

Special Edition – January 2025

Cybersecurity in Mobility

Recent developments

Curated and summarized - Industry and Patent news

Published by Denne Meyer India Private Limited
Parag Thakre (pthakre@denne Meyer.com)

Subscribe now



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

Special Edition

In this special edition of our monthly report, we explore the world of electric mobility with a spotlight on Mahindra's latest product launch in passenger vehicles segment — Electric SUV BE 6. As the automotive industry transitions towards electrification, this vehicle has generated considerable interest. This special edition explores the vehicle's design, technology, key features, and some key insights from its launch.

This month's report includes the following content:

- Mahindra's new EV launch: BE 6
 - Global Spotlight
 - Interesting Features
 - Product-to-Patent Mapping
- Industry news
- Patents of the month

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.

In this special edition, we will also be exploring Mahindra's new product launch – Electric SUV BE 6 and its potential impact in the industry.

Key Insights this month

- ❑ Mahindra's product pricing, combined with high-tech features, long range, and lifetime warranty of their batteries, are initiating a competitive race in the Indian market. With new products expected from various OEMs in 2025, this trend may also mark the dawn of subsidy-free electric vehicles (EVs) in India.
- ❑ The Mahindra BE 6, priced much lesser than its foreign competitors, offers advanced autonomous and safety features like auto-parking and multi-link suspension, specifically tailored for Indian roads. These features provide an enhanced driving experience at an affordable price, giving Mahindra a competitive edge in both local and international markets.
- ❑ Localization in the production of EV parts is leading to better pricing strategies, making it difficult for imported cars to compete in markets like India. Companies that localize their production, can cut costs and offer affordable vehicles. Holding multiple patents for innovations further gives these companies a competitive edge, allowing them to price their EVs competitively against global brands.
- ❑ Key collaborations and the adoption of advanced technologies are significantly enhancing the capabilities of connected cars, especially as countries prepare for the next-generation network rollout.

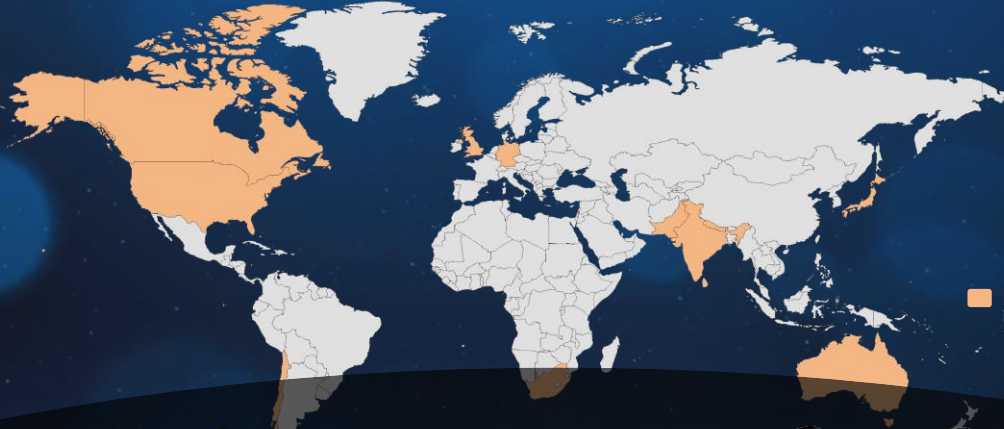
Key Insights continued on the next page ...

