UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN
ELECTRÓNICA Y AUTOMATIZACIÓN
Resolución: RPC-SO-09-No.265-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
Vulnerabilidades en la comunicación multiplexada de redes CAN-BUS para la detección y mitigación de mensajes maliciosos mediante inteligencia artificial
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento:
Ingeniería, industria y construcción
Autor/a:
Ing. Manuel Rodrigo Passo Guamangate
Tutor/a:
Mg. Wilmer Fabián Albarracín Guarochico PhD. Paúl Francisco Baldeón Egas

Quito – Ecuador

2025

APROBACIÓN DEL TUTOR

Yo, **Mg. Wilmer Fabián Albarracín Guarochico** con C.I: **1713341152** en mi calidad de Tutor del proyecto de investigación titulado: **VULNERABILIDADES EN LA COMUNICACIÓN MULTIPLEXADA DE REDES CAN-BUS PARA LA DETECCIÓN Y MITIGACIÓN DE MENSAJES MALICIOSOS MEDIANTE INTELIGENCIA ARTIFICIAL.**

Elaborado por: **MANUEL RODRIGO PASSO GUAMANGATE**, de C.I: **1723741300** estudiante de la Maestría: **ELECTRÓNICA Y AUTOMATIZACIÓN** de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., 11 de septiembre de 2025

Firmado electrónicamente por:
WILMER FABIAN ALBARRACIN GUAROCHICO
Validar únicamente con FirmaEC

_____

Mg. Wilmer Fabián Albarracín Guarochico

C.I: 1713341152

APROBACIÓN DEL TUTOR

Yo, **PhD. Paúl Francisco Baldeón Egas** con C.I: **1002807814** en mi calidad de Tutor del proyecto de investigación titulado: **VULNERABILIDADES EN LA COMUNICACIÓN MULTIPLEXADA DE REDES CAN-BUS PARA LA DETECCIÓN Y MITIGACIÓN DE MENSAJES MALICIOSOS MEDIANTE INTELIGENCIA ARTIFICIAL.**

Elaborado por: **MANUEL RODRIGO PASSO GUAMANGATE**, de C.I: **1723741300** estudiante de la Maestría: **ELECTRÓNICA Y AUTOMATIZACIÓN** de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., 11 de septiembre de 2025

Firmado electrónicamente por:
PAUL FRANCISCO BALDEON EGAS
Validar únicamente con FirmaEC

_____

PhD. Paúl Francisco Baldeón Egas

C.I: 1002807814

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, **Manuel Rodrigo Passo Guamangate** con C.I: **1723741300**, autor del proyecto de titulación denominado: **VULNERABILIDADES EN LA COMUNICACIÓN MULTIPLEXADA DE REDES CAN-BUS PARA LA DETECCIÓN Y MITIGACIÓN DE MENSAJES MALICIOSOS MEDIANTE INTELIGENCIA ARTIFICIAL**. Previo a la obtención del título de Magister en ELECTRÓNICA Y AUTOMATIZACIÓN.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., 10 de septiembre de 2025

Manuel Rodrigo
Passo Guamangate
Time Stamping
Security Data

_____

Ing. Passo Guamangate Manuel Rodrigo

C.I: 1723741300

Tabla de contenidos

Índice de tablas

Índice de figuras

Índice de anexos

INFORMACIÓN GENERAL

Contextualización del tema

En base a estudios y experiencias previas se indica que la comunicación de redes CAN en vehículos actuales las conexiones de datos entre microcontroladores cada vez son más complejas y, sin embargo, las formas de vulnerar el sistema de comunicación vehicular para un control fuera de borda por hackers van en aumento.

Según Aguirre et al. (2021) menciona que:

> En los últimos años, los automóviles están equipados con muchas computadoras a bordo, lo que conduce a nuevos tipos de ataques. De hecho, los sistemas operativos que se ejecutan en los automóviles están expuestos a errores y vulnerabilidades. Dado que los automóviles evolucionan con computadoras a bordo, otras técnicas desarrolladas consisten en hacer que los propietarios instalen software malicioso en su teléfono inteligente que funciona como una cerradura de puerta para hacer que se ejecute alguna acción controlada. (p. 2-3)

Los hackers pueden usar estas vulnerabilidades para lanzar ataques sofisticados que pueden causar pérdidas humanas y daños materiales. Por lo tanto, la seguridad del vehículo debe manejarse con cuidado y no debe comprometer la seguridad del conductor ni de los pasajeros. Tanto la seguridad como la protección deben priorizarse al diseñar una red vehicular, ya que hay vidas humanas en juego. Por lo tanto, la protección contra ataques externos es fundamental en las funciones de conducción automatizada en el vehículo.

Jo and Choi (2022) establece que para abordar la necesidad de conectar diferentes sensores, actuadores y sus controladores entre sí para que puedan tomar decisiones informadas, BOSCH desarrolló un nuevo bus de comunicación en 1983. Por ejemplo, el sistema de control de tracción generalizado (TCS) también conocido como programa de estabilidad electrónica (ESP) podría usar CAN para conectar los sensores en la rotación de las ruedas y actuadores como los frenos que son necesarios la ejecución de control. El TCS monitorea el giro de las ruedas en cada una de las cuatro ruedas y frena intencionalmente las ruedas individuales para recuperar la tracción.

Hoy en día, casi todos los vehículos nuevos en producción en Ecuador y a nivel global utilizan radios de corto alcance integradas para el acceso sin llave a llaveros inalámbricos. Las llaves de seguridad utilizadas en los llaveros de vehículos han sido pirateadas. Los investigadores también han logrado transmitir las señales de radio de un llavero al vehículo sin comprometer sus llaves de seguridad. Esto puede hacerse incluso cuando los llaveros están lejos del vehículo, por ejemplo, cuando el vehículo está en un estacionamiento y el conductor está dentro de un lugar fuera del vehículo y utilizando dispositivos de bajo costo disponibles comercialmente. Esto permite a los atacantes desbloquear fácilmente las puertas para robar o asaltar el vehículo.

Otro tipo de paquetes CAN que se ven en los sistemas automotrices son los paquetes de diagnóstico. Estos paquetes son enviados por herramientas de diagnóstico utilizadas por los mecánicos para comunicarse e interrogar a una ECU. Estos paquetes normalmente no se verán durante el funcionamiento normal del vehículo (Rathore et al., 2022).

Los paquetes CAN están contenidos en un mensaje: cada mensaje está compuesto por valores de seguimiento como:

- Marca de tiempo: tiempo registrado (s);
- CAN ID: identificador del mensaje CAN en HEXADECIMAL;
- DLC: número de bytes de datos, de 0 a 8;
- DATA: valor del dato (byte);

Este trabajo de titulación aborda el cómo proteger los vehículos contra ataques de malware. Proteger los vehículos contra el malware requiere abordar desafíos únicos que no se han abordado adecuadamente en otros tipos de redes. Este trabajo de investigación identifica y analiza estos desafíos y presenta un marco de protección contra malware vehicular basado en la nube que puede abordarlos.

Problema de investigación

El número cada vez mayor de componentes que están conectados a la red de comunicación CAN bus presenta una alta probabilidad de que cualquiera de dichos componentes se vea comprometido desafortunadamente, tal compromiso puede tener severas implicaciones de seguridad y por lo tanto también de seguridad para la red automotriz.

Existen ataques maliciosos que se perpetran a través de tramas CAN bus falsificadas, ya que estos datos tienen campos como la marca de tiempo (timestamp), identificación CAN, conector DLC, PID adulterados y flujo de datos en vivo, esto pudiendo generar alteración de

funcionamiento en los componentes del vehículo ya sea en la línea de sensores o actuadores de las diferentes ECUs automotrices.

"De todas las amenazas posibles, la falsificación de mensajes sigue siendo una de las más importantes sin resolver en los diseños de bus CAN actuales" (Avatefipour et al., 2019, p. 5).

"Así mismo hace mención que, en el peor de los casos, un componente comprometido puede inyectar mensajes CAN falsos, por ejemplo, mensajes que hacen que el asistente de estacionamiento gire el volante" (Marchetti & Stabili, 2017, pp. 3-4).

De acuerdo a la revisión de varios artículos mencionan que en el diseño CAN actual, no hay protección contra estas amenazas. En primer lugar, CAN no tiene ningún esquema para verificar la autenticidad de los mensajes, es decir, ni la información del remitente ni la carga real del mensaje del sistema de comunicación.

En principio, un atacante que controla cualquier componente en el bus CAN, por lo tanto, puede:

- Falsificar la identidad de cualquier otro componente (por ejemplo, para escalar privilegios), o
- enviar carga útil arbitraria (por ejemplo, para realizar acciones maliciosas).

Las redes CAN automotrices son redes de datos en el automóvil. Tienen algunas características importantes que las distinguen de otras redes informáticas. El protocolo CAN es relativamente simple y robusto, y se adapta bien al entorno hostil del motor. Sin embargo, no fue diseñado para incluir las capacidades necesarias para la seguridad cibernética en un entorno conectado, como el reconocimiento de mensajes dirigidos a nodos, la autenticación del remitente o el cifrado. Incluso si se introdujeran en los futuros diseños de automóviles, la gran cantidad de sistemas CAN preexistentes no tendrían estas funciones ampliadas.

Las redes CAN a menudo son críticas para la seguridad, sin embargo, estudios recientes han resaltado las vulnerabilidades de ciberseguridad de CAN. Los ataques demostrados en automóviles reales han consistido en inyectar paquetes CAN que contienen datos maliciosos, o forzar, mientras se conduce, un reinicio de una ECU para inyectar código malicioso. Claramente, a medida que aumenta la cantidad de nodos de interfaz y ECU con el aumento de la conectividad y la autonomía del vehículo, también lo hará el potencial de ciberataque desde fuera de bordo a los diferentes microcontroladores de la red de comunicación vehicular.

A esto se suman los intentos de facilitar la actualización del software de la ECU lo que aumenta el riesgo de infección por código malicioso, por ejemplo, proponen formas de hacer

que la actualización de la ECU sea más rápida, simple y liviana, lo que facilita la actualización del software de la ECU en el aire por medio de programaciones por medio de algoritmos teóricos.

El problema mayor está en considerar que en la actualidad los vehículos modernos contienen muchas ECUs interconectadas y que de manera general todos estos automotores tienen el protocolo CAN, el cual no a sido realizado una mejora en la estructura tecnológica de seguridad, convirtiendo esto en el objetivo prioritario de los ciberataques maliciosos, dando como consecuencia poniendo en riesgo la seguridad activa y pasiva del vehículo y su ocupante.

Con esto se indica que es importante el análisis de las vulnerabilidades que existen en las redes de comunicación CAN para implementar mecanismos de identificación de mensajes de ataques en base a la adaptación de la IA para la detección de patrones anormales en la segmentación del flujo de datos y de esta manera proteger la integridad electrónica de las ECUS automotrices.

Objetivo general

Analizar las vulnerabilidades en la comunicación multiplexada de redes CAN-BUS para la detección y mitigación de mensajes maliciosos mediante inteligencia artificial

Objetivos específicos

- Contextualizar la fundamentación teórica indexada en bases científicas sobre contenidos de protocolos de comunicación de redes CAN-BUS para la comprensión y proyección de información.
- Determinar las principales debilidades del protocolo de comunicación CAN-BUS, poniendo especial atención en aquellas que permiten la falsificación o inyección de mensajes maliciosos.
- Elaborar un informe técnico de las vulnerabilidades en la comunicación multiplexada en redes CAN-BUS, por medio de tramas topológicas.
- Validar la propuesta mediante la aprobación del informe técnico y criterios de especialistas del área automotriz

Vinculación con la sociedad y beneficiarios directos:

Los beneficiarios directos del presente trabajo de titulación será la comunidad estudiantil de la carrera de Mecánica Automotriz, de tal manera que se puede realizar estudios de comportamientos de comunicación entre computadoras automotrices por medio de redes CAN-BUS en base a oscilogramas al usar herramientas de diagnóstico electrónico, tales como: banco

téster de computadoras automotrices, osciloscopio, multímetro, punta lógica, scanner automotriz, caja de desconexión OBD II y simuladores de señales.

Con base en esto, el presente trabajo de titulación no solo beneficia al ámbito académico y científico, sino que también impacta directamente en la seguridad de la sociedad en general. Dada la problemática abordada, el tema de la seguridad electrónica automotriz en las comunicaciones es uno de los más críticos de la seguridad en la actualidad.

Al proponer un análisis y soluciones a las vulnerabilidades en la comunicación multiplexada en redes CAN-BUS la comunidad de técnicos automotrices tendrán información necesaria para diagnosticar de manera eficiente posibles ataques a la red CAN-BUS.

Divulgación de resultados a la comunidad estudiantil de la carrera de mecánica automotriz y sociedad en general por medio de un video explicativo del comportamiento de redes de comunicación CAN bus en base al análisis de ataques de manera remota o directa que se encuentra publicado en el siguiente link:

https://drive.google.com/file/d/1Tu8UBhbXH4ULSG1uRgb99q8DbAlVqG0/view?usp=drive_liNk

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

La evolución tecnológica en la industria automotriz ha revolucionado la manera en que los automóviles funcionan y se comunican internamente. Con la introducción del bus de comunicación CAN por BOSCH, se configuró un estándar sólido y eficiente para la transferencia de datos entre sensores, actuadores y unidades de control electrónico (ECU). Este protocolo permitió la integración de sistemas de seguridad, tanto activos como pasivos, como el control de tracción, el sistema antibloqueo de frenos y el programa de estabilidad electrónica, que dependen de la sincronización y comunicación de datos en tiempo real. Hoy en día, los vehículos contemporáneos están equipados con múltiples ECU que gestionan funciones esenciales, desde la inyección de combustible hasta las ayudas a la conducción. Sin embargo, esta interconexión ha creado una nueva superficie de ataque, haciendo que las redes CAN sean un blanco vulnerable para actores malintencionados. Estudios recientes han demostrado que el protocolo CAN carece de mecanismos nativos para la autenticación, cifrado y verificación de integridad, lo que facilita ataques como la inyección de mensajes, la suplantación de nodos y la manipulación de datos críticos (Aliwa et al., 2021).

> Para el presente trabajo de titulación se hará uso de herramientas de diagnóstico automotriz tales como, osciloscopio, caja de desconexión, scanner automotriz, analizador de tramas de oscilogramas. Sin embargo, el osciloscopio es la herramienta fundamental ya que, dado que la seguridad del conductor depende de la correcta comunicación de estos sistemas, es fundamental garantizar la correcta configuración del bus CAN. Afortunadamente, decodificar y solucionar problemas del bus CAN es fácil con las herramientas adecuadas, como un osciloscopio de señal mixta. En esta investigación, se dará a conocer tips para la resolución de problemas y los instrumentos necesarios para realizar la tarea rápidamente (Hartzell et al., 2020, p. 20; Kang & Shen, 2022, p. 3).

La siguiente investigación muestra que la mayoría de los estudios sobre seguridad CAN-BUS analizan principalmente las vulnerabilidades de CAN, sus posibles defectos y las contramedidas correspondientes. Además, gran parte de los estudios existentes en la literatura que se centran en un aspecto específico de seguridad, realizando una revisión detallada y comparando los mecanismos de seguridad existentes, se centran principalmente en los IDS[1]. Por el contrario,

[1] Sistema de detección de intrusiones

solo unos pocos trabajos analizan específicamente las soluciones de autenticación criptográfica de forma exhaustiva y en profundidad. La ausencia de una revisión exhaustiva de la literatura sobre el marco de autenticación para el bus CAN y las limitaciones que presentan los trabajos existentes nos impiden alcanzar una solución definitiva para los protocolos de autenticación CAN, lo que resalta la importancia de realizar un análisis comparativo exhaustivo y profundo entre los protocolos de autenticación más debatidos y prometedores para CAN. Varios estudios revisan las vulnerabilidades más comunes y debatidas, así como sus amenazas y correcciones correspondientes, junto con posibles contramedidas para soluciones de seguridad (Lotto et al.), (Nagarajan et al.), (Rajapaksha et al.) y (2021). Del análisis de estos estudios, se puede concluir que los enfoques más avanzados para proteger el entorno de bus CAN son los mecanismos basados en cifrado (esquemas de autenticación y cifrado), los IDS, los cortafuegos y la segmentación de red. Sin embargo, estos artículos solo ofrecen una discusión general y de alto nivel sobre posibles contramedidas y soluciones de mitigación, presentando algunos casos prácticos como ejemplos. Los trabajos de los siguientes autores (Rajapaksha) y (Pesé et al.) presentan una sección dedicada a los esquemas de autenticación. No obstante, el análisis de protocolos y, cuando existe, la comparación se realiza desde una perspectiva de alto nivel, sin proporcionar un análisis de seguridad detallado ni criterios de comparación, que es el objetivo del trabajo de investigación. Estos trabajos son de considerable valor y, por lo tanto, constituirán el punto de partida del trabajo de titulación. Las redes consideradas para el estudio de protocolos de comunicación. Para el presente análisis, considero los protocolos más prometedores de la literatura se enlistará más adelante en la sección de fundamentos teóricos (Hartzell et al., 2020; Xie et al., 2021).

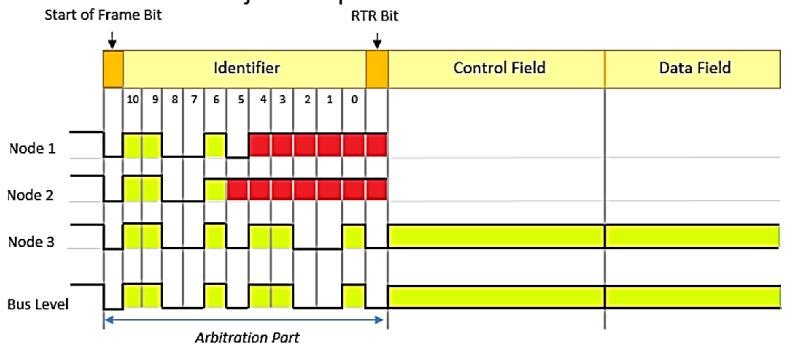
Para finalizar se pretende realizar la aplicación de análisis de protocolos considerados para nuestra comparación. Se muestra una descripción detallada de sus puntos clave de funcionamiento, mientras que la información relacionada con las decisiones de diseño y los resultados de rendimiento se puede encontrar, si no se especifica, en los artículos referenciados anteriormente. Cuando está disponible, también se informa sobre la sobrecarga computacional de cada protocolo. Sin embargo, esto no siempre es posible, ya que algunos artículos no incluyen suficientes detalles sobre la implementación propuesta para realizar una evaluación detallada. Además, algunos estudios se centran en puntos de referencia o evaluaciones de tiempos en lugar de análisis formales. Para el cual se usará un osciloscopio de interfaz y uno de mano para determinar las variaciones de comportamiento de señales de redes CAN de extremo a extremo, un scanner automotriz para la detección del tipo de protocolo de comunicación a estudiar y

analizar, una caja de desconexión que ayudará para determinar las pineras como salidas de análisis de datos paramétricos.

Para cumplir con los requisitos de plazo de los sistemas en tiempo real, a cada mensaje se le asigna un identificador que define su prioridad. Cuanto menor sea el valor de identificación del mensaje, mayor será su prioridad para acceder al bus. Esta función de priorización también resuelve el conflicto de acceso al bus, de modo que, si dos nodos desean enviar datos simultáneamente, la ECU con menor valor de ID publicará primero el mensaje (debido a la mayor prioridad). Esta técnica también se conoce como arbitraje de mensajes. Generalmente, CAN regula el arbitraje de forma predecible y eficiente. La Figura 1 muestra una situación en la que tres nodos (primer nodo: 11001011111 en binario, segundo nodo: 11001111111 en binario y tercer nodo 110010110010 en binario) intentan transmitir un mensaje simultáneamente. Para evitar colisiones de bus, el nodo con el ID más bajo (en este caso, el tercer nodo) transmitirá la información, ya que tiene el valor más bajo y la mayor prioridad que los otros dos nodos. La Figura 1 muestra el arbitraje de mensajes en este escenario (Avatefipour & Malik, 2018; Wu et al., 2020).

Figura 1

Condición de arbitraje en el protocolo CAN-Bus

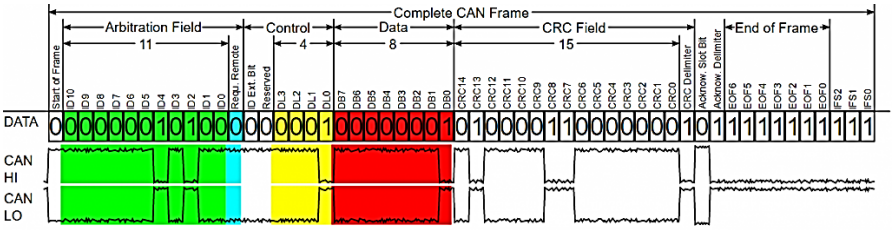


Antes de analizar las vulnerabilidades de seguridad del protocolo CAN-Bus, en esta sección se ofrece una descripción general del protocolo CAB-Bus. Generalmente, existen dos formatos de CAN-Bus: el formato estándar, con 11 bits para el identificador, y el formato extendido, con una trama de identificador de 29 bits. La trama de datos, la trama remota, la trama de sobrecarga y la trama de error son los cuatro tipos principales de tramas en la red de área controlada CAN-Bus. La trama de datos se utiliza para transportar datos desde un transmisor a un receptor y consta de los siguientes campos de bits: inicio de trama (un bit dominante), campo de arbitraje (12 bits), campo de control (6 bits), campo de datos (en un rango de 0 a 64 bytes), campo CRC (16 bits), campo ACK (2 bits) y fin de trama (7 bits) . (Bhatia et al., 2021; Donadel et al., 2025)

La ilustración completa de la trama de datos se muestra en la figura 2. El campo de arbitraje define la prioridad de cada mensaje y, además, un solo bit en este campo define si se trata de una trama de datos o una trama remota. La trama remota permite al receptor solicitar datos adicionales al transmisor. La trama de datos puede tener una longitud de cero (trama remota) a ocho bytes, y el campo de control especifica su longitud. Trama CRC: La trama CRC consta de 16 bits en total; 15 bits se utilizan para el algoritmo de suma de comprobación redundante cíclica (CRC) para la detección de errores y un bit recesivo como delimitador. Campo ACK: El nodo receptor recalcula el CRC y, si coincide, informa al transmisor que el mensaje válido se ha recibido correctamente. Esto se realiza sobrescribiendo el bit recesivo (1 lógico) en la ranura ACK con el bit dominante (0 lógico) (Avatefipour & Malik, 2018; Rajapaksha, 2024).

