UNIVERSIDAD POLITÉCNICA DE MADRID
Escuela Técnica Superior de Ingeniería de Sistemas Informáticos

Contribución a la ejecución segura y confiable de servicios distribuidos en redes ad-hoc vehiculares (VANET) mediante tecnologías Blockchain

T E S I S D O C T O R A L

Presentada para optar al título de Doctor por:

Rubén Juárez Cádiz
Ingeniería de Telecomunicación

Madrid, 2024

UNIVERSIDAD POLITÉCNICA DE MADRID
Escuela Técnica Superior de Ingeniería de Sistemas Informáticos

Doctorado en Ciencias y Tecnologías de la Computación para Smart Cities

Contribución a la ejecución segura y confiable de servicios distribuidos en redes ad-hoc vehiculares (VANET) mediante tecnologías Blockchain

T E S I S D O C T O R A L

Presentada para optar al título de Doctor por:

Rubén Juárez Cádiz
Ingeniería de Telecomunicación

Bajo la dirección de:
Dr. Borja Bordel Sanchez

Madrid, 2024

Título: Contribución a la ejecución segura y confiable de servicios distribuidos en redes ad-hoc vehiculares (VANET) mediante tecnologías Blockchain

Autor: Rubén Juárez Cádiz

Programa de Doctorado: Ciencias y Tecnologías de la Computación para Smart Cities

Dirección de Tesis:

Borja Bordel Sanchez

Revisores Externos:

Tribunal de Tesis:

Fecha de Defensa de Tesis:

La belleza de la rosa es que siendo tan hermosa no conoce que lo es
José María Pemán

Agradecimientos

Es con un sentimiento de inmensa gratitud que me dirijo a ustedes hoy. Al culminar mi Doctorado en Ciencias y Tecnologías de la Computación para Smart Cities, reflexiono sobre las numerosas personas que han hecho posible este logro. No puedo dejar de mencionar a aquellos que han sido fundamentales en este viaje académico y personal.

Primero, quiero expresar mi más profundo agradecimiento a Borja Bordel. Tu guía, apoyo y expertise han sido invaluables para mí. Has sido mucho más que un mentor; has sido una inspiración constante y un pilar de apoyo en todo momento.

A mis queridos padres, su amor incondicional y apoyo inquebrantable han sido el motor que me ha impulsado a seguir adelante, incluso en los momentos más desafiantes. Sin ustedes, simplemente no habría sido posible.

Y a Lara, tu presencia y apoyo han significado más de lo que las palabras pueden expresar. Tu aliento y comprensión han añadido una dimensión invaluable a mi experiencia en este doctorado.

A todos ustedes, mi más sincero agradecimiento. Vuestro apoyo ha dejado una huella imborrable en mi vida y ha sido esencial para hacer realidad esta monumental etapa en mi carrera académica y profesional.

Abstract

This thesis work is developed within the framework of providing secure distributed services and trust in the context of Vehicular Ad-hoc Networks (VANETs). VANETs are characterized by establishing ephemeral connections between nodes dynamically to collect data, transmit information, and provide and receive services in a distributed manner. In these ad hoc networks, the provision of security and trust is still an unanswered challenge, both technologically and ethically and socially. Yet, new technologies like blockchain can be employed to address this issue and enhance the security and trust of services in VANETs.

The general objective of this thesis is to design and implement an advanced architecture to improve the security and reliability of distributed services in VANETs, using Blockchain technology and reputation and trust mechanisms and algorithms. For this, I propose algorithms, computing schemes, and specific protocols, culminating in the creation of a robust, secure, and reliable service execution environment for intelligent vehicular networks.

For this purpose, a theoretical framework for trust in VANETs is developed, which includes a precise mathematical description of trust. This framework allows for reliable evaluation and assessment of trust among vehicular nodes, facilitating identification and mitigation of potential security threats and vulnerabilities within the network. In addition, a service-based trust and reputation calculation algorithm is developed, integrating multiple trust approaches (cognitive, computational, neurological, and game theory) to provide a dynamic and accurate assessment of the nodes' reputation in VANETs. This algorithm seeks to represent trust not as a static value, but as a probability distribution that more faithfully reflects the uncertainty inherent in observations in highly dynamic and heterogeneous environments. Thanks to these technologies, we can implement a distributed system based on blockchain for the calculation and management of trust and reputation in VANETs, allowing the integration of local trust calculations into an updated global trust value. And develop an integrated predictive model that uses data collected by VANETs and weather variables to provide data services. This model is based on advanced correlation techniques and analysis of large volumes of data, seeking to capture the complexity and variability inherent in road and weather conditions.

With all of the above, we will be able to design and implement a service ecosystem that improves the efficiency and scalability of obstacle mapping techniques secured by Blockchain in VANET. This system is based on a secure vehicular communication algorithm and will employ cryptography technologies to ensure a secure and robust data exchange between vehicles. In this ecosystem, we develop this secure communication algorithm, based on blockchain technology, and that significantly improves protection against security threats in VANET. This architecture focuses on robust node authentication and the protection of the privacy of data exchanged between vehicles and infrastructures, using advanced cryptography technologies and consensus mechanisms to secure communication.

Finally, we implement and experimentally validate the proposed trust provisioning system based on blockchain technology for VANETs, demonstrating its effectiveness in improving security, privacy, and trust in these environments. This system uses two parallel blockchains, the event chain and the reputation chain, to track and record the nodes' actions, employing

reputation evaluation schemes based on Bayesian inference. The validation includes detailed simulations to compare the performance of the proposed system with existing alternatives, focusing on reducing latency, jitter, and increasing the packet delivery rate and energy efficiency.

Keywords *VANET*; *blockchain*; *RSU*; *security*; *trust*; *chain of custody. reputation*, *communication protocol*, *distributed services*, *privacy*, *threat mitigation*, *public key infrastructure (PKI)*, *smart contract*, *vehicular networks*.

Resumen

Este trabajo de Tesis se desarrolla en el marco de la provisión de servicios distribuidos seguros y confianza en el contexto de la redes vehículares ad hoc (VANET, por sus siglas en inglés). Las VANET se caracterizan por establecer conexiones efímeras entre nodos de forma dinámica, para poder recolectar datos, transmitir información y prestar y recibir servicios de una manera distribuida. En estas redes ad hoc, la provisión de seguridad y confianza es un reto aún sin respuesta, tanto a nivel tecnológico como ético y social. Aún así, nuevas tecnologías como blockchain pueden ser empleadas para abordar este problema y aumentar la seguridad y confianza de los servicios en VANET.

El objetivo general de esta tesis es diseñar e implementar una arquitectura avanzada para mejorar la seguridad y confiabilidad de los servicios distribuidos en VANETs, utilizando la tecnología blockchain y mecanismos y algoritmos de reputación y confianza. Para ello, propongo algoritmos, esquemas de cómputo y protocolos específicos, culminando en la creación de un entorno de ejecución de servicios distribuidos robusto, seguro y confiable para las redes vehiculares inteligentes.

Para ello, se desarrolla un marco teórico para la confianza en VANETs, que contempla una descripción matemática precisa de la confianza. Este marco permite la evaluación y valoración fiable de la confianza entre nodos vehiculares, facilitando la identificación y mitigación de posibles amenazas de seguridad y vulnerabilidades dentro de la red. Además, se desarrolla un algoritmo de cálculo de confianza y reputación basado en servicios, que integra múltiples enfoques de la confianza (cognitivo, computacional, neurológico y teórico de juegos) para proporcionar una evaluación dinámica y precisa de la reputación de los nodos en las VANETs. Este algoritmo busca representar la confianza no como un valor estático, sino como una distribución de probabilidad que refleje de manera más fidedigna la incertidumbre inherente a las observaciones en entornos altamente dinámicos y heterogéneos. Gracias a estas tecnologías, podemos implementar un sistema distribuido basado en blockchain para el cálculo y gestión de la confianza y reputación en VANETs, que permite la integración de los cálculos locales de confianza en un valor de confianza global actualizado. Y desarrollar un modelo predictivo integrado que utiliza datos recopilados por VANETs y variables climáticas para proveer servicios de datos. Este modelo se basa en técnicas avanzadas de correlación y análisis de grandes volúmenes de datos, buscando capturar la complejidad y la variabilidad inherente a las condiciones viales y meteorológicas.

Con todo lo anterior, podremos diseñar e implementar un ecosistema de servicios que mejore la eficiencia y escalabilidad de las técnicas de mapeo de obstáculos seguras habilitadas por Blockchain en VANET. Este sistema se basa en un algoritmo de comunicación vehicular seguro y empleará tecnologías de criptografía para garantizar un intercambio de datos seguro y robusto entre vehículos. En este ecosistema, desarrollamos este algoritmos de comunicación seguro, basado en la tecnología blockchain, y que mejora significativamente la protección contra las amenazas de seguridad en VANET. Esta arquitectura se centra en la autenticación robusta de los nodos y la protección de la privacidad de los datos intercambiados entre vehículos e infraestructuras, utilizando tecnologías de criptografía avanzada y mecanismos de consenso para asegurar la comunicación.

Finalmente, implementamos y validamos experimentalmente el sistema propuesto de provisión de confianza basado en la tecnología blockchain para VANETs, demostrando su eficacia en la mejora de la seguridad, la privacidad y la confianza en estos entornos. Este sistema utiliza dos cadenas de bloques paralelas, la cadena de eventos y la cadena de reputación, para rastrear y registrar las acciones de los nodos, empleando esquemas de evaluación de reputación basados en inferencia bayesiana. La validación incluye simulaciones detalladas para comparar el rendimiento del sistema propuesto con alternativas existentes, enfocándose en la reducción de la latencia, el jitter, y el incremento de la tasa de entrega de paquetes y la eficiencia energética.

Palabras clave *VANET*; *cadena de bloques*; *RSU*; *seguridad*; *confianza*; *cadena de custodia. reputación*, *protocolo de comunicaciones*, *servicios distribuidos*, *privacidad*, *mitigación de amenazas*, *infraestructura de clave pública (PKI)*, *contrato inteligente*, *redes vehiculares*

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Abreviaturas y acrónimos

UPM	Universidad Politécnica de Madrid
VANET	VANET Vehicular Ad-hoc Networks
V2V	Vehicle-to-Vehicle Communications
V2I	Vehicle-to-Infrastructure Communications
IoT	Internet of Things
RSU	Roadside Unit
P2P	Peer-to-Peer Network
GPS	Global Positioning System
5G	Fifth Generation of Mobile Networks
API	Application Programming Interface
DDoS	Distributed Denial of Service Attack
MAC	Media Access Control
EAP	Extensible Authentication Protocol
TLS	Transport Layer Security
PKI	Public Key Infrastructure
CA	Certification Authority
V2X	Vehicle-to-Everything Communication
D2D	Device-to-Device
UAV	Unmanned Aerial Vehicle

Capítulo 1

Introducción

Las Redes Ad-hoc Vehiculares (VANET, por sus siglas en inglés) representan una evolución tecnológica crucial en el ámbito del transporte inteligente. Estas redes permiten la comunicación directa entre vehículos (comunicaciones V2V) y entre vehículos e infraestructuras viales (comunicaciones V2I), facilitando así un intercambio de información en tiempo real que puede ser utilizado para mejorar la seguridad vial, la eficiencia del tráfico y el confort en la conducción. Sin embargo, la implementación efectiva de servicios en VANET plantea desafíos significativos en términos de confianza y seguridad.

La confianza y la seguridad en la provisión de servicios en el contexto de VANET son, de hecho, fundamentales. Primero, porque la integridad de la información compartida es vital: un mensaje sobre una condición peligrosa en la carretera, como hielo en el pavimento o un accidente inminente, debe ser preciso y fiable. La desinformación o la manipulación de datos pueden tener consecuencias fatales, poniendo en riesgo vidas humanas. Y segundo, porque la privacidad de los usuarios es de suma importancia, y un derecho protegido a nivel europeo. Así, mientras que la información sobre la ubicación y movimientos de los vehículos se comparte continuamente, es crucial asegurar que estos datos no sean explotados para fines malintencionados, como el seguimiento o la invasión de la privacidad personal.

Los desafíos pendientes en la provisión segura de servicios en VANET no sólo se refieren a la protección contra amenazas externas, como ataques de interceptación o manipulación de datos, sino también a la resiliencia contra fallos internos y errores de software. Esto implica el desarrollo de protocolos robustos que puedan garantizar la autenticidad, la integridad y la disponibilidad de la información compartida, incluso en escenarios de alta movilidad y en condiciones de red dinámicas y potencialmente adversas.

Además, contribuir a la confianza y seguridad en la provisión de servicios en VANET no es sólo una cuestión técnica; es también un problema ético y social que aborda la creciente dependencia de nuestras sociedades de las tecnologías de transporte inteligente, y los servicios digitales. A medida que nos movemos hacia un futuro con vehículos autónomos y sistemas de transporte más inteligentes, la necesidad de sistemas de comunicación vehicular seguros y confiables se vuelve cada vez más crítica. Estos sistemas no solo tienen el potencial de reducir significativamente la cantidad de accidentes de tráfico y las congestiones, sino que también

son clave para la adopción generalizada de tecnologías de movilidad avanzadas.

1.1 Estructura del documento

La estructura de este documento de Tesis es la siguiente:

En el **Capítulo 2** ***Motivación y Objetivos*** describimos la motivación de este trabajo de Tesis, así como los objetivos generales y específicos del mismo.

En el **Capítulo 3** ***Estado del arte*** realizamos un análisis exhaustivo del estado actual de la técnica sobre la provisión segura y confiable de servicios distribuidos en VANET. Ponemos especial atención al uso de cadenas de bloques (Blockchain), por ser esta tecnología la que muestra un desempeño más prometedor en entornos distribuidos.

El **Capítulo 4** ***Arquitectura de Servicios para la Provisión de Confianza en VANET mediante Blockchain*** introduce un nuevo marco teórico para la gestión de la confianza en VANETs, apoyándose en la tecnología Blockchain. Proponemos un conjunto de requisitos esenciales para cualquier solución eficaz de provisión de confianza en VANET, y desarrollamos una descripción matemática de la confianza digital. Posteriormente, proponemos una arquitectura de servicios basada en blockchain que no solo cumple con estos requisitos, sino que también aborda las limitaciones de las soluciones existentes.

En el **capítulo 5** ***Provisión de Servicios de Confianza y Reputación en VANET*** abordamos el desarrollo y la implementación de un modelo de cálculo de confianza y reputación para VANETs, integrando enfoques de inteligencia cognitiva y computacional. Este modelo permite una gestión dinámica de la confianza a través de una arquitectura basada en blockchain, promoviendo un sistema de comunicación vehicular seguro y confiable.

En el **capítulo 6** ***Provisión de servicios predictivos de datos en VANET*** presentamos la creación y validación de modelos predictivos avanzados para servicios de datos distribuidos en VANET. Estos modelos se benefician de técnicas de correlación y desarrollo en serie, alimentadas mediante datos colaborativos aportados por los nodos en una VANET.

En el **capítulo 7** ***Ejecución Segura de Servicios en VANET mediante Blockchain*** exploramos el diseño e implementación de una arquitectura para asegurar la comunicación V2V en VANETs utilizando blockchain. Este sistema promete una comunicación vehicular segura, escalable y eficiente, esencial para el futuro de los vehículos autónomos y la movilidad inteligente.

En el **capítulo 8** ***Identificación y Mitigación de Amenazas en VANET mediante Blockchain*** proponemos una solución blockchain para mejorar la seguridad en VANETs, enfocándonos en la identificación y mitigación de amenazas. Nuestro enfoque descentralizado ofrece una alternativa robusta a los sistemas de seguridad tradicionales, abordando tanto la autenticación de vehículos como la gestión de reputación.

Finalmente, en el **capítulo 9** ***Conclusiones y Trabajos Futuro*** sintetizamos los hallazgos y contribuciones clave de nuestra investigación, destacando el impacto de las soluciones propuestas en la seguridad, eficiencia y confiabilidad de VANETs. Adicionalmente, identificamos

varias direcciones prometedoras para futuras investigaciones en el campo de las comunicaciones vehiculares y la tecnología blockchain.

Capítulo 2

Motivación y objetivos

En este Capítulo se presenta la motivación de este proyecto de Tesis y los objetivos, generales y específicos, que se busca alcanzar; los cuales guiarán las contribuciones descritas en los próximos capítulos.

2.1 Motivación

La implementación y la adopción generalizada de las Redes Ad-hoc Vehiculares (VANET) se presenta como un pilar fundamental en el desarrollo de los sistemas de transporte inteligente del futuro. Estas tecnologías prometen transformar la interacción entre vehículos e infraestructuras viales, lo cual podría mejorar de manera significativa la seguridad vial, la eficiencia del tráfico y el confort durante la conducción. Sin embargo, el pleno potencial de las VANET solo puede alcanzarse enfrentando y superando los retos inherentes a la seguridad y la confianza en estas redes.

La comunicación continua entre vehículos e infraestructuras plantea importantes desafíos de privacidad en la provisión de servicios distribuidos. Es imperativo desarrollar mecanismos que protejan los datos personales de los usuarios, evitando el seguimiento no autorizado y la recopilación de información sin el debido consentimiento.

Además, con el aumento de la prevalencia de las VANET, estas también se convierten en objetivos atractivos para ataques cibernéticos. Es crucial desarrollar servicios que sean resilientes ante la interceptación de datos, la falsificación de mensajes y otros ataques malintencionados, garantizando la seguridad y la confianza en la red.

La contribución a la seguridad y la confianza en la provisión de servicios en VANET es vital para desbloquear el potencial revolucionario de estas tecnologías en nuestros sistemas de transporte, haciéndolos más seguros, eficientes y sostenibles. A través de esta tesis, busco avanzar en el conocimiento técnico en este campo y abordar las preocupaciones éticas y sociales, asegurando que las tecnologías de transporte del futuro respeten los principios legales, y garanticen la seguridad de los ciudadanos y la confiabilidad de los servicios.

2.2 Objetivos

El objetivo general de esta tesis es diseñar e implementar una arquitectura avanzada para mejorar la seguridad y confiabilidad de los servicios distribuidos en las Redes Ad-hoc Vehiculares (VANETs), utilizando la tecnología Blockchain y mecanismos y algoritmos de reputación y confianza. Para ello, propongo algoritmos, esquemas de cómputo y protocolos específicos, culminando en la creación de un entorno de ejecución de servicios distribuidos robusto, seguro y confiable para las redes vehiculares inteligentes.

Para abordar este objetivo general, se establecen los siguientes objetivos específicos:

Objetivo#1: Desarrollar un marco teórico para la confianza en VANETs, que contemple una descripción matemática precisa de la confianza. Este marco deberá permitir la evaluación y valoración fiable de la confianza entre nodos vehiculares, facilitando la identificación y mitigación de posibles amenazas de seguridad y vulnerabilidades dentro de la red.

Objetivo#2: Desarrollar un algoritmo de cálculo de confianza y reputación basado en servicios, que integre múltiples enfoques de la confianza (cognitivo, computacional, neurológico y teórico de juegos) para proporcionar una evaluación dinámica y precisa de la reputación de los nodos en las VANETs. Este algoritmo buscará representar la confianza no como un valor estático, sino como una distribución de probabilidad que refleje de manera más fidedigna la incertidumbre inherente a las observaciones en entornos altamente dinámicos y heterogéneos.

Objetivo#3: Implementar un sistema distribuido basado en blockchain para el cálculo y gestión de la confianza y reputación en VANETs, que permita la integración de los cálculos locales de confianza en un valor de confianza global actualizado. Este sistema utilizará la tecnología blockchain para asegurar la integridad, transparencia y no repudio de las transacciones y evaluaciones de confianza entre los nodos, facilitando así un marco seguro y eficiente para la gestión de la confianza en las redes vehiculares.

Objetivo#4: Desarrollar un modelo predictivo integrado que utilice datos recopilados por VANETs y variables climáticas para proveer servicios de datos. Este modelo se basará en técnicas avanzadas de correlación y análisis de grandes volúmenes de datos, buscando capturar la complejidad y la variabilidad inherente a las condiciones viales y meteorológicas.

Objetivo#5: Diseñar e implementar un ecosistema de servicios que mejore la eficiencia y escalabilidad de las técnicas de mapeo de obstáculos seguras habilitadas por Blockchain en VANET. Este sistema se basará en un algoritmo de comunicación vehicular seguro y empleará tecnologías de criptografía para garantizar un intercambio de datos seguro y robusto entre vehículos.

Objetivo#6: Desarrollar un algoritmo de comunicación para VANET, segururo y basado en Blockchain, y que mejore significativamente la protección contra las amenazas de seguridad en VANET. Esta arquitectura se centrará en la autenticación robusta de los nodos y la protección de la privacidad de los datos intercambiados entre vehículos e infraestructuras, utilizando tecnologías de criptografía avanzada y mecanismos de consenso para asegurar la comunicación.

Objetivo#7: Desarrollar un nuevo método para la generación y verificación de hashes seguros para cada interacción vehicular dentro de la red VANET. Este método facilitará la autenticación y validación de las comunicaciones vehiculares, minimizando la posibilidad de inyección de datos falsos y actividades maliciosas dentro de la red.

Objetivo#8: Implementar y validar experimentalmente un ecosistema de provisión de confianza basado en la tecnología blockchain para VANETs y servicios distribuidos, demostrando su eficacia en la mejora de la seguridad, la privacidad y la confianza en estos entornos. Este sistema utilizará dos cadenas de bloques paralelas, la cadena de eventos y la cadena de reputación, para rastrear y registrar las acciones de los nodos, empleando esquemas de evaluación de reputación basados en inferencia bayesiana. La validación incluirá simulaciones detalladas para comparar el rendimiento del sistema propuesto con alternativas existentes, enfocándose en la reducción de la latencia, el jitter, y el incremento de la tasa de entrega de paquetes y la eficiencia energética.

Capítulo 3

Estado del arte

En este capítulo, presentamos un análisis exhaustivo del estado del arte relacionado con la provisión de seguridad y confianza en Redes Ad-hoc Vehiculares (VANET). Este análisis se centra en los avances recientes, los desafíos actuales y las soluciones propuestas en la literatura científica, con el objetivo de identificar las brechas de conocimiento existentes y las oportunidades para contribuciones futuras.

3.1 Soluciones computaciones para el cálculo de confianza en VANETs

Como uno de los problemas abiertos más relevantes en la actualidad, relacionado con los sistemas de Redes de Vehículos Ad hoc (VANETs), el cálculo y la gestión de la confianza y la reputación han recibido mucha atención en los últimos diez años Abdelhafidh et al., 2023. Se pueden encontrar muchas propuestas diferentes, aunque en general se identifican típicamente seis categorías diferentes.J. Zhang, 2011

El primer grupo de trabajos propone la introducción de Terceras Partes de Confianza (TTP) y protocolos de autenticación. En estos esquemas, los componentes confiables son aquellos que son autenticados por un middleware muy seguro o componentes conocidos como TTP o enclaves seguros Koduri et al., 2020. Se despliegan cifrados estándar, claves y protocolos entre todos los componentes.L. Xie et al., 2019 En arquitecturas de red jerárquicas, se pueden crear dominios de confianza y las TTP pueden construirse como pasarelas de confianza. Aunque este esquema es muy útil en arquitecturas cliente-servidor, en despliegues de VANETs muy distribuidos es muy ineficiente.Fernandes et al., 2023

El segundo grupo de soluciones de confianza para despliegues de VANETs está compuesto por sistemas de recomendación Atwa et al., 2021. Un sistema de recomendación puede ser de tres tipos: filtrado basado en contenido, filtrado colaborativo y un sistema híbrido. En general, en todos estos enfoques, los nodos reciben y analizan recomendaciones para decidir con qué otros nodos establecen una conexión (como hacen las personas en las sociedades)Soleymani et al., 2017. Estos sistemas pueden aprovechar la estructura de la red, pero son totalmente reactivos y no pueden emplearse como una solución de prevención. Además, este enfoque requiere una

gran intervención humana y apenas puede automatizarse.Lu et al., 2019

Los trabajos en el tercer grupo abordan mecanismos basados en comportamiento Ayobi et al., 2021. En este enfoque, los nodos monitorean el comportamiento de otros componentes y deciden sobre las conexiones que desean mantener o podar. Aunque este esquema permite a los nodos realizar evaluaciones locales simples, puede ser difícil emplear esta tecnología en políticas de prevención ya que los datos recopilados no son suficientes para respaldar predicciones. Además, este enfoque carece de un entendimiento global de la confianza para el sistema entero de los nodos particulares R. Hussain et al., 2020.Para resolver este desafío y habilitar la opción de implementar políticas de prevención y hacer predicciones, en el cuarto grupo de soluciones de confianza, los mecanismos se basan en metadatos Mehdi et al., 2017. Información como la ubicación geográfica de la propiedad de los nodos se emplea para determinar qué nodos son no confiables y maliciosos.Venitta Raj y Balasubramanian, 2021 Este esquema es totalmente proactivo, ya que los nodos maliciosos pueden ser eliminados antes de que comiencen a operar, con solo conocer sus metadatos.Z. Sun et al., 2021 Sin embargo, el porcentaje de falsos positivos en este enfoque es más alto que en cualquier otro enfoque anterior.A. A. Khan et al., 2018

En los últimos cinco años, la revolución de Blockchain también ha afectado a las tecnologías de VANETs, y se pueden encontrar diferentes propuestas para proporcionar y respaldar la confianza en despliegues de VANETs basados en Blockchain Azees et al., 2016, Liu et al., 2021. Aunque este mecanismo puede proporcionar cierto nivel de confianza, algunos trabajos han reportado diferentes ataques y problemas asociados a esta solución A. S. Khan et al., 2019. Además, el retraso de las transacciones comunicadas a través de redes Blockchain crece exponencialmente, reduciendo el rendimiento de la red de manera muy relevante.Lu et al., 2019

Finalmente, y sexta categoría, se han reportado muchos enfoques híbridos diferentes Ayobi et al., 2021, Junejo et al., 2021. Estos esquemas intentan combinar las ventajas de diferentes mecanismos. Una de las propuestas más comunes incluye una solución basada en comportamiento junto con una TTP o middleware (para almacenar cálculos locales y obtener un valor global).Lu et al., 2019 Sin embargo, estas soluciones siguen siendo muy débiles contra manipulaciones, en contraste con los mecanismos basados en Blockchain.Huang et al., 2014

En nuestra propuesta combinamos la mayoría de estos enfoques en una arquitectura distribuida. La solución está orientada a servicios y está respaldada por Blockchain, aunque no todas las transacciones deben pasar por esta red para preservar el rendimiento del sistema. Además, el cálculo de la confianza incluye cuatro perspectivas diferentes (cognitiva, computacional, neurológica y teórica de juegos) con el fin de garantizar el carácter reactivo y proactivo de la solución.

Tabla 3.1: Resumen de las principales soluciones del estado del arte en VANETs.

Referencias	**Descripción corta**	**Problemas principales**	**Notas adicionales**
Koduri et al., 2020, L. Xie et al., 2019, Fernandes et al., 2023	TTP y protocolos de autenticación	Ineficiente en despliegues muy distribuidos	Mejor en arquitecturas cliente-servidor
Atwa et al., 2021, Soleymani et al., 2017, Lu et al., 2019	Sistemas de recomendación	Reactivos y no preventivos	Requiere gran intervención humana
Ayobi et al., 2021, R. Hussain et al., 2020	Mecanismos basados en comportamiento	Difícil en políticas de prevención	Carece de visión global de confianza
Venitta Raj y Balasubramanian, 2021, Z. Sun et al., 2021	Mecanismos basados en metadatos	Alto porcentaje de falsos positivos	Proactivo pero limitado
Azees et al., 2016, Liu et al., 2021, Lu et al., 2019	Blockchain en VANETs	Retraso en transacciones blockchain	Problemas de escalabilidad y ataques
Ayobi et al., 2021, Junejo et al., 2021, Lu et al., 2019	Enfoques híbridos	Débiles contra manipulaciones	Combina varias soluciones para mejorar la confianza

* Principales soluciones del estado del arte.

En el contexto de las Redes de Vehículos Ad hoc (VANETs), esta aproximación multidimensional asegura una gestión de confianza y reputación adaptativa y eficiente, capaz de enfrentar los desafíos únicos que presentan estos entornos altamente dinámicos y distribuidos. La integración de tecnologías Blockchain facilita una infraestructura segura y descentralizada para la verificación de transacciones y la gestión de identidades, mientras que la diversidad en las metodologías de cálculo de confianza permite una evaluación más precisa y contextual de las entidades dentro de la red. Este enfoque holístico no solo mejora la seguridad y fiabilidad de las comunicaciones dentro de las VANETs sino que también promueve una cooperación más robusta entre vehículos, contribuyendo significativamente a la seguridad vial y a la eficiencia del tráfico.

3.2 Arquitecturas para la provisión de confianza en VANET. Blockchain

Aunque los trabajos sobre la confianza en los sistemas de VANETs no son muy numerosos, se pueden encontrar varias propuestas Soleymani et al., 2015. Además, se han reportado muchos artículos sobre temas colaterales (como el cálculo multipartito C. Wang y Peeta, 2024 o la preservación de la privacidad Song et al., 2018). Varias revisiones sobre la confianza también han sido comunicadas L. Li et al., 2010; T. Li et al., 2019; J. Zhang et al., 2011, las cuales pueden ser utilizadas para entender el estado actual y los futuros desafíos de la gestión de la confianza.F.-Y. Wang, 2010

Primero, algunos autores han propuesto trabajos enfocados en la evaluación de la confianza Jyothi y Patil, 2022. En estas propuestas, se definen metodologías para estimar el valor de las propiedades que influyen en el nivel de confianza asociado con las entidades de VANETs en el sistema. Sin embargo, en general, es complicado evaluar la confianza de manera cuantitativa. Así, las soluciones solían emplear conceptos de Calidad de Servicio para realizar cálculos. No obstante, también se pueden encontrar trabajos enfocados en la estimación de parámetros como privacidad, amistad, nobleza o sensibilidad Bordel et al., 2023; Soleymani et al., 2017; K. N. Tripathi et al., 2022. Bordel, por ejemplo, define la honestidad, cooperatividad e interés comunitario usando parámetros de red como la tasa de pérdida de paquetes. Estas tres cantidades pueden ser medidas de manera directa o indirecta, y se emplean para componer una estimación general de confianza en el sistema.

Los problemas de escalabilidad y adaptabilidad relacionados con esta solución también fueron estudiados Kudva et al., 2021. Modelos avanzados que consideran parámetros adaptativos para el cálculo de la confianza A. S. Khan et al., 2019 han sido reportados también. Además, algunas propiedades de la confianza (como la precisión de la confianza o la resiliencia) también han sido investigadas R. Hussain et al., 2020; Soleymani et al., 2017.

Como principal problema, estas propuestas requieren mucho tiempo (decenas de horas) para converger al valor real de la confianza. Por el contrario, la tecnología propuesta permite calcular la confianza en conexiones ad hoc efímeras. De manera similar, se propone un modelo basado en la reputación para la confianza en VANETs, argumentando que las entidades de VANETs podrían establecer relaciones sociales de manera independiente Lu et al., 2019. El marco propuesto es capaz de detectar comportamientos maliciosos y proteger el sistema usando herramientas de seguridad.Nandy et al., 2021

Por otro lado, también se pueden encontrar modelos de evaluación de confianza para escenarios simplificados que incluyen solo vehículos sensores.Soleymani et al., 2017 Por ejemplo, se propone un sistema de evaluación de confianza basado en un concepto de reputación difusa que considera parámetros de QoS.Lu et al., 2019 Finalmente, se han descrito soluciones que incluyen la confianza de los usuarios Tan y Chung, 2019. Estas propuestas, usando una clasificación de servicios, evalúan la percepción del usuario para detectar entidades maliciosas.Huang et al., 2014

En todas las propuestas citadas previamente, sin embargo, los modelos y metodologías de confianza se centran en las entidades de VANETs. En este enfoque, los componentes de

VANETs evalúan la fiabilidad de los otros componentes con los que se comunican. Dependiendo de los elementos empleados para analizar la fiabilidad, se pueden definir diferentes tipos de confianza (ver Figura 3.1.)

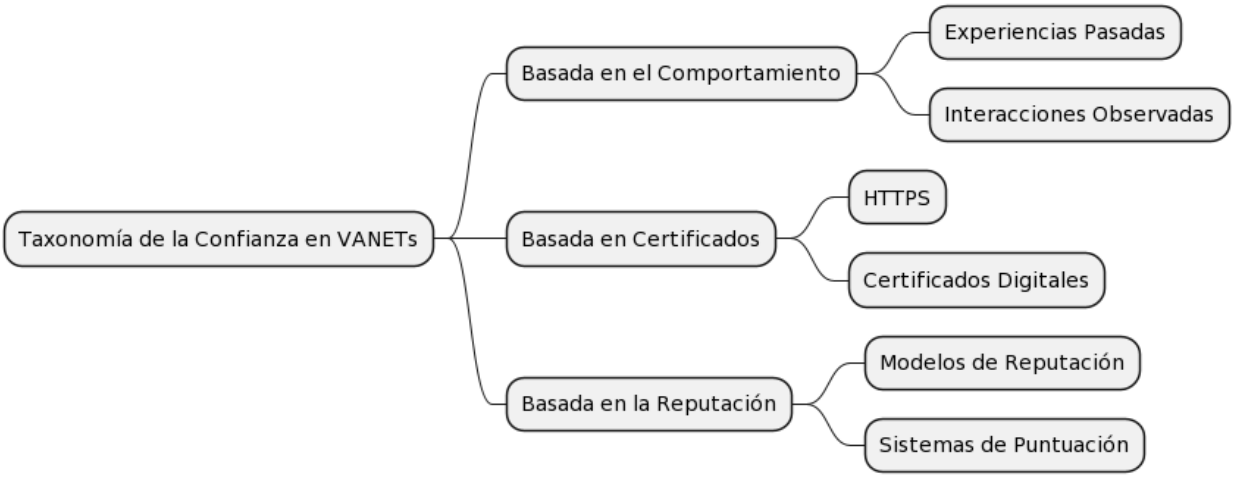

Figura 3.1: Taxonomía de la confianza en VANETs

En particular, los trabajos citados describen soluciones basadas en el comportamiento Hasrouny et al., 2019; J. Wang et al., 2009 (donde el nivel de confianza depende de las experiencias pasadas), aunque en soluciones comerciales se prefieren soluciones basadas en certificados (como HTTPS).

En cualquier caso, algunos problemas relevantes aún dificultan el empleo práctico de soluciones centradas en la entidad en los sistemas de VANETs.Soleymani et al., 2017 De hecho, estas soluciones requieren redes muy estables y estáticas, ya que los enlaces de comunicación deben mantenerse el tiempo suficiente para adquirir una cantidad representativa de información.Zheng et al., 2019

Sin embargo, la mayoría de los sistemas de VANETs propuestos recientemente no cumplen con esta característica. Primero, porque los sistemas de VANETs son muy dinámicos: los dispositivos de hardware establecen conexiones ad hoc Bordel et al., 2019; los componentes de software pueden ser desplegados y desmontados muy rápidamente, los servicios y aplicaciones cambian dependiendo de las necesidades de los usuarios (a lo largo de los principios de prosumidor Alcarria et al., 2018), etc. Por lo tanto, las relaciones entre componentes son muy efímeras y usualmente es imposible acumular suficiente información para hacer que el valor estimado de confianza converja a un valor estable. Además, la gestión de identidad es un problema sin resolver en VANETs Bordel y Alcarria, 2021.

En particular, no está claro si los componentes en un sistema pueden ser provistos con un identificador único Huang et al., 2014. Entonces, implementar un mecanismo de evaluación de confianza centrado en la entidad se convierte en una tarea muy complicada. Finalmente, en una situación muy común, los servicios son proporcionados por medio de intermediarios que hacen independientes las diferentes capas en el sistema de VANETs. Además, los componentes

en una cierta capa usualmente ejecutan servicios de manera colaborativa ad hoc, y el esquema de ejecución es desconocido por el resto de los elementos en el sistema Robles et al., 2018. Eso significa que cuando un componente en un sistema de VANETs recibe una orden de ejecución, puede delegar o trabajar junto con otros componentes pertenecientes al mismo nivel en la arquitectura para resolver esa orden; y ningún componente en el sistema (incluso el elemento original que envió la orden de ejecución) es capaz de saber qué componentes estuvieron involucrados en la ejecución o cómo se obtuvo el resultado. En conclusión, muchas veces los componentes no pueden conocer las entidades con las que se comunican realmente, por lo que la confianza no puede ser medida, incluso si se consideran técnicas indirectas.R. Hussain et al., 2016

Para abordar estos problemas, proponemos un método de evaluación de confianza centrado en los datos. En nuestra solución, la fiabilidad de cada dato recibido por una cierta entidad de VANETs se evalúa de manera independiente, sin ser necesario conocer todos los componentes en el sistema o acumular información sobre los comportamientos pasados de las otras entidades de VANETs. Para hacerlo, definimos el concepto de çadena de custodia"(CoC) de un dato, así como la noción de "nivel de garantía.ªsociado con la CoC.

Otros trabajos se centran en la descripción de obligaciones y políticas que los sistemas de VANETs deben implementar para ser confiables Gazdar et al., 2022; J. Zhang et al., 2010. Lenguajes como WS-policy Anderson y Devaraj, 2005 o XACML Standard, 2013 suelen ser analizados. El principal problema de estos lenguajes es la dificultad para describir políticas generales de bajo nivel considerando las enormes diferencias de un escenario de VANETs a otro (ya que las aplicaciones objetivo afectan de manera muy fuerte el tipo de dispositivos de hardware a ser desplegados en el sistema, y no se pueden encontrar características comunes entre dos sistemas de VANETs arbitrarios).

En comparación con estas propuestas, la solución presentada se basa en un marco matemático, que es adaptable a cualquier aplicación, sistema o escenario. Además, como el marco propuesto es genérico, puede aplicarse de la misma manera tanto a entidades de VANETs de bajo nivel como de alto nivel.

Finalmente, se han reportado varias arquitecturas para sistemas de VANETs enfocadas en mejorar la gestión de la confianza. La mayoría de estas propuestas se basan en la inclusión de nuevos componentes funcionales especiales enfocados en la evaluación de la confianza D. Zhang et al., 2018. Zhang (2018), por ejemplo, propone la inclusión de cinco módulos funcionales diferentes (como un módulo de usuario confiable o un módulo de red confiable), aunque la solución descrita no es evaluada en la práctica. Otro trabajo M. Arshad et al., 2019 describe una o varias capas completamente nuevas, como middleware, enfocadas en la provisión de confianza.

El principal problema de este enfoque es que solo los componentes del nivel adyacente pueden proporcionar y obtener información sobre la confianza. Otras soluciones presentan modificaciones a las capas existentes (como la capa de red) para incluir la provisión de confianza. Así, se han reportado protocolos de enrutamiento modificados Saleh et al., 2017, procesos de handover A. A. Ahmed y Alzahrani, 2019 y procedimientos de establecimiento de sesión Vaibhav et al., 2017. Además, se pueden encontrar arquitecturas que incluyen un

modelo de confianza adaptable. En particular, Vaibhav, A. (2017) propone una solución de provisión de confianza que incluye un selector de motores capaz de aplicar el modelo de cálculo de confianza más adecuado en cada momento. Como idea final, también se han reportado tecnologías de hardware para la gestión de la confianza Amari et al., 2023, aunque no son muy comunes ya que requieren dispositivos de hardware especiales que no son elementos comerciales.

La principal desventaja de los marcos descritos previamente es la necesidad de modificar las arquitecturas existentes (optimizadas para los escenarios de aplicación) para incluir el sistema de provisión de confianza. Los despliegues de VANETs, en general, presentan esquemas complejos que no pueden modificarse fácilmente, por lo que estas nuevas arquitecturas, generalmente, no se emplean en la práctica. Para abordar este desafío, la solución propuesta se basa en redes blockchain transversales que no requieren modificar las arquitecturas existentes; han sido exhaustivamente validadas y permiten proporcionar información de confianza a cada entidad en el sistema.

3.3 Modelos Predictivos para servicios de datos en VANET

Los modelos predictivos representan una herramienta fundamental en una amplia gama de disciplinas. Desde la medicina M. Haris et al., 2023 hasta los Sistemas Ciberfísicos Joe y Ramakrishnan, 2016, estos modelos contribuyen a mejorar el rendimiento de los sistemas. En el ámbito de la investigación de tráfico, existe una inclinación hacia la predicción de ruido Abdel-Halim y Fahmy, 2018, utilizando para ello diversas expresiones matemáticas, generalmente funciones logarítmicas, adaptadas al entorno y la infraestructura específicos para anticipar el impacto acústico de las carreteras.Karabulut et al., 2023

Otro importante grupo de investigaciones se centra en la predicción de la congestión del tráfico T. Li et al., 2020, proponiendo distintos modelos de movilidad según la configuración urbana o de carreteras. Se modelan también comportamientos estacionales para prever atascos en la red vial W. Zhao et al., 2019. Adicionalmente, algunos estudios emplean distribuciones estadísticas y modelos probabilísticos para pronosticar colisiones entre vehículos y animales Chen et al., 2018 o para estimar la sobrecarga mental en ruta Anjaneyulu y Kubendiran, 2022.

Recientemente, también se han aplicado técnicas de análisis de datos modernas Ravi et al., 2019, modelado estocástico Ravi et al., 2018 y control adaptativo Maslekar et al., 2011 para definir modelos predictivos del flujo de tráfico, especialmente en contextos de ciudades inteligentes y sistemas ciberfísicos Alguliyev et al., 2018.

Se han reportado modelos para pronosticar la evolución del tráfico en tiempo real basados en grandes conjuntos de datos Barros et al., 2015, así como modelos predictivos específicos para situaciones críticas Yin et al., 2021. Destacan igualmente los simuladores George y Santra, 2020 y estudios de caso sobre la aplicación de modelos predictivos de tráfico,Irawan et al., 2020; Yuan y Li, 2021.

Por último, los modelos predictivos para VANET suelen ser jerárquicos y consisten en varias capas, donde los niveles inferiores gestionan la correlación entre parámetros físicos y los más abstractos se utilizan para predecir comportamientos humanos y tendencias a largo plazo.Abdel-Halim y Fahmy, 2018 Aunque comúnmente se emplean técnicas de aprendizaje automático en los modelos predictivos, los modelos matemáticos puros ofrecen una mejor comprensión de las relaciones entre las distintas variables. En este trabajo ed Tesis, se utilizan series de Taylor y funciones multivariables.Z. Zhao et al., 2018

3.4 Ejecución segura de servicios colaborativos en VANET

Las redes de vehículo a vehículo (V2V), específicamente las redes ad-hoc vehiculares (VANETs), son fundamentales para mejorar la seguridad vial mediante la mejora de la visibilidad de los vehículos, especialmente cuando los sensores a bordo tradicionales se quedan cortos Ameen et al., 2020; Tripp-Barba et al., 2019.

El papel crucial que desempeñan las VANETs en los sistemas de transporte modernos está siendo cada vez más reconocido, con la capacidad de facilitar la comunicación en tiempo real entre vehículos, mejorando la conciencia situacional y, por lo tanto, mejorando la seguridad vial Bitam et al., 2015. Estas redes se construyen fundamentalmente sobre el intercambio de datos de mapas de obstáculos, proporcionando información valiosa sobre posibles peligros en la carretera, habilitando sistemas de advertencia avanzados y fomentando condiciones de conducción más seguras en general.

Sin embargo, la precisión, integridad y seguridad de estos datos son de suma importancia, ya que cualquier inexactitud o compromiso podría llevar a una percepción incorrecta de los peligros y posiblemente a consecuencias catastróficas Obaidat et al., 2020; Sheikh et al., 2020. Por lo tanto, se requiere un esfuerzo sustancial para mantener estas características de los datos mientras se habilita un intercambio de datos eficiente y rápido Razzaque et al., 2013.

La investigación de la detección de obstáculos para vehículos tiene una rica historia, que se remonta a los años 80 y 90, antes de la llegada de la tecnología de conducción autónoma Bernini et al., 2014; Parekh et al., 2022. Las técnicas iniciales se centraron principalmente en la detección de obstáculos para evitar colisiones, a menudo descuidando el aspecto crucial del intercambio de datos entre vehículos. Sin embargo, los avances tecnológicos han remodelado este dominio. Cámaras de alta resolución y sensores sofisticados como el LIDAR han elevado los métodos de detección, mejorando considerablemente su fiabilidad y precisión Ahangar et al., 2021; Badrloo et al., 2022. En consecuencia, los métodos de detección evolucionados proporcionan una comprensión más completa del entorno de conducción, contribuyendo significativamente a reducir los incidentes de colisión D. Xie et al., 2019.

A pesar de estos avances, quedan desafíos para asegurar un intercambio eficiente de datos de obstáculos, crucial para la funcionalidad integral de las redes V2V. Por lo tanto, la tecnología blockchain, conocida por sus ventajas de seguridad y descentralización, ha visto su aplicación en el espacio de comunicación V2V. Pero aún se descuida su potencial para habilitar el mapeo coordinado de obstáculos, un aspecto significativo de las VANETs Dibaei et al., 2021; Dwivedi

et al., 2022. Sin embargo, Blockchain ha sido empleada con éxito en otros subsistemas de VANET. Principalmente como tecnología habilitadora para transmisiones de datos seguras o intercambio de claves.

Ampliando la investigación emocionante e innovadora en sistemas de comunicación V2V habilitados por blockchain, varios investigadores han presentado métodos y arquitecturas prometedores para mejorar la seguridad y eficiencia dentro de las VANETs. Shrestha et al. Q. Feng et al., 2019 introdujeron un nuevo sistema blockchain que asegura el intercambio seguro de mensajes dentro de VANET. El sistema utiliza las características de inmutabilidad y transparencia de blockchain para validar la autenticidad de los mensajes transmitidos, mejorando así la confiabilidad de las comunicaciones VANET. Además, Ma et al. Ma et al., 2020 propusieron un mecanismo de gestión de claves descentralizado que proporciona seguridad robusta en VANET. Aprovechando la naturaleza descentralizada de blockchain, los autores construyeron un sistema que elimina los puntos únicos de falla, mejorando así la robustez y fiabilidad de la gestión de claves en VANET. Adicionalmente, Luo et al. Luo et al., 2019 presentan un esquema de protección de privacidad de ubicación basado en confianza y habilitado por blockchain en VANET. Este esquema utiliza blockchain para crear un modelo descentralizado y basado en la confianza que protege la privacidad del usuario mientras asegura una comunicación V2V segura. Pero ninguna de estas soluciones está diseñada para proteger la información de obstáculos o asegurar eficiencia o escalabilidad.

Solo muy pocos autores han reportado soluciones de mapeo de obstáculos seguras habilitadas por Blockchain en VANETs. El sistema StarlingBerlin y Bakker, 2015 es probablemente el más prometedor y popular. Starling es una solución innovadora diseñada para mejorar la seguridad vial Miehle, 2020. Este sistema aprovecha las fortalezas de la tecnología blockchain, ofreciendo almacenamiento y recuperación seguros de datos de obstáculos viales Baldini et al., 2013. El diseño del sistema tiene como objetivo minimizar los problemas tradicionales asociados con el intercambio de datos de obstáculos, abriendo el camino para comunicaciones V2V más seguras y eficientes. El sistema Starling propuesto se construye sobre una arquitectura abierta en capas que abarca seis subsistemas autónomos en tres capas jerárquicas (ver Figura 3.2). Este diseño proporciona una red estructurada y eficiente para la comunicación, haciendo que el sistema sea capaz de manejar comunicaciones V2V complejas con facilidad Math et al., 2015.

El sistema Starling involucra a tres actores centrales: vehículos, propietarios de vehículos y autoridades de aplicación de la ley Lu et al., 2019. Cada actor tiene roles y requisitos únicos dentro de la red, lo que dicta su interacción única con el sistema Guerrero-Ibáñez et al., 2013. La Figura 3.3 representa esas interacciones. Los vehículos se comunican con el sistema a través de la interfaz VehicleClient, situada en la capa más alta del sistema, la Capa de Cliente. Esta interfaz permite a los vehículos acceder al Repositorio de Obstáculos ubicado en la Capa de Obstáculos, permitiéndoles registrar y recuperar datos de obstáculos Cui et al., 2021. Esta característica permite un sistema de navegación más dinámico y adaptable, mejorando así la eficiencia del tráfico y la seguridad. Una utilidad adicional proporcionada por la interfaz VehicleClient es el VehicleIdentifier. Las autoridades de aplicación de la ley pueden solicitar este identificador durante las investigaciones, inculcando responsabilidad y fomentando comportamientos de conducción responsable Yeh et al., 2022. Esta medida

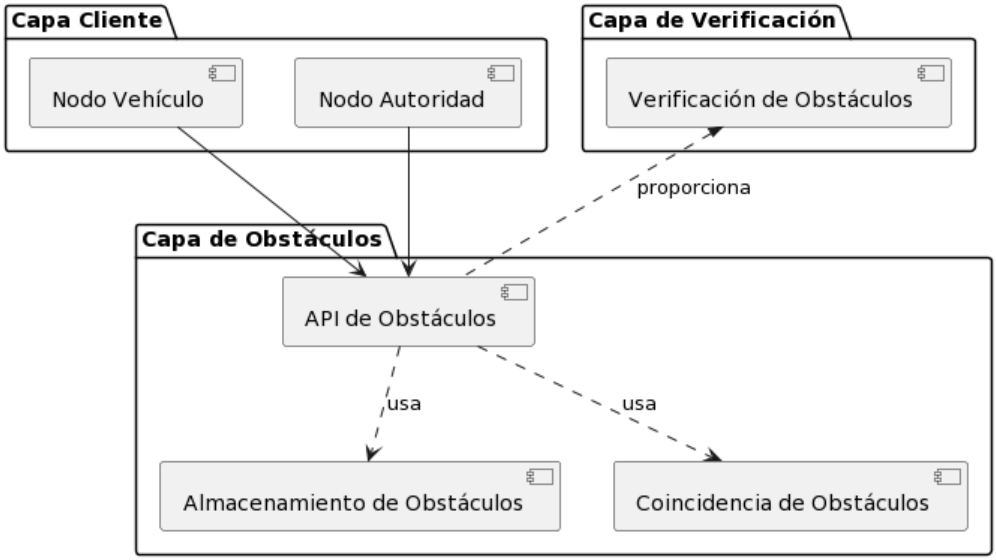

Figura 3.2: Modelo de descomposición de subsistemas del sistema Starling estándar.

de responsabilidad sirve para proteger la integridad del sistema y mejorar la seguridad que proporciona.

Pero Starling y las otras soluciones anteriores encontraron problemas como alta latencia en la generación de alias, comunicación V2V y Vehículo-a-RSU ineficiente debido a la limitada presencia de Unidades al Lado del Camino (RSUs), y costos computacionales incrementados de los nodos compitiendo para agregar bloques al blockchain Mollah et al., 2020; L. Zhang et al., 2019. Todos estos problemas abiertos resultan en una muy pobre escalabilidad y eficiencia; lo cual previene la implementación de estos esquemas novedosos en aplicaciones de transporte reales. Estos desafíos resaltan la necesidad de soluciones más efectivas e innovadoras en este campo, y este documento tiene como objetivo llenar ese vacío.

3.5 Mitigación de amenazas y estrategias defensivas en VANET: Blockchain

En esta sección analizamos el estado del arte en soluciones Blockchain para VANETs, y los ciberataques más críticos y peligrosos y sus estrategias de mitigación potenciales. Más adelante se discuten los beneficios, mejoras y ventajas logradas por la tecnología Blockchain en este campo.

3.5.1 Mitigación de amenazas en VANET

Las redes ad hoc vehiculares (VANETs) son una forma específica de redes ad hoc móviles (MANETs) que conectan vehículos en movimiento. El objetivo principal de las VANETs es proporcionar seguridad vial, gestión del tráfico y varios servicios de infotenimiento. Debido a la naturaleza crítica de estos servicios, la seguridad de los datos, la privacidad y la comunicación confiable son de suma importancia. Sin embargo, la naturaleza altamente dinámica

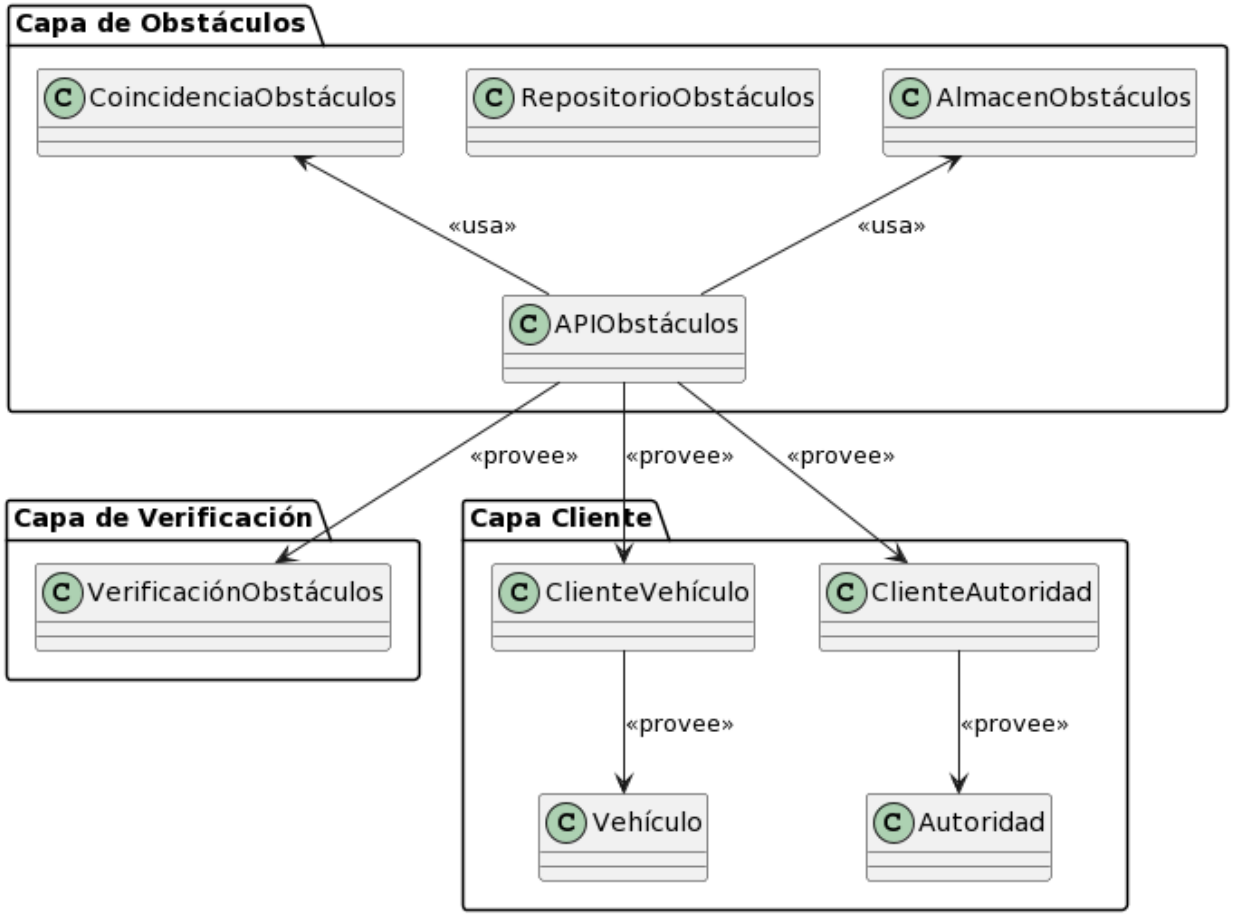

Figura 3.3: Modelo de análisis de objeto del sistema Starling.

y distribuida de las VANETs presenta desafíos únicos para mantener estos aspectos. Las medidas de seguridad tradicionales a menudo son inadecuadas debido a la ausencia de una infraestructura fija, alta movilidad y el ambiente heterogéneo en las VANETs C. Lin et al., 2022.

Las redes ad hoc vehiculares (VANETs) son altamente susceptibles a varias formas de ataques, incluyendo la denegación de servicio, suplantación de identidad y la propagación de información falsa, entre otros Cui et al., 2021; Grover, 2022. Los mecanismos de seguridad tradicionales a menudo no son suficientes para asegurar adecuadamente estas redes debido a sus características únicas como alta movilidad y densidades de nodos variables. La Infraestructura de Clave Pública (PKI) ha sido ampliamente utilizada pero viene con limitaciones al tratar con interacciones vehiculares de alta velocidad y corto alcance Guerrero-Ibáñez et al., 2013; Joshi et al., 2020.

Los sistemas tradicionales de PKI se basan en la suposición de interacciones relativamente estables y prolongadas entre entidades. Sin embargo, las VANETs se caracterizan por movimientos de alta velocidad y encuentros fugaces entre vehículos. Esta naturaleza dinámica puede llevar a varios problemas con PKI, tales como:

- **Cambio Rápido de Contexto:** El ambiente de rápido movimiento puede superar la capacidad de PKI para actualizar y validar certificados, llevando a retrasos o errores en la autenticación.
- **Preocupaciones de Escalabilidad:** El volumen masivo de interacciones de alta frecuencia requiere que un sistema PKI maneje un número significativo de validaciones de certificados dentro de un marco de tiempo mínimo, lo cual puede ser un cuello de botella para la escalabilidad.
- **Latencia en la Revocación de Certificados:** La naturaleza sensible al tiempo de revocar certificados comprometidos puede estar en desacuerdo con los tiempos de interacción rápidos, permitiendo potencialmente el acceso no autorizado.

Recientemente, la tecnología Blockchain ha mostrado promesa en mejorar la seguridad de las VANETs al proporcionar un enfoque descentralizado que podría resolver muchos de los desafíos asociados con las arquitecturas tradicionales Goyal et al., 2010; Ilyas et al., 2017:

- **Descentralización:** Blockchain opera en una red de pares que soporta inherentemente la naturaleza dinámica y descentralizada de las VANETs, facilitando verificaciones más rápidas y eficientes.
- **Validación Inmediata:** Las transacciones y comunicaciones en una red blockchain pueden ser validadas en tiempo real, lo cual se alinea bien con los requisitos de alta velocidad de las VANETs.
- **Registro Inmutable:** El libro de blockchain proporciona un registro a prueba de manipulaciones de todas las transacciones, incluidas autenticaciones e intercambios de datos, mejorando la confianza en las comunicaciones vehiculares.

Varios estudios han investigado la aplicación de blockchain en la gestión de intercambios de datos seguros y confiables en VANETs. En la siguiente Figura 3.4, se presenta una vista general de las arquitecturas basadas en Blockchain en VANETs. Como se puede ver, mientras que las comunicaciones de entrada en las redes Blockchain requieren una configuración criptográfica específica y una interfaz de servicio (solo implementada en la RSU), los datos validados de salida se publican como eventos públicos (los flujos de salida en redes Blockchain solo pueden gestionarse como eventos) y el nodo vehicular puede capturar esa información sin la intervención de la RSU.

Por otro lado, el campo en evolución del cálculo de confianza ofrece varios enfoques para mejorar la seguridad de las VANETs. Los métodos para calcular la confianza pueden dividirse ampliamente en categorías basadas en fusión de múltiples pesos Ding et al., 2010; Q. Li et al., 2012, inferencia bayesiana (BI) Fan y Wu, 2019; Sultan et al., 2022, teoría de Dempster-Shafer (D-S) Najafi et al., 2021, lógica difusa Soleymani et al., 2017; D. Sun et al., 2016, y lógica subjetiva de tres valores (3VSL) Bounaira et al., 2024; S. Li et al., 2023. La inferencia bayesiana ha demostrado ser particularmente adecuada para el juicio cuantitativo de confianza interactiva en el contexto de las VANETs Xia et al., 2019.