Key Insights this month

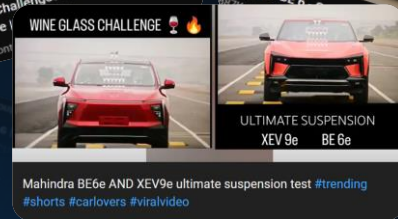
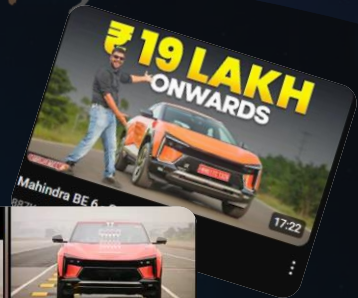
- ❑ Cybersecurity and data privacy can be crucial features for any product. This presents a significant opportunity for OEMs and suppliers to offer a unique value proposition. As consumers become more aware of the importance of protecting their personal information, companies that integrate robust cybersecurity measures and prioritize data privacy can differentiate themselves in the market.
- ❑ Recent incidents involving flaws in infotainment systems and data breaches, such as those in Skoda sedans and Volkswagen EVs, have allowed hackers to control car functions. Additionally, innovative car theft methods, like hacking cars via Vehicle Identification Number (VIN) photos, have emerged. These incidents highlight the critical importance of protecting sensitive user data and vehicle systems against evolving cybersecurity threats.
- ❑ Many companies have now started following and implementing the latest cybersecurity standards and regulations to make vehicles safer. For example, PlaxidityX has partnered with Marquardt to enhance the security of electronic control units (ECUs) in cars.
- ❑ The patents published last month focuses on securing in-vehicle networks and ECUs. For in-vehicle networks, patents talk about using software-defined networking (SDN) for intrusion prevention; and providing protection against Denial of Service (DoS) attacks with advanced tech like convolutional neural networks (CNNs). For ECUs, the patents cover maintaining the accuracy of intrusion detection systems (IDS) against fake messages and analyzing cyber attack paths during vehicle-to-everything (V2X) communication.



◀ Mahindra's new EV launch:
BE 6



Major global EV markets showing interest in Mahindra BE 6.
**Data extracted from Google trends*



The global buzz around Mahindra's BE 6 makes it an interesting product to be reviewed in our special edition report. India's emergence as a strong player in sustainable mobility highlights the country's ability to produce high-tech products at affordable prices.



BE 6 Image taken from Mahindra's design patent #IND369130-001S

Car & Cabin

- Twin-screen cockpit design with aircraft-inspired controls
- Rear spoiler design
- Wheel rim design
- Infinity roof
- Dolby Atmos integration

INGLO Platform

Powertrain

- Multi-link suspension
- Brake by wire with Integrated Electronic Booster (IEB)
- Electric power steering with Variable Gear Ratio (VGR)
- Acceleration – 0 to 100 km/h in 6.7 sec
- Max power – 282bhp, Max Torque – 380Nm

Battery

- Superfast charging: 20-80% in 20 mins (175 kW DC charger)
- 500 km+ range on a single charge with a lifetime warranty
- Advanced Lithium Iron Phosphate (LFP) battery with Cell to pack, Compact lean module, Bottom transverse cooling, and Nail penetration robustness tech

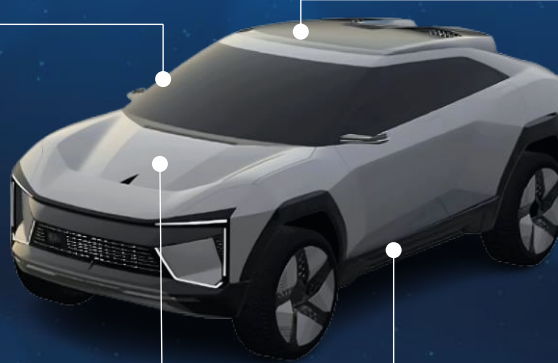
Autonomous - Mahindra Artificial Intelligence Architecture (MAIA)

- Auto park
- ADAS level 2+
- VisionX – AR Display
- Eyedentity - Driver fatigue tracker

CAR & CABIN DESIGN

- **Two spoke steering wheel** –
[IND369145-001S](#)
- **Twin screen dashboard** –
[IND369122-001S](#)
- **Rear spoiler** –
[IND370519-001S](#)
- **Wheel rim** –
[IND370513-001S](#)

