

Report of July 2025

# Cybersecurity in mobility

Recent developments

Curated and summarized - Industry and Patent news

Published by Dennemeyer India Private Limited

Parag Thakre ( [pthakre@dennemeyer.com](mailto:pthakre@dennemeyer.com) )

Himanshu Varun ( [hvarun@dennemeyer.com](mailto:hvarun@dennemeyer.com) )

This report is subject to copyrights and may only be reproduced with permission of Dennemeyer.



# Subscribe now



Scan the QR code to receive this monthly report via email in your inbox.



# Preface

The rise of connected cars and software-defined vehicles has revolutionized the automotive industry, but it comes with a surge in cybersecurity threats. Thus, cybersecurity becomes paramount for the OEMs, suppliers and users.

This monthly report is focused on “Cybersecurity in Mobility” including applications in Electric Vehicles, Autonomous Vehicles, Software Defined Vehicles, UAVs, Drones, Aircrafts, Fleets, etc. This report is a free resource for anyone working in this domain including technologists, innovators, Intellectual Property (IP) managers, strategy makers, etc. The report contains curated insights and summaries of the latest news and key patents published in the last one month, including the latest products, business updates, collaborations, new innovations, etc.



# Key Insights

- ❑ Researchers have identified vulnerabilities in modern vehicles, particularly in keyless entry systems, making them potential targets for hackers. As a result, automakers need to implement new cryptographic protocols to strengthen vehicle security, while regulatory bodies enforce stricter regulations.
- ❑ As adoption of software-defined vehicles (SDVs) increases worldwide, companies lacking in-house expertise may struggle to keep pace with compliance and innovation. To address this, Accenture and IIT Madras have launched the SDV Academy to upskill engineers in embedded software, connectivity, AI, and cybersecurity, positioning India as a future SDV engineering hub.
- ❑ Strategic partnerships between FPT & Cymotive, LDRA & Renesas, and PlaxidityX & GlobalLogic reflect a unified industry push to embed security and compliance throughout the SDV development lifecycle. This collaborative approach accelerates secure-by-design, standards-compliant software delivery and enables OEMs to validate their code even before actual hardware is ready.
- ❑ Many inventions that were published last month had major themes as below:
  - In the connected vehicle space, recent inventions are introducing multi-layered intrusion detection systems (IDS) that use AI, real-time threat scoring, and adaptive rules to secure ECUs and CAN buses. When integrated with cloud analytics, behavior tracking, and blockchain, these systems improve detection accuracy and reduce false alarms.
  - Recent inventions in the UAV space are enhancing security with layered GPS spoofing defenses that leverage fog computing nodes, blockchain, and machine learning. This approach enables localized location verification and early anomaly detection, supporting safer navigation and deployment in dense urban environments.