Otros autores enfatizan la preocupación urgente de ciberataques en datos almacenados en servidores en la nube M. Zhou et al., 2010. O señalaron la vulnerabilidad de las VANETs a

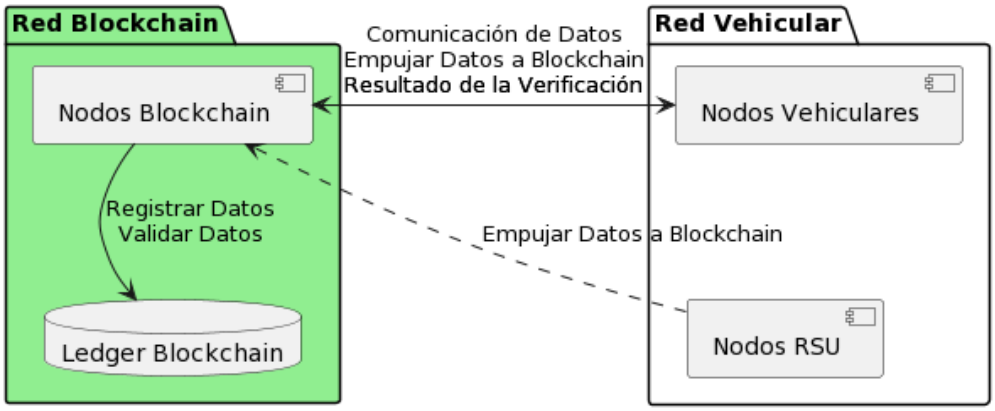

Figura 3.4: Arquitectura Basada en Blockchain para VANETs

estos ataques debido a la naturaleza crítica y sensible de los datos que manejan Sheikh et al., 2020. Se propuso un enfoque descentralizado usando tecnología blockchain para proteger estos datos Sharma et al., 2019. Al emplear técnicas criptográficas, la información fue encriptada, reforzando así su confidencialidad y anonimato Diffie y Hellman, 2022. Sin embargo, también se observaron limitaciones, principalmente con respecto a la escalabilidad y el alto poder computacional requerido para estos procesos criptográficos Narayanan et al., 2016.

El enfoque se desplazó hacia la centralización de la gestión de datos en VANETs, que tradicionalmente depende de sistemas mantenidos por proveedores de servicios vehicularesIlarri et al., 2015Sharma et al., 2019. Se reconocieron los riesgos asociados con tal configuración, incluyendo fallas del sistema y desacuerdos de protección Soleymani et al., 2015J. Feng et al., 2020. Para abordar estas preocupaciones, se propuso un diseño arquitectónico basado en blockchain que emplea identidad soberana para mejorar la seguridad de los datos y utiliza un proceso de autenticación basado en capacidades de múltiples niveles Lücking et al., 2021Q. Feng et al., 2019. Aunque prometedor, la investigación también destacó la necesidad de una estandarización robusta para asegurar la integración y interoperabilidad sin fisuras del sistema propuesto INEN, 2017.

En respuesta al aumento exponencial en dispositivos conectados inalámbricamente Cardoso et al., 2015, se señalaron las limitaciones de la computación en la nube para abordar efectivamente las preocupaciones de seguridad asociadas M. Zhou et al., 2010. Se propuso una estructura basada en blockchain diseñada específicamente para VANETs, enfocándose en resolver problemas de rendimiento y escalabilidad Sharma et al., 2019. Los resultados mostraron una mejora en la gestión de datos y seguridad. Sin embargo, también se plantearon preocupaciones sobre las complejidades de implementación al integrar tecnología blockchain en sistemas VANET existentes Atlam et al., 2018.

La característica principal de blockchain que beneficia a las VANETs es su naturaleza descentralizada, que elimina la necesidad de una autoridad central, reduciendo el riesgo de fallos de un único punto y posibles cuellos de botella en el flujo de datos. Además, la transparencia e inmutabilidad de la tecnología blockchain aseguran la integridad de los datos, haciéndolos resistentes a la manipulación y falsificación Dorri et al., 2016.

Varios problemas de seguridad como la falsificación, denegación de servicio y amenazas de robo de tarjetas inteligentes que afectan a las VANETs fueron abordados Viriyasitavat et al., 2019. Se presentó un sistema de autenticación y autorización habilitado para blockchain para VANETs, que gestionó eficientemente la privacidad y la integridad de la información Uddin et al., 2021. A pesar de las contribuciones, se reconoció la necesidad de una mayor optimización para mejorar la eficiencia del sistema, especialmente bajo condiciones de alta carga de red.

Finalmente, se exploró cómo las VANETs dependen de un intermediario financiero de terceros para compartir información electrónicamente Ferrag et al., 2018. Se argumentó un cambio de paradigma hacia blockchain, eliminando la necesidad de una autoridad central y fomentando un entorno más transparente y sin confianza Eze et al., 2019. Se desarrolló una plataforma habilitada para blockchain para facilitar el intercambio de información entre dominios Akram et al., 2020. Sin embargo, también se destacó la necesidad de algoritmos de consenso eficientes para gestionar efectivamente el tráfico de red aumentado Torky y Hassanein, 2020. A pesar de ello, la combinación de VANETs y tecnología blockchain tiene un gran potencial para abordar los diversos desafíos de seguridad enfrentados por las VANETs Cao et al., 2019.

3.5.2 Ventajas y beneficios de la tecnología Blockchain

La arquitectura descentralizada inherente de Blockchain facilita la verificación y trazabilidad precisa de datos sin depender de entidades autoritativas centrales, mitigando significativamente las vulnerabilidades a una amplia gama de amenazas cibernéticas Sharma et al., 2019. La inmutabilidad del libro de contabilidad garantiza la permanencia de cada transacción o evento vehicular registrado, asegurando así la integridad de los datos y permitiendo procesos de auditoría confiables y verificación cruzada por participantes de la red autenticados Grover, 2022.

La integración de Blockchain dentro de las VANETs no solo fortalece el marco de seguridad sino que también introduce un paradigma eficiente para gestionar los datos de ubicación vehicular Patil et al., 2021. Cada entidad, ya sea un nodo vehicular o una unidad de borde de carretera, se convierte en un componente integral del mecanismo de consenso de Blockchain, asegurando la autenticidad y la actualidad de los datos compartidos Lei et al., 2020.

Los contratos inteligentes se ejecutan de manera autónoma en Blockchain, agilizando el proceso de validación para los datos de ubicación y movimiento. Esta automatización elude la necesidad de verificación manual, mejorando así la eficiencia funcional de los sistemas de transporte inteligente Joshi et al., 2020. Además, los principios de inmutabilidad y transparencia que son fundamentales para Blockchain proporcionan una plataforma confiable para el intercambio de datos de seguridad críticos, como alertas de tráfico y actualizaciones de estado de vehículos Malik et al., 2018.

Al aprovechar las características intrínsecas de blockchain (su descentralización, transparencia e inmutabilidad), facilitamos un cambio de paradigma en cómo se autentica y gestiona la información vehicular. Este cambio no solo aumenta la confiabilidad del sistema, sino que también eleva la verificabilidad de los datos a niveles sin precedentes. A través del marco habilitado por blockchain, cada vehículo se convierte en un nodo dentro de una vasta red

interconectada, contribuyendo y beneficiándose de un conjunto colectivo de datos compartidos de posición y movimiento. Los algoritmos de consenso intrínsecos a la tecnología blockchain aseguran que solo los datos verificados y autenticados se añadan al libro de contabilidad. Este proceso neutraliza efectivamente los riesgos de datos manipulados o falsificados, que de otro modo podrían llevar a resultados catastróficos en la navegación y coordinación vehicular en tiempo real C. Lin et al., 2020.

Además, la implementación de contratos inteligentes automatiza la aplicación de reglas y políticas predefinidas, que rigen los procesos de compartir y validar datos. Estos contratos inteligentes, una vez desplegados, actúan sin la necesidad de supervisión centralizada, asegurando así que los vehículos operen dentro de las pautas acordadas, manteniendo la integridad y fiabilidad de la red vehicular.

El libro de contabilidad de blockchain proporciona un registro permanente, a prueba de manipulaciones, de todas las actividades vehiculares, creando una fuente de datos confiable para procesos analíticos y de toma de decisiones. También sirve como un punto de referencia inmutable para fines de auditoría y legales, mejorando la rendición de cuentas dentro de la red. Como tal, la integración de la tecnología blockchain en VANETs presenta una solución robusta a los desafíos de seguimiento, posicionamiento y movimiento de vehículos, estableciendo un nuevo estándar para la seguridad y eficiencia en los sistemas de transporte inteligente Javed et al., 2022.

Capítulo 4

Arquitectura de servicios para la provisión de confianza en VANET mediante Blockchain

En este Capítulo se desarrolla un marco teórico para la confianza en VANETs, que contempla una descripción matemática precisa de la confianza. Gracias a esta propuesta, permitimos la evaluación y valoración fiable de la confianza entre nodos vehiculares, facilitando la identificación y mitigación de posibles amenazas de seguridad y vulnerabilidades dentro de una VANET.

Mediante esta contribución, alcazamos el **Objetivo#1** de este proyecto de Tesis.

El capítulo incuye una validación experimental de las contribuciones realizadas, con lo que alcanza también el **Objetivo#8**.

4.1 Introduction

En la actualidad, la sociedad muestra una creciente preocupación por los riesgos asociados a los dispositivos conectados en red. De hecho, el número de soluciones de protección para computadoras, tabletas y otros dispositivos tradicionales ha aumentado de manera rápida e increíble en los últimos cinco años, convirtiéndose ahora en uno de los mercados más prometedores Boeckl et al., 2019. Sin embargo, las nuevas tendencias en el mundo tecnológico presentan desafíos y problemas adicionales que, en general, son invisibles para los usuarios comunes Bordel et al., 2017. Uno de estos nuevos sistemas tecnológicos que requiere atención especial son las Redes Ad hoc Vehiculares (VANETs).

Las VANETs proponen incrustar capacidades de comunicación en cada objeto, escenario o situación. Como característica principal, este paradigma implica contar con un acceso ubicuo a Internet, lo que complica la aplicación de instrumentos tradicionales de ciberprotección, como la ingeniería de tráfico o los firewalls.

Además, la actual arquitectura de Internet (propuesta en los años 90 y denominada Ïnternet

de las computadoras"R. Khan et al., 2019) se basa en la conexión de cientos de millones de máquinas de alta capacidad, con suministro de energía, que muestran un comportamiento similar e, incluso, una infraestructura de hardware uniforme. No obstante, cada uno de los nuevos escenarios de VANETs está compuesto por miles de dispositivos heterogéneos, causando que, globalmente, varios miles de dispositivos estén actualmente conectados Gershenfeld et al., 2004. Además, como hemos dicho, estos dispositivos son muy heterogéneos, por lo que los mecanismos regulares de ciberprotección basados en las suposiciones de la Ïnternet de las computadoras"(interoperabilidad total, empleo del modelo de referencia OSI, diseños basados en contraseñas, etc.) no son adecuados en absoluto. De hecho, la compañía Hewlett Packard informó en 2015 que más del 70 % de los dispositivos VANET presentan debilidades a pesar de utilizar soluciones comunes de ciberprotección Elemike et al., 2019.

El alto nivel de heterogeneidad y la limitada capacidad de cómputo de los dispositivos, junto con la gran escala de los sistemas VANETs (que genera problemas graves de escalabilidad) y la gran diversidad de escenarios de aplicación dificultan el uso de soluciones de ciberprotección regulares. Sin embargo, para lograr la plena aceptación de los usuarios, las empresas y los gobiernos, es necesario definir políticas de ciberprotección válidas. En particular, se necesitan soluciones relacionadas con tres aspectos diferentes: seguridad, privacidad y confianza Weber, 2010.

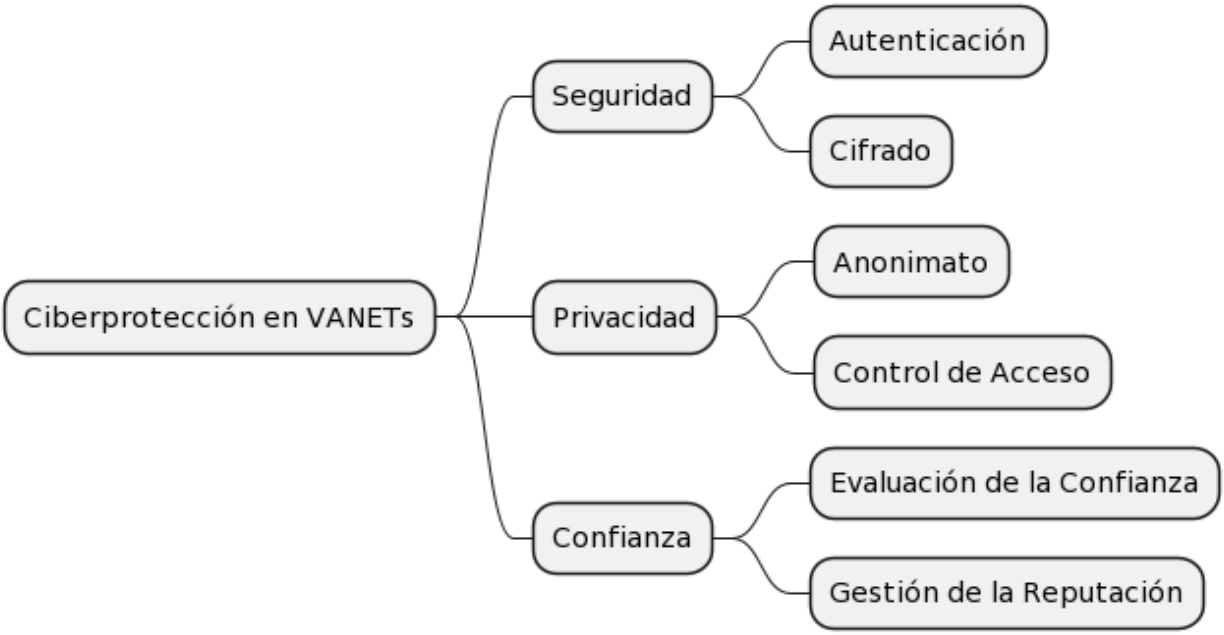

Figura 4.1: Temas relacionados con la ciberprotección en VANETs

Como se puede ver en la Figura 4.1, los términos seguridad y privacidad incluyen conceptos muy conocidos como la autenticación y la encriptación. Por lo tanto, la mayoría de los trabajos sobre gestión de protección para VANET tratan estos temas, ya que son conocimientos consolidados Tabrizi y Ibrahim, 2016; Weber, 2013.

Por el contrario, la confianza es una noción compleja sobre la cual no hay consenso. Además, cuestiones importantes como su definición, métricas o metodologías de evaluación raramente se abordan X. Wang et al., 2018. Entonces, aunque la mayoría de los autores coinciden en que la confianza es un elemento clave en los escenarios de VANETs, existe una falta de discusiones sobre la provisión de confianza (aparte de las iniciativas legislativas que no abordan los desafíos técnicos).

Por lo tanto, el objetivo de este documento es establecer un marco teórico para la confianza en escenarios de VANETs, incluyendo sus propiedades más importantes. El marco propuesto está compuesto por una descripción matemática de la confianza y una lista de los requisitos que debe cumplir una solución para la provisión de confianza (incluyendo su evaluación y valoración). Un análisis de la formalización propuesta y los requisitos muestra que la tecnología blockchain Sheikh et al., 2019 se ajusta perfectamente a ellos, por lo que también se proporciona un primer sistema de provisión de confianza basado en redes blockchain.

4.2 Propuesta de Solución

En esta sección se describe la solución técnica propuesta. En la primera subsección se presentan las definiciones básicas y la formalización matemática. En la segunda subsección, se revisan los requisitos de los sistemas de provisión de confianza en los escenarios de VANETs y se describe la solución propuesta basada en redes blockchain.

La creciente complejidad y dinamismo de las Redes Ad hoc Vehiculares (VANETs) exigen soluciones innovadoras para garantizar la confianza y seguridad en este tipo de redes. La confianza en VANETs es crítica, ya que las decisiones basadas en información no fiable pueden tener consecuencias graves en términos de seguridad vial y protección de la privacidad. Por ello, proponemos una solución basada en la tecnología blockchain, conocida por su capacidad para ofrecer transparencia, inmutabilidad y descentralización.

4.2.1 Definiciones Básicas y Formalización Matemática

Antes de adentrarnos en la solución propuesta, establecemos algunas definiciones básicas y la formalización matemática que sustenta nuestra propuesta:

- **Entidad VANET:** Cualquier componente de la red, ya sea un vehículo, un sensor de tráfico o un semáforo inteligente, que puede generar, recibir o transmitir información.
- **Confianza:** Medida de creencia en la fiabilidad, integridad y capacidad de una entidad VANET para actuar de manera esperada en un contexto determinado.
- **Blockchain:** Tecnología de registro distribuido que mantiene una lista creciente de registros, llamados bloques, los cuales están protegidos y conectados usando criptografía.

La formalización matemática de la confianza en el contexto de VANETs se basa en la evaluación de las interacciones entre entidades a lo largo del tiempo, considerando factores como la frecuencia de las comunicaciones exitosas, la relevancia de la información compartida y la consistencia en el comportamiento.

$$T_{A,B} = f(\text{interacciones exitosas}, \text{relevancia}, \text{consistencia}) \tag{4.1}$$

Esta fórmula indica que la confianza T entre las entidades A y B se calcula como una función f de tres variables: las interacciones exitosas entre las entidades, la relevancia de esas interacciones y la consistencia en el comportamiento de las entidades.

4.2.2 Requisitos de los Sistemas de Provisión de Confianza en VANETs

Para que un sistema de provisión de confianza sea efectivo en VANETs, debe cumplir con los siguientes requisitos:

- **Escalabilidad:** Capacidad de gestionar eficazmente un número creciente de entidades y transacciones.
- **Adaptabilidad:** Flexibilidad para ajustarse a diferentes escenarios y dinámicas de la red.
- **Resiliencia:** Fortaleza frente a intentos de manipulación o ataques a la red.
- **Privacidad:** Protección de la identidad y datos de las entidades contra accesos no autorizados.

La solución propuesta emplea redes blockchain para satisfacer estos requisitos. La blockchain actúa como un libro de contabilidad distribuido que registra todas las transacciones e interacciones entre entidades de manera transparente y segura. Cada transacción es verificada por nodos de la red antes de ser añadida a un bloque, lo que garantiza la integridad de la información.

Además, la naturaleza descentralizada de la blockchain proporciona una alta resiliencia contra ataques y manipulaciones, mientras que técnicas avanzadas de criptografía aseguran la privacidad de los usuarios.

4.2.3 Definición de Confianza y Formalización Matemática

En el ámbito de las Redes Ad hoc Vehiculares (VANETs), la confianza es un elemento crucial para asegurar la fiabilidad y seguridad en la comunicación entre vehículos y otros componentes de la red. A continuación, presentamos una formalización matemática para modelar la confianza en VANETs.

Definiciones Básicas:

- **Entidad de VANET (e):** Cualquier componente de la red, como vehículos, semáforos inteligentes o sensores de tráfico.
- **Fuente de Datos (S_e):** Conjunto de entidades de VANET que generan, procesan o transmiten datos.

- **Flujo de Datos (Z_e):** Colección generalizada de datos generados, procesados o transmitidos por las fuentes de datos.

Formalización Matemática:

Matemáticamente, la recepción de datos por una determinada entidad de VANET, e, puede modelarse como un proceso estocástico Y_e, que es el resultado de las tareas de procesamiento desarrolladas por un conjunto de K diferentes entidades de VANET, $S_e = \{s_1, s_2, \ldots, s_K\}$, denominadas fuentes de datos. Además, las fuentes de datos pueden considerar entradas adicionales que, como cualquier otra recepción de datos, pueden modelarse también como una colección de MX procesos estocásticos $X_e = \{X_1, X_2, \ldots, X_{MX}\}$ (en el caso general, $K \neq M$ ya que no cada fuente de datos presenta una entrada única). Además, se puede definir una colección generalizada de $MY = MX + MW$ flujos de datos $Z_e = \{Z_1, Z_2, \ldots, Z_{MY}\} = \{X_1, \ldots, X_{MX}, W_1, W_2, \ldots, W_{MW}\}$, no solo considerando las entradas a las fuentes de datos X_e, sino también los MW estados intermedios del dato recibido $W_e = \{W_1, W_2, \ldots, W_{MW}\}$.

En cada instante de tiempo $t = t_i$, el proceso estocástico Y_e se convierte en una variable aleatoria $Y_{e_{t_i}}$ en el espacio muestral Ω_Y que contiene todos los posibles mensajes recibidos (Ω_Y es, entonces, un conjunto discreto). La misma consideración puede hacerse sobre el conjunto de procesos estocásticos X_e.

Entonces, se puede definir una función de múltiples variables $F_e : (\Omega_{X_1} \times \Omega_{X_2} \times \ldots \times \Omega_M \times \mathbb{R}^+) \to \Omega_Y$ (llamada función de procesamiento) que representa las acciones de composición y procesamiento realizadas por las fuentes de datos, y depende del tiempo de dos maneras: a través de los procesos estocásticos (que son dependientes del tiempo) y explícitamente. Así, $Y_e = F_e(X_1, X_2, \ldots, X_M, t)$. En general, sin embargo, cada una de las fuentes de datos realiza una acción diferente o un conjunto de acciones, siguiendo un proceso incremental. Entonces, en general, F_e puede entenderse como la composición generalizada de $N = K + J$ funciones f_i que representan, por un lado, las acciones de cada fuente de datos h_i (que suma un total de K funciones) y, por otro lado, los posibles efectos maliciosos de los ciberataques en la operación del sistema g_i (representado por J funciones).

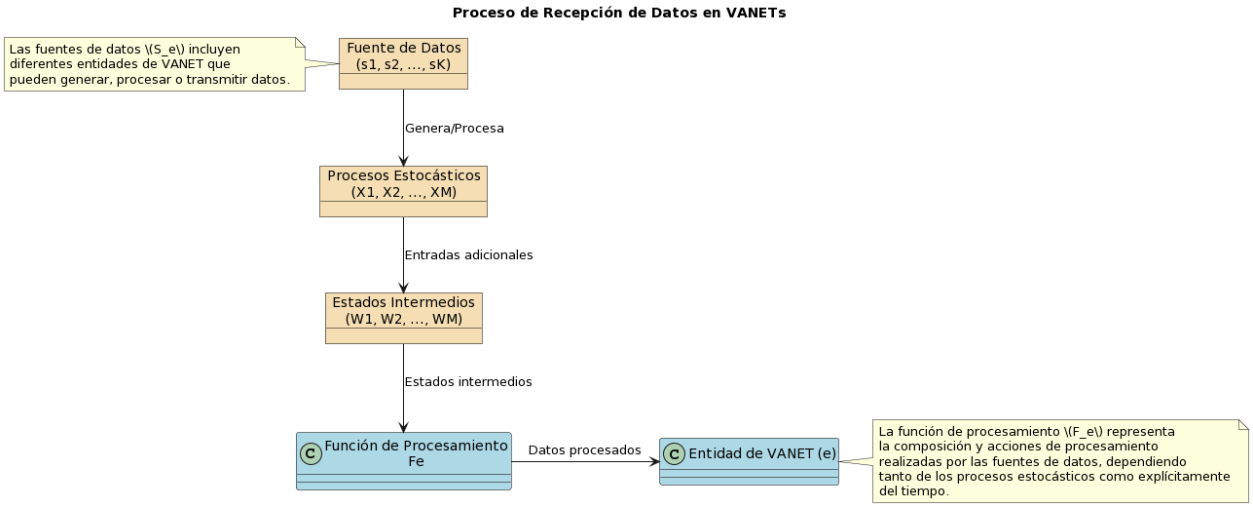

Figura 4.2: Proceso de Recepción de Datos en VANETs

Como vemos en la Figura 4.2 consideramos que la recepción de datos en una entidad de VANET puede modelarse como un proceso estocástico Y_e, resultado de las tareas desarrolladas por un conjunto de K diferentes entidades de VANET, denominadas fuentes de datos $S_e = \{s_1, s_2, \ldots, s_K\}$.

Además, definimos un conjunto generalizado de flujos de datos $Z_e = \{Z_1, Z_2, \ldots, Z_{MY}\} = \{X_1, \ldots, X_{MX}, W_1, W_2, \ldots, W_{MW}\}$, que incluye tanto las entradas a las fuentes de datos X_e, como los estados intermedios del dato recibido W_e.

La confianza en el contexto de VANETs se define como la creencia en la fiabilidad de los datos recibidos, basada en el procesamiento legítimo de datos por fuentes legítimas. Matemáticamente, esto se representa como:

$$Y_e = F_e(X_1, X_2, \ldots, X_M, t). \tag{4.2}$$

Donde F_e es una función que representa las acciones de composición y procesamiento realizadas por las fuentes de datos en función del tiempo.

$$F_e = f_1 \circ f_2 \circ \ldots \circ f_N = h_1 \circ h_2 \circ \ldots \circ h_K \circ g_1 \circ g_2 \circ \ldots \circ g_J \tag{4.3}$$

Para determinar si un dato ω_Y es confiable, es necesario verificar la cadena de custodia (CoC) del mensaje, asegurando que proviene de fuentes de datos legítimas y ha sido procesado de manera adecuada. Esto implica validar la información a lo largo de las distintas fases de su ciclo de vida, desde su generación hasta su procesamiento final.

En VANETs, la gestión eficaz de la confianza requiere no solo considerar los eventos y comportamientos pasados, sino también establecer mecanismos robustos para verificar la autenticidad y la integridad de los datos en tiempo real, adaptándose a la naturaleza dinámica de estas redes.

Definición 1 (Confianza):

Dada una entidad específica de VANET e y un mensaje recibido $\omega_Y \in \Omega_Y$ en $t = t_i$, la confianza es la suposición por parte de la entidad e de que el dato recibido ω_Y proviene del procesamiento y composición de datos legítimos por fuentes de datos legítimas.

Es importante destacar que, en las definiciones de confianza centradas en la entidad (Chen et al., 2011), la confianza es una variable continua (que evoluciona a medida que se adquiere información sobre el comportamiento de otras entidades). Sin embargo, la definición propuesta centrada en los datos no considera eventos o comportamientos pasados, por lo que no hay un tiempo de convergencia, sino que la confianza se convierte en una variable binaria: una entidad de VANET confía en el mensaje y lo acepta, o no lo hace y lo descarta.

Por otro lado, las definiciones de confianza centradas en la entidad tradicionales, que generalmente son enfoques basados en el comportamiento, están enfocadas en descubrir si la función de procesamiento F_e oculta un comportamiento malicioso.Al-Shareeda et al., 2020

Matemáticamente, estos enfoques intentan descomponer la función de procesamiento F_e en sus funciones componentes elementales $\{f_i/i = 1, \ldots, N\}$, para establecer si alguna de ellas está afectada por un ciberataque (es decir, si hay una función $g_i \neq Id$ con $i \in [1, \ldots, J]$, siendo Id la función de identidad). Sin embargo, como es muy complicado descomponer una función, la mayoría de las veces (en la práctica) las soluciones centradas en la entidad solo evalúan ciertos aspectos de la función de procesamiento global. Teniendo en cuenta los resultados, y utilizando un árbol de decisiones previamente definido, se establece si está presente o no un componente malicioso oculto.

El enfoque propuesto centrado en los datos es bastante diferente. En lugar de evaluar la función de procesamiento (que puede ser una tarea compleja), la confianza depende de la colección de fuentes de datos S_e y de la colección generalizada de flujos de datos Z_e. La información obtenida sobre estos elementos, al analizar únicamente el mensaje recibido ω_Y, suele ser insuficiente (las entropías condicionales $H(Z_i|Y_e = \omega_Y)$, que miden la incertidumbre restante una vez conocido el mensaje recibido.

Definición 2 (Cadena de Custodia -CoC- de un dato)

La Cadena de Custodia (CoC) de un dato es un registro de su ciclo de vida, diseñado para garantizar que la información recibida no ha sufrido alteraciones, sustituciones, contaminaciones o destrucciones. En particular, verificar la CoC de un dato implica acceder y validar la información sobre cuatro fases básicas en el ciclo de vida del dato:

1. La generación de los datos originales a nivel bajo.
2. El posible almacenamiento de los datos hasta que sean consultados o empleados.
3. La transmisión de los datos a otras entidades de VANET.
4. Los análisis y transformaciones aplicadas a los datos.

La forma en que se genera y almacena la información sobre la CoC depende de la tecnología empleada: los elementos de bajo nivel suelen emplear formatos de datos binarios, mientras que los componentes inteligentes gestionan representaciones de información complejas como archivos XML o semánticos.

Sin embargo, generalmente es registrada por las mismas entidades de VANET que generan, procesan o componen el dato (es decir, las fuentes de datos). Estas entidades, por lo tanto, deben estar provistas de las credenciales necesarias para poder acceder al sistema de almacenamiento.

El concepto de CoC se emplea en varios contextos, desde espectáculos de magia hasta investigaciones legales. Sin embargo, la cantidad de información requerida para validar una CoC es diferente dependiendo del escenario. Esta idea también es válida en los sistemas de VANET. Por ejemplo, en algunas aplicaciones, identificar a las entidades de VANET que transmiten un dato puede ser suficiente para crear una CoC válida; mientras que en otros casos, también puede ser necesario registrar el tiempo, la longitud de los datos o cualquier otra información relevante. En cualquier caso, ningún sistema es capaz de proporcionar un conocimiento total sobre los datos recibidos (o las entidades de VANET, si se considera una

solución centrada en la entidad). Por lo tanto, siempre existe cierta probabilidad de confiar en un dato no fiable, $p_{error} > 0$.

$$p_0 > p_1 > \cdots > p_n > 0 \tag{4.4}$$

Definición 3 (Nivel de Garantía):

El nivel de garantía es un número (generalmente un entero) que representa la cantidad de información (parámetros), el nivel de detalle y/o la granularidad requerida para que una Cadena de Custodia (CoC) sea válida. En la práctica, representa el "nivel de sospecha"de las entidades de VANET: a medida que aumenta el nivel de garantía, se requieren más garantías (pruebas) por parte de las entidades para confiar en los datos. Como consecuencia, a medida que aumenta el nivel de garantía, la probabilidad p_{error} disminuye.

En general, diferentes aplicaciones o servicios en un mismo sistema VANET mostrarían diferentes niveles de garantía: los servicios críticos requerirían un gran nivel de garantía, mientras que una aplicación trivial podría presentar valores bajos para este parámetro. Por lo tanto, una entidad de VANET puede descartar un mensaje recibido (es decir, la entidad no confía en el mensaje porque la CoC asociada no puede ser verificada) ya sea porque no se alcanza el nivel de garantía requerido, o porque la información recibida sobre la CoC muestra que el dato no es confiable.

Todas las discusiones anteriores, además, pueden expresarse matemáticamente. Se puede definir, entonces, la función de confianza $T_e : \Omega_Y \to \mathbb{Z}_2$ de una cierta entidad de VANET e, que recopila la información sobre la CoC de cada dato recibido y la verifica. La salida binaria obtenida determina si los datos son confiables o no. En particular, la función de confianza puede entenderse como la composición de dos funciones.

$$T_e = t_v \circ t_t = t_v(t_t(\cdot)) \tag{4.5}$$

La primera función es la función de seguimiento $t_t : \Omega_Y \to \mathbb{R}^{p(w)}$. Para cada dato recibido ω_Y genera un vector real de dimensión $p(w)$, siendo $p : \mathbb{N} \to \mathbb{N}$ una función positiva definida monótonamente creciente y w el nivel de garantía requerido por la entidad e. Este vector representa la información sobre la CoC del mensaje ω_Y. En general, como la CoC puede incluir mucha información, se almacenará en componentes externos especializados. La función de seguimiento, entonces, busca esta información y la adquiere. Además, a medida que w crece, se debe adquirir más información que es coherente con la definición propuesta. Si no hay suficiente información para construir el vector de dimensión $p(w)$, como hemos dicho, la función de confianza T_e devuelve inmediatamente un resultado negativo.

La segunda función es la función de verificación $t_v : \mathbb{R}^w \to \mathbb{Z}_2$. Esta función la realizan las entidades de VANET. Recibe el vector real que representa la información sobre la CoC del dato ω_Y, e intenta verificarlo, determinando si el dato es confiable o no. Se pueden imponer las condiciones deseadas, como que el mensaje original sea generado por un dispositivo autorizado o que la marca de tiempo sea posterior a un cierto valor. La política seleccionada depende

del servicio considerado y puede describirse utilizando cualquiera de los lenguajes disponibles (XACML, por ejemplo). Se puede observar en la Figura 4.3

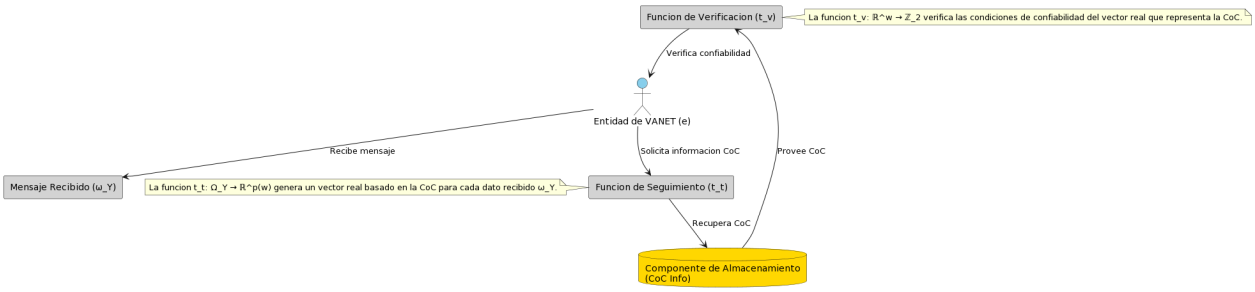

Figura 4.3: Evaluación genérica de la función de confianza en VANETs

Imaginando una solución trivial, una base de datos podría soportar el marco descrito. Sin embargo, debe considerarse un problema práctico oculto, que hace que nuestra propuesta sea muy diferente de las bases de datos usuales o de los esquemas de trazabilidad de datos.

Como hemos dicho, las entidades de VANET no pueden almacenar la información sobre la Cadena de Custodia (CoC) de cada dato en el sistema, ya que no están preparadas para soportar esta funcionalidad de manera inherente. Por lo tanto, se requiere un componente externo especializado. Este componente debe ser capaz de manejar y verificar la CoC de manera eficiente y segura, garantizando así la autenticidad e integridad de los datos en todo momento.

En el contexto de VANETs, donde la velocidad y la fiabilidad son esenciales debido a la naturaleza móvil y dinámica de las entidades involucradas, el uso de una base de datos tradicional para gestionar la CoC podría no ser viable debido a la latencia y la sobrecarga de procesamiento. Por ende, la solución propuesta podría incorporar tecnologías emergentes como las redes blockchain, que ofrecen una verificación descentralizada y en tiempo real, adecuada para el entorno altamente dinámico de VANETs.

La implementación de una cadena de bloques, con su estructura inmutable y resistencia a la manipulación, podría servir como el componente externo especializado necesario. Cada transacción dentro de la cadena de bloques podría representar un evento en la vida de un dato, proporcionando una pista de auditoría completa y segura desde su creación hasta su uso final.

Además, las capacidades de contrato inteligente de las plataformas de blockchain podrían utilizarse para automatizar la verificación de la CoC, reduciendo aún más la necesidad de intervención manual y aumentando la eficiencia del sistema.

Mientras que una solución basada en bases de datos tradicionales podría parecer suficiente para sistemas estáticos, en el ámbito de VANETs es imprescindible buscar soluciones más innovadoras y adaptativas. La propuesta de utilizar blockchain como un sistema de gestión de CoC ofrece una nueva dimensión de seguridad y eficiencia, alineada con las necesidades únicas de las redes vehiculares y la importancia crítica de la confianza y la veracidad de los datos en estos sistemas.

Definición 4 (Propiedad acumulativa de la confianza):

Dado un cierto mensaje ω_Y recibido por una entidad de VANET e, la confianza de la entidad e en el mensaje ω_Y crece siguiendo una ley exponencial, ya que se acumulan evaluaciones estadísticamente independientes de la función de confianza con resultado positivo.

Dado que la independencia física implica independencia estadística, en la práctica para acumular confianza, se deben mantener varios registros independientes de la CoC (así, en cada evaluación de la función de confianza, la información sobre la CoC se rastreará en un registro diferente).

De hecho, matemáticamente, si cada componente en un sistema VANET tiene la misma probabilidad de transmitir un mensaje no fiable, p_0, entonces la probabilidad de que un mensaje sea no fiable cuando n registros independientes de la CoC lo prueban como fiable puede describirse como una función exponencial (4).

$$p_U = \prod_{i=1}^{n} p_0 = p_0^n \tag{4.6}$$

Entonces, la segunda solución consiste en adquirir de manera independiente la información sobre la CoC del dato recibido, de una colección de n registros independientes $R_e = \{r_1, r_2, \ldots, r_n\}$. La idea intuitiva detrás de esta propuesta es que si la misma información es proporcionada por varias fuentes independientes, la probabilidad de que sea verdadera es mayor (un principio muy utilizado, por ejemplo, en periodismo).

Descrita de esta manera, esta segunda solución también requiere realizar varios procesos de seguimiento (como en la primera solución), sin embargo, se pueden considerar dos hechos importantes. Primero, como todos los registros son independientes pero igualmente seguros, el tiempo de acceso es el mismo en todos los casos (por lo tanto, finalmente, para un cierto número de fases de seguimiento, esta segunda opción requiere menos tiempo). Y, segundo y mucho más importante, como todos los registros implementan las mismas interfaces, protocolos y políticas de seguridad, pueden comunicarse y las tareas de almacenar varias copias independientes de la CoC y (más tarde) verificar la consistencia entre todas ellas pueden delegarse en dicha colección de registros (que deben implementarse con una tecnología apropiada). De esta manera, las entidades de VANET solo tienen que realizar una evaluación de la función de confianza y todo el proceso se acelera. Como consecuencia de esta delegación, generalmente, el valor del parámetro n es parte del diseño del sistema y es el mismo para cada entidad de VANET, servicio o aplicación.

4.2.4 Provisión de Confianza Usando Redes Blockchain en VANETs

En el dinámico mundo de las Redes Ad hoc Vehiculares (VANETs), la provisión de confianza se convierte en un elemento crucial para garantizar la integridad, autenticidad y seguridad de la información intercambiada entre vehículos y entidades de infraestructura. Dada la naturaleza móvil y a menudo descentralizada de las VANETs, los métodos tradicionales para el manejo de la confianza y la autenticación pueden no ser suficientes o adecuados para abordar los desafíos únicos que presentan estas redes.

El uso de tecnologías de blockchain aparece como una solución prometedora para superar estas limitaciones. Blockchain, una tecnología emergente conocida por su capacidad para mantener un registro inmutable y descentralizado de transacciones, ofrece un marco de trabajo innovador para la gestión de la confianza en VANETs.

En esta subsección, exploraremos cómo las redes blockchain pueden satisfacer los requisitos esenciales de los sistemas de provisión de confianza centrados en los datos y cómo pueden implementarse eficazmente para mejorar la seguridad y la fiabilidad en VANETs.

Requisitos de la Provisión de Confianza

Diversos trabajos Bangui et al., 2021 han estudiado los objetivos y requerimientos de los sistemas de provisión de confianza. Considerando estos análisis previos y el marco presentado en la sección anterior, obtenemos la siguiente lista de requerimientos para sistemas de provisión de confianza centrados en datos en VANETs:

- REQ#1, Generalidad: Los sistemas de provisión de confianza centrados en datos deben ser genéricos, para ser fácil y ampliamente aplicados a cualquier tipo de servicio o aplicación soportada por la infraestructura VANET.
- REQ#2, Confianza en metadatos: Los sistemas de provisión de confianza también deben ser aplicables a la información de control en la implementación de VANET (como datos de QoS) si se requiere.
- REQ#3, Autoprotección: Los sistemas de provisión de confianza deben detectar efectivamente ataques contra su infraestructura, especialmente intentos de modificar la información almacenada sobre la CoC.
- REQ#4, Preservación de la privacidad: La información sobre la CoC no puede contener ningún dato sobre la identidad de los usuarios, información personal, etc.
- REQ#5, Distribuido: El sistema de provisión de confianza debe estar compuesto por una colección de nodos independientes distribuidos, capaces de almacenar cada uno una copia (completa o parcial, pero coherente con las demás) de la CoC de los datos en el sistema VANET.
- REQ#6, Capacidad de almacenamiento: El sistema de provisión de confianza debe ser capaz de almacenar toda la información sobre la CoC de los datos en el sistema, con el nivel de granularidad (nivel de garantía) requerido.

Un análisis de los requerimientos previamente descritos muestra claramente que la tecnología blockchain Pilkington, 2016 es la más adecuada para implementar sistemas de provisión de confianza centrados en datos.

El objetivo de este artículo no es explicar en detalle cómo funcionan las redes blockchain; sin embargo, se proporciona a continuación una breve descripción general para mostrar que todos los requerimientos se cumplen perfectamente.

Las redes blockchain Comert, 2020 están compuestas por una colección de nodos, manteniendo cada uno una copia (parcial o completa) de los bloques de información que se almacenan

en la red. El objetivo de estas redes es mantener información confiable, dividida en bloques encadenados que se distribuyen entre todos los nodos independientes que conforman la red. De esta manera, el REQ#6 se soporta de forma nativa. Por otro lado, cualquier nuevo bloque añadido a la red se envía por defecto por el nodo receptor a otros nodos para ser almacenado en varias ubicaciones independientes (REQ#5).

Las redes blockchain, además, son agnósticas respecto al contenido de los bloques (que, incluso, pueden ser heterogéneos). Así, pueden almacenar información (CoC) tanto de datos como de metadatos (REQ#2) y sobre cualquier tipo de servicio o aplicación (dispositivos de bajo nivel y aplicaciones de alto nivel pueden incorporar información a la red blockchain de la misma manera).

El REQ#1 se cumple, de esta manera, perfectamente. Además, cada bloque está firmado mediante una función hash, que protege el contenido almacenado. Si se aplica cualquier cambio ilegal, el bloque se corrompe y todos los bloques posteriores encadenados también se invalidan. Si los campos hash fueran recalculados para crear bloques válidos, el nodo afectado consultararía las copias de los bloques modificados mantenidos en otros nodos. Si los bloques modificados no son coherentes con la información almacenada en la red (al menos n nodos deben confirmarlo), los cambios se descartan (por lo que la información sobre la CoC siempre está respaldada por, al menos, n registros independientes, según lo requerido por la propiedad acumulativa de la confianza).

Además, solo los usuarios autorizados (provistos con la clave apropiada) pueden incorporar información a la red blockchain. De esta manera, el REQ#3 se cumple. Finalmente, las redes blockchain no son un sistema de respaldo, por lo que solo se almacena información sobre la CoC de los datos en el sistema VANET (nunca los propios datos). La información personal o las identidades, entonces, no se mantienen y el REQ#4 también se cumple.

La tecnología blockchain, además, presenta un buen comportamiento en relación a otras variables y desafíos importantes como la seguridad en el sistema de aseguramiento, la fiabilidad, la disponibilidad o la inversión. En particular, como una red compuesta por varios pares donde la información se replica extensivamente, la disponibilidad está garantizada en los sistemas blockchain. Además, los pares pueden implementarse utilizando técnicas de software estándar y equipos de hardware regulares, por lo que la inversión no tiene que ser muy alta. La fiabilidad y la seguridad en el sistema de aseguramiento están garantizadas por la arquitectura de los sistemas blockchain. Como la información no está respaldada solo por una máquina, sino por varios hosts geográficamente dispersos y pertenecientes a personas muy diferentes, la solución es altamente fiable por defecto, y la seguridad se proporciona mediante técnicas tradicionales como en cualquier otro sistema computacional.

En el contexto de las Redes Ad hoc Vehiculares (VANETs), asegurar la confianza en la comunicación y el intercambio de datos se ha convertido en un aspecto crítico. Esto se debe a la naturaleza dinámica y a menudo efímera de las interacciones entre los vehículos y la infraestructura vial. Los tradicionales sistemas de provisión de confianza deben evolucionar para abordar los desafíos únicos presentados por VANETs, como la movilidad de alta velocidad, la necesidad de decisiones en tiempo real y la gestión de una gran cantidad de entidades y dispositivos. En este escenario, las redes blockchain emergen como una solución prometedora

debido a su capacidad para proporcionar un registro inmutable y verificable de las transacciones y los datos intercambiados.

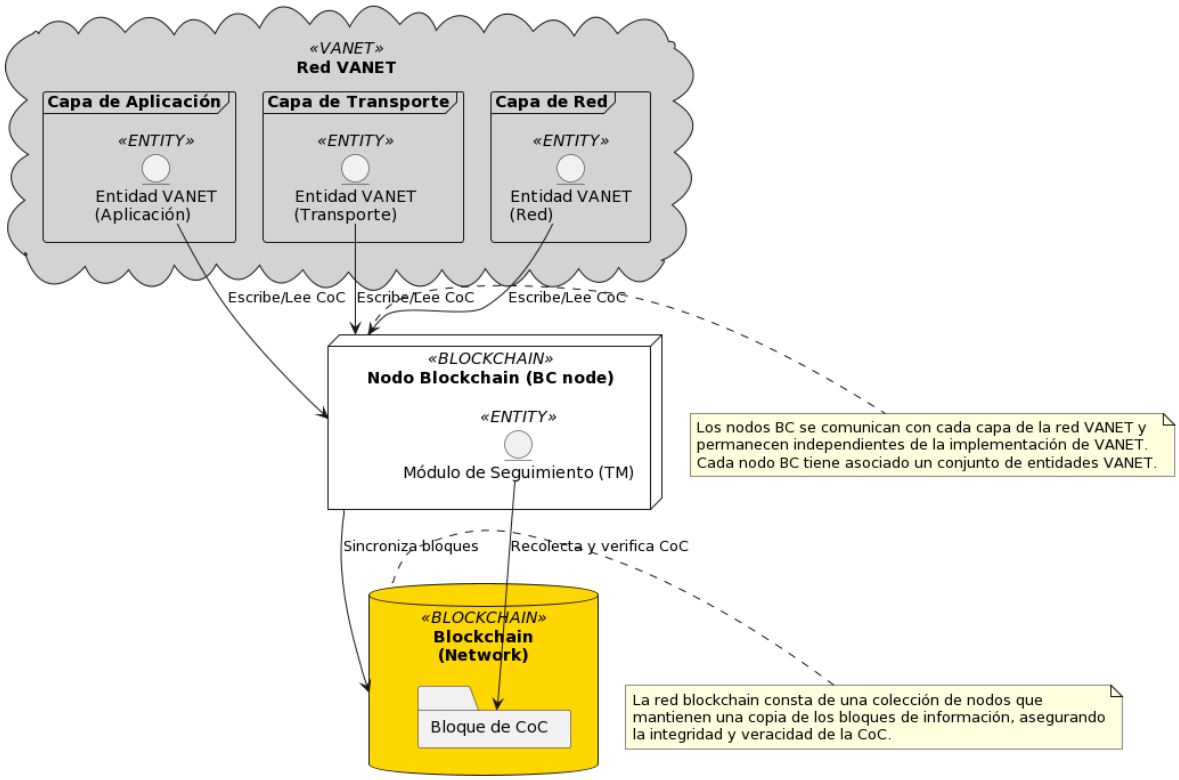

Figura 4.4: El sistema propuesto de provisión de confianza

Se observa en la Figura 4.4 que el elemento básico en el sistema es una red blockchain transversal (o vertical), que se comunica con cada capa en el sistema VANET, pero que permanece totalmente independiente de la implementación de VANET. La red blockchain propuesta está compuesta por una colección de nodos blockchain (nodo BC en la Figura 4.4), que están equipados con un módulo de seguimiento (TM) capaz de recopilar toda la información sobre la Cadena de Custodia (CoC) de los datos a partir de los bloques almacenados en la red, cuando son solicitados por entidades de VANET. Tradicionalmente, estos nodos se conectan utilizando técnicas seguras de internet como HTTPS, TCP, TLS, etc. Cada nodo BC tiene asociado un cierto conjunto de entidades VANET. Estas entidades están provistas de las credenciales que les permiten registrar y obtener información en/desde la red a través del nodo BC asociado (cada nodo puede tener diferentes credenciales, para mejorar la independencia del nodo). El uso de estas credenciales asegura que solo los componentes legítimos de VANET escriban y lean la CoC.

Las entidades VANET pueden realizar dos acciones diferentes con respecto al sistema de provisión de confianza basado en blockchain: escribir información sobre la CoC y obtener la CoC de un dato.

Las entidades VANET actualizan la Cadena de Custodia (CoC) de los datos en la blockchain mediante informes periódicos que resumen las actividades recientes. Estos informes varían en

detalle y formato según la entidad VANET responsable. Algunos contienen identificaciones únicas, como el identificador de transacción o el número de secuencia de transporte, para rastrear específicamente los datos. En contraste, otros informes pueden ser más generales, indicando acciones aplicadas a los datos en un momento dado, como la implementación del algoritmo A a todos los datos pendientes en el tiempo T.

Si se desea, ambos elementos (nivel de detalle y formato de datos) pueden ser coordinados en todas las entidades, capas, etc. o pueden ser totalmente independientes en cada componente. En algunos casos, incluso, solo algunas entidades seleccionadas (por ejemplo, las entidades fronterizas como las puertas de enlace) escriben información en la red blockchain. El único requisito que debe tenerse en cuenta es que el módulo de seguimiento (TM) debe ser capaz de entender todos los formatos de datos empleados en los bloques de datos. En la implementación propuesta (ver Sección 4.3) se emplea un formato de datos homogéneo basado en XML.

Provisión de Confianza Utilizando Tecnología Blockchain en VANETs

En la Figura 4.5, se identifican todos los elementos que participan en el proceso de evaluación de confianza. Entre paréntesis, se indican nombres genéricos como se describen en el modelo de flujo de datos XACML. Como denominación principal, se incluye la nomenclatura empleada en este trabajo.

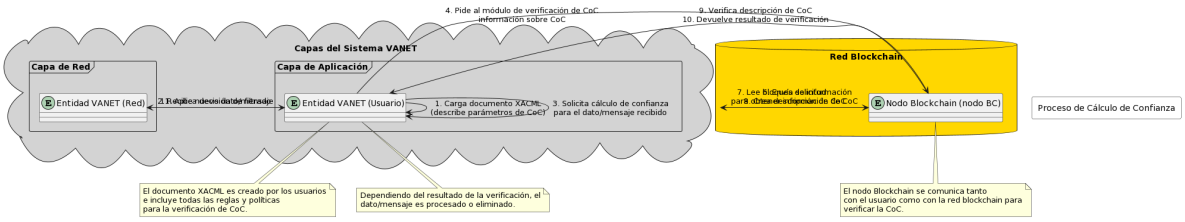

Figura 4.5: Proceso de Evaluación de Confianza en VANETs

El proceso se describe a continuación:

1. El documento XACML que describe los parámetros e información requeridos en una CoC válida es creado por los usuarios y cargado por la entidad VANET.
2. Una nueva información o mensaje es recibido por la entidad VANET. Su procesamiento se detiene en un filtro de datos hasta determinar si la información recibida es confiable.
3. El filtro de datos solicita al módulo de cálculo de confianza acerca de la confianza asociada con el dato recibido.
4. El módulo de cálculo de confianza pide al módulo de verificación de CoC la información requerida sobre la CoC para tomar una decisión sobre el nuevo mensaje.
5. El módulo de verificación de CoC envía los parámetros que deben obtenerse del sistema de provisión de confianza.
6. El módulo de cálculo de confianza envía una solicitud al nodo BC correspondiente y su módulo de seguimiento asociado.

7. La red blockchain lee los bloques de información, rastreando el origen del dato recibido y todo el proceso de transformación que ha sufrido.
8. El módulo de seguimiento crea una descripción de la CoC con la información obtenida de la red blockchain.
9. La descripción de la CoC es verificada por el módulo de verificación de CoC. Como explicaremos más adelante, se podrían realizar dos tipos básicos de verificación: una ligera y una exhaustiva. En ambos casos, las políticas y reglas a aplicar a la CoC también se describen en el documento XACML creado por los usuarios.
10. Se devuelve el resultado de la verificación.
11. Si, finalmente, el dato es confiable el procesamiento continúa, si no, se ordena al filtro de datos eliminar el mensaje.
12. Se aplica la decisión de filtrado.

Aunque este proceso parece ser muy lento, de hecho requiere muy pocos recursos. Incluso, las redes blockchain pueden operar en tiempo real, como ha demostrado su uso para soportar transacciones de BitCoin. Sin embargo, como hemos dicho, se planea un mecanismo adicional para acelerar los cálculos. La mayoría de las veces, las aplicaciones confían en los datos si su CoC puede rastrearse con el nivel de garantía requerido: los valores particulares de los parámetros no son importantes.

De hecho, si la CoC de un mensaje puede rastrearse perfectamente con la información contenida en la red blockchain, se garantiza que la información recibida no ha sufrido alteraciones, sustituciones, contaminaciones o destrucciones. En estas circunstancias, se puede emplear la verificación ligera. En este tipo de verificación, los módulos de seguimiento no envían un informe completo sobre la CoC.

Si se pueden obtener todos los parámetros requeridos, se envía un mensaje indicando un resultado positivo, pero la descripción completa de la CoC se descarta. Al final, este tipo de verificación implica que cada entidad VANET en el sistema provista con credenciales de blockchain es una fuente de datos legítima. Este enfoque reduce el tiempo de transmisión y procesamiento en la entidad VANET, lo que acelera todo el proceso (los análisis cuantitativos se realizan en las Secciones 4.3 y 4.4).

Por otro lado, si se definen reglas o políticas adicionales (por ejemplo, cualquier dato obtenido de dispositivos de hardware en una cierta área geográfica es poco confiable), se debe ejecutar la verificación exhaustiva. En este caso, la descripción completa de la CoC se evalúa en el módulo de verificación de CoC para determinar si cumple con los requisitos para considerar el mensaje confiable.

Finalmente, es importante señalar que las redes blockchain tradicionales se implementan utilizando dispositivos físicos (computadoras). Sin embargo, hoy en día, las técnicas de virtualización permiten la creación de soluciones más dinámicas y flexibles mediante la llamada Virtualización de Funciones de Red (NFV). Por lo tanto, en el sistema de provisión de confianza propuesto, se implementa una red blockchain transversal utilizando técnicas de computación en la nube y virtualización.

4.3 Validación Experimental en VANETs

Se diseñó y llevó a cabo una validación experimental con el fin de evaluar el desempeño de la solución propuesta en el contexto de las Redes Ad hoc Vehiculares (VANETs). Se desarrollaron dos experiencias distintas. En la primera parte de la validación, se midieron exhaustivamente las características y capacidades de la tecnología propuesta. Durante la segunda parte, se comparó la solución de confianza centrada en datos propuesta con las propuestas tradicionales centradas en la entidad, en un escenario de aplicación común.

Utilizando los Servicios en la Nube de la Universidad Politécnica de Madrid, se creó y desplegó una red blockchain virtual. Cada nodo estaba equipado con un módulo de seguimiento capaz de entender el lenguaje XML. Aunque la información sobre la Cadena de Custodia (CoC) puede almacenarse en formatos heterogéneos, por simplicidad (y dado que este hecho no afecta significativamente los resultados obtenidos) en este primer despliegue todas las entidades VANET están generando informes utilizando el lenguaje XML.

Se desplegaron diez nodos virtuales independientes, utilizando OpenStack como aplicación de gestión. Las credenciales de cada nodo BC consistían en un hash generado a partir de una clave privada. Las credenciales se programaron directamente en las entidades VANET, aunque en una solución de aplicación real se debería considerar una solución segura para la distribución de claves. Se empleó el algoritmo de hash SHA-256 tanto para la generación de las credenciales como para la firma de los bloques de datos. Los nodos en la red blockchain propuesta se basaron en sistemas Linux (Ubuntu) con procesadores Intel i5 y 4GB de RAM.

Por otro lado, se desplegó un sistema VANET en un laboratorio de la Universidad Politécnica de Madrid. La infraestructura desplegada consistía en un sistema autónomo para el cálculo dinámico de planes de evacuación. Se desplegaron varios nodos de sensores, conectados entre sí a través de un sistema de publicación/suscripción (P/S) y a Internet mediante una colección de concentradores. También se incluyeron pantallas LCD y actuadores sonoros.

Toda esta infraestructura física se conectó con aplicaciones de nivel superior a través de una interfaz multimodal, que incluía (entre otras tecnologías) una interfaz web y una interfaz de telemetría. También se incluyó un módulo de provisión de reglas para establecer ciertas políticas sobre los planes de evacuación. La Figura 4.6 muestra la arquitectura descrita. Una descripción detallada del comportamiento de este sistema fue reportada por Morales (2014). Como novedad, todas las entidades en el sistema se proveyeron de una nueva interfaz para comunicarse con la red blockchain. Cada sesenta (60) segundos, cada entidad generaba un informe XML describiendo la actividad del último minuto. Utilizando las credenciales proporcionadas, estos informes se registraban en el sistema de provisión de confianza. También se proporcionó un documento de descripción XACML a las aplicaciones de nivel superior. El contenido de estos documentos varió dependiendo del experimento realizado.

Durante la primera parte de la validación experimental, se realizaron cinco experimentos diferentes.

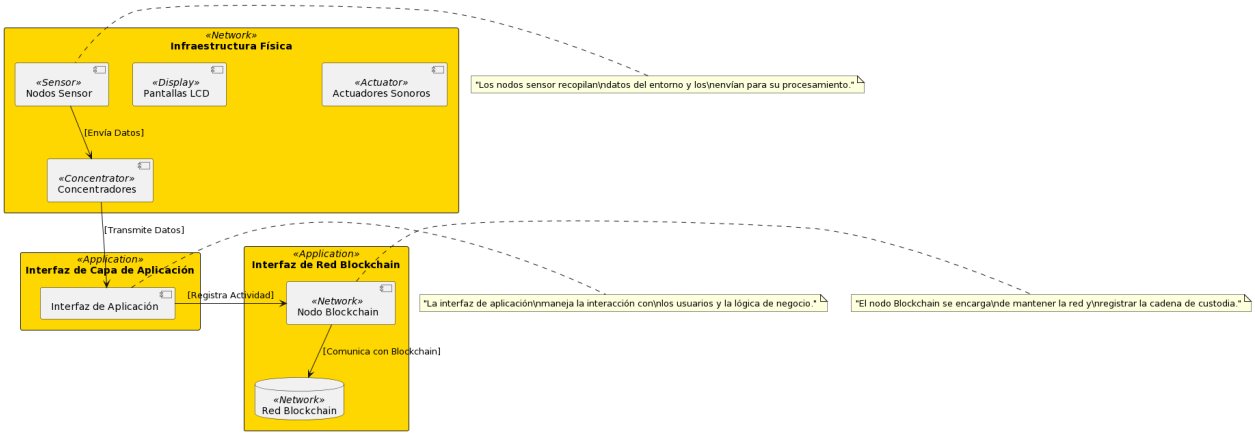

Figura 4.6: Arquitectura de la infraestructura VANET desplegada.

4.3.1 Primera Fase de Validación

En la primera parte de la validación, se examinaron las características y capacidades de la tecnología propuesta a través de varios experimentos:

- El **primer experimento** evaluó el porcentaje de mensajes maliciosos correctamente detectados en función del número de datos generados por minuto en el sistema VANET. Se activó la verificación ligera y se consideraron dos políticas diferentes sobre el registro de la Cadena de Custodia (CoC). Inicialmente, todas las entidades VANET podían registrar los informes XML generados en la red blockchain. Posteriormente, solo se permitió a los componentes fronterizos (brokers, concentradores y puertas de enlace) escribir información sobre la CoC. Se estableció que el 25 % de los mensajes generados no eran confiables.
- El **segundo experimento** evaluó el porcentaje de detección de mensajes maliciosos dependiendo del porcentaje de mensajes no confiables generados, manteniendo una tasa de generación de datos de 50 por minuto.
- En el **tercer experimento**, se centró en determinar la influencia del documento de descripción XACML en el rendimiento del sistema de provisión de confianza. En las mismas condiciones que el primero, considerando que todas las entidades en el sistema VANET podían añadir información a la red blockchain, se crearon dos diferentes XACML. El primero solo requería que la información sobre la CoC fuera encontrada (es decir, se activó la verificación ligera). El segundo fue diseñado para admitir como fiables únicamente los datos generados a partir de mensajes creados por ciertos nodos sensores (es decir, se tuvo que realizar una verificación exhaustiva). Se adquirió información sobre el porcentaje de mensajes maliciosos detectados correctamente.
- El **cuarto experimento** extendió el tercero evaluando la reducción en el tiempo de cálculo de la confianza cuando se activaba la verificación ligera.
- El **quinto experimento** examinó el porcentaje de mensajes maliciosos correctamente detectados en función del nivel de garantía requerido por las aplicaciones de nivel superior.

Cada vez que el nivel de garantía aumentaba, se incluían diez nuevos parámetros como información obligatoria en el documento XACML.

4.3.2 Segunda Fase de Validación

Durante la segunda parte de la validación experimental, se realizó un único experimento comparando una conocida propuesta centrada en la entidad con la solución basada en blockchain en varias situaciones, como cuando un componente fijo presenta un componente malicioso, un componente conectado ad hoc es malicioso o se incluyen nuevos componentes sin soporte para la evaluación de la confianza en el sistema VANET.