**Mahindra holds numerous design patents; however, above ones are unique to BE 6 and upcoming models.*



IN-CABIN FEATURES

- **VisionX – AR display**
[KR102447826B1](#)
[KR20220094333A](#)
- **Infinity roof** –
[IN202241008660A](#)
- **EyeDentity – Fatigue tracker**
[KR20230127386A](#),
[KR20180077891A](#)

AUTONOMOUS & CYBERSECURITY FEATURES

- **Auto park** –
[IN381067A1](#),
[IN420236A1](#),
[KR102220702B1](#)
- **ADAS** -
[KR102678438B1](#),
[KR102560858B1](#),
[KR102537901B1](#)
- **Cybersecurity** –
[KR102472413B1](#),
[KR102411797B1](#),
[KR102391791B1](#)

INGLO PLATFORM - BATTERY

- **Superfast charging** –
[IN202041044102A](#),
[KR20240143319A](#),
[KR20240143316A](#)
- **Compact lean module** –
[IN202321009780A](#)
- **Bottom transverse cooling** -
[IN202321022552A](#),
[IN202321010521A](#)

INGLO PLATFORM - POWERTRAIN

- **Multi-link suspension** –
[IN202321031290A](#),
[IN202341010534A](#)
- **Braking** –
[IN202341042654A](#),
[IN202341002031A](#),
[KR102514400B1](#)
- **Electric power steering** -
[IN202024047409A](#),
[US2021129901A1](#)



◀ Industry news

Remote Cyberattack

Vulnerabilities in Skoda & Volkswagen Cars Let Hackers Remotely Track Users

Cybersecurity researchers found security weaknesses in the infotainment systems of some Skoda and Volkswagen cars, which could allow hackers to access sensitive user data remotely. PCAutomotive, a cybersecurity firm, discovered 12 security flaws in the Skoda Superb III sedan at the Black Hat Europe event. These flaws could let hackers install malware and control various car functions, such as tracking GPS locations, recording conversations, capturing screen images, playing sounds, and accessing phone contacts. Additionally, some problems in the OBD interface could even allow hackers to turn off the engine while driving, but this requires physical access. These security issues could affect over 1.4 million vehicles, including other models with similar systems.

Source

<https://cybersecuritynews.com/>



Data Breach

Volkswagen Data Breach: 800,000 Electric Car Owners' Data Leaked

Volkswagen accidentally exposed the personal information of 800,000 electric vehicle (EV) owners because of a mistake in the software of its subsidiary, Cariad. Sensitive data, including locations and contact details, was left publicly accessible on Amazon Cloud for months. This data included precise GPS information that could track the movements of vehicles and their owners. The breach was discovered by the Chaos Computer Club (CCC), a German ethical hacking group. They informed Volkswagen, allowing the company to fix the issue before it could be misused. This incident raises concerns about data privacy in the automotive industry, especially with the increase in connected vehicles.

Source

<https://cybersecuritynews.com/>



Partnership

Marquardt Selects PlaxidityX as a Trusted Partner for Vulnerability Management and Cybersecurity Compliance

PlaxidityX has teamed up with Marquardt, a leading manufacturer of mechatronics systems, to improve Marquardt's cybersecurity and market offerings. As vehicles become more software-based, they are becoming more vulnerable to threats. New cybersecurity regulations and standards, such as UNECE R155 and ISO/SAE 21434 now require continuous monitoring and response to software threats. Car manufacturers want their suppliers to ensure that their electronic control units (ECUs) are secure, but many are not happy with current monitoring tools. Marquardt aims to lead in secure software and electronics by using PlaxidityX's expertise. PlaxidityX's software helps find and manage security issues early in the development process, making it easier and cheaper to fix problems.