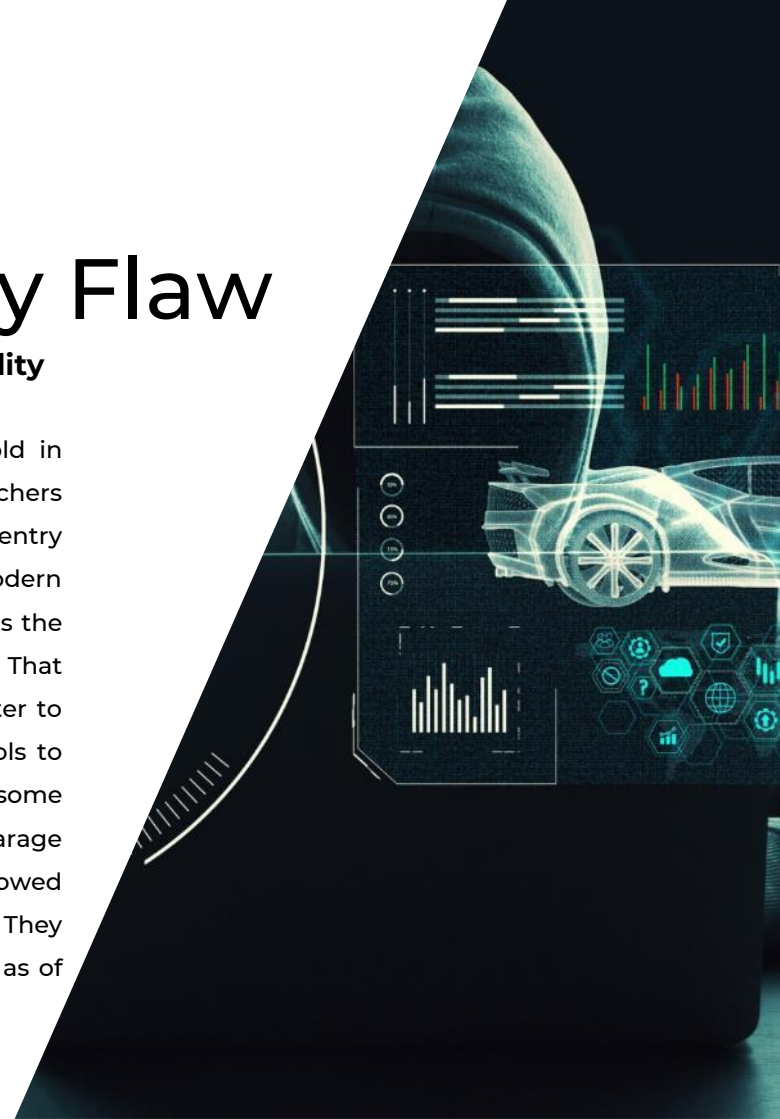
# KIA Keyless Entry Flaw

## **KIA Ecuador keyless entry systems vulnerability exposes thousands of vehicles to theft**

A major security flaw has been found in KIA cars sold in Ecuador, affecting models from 2022 to 2025. Researchers discovered that these vehicles use an old type of keyless entry system that's easy to hack. Instead of using modern technology that changes the signal every time you press the key fob, these cars use the same signal again and again. That means a thief can record the signal once and use it later to unlock the car. Even worse, hackers can use cheap tools to create their own fake keys that work on these cars. In some cases, one key fob could even open other cars or garage doors because the codes are too similar. Researchers showed how this hack works using a tool called AutoRFKiller. They warned KIA Ecuador about this issue back in 2024, but as of now, nothing has been done to fix it.

Source

<https://cybersecuritynews.com/>





# Strategic Alliance

## **FPT and Cymotive form strategic alliance to advance automotive cybersecurity innovation**

FPT, a global IT services company, has signed a Memorandum of Understanding (MoU) with Israeli cybersecurity firm Cymotive Technologies to jointly develop cybersecurity solutions for Software-Defined Vehicles (SDVs). This partnership aims to protect modern cars that rely heavily on software by combining FPT's global reach with Cymotive's deep cybersecurity expertise. The collaboration will create new security tools to meet the growing technical and legal demands of the auto industry. These tools will help carmakers and suppliers defend against cyber threats as vehicles become more connected and autonomous.

Source

<https://fptsoftware.com/>





# Collaboration

## **LDRA joins Renesas ready partner network and R-Car consortium to accelerate safety-critical software development, verification and certification**

LDRA, a provider of software testing tools for safety-critical systems like automotive and aerospace, has partnered with Renesas, a leading manufacturer of vehicle chips that power features such as autonomous driving and infotainment. With this partnership, LDRA's tools are now integrated with Renesas chips and development platforms, enabling developers to test and optimize their code more quickly, even before the actual hardware is ready. This collaboration also streamlines compliance with rigorous safety and cybersecurity standards like ISO 26262 and Automotive SPICE.





# Upskilling for Automotive Future

## **Accenture LearnVantage and IIT Madras's CAAR collaborate to skill talent for software-defined vehicles**

Accenture and IIT Madras have partnered to train professionals in building software-defined vehicles (SDVs). They have launched specialized training programs through Accenture's LearnVantage SDV Academy to help automotive workers and engineers develop the digital skills required for these advanced vehicles. The courses cover areas such as connected devices (IoT), cybersecurity, in-car software systems, and global industry standards like AUTOSAR and ASPICE. Training will be delivered by IIT Madras through a mix of online and instructor-led sessions. With SDVs projected to reach a \$3.5 trillion by 2040, this initiative aims to prepare the workforce for the future of the automotive industry.