Figura 2

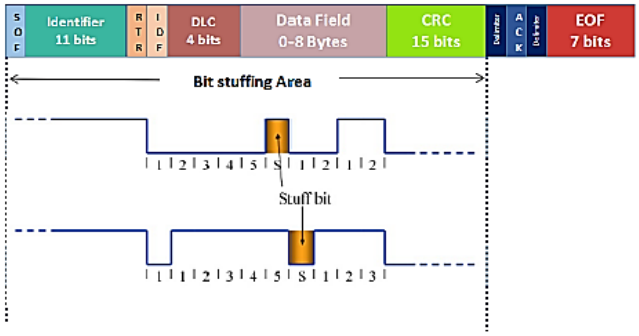
Data frame del CAN bus



La técnica de relleno de bits se utiliza en CAN-Bus. Esto significa que, si se transmiten seis bits idénticos consecutivos en el bus, se considera un error debido a una violación de la ley de relleno de bits. El relleno de bits se puede aplicar en diferentes tramas de CAN-Bus, como el campo de arbitraje, el campo de control y el campo CRC. Esto significa que se añadirá un bit complementario a la trama cuando el transmisor detecte cinco bits idénticos consecutivos. Por lo tanto, seis bits idénticos consecutivos durante la transmisión se consideran una violación de relleno de bits y cada nodo que detecte esta situación transmitirá una trama con error. La figura 3 muestra la trama CAN y cómo se aplica el relleno de bits (Rajapaksha, 2024; Rathore et al., 2022).

Figura 3

Técnica de relleno de bits en CAN-Bus



1.2. Proceso investigativo metodológico

Enfoque: Mixto

Tipo de investigación: Descriptiva y experimental.

Población y muestra: Estudiantes de la carrera de mecánica automotriz y sociedad en general.

Muestra: Estudiantes de la carrera de mecánica automotriz.

Técnicas: Recolección de datos en base al banqueo de ECU y dentro del vehículo, Aplicación de osciloscopio para la detección de las tramas, entrevistas a técnicos del área, análisis documental de la investigación.

Instrumentos: Hojas de verificación, Scanner automotriz, Osciloscopio, Interfaz, Caja de desconexión, Software de IA.

Validación: Revisión y aprobación de resultados por expertos del área.

La investigación se llevará a cabo mediante un enfoque mixto que combina métodos descriptivos y experimentales. Por un lado, tiene como objetivo identificar las vulnerabilidades en la comunicación multiplexada de las redes CAN-BUS. Por otro lado, busca validar empíricamente la detección y mitigación de mensajes maliciosos utilizando inteligencia artificial. El diseño experimental facilitará la creación de escenarios controlados para la inyección de mensajes falsos, proporcionando así evidencia objetiva que respalde la propuesta.

La investigación se llevará a cabo mediante un enfoque mixto que combina métodos descriptivos y experimentales. Por un lado, tiene como objetivo identificar las vulnerabilidades en la comunicación multiplexada de las redes CAN-BUS. Por otro lado, busca validar empíricamente la detección y mitigación de mensajes maliciosos utilizando inteligencia artificial. El diseño experimental facilitará la creación de escenarios controlados para la inyección de mensajes falsos, proporcionando así evidencia objetiva que respalde la propuesta.

Según Murlidharan et al. (2025) describe que:

> Esta investigación utilizará métodos de investigación descriptivos y experimental que pueden describir un suceso o evento basado en hechos y relacionados a la industria automotriz. El método de investigación descriptivo utiliza investigaciones previas relacionadas con el desarrollo de inteligencia artificial en la industria automotriz para producir un análisis de cómo la inteligencia artificial influye en la industria automotriz en la era tecnológica. (p. 11)

De acuerdo a la experiencia que llevo en el área automotriz este tipo de estudio de análisis de comunicación entre computadoras de vehículos (ECU) y evaluar la seguridad en redes de comunicación CAN-BUS, se requiere una combinación de instrumentos de hardware y software los cuales permitirá:

- Capturar tramas de oscilogramas
- Analizar tráfico de datos entre microcontroladores
- Inyectar mensajes maliciosos a la red de comunicación
- Detectar anomalías en la red de comunicación

1.2.1. Técnicas de recolección de datos en base a instrumentos utilizados

1.2.1.1. Hardware

- **Osciloscopio digital**

Para observar y diagnosticar las señales en tramas de la línea CAN-H y CAN-L de esta manera ayudar a validar el nivel de señal, interferencias, voltajes anormales.

- **ECU y/o simulador de red CAN**

Se usará estos emuladores para generar tráfico de datos CAN controlado en un entorno de prueba dentro o fuera del vehículo.

- **Gateway o firewall automotriz**

Para analizar el comportamiento de cómo el tráfico CAN puede segmentarse o filtrarse en los microcontroladores de la ECM automotriz.

1.2.1.2. Software de análisis de tráfico de tramas CAN-bus

Se hará uso de programas que permiten visualizar, filtrar, y analizar tramas CAN, el cual se podrá realizar en base a uso de osciloscopios de interfaces propiamente desarrollados para estos análisis. Para esto usaré la interfaz de osciloscopio picoscope que será la herramienta para este análisis de tramas en topologías en códigos.

Por lo que se seguirá el siguiente procedimiento para la investigación propuesta:

a) Datos

Recopilar datos de bus CAN de la ECU del vehículo Chevrolet Aveo 1.6 año 2006 para el análisis de tráfico capturado simultáneamente desde los buses CAN en el vehículo.

Los bytes de datos de los paquetes insertados se copian de una instancia anterior de ese ID de paquete. Los paquetes borrados simplemente se eliminan de la captura sin otras modificaciones. En estos experimentos, no modificamos el contenido de datos de los paquetes existentes (Olufowobi et al., 2020).

b) Procedimiento del experimento

Según Hernández-Sampieri et al. (2018) y el autor menciona que:

El objetivo de los experimentos a realizar es determinar la sensibilidad de nuestro detector a un rango de velocidades y duraciones de inserción de paquetes. Los datos de prueba se dividieron en segmentos de tres segundos de duración. Alrededor de la mitad de los segmentos se seleccionarán al azar para permanecer inalterados, y así constituir el tráfico normal. La otra mitad se modificará para incluir paquetes adicionales o eliminar paquetes. Para cada segmento modificado, se seleccionará un solo ID de paquete para insertarlo o borrarlo de acuerdo con las reglas descritas anteriormente. Todos los ID serán seleccionados el mismo número de veces para realizar la iteración. (p. 152)

CAPÍTULO II: PROPUESTA

2.1. Fundamentos teóricos aplicados

2.1.1. Protocolo de comunicación CAN-BUS

Según Hartzell et al. (2020) menciona que:

A medida que los vehículos incorporaban sistemas eléctricos más complejos, el cableado eléctrico punto a punto se volvió pesado y costoso. En 1986, la Sociedad de Ingenieros Automotrices propuso la primera red vehicular, conocida como red de área del controlador (CAN). La red propuesta se concibió como una red simple para reducir el cableado y permitir la comunicación de múltiples microcontroladores en un solo bus. (pp. 1-2)

La mayoría de los vehículos utilitarios modernos están equipados con varias controladoras basadas en microprocesadores para controlar diversos subsistemas, incluidos el motor, la transmisión y la gestión del chasis. Para operar de manera óptima, estas controladoras deben intercambiar información continuamente. Si se considera que la cantidad de datos intercambiados puede ser relativamente pequeña, la demanda de información en tiempo real puede ser más elevada. Para satisfacer esta necesidad, es necesario utilizar una única red vehicular que ofrezca soporte para tiempos de transmisión, gran capacidad de manejo de la información y alta confiabilidad (Rajapaksha, 2024).

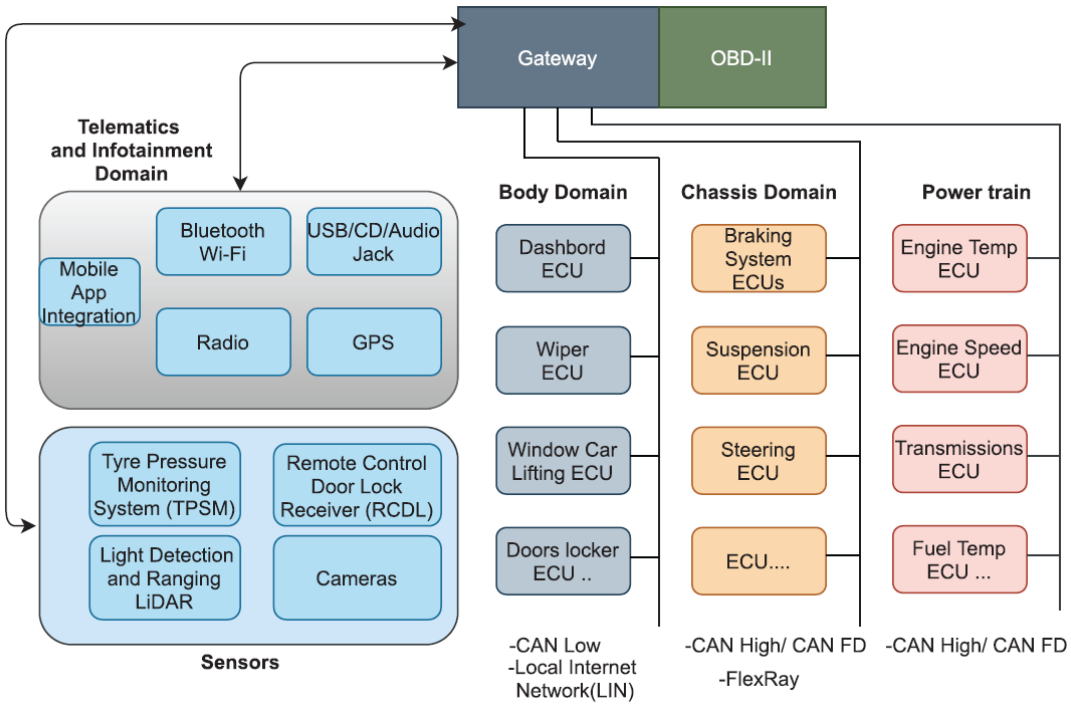
Tres protocolos clave se utilizan dentro de los vehículos para la comunicación de datos: CAN, FlexRay y la Red de Interconexión Local (LIN) ver figura 4. El protocolo CAN Bus es el más utilizado para soportar funciones críticas como el tren de potencia, la gestión del motor, el sistema antifrenos y la transmisión. Un sistema vehicular se divide en cuatro dominios, en términos de la función que realiza y si requiere datos en tiempo real:

- El dominio del tren de potencia, que incluye las funciones del motor y la transmisión; este dominio es crítico y requiere respuesta en tiempo real;
- El dominio del chasis, que incluye el sistema de frenos, la suspensión y la dirección, y que también proporciona funciones críticas de seguridad en tiempo real dentro del vehículo;
- El dominio de la carrocería para funciones como el tablero, los limpiaparabrisas, las luces, las ventanas y los asientos; estas funciones generalmente no requieren respuesta en tiempo real.
- El dominio de telemática e infoentretenimiento, que gestiona los diversos servicios de

comunicación, información y entretenimiento dentro de un vehículo, como la navegación, los reproductores de CD/DVD, los sistemas de entretenimiento para los asientos traseros, la asistencia a la conducción y las interfaces inalámbricas. Estos dominios difieren en las funciones que ofrecen y en el rendimiento y la calidad de la red que requieren. En función de estas diferencias, cada dominio tiene diferentes requisitos de rendimiento y tiempo de respuesta.

Figura 4

Los tres protocolos más populares: CAN, LIN y FlexRay.



El protocolo CAN-Bus ha sido el que ha sobrevivido con mayor éxito y, en consecuencia, se ha convertido en el de uso más extendido en los sistemas de redes vehiculares. Sin embargo, a pesar de su alta eficacia en la comunicación de datos, carece de sistemas de seguridad tales como la identificación de mensajes y el cifrado, sus principales funciones de seguridad. En este punto reside la vulnerabilidad del CAN-Bus frente a ataques cibernéticos. El objetivo de este capítulo es ofrecer una visión general de las redes vehiculares centrándose específicamente en el protocolo CAN-Bus, que es conocido por sus vulnerabilidades que permitieron la infiltración de ataques en el sistema CAN-Bus, tales como la inyección, el spoofing y la denegación (Nagarajan et al., 2023; Rajapaksha et al., 2023).

Figura 5
Red de área de controlador

2.1.1.1. Origen y desarrollo del bus CAN.

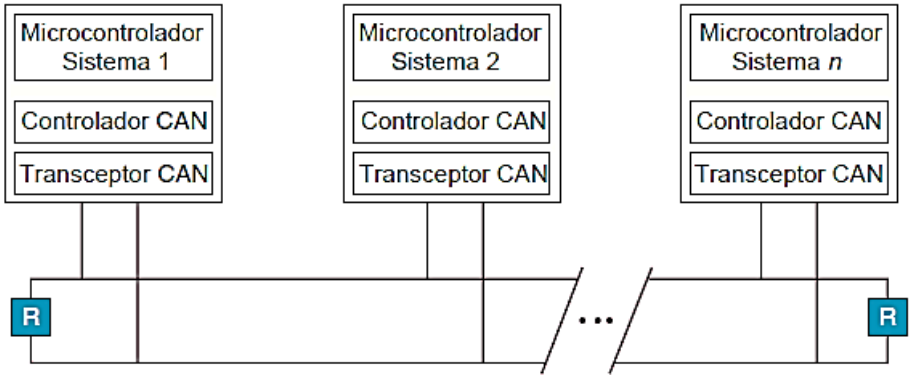
El protocolo de Red de Área de Controlador (CAN-Bus) fue introducido en 1983 por Robert Bosch y se ha aplicado ampliamente en la comunicación automotriz, e incluso en electrodomésticos, dispositivos médicos y entretenimiento. A diferencia del protocolo TCP/IP, donde las direcciones de origen y destino se definen en cada paquete, los mensajes CAN-Bus no tienen direcciones de origen y destino, sino que utilizan la técnica de comunicación por difusión, de modo que cada nodo de la red puede enviar y recibir paquetes hacia/desde el bus (Hartzell et al., 2020; Wen et al., 2020).

Entre los diversos protocolos de red, el bus CAN destaca como la opción predominante para la comunicación en el vehículo, gracias a sus numerosas ventajas, como su bajo coste, alta velocidad, diseño ligero, robustez e instalación simplificada. El bus CAN funciona como un protocolo basado en mensajes, lo que facilita la comunicación entre diferentes ECU (Bloom, 2021). El bus CAN se clasifica a su vez en bus CAN de alta velocidad y bus CAN de baja velocidad según la velocidad de datos. La variante de alta velocidad opera con una velocidad de bits que oscila entre 125 kbps y 1 Mbps, mientras que la variante de baja velocidad varía entre 5 kbps y 125 kbps. El bus CAN admite una carga útil de hasta 8 bytes. Las ECU con funciones críticas en el tiempo, como el control del motor y el control de la transmisión, generalmente se conectan al bus CAN de alta velocidad, mientras que las ECU que manejan funciones menos sensibles al tiempo, como el control de puertas y el control de luces, se conectan al bus CAN de baja velocidad. Estos dos buses están interconectados a través de una puerta de enlace. Además, el protocolo CAN Flexible Data (CAN-FD) amplía las capacidades del bus CAN tradicional al admitir una tasa de bits de hasta 8 Mbps y una carga útil máxima de 64 bytes (Contreras-Castillo et al., 2018; Rajapaksha, 2024).

2.1.1.2. Estructura y funcionamiento.

El bus CAN, mostrado en la figura 6, es un sistema de comunicación diferencial multimaestro. En esta red, los mensajes intercambiados son multidifusión, lo que significa que cada componente conectado al bus CAN recibe todos los mensajes. Todos los mensajes se envían y reciben de forma regular y sincronizada. Este diseño permite la integración de múltiples sistemas diseñados por diferentes empresas. Además, es robusto ante fallos leves de nodos individuales (Araujo-Filho et al., 2021; Hartzell et al., 2020).

Figura 6
La arquitectura de bus CAN de alto nivel



En un vehículo promedio, suelen existir múltiples redes de bus CAN, conectadas entre sí por una puerta de enlace común. Se puede acceder físicamente a la puerta de enlace a través del puerto OBD-II (diagnóstico a bordo II) del vehículo, un conector accesible que se utiliza para informar del estado de los sistemas del vehículo durante las revisiones o reparaciones programadas (Ben Chehida Douss et al., 2023).

Aunque el bus CAN admite velocidades de datos de hasta 1 Mbps, la mayoría de los vehículos tienen una velocidad de datos de 500 kb/s. El bus CAN también tiene una verificación de redundancia cíclica (CRC) para garantizar la integridad del mensaje al recibirlo en cualquier nodo (Bozdal et al., 2020; Hartzell et al., 2020).

Un nodo CAN consta de tres componentes principales: un programa de aplicación, un controlador CAN y un transceptor CAN. El programa de aplicación escribe/lee los datos del mensaje y su identificador (ID) en el controlador. El controlador es responsable del entramado, el arbitraje del bus, el envío/recepción de acuses de recibo y la gestión de errores. Finalmente, el transceptor traduce el flujo de bits que sale del controlador CAN en una señal de voltaje que se transmite por el bus. Cabe destacar que el código de aplicación no puede controlar directamente el controlador CAN para la transmisión de bits individuales en el bus, ni tampoco

puede controlar con precisión el tiempo de transmisión de un mensaje (Serag et al., 2021; Taylor et al., 2015).

2.1.1.3. Composición de los mensajes.

El autor y (Araujo-Filho et al., 2021) describen que:

> Dado que CAN no se diseñó pensando en la seguridad, una ECU comprometida puede ser explotada para lanzar diversos ataques a otras ECU críticas para la seguridad, que no pueden ser comprometidas directamente. En la presente investigación, se estudia un tipo alarmante de ataque que explota directamente el mecanismo de gestión de errores y confinamiento de fallos de CAN, convirtiendo su función en una debilidad de seguridad. (p. 2)

Comunicación de bits: El transceptor comunica un bit (0/1) en el bus mediante un valor de voltaje de dos niveles (alto/bajo).

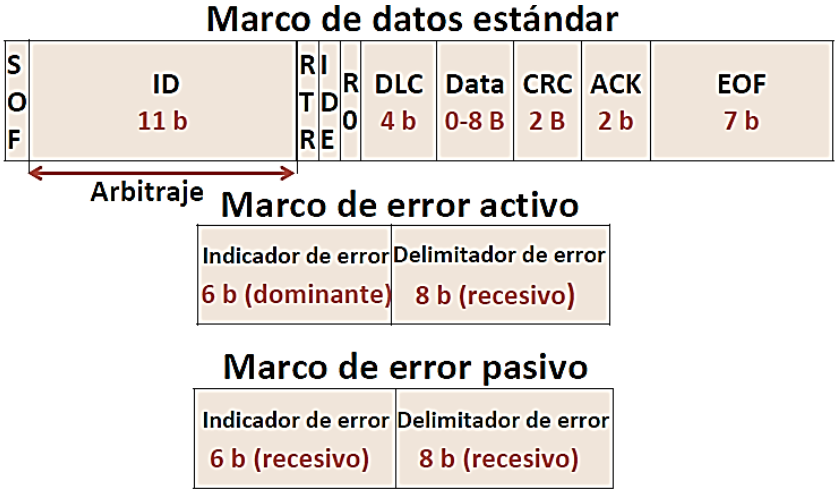
Por lo tanto, los bits 0 y 1 se denominan bits dominantes y recesivos, respectivamente. Durante la transmisión simultánea de diferentes bits por dos o más nodos, el bus actúa como una puerta AND cableada; por ejemplo, cuando un bit dominante y uno recesivo se transmiten simultáneamente, el bit resultante en el bus es dominante (Serag et al., 2021; Wen et al., 2020).

Entramado: Se pueden utilizar dos formatos de trama de datos: el estándar y el extendido. Como se muestra en la figura 7, en el formato estándar, el ID tiene una longitud de 11 bits. El ID no indica el origen ni el destino del mensaje, sino que describe el significado de los datos que contiene. Por lo tanto, la ECU del receptor no puede determinar el origen. Aunque no se pretende que tenga ningún impacto en la seguridad, este hecho funciona como un arma de doble filo: facilita los ataques de suplantación de identidad, pero al mismo tiempo proporciona anonimato al transmisor (Wen et al., 2020; Xie et al., 2021).

Arbitraje: CAN utiliza arbitraje bit a bit sin pérdidas para detectar colisiones y establecer prioridades de transmisión. Si dos nodos comienzan a transmitir simultáneamente, primero pasan por una fase de arbitraje, que comienza en el campo ID y termina en el bit RTR, como se muestra en la figura 7. Los controladores CAN detectan el bus al transmitir cada bit. Durante el arbitraje, si un controlador que envía un bit recesivo detecta que el bus es dominante, detiene la transmisión. En consecuencia, este mecanismo otorga mayor prioridad a los mensajes con un valor de ID menor. Después del arbitraje, si un controlador que envía un bit recesivo detecta que

el bus es dominante, detiene la transmisión y genera un error (Serag et al., 2021; Zhang et al., 2014).

Figura 7
Diferentes marcos CAN

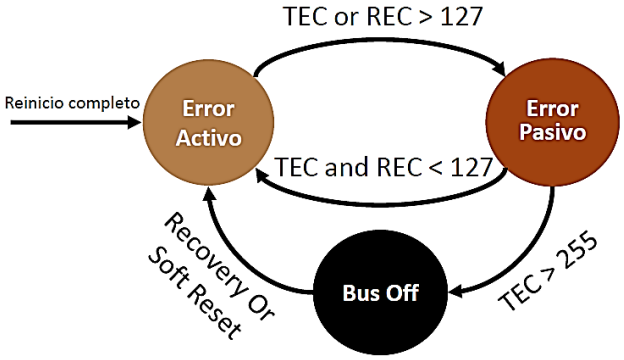


2.1.1.4. Manejo y confinamiento de fallas.

Errores CAN: CAN define cinco tipos de errores: errores de bit, errores de contenido, errores de formulario, errores de acuse de recibo y errores de CRC. Estos errores pueden ocurrir durante la transmisión o la recepción. Cada nodo mantiene dos contadores: el contador de errores de transmisión (TEC) y el contador de errores de recepción (REC). Cuando un transmisor detecta un error, envía una trama de error y aumenta el TEC en 8. De igual forma, cuando un receptor detecta un error, envía una trama de error y aumenta el REC en 1. Una transmisión exitosa reduce el TEC en 1 y una recepción exitosa reduce el REC en 1. El formato de las tramas de error varía según el estado de error del nodo (Bloom, 2021; Jo & Choi, 2022).

Estados de error: Para limitar las fallas, CAN define tres estados de error, como se ilustra en la figura 8.

Figura 8
Estados de error en el bus CAN



Error activo: Un nodo se encuentra en este estado por defecto. En este estado, el tiempo mínimo de inactividad entre dos tramas consecutivas es de 3 bits. Además, en este estado, cuando el nodo detecta un error, envía una trama de error activa, compuesta por 6 bits dominantes, seguida de 8 bits recesivos como se muestra en la figura 7. Las tramas de error activas anulan y terminan cualquier transmisión en curso (Kang & Shen, 2022; Serag et al., 2021).