Source

<https://plaxidityx.com/>



Certification

LG Secures Advanced Vehicle Cybersecurity Certification

LG Electronics has become a top automotive technology supplier by earning the highest level of Cybersecurity Management Systems (CSMS) certification, Level 3, from TÜV Rheinland. This certification is required for automakers in 56 markets and involves tough evaluations, including simulated cyberattacks. LG's upgrade from Level 2 to Level 3 shows its commitment to strong cybersecurity standards. LG also follows the Automotive SPICE® framework to improve vehicle software development and has been recognized for its cybersecurity assessments. LG continues to enhance its security technologies to tackle evolving cyber threats in the automotive industry.

Source

<https://www.lgnewsroom.com/>



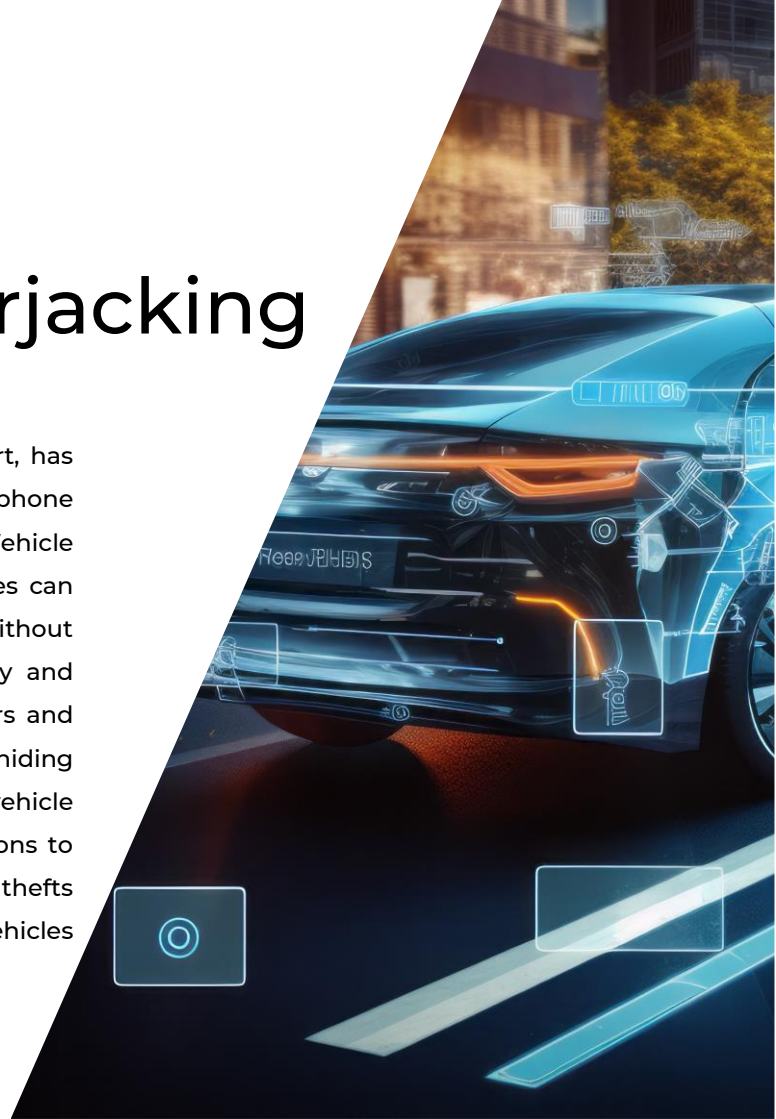
Phone Camera Carjacking

How hackers steal cars with phone camera

Sunday Aluko, a Nigerian automotive cybersecurity expert, has warned about a new global threat where hackers use phone cameras to steal cars. By taking a picture of the Vehicle Identification Number (VIN) on a car's windscreen, thieves can make duplicate keys and bypass security systems without touching the car. This allows them to steal cars quickly and quietly. Aluko emphasizes the need for car manufacturers and owners to adopt strong cybersecurity measures, such as hiding VINs, using steering wheel locks, and regularly updating vehicle software. He also calls for better encryption and regulations to improve vehicle security. The rise in VIN-based car thefts highlights the urgent need for global action to protect vehicles and secure the future of transportation.