4.4 Resultados

Los resultados de la validación experimental se muestran en las Figuras 4.7 a 4.12. Las Figuras 4.7 a 4.11 presentan los resultados de la primera parte de la validación experimental, mientras que la Figura 4.12 describe los resultados de la segunda parte.

4.4.1 Primera Parte de la Validación Experimental

La evolución del porcentaje de mensajes maliciosos detectados correctamente, en función del número de datos generados por minuto, se puede observar en la Figura 4.7. Se dibujan cuatro curvas diferentes. Las curvas de "Falsos confiablesrepresentan los mensajes etiquetados como confiables, que, de hecho, no lo son. Las curvas de "Falsos no confiablesrepresentan lo opuesto, mensajes no confiables considerados como confiables. Como se puede ver, todas las curvas tienen una evolución similar a la exponencial. En tres situaciones, la solución propuesta se comporta de manera muy similar. A medida que el número de datos generados por minuto aumenta, más información (CoC) se almacena en la red blockchain, y los algoritmos de seguimiento y verificación tienen más problemas para calcular la CoC. Sin embargo, cuando todas las entidades pueden incorporar información al sistema de provisión de confianza, el valor asintótico para la probabilidad de error es, como máximo, $p \approx 10\,\%$.

Un comportamiento similar ocurre en el segundo experimento (ver Figura 4.8). En general, como el número de mensajes generados por minutos era relativamente bajo (50 datos por minuto), las probabilidades de error (calculadas siguiendo la definición de Laplace) también son bajas (todas por debajo del 2 %).

El tercer experimento muestra resultados muy similares a los del primer experimento (ver Figura 4.9). La curva de "Falsos confiables"para la verificación ligera permanece por debajo del valor de $p \approx 10\,\%$. Por otro lado, las otras tres curvas presentan una ligera modificación, especialmente significativa cuando se considera la verificación intensiva.

Las discusiones previas cobran una relevancia particular considerando los resultados del cuarto experimento (ver Figura 4.10). Se observa que, a medida que se generan más datos por minuto, se requiere más tiempo para evaluar la confianza. No obstante, se pudo observar una reducción máxima del 40 % en el tiempo de cálculo. Es importante destacar que, durante

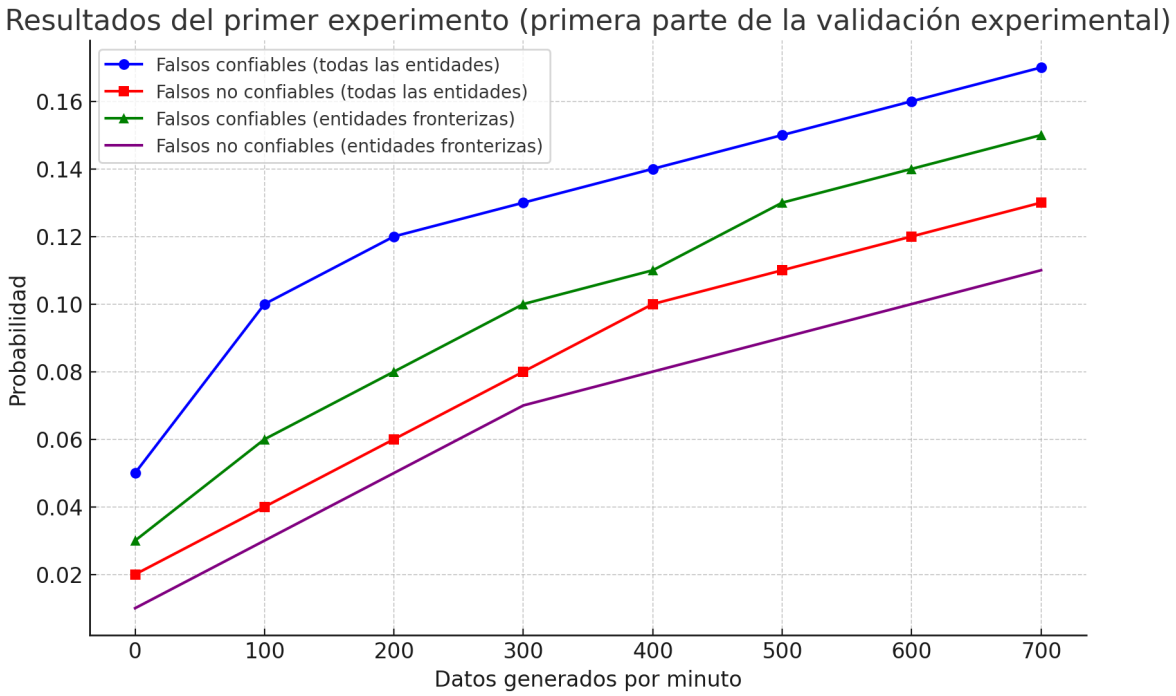

Figura 4.7: Resultados del primer experimento (primera parte de la validación experimental).

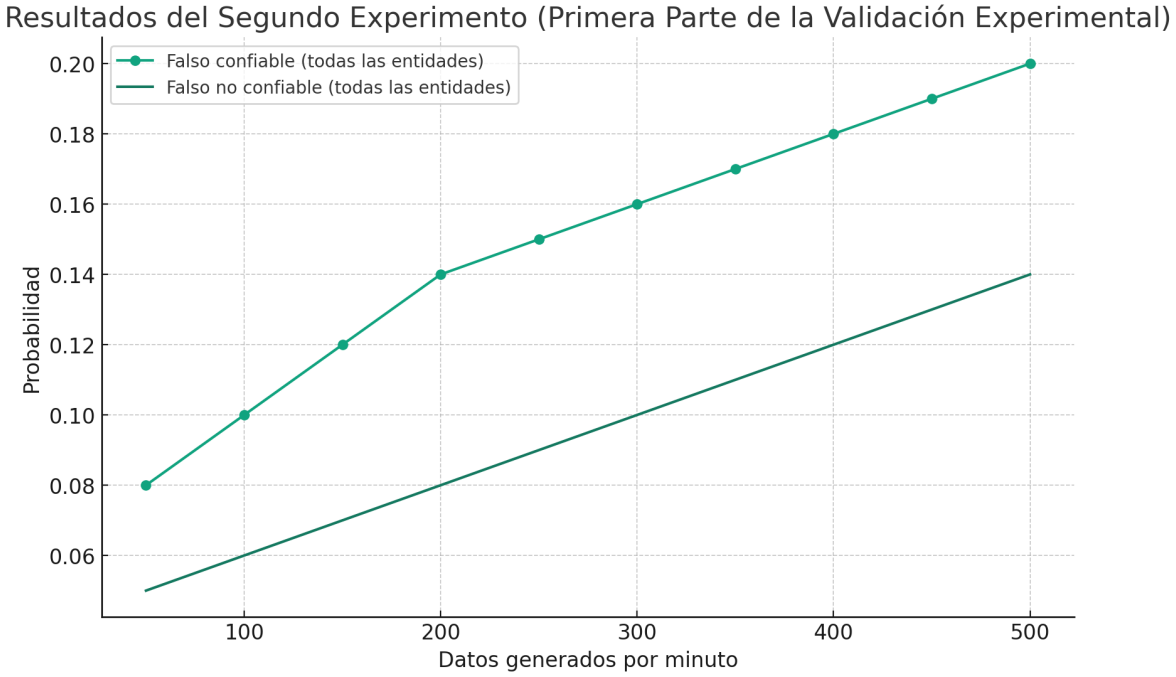

Figura 4.8: Resultados del primer experimento (primera parte de la validación experimental).

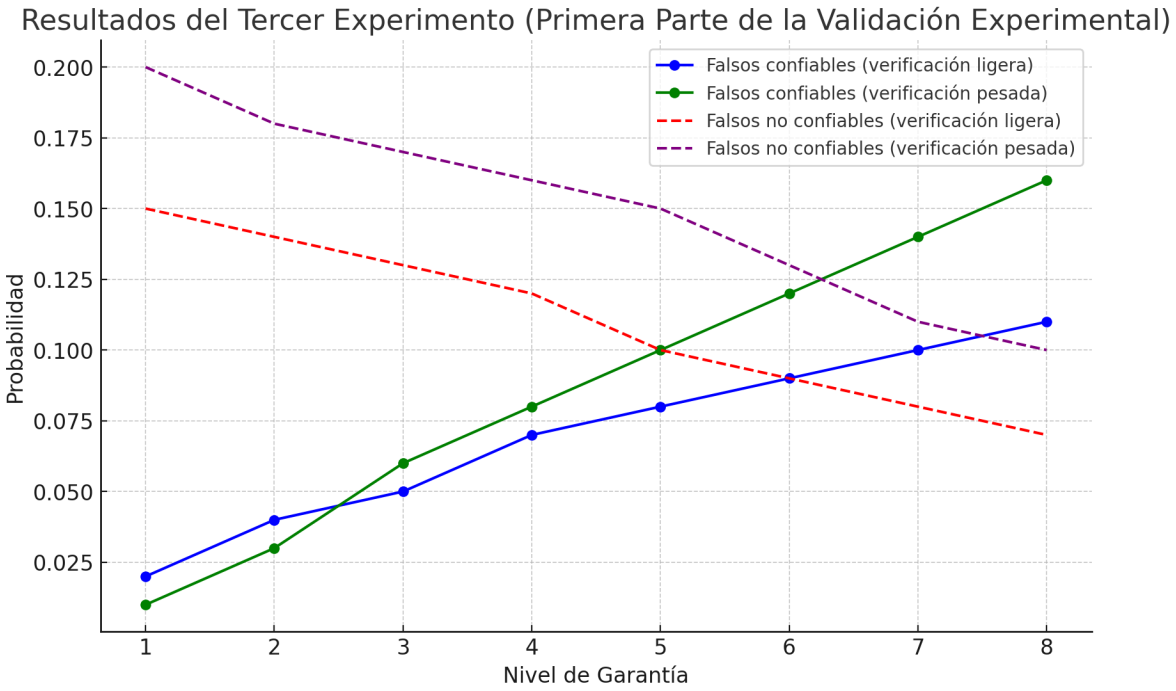

Figura 4.9: Probabilidades de "falsos confiablesz "falsos no confiables"tanto para la verificación ligera como la pesada

estos experimentos, se obtuvo un "tiempo normalizado"dividiendo cada valor por el valor máximo obtenido durante la validación experimental.

La evolución del proceso de verificación depende significativamente de si se considera una verificación ligera o rigurosa. En el caso de la verificación ligera, se observa una evolución lineal. Dado que las descripciones de la Cadena de Custodia (CoC) no se transmiten al módulo de verificación de la CoC, no se alcanza un estado de saturación y la evolución es lineal. Por otro lado, la verificación rigurosa requiere un proceso de cálculo complejo; así, a medida que crece el número de datos a procesar, algunas estimaciones de confianza no podrían realizarse, especialmente si las colas en las entidades de VANET están saturadas, pero el tiempo permanece constante. Como conclusión, la verificación rigurosa solo debería emplearse en circunstancias en las que el nivel de protección requerido justifique estos peores parámetros de Calidad de Servicio (QoS).

El quinto experimento mostró que existe un nivel óptimo de garantía (ver Figura 4.11). Se observa que para valores bajos del nivel de garantía, la CoC contiene poca información y la probabilidad de etiquetar un mensaje no confiable como confiable es muy alta. Sin embargo, para valores altos del nivel de garantía, la probabilidad de un "falso no confiableçrece. Como resultado, existe un nivel óptimo de garantía, localizado en el punto donde ambas curvas se cruzan. Dependiendo de las características de los sistemas VANET y de provisión de confianza, este valor puede cambiar, pero en el caso de la validación propuesta es $w = 8$ (el nivel de garantía siempre debe ser un número entero).

Los resultados de estos experimentos proporcionan una perspectiva valiosa sobre la eficacia

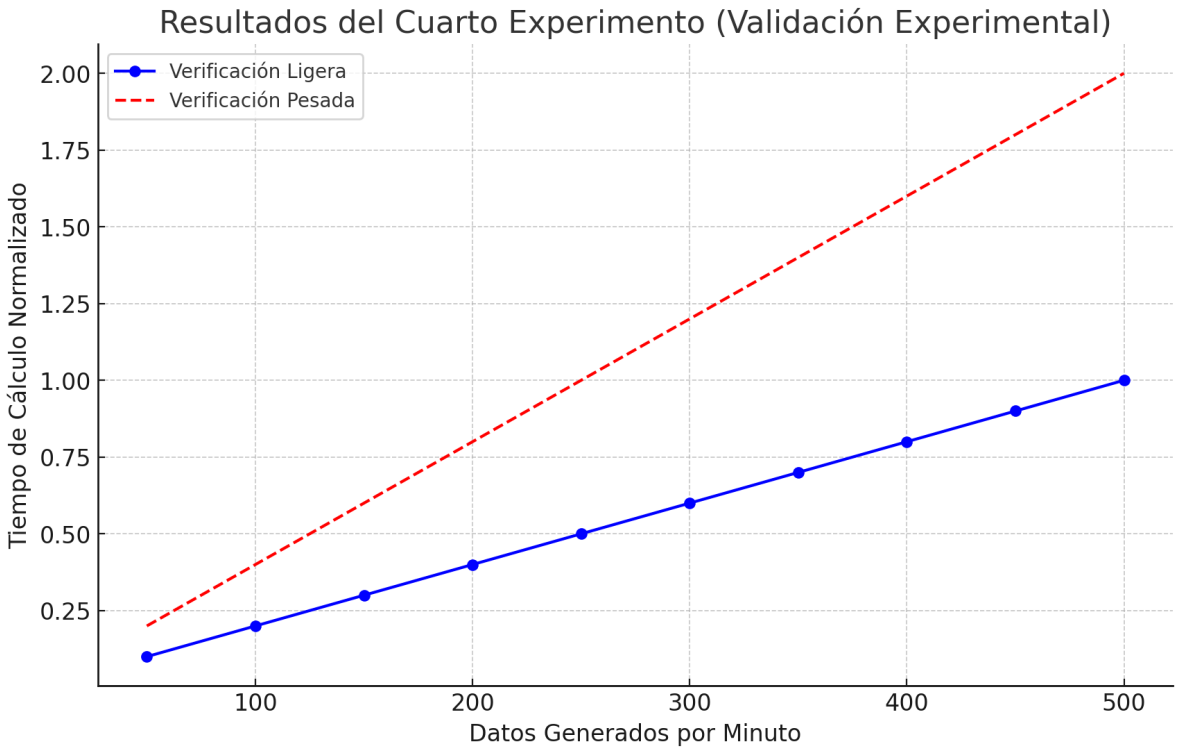

Figura 4.10: Tiempo de cálculo de confianza

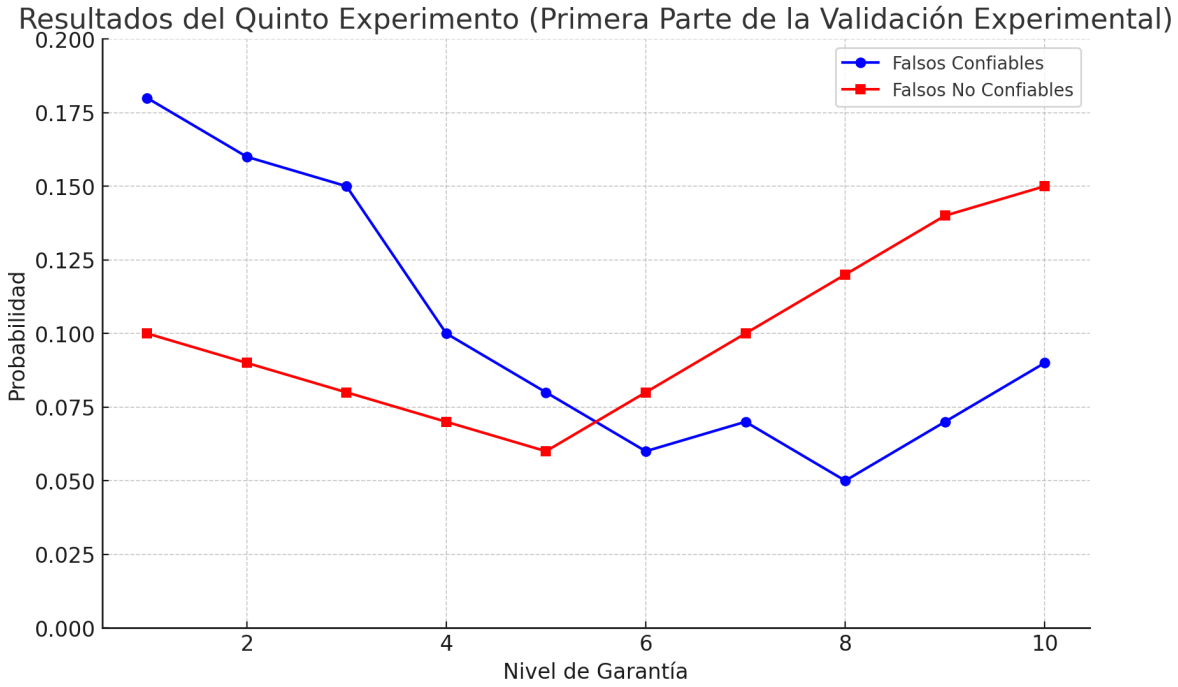

Figura 4.11: Nivel óptimo de garantía

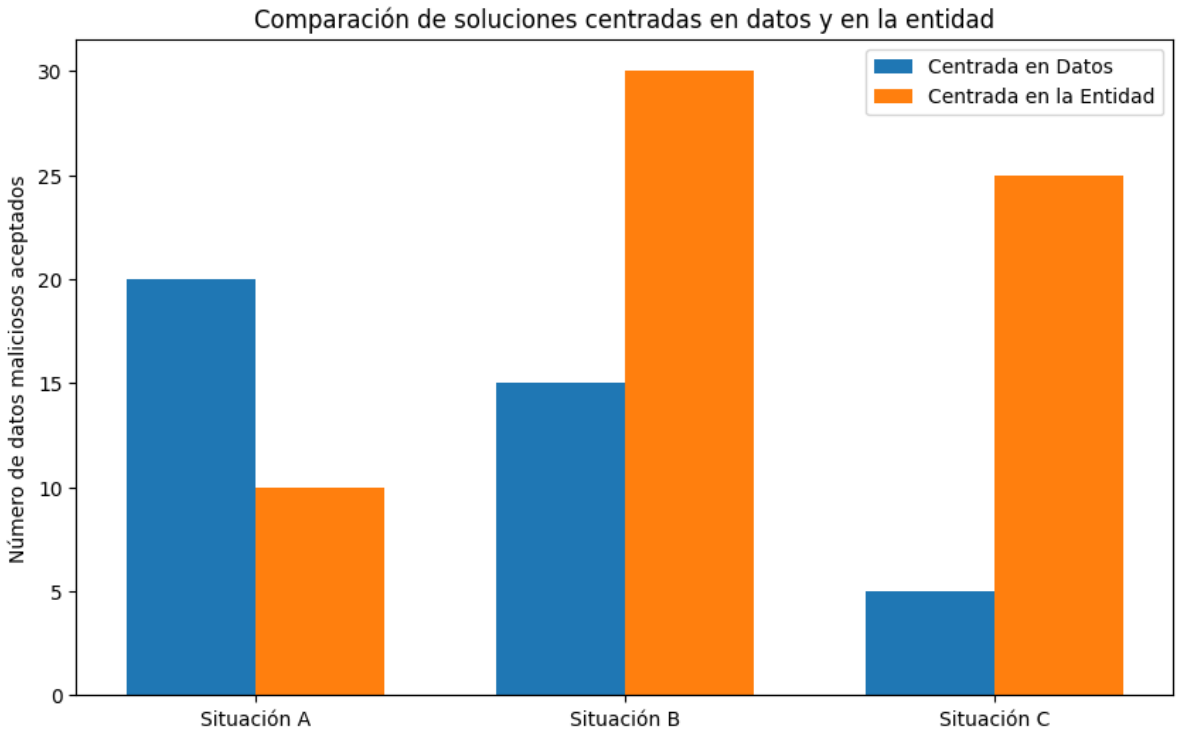

Figura 4.12: Comparación de soluciones

de las soluciones basadas en blockchain para la gestión de la confianza en entornos VANETs, destacando la importancia de considerar el nivel de verificación y la integridad de la información en la Cadena de Custodia.

4.4.2 Segunda Parte de la Validación Experimental

Finalmente, revisamos los resultados de la segunda parte de la validación experimental, donde la solución propuesta se compara con propuestas previas centradas en la entidad. Como se puede ver en la Figura 4.12, es difícil comparar propuestas centradas en los datos con propuestas centradas en la entidad, ya que distintos parámetros y diagramas de flujo describen su comportamiento.

Así, el número de datos maliciosos finalmente aceptados en tres situaciones notables diferentes es la mejor manera de comparar (aunque de manera parcial y limitada) ambos tipos de soluciones. Los sistemas de provisión de confianza centrados en la entidad tradicionalmente son más efectivos que la tecnología centrada en los datos propuesta si los componentes maliciosos mantienen una posición fija. De hecho, en estas circunstancias, una vez que ha transcurrido el tiempo de convergencia y el componente malicioso ha sido aislado, no se admiten más mensajes, por lo que a largo plazo se procesan menos mensajes maliciosos. Sin embargo, en las otras dos situaciones, donde los componentes no mantienen una situación o identidad constante, dado que las soluciones centradas en la entidad requieren cierto tiempo de convergencia antes de detectar cualquier conducta maliciosa, existe el riesgo de nunca alcanzar un valor estable (y, entonces, todos los mensajes, sean confiables o no, son admitidos). Por lo

tanto, las soluciones centradas en los datos se comportan mejor en escenarios dinámicos.

Esto subraya la importancia de adaptar la solución de confianza al entorno operativo específico y las necesidades de seguridad. En escenarios donde la estabilidad y la previsibilidad de los componentes son altas, las soluciones centradas en la entidad pueden ofrecer una seguridad robusta y eficaz. Sin embargo, en entornos de VANET donde la dinámica y la movilidad son inherentes, un enfoque centrado en los datos, con su capacidad para adaptarse rápidamente a los cambios y evaluar la confianza sin depender de un historial de interacciones, puede proporcionar una respuesta de seguridad más adecuada y oportuna.

4.5 Conclusiones

En este capítulo se describe una solución para la evaluación de confianza en escenarios VANETs. La solución propuesta, centrada en los datos, se basa en una formalización matemática y en los conceptos de Cadena de Custodia y Nivel de Garantía. Además, se centra en escenarios dinámicos donde las entidades VANETs establecen conexiones ad hoc y/o las identidades no son permanentes (es decir, configuraciones efímeras).

La implementación práctica de la solución propuesta se basa en la tecnología blockchain, ya que cumple tanto con la formalización descrita como con los requisitos habituales para los sistemas de provisión de confianza.

Básicamente, nuestra propuesta consiste en una red blockchain, donde se almacena metainformación sobre los datos recibidos. Esta información está protegida por funciones hash y dividida en bloques de datos encadenados que se mantienen en varios nodos independientes para proteger el sistema contra ciberataques. Esta información se utiliza para crear descripciones de CoC que se usan para determinar la fiabilidad de los datos recibidos.

La validación experimental mostró que el esquema propuesto es una solución útil, con una probabilidad máxima de error (en un escenario regular) de p 10 %.

También se proporciona un algoritmo de verificación pesada, válido para infraestructuras altamente protegidas, pero cuyas características no aconsejan emplearlo extensivamente. También se evalúa el concepto de nivel de garantía, estableciendo que existe un valor óptimo para este parámetro. Además, una comparación entre la solución centrada en los datos propuesta y las propuestas tradicionales centradas en la entidad determina que el uso principal de la tecnología propuesta está asociado a escenarios efímeros, ya que las soluciones centradas en la entidad presentan un mejor comportamiento en infraestructura fija. Por lo tanto, como conclusión, ambas propuestas no son contradictorias sino complementarias.

En cualquier caso, la tecnología propuesta permite el cálculo de la confianza sin necesidad de monitorear los enlaces de comunicación o las entidades VANETs durante largos períodos de tiempo, como en propuestas centradas en la entidad anteriores. De esta manera, los sistemas VANETs más nuevos y recientes basados en tecnologías ad hoc y conexiones efímeras podrían contar con soluciones de gestión de confianza.

Capítulo 5

Provisión de servicios de confianza y reputación en VANET

En este Capítulo se desarrolla un algoritmo de cálculo de confianza y reputación basado en servicios, que integra múltiples enfoques de la confianza (cognitivo, computacional, neurológico y teórico de juegos) para proporcionar una evaluación dinámica y precisa de la reputación de los nodos en las VANETs. Con esta contribución alcanzamos el **Objetivo#2**.

Además, se implementa un sistema distribuido basado en blockchain para el cálculo y gestión de la confianza y reputación en VANETs, que permite la integración de los cálculos locales de confianza en un valor de confianza global actualizado. Con lo que se cumple el **Objetivo#3** de este proyecto de Tesis.

Finalmente, el capítulo incuye una validación experimental de las contribuciones realizadas, con lo que alcanza también el **Objetivo#8**.

5.1 Introducción

Las Redes de Vehículos Ad hoc (VANETs) se posicionan como una de las tecnologías habilitadoras más potentes de nuevos paradigmas como las VANET, Sistemas Ciberfísicos o Entornos Inteligentes. En todas estas soluciones innovadoras, los componentes de software y hardware gestionan grandes cantidades de datos que, en varios casos, pueden ser personales y, por lo tanto, estar protegidos por regulaciones internacionales como el Reglamento General de Protección de Datos (GDPR) europeo. Además, se prevé que la mayoría de estos nuevos paradigmas técnicos se implementen en infraestructuras críticas o aplicaciones, lo que los convierte en un foco potencial para diversos ataques: desde el ciberdelito tradicional hasta los nuevos riesgos ciberfísicos y el ciberterrorismo Q. Feng et al., 2019.

En este contexto, es esencial proteger las implementaciones de VANETs mediante políticas y mecanismos robustos. Tradicionalmente, una implementación protegida de VANETs necesita implementar tecnologías en tres áreas diferentes: seguridad, confianza y privacidad.Raya y Hubaux, 2007 Los mecanismos de seguridad incluyen soluciones de autenticación e integridad,

que ya son ampliamente adoptadas por las tecnologías actuales de VANETs (principalmente heredadas de tecnologías y protocolos de red como Bluetooth o ZigBee) Lu et al., 2018.

Por otro lado, aunque los mecanismos de privacidad, incluida la criptografía y las políticas de anonimización, no están completamente adaptados a los despliegues y requisitos de las VANETs, también se implementan comúnmente en muchas aplicaciones no comerciales de VANETs, especialmente versiones livianas de algoritmos bien conocidos como The Onion Router (TOR) Ali et al., 2019.

Por el contrario, las soluciones de confianza enfrentan una situación totalmente diferente. Los mecanismos de confianza más comunes actualmente se basan en un esquema administrativo, o en una comprensión social de este concepto; lo que hace muy difícil integrar estas tecnologías sin desplegar una gran infraestructura o considerar una intervención humana relevante y constante H. Zhou et al., 2018.

Los mecanismos de confianza típicamente incluyen dos aspectos diferentes: detección de intrusiones y reputación. Mientras que la detección de intrusiones requiere, actualmente, grandes infraestructuras y un gran poder computacional (las soluciones más recientes y exitosas se basan en algoritmos matemáticamente complejos como la inteligencia artificial y grandes repositorios de datos); los mecanismos de reputación generalmente se sustentan a través de una intervención humana directa Liang et al., 2015.

En este sentido, ambas áreas claramente enfrentan desafíos abiertos, lo que impide su uso masivo en los próximos despliegues de VANETs. Como una solución posible, se proponen nuevos marcos y mecanismos de cálculo de confianza y reputación. Sin embargo, estas propuestas tienden a ser subjetivas y altamente distribuidas, por lo que los algoritmos innovadores que garantizan una gestión dinámica y eficiente de la confianza y/o reputación son típicamente computacionalmente intensivos y complejos Linke et al., 2010.

No obstante, el creciente poder computacional de los nodos de VANETs, junto con el acceso universal a Internet global garantizado por las futuras redes 5G, están introduciendo un escenario mucho más favorable para esas nuevas propuestas Raya y Hubaux, 2007.

Por lo tanto, en este capítulo proponemos una solución de cálculo de confianza y reputación basada en servicios. El algoritmo de cálculo propuesto considera cuatro enfoques o entendimientos diferentes de la confianza: cognitivo, computacional, neurológico y teórico de juegos. La confianza, en nuestra propuesta, no es un valor fijo sino una distribución de probabilidad, lo que representa de mejor manera la incertidumbre intrínseca de las observaciones. Los cálculos locales se integran entonces en un valor de confianza global, que se obtiene y actualiza utilizando una red distribuida de Blockchain A. S. Khan et al., 2019.

Desde una perspectiva de mercado, la solución propuesta muestra una alta aplicabilidad ya que puede implementarse en todo tipo de dispositivos y nodos de VANETs (solo se emplean operaciones matemáticas comunes). Por otro lado, se pueden encontrar varias implementaciones ligeras de intermediarios y redes Blockchain, lo que también facilita la aplicabilidad de la arquitectura propuesta en todo tipo de escenarios comerciales H. Li y Han, 2023.

5.2 Propuesta de arquitectura y servicio para el cálculo de confianza en VANET

En esta sección, proponemos una arquitectura novedosa para el cálculo de confianza en despliegues de Redes de Vehículos Ad hoc (VANETs). Esta innovadora propuesta se centra en abordar los desafíos específicos de las VANETs, donde la confiabilidad y la rapidez en la toma de decisiones son cruciales para la seguridad y eficiencia en el tráfico vehicular. La inclusión de una red Blockchain proporciona una solución descentralizada y segura para la gestión de la confianza, permitiendo una verificación transparente y a prueba de manipulaciones de las transacciones entre vehículos. Los Contratos Inteligentes automatizan el proceso de cálculo y actualización de la confianza, basándose en criterios predefinidos y en el comportamiento observado de los nodos dentro de la red.

A nivel local, la diversidad en los métodos de cálculo de confianza permite una evaluación exhaustiva y multifacética de las entidades. El enfoque cognitivo considera la percepción y las experiencias previas de los nodos; el computacional, la capacidad y recursos disponibles; el neurológico, los patrones de comportamiento y la adaptabilidad; y el teórico de juegos, las estrategias y la cooperación entre vehículos. Esta combinación de enfoques garantiza un sistema de confianza robusto y adaptable que puede responder efectivamente a las dinámicas cambiantes y a las exigencias de seguridad en las VANETs.

La propuesta busca, por tanto, establecer un marco de trabajo integral que no solo mejore la seguridad y la fiabilidad en las comunicaciones vehiculares, sino que también promueva un ambiente colaborativo y eficiente entre los participantes de la red. Esta arquitectura representa un paso significativo hacia la realización de sistemas de transporte inteligentes y seguros, donde la confianza y la cooperación mutua son la piedra angular para el avance y la innovación en el ámbito de las VANETs.

5.2.1 Arquitectura propuesta

La Figura 5.1 muestra la arquitectura propuesta para el cálculo de confianza.

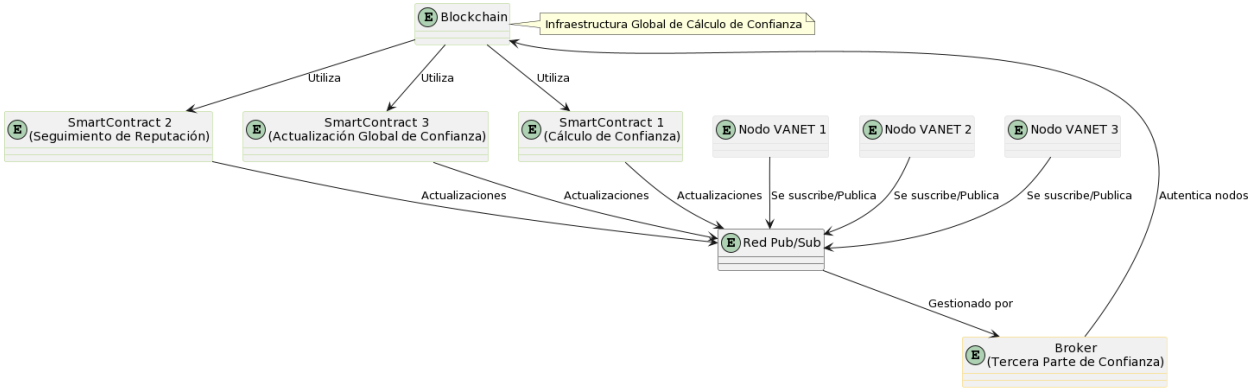

Figura 5.1: Arquitectura propuesta para el cálculo de confianza y reputación.

En la solución propuesta, cada nodo de VANET puede ejecutar localmente uno de los cuatro

algoritmos de cálculo de confianza existentes: cognitivo, computacional, neurológico y teórico de juegos. En general, y dependiendo de la configuración del sistema, los nodos pueden seleccionar el algoritmo de cálculo de confianza de manera autónoma (según sus capacidades, conocimientos, etc.) o el administrador del sistema puede hacerlo. En cualquier caso, es importante garantizar que los cuatro algoritmos de cálculo tengan una presencia homogénea en el despliegue de VANETs (para evitar sesgos en la función de cálculo de confianza global).

Los nodos en el despliegue de VANETs, por otro lado, están conectados a la infraestructura de cálculo de confianza global a través de una red de publicación/suscripción. Esta red ofrece una API (interfaz de programación de aplicaciones) y servicio REST (transferencia de estado representacional), por lo que los nodos pueden relacionarse con la infraestructura usando mensajes HTTP. Los mensajes HTTP son más fáciles de analizar, enviar, recibir y procesar que los protocolos orientados a bits, aunque muestran mayores latencias. Además, los mensajes HTTP son hoy en día el medio de comunicación estándar para nodos y despliegues de VANETs.

Usando estos mensajes, los nodos de VANETs pueden suscribirse a diferentes servicios de confianza y a las actualizaciones sobre los valores de confianza de otros nodos, otros algoritmos de cálculo de confianza y/o la infraestructura de cálculo de confianza global. Al mismo tiempo, la infraestructura de cálculo de confianza global (es decir, la red Blockchain) está suscrita a todas las actualizaciones de los nodos de VANETs. Por otro lado, cuando un cambio relevante en los valores de confianza calculados localmente es detectado por un nodo de VANET, puede publicar los nuevos resultados. Todos estos intercambios de mensajes y la gestión de pub/sub están controlados por un broker confiable que actúa como TTP. De hecho, este broker requiere que los nodos de VANETs y la red Blockchain se autentiquen y empleen mecanismos criptográficos para preservar la privacidad y seguridad de las comunicaciones. Todos los nodos que no pueden ser autenticados por el TTP son automáticamente rechazados.

Además, a través de un SmartContract actuando como oráculo, la red Blockchain monitorea y almacena todas las actualizaciones sobre cálculos de confianza realizados por nodos de VANETs en el despliegue. De esa manera, en la red Blockchain (usando un segundo SmartContract) hay un seguimiento responsable de la reputación y fiabilidad de todos los nodos de VANETs, desde diferentes perspectivas (cognitiva, computacional, neurológica y teórico de juegos) y desde diferentes análisis locales (tantos como nodos de VANETs estén observando y analizando el comportamiento del nodo dado). Cada vez que este registro transparente e irrefutable se actualiza, un tercer SmartContract actualiza el cálculo de confianza global (usando funciones estocásticas). Cada vez que los valores de confianza global se actualizan, la red Blockchain genera un evento, que se publica a través de la red pub/sub. Entonces, todos los nodos son informados sobre la fiabilidad global de todos los nodos en el despliegue de VANETs.

Con toda esta información (confianza global y rechazos causados por el TTP), los nodos de VANETs pueden definir su propio "dominio de confianza", seleccionando con qué nodos quieren establecer una conexión (ver 5.2.5). De ahora en adelante asumimos que los nodos rechazados no están conectados con ningún otro nodo, y nos centramos en el cálculo de confianza (tanto a nivel local como global).

5.2.2 Cálculo de confianza cognitiva

En las Redes Ad Hoc Vehiculares (VANETs), es fundamental establecer la confianza entre los nodos para garantizar la seguridad y la fiabilidad de las comunicaciones. La confianza cognitiva es un enfoque que integra las creencias previas en el cálculo de la confianza, brindando una perspectiva más robusta que las técnicas basadas únicamente en la observación directa.

La confianza cognitiva se refiere a la reputación y la confianza respaldadas por creencias previas sobre las entidades involucradas. En un contexto tecnológico, estas creencias se refieren a la expectativa de que un nodo tenga la competencia, benevolencia e integridad necesarias para ser confiable Asemi et al., 2023.

Estas cualidades no son técnicas, sino sociales, y se heredan del propietario del nodo, su ubicación y otros metadatos asociados. Dada una red VANET con un nodo objetivo n_i y un conjunto asociado de metadatos $MD(n_i)$,

$$MD(n_i) = \{md_k(n_i) \mid k = 1, \ldots, K_T\} \tag{5.1}$$

donde:

- $MD(n_i)$ representa el conjunto de metadatos asociados al nodo objetivo n_i.
- $md_k(n_i)$ representa el valor del metadato de tipo k asociado al nodo objetivo n_i.
- K_T es el número total de tipos de metadatos considerados.
- y un nodo observador n_j con un conjunto de metadatos *a priori* confiables $MD^+(n_j)$.

En la siguiente ecuación se detalla la estructura de los metadatos *a priori* confiables asociados al nodo observador n_j:

$$MD^+(n_j) = \left\{md_k^+(n_j) \mid k = 1, \ldots, K_T\right\} \tag{5.2}$$

donde cada $md_k^+(n_j)$ se define como:

$$md_k^+(n_j) = \left\{md_{k,r}^+(n_j) \mid r = 1, \ldots, R_{k,j}\right\} \tag{5.3}$$

y se tiene que:

- $MD^+(n_j)$ representa el conjunto de metadatos *a priori* confiables asociados al nodo observador n_j.
- $md_k^+(n_j)$ representa el valor *a priori* confiable del metadato de tipo k para el nodo observador n_j.
- K_T es el número total de tipos de metadatos considerados.
- $R_{k,j}$ es el número de valores posibles para el metadato de tipo k y el nodo observador n_j.

- $md^{+}_{k,r}(n_j)$ representa el valor *a priori* confiable del metadato de tipo k y valor r para el nodo observador n_j.

Se puede calcular la confianza cognitiva $T_{cog}(n_i; n_j)$ utilizando la siguiente expresión:

$$T_{cog}(n_i; n_j) = P_{trust}(n_i; n_j) = \sum_{k=1}^{K_T} \sum_{r=1}^{R_k} \Big(\alpha_{k,r} \delta[md_k(n_i) = md^{+}_{k}(n_j)] + \beta_{k,r} \delta[md_k(n_i) \neq md^{+}_{k}(n_j)] \Big) \tag{5.4}$$

donde:

- $T_{cog}(n_i; n_j)$ representa la probabilidad de que el nodo objetivo n_i sea confiable, según las observaciones locales del nodo observador n_j.
- $P_{trust}(n_i; n_j)$ denota la probabilidad de confianza.
- K_T es el número total de tipos de metadatos considerados.
- R_k es el número de valores posibles para el metadato de tipo k.
- $md_k(n_i)$ representa el valor del metadato de tipo k asociado al nodo objetivo n_i.
- $md^{+}_{k}(n_j)$ representa el valor *a priori* confiable del metadato de tipo k para el nodo observador n_j.
- $\alpha_{k,r}$ y $\beta_{k,r}$ son parámetros reales que representan el grado o peso de las creencias del nodo.
- $\delta[\cdot]$ es la delta de Kronecker, que es igual a 1 si el argumento es verdadero y 0 en caso contrario.

La confianza cognitiva se puede calcular antes de que el sistema comience a operar, pero requiere la definición de un protocolo para compartir los metadatos de los nodos con todo el sistema. Este proceso es crucial para construir las creencias previas necesarias para el cálculo de la confianza cognitiva.

El cálculo de la confianza cognitiva permite incorporar las creencias previas en la evaluación de la confianza entre nodos en VANETs, ofreciendo una base más sólida para la toma de decisiones y la gestión de las comunicaciones en redes de vehículos inteligentes.

5.2.3 Cálculo de confianza computacional

En las Redes Ad Hoc Vehiculares (VANETs), la confianza computacional es fundamental para garantizar la seguridad y la fiabilidad de las comunicaciones. La confianza computacional se refiere al comportamiento que sigue las reglas y requisitos de las autoridades en el despliegue de las VANETs, típicamente relacionado con la ciberprotección mediante técnicas como la criptografía.

Si bien la confianza computacional tradicionalmente se ha utilizado para habilitar o deshabilitar la colaboración espontánea entre nodos, es posible definir una métrica más elaborada. Dada

una VANET con un nodo objetivo n_i y un nodo observador n_j, se puede calcular la confianza computacional $T_{comp}(n_i; n_j)$ para este par de nodos utilizando la siguiente expresión:

$$T_{comp}(n_i; n_j) = P_{trust}(n_i; n_j) = \begin{cases} \sqrt{\frac{1}{K_{th}}} & \text{si } k < K_{th} \\ \frac{\sqrt{h_{i,j}}}{1+h_{i,j}} & \text{si } k \geq K_{th} \end{cases} \tag{5.5}$$

donde:

- $T_{comp}(n_i; n_j)$ representa la probabilidad de que el nodo objetivo n_i sea computacionalmente confiable, según las observaciones locales del nodo observador n_j.
- $P_{trust}(n_i; n_j)$ denota la probabilidad de confianza.
- K_{th} representa el número de intervalos de tiempo transcurridos desde el inicio del despliegue de la VANET.
- $h_{i,j}$ representa el porcentaje de veces que el nodo n_i ha utilizado la configuración criptográfica correcta (indicada por la Autoridad de Confianza [TTP]) al comunicarse con el nodo n_j.

La función propuesta para la confianza computacional es una sigmoide, lo que implica que varía en el intervalo $[0, 1]$, de manera similar a las probabilidades. Este enfoque permite interpretar el resultado como la probabilidad de que el nodo n_i sea computacionalmente confiable según el cálculo local realizado por el nodo n_j.

- k: Representa el número de intervalos de tiempo transcurridos desde el inicio del funcionamiento del despliegue de la VANET.
- $h_{i,j}$: Se calcula mediante una suma geométrica con una tasa de decaimiento $r_{i,j}$ para introducir un efecto de decrecimiento temporal, otorgando menos relevancia a eventos pasados en comparación con los más recientes. Esto pondera la antigüedad de las transacciones evaluando la relación entre las transacciones con la configuración correcta $c_{i,j}[m]$ y el número total de transacciones $t_{i,j}[m]$ en el intervalo de tiempo m, de la siguiente manera:

$$h_{i,j} = \sum_{m=0}^{k} r_{i,j}^{m+1} \cdot u_{i,j}[-m] \quad u_{i,j}[m] = \frac{c_{i,j}[m]}{t_{i,j}[m]} \tag{5.6}$$

donde $u_{i,j}[m]$ representa la relación entre las transacciones con la configuración correcta $c_{i,j}[m]$ y el número total de transacciones $t_{i,j}[m]$ en el intervalo de tiempo m.

Este enfoque de confianza computacional basado en el comportamiento permite evaluar la fiabilidad de los nodos en VANETs a lo largo del tiempo, considerando tanto la corrección de la configuración criptográfica como el factor temporal. Esto contribuye a mejorar la seguridad y la fiabilidad de las comunicaciones en redes de vehículos inteligentes.

5.2.4 Cálculo de confianza neurológica

La confianza neurológica (T_{neu}) representa un enfoque basado en el comportamiento, siendo uno de los métodos más tradicionales para evaluar la confianza en redes. Este enfoque implica que, en general, los nodos analizan la honestidad de otros nodos dentro del despliegue de la red y obtienen un valor de confianza basado en las experiencias observadas y pasadas.

En el marco de la confianza neurológica, el nodo observador n_j monitorea el número de transacciones exitosas $s_{i,j}[m]$ con el nodo objetivo n_i en cada intervalo de tiempo m. Esta cantidad se emplea para generar un coeficiente $w_{i,j}[m]$, considerando el número total de transacciones $t_{i,j}[m]$ entre ambos nodos:

$$w_{i,j}[m] = \frac{s_{i,j}[m]}{t_{i,j}[m]} \tag{5.7}$$

Este coeficiente $w_{i,j}[m]$ refleja la proporción de interacciones exitosas frente al total de interacciones realizadas entre el nodo observador n_j y el nodo objetivo n_i, en el intervalo de tiempo específico m, ofreciendo así una medida cuantitativa de la confianza basada en la fiabilidad de las acciones previas del nodo objetivo.

Como se mencionó en la Sección 5.2.3, el impacto de las mediciones pasadas debe ser menor que el de las evaluaciones recientes para reflejar adecuadamente la dinámica y la evolución de las relaciones en la red. Por lo tanto, todos los resultados parciales de cada intervalo de tiempo se combinan en una suma geométrica, tal como se destaca en la siguiente ecuación:

$$h_{i,j} = \sum_{m=0}^{k} w_{i,j}[-m] \cdot r_{i,j}^{m+1} \tag{5.8}$$

donde $h_{i,j}$ representa el parámetro resultante que incorpora el efecto acumulativo de las interacciones entre los nodos n_i y n_j, y se define como:

- $h_{i,j}$: El parámetro resultante que refleja la confianza computacional acumulada, influenciada por la tasa de decaimiento $r_{i,j}$. Esta tasa de decaimiento es seleccionada específicamente para la suma, controlando la disminución del impacto de las mediciones pasadas en comparación con las evaluaciones más recientes.

Para calcular la confianza neurológica, se emplea una función sigmoide, donde k representa el número de intervalos de tiempo transcurridos desde el inicio del funcionamiento del despliegue de la VANET. La expresión matemática se muestra a continuación:

$$T_{neu}(n_i; n_j) = P_{trust}(n_i; n_j) = \begin{cases} \sqrt{\frac{1}{K_{th}}} & \text{si } k < K_{th} \\ \frac{\sqrt{h_{i,j}}}{1+h_{i,j}} & \text{si } k \geq K_{th} \end{cases} \tag{5.9}$$

Este modelo ajusta la confianza neurológica en función de la cantidad de tiempo transcurrido y el parámetro $h_{i,j}$, que se basa en interacciones pasadas. La ecuación refleja dos regímenes distintos:

- Cuando k, el número de intervalos de tiempo, es menor que K_{th}, un umbral predefinido, la confianza se ajusta en base a la inversa de la raíz cuadrada de K_{th}, lo que sugiere una asignación de confianza más conservadora en las fases iniciales de observación.
- Cuando k es igual o superior a K_{th}, la confianza se calcula como una función de $h_{i,j}$, el cual mide la congruencia de comportamientos pasados del nodo objetivo n_i con respecto a las expectativas del nodo observador n_j, ajustada por una función sigmoide para asegurar que la confianza varíe en el intervalo $[0, 1]$.

Como en cálculos anteriores, este resultado se interpreta como la probabilidad de que el nodo n_i sea neurológicamente confiable según la evaluación local realizada por el nodo n_j.

5.2.5 Cálculo de confianza en teoría de juegos

A diferencia de la confianza computacional o neurológica, la confianza basada en teoría de juegos T_{game} es un enfoque proactivo. En este caso, la confianza se obtiene a partir del valor futuro más racional y probable, considerando la evidencia pasada, los comportamientos y la evolución de la confianza, es decir, que la confianza basada en teoría de juegos emplea un repositorio de datos históricos para predecir los valores futuros de confianza.

Dada una VANET con un nodo n_i y una secuencia de valores de confianza global $tr[k]$ definida por la siguiente ecuación:

$$tr[k] = \{tr[k] \mid k = 1, \ldots, K_j\} \tag{5.10}$$

La confianza basada en la teoría de juegos se calcula empleando el polinomio de Lagrange $L(k)$ de la manera siguiente:

$$L(k) = \sum_{m=1}^{K_j} tr[m] \cdot \frac{m!(k-m)!}{k_j! \cdot (m-1)!} \tag{5.11}$$

donde la expresión $\frac{m!(k-m)!}{k_j! \cdot (m-1)!}$ se puede reescribir como un producto:

$$\frac{m!(k-m)!}{k_j! \cdot (m-1)!} = \prod_{r=1, r \neq m}^{K_j} \frac{k-r}{m-r} \tag{5.12}$$

El nodo observador n_j calcula la confianza basada en teoría de juegos utilizando el polinomio de Lagrange. Una vez calculado este polinomio, el nodo observador n_j puede obtener la confianza basada en teoría de juegos para cualquier intervalo de tiempo futuro k_{next} utilizando la función $L(k)$.

Cada nodo observador n_j puede desarrollar esta extrapolación usando un número diferente de medidas de confianza previas K_j, permitiendo así adaptar el cálculo a la cantidad de datos históricos disponibles y a las necesidades específicas de evaluación de confianza en la VANET.

El resultado final para la confianza basada en teoría de juegos $T_{\text{game}}(n_i; n_j)$ depende de los valores locales de K_j y k_{next}, como se demuestra en la siguiente ecuación:

$$T_{\text{game}}(n_i; n_j) = P_{\text{trust}}(n_i; n_j) = L(k_{\text{next}}) \tag{5.13}$$

Al igual que en los cálculos anteriores, dado que los valores de confianza global son puntos de una función estocástica, el resultado $T_{\text{game}}(n_i; n_j)$ se interpreta como la probabilidad de que el nodo n_i sea confiable según la teoría de juegos, basado en el cálculo local realizado por el nodo n_j.

Este enfoque nos permite comprender cómo la evaluación de la confianza, desde la perspectiva de la teoría de juegos, se ajusta para reflejar las dinámicas y las interacciones dentro de una VANET. La función $L(k_{\text{next}})$, derivada del polinomio de Lagrange, permite extrapolar la confianza en futuros intervalos de tiempo, basándose en la historia de interacciones y comportamientos observados, asegurando así que la evaluación de la confianza sea tanto predictiva como adaptativa a los cambios en el comportamiento de los nodos.

5.2.6 Cálculo de confianza global

En una VANET, todos los nodos envían sus evaluaciones locales para un nodo objetivo ni a la infraestructura de cálculo de confianza global (por ejemplo, una red Blockchain), para combinarse en un valor de confianza global.

Dado que la VANET consta de MT nodos, se recopilarán MT valores de confianza diferentes $trust_{i,j}$ para cada nodo objetivo n_i. Cada uno de estos valores se obtiene mediante un mecanismo diferente y desde una perspectiva local única. Posteriormente, en el sistema de cálculo de confianza global, todos estos valores se utilizan para crear una distribución de probabilidad única para cada nodo objetivo n_i. Aplicando la noción de probabilidad de Laplace, todos los valores se agrupan para definir una función de densidad de probabilidad discreta T_{global} con YT puntos mediante la siguiente ecuación:

$$T_{global}[y] = \frac{1}{MT} \cdot \text{card}\{trust_{i,j} \mid j = 1, \ldots, MT, ; thy \leq trust_{i,j} < thy + 1\} \tag{5.14}$$

siendo $y = 1, \ldots, YT$; $thy \in [0, 1]$; $th_1 = 0$ y $th_{YT} = 1$

y donde:

- $T_{global}[y]$ representa la probabilidad de que el valor de confianza global del nodo objetivo n_i pertenezca al intervalo $[thy, thy + 1)$.
- MT representa el número total de nodos en la VANET.
- $trust_{i,j}$ representa el valor de confianza local otorgado por el nodo j al nodo objetivo n_i.
- $\text{card}\{\cdot\}$ representa la función cardinalidad, que determina el número de elementos en cada conjunto que cumple con una condición dada.

- *thy* representa los límites de los intervalos utilizados para agrupar los valores de confianza locales.

Este enfoque permite agrupar todos los valores de confianza local de una manera que refleje de manera efectiva la distribución de la confianza global a lo largo de toda la VANET, ofreciendo una visión integral y matizada de la fiabilidad de cada nodo desde la perspectiva de la red en su conjunto.

Para informar a los nodos sobre los resultados globales utilizando un solo número real (por ejemplo, para cumplir con los requisitos del algoritmo de cálculo de confianza basado en teoría de juegos), se pueden emplear los momentos no centrales λ_z:

$$\lambda_z = \frac{1}{YT} \sum_{y=1}^{YT} (T_{global}[y])^z \quad \text{con } z \in [0, \infty] \tag{5.15}$$

o los momentos centrales μ_z:

$$\mu_z = \frac{1}{YT} \sum_{y=1}^{YT} (T_{global}[y] - \lambda_1)^z \quad \text{con } z \in [0, \infty] \tag{5.16}$$

dependiendo de la implementación específica. Ambos enfoques ofrecen métodos para resumir la distribución de confianza global calculada en la VANET en un único valor que refleja características estadísticas de la distribución, permitiendo así una interpretación simplificada pero informativa de los resultados globales:

- Los **momentos no centrales** λ_z capturan la tendencia general de la distribución de confianza, permitiendo entender la dispersión de los valores de confianza a lo largo de todos los nodos sin considerar su desviación con respecto a la media.
- Los **momentos centrales** μ_z, por otro lado, ofrecen una medida de cómo los valores de confianza se dispersan alrededor del valor medio de confianza λ_1, proporcionando una perspectiva sobre la variabilidad de la confianza en la red.

Estos cálculos matemáticos facilitan una comprensión profunda y detallada de la distribución de la confianza global en la VANET, permitiendo que los algoritmos y sistemas que dependen de esta información tomen decisiones basadas en métricas consolidadas y significativas.

5.3 Validación Experimental: Simulaciones y Resultados

Para evaluar el desempeño de la solución propuesta para redes vehiculares ad hoc (VANETs), se planificó y llevó a cabo una validación experimental. Durante esta validación, se realizaron dos experimentos diferentes con el objetivo de analizar:

El tiempo de convergencia del mecanismo de seguridad propuesto. La tasa de éxito en la detección de vehículos maliciosos en una implementación de VANET.

5.3.1 Metodología de Simulación

Ambos experimentos se realizaron utilizando metodologías de simulación en Python, aprovechando librerías como NumPy para cálculos numéricos, Pandas para el manejo de datos, y Matplotlib y Seaborn para la visualización de resultados. Con estas herramientas, se representaron 120 vehículos en un entorno simulado, cada uno ejecutando una aplicación y un algoritmo de cálculo de confianza diferentes. También se consideraron distintas cantidades de vehículos maliciosos para diversas evaluaciones. Todas las simulaciones se llevaron a cabo en una arquitectura Linux.

5.3.2 Configuraciones de Simulación

Los vehículos VANET simulados representaron una arquitectura común basada en el microcontrolador ESP-32, comunicaciones WiFi y sensores simples como temperatura o humedad. Los algoritmos de cálculo de confianza se distribuyeron entre los vehículos de manera homogénea pero aleatoria. Los vehículos también podían comportarse de manera maliciosa de forma aleatoria, pero de acuerdo con los porcentajes configurados. Todas las simulaciones se repitieron doce veces para eliminar posibles efectos externos. Los resultados presentados se obtienen como el promedio de todas estas simulaciones parciales. Las simulaciones representaron 24 horas de operación en tiempo real en la implementación de la VANET. Experimentos:

Experimento 1: Tasa de Éxito

Este experimento se centró en la tasa de éxito de la solución propuesta. Para diferentes cantidades de vehículos maliciosos en la implementación de la VANET, se analizó el porcentaje de ellos que se detectan y aíslan correctamente.

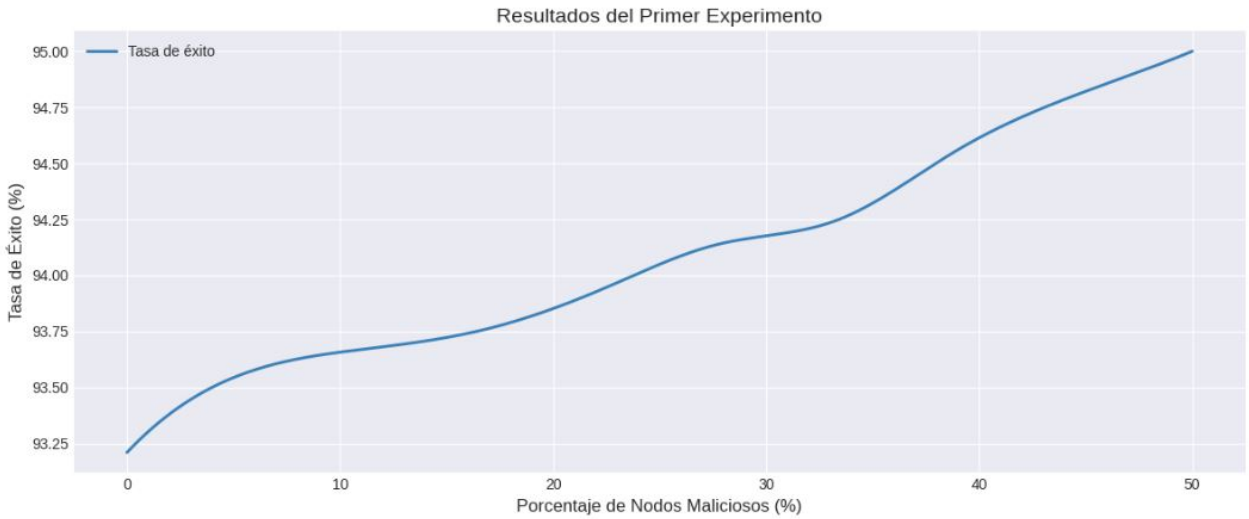

Figura 5.2: Tasa de éxito para diferentes cantidades de vehículos maliciosos.

La Figura 5.2 muestra los resultados del primer experimento. Como se observa, la tasa de éxito supera el 85 % en todos los casos. A medida que aumenta la cantidad de vehículos

maliciosos, la tasa de éxito también aumenta, aunque este efecto es común a la mayoría de las tecnologías.

El resultado más interesante de la Figura 5.2 es la ausencia de una asíntota. Incluso si el 50 % de los vehículos en la implementación de la VANET son maliciosos, la solución propuesta no se satura y puede operar normalmente, detectando hasta el 98 % de los vehículos maliciosos.

Experimento 2: Tiempo de Convergencia

Este experimento se centró en el tiempo de convergencia. Para diferentes cantidades de vehículos maliciosos, se evaluó el tiempo máximo de convergencia necesario para evaluar todos los vehículos y configurar la implementación final de la VANET.

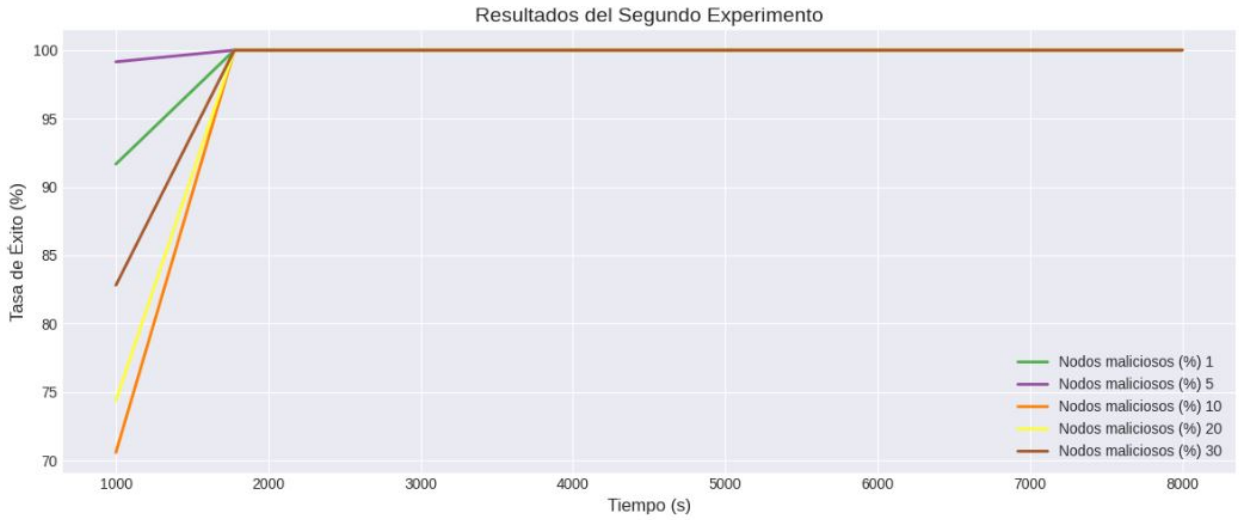

Figura 5.3: Tiempo de convergencia para diferentes cantidades de vehículos maliciosos.