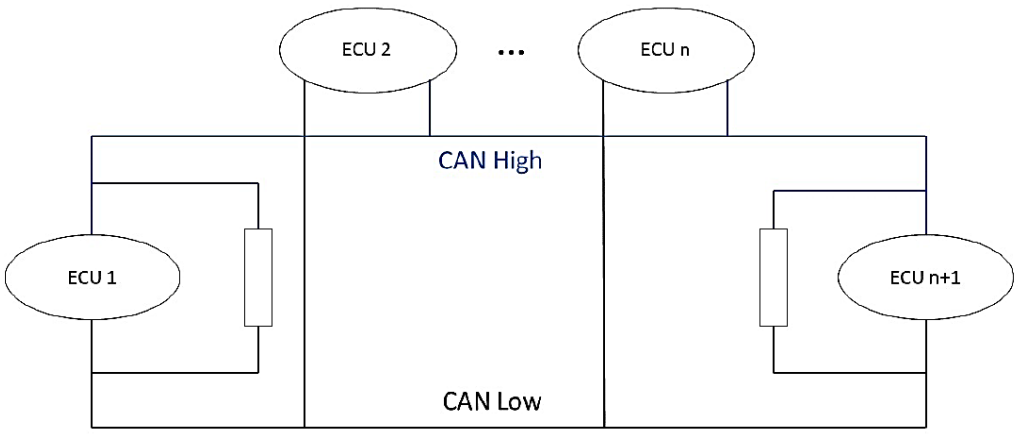
Error pasivo: Un nodo entra en este estado cuando su REC o TEC supera 127. En este estado, se añade un periodo de suspensión de transmisión de 8 bits entre transmisiones sucesivas. Además, al detectar un error, el nodo transmite una trama de error pasiva, compuesta por 14 bits recesivos como se muestra en la figura 7. A diferencia de la trama de error activa, una trama de error pasiva no es observable en el bus y no interrumpe ninguna transmisión en curso (Minawi et al., 2020; Serag et al., 2021).

Bus desactivado: Un nodo entra en este estado cuando su TEC supera los 255. En este estado, el nodo se desconecta de la red. Deja de transmitir o recibir mensajes. El nodo puede volver al estado de error activo tras observar al menos 128 instancias de 11 bits recesivos en el bus (Rajapaksha, 2024; Serag et al., 2021).

2.1.1.5. Topologías y tramas multiplexadas en redes automotrices.

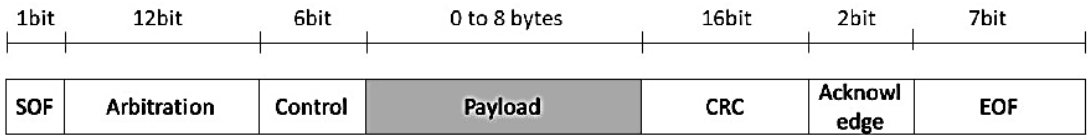
Las colisiones se resuelven mediante una comunicación basada en prioridades, donde el identificador de mensaje más bajo, contenido en el campo de encabezado de las tramas, tiene la máxima prioridad. CAN utiliza par trenzado sin blindaje (UTP) de cables de cobre, donde un cable se denomina CAN Alto y el otro CAN Bajo. La señal entre los dos cables tiene un voltaje de 2,5 V; cuando aparece un bit dominante 0, el voltaje de CAN Alto aumenta el valor nominal en 1 V; en cambio, el voltaje de CAN Bajo lo disminuye en 1 V. Cuando aparece un 1 lógico, tanto CAN Alto como CAN Bajo tienen 2,5 V (Cataldo, 2021; Li et al., 2024).

Figura 9
Estructura de red CAN bus



En la figura 10 se muestra un marco de datos CAN estándar, que contiene hasta 8 bytes de datos, donde:

Figura 10
Marco de datos del bus CAN



- **SOF:** Subraya el inicio de la transmisión de la trama;
- **Arbitraje:** Los primeros 11 bits corresponden al identificador (ID) que establece la prioridad de la trama de datos. Como se explicó anteriormente, el ID más bajo indica la máxima prioridad. El duodécimo bit corresponde a la solicitud de transmisión remota, igual a 0 para la trama de datos;
- **Control:** Este campo contiene la longitud de la carga útil (4 bits) y más de dos bits para el protocolo;
- **Payload:** Datos;
- **CRC:** Se utiliza para verificar la transmisión, como se explica más adelante;
- **ACK:** Confirmación del campo CRC;
- **EOF:** Siete bits recesivos para finalizar la trama.

CAN también posee muchas detecciones de errores como:

- Comparación del campo CRC entre la trama transmitida y la recibida;
- Los contadores de errores (contador de errores de transmisión TEC y Contador de errores de recepción REC) se modifican cuando una trama se recibe correctamente o contiene un error.

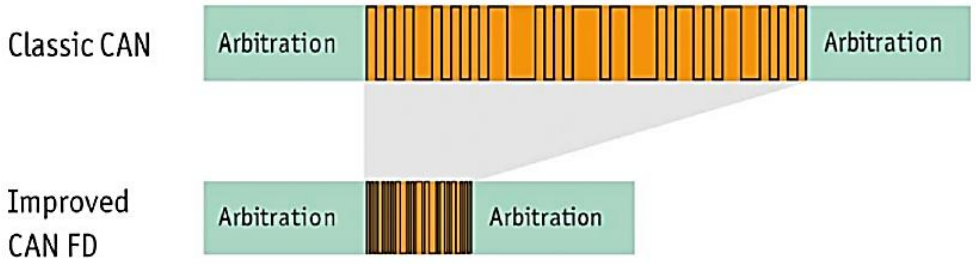
Cuando un nodo CAN detecta un error, se envía una trama de error específica a todos los demás nodos conectados a la red CAN.

2.1.1.5.1. CAN-FD

Se debe prestar especial atención a CAN-FD, la última versión de la red CAN, con velocidad de datos flexible. En este caso, la carga útil aumenta de 8 bytes de CAN a 64 bytes. Esto reduce la sobrecarga y aumenta la eficiencia. CAN-FD se utiliza para velocidades de datos de 2 a 5 Mbps;

esta velocidad se alcanza porque el arbitraje no es útil durante alguna parte de la trama (Cataldo, 2021; Hartzell et al., 2020).

Figura 11
Comparación del campo de arbitraje entre CAN y CAN-FD.



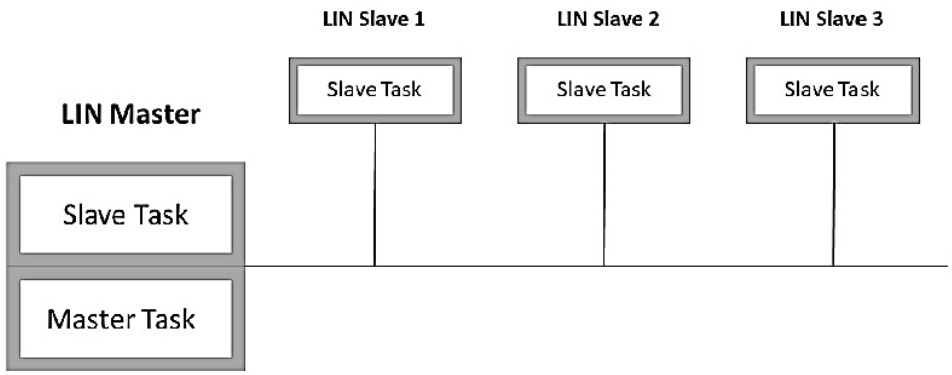
2.1.1.5.2. LIN

Para algunas aplicaciones, como ventanas, espejos, asientos, control del aire acondicionado y muchas otras, la tecnología CAN resulta demasiado costosa y ofrece demasiada protección para aquellas aplicaciones que no requieren seguridad ni velocidad. Por ello, a finales de la década de 1990, el Consorcio LIN, compuesto por empresas (Volkswagen, BMW, Volvo y Daimler), desarrolló la Red de Interconexión Local (LIN) (Wen et al., 2020; Zhang et al., 2014).

LIN se diseñó con un cable sin blindaje de un solo cable, con una velocidad de datos limitada a 20 Kbit/s y opera a 12 V nominales con símbolos binarios: dominante 0 y recesivo 1.

Es un sistema de bus maestro/esclavo simple con dos tipos de ECU: una LIN maestra y varias LIN esclavas, como se muestra en la figura 12. Las ECU esclavas solo pueden transmitir tras ser consultadas por la ECU maestra con el encabezado correspondiente. La programación se predefine en la fase de diseño en una tabla de programación, que contiene la lista de tramas que deben enviarse y el período de tiempo programado, de hecho, cada trama se transmite dentro de un período de tiempo, llamado Frame Slot (Cataldo, 2021; Serag et al., 2021).

Figura 12
LIN bus



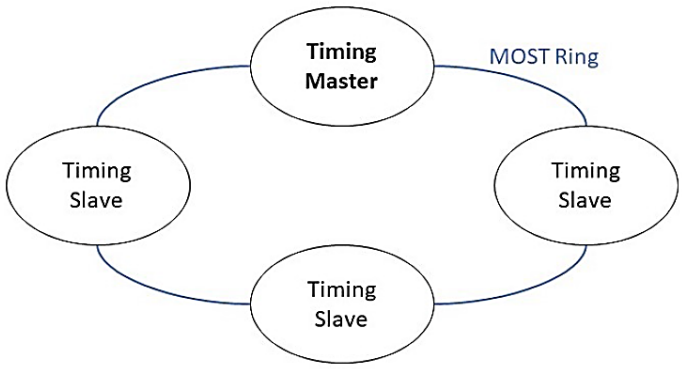
2.1.1.5.3. MOST

MOST se desarrolló para optimizar el transporte de datos de audio y vídeo, ya que las redes CAN y LIN no pueden garantizar un alto ancho de banda para dicho fin. En particular, MOST150, la última tecnología MOST, puede alcanzar los 150 Mbps y es compatible con el Canal de Paquetes Ethernet con funcionalidades del Protocolo de Internet (IP) (Cataldo, 2021; Hartzell et al., 2020).

MOST se basa en todas las capas del modelo OSI. Como capa física, suele funcionar con cable de fibra óptica plástica (POF) para evitar problemas de compatibilidad electromagnética y garantizar el aislamiento eléctrico. Sin embargo, MOST150 también admite cable coaxial. Ambas capas físicas ofrecen ventajas en términos de ancho de banda, pero son demasiado costosas. De hecho, esta razón, y muchas otras que se explicarán más adelante, llevaron a una rápida disminución en el uso de la tecnología MOST (Hartzell et al., 2020; Li et al., 2024).

Dado que esta tecnología es síncrona y se basa en el Acceso Múltiple por División en el Tiempo (TDMA), todos los nodos tienen la misma conexión para evitar colisiones. MOST utiliza una topología de anillo, como se muestra en la figura 13, con una ECU que funciona como maestra de sincronización, lo que permite la sincronización, mediante mensajes de sincronización, con todas las demás ECU. La ECU maestra inicia la comunicación unidireccional con el siguiente nodo, quien transmite la trama al siguiente nodo hasta que llega al receptor (Cataldo, 2021; Lotto et al., 2025).

Figura 13
Topología de anillo MOST



2.1.1.5.4. FlexRay

Según Cataldo (2021) “FlexRay presenta numerosas ventajas y desventajas, pero muchas empresas han dejado de usarlo o están dejando de usarlo, centrándose en Ethernet automotriz” (p. 21).

La tecnología se basa en ciclos, que son una combinación de dos tipos de ventanas: activadas por tiempo (estáticas) y activadas por eventos (dinámicas). La primera utiliza un protocolo de Acceso Múltiple en el Dominio del Tiempo (TDMA), donde existen múltiples ranuras idénticas divididas en el tiempo. Si un nodo no tiene que transmitir, se envía una trama nula, de modo que siempre se recibe algo (Cataldo, 2021; Minawi et al., 2020).

"La segunda utiliza el Acceso Múltiple por División de Tiempo Flexible (FTDMA), donde el tiempo se divide en subranuras y cada estación puede iniciar la comunicación dentro de su subranura" (Cataldo, 2021, p. 22).

En cuanto a la topología, esta red es muy flexible: puede utilizarse: bus lineal, estrella activa y pasiva, y punto a punto, como se muestra en las figuras 14 y 15. La topología también puede ser redundante utilizando canales duales (Bozdal et al., 2020; Cataldo, 2021).

Un formato de trama FlexRay, mostrado en la figura 16, consta de tres partes: encabezado, carga útil y pie de página. En el encabezado se encuentran:

- **Bit de estado:** Representa el inicio de la trama, que puede ser una trama nula, una trama de sincronización o una trama de inicio.

Figura 14
Topología de bus estrella FlexRay

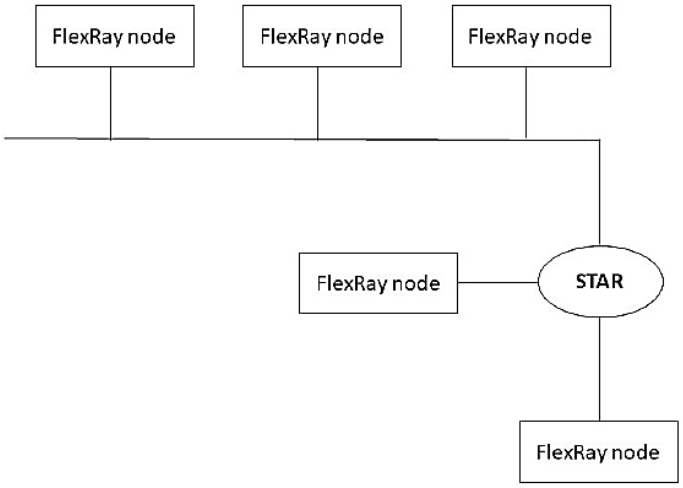


Figura 15
Topología de bus lineal FlexRay

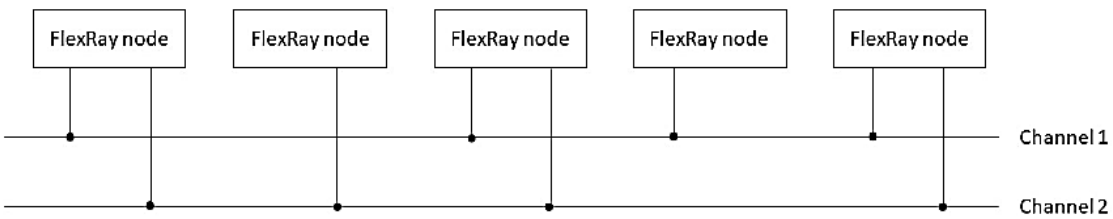
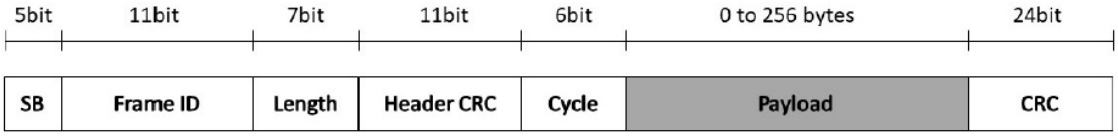


Figura 16
ID de trama FlexRay



ID de trama: identificador único de la trama;

Longitud: longitud de la sección de datos;

CRC de encabezado: comprobación de errores de la sección de encabezado;

Ciclo: número del ciclo.

En cambio, la sección de pie de página se compone del campo CRC para comprobar errores en la carga útil.

A continuación, se presenta la siguiente tabla de comparaciones entre protocolos de comunicación vehiculares.

Tabla 1
Clasificación de los protocolos de comunicación de la red en el vehículo

Protocolos de comunicación de red en el vehículo	Dominio	Ancho de banda	Características destacadas	Desventajas	Topología	Estándar	Cableado	Máximo de nodos admitidos	Mensajería
Red de área del controlador (CAN)	Tren motriz, control de la carrocería	125 Kbps–1 Mbps	Bajo costo	Menos ancho de banda	Estrella, Anillo, Bus lineal	ISO 11898	UTP	30	Multi-Master
Red de interconexión local (LIN)	Aplicaciones sencillas (menos críticas en términos de tiempo)	125 Kbps–1 Mbps	Bajo costo	Baja velocidad	Autobús de línea	ISO 17987	Cableado de 1 cable	16	Amo-esclavo
FlexRay	Control avanzado del chasis	Hasta 10 Mbps	Alta velocidad	Alto costo	Estrella, bus lineal, híbrido	ISO 17458	UTP	22	Multi-Master

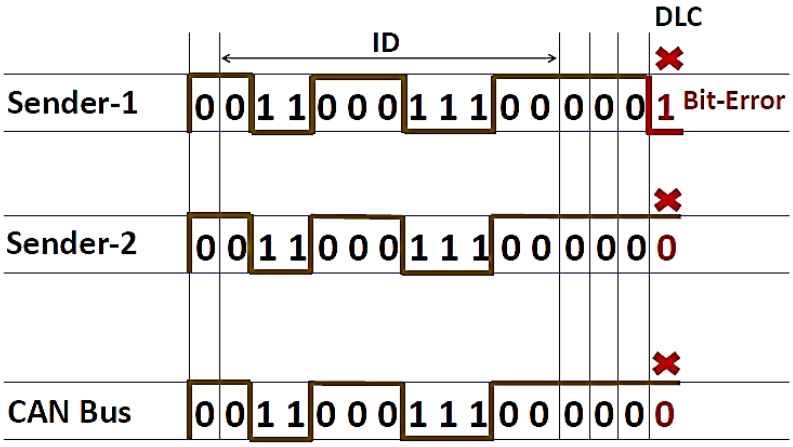
Sistemas de transporte orientados a los medios (MOST)	Aplicaciones de infoentretenimiento	Hasta 150 Mbps	Alta velocidad	Alto costo	Anillo	ISO 21806	UTP y Óptico	64	Flujos/Cuadros cíclicos
Ethernet automotriz	Aplicaciones de gran ancho de banda	Hasta 100 Mbps	Alta velocidad	Alto costo	Estrella, bus lineal	ISO 21111	UTP	Basado en puertos Switch	Basado en IP

2.1.2. Vulnerabilidades en redes de comunicación automotriz

2.1.2.1. Superficie de ataque en redes CAN-BUS.

Colisiones deliberadas de paquetes. Los autores proponen un método para provocar colisiones deliberadas en el bus mediante errores de bits. El método implica que dos nodos transmitan simultáneamente mensajes con el mismo ID, pero con diferente contenido, como se muestra en la figura 17. Para lograr la transmisión simultánea con un ID de mensaje específico, se debe conocer el tiempo de llegada del mensaje para ese ID. El Apéndice A explica con más detalle cómo sincronizar dos mensajes para provocar una colisión (Aliwa et al., 2021; Ben Chehida Douss et al., 2023).

Figura 17
Producción de un bit-error



2.1.2.2. Tipos de ataques: inyección, suplantación, denegación de servicio y manipulación de datos.

Los buses CAN clásicos y CAN FD son vulnerables a diversos ataques. Una vez que los atacantes acceden desde dentro o fuera del vehículo, pueden generar diversos ataques a la red CAN Bus, como rastreo de CAN, fuzzing de CAN, reproducción de CAN y ataques de denegación

de servicio (DoS). Algunos de los mecanismos para iniciar estos ataques son los siguientes (Aliwa et al., 2021).

2.1.2.2.1. Rastreo del bus CAN.

Sin mecanismos de autenticación, cifrado ni transmisión de difusión, es posible rastrear los datos del bus CAN. Utilizando un rastreador OBD2 estándar, como la placa codificada, es posible leer y analizar los datos del bus para manipularlos y generar mensajes similares. Este ataque puede evitarse implementando cifrado para evitar la exposición de las tramas CAN. Este ataque es difícil de detectar debido a la naturaleza pasiva del tráfico de rastreo. El siguiente paso es aplicar ingeniería inversa a los mensajes CAN sin procesar para que puedan utilizarse para atacar partes específicas del vehículo. Este paso es importante, ya que los fabricantes no suelen publicar sus especificaciones de mensajes CAN (Aliwa et al., 2021; Cataldo, 2021).

2.1.2.2.2. Ataque de fuzzing del bus CAN.

El protocolo del bus CAN carece de autenticación y verificación de la integridad de los datos, por lo que las ECU aceptan mensajes CAN y responden a ellos. Este ataque se utiliza para enviar tramas de datos CAN aleatorias, verificando el bus y observando cambios en el panel de instrumentos del vehículo. Este ataque analiza el impacto de las tramas CAN en las ECU, como la observación de cambios en la velocidad del vehículo al inyectar tramas CAN. Suele ocurrir tras rastrear y analizar los mensajes CAN capturados. También puede generarse mediante una caja negra, donde el ID CAN y los valores de carga útil se generan aleatoriamente sin conocimiento previo del ID CAN utilizado. Implica el envío de tramas CAN capturadas aleatoriamente y el registro del resultado. Se requiere cifrado para evitar el análisis de los datos capturados, junto con autenticación para aceptar únicamente tramas CAN de ECU legítimas (Aliwa et al., 2021; Rajapaksha et al., 2023).

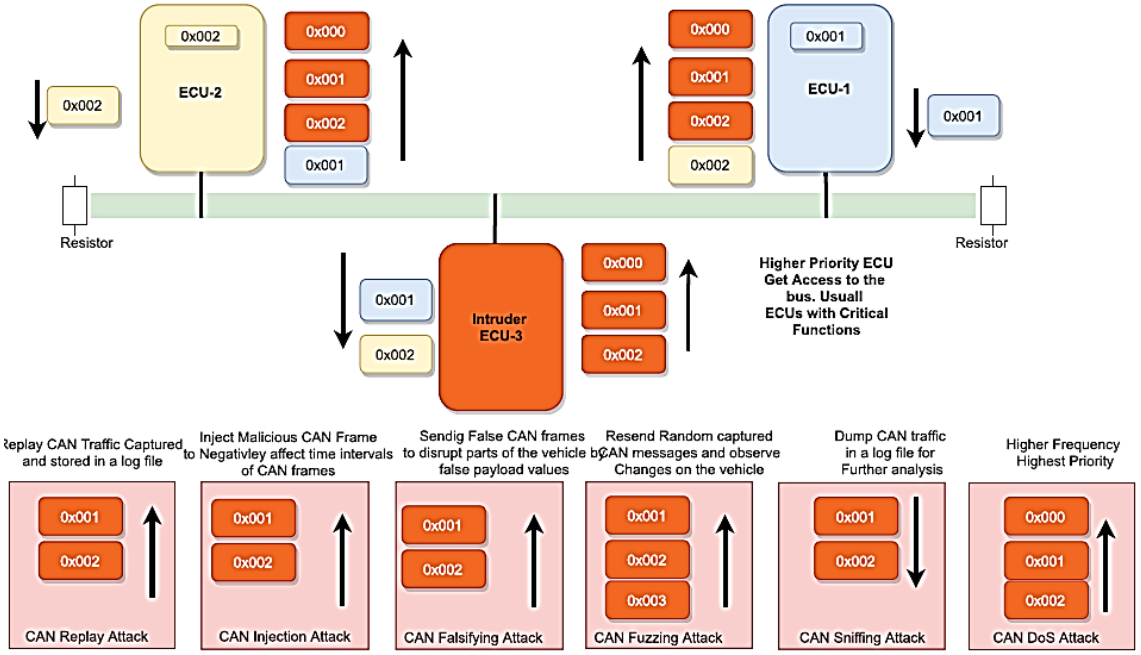
2.1.2.2.3. Ataque de falsificación de tramas del bus CAN.