Source

<https://www.chronicle.ng/>





PATENT

The editor's shortlist

◀ Patents of the month

Patents of the month

Published in December 2024

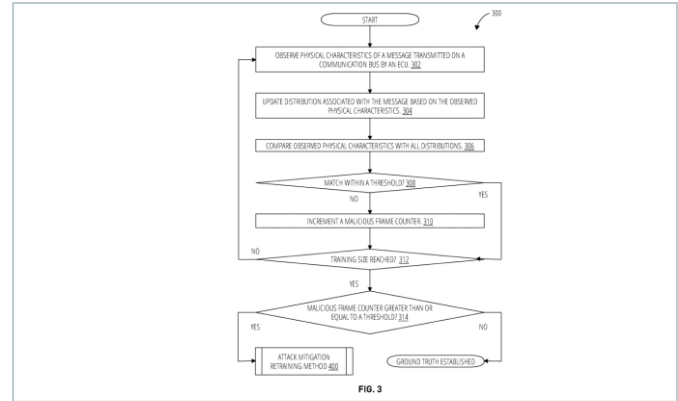


Shortlisted and summarized by our analyst

- [US12164627B2](#) - Re-training intrusion detection fingerprints in the presence of an attacker
Assignee: Intel Corp
- [US12177239B2](#) - Attack analyzer, attack analysis method and attack analysis program
Assignee: Denso Corp
- [US12184408B2](#) - Cooperative early threat detection and avoidance in C-V2X
Assignee: Qualcomm Inc
- [US12100304B2](#) - Blockchain enabled aircraft secure communications
Assignee: Gulfstream Aerospace
- [US20240406196A1](#) - Protecting vehicle buses from cyber-attacks
Assignee: Nvidia Corp
- [IN202441079959A](#) - System And Method For Detecting Intrusions In Vehicular Ad-hoc Networks (Vanets) Using Convolutional Neural Networks
Assignee: SRM Univ
- [EP4476938A1](#) - Mitigating anomalous activities introduced into an on-board vehicle network
Assignee: Robert Bosch GMBH
- [KR20240170620A](#) - CAN communication apparatus for vehicle
Assignee: Korea Automobile Research Institute
- [CN114208116B](#) - Intrusion handling system and method
Assignee: Hyundai Motor Co
- [CN118870367B](#) - Intrusion detection method and device for vehicle-mounted CAN (controller area network), vehicle and storage medium
Assignee: Hefei University Of Technology

US12164627B2

Re-training intrusion detection fingerprints in the presence of an attacker



The patent talks about improving systems that detect fake messages in vehicle networks by retraining them, especially focusing on electronic control units (ECUs). The solution is to generate and update patterns for unique message identifiers (MIDs) based on the physical characteristics of transmitted messages. Initially, balanced patterns are created from real messages. These are then compared with collected patterns to identify fake ones. When differences exceed a certain level, the system updates (retrain) to flag potential attacking ECUs. This approach ensures that detection systems remain accurate and resilient against unauthorized access or manipulation in challenging environments.

Company name	Intel Corp
Inventors	Ahmed Shabbir, Juliato Marcio, Lesi Vuk, Wang Qian, Sastry Manoj
Priority date	24-Sep-2021
Publication date	10-Dec-2024