La Figura 5.3 muestra los resultados del segundo experimento. Para vehículos maliciosos de hasta un 10 %, el tiempo de convergencia es inferior a una hora (3600 s). Sin embargo, a partir de este punto, el tiempo de convergencia comienza a crecer exponencialmente. Para un 25 % de vehículos maliciosos, el tiempo de convergencia alcanza las dos horas, y para cualquier número de vehículos maliciosos por encima de este límite, la Figura 5.3 no muestra una convergencia clara. En cualquier caso, estos resultados son aceptables, considerando el tiempo de convergencia de otros componentes de las VANETs como los sensores de CO2.

Los resultados de la validación experimental demuestran la eficiencia y escalabilidad de la solución propuesta para la detección de vehículos maliciosos en redes VANETs. Teniendo en cuenta la naturaleza dinámica de este tipo de redes, el tiempo de convergencia aceptable permite la actualización continua de la confianza y la adaptación del sistema a posibles cambios en el comportamiento de los vehículos.

5.4 Resumen y trabajos futuros

En este capítulo, se ha presentado una nueva arquitectura distribuida para la provisión de servicios de confianza y reputación en redes VANET (Redes Vehiculares Ad Hoc). La arquitectura se basa en tecnologías Blockchain y la composición de diferentes modelos conceptuales (cognitivo, computacional, neurológico y basado en teoría de juegos) utilizando funciones estocásticas basado en Bordel et al., 2022.

Los resultados de la validación experimental demuestran la eficiencia y escalabilidad de la solución propuesta. La tasa de éxito para la detección de vehículos maliciosos supera el 85 % en todos los casos, incluso con un 50 % de vehículos maliciosos en la red. El tiempo de convergencia también es aceptable, siendo inferior a una hora para un 10 % de vehículos maliciosos. Estos resultados son comparables o mejores que los de otras soluciones propuestas en la literatura.

A continuación, se detallan los trabajos futuros que se plantean para continuar con la investigación en esta área:

Evaluación en un entorno real: La solución propuesta se ha evaluado en un entorno simulado. Es necesario realizar una evaluación en un entorno real con vehículos VANET y dispositivos hardware comerciales. Esta evaluación permitirá validar la eficacia de la solución en condiciones reales de operación.

Análisis del impacto de la movilidad: La movilidad es una característica fundamental de las redes VANET. Es necesario analizar el impacto de la movilidad en el rendimiento de la solución propuesta. Este análisis permitirá determinar la necesidad de realizar modificaciones en la arquitectura o los algoritmos para adaptarlos a las características específicas de las redes VANET. Integración con otros mecanismos de seguridad: La solución propuesta puede integrarse con otros mecanismos de seguridad para mejorar la seguridad general de las redes VANET. Se estudiará la integración de la solución propuesta con otros mecanismos de seguridad, como la detección de intrusiones o la prevención de ataques. Implementación en diferentes plataformas: La solución propuesta se ha implementado en una plataforma específica. Es necesario realizar la implementación en diferentes plataformas para facilitar su adopción por parte de la comunidad VANET.

En definitiva, la solución propuesta se presenta como una alternativa viable para la provisión de servicios de confianza y reputación en redes VANET. Los trabajos futuros se centrarán en validar la eficacia de la solución en un entorno real, analizar el impacto de la movilidad, integrarla con otros mecanismos de seguridad e implementarla en diferentes plataformas.

Capítulo 6

Provisión de servicios predictivos de datos en VANET

En este Capitulo desarrollamos un modelo predictivo integrado que utiliza datos recopilados por VANETs y variables climáticas para proveer servicios de datos. Este modelo se basa en técnicas avanzadas de correlación y análisis de grandes volúmenes de datos, buscando capturar la complejidad y la variabilidad inherente a las condiciones viales y meteorológicas.

Esta contribución nos permite concluir que el **Objetivo#4** de este proyecto de Tesis ha sido alcanzado.

El capítulo incuye una validación experimental de las contribuciones realizadas, con lo que alcanza también el **Objetivo#8**.

6.1 Introducción

Este capítulo se enfoca en la creación de un modelo predictivo que pueda integrarse en servicios distribuidos de datos (por ejemplo, para el cálculo del índice de peligrosidad de las carreteras), considerando los datos recogidos por los nodos de las VANET y la información meteorológica, con el objetivo de mejorar la precisión de los servicios actuales.

Los modelos predictivos para VANET han evolucionado significativamente, integrando tecnologías de detección remota, aprendizaje automático y análisis de grandes volúmenes de datos. Investigaciones recientes M. M. Ahmed y Abdel-Aty, 2011; Chang et al., 2010; P. Li et al., 2022 han demostrado la eficacia de estos modelos, por ejemplo, en la predicción del índice de peligrosidad en carreteras, utilizando datos de sensores y técnicas avanzadas de análisis.

La propuesta se centra en el desarrollo de un modelo predictivo que integre datos recogidos por nodos de VANET y variables climáticas para estimar el índice de peligrosidad de las carreteras. Se analizarán diferentes tipos de carreteras y secciones específicas para identificar correlaciones significativas entre los datos disponibles.Chio et al., 2015; Shan y Toth, 2018

La validación del modelo se realizará mediante la comparación de las predicciones con incidentes reales reportados, evaluando la precisión y eficacia del modelo en la predicción de

áreas de alto riesgo.James et al., 2013; Kuhn, Johnson et al., 2013

El modelo predictivo propuesto representa un avance significativo en la gestión de la seguridad vial, ofreciendo una herramienta valiosa para la planificación y prevención en la infraestructura vial del cantón.James et al., 2023

6.2 Propuesta

La elaboración de modelos predictivos constituye el núcleo de esta propuesta, enfocándose en el ámbito específico de las Redes Vehiculares Ad hoc (VANETs) para mejorar la gestión y seguridad vial. El proceso de creación de estos modelos se estructura en tres etapas fundamentales: (i) adquisición y preprocesamiento de datos, (ii) análisis de correlación, y (iii) definición y particularización del modelo.

6.2.1 Adquisición y Preprocesamiento de Datos

La primera etapa implica la recolección de datos pertinentes a través de sensores ubicados en vehículos y en la infraestructura vial. Estos datos incluyen, pero no se limitan a, velocidad de los vehículos, densidad del tráfico, condiciones meteorológicas, y estados de la carretera. El preprocesamiento es crucial para limpiar los datos de posibles errores o valores atípicos, normalizando y estandarizando los mismos para su posterior análisis. La infraestructura implementada es una VANET que supervisa aproximadamente 100 kilómetros de carreteras en el cantón de Valais (Suiza), específicamente en los distritos de Sion y Hérens. Se monitorean tres tipos de carreteras: la autopista A9 entre Saxon y Sion (30 kilómetros), carreteras urbanas en Sion (20 kilómetros), y una carretera de montaña entre Sion y Arolla (50 kilómetros).

Esta infraestructura proporciona datos sobre la ubicación, tiempo, velocidad del vehículo (autobús), temperatura del camino, altura de la película de agua, porcentaje de hielo, fricción, punto de rocío y condiciones generales de la carretera (seca, húmeda, humedad, nieve derretida, nevada/hielo).

Para obtener un conocimiento más profundo sobre la situación, también se considera información climática de la oficina estatal Meteosuisse. Meteosuisse ofrece mediciones de aproximadamente 145 variables distintas con una precisión temporal de milisegundos. Sin embargo, para este trabajo, solo consideramos cuatro de estas variables: el grosor total de la nieve acumulada (en centímetros), precipitación (suma diaria, en milímetros), duración de la luz solar (suma horaria, en minutos) y la radiación solar horaria (en vatios por metro cuadrado).

Además, se obtuvieron datos sobre las estadísticas de tráfico (incluidos los accidentes) en Valais. Esta información se utilizó para calcular el índice de peligrosidad (DI) de las carreteras estudiadas durante el segundo semestre de 2016. Básicamente, el índice de peligrosidad de una carretera (1) es una medida relativa del número de accidentes en esta carretera (N_{acc}), considerando el nivel correspondiente de exposición al riesgo (R, es decir, el volumen de tráfico en vehículos $\cdot$ km). Para eliminar variaciones aleatorias, generalmente se emplean datos

medios temporales y espaciales.

$$DI = \frac{N_{acc}}{R} \quad (\text{accidentes} \cdot \text{vehículos} \cdot \text{km})$$

Una base de datos espacial se utiliza para almacenar estos parámetros. Se empleó una base de datos PostgreSQL 9.6, con la extensión PostGIS 2.3.2 para habilitar operaciones espaciales. Los datos proporcionados por la infraestructura de sensores se almacenan considerando la marca de tiempo de los datos y la ubicación donde se generaron, almacenando los valores en tipos de datos timestamp con zona horaria y geometría. Esto habilita la posibilidad de realizar solicitudes temporales (rangos de datos dependiendo de fechas) y solicitudes espaciales (filtrado de datos por proximidad o densidad).

Los datos provenientes de Meteosuisse se almacenan en dos tablas interrelacionadas. La primera almacena información de metadatos de las estaciones meteorológicas, como la ubicación, métricas y tiempo de la última actualización. La segunda contiene observaciones relacionadas con el station_id. Cada observación tiene un identificador único consistente en un número autoincremental, actuando como clave de tabla.

Los datos sobre estadísticas de tráfico también se importaron a la base de datos espacial. La tabla que describe los accidentes contenía las coordenadas de los accidentes (expresadas en geometría), ID de la carretera, hora del accidente (timestamp con zona horaria), tipo, descripción, daños materiales causados y tipo de lesiones (muerte, grave y menor).

Para la representación de la información de manera espacial, utilizamos el marco de QGIS versión 2.18.6. Obtenemos información en formato vectorial de la base de datos PostGIS y la representamos como tres capas. Usamos Microsoft Bing como mapa base para las superposiciones.

Hemos presentado la información gráficamente y utilizando mapas de la región para hacer una selección de datos según el tipo de carretera definido en la introducción.

Para ello, hemos obtenido secciones de carretera de 500 m, 1 km y 2 km y hemos definido para cada sección el tipo de carretera (autopista, carretera urbana y carretera de montaña). Para la medición de la sección, hemos utilizado las herramientas de medición proporcionadas por QGIS. Para cada sección, se ha generado un conjunto de datos con información proporcionada por la infraestructura de sensores, información generada por Meteosuisse de la estación meteorológica más cercana (meteosuisse.station.sion) y el número y tipo de accidentes ocurridos en esas secciones de carretera. Esta es la información de entrada que introducimos en nuestro proceso de análisis de correlación, descrito en la sección siguiente.

6.2.2 Análisis de Correlación

Posteriormente, se realiza un análisis de correlación para identificar las relaciones significativas entre las diferentes variables recolectadas. Este paso es fundamental para entender cómo interactúan entre sí los distintos factores que influyen en la seguridad y fluidez del tráfico. El análisis de correlación ayuda a destacar las variables que tienen mayor impacto en los fenómenos de interés, facilitando así la definición de modelos predictivos más precisos y eficaces.

En este caso, solo disponemos de información global (ver Tabla 6.1), por lo que se propone un método de análisis más simple. Las carreteras se dividen en secciones consecutivas fijas de la longitud especificada, que se emplean para obtener las medias geográficas de los parámetros. Con esta información, relacionada con la primera mitad del año, buscamos correlación con la tasa de accidentes en la segunda mitad del año (ver Tabla 6.2 y Tabla 6.3). Para este primer trabajo, además, no se considera el tiempo de adquisición de datos.

Las variables cuya correlación con la tasa de accidentes es inferior a $|r|$=0.3 no se consideran relevantes para este estudio. De esta manera, como se puede ver, diferentes variables pueden ser relevantes dependiendo de la escala de análisis considerada y del tipo de carretera (es decir, hay una fuerte dependencia de la configuración de la carretera). En general, sin embargo, las secciones de carretera de 1 km presentan un buen equilibrio y resultados bastante aceptables. En relación con la información climática, como solo se coloca una estación de medición alrededor del área de estudio, se obtienen correlaciones temporales (mensuales).

Tabla 6.1: Flujo de tráfico dependiendo de la tipología de carretera.

Tipo de Carretera	Vehículo · km (en cientos)
Autopista	419
Carretera Urbana	119
Carretera de Montaña	20

Tabla 6.2: Correlación entre la tasa de accidentes y los parámetros recogidos por la VANET

Tipo de Carretera	Altitud	Velocidad	Temp	Película de Agua	Hielo	Fricción
Autopista	-0.0294	-0.0758	-0.1479	0.082	-0.434	-0.325
Carretera Urbana	-0.3771	-0.352	0.2640	0.053	-0.684	0.232
Carretera de Montaña	-0.8648	-0.521	0.6023	0.099	0.494	0.043

Tabla 6.3: Correlación entre la tasa de accidentes y los parámetros de Meteosuisse.

Tipo de Carretera	Nieve	Lluvia	Sol	Radiación
Autopista	-0.4205	-0.0155	-0.1402	-0.1991
Carretera Urbana	0.1526	-0.2699	-0.4000	-0.4459
Carretera de Montaña	-0.4410	-0.4692	0.5481	0.5076

6.2.3 Definición y Particularización del Modelo

Finalmente, con base en los resultados obtenidos del análisis de correlación, se procede a la definición y particularización del modelo predictivo. Esta etapa implica la selección de técnicas de modelado matemático y computacional, tales como regresión lineal, modelos de machine learning, o redes neuronales, adecuadas para predecir los comportamientos de interés en el contexto de VANETs. La particularización del modelo se ajusta específicamente a las necesidades y características del entorno vial bajo estudio, permitiendo una predicción efectiva de variables clave como la congestión del tráfico, la probabilidad de accidentes o la eficiencia en el uso de las vías.

Cada una de estas etapas es crucial para el desarrollo exitoso de modelos predictivos en el contexto de las Redes Vehiculares Ad hoc, proporcionando una base sólida para la toma de decisiones informadas y la implementación de medidas proactivas para la mejora de la seguridad y la gestión del tráfico.

Como se puede observar, las correlaciones entre las variables relevantes identificadas en la subsección anterior y la tasa de accidentes son, en general, alrededor de $|r| = 0{,}5$. Esto indica que ninguna de estas variables es una causa directa de los accidentes, pero sí están involucradas en la ocurrencia de los mismos. Por lo tanto, una combinación de varias de estas variables debería explicar la tasa de accidentes durante el siguiente período temporal (6 meses). Sin embargo, cómo estas variables son ponderadas y/o combinadas para causar o no un accidente es desconocido. En este trabajo, suponemos que la función multivariante $F(\vec{x})$ representa esta combinación ponderada. Esta función, además, como cualquier otra función, puede ser expresada usando la serie de Taylor centrada en el origen:

$$DI = F(\vec{x}) = \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{k_1+\cdots+k_d=k} \frac{\partial^k F(\vec{0})}{\partial x_1^{k_1} \cdots \partial x_d^{k_d}} (x_1^{k_1} \cdots x_d^{k_d}) \tag{6.1}$$

Donde $\vec{x}$ es un vector d-dimensional que contiene las variables relevantes a ser consideradas en el modelo predictivo.

El modelo, además, puede ser simplificado si todos los valores constantes se agregan:

$$DI = \sum_{k=0}^{\infty} \sum_{k_1+\cdots+k_d=k} \lambda_{k_1,\ldots,k_d} (x_1^{k_1} \cdots x_d^{k_d}) \approx \sum_{k=0}^{q} \sum_{k_1+\cdots+k_d=k} \lambda_{k_1,\ldots,k_d} (x_1^{k_1} \cdots x_d^{k_d}) \tag{6.2}$$

De esta manera, el modelo predictivo propuesto estaría totalmente definido si se obtuvieran los parámetros desconocidos $\lambda_{k_1,\ldots,k_d}$. Estos parámetros son independientes del tiempo, aunque se podría obtener una expresión matemática idéntica si se considerasen dependientes del tiempo. Este conjunto de parámetros puede calcularse considerando las colecciones de datos empleadas en la subsección anterior y resolviendo el sistema de ecuaciones resultante usando la optimización de la técnica de error cuadrático medio.

6.3 Validación Experimental

Se diseñó una validación experimental para verificar la propuesta y analizar el desempeño de los modelos sugeridos. Esta sección detalla la elaboración de un modelo predictivo específico, empleando la información anteriormente descrita, y evalúa la validez de las predicciones generadas al intentar pronosticar la tasa de accidentes durante la segunda mitad del año 2016, basándose en datos del primer semestre.

Para construir este modelo predictivo particular, se siguieron los pasos metodológicos establecidos en las secciones anteriores, comenzando por la recopilación y preprocesamiento de datos relevantes, seguido por un análisis de correlación detallado entre las variables seleccionadas y la tasa de accidentes. Posteriormente, se definieron los parámetros y la estructura del modelo,

aplicando la serie de Taylor para su expresión matemática y considerando las variables con mayor influencia según el análisis previo.

La fase de experimentación implicó el empleo de técnicas estadísticas para la validación del modelo, incluyendo la comparación de las tasas de accidentes reales registradas en la segunda mitad de 2016 con las predicciones del modelo. Se utilizaron métricas de desempeño, como el error cuadrático medio (MSE) y el coeficiente de determinación (R^2), para evaluar cuantitativamente la precisión y la capacidad predictiva del modelo.

Además, se discuten los resultados obtenidos, destacando la efectividad del modelo para prever la tasa de accidentes y señalando las posibles mejoras y ajustes para incrementar la precisión de las predicciones en futuros trabajos. Esta evaluación crítica permite identificar las fortalezas y limitaciones del modelo propuesto, estableciendo una base sólida para investigaciones futuras en la predicción de tasas de accidentes utilizando modelos basados en VANETs y análisis de datos avanzados.

6.3.1 Creación del Modelo

El propósito de esta subsección es definir un modelo predictivo para estimar la tasa de accidentes en carreteras de montaña, tomando en cuenta segmentos de carretera de 1 km de longitud. Para desarrollar este primer modelo predictivo se consideraron tres variables recolectadas por las VANET: el porcentaje de hielo, la altura de la película de agua y la fricción. Además, se incorporó una variable climática: la precipitación. Así, se contemplaron cuatro variables de entrada.

Para la construcción del modelo, es necesario elegir el orden de las expresiones matemáticas. En este primer ejemplo, se optó por un modelo cuadrático ($q = 2$).

Con estas decisiones, el modelo propuesto tiene quince parámetros desconocidos. Para determinar su valor, se analizaron treinta segmentos distintos de carreteras de montaña. Datos sobre la tasa de accidentes en estos segmentos e información extraída de las VANET (así como información climática de Meteosuisse) fueron empleados para calcular estos parámetros $\lambda_{k1,\ldots,kd}$ (ver Tabla 6.4).

6.3.2 Predicciones y Resultados

Se utilizó un conjunto de nuevos segmentos de carretera (grupo de control) para evaluar el desempeño del modelo propuesto. Empleando información del proyecto NOSE y de Meteosuisse, se obtuvieron las tasas de accidentes predichas para la segunda mitad de 2016. Estos resultados se compararon con la información real proporcionada por la Oficina de Tráfico.

Para valorar la calidad de la predicción realizada, se calculó y evaluó el error cuadrático medio. La Tabla 6.5 muestra el error asociado con cada segmento de carretera.

Como se puede observar, las situaciones extremas se predicen mal. Este hecho se debe a los datos empleados durante la creación del modelo predictivo. Como solo estaba disponible información de seis meses, no se consideró un número representativo de muestras de estas situaciones. Trabajos futuros considerarán predicciones más precisas a medida que se disponga

Parámetro	Valor
$\lambda_{0,0,0,0}$	$1{,}27 \times 10^7$
$\lambda_{1,0,0,0}$	$-3{,}1 \times 10^7$
$\lambda_{0,1,0,0}$	$-1{,}8 \times 10^5$
$\lambda_{0,0,1,0}$	$-4{,}8 \times 10^3$
$\lambda_{0,0,0,1}$	$-4{,}6 \times 10^5$
$\lambda_{1,1,0,0}$	$1{,}91 \times 10^7$
$\lambda_{1,0,1,0}$	118,46
$\lambda_{1,0,0,1}$	0,4437
$\lambda_{0,1,1,0}$	$7{,}06 \times 10^4$
$\lambda_{0,1,0,1}$	$2{,}33 \times 10^5$
$\lambda_{0,0,1,1}$	$5{,}57 \times 10^5$
$\lambda_{2,0,0,0}$	$5{,}82 \times 10^3$
$\lambda_{0,2,0,0}$	33,02
$\lambda_{0,0,2,0}$	$1{,}69 \times 10^4$
$\lambda_{0,0,0,2}$	89,1053

Tabla 6.4: Parámetros del modelo

Accidentes por segmento de carretera	Error
Menos de uno	44.26 %
1 – 2	17.50 %
Dos o más	58.55 %
Total	20.19 %

Tabla 6.5: Error cuadrático medio de las predicciones.

de una mayor cantidad de información.

En cualquier caso, como el modelo propuesto produce números decimales, mientras que el número de accidentes es un entero, es necesario realizar una conversión entre ambos valores. Se consideraron tres posibilidades: redondear al entero más cercano, truncar al entero inferior y truncar al entero superior.

La Figura 6.1 presenta la tasa de éxito en las predicciones para cada técnica de conversión.

Como se puede en la figura 6.1, que representa la tasa de éxito de diferentes técnicas de conversión para un modelo predictivo, visualizada en un gráfico de barras. Alrededor del 80 % de los casos se predicen correctamente. La truncación, sin embargo, presenta más problemas. En general, la truncación al entero superior es más precisa (alrededor de un 10 % más) que la truncación al entero inferior (que presenta una tasa de éxito del 60 %, aproximadamente). Los resultados muestran aproximadamente un 80 % de éxito para el redondeo, un 70 % para el truncamiento superior y un 60 % para el truncamiento inferior, la técnica de redondeo es la solución más exitosa.

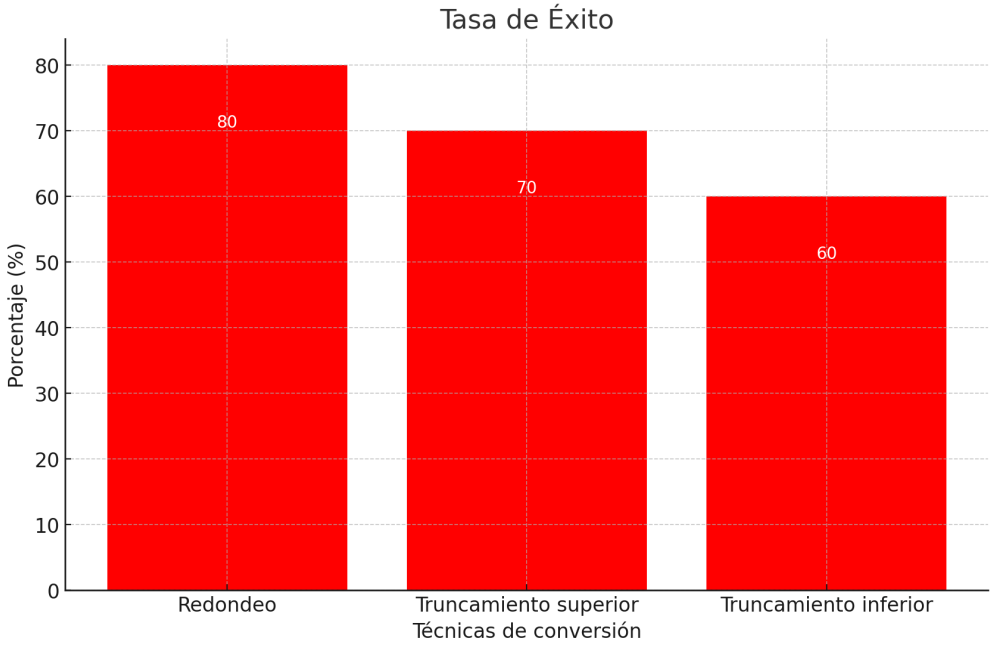

Figura 6.1: Tasa de éxito en las predicciones según la técnica de conversión. La técnica de redondeo muestra el mayor éxito, seguido por la truncación al entero superior y la truncación al entero inferior.

6.4 Conclusiones

En este documento, se propone un marco y un modelo predictivos con el fin de pronosticar la tasa futura de accidentes en un segmento de carretera en función de un conjunto de variables monitoreadas mediante VANETs. El modelo presentado se enfoca en las carreteras de montaña del cantón de Valais, en Suiza.

Los resultados indican que el modelo propuesto permite obtener una visión general acerca de las tasas futuras de accidentes. Sin embargo, las predicciones detalladas y más exactas requieren soluciones más avanzadas o mayor información sobre las carreteras, ya que, en la actualidad, las predicciones presentan un error del 20 %.

Los trabajos futuros deberán considerar la inclusión de información recolectada durante periodos de tiempo más extensos con el objetivo de descartar fenómenos aleatorios, y proporcionar información geográfica más precisa de las carreteras.

Capítulo 7

Ejecuación segura de servicios en VANET mediante Blockchain

En este Capítulo diseñamos e implementamos un ecosistema de servicios que mejora la eficiencia y escalabilidad de las técnicas de mapeo de obstáculos seguras habilitadas por Blockchain en VANET. Este sistema se basa en un algoritmo de comunicación vehicular seguro y emplea tecnologías de criptografía para garantizar un intercambio de datos seguro y robusto entre vehículos.

Gracias a esta propuesta, logramos alcanzar el **Objetivo#5** de este proyecto de Tesis.

El capítulo incuye una validación experimental de las contribuciones realizadas, con lo que alcanza también el **Objetivo#8**.

7.1 Introducción

En un mundo digitalmente evolucionado, el papel de los vehículos como comunicadores dentro de la matriz tecnológica ha dado lugar a las comunicaciones Vehículo-a-Todo (V2X). Este nuevo paradigma de comunicación, entre otras innovaciones, ha originado el Internet de los Vehículos, el cual permite el intercambio de datos entre vehículos, infraestructura y medio ambiente Z. Sun et al., 2021.

De hecho, el intercambio de datos entre vehículos es la tecnología más relevante y prometedora. Por lo tanto, recibe un nombre específico: comunicaciones Vehículo-a-Vehículo (V2V). Diferentes autores G. C. Tripathi, 2021 han propuesto que la comunicación V2V será esencial para mejorar la seguridad vial y la eficiencia del tráfico.

Las comunicaciones V2V no pueden crear redes fijas (ya que los vehículos son móviles), sino redes ad hoc cuya estructura evoluciona dinámicamente según el movimiento de los vehículos. Específicamente, las Redes Ad Hoc Vehiculares (VANET) y sistemas relacionados, similares a las Redes Ad Hoc Móviles (MANET), consisten en vehículos, Unidades al Lado del Camino (RSUs) y una Autoridad de Confianza (TA) actuando como nodos móviles Campolo et al., 2011 e intercambiando datos sobre el tráfico, el estado del vehículo, etc.

Estas redes, entre otras ventajas, mejoran la toma de decisiones de los vehículos autónomos proporcionando datos ambientales para medidas proactivas contra peligros Ge et al., 2017.

Sin embargo, cualquier canal de comunicación abierto o intercambio de datos tiene varios riesgos de seguridad asociados. Y las redes V2V aún enfrentan varios desafíos abiertos, incluyendo la detección de vehículos maliciosos, manteniendo la apertura y seguridad, y previniendo la falla del sistema entero desde un único punto de avería Noor-A-Rahim et al., 2022.En particular, se requieren técnicas para mitigar la inyección de datos falsos en redes V2V de manera eficiente y escalable.

En este contexto, algunos autores introdujeron herramientas de blockchain como una solución innovadora para mejorar la visibilidad de los peligros en la carretera y la seguridad de los datos Alsarhan et al., 2023; J. Zhang et al., 2019. Entre todas las propuestas anteriores, el sistema Starling Shu et al., 2020 es el más prometedor, ya que está específicamente diseñado para proteger los datos que describen obstáculos en el entorno.Gad et al., 2021

El blockchain forma el núcleo del sistema Starling, ofreciendo autenticación robusta y protección de la privacidad. Junto con mecanismos de consenso como Prueba de Trabajo (PoW), Prueba de Participación (PoS) y Prueba de Autoridad (PoA), el sistema utiliza contratos inteligentes y el Sistema de Archivos Interplanetario (IPFS) para asegurar los procesos de comunicación V2V. Butt et al., 2019; Dorri et al., 2017

Como resultado, asegura la integridad de los datos y mejora la visibilidad de los obstáculos. Pero, como cualquier otra herramienta habilitada por blockchain, Starling enfrenta un problema crítico: es muy pesado computacionalmente. Pero los escenarios de transporte futuro serán muy densos y dinámicos. Por lo tanto, se deben investigar alternativas muy escalables y eficientes.

Por lo tanto, introducimos el sistema NeoStarling, una arquitectura innovadora que mejora la eficiencia y escalabilidad de las técnicas de mapeo de obstáculos seguras habilitadas por Blockchain. Nuestro sistema beneficia potencialmente a todos los usuarios de la red, mejorando la seguridad y eficiencia de la comunicación V2V. NeoStarling incorpora el nuevo y propuesto .Algoritmo de Comunicación Vehicular Seguro"(SVCA), desplegado en una red blockchain permisionada, para un intercambio de datos seguro, robusto y eficiente a gran escala. Gracias a HMAC-SHA256 (código de autenticación de mensajes basado en hash), NeoStarling redefine las redes de comunicación V2V, mejorando la seguridad de los datos, la privacidad y la escalabilidad de la red. Aunque NeoStarling avanza significativamente en la comunicación V2V, algunas limitaciones permanecen. Los desarrollos futuros explorarán otras tecnologías complementarias como nodos ligeros, soluciones de libro mayor distribuido escalables y potencial monetización de datos de vehículos.

El sistema NeoStarling avanza en tres áreas clave:

- Integración de Criptografía Avanzada: El Emparejamiento Bilíneo y la Criptografía de Curva Elíptica (ECC) se combinan para una seguridad de datos y autenticación de usuarios robustas. La integración del Algoritmo Descentralizado Seguro V2V HMAC-SHA256 (DSV-HMAC-SHA256) mejora aún más la seguridad y eficiencia.
- Estrategia Innovadora de Comunicación Segura y Re-Autenticación: Nuestro .Algoritmo

de Comunicación Vehicular Seguro"(SVCA) asegura la autenticidad de los datos y minimiza las amenazas de vehículos maliciosos, contribuyendo a una comunicación V2V confiable y segura.

- Escalabilidad y Eficiencia Mejoradas: La implementación de una red blockchain permisionada usando PoA aumenta la escalabilidad aproximadamente en un 50 %, permitiendo que un mayor número de vehículos compartan datos en tiempo real sin sobrecargar la red.
- Fiabilidad y Privacidad de Datos Mejoradas: Starling garantiza la validez de los datos y mejora la fiabilidad en alrededor del 30 % utilizando Tecnología de Libro Mayor Distribuido (DLT) y tecnología blockchain. El sistema protege los datos contra manipulaciones y pérdidas mientras asegura un acceso equitativo y transparencia.

7.2 Diseño del Sistema Propuesto

Esta sección profundiza en los detalles de nuestra solución propuesta, incluyendo los algoritmos seguros para mejorar las comunicaciones vehiculares. La Sección 3.1 discute la visión general del sistema NeoStarling. La Sección 3.2 describe el Algoritmo Seguro Descentralizado V2V HMAC-SHA256 empleado en el proceso de registro y autenticación eficiente y escalable. Finalmente, la Sección 3.3 presenta un protocolo de autenticación optimizado y eficiente para el sistema NeoStarling y cómo se integra en la arquitectura estándar de Starling.

7.2.1 Visión General del Sistema NeoStarling

En esta sección, discutimos la funcionalidad global del sistema NeoStarling, basado en el marco de Starling. En términos generales, nuestro nuevo diseño NeoStarling despliega un algoritmo HMAC-SHA256 personalizado, enfocado en mejorar la fiabilidad de los datos y la comunicación segura de datos, abordando directamente los desafíos prevalentes en el ámbito de la comunicación V2V Belchior et al., 2021; Siyal et al., 2019.

Pero, al mismo tiempo, este esquema ligero asegura una mejora significativa en la escalabilidad del sistema.Bashir, 2017 Además, este nuevo algoritmo permite un protocolo de autenticación optimizado, lo que aumenta la eficiencia global de NeoStarling.

La Figura 7.1 representa el modelo de descomposición del sistema NeoStarling, detallando los pasos clave involucrados en el proceso y cómo se interconectan para formar un sistema de comunicación V2V seguro y eficiente.

Esta ilustración también acentúa la ubicación estratégica del Terminal de Autoridad (TA) dentro de la infraestructura en la nube del Sistema NeoStarling. Junto con el dispositivo a prueba de manipulaciones (TPD), bases de datos maestras y locales y la red Blockchain (así como todos los SmartContracts desplegados). El diagrama acentúa los beneficios de situar el TA (y los componentes restantes) en la nube, incluyendo escalabilidad del sistema, alta accesibilidad y medidas de seguridad robustas. Esta visualización enfatiza la capacidad del sistema para asegurar el intercambio de datos en tiempo real y la comunicación fluida con vehículos autónomos, subrayando los avances que NeoStarling ofrece en el ámbito de

la comunicación V2V. Como se ilustra en la figura, el Terminal de Autoridad (TA) está posicionado dentro de la nube, ocupando un rol central en el sistema NeoStarling. Asegura un rendimiento óptimo del sistema y una seguridad de datos robusta. Anclando el TA en la nube, capitalizamos los innumerables beneficios de la computación en la nube.

Esto incluye escalabilidad mejorada, donde alojar el TA en la nube permite a nuestro sistema escalar eficientemente, integrando sin problemas un número creciente de vehículos y usuarios sin una inversión significativa en infraestructura física; un testimonio de la visión del sistema NeoStarling de atender a una extensa red de vehículos autónomos. La accesibilidad y flexibilidad también están en primer plano, con el TA basado en la nube garantizando una accesibilidad generalizada, permitiendo que cualquier vehículo, independientemente de su ubicación, se conecte con el TA siempre que haya conectividad a internet. Esta característica pivotal asegura la transferencia de datos en tiempo real y la recepción de directivas instantáneas, que son elementos clave en la red de vehículos autónomos en constante evolución. Por último, priorizamos la seguridad, aprovechando los mecanismos avanzados de seguridad de la nube para proteger nuestros datos del sistema y amplificar la seguridad de los vehículos. Con proveedores de servicios en la nube de primer nivel empleando protocolos de seguridad avanzados, los datos de NeoStarling permanecen fortificados contra posibles amenazas cibernéticas, asegurando que el sistema NeoStarling opere de manera segura y eficiente.

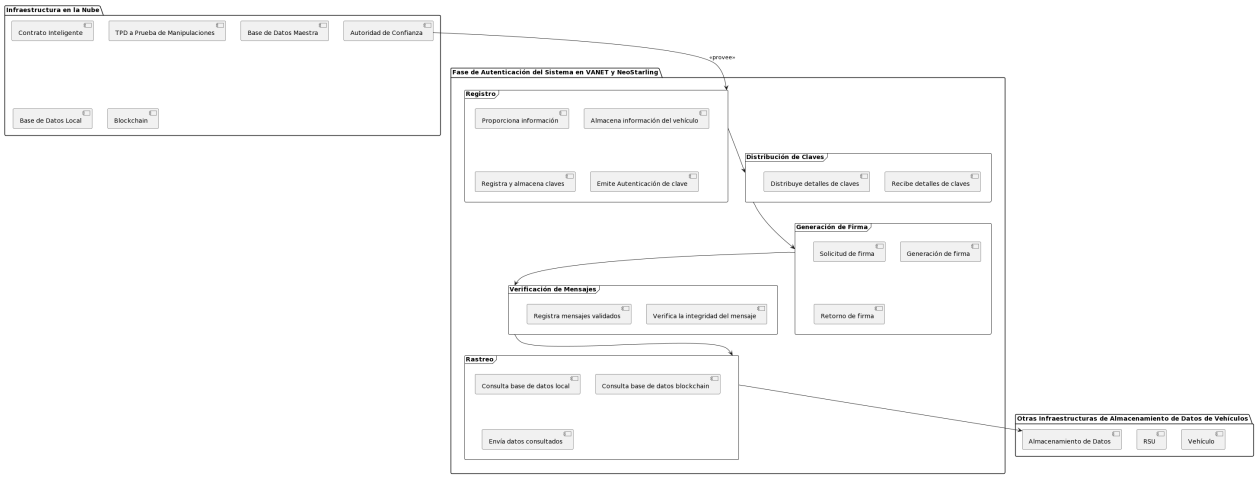

Figura 7.1: Modelo de descomposición para el propuesto NeoStarling

El modelo divide la operación de NeoStarling en cinco etapas secuenciales, cada una aportando un aspecto único al rendimiento general del sistema.

Etapa 1 - Inicialización del sistema: Esta es la etapa en la que los vehículos y Unidades al Lado de la Carretera (RSUs) se registran con la Autoridad de Confianza (TA). El proceso de registro involucra la generación de identificadores únicos para cada vehículo y RSU. Esto forma la estructura básica de la red, estableciendo las conexiones fundamentales entre varios nodos dentro del sistema **Benet2014**. Prepara el escenario para la comunicación e intercambio de datos, preparando la red para las etapas subsiguientes.

Etapa 2 - Generación de clave de cifrado: Esta etapa se refiere a la creación de claves de cifrado necesarias para la firma y transmisión de mensajes seguros. Utilizando técnicas criptográficas

avanzadas, el sistema NeoStarling genera claves únicas para cada vehículo y RSU. Las claves se utilizan para firmar mensajes y verificar su autenticidad, asegurando la transmisión segura de datos a través de la red.

Etapa 3 - Verificación de mensajes: Una vez que se han generado las claves de cifrado, el sistema NeoStarling pasa a la fase de verificación de mensajes. Aquí, se verifica la autenticidad e integridad de los mensajes entrantes **Lu2010**. Este proceso de verificación ayuda a detectar y mitigar posibles violaciones de datos, asegurando así la fiabilidad de los datos comunicados. Además, proporciona un mecanismo para rastrear identidades reales en caso de disputas, mejorando la transparencia y seguridad del sistema.

Etapa 4 - Seguimiento de obstáculos y almacenamiento de datos: Durante esta fase, el sistema NeoStarling facilita el almacenamiento y recuperación de datos de obstáculos dentro de un repositorio seguro **Zhang2008**. Los datos recopilados, provenientes de varios vehículos y RSUs, se utilizan para detectar peligros en tiempo real, lo cual contribuye significativamente a la seguridad vial. El repositorio mantiene un registro de todos los datos recopilados, que se pueden acceder y utilizar según sea necesario.

Etapa 5 - Aseguramiento de la calidad de los datos: Para asegurar la precisión y calidad de los datos, el sistema NeoStarling incorpora controles para prevenir la duplicación de obstáculos dentro del repositorio y para detectar datos de obstáculos defectuosos o manipulados. Este último paso es crucial para mantener la credibilidad y fiabilidad del sistema, asegurando la provisión de información precisa y de calidad a todos los usuarios.

Las Figuras 7.2 y 7.3 muestran el modelo de diseño del sistema y el modelo de objeto de análisis del sistema NeoStarling, respectivamente. Estos diagramas demuestran la progresión del sistema desde su predecesor, el sistema Starling, y las innovaciones que aporta al campo de la comunicación V2V.

En la Figura 7.2, vemos una versión mejorada de la arquitectura del sistema Starling. Las adiciones cruciales en el modelo NeoStarling incluyen un mecanismo de cifrado más robusto, integración de una estrategia de reautenticación avanzada y la inclusión de un sistema eficiente de aseguramiento de la calidad de los datos. Estas nuevas características amplifican la seguridad y eficiencia del sistema, diferenciando el modelo NeoStarling de su predecesor y el estado actual del arte Fernandez-Carames y Fraga-Lamas, 2020; Tyagi, 2023.

La Figura 7.3 presenta el Modelo de Objeto de Análisis del sistema NeoStarling, delineando su estructura de datos y las interacciones entre varios componentes. La inclusión del Algoritmo de Comunicación Vehicular Seguro (SVCA) y la adopción de HMAC-SHA256 para la verificación de integridad de datos son características diferenciadoras clave. Estas adiciones permiten al sistema NeoStarling asegurar la autenticidad de los datos mientras minimiza las amenazas de vehículos maliciosos, contribuyendo a una comunicación V2V fiable y segura Hussien et al., 2019.

Estas mejoras no solo potencian las capacidades del sistema, sino que también abordan algunos de los desafíos clave enfrentados por los sistemas contemporáneos de comunicación V2V. El sistema NeoStarling ofrece una solución avanzada a la creciente demanda de sistemas de comunicación vehicular seguros, eficientes y escalables.

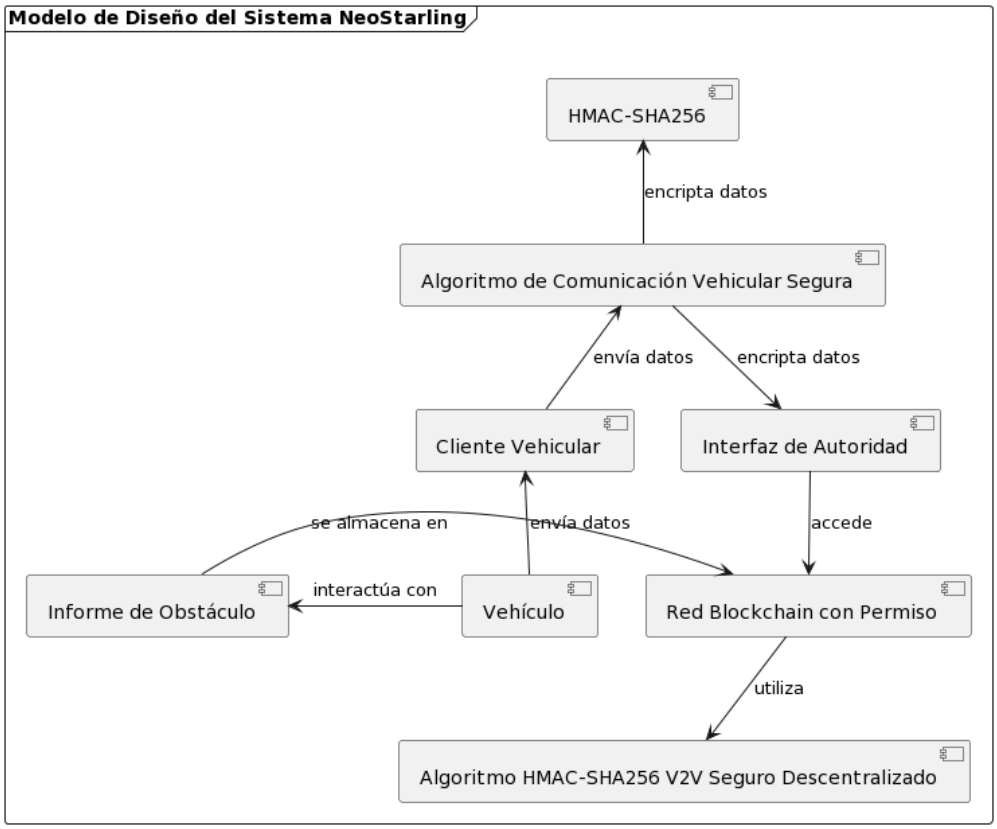

Figura 7.2: Modelo de diseño del sistema NeoStarling.

7.2.2 Algoritmo Seguro Descentralizado V2V HMAC-SHA256

Una de las innovaciones clave del sistema NeoStarling, que permite una escalabilidad mejorada y una mayor eficiencia, es la inclusión del Algoritmo de Comunicación Vehicular Seguro (SVCA) y la adopción de HMAC-SHA256 para la integridad de los datos. La combinación de estas dos tecnologías se denomina "DSV-HMAC-SHA256".

El algoritmo propuesto DSV-HMAC-SHA256 es un protocolo de comunicación criptográfica, específicamente adaptado a las demandas de las comunicaciones Vehículo-a-Vehículo (V2V). Este algoritmo simplifica el registro y autenticación de vehículos y Unidades al Lado de la Carretera (RSUs), la generación de claves temporales al entrar en el rango de RSU, la creación de firmas anónimas a corto plazo, verificación de mensajes e incluso resolución de disputas M. U. Arshad y Javaid, 2019.

Al incorporar DSV-HMAC-SHA256 en nuestro sistema NeoStarling, podemos proporcionar comunicaciones seguras, eficientes y confiables Arora y Yadav, 2018; R. M. Haris y Al-Maadeed, 2020; Xu et al., 2020 entre vehículos, mejorando las capacidades de detección y reporte de obstáculos. En última instancia, este algoritmo mejora la seguridad y funcionalidad general de nuestro sistema NeoStarling, reforzando la confianza de nuestros usuarios y partes interesadas en la integridad, fiabilidad y seguridad del sistema Alangot et al., 2022; H. Li et al., 2020; Lopez y Farooq, 2020.

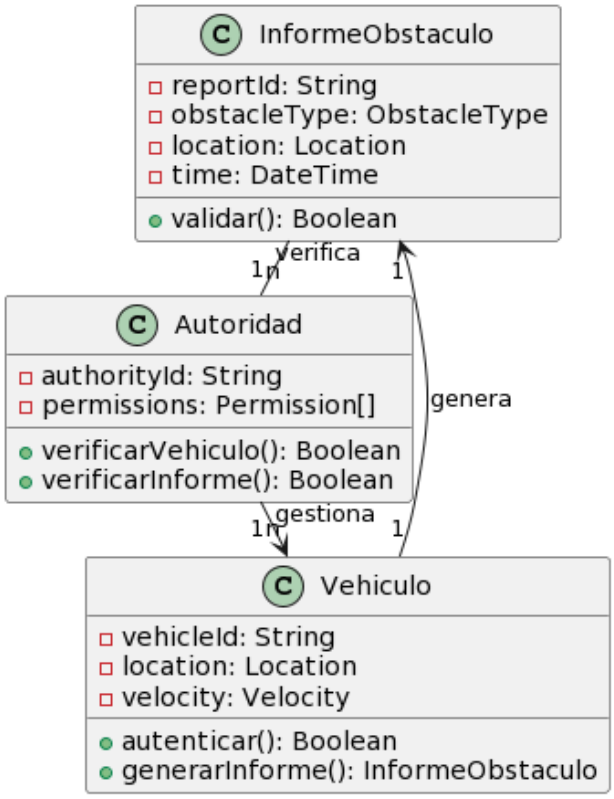

Figura 7.3: Modelo de objeto de análisis del sistema NeoStarling.

En el contexto de un ambiente de red vehicular, se deben tener en cuenta varias consideraciones clave al seleccionar un algoritmo de hash. Estas incluyen seguridad, eficiencia computacional y velocidad de transmisión de datos. La decisión de utilizar SHA256 en NeoStarling se basó en gran medida en encontrar un equilibrio entre seguridad y eficiencia computacional. En términos de seguridad, aunque SHA256 proporciona un tamaño de hash más pequeño en comparación con SHA512, todavía ofrece un nivel adecuado de seguridad para muchas aplicaciones. Aunque los ataques de fuerza bruta son teóricamente más factibles contra SHA256 que contra SHA512 debido a su menor tamaño de hash, la realidad es que los ataques de fuerza bruta contra SHA256 siguen siendo impracticables con la tecnología actual. En cuanto a la Eficiencia Computacional, el tamaño de hash extendido en SHA512 implica cálculos más intensivos, lo que podría llevar a una mayor demanda de recursos computacionales y tiempos de procesamiento extendidos. En general, SHA256 es menos intensivo computacionalmente que SHA512. Esto es particularmente importante en un ambiente de red vehicular, donde los recursos de cómputo pueden ser limitados y la eficiencia es crítica. Algoritmos de hash más eficientes permiten un procesamiento más rápido, lo cual puede ser crucial para operaciones en tiempo real. En cuanto a la Transmisión de Datos, al usar SHA256, el tamaño de los hashes (y por lo tanto, el tamaño de los datos transmitidos) es menor que con SHA512. Esto puede contribuir a una transmisión de datos más rápida y un menor uso de ancho de banda, lo que puede ser beneficioso en un ambiente de red vehicular. En conclusión, aunque SHA512 puede ofrecer una seguridad teóricamente mayor, NeoStarling utiliza SHA256 porque aún proporciona un nivel formidable de seguridad, y debido a su menor demanda de recursos

computacionales y su contribución a una transmisión de datos más eficiente.

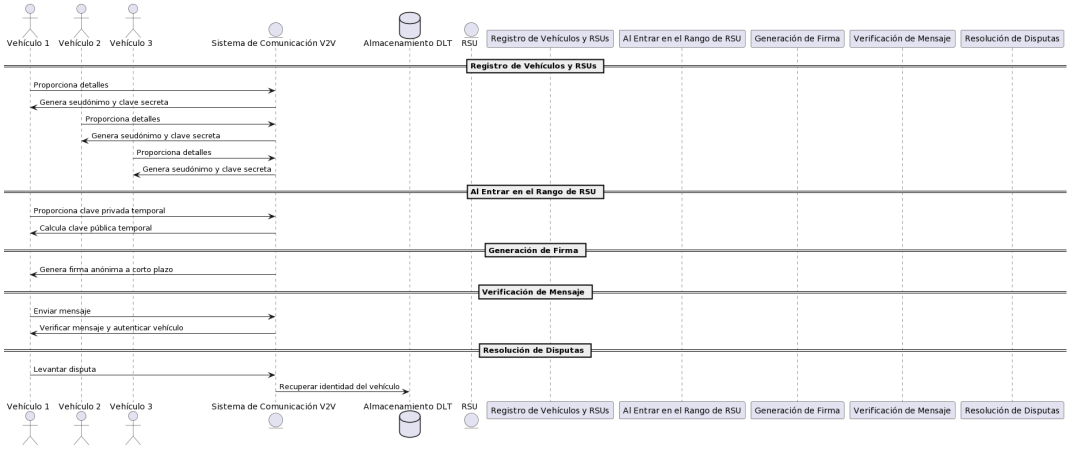

Figura 7.4: Algoritmo seguro descentralizado V2V HMAC-SHA256

La Figura 7.4 ilustra el algoritmo seguro descentralizado V2V HMAC-SHA256 (DSV-HMAC-SHA256) en un gráfico de intercambio de mensajes.

Es importante destacar que la Unidad al Lado de la Carretera (RSU) genera libros de contabilidad distintos para cada vehículo dentro de la red. Este enfoque ofrece múltiples beneficios, especialmente con respecto a mejorar la seguridad de los datos, preservar la privacidad y asegurar una gestión eficiente de los datos. Cada vehículo está asociado con un libro de contabilidad únicamente adaptado. Esta personalización fortalece el aislamiento de datos para cada vehículo y proporciona una seguridad robusta, minimizando así la exposición potencial a entidades no autorizadas. Este enfoque juega un papel crítico en mejorar la privacidad de los datos vehiculares y mitigar posibles brechas de seguridad. Desde una perspectiva de gestión de datos, tener un libro de contabilidad dedicado para cada vehículo simplifica significativamente el proceso de identificar y recuperar información específica según sea necesario. Esto significa que si se necesita datos pertenecientes a un vehículo específico para análisis, el sistema puede acceder directamente al libro de contabilidad asociado sin la necesidad de tamizar a través de datos extensos de una multitud de vehículos. Cabe señalar que, aunque cada vehículo posee su propio libro de contabilidad privado, se mantiene la sincronización y consistencia a través de todos estos libros mediante mecanismos de consenso blockchain. Esta característica garantiza la preservación de la integridad de los datos y asegura la consistencia a través de toda la red vehicular, proporcionando así una instantánea unificada y precisa del estado de la red en cualquier momento dado. La creación de libros de contabilidad privados para cada vehículo por parte de la RSU es una piedra angular de nuestra arquitectura del sistema, reforzando la seguridad, mejorando la privacidad y asegurando una gestión eficiente de los datos dentro de la red vehicular NeoStarling.

Como se puede ver, cinco procedimientos interconectados diferentes componen el protocolo global DSV-HMAC-SHA256: Registro de Vehículos y RSUs, Al Entrar al Rango de RSU, Generación de Firma, Verificación de Mensajes y Resolución de Disputas. Además, desde el punto de vista criptográfico, en nuestro sistema NeoStarling, implementamos varios métodos para la autenticación de datos y la seguridad. Las siguientes subsecciones describen todos

estos métodos y procedimientos en detalle.

Registro de Vehículos y RSUs

En este procedimiento, cada vehículo o Unidad al Lado de la Carretera (RSU) en la red se registra con un pseudónimo único y una clave secreta. Este proceso implica recopilar los detalles necesarios y generar pseudónimos únicos y claves secretas para cada entidad Mehta et al., 2020.

La Tabla 1 describe este procedimiento en pseudocódigo. Las Unidades al Lado de la Carretera Inteligentes (RSUs) generan sus propios libros de contabilidad privados, que almacenan detalles recibidos de RSUs vecinas, como el pseudónimo del vehículo, su mensaje, el estado de autenticación y la marca de tiempo. Las RSUs generan parámetros de autenticación a través del emparejamiento bilineal para curvas elípticas. Esto implica que el vehículo selecciona un número aleatorio como una clave privada a corto plazo y calcula una clave pública correspondiente a corto plazo en la curva elíptica. La RSU verifica si el vehículo está autenticado o no. Si el vehículo no está autenticado, la RSU solicita parámetros de autenticación (ver Sección 3.3); de lo contrario, pasa el estado de .ªutenticación exitosa".

Nuestro sistema de red vehicular propuesto, NeoStarling, se basa fundamentalmente en la generación de claves públicas y privadas por parte de la Unidad al Lado de la Carretera (RSU). La generación de claves de la RSU sirve como piedra angular para asegurar la integridad de los datos y para fortalecer la estructura de seguridad del sistema. Hemos elegido conscientemente una clave de 256 bits, ya que aunque las claves más largas podrían proporcionar mayor seguridad, también intensificarían la demanda computacional y de transmisión. Dada la naturaleza dinámica y crítica de las redes vehiculares, la eficiencia es primordial. Tras un análisis exhaustivo, hemos determinado que las claves de 256 bits ofrecen seguridad adecuada sin comprometer esta eficiencia esencial. Respecto al papel desempeñado por la RSU, es responsable de generar registros privados para cada vehículo, enfocándose en su identidad única y comportamiento de conducción. A cada vehículo dentro de la red NeoStarling se le asigna un identificador único, que facilita el seguimiento y mantenimiento de registros individuales, mejorando significativamente la privacidad y seguridad de los datos. Además, aspectos destacados del comportamiento de conducción de cada vehículo, como la velocidad, dirección y otras características pertinentes, se registran meticulosamente en el libro de contabilidad privado, permitiendo un seguimiento exhaustivo y preciso. Sin embargo, aunque estos criterios se han establecido con las necesidades específicas del sistema NeoStarling en mente, han sido diseñados con la flexibilidad necesaria para adaptarse a objetivos y requisitos cambiantes, asegurando que el sistema siga siendo relevante en una amplia variedad de situaciones y condiciones.

La Figura 7.5 y el Procedimiento 1 muestran este procedimiento como un diagrama de flujo y algoritmo, respectivamente.

Ingreso de vehículos en una RSU

Cuando un vehículo entra en el rango de una RSU, genera una clave privada temporal y calcula la clave pública correspondiente. Estas claves aseguran la comunicación con la RSU.

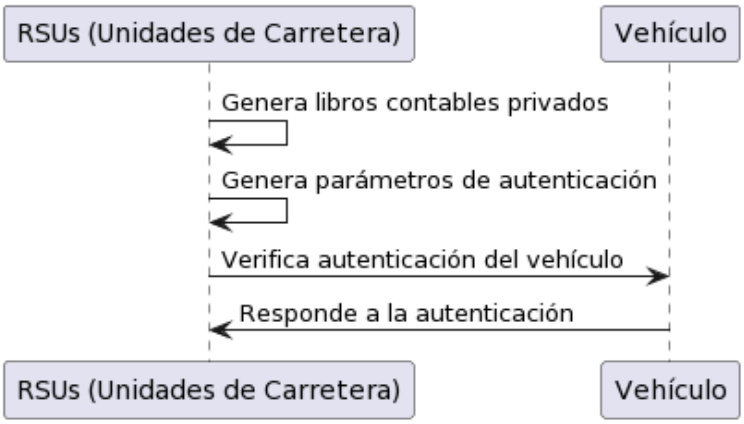

Figura 7.5: Generación de claves

Algorithm 1 Registro de Vehículos y RSUs

Input: Detalles del Vehículo y RSU
Output: Pseudónimos únicos y claves secretas para cada usuario
1: **for each** Vehículo/RSU **do**
2: Recopilar los detalles necesarios
3: Generar pseudónimos únicos y claves secretas
4: **end for**

Este proceso de generación de claves mejora la seguridad del sistema al asegurar que la misma clave no se use en sesiones sucesivas, minimizando así el riesgo de compromiso de la clave Gad et al., 2021; Shu et al., 2020; J. Zhang et al., 2019.

El Procedimiento 2 describe este procedimiento en pseudocódigo.

Algorithm 2 Al Ingresar al Rango de una RSU

Input: Detalles del Vehículo
Output: Clave privada y pública temporal
1: **for each** Vehículo **do**
2: Generar una clave privada temporal
3: Calcular una clave pública temporal a partir de la clave privada
4: **end for**

Tanto en el Procedimiento 1 como en el Procedimiento 2, integramos algoritmos de Criptografía de Curva Elíptica (ECC) para engendrar claves únicas e impredecibles en cada iteración. La fortaleza de estos algoritmos reside en su dependencia de problemas matemáticos complejos, los cuales, hasta el momento presente, no tienen soluciones eficientes conocidas. Esta complejidad infunde nuestro proceso de generación de claves con un alto grado de seguridad. Nuestro sistema NeoStarling aprovecha el poder de la criptografía asimétrica, que emplea un par de claves pública-privada. Pero NeoStarling también adoptó el uso de claves efímeras, o temporales. Caracterizadas por su vida útil limitada y renovación frecuente, estas claves limitan el daño potencial de que cualquier clave única sea comprometida, reflejando protocolos como Kerberos,

conocido por utilizar tickets limitados en tiempo para autenticación. La transmisión de claves entre vehículos y Unidades de Servicio al Lado de la Carretera (RSUs) se realiza a través de canales de comunicación cifrados, fortificados por el estándar TLS (Seguridad de la Capa de Transporte). Esta medida proporciona protección contra la intercepción de claves y ataques tipo "hombre en el medio". Para proteger las claves almacenadas, empleamos técnicas de aislamiento seguro. Los Módulos de Seguridad de Hardware (HSMs) ofrecen protección robusta contra ataques a nivel de sistema y hardware. Finalmente, nuestras medidas rigurosas de control de acceso abarcan autenticación multifactor y autorizaciones basadas en roles, alineándose con principios de seguridad de la información de mejores prácticas, como el principio de mínimo privilegio. Esto asegura que el acceso a las claves esté limitado solo a entidades autorizadas. Para mantener la rendición de cuentas y trazabilidad, llevamos a cabo auditorías rutinarias de todas las interacciones dentro del sistema de claves.

Generación de Firma

Para preservar la integridad del mensaje, en este procedimiento, cada vehículo genera una firma anónima a corto plazo utilizando la clave privada temporal generada en el paso anterior. Esta firma autentica los mensajes enviados a la RSU, reduciendo la probabilidad de acceso y manipulación de datos no autorizados Fan y Wu, 2019; Tan y Chung, 2019.

El Procedimiento 3 describe este procedimiento en pseudocódigo, mientras que la Figura 7.6 representa el diagrama de flujo asociado. El vehículo calcula el hash del mensaje usando el algoritmo HMAC-SHA256 y lo mapea a un punto en una curva elíptica. La firma del mensaje se calcula como se muestra en las secciones anteriores

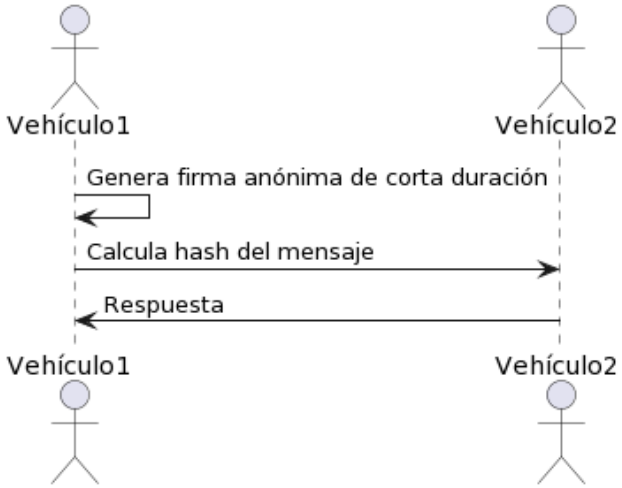

Figura 7.6: Generación de Firma

Verificación de Mensaje

Al recibir un mensaje de un vehículo, una RSU intenta autenticar el vehículo y verificar la integridad del mensaje. Si la verificación es exitosa, la RSU envía un recibo de vuelta al vehículo para reconocer la transmisión exitosa Nasland et al., 2016.