Este ataque se utiliza para modificar la carga útil de los mensajes CAN mediante la inserción de valores incorrectos. Por ejemplo, el atacante puede inyectar valores de parámetros incorrectos en un vehículo. Este tipo de ataque de modificación se utiliza cuando se conoce el ID de CAN y la intención es proporcionar una carga útil de datos incorrecta para interrumpir los servicios del vehículo. Esto se debe a la falta de integridad de los datos y compatibilidad con la autenticación en el protocolo del bus CAN. Para prevenir este ataque, el bus CAN debe proporcionar autenticación para verificar el origen de los datos antes de actuar. Normalmente, este ataque implica una pequeña cantidad de datos, lo que dificulta su detección y monitorización. Para detectarlo, un sistema debe considerar la comprobación de la consistencia

del ID de CAN y la carga útil de datos en un intervalo de tiempo (Aliwa et al., 2021; Bloom, 2021; Rajapaksha et al., 2023).

Figura 18

Descripción general de algunos ataques a la red de bus CAN del vehículo (IVN)



2.1.2.2.4. Ataque de inyección de bus CAN.

La inyección de datos en un bus CAN permite enviar mensajes a una velocidad anormal. El objetivo de este ataque es modificar la frecuencia y la cantidad de tramas CAN en el bus, así como la secuencia de tramas CAN legítimas y la carga útil de datos. Dado que el bus CAN no proporciona autenticación para verificar la legitimidad del remitente, este ataque inyecta tráfico CAN anormal en el bus, dirigido a la velocidad del vehículo. La falta de cifrado también permite que nodos arbitrarios se conecten al bus. Los datos del bus pueden monitorizarse para obtener el arbitraje y el campo de datos, y generar mensajes para simular eventos. Esto podría generar eventos falsos que hagan que partes del vehículo se comporten según lo requerido por el atacante. Este ataque puede prevenirse mediante mecanismos de autenticación e integridad. El resultado del ataque puede aumentar la frecuencia de ciertos ID de CAN que pueden detectarse mediante un comportamiento anormal (Bozdal et al., 2020; Cheng et al., 2020).

2.1.2.2.5. Ataque DoS de bus CAN.

Los nodos CAN clásicos y CAN FD utilizan el mismo mecanismo para acceder al medio con acceso múltiple mediante la prioridad del ID de CAN. Los nodos en el bus CAN utilizan el campo de arbitraje para determinar la prioridad del mensaje y qué nodo puede ocupar el bus y enviar datos. En este caso, se puede iniciar un ataque DoS utilizando el ID de atribución más alto, como

0x000, para ocupar el bus y mantenerlo ocupado mediante el esquema de arbitraje de prioridad de trama CAN y enviar demasiadas tramas de máxima prioridad para que otros nodos no puedan utilizar el bus. Además, se puede utilizar el mismo ID de mensaje CAN de una ECU existente y, al conocer su velocidad de transmisión, se puede realizar un DoS incrementando el tiempo de frecuencia. Por ejemplo, si una ECU envía un mensaje cada 200 ms, el atacante puede aumentar la frecuencia inyectando el mismo mensaje con una frecuencia más alta, lo que puede provocar la interrupción del sensor (Donadel et al., 2025; Fakhfakh et al., 2021).

2.1.2.2.6. Suplantación de ECU.

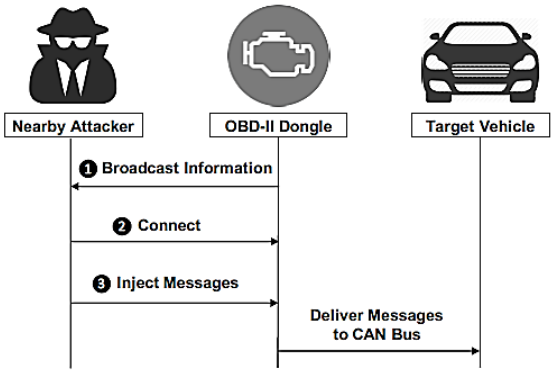
Una vez que un atacante accede a la red CAN Bus, puede recibir todo el tráfico disponible en el bus. Mediante un análisis preciso del tráfico, los atacantes pueden comprender el comportamiento de cada ECU, como su ID CAN, rango de carga útil y velocidad de transmisión. De esta forma, pueden simular el comportamiento de la ECU enviando los mismos datos con la misma frecuencia. Un aumento en la velocidad de los mensajes CAN generará un ataque. Sin embargo, si el ataque fuera más específico, podrían iniciar un ataque para deshabilitar ECU específicas. Por ejemplo, Aliwa et al. (2021) introdujeron un sofisticado ataque de suplantación de ECU. Primero, atacaron una ECU aprovechando el mecanismo de gestión de errores del protocolo CAN Bus. Este ataque funciona imitando el comportamiento de la ECU objetivo, su ID CAN y su frecuencia. Luego, la ECU atacante contradice a la ECU objetivo enviando un bit dominante mientras que la ECU original envía un bit recesivo. Esto generaría un error en el controlador de la ECU que, en cierto punto, provocaría la desconexión de la ECU del bus y la interrupción de la comunicación del bus CAN. Esto permite a un atacante realizar diversos ataques, como un ataque de suplantación de la ECU, difícil de detectar (Taylor et al., 2015; Wu et al., 2020).

2.1.2.3. Consecuencias de las vulnerabilidades en la seguridad del vehículo.

El objetivo del atacante que se considera es explorar la nueva superficie de ataque vehicular expuesta por los nuevos adaptadores OBD-II inalámbricos y, de este modo, lograr ataques inalámbricos al bus CAN del vehículo víctima. Por lo tanto, el atacante debe estar dentro del alcance de la red inalámbrica para poder establecer una conexión con el adaptador objetivo, que suele estar a una distancia de hasta 100 metros. Sin embargo, con un amplificador, un atacante puede detectar señales inalámbricas a una distancia remota (por ejemplo, hasta 1000 metros utilizando la antena BLE), lo que le permite descubrir y acercarse a la víctima para realizar ataques (Serag et al., 2021; Wen et al., 2020).

El modelo general de amenaza se presenta en la figura 19. Antes del ataque, el primer paso, pero muy importante, es identificar un adaptador OBD-II cercano en el aire. Posteriormente, intenta establecer una conexión con él a través de la red inalámbrica. Si la conexión se establece correctamente, intenta atacar el vehículo inyectando mensajes maliciosos en el bus CAN a través del adaptador OBD-II, por ejemplo, leyendo datos confidenciales o provocando comportamientos de conducción inseguros. El ataque tiene éxito si el adaptador envía los mensajes al bus CAN y se desencadenan las consecuencias del ataque (Wen et al., 2020; Yánez & Francisco, 2023).

Figura 19
Modelo general de amenaza



2.1.2.3.1. Superficie de ataque

Antes de diseñar nuestra herramienta automatizada de análisis de seguridad, es necesario identificar exhaustivamente la superficie de ataque de estos dispositivos OBD-II inalámbricos. Según investigaciones previas un ataque exitoso debe tener las siguientes tres etapas: (I) Etapa de transmisión, es decir, cuando el atacante busca dispositivos víctimas antes de la conexión; (II) Etapa de conexión, es decir, cuando el atacante se conecta con el dispositivo; y (III) Etapa de comunicación, es decir, cuando el atacante inyecta mensajes maliciosos después de la conexión (Wen et al., 2020; Wu et al., 2020).

Por lo tanto, la superficie de ataque considerada en nuestro análisis se define como los vectores de ataque en cada una de estas tres etapas:

(I) Etapa de transmisión: Antes de conectarse, un dispositivo OBD-II inalámbrico transmite su información de conexión a los dispositivos cercanos para indicar su disponibilidad. Por lo tanto, los dispositivos cercanos pueden detectarlo, reconocerlo e intentar establecer una conexión. Como atacante cercano, puede recopilar esta información de transmisión y su objetivo es identificar el dispositivo víctima y establecer la conexión basándose en ella (Nagarajan et al., 2023; Wen et al., 2020).

(II) Etapa de conexión: En esta etapa, la tarea del atacante es establecer una conexión de red con el dispositivo para enviarle comandos relacionados con la entrega de mensajes del bus CAN. Al establecerse la conexión, es posible que se le soliciten credenciales suficientes, como una contraseña o un código PIN, antes de conectarse legítimamente al dispositivo. Si no se necesitan credenciales, el atacante puede conectarse al dispositivo arbitrariamente (Pesé et al., 2021; Wen et al., 2020).

(III) Etapa de comunicación: Una vez establecida la conexión, el atacante puede enviar mensajes no autorizados del bus CAN para comunicarse con el dispositivo y realizar ataques. Previamente, puede que necesite omitir el paso de autenticación en el protocolo de comunicación entre la aplicación y el dispositivo. Posteriormente, el atacante envía los mensajes del bus CAN deseados al dispositivo, solicitándole que los retransmita al bus CAN para desencadenar las consecuencias correspondientes. En este artículo, denominamos mensajes predefinidos a los mensajes del bus CAN que realizan las funciones diseñadas de un dispositivo, y mensajes indefinidos a los demás. Los primeros están permitidos por diseño y, por lo tanto, deben retransmitirse directamente al bus CAN. Sin embargo, las funciones diseñadas del dispositivo pueden ser bastante limitadas, por ejemplo, solo funciones de diagnóstico. Por lo tanto, para ciertos objetivos de ataque, como los relacionados con la seguridad, resulta interesante inyectar mensajes indefinidos (por ejemplo, aquellos que interfieren con el control del vehículo). Sin embargo, dado que estos mensajes no están permitidos por diseño, el éxito del ataque depende del proceso de filtrado de mensajes en el lado del dispositivo (Nagarajan et al., 2023; Wen et al., 2020).

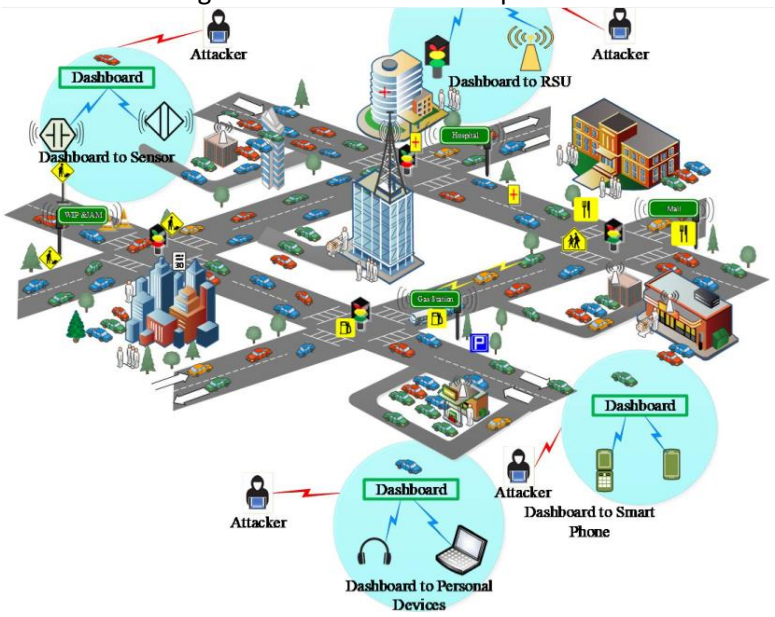
2.1.3. Ciberseguridad y estrategias de protección

El impacto de la investigación avanzada en la seguridad vehicular depende de conjuntos de datos genuinos en tiempo real que contengan la semántica de los mensajes para la experimentación. Desafortunadamente, la disponibilidad de conjuntos de datos genuinos relacionados es la principal limitación en la investigación avanzada. Los conjuntos de datos del bus CAN son propiedad intelectual de fabricantes de automóviles específicos y, por lo tanto, no están disponibles públicamente para la experimentación. La posible solución a este problema es la colaboración entre los fabricantes de automóviles y los investigadores. Además, las tramas de datos en las redes vehiculares se generan en milisegundos, por lo que el etiquetado de los datos es un asunto complejo. Si bien los ataques predefinidos se identifican mediante aprendizaje supervisado, debemos centrarnos en el desarrollo de soluciones de seguridad capaces de gestionar ataques nuevos y diversificados (Aliwa et al., 2021; Bozdal et al., 2020).

Algunos enfoques de seguridad no consideran los diferentes estados del vehículo. Por lo tanto, su eficacia se limita únicamente a estados específicos del vehículo. Los mecanismos de seguridad deben ser robustos y tener mayor cobertura para diferentes estados del vehículo (Aliwa et al., 2021; Bhatia et al., 2021).

Figura 20

Escenarios de seguridad en vehículos con posibles amenazas



2.1.3.1. Técnicas de autenticación y cifrado aplicadas a CAN.

Los avances en investigación para contrarrestar los ciberataques a vehículos inteligentes deben implementarse en escenarios reales para obtener resultados óptimos. Sin embargo, la implementación de soluciones de investigación en escenarios reales presenta diversas limitaciones. Un investigador no puede permitirse comprar un coche para realizar experimentos. La solución ideal en estas circunstancias es la colaboración entre organizaciones de investigación y fabricantes de automóviles (Aliwa et al., 2021; Rathore et al., 2022).

2.1.3.2. Sistemas de detección de intrusos (IDS) en redes automotrices.

Según Aliwa et al. (2021) menciona que “las soluciones de seguridad propuestas deben ser compatibles y contar con características de portabilidad, lo cual se puede lograr probando su rendimiento en tiempo real. Asimismo, deben cumplir con los estándares mínimos de ciberseguridad” (p. 27).

2.1.3.2.1. Recursos de hardware mejorados

Las soluciones de seguridad avanzadas requieren recursos de hardware actualizados en las redes vehiculares. Se necesitan recursos de hardware escalables en las redes vehiculares para

soportar nuevas funcionalidades. Se está investigando el desarrollo de ECU y puertas de enlace de última generación para identificar mensajes sospechosos y, por lo tanto, detener la transmisión de estos mensajes falsos en la red (Aliwa et al., 2021; Zhang et al., 2014).

2.1.3.2.2. Seguridad entre capas

Las soluciones de seguridad avanzadas son más eficientes que los enfoques tradicionales, ya que se centran en la seguridad intercapa para proporcionar comunicaciones de datos seguras en las redes vehiculares. Las soluciones de seguridad tradicionales se centran en la seguridad de la capa física o de la capa de aplicación, por lo que su eficiencia es limitada (Aliwa et al., 2021; Fakhfakh et al., 2021).

2.1.4. Inteligencia artificial en la seguridad automotriz

Para muchas empresas e instituciones, el modelo de la cadena de suministro para la confiabilidad y mantenibilidad de los sistemas puede representar una ventaja competitiva o su punto más débil. El big data y la analítica desempeñan un papel fundamental en la cadena de suministro, especialmente para las empresas que utilizan los principios de confiabilidad y mantenibilidad, donde estas prácticas nacieron y maduraron. La industria automotriz ha liderado numerosas iniciativas para aumentar la adopción de estas arquitecturas de la cadena de suministro en sus ecosistemas vehiculares, permitiendo que el big data y la analítica desempeñen un papel clave para asegurar el rendimiento de los vehículos. La industria automotriz continúa utilizando estas prácticas para abordar las disrupciones en la conducción autónoma, las baterías eficientes con autorreparación, la robótica, las evaluaciones de riesgos de seguros y las experiencias excepcionales del cliente. Ya se trate de fabricantes de automóviles, concesionarios, conductores o compañías de seguros, el confiabilidad y mantenibilidad ha obtenido resultados positivos. Sin embargo, hoy en día, otra tecnología está surgiendo rápidamente, transformando las prácticas y aplicaciones estándar de confiabilidad y mantenibilidad. La Inteligencia Artificial (IA) está impactando y transformando todo el ecosistema de la industria automotriz (Gupta et al., 2021; Yánez & Francisco, 2023).

2.1.4.1. Definición y trayectoria de la inteligencia artificial.

La industria automotriz está experimentando una disrupción masiva, al igual que la electrificación, la conducción autónoma, la autorreparación, las baterías como servicio, la movilidad compartida, la conectividad y las experiencias excepcionales para el cliente. Y todo esto se está volviendo real muy rápidamente. Ya se trate de fabricantes de automóviles, concesionarios, ingenieros, empresas de viajes compartidos, conductores individuales o aseguradoras, la IA está impactando, habilitando y cambiando toda la experiencia en la industria

automotriz. Si bien los avances en chipsets, edge computing, 5G, IoT y la nube son facilitadores, el big data y la IA están en el corazón de estas disrupciones (Gupta et al., 2021).

Transforme la disrupción en transformación:

- **Transforma productos y operaciones:** Desarrollo de vehículos de próxima generación y mejora de la eficiencia operativa y la calidad del producto.
- **Transforma la movilidad:** Explore cómo la industria automotriz puede evolucionar hacia un futuro autónomo.
- **Transforma la conectividad:** Sistemas conectados impulsados por 5G e IoT.

Transforme la interacción/experiencia: Redefiniendo las formas de interactuar y conectar con los clientes.

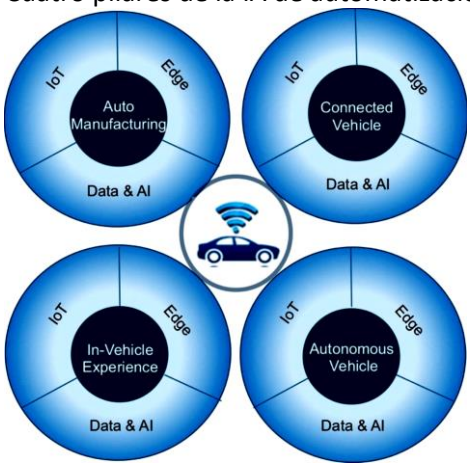
En el propio vehículo, se procesan en tiempo real grandes cantidades de datos telemáticos provenientes de cámaras, sensores, datos meteorológicos y otros puntos finales del IoT. La potencia informática del vehículo procesa y analiza estos datos directamente en el borde del vehículo en tiempo real o los almacena para su posterior procesamiento, con el fin de entrenar modelos de aprendizaje automático y proporcionar información predictiva y práctica. Estos vehículos inteligentes desvelan la historia con datos contextuales para crear soluciones como cobertura de seguros personalizada, experiencias a bordo y operaciones de flota (Aguirre et al., 2021; Gupta et al., 2021).

2.1.4.1.1. Impacto de la IA en la industria automotriz

La industria en sí está fuertemente impulsada por la economía actual, el comportamiento de compra de los usuarios y los modelos de consumo de movilidad. Un modelo de negocio flexible para el crecimiento es la única manera de que la industria automotriz sea relevante en el mercado y se mantenga competitiva. Esto solo es posible mediante la sinergia entre los modelos independientes, y estos algoritmos pueden ajustarse independientemente según sea necesario para ajustar el modelo de crecimiento. La confluencia de la transformación requerida y tecnologías como la IA, el Edge y el IoT está creando y configurando cuatro aspectos relativamente nuevos de la industria automotriz: la fabricación de automóviles, los vehículos conectados, la experiencia a bordo y los vehículos autónomos, como se muestra en la figura 21. (Gupta et al., 2021, pp. 2-3; Minawi et al., 2020, p. 3)

- **Vehículo autónomo:** posible gracias a las innovaciones en sistemas de conducción automatizada, el Edge y la tecnología conectada.
- **Fabricación de automóviles:** la columna vertebral de la industria, que continúa transformándose mediante la adopción de los paradigmas de la Industria 4.0.
- **Vehículo conectado:** la comunicación del vehículo a todo (V2X) proporciona viajes seguros y eficientes mediante una red distribuida de sensores y sistemas en el borde.
- **Experiencia en el vehículo:** utiliza tecnologías digitales para ofrecer experiencias personalizadas para un mejor estilo de vida.

Figura 21
Cuatro pilares de la IA de automatización



2.1.5. Arquitectura y componentes del sistema vehicular

Las redes vehiculares (IVN) son un campo de investigación emergente en las redes vehiculares modernas. La arquitectura de red vehicular consta de varios componentes principales: el dominio de sensores (que incluye sensores de alta precisión), el dominio del chasis, el dominio de infoentretenimiento, el dominio telemático y el dominio del sistema de propulsión. Para una comunicación eficaz entre estos componentes principales de las redes vehiculares, los protocolos, como Ethernet, FlexRay y la red de área del controlador (CAN), desempeñan un papel fundamental. El rápido crecimiento de la conectividad entre las instalaciones de transporte integradas con tecnologías modernas y avanzadas, como las comunicaciones V2X, ha agravado las vulnerabilidades de seguridad y, en consecuencia, ha permitido que los atacantes accedan a la red vehicular (Rathore et al., 2022).

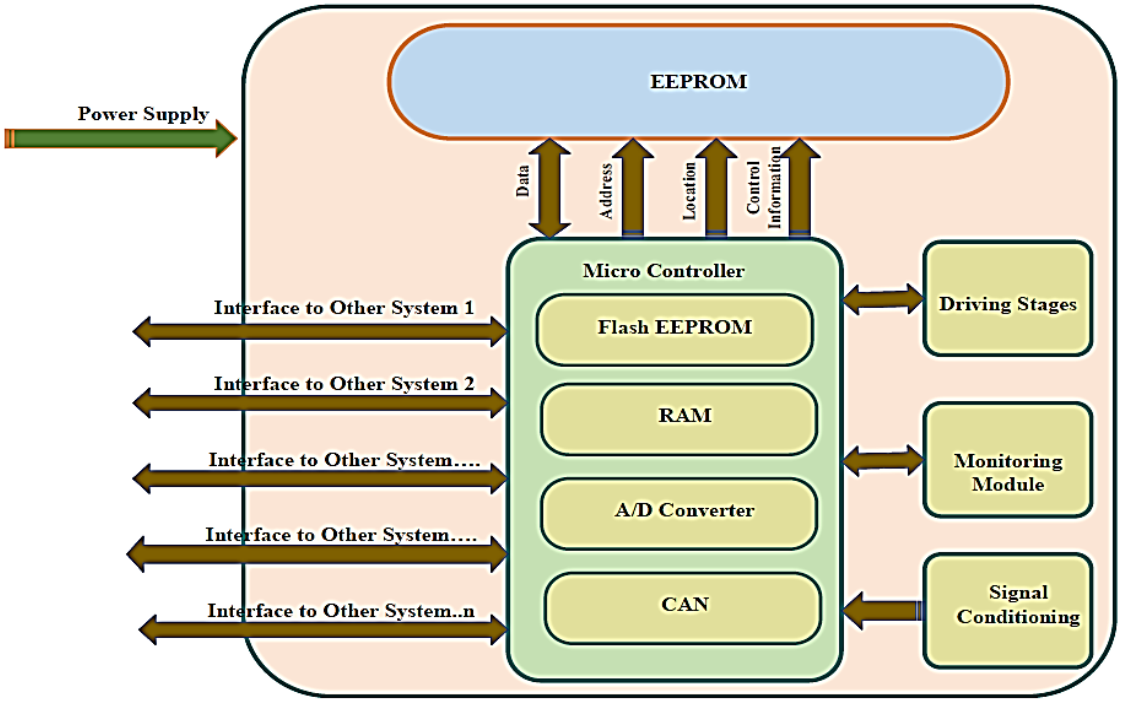
2.1.5.1. Configuración Interna de Unidades de Control Electrónico ECU

Se intercambia información crítica entre las diferentes unidades de control electrónico (ECU) instaladas en el vehículo. En los vehículos modernos avanzados, a medida que aumenta el

número de ECU, también aumenta la complejidad de las redes vehiculares, ya que cada componente tiene requisitos diferentes en términos de ancho de banda y latencia. El número de ECU aumenta continuamente en los vehículos inteligentes modernos para dotarlos de nuevas funcionalidades en materia de seguridad, comodidad, etc. Además, para la interconexión de un gran número de ECU, se han desarrollado varios protocolos vehiculares y se continúa investigando para obtener funciones más avanzadas. Además, las ECU suelen estar conectadas a más de una red de bus debido a su diversificada funcionalidad, que incluye el control y la monitorización del vehículo (Rajapaksha, 2024; Rathore et al., 2022).

