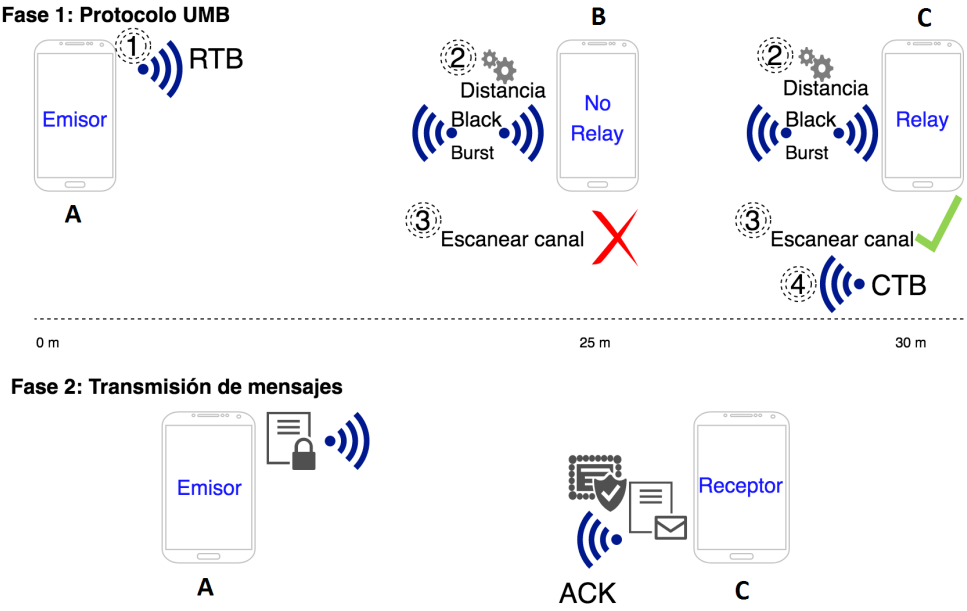

Figura 5.13: Escenario de pruebas con el protocolo UMB.

- Carga generada por paquete broadcast: Número total de bits transmitidos para diseminar un paquete a toda la red. Se obtiene el promedio dividiendo el total de bits enviados entre el número total de paquetes *broadcast* transmitidos.

- Error en selección de nodo retransmisor: Promedio de equivocaciones al seleccionar el nodo encargado de retransmitir los mensajes *broadcast*.

- Retardo (RTT): Tiempo transcurrido desde la emisión de un paquete hasta la llegada de la confirmación de recepción de dicho mensaje de vuelta al emisor.

- Périda de paquetes: Porcentaje de paquetes emitidos por el receptor que no fueron recibidos por su contraparte.

En la Tabla 5.12 se presentan los resultados obtenidos de esta experimentación para el caso de las métricas que considera el protocolo UMB. En ella se observa una recepción exitosa que no alcanza el cien por ciento, esto debido a lo reducido del número de nodos utilizados en las pruebas ya que se consideraron solamente tres nodos receptores, por lo que, si uno de ellos no recibía un mensaje,

disminuye considerablemente el valor para esta métrica. Por su parte, la velocidad de diseminación promedio ha sido cuantificada en el nodo más lejano (retransmisor), el cual se ha situado a 30 metros de distancia con respecto al emisor. Se observa un valor muy cercano en todos los casos, ya que el factor de retardo se vio modificado de un caso a otro, sin embargo su variación fue mínima debido a que en todos los experimentos se conservó la misma separación de 30 metros entre emisor y receptor/retransmisor. La carga generada en la red por paquete transmitido toma un valor mayor en los casos con seguridad, pues un factor que la determina es el número total de paquetes que se propagaron por la red y, como se puede observar, la pérdida de paquetes presentada es elevada cuando se implementa el esquema CLS debido al aumento del tamaño de los paquetes transmitidos.