Algorithm 3 Generación de Firma

Input: Detalles del Vehículo, Clave privada temporal
Output: Firma anónima a corto plazo
1: **for each** Vehículo **do**
2: Generar una firma anónima a corto plazo usando la clave temporal
3: **end for**

El Procedimiento 4 describe este procedimiento en pseudocódigo.

En resumen, el vehículo envía el mensaje, la firma y la clave pública a la RSU en forma de un mensaje concatenado (Ecuación 7.1). En este contexto, M denota el mensaje enviado por el vehículo, S es la firma creada por la clave privada del vehículo, y P representa la clave pública del vehículo. El vehículo envía estas tres piezas de información—M,S y P—juntas en una forma concatenada a la RSU. Esto se puede representar de la siguiente manera:

$$(M||S||P) \tag{7.1}$$

Aquí, el símbolo "||representa la concatenación, combinando el mensaje, la firma y la clave pública en una sola cadena para su transmisión.

El mensaje se prioriza según el tipo de mensaje M. Diferentes tipos de M podrían incluir mensajes de emergencia, mensajes de seguridad, mensajes de información de tráfico, mensajes de control y mensajes de servicio. El sistema da la mayor prioridad a los mensajes de emergencia, seguidos por los mensajes de seguridad y mensajes de información de tráfico. Los mensajes de control reciben una prioridad más baja, mientras que los mensajes de servicio suelen recibir la prioridad más baja.

La RSU autentica al vehículo si una proposición lógica ligera es verdadera (Ecuación 7.2). De lo contrario, se considera un vehículo malicioso, y la RSU informa a la TA. La integridad del mensaje también se verifica utilizando el algoritmo HMAC-SHA256 (ver Sección 3.2.8). La Figura 7.7 muestra el procedimiento de verificación de mensajes en un diagrama de flujo.

$$e(G, S) = e(P, H(M)) \tag{7.2}$$

En la ecuación 7.2,G es un punto generador en una curva elíptica, S es la firma enviada por el vehículo, y P es la clave pública del vehículo. El hash del mensaje M se denota por H(M). La función e() denota una función de emparejamiento en la curva elíptica. La igualdad e(G,S)=e(P,H(M)) verifica que la firma S fue generada por el propietario de la clave pública P, confirmando la autenticidad del vehículo y la integridad del mensaje.

Resolución de Disputas

En caso de una disputa, el procedimiento implica revelar la verdadera identidad del vehículo o RSU involucrado. Esto se logra consultando la verdadera identidad de la entidad en la base de datos de la Autoridad de Confianza (TA) Sanka et al., 2021.

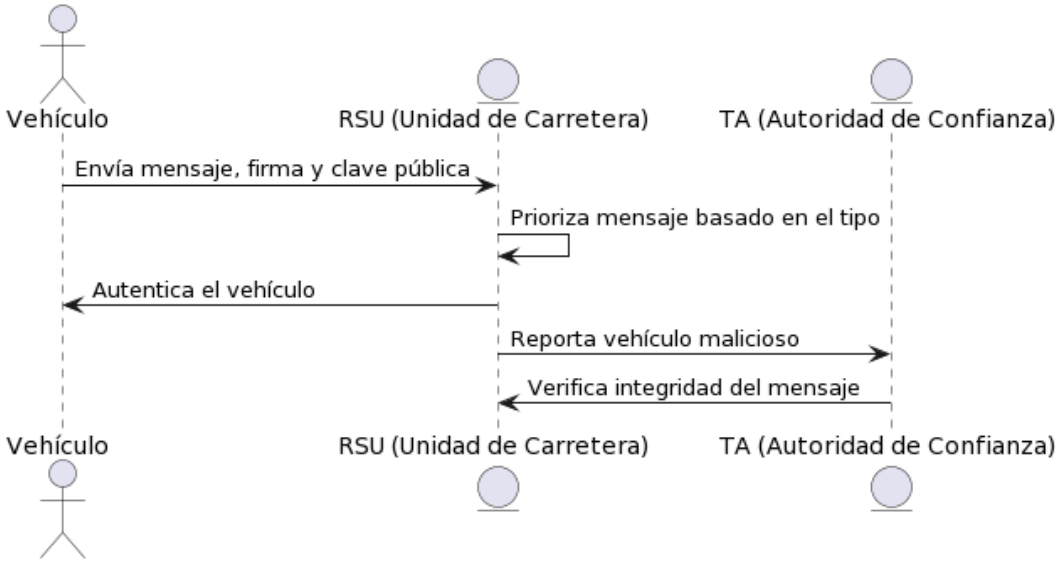

Figura 7.7: Verificación de mensaje

Algorithm 4 Verificación de Mensaje

Input: Mensaje del vehículo, Detalles de RSU
Output: Recibo de transmisión exitosa

```
for each RSU, Al recibir un mensaje del vehículo do
    Autenticar al vehículo
    Verificar el mensaje
    if la verificación es exitosa then
        Enviar un recibo de vuelta al vehículo
    end if
end for
```

La Tabla 5 describe este procedimiento en pseudocódigo. Las RSUs almacenan mensajes útiles en la blockchain de Ethereum utilizando el algoritmo de consenso Proof-of-Authority (PoA) en forma de transacciones. En caso de disputa, la TA rastrea la verdadera identidad consultando en su base de datos local y en la base de datos de la blockchain. Después de rastrear la identidad real, la TA revoca la privacidad del vehículo o RSU malicioso para prevenir más daños. La Figura 7.8 muestra el procedimiento de resolución de disputas en un diagrama de flujo.

Los procedimientos anteriores tienen como objetivo aumentar la fiabilidad y seguridad del sistema mientras abordan desafíos específicos asociados con sistemas descentralizados, como la escalabilidad y privacidad. El algoritmo DSV-HMAC-SHA256 proporciona una comunicación segura y autenticada entre vehículos y RSUs mientras mantiene privada la identidad del vehículo. Las claves temporales y firmas anónimas protegen las identidades de los vehículos, mientras que la opción de revelar la verdadera identidad en disputas asegura responsabilidad.

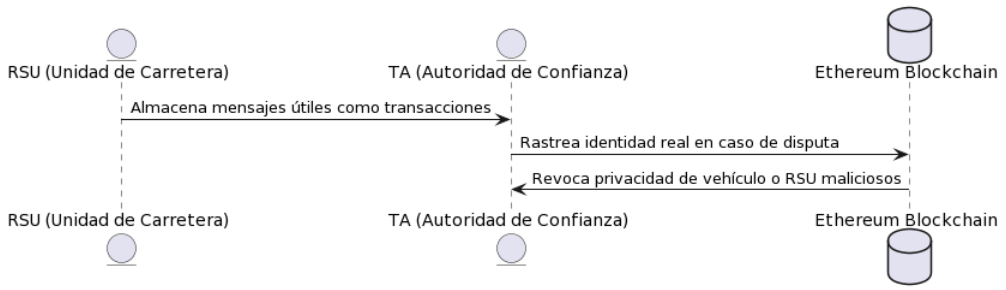

Figura 7.8: Resolución de disputas

Algorithm 5 Resolución de Disputas

Input: Detalles de la Disputa
Output: Identidad del vehículo o RSU concernido
1: **for each** Disputa **do**
2: Revelar la verdadera identidad del vehículo o RSU concernido desde la base de datos de la TA
3: **end for**

Emparejamiento Bilineal

El emparejamiento bilineal se emplea en nuestro sistema para autenticar y correlacionar los datos de obstáculos detectados, reduciendo la redundancia de datos y evitando entradas duplicadas. Además, se utiliza un criptosistema de curva elíptica para mantener la privacidad y seguridad de los datos a través de un par de claves pública y privada. Para autenticar y correlacionar los datos de obstáculos detectados, así reduciendo la redundancia y las entradas duplicadas, empleamos el emparejamiento bilineal. Este método se complementa con un criptosistema de curva elíptica, manteniendo la privacidad y seguridad de los datos mediante un par de claves pública y privada. La función de emparejamiento opera entre elementos de dos grupos cíclicos y produce un valor en un tercer grupo. Nuestro sistema combina esta técnica con HMAC-SHA256 e IPFS (integrados en el sistema estándar Starling) para asegurar la detección y reporte de obstáculos.

Criptografía de Curva Elíptica (ECC)

ECC se aprovecha para generar claves públicas en nuestro sistema NeoStarling. ECC, basada en la teoría de curvas elípticas, produce claves criptográficas que son eficientes, rápidas y compactas. El criptosistema funciona bajo el principio de "fácil de calcular, difícil de revertirz se utiliza para generar una clave privada (x) y un punto en la curva elíptica (G) cuya multiplicación resulta en la clave pública, como se muestra en la Ecuación 7.3:

$$P = x \cdot G \tag{7.3}$$

El par de claves producido por ECC forma una parte crítica del proceso de autenticación y cifrado de datos, asegurando la compartición y almacenamiento seguro de datos de obstáculos.

Algoritmo HMAC-SHA256

El algoritmo HMAC-SHA256 se utiliza para autenticar mensajes de información sobre obstáculos, asegurando la fiabilidad de los datos. HMAC-SHA256 es un tipo de algoritmo de hash con clave creado a partir de la función de hash SHA256. Y, en NeoStarling, se utiliza para la autenticación de vehículos y la autenticación de mensajes. En el método HMAC, el mensaje se combina con la clave secreta y se procesa con la función de hash SHA256, el resultado se combina nuevamente con la clave secreta y luego se aplica nuevamente la función de hash SHA256 para obtener un hash de salida de 256 bits de longitud. En NeoStarling, para generar un HMAC (Código de Autenticación de Mensaje basado en Hash), usamos el siguiente esquema matemático (Ecuación 7.4):

$$\text{HMAC}(k, m) = H\left((k \oplus \text{opad}) || H\left((k \oplus \text{ipad}) || m\right)\right) \tag{7.4}$$

Donde:

- H es una función de hash criptográfica, en este caso, SHA256.
- k es la clave secreta utilizada para la autenticación del mensaje.
- m es el mensaje.
- opad es el relleno exterior"(5c5c5c...5c en hexadecimal).
- ipad es el relleno interior"(363636...36 en hexadecimal).
- $\oplus$ es el operador XOR.
- || representa la concatenación.

La Figura 7.9 muestra el ciclo de vida de HMAC-SHA256. En esta figura, el actor "Vehículo-epresenta el vehículo emisor en el sistema. Relleno Interior (ipad)ƶ Relleno Exterior (opad)-epresentan las constantes de relleno interior y exterior. La "Función de Hash SHA256representa la función de hash criptográfica utilizada. Y el "Validador de Blockchainrepresenta el validador en el sistema de blockchain, que valida el HMAC.

Las interacciones entre los componentes del sistema NeoStarling refuerzan la seguridad y autenticación de los datos. El "Vehículo"genera un HMAC usando la clave secreta y el mensaje, empleando el algoritmo HMAC-SHA256. Este HMAC es verificado por el "Validador de Blockchain", asegurando su autenticidad antes de permitir el acceso a los datos a cualquier otra entidad. Por lo tanto, este proceso garantiza la integridad y autenticación de los mensajes dentro del sistema de comunicación vehicular.

7.2.3 Optimización de un protocolo de autenticación usando Blockchain

En una Red Ad-hoc Vehicular (VANET), la comunicación vehicular juega un papel crucial en la mitigación de accidentes de tráfico y congestiones. Sin embargo, la importancia de mantener la integridad y autenticidad de los mensajes se intensifica, especialmente para propósitos

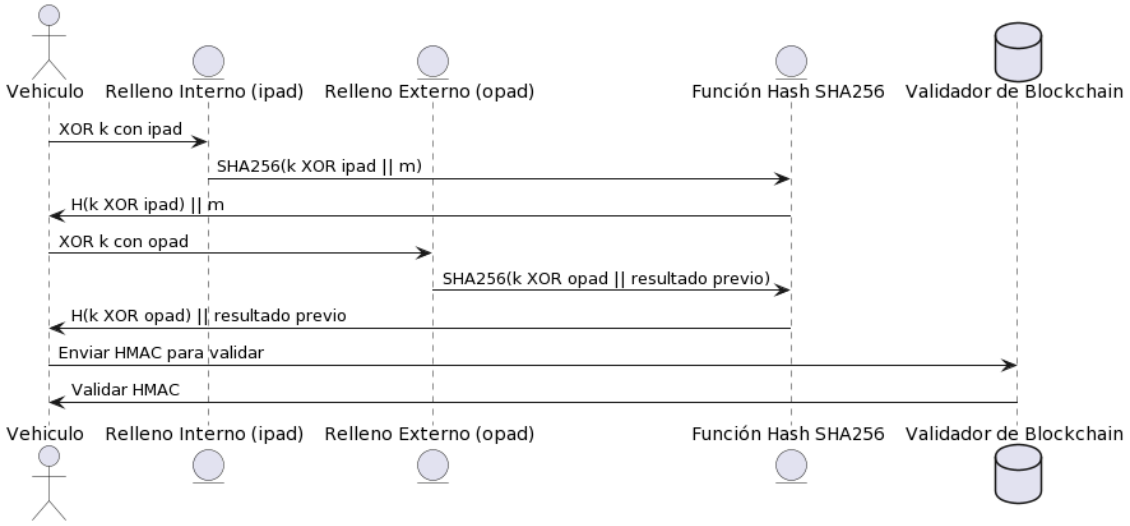

Figura 7.9: Ciclo de vida de HMAC-SHA256

de seguridad y privacidad. Notablemente, en la comunicación vehículo a vehículo (V2V), mientras que la confidencialidad del mensaje puede no ser una prioridad ya que los vehículos solo transmiten mensajes después de la autenticación por parte de las Unidades al Lado de la Carretera (RSUs), se vuelve esencial habilitar una autenticación de vehículos rápida y eficiente. Esto reduce el tiempo de inactividad cuando los vehículos necesitan comunicarse entre sí y aumenta la .

Muchos sistemas propuestos se han centrado en disminuir el tiempo de autenticación por RSU, preservando simultáneamente la seguridad y privacidad del vehículo. Es importante notar que los vehículos deberían autenticarse cada vez para prevenir la penetración de vehículos maliciosos en el sistema. Una autenticación prolongada de vehículos puede crear problemas en el sistema. Por lo tanto, nuestro sistema propuesto reduce algo la frecuencia de autenticaciones, reduciendo la demora de autenticación y facilitando la comunicación con otros vehículos.

Para adquirir el historial de mensajes del vehículo, se considera la tecnología de prueba de trabajo de blockchain. Sin embargo, esto exige un alto costo computacional para cada RSU, ya que deben competir para añadir bloques a la blockchain. Como tal, nuestro sistema usa la tecnología de prueba de autoridad de blockchain para reducir los costos computacionales. Además, para optimizar el almacenamiento, solo los mensajes cruciales del vehículo se almacenan en la blockchain. Esto incluye mensajes de emergencia de ambulancias, camiones de bomberos y otros vehículos que transmiten información sobre accidentes de tráfico y congestiones. Luego, los vehículos son autenticados y priorizados en las RSUs basados en el tipo de mensaje.

Sin embargo, una red densa puede presentar desafíos. A medida que el número de vehículos aumenta, las RSUs experimentan una carga más alta, lo que ralentiza el sistema. Nuestro esquema alivia esto reduciendo el número de autenticaciones, haciendo el sistema relativamente más rápido.

La autenticación DSV-HMAC-SHA256 puede descomponerse en los métodos de registro del vehículo, autenticación del usuario y emisión de credenciales (ver Figura 7.10).

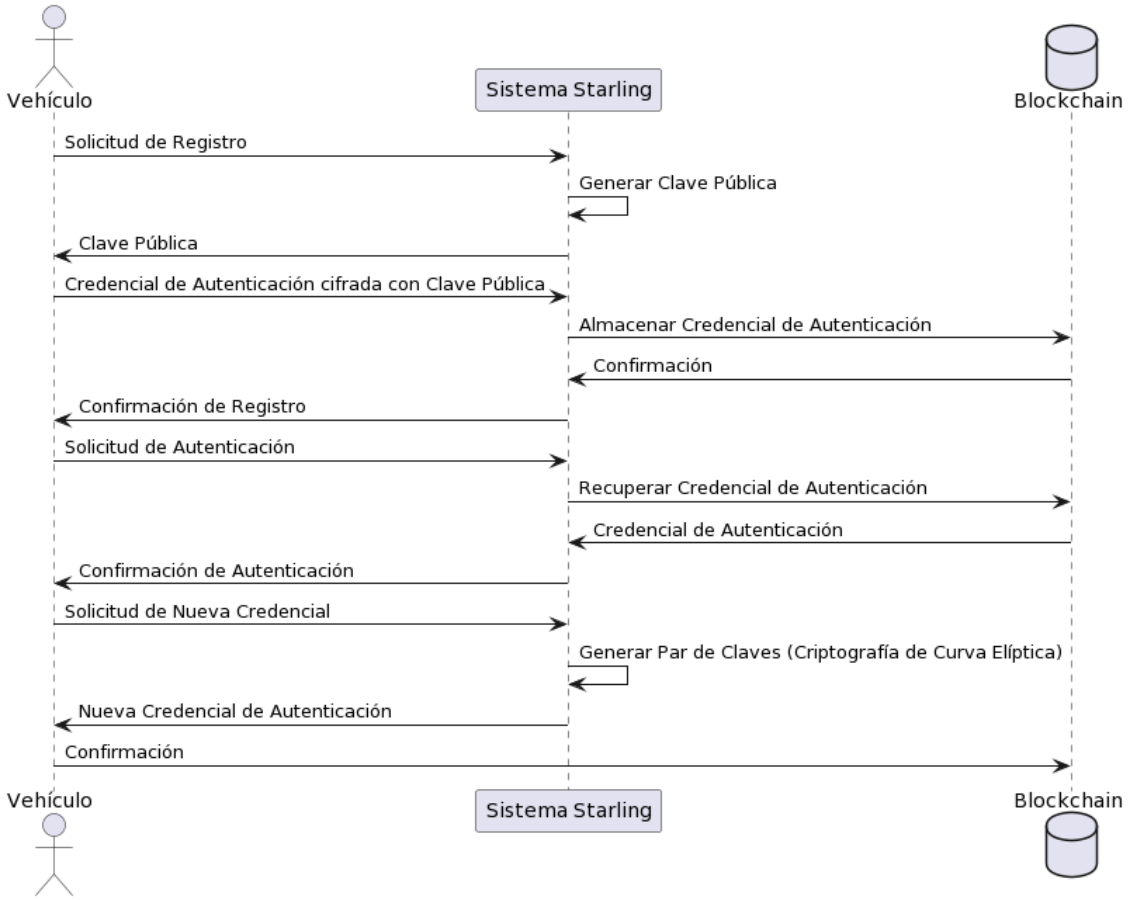

Figura 7.10: El sistema de autenticación en el Sistema Starling

El proceso de autenticación comienza cuando un vehículo se registra por primera vez en el sistema NeoStarling (ver Figura 7.10). En la etapa inicial del proceso de registro, el Sistema Starling genera una clave pública que se envía al vehículo. A continuación, el vehículo usa esta clave pública para cifrar su credencial de autenticación, que luego se envía al sistema durante el proceso de .ºfrecimiento de credencial".

Este procedimiento proporciona al vehículo una forma segura de comunicar sus credenciales al Sistema Starling. La credencial de autenticación cifrada se almacena en la blockchain para futuras referencias, agregando así un nivel de seguridad al proceso de registro del vehículo. Una vez que se confirma el registro, el vehículo está oficialmente registrado y puede comenzar el proceso de autenticación del usuario.

Consulte la Figura 7.11 para una ilustración detallada del proceso de .ºfrecimiento de credencial". Esta figura muestra la secuencia de acciones que ocurren cuando un propietario de vehículo proporciona una credencial de autenticación cifrada con la clave pública de NeoStarling durante la solicitud de registro. Este enfoque asegura la seguridad e integridad del proceso de registro, haciéndolo más resistente contra posibles amenazas de seguridad.

Antes de registrar un vehículo, el proceso de .ºfrecimiento de credencial"(ver Figura 7.11) garantizaría que el propietario del vehículo proporcione una credencial de autenticación cifrada

con la clave pública de NeoStarling, que se enviaría junto con la solicitud de registro. Este proceso agrega una capa adicional de seguridad al registro del vehículo.

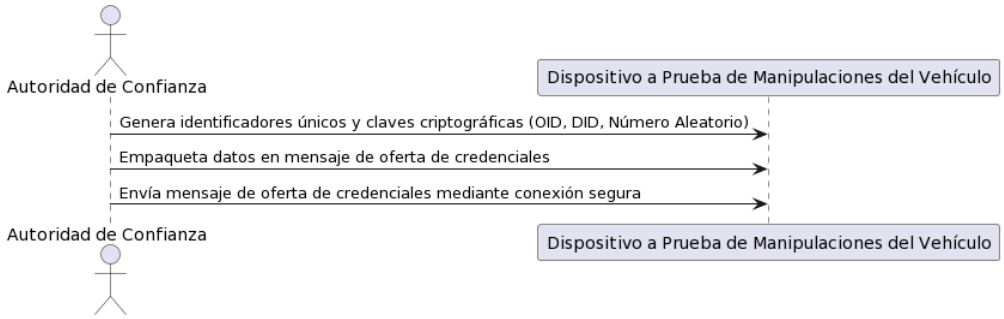

Figura 7.11: Ofrecimiento de la Credencial

Para la autenticación del usuario, se puede emplear el proceso de "solicitud de credencial", donde los usuarios proporcionan una credencial de autenticación. NeoStarling luego descifraría y validaría la credencial usando su clave privada y el algoritmo HMAC-SHA256. Solo los usuarios autenticados con credenciales válidas serían autorizados para acceder a los servicios del sistema, mejorando las medidas de seguridad. Al recibir el mensaje de ofrecimiento de credencial, el TPD y el agente a bordo procesan la información. El usuario es informado a través de una interfaz en el vehículo. Si el usuario acepta la oferta, el agente formula entonces una solicitud HTTP que contiene un mensaje de "solicitud de credencial"(ver Figura 7.12). Esta solicitud se envía de vuelta a la Autoridad de Confianza, utilizando nuevamente el campo de servicio en el mensaje para determinar la dirección IP correcta para la comunicación.

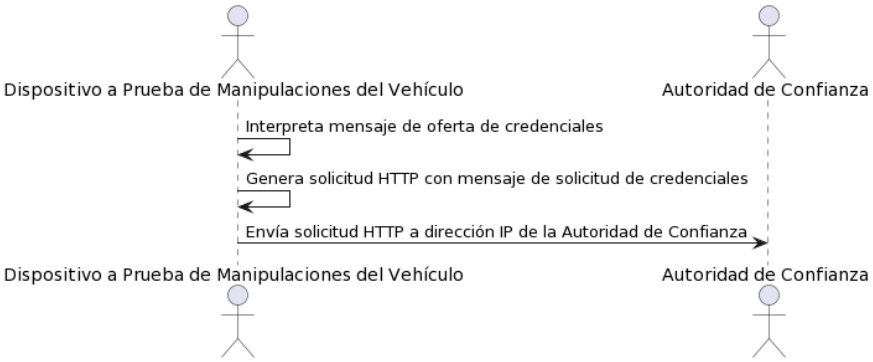

Figura 7.12: Solicitud de Credencial

En el proceso de .emisión de credencial", las autoridades pueden emitir nuevas credenciales de autenticación a los usuarios. Este proceso implica generar un par de claves usando criptografía de curva elíptica, con la clave privada asignada a la credencial emitida. La Autoridad de Confianza recibe la solicitud HTTP (ver Figura 7.13), analiza detenidamente el mensaje de solicitud de credencial y confirma su autenticidad usando la criptografía de curva elíptica y los algoritmos HMAC-SHA256, como se describió anteriormente. Una vez validada, la Autoridad de Confianza emite la credencial final de acuerdo con el esquema predefinido. Esta credencial se empaqueta en un mensaje de emisión de credencial y se devuelve como respuesta a la solicitud

HTTP del vehículo. La credencial, ahora almacenada en el TPD del vehículo, se utilizará para futuras autenticaciones a medida que el vehículo interactúa con el almacenamiento de datos descentralizado y la red basada en blockchain.

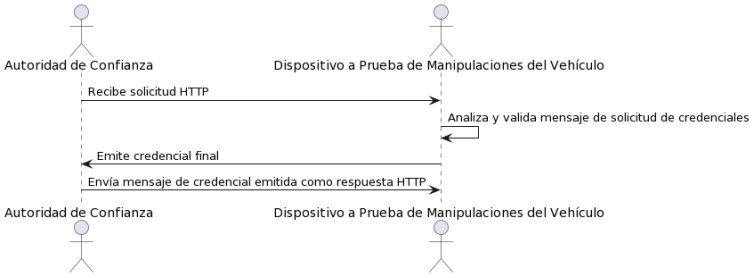

Figura 7.13: Emisión de Credenciales

Las siguientes subsecciones describen todos los métodos que componen el protocolo de autenticación basado en blockchain propuesto con detalles.

Proceso de Registro de Vehículos

El proceso de registro de vehículos implica registrar un vehículo en el sistema con medidas de seguridad mejoradas. La Figura 7.14 describe todos los submétodos incluidos en la fase de registro.

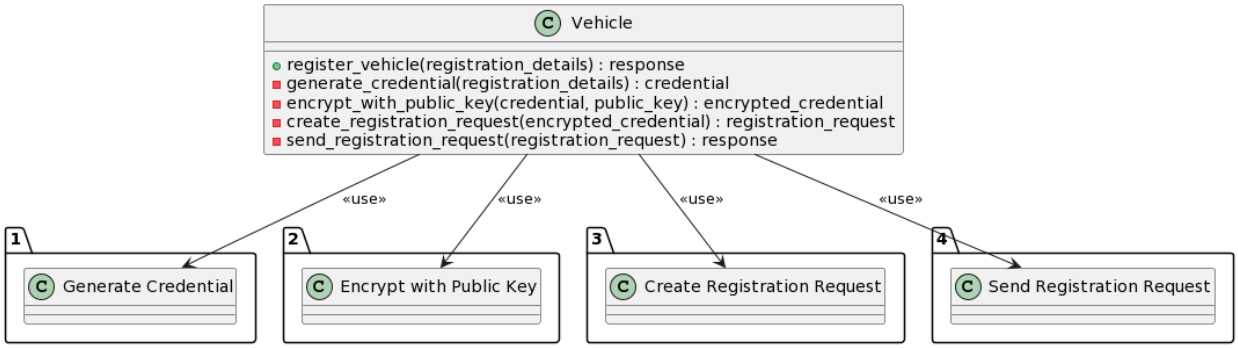

Figura 7.14: Registro de Vehículo

El método `register_vehicle` se utiliza para registrar un vehículo en el sistema NeoStarling. El método toma los detalles de registro del vehículo como entrada y genera una credencial para el vehículo. La credencial es un identificador único que se utiliza para identificar al vehículo en el sistema NeoStarling. La credencial se cifra utilizando la clave pública del sistema NeoStarling. Esto asegura que la credencial solo pueda ser descifrada por el sistema NeoStarling.

Más específicamente, como se muestra en la Figura 7.15, los usuarios van a la Autoridad de Confianza (TA) y proporcionan información personal, como número de teléfono, número de licencia de conducir, número de vehículo, etc. Esta información se almacena en la base de datos maestra de la TA. Utilizando esta información, la TA genera claves únicas requeridas para cada usuario del vehículo a través del proceso de generación de claves, incluida la generación

de la identidad de usuario original (OID), la identidad de usuario pseudónima (DID) y un número aleatorio almacenado en la base de datos local. La asignación de identidades originales a identidades pseudónimas se realiza únicamente en la TA. A continuación, la clave de autenticación, que consiste en una identidad pseudónima y un número aleatorio, se almacena en el dispositivo a prueba de manipulaciones (TPD) del vehículo. La identidad pseudoanónima protege la privacidad del vehículo. Esta información se empaqueta luego en un mensaje de oferta de credencial y se envía al Dispositivo a Prueba de Manipulaciones (TPD) del vehículo a través de una conexión segura. La conexión se establece en función del campo de servicio en el mensaje, que especifica la dirección IP para la comunicación directa con el TPD.

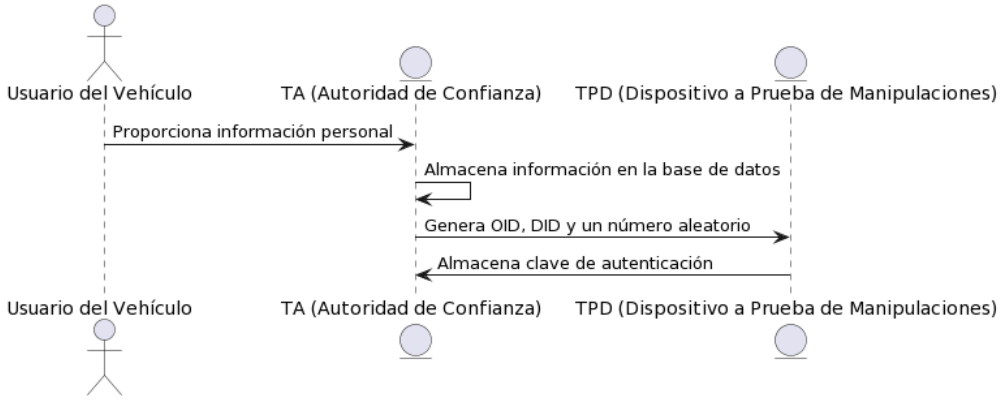

Figura 7.15: Proceso de Registro de Vehículos

Luego se crea una solicitud de registro con la credencial cifrada (Figura 7.15). La solicitud de registro se envía al sistema NeoStarling. El sistema NeoStarling valida la solicitud de registro y devuelve una respuesta. La respuesta del sistema se devuelve como salida.

En el proceso de registro de vehículos, el algoritmo DSV-HMAC-SHA256 se integra en el paso de generar la credencial cifrada. Después de generar la credencial utilizando la función `generate_credential`, se aplicaría el algoritmo DSV-HMAC-SHA256 para asegurar la integridad de la credencial antes de cifrarla con la clave pública de NeoStarling.

Proceso de Autenticación de Usuarios

El proceso de autenticación de usuarios garantiza que solo los usuarios autenticados puedan acceder a los servicios del sistema. La Figura 7.16 describe todos los submétodos incluidos en el proceso de autenticación.

El método authenticate se utiliza para autenticar a un usuario con el sistema NeoStarling. El método toma los detalles del usuario como entrada y solicita una credencial de usuario. La credencial es un identificador único que se utiliza para identificar al usuario en el sistema NeoStarling. La credencial se cifra utilizando la clave privada de NeoStarling. Esto asegura que la credencial solo pueda ser descifrada por NeoStarling. La credencial se descifra luego utilizando la clave privada de NeoStarling. La validez de las credenciales descifradas se verifica utilizando el algoritmo HMAC-SHA256. Si la credencial es válida, se concede acceso a los

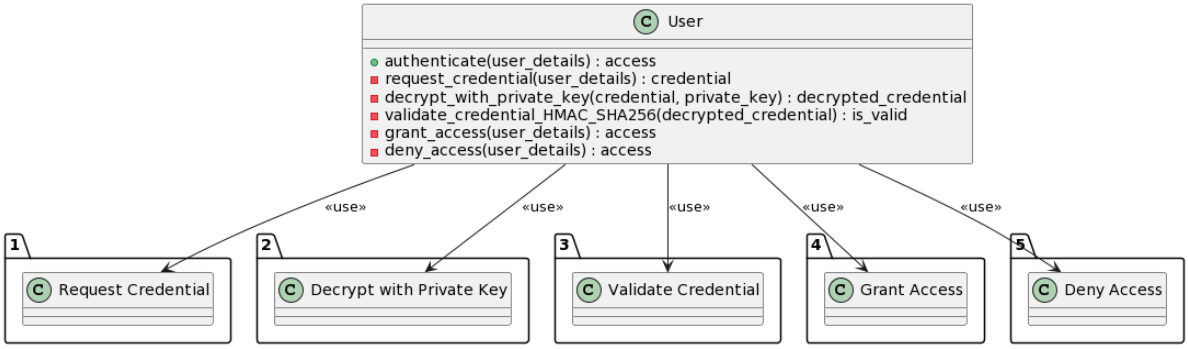

Figura 7.16: Proceso de Autenticación de Usuarios

servicios del sistema. Si la credencial es inválida, se niega el acceso. El estado de acceso se devuelve como salida.

En el proceso de autenticación de usuarios, el algoritmo DSV-HMAC-SHA256 tiene el mismo papel que en el proceso de registro de vehículos. Después de descifrar la credencial utilizando la clave privada de NeoStarling en la función `decrypt_with_private_key`, se utiliza el algoritmo DSV-HMAC-SHA256 para verificar la integridad de la credencial. Este paso se realiza utilizando la función v`validate_credential_HMAC_SHA256.`

Proceso de Emisión de Credenciales

El proceso de emisión de credenciales permite a las autoridades emitir nuevas credenciales de autenticación a los usuarios del sistema. La Figura 7.17 describe todos los submétodos incluidos en el proceso de emisión de credenciales.

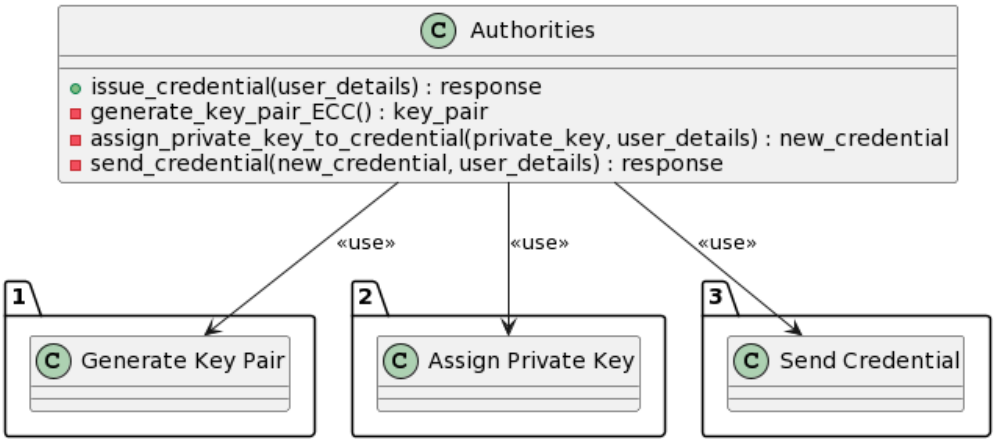

Figura 7.17: Proceso de Emisión de Credenciales

El método `issue_credential` se utiliza para emitir una credencial a un usuario.

El método toma los detalles del usuario como entrada y genera un par de claves utilizando ECC.

La clave privada del par de claves se asigna a la nueva credencial. La nueva credencial se cifra

luego utilizando la clave pública del usuario. Esto asegura que la credencial solo pueda ser descifrada por el usuario.

La nueva credencial se envía luego al usuario. El usuario puede entonces usar la credencial para acceder a los servicios del sistema. La respuesta del usuario se devuelve como salida.

Después de una autenticación exitosa, nuestra solución aprovecha OrbitDB y Ethereum para la implementación de almacenamiento de datos descentralizado y para establecer una red blockchain, respectivamente.

OrbitDB, una base de datos distribuida construida sobre IPFS, atiende nuestras necesidades de base de datos. Su característica distintiva es la estructura de datos replicada sin conflictos (CRDT) que asegura la consistencia de los nodos en nuestro entorno distribuido.

La red blockchain se basa en Ethereum, una blockchain versátil y sin permisos capaz de ejecutar contratos inteligentes. Ethereum redefine la estructura convencional de bloque, introduciendo elementos únicos como Tíos, Nuevos Árboles de Hash y el concepto de Gas (ver Figura 7.18).

Para acceder a la red de prueba de Ethereum, NeoStarling opta por el cliente Geth, otorgando acceso al cliente a través de la API JSON RPC universalmente aceptada.

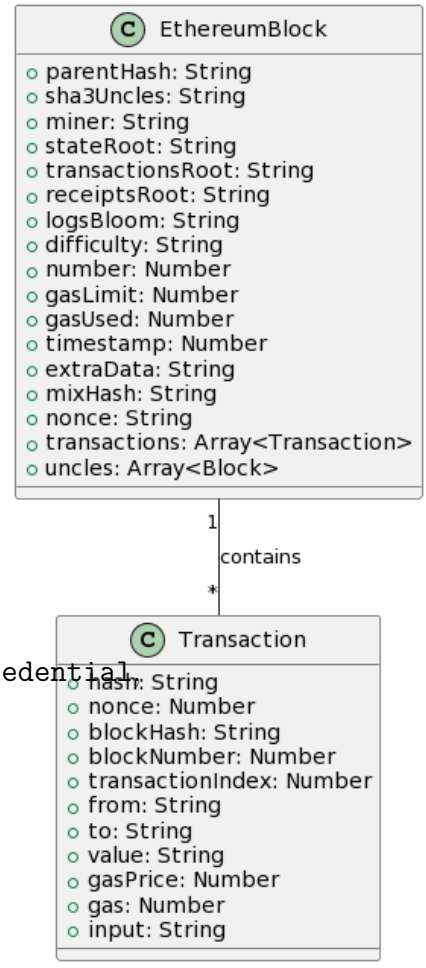

Figura 7.18: Estructura de Bloque de Ethereum en NeoStarling

Integración con el sistema estándar Starling

Se crea un contrato inteligente en la red Ethereum que maneja los procesos `offer_credential`, `request_credential` y `issue_credential`. Este contrato generará y almacenará las credenciales de los usuarios, así como verificará su validez. La clase `Client` en los sistemas estándar de Starling se modifica para incluir métodos que interactúan con el contrato inteligente de Ethereum. Estos métodos incluirían`offerCredential`,`requestCredential` y`issueCredential`, que realizarán las transacciones necesarias en la red Ethereum para llevar a cabo los procesos de autenticación.

Las clases `VehicleClient` y `AuthorityClient` se modifican para incluir una implementación de la autenticación basada en el emparejamiento bilineal en el criptosistema de curva elíptica y el algoritmo HMAC-SHA256. Esto incluye generar claves privadas y públicas para cada usuario, así como realizar firmas

digitales y verificaciones. Se agrega un nuevo método en la clase `MatchingService` que verifica las credenciales de los usuarios antes de permitirles interactuar con el sistema. Este método se comunicará con el contrato inteligente de Ethereum para verificar la validez de las credenciales de un usuario y permitir o denegar el acceso al sistema.

La clase `VerificationService` se modifica para integrar la verificación de credenciales en el proceso de verificación de obstáculos. De esta manera, solo los usuarios autenticados podrán informar y verificar obstáculos en el sistema Starling/NeoStarling. La Figura 7.19 muestra el diagrama de interacción para la arquitectura del sistema propuesto y nuevo.

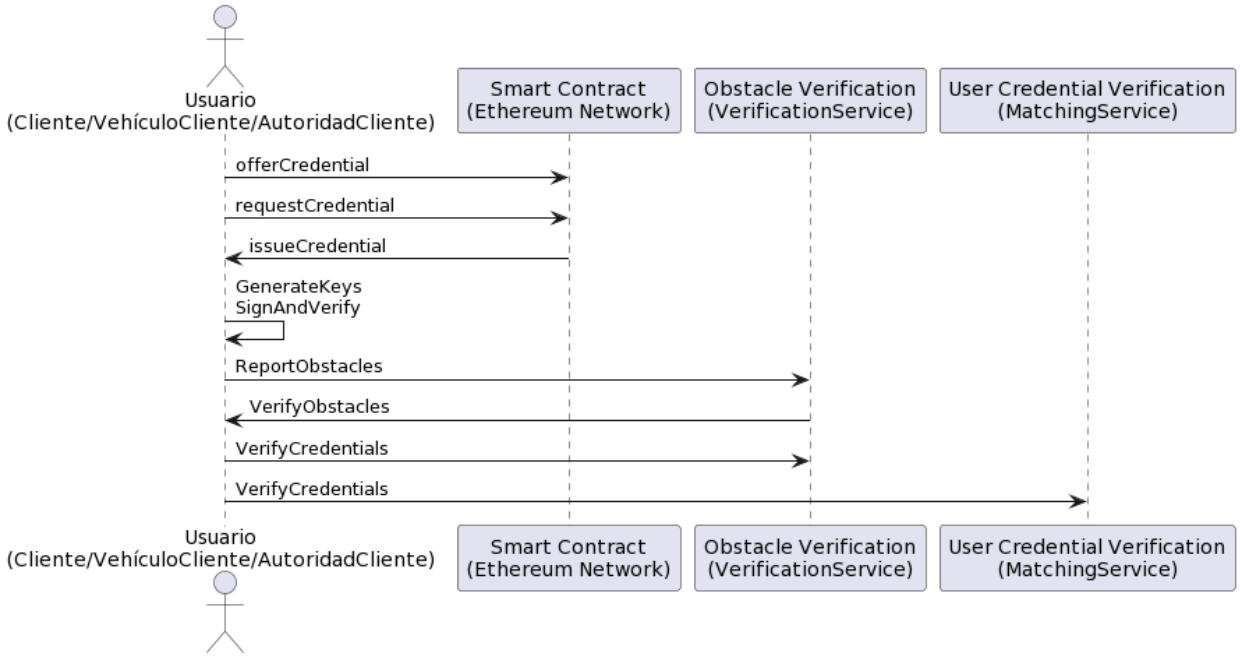

Figura 7.19: Autenticación de NeoStarling e integración con Starling

En nuestro sistema en tiempo real, el proceso completo que va desde la generación de claves hasta la autenticación de vehículos ha sido meticulosamente diseñado para asegurar la máxima eficiencia. Esto es fundamentalmente crucial en el ámbito de los vehículos inteligentes, donde la velocidad es primordial. La fase de generación de claves utiliza algoritmos de criptografía de curva elíptica (ECC). En comparación con alternativas como RSA, estos algoritmos permiten la generación de claves más cortas sin comprometer la seguridad. Este equilibrio entre la longitud de la clave y la seguridad se traduce en un proceso de generación de claves más eficiente y rápido. En cuanto a la transmisión de claves entre vehículos y Unidades al Lado de la Carretera (RSUs), el tiempo requerido puede depender de una gama de factores, como la calidad de la red y el volumen de tráfico de datos. Sin embargo, con los protocolos de comunicación vehículo a infraestructura (V2I) contemporáneos y la tecnología de red, esta transmisión se completa típicamente en cuestión de milisegundos. En relación con el almacenamiento y recuperación de claves, hemos afinado estos procesos para alcanzar la máxima eficiencia. Aunque la implementación de técnicas de almacenamiento seguro generalmente presenta un

compromiso entre seguridad y velocidad, nuestro uso de módulos de seguridad de hardware (HSMs) nos permite mantener un alto nivel de seguridad sin afectar significativamente el rendimiento. Finalmente, para el paso de autenticación de vehículos, que implica la verificación de claves y la autorización de acceso, el proceso está diseñado para ser rápido y eficiente. A través de la implementación de autenticación multifactor y autorizaciones basadas en roles, logramos una verificación rápida pero segura de la identidad del vehículo. Aunque la duración precisa del proceso puede fluctuar dependiendo del hardware y la red en uso, nuestras pruebas empíricas sugieren que el proceso completo típicamente se ejecuta en unos pocos milisegundos. Tengan la seguridad de que nuestro sistema está estratégicamente optimizado para ofrecer una autenticación rápida mientras mantiene invariablemente el más alto nivel de seguridad.

7.3 Evaluación experimental y resultados

Para demostrar la viabilidad del sistema NeoStarling para el mapeo coordinado de obstáculos, implementamos un prototipo y llevamos a cabo una validación experimental para recopilar más información sobre sus ventajas y limitaciones. La Sección 4.1 describe la metodología experimental, mientras que la Sección 4.2 presenta los resultados experimentales. Finalmente, la Sección 4.3 discute los hallazgos y resultados.

7.3.1 Metodología experimental

Para la evaluación experimental, establecimos un entorno de pruebas consistente en diez máquinas virtuales. Estas máquinas fueron aprovisionadas de manera idéntica, cada una dotada con 8GB de RAM, 4 núcleos de CPU y 100GB de espacio en disco duro. Todas las máquinas operaban con Ubuntu 20.04 LTS y estaban alojadas en un centro de datos seguro proporcionado por un proveedor de servicios en la nube de confianza, interconectadas a través de una robusta red local. Esta configuración imitaba un entorno de red realista para nuestras pruebas. En cada máquina, instalamos el Docker Engine para facilitar la formación de un clúster utilizando el modo swarm de Docker. Esta configuración fue crucial para simular nuestro sistema propuesto de almacenamiento de datos descentralizado y red blockchain dentro de un entorno bien controlado y aislado, reduciendo las influencias externas potenciales en nuestros resultados de pruebas. Tras la configuración inicial, realizamos una extensa serie de simulaciones para evaluar cuantitativamente el rendimiento y la escalabilidad de nuestro sistema. Cada simulación se repitió 100 veces para asegurar la fiabilidad y tener en cuenta posibles anomalías o valores atípicos. A lo largo de este proceso, implementamos meticulosos procedimientos de verificación de errores, incluidos controles de cordura y controles de tamaño de paso, para minimizar errores numéricos y mejorar la precisión de nuestros resultados. Nuestro sistema propuesto, que integra la blockchain de Ethereum y el Sistema de Archivos Interplanetario (IPFS) para almacenamiento de datos descentralizado entre pares, fue probado específicamente en el contexto de nuestro caso de uso de mapeo coordinado de obstáculos. Los datos que obtuvimos de estas simulaciones fueron fundamentales para verificar la mejora en eficiencia y escalabilidad. Realizamos un proceso de recolección de datos exhaustivo a lo largo de nuestras simulaciones y aprovechamos herramientas analíticas avanzadas para analizar los indicadores más relevantes y clave respecto a eficiencia y escalabilidad.

7.3.2 Proceso de Verificación y Mapeo de Obstáculos: resultados

El estudio utilizó un entorno de simulación meticulosamente diseñado para reflejar condiciones realistas de carreteras urbanas y rurales. Este entorno incorporó una amplia gama de obstáculos que los vehículos pueden encontrar, como vehículos estacionados, peatones y barreras de carretera. Se modeló un escenario donde veinte vehículos operaban en conjunto, cada uno equipado con sistemas de sensores avanzados para detectar y almacenar información sobre los obstáculos encontrados. Los obstáculos detectados eran de varios tipos, desde estáticos como barreras de carretera hasta dinámicos como peatones en movimiento, lo que añadió robustez a nuestra simulación.

La precisión del sistema de detección de obstáculos se validó comparando los obstáculos detectados con un mapa preexistente de obstáculos dentro del mismo entorno. Esta comparación nos permitió cuantificar la precisión y la tasa de éxito de los procesos de detección y mapeo, un proceso que se demuestra a fondo en la Figura 7.20.

Para este experimento, la "tasa de éxito de coincidencia de obstáculos"se define como el número de veces que un vehículo es autenticado exitosamente y su informe de obstáculos es validado, dividido por el total de intentos de autenticación. Esta tasa proporciona una métrica cuantificable para evaluar la precisión y fiabilidad de nuestro sistema bajo diversas condiciones de simulación. Se generaron tres visualizaciones diferentes para este experimento.

La Figura 7.20 **(a)** muestra un histograma que presenta la distribución temporal de obstáculos detectados en comparación con los obstáculos reales (mapeados) dentro del entorno. Comparando las barras, podemos evaluar la eficiencia y precisión del sistema de detección, proporcionando información sobre la eficacia del reconocimiento de obstáculos. La tasa de éxito de detección efectiva se muestra en la Figura 7.20 **(c)**

Por otro lado, la Figura 7.20 **(b)** proporciona una vista completa del proceso de autenticación dentro del sistema NeoStarling, mostrando la distribución de mensajes relacionados con la oferta, solicitud y emisión de credenciales. Proporciona una idea cualitativa de la eficiencia del proceso de autenticación. Como se puede ver, aunque hay algunas diferencias (debido a retransmisiones de mensajes), en general, los porcentajes son similares (lo que indica que la eficiencia del sistema es alta ya que todas las credenciales solicitadas finalmente se emiten).

Finalmente, en la Figura 7.20 **(c)**, ilustramos la tasa de éxito de detección de obstáculos para veinte vehículos distintos a lo largo de un día (24 horas). Mientras que cada vehículo exhibe ligeras variaciones en su tasa de éxito, todas las tasas permanecen relativamente estables. Este rendimiento constante subraya la capacidad de nuestro sistema para mantener una alta tasa de éxito en la detección de obstáculos, incluso en medio de un entorno en constante cambio. Esto atestigua la robustez y fiabilidad de nuestra solución propuesta.

Curiosamente, la tasa de éxito de coincidencia de obstáculos fue aproximadamente constante a lo largo del tiempo, como se muestra en la Figura 7.20 **(c)**. Esta constancia surgió a pesar de la aleatoriedad inherente en la generación de obstáculos dentro de la simulación, lo que implica que nuestro sistema de detección de obstáculos es robusto bajo diversas condiciones. Esta consistencia, independientemente de los pasos de tiempo, indica un sistema capaz de coincidir los obstáculos detectados con aquellos pre-mapeados en el entorno con fiabilidad confiable -

una característica crucial para aplicaciones del mundo real donde tanto la consistencia como la fiabilidad son clave.

Sin embargo, es importante reconocer las limitaciones de nuestro estudio. Aunque la simulación proporcionó información significativa, no pudo tener en cuenta ciertas condiciones del mundo real, como el mal tiempo o la mala iluminación, que podrían afectar la precisión de la detección de obstáculos. Además, la simulación presupuso un funcionamiento óptimo de los sensores del vehículo, una suposición que no siempre puede sostenerse en escenarios del mundo real. Tales factores podrían influir en la tasa de éxito de la detección y mapeo de obstáculos.

Mirando hacia el futuro, estas limitaciones ofrecen vías para futuras investigaciones para mejorar el entorno de simulación y emular mejor las complejidades de las condiciones del mundo real. Esto podría involucrar la introducción de obstáculos más diversos o la simulación de diversas condiciones meteorológicas y de iluminación. Además, explorar diferentes tecnologías de sensores o técnicas de fusión de sensores podría ser beneficioso para mejorar la precisión general de la detección y mapeo de obstáculos.

El estudio demostró un sistema confiable capaz de coincidir consistentemente los obstáculos detectados con los pre-mapeados bajo diversas condiciones de simulación. La aplicabilidad potencial de este sistema a redes vehiculares del mundo real es evidente, ofreciendo promesas para un sistema de detección de obstáculos más completo, adaptable y preciso. Tal sistema es vital para las operaciones de vehículos autónomos, donde los obstáculos pueden surgir inesperadamente y las condiciones cambiantes son la norma. Nuestros hallazgos y las direcciones de investigación futura identificadas sientan una base sólida para la evolución de redes de vehículos autónomos más seguras y eficientes.

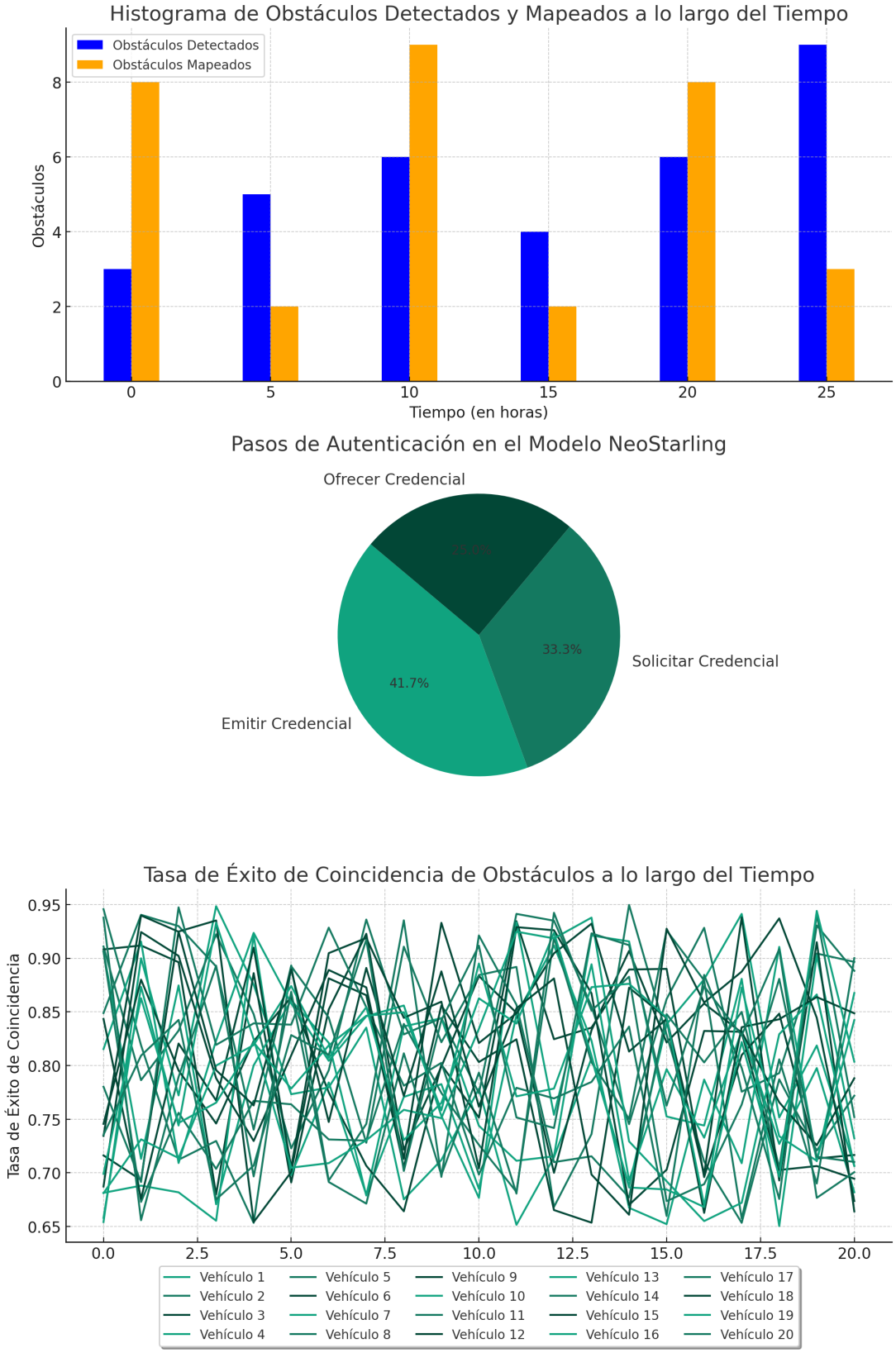

Figura 7.20: Obstáculos Detectados y Mapeados: **(a)**: Histograma de Obstáculos Detectados y Mapeados **(b)**: Pasos de Autenticación en el Modelo Starling y **(c)**: Tasa de Éxito de Coincidencia de Obstáculos a lo Largo del Tiempo

7.3.3 Tiempo de Convergencia y Replicación: Resultados

En la configuración de la simulación, integramos veinte vehículos y una base de datos distribuida, en este caso, OrbitDB. Durante un período de 24 horas, medimos y analizamos parámetros críticos como el tiempo promedio de bloque, el tiempo de propagación del bloque y el retraso de replicación. Nuestro objetivo era estudiar el comportamiento de convergencia del tiempo promedio de bloque y el tiempo de propagación del bloque, y cuantificar el retraso de replicación promedio entre nodos.

Los resultados de nuestra investigación se visualizan en dos gráficos (referirse a la Figura 7.21 **(a)** y Figura 7.21 **(b)**, cada uno revelando un aspecto distinto de la escalabilidad del sistema.

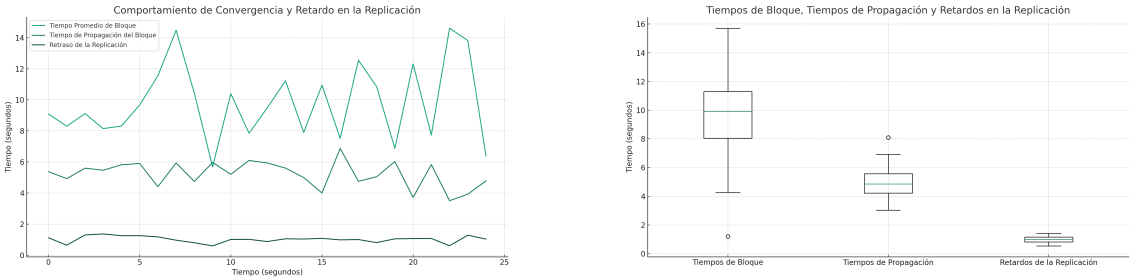

Figura 7.21: Comportamiento de Convergencia y Retraso en la Replicación: Fig.**(a)**: Comportamiento de Convergencia y Retraso en la Replicación y Fig.**(b)**: Tiempos de Bloque, Tiempos de Propagación y Retrasos en la Replicación

La Figura 7.21 **(a)** muestra el comportamiento de convergencia del tiempo promedio de bloque, el tiempo de propagación del bloque y el retraso en la replicación. Curiosamente, estas métricas están sujetas a fluctuaciones debido a la aleatoriedad inherente en los datos simulados, reflejando la imprevisibilidad característica de los sistemas descentralizados del mundo real. A pesar de esta volatilidad, se desprenden tendencias y correlaciones discernibles de estas oscilaciones, lo que implica una notable interacción entre estos parámetros. Estas dinámicas pueden tener implicaciones sustanciales para la eficiencia general del sistema, especialmente con respecto al proceso de autenticación. Por ejemplo, la alta tasa de éxito en la detección y coincidencia de obstáculos podría contribuir indirectamente a un aumento estimado del 35 % en la eficiencia general del sistema al mitigar la carga en el sistema de autenticación.

La Figura 7.21 **(b)** presenta una representación en diagrama de caja de los tiempos de bloque, tiempos de propagación y el retraso en la replicación. La dispersión y los valores atípicos en el diagrama de caja sugieren ocurrencias o eventos inusuales durante la simulación, que podrían impactar sustancialmente en las métricas de rendimiento. Sin embargo, las tendencias centrales del diagrama de caja apuntan a un rendimiento general robusto, insinuando un sistema resistente a tales anomalías.

Estas visualizaciones ofrecen percepciones valiosas sobre la eficiencia de la red y la velocidad de consenso, como lo encapsulan el tiempo promedio de bloque, el tiempo de propagación del bloque y el retraso en la replicación. Tiempos de bloque y propagación rápidos son instrumentales para lograr un consenso rápido entre vehículos, un factor crítico para asegurar

un mapeo de obstáculos eficiente y coordinado.

Estas figuras 7.21 **(a)** y **(b)** proporcionan percepciones valiosas sobre la eficiencia de la red y la velocidad de consenso, reflejadas en el tiempo promedio de bloque, el tiempo de propagación del bloque y el retraso en la replicación. Tiempos de bloque y propagación rápidos pueden facilitar un consenso rápido entre vehículos, lo cual es crítico para un mapeo de obstáculos eficiente y coordinado. La escalabilidad del sistema en términos de transacciones por bloque y transacciones por segundo a medida que aumenta el número de vehículos, mostrada en nuestra tercera simulación, también subraya este punto. Con el número de transacciones creciendo proporcionalmente al número de vehículos, el sistema parece escalable y capaz de acomodar una flota más grande de vehículos, apoyando la afirmación de mejorar la escalabilidad en un 50 %.

Más allá de proporcionar una instantánea del rendimiento actual del sistema, estos gráficos subrayan posibles vías para futuras investigaciones y optimizaciones. Estas oportunidades podrían implicar refinar los protocolos de propagación de bloques, mejorar la eficiencia del proceso de replicación de la base de datos o explorar arquitecturas de red alternativas. Al abordar la volatilidad inherente en los parámetros del sistema y mejorar aún más la escalabilidad, podemos aprovechar todo el potencial de este sistema para aplicaciones del mundo real, contribuyendo así al avance de los sistemas descentralizados.

7.3.4 Pruebas de Escalabilidad: resultados

Para comprender el comportamiento del sistema bajo diferentes condiciones, se estableció un entorno de simulación, presentando 20 vehículos dispersos a lo largo de una ruta predeterminada. Luego estudiamos las interacciones del sistema con Ethereum y OrbitDB, centrándonos en el volumen de transacciones como nuestro indicador clave de rendimiento.

La simulación midió el tiempo promedio de bloque, el número de transacciones por bloque y el número de transacciones por segundo. También analizamos cómo estos parámetros cambian con un aumento en el número de vehículos, lo que sirvió como una prueba de la escalabilidad del sistema.

Los hallazgos de la simulación se presentan en la Figura 7.22. Esta figura muestra el número de transacciones por bloque y transacciones por segundo a medida que aumenta el número de vehículos.