La Figura 22 muestra la configuración interna de la ECU en detalle.

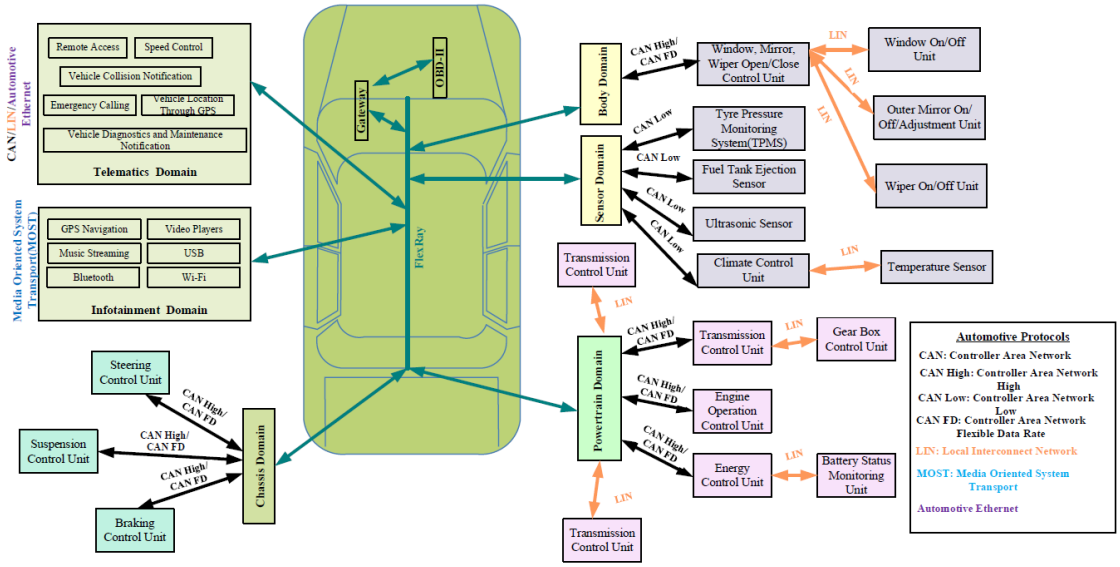
Figura 22
Configuración interna de una ECU-PCM



Es un hecho que los sensores actuadores son la columna vertebral de los vehículos inteligentes modernos, ya que los sensores suelen reconocer e informar de inmediato el problema para su resolución, por ejemplo, incluyendo servicio debido, falla del componente, etc (Sharma et al., 2024). Los sensores observan diversos eventos clave como la velocidad del vehículo, el combustible, la temperatura, la velocidad de rotación del cigüeñal, la presión de los neumáticos, la proporción de oxígeno en los gases de escape, la densidad del aire en el motor, etc. Por lo tanto, los sensores diminutos deben tener altos estándares, como precisión, resolución, sensibilidad, exactitud, bajo consumo de energía y menos ruido. La observación y el informe de estos eventos ayudan en la detección temprana del problema y resultan en la

prevención de daños al vehículo. Los vehículos autónomos tienen sensores de diferentes tipos que van desde sensores eléctricos, mecánicos, ópticos, de sonido, de imagen y de luz, etc (Bhatia et al., 2021; Rathore et al., 2022).

Figura 23
Arquitectura de red en vehículos con protocolos automotrices



2.1.6. Herramientas de diagnóstico y validación

2.1.6.1. Osciloscopio y análisis de señales CAN-H y CAN-L.

Para quienes buscamos la comodidad de un osciloscopio, el YEAPOOK ADS1013D ofrece un rendimiento inigualable. Es de tamaño que cabe en una bolsa para portátil, ofrece especificaciones robustas, incluyendo anchos de banda de hasta 100 MHz y una frecuencia de muestreo máxima de 1 GSa/s, con opciones para 2 canales analógicos. Los puertos de E/S frontales y laterales facilitan el acceso y la conectividad. Además, la batería extraíble opcional ofrece versatilidad para su uso en laboratorio o en campo.

Figura 24
Osciloscopio a usar durante las pruebas de señales del bus CAN

2.1.6.1.1. Análisis exhaustivo para una comprensión rápida

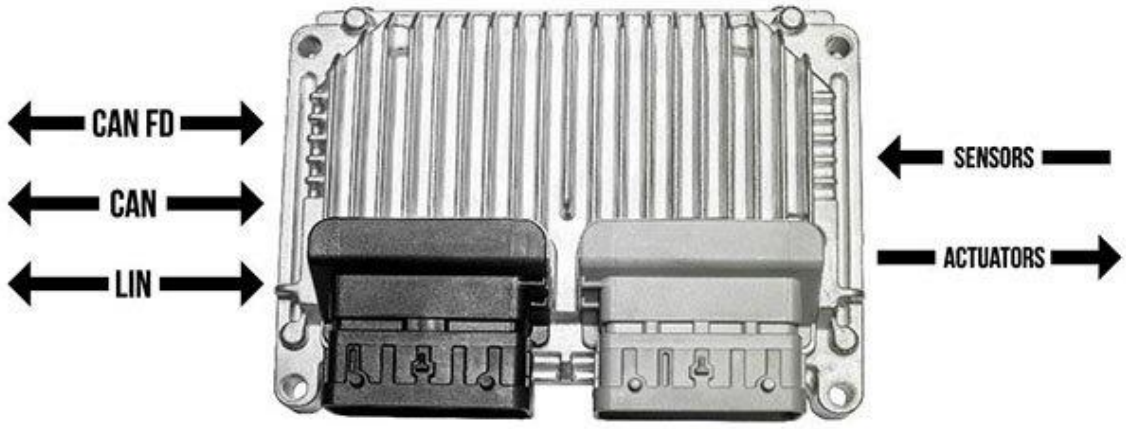
Un conjunto completo de herramientas de análisis proporciona acceso inmediato a la configuración del instrumento o a las tareas de gestión de formas de onda con un solo toque.

- Cursores basados en forma de onda y pantalla con ubicación de lectura seleccionable por el usuario.
- Mediciones automatizadas ilimitadas.
- Matemáticas de formas de onda básicas y avanzadas, incluida el análisis de tramas a izquierda y derecha.

Debido a la complejidad de los sistemas multibus y multisensor/actuador, a menudo resulta difícil obtener una visión general del entorno de trabajo.

La mayoría de los osciloscopios permiten visualizar múltiples buses y señales de control simultáneamente. Los osciloscopios de señal mixta permiten el uso de canales digitales para la decodificación de buses, liberando canales analógicos para evaluar la calidad de la señal.

Figura 25
Comunicación a través de CAN, LIN y otros buses, y directamente con sensores y actuadores



2.1.6.2. Escáner automotriz y puerta de pruebas.

2.1.6.2.1. Thinkdiag

El escáner Thinkdiag OBD2 admite todas las funciones de diagnóstico del sistema, puede leer/borrar códigos de falla, leer datos en vivo, leer información del módulo de control, pruebas de actuación y funciones de mantenimiento para ECM, BCM, SRS, TCM, BMS, TPMS, SAS, sistema A/C, etc. Funciona con la mayoría de los modelos de automóviles posteriores al año 1996 de más de 120 marcas de automóviles.

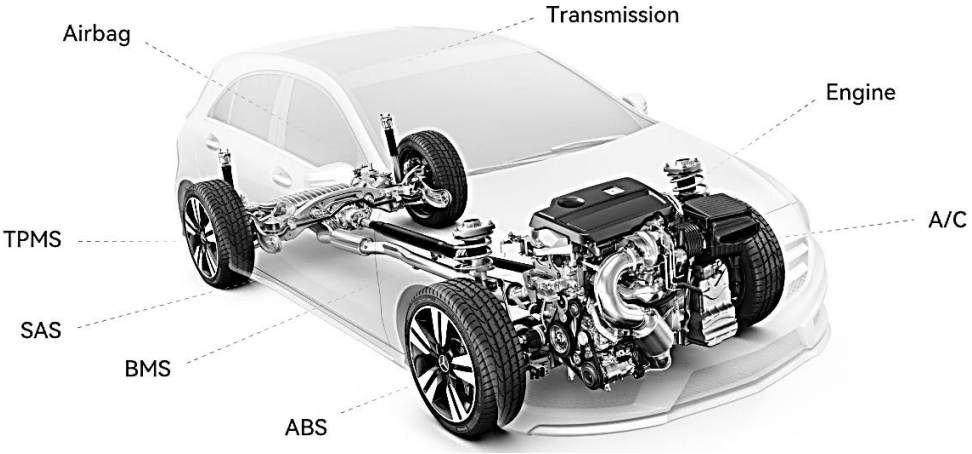
Figura 26

Escáner a utilizar para las pruebas de datos

El lector de códigos Thinkdiag activa solenoides y actuadores para realizar pruebas activas y envía comandos a sistemas/componentes para comprobar su funcionamiento sin usar los controles del vehículo, lo que ahorra tiempo a la hora de identificar las causas de las averías. La codificación de la ECU permite asociar los componentes reemplazados con la ECU y activar funciones ocultas para los vehículos. Tanto si es un particular como un técnico profesional, Thinkdiag es una potente herramienta de escaneo bidireccional.

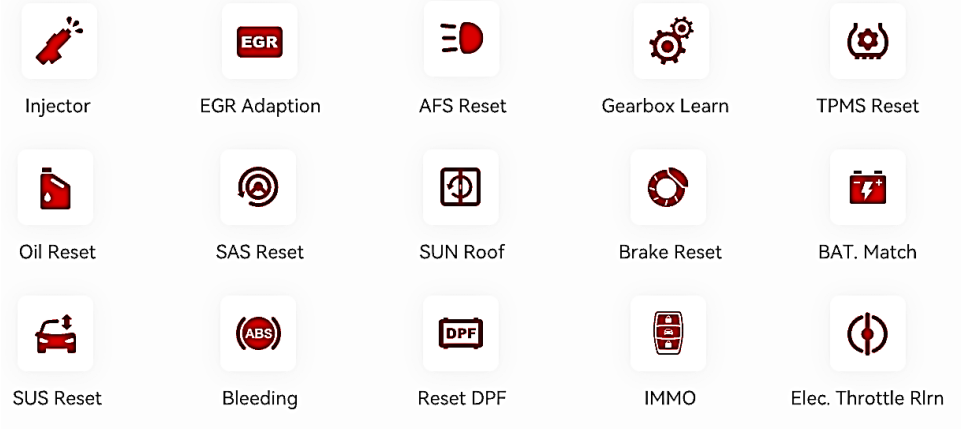
Figura 27

Diversos microcontroladores del vehículo



El escáner Thinkdiag cuenta con funciones de reinicio y más funciones de mantenimiento en el menú del vehículo: reinicio de aceite, purga de ABS, codificación de inyectores, reinicio de SAS, reinicio de TPMS, reinicio de DPF, reinicio de BMS, reinicio de caja de cambios, reinicio de AFS, adaptación de EGR, techo solar, reinicio de frenos, suspensión, reaprendizaje del acelerador eléctrico, calibración de SEAT, codificación de llaves, etc. Thinkdiag es una herramienta profesional de escaneo de vehículos para mecánicos. La codificación de la ECU no es compatible con todos los módulos del vehículo.

Figura 28
Funciones de mantenimiento del escáner



2.1.6.2.2. Caja de desconexión

Esta caja de conexiones J1962 permite el acceso a todos los cables de la interfaz de diagnóstico OBD-II/EOBD III. Esto facilita el rastreo de fallas del bus CAN, problemas de alimentación y el seguimiento de controladores de diagnóstico defectuosos.

Figura 29
BreakBox OBD II

2.1.6.2.3. Téster de computadores automotrices

Con la diversidad que se tiene en el medio y los avances tecnológicos con los que son construidos equipos de diagnóstico automotriz, es indispensable estar actualizados para dar las soluciones rápidas, con equipos de diagnóstico especializado. Este equipo está enfocado en simular el sensor CKP (Sensor de Posición de Cigüeñal) y CMP (Sensor de Posición de Árbol de levas) inductivo y de efecto hall, el cual entregará la señal a la unidad de control electrónico, que en respuesta enciende la bomba de combustible, además dará pulsos de inyección, bobinas, bobinas transistorizadas, check engine y realiza los ajustes necesarios al encendido del motor.

Figura 30
Téster de ECUs para banqueo

2.1.6.3. Software para análisis de tráfico.

A veces es necesario averiguar rápidamente qué paquete del bus CAN es responsable de cada función. Si el protocolo de intercambio no está estandarizado, esto resulta bastante difícil y requiere mucho tiempo. O bien, en otra situación: solo tenemos el tablero del coche y queremos averiguar qué paquete es responsable, por ejemplo, de indicar la velocidad o el ángulo de giro de la aguja del tacómetro. Sin tener el coche completo, nos resultará difícil averiguarlo. Nos hemos propuesto simplificar la búsqueda de paquetes en el bus CAN y determinar su propósito (Aguirre et al., 2021).

El resultado de resolver este problema se da con la utilidad del **CAN-Hacker** que permite estudiar el bus CAN mediante suplantación de identidad o fuerza bruta.

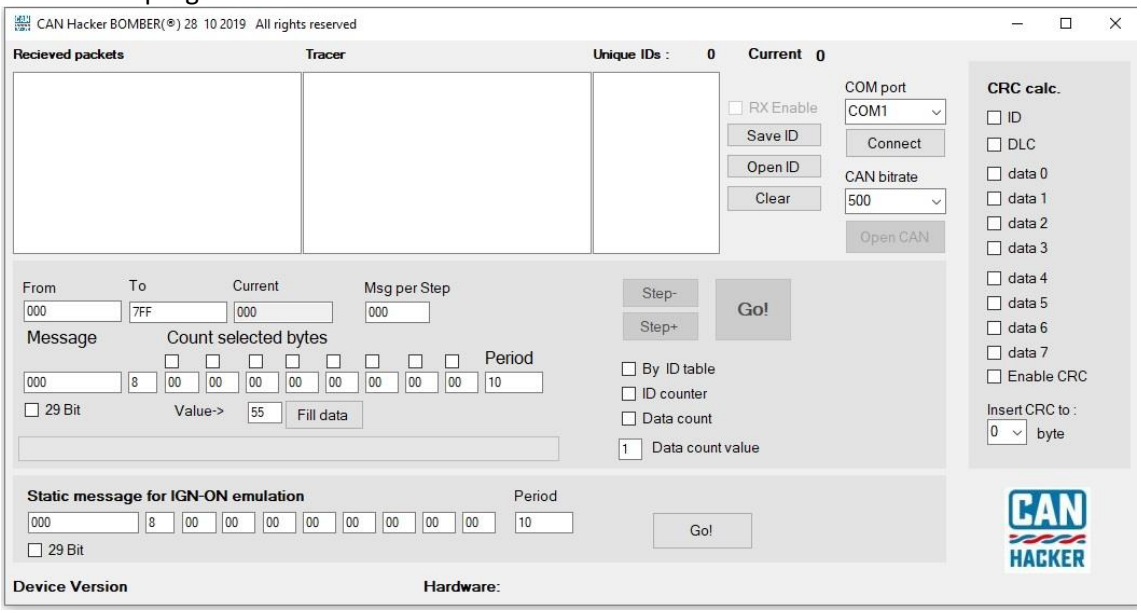
La esencia del método es que hacker envía un paquete con cualquier dato de usuario dentro de un rango de ID determinado. Los ID pueden ser de 11 o 29 bits.

Además, CAN-Hacker puede operar en dos modos:

1. **Contador de ID:** Modo de incremento de ID. Cada paquete subsiguiente tendrá un valor superior al anterior.
2. **Contador de datos:** Modo de incremento de datos. En este modo, el ID no cambia, pero sí los bytes seleccionados del paquete.

Figura 31

Interfaz del programador CAN Hacker



2.1.6.4. Validación de tramas utilizando inteligencia artificial.

Ejemplos como los siguientes ilustran las primeras iniciativas para integrar la inteligencia artificial (IA) en los automóviles con el fin de facilitar la vida de los consumidores:

Conducción autónoma: Combina cámaras, sensores y algoritmos de aprendizaje automático para detectar el entorno y tomar decisiones de conducción. Esto no solo incrementa la seguridad vial, sino que también permite a los conductores realizar otras actividades mientras el automóvil se maneja solo.

Personalización del entretenimiento: Los sistemas de entretenimiento inteligentes pueden aprender las preferencias del conductor y los pasajeros, ajustando la música, la televisión y otras opciones de entretenimiento, lo que genera una experiencia de conducción más cómoda y adaptada a sus gustos.

Mantenimiento predictivo: Sensores en el automóvil identifican problemas antes de que escalen a fallas graves, permitiendo a los conductores llevar a cabo reparaciones preventivas en lugar de esperar a que ocurran fallas.

Asistente de voz: Estas herramientas son cada vez más comunes en los automóviles. Los conductores pueden utilizar comandos de voz para gestionar música, navegación y otras funcionalidades del vehículo, manteniendo así sus manos en el volante y sus ojos en la vía.

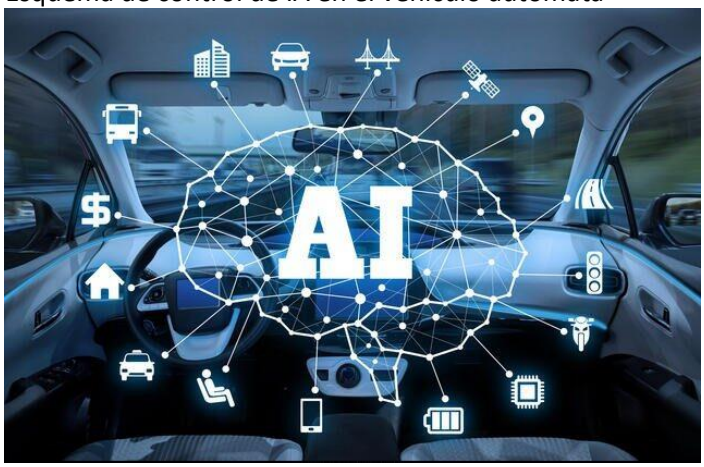
Alertas de seguridad: La IA puede proporcionar alertas de seguridad en tiempo real, ya que los sensores del automóvil pueden detectar peligros en la carretera y advertir al conductor, mejorando la seguridad vial.

Navegación inteligente: Puede utilizar IA para ofrecer a los conductores rutas más eficientes y sugerencias de destinos basadas en sus preferencias y hábitos de conducción.

Comunicación vehículo a vehículo: Los vehículos equipados con tecnología V2V pueden intercambiar información en tiempo real sobre las condiciones de tráfico y otros peligros en la ruta.

La inteligencia artificial presenta una amplia gama de aplicaciones en automóviles, muchas de las cuales ya se están implementando en la actualidad. Aunque no hemos alcanzado la realidad de vehículos completamente autónomos, varios expertos indican que estamos avanzando hacia esa meta, que alguna vez pareció de ciencia ficción. La IA en los automóviles es un paso necesario hacia ese objetivo, al pasar de asistir al conductor con advertencias o maniobras de estacionamiento, a potencialmente prescindir de su intervención. Actualmente, ya existen automóviles que cuentan con inteligencia artificial capaz de activar un piloto automático una vez que se establece un destino y una ruta (Aguirre et al., 2021; Aliwa et al., 2021).

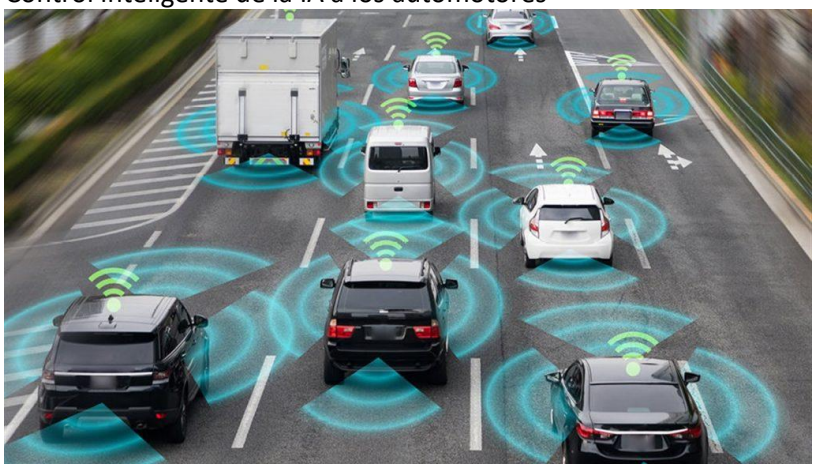
Figura 32
Esquema de control de IA en el vehículo autómata



Sin embargo, algunos de los desafíos que surgen incluyen preocupaciones sobre la privacidad de los datos, la responsabilidad legal en caso de accidentes de vehículos autónomos, y la necesidad de actualizaciones y mantenimiento de los sistemas de IA conforme la tecnología avanza. Por tanto, es esencial establecer regulaciones claras y mecanismos de seguridad

robustos para proteger la privacidad de los usuarios y asegurar un uso ético de los datos (Park et al., 2023; Yánez & Francisco, 2023).

Figura 33
Control inteligente de la IA a los automotores



2.2. Descripción de la propuesta

Este proyecto de titulación tiene por objetivo analizar ciertas vulnerabilidades que presenta las redes de comunicación automotriz CAN bus, ya que este microcontrolador es la matriz de todas comunicaciones existentes de las demás computadoras complementarias de sistemas de control, el proyecto se desarrolla en las instalaciones del Instituto Superior Tecnológico Ciudad de Valencia de la provincia de Los Ríos en el cantón Pueblovieja.

Para mostrar una solución tecnológica se hará uso de diversas herramientas de diagnóstico electrónico tales como, escáner automotriz, osciloscopio, caja de desconexión, téster de ECUs y software de análisis de tramas de vulnerabilidades de acuerdo a vehículos. Ya que este software servirá como un puente de transferencia de información entre la ECU y el escáner quien permitirá la visualización de datos en vivo de funcionamiento del vehículo.