Adicionalmente, se han observado métricas que permiten evaluar el desempeño de la plataforma: el porcentaje de error que se presenta en la selección del nodo retransmisor y la pérdida de paquetes en diferentes segmentos de la red. Como se observa en la Tabla 5.13, en el caso donde se consideraron las lecturas de ubicación del GPS externo, se presentó una tasa de error menor. Esto se atribuye al cálculo de la distancia que se requiere en la operación del tiempo que dura la transmisión del *Black Burst* según el protocolo de diseminación UMB. Esto indica que la precisión del sensor externo se ha probado mayor que la del sensor nativo ya que, utilizando el nativo, en un número mayor de ocasiones, la distancia calculada entre los nodos A y B resultó ser mayor a la distancia entre los nodos A y C. Esto provocó que el nodo más alejado del receptor no fuera elegido como el nodo retransmisor, comportamiento contrario a lo esperado. Por su parte, la pérdida de paquetes presenta los valores más elevados en las transmisiones del nodo C hacia el nodo A, seguido de aquellas del nodo A al nodo B, mientras que las del nodo B al nodo C presentan los valores más bajos. Lo anterior se debe a la distancia de separación entre estos nodos, 30, 25 y 5 metros, respectivamente.

Sensor GPS	Seguridad	Recepción exitosa (%)	Velocidad de diseminación (m/s)	Carga generada por paquete (bits)
Nativo	No	79.13	779.16	1754.49
	Si	57.94	582.62	10264.78
Externo	No	90.36	583.03	1722.13
	Si	85.21	671.79	10820.89

Tabla 5.12: Resultados para las métricas consideradas por el protocolo UMB.

Sensor GPS	Seguridad	Error en selección de nodo retransmisor (%)	Pérdida de paquetes A ->B (%)	Pérdida de paquetes B ->C (%)	Pérdida de paquetes C ->A (%)
Nativo	No	53.13	19.41	17.22	25.97
	Si	84.38	17.13	12.80	21.24
Externo	No	40.63	8.18	7.42	13.32
	Si	65.63	6.12	4.78	33.46

Tabla 5.13: Resultados para las métricas consideradas para analizar el rendimiento de la plataforma.

5.7 Integración de nuevos protocolos de diseminación de mensajes en la plataforma

Es importante mencionar que la experimentación ha considerado únicamente la validación de un protocolo de diseminación para VANETs (protocolo UMB). Sin embargo, como se ha descrito a lo largo de este documento, se han considerado las características de la familia de protocolos *broadcast* basados en ubicación para el diseño de la plataforma (criterios de selección de nodos retransmisores y cálculo de distancias, principalmente). Debido a esto, la plataforma permite la validación de otros protocolos pertenecientes a esta familia. Adicionalmente, una consideración para estas validaciones es la infraestructura (principalmente el número de nodos en la red) necesaria para que el prototipo de VANET se aproxime a los escenarios en los que dichos protocolos han sido evaluados en simulaciones.

La integración de un nuevo protocolo a la plataforma, por ejemplo, el protocolo TSM (listado en la Tabla 5.11) sería posible sin necesidad de adecuaciones a la plataforma. Lo anterior debido a que, como se muestra en la Tabla 5.14, este protocolo, al ser de la misma familia, implementa características muy similares a las de UMB para su funcionamiento. A nivel de implementación esto se puede ver como la existencia de una clase abstracta, cuyos métodos deben ser implementados según la lógica de cada protocolo, con la capacidad de añadir los que sean necesarios para integrar el nuevo protocolo.

Objetivo	Solución	Características	Soporte en la plataforma
Evitar colisiones	Selección de nodos retransmisores	División de la vialidad en segmentos	Sí
		Mecanismo de selección de líder de segmento	Sí
Uso del canal de comunicación	RTB/CTB	Asignación de bloques de tiempo separados para la diseminación multi-hop de mensajes de alerta	Sí
		Reservación del canal de comunicación	Sí
Confiabilidad en las transmisiones	Confirmación de recepción de mensajes	Envío de mensajes de confirmación (ACK)	Sí

Tabla 5.14: Características del protocolo de diseminación TSM soportadas en la plataforma.