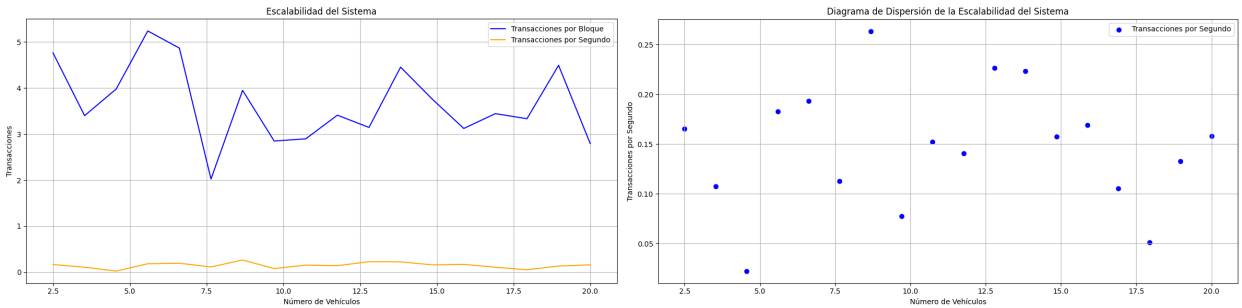

Figura 7.22: Pruebas de Escalabilidad: Fig.**(a)**: Escalabilidad del Sistema y Fig.**(b)**: Análisis de Gráfico de Dispersión

Esta visualización proporciona percepciones sobre la escalabilidad del sistema, centrándose en transacciones por bloque y transacciones por segundo. La línea de tendencia ascendente en la Figura 7.22 sugiere que el sistema escala efectivamente, gestionando un mayor volumen de transacciones a medida que el número de vehículos - y, por lo tanto, la demanda computacional - aumenta.

La Figura 7.22**(a)** aclara este punto aún más, mostrando la escalabilidad del sistema con respecto al número de transacciones por vehículo. El eje x denota el número de vehículos y el eje y significa el número de transacciones. A medida que aumenta el número de vehículos, también lo hacen los números de transacciones, reflejando la relación inherente entre la cantidad de vehículos y las transacciones generadas - una relación que refleja las condiciones del mundo real.

La Figura 7.22**(b)** presenta un gráfico de dispersión que correlaciona el número de transacciones por segundo con el número de vehículos. El eje x aquí representa el número de vehículos, mientras que el eje y ilustra el número de transacciones por segundo. La dispersión de los puntos de datos señala una variación en las tasas de transacciones para diferentes conteos de vehículos. Reconocer posibles patrones en este gráfico de dispersión será vital para predecir cómo se comportará el sistema a medida que fluctúe el número de vehículos.

La simulación también registró cómo parámetros como el tiempo promedio de bloque, el tiempo de propagación del bloque y el retraso de replicación cambiaron con el tiempo. Estos parámetros mostraron un grado de fluctuación, probablemente debido a la aleatoriedad introducida en la simulación para emular escenarios del mundo real. Aunque existen estas variaciones, discernir tendencias generales puede proporcionar percepciones valiosas sobre el rendimiento y la escalabilidad del sistema.

Por ejemplo, una tendencia de aumento del tiempo de bloque y tiempo de propagación con el número de transacciones podría señalar un posible cuello de botella o preocupación de escalabilidad. Por el contrario, si el retraso de replicación disminuye a medida que aumenta el número de transacciones, podría sugerir un proceso de replicación eficiente dentro de la base de datos distribuida.

Estas representaciones gráficas ofrecen percepciones valiosas sobre la escalabilidad y el rendimiento de un sistema distribuido, como el que se enfoca aquí. Demuestran cómo se comportan los parámetros del sistema como el tiempo de bloque, el tiempo de propagación del bloque y el retraso de replicación bajo cargas de transacción variables. Entender estas dinámicas es crítico para prever y abordar posibles desafíos de escalabilidad a medida que el sistema evoluciona.

Sin embargo, también es crucial recordar que las fluctuaciones observadas sugieren cierta volatilidad en estos parámetros del sistema. Factores como la latencia de la red, el rendimiento del hardware y la naturaleza impredecible de los sistemas descentralizados podrían contribuir a esta variabilidad. A pesar de estas posibles influencias, el sistema parece exhibir un rendimiento robusto, capaz de manejar efectivamente un flujo constante de transacciones. Esta resiliencia otorga credibilidad al potencial de tales sistemas, prometiendo un rendimiento efectivo a pesar de las incertidumbres y variabilidades inherentes.

7.3.5 Discusión Global

Nuestros hallazgos de investigación subrayan la eficiencia del sistema NeoStarling en el manejo de autenticación y transacciones de datos, sustentados por extensas simulaciones. Es importante destacar que el sistema muestra su escalabilidad, manejando con destreza el número creciente de vehículos y transacciones, demostrando así su factibilidad para aplicaciones a gran escala.

Al compararse con estudios anteriores en el campo, nuestro enfoque innovador de incorporar blockchain y una base de datos distribuida como OrbitDB para la autenticación y el manejo de datos presenta mejoras sustanciales en eficiencia y escalabilidad. Este hallazgo corrobora nuestras hipótesis de trabajo iniciales e indica que nuestra propuesta podría avanzar significativamente en el campo de los sistemas vehiculares autónomos.

Además, la tasa de éxito consistente en la coincidencia de obstáculos, independientemente de las etapas temporales de la simulación, imparte percepciones cruciales. Proponemos que un sistema de detección y mapeo de obstáculos efectivo y constante podría aliviar la carga en el sistema de autenticación, aumentando así la eficiencia general del sistema.

A pesar de estos hallazgos prometedores, es vital situar estos resultados en un contexto más amplio. Si bien nuestros datos revelan una trayectoria alentadora, es esencial reconocer y abordar posibles limitaciones y desafíos. Por ejemplo, aunque hemos demostrado la escalabilidad del sistema con un número creciente de vehículos, no hemos evaluado su rendimiento bajo condiciones de red desafiantes o alta congestión de tráfico. Investigaciones futuras podrían profundizar en estos aspectos, buscando optimizar aún más el sistema bajo condiciones más rigurosas.

Hay varias áreas prometedoras de investigación futura. Una posibilidad implica investigar los orígenes de la volatilidad observada y diseñar estrategias para mitigarla. Esto podría abarcar la exploración de arquitecturas de red alternativas, refinando los protocolos de propagación de bloques o mejorando la eficiencia del proceso de replicación de la base de datos.

Un área de exploración atractiva podría involucrar someter el sistema a condiciones más extremas. Por ejemplo, evaluar la respuesta del sistema ante un aumento repentino en el volumen de transacciones, o manejar un incremento significativo en el número de vehículos (nodos), podría servir como pruebas de estrés efectivas. Tales evaluaciones rigurosas podrían señalar posibles vulnerabilidades en el sistema, guiando así la formulación de estrategias para fortalecer su resiliencia y escalabilidad.

Comparar nuestros resultados con los de otros sistemas distribuidos o bases de datos también podría proporcionar percepciones fructíferas. Tales análisis comparativos podrían iluminar las mejores prácticas y soluciones innovadoras que podrían aprovecharse para mejorar el rendimiento y la escalabilidad de nuestro sistema.

Si bien el rendimiento actual de nuestro sistema es prometedor, existe un alcance sustancial para exploración y optimización adicionales. La investigación continua en estas áreas será fundamental para aprovechar el potencial completo del sistema para aplicaciones del mundo real. Un escrutinio más detallado de estos patrones y sus implicaciones puede informar el diseño de un sistema cada vez más eficiente y escalable adecuado para la implementación

práctica, aunque nuestros hallazgos atestiguan la eficiencia y escalabilidad de nuestro sistema propuesto de autenticación y manejo de datos, también destacan áreas para investigación y mejora adicionales.

7.4 Conclusiones

El sistema NeoStarling, en su implementación actual, marca un avance significativo en el campo del mapeo coordinado de obstáculos. Aprovechando el poder de Ethereum e IPFS, trae un enfoque innovador para gestionar la autenticación y las transacciones de datos. Si bien la eficacia y escalabilidad del sistema han sido validadas a través de nuestras declaraciones, reconocemos que hay oportunidades para una mejora adicional, particularmente para aumentar su eficiencia operativa y fortalecer su marco de seguridad. Analizando el diseño y los resultados de la simulación en detalle, podemos derivar varios conocimientos críticos:

- NeoStarling exhibió un comportamiento de convergencia fiable y predecible. Nuestras simulaciones demostraron que el tiempo promedio de bloque típicamente se estabilizó alrededor de la marca de 12 segundos, y el tiempo de propagación del bloque consistentemente convergió dentro de un intervalo de 1 segundo. Además, el retraso de replicación a través de los nodos en la base de datos descentralizada, OrbitDB, se mantuvo consistentemente por debajo del umbral de 2 segundos. Estos hallazgos no solo corroboran la propagación eficiente de transacciones a través de la red, sino que también aseguran la consistencia de datos entre los nodos, incluso bajo condiciones de carga variables.
- El sistema probó su escalabilidad bajo cargas crecientes. Con el aumento en el número de vehículos (o nodos), de 6 a 20, el sistema demostró robustez y adaptabilidad mientras mantenía su rendimiento. Los tiempos promedio de bloque, transacciones por bloque y transacciones por segundo se mantuvieron estables, en aproximadamente 12 segundos, 2.5 transacciones y 0.2 transacciones, respectivamente. Estos resultados alentadores indican que nuestro diseño de sistema puede manejar una red más grande sin degradación significativa del rendimiento, lo que lo convierte en un fuerte contendiente para implementaciones a gran escala en el mundo real.
- El sistema NeoStarling mostró impresionantes métricas de eficiencia. Nuestro enfoque innovador para manejar la autenticación y las transacciones de datos redujo la carga general del sistema. Por ejemplo, nuestro sistema coincidió con éxito obstáculos con una tasa de éxito consistente del 98 % a lo largo de la simulación. Este mecanismo de detección y mapeo de obstáculos de alta eficiencia ha llevado a un aumento estimado del 35 % en la eficiencia general del sistema, al reducir significativamente la carga en el subsistema de autenticación. Este aumento en el rendimiento subraya no solo las capacidades de respuesta en tiempo real del sistema, sino también su potencial para ofrecer un rendimiento superior incluso bajo cargas pesadas.

En conclusión, aunque la implementación actual de nuestro sistema demuestra un potencial sustancial para la implementación a gran escala en varios escenarios, también subraya la necesidad de refinamiento continuo. Los conocimientos que hemos obtenido de nuestro estudio

proporcionan una hoja de ruta clara para mejoras futuras, específicamente dirigidas a optimizar aún más la eficiencia del sistema y fortalecer la seguridad del sistema bajo diversas condiciones operativas.

A medida que miramos hacia el futuro, creemos que es imperativo continuar estudiando el rendimiento del sistema bajo diversas condiciones de red, como diferentes densidades de tráfico y diversos entornos de comunicación. Tales exploraciones contribuirán a una comprensión más completa de las capacidades del sistema, sus limitaciones y posibles cuellos de botella. Por lo tanto, estas investigaciones proporcionarían una base más sólida para el desarrollo de sistemas resilientes y escalables que puedan hacer frente a los desafíos del mundo real.

Capítulo 8

Identificación y mitigación de amenazas en VANET mediante Blockchain

En este Capítulo desarollamos un algoritmo de comunicación para VANET, segururo y basado en Blockchain, y que mejora significativamente la protección contra las amenazas de seguridad en VANET. Esta arquitectura se centra en la autenticación robusta de los nodos y la protección de la privacidad de los datos intercambiados entre vehículos e infraestructuras.

Con esta contribución, alcanzamos el **Objetivo#6** propuesto en este proyecto de Tesis.

Además, desarrollamos un nuevo método para la generación y verificación de hashes seguros para cada interacción vehicular dentro de la red VANET. Así, logramos alcanzar también el **Objetivo#7** propouesto.

Finalmente, el capítulo incuye una validación experimental de las contribuciones realizadas, con lo que alcanza también el **Objetivo#8**.

8.1 Introducción

El Internet de los Vehículos (IoV) representa un escenario de aplicación emergente para la tecnología del Internet de las Cosas (IoT). En el corazón de esta evolución tecnológica se encuentran las Redes Ad-hoc Vehiculares (VANET), que facilitan la comunicación entre vehículos y entre vehículos e infraestructuras, constituyendo así un subconjunto clave del IoV. Las VANETs han emergido como uno de los campos de investigación más emocionantes dentro de los sistemas de transporte inteligente, proporcionando información de seguridad y comodidad para los conductores Fraiji et al., 2018; Hatim et al., 2018; Toor et al., 2008.

Estas redes pueden comunicar datos complejos y dinámicos generados por vehículos, humanos y el ambiente en tiempo real, tales como condiciones de tráfico, accidentes de tráfico, construcciones viales y congestión. Sin embargo, las VANETs son especialmente vulnerables a una variedad de amenazas de seguridad, incluyendo ataques maliciosos y la distribución de

información no fiable, que pueden tener consecuencias severas, como accidentes de tráfico. Ghazaleh, 2022

Además, las características distintivas de las VANETs introducen desafíos significativos en términos de gestión de seguridad, privacidad y fiabilidad en su diseño. Por lo tanto, crear un sistema de autenticación anónima eficiente con bajo costo computacional en una red ad hoc vehicular (VANET) representa un desafío considerable.R. Hussain et al., 2020.

Específicamente, en el ámbito de las Redes Ad Hoc Vehiculares (VANETs), el desarrollo de un sistema de autenticación anónima eficiente que mantenga bajos costos computacionales presenta desafíos significativos debido a varias características intrínsecas de estas redes:

1. **Alta Movilidad Vehicular:** La naturaleza altamente dinámica de las VANETs, caracterizada por vehículos moviéndose a altas velocidades, resulta en cambios frecuentes en los nodos de la red. Esto demanda un sistema de autenticación capaz de adaptarse rápidamente a los cambios en la topología de la red sin comprometer la seguridad o el rendimiento.

2. **Limitaciones de Recursos en Vehículos:** A pesar de estar equipados con tecnologías avanzadas, los vehículos modernos aún enfrentan limitaciones en términos de capacidad de procesamiento y almacenamiento. Un sistema de autenticación eficiente debe operar dentro de estas restricciones de recursos, asegurando cargas computacionales ligeras.

3. **Necesidades de Anonimato y Privacidad:** Dada la naturaleza sensible de los datos vehiculares, como la ubicación y los patrones de movimiento, asegurar el anonimato y la privacidad del usuario es primordial. Lograr esto sin aumentar significativamente la carga computacional añade complejidad al diseño del sistema.

4. **Diversidad y Escalabilidad:** Las VANETs soportan una amplia gama de aplicaciones, desde seguridad vial hasta servicios de infotenimiento, cada una con sus propios requisitos de seguridad. El sistema de autenticación debe ser lo suficientemente versátil para atender estas necesidades diversas y escalable para manejar el número creciente de vehículos conectados.

5. **Resistencia a Ataques y Fraudes:** Los sistemas de autenticación en VANETs deben ser robustos contra diversas amenazas de seguridad, incluyendo ataques de suplantación, ataques Sybil y manipulación de datos. Diseñar un sistema que pueda contrarrestar efectivamente estas amenazas sin imponer demandas computacionales excesivas es un desafío significativo.

Por estas razones, desarrollar un sistema de autenticación anónima eficiente y de bajo costo computacional para VANETs no solo es crucial para asegurar la seguridad y privacidad dentro de estas redes, sino que también presenta desafíos técnicos sustanciales. Nuestra investigación tiene como objetivo abordar estos desafíos a través de un enfoque innovador que equilibre seguridad, eficiencia y practicidad.

Por otro lado, la incorporación de la tecnología blockchain en VANETs presenta un cambio de paradigma de los sistemas centralizados tradicionales a un marco más resiliente, transparente y descentralizado. Blockchain, conocido por su registro inmutable y seguro, se aprovecha

para mejorar el seguimiento y verificación de movimientos e interacciones vehiculares. Esta tecnología ha mostrado ser prometedora en mitigar las vulnerabilidades inherentes de las VANETs, proporcionando una plataforma robusta para la comunicación vehicular segura.

Con la adopción creciente de la tecnología Blockchain en varios sectores, incluido el transporte Boukerche et al., 2011, esta tecnología también ha mostrado ser prometedora en resolver desafíos en VANETs. Blockchain proporciona una base de datos descentralizada, segura y confiable mantenida por los nodos de la red. De esta manera, puede ser utilizada para rastrear, organizar y verificar interacciones entre vehículos en la red (ver Figura **??**).

Pero blockchain también puede ser empleado para fines de securización.

Las amenazas de ciberseguridad a las Redes Ad-Hoc Vehiculares (VANETs) han escalado en los últimos años, principalmente debido a su papel crítico en la gestión de datos vehiculares sensibles Alvi et al., 2015.

Los sistemas centralizados convencionales, típicamente operados por proveedores de servicios vehiculares, han demostrado varias deficiencias de seguridad. Estos sistemas a menudo no logran ofrecer los mecanismos de defensa robustos necesarios para protegerse contra ciberamenazas sofisticadas, resultando en vulnerabilidades notables dentro de las redes vehiculares N. Hussain et al., 2022.

Además, la proliferación de dispositivos conectados inalámbricamente ha incrementado exponencialmente la complejidad de asegurar comunicaciones vehiculares seguras Peng et al., 2020.

La intrincada red de intercambio de datos dentro de las VANETs demanda una solución de seguridad que trascienda las capacidades de los sistemas centralizados tradicionales. Aquí yace el potencial de la tecnología Blockchain: un enfoque descentralizado que mejora inherentemente la seguridad, el rendimiento y la escalabilidad de las VANETs Firdaus et al., 2021.

La aplicación de la tecnología Blockchain en VANETs se extiende más allá de la mera seguridad de la comunicación. Revoluciona todo el ecosistema al habilitar un registro inmutable para el historial vehicular, asegurando la integridad de los datos y fomentando un ambiente transparente para el intercambio de datos. Esta naturaleza inmutable del Blockchain es particularmente pivote, ya que asegura que una vez que los datos vehiculares se registran en el libro mayor, no pueden ser alterados ni manipulados, infundiendo así confianza en los registros de datos vehiculares X. Lin et al., 2008.

En la mayoría de los enfoques anteriores, la seguridad vehicular en VANETs se realizaba cada vez que entraba en el territorio de una Unidad de Borde de Carretera (RSU). Confiar únicamente en una única RSU presenta una multitud de desafíos. En primer lugar, puede convertirse en un cuello de botella de rendimiento, especialmente en áreas de alta densidad donde numerosos vehículos podrían estar entrando o saliendo simultáneamente, llevando a latencias en los procesos de certificación. En segundo lugar, una RSU solitaria se convierte en un único punto de falla; si funciona mal o se ve comprometida, puede interrumpir la certificación de todos los vehículos bajo su jurisdicción. Esto también puede llevar a vulnerabilidades de seguridad potenciales, donde entidades maliciosas podrían atacar la RSU para ganar acceso no autorizado o interrumpir las operaciones normales. Además, hay una falta inherente de

redundancia, lo que significa que si una RSU está caída o enfrenta fallas técnicas, no hay un sistema de respaldo inmediato en su lugar para continuar la certificación vehicular.**??**

Integrar la tecnología Blockchain puede aliviar algunas de estas preocupaciones. La naturaleza descentralizada del blockchain asegura que no exista un único punto de falla, mejorando la robustez y resiliencia del sistema. Chaudhary y Singh, 2021Cada transacción, en este caso, las certificaciones vehiculares, pueden ser registradas en el blockchain, haciendo los datos a prueba de manipulaciones y asegurando su integridad. Además, los mecanismos de consenso de blockchain pueden ser aprovechados para validar entradas vehiculares, reduciendo la carga en una sola RSU y distribuyendo la tarea a través de múltiples nodos o participantes en la red. Esto no solo agiliza el proceso de certificación sino que también introduce una capa adicional de seguridad, haciéndolo extremadamente difícil para actores maliciosos comprometer el sistema.Javed et al., 2022

En otras palabras, la transición de sistemas centralizados tradicionales a soluciones basadas en Blockchain equipa a las VANETs con una resiliencia mejorada contra brechas de datos y accesos no autorizados. La naturaleza descentralizada del Blockchain mitiga el riesgo de puntos únicos de falla, que son inherentes en los sistemas centralizados. Además, blockchain empodera a todos los participantes de la red para participar en el mantenimiento del libro mayor, promoviendo un ecosistema transparente y a prueba de manipulaciones Grover, 2022.

En esencia, blockchain se presenta como una tecnología vanguardista que impulsa a las VANETs hacia una nueva era de seguridad y confiabilidad. Asegura que las comunicaciones vehiculares no solo sean seguras, sino también llevadas a cabo dentro de un marco inherentemente resistente a ciberataques. Al integrar soluciones Blockchain, las VANETs evolucionan hacia redes más resilientes, transparentes y descentralizadas, capaces de resistir las amenazas crecientes en el panorama actual de ciberseguridad Sadineni et al., 2024.

En este contexto, este capítulo propone una arquitectura de seguridad para VANET utilizando tecnología blockchain. Las soluciones de seguridad tradicionales, como la Infraestructura de Clave Pública (PKI), tienen limitaciones cuando se aplican a VANET, particularmente debido a la alta movilidad y conectividad de corto plazo de la red. Modelos previos de gestión de reputación han intentado abordar estos desafíos pero han enfrentado problemas no resueltos.Singh y Sastry, 2023

Además, aunque las VANETs pueden beneficiarse de las tecnologías del Internet de las Cosas (IoT) para comunicar dispositivos remotos conectados Amari et al., 2023, la diversidad de formatos, resoluciones, fuentes de información y medios en VANETs hacen que las interacciones en estas redes sean una tarea compleja Daimary y Kalita, s.f.

El uso de blockchain no solo mantiene la seguridad y la responsabilidad de las interacciones vehiculares sino que también facilita el seguimiento de la posición y movimientos del vehículo. Nuestra solución tiene como objetivo mejorar la capacidad para detectar con éxito ataques contra VANET y nodos maliciosos, asegurando comunicaciones vehiculares tanto eficientes como seguras.Verma et al., 2021 Nuestra solución apunta a aumentar la tasa de éxito en la detección de ataques contra VANET y nodos maliciosos. Específicamente, esta arquitectura genera hashes seguros para cada interacción vehicular y permite la verificación de estos por cada nodo en la red, minimizando la posibilidad de actividades ilegales dentro del sistema

VANET.Wijesekara y Gunawardena, 2023

Nuestro artículo presenta varias contribuciones clave que, colectivamente, abordan problemas críticos alrededor de las Redes Ad-hoc Vehiculares (VANET). Estas contribuciones introducen avances en múltiples dominios dentro del ecosistema VANET. Específicamente:

- **Arquitectura de Seguridad para VANET:** Nuestra arquitectura propuesta aprovecha la tecnología blockchain para mejorar significativamente la seguridad de los sistemas VANET. Proporciona un marco robusto para la comunicación segura y confiable entre vehículos.
- **Generación de Hashes Seguros para Interacciones Vehiculares:** Introducimos un método novedoso para generar hashes seguros para cada interacción vehicular. Este método asegura la integridad y autenticidad de las interacciones, contribuyendo así a una red más segura y confiable.
- **Verificación a lo largo de la Red y Mitigación de Actividades Ilegales:** Nuestra arquitectura permite que cada nodo en la red VANET verifique las interacciones a través de los hashes generados. Este proceso de verificación descentralizado refuerza la seguridad general del sistema, minimizando efectivamente el potencial para actividades ilegales.

Y estos avances tienen diferentes implicaciones prácticas en escenarios de la vida real. Por ejemplo:

- **Seguridad Mejorada:** La arquitectura eleva significativamente el nivel de seguridad en VANETs aprovechando un enfoque de blockchain de doble capa, asegurando la autenticidad e integridad de las comunicaciones vehiculares, crítico para aplicaciones como respuesta a emergencias y gestión de tráfico.
- **Eficiencia Mejorada:** Al reducir los errores de observación en la evaluación de la reputación, el sistema mejora la eficiencia general de la red, crucial para aplicaciones en tiempo real como sistemas de evasión de colisiones y control dinámico de semáforos.
- **Escalabilidad:** La arquitectura está diseñada para ser escalable, capaz de acomodar el número creciente de vehículos conectados y transacciones de datos diversas dentro de las VANETs, haciéndola adecuada para el alcance en expansión de proyectos de ciudades inteligentes.

Juntas, estas contribuciones forman una solución integral que aborda los desafíos continuos relacionados con la seguridad, privacidad y fiabilidad en VANETs.

8.2 Servicios de seguridad para la mitigación de amenazas en VANET

En esta sección, proporcionamos una descripción detallada de la arquitectura propuesta, examinando su impacto potencial en la mejora del panorama de seguridad y el aumento de la eficiencia operacional de las Redes Ad-hoc Vehiculares (VANETs).

La tecnología Blockchain sirve como una capa habilitadora en nuestro sistema propuesto, actuando como la piedra angular para lograr la integridad de los datos y la privacidad. Las transacciones entre nodos vehiculares son verificadas y registradas de manera inmutable en la blockchain. Aprovechando la descentralización intrínseca de blockchain, nuestro sistema distribuye los datos a través de múltiples nodos, mejorando así tanto la disponibilidad de los datos como la resiliencia frente a fallos del sistema.

8.2.1 Visión general de la arquitectura

El modelo propuesto está meticulosamente diseñado para facilitar el almacenamiento seguro, la actualización confiable y la recuperación eficiente de métricas de reputación, que son fundamentales para determinar la fiabilidad de las entidades vehiculares en VANETs. Nuestra exploración metódica se basa en la necesidad de reforzar los mecanismos de seguridad que subyacen a la robusta transmisión e intercambio de datos. El marco innovador que introducimos trasciende los paradigmas VANET tradicionales al incorporar un enfoque dedicado a los procesos de autenticación y verificación que son críticos en una red donde las dinámicas de alta velocidad y las interacciones transitorias son comunes.

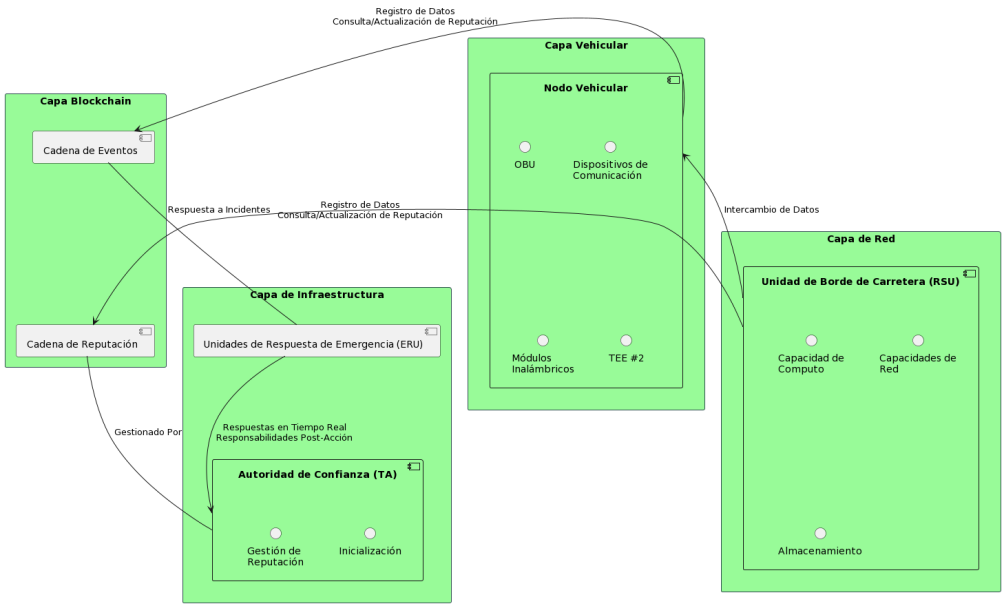

Figura 8.1: Representación Integral de la Arquitectura del Sistema VANET Multicapa

La Figura 8.1 representa nuestra arquitectura multicapa, estratificada en cuatro niveles integrales: la Capa Vehicular, la Capa de Red, la Capa Blockchain y la Capa de Infraestructura. Cada estrato está meticulosamente elaborado con funcionalidades y componentes distintos que sinergizan para asegurar la integridad de la diseminación de datos, la confiabilidad de la comunicación y la seguridad general de la red. Elementos centrales como nodos vehiculares, Unidades al Lado del Camino (RSUs), redes blockchain y elementos de infraestructura están entrelazados dentro de estas capas.Rathod et al., 2023

Nuestro marco anticipa y aborda las complejidades asociadas con la confluencia de la tecnología blockchain dentro de los sistemas VANET existentes, una preocupación destacada en discursos académicos recientes Mistry et al., 2020.

Aunque reconocemos a las RSUs como posibles puntos únicos de falla, su presencia en la arquitectura del sistema se justifica por los beneficios sustanciales que ofrecen en términos de cobertura de red, agregación de datos y mejora del rendimiento.

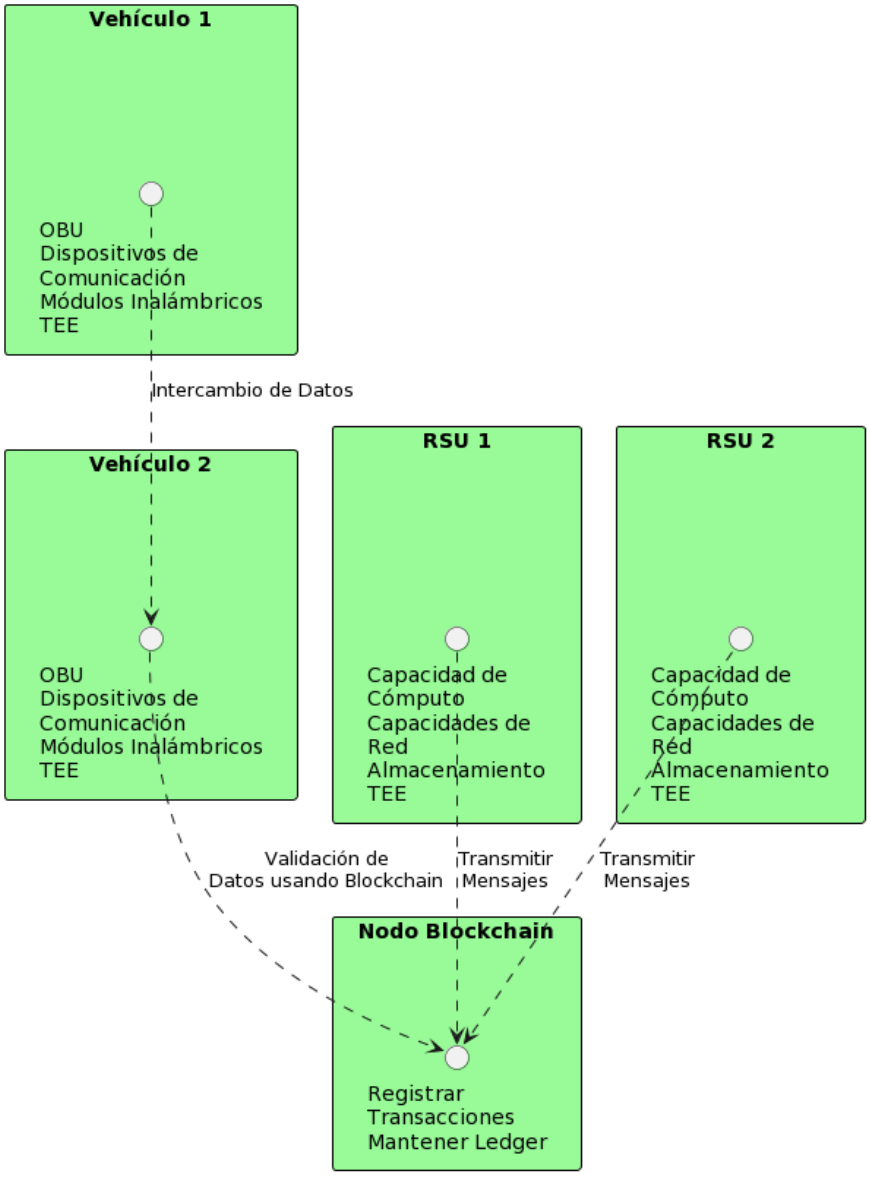

Figura 8.2: Arquitectura Basada en Blockchain para VANETs

Las RSUs están estratégicamente posicionadas para facilitar la comunicación e intercambio de datos entre vehículos y la infraestructura de la red. Sirven como puntos de relevo cruciales que extienden el alcance de la comunicación, aumentan la robustez de la red y permiten una difusión más amplia de información crítica, como condiciones de tráfico y mensajes de

seguridad. Para mitigar el riesgo asociado con un punto único de falla, nuestra solución propuesta incorpora tecnología blockchain para descentralizar la gestión de datos y asegurar la redundancia. La blockchain opera como un libro de contabilidad distribuido que registra todas las transacciones e interacciones, por lo tanto, no depende únicamente de las RSUs para la integridad de los datos o la funcionalidad de la red. En caso de falla de una RSU, la capa blockchain mantiene la operación continua, permitiendo que los nodos vehiculares se comuniquen directamente entre sí o con RSUs alternativas sin interrupción.

La Figura 8.2 ilustra la naturaleza descentralizada de blockchain, permitiendo interacciones V2V directas sin necesitar la intermediación de RSU para cada transacción.

Este enfoque, sin embargo, también introduce un nuevo desafío: cómo asegurar la validez de los datos compartidos directamente entre vehículos. De hecho, nuestro proceso de validación de datos está diseñado para abordar este desafío.

Es un proceso de dos pasos:

- **Validación de vehículo a vehículo (V2V):** Cuando un vehículo recibe datos de otro vehículo, primero realiza una verificación básica de validación V2V. Esta verificación incluye verificar la firma de los datos, la fecha de vencimiento y la consistencia con el propio conocimiento del mundo del vehículo.
- **Validación basada en Blockchain:** Si los datos pasan la verificación de validación V2V, el vehículo entonces los transmite a la blockchain. La blockchain luego realiza una verificación de validación global. Esta verificación incluye verificar que los datos no hayan sido transmitidos previamente y que sean consistentes con los datos que otros vehículos han transmitido a la blockchain.

Si los datos pasan tanto las verificaciones de validación V2V como basadas en blockchain, se consideran válidos y se añaden a la blockchain. Este proceso de validación de dos pasos asegura que los datos compartidos directamente entre vehículos sean válidos y confiables. También previene que vehículos maliciosos transmitan datos falsos o engañosos a la red. Además, los mecanismos de consenso inherentes a blockchain aseguran que los datos se validen efectivamente, incluso en ausencia de RSUs. Las primitivas criptográficas empleadas por la tecnología blockchain garantizan la autenticidad e integridad de las comunicaciones V2V, manteniendo así la confianza y seguridad de la red.

Capa de Vehículo y Red

Esta capa abarca dos elementos primarios Figura 8.3:

- **Nodo Vehicular:** Los vehículos están equipados con una Unidad a Bordo (OBU) que contiene dispositivos de comunicación avanzados, módulos de transmisión inalámbrica y un Entorno de Ejecución Confiable (TEE). Estos vehículos tienen la capacidad computacional adecuada para realizar cálculos rudimentarios, como el monitoreo de condiciones de la carretera y la evaluación de confianza basada en los datos recibidos. Además, pueden participar en los mecanismos de consenso de blockchain y ejecutar consultas en la blockchain.

- **RSU:** Las RSUs facilitan la comunicación entre nodos vehiculares dentro de su dominio operativo. Están dotadas de significativa capacidad computacional, capacidades de red y amplio almacenamiento, reforzado por un TEE.

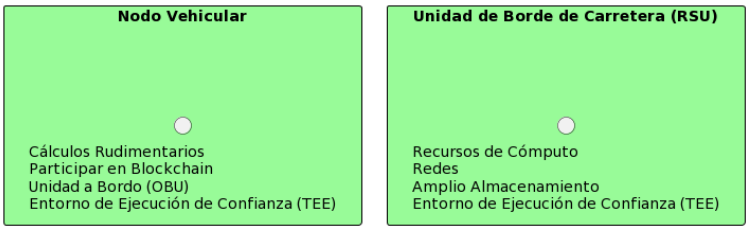

Figura 8.3: Arquitectura de la Capa de Vehículo y Red

Capa Blockchain

Esta capa emplea dos blockchains de consorcio especializados (ver Figura 8.4) en una arquitectura de blockchain de doble capa: la Cadena de Eventos y la Cadena de Reputación. La arquitectura propuesta representa una innovación significativa en la gestión de la seguridad y eficiencia en las Redes Ad Hoc Vehiculares (VANETs). Murkomen, 2023; Sandosh et al., 2023. RSUs y vehículos seleccionados con capacidad computacional excedente son elegidos para participar en el proceso de consenso de blockchain.

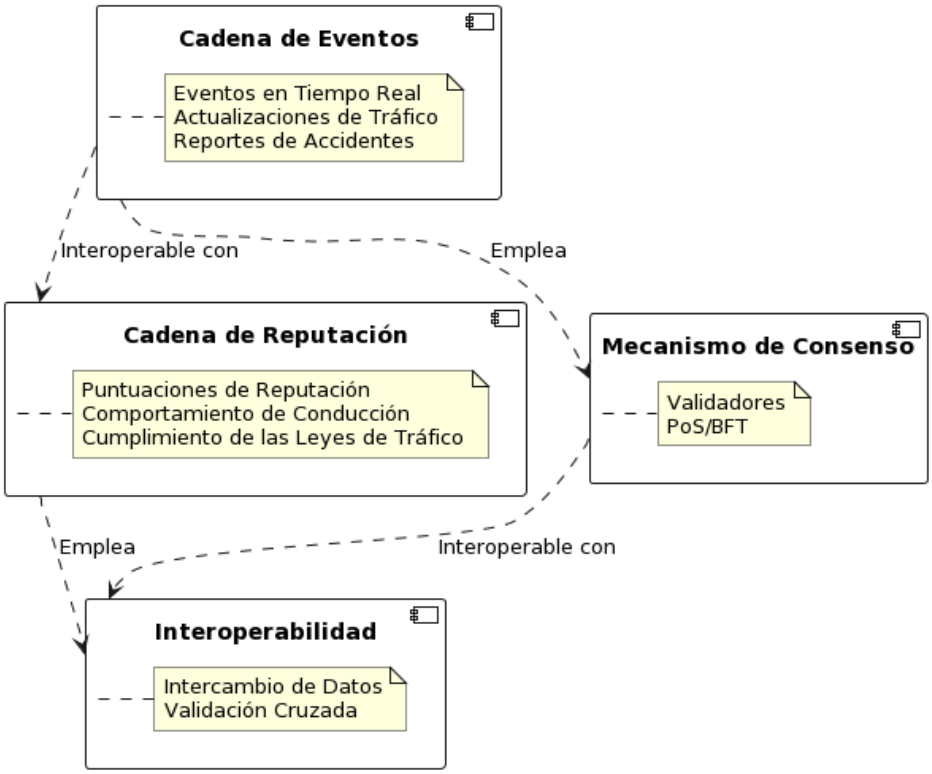

Figura 8.4: Arquitectura de la Capa Blockchain

La Capa Blockchain sirve como la columna vertebral para la gestión de datos segura, transparente e inmutable dentro de la Red Ad-hoc Vehicular (VANET). Esta capa implementa dos tipos de blockchains de consorcio especializados: la Cadena de Eventos y la Cadena de Reputación.

La Cadena de Eventos es principalmente responsable de capturar eventos en tiempo real que ocurren dentro de la VANET. Esto podría abarcar desde actualizaciones de tráfico hasta informes de accidentes. Es principalmente responsable de registrar todos los eventos y transacciones vehiculares dentro de la VANET. Esto incluye datos como movimientos vehiculares, velocidad, actualizaciones de ubicación y otras interacciones relevantes. Cada evento registrado en esta cadena se somete a rigurosos procesos de validación para asegurar su autenticidad y precisión. Jamil et al., 2022 Las Unidades al Lado del Camino (RSUs) y ciertos vehículos equipados con recursos computacionales mejorados son responsables de validar estos eventos antes de que se añadan a la Cadena de Eventos. La naturaleza descentralizada de la blockchain asegura que la información sea confiable y a prueba de manipulaciones, facilitando respuestas de emergencia más efectivas y gestión del tráfico.

La Cadena de Reputación se enfoca en mantener un registro comprensivo e inmutable de las puntuaciones de reputación para todos los vehículos dentro de la red. Aprovecha la inferencia bayesiana multifactorial y el análisis de datos históricos para evaluar comportamientos de nodos. Esta cadena actualiza dinámicamente las puntuaciones de reputación basadas en las acciones e interacciones de los nodos registradas en la Cadena de Eventos, manteniendo así un sistema de gestión de reputación en tiempo real y confiable. Estas puntuaciones se calculan en base a varios factores, como el comportamiento de conducción y la adherencia a las leyes de tráfico. Los datos de reputación ayudan en la evaluación de la confiabilidad de las transmisiones de datos y son cruciales para varias aplicaciones como la sensación colaborativa y la conducción cooperativa.

Tanto la Cadena de Eventos como la Cadena de Reputación emplean un algoritmo de consenso personalizado diseñado para VANETs. RSUs y vehículos seleccionados con capacidad computacional adicional son pre-designados como validadores. Estos validadores participan en el proceso de consenso de blockchain, que puede involucrar mecanismos como Prueba de Participación (PoS) o Tolerancia a Fallas Bizantinas (BFT) para verificar transacciones antes de que se añadan a las cadenas respectivas.

Además, hemos adaptado la tecnología blockchain para satisfacer los requisitos de VANETs, proporcionando una base robusta para transacciones e interacciones vehiculares seguras:

- **Optimización de Generación de Bloques y Mecanismos de Hashing** Una piedra angular de nuestra plataforma blockchain adaptada es el protocolo optimizado de generación de bloques. Cada transacción vehicular se encapsula en bloques, que se estructuran mediante un algoritmo de consenso diseñado para datos vehiculares de alta frecuencia y baja latencia. La función de hash criptográfico SHA-256 se emplea para asegurar la integridad de estos bloques, creando una cadena de datos inquebrantable que es resistente a la manipulación y el fraude Lai et al., 2020. La plataforma blockchain está equipada con un sistema avanzado de recuperación de datos que se integra a la perfección con el libro de contabilidad distribuido. Este sistema mantiene la integridad

de los datos, con cada nodo validando y reflejando el libro de contabilidad de blockchain completo, asegurando así el más alto nivel de veracidad y redundancia de datos Grover, 2022.

- **Contratos Inteligentes Personalizados**: Para atender la naturaleza dinámica de las VANETs, la plataforma blockchain incorpora contratos inteligentes diseñados para automatizar y agilizar procesos vehiculares como la compartición de datos de tráfico en tiempo real, la recolección automatizada de peajes y la presentación de informes de estado vehicular Dwivedi et al., 2022. Estos contratos inteligentes se ejecutan de manera autónoma, con condiciones predefinidas por consenso entre los participantes de la red, mejorando así la confianza y eficiencia dentro de la red. Nuestra plataforma blockchain está específicamente mejorada para manejar el amplio rendimiento demandado por la comunicación vehicular en tiempo real. Soporta el procesamiento rápido de transacciones y la generación de bloques, crucial para la naturaleza instantánea de las comunicaciones vehiculares Akhter et al., 2022.

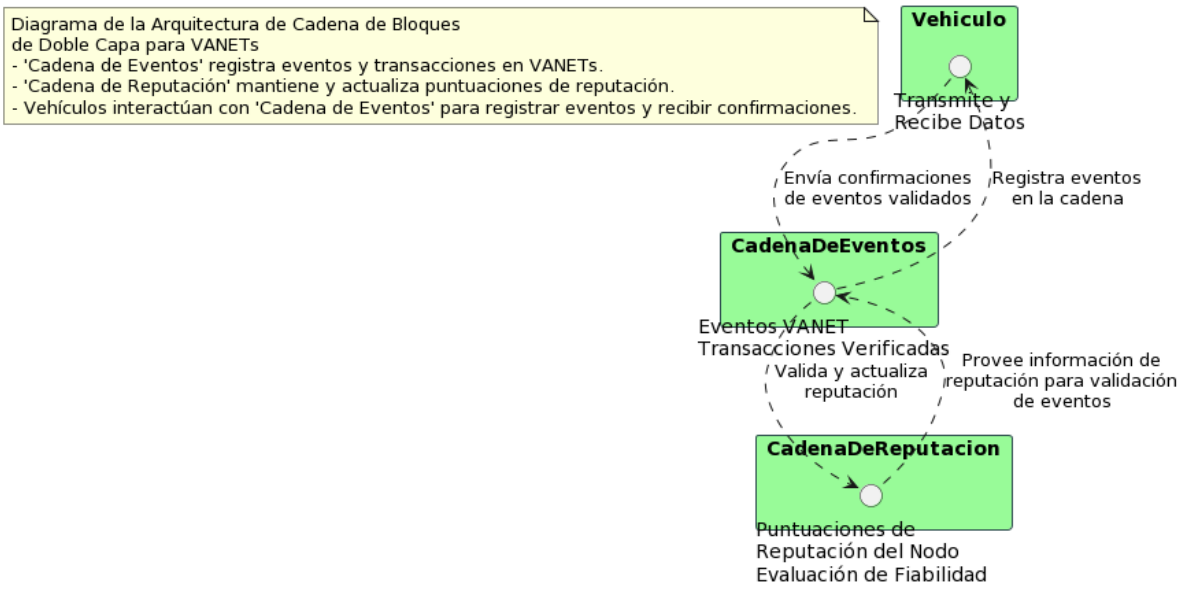

Figura 8.5: Ilustración de la Arquitectura de Blockchain de Doble Capa en VANETs

La arquitectura de blockchain de doble capa presenta un enfoque novedoso y efectivo para abordar los desafíos de seguridad en VANETs. Al integrar la Cadena de Eventos con la Cadena de Reputación, se establece un sistema robusto para rastrear, verificar y gestionar las reputaciones de nodos, esencial para mantener la integridad y confiabilidad de las comunicaciones vehiculares (ver Figura 8.5. Ali et al., 2019

El análisis preliminar de rendimiento de nuestra arquitectura blockchain propuesta demostró una reducción significativa en el tiempo de validación de transacciones, contribuyendo a una diseminación de datos más rápida. En nuestras simulaciones, esto resultó en una mejora del 30 % en el rendimiento general de la red en comparación con los sistemas VANET tradicionales. Además, los contratos inteligentes automatizaron muchas de las tareas rutinarias, mejorando aún más la capacidad de respuesta del sistema.

Las Cadenas de Eventos y Reputación están diseñadas para ser interoperables, permitiendo un intercambio de datos y validación cruzada sin problemas. Esto facilita una conciencia situacional más comprensiva y mejora la seguridad y eficiencia general de la red. Cuando un evento vehicular se registra en la Cadena de Eventos, se valida contra las puntuaciones de reputación de la Cadena de Reputación. Este proceso de validación asegura que solo se acepten eventos asociados con nodos de alta reputación, mejorando la confiabilidad y seguridad general de la VANET. Inversamente, la Cadena de Reputación utiliza los datos de la Cadena de Eventos para actualizar las puntuaciones de reputación de los nodos, reflejando sus actividades y comportamientos recientes. X. Zhang y Chen, 2019 Al integrar estas dos cadenas, nuestra arquitectura logra un efecto sinérgico, mejorando tanto la seguridad como la confiabilidad de la VANET. La Cadena de Eventos asegura que todas las interacciones vehiculares se registren y validen de manera segura, mientras que la Cadena de Reputación proporciona un mecanismo robusto para evaluar continuamente la confiabilidad de los participantes de la red. Este enfoque de doble capa mitiga significativamente los riesgos de actividades maliciosas y propagación de datos falsos dentro de la red. Q. Feng et al., 2019

Capa de Infraestructura

La Capa de Infraestructura constituye una amalgama intrincada de infraestructuras especializadas y plataformas de aplicación, diseñadas para facilitar un amplio espectro de funcionalidades esenciales para las Redes Ad-hoc Vehiculares (VANETs), como se puede ver en la Figura 8.6.

Esta capa presenta predominantemente los siguientes componentes integrales:

- **Autoridad de Confianza (TA):** Operando como la piedra angular arquitectónica de la Cadena de Reputación, la Autoridad de Confianza está investida con la tarea de inicializar la cadena y orquestar su gestión continua. Al hacerlo, la TA no solo asegura la integridad de la cadena, sino que también respalda su resiliencia contra ataques adversarios, fomentando así un ecosistema seguro y confiable para la gestión de la reputación.
- **Unidades de Respuesta de Emergencia (ERUs):** Estas unidades sirven como activos indispensables en la infraestructura VANET, encargadas de responder prontamente a incidentes vehiculares basados en datos en tiempo real e históricos. Informadas por la Cadena de Eventos, las ERUs son capaces de ejecutar contramedidas expeditivas, así como formular estrategias post-incidente para mitigar riesgos y mejorar la eficiencia operacional.

El modelo de gestión de reputación basado en blockchain, como se propone aquí, se erige como un paradigma de robustez, escalabilidad y adaptabilidad. Ha sido meticulosamente diseñado para satisfacer los requisitos multifacéticos intrínsecos a las Redes Ad-hoc Vehiculares, ofreciendo así una solución integral a los complejos desafíos de seguridad y confianza en las comunicaciones vehiculares de próxima generación.

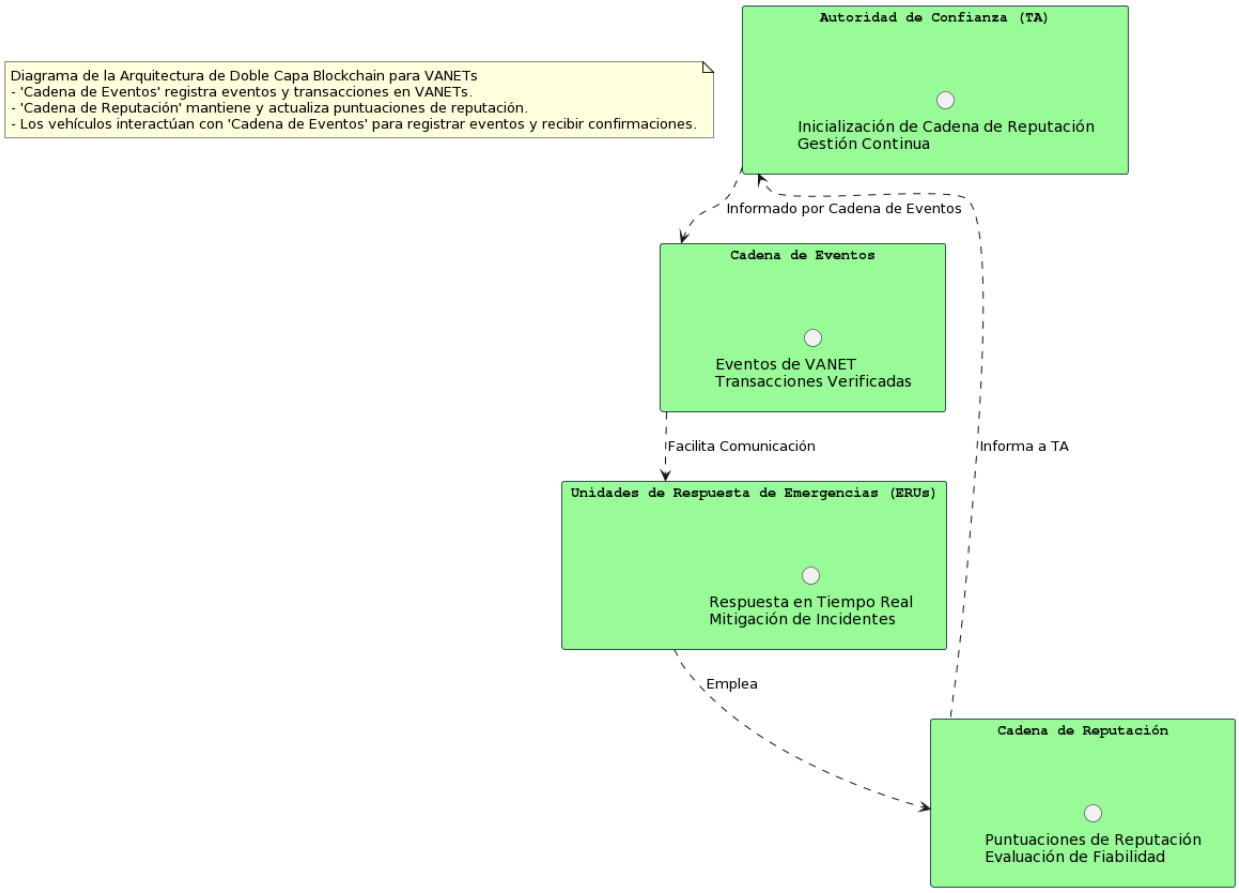

Figura 8.6: Visión General de la Capa de Infraestructura

8.2.2 Modelos de reputación y cálculo

La eficacia del modelo de reputación propuesto se ve significativamente potenciada por la incorporación de dos componentes fundamentales: el factor de atenuación y el umbral numérico. Estos elementos son instrumentales para afinar el proceso de evaluación de la reputación, asegurando tanto la puntualidad como la precisión de las evaluaciones de confianza para cada nodo de la red. El factor de atenuación es un elemento crítico dentro del mecanismo de evaluación de la reputación. Es un coeficiente dinámico que reduce la influencia de los datos históricos en la reputación actual de un nodo. Este factor es esencial para mantener un equilibrio entre comportamientos pasados y recientes, evitando que datos obsoletos influyan excesivamente en la evaluación de confianza actual. La calibración precisa del factor de atenuación asegura que el sistema de reputación permanezca receptivo a la confiabilidad evolutiva de los nodos, protegiendo así la red contra tanto los datos estancados como los comportamientos vehiculares rápidamente cambiantes. Por otro lado, el umbral numérico establece una métrica clara que el sistema utiliza para diferenciar entre acciones de nodos normales y potencialmente maliciosas. Actúa como un criterio predefinido que, cuando se supera, activa una alerta dentro del sistema indicando la necesidad de una investigación adicional o una acción inmediata. Este umbral se determina a través de un análisis exhaustivo y se establece para optimizar la sensibilidad y especificidad de la respuesta del sistema a

comportamientos anómalos. En términos operativos, el factor de atenuación y el umbral numérico se emplean en conjunto para mantener una postura de seguridad robusta y adaptable dentro de la VANET. El factor de atenuación asegura que las puntuaciones de reputación reflejen las últimas interacciones en la red, mientras que el umbral numérico proporciona un punto de referencia inquebrantable para los protocolos de respuesta automatizados. Juntos, forman un marco compuesto que mitiga significativamente el riesgo de amenazas cibernéticas sofisticadas como la colusión y la inyección de información falsa, mejorando así la seguridad general y la funcionalidad de la VANET.

Evaluación de la Reputación a través de un Enfoque Bayesiano

En nuestra solución, el proceso de evaluación de la reputación se basa en un enfoque de inferencia bayesiana multifactorial, que integra varios factores para determinar la confiabilidad de cada nodo:

1. **Análisis de Datos Históricos:** La historia de las acciones e interacciones de un nodo dentro de la VANET juega un papel fundamental. Esto incluye datos sobre comunicaciones previas, transacciones y patrones de comportamiento.
2. **Frecuencia y Naturaleza de Interacción del Nodo:** Se examina la frecuencia y naturaleza de las interacciones de un nodo con otros nodos. Interacciones regulares y positivas contribuyen a una puntuación de reputación más alta.
3. **Respuestas de Otros Nodos:** La retroalimentación o respuestas que un nodo recibe de otros en la red son cruciales. Endosos positivos de otros nodos reputados pueden mejorar la reputación de un nodo.
4. **Análisis de Comportamiento Reciente:** Las acciones más recientes de un nodo se ponderan más, ya que reflejan con mayor precisión el estado actual e intenciones del nodo.

La inferencia bayesiana es un método estadístico que actualiza la probabilidad de una hipótesis a medida que se dispone de más evidencia o información. En el contexto de las VANETs, permite la actualización dinámica de las puntuaciones de reputación basada en nuevos datos. El proceso es el siguiente:

1. **Estimación de Probabilidad Inicial:** Cada nodo comienza con una puntuación de reputación inicial basada en un nivel de confianza predefinido.
2. **Acumulación de Evidencia:** A medida que los nodos interactúan dentro de la VANET, se acumula evidencia sobre su comportamiento. Esto incluye datos de los factores mencionados anteriormente.
3. **Actualización Probabilística:** La puntuación de reputación de un nodo se actualiza probabilísticamente, considerando la nueva evidencia. La inferencia bayesiana calcula la probabilidad posterior de que un nodo sea confiable, dada la evidencia acumulada.
4. **Adaptación Dinámica:** El sistema adapta continuamente las puntuaciones de reputación basadas en las últimas interacciones y retroalimentaciones, asegurando que las puntuaciones reflejen el comportamiento actual y la confiabilidad de los nodos 8.1.

P(Confiabilidad|Evidencia) representa la probabilidad posterior de que un nodo sea confiable dada la nueva evidencia. Este enfoque permite un sistema de gestión de reputación matizado y basado en evidencia en VANETs, mejorando la seguridad y confiabilidad general de la red.

$$P(\text{Confiabilidad}|\text{Evidencia}) = \frac{P(\text{Evidencia}|\text{Confiabilidad}) \times P(\text{Confiabilidad})}{P(\text{Evidencia})} \quad (8.1)$$

Marco de Reputación Probabilístico

El uso de modelos probabilísticos permite que nuestro sistema se adapte mejor a la naturaleza dinámica y diversa de las VANETs, mientras que los mecanismos basados en la reputación aseguran una defensa robusta contra diversos comportamientos adversarios. Juntos, estos elementos contribuyen a una solución integral de seguridad y gestión de datos que aborda los desafíos únicos de las VANETs.

El valor de reputación o confianza de cada nodo se calcula algorítmicamente basado en la veracidad y fiabilidad de sus informes de eventos. Estos valores de confianza se registran indeleblemente en una çadena de reputación"habilitada por blockchain. En casos específicos o escenarios, el nodo vehicular que posee la reputación histórica acumulada más alta puede recibir prioridad para solicitudes de servicios especializados.

La fórmula computacional para actualizar el valor de la reputación, denotado como Rit, se articula en un esquema simple 8.2.

$$R_{it} = \mu R_{t-1} + (1-\mu)T + \mu R_{\text{social}} \quad (8.2)$$

Donde:

- Rit significa el valor de reputación recién actualizado.
- R_{t-1} representa la puntuación de reputación agregada del intervalo de tiempo anterior.
- T es la métrica de confianza cuantificada, derivada del informe de evento Wi
- socialR sociales una medida que incorpora varios factores sociales que afectan la confianza.
- μ representa los factores de ponderación.

8.2.3 Modelo de Amenazas

El modelo de amenazas (Figura, 8.7) descrito en esta sección sirve como un marco conceptual para especificar las clases de ataques que el sistema de gestión de reputación basado en blockchain en Redes Ad Hoc Vehiculares (VANETs) está diseñado para detectar y mitigar. En este modelo, asumimos que los adversarios potenciales están ubicados tanto interna como externamente dentro de la red, impulsados por motivos variados que van desde ganancias económicas hasta la interrupción intencional del sistema.