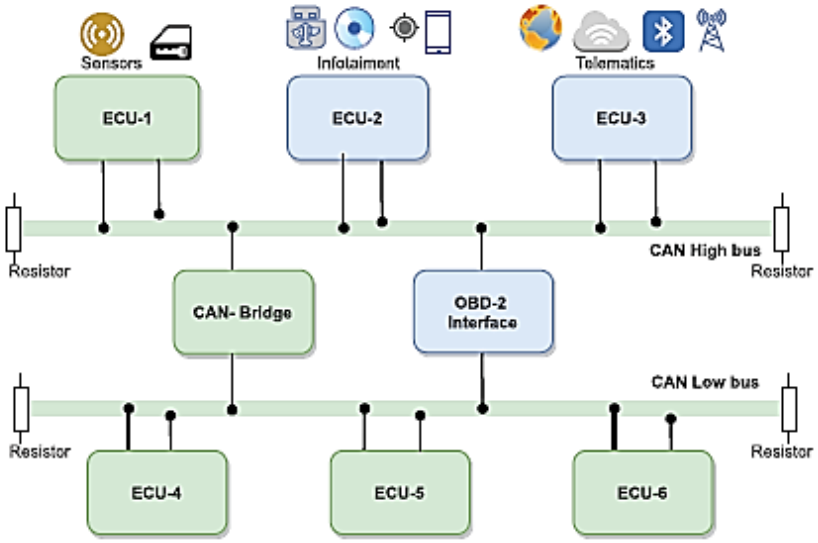
Con este proyecto se presenta a la sociedad en general las vulnerabilidades de ataques a la red CAN bus en el vehículo que pueden sufrir al momento de algún ataque, esto permitirá estar alerta ante los diferentes tipos de ataques para de esta manera tratar de blindar mejor los microprocesadores del vehículo ante lo posibles riesgos de ataques.

a. Estructura general

Se presenta una conexión de las interfaces de diagnóstico automotriz los cuales son escáner, osciloscopio, téster de ECUs, ECU, software de decodificación, los cuales permitirán el control constante de las señales del lado alto y bajo y determinar así si existe alguna variación al inyectar un mensaje malicioso y de la misma manera verificar por medio del flujo de datos en vivo en el

escáner el cual se ingresará por marca, modelo, año y/o VIN de identificación para su detección automática.

Figura 34
Dos buses CAN conectados entre sí a través de un puente



Se presenta las vulnerabilidades de las redes CAN y el modelo de amenazas considerado en esta investigación. A continuación, se analiza cómo descartar tramas maliciosas y el tiempo necesario para detener los ciberataques antes de que se produzcan daños a las redes de comunicación del vehículo.

Aunque el protocolo CAN se considera una tecnología heredada y existen otros protocolos de red que ofrecen mayor rendimiento, como el transporte de sistemas orientados al medio que la tecnología MOST y el ethernet automotriz, por lo que sigue siendo el protocolo más utilizado en los automóviles actuales. Su robustez y baja complejidad permiten a los fabricantes de automóviles seguir confiando en él para muchas aplicaciones modernas, por lo que se espera que el uso de CAN siga siendo generalizado en vehículos.

Además, CAN es una tecnología económica y reconocida que ofrece una velocidad de datos lo suficientemente alta como para transmitir la mayoría de las señales del vehículo. Es compatible y perfectamente interoperable con la velocidad de datos flexible CAN (CAN-FD), que mejora las redes CAN y permite la transmisión de cargas útiles más grandes a velocidades de datos más altas.

Finalmente, la adopción de otras redes a bordo de vehículos para aplicaciones de infoentretenimiento y conducción autónoma, por ejemplo, no implica que las redes CAN vayan

a ser reemplazadas por completo. De hecho, ya coexisten diferentes redes a bordo de vehículos y están conectadas mediante pasarelas multiplexadas.

b. Explicación del aporte

Debido a la falta de seguridad en los vehículos y a su amplia y creciente capacidad de conectividad, se puede acceder a las redes CAN de automóviles a través de diferentes tipos de interfaces de comunicación. Los atacantes pueden acceder físicamente a las redes CAN conectándose al puerto OBD-II del vehículo, lo que permite a los concesionarios y talleres extraer información del vehículo. También pueden acceder remotamente a las redes CAN aprovechando vulnerabilidades de interfaces inalámbricas, como Bluetooth y redes celulares, utilizadas para aplicaciones telemáticas y actualizaciones inalámbricas de la ECU. En esta investigación, se obtuvo el control de la red CAN de un Chevrolet Aveo 2006 aprovechando remotamente su sistema de comunicación ISO 14230-4 KWP de protocolo rápido.

En base a esto se realizará un banqueó de la computadora de dicho vehículo, así mismo, in situ con los equipos de diagnóstico electrónico antes mencionado. De esta manera obtendremos la señal del par trenzado CAN en el lado alto y bajo.

Evalué este proceso en base al uso del procedimiento de banqueo e in situ, esta información será pública. Cada uno contiene de 30 a 40 flujos de datos de tráfico regulares registrados desde una CAN a través del puerto OBD-II del vehículo real. Además, cada conjunto de datos contiene mensajes CAN de ataque, como fuzzing y falsificación del indicador de RPM, realizados durante la adquisición de datos. En los ataques de fuzzing, los mensajes CAN tienen identificadores y bytes de datos aleatorios y en los ataques de falsificación del indicador de RPM, los mensajes CAN utilizan el identificador relacionado con la información de RPM.

c. Estrategias y/o técnicas

Para realizar el levantamiento de flujo de datos en vivo, se requiere en primer lugar estar relacionado directamente al tipo de protocolo CAN bus de comunicación, en este caso la comunicación ISO 14230-4 KWP de protocolo rápido del Chevrolet Aveo 2006, la parte de investigación teórica es parte fundamental para dar inicio al tipo de protocolo que usa la computadora de ese vehículo para posterior tener la comunicación directa entre escáner y ECU.

El pin data del diagrama electrónico de la ECU a prueba es importante tener en cuenta para la detección de la pinera y no realizar una conexión errónea generando un corto del sistema de comunicación en base al banqueo de la ECU.

Una vez conectado el escáner y la caja de desconexión al ECU del vehículo y el téster se hará un ataque simulado y controlado en base al uso del test de actuadores y funciones especiales y determinar cómo se comporta el motor del vehículo en base a cambios de diferentes sensores y actuadores, específicamente de la PCM. Esta investigación se centra directamente al powertrain del vehículo para sus pruebas. Posterior a estos ataques controlados se hará uso de la inteligencia artificial para determinar sus vulnerabilidades acompañado del software de decodificaciones.

2.3. Validación de la propuesta

El presente trabajo de titulación se validó por profesionales expertos en el área de la comunicación electrónica automotriz, los cuales cuentan con experiencias amplias del campo, los cuales certifican la viabilidad de desarrollar este tema de investigación.

Tabla 2
Descripción de perfiles validadores

Nombres y Apellidos	Años de experiencia	Titulación Académica	Cargo
Víctor Patricio Pachacama Nasimba	7	Ingeniero Automotriz, Magíster en Diseño Mecánico	Docente, Universidad Técnica Estatal de Quevedo
Lorena Maribel Camacho Játiva	10	Ingeniera Automotriz, Magíster en Gestión de Energías	Docente, Instituto Superior Tecnológico Tecnoecuatoriano
Víctor Fabricio Moreno Riquero	7	Ingeniero Industrial, Magíster en Mantenimiento industrial	Docente, Universidad Técnica Estatal de Quevedo
César Andrés Minaya Andino	4	Ingeniero Mecatrónica y Robótica, Máster en Mecatrónica y Robótica	Docente investigador, Instituto Superior Tecnológico Rumiñahui

Tabla 3
Criterios de evaluación

Criterios	Descripción
Impacto	Representa el alcance que tendrá el modelo de gestión y su representatividad en la generación de valor público.
Aplicabilidad	La capacidad de implementación del modelo considerando que los contenidos de la propuesta sean aplicables
Conceptualización	Los componentes de la propuesta tienen como base conceptos y teorías propias de la gestión por resultados de manera sistémica y articulada.
Actualidad	Los contenidos de la propuesta consideran los procedimientos actuales y los cambios científicos y tecnológicos que se producen en la nueva gestión pública.

Calidad Técnica	Miden los atributos cualitativos del contenido de la propuesta.
Factibilidad	Nivel de utilización del modelo propuesto por parte de la Entidad.
Pertinencia	Los contenidos de la propuesta son conducentes, concernientes y convenientes para solucionar el problema planteado.

Tabla 4

Modelo de escala de evaluación

CRITERIOS	EVALUACION SEGUN IMPORTANCIA Y REPRESENTATIVIDAD				
	En Total Desacuerdo	En Desacuerdo	Ni de Acuerdo Ni en Desacuerdo	De Acuerdo	Totalmente Acuerdo
Impacto					
Aplicabilidad					
Conceptualización					
Actualidad					
Calidad Técnica					
Factibilidad					
Pertinencia					

2.4. Matriz de articulación de la propuesta

Es aquí donde se describen los elementos y equipos utilizados para el proyecto, así como también la metodología y los conceptos de cada elemento usado para la operatividad del sistema.

Tabla 5

Matriz de articulación de la propuesta

Ejes o partes principales del proyecto		Breve descripción de los resultados de cada parte	Sustento teórico que se aplicó en la construcción del proyecto	Metodologías, herramientas técnicas y tecnológicas que se emplearon
1	Definición: de los elementos electrónicos de comunicación, de comunicaciones de buses CAN, variables de entrada a controlar, variables de salida a controlar, etc.	1.1. Análisis de protocolo de comunicación ISO 14230-4 KWP de protocolo rápido 1.2. Análisis de factibilidad 1.3. Tomas de decisiones en base a variables controladas	Inteligencia Artificial Base de datos científicos	Software de hackeo Computadora personal
2	Diseño: de banqueo de ECUs, de control, aplicación, flujo de datos en vivo, funciones especiales, etc.	2.1. Pin data de la ECU 2.2. Análisis de datos en vivo 2.3. Cambios de funciones especiales	Codificaciones de datos CAN bus Adaptación de escáner	Pin data del vehículo Conectores Escáner
3	Implementación: Banqueo de téster y ECU, escáner, oscilogramas, caja de desconexión, etc.	3.1. Obtención de señal alta y baja en banqueo 3.2. Obtención de señal alta y baja en el vehículo 3.3. Análisis de oscilogramas del CAN bus	Cableado estructurado Sistemas de comunicaciones Desarrollo de bases de datos Protocolos de comunicación	Téster de ECUs Caja de desconexión Escáner Vehículo Osciloscopio

2.5. Análisis de resultados. Presentación y discusión.

El presente trabajo de titulación tiene como objetivo banquear una ECU en un téster de control y a la vez controlando sus parámetros con un osciloscopio y el escáner. Esta configuración ayuda a monitorear los valores de parámetros en vivo que proporcionará el escáner y la trama CAN bus obtenido por medio del osciloscopio.

Adicional, se requiere el pin data de la computadora a prueba que es la HV 240 que por lo general viene equipada en los vehículos Chevrolet en los modelos Aveo y Optra para el cual se requiere una fuente de alimentación de 12 voltios. De esta manera se realiza la simulación de ataques directamente por medio del OBD II y el escáner alterando su funcionamiento, el banco probador nos permite simular ataques como el aumento o reducción del flujo másico de aire MAF provocando un aumento de consumo de combustible lo que conlleva a humareda excesiva, en base al sensor MAP se provocaría una disminución de presión en el múltiple de admisión dando una valor de voltaje demasiado bajo lo que no asimilaría la ECU, la aceleración estará simulada al TPS enviando una señal excesiva de aceleración con apertura de mariposa al límite con esto elevando las rpm de motor al máximo, el señor de temperatura del aire IAT y del motor ECT también sufrirían ataques con cambios de temperatura demasiado elevado y bajo dando en base a esto controles inestables del vehículo y el ataque más directo es al sensor de posición del cigüeñal CKP cortando la señal de identificación del cilindro número 1, en base a esto el motor dejará de funcionar ya que no tendría la forma de reconocer la posición del cilindro 1.

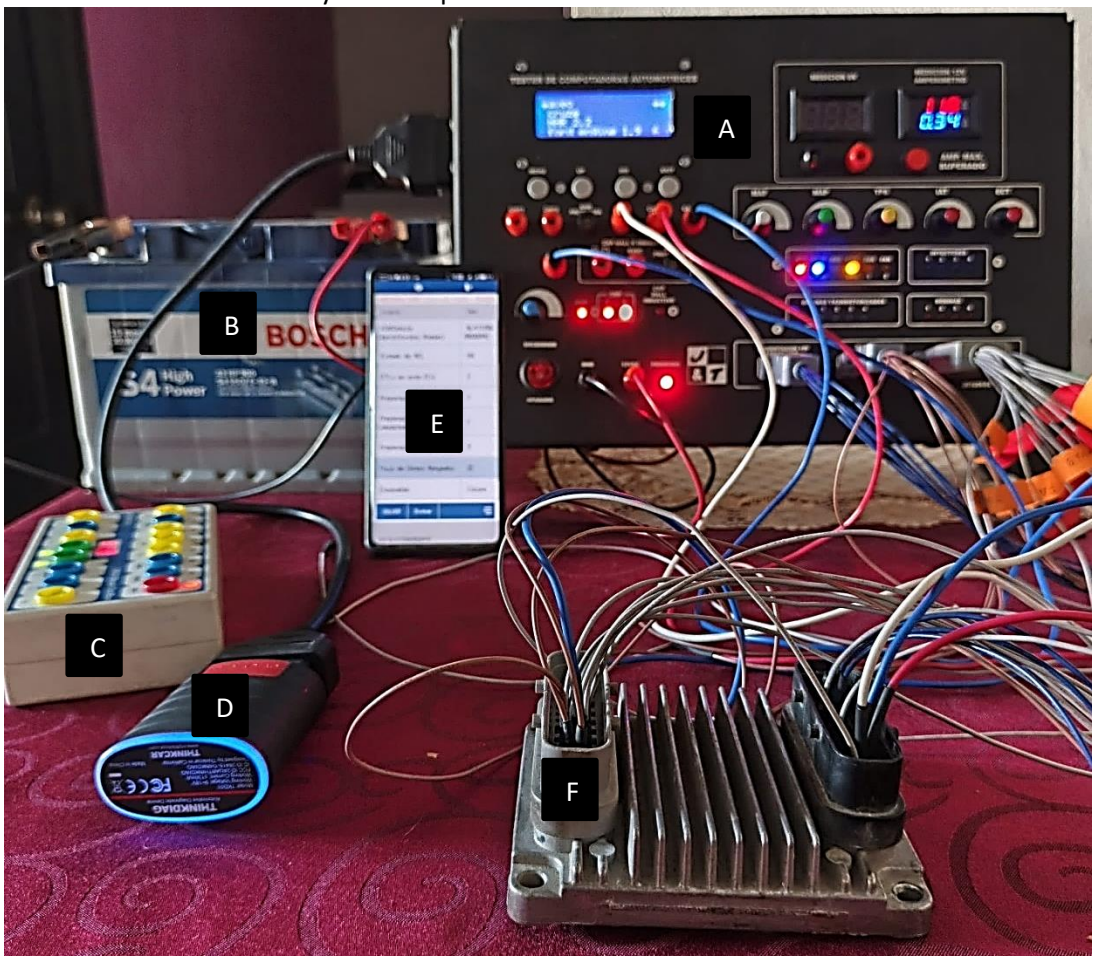
Figura 35

Esquema de conexión del téster y la ECU

Se procede a la comunicación y conexión entre la ECU y el probador téster de ECUs para hacer la simulación de encendido del motor del vehículo por medio de sus cables conectores a los diferentes puertos de conexión.

Figura 36

Banco conectado a la ECU y escaner para el monitoreo de redes CAN



La figura 36 muestras los siguientes detalles para el proceso de identificación de tramas:

A. Téster de computadoras ECU

B. Fuente de alimentación de 12 voltios

C. Caja de desconexión para escáner

D. Escáner automotriz

E. Interfaz de comunicación de salida de datos del escáner

F. ECU

Figura 37

Entrada del escáner a la ECU

Estado de MIL	ON
DTCs en esta ECU	2
Preparación Completada	7
Preparación No Completada	1
Preparación No Apoyada	3
Flujo de Datos Apoyados	22
Encendido	Chispa
Tipo de Protocolo	ISO 14230-4 KWP

La figura 37 muestra el estado de conexión a la ECU en base al protocolo de comunicación ISO 1430-4 KWP.

Figura 38

Flujo de datos con inyección de mensaje malicioso en base a funciones especiales

Data Stream

Nombre	Valor	Rango estándar	Unidad
Posición Absoluta de la Mariposa	56.471	0 - 14	%
Presión absoluta del colector de admisión	10	20 - 108	kPa
RPM del motor	1226	0 - 6000	rpm
Temperatura del aire de admisión	27	30 - 80	degree C
Temperatura del refrigerante del motor	18	80 - 110	degree C

La figura 38 muestra como los parámetros manipulados están rojo, el cual indica un mal funcionamiento de los sensores de control principales de funcionamiento del vehículo.

Figura 39

Flujo de datos sin inyección de mensaje malicioso en base a funciones especiales

Data Stream

Nombre	Valor	Rango estándar	Unidad
Posición Absoluta de la Mariposa	9.804	0 - 14	%
Presión absoluta del colector de admisión	22	20 - 108	kPa
RPM del motor	2944.75	0 - 6000	rpm
Temperatura del aire de admisión	42	30 - 80	degree C
Temperatura del refrigerante del motor	90	80 - 110	degree C

La figura 39 muestra valores normales de funcionamiento de la ECU en base a la comunicación CAN.

Posterior a estas identificaciones de vulnerabilidades en simulaciones de ataques a la ECU en base al protocolo de comunicación CAN se obtiene las codificaciones en hexadecimal en base al osciloscopio usado cuando los parámetros están normales.

Tabla 6

Codificaciones de datos en base a la trama multiplexada CAN bus obtenida por medio del osciloscopio de interfaz

Packet	Start Time	End Time	ID	Data	Max Voltage	Min Voltage	Packet Time
1	0,0002454	0,0004874	1F5	5F 00 00 00 80 11 00 00	3,03046	-0,0705042	0,000242
2	0,0027358	0,0029758	43F	08 08 A0 FF 00 00 00 00	3,1559	-0,2435601	0,00024
3	0,0039978	0,004228	153	E4 49 00 FF 00 FF FF 82	2,63674	-0,7682211	0,00023
4	0,004234	0,00447	1F0	09 60 09 00 09 00 09 00	2,76187	-0,7325113	0,000236
5	0,004476	0,0047162	1F3	00 80 00 FF 01 80 00 08	2,75028	-1,054206	0,00024
6	0,008506	0,0087438	316	05 40 00 00 00 14 00 00	2,89342	-0,52985	0,000238
7	0,00875	0,0089882	1F5	5F 00 00 00 80 21 00 00	3,20352	-0,0408983	0,000238
8	0,0089942	0,0092244	329	80 73 D5 09 00 00 00 00	2,97674	-0,2911732	0,00023
9	0,0092304	0,0094724	545	02 00 00 00 00 01 00 00	2,82749	-0,1956415	0,000242
10	0,0110164	0,0112466	153	E4 49 00 FF 00 FF FF 82	2,61903	-1,048407	0,00023

11	0,0112526	0,0114906	1F0	09 00 09 00 09 00 09 00	2,64864	-0,7920277	0,000238
12	0,0114968	0,011737	1F3	00 80 00 FF 01 80 00 08	2,73837	-0,8161397	0,00024
13	0,015285	0,0155232	43B	51 00 00 00 00 00 00 00	3,1675	-0,1004152	0,000238
14	0,0180132	0,0182432	153	E4 49 00 FF 00 FF FF 82	2,73227	-1,030704	0,00023
15	0,0182492	0,0184852	1F0	09 20 09 00 09 00 09 00	2,65474	-0,803931	0,000236

En la tabla 6 se muestra datos en formato hexadecimal los cuales indican parámetros diferentes tales como el rpm, CKP, CMP, IAT, ECT, inyectores, MAP, MAF en los diferentes tiempos de funcionamiento monitoreado por la ECU, en este ejemplo se muestra 15 datos de los 1553 datos que se obtuvo.

Figura 40

Trama CAN bus de la ECU puesta a pruebas

En la figura 40 se aprecia la forma de onda de la red CAN BUS obtenida para su análisis el cual fue mostrado en datos hexadecimales en la tabla 6, anteriormente descrita. La trama CAN está directamente relacionada a los parámetros de funcionamiento del motor ya que una mala comunicación entre procesadores se tendrá fallas de funcionamiento en el motor.

- Las formas de onda CAN-L y CAN-H se reflejan mutuamente aproximadamente a 2,5 V y tienen una amplitud pico a pico de 1 V.
- La forma de onda CAN-L varía de 2,5 V a 1,5 V, y la forma de onda CAN-H varía de 2,5

V a 3,5 V.

- CAN-L y CAN-H se mantienen a 2,5 V entre mensajes.
- Los voltajes bajo y alto son relativamente uniformes, sin ruido ni distorsión significativos.
- Un tercer canal, A-B, muestra la diferencia de voltaje entre CAN-H y CAN-L y representa el estado lógico del bus.
- Muchos mensajes se capturan en la pantalla (búfer). La decodificación en serie asigna a cada uno una fila en la tabla de datos.
- El identificador (ID), la carga útil (datos) y las propiedades relacionadas de cada mensaje se muestran en las columnas de la tabla.
- Los datos del mensaje en cada fila se muestran en negro. Cuando aparecen, los datos de mensajes no válidos o de error se muestran en rojo.

2.5.1. Decodificación serial del bus CAN

El propósito de esta prueba es visualizar y evaluar los mensajes del bus CAN en número, no en voltaje.

Cómo realizar la prueba:

1. Localizar el conector de enlace de diagnóstico (DLC).
2. Conectar el canal A del osciloscopio al terminal 6 (CAN-H) y a la tierra del chasis.
3. Conectar el canal B del Osciloscopio al terminal 14 (CAN-L) y a la tierra del chasis.
4. Se verá que el osciloscopio ha mostrado una forma de onda de ejemplo y está preconfigurado para capturar su forma de onda como en la figura 40.
5. El osciloscopio también ha tabulado los datos de decodificación serial para cada mensaje en la forma de onda preconfigurada. Estos se reemplazan con sus datos al iniciar la captura.
6. Iniciar el osciloscopio para ver los datos en tiempo real.
7. Dar inicio al téster de pruebas que simula el motor.
8. Con las formas de onda en tiempo real en pantalla, detener el osciloscopio.
9. Apagar el téster.
10. Utilizar las herramientas de búfer de forma de onda, zoom y mediciones para examinar su forma de onda en la interfaz de la misma.

11. Analizar las tramas en código hexadecimal obtenido.

2.5.2. Análisis de resultados

Los resultados encontrados fueron llevados a la inteligencia artificial para la detección de vulnerabilidades y se encontraron los siguientes resultados, para este proceso de análisis hice uso del ChatGPT como herramienta de inteligencia artificial como se indica el tema el uso de la IA para su análisis.

En la siguiente tabla se muestra el número de repeticiones de acuerdo al id_hex que es la identificación hexadecimal de repeticiones en las comunicaciones CAN bus.

Tabla 7
Frecuencia de repeticiones de tarmas

Orden	Repeticio	id_hex	tramas	radio de frecuencia	media de tiempo	tiempo máximo	bits
1	0	153	286,0	18.387096774193548	50,000000000000000	80,000000000000000	8,0
2	1	1F0	285,0	18,369987060000000	50,000000000000000	80,000000000000000	8,0
3	2	1F3	285,0	18,369987060000000	50,000000000000000	80,000000000000000	8,0
4	3	1F5	217,0	13,926499030000000	80,000000000000000	110,00000000000000	8,0
5	4	316	100,0	6,432748538000000	160.00000000000014	169.99999999999994	8,0
6	5	329	100,0	64369310793237%	160.00000000000014	169.99999999999994	8,0
7	8	545	100,0	6,436931079000%	160.00000000000014	169.99999999999994	8,0
8	6	43B	80,0	5,146579805000000	200,00000000000000	229.99999999999878	8,0
9	7	43F	80,0	5,146579805000000	200,00000000000000	250,0	8,0
10	9	613	10,0	0.643776824034334 8	1559.999999999986	1570.000000000002	8,0
11	10	615	10,0	0.643776824034334 8	1559.999999999986	1570.000000000002	8,0

En base a los datos obtenidos se trabajó con 1553 identificaciones de tramas en código hexadecimal y la IA encontró 11 ID que son únicos, ya que indica que son un número suficiente de patrones de comunicación del bus, se determinó los IDs que interpretan con mayor frecuencia y la forma en cómo se distribuyen los mensajes.