En la Tabla 5.15 se muestra una comparativa entre los métodos necesarios para la implementación de los protocolos UMB y TSM. En ella se observa que la mayoría de los métodos coincide para ambos casos, debido a que pertenecen a la misma familia (protocolos *broadcast* basados en ubicación).

UMB	TSM
sendRTB() sendBlackBurst() sendCTB() sendACK() senseChannel() calculateDistance() getCurrentDateTime()	sendBlackBurst() sendCLEAR() sendACK() senseChannel() calculateDistance() getCurrentDateTime()

Tabla 5.15: Métodos necesarios para la implementación de los protocolos UMB y TSM.

El procedimiento para incluir un nuevo protocolo de diseminación de mensajes se puede resumir en los siguientes pasos.

1. Identificar e implementar los métodos comunes que presenta la clase abstracta.

2. Verificar que las entradas y salidas de los nuevos métodos necesarios coincida con los de la plataforma.

3. Implementar los métodos adicionales que sean necesarios para el funcionamiento del nuevo protocolo.

5.8 Resumen

En esta sección se han definido los escenarios y métricas de evaluación. Se han evaluado las características de la plataforma, iniciando por explorar las diferencias en tamaño de los paquetes generados cuando se considera o no, el añadir los campos de la firma digital. Se analizaron las diferencias en tiempo de procesamiento de los diferentes esquemas de seguridad, seleccionando el enfoque simétrico como el menos costoso en términos de tiempo de procesamiento, que se traduce en tiempo de respuesta para las aplicaciones. De igual manera se justificó la implementación de la característica de agregación de paquetes, pues el acumular paquetes hasta obtener una carga útil mucho mayor al original, no tiene un impacto significativo sobre el tiempo de firma del

esquema de seguridad, ya que se obtiene un resumen *hash* sobre el carga útil total (n paquetes agregados) y con éste se realizan las operaciones del esquema de seguridad. Además, se exploró el comportamiento de las transmisiones vía inalámbrica a diferentes distancias, observando en su mayoría un comportamiento proporcional entre el incremento de distancia y pérdida de paquetes. La validación de la plataforma ha sido complementada con la implementación de un protocolo de diseminación, el cual ha sido evaluado bajo condiciones controladas, con un número reducido de nodos (una red de 3 nodos).

6

Conclusiones y trabajo futuro

En este capítulo se presentan las conclusiones y aportes de esta investigación. Además, se mencionan las actividades con las que se puede dar seguimiento a la misma, para así complementar el trabajo.

6.1 Conclusiones

En la presente tesis se ha propuesto una plataforma que integra características de comunicación, obtención de ubicación y seguridad informática para las transmisiones que realiza. Esta plataforma ha sido diseñada para que pueda dar soporte a implementaciones de protocolos de diseminación basados en ubicación y puedan ser validados en escenarios reales mediante la generación de un entorno de pruebas basado en dispositivos móviles inteligentes.

La plataforma desarrollada ha sido validada a nivel de bloques, donde se han analizado sus características principales y secundarias para después ser validada en escenarios reales controlados, variando aspectos como distancia y configuraciones de seguridad, observando métricas de retardo y

pérdida de paquetes durante las transmisiones. Mediante la investigación realizada se confirma que las capacidades de los dispositivos móviles actuales permiten la implementación de una plataforma capaz de realizar comunicaciones según los requerimientos de las VANETs, así como la validación de protocolos de diseminación para este tipo de redes. Se comprueba el funcionamiento de la plataforma desarrollada con la realización de transmsiones y el análisis de las métricas de retardo y pérdida de paquetes, cuyos valores presentan un comportamiento esperado en virtud del incremento en la distancia de separación entre los nodos.