US12177239B2

Attack analyzer, attack analysis method and attack analysis program

Company name Denso Corp

Inventors Murakami Ryosuke,
Imoto Reiichiro,
Egawa Masumi

Priority date 30-Jun-2021

Publication date 24-Dec-2024

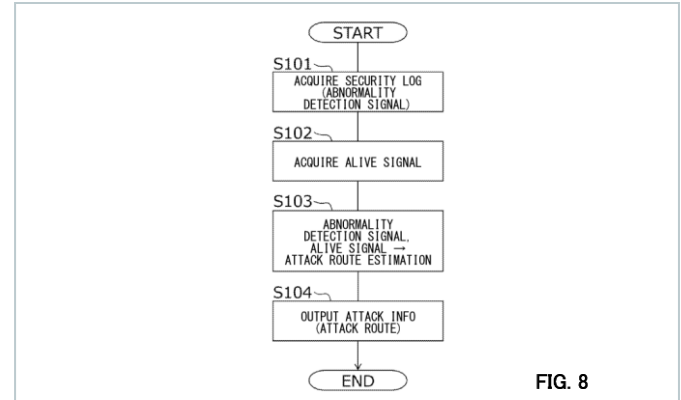


FIG. 8

The patent addresses the growing vulnerability of vehicle electronic control units (ECUs) to cyber attacks during communication with other vehicles. The solution is an attack analyzer that figures out the path of a cyber attack using data from security logs created by sensors that detect unusual activities. It collects security logs and live signals and stores them in tables that predict attack paths, estimating possible attack routes, and providing relevant attack information. The key improvements include more accurate estimation of attack paths by using both abnormal signals and sensor status, and a method for calculating the reliability of the signal. Additionally, the system can work in different setups, either on the vehicle or as external server devices.

◀ US12184408B2

Cooperative early threat detection and avoidance in C-V2X

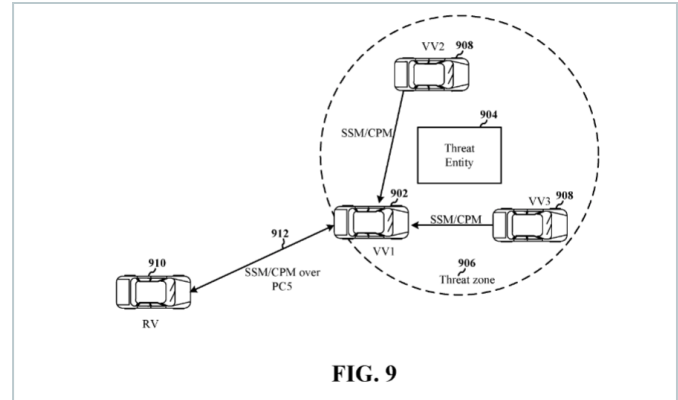


FIG. 9

The patent addresses the problem of detecting and handling threats in automated driving systems, especially those that interfere with communication between connected vehicles. These threats can come from attacks like denial of service, jamming, misbehaving vehicles, and interference. The solution is to detect and avoid these threats early. A wireless device identifies a threat based on a signal from the threat source, which disrupts the wireless spectrum or resources utilized in automated driving. When a threat is detected, one or more communication operations are stopped, and a message is sent to another device with details about the threat, like its type, location, signal strength, and other important information to help take preventive actions.

Company name Qualcomm Inc

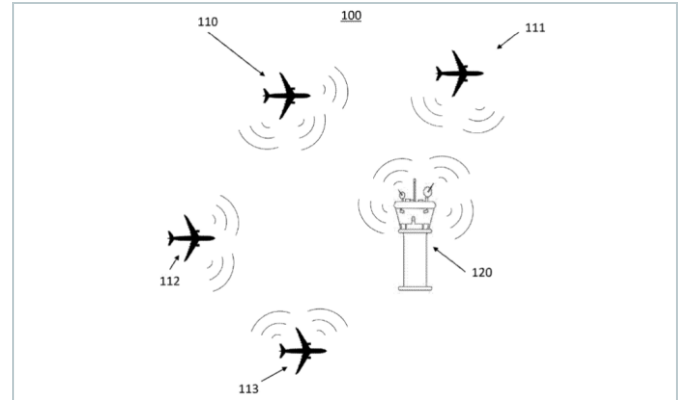
Inventors Nekoui Mohammad,
Das Soumya,
Shuman Mohammed Ataur Rahman