Tabla 8

Análisis de tramas con mayor volumen y frecuencia de la red CAN

Orden	# de ejecución	_id_hex	tramas
1	9	93A	243,0
2	26	EE	230,0
3	25	EC	151,0
4	11	94E	146,0
5	8	926	145,0
6	27	F2	130,0
7	1	18	110,0
8	0	17	97,0
9	24	EA	96,0
10	14	962	54,0
11	5	8FE	49,0
12	28	F4	23,0
13	17	976	20,0
14	10	94A	13,0
15	29	F6	9,0

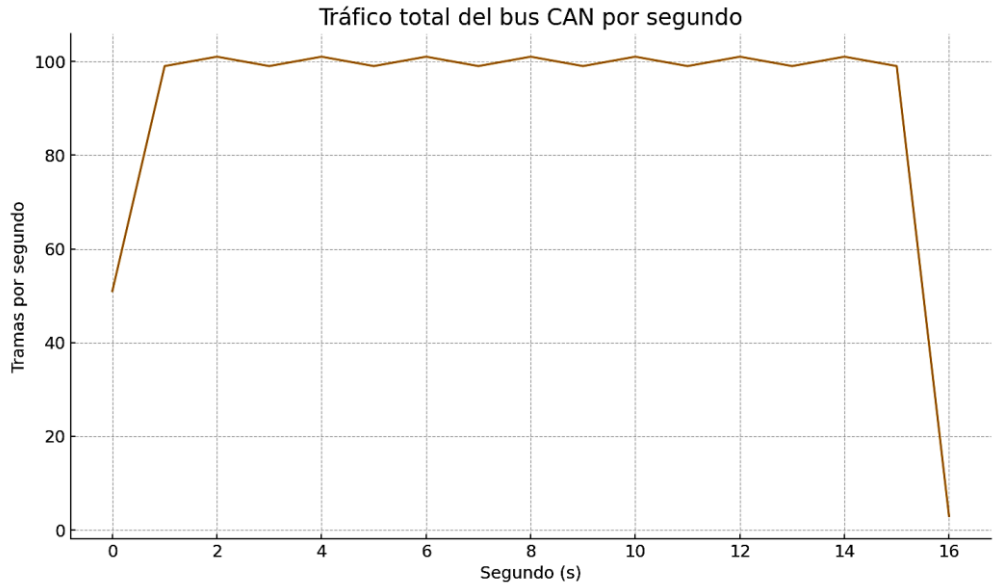
A partir de los datos cargados a la IA se encontró una conexión DLC que se mantiene dentro del rango operatorio que es de 8 bits, lo que muestra una señal excelente de trabajo, en las tramas cargadas no aparecen muestras de mensajes maliciosos.

También se encontró datos como los voltajes de tramas en el lado alto y bajo que se aprecian variaciones de entre -1,13 a 4,64 voltios de rango.

A continuación, se muestra la gráfica del tráfico total de del bus CAN por segundo en los análisis de tramas, donde el máximo tráfico se da con 100 tarmas/sec durante 16 segundos.

Figura 41

Tráfico total de tramasen función del tiempo



La figura 42 muestra como las tramas se distribuyen en post de las repeticiones de manera global del documento analizado.

Figura 42

Distribución de tiempos entre tramas

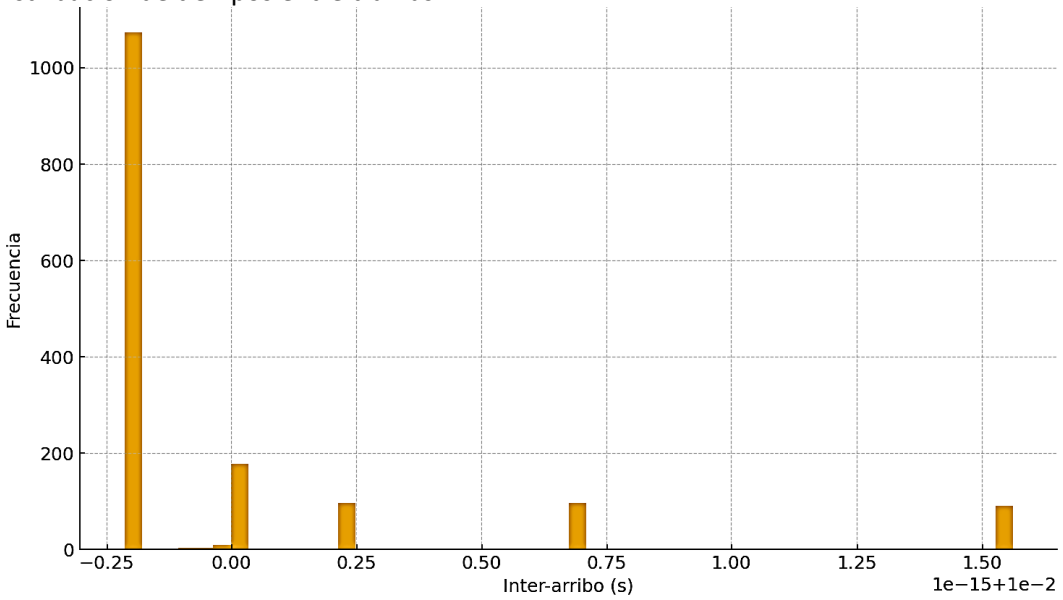
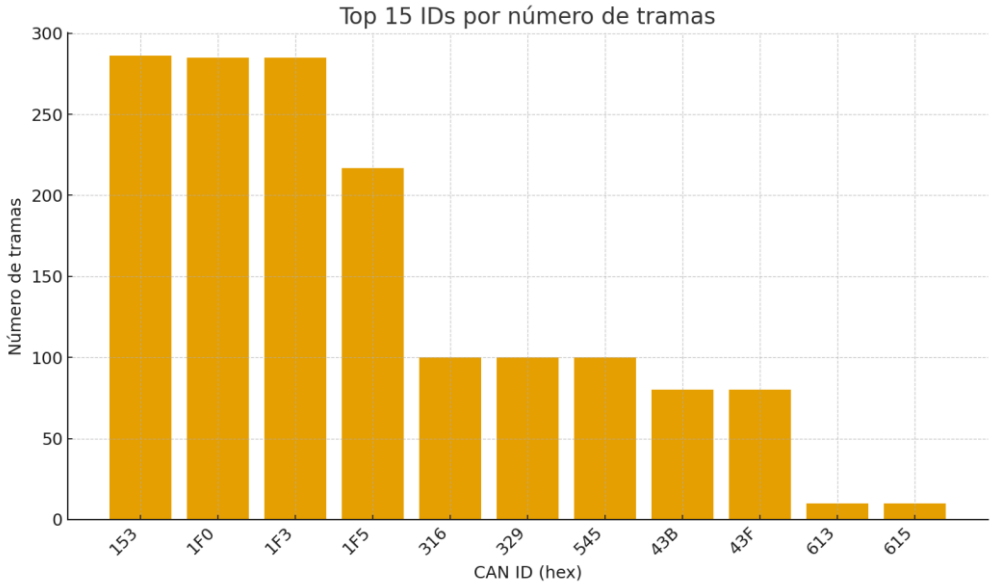


Figura 43

Frecuencia de repeticiones de tramas en función del ID



El análisis muestra que los datos analizados del CAN bus es de manera rítmica y que también es predecible, lo que en base a esto se obtienes bases necesarias para identificar anomalías con mucha facilidad, cuando algún dato se salta o rompe se apreciará de manera directa y rápida.

CONCLUSIONES

La contextualización de la fundamentación teórica es importante ya que conlleva de la mano datos investigados que son necesarios para los trabajos de banqueos de computadoras en base al análisis de protocolos de comunicación, de esta manera teniendo en cuenta los principios de funcionamiento y operación de cada uno de los elementos usados para este monitoreo de tramas. Se concluyó que los datos obtenidos ´tanto del escáner como del osciloscopio de interfaz fueron importantes para poder analizar y concluir las vulnerabilidades que la ECU está sometida. Esta adaptación de conocimientos fue determinante para iniciar el banqueo de la ECU y poder obtener el trazado de la trama multiplexada.

Se determinó que las principales debilidades del sistema CAN bus son los mensajes maliciosos que llegan a introducirse al microcontrolador ya sea por OBD II, bluetooth, wifi conectados a la red del vehículo ya que cada vez son más autómatas y necesitan estar conectados constantemente a dispositivos de control sin embargo, esto es aprovechado por los hackers que introducen mensajes maliciosos a la red de la ECU u otros microprocesadores conectados a esta red, como se indica un sujeto puede manipular datos incluso por medio del OBD II inyectando mensajes de funciones especiales desde el escáner a la ECU.

La elaboración del informe técnico fue muy satisfactoria ya que en base a esto se encontró datos relevantes como trabajan las tramas durante su operación, encontrando las vulnerabilidades tanto a modo in situ como a distancia remota controlada. La inyección de malware es relativamente sencilla, ya que alguien que sabe manejar estos equipos de diagnóstico electrónico lo puede realizar deliberadamente desde mandos remotos y de esta manera afectar el funcionamiento del vehículo incluso llegando a apagar el motor completamente.

Este informe se envió a 4 validadores expertos en el área automotriz enfocado a las redes CAN bus, los cuales dieron su aprobación posterior a revisar el contenido de los resultados encontrados y dando de esta manera una veracidad del trabajo realizado. Esta evaluación es significativa ya que se encontró muchas formas de atacar una red y que esta sea muy vulnerable ante los hackers.

RECOMENDACIONES

Se sugiere al personal realizar capacitaciones enfocados al área CAN bus y llevar de la mano la teoría de los principios de funcionamiento, especialmente en el área electrónico de comunicaciones CAN, así mismo tener información relacionado a redes multiplexadas y que en base a esto puedan decodificar los segmentos de operación.

Se recomienda hacer cursos de capacitación para determinar con mayor facilidad los datos maliciosos que están en una ECU infectado en base a los códigos binarios, decimales, hexadecimales y que de esta manera sea de manera rápida identificar que código el un mensaje malicioso y poder detener esta amenaza, ya que sería una afectación directa al vehículo y sus sistemas de comunicación.

Se recomienda realizar procesos de informes para determinar con exactitud tramas maliciosas por medio de bases de datos que se va adquiriendo en base a la experimentación del uso de herramientas de diagnóstico electrónico y software que ayudan a decodificar esta segmentación de códigos para detectar si existe o no ataques de mensajes al intencionados al sistema de comunicación CAN.

Validar por medio de pares expertos en el área automotriz específicamente redes de comunicación es indispensable, ya que de esta manera el trabajo de titulación tiene mayor veracidad tanto en lo escrito como en la experimentación, recomiendo realizar estos procesos ya que de la misma manera surgen ideas nuevas para futuras investigaciones dentro del marco del tema presentado.

BIBLIOGRAFÍA

Aguirre, J., García, F., Ramírez, C., Floreano, S., Guarda, T., Sanchez, I., Riviera, J., & Sanchez, C. (2021). Aplicación de la inteligencia artificial en la industria automotriz. *Revista Ibérica de Sistemas e Tecnologias de Informação*(E42), 149-158.

Aliwa, E., Rana, O., Perera, C., & Burnap, P. (2021). Cyberattacks and countermeasures for in-vehicle networks. *ACM computing surveys (CSUR)*, *54*(1), 1-37. https://doi.org/https://doi.org/10.1145/3431233

Araujo-Filho, P. F. D., Pinheiro, A. J., Kaddoum, G., Campelo, D. R., & Soares, F. L. (2021). An Efficient Intrusion Prevention System for CAN: Hindering Cyber-Attacks With a Low-Cost Platform. *IEEE Access*, *9*, 166855-166869. https://doi.org/https://doi.org/10.1109/ACCESS.2021.3136147

Avatefipour, O., Al-Sumaiti, A. S., El-Sherbeeny, A. M., Awwad, E. M., Elmeligy, M. A., Mohamed, M. A., & Malik, H. (2019). An Intelligent Secured Framework for Cyberattack Detection in Electric Vehicles' CAN Bus Using Machine Learning. *IEEE Access*, *7*, 127580-127592. https://doi.org/https://doi.org/10.1109/ACCESS.2019.2937576

Avatefipour, O., & Malik, H. (2018). State-of-the-art survey on in-vehicle network communication (CAN-Bus) security and vulnerabilities. *arXiv preprint arXiv:1802.01725*. https://doi.org/https://doi.org/10.48550/arXiv.1802.01725

Ben Chehida Douss, A., Abassi, R., & Sauveron, D. (2023). State-of-the-art survey of in-vehicle protocols and automotive Ethernet security and vulnerabilities. *Mathematical Biosciences and Engineering*, *20*, 17057-17095. https://doi.org/http://dx.doi.org/10.3934/mbe.2023761

Bhatia, R., Kumar, V., Serag, K., Celik, Z. B., Payer, M., & Xu, D. (2021). Evading Voltage-Based Intrusion Detection on Automotive CAN. NDSS,

Bloom, G. (2021). WeepingCAN: A stealthy CAN bus-off attack. Workshop on Automotive and Autonomous Vehicle Security,

Bozdal, M., Samie, M., Aslam, S., & Jennions, I. (2020). Evaluation of CAN Bus Security Challenges. *Sensors*, *20*(8). https://doi.org/10.3390/s20082364

Cataldo, C. (2021). *Ethernet Network in the Automotive field: Standards, possible approaches to Protocol Validation and Simulations* Politecnico di Torino].

Cheng, K., Bai, Y., Zhou, Y., Tang, Y., Sanan, D., & Liu, Y. (2020). CANeleon: Protecting CAN Bus With Frame ID Chameleon. *IEEE Transactions on Vehicular Technology*, *69*(7), 7116-7130. https://doi.org/https://dx.doi.org/10.1109/TVT.2020.2990417

Contreras-Castillo, J., Zeadally, S., & Guerrero-Ibañez, J. A. (2018). Internet of Vehicles: Architecture, Protocols, and Security. *IEEE Internet of Things Journal*, *5*(5), 3701-3709. https://doi.org/10.1109/JIOT.2017.2690902

Donadel, D., Balasubramanian, K., Brighente, A., Ramasubramanian, B., Conti, M., & Poovendran, R. (2025, 2025//). CANTXSec: A Deterministic Intrusion Detection and Prevention System for CAN Bus Monitoring ECU Activations. Applied Cryptography and Network Security, Cham.

Fakhfakh, F., Tounsi, M., & Mosbah, M. (2021). Cybersecurity attacks on CAN bus based vehicles: a review and open challenges. *Library Hi Tech*, *40*(5), 1179-1203. https://doi.org/https://doi.org/10.1108/LHT-01-2021-0013

Gupta, S., Amaba, B., McMahon, M., & Gupta, K. (2021, 24-27 May 2021). The Evolution of Artificial Intelligence in the Automotive Industry. 2021 Annual Reliability and Maintainability Symposium (RAMS),

Hartzell, S., Stubel, C., & Bonaci, T. (2020). Security Analysis of an Automobile Controller Area Network Bus. *IEEE Potentials*, *39*(3), 19-24. https://doi.org/https://doi.org/10.1109/MPOT.2018.2837686

Hernández-Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2018). *Metodología de la investigación* (Vol. 4). McGraw-Hill Interamericana México.

Jo, H. J., & Choi, W. (2022). A Survey of Attacks on Controller Area Networks and Corresponding Countermeasures. *IEEE Transactions on Intelligent Transportation Systems*, *23*(7), 6123-6141. https://doi.org/https://doi.org/10.1109/TITS.2021.3078740

Kang, L., & Shen, H. (2022). Detection and mitigation of sensor and CAN bus attacks in vehicle anti-lock braking systems. *ACM Transactions on Cyber-Physical Systems (TCPS)*, *6*(1), 1-24. https://doi.org/https://doi.org/10.1145/3495534

Li, J., Su, Y., Yang, M., Li, Z., Huang, J., & Zhong, Z. (2024, 1-5 July 2024). Topology Design of Electronic and Electrical Architecture for Time-Sensitive Network. 2024 IEEE 24th International Conference on Software Quality, Reliability, and Security Companion (QRS-C),

Lotto, A., Marchiori, F., Brighente, A., & Conti, M. (2025). A Survey and Comparative Analysis of Security Properties of CAN Authentication Protocols. *IEEE Communications Surveys & Tutorials*, *27*(4), 2470-2504. https://doi.org/https://doi.org/10.1109/COMST.2024.3486367

Marchetti, M., & Stabili, D. (2017). Anomaly detection of CAN bus messages through analysis of ID sequences. *2017 IEEE Intelligent Vehicles Symposium (IV)*, 1577-1583. https://doi.org/https://doi.org/10.1109/IVS.2017.7995934

Minawi, O., Whelan, J., Almehmadi, A., & El-Khatib, K. (2020). Machine learning-based intrusion detection system for controller area networks. Proceedings of the 10th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications,

Murlidharan, S., Ravulakole, V., Karnati, J., & Malik, H. (2025). Battery Management System: Threat Modeling, Vulnerability Analysis, and Cybersecurity Strategy. *IEEE Access*, *13*, 37198-37220. https://doi.org/https://doi.org/10.1109/ACCESS.2025.3543249

Nagarajan, J., Mansourian, P., Shahid, M. A., Jaekel, A., Saini, I., Zhang, N., & Kneppers, M. (2023). Machine Learning based intrusion detection systems for connected autonomous vehicles: A survey. *Peer-to-Peer Networking and Applications*, *16*(5), 2153-2185. https://doi.org/https://doi.org/10.1007/s12083-023-01508-7

Olufowobi, H., Young, C., Zambreno, J., & Bloom, G. (2020). SAIDuCANT: Specification-Based Automotive Intrusion Detection Using Controller Area Network (CAN) Timing. *IEEE Transactions on Vehicular Technology*, *69*(2), 1484-1494. https://doi.org/https://doi.org/10.1109/TVT.2019.2961344

Park, S. B., Jo, H. J., & Lee, D. H. (2023). Flooding attack mitigator for in-vehicle CAN using fault confinement in CAN protocol. *Computers & Security*, *126*, 103091. https://doi.org/https://doi.org/10.1016/j.cose.2023.103091

Pesé, M. D., Schauer, J. W., Li, J., & Shin, K. G. (2021). S2-can: Sufficiently secure controller area network. Proceedings of the 37th Annual Computer Security Applications Conference,

Rajapaksha, S. (2024). *Protecting vehicles from cyberattacks: context aware AI-based intrusion detection for vehicle CAN bus security* https://rgu-repository.worktribe.com/OutputFile/2801142

Rajapaksha, S., Kalutarage, H., Al-Kadri, M. O., Petrovski, A., Madzudzo, G., & Cheah, M. (2023). Ai-based intrusion detection systems for in-vehicle networks: A survey. *ACM Computing Surveys*, *55*(11), 1-40. https://doi.org/https://doi.org/10.1145/3570954

Rathore, R. S., Hewage, C., Kaiwartya, O., & Lloret, J. (2022). In-Vehicle Communication Cyber Security: Challenges and Solutions. *Sensors*, *22*(17). https://doi.org/10.3390/s22176679

Serag, K., Bhatia, R., Kumar, V., Celik, Z. B., & Xu, D. (2021). Exposing new vulnerabilities of error handling mechanism in {CAN}. 30th USENIX Security Symposium (USENIX Security 21),

Sharma, B., Thakur, A., & Srivastava, R. (2024, 9-11 May 2024). The State-of-the-Art Review on the Sensors used in the Automotive Sector. 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE),

Taylor, A., Japkowicz, N., & Leblanc, S. (2015, 14-16 Dec. 2015). Frequency-based anomaly detection for the automotive CAN bus. 2015 World Congress on Industrial Control Systems Security (WCICSS),

Wen, H., Chen, Q. A., & Lin, Z. (2020). {Plug-N-Pwned}: Comprehensive vulnerability analysis of {OBD-II} dongles as a new {Over-the-Air} attack surface in automotive {IoT}. 29th USENIX security symposium (USENIX Security 20),

Wu, W., Li, R., Xie, G., An, J., Bai, Y., Zhou, J., & Li, K. (2020). A Survey of Intrusion Detection for In-Vehicle Networks. *IEEE Transactions on Intelligent Transportation Systems*, *21*(3), 919-933. https://doi.org/https://doi.org/10.1109/TITS.2019.2908074

Xie, Y., Guo, Y., Yang, S., Zhou, J., & Chen, X. (2021). Security-Related Hardware Cost Optimization for CAN FD-Based Automotive Cyber-Physical Systems. *Sensors*, *21*(20). https://doi.org/10.3390/s21206807

Yánez, C., & Francisco, J. (2023). *Procesamiento Digital de imágenes mediante Inteligencia Artificial para la Detección de accidentes de Tránsito en Quito* Quito, Ecuador: Editorial UISRAEL].