Se ha cuantificado el impacto del esquema de seguridad sobre los paquetes generados y las transmisiones en términos de tiempo de procesamiento y tamaño de los paquetes transmitidos. En este sentido, se ha identificado un compromiso entre el aseguramiento en las comunicaciones y el tiempo de respuesta para las aplicaciones, el cual refleja el tiempo de procesamiento necesario para las operaciones de firma y verificación. Se han desarrollado dos enfoques (simétrico y asimétrico) para los emparejamientos bilineales con la finalidad de explorar el comportamiento que presentan en cuanto al tiempo de procesamiento en las operaciones del esquema de seguridad CLS. Con esto se ha identificado que enfoque el simétrico presenta mayor tamaño en sus componentes, sin embargo, ofrece menor tiempo de procesamiento que el enfoque asimétrico.

La integración del receptor GPS externo ha permitido confirmar que se requiere de receptores GPS con mayores prestaciones en cuanto a frecuencia y precisión en la adquisición de la ubicación para validar protocolos de diseminación *broadcast* basados en ubicación. Lo anterior debido a que el funcionamiento del protocolo evaluado en la plataforma resultó beneficiado con la precisión que el receptor GPS externo ofrece, obteniendo menor tasa de error en la selección de nodos retransmisores al utilizar este sensor.

6.2 Contribuciones

Con este trabajo de tesis se ha obtenido una plataforma móvil que permite la evaluación de protocolos de diseminación *broadcast* que incluyen la información de ubicación de los nodos en los paquetes transmitidos. Esta plataforma implementa un esquema de seguridad que no requiere certificados para su funcionamiento, el cual se centra en las operaciones de firma y verificación de los mensajes. Integra, además, un sensor GPS externo vía Bluetooth con mayor precisión que el sensor nativo de los dispositivos empleados en la experimentación, lo cual mejora el rendimiento de los protocolos de diseminación soportados.

6.3 Dificultades y limitaciones

La API de Android para comunicaciones y gestión de redes inalámbricas no ofrece soporte para el modo ad-hoc simple. Por ello, la selección de la tecnología para las comunicaciones realizadas con la plataforma concluyó en la implementación de la tecnología Wi-Fi P2P. Esta tecnología implica una organización jerárquica para los nodos de la red: propietario del grupo y cliente en el grupo.

Este trabajo de tesis involucra labores de implementación y experimentación con la plataforma desarrollada, por lo que una limitación importante es la infraestructura disponible para la formación de un entorno de pruebas. El reducido número de dispositivos móviles con los que se ha realizado la experimentación ha permitido validar la solución en escenarios controlados, sin embargo, para permitir extender dichos escenarios se requiere de más dispositivos.

De igual manera, la validación de la plataforma se ha efectuado en escenarios sin movilidad, sin embargo, emular el movimiento de los nodos en una VANET requiere del uso de automóviles y personal que los conduzca. Esto debe ser tomado en cuenta si se desea evaluar protocolos en escenarios con movilidad. Para este trabajo se ha podido prescindir de esto ya que el protocolo UMB permite que se trabaje con escenarios estáticos.

La experimentación para este proyecto se ha realizado en un ambiente real, por lo que la preparación del entorno y dispositivos en cada sesión de prueba implica un tiempo invertido considerable. Además, la duración de las pruebas y el área en que se han llevado a cabo han requerido frecuente monitoreo de los dispositivos y condiciones del entorno.

Finalmente, la obtención del valor para algunas de las métricas analizadas requiere del cálculo del retardo en las transmisiones. Sin embargo, para el cálculo exacto de esta métrica se requiere de una sincronización de los relojes de los dispositivos empleados en la experimentación. Por esta restricción fue necesario el medir este retardo en términos de RTT y no de E2ED.

6.4 Trabajo futuro

Una de las características principales de esta tesis es la implementación de un esquema de seguridad para garantizar los servicios de integridad y autenticación mediante el mecanismo de firma digital. Sin embargo, las operaciones que se realizan para dicho esquema requieren de un tiempo considerable de procesamiento. Lo anterior impacta en el tiempo de respuesta de las aplicaciones que trabajen, en determinado momento, sobre la plataforma. Por ello es importante analizar el esquema implementado y trabajar en la reducción del tiempo necesario para dichas operaciones. O bien, buscar alternativas al esquema.