Source

<https://www.iitm.ac.in/>





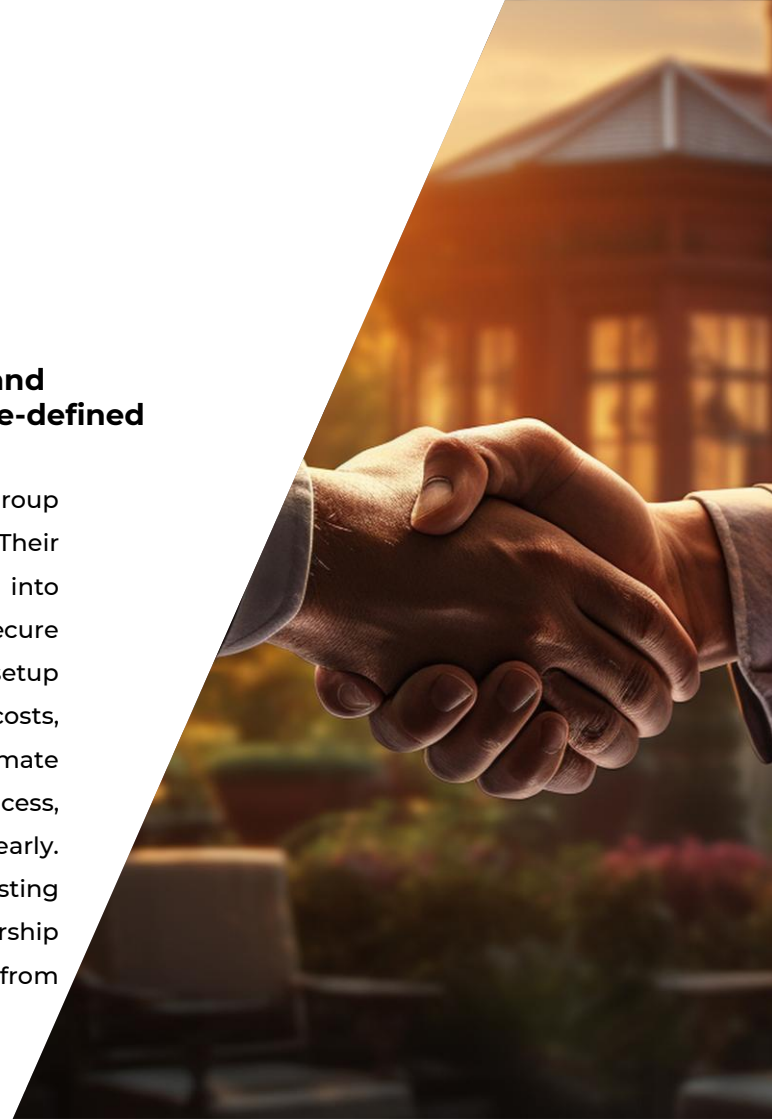
# Partnership

## **GlobalLogic and PlaxidityX partner to secure and streamline the development cycle for software-defined vehicles (SDVs)**

PlaxidityX has partnered with GlobalLogic, a Hitachi Group company, to enhance the security of SDV development. Their collaboration integrates PlaxidityX's security tools into GlobalLogic's SDV Cloud Framework, creating a secure environment for vehicle software engineering. This setup helps OEMs and suppliers speed up development, cut costs, and meet strict security standards. PlaxidityX's tools automate security checks throughout the development process, checking for vulnerabilities ensuring issues are caught early. Meanwhile, GlobalLogic's system allows real hardware testing and continuous updates to the software. This partnership shows how important it is to build software that's secure from the ground up.