Zhang, T., Antunes, H., & Aggarwal, S. (2014). Defending Connected Vehicles Against Malware: Challenges and a Solution Framework. *IEEE Internet of Things Journal*, *1*(1), 10-21. https://doi.org/https://doi.org/10.1109/JIOT.2014.2302386

ANEXOS

ANEXO 1
PIN DATA ECU AVEO 1,6

PinOut Chevrolet Aveo 2006 – 2010 1.6

Ecm de 64 terminales(HV-240)

Conector A (X 1) (Color Gris)

1	Tierra
2	Tierra
3	Señal del sensor de detonación
4	Control de la válvula de recirculación de gases de escape (EGR)
5	No utilizado
6	Baja referencia
7	Señal del sensor de posición del acelerador (TP)
8	Control de inyector de combustible 3
9	Control de inyector de combustible 1
10	Baja referencia
11	Señal del sensor de temperatura del refrigerante del motor (ECT)
12	Sensor de oxígeno (O 2) 1 Referencia baja (solo sin plomo)
13	Control de aire inactivo (IAC) Bobina B Control alto
14	No utilizado
15	Referencia de 5 voltios
16	Baja referencia
17	Tierra
18	Control de bobina de encendido (IC) 1 y 4
19	Bobina de encendido (IC) 2 y 3 de control
20	Control de solenoide de purga del bote de emisiones

	evaporativas (EVAP)
21	Señal del sensor de posición del cigüeñal (CKP)
22	Control de inyector de combustible 2
23	Sensor de temperatura del aire de admisión (IAT) Referencia de 5 voltios
24	Señal del sensor de presión absoluta del múltiple (MAP)
25	Señal del sensor de posición del árbol de levas (CMP)
26	Control de inyector de combustible 4
27	Señal del sensor 1 de oxigeno (O 2) (solo sin plomo)
28	Bobina de control de aire inactivo (IAC) A Control alto
29	Control de aire inactivo (IAC) B Control bajo
30	Control de aire inactivo (IAC) Un control bajo
31	Voltaje de referencia de 5 voltios
32	Baja referencia

Conector B (X 2) (Color Negro)

1	Baja referencia
2	Voltaje positivo de la batería
3	Encendido 1 voltaje
4	No utilizado
5	No utilizado
6	No utilizado
7	Señal del sensor de presión de refrigerante del aire acondicionado (ACP)

8	Señal de interruptor de octano
9	Señal de velocidad del motor
10	Señal de solicitud de aire acondicionado
11	No utilizado
12	Control de relé de ventilador de enfriamiento de alta velocidad
13	Control de solenoide de la válvula de sintonización del múltiple de admisión
14	Datos seriales CAN altos
15	Datos seriales de palabras clave
16	No utilizado
17	Referencia de 5 voltios
18	Voltaje positivo de la batería
19	Medidor de combustible
20	No utilizado
21	No utilizado
22	Señal de interruptor de octano
23	Señal de velocidad del vehículo (transmisión manual)
24	Señal del medidor del sensor de refrigerante del motor (ECT)
25	No utilizado
26	Control de relé de bomba de combustible
27	Control de relé de ventilador de enfriamiento de baja velocidad
28	A / C Compresor Embraque Bobina Tensión de alimentación
29	No utilizado
30	Datos seriales CAN bajos
31	Señal del sensor de nivel de combustible
32	Control de la lámpara indicadora de mal funcionamiento (MIL)

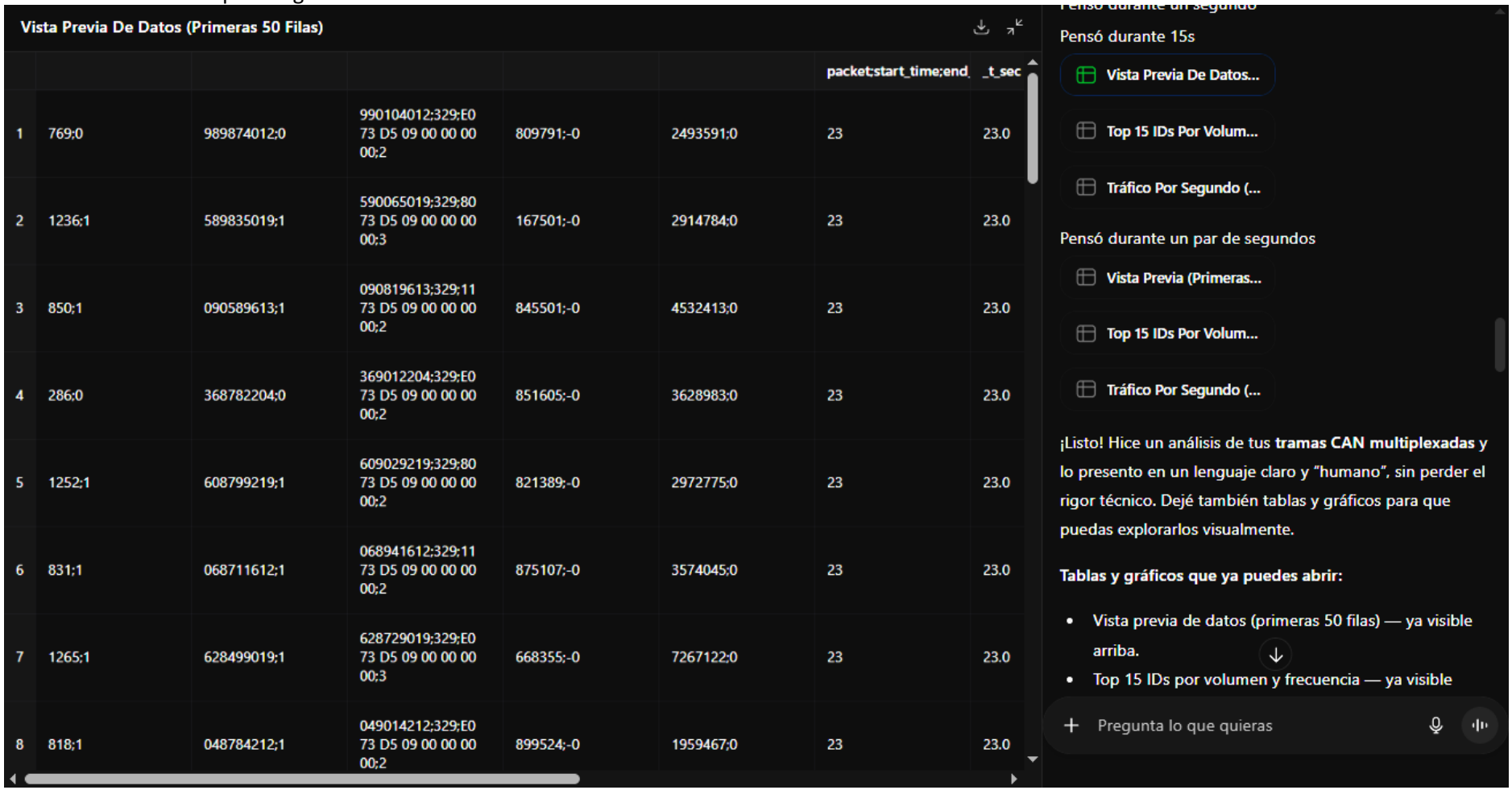
ANEXO 2

Interfaz del osciloscopio y la detección de las tramas

Packet	Start Time	End Time	ID	RTR	FDF	DLC	Data	CRC	ACK	CRC Valid	Bit Stuffing Valid	Valid	IDE
1	245,4 µs	487,4 µs	1F5	0	0	8	5F 00 00 00 80 11 00 00	68 1E	0	✔	✔	✔	0
2	2,736 ms	2,976 ms	43F	0	0	8	08 08 A0 FF 00 00 00 00	02 94	0	✔	✔	✔	0
3	3,998 ms	4,228 ms	153	0	0	8	E4 49 00 FF 00 FF FF 82	4E A2	0	✔	✔	✔	0
4	4,234 ms	4,47 ms	1F0	0	0	8	09 60 09 00 09 00 09 00	13 08	0	✔	✔	✔	0
5	4,476 ms	4,716 ms	1F3	0	0	8	00 80 00 FF 01 80 00 08	7C 94	0	✔	✔	✔	0
6	8,506 ms	8,744 ms	316	0	0	8	05 40 00 00 00 14 00 00	43 EB	0	✔	✔	✔	0
7	8,75 ms	8,988 ms	1F5	0	0	8	5F 00 00 00 80 21 00 00	08 E2	0	✔	✔	✔	0
8	8,994 ms	9,224 ms	329	0	0	8	80 73 D5 09 00 00 00 00	6F 16	0	✔	✔	✔	0
9	9,23 ms	9,472 ms	545	0	0	8	02 00 00 00 00 01 00 00	15 F1	0	✔	✔	✔	0

ANEXO 3

Interfaz de la IA usada para la gestión de identifiación de vulnerabilidades



ANEXO 4

Encuesta desarrollada a estudiantes y técnicos automotrices

ENCUESTA DE VALIDACIÓN DE PROYECTO

Encuesta estructurada en base a autores certificados para evaluar la aceptación y viabilidad del tema "**Vulnerabilidades en la comunicación multiplexada de redes CAN-BUS para la detección y mitigación de mensajes maliciosos mediante inteligencia artificial"**

Este estudio pretende responder a siete preguntas ilustradas en base al siguiente cuestionario. Obviamente, también se pueden plantear otras preguntas, pero se basa al autor certificado del artículo que son suficientes para exponer una amplia variedad de investigaciones en el campo estudiado.

Marca con una **x** en el casillero correspondiente de acuerdo a su experiencia y conocimiento.

Preguntas:

1. **¿Conoce los conceptos básicos relacionados con los protocolos de comunicación que se implementan actualmente en los vehículos actuales, así como también las ventajas y desventajas de cada uno?**

…….. SI

…….. NO

2. **¿Conoce los atributos que se pueden considerar para comparar los distintos protocolos utilizados en las comunicaciones de red a bordo de vehículos?**

…….. SI

…….. NO

3. **¿Conoce los requisitos y las limitaciones de seguridad en las redes a bordo de vehículos, según el protocolo AE?**

…….. SI

…….. NO

4. **¿Conoce las vulnerabilidades de seguridad se pueden encontrar en una red AE y cuáles son los posibles resultados de los ataques a los sistemas del vehículo?**

…….. SI

…….. NO

5. **¿Conoce los ataques dirigidos a las redes a bordo de vehículos basadas en AE?**

…….. SI

…….. NO

6. **¿Conoce las defensas existentes contra estos ataques?**

…….. SI

…….. NO

7. **¿Conoce las recomendaciones y los desafíos para encontrar posibles soluciones para proteger las AE?**

…….. SI

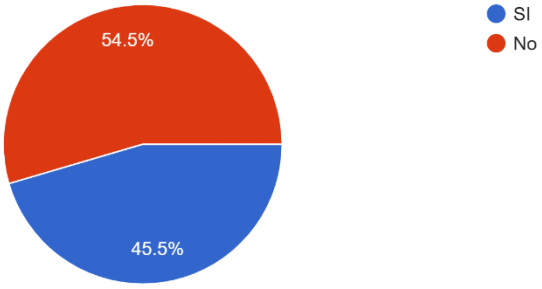
…….. NO

ANEXO 5

Evidencia de respuestas de la encuesta

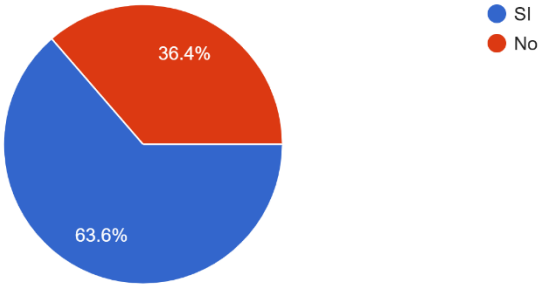
¿Conoce las vulnerabilidades de seguridad se pueden encontrar en una red AE y cuáles son los posibles resultados de los ataques a los sistemas del vehículo?

11 respuestas



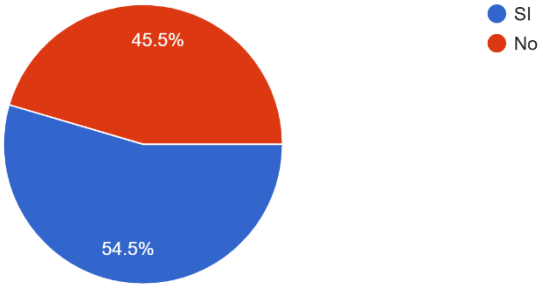
¿Conoce los conceptos básicos relacionados con los protocolos de comunicación que se implementan actualmente en los vehículos actuales... también las ventajas y desventajas de cada uno?

11 respuestas



¿Conoce los atributos que se pueden considerar para comparar los distintos protocolos utilizados en las comunicaciones de red a bordo de vehículos?

11 respuestas



ANEXO 6
Certificado de validación de propuesta 1

Universidad Israel

Yo, **Lorena Maribel Camacho Játiva** con C.I **1715963797** en mi calidad de validador de la propuesta del proyecto titulado: "**Vulnerabilidades en la comunicación multiplexada de redes CAN-BUS para la detección y mitigación de mensajes maliciosos mediante inteligencia artificial**".

Elaborado por el **Ing. Manuel Rodrigo Passo Guamangate**, con C.I **1723741300**, estudiante de la Maestría en Electrónica y Automatización de la Universidad Tecnológica Israel (UISRAEL), como parte de los requisitos para obtener el Título de Magister, me permito declarar haber revisado el proyecto y realizado la evaluación de criterios.

Quito D.M., 09 de septiembre de 2025

Firmado electrónicamente por:
LORENA MARIBEL CAMACHO JATIVA
Validar únicamente con FirmaEC

Ing. **Lorena Maribel Camacho Játiva** M.Sc.

C.I:1715963797

Registro SENESCYT: 1020-14-86043065

ANEXO 7

Instrumento de validación de la propuesta 1

Universidad Israel

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN ELECTRÓNICA Y AUTOMATIZACIÓN

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **"Vulnerabilidades en la comunicación multiplexada de redes CAN-BUS para la detección y mitigación de mensajes maliciosos mediante inteligencia artificial"**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por:

Título obtenido
MAGISTER EN GESTIÓN DE ENERGÍAS
Cédula de Identidad
1715963797
E- mail
Lcamacho220683@gmail.com
Institución de Trabajo
INSTUTUTO SUPERIOR TECNOLOGICO TECNOECUATORIANO
Cargo
COORDINADORA DE PPP
Años de experiencia en el área
12 AÑOS

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema:

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	*X*				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	***X***				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	***X***				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	***X***				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	***X***				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	***X***				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	*X*				
Total		*35*				

Observaciones:

_____

_____

Recomendaciones

_____

_____

Lugar, fecha de validación: QUITO 09 DE SEPTIEMBRE DE 2025

LORENA MARIBEL CAMACHO JATIVA

Firma del especialista

ANEXO 8

Certificado de validación de propuesta 2

Universidad Israel

Yo, **César Andrés Minaya Andino**, con C.I **0604887919**, en mi calidad de validador de la propuesta del proyecto titulado: "**Vulnerabilidades en la comunicación multiplexada de redes CAN-BUS para la detección y mitigación de mensajes maliciosos mediante inteligencia artificial**".

Elaborado por el **Ing. Manuel Rodrigo Passo Guamangate**, con C.I **1723741300**, estudiante de la Maestría en Electrónica y Automatización de la Universidad Tecnológica Israel (UISRAEL), como parte de los requisitos para obtener el Título de Magister, me permito declarar haber revisado el proyecto y realizado la evaluación de criterios.

Quito D.M., 11 de agosto de 2025

CESAR ANDRES MINAYA ANDINO

Firmado digitalmente por CESAR ANDRES MINAYA ANDINO
Fecha: 2025.09.11 21:14:33 -05'00'

Ing. César Andrés Minaya Andino, MSc.

C.I: 0604887919

Registro SENESCYT: 6432152936

ANEXO 9

Instrumento de validación de la propuesta 2

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN ELECTRÓNICA Y AUTOMATIZACIÓN

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **"Vulnerabilidades en la comunicación multiplexada de redes CAN-BUS para la detección y mitigación de mensajes maliciosos mediante inteligencia artificial"**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por:

Título obtenido
Master en Mecatrónica y Robótica
Cédula de Identidad
0604887919
E- mail
candresma3@gmail.com
Institución de Trabajo
Instituto Superior Tecnológico Rumiñahui
Cargo
Docente Investigador
Años de experiencia en el área
4

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema:

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	*X*				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*		*X*			
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	*X*				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	*X*				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	*X*				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*			*X*		
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*		*X*			
	Total	*20*	*8*	*3*		

Observaciones:

La propuesta aborda un problema crítico en la ciberseguridad de vehículos conectados, donde las redes CAN-BUS son vulnerables a ataques como inyecciones de mensajes maliciosos. Su impacto potencial es alto en industrias automotrices, pero podría beneficiarse de mayor énfasis en mitigación activa. La factibilidad depende de hardware embebido eficiente, ya que modelos pesados de IA podrían sobrecargar ECUs limitadas en recursos.

Recomendaciones

Desarrollar modelos de inteligencia artificial ligeros, como redes neuronales comprimidas o técnicas de poda (pruning), para garantizar que sean compatibles con las limitaciones computacionales de las Unidades de Control Electrónico (ECUs) en vehículos. Evaluar el costo de implementación (hardware, software, entrenamiento de modelos) y proponer estrategias para escalar la solución a diferentes tipos de vehículos.

Lugar, fecha de validación: Quito D.M., 11 de agosto de 2025

CESAR ANDRES MINAYA ANDINO

Firmado digitalmente por CESAR ANDRES MINAYA ANDINO
Fecha: 2025.09.11 21:14:33 -05'00'

Firma del especialista

ANEXO 10
Certificado de validación de propuesta 3

Universidad Israel

Yo, **Víctor Fabricio Moreno Riquero**, con C.I **1205315235**, en mi calidad de validador de la propuesta del proyecto titulado: "**Vulnerabilidades en la comunicación multiplexada de redes CAN-BUS para la detección y mitigación de mensajes maliciosos mediante inteligencia artificial**".

Elaborado por el **Ing. Manuel Rodrigo Passo Guamangate**, con C.I **1723741300**, estudiante de la Maestría en Electrónica y Automatización de la Universidad Tecnológica Israel (UISRAEL), como parte de los requisitos para obtener el Título de Magister, me permito declarar haber revisado el proyecto y realizado la evaluación de criterios.

Quevedo, 12 de septiembre de 2025

VICTOR FABRICIO MORENO RIQUERO

Ing. Víctor Fabricio Moreno Riquero, M.Sc.

C.I: 1205315235

Registro SENESCYT: 1014-16-1448959

ANEXO 11

Instrumento de validación de la propuesta 3

Universidad Israel

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN ELECTRÓNICA Y AUTOMATIZACIÓN

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **"Vulnerabilidades en la comunicación multiplexada de redes CAN-BUS para la detección y mitigación de mensajes maliciosos mediante inteligencia artificial"**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por:

Título obtenido
Ingeniero Industrial
Cédula de Identidad
1205315235
E- mail
victormoreno@itscv.edu.ec
Institución de Trabajo
Instituto Superior Tecnológico Ciudad de Valencia
Cargo
Docente Tecnología Superior en Mecánica Automotriz
Años de experiencia en el área
10

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema:

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	*X*				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	*X*				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*		*X*			
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	*X*				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	*X*				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	*X*				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	*X*				
Total		*34*				

Observaciones:

Se evidencia una presentación adecuada de los conceptos clave relacionados con el tema del proyecto de titulación. Sin embargo, algunos términos fundamentales innovadores carecen de definición precisa o están poco fundamentados con el avance tecnológico en la industria automotriz, lo que puede afectar la claridad y el rigor teórico- práctico del trabajo de titulación.

Recomendaciones

Se sugiere establecer la data de las marcas de los vehículos y la tecnología que poseen, para efectuar el estudio del proyecto de titulación.

Lugar, fecha de validación: Quevedo, 12 de septiembre de 2025

Ing. Víctor Moreno Riquero, MSc.

Firma del especialista

ANEXO 12
Certificado de validación de propuesta 4

Universidad Israel

Yo, **Victor Patricio Pachacama Nasimba,** con C.C 0104685284, en mi calidad de validador de la propuesta del proyecto titulado: "**Vulnerabilidades en la comunicación multiplexada de redes CAN-BUS para la detección y mitigación de mensajes maliciosos mediante inteligencia artificial**".

Elaborado por el **Ing. Manuel Rodrigo Passo Guamangate**, con C.C **1723741300**, estudiante de la Maestría en Electrónica y Automatización de la Universidad Tecnológica Israel (UISRAEL), como parte de los requisitos para obtener el Título de Magister, me permito declarar haber revisado el proyecto y realizado la evaluación de criterios.

Quevedo, 9 de septiembre de 2025

firman electrónicamente por:
VICTOR PATRICIO
PACHACAMA NASIMBA
validar únicamente con firmasec

Ing. Victor Patricio Pachacama Nasimba, M.Sc.

C.C: 0104685284

Registro SENESCYT: 1002-2023-2798012

ANEXO 13

Instrumento de validación de la propuesta 4

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN ELECTRÓNICA Y AUTOMATIZACIÓN

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **"Vulnerabilidades en la comunicación multiplexada de redes CAN-BUS para la detección y mitigación de mensajes maliciosos mediante inteligencia artificial"**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Victor Patricio Pachacama Nasimba

Título obtenido
Magister en Diseño Mecánico Magister en Educación mención Pedagogía en Entornos Digitales
Cédula de Identidad
0104685284
E- mail
ingvictorpachacama@gmail.com
Institución de Trabajo
Universidad Técnica Estatal de Quevedo
Cargo
Docente
Años de experiencia en el área
6

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema:

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	x				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	x				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	x				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	x				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*		x			
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*			x		
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	x				
Total		*32*				

Observaciones:

La factibilidad del proyecto se ha calificado como Adecuado porque, si bien la propuesta es conceptualmente sólida y altamente relevante, su ejecución práctica presenta tres desafíos significativos que deben ser gestionados con sumo cuidado para garantizar el éxito dentro de los plazos y recursos típicos de un proyecto de titulación. No es que el proyecto sea inviable, sino que su complejidad práctica exige un enfoque realista.

El primer desafío radica en el acceso a los recursos necesarios. A diferencia de un proyecto puramente basado en software, esta investigación tiene una dependencia crítica de hardware específico para interactuar con una red CAN-BUS. Esto implica la necesidad de contar con un analizador CAN-to-USB, un banco de pruebas con Unidades de Control Electrónico (ECU) o, idealmente, acceso a un vehículo real. Como alternativa, se podría recurrir a simuladores de software (como CANoe o VectorCAST), pero estos pueden tener costos de licencia elevados o no replicar con total fidelidad las sutilezas del tráfico en un entorno físico. La disponibilidad y el costo de estos recursos son un factor que modera la factibilidad, situándola en un nivel adecuado, pero no garantizado de antemano.

El segundo y quizás el obstáculo más formidable es la obtención o generación de un conjunto de datos (dataset) de calidad. Los modelos de inteligencia artificial son tan buenos como los datos con los que se entrenan. Para este proyecto, se requiere un dataset robusto que contenga

no solo un gran volumen de tráfico normal de la red CAN, sino también una muestra representativa y, fundamentalmente, etiquetada de diversos ataques maliciosos (como inyección de mensajes, ataques de suplantación o de denegación de servicio). Conseguir datasets públicos que cumplan estas características es difícil, y crear uno propio es una tarea monumental que podría constituir un proyecto de titulación por sí solo. Este factor representa el mayor riesgo para el cronograma del proyecto.

Finalmente, la propuesta incluye tanto la detección como la mitigación de ataques. Mientras que la detección es un objetivo desafiante pero alcanzable, la mitigación introduce una capa de complejidad y riesgo mucho mayor. Implementar un mecanismo de mitigación activo en una red CAN-BUS es una tarea delicada; una acción incorrecta, como bloquear un mensaje que se identifica erróneamente como malicioso (un falso positivo), podría tener consecuencias graves en el funcionamiento del vehículo. Por ello, la parte de mitigación, si se pretende implementar de forma práctica, eleva considerablemente la dificultad técnica y los riesgos asociados.

Recomendaciones

La propuesta es excelente, altamente relevante y con un gran potencial de impacto. Sus puntos más fuertes son su actualidad, conceptualización y pertinencia.

Para asegurar su éxito, se recomienda al estudiante:

Definir un Alcance Realista: Considerar enfocarse principalmente en la detección de ataques, desarrollándola de manera profunda y robusta. La parte de mitigación podría abordarse a nivel de propuesta o con un prototipo simple, ya que su implementación en un sistema real es compleja y delicada.

Plan de Obtención de Datos: Investigar desde el inicio la disponibilidad de datasets públicos de tráfico CAN (como el "Car-Hacking Dataset") o planificar la estrategia para generar uno propio, ya sea mediante simulación o experimentación en un vehículo real.

Identificar los Recursos Necesarios: Listar tempranamente el hardware (ej. CAN-to-USB adapter, Raspberry Pi) y software (simuladores, librerías de IA) que se necesitarán para llevar a cabo el proyecto.

Lugar, fecha de validación: Quevedo, 9 de sep. de 2025

Firma del especialista