La experimentación es parte también importante de este trabajo, por lo que la exploración de nuevos y más complejos escenarios de prueba es una tarea relevante en aras de complementar las capacidades de la plataforma y ofrecer mejores características a futuras implementaciones de protocolos de diseminación sobre ésta.

Anexos

A

Diagrama de despliegue UML de la plataforma

Las entidades participantes en el despliegue de la plataforma y los componentes de cada una de ellas son presentados en la siguiente figura. En ella se observa el flujo de interacción entre dichos componentes y las vías de comunicación entre las entidades.

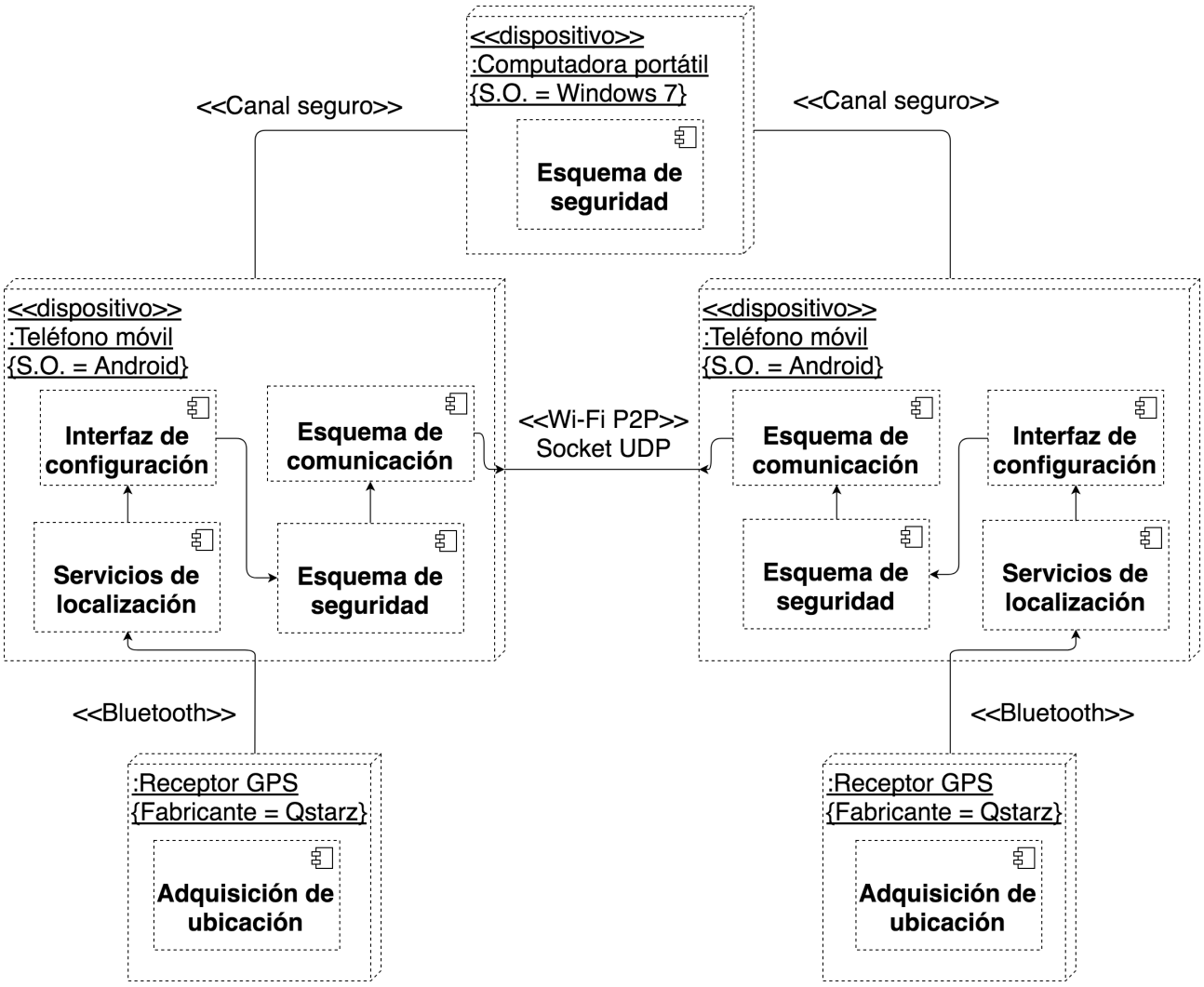

Figura A.1: Diagrama UML de despliegue de la plataforma.