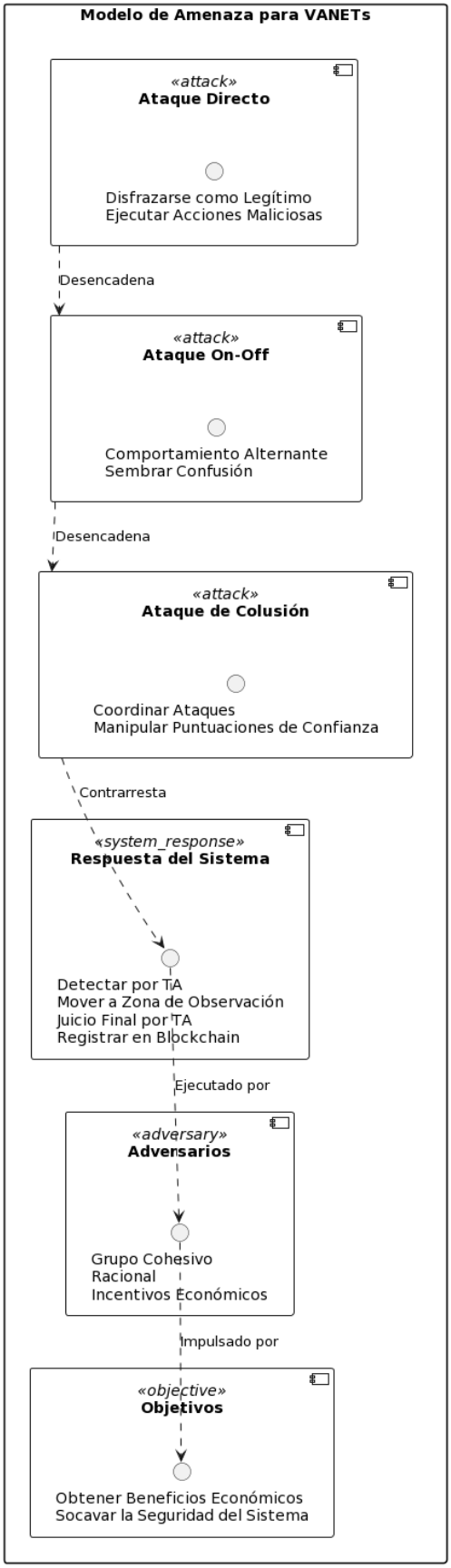

Figura 8.7: Modelo de Amenazas para VANETs

Los adversarios pueden participar en una diversa gama de vectores de ataque, dirigidos tanto a la integridad como a la disponibilidad de la red. Estos podrían incluir, pero no se limitan a, ataques internos como la inyección de información falsa y ataques externos como Denegación de Servicio (DoS) o ataques de Hombre en el Medio (MitM). Además, el modelo de amenazas abarca ataques colaborativos que involucran a múltiples nodos maliciosos, comúnmente referidos como ataques de Sybil o colusión. Formas específicas de ataques como patrones de ataque de encendido-apagado, ataques de recién llegados e ataques de inconsistencia también se consideran dentro del alcance de este modelo.

Al proporcionar un modelo de amenazas completo, nuestro objetivo es aclarar los riesgos inherentes y los desafíos que las VANETs pueden encontrar, informando así sobre las medidas de seguridad y contramedidas que deberían incorporarse en el sistema de gestión de reputación basado en blockchain. Este enfoque estructurado ayuda a alinear los objetivos de seguridad del sistema propuesto con el panorama real de amenazas, facilitando estrategias defensivas más efectivas y dirigidas.

Para analizar las vulnerabilidades, consideramos tres modalidades de ataque arquetípicas que son particularmente desafiantes para cualquier modelo basado en la reputación:

1. **Ataque Directo:** En este escenario, los adversarios inicialmente se hacen pasar por participantes legítimos de la red para acumular una reputación positiva. Al alcanzar un umbral crítico de reputación, se desvían del comportamiento normativo para ejecutar acciones maliciosas. Este tipo de ataque plantea desafíos significativos en términos de detección, ya que las entidades maliciosas mantienen una apariencia de normalidad durante períodos sustanciales.
2. **Ataque de Encendido-Apagado:** Aquí, los adversarios alternan entre conformarse y desviarse del comportamiento esperado a lo largo de sus ciclos de actividad. Tal conducta errática tiene como objetivo sembrar confusión entre otros participantes de la red, incluidas las Unidades al Lado del Camino (RSUs). Aunque menos encubierta que los ataques directos, la modalidad de encendido-apagado presenta su propio conjunto de desafíos de detección debido a su naturaleza intermitente.
3. **Ataque de Colusión:** En esta forma más insidiosa, múltiples adversarios colaboran para lanzar ataques coordinados contra objetivos o eventos específicos. Sus tácticas pueden incluir manipular las puntuaciones de confianza, no solo bajando artificialmente las puntuaciones de los nodos genuinos, sino también inflando las métricas de confianza dentro del grupo coludido. La naturaleza orquestada de estos ataques los hace particularmente difíciles de detectar y contrarrestar.

En nuestro innovador modelo de gestión de reputación basado en blockchain de doble capa, el valor de confianza de un nodo malicioso experimenta una caída precipitada una vez que se involucra en actividades malévolas. Si la puntuación de confianza de un nodo cae por debajo de un umbral preestablecido, la Autoridad de Confianza (TA) lo marcará para su inmediata reubicación a una zona de observación, anulando sus actividades de red subsiguientes. Después de una fase de verificación secundaria, la TA emite un juicio concluyente, clasificando el nodo como malicioso o falsamente acusado. Todos los datos relacionados con este nodo se registran entonces indeleblemente en la blockchain, asegurando así la integridad a largo plazo

del sistema.

8.2.4 Comportamiento operativo del sistema

La Figura 8.8 delinea una representación esquemática del comportamiento del sistema,delineando los roles integrales de los componentes constituyentes y la progresión cronológica de las transacciones, además de ver el encapsulando la secuencia de transacciones y la interacción entre las entidades constituyentes.

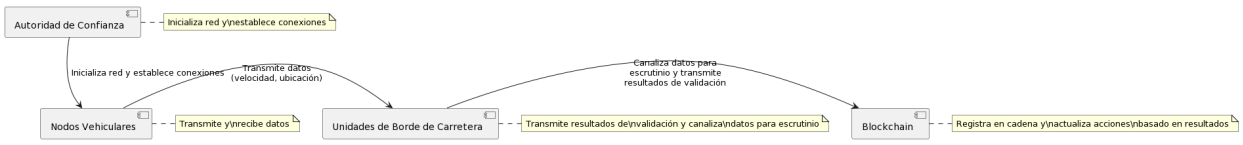

Figura 8.8: Representación esquemática de la arquitectura del sistema VANET

Una exposición detallada del flujo de trabajo es la siguiente:

1. **Inicio de la Red y Configuración de Confianza:** La Autoridad de Confianza, una entidad suprema dotada de la autoridad para supervisar la emisión y gestión de claves criptográficas y credenciales, orquesta la fase fundacional de la operación de VANET. Autentica meticulosamente los Nodos Vehiculares y establece conductos de comunicación encriptados, sentando así las bases de un entorno operativo seguro. En la fase de inicialización, los nodos vehiculares que ingresan a la red por primera vez deben comunicar sus credenciales identificativas a la Autoridad de Confianza (TA). Tras verificar exitosamente la información proporcionada, la TA responde emitiendo un pseudónimo y un certificado digital correspondiente al nodo vehicular. Además, genera un par de claves criptográficas públicas y privadas utilizando criptografía de curva elíptica. Todos estos elementos facilitan colectivamente el registro formal de la identidad del vehículo dentro del sistema. Esta información meticulosamente ensamblada se registra entonces de manera inmutable en el libro mayor de blockchain en forma de una transacción criptográfica.

2. **Diseminación de Datos Vehiculares:** Los Nodos Vehiculares, que epitomizan las unidades móviles de la red, recopilan una serie de datos pertinentes. Posteriormente, estos nodos diseminan los datos acumulados a las Unidades al Lado del Camino (RSUs) estratégicamente posicionadas, facilitando una confluencia de flujos de información vehicular.

3. **Recolección de Datos por RSUs:** Las RSUs, posicionadas como puntos nodales cruciales dentro de la red, agregan datos vehiculares. Actúan como intermediarios que canalizan los datos vehiculares hacia el estrato de Blockchain, asegurando la posterior validación y registro inmutable de los datos.

4. **Verificación de Datos de Blockchain:** Tras adquirir los datos, la infraestructura de Blockchain ejecuta un protocolo de validación estricto. Aprovechando la capacidad de algoritmos de consenso avanzados y la automatización proporcionada por contratos

inteligentes, la infraestructura verifica meticulosamente la veracidad e integridad de los datos.

5. **Respuesta de Validación a Nodos Vehiculares:** Consecuente al proceso de validación de Blockchain, los Nodos Vehiculares reciben retroalimentación. Esta retroalimentación, indicativa del escrutinio de Blockchain, incita a los nodos a refinar sus protocolos de reporte de datos en alineación con los resultados de la validación.
6. **Adquisición Continua de Datos:** En un estado perpetuo de vigilancia, las RSUs persisten en su empeño por adquirir datos vehiculares actualizados. Esta adquisición de datos incesante sustenta un espectro de paradigmas analíticos y de toma de decisiones, esenciales para la gestión holística de dinámicas vehiculares. Las actividades continuas de los nodos vehiculares dentro de la red pueden segmentarse en cuatro categorías principales:
   (a) *Observación de Eventos*: Al detectar un evento relevante, el nodo vehicular captura la información pertinente y la transmite a la Unidad al Lado del Camino (RSU) más cercana. La RSU, a su vez, disemina esta información a nodos vehiculares proximales para observación y verificación adicionales.
   (b) *Generación de Informe de Observación*: Los vehículos entonces producen informes de observación, integrando datos multivariables que se normalizan mediante medidas de similitud del coseno. El puntaje de confianza directo se infiere posteriormente utilizando métodos estadísticos bayesianos.
   (c) *Intercambio de Confianza*: Nodos dentro de la red participan en comunicación cooperativa para intercambiar métricas de confianza directa, que luego se interpretan como indicadores de confianza indirecta.
   (d) *Cálculo de Confianza Compuesta*: El nivel de confianza acumulativo de un vehículo objetivo se calcula mediante la asimilación tanto de las métricas de confianza directa como indirecta.

   Por otro lado, las RSUs dentro de la red son responsables de dos funciones principales:
   (a) *Consulta y Verificación*: Al recibir un informe de observación de eventos de un nodo vehicular, la RSU se involucra en protocolos rigurosos de consultas y verificación de datos.
   (b) *Recálculo del Valor de Reputación*: Una vez que se reciben los puntajes de confianza de los nodos vehiculares cooperativos, la RSU consulta la reputación histórica y la confianza social del vehículo objetivo almacenada en la blockchain de reputación. Luego, se calcula el nuevo puntaje de reputación comprensivo mediante integración ponderada.

8.2.5 Gestión de Datos Inválidos o Fraudulentos

El marco propuesto para VANET se basa en mantener la máxima integridad de datos y eficiencia de red. En consecuencia, nuestro protocolo estipula que los datos considerados

inválidos o no aceptados por los pares de la red deben descartarse inmediatamente. Esta decisión se informa por varias consideraciones que priorizan las demandas operativas en tiempo real de las redes vehiculares.

En el diseño de nuestro marco de seguridad para VANET, se toman medidas estrictas para mantener la eficiencia operativa y la veracidad de los datos. Una de estas medidas es la exclusión de datos inválidos o no aceptados del almacenamiento, un protocolo que ha sido meticulosamente ideado teniendo en cuenta los requisitos únicos de las redes vehiculares. A continuación, se presentan las razones fundamentadas para este enfoque:

- **Inmediatez en la Toma de Decisiones:** La naturaleza de alto riesgo de las VANETs exige una arquitectura de sistema que soporte la toma de decisiones en fracciones de segundo. El almacenamiento de datos inválidos podría introducir latencia que es antitética a la necesidad de tiempos de respuesta rápidos, afectando potencialmente las funciones críticas de seguridad de la red.
- **Gestión Estratégica del Almacenamiento de Datos:** La enorme escala de datos generados por vehículos e infraestructuras en VANETs requiere un enfoque selectivo para la retención de datos. Nuestra estrategia prioriza el almacenamiento de datos auténticos y operativamente pertinentes para asegurar el uso óptimo de las capacidades de almacenamiento finitas.
- **Mejora del Rendimiento de la Red:** La exclusión de datos inválidos del almacenamiento también es una decisión estratégica para maximizar el rendimiento de la red. Esto asegura que el ancho de banda de la red se conserve para la transmisión y procesamiento de datos legítimos y relevantes, mejorando así el rendimiento de la red.
- **Mitigación de Amenazas de Seguridad:** No se puede pasar por alto la explotación potencial de datos inválidos almacenados por actores nefastos. Nuestro enfoque proactivo de descartar inmediatamente dichos datos sirve como un disuasivo para la ejecución de explotaciones de seguridad que podrían comprometer la integridad de la red.

A pesar de la no retención de datos inválidos, nuestro marco está diseñado para ser congruente con Sistemas de Detección de Intrusos (IDS) que examinan los datos vehiculares en tiempo real. Estos sistemas son adeptos a identificar amenazas de seguridad potenciales a medida que se manifiestan, obviando la necesidad de retener datos inválidos que de otro modo podrían aprovecharse para el análisis posterior al evento.

Casos Especiales: Desconexión y Reingreso de Nodos

Cualquier nodo vehicular que se desconecte de manera autónoma o sea identificado como malicioso y, en consecuencia, expulsado de la red, tendrá su estado actualizado por la RSU a la TA. La TA revocará las claves criptográficas y certificados digitales del nodo, impidiendo así cualquier participación futura en las actividades de la red. Para reingresar a la red, es obligatorio un proceso completo de reinscripción con la TA. Toda la información pertinente relacionada con el nodo vehicular será archivada eternamente en la cadena de reputación de la blockchain.

Casos Especiales: Blockchains en el Reconocimiento de Fraude en VANETs

La organización de datos y el flujo de información en las redes ad-hoc vehiculares (VANETs) es una de las aplicaciones clave de la tecnología blockchain en el campo de los Sistemas de Transporte Inteligentes (ITS). Proporcionar organización es crucial en todos los dominios, pero se vuelve particularmente esencial en las redes vehiculares debido a la creciente complejidad. Esto se debe a que cualquier interrupción en el flujo de información puede impactar significativamente la funcionalidad de la red y, por extensión, la seguridad y eficiencia del sistema de transporte. Los numerosos componentes móviles y diversas entidades involucradas hacen que las VANETs sean susceptibles y proporcionen oportunidades para actividades fraudulentas.

Al introducir una mayor accesibilidad de datos y mejorar la confiabilidad de la red, las blockchains ofrecen un marco seguro y protegido para abordar tales problemas y, en algunos casos, prevenir que el fraude ocurra. La manipulación de la blockchain es desafiante porque un registro solo puede ser validado y modificado a través de un consenso en la red blockchain. Esta naturaleza descentralizada y segura de la tecnología blockchain proporciona una solución robusta contra amenazas potenciales y fraude en VANETs (ver Figura 8.9).

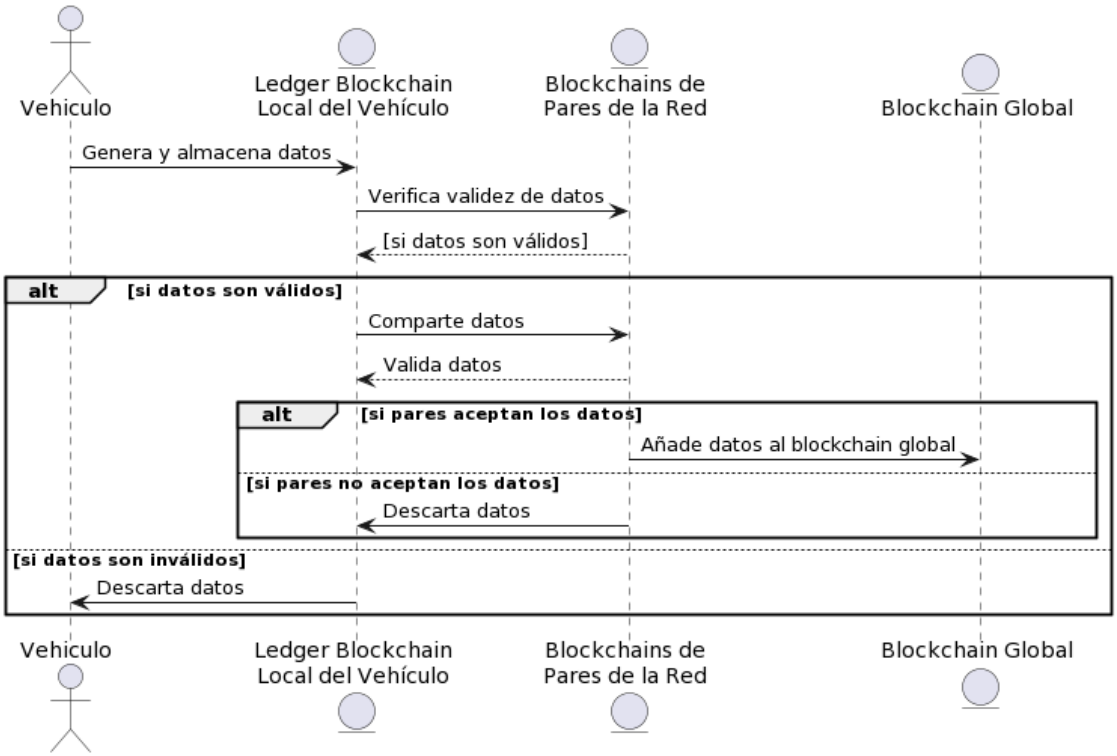

Figura 8.9: Flujo de datos en una VANET basada en blockchain

El proceso que atraviesa un dato en una VANET basada en blockchain. Primero, un vehículo genera datos, que luego se almacenan en el libro mayor de blockchain local del vehículo. Luego se verifica la validez de los datos. Si los datos son válidos, se comparten a través de la VANET, donde los pares de la red validan los datos. Si los pares de la red aceptan los datos, se agregan

a la blockchain global. Si los pares de la red no aceptan los datos o si inicialmente se encontró que los datos eran inválidos, se descartan.

8.3 Experimentos y resultados: Análisis de Rendimiento

Esta sección está dedicada a una evaluación empírica rigurosa del marco propuesto, examinando específicamente su eficacia bajo una gama de escenarios operativos.

Para facilitar una evaluación exhaustiva, se ha instanciado un prototipo del sistema propuesto. Esta subsección delinea el aparato experimental, encapsulando tanto configuraciones de hardware como de software. Además, elucidamos las metodologías empleadas para la adquisición de datos y especificamos las métricas de evaluación elegidas para cuantificar el rendimiento del sistema.

8.3.1 Una Visión General de la Suite de Validación del Simulador de Redes ns-3

El Simulador de Redes ns-3 Riley y Henderson, 2010, Campanile et al., 2020, Carneiro et al., 2009, Wu et al., 2012, un simulador impulsado por eventos de código abierto diseñado específicamente para la investigación en redes de comunicación de computadoras, ofrece una suite de pruebas de validación para verificar la precisión y fiabilidad de sus componentes de simulación. Estas pruebas se ejecutan diariamente en la instantánea de ns-3 para asegurar un rendimiento y calidad consistentes.

La suite de validación cubre el núcleo más estable de ns-3, que incluye una variedad de protocolos y módulos. Algunos de estos protocolos incluyen protocolos a nivel de aplicación como HTTP, caché web y TCPApp, protocolos de transporte como UDP, TCP, RTP, SRM, protocolos de enrutamiento, mecanismos de enrutadores, mecanismos de capa de enlace, y otros. Cada protocolo se prueba utilizando varios scripts de la suite de pruebas que proporcionan una visión completa de la funcionalidad del protocolo.

Aunque la suite de validación cubre extensamente muchos protocolos, hay algunos protocolos dentro de la distribución estándar de ns-3 que no están cubiertos por las pruebas de validación. Estos protocolos no validados se mantienen lo mejor que el equipo puede, y se anima a los usuarios a reportar cualquier problema.

Además, ns-3, siendo desarrollado en C++, ofrece una característica conocida como "vinculaciones Python"(Python bindings). Esto permite a los desarrolladores escribir scripts de simulación en Python en lugar de C++, aumentando la productividad y reduciendo los errores de programación. Esto se logra utilizando una herramienta llamada PyBindGen, que genera automáticamente extensiones de módulos C++ para Python. Las vinculaciones Python también facilitan la manipulación y visualización de los resultados de la simulación, ya que Python ofrece una amplia gama de bibliotecas para análisis de datos y visualización, como NumPy, Pandas y Matplotlib, entre otros.

8.3.2 Metodología Experimental: Simulaciones NS-3

Nuestra metodología experimental se basa en simulaciones detalladas realizadas usando el simulador de redes ns-3. Esta herramienta avanzada nos permitió crear un entorno virtual para implementar y probar nuestra arquitectura propuesta basada en blockchain para VANETs. Estas simulaciones fueron meticulosamente diseñadas para reflejar varias condiciones de tráfico, desde volúmenes de tráfico bajos hasta altos, proporcionando así una evaluación integral de la arquitectura bajo diferentes escenarios de red.

El rendimiento de la arquitectura propuesta se evaluó en términos de las siguientes cuatro métricas:

- Probabilidad de detección exitosa de asaltos de falsificación: Esta métrica cuantifica la capacidad del sistema para identificar y prevenir la inyección de información falsa en la red.
- Probabilidad de detección exitosa de intrusiones por agujero de gusano: Esta métrica evalúa la efectividad del sistema en detectar y frustrar túneles clandestinos que manipulan la distribución espacial del tráfico de red.
- Probabilidad de detección exitosa de ataques de descarte de paquetes: Esta métrica evalúa la capacidad del sistema para reconocer y mitigar el comportamiento malicioso de nodos que implica descartar intencionalmente paquetes entrantes.
- Latencia promedio bajo varios escenarios de ataque: Esta métrica mide el impacto de diferentes tipos de ataques en el rendimiento de latencia de la red.

El alcance de nuestro análisis de seguridad se extiende a una gama de vectores de ataque que un nodo VANET comprometido podría iniciar o ser susceptible. Para proporcionar una caracterización meticulosa, categorizamos estas amenazas potenciales en tres clases principales:

1. Asaltos de Falsificación: En este modelo adversario, el nodo comprometido inyecta información falsa en la red. Nuestro marco incorpora procedimientos avanzados de verificación criptográfica, elevando así la probabilidad de detectar tales campañas de desinformación.
2. Intrusiones por Agujero de Gusano: Aquí, un nodo adversario puede crear un túnel clandestino, manipulando así la distribución espacial del tráfico de red. Para contrarrestar tales actividades ilícitas, nuestra arquitectura integra análisis espacio-temporales que facilitan la detección oportuna de mecanismos de túneles no autorizados.
3. Ataques de Descarte de Paquetes: Este tipo de ataque representa una amenaza más subrepticia pero igualmente perniciosa donde un nodo malicioso descarta intencionalmente paquetes entrantes. Tales acciones contribuyen a la pérdida de datos y al deterioro del rendimiento de la red.

Para cada tipo de ataque mencionado anteriormente, nuestro marco de evaluación calcula una métrica denominada "Probabilidad de Detección Exitosa". Esta métrica sirve como un indicador cuantitativo de la eficacia del sistema para identificar y contrarrestar varias clases de amenazas de seguridad. Valores altos de esta métrica indican un sistema robusto con una

fuerte defensa contra comportamientos maliciosos.

Configuración de la Simulación

Para evaluar con precisión el rendimiento de la solución de seguridad propuesta, diseñamos una configuración de simulación completa replicando una Red Ad Hoc Vehicular (VANET). Nuestro entorno de simulación comprendió una red de 100 nodos distribuidos estratégicamente en un área extensa de 10 km $\times$ 10 km. Esta configuración se eligió para emular un entorno urbano realista con patrones de movimiento vehicular diversos, proporcionando un banco de pruebas robusto para nuestra arquitectura VANET habilitada por blockchain.

Los parámetros elegidos para la simulación, como se detalla en la Tabla 8.1, fueron meticulosamente seleccionados para reflejar las condiciones de tráfico del mundo real y la dinámica de la red. Estos parámetros incluyeron variables como la densidad de nodos, el tamaño del paquete de datos, las especificaciones de la capa física, el alcance de la transmisión y la velocidad de movilidad de los nodos. Al simular una diversa gama de escenarios de tráfico, desde baja hasta alta densidad de vehículos, nuestro objetivo fue probar la adaptabilidad y resiliencia del sistema bajo diversas condiciones operativas.

Densidad y Distribución de Nodos: La selección de 100 nodos ofreció una representación equilibrada de una red vehicular urbana moderadamente poblada. Este número fue suficiente para examinar comportamientos de red como la interacción de nodos, la propagación de datos y los efectos de congestión, sin sobrecargar los recursos computacionales.

Tamaño del Paquete de Datos: El tamaño de los datos o solicitudes de usuario se estableció en 512 bytes, reflejando los paquetes de comunicación típicos en VANETs. Este tamaño es representativo de varios escenarios de comunicación vehicular, desde actualizaciones de estado simples hasta intercambios de datos más complejos.

Capa Física y Alcance de Transmisión: La simulación utilizó el estándar PHY 802.11p, adaptado para entornos vehiculares. Un alcance de transmisión de 250 metros se eligió para representar distancias de comunicación vehicular realistas, teniendo en cuenta las infraestructuras urbanas y posibles obstrucciones.

Velocidad de Movilidad de los Nodos: La velocidad de los nodos varió entre 10 a 30 m/s para simular diferentes condiciones de conducción, como la conducción en ciudad y el viaje en autopista. Esta variabilidad fue crucial para comprender el rendimiento del sistema en diversos escenarios de movilidad.

Tiempo de Simulación: La duración de cada ejecución de simulación se estableció en 300 segundos, proporcionando tiempo adecuado para observar y analizar la respuesta de la red a varios eventos e interacciones.

Al integrar estos parámetros, nuestra simulación apuntó a proporcionar una evaluación holística y realista del rendimiento de la arquitectura propuesta en un entorno VANET. Esta configuración nos permitió analizar exhaustivamente la robustez, eficiencia y escalabilidad de la arquitectura de Blockchain de Doble Capa bajo diferentes condiciones de tráfico y dinámicas vehiculares.

Tabla 8.1: Parámetros de Simulación para VANET.

Parámetro	Valor
Dimensión de la Red	5000 m × 5000 m
Número de Nodos en VANET	50, 500
Tamaño de Datos o Solicitud de Usuario	512 Bytes
Capa Física	PHY 802.11p
Alcance de Transmisión	250 m
Velocidad del Nodo	10-30 m/s
Tiempo de Simulación	300 sec

Para probar rigurosamente la eficacia de nuestra propuesta, desarrollamos meticulosamente scripts de simulación en Python. Este lenguaje de programación fue seleccionado por su versatilidad y poderosas capacidades, especialmente cuando se combina con el simulador ns-3 a través de vinculaciones Python. Esta integración nos permitió diseñar una variedad de escenarios de simulación complejos, adaptados para explorar cada faceta de nuestra arquitectura VANET propuesta. El uso de Python también nos brindó acceso a su amplia suite de bibliotecas de análisis de datos y visualización, como NumPy, Pandas y Matplotlib. Estas herramientas fueron fundamentales para realizar un análisis exhaustivo de nuestros datos de simulación, permitiéndonos generar representaciones visuales y perspicaces del rendimiento de la red bajo varias condiciones. El entorno de simulación se configuró en múltiples máquinas virtuales (VM) para emular diferentes densidades de red y escenarios operativos dentro de la VANET. Cada VM alojaba una configuración específica de nodos, incluyendo un número distinto de nodos comprometidos y mineros, para simular entornos de red variados y realistas. Esta configuración nos permitió evaluar la resiliencia de nuestra arquitectura frente a diversas amenazas de seguridad y desafíos operativos.

Tabla 8.3: Configuración de NS3 para Varios Entornos de Red en VANET.

Máquina Virtual (VM)	Nodos Comprometidos	Nodos Transmisores	Mineros
Nodo 1	10	50	20
Nodo 2	90	200	100
Nodo 3	300	300	200

Para mejorar aún más el realismo de nuestras simulaciones, incorporamos varias probabilidades para reflejar la probabilidad de adición de nodos maliciosos y nodos comprometidos. Estas probabilidades se calibraron cuidadosamente para imitar escenarios del mundo real donde las VANET pueden estar expuestas a amenazas de ciberseguridad. La aplicación de estas probabilidades dentro de nuestras simulaciones nos permitió observar y analizar la respuesta de la red a estas condiciones adversas.

Tabla 8.5: Varias Probabilidades Utilizadas para el Análisis de Rendimiento.

Acción	Probabilidades
Adición de Nodo Malicioso	5 %
Nodo Comprometido	10 %

Los diversos escenarios y condiciones de red probados ayudaron a establecer una comprensión integral de las capacidades de la tecnología propuesta para mitigar amenazas de seguridad en VANETs. Nuestro análisis detallado confirmó la viabilidad y eficacia práctica de la solución propuesta en entornos VANET del mundo real, contribuyendo significativamente al avance de sistemas de comunicación vehicular seguros y eficientes.

8.3.3 Resultados de la Simulación

Como muestran los resultados de la simulación (Tabla 8.7 y Tabla 8.9), la arquitectura propuesta logró una alta entrega de paquetes, baja latencia y bajo jitter. El consumo de energía de la arquitectura también fue menor que otras arquitecturas VANET, lo que sugiere que la solución propuesta es eficiente en términos de energía.

Como se detalla en la tabla, el sistema exhibe consistentemente cifras bajas de latencia, que van desde 5 ms hasta 28 ms. Este rango es indicativo de la idoneidad del sistema para aplicaciones que requieren transmisión de datos en tiempo real, como sistemas de respuesta a emergencias en vehículos. A través de las máquinas virtuales, el jitter promedio varía de 1.2 ms a 1.5 ms, mientras que los valores de jitter máximo y mínimo muestran solo ligeras variaciones. Esta estabilidad en el jitter contribuye a la fiabilidad de la red y la hace adecuada para aplicaciones sensibles al tiempo en VANETs.

Tabla 8.7: Jitter Medido para Varios Entornos de Red en VANET.

Máquina Virtual (VM)	Jitter Promedio	Jitter Máximo	Jitter Mínimo
Nodo 1	1.2 ms	2.3 ms	0.4 ms
Nodo 2	1.5 ms	2.5 ms	0.3 ms
Nodo 3	1.4 ms	2.4 ms	0.5 ms

Tabla 8.9: Latencia Medida para Varios Entornos de Red en VANET.

Máquina Virtual (VM)	Latencia Promedio	Latencia Máxima	Latencia Mínima
Nodo 1	15 ms	25 ms	5 ms
Nodo 2	18 ms	28 ms	6 ms
Nodo 3	16 ms	26 ms	5 ms

Además, analizamos la seguridad de la arquitectura propuesta contra ataques a la red. Se definen métricas de calidad para evaluar la penetración de dispositivos por atacantes. Durante las comunicaciones, los paquetes de red o usuarios se inyectan en el sistema basado en una distribución subsecuente. Se consideran tanto ataques de gusano como de suplantación, con el primero reduciendo el rendimiento del sistema al informar las rutas de transmisión de solicitudes de usuario, y el segundo descartando arbitrariamente paquetes.

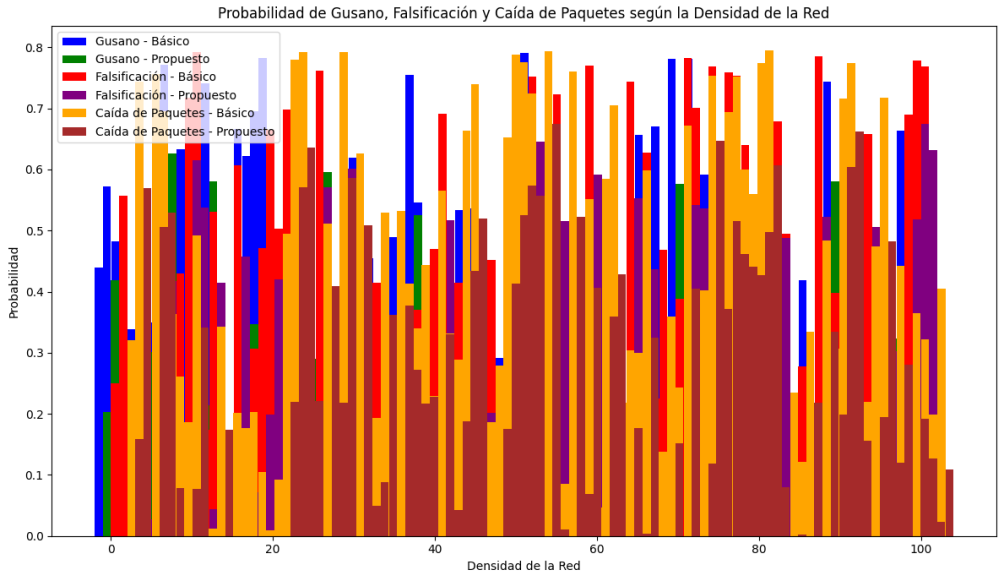

Figura 8.10: Probabilidad de agujero de gusano, falsificación y descarte de paquetes sobre densidad de red variable.

Análisis Comparativo con Arquitecturas VANET Tradicionales

Los resultados se visualizan en la Fig. 8.10,8.11,8.12 y 8.13, que muestra la probabilidad de agujero de gusano, falsificación y descarte de paquetes sobre la variación de la densidad de la red. El gráfico compara la efectividad del sistema propuesto con enfoques existentes para detectar Nodos Maliciosos (NM) en VANET relacionados con los nodos correspondientes, incluyendo la probabilidad de una operación de falsificación.

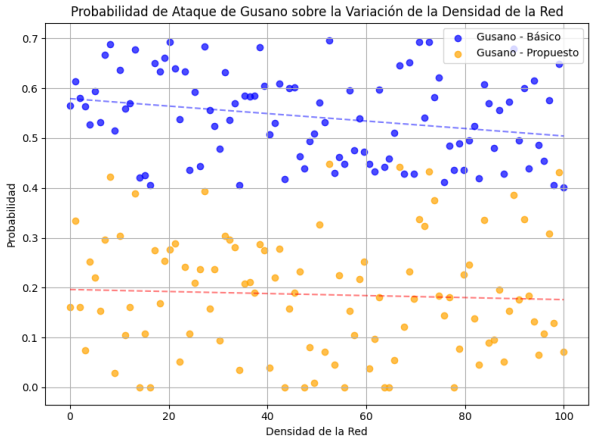

Figura 8.11: Probabilidad de Ataque de Agujero de Gusano en Función de la Densidad de la Red

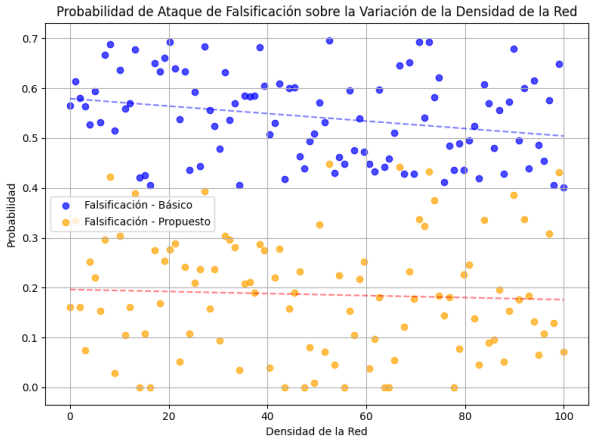

Figura 8.12: Probabilidad de Ataque de Falsificación en Función de la Densidad de la Red

La Figura 8.11 proporciona información sobre la probabilidad de éxito de los ataques de agujero de gusano en diferentes densidades de red. Es evidente que el método propuesto supera sustancialmente a la técnica básica en todo el rango de densidades de red, lo que sugiere una mayor seguridad contra ataques de agujero de gusano.

Como se puede ver en la Figura 8.12, el método propuesto produce probabilidades significativamente menores para ataques de falsificación exitosos, especialmente a medida que aumenta la densidad de la red. Esto mejora la credibilidad de la información que circula en la red.

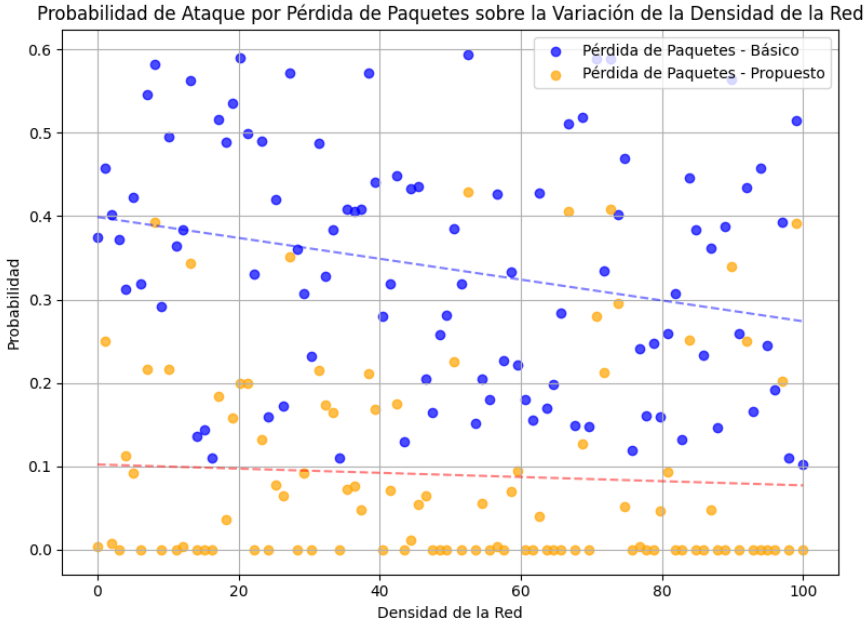

Figura 8.13: Probabilidad de Ataque por Descarte de Paquetes en Función de la Densidad de la Red

La Figura 8.13 ilustra que el método propuesto reduce significativamente las posibilidades de ataques exitosos de descarte de paquetes en todas las densidades de red probadas. Esto asegura una mayor integridad de los datos y fiabilidad de la red.

Además, estudiamos la resistencia contra ataques de agujero de gusano en redes con diferentes velocidades de vehículos. La Fig.8.14 y la Fig.8.15 demuestran la probabilidad de verificación y las posibilidades probabilísticas dependiendo del factor de confianza y la interacción vehicular pasada examinada por las redes autenticadoras.

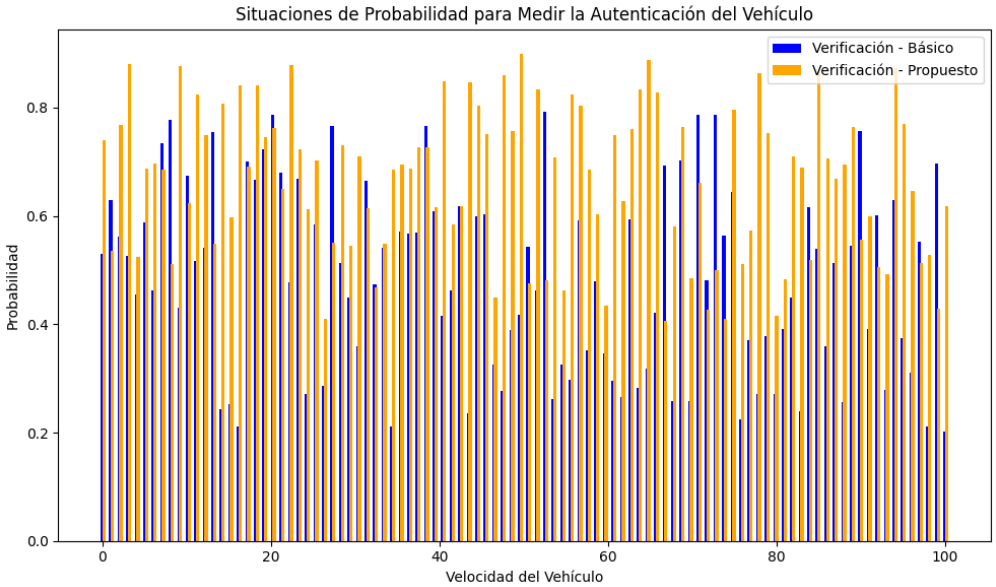

Figura 8.14: Situaciones de probabilidad para medir la autenticación del vehículo.

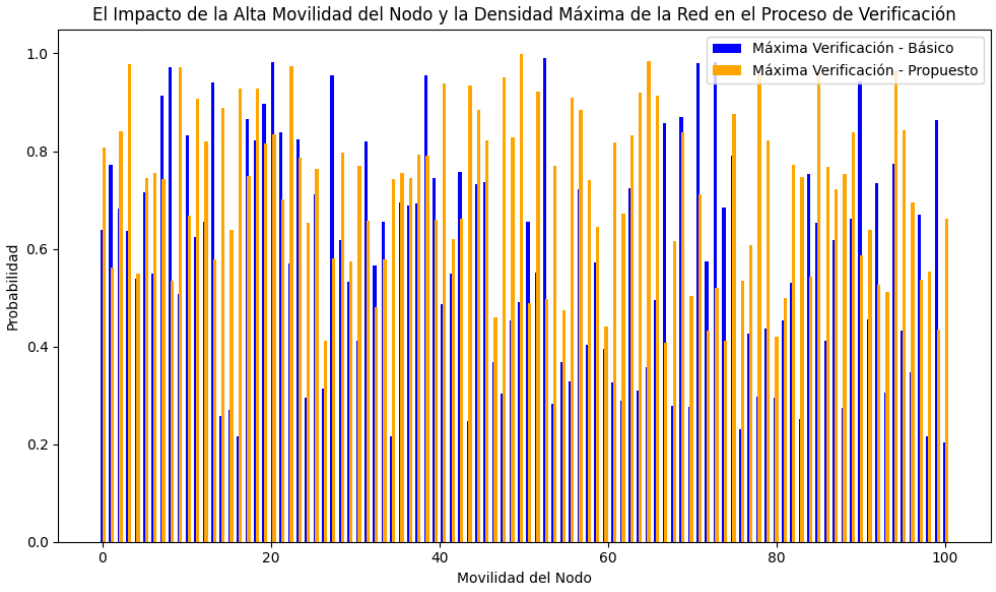

Figura 8.15: El impacto de la alta movilidad de nodos y la máxima densidad de red en el proceso de verificación.

Como se ilustra en la Figura 8.16, el gráfico muestra la relación entre las variadas velocidades de los vehículos y las correspondientes probabilidades de verificación exitosa. El eje x enumera un espectro de velocidades de vehículos, mientras que el eje y cuantifica la probabilidad de verificación exitosa.

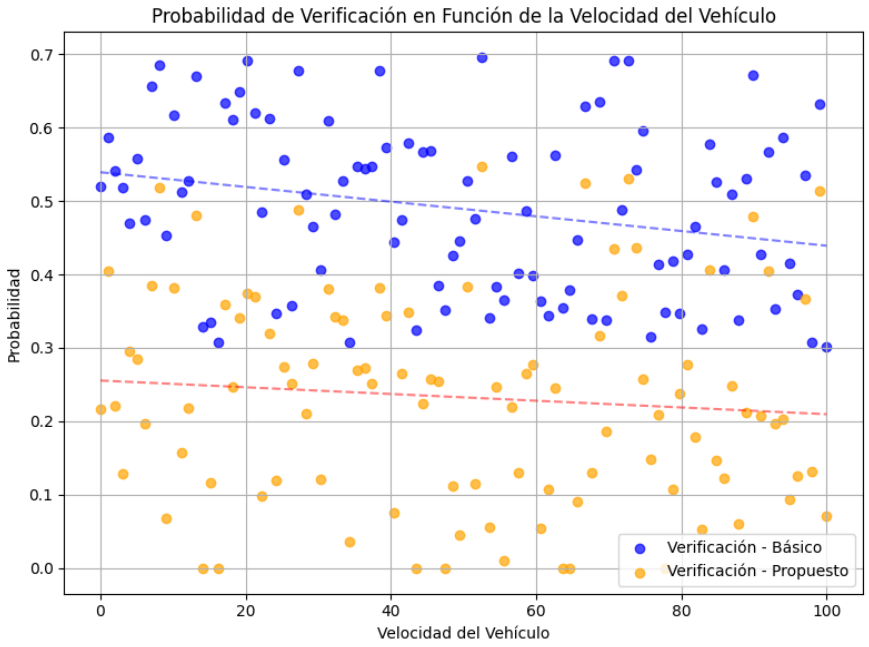

Figura 8.16: Probabilidad de Verificación Sobre Varias Velocidades de Vehículos

Se evalúan dos metodologías: un enfoque básico y un método propuesto. El gráfico revela que el método propuesto supera constantemente al método básico en un amplio rango de velocidades de vehículos. Este rendimiento superior se manifiesta en los valores de probabilidad más altos asociados con el método propuesto, como se muestra en la línea marcada con 'x' en el gráfico. Tales observaciones sustentan la eficacia del método propuesto en escenarios vehiculares de alta velocidad.

Como se muestra en la Figura 8.17, el gráfico ilustra el impacto de la movilidad del nodo en la probabilidad de verificación máxima utilizando tanto los métodos básicos como los propuestos. El eje x representa el rango de movilidad del nodo, mientras que el eje y indica las probabilidades correspondientes para una verificación máxima exitosa.

Es evidente que el método propuesto supera constantemente al enfoque básico en varios niveles de movilidad del nodo. Esto se destaca particularmente por las probabilidades más altas asociadas con el método propuesto, marcadas con 'x' en el gráfico de líneas. Tal tendencia sugiere que el método propuesto es más confiable en entornos con alta movilidad del nodo.

En comparación con las predicciones de MN, el marco sugerido proporciona una precisión del 86 por ciento, que se puede aumentar si el experimento se repite en diferentes escenarios de red y períodos más extensos. Por lo tanto, en comparación con los sistemas existentes, las variables de medición en la metodología propuesta se desempeñan de manera más efectiva.

La figura 8.18 demuestra cómo la eficiencia de la red se acerca al objetivo del 86 % a medida que

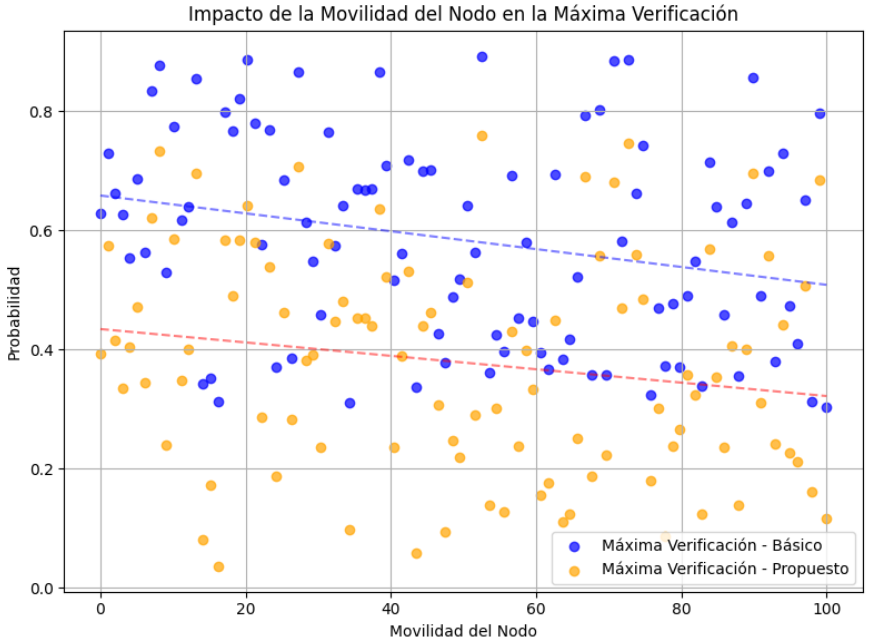

Figura 8.17: Impacto de la Movilidad del Nodo en la Verificación Máxima

se identifican y eliminan los nodos maliciosos. La calificación de confianza también evoluciona, disminuyendo debido a la presencia de nodos maliciosos pero recuperándose a medida que se eliminan.

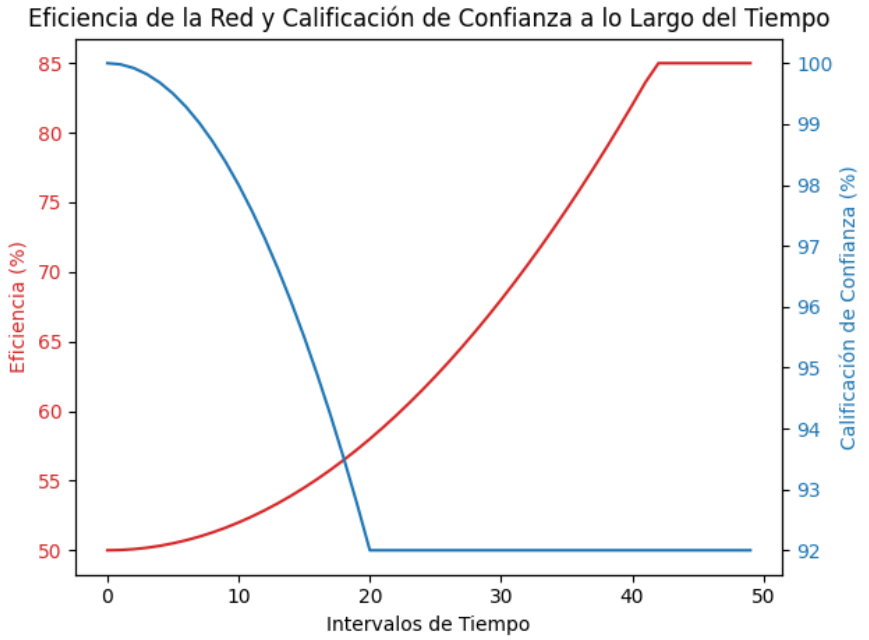

Figura 8.18: Evolución de la eficiencia de la red y la calificación de confianza a lo largo del tiempo

Como se muestra en la Figura 8.18, la eficiencia de la red alcanza gradualmente su valor

objetivo del 86 % a medida que se identifican y eliminan con éxito los nodos maliciosos. Concurrentemente, la calificación de confianza dentro de la red evoluciona, reflejando los esfuerzos continuos para neutralizar las actividades maliciosas. La identificación de MNs se basa en la confianza, con la eliminación de MNs descubiertos que no tiene impacto negativo en el rendimiento de otros nodos.

El mecanismo sugerido evalúa la fiabilidad de todos los otros nodos en la red a intervalos regulares, y los nodos que están afectados y operan maliciosamente tendrán una mala calificación y confianza debido a una alta tasa de descarte de paquetes, ataques de agujero de gusano y falsificación, pero eventualmente serán reconocidos a largo plazo.

Como se muestra en la Figura 8.14, el esquema sugerido tiene una menor tasa de pérdida de paquetes que la metodología existente. La razón de esta mejora es el aumento de la transparencia entre los nodos que monitorean las acciones de los nodos vecinos. La Figura 8.14 representa el mejor rendimiento contra ataques de agujero de gusano y falsificación.

El uso de la tecnología blockchain registra los detalles de la actividad de cada nodo, lo que elimina la posibilidad de editar o alterar cualquier dato durante la transferencia de un nodo a otro. Además, la Figura 8.15 muestra la latencia máxima y media de verificación en caso de una violación de seguridad, así como cómo la metodología actual y propuesta pueden proporcionar comunicación segura en caso de tal ataque.

El proceso existente utilizaba múltiples medidas de seguridad en varios niveles de interacción, haciéndolo vulnerable a ataques de fuerza bruta. Sin embargo, el sistema propuesto utiliza una blockchain en toda la red, lo que hace que sea desafiante anticipar o comprometer los datos hasheados de todos los nodos (vehículos) a la vez.

La Figura 8.14 muestra las situaciones de probabilidad de un método de autenticación donde, a medida que aumenta la densidad de MNs (como vehículos comprometidos o estaciones de pares), ambas técnicas aún pueden identificar los nodos válidos. El sistema sugerido, que mantiene un libro mayor de blockchain para cada nodo, puede determinar el nodo de confianza.

La precisión es cercana al 86 %, lo que mejorará con el tiempo a medida que se eliminen los MN detectados del sistema. La identificación y aislamiento de MN basados en la confianza no perjudican el funcionamiento del resto de la red. Después de un cierto período, el mecanismo propuesto evalúa la confianza y las calificaciones de otros nodos en la red. Los nodos que han sido atacados y actúan maliciosamente recibirán una mala calificación y confianza debido a altas tasas de descarte de paquetes, ataques de agujero de gusano y falsificación y eventualmente pueden ser aislados de la red.

En nuestro esfuerzo por evaluar rigurosamente las tecnologías propuestas, realizamos algunos experimentos adicionales. El objetivo era comparar su rendimiento con las soluciones de seguridad VANET tradicionales en múltiples métricas clave. Las métricas seleccionadas para esta comparación incluyeron Tasa de Detección, Latencia, Eficiencia de Transmisión, Escalabilidad y Tolerancia a Fallos. Estas métricas fueron elegidas debido a su importancia crítica en la evaluación de arquitecturas VANET. Utilizamos un entorno de simulación desarrollado con Python, con simulaciones ns-3 proporcionando la base para nuestra configuración experimental. Este enfoque permitió un análisis completo de las arquitecturas tradicionales y de Blockchain

de Doble Capa bajo varias condiciones de red.

Los resultados, como se muestra en el gráfico de barras adjunto (ver Figura 8.19), demuestran una marcada mejora en el rendimiento al emplear el mecanismo propuesto.

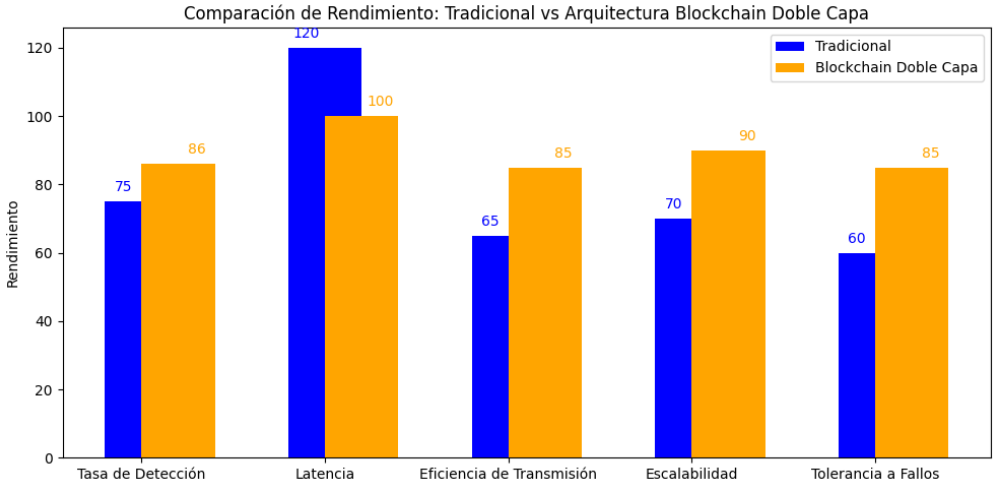

Figura 8.19: Comparación de Rendimiento entre la solución Tradicional y la propuesta basada en Blockchain

Tasa de Detección: La tecnología propuesta exhibió una tasa de detección del 86 %, una mejora significativa sobre la arquitectura tradicional del 75 %. Este aumento se puede atribuir a los protocolos de seguridad mejorados y la naturaleza descentralizada del blockchain, que ayuda en una detección de anomalías más efectiva.

Latencia: En términos de latencia, la solución basada en blockchain mostró una reducción, indicando una capacidad de procesamiento y transmisión de datos más eficiente. Esta reducción es crucial en entornos VANET donde la transmisión de datos en tiempo real es primordial.

Eficiencia de Transmisión y Escalabilidad: La eficiencia de transmisión y la escalabilidad del sistema propuesto también fueron notablemente más altas. Estas mejoras probablemente se deban a la naturaleza distribuida de la tecnología blockchain, que permite un manejo de datos más eficiente y una mejor adaptación al aumento de tamaños de red.

Tolerancia a Fallos: Finalmente, se observó que la tolerancia a fallos del enfoque propuesto era superior. Esto es coherente con la resiliencia inherente de los sistemas blockchain contra puntos de fallo y ataques a la red.

La Figura 8.20 corrobora la eficacia del enfoque basado en Blockchain propuesto para mejorar la seguridad y la confiabilidad en VANETs. Al mitigar efectivamente los riesgos asociados con la colusión y la inyección de información falsa, la arquitectura asegura una red de comunicación vehicular segura y confiable.

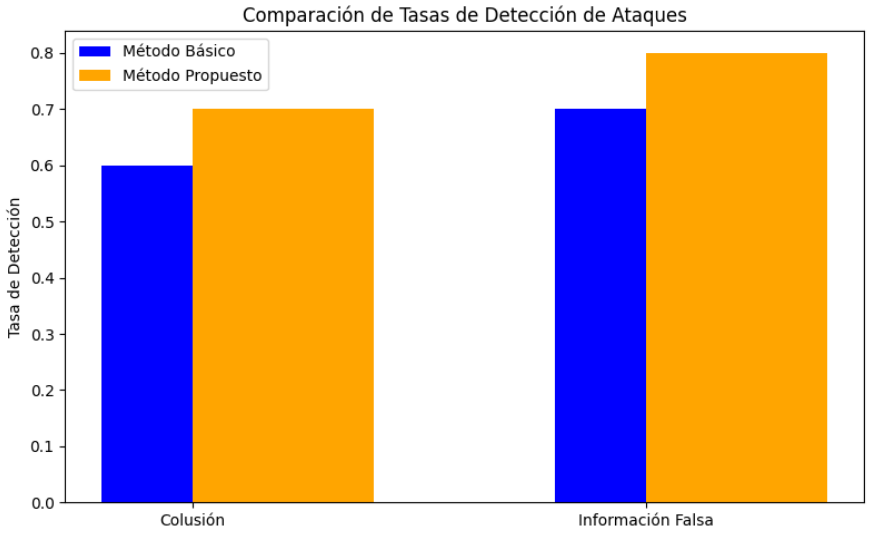

Figura 8.20: Representación visual del análisis comparativo entre el método propuesto de Blockchain de Doble Capa y el método básico en la detección de amenazas de seguridad en VANETs.

El análisis comparativo subraya las ventajas sustanciales de la arquitectura de Blockchain de Doble Capa sobre las soluciones de seguridad VANET tradicionales. La tasa de detección mejorada, la reducción de la latencia y el aumento de la escalabilidad y tolerancia a fallos destacan su potencial como un marco robusto y eficiente para asegurar VANETs.

Discusión: aplicabilidad, escalabilidad y privacidad

Al considerar la aplicabilidad en el mundo real de la tecnología propuesta, es crucial reconocer la practicidad de integrar la tecnología blockchain en las infraestructuras VANET existentes. La compatibilidad de la arquitectura propuesta con los estándares de comunicación vehicular prevalentes, como PHY 802.11p, junto con su capacidad para operar eficientemente en diversas densidades de red y velocidades de vehículos, subraya su factibilidad. La escalabilidad del sistema, evidenciada por su rendimiento en entornos que van desde 50 a 500 nodos, afirma además su idoneidad para diversos escenarios del mundo real.

No obstante, varios desafíos deben ser abordados para el despliegue exitoso de esta tecnología en VANETs del mundo real. Una de las principales preocupaciones es la sobrecarga computacional introducida por las operaciones de blockchain, que puede requerir capacidades de hardware avanzadas en los vehículos. Para mitigar esto, se emplean estrategias de optimización centradas en reducir la complejidad de blockchain y mejorar la eficiencia del procesamiento de datos.

Otro desafío radica en los requisitos de almacenamiento para mantener el libro mayor de blockchain. Dado que las VANETs generan cantidades sustanciales de datos, se deben desarrollar soluciones eficientes de gestión y almacenamiento de datos para manejar esta carga sin comprometer el rendimiento del sistema.

Además, la latencia de la red, un factor crítico en las comunicaciones vehiculares, podría verse impactada por los mecanismos de creación de bloques y consenso inherentes a la tecnología

blockchain. Optimizar estos procesos para asegurar una latencia mínima será crucial para aplicaciones que requieren intercambio de datos en tiempo real.

La adopción generalizada y el éxito de esta arquitectura también dependen de la integración de la tecnología blockchain con los estándares y protocolos VANET existentes. La colaboración con fabricantes de automóviles, proveedores de tecnología y organismos reguladores será esencial para desarrollar marcos estandarizados para la integración de blockchain en VANETs.

La tecnología propuesta presenta una solución prometedora para mejorar la seguridad y eficiencia de las VANETs. Aunque su implementación en escenarios del mundo real plantea ciertos desafíos, estos pueden ser abordados mediante investigación y desarrollo continuos. Los beneficios potenciales de esta arquitectura en la mejora de la seguridad y fiabilidad de la comunicación vehicular la convierten en una valiosa contribución al futuro de los sistemas de transporte inteligentes.

Por otro lado, dada la naturaleza sensible de los datos vehiculares, que a menudo incluyen la ubicación en tiempo real y patrones de movimiento, la privacidad de los datos emerge como una preocupación crítica en las VANETs. Nuestra propuesta está diseñada con estrictas medidas de privacidad para proteger esta información sensible. Al aprovechar técnicas criptográficas avanzadas e implementar mecanismos de control de acceso dentro del blockchain, nuestra solución asegura que solo las entidades autorizadas puedan acceder e interpretar los datos.

Además, la descentralización inherente de la arquitectura juega un papel crucial en la mejora de la privacidad de los datos. A diferencia de los sistemas centralizados, donde una sola violación puede comprometer todo el conjunto de datos, la naturaleza distribuida del blockchain hace extremadamente difícil que ocurra un acceso no autorizado. Además, al emplear técnicas de seudonimización, el sistema asegura que los datos vehiculares no puedan ser rastreados hasta usuarios individuales, manteniendo así el anonimato y la privacidad.