Priority date 21-May-2021

Publication date 31-Dec-2024

◀ US12100304B2

Blockchain enabled aircraft secure communications



The patent addresses the need for secure communication between aircraft and ground stations because current methods can be easily compromised. Accurate location information is essential for safe air traffic control, but existing systems might not always be reliable. The proposed solution is a blockchain technology for communication, which acts like a secure digital ledger that's difficult to hack. It works by creating a network where each data block contains key information such as speed, altitude, location, and environmental conditions, using special codes to ensure the data's integrity. This incoming data is verified against the stored information and confirmation is obtained from multiple sources before updating the local records and airspace maps.

Company name Gulfstream Aerospace

Inventors Winslow Matthew,
Bohanan Scott

Priority date 16-Dec-2020

Publication date 19-Dec-2024



US20240406196A1

Protecting vehicle buses from cyber-attacks

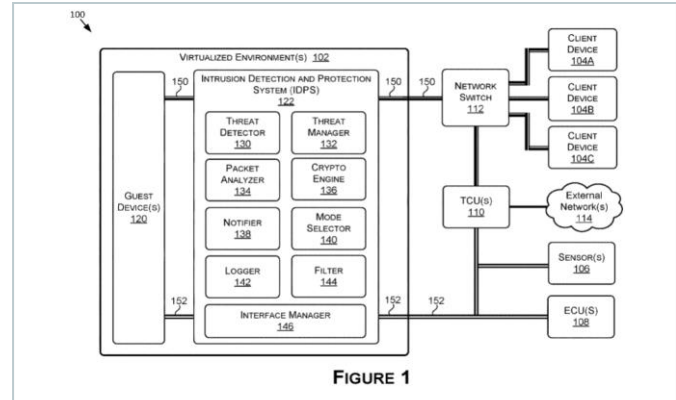


FIGURE 1

The patent addresses vulnerabilities in modern vehicle networks that expose them to cyber-attacks, where malicious parties can send unauthorized messages to interfere with critical vehicle functions. The solution is a system inside the vehicle that uses a hypervisor to create separate virtual environments for multiple operating systems (OSes). Each OS works independently in isolated environments, with security engines watching the communications between the OSes and the vehicle's external network. The security engine checks network traffic for potential threats and decides how to respond when it detects a security event. Additionally, it can corrupt harmful messages on the network before they reach other components.

Company name Nvidia Corp

Inventors Overby Mark,
Dingle Rick,
Di Miscio Nicola,
Kannan Varadharajan,
Zhang Yong,
Saracino Francesco

Priority date 08-Jun-2018

Publication date 05-Dec-2024

IN202441079959A

System And Method For Detecting Intrusions In Vehicular Ad-hoc Networks (Vanets) Using Convolutional Neural Networks

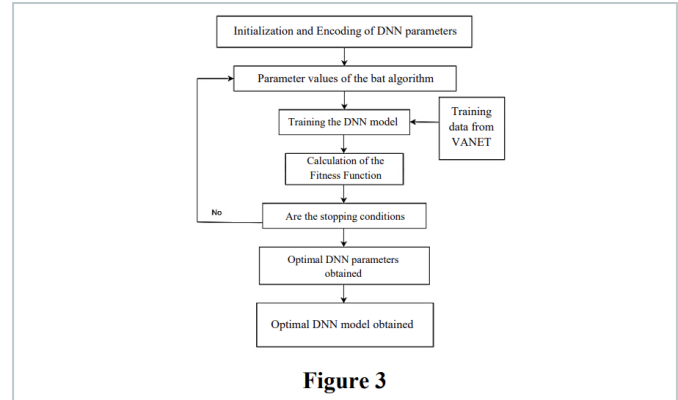


Figure 3

The patent talks about the security risks of vehicle networks that can connect to each other (VANETS). These networks can be attacked, causing problems like Denial of Service (DoS) or fake vehicle identities (Sybil attacks). Existing security systems aren't sufficient to protect them. The solution is to detect these attacks using convolutional neural networks (CNNs), which are smart computer systems that can learn and recognize patterns. The system collects and processes network traffic data, uses a CNN model to find both known and new attacks, and assigns risk scores. It sends real-time alerts, takes steps to stop attacks, and logs data for ongoing improvement.