Source

<https://plaxidityx.com/>





PATENT

The editor's shortlist

# Patents of the month



## Patents of the month

Published in June 2025

### Shortlisted and summarized by our analyst

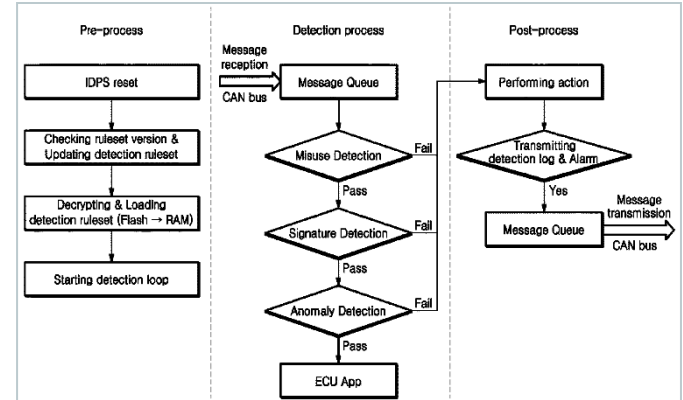
- [US12335278B2](#) - System and method for detecting intrusion into in-vehicle network  
[Assignee: Hyundai Motor Co, Kia Corp](#)
- [US2025202913A1](#) - Universal intrusion detection and prevention for vehicle networks  
[Assignee: Sonatus Inc](#)
- [US12341750B2](#) - Arrangement of cyber security and prognostics, coexisting on a single platform  
[Assignee: Dearborn Group Inc](#)
- [US2025200172A1](#) - Systems and methods for detecting spoofing attacks on an unmanned aerial system  
[Assignee: Intelligent Fusion Tech Inc, Research Foundation Of State Univ Of New York](#)
- [EP4068690B1](#) - Attack analyzer, attack analysis method and attack analysis program  
[Assignee: KIA Corporation, Hyundai Motor Company](#)
- [DE112021008401B4](#) - Intrusion detection system  
[Assignee: Mitsubishi Electric Corp](#)
- [JP7694824B2](#) - Monitoring device, vehicle monitoring method, and vehicle monitoring program  
[Assignee: Sumitomo Electric Ind Ltd; Sumitomo Wiring System Ltd; Auto Network Gijutsu Kenkyusho Kk](#)
- [KR102825990B1](#) - CAN communication security method for detecting can bus attacks, recording medium and CAN communication device for performing the same  
[Assignee: AY Innovation Co., Ltd.](#)
- [CN115130113B](#) - Vulnerability analysis method, system and medium of automobile ECU firmware  
[Assignee: Dongfeng Motor Group Co Ltd](#)
- [CN120090881A](#) - Intrusion detection method for edge node of Internet of vehicles, electronic equipment and medium  
[Assignee: Thalys Automobile Co Ltd](#)





## US12335278B2

# System and method for detecting intrusion into in-vehicle network



This patent tackles the rising security risks in modern vehicles caused by more Electronic Control Units (ECUs) being connected through wired and wireless networks, which traditional intrusion detection systems (IDS) can't handle effectively, leaving cars vulnerable. To fix this, the patent suggests a smarter IDS system built into the car. It collects messages from the network, uses secure memory to store rules for spotting threats, and applies these rules using a special engine. This engine also gives each threat a score based on how serious and trustworthy it is, then sends detailed reports to a remote server and ranks them by how dangerous and reliable each threat is, especially when multiple issues occur in a short time.

Company name Hyundai Motor Co, Kia Corp

Inventors Kim Tae Guen,  
Cho A Ram,  
Park Seung Wook,  
Lim Wha Pyeong

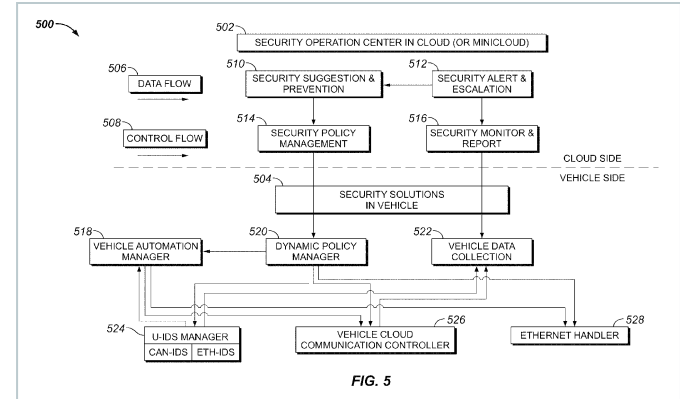
Priority date 10 Feb 2020

Publication date 17 Jun 2025



## US2025202913A1

# Universal intrusion detection and prevention for vehicle networks



This patent deals with the rising security risks in modern cars as they become more connected to external networks. These connections make cars vulnerable to malware, hackers, and communication-based attacks that can interfere with how the car works or steal private data. To solve this, the patent introduces a setup that includes a controller to keep an eye on different parts of the car's internal network. Each part may include sensors or control units. The setup watches the communication between these parts and uses special tools to detect anything suspicious. If it finds a threat, the system can take action right away without needing someone to step in manually. It also connects to cloud services to gather and analyze data from many vehicles at once, making it easier to spot and deal with security threats quickly and accurately.