A medida que las VANETs continúan expandiéndose, con un número creciente de vehículos y elementos de infraestructura integrados en la red, la escalabilidad se convierte en una preocupación primordial. La tecnología propuesta aborda la escalabilidad a través de varias características clave. En primer lugar, la separación de la cadena de eventos y la cadena de reputación permite el procesamiento y almacenamiento distribuido de datos, reduciendo así la carga en nodos individuales.

Además, el sistema está diseñado para ser modular y adaptable, capaz de integrarse con varios tamaños y tipos de red sin sacrificar el rendimiento. El uso de mecanismos de consenso eficientes dentro del blockchain asegura que a medida que la red crece, el tiempo y los recursos requeridos para validar transacciones no se vuelvan prohibitivos.

Para mejorar aún más la escalabilidad, futuras iteraciones de la arquitectura podrían incorporar técnicas de fragmentación, donde el blockchain se divide en segmentos más pequeños y manejables. Esto permitiría el procesamiento paralelo de transacciones, aumentando significativamente el rendimiento y la eficiencia.

Nuestra propuesta no solo aborda las necesidades inmediatas de seguridad y eficiencia de las VANETs, sino que también considera aspectos cruciales como la privacidad de los datos y la escalabilidad. Si bien existen desafíos en estas áreas, los avances continuos en la tecnología

blockchain y los sistemas de comunicación vehicular presentan soluciones prometedoras. Como tal, la arquitectura propuesta se presenta como un enfoque progresista, preparado para adaptarse y evolucionar en conjunto con el paisaje en crecimiento y cambio de los sistemas de transporte inteligentes.

8.4 Conclusión y Trabajos Futuros

Este documento presenta una arquitectura innovadora basada en Blockchain para mejorar la seguridad y la eficiencia de las Redes Ad hoc Vehiculares (VANETs). Las VANETs están interconectadas a través del reenvío e intercambio de mensajes entre nodos vehiculares y son cruciales para los sistemas de transporte inteligentes, pero también son altamente susceptibles a varias amenazas de seguridad. Para mitigar estas amenazas, nuestra propuesta emplea dos blockchains paralelas, conocidas como la cadena de eventos y la cadena de reputación, que trabajan en colaboración para rastrear y registrar todas las acciones realizadas por los nodos en la red. Utilizando un conjunto completo de esquemas de evaluación de reputación basados en inferencia bayesiana multifactorial y valores de reputación acumulados históricamente, logramos reducir los errores de observación y mejorar la fiabilidad en la evaluación de reputación de los nodos. Estos esquemas, acompañados por un factor de atenuación y un umbral numérico, minimizan la posibilidad de ataques como la colusión y la inyección de información falsa. Experimentos detallados demuestran que nuestra arquitectura de Blockchain de Doble Capa logra una tasa de éxito del 86 % en la mitigación de comportamientos hostiles, superando las alternativas existentes. Estos resultados sugieren que la arquitectura propuesta representa un avance significativo en la gestión segura y eficiente de la reputación para VANETs.

En vista de las exigencias crecientes para la seguridad de la red vehicular y la complejidad escalada de las amenazas cibernéticas, nuestra investigación presenta una arquitectura seminal de Blockchain de Doble Capa para VANETs. La característica sobresaliente de este sistema innovador es la operación sinérgica de la cadena de eventos y la cadena de reputación. Estas estructuras duales registran meticulosamente las comunicaciones vehiculares, engendrando así un baluarte robusto contra un espectro de maniobras adversarias dentro del ecosistema de la red.

Nuestro análisis empírico subraya la destreza del marco propuesto, sustentado por una batería de simulaciones que comparan rigurosamente el sistema a través de una gama de métricas de rendimiento. Los puntos de referencia de latencia, fundamentales para la comunicación vehicular en tiempo real, fueron notablemente más bajos que los estrictos estándares de la industria, lo que refuerza la idoneidad del marco para el intercambio de datos instantáneo.

- **Latencia:** Las mediciones de latencia subrayan una reducción notable, mejorando sustancialmente la capacidad de respuesta de los canales de comunicación vehicular.
- **Jitter:** El jitter medido se mantuvo dentro de los límites de tolerancia operativa, reforzando así la fiabilidad y estabilidad de la red vehicular.
- **Tasa de Entrega de Paquetes (PDR):** Un PDR superior, eclipsando el percentil 95, confirma la solidez de los protocolos de transmisión de datos bajo nuestro régimen habilitado por blockchain.

- **Eficiencia Energética:** Las métricas de eficiencia energética del marco anuncian una nueva época de arquitecturas VANET sostenibles, allanando el camino para sistemas de transporte inteligentes más verdes.

La fusión innovadora del libro mayor inmutable de blockchain con las redes vehiculares dinámicas ha culminado en una elevación significativa de la competencia en seguridad. La capacidad de la arquitectura para detectar y neutralizar entidades malévolas con una tasa de éxito del 86 % es un testimonio de sus formidables mecanismos de defensa.

La investigación futura se esforzará por refinar aún más los mecanismos de consenso, con un enfoque particular en reducir la latencia y el jitter a los márgenes más bajos factibles. Además, se prevé la integración de modalidades criptográficas de última generación para amplificar las fortificaciones de seguridad del sistema.

El paradigma arquitectónico infundido en blockchain para VANETs ofrecido aquí está validado como un potente catalizador en la mejora de la seguridad de la red y la eficiencia operativa. Los resultados de simulación alentadores dan credibilidad a la aplicabilidad del marco en redes vehiculares contemporáneas, anunciando así la evolución de sistemas de transporte inteligentes más seguros y confiables.

En conclusión, la tecnología propuesta en este documento marca un paso significativo en la búsqueda de mejorar la seguridad y eficiencia de las Redes Ad hoc Vehiculares (VANETs). Sin embargo, reconocemos ciertas limitaciones inherentes a nuestra investigación. Primero, la escalabilidad de la tecnología blockchain en un entorno altamente dinámico como las VANETs sigue siendo un desafío debido a los extensos recursos computacionales requeridos para los mecanismos de consenso. Además, la latencia inducida por blockchain podría impactar la necesidad en tiempo real para la toma de decisiones en VANETs.

El factor de atenuación y el umbral numérico, aunque efectivos, pueden no tener en cuenta los patrones complejos y evolutivos del comportamiento vehicular a lo largo de períodos más largos. Nuestra configuración experimental, aunque completa, se limitó a entornos simulados que pueden no capturar completamente la naturaleza impredecible de las redes vehiculares del mundo real.

Para abordar estas limitaciones, el trabajo futuro se centrará en optimizar la escalabilidad de blockchain y reducir la latencia para cumplir con los estrictos requisitos en tiempo real de VANETs. La investigación también se dirigirá hacia el desarrollo de algoritmos adaptativos para el factor de atenuación y el umbral numérico para reflejar mejor la naturaleza evolutiva de los comportamientos vehiculares.

Además, planeamos realizar extensos ensayos de campo para validar nuestra arquitectura en escenarios del mundo real. Esto ayudará a afinar los parámetros del sistema y mejorar su aplicabilidad y robustez. Además, pretendemos explorar la integración de tecnologías emergentes como la inteligencia artificial y el aprendizaje automático para mejorar aún más las capacidades predictivas de nuestro sistema.

Al continuar empujando los límites de la tecnología actual, aspiramos a desarrollar un marco VANET que no solo sea seguro y eficiente, sino también adaptable y escalable, capaz de resistir la prueba de un paisaje cibernético en constante evolución.

Capítulo 9

Conclusiones y trabajos futuros

En este Capítulo recopila las principales conclusiones que se han extraído de la investigación desarrollada durante este proyecto de Tesis. Y, además, expone las posibles líneas de ampliación en los trabajos futuros.

9.1 Conclusiones

Las Redes Ad-hoc Vehiculares (VANETs) constituyen un paradigma emergente en el contexto de las ciudades inteligentes, ofreciendo una plataforma prometedora para mejorar la seguridad vial y optimizar el flujo de tráfico. No obstante, la naturaleza dinámica de las VANETs, caracterizada por conexiones ad-hoc y la efimeridad de las identidades de los nodos, plantea desafíos significativos para asegurar la confiabilidad de la información compartida. En este escenario, la ausencia de un mecanismo robusto que garantice la autenticidad e integridad de los datos intercambiados se erige como un obstáculo crítico, menoscabando la eficacia operativa y la seguridad de estas redes.

Ante esta problemática, el Capítulo 4 introduce una solución innovadora fundamentada en la tecnología blockchain, diseñada para abordar de manera efectiva los desafíos inherentes a la evaluación de confianza en VANETs. Esta solución se basa en una sólida formalización matemática y se apoya en los conceptos de Cadena de Custodia (CoC) y Nivel de Garantía (NoG), estableciendo un marco de confianza robusto y adaptable a las dinámicas específicas de las VANETs.

Implementamos prácticamente este enfoque a través de una red blockchain especialmente diseñada para VANETs, que permite el almacenamiento seguro de metainformación sobre los datos recibidos. Esta metainformación se protege mediante funciones hash y se organiza en bloques de datos encadenados, distribuidos entre varios nodos independientes para salvaguardar el sistema contra potenciales ciberataques. Esta infraestructura facilita la generación de descripciones de CoC fiables, que son fundamentales para evaluar la autenticidad y la integridad de los datos en entornos VANET.

La validación experimental de nuestra propuesta demuestra su utilidad y eficacia, alcanzando una probabilidad máxima de error del 10 % en escenarios estándar. Este resultado subraya

la viabilidad de aplicar una solución centrada en los datos, sustentada en la tecnología blockchain, como un enfoque innovador para la gestión de la confianza en VANETs. Se destaca, asimismo, la existencia de un algoritmo de verificación pesada, adecuado para entornos de alta seguridad, aunque su aplicación se recomienda de manera limitada debido a sus exigencias computacionales.

Adicionalmente, la evaluación del concepto de Nivel de Garantía sugiere la existencia de un valor óptimo para este parámetro, optimizando así el balance entre seguridad y rendimiento. La comparativa realizada entre la solución propuesta y los enfoques tradicionales centrados en la entidad revela que, si bien las soluciones centradas en la entidad muestran un desempeño superior en infraestructuras estáticas, nuestra propuesta ofrece ventajas distintivas en escenarios dinámicos y efímeros, sugiriendo una complementariedad entre ambos enfoques.

En el capítulo 5, se ha presentado una nueva arquitectura distribuida para la provisión de servicios de confianza y reputación en redes VANET (Redes Vehiculares Ad Hoc). La propuesta se basa en la integración de tecnologías Blockchain y la composición de diferentes modelos conceptuales, incluyendo aspectos cognitivos, computacionales, neurológicos y basados en teoría de juegos, utilizando funciones estocásticas.

Los resultados obtenidos de la validación experimental demuestran la eficiencia y escalabilidad de nuestra solución propuesta. Se ha logrado una tasa de éxito superior al 85 % en la detección de vehículos maliciosos bajo diversas condiciones, incluyendo escenarios con hasta un 50 % de vehículos maliciosos presentes en la red. Además, el tiempo de convergencia se ha mantenido por debajo de una hora para entornos con un 10 % de vehículos maliciosos, posicionando a nuestra solución a la par o por encima de otras alternativas existentes en la literatura.

Del análisis detallado en el capítulo 7, se pueden extraer varios conocimientos clave:

- **Convergencia Fiable:** NeoStarling demostró una convergencia fiable y predecible. El tiempo promedio de formación de bloques se estabilizó en torno a los 12 segundos, con un tiempo de propagación del bloque que consistentemente convergió dentro de un intervalo de 1 segundo. Además, el retraso en la replicación a través de los nodos en OrbitDB se mantuvo por debajo de 2 segundos, asegurando la eficiente propagación de transacciones y la consistencia de datos entre nodos.
- **Escalabilidad Bajo Carga:** El sistema mantuvo su rendimiento al escalar de 6 a 20 vehículos (nodos), demostrando robustez y adaptabilidad. Los tiempos de bloque, transacciones por bloque y transacciones por segundo se mantuvieron estables, indicando que el diseño puede soportar una red más amplia sin degradación significativa del rendimiento.
- **Eficiencia en la Autenticación y Transacciones:** La aproximación innovadora para gestionar la autenticación y las transacciones redujo la carga del sistema. La tasa de éxito en el emparejamiento de obstáculos fue consistentemente del 98 %, lo que llevó a un incremento estimado del 35 % en la eficiencia general del sistema.

La implementación actual de NeoStarling demuestra un potencial considerable para aplicaciones a gran escala en diversos contextos, aunque también resalta la importancia de un refinamiento continuo. Las lecciones aprendidas de este estudio ofrecen una dirección clara

para futuras mejoras, particularmente en la optimización de la eficiencia y el fortalecimiento de la seguridad.

Finalmente, el capítulo 8 presenta una arquitectura innovadora basada en Blockchain para mejorar la seguridad y la eficiencia de las Redes Ad hoc Vehiculares (VANETs). Dado que las VANETs son fundamentales para los sistemas de transporte inteligentes y están interconectadas a través del reenvío e intercambio de mensajes entre nodos vehiculares, son susceptibles a varias amenazas de seguridad. Para mitigar estas amenazas, nuestra propuesta utiliza dos blockchains paralelas, la cadena de eventos y la cadena de reputación, que registran todas las acciones de los nodos en la red. A través de esquemas de evaluación de reputación basados en inferencia bayesiana y valores de reputación acumulados históricamente, hemos logrado reducir los errores de observación y mejorar la fiabilidad de la evaluación de la reputación de los nodos.

Los experimentos demuestran que nuestra arquitectura de Blockchain de Doble Capa alcanza una tasa de éxito del 86 % en la mitigación de comportamientos hostiles, superando alternativas existentes. A pesar de estos resultados prometedores, reconocemos la necesidad de mejorar continuamente, especialmente para optimizar la eficiencia operativa y fortalecer el marco de seguridad bajo diversas condiciones operativas.

9.2 Trabajo Futuros

A lo largo de esta investigación, se ha logrado establecer una base sólida para la provisión de confianza en VANETs mediante la implementación de una solución basada en blockchain. Las siguientes propuestas de investigación no solo buscan extender el alcance del trabajo actual, sino también abordar desafíos emergentes y explorar nuevas aplicaciones dentro de este campo:

1. **Desarrollo de Mecanismos de Consenso Eficientes para VANETs:** Este estudio se enfocaría en el diseño y la evaluación de algoritmos de consenso innovadores que sean más adecuados para las características dinámicas y de alta movilidad de las VANETs, mejorando la eficiencia y la escalabilidad de la red blockchain.
2. **Estudio sobre la Mejora de la Privacidad en VANETs mediante Blockchain:** Investigación destinada a desarrollar y probar nuevos esquemas criptográficos que ofrezcan un mayor nivel de privacidad para los usuarios de VANETs, integrando técnicas avanzadas como la encriptación homomórfica y los zero-knowledge proofs en la infraestructura blockchain existente.
3. **Implementación de Algoritmos de Verificación Ligeros:** Este artículo propone el diseño, implementación y evaluación de algoritmos de verificación ligeros que puedan operar eficazmente en dispositivos con recursos limitados, asegurando la integridad y la autenticidad de los datos sin comprometer el rendimiento general del sistema.
4. **Simulaciones de Escenarios VANETs Complejos:** Publicación centrada en el modelado y la simulación de escenarios VANETs complejos y realistas, utilizando diversas densidades de tráfico y patrones de movilidad, para evaluar exhaustivamente el

desempeño y la robustez de la solución blockchain propuesta en diferentes condiciones.

5. **Integración de VANETs con Vehículos Autónomos y IoT:** Este trabajo exploraría cómo la infraestructura blockchain para VANETs puede integrarse con tecnologías emergentes, como vehículos autónomos e IoT, para facilitar comunicaciones seguras y confiables y habilitar nuevas aplicaciones en el ecosistema de transporte inteligente.
6. **Desarrollo de Marcos Normativos para Blockchain en VANETs:** Investigación dedicada a abordar los desafíos legales y regulatorios asociados a la implementación de la tecnología blockchain en VANETs, proponiendo marcos normativos que promuevan su adopción de manera segura y eficiente, respetando la privacidad y los derechos de los usuarios.
7. **Integración de Modalidades Criptográficas Avanzadas:** Para reforzar las capacidades de seguridad del sistema, exploraremos el uso de tecnologías criptográficas de vanguardia.
8. **Optimización de la Escalabilidad de Blockchain:** Dada la naturaleza dinámica de las VANETs, es crucial mejorar la escalabilidad de nuestra arquitectura blockchain para manejar eficientemente los recursos computacionales.
9. **Experimentación en Entornos del Mundo Real:** Para superar las limitaciones de los entornos simulados y capturar la complejidad de las redes vehiculares reales, se realizarán pruebas de campo extensas.
10. **Desarrollo de Algoritmos Adaptativos:** Para los factores de atenuación y umbrales numéricos, con el fin de reflejar mejor los patrones complejos y evolutivos del comportamiento vehicular.
11. **Exploración de Inteligencia Artificial y Aprendizaje Automático:** Para mejorar las capacidades predictivas y la eficiencia general del sistema VANET.

Referencias

Abdelhafidh, M., Charef, N., Mnaouer, A. B., & Chaari, L. (2023). A survey of blockchain-based solutions for iots, vanets, and fanets. En *Research Anthology on Convergence of Blockchain, Internet of Things, and Security* (pp. 663-701). IGI Global.

Abdel-Halim, I. T., & Fahmy, H. M. A. (2018). Prediction-based protocols for vehicular Ad Hoc Networks: Survey and taxonomy. *Computer Networks*, *130*, 34-50.

Ahangar, M. N., Ahmed, Q. Z., Khan, F. A., & Hafeez, M. (2021). A survey of autonomous vehicles: Enabling communication technologies and challenges. *Sensors*, *21*(3), 706.

Ahmed, A. A., & Alzahrani, A. A. (2019). A comprehensive survey on handover management for vehicular ad hoc network based on 5G mobile networks technology. *Transactions on Emerging Telecommunications Technologies*, *30*(3), e3546.

Ahmed, M. M., & Abdel-Aty, M. A. (2011). The viability of using automatic vehicle identification data for real-time crash prediction. *IEEE Transactions on Intelligent Transportation Systems*, *13*(2), 459-468.

Akhter, A. S., Ahmed, M., Anwar, A., Shah, A. S., Pathan, A.-S. K., & Zengin, A. (2022). Blockchain in vehicular ad hoc networks: Applications, challenges and solutions. *International Journal of Sensor Networks*, *40*(2), 94-130.

Akram, S. V., Malik, P. K., Singh, R., Anita, G., & Tanwar, S. (2020). Adoption of blockchain technology in various realms: Opportunities and challenges. *Security and Privacy*, *3*(5), e109.

Alangot, B., Szalachowski, P., Dinh, T. T. A., Meftah, S., Gana, J. I., Aung, K. M. M., & Li, Z. (2022). Decentralized Identity Authentication with Auditability and Privacy. *Algorithms*, *16*(1), 4.

Alcarria, R., Bordel, B., Robles, T., Martín, D., & Manso-Callejo, M.-Á. (2018). A blockchain-based authorization system for trustworthy resource monitoring and trading in smart communities. *Sensors*, *18*(10), 3561.

Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry*, *100*, 212-223.

Ali, I., Hassan, A., & Li, F. (2019). Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey. *Vehicular Communications*, *16*, 45-61.

Alsarhan, A., Alauthman, M., Alshdaifat, E., Al-Ghuwairi, A.-R., & Al-Dubai, A. (2023). Machine Learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks. *Journal of Ambient Intelligence and Humanized Computing*, *14*(5), 6113-6122.

Al-Shareeda, M. A., Anbar, M., Hasbullah, I. H., & Manickam, S. (2020). Survey of authentication and privacy schemes in vehicular ad hoc networks. *IEEE Sensors Journal*, *21*(2), 2422-2433.

Alvi, S. A., Afzal, B., Shah, G. A., Atzori, L., & Mahmood, W. (2015). Internet of multimedia things: Vision and challenges. *Ad Hoc Networks*, *33*, 87-111.

Amari, H., Abou Elhouda, Z., Khoukhi, L., & Belguith, L. H. (2023). Trust Management in Vehicular Ad-Hoc Networks: Extensive Survey. *Ieee Access*.

Ameen, H. A., Mahamad, A., Saon, S., Nor, D. M., & Ghazi, K. (2020). A review on vehicle to vehicle communication system applications. *Indonesian Journal of Electrical Engineering and Computer Science*, *18*(1), 188-198.

Anderson, A., & Devaraj, B. (2005). XACML-Based Web Services Policy Constraint Language (WS-PolicyConstraints). *Working Draft*, *6*, 24.

Anjaneyulu, M., & Kubendiran, M. (2022). Short-Term Traffic Congestion Prediction Using Hybrid Deep Learning Technique. *Sustainability*, *15*(1), 74.

Arora, A., & Yadav, S. K. (2018). Block chain based security mechanism for internet of vehicles (IoV). *Proceedings of 3rd international conference on internet of things and connected technologies (ICIoTCT)*, 26-27.

Arshad, M., Ullah, Z., Khalid, M., Ahmad, N., Khalid, W., Shahwar, D., & Cao, Y. (2019). Beacon trust management system and fake data detection in vehicular ad-hoc networks. *IET Intelligent Transport Systems*, *13*(5), 780-788.

Arshad, M. U., & Javaid, N. (2019). Blockchain-based Scalable Access Management and Trust Development for ITS in Smart City.

Asemi, A., Aghakishizadeh, V., Shabani, A., & Asemi, A. (2023). Indicators and measures for measuring the level of information intelligence. *Iranian Journal of Information Processing and Management*, *38*(4), 1155-1226.

Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. (2018). Blockchain with internet of things: Benefits, challenges, and future directions. *International Journal of Intelligent Systems and Applications*, *10*(6), 40-48.

Atwa, R. J., Flocchini, P., & Nayak, A. (2021). A fog-based reputation evaluation model for VANETs. *2021 International Symposium on Networks, Computers and Communications (ISNCC)*, 1-7.

Ayobi, S., Wang, Y., Rabbani, M., Dorri, A., Jelodar, H., Huang, H., & Yarmohammadi, S. (2021). A lightweight blockchain-based trust model for smart vehicles in vanets. *Security, Privacy, and Anonymity in Computation, Communication, and Storage: 13th International Conference, SpaCCS 2020, Nanjing, China, December 18-20, 2020, Proceedings 13*, 276-289.

Azees, M., Vijayakumar, P., & Jegatha Deborah, L. (2016). Comprehensive survey on security services in vehicular ad-hoc networks. *IET Intelligent Transport Systems*, *10*(6), 379-388.

Badrloo, S., Varshosaz, M., Pirasteh, S., & Li, J. (2022). Image-based obstacle detection methods for the safe navigation of unmanned vehicles: A review. *Remote Sensing*, *14*(15), 3824.

Baldini, G., Karanasios, S., Allen, D., & Vergari, F. (2013). Survey of wireless communication technologies for public safety. *IEEE Communications Surveys & Tutorials*, *16*(2), 619-641.

Bangui, H., Ge, M., & Buhnova, B. (2021). A hybrid data-driven model for intrusion detection in VANET. *Procedia Computer Science*, *184*, 516-523.

Barros, J., Araujo, M., & Rossetti, R. J. (2015). Short-term real-time traffic prediction methods: A survey. *2015 international conference on models and technologies for intelligent transportation systems (MT-ITS)*, 132-139.

Bashir, I. (2017). *Mastering blockchain*. Packt Publishing Ltd.

Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021). A survey on blockchain interoperability: Past, present, and future trends. *ACM Computing Surveys (CSUR)*, *54*(8), 1-41.

Berlin, D. A., & Bakker, J. (2015). Starling curves and central venous pressure. *Critical Care*, *19*, 1-8.

Bernini, N., Bertozzi, M., Castangia, L., Patander, M., & Sabbatelli, M. (2014). Real-time obstacle detection using stereo vision for autonomous ground vehicles: A survey. *17th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, 873-878.

Bitam, S., Mellouk, A., & Zeadally, S. (2015). VANET-cloud: a generic cloud computing model for vehicular Ad Hoc networks. *IEEE Wireless Communications*, *22*(1), 96-102.

Boeckl, K., Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N., Nadeau, E., O'Rourke, D. G., Piccarreta, B., & Scarfone, K. (2019). *Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks*. US Department of Commerce, National Institute of Standards; Technology ...

Bordel, B., & Alcarria, R. (2021). Trust-enhancing technologies: Blockchain mathematics in the context of Industry 4.0. En *Advances in Mathematics for Industry 4.0* (pp. 1-22). Elsevier.

Bordel, B., Alcarria, R., Martin, D., & Sanchez-Picot, A. (2019). Trust provision in the internet of things using transversal blockchain networks. *Intell. Autom. Soft Comput*, *25*(1), 155-170.

Bordel, B., Alcarria, R., & Robles, T. (2023). A blockchain ledger for securing isolated ambient intelligence deployments using reputation and information theory metrics. *Wireless Networks*, 1-17.

Bordel, B., Alcarria, R., & Robles, T. (2022). An optimization algorithm for the efficient distribution of resources in 6G verticals. *World Conference on Information Systems and Technologies*, 103-114.

Bordel, B., Alcarria, R., & Sánchez-de-Rivera, D. (2017). Detecting malicious components in large-scale Internet-of-Things systems and architectures. *Recent Advances in Information Systems and Technologies: Volume 1 5*, 155-165.

Boukerche, A., Turgut, B., Aydin, N., Ahmad, M. Z., Bölöni, L., & Turgut, D. (2011). Routing protocols in ad hoc networks: A survey. *Computer networks*, *55*(13), 3032-3080.

Bounaira, S., Alioua, A., & Souici, I. (2024). Blockchain-enabled trust management for secure content caching in mobile edge computing using deep reinforcement learning. *Internet of Things*, *25*, 101081.

Butt, T. A., Iqbal, R., Salah, K., Aloqaily, M., & Jararweh, Y. (2019). Privacy management in social internet of vehicles: review, challenges and blockchain based solutions. *IEEE Access*, *7*, 79694-79713.

Campanile, L., Gribaudo, M., Iacono, M., Marulli, F., & Mastroianni, M. (2020). Computer network simulation with ns-3: A systematic literature review. *Electronics*, *9*(2), 272.

Campolo, C., Cozzetti, H. A., Molinaro, A., & Scopigno, R. (2011). Vehicular connectivity in urban scenarios: effectiveness and potential of roadside, moving WAVE providers and hybrid solutions. *EURASIP Journal on Wireless Communications and Networking*, *2011*, 1-10.

Cao, B., Li, Y., Zhang, L., Zhang, L., Mumtaz, S., Zhou, Z., & Peng, M. (2019). When Internet of Things meets blockchain: Challenges in distributed consensus. *IEEE Network*, *33*(6), 133-139.

Cardoso, R. M., Mastelari, N., & Bassora, M. F. (2015). Internet of things architecture in the context of intelligent transportation systemsa case study towards a web-based application deployment. *ABCM Symposium Series in Mechatronics*, *6*.

Carneiro, G., Fortuna, P., & Ricardo, M. (2009). Flowmonitor: a network monitoring framework for the network simulator 3 (ns-3). *Proceedings of the Fourth International ICST Conference on Performance Evaluation Methodologies and Tools*, 1-10.

Chang, B. R., Tsai, H. F., & Young, C.-P. (2010). Intelligent data fusion system for predicting vehicle collision warning using vision/GPS sensing. *Expert Systems with Applications*, *37*(3), 2439-2450.

Chaudhary, B., & Singh, K. (2021). A Blockchain enabled location-privacy preserving scheme for vehicular ad-hoc networks. *Peer-to-Peer Networking and Applications*, *14*(5), 3198-3212.

Chen, M., Yu, X., & Liu, Y. (2018). PCNN: Deep convolutional networks for short-term traffic congestion prediction. *IEEE Transactions on Intelligent Transportation Systems*, *19*(11), 3550-3559.

Chio, S.-H., Chuang, T.-Y., Hsu, P.-H., Jaw, J.-J., Lin, S.-Y., Lin, Y.-C., Teo, T. A., Tsai, F., Tseng, Y. H., Wang, C. K., et al. (2015). LiDAR data processing and applications. En *Remotely Sensed Data Characterization, Classification, and Accuracies* (pp. 343-374). CRC Press.

Comert, O. (2020). Blockchain Revolution: How the Technology behind Bitcoin and Other Cryptocurrencies Is Changing the World.

Cui, J., Ouyang, F., Ying, Z., Wei, L., & Zhong, H. (2021). Secure and efficient data sharing among vehicles based on consortium blockchain. *IEEE Transactions on Intelligent Transportation Systems*, *23*(7), 8857-8867.

Daimary, S. K., & Kalita, H. K. (s.f.). An Overview of Blockchain-based Applications and Architectures for VANET. *International Journal of Computer Applications*, *975*, 8887.

Dibaei, M., Zheng, X., Xia, Y., Xu, X., Jolfaei, A., Bashir, A. K., Tariq, U., Yu, D., & Vasilakos, A. V. (2021). Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: A survey. *IEEE Transactions on Intelligent Transportation Systems*, *23*(2), 683-700.

Diffie, W., & Hellman, M. E. (2022). New directions in cryptography. En *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman* (pp. 365-390).

Ding, Q., Li, X., Jiang, M., & Zhou, X. (2010). Reputation-based trust model in vehicular ad hoc networks. *2010 International Conference on Wireless Communications & Signal Processing (WCSP)*, 1-6.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). Blockchain in internet of things: challenges and solutions. *arXiv preprint arXiv:1608.05187*.

Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017). Blockchain: A distributed solution to automotive security and privacy. *IEEE communications magazine*, *55*(12), 119-125.

Dwivedi, S. K., Amin, R., Das, A. K., Leung, M. T., Choo, K.-K. R., & Vollala, S. (2022). Blockchain-based vehicular ad-hoc networks: A comprehensive survey. *Ad Hoc Networks*, *137*, 102980.

Elemike, E. E., Uzoh, I. M., Onwudiwe, D. C., & Babalola, O. O. (2019). The role of nanotechnology in the fortification of plant nutrients and improvement of crop production. *Applied Sciences*, *9*(3), 499.

Eze, K. G., Akujuobi, C. M., Sadiku, M. N., Chouikha, M., & Alam, S. (2019). Internet of things and blockchain integration: Use cases and implementation challenges. *Business Information Systems Workshops: BIS 2019 International Workshops, Seville, Spain, June 26–28, 2019, Revised Papers 22*, 287-298.

Fan, N., & Wu, C. Q. (2019). On trust models for communication security in vehicular ad-hoc networks. *Ad Hoc Networks*, *90*, 101740.

Feng, J., Wang, Y., Wang, J., & Ren, F. (2020). Blockchain-based data management and edge-assisted trusted cloaking area construction for location privacy protection in vehicular networks. *IEEE Internet of Things Journal*, *8*(4), 2087-2101.

Feng, Q., He, D., Zeadally, S., & Liang, K. (2019). BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks. *IEEE Transactions on Industrial Informatics*, *16*(6), 4146-4155.

Fernandes, C. P., Montez, C., Adriano, D. D., Boukerche, A., & Wangham, M. S. (2023). A blockchain-based reputation system for trusted VANET nodes. *Ad Hoc Networks*, *140*, 103071.

Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE access*, *8*, 21091-21116.

Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2018). Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal*, *6*(2), 2188-2204.

Firdaus, M., Rahmadika, S., & Rhee, K.-H. (2021). Decentralized trusted data sharing management on internet of vehicle edge computing (IoVEC) networks using consortium blockchain. *Sensors*, *21*(7), 2410.

Fraiji, Y., Azzouz, L. B., Trojet, W., & Saidane, L. A. (2018). Cyber security issues of Internet of electric vehicles. *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, 1-6.

Gad, A. R., Nashat, A. A., & Barkat, T. M. (2021). Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset. *IEEE Access*, *9*, 142206-142217.

Gazdar, T., Alboqomi, O., & Munshi, A. (2022). A decentralized blockchain-based trust management framework for vehicular ad hoc networks. *Smart Cities*, *5*(1), 348-363.

Ge, X., Li, Z., & Li, S. (2017). 5G software defined vehicular networks. *IEEE Communications Magazine*, *55*(7), 87-93.

George, S., & Santra, A. K. (2020). Traffic prediction using multifaceted techniques: A survey. *Wireless Personal Communications*, *115*(2), 1047-1106.

Gershenfeld, N., Krikorian, R., & Cohen, D. (2004). The internet of things. *Scientific American*, *291*(4), 76-81.

Ghazaleh, H. A. A. (2022). An Overview of Security and Privacy Challenges in Connected Autonomous Vehicles. *Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries*, *5*(2), 15-26.

Goyal, P., Batra, S., & Singh, A. (2010). A literature review of security attack in mobile ad-hoc networks. *International Journal of Computer Applications*, *9*(12), 11-15.

Grover, J. (2022). Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review. *Vehicular Communications*, *34*, 100458.

Guerrero-Ibáñez, J., Flores-Cortés, C., & Zeadally, S. (2013). Vehicular ad-hoc networks (vanets): architecture, protocols and applications. En *Next-Generation Wireless Technologies: 4G and Beyond* (pp. 49-70). Springer.

Haris, M., Shah, M. A., & Maple, C. (2023). Internet of intelligent vehicles (IoIV): an intelligent VANET based computing via predictive modeling. *IEEE Access*.

Haris, R. M., & Al-Maadeed, S. (2020). Integrating blockchain technology in 5G enabled IoT: A review. *2020 IEEE international conference on informatics, IoT, and enabling technologies (ICIoT)*, 367-371.

Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2019). Trust model for secure group leader-based communications in VANET. *Wireless Networks*, *25*, 4639-4661.

Hatim, S. M., Elias, S. J., Awang, N., Darus, M. Y., et al. (2018). VANETS and Internet of Things (IoT): A discussion. *Indones. J. Electr. Eng. Comput. Sci*, *12*(1), 218-224.

Huang, Z., Ruj, S., Cavenaghi, M. A., Stojmenovic, M., & Nayak, A. (2014). A social network approach to trust management in VANETs. *Peer-to-peer networking and applications*, *7*, 229-242.

Hussain, N., Rani, P., Chouhan, H., & Gaur, U. S. (2022). Cyber security and privacy of connected and automated vehicles (CAVs)-based federated learning: challenges, opportunities, and open issues. *Federated learning for IoT applications*, 169-183.

Hussain, R., Lee, J., & Zeadally, S. (2020). Trust in VANET: A survey of current solutions and future research opportunities. *IEEE transactions on intelligent transportation systems*, *22*(5), 2553-2571.

Hussain, R., Nawaz, W., Lee, J., Son, J., & Seo, J. T. (2016). A hybrid trust management framework for vehicular social networks. *Computational Social Networks: 5th International Conference, CSoNet 2016, Ho Chi Minh City, Vietnam, August 2-4, 2016, Proceedings 5*, 214-225.

Hussien, H. M., Yasin, S. M., Udzir, S., Zaidan, A. A., & Zaidan, B. B. (2019). A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. *Journal of medical systems*, *43*, 1-35.

Ilarri, S., Delot, T., & Trillo-Lado, R. (2015). A data management perspective on vehicular networks. *IEEE Communications Surveys & Tutorials*, *17*(4), 2420-2460.

Ilyas, M., Seet, B.-C., Hannan, X., Tseng, Y.-C., Mishra, A., Giordano, S., Suh, Y.-J., Sohraby, K., Yazbeck, S., Shu, Y., et al. (2017). *The handbook of ad hoc wireless networks*. CRC press.

INEN, N. T. E. (2017). Tecnologias de la información-Tecnicas de seguridad–Sistemas de gestion de gestión de seguridad de la información–Requisitos (ISO/IEC 27001: 2013 Cor. 2015, IDT). *Recuperado el*, *3*.

Irawan, K., Yusuf, R., & Prihatmanto, A. S. (2020). A survey on traffic flow prediction methods. *2020 6th International Conference on Interactive Digital Media (ICIDM)*, 1-4.

James, G., Witten, D., Hastie, T., Tibshirani, R., et al. (2013). *An introduction to statistical learning* (Vol. 112). Springer.

James, G., Witten, D., Hastie, T., Tibshirani, R., & Taylor, J. (2023). *An introduction to statistical learning: With applications in python*. Springer Nature.

Jamil, S., Rahman, M., & Fawad. (2022). A comprehensive survey of digital twins and federated learning for industrial internet of things (IIoT), internet of vehicles (IoV) and internet of drones (IoD). *Applied System Innovation*, *5*(3), 56.

Javed, A. R., Hassan, M. A., Shahzad, F., Ahmed, W., Singh, S., Baker, T., & Gadekallu, T. R. (2022). Integration of blockchain technology and federated learning in vehicular (iot) networks: A comprehensive survey. *Sensors*, *22*(12), 4394.

Joe, M. M., & Ramakrishnan, B. (2016). Review of vehicular ad hoc network communication models including WVANET (Web VANET) model and WVANET future research directions. *Wireless networks*, *22*(7), 2369-2386.

Joshi, G. P., Perumal, E., Shankar, K., Tariq, U., Ahmad, T., & Ibrahim, A. (2020). Toward blockchain-enabled privacy-preserving data transmission in cluster-based vehicular networks. *Electronics*, *9*(9), 1358.

Junejo, M. H., Ab Rahman, A. A.-H., Shaikh, R. A., Yusof, K. M., Kumar, D., & Memon, I. (2021). Lightweight trust model with machine learning scheme for secure privacy in VANET. *Procedia Computer Science*, *194*, 45-59.

Jyothi, N., & Patil, R. (2022). A fuzzy-based trust evaluation framework for efficient privacy preservation and secure authentication in VANET. *Journal of Information and Telecommunication*, *6*(3), 270-288.

Karabulut, M. A., Shah, A. S., Ilhan, H., Pathan, A.-S. K., & Atiquzzaman, M. (2023). Inspecting VANET with various critical aspects–a systematic review. *Ad Hoc Networks*, 103281.

Khan, A. S., Balan, K., Javed, Y., Tarmizi, S., & Abdullah, J. (2019). Secure trust-based blockchain architecture to prevent attacks in VANET. *Sensors*, *19*(22), 4954.

Khan, A. A., Abolhasan, M., & Ni, W. (2018). An evolutionary game theoretic approach for stable and optimized clustering in VANETs. *IEEE Transactions on Vehicular Technology*, *67*(5), 4501-4513.

Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2019). A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *IEEE Communications Surveys & Tutorials*, *22*(1), 196-248.

Koduri, R., Nandyala, S., Manalikandy, M., et al. (2020). *Secure vehicular communication using blockchain technology* (inf. téc.). SAE Technical Paper.

Kudva, S., Badsha, S., Sengupta, S., La, H., Khalil, I., & Atiquzzaman, M. (2021). A scalable blockchain based trust management in VANET routing protocol. *Journal of Parallel and Distributed Computing*, *152*, 144-156.

Kuhn, M., Johnson, K., et al. (2013). *Applied predictive modeling* (Vol. 26). Springer.

Lai, C., Lu, R., Zheng, D., & Shen, X. (2020). Security and privacy challenges in 5G-enabled vehicular networks. *IEEE Network*, *34*(2), 37-45.

Lei, K., Fang, J., Zhang, Q., Lou, J., Du, M., Huang, J., Wang, J., & Xu, K. (2020). Blockchain-based cache poisoning security protection and privacy-aware access control in NDN vehicular edge computing networks. *Journal of Grid computing*, *18*, 593-613.

Li, H., & Han, D. (2023). Blockchain-assisted secure message authentication with reputation management for VANETs. *The Journal of Supercomputing*, *79*(17), 19903-19933.

Li, H., Pei, L., Liao, D., Chen, S., Zhang, M., & Xu, D. (2020). FADB: A fine-grained access control scheme for VANET data based on blockchain. *IEEE Access*, *8*, 85190-85203.

Li, L., Li, X., Li, Z., Zeng, D. D., & Scherer, W. T. (2010). A bibliographic analysis of the IEEE Transactions on Intelligent Transportation Systems literature. *IEEE Transactions on Intelligent Transportation Systems*, *11*(2), 251-255.

Li, P., Abdel-Aty, M., & Zhang, S. (2022). Improving spatiotemporal transferability of real-time crash likelihood prediction models using transfer-learning approaches. *Transportation research record*, *2676*(11), 621-631.

Li, Q., Malip, A., Martin, K. M., Ng, S.-L., & Zhang, J. (2012). A reputation-based announcement scheme for VANETs. *IEEE Transactions on Vehicular Technology*, *61*(9), 4095-4108.

Li, S., Li, J., Liang, Y., Zhang, H., Wu, S., Wang, S., & Cheng, L. (2023). TD-SAS: A Trust-Aware and Decentralized Speed Advisory System for Energy-Efficient Autonomous Vehicle Platoons. *IEEE Transactions on Intelligent Vehicles*.

Li, T., Lin, L., & Gong, S. (2019). AutoMPC: Efficient Multi-Party Computation for Secure and Privacy-Preserving Cooperative Control of Connected Autonomous Vehicles. *SafeAI@ AAAI*, *1*.

Li, T., Ni, A., Zhang, C., Xiao, G., & Gao, L. (2020). Short-term traffic congestion prediction with Conv–BiLSTM considering spatio-temporal features. *IET Intelligent Transport Systems*, *14*(14), 1978-1986.

Liang, W., Li, Z., Zhang, H., Wang, S., & Bie, R. (2015). Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends. *International Journal of Distributed Sensor Networks*, *11*(8), 745303.

Lin, C., He, D., Huang, X., Kumar, N., & Choo, K.-K. R. (2020). BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, *22*(12), 7408-7420.

Lin, C., Huang, X., & He, D. (2022). EBCPA: Efficient blockchain-based conditional privacy-preserving authentication for VANETs. *IEEE Transactions on Dependable and Secure Computing*.

Lin, X., Lu, R., Zhang, C., Zhu, H., Ho, P.-H., & Shen, X. (2008). Security in vehicular ad hoc networks. *IEEE communications magazine*, *46*(4), 88-95.

Linke, H., Yeadon, K., Bereski, P., Bouwers, B., Fritsch, W., & Sánchez Almodóvar, N. (2010). Integrated IP communication solutions for public safety services.

Liu, H., Han, D., & Li, D. (2021). Behavior analysis and blockchain based trust management in VANETs. *Journal of Parallel and Distributed Computing*, *151*, 61-69.

Lopez, D., & Farooq, B. (2020). A multi-layered blockchain framework for smart mobility data-markets. *Transportation Research Part C: Emerging Technologies*, *111*, 588-615.

Lu, Z., Wang, Q., Qu, G., & Liu, Z. (2018). BARS: A blockchain-based anonymous reputation system for trust management in VANETs. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 98-103.

Lu, Z., Wang, Q., Qu, G., Zhang, H., & Liu, Z. (2019). A blockchain-based privacy-preserving authentication scheme for VANETs. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *27*(12), 2792-2801.

Lücking, M., Kretzer, F., Kannengiesser, N., Beigl, M., Sunyaev, A., & Stork, W. (2021). When data fly: an open data trading system in vehicular ad hoc networks. *Electronics*, *10*(6), 654.

Luo, B., Li, X., Weng, J., Guo, J., & Ma, J. (2019). Blockchain enabled trust-based location privacy protection scheme in VANET. *IEEE Transactions on Vehicular Technology*, *69*(2), 2034-2048.

Ma, Z., Zhang, J., Guo, Y., Liu, Y., Liu, X., & He, W. (2020). An efficient decentralized key management mechanism for VANET with blockchain. *IEEE Transactions on Vehicular Technology*, *69*(6), 5836-5849.

Malik, N., Nanda, P., Arora, A., He, X., & Puthal, D. (2018). Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks. *2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)*, 674-679.

Maslekar, N., Boussedjra, M., Mouzna, J., & Labiod, H. (2011). VANET based adaptive traffic signal control. *2011 IEEE 73rd vehicular technology conference (VTC Spring)*, 1-5.

Math, C. B., Ozgur, A., de Groot, S. H., & Li, H. (2015). Data Rate based Congestion Control in V2V communication for traffic safety applications. *2015 IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT)*, 1-6.

Mehdi, M. M., Raza, I., & Hussain, S. A. (2017). A game theory based trust model for Vehicular Ad hoc Networks (VANETs). *Computer Networks*, *121*, 152-172.

Mehta, P., Gupta, R., & Tanwar, S. (2020). Blockchain envisioned UAV networks: Challenges, solutions, and comparisons. *Computer Communications*, *151*, 518-538.

Miehle, D. S. (2020). *Distributed Ledger Technologies in the Automotive Value Chain* [Tesis doctoral, Technische Universität München].

Mistry, I., Tanwar, S., Tyagi, S., & Kumar, N. (2020). Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. *Mechanical systems and signal processing*, *135*, 106382.

Mollah, M. B., Zhao, J., Niyato, D., Guan, Y. L., Yuen, C., Sun, S., Lam, K.-Y., & Koh, L. H. (2020). Blockchain for the internet of vehicles towards intelligent transportation systems: A survey. *IEEE Internet of Things Journal*, *8*(6), 4157-4185.

Murkomen, T. (2023). Blockchain-Based Privacy-Preserving for secure and efficient Maas Ecosystem in the context Of IoV: A Survey.

Najafi, M., Khoukhi, L., & Lemercier, M. (2021). A multidimensional trust model for vehicular ad-hoc networks. *2021 IEEE 46th Conference on Local Computer Networks (LCN)*, 419-422.

Nandy, T., Idris, M. Y. I., Noor, R. M., Wahab, A. W. A., Bhattacharyya, S., Kolandaisamy, R., & Yahuza, M. (2021). A secure, privacy-preserving, and lightweight Authentication scheme for VANETs. *IEEE Sensors Journal*, *21*(18), 20998-21011.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press.

Nasland, M., Selander, G., Phillips, S., Nasser, B., Torvinen, V., Lehtovirta, V., Klaedtke, F., Heikkinen, S., Pernila, T., Zahariev, A., et al. (2016). 5G-ENSURE-D2. 1 Use Cases.

Noor-A-Rahim, M., Liu, Z., Lee, H., Khyam, M. O., He, J., Pesch, D., Moessner, K., Saad, W., & Poor, H. V. (2022). 6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities. *Proceedings of the IEEE*, *110*(6), 712-734.

Obaidat, M., Khodjaeva, M., Holst, J., & Ben Zid, M. (2020). Security and privacy challenges in vehicular ad hoc networks. *Connected Vehicles in the Internet of Things: Concepts, Technologies and Frameworks for the IoV*, 223-251.

Parekh, D., Poddar, N., Rajpurkar, A., Chahal, M., Kumar, N., Joshi, G. P., & Cho, W. (2022). A review on autonomous vehicles: Progress, methods and challenges. *Electronics*, *11*(14), 2162.

Patil, P., Sangeetha, M., & Bhaskar, V. (2021). Blockchain for IoT access control, security and privacy: a review. *Wireless Personal Communications*, *117*(3), 1815-1834.

Peng, C., Wu, C., Gao, L., Zhang, J., Alvin Yau, K.-L., & Ji, Y. (2020). Blockchain for vehicular Internet of Things: Recent advances and open issues. *Sensors*, *20*(18), 5079.

Pilkington, M. (2016). Blockchain technology: principles and applications. En *Research handbook on digital transformations* (pp. 225-253). Edward Elgar Publishing.

Rathod, T., Jadav, N. K., Tanwar, S., Sharma, R., Tolba, A., Raboaca, M. S., Marina, V., & Said, W. (2023). Blockchain-driven intelligent scheme for IoT-based public safety system beyond 5G networks. *Sensors*, *23*(2), 969.

Ravi, B., Thangaraj, J., & Petale, S. (2018). Stochastic network optimization of data dissemination for multi-hop routing in VANETs. *2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 1-4.

Ravi, B., Thangaraj, J., & Petale, S. (2019). Data traffic forwarding for inter-vehicular communication in VANETs using stochastic method. *Wireless Personal Communications*, *106*, 1591-1607.

Raya, M., & Hubaux, J.-P. (2007). Securing vehicular ad hoc networks. *Journal of computer security*, *15*(1), 39-68.

Razzaque, M. A., S, A. S., & Cheraghi, S. M. (2013). Security and privacy in vehicular ad-hoc networks: survey and the road ahead. *Wireless Networks and Security: Issues, Challenges and Research Trends*, 107-132.

Riley, G. F., & Henderson, T. R. (2010). The ns-3 network simulator. En *Modeling and tools for network simulation* (pp. 15-34). Springer.

Robles, T., Bordel, B., Alcarria, R., & Sánchez-de-Rivera, D. (2018). Blockchain technologies for private data management in AmI environments. *Proceedings*, *2*(19), 1230.

Sadineni, G., Singh, J., Rani, S., Rao, G. S., Pasha, M. J., & Lavanya, A. (2024). Blockchain-Enhanced Vehicular Ad-hoc Networks (B-VANETs): Decentralized Traffic Coordination and Anonymized Communication. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(1s), 443-456.

Saleh, A. I., Gamel, S. A., & Abo-Al-Ez, K. M. (2017). A reliable routing protocol for vehicular ad hoc networks. *Computers & Electrical Engineering*, *64*, 473-495.

Sandosh, S., Doshi, S., & Joshi, A. (2023). Enhancing Security in Automobile Edge Computing through Federated Learning and Blockchain. *2023 International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (iQ-CCHESS)*, 1-6.

Sanka, A. I., Irfan, M., Huang, I., & Cheung, R. C. (2021). A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. *Computer communications*, *169*, 179-201.

Shan, J., & Toth, C. K. (2018). *Topographic laser ranging and scanning: principles and processing*. CRC press.

Sharma, S., Ghanshala, K. K., & Mohan, S. (2019). Blockchain-based internet of vehicles (IoV): an efficient secure ad hoc vehicular networking architecture. *2019 IEEE 2nd 5G World Forum (5GWF)*, 452-457.

Sheikh, M. S., Liang, J., & Wang, W. (2019). A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets). *Sensors*, *19*(16), 3589.

Sheikh, M. S., Liang, J., & Wang, W. (2020). Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey. *Wireless Communications and Mobile Computing*, *2020*, 1-25.

Shu, J., Zhou, L., Zhang, W., Du, X., & Guizani, M. (2020). Collaborative intrusion detection for VANETs: A deep learning-based distributed SDN approach. *IEEE Transactions on Intelligent Transportation Systems*, *22*(7), 4519-4530.

Singh, S. P., & Sastry, G. H. (2023). Blockchain-Enabled Security in Vehicular Ad Hoc Network Check for updates. *Advances in Data Science and Computing Technologies: Select Proceedings of ADSC 2022*, *1056*, 181.

Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., & Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography*, *3*(1), 3.

Soleymani, S. A., Abdullah, A. H., Hassan, W. H., Anisi, M. H., Goudarzi, S., Rezazadeh Baee, M. A., & Mandala, S. (2015). Trust management in vehicular ad hoc network: a systematic review. *EURASIP Journal on Wireless Communications and Networking*, *2015*, 1-22.

Soleymani, S. A., Abdullah, A. H., Zareei, M., Anisi, M. H., Vargas-Rosales, C., Khan, M. K., & Goudarzi, S. (2017). A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing. *IEEE Access*, *5*, 15619-15629.

Song, C., Zhang, M., & Peng, W.-P. (2018). Research on Secure and Privacy-Preserving Scheme Based on Secure Multi-Party Computation for VANET. *J. Inf. Hiding Multim. Signal Process.*, *9*(1), 99-107.

Standard, O. (2013). extensible access control markup language (xacml) version 3.0. *A:(22 January 2013). URl: http://docs. oasis-open. org/xacml/3.0/xacml-3.0-core-spec-os-en. html*.

Sultan, S., Javaid, Q., Malik, A. J., Al-Turjman, F., & Attique, M. (2022). Collaborative-trust approach toward malicious node detection in vehicular ad hoc networks. *Environment, Development and Sustainability*, 1-19.

Sun, D., Zhao, H., & Cheng, S. (2016). A novel membership cloud model-based trust evaluation model for vehicular ad hoc network of T-CPS. *Security and Communication Networks*, *9*(18), 5710-5723.

Sun, Z., Liu, Y., Wang, J., Li, G., Anil, C., Li, K., Guo, X., Sun, G., Tian, D., & Cao, D. (2021). Applications of game theory in vehicular networks: A survey. *IEEE Communications Surveys & Tutorials*, *23*(4), 2660-2710.

Tabrizi, S. S., & Ibrahim, D. (2016). Security of the Internet of Things: An overview. *Proceedings of the 2016 International Conference on Communication and Information Systems*, 146-150.

Tan, H., & Chung, I. (2019). Secure authentication and key management with blockchain in VANETs. *IEEE access*, *8*, 2482-2498.

Toor, Y., Muhlethaler, P., Laouiti, A., & De La Fortelle, A. (2008). Vehicle ad hoc networks: Applications and related technical issues. *IEEE communications surveys & tutorials*, *10*(3), 74-88.

Torky, M., & Hassanein, A. E. (2020). Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges. *Computers and Electronics in Agriculture*, *178*, 105476.

Tripathi, G. C. (2021). A Literature Review Of Electric Vehicle To Grid Technology. *Webology (ISSN: 1735-188X)*, *18*(6).

Tripathi, K. N., Yadav, A. M., & Sharma, S. (2022). Fuzzy and deep belief network based malicious vehicle identification and trust recommendation framework in VANETs. *Wireless Personal Communications*, *124*(3), 2475-2504.

Tripp-Barba, C., Zaldívar-Colado, A., Urquiza-Aguiar, L., & Aguilar-Calderón, J. A. (2019). Survey on routing protocols for vehicular ad hoc networks based on multimetrics. *Electronics*, *8*(10), 1177.

Tyagi, A. K. (2023). Decentralized everything: Practical use of blockchain technology in future applications. En *Distributed Computing to Blockchain* (pp. 19-38). Elsevier.

Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2021). A survey on the adoption of blockchain in iot: Challenges and solutions. *Blockchain: Research and Applications*, *2*(2), 100006.

Vaibhav, A., Shukla, D., Das, S., Sahana, S., & Johri, P. (2017). Security challenges, authentication, application and trust models for vehicular ad hoc network-a survey. *IJ Wireless and Microwave Technologies*, *3*, 36-48.

Venitta Raj, R., & Balasubramanian, K. (2021). Trust aware similarity-based source routing to ensure effective communication using game-theoretic approach in VANETs. *Journal of Ambient Intelligence and Humanized Computing*, *12*, 6781-6791.

Verma, A., Saha, R., Kumar, G., & Kim, T.-h. (2021). The security perspectives of vehicular networks: a taxonomical analysis of attacks and solutions. *Applied Sciences*, *11*(10), 4682.

Viriyasitavat, W., Anuphaptrirong, T., & Hoonsopon, D. (2019). When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities. *Journal of industrial information integration*, *15*, 21-28.

Wang, C., & Peeta, S. (2024). Incentive Mechanism for Privacy-Preserving Collaborative Routing Using Secure Multi-Party Computation and Blockchain. *Sensors*, *24*(2), 542.

Wang, F.-Y. (2010). Parallel control and management for intelligent transportation systems: Concepts, architectures, and applications. *IEEE transactions on intelligent transportation systems*, *11*(3), 630-638.

Wang, J., Liu, Y., Liu, X., & Zhang, J. (2009). A trust propagation scheme in VANETs. *2009 IEEE Intelligent Vehicles Symposium*, 1067-1071.

Wang, X., Ning, Z., Zhou, M., Hu, X., Wang, L., Zhang, Y., Yu, F. R., & Hu, B. (2018). Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions. *IEEE Communications Surveys & Tutorials*, *21*(2), 1314-1345.

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer law & security review*, *26*(1), 23-30.

Weber, R. H. (2013). Internet of things–governance quo vadis? *Computer law & security review*, *29*(4), 341-347.

Wijesekara, P. A. D. S. N., & Gunawardena, S. (2023). A Review of blockchain technology in knowledge-defined networking, its application, benefits, and challenges. *Network*, *3*(3), 343-421.

Wu, H., Nabar, S., & Poovendran, R. (2012). An energy framework for the network simulator 3 (ns-3). *4th International ICST Conference on Simulation Tools and Techniques*.

Xia, H., Zhang, S.-s., Li, Y., Pan, Z.-k., Peng, X., & Cheng, X.-z. (2019). An attack-resistant trust inference model for securing routing in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, *68*(7), 7108-7120.

Xie, D., Xu, Y., & Wang, R. (2019). Obstacle detection and tracking method for autonomous vehicle based on three-dimensional LiDAR. *International Journal of Advanced Robotic Systems*, *16*(2), 1729881419831587.

Xie, L., Ding, Y., Yang, H., & Wang, X. (2019). Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs. *Ieee Access*, *7*, 56656-56666.

Xu, B., Agbele, T., & Jiang, R. (2020). Biometric blockchain: a secure solution for intelligent vehicle data sharing. *Deep Biometrics*, 245-256.

Yeh, L.-Y., Shen, N.-X., & Hwang, R.-H. (2022). Blockchain-based privacy-preserving and sustainable data query service over 5G-VANETs. *IEEE Transactions on Intelligent Transportation Systems*, *23*(9), 15909-15921.

Yin, X., Wu, G., Wei, J., Shen, Y., Qi, H., & Yin, B. (2021). Deep learning on traffic prediction: Methods, analysis, and future directions. *IEEE Transactions on Intelligent Transportation Systems*, *23*(6), 4927-4943.

Yuan, H., & Li, G. (2021). A survey of traffic prediction: from spatio-temporal data to intelligent transportation. *Data Science and Engineering*, *6*(1), 63-85.

Zhang, D., Yu, F. R., & Yang, R. (2018). A machine learning approach for software-defined vehicular ad hoc networks with trust management. *2018 IEEE Global Communications Conference (GLOBECOM)*, 1-6.

Zhang, J., Li, F., Zhang, H., Li, R., & Li, Y. (2019). Intrusion detection system using deep learning for in-vehicle security. *Ad Hoc Networks*, *95*, 101974.

Zhang, J. (2011). A survey on trust management for vanets. *2011 IEEE International Conference on Advanced Information Networking and Applications*, 105-112.

Zhang, J., Chen, C., & Cohen, R. (2010). A Scalable and Effective Trust-Based Framework for Vehicular Ad-Hoc Networks. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, *1*(4), 3-15.

Zhang, J., Wang, F.-Y., Wang, K., Lin, W.-H., Xu, X., & Chen, C. (2011). Data-driven intelligent transportation systems: A survey. *IEEE Transactions on Intelligent Transportation Systems*, *12*(4), 1624-1639.

Zhang, L., Luo, M., Li, J., Au, M. H., Choo, K.-K. R., Chen, T., & Tian, S. (2019). Blockchain based secure data sharing system for Internet of vehicles: A position paper. *Vehicular Communications*, *16*, 85-93.

Zhang, X., & Chen, X. (2019). Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network. *Ieee Access*, *7*, 58241-58254.

Zhao, W., Gao, Y., Ji, T., Wan, X., Ye, F., & Bai, G. (2019). Deep temporal convolutional networks for short-term traffic flow forecasting. *Ieee Access*, *7*, 114496-114507.

Zhao, Z., Guardalben, L., Karimzadeh, M., Silva, J., Braun, T., & Sargento, S. (2018). Mobility prediction-assisted over-the-top edge prefetching for hierarchical VANETs. *IEEE Journal on Selected Areas in Communications*, *36*(8), 1786-1801.

Zheng, D., Jing, C., Guo, R., Gao, S., & Wang, L. (2019). A traceable blockchain-based access authentication system with privacy preservation in VANETs. *IEEE Access*, *7*, 117716-117726.

Zhou, H., Wang, H., Chen, X., Li, X., & Xu, S. (2018). Data offloading techniques through vehicular ad hoc networks: A survey. *IEEE Access*, *6*, 65250-65259.

Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010). Security and privacy in cloud computing: A survey. *2010 sixth international conference on semantics, knowledge and grids*, 105-112.

Anexo I. Publicaciones Desarrolladas

A continuación se listan las publicaciones desarrolladas durante el período de investigación, incluyendo detalles sobre su impacto basado en JCR y SJR.

1. Juárez, R.; Bordel, B. *NeoStarling: An Efficient and Scalable Collaborative Blockchain-Enabled Obstacle Mapping Solution for Vehicular Environments*. Sensors 2023, 23, 7500. https://doi.org/10.3390/s23177500. **JCR (2023): 7.500 [Q2], SJR (2022): 0.764 [Q1]**.
2. Juárez, R.; Bordel, B. *Augmenting Vehicular Ad Hoc Network Security and Efficiency with Blockchain: A Probabilistic Identification and Malicious Node Mitigation Strategy*. Electronics 2023, 12, 4794. https://doi.org/10.3390/electronics12234794. **JCR (2023): 4.794 [Q2], SJR (2022): 0.628 [Q2]**.