Bibliografía

[1] Elyes Ben Hamida, Hassan Noura, and Wassim Znaidi. Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures. *Electronics*, 4(3):380–423, 2015.

[2] Y. Toor, P. Muhlethaler, A. Laouiti, and A. D. La Fortelle. Vehicle ad hoc networks: applications and related technical issues. *IEEE Communications Surveys Tutorials*, 10(3):74–88, Third 2008.

[3] F-Y Wang, Charles Herget, and Deze Zeng. Guest editorial developing and improving transportation systems: the structure and operation of ieee intelligent transportation systems society. *IEEE Transactions on Intelligent Transportation Systems*, 6(3):261–264, 2005.

[4] Lino Figueiredo, Isabel Jesus, JA Tenreiro Machado, J Ferreira, and JL Martins de Carvalho. Towards the development of intelligent transportation systems. In *Intelligent transportation systems*, volume 88, pages 1206–1211, 2001.

[5] Richard J Weiland and Lara Baughman Purser. Intelligent transportation systems. *Transportation in the new millennium*, 2000.

[6] Anthony D Joseph, Alastair R Beresford, Jean Bacon, David N Cottingham, Jonathan J Davies, Brian D Jones, Haitao Guo, Wei Guan, Yong Lin, Houbing Song, et al. Intelligent transportation systems. *IEEE Pervasive Computing*, 5(4):63–67, 2006.

[7] Muhammad Awais Javed, Duy Trong Ngo, and Jamil Yusuf Khan. A multi-hop broadcast protocol design for emergency warning notification in highway vanets. *Eurasip journal on wireless communications and networking*, 2014(1):1–15, 2014.

[8] Hannes Hartenstein, Bernd Bochow, André Ebner, Matthias Lott, Markus Radimirsch, and Dieter Vollmer. Position-aware ad hoc wireless networks for inter-vehicle communications: the fleetnet project. In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, pages 259–262. ACM, 2001.

[9] Wim Vandenberghe, Ingrid Moerman, and Piet Demeester. On the feasibility of utilizing smartphones for vehicular ad hoc networking. In *ITS Telecommunications (ITST), 2011 11th International Conference on*, pages 246–251. IEEE, 2011.

[10] Scott J Weiner. Feasibility of a 802.11 vanet based car accident alert system. *Northeastern University*, 2010.

[11] Sergio M Tornell, Carlos T Calafate, Juan-Carlos Cano, Pietro Manzoni, Manuel Fogue, and Francisco J Martinez. Evaluating the feasibility of using smartphones for its safety applications. In *Vehicular Technology Conference (VTC Spring), 2013 IEEE 77th*, pages 1–5. IEEE, 2013.

[12] Wim Vandenberghe, Ingrid Moerman, and Piet Demeester. On the feasibility of utilizing smartphones for vehicular ad hoc networking. In *ITS Telecommunications (ITST), 2011 11th International Conference on*, pages 246–251. IEEE, 2011.

[13] Yu Wang and Fan Li. *Vehicular Ad Hoc Networks*, pages 503–525. Springer London, London, 2009.

[14] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, and Aamir Hassan. Vehicular ad hoc networks (vanets): status, results, and challenges. *Telecommunication Systems*, 50(4):217–241, 2012.

[15] F. Li and Y. Wang. Routing in vehicular ad hoc networks: A survey. *IEEE Vehicular Technology Magazine*, 2(2):12–22, June 2007.

[16] Rex Chen, Wen-Long Jin, and Amelia Regan. Broadcasting safety information in vehicular networks: issues and approaches. *IEEE network*, 24(1):20–25, 2010.