Company name Sonatus Inc

Inventors Fang Yu, Ling Andrew,  
Valenzuela Felipe Andres Valdes,  
Zong Xuanran, Dhankhar Sudhir Ramphal,  
Chai Fangming

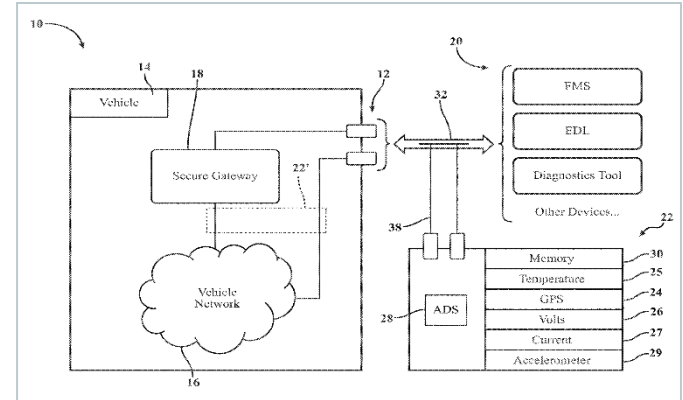
Priority date 20 Sep 2019

Publication date 19 Jun 2025



## US12341750B2

# Arrangement of cyber security and prognostics, coexisting on a single platform



This patent addresses the cyber vulnerabilities in vehicle networks, especially in older models lacking built-in security, which are at risk from threats entering through diagnostic ports via wired or wireless connections. To solve this, a cybersecurity device that connects to the vehicle's network is proposed. This device watches all data coming in and going out and uses an anomaly detection system (ADS) to spot anything unusual or dangerous. It can detect threats from both incoming and outgoing data. It also stores all this activity in a memory log, which can be reviewed later for investigation. It even has built-in sensors that collect extra information, helping monitor the vehicle's condition. Based on this data, the device can also create maintenance alerts when it detects signs that something might need servicing.

Company name Dearborn Group Inc

Inventors Zachos Mark P,  
Kulkarni Prakash K

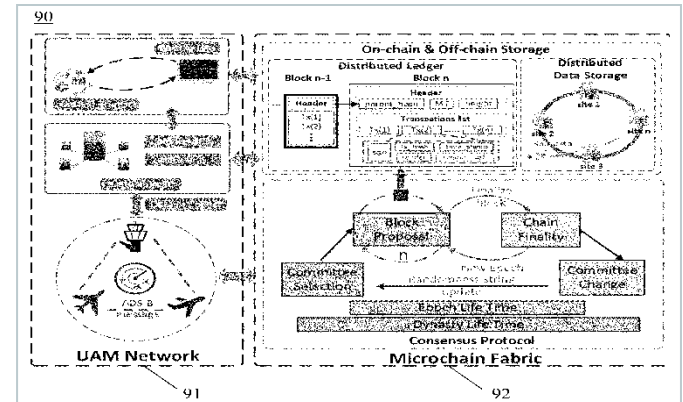
Priority date 20 Oct 2021

Publication date 24 Jun 2025



## ◀ US2025200172A1

# Systems and methods for detecting spoofing attacks on an unmanned aerial system



This patent is about protecting unmanned aerial vehicles (UAVs) from spoofing attacks, which are fake signals that can tamper with the GPS data. This is an increasing risk in crowded city skies. The idea involves each drone sending its GPS data to a nearby processing unit called a "fog node" for verification. Instead of relying on a central server, it uses lightweight blockchain technology to keep the data safe and secure. It also employs advanced machine learning tools to detect unusual GPS patterns that may indicate spoofing. To handle data efficiently, it stores some information on the blockchain (on-chain) and some off-chain, balancing security and performance. This setup helps drones detect GPS attacks early and keeps them flying safely and accurately in busy urban areas.

**Company name** Intelligent Fusion Tech Inc, Research Foundation Of State Univ Of New York

**Inventors** Wei Sixiao, Xu Ronghua, Chen Yu, Blasch Erik, Pham Khanh, Chen Genshe

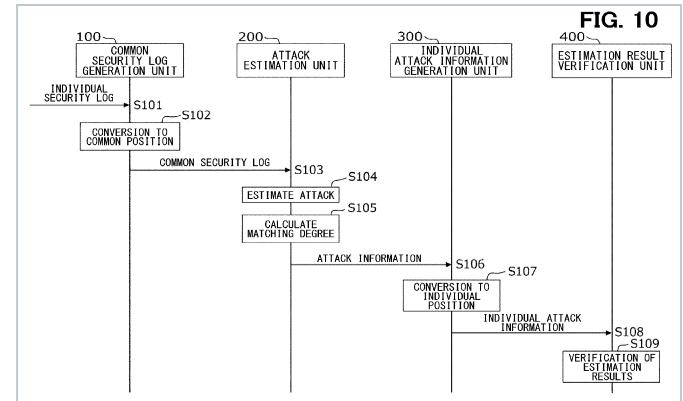
**Priority date** 15 Dec 2023

**Publication date** 19 Jun 2025



## EP4068690B1

# Attack analyzer, attack analysis method and attack analysis program



This patent addresses the difficulty of analyzing cyberattacks on vehicle electronic control systems, especially since different vehicles have different setups, making it hard to spot common patterns. It introduces an attack analyzer that collects security logs from vehicles in a standard format. These logs include information about where and what kind of problems were detected. It also has a stored table that links known attack types with the kinds of strange behavior and locations they usually affect, also using the same format. By comparing what actually happened in the vehicle with what is expected for certain attacks, it can be figured out what kind of attack it might be. This approach works across different vehicle models, reduces the need for separate tools for each part, and helps respond to cyber threats more quickly by allowing real-time analysis.

Company name KIA Corporation, Hyundai Motor Company

Inventors Nagara Keigo,  
Abe Taiji,  
Imoto Reiichiro

Priority date 29 Mar 2021

Publication date 18 Jun 2025



◀ DE112021008401B4

## Intrusion detection system

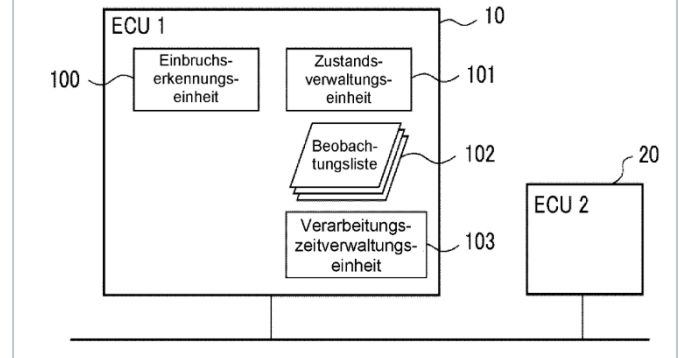
Company name Mitsubishi Electric Corp

Inventors Okuyama Hiroshi,  
Matsui Toshinori

Priority date 25 Oct 2021

Publication date 05 Jun 2025

FIG. 15



This invention deals with the problem of hackers sending harmful data to a car's control systems, which can cause serious malfunctions. Current solutions often fail to detect these attacks, especially when hackers try to hide their actions. To fix this, the invention proposes an IDS that uses a list of rules defining what kind of data is considered normal or suspicious based on the car's current state. The system checks all data on the vehicle's communication lines against this list to spot anything unusual, while continuously updating the list in real time as the car's condition changes, making detection more accurate. It also includes a delay feature that slightly slows down data processing to confuse attackers trying to figure out how the system works. Finally, if suspicious data is found, the system takes immediate action to address the threat.



## ◀ JP7694824B2

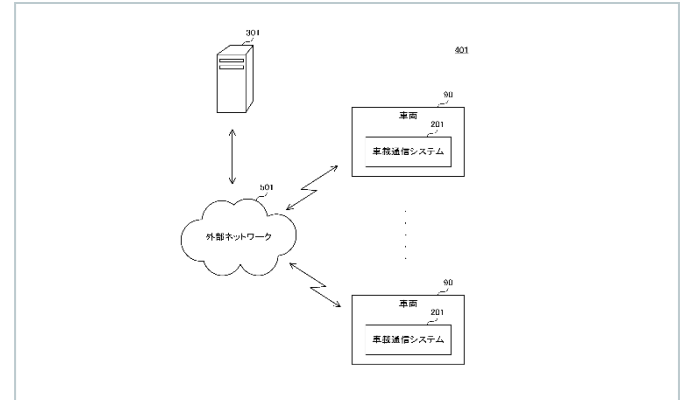
# Monitoring device, vehicle monitoring method, and vehicle monitoring program