[17] Felipe Domingos Da Cunha, Azzedine Boukerche, Leandro Villas, Aline Carneiro Viana, and Antonio AF Loureiro. *Data communication in VANETs: a survey, challenges and applications*. PhD thesis, INRIA Saclay; INRIA, 2014.

[18] Fouad Tobagi and Leonard Kleinrock. Packet switching in radio channels: part ii–the hidden terminal problem in carrier sense multiple-access and the busy-tone solution. *IEEE Transactions on communications*, 23(12):1417–1433, 1975.

[19] Zhenghua Fu, Xiaoqiao Meng, and Songwu Lu. How bad tcp can perform in mobile ad hoc networks. In *Computers and communications, 2002. Proceedings. ISCC 2002. Seventh international symposium on*, pages 298–303. IEEE, 2002.

[20] Marc Bechler, Sven Jaap, and Lars Wolf. An optimized tcp for internet access of vehicular ad hoc networks. *NETWORKING 2005. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems*, pages 869–880, 2005.

[21] Jian Liu and Suresh Singh. Atcp: Tcp for mobile ad hoc networks. *IEEE Journal on selected areas in communications*, 19(7):1300–1315, 2001.

[22] Yu-Chee Tseng, Sze-Yao Ni, Yuh-Shyan Chen, and Jang-Ping Sheu. The broadcast storm problem in a mobile ad hoc network. *Wireless networks*, 8(2/3):153–167, 2002.

[23] Anna Maria Vegni, Mauro Biagi, and Roberto Cusani. Smart vehicles, technologies and main applications in vehicular ad hoc networks. In Lorenzo Galati Giordano and Luca Reggiani, editors, *Vehicular Technologies - Deployment and Applications*, chapter 01. InTech, Rijeka, 2013.

[24] J. Jakubiak and Y. Koucheryavy. State of the art and research challenges for vanets. In *2008 5th IEEE Consumer Communications and Networking Conference*, pages 912–916, Jan 2008.

[25] Marco Di Felice, Rahman Doost-Mohammady, Kaushik R Chowdhury, and Luciano Bononi. Smart radios for smart vehicles: cognitive vehicular networks. *IEEE Vehicular Technology Magazine*, 7(2):26–33, 2012.

[26] Guillaume Remy, Sidi-Mohammed Senouci, François Jan, and Yvon Gourhant. Lte4v2x: Lte for a centralized vanet organization. In *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, pages 1–6. IEEE, 2011.

[27] Sandor Dornbush and Anupam Joshi. Streetsmart traffic: Discovering and disseminating automobile congestion using vanet's. In *Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th*, pages 11–15. IEEE, 2007.

[28] Ottmar Gehring and Hans Fritz. Practical results of a longitudinal control concept for truck platooning with vehicle to vehicle communication. In *Intelligent Transportation System, 1997. ITSC'97., IEEE Conference on*, pages 117–122. IEEE, 1997.

[29] T. L. Willke, P. Tientrakool, and N. F. Maxemchuk. A survey of inter-vehicle communication protocols and their applications. *IEEE Communications Surveys Tutorials*, 11(2):3–20, Second 2009.

[30] Jeremy Blum and Azim Eskandarian. The threat of intelligent collisions. *IT professional*, 6(1):24–29, 2004.

[31] Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. Survey on vanet security challenges and possible cryptographic solutions. *Vehicular Communications*, 1(2):53–66, 2014.

[32] Nicholas D Lane, Emiliano Miluzzo, Hong Lu, Daniel Peebles, Tanzeem Choudhury, and

Andrew T Campbell. A survey of mobile phone sensing. *IEEE Communications magazine*, 48(9), 2010.

[33] Arvind Thiagarajan, Lenin Ravindranath, Katrina LaCurts, Samuel Madden, Hari Balakrishnan, Sivan Toledo, and Jakob Eriksson. Vtrack: accurate, energy-aware road traffic delay estimation using mobile phones. In *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems*, pages 85–98. ACM, 2009.