Company name Sumitomo Electric Ind Ltd; Sumitomo Wiring System Ltd; Auto Network Gijutsu Kenkyusho Kk

Inventors Aiba Shinichi

Priority date 12 May 2022

Publication date 18 June 2025



This patent improves how vehicles detect problems in their internal networks by reducing false alarms caused by harmless errors like electromagnetic interference. Instead of just counting how many errors happen and triggering alerts when they pass a set limit. This invention tracks how the number of errors changes over time and compares that pattern to known, normal patterns from the past. A special monitoring device inside the car watches error counts, builds a timeline of these counts, and uses an anomaly detection unit to find unusual behavior by comparing it with stored data. This helps catch real problems earlier, even before the number of errors becomes too high. It also uses machine learning to better tell the difference between normal and abnormal patterns, making the car's network monitoring smarter and more accurate.



## ◀ KR102825990B1

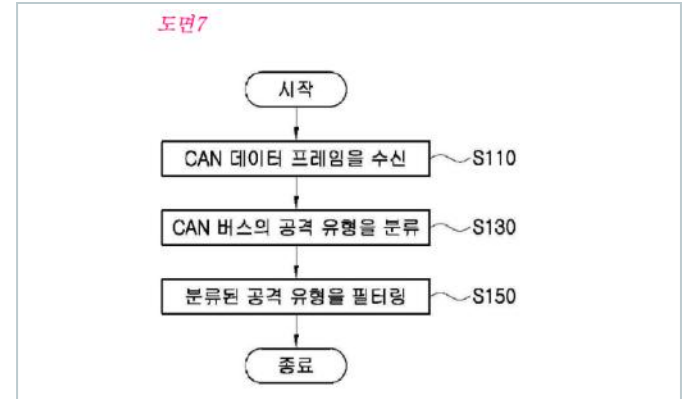
CAN communication security method for detecting CAN bus attacks, recording medium and CAN communication device for performing the same

Company name AY Innovation Co., Ltd.

Inventors Lee Sung-su,  
Lim Hyung-cheol

Priority date 16 Nov 2023

Publication date 26 Jun 2025

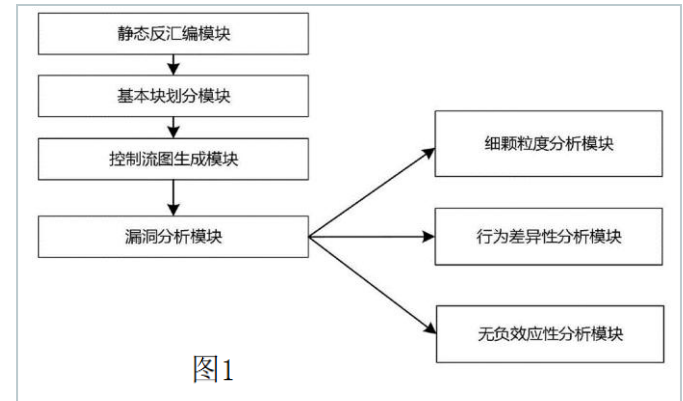


This patent describes a new method to improve security for vehicles by detecting cyberattacks on the CAN bus. Current intrusion detection systems (IDS) struggle to catch real attack patterns or require heavy computing. This invention combines IDS with a simple rule-based filter that uses real CAN message data. First, it uses a trained IDS model to label each message as normal or as a type of attack like DoS, spoofing, or fuzzy attacks. Then, it applies specific rules: for example, counting how many times certain message IDs or payloads appear. If the counts go over set limits, the system can reclassify the message as an attack, even if the IDS didn't catch it at first. It also checks if message IDs follow expected patterns. This ensures better detection of attacks that manipulate or flood CAN messages.



## ◀ CN115130113B

# Vulnerability analysis method, system and medium of automobile ECU firmware



This patent solves the problem of traditional methods for checking ECU firmware, which usually depend on known bugs or access to the source code. These older methods can miss new issues and delay detection, leading to security risks. Instead, this invention looks directly at the ECU's binary code. It breaks the code into small parts and maps how these parts connect to understand how the program flows. It then looks for unusual behavior, like too many risky data changes or code patterns that might crash the system. If these problems go beyond certain limits, the firmware is marked as vulnerable. This method doesn't need source code or knowledge of past bugs. It can find new security issues by analyzing how the binary code behaves in all possible paths, making the analysis safer and more complete.

Company name Dongfeng Motor Group Co Ltd

Inventors Li Chuang, Sun Wei,  
Shu Chang, Cai Yanbo,  
Wang Chuang

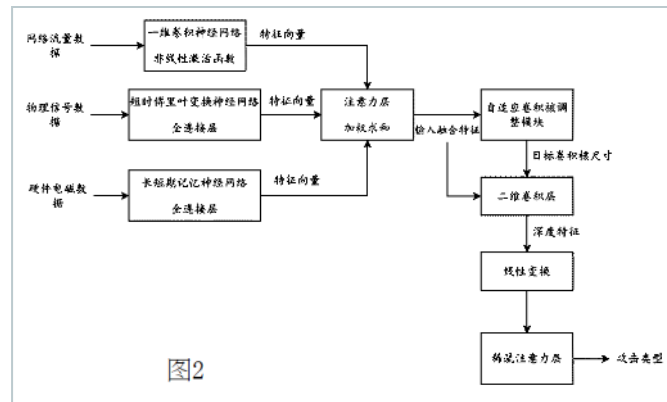
Priority date 19 Jul 2022

Publication date 27 Jun 2025



## ◀ CN120090881A

# Intrusion detection method for edge node of Internet of vehicles, electronic equipment and medium



This patent tackles the problem of weak security at the edge nodes of vehicle networks, where cyberattacks can cause fake identities, data leaks, or traffic issues. It suggests an approach that collects data from three levels: network traffic, physical signals, and low-level electromagnetic signals from the edge node. By studying all this data together, the system can better identify the type of attack and quickly come up with a defense plan. It uses smart algorithms, like hybrid neural networks, to find patterns and detect even new or complex attacks. This layered approach makes the system more accurate, better at spotting combined threats, and more reliable at protecting the vehicle's communication network.

Company name Thalys Automobile Co Ltd

Inventors Gong Wei,  
Li Yun,  
Ni Qingjie,  
Zhang Xiaoxiao

Priority date 06 May 2025

Publication date 03 Jun 2025



# We are now in India

## Your global full-service IP partner

With 60+ years of experience and over 20 offices worldwide, Dénemeyer Group is committed to being the first choice partner for the protection and management of Intellectual Property (IP) rights globally.

Our India office is your gateway to the world of IP, offering a single point of contact and full-service IP management solutions to support you throughout your IP life cycle.



IP consulting



IP law firm  
services



IP maintenance  
services



IP management  
software



Octimine patent  
analysis software



## By the numbers



Founded in  
**1962**



**180**  
jurisdictions  
covered worldwide



**~2 Million**  
patents maintained



**~1 Million**  
trademarks managed



**>60**  
years  
of experience in IP



**>20**  
global offices



**>900**  
employees and  
associates

## Global presence



Abu Dhabi, UAE



Beijing, CN



Bengaluru, IN



Brasov, RO



Chicago, USA



Dubai, UAE



Howald, LU



Johannesburg, ZA



Manila, PH



Melbourne, AU



Munich, DE



Paris, FR



Rio de Janeiro, BR



Rome, IT



Singapore, SG



Stockport, UK



Taipei, TW



Tokyo, JP



Turin, IT



Warsaw, PL



Woking, UK



Zagreb, HR



Zug, CH

## Talk to us now


Find out how we can support you  
in these services and more.

- International Patent and Trademark Renewals
- International Patent and Trademark Filings
- European Patent Validation
- PCT Nationalization
- Records
- DIAMS IP Management Software
- Patent Search & Analysis



# Visit us

at [www.dennemeyer.com](http://www.dennemeyer.com) to find out more about us.

 **Dennemeyer India Private Limited**  
Bengaluru  
[info-india@dennemeyer.com](mailto:info-india@dennemeyer.com) **North & East India**  
**+91 9818599822****South & West India**  
**+91 88266 88838**