[34] Alexandre M Bayen, Anthony David Patire, et al. *Mobile Millennium final report*. California Center for Innovative Transportation, Institute of Transportation Studies, University of California, Berkeley, 2011.

[35] Rakesh Kumar and Mayank Dave. A comparative study of various routing protocols in vanet. *arXiv preprint arXiv:1108.2094*, 2011.

[36] Abdelmalik Bachir and Abderrahim Benslimane. A multicast protocol in ad hoc networks inter-vehicle geocast. In *Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual*, volume 4, pages 2456–2460. IEEE, 2003.

[37] Harshvardhan P Joshi, Mihail L Sichitiu, and Maria Kihl. Distributed robust geocast multicast routing for inter-vehicle communication. In *Proceedings of WEIRD workshop on WiMax, wireless and mobility*, volume 921, 2007.

[38] Gökhan Korkmaz, Eylem Ekici, Füsun Özgüner, and Ümit Özgüner. Urban multi-hop broadcast protocol for inter-vehicle communication systems. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 76–85. ACM, 2004.

[39] Alessandro Amoroso, Gustavo Marfia, Marco Roccetti, and Giovanni Pau. Creative testbeds for vanet research: a new methodology. In *2012 IEEE Consumer Communications and Networking Conference (CCNC)*, pages 477–481. IEEE, 2012.

[40] Jamal Toutouh and Enrique Alba. Light commodity devices for building vehicular ad hoc networks: An experimental study. *Ad Hoc Networks*, 37:499–511, 2016.

[41] Wantanee Viriyasitavat, Soranut Midtrapanon, Takkachai Rittirat, and Sornrakitch Thanumaiweerakun. Performance analysis of android-based real-time message dissemination in vanets. In *Computing, Networking and Communications (ICNC), 2016 International Conference on*, pages 1–5. IEEE, 2016.

[42] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security*, 15(1):39–68, 2007.

[43] Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In *Advances in Cryptology—CRYPTO 2001*, pages 213–229. Springer, 2001.

[44] Kenneth G Paterson and Geraint Price. A comparison between traditional public key infrastructures and identity-based cryptography. *Information Security Technical Report*, 8(3):57–72, 2003.

[45] Yvo Desmedt and Mike Burmester. Identity-based key infrastructures (iki). In *IFIP International Information Security Conference*, pages 167–176. Springer, 2004.

[46] Sattam S Al-Riyami and Kenneth G Paterson. Certificateless public key cryptography. In *Asiacrypt*, volume 2894, pages 452–473. Springer, 2003.

[47] C. Leyva M. Morales and H. Galeana. Comparación cualitativa de los enfoques basados en certificados digitales y en identidad para seguridad en redes vehiculares. *Tercer Congreso Nacional de Ingeniería CONNAI 2016, Cd. Victoria, Tamaulipas, September 2016*, pages 33–38, 2016.

[48] Amizah Malip, Siaw-Lynn Ng, and Qin Li. A certificateless anonymous authenticated

announcement scheme in vehicular ad hoc networks. *Security and Communication Networks*, 7(3):588–601, 2014.

[49] A. De Caro and V. Iovino. jpbc: Java pairing based cryptography. In *2011 IEEE Symposium on Computers and Communications (ISCC)*, pages 850–855, June 2011.

[50] Miguel Morales-Sandoval and Arturo Diaz-Perez. *DET-ABE: A Java API for Data Confidentiality and Fine-Grained Access Control from Attribute Based Encryption*, pages 104–119. Springer International Publishing, Cham, 2015.

[51] Elena Fasolo, Andrea Zanella, and Michele Zorzi. An effective broadcast scheme for alert message propagation in vehicular ad hoc networks. In *Communications, 2006. ICC'06. IEEE International Conference on*, volume 9, pages 3960–3965. IEEE, 2006.

[52] Chakkaphong Suthaputchakun and Zhili Sun. Priority based routing protocol in vehicular ad hoc network. In *Computers and Communications (ISCC), 2011 IEEE Symposium on*, pages 723–728. IEEE, 2011.