Company name SRM Univ

Inventors Amit Kumar Singh,
Harinath Ankarbina

Priority date 21-Oct-2024

Publication date 06-Dec-2024

EP4476938A1

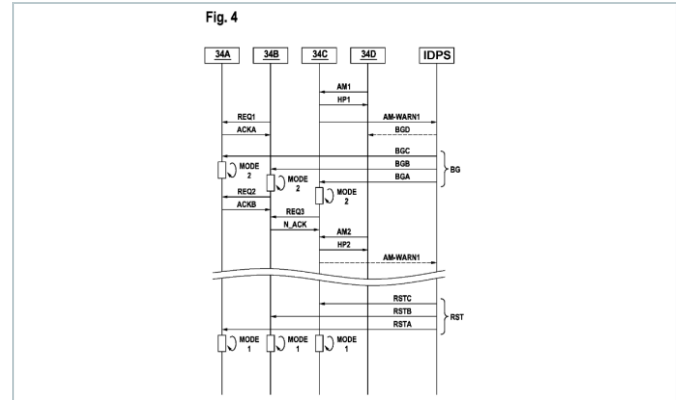
Mitigating anomalous activities introduced into an on-board vehicle network

Company name Robert Bosch GMBH

Inventors Kamphuis Fredrik,
Zimmermann Christian,
Duplys Paulius,
Gehrmann Tobias,
Munk Peter,
Huth Christopher

Priority date 09-Feb-2022

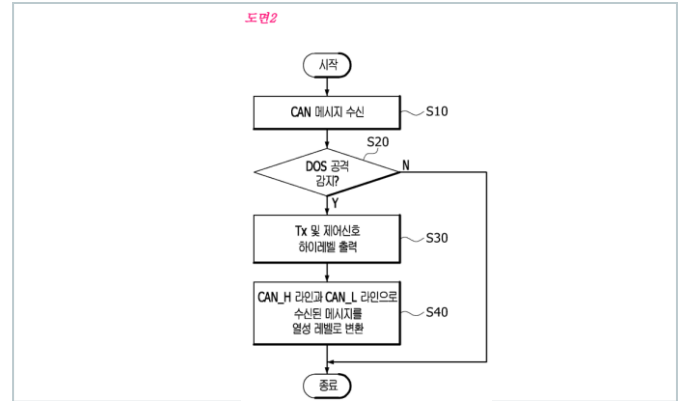
Publication date 18-Dec-2024



The patent addresses the rising threat of cyber attacks on in-vehicle networks, which are made up of various ECUs that communicate with each other. These networks can be at risk from attacks that can change or insert malicious messages, compromising vehicle safety. The solution is to detect and reduce these threats by identifying unusual messages, sending secure alerts to the affected ECUs, and switching these ECUs to a limited mode to keep important functions working while reducing risk. Key improvements include maintaining essential vehicle functions during security events, using secure keys for ECU communication, and randomizing identifiers to protect against intrusions.

◀ KR20240170620A

CAN communication apparatus for vehicle



The patent discusses how to prevent Denial of Service (DoS) attacks on Controller Area Network (CAN) systems in vehicle networks. These attacks can mess up communication by sending high-priority messages or keeping certain signals active. The solution is a communication device in the vehicle that has a unit to change signal levels and a controller. The signal level unit adjusts messages during a DoS attack to reduce its impact, while the controller watches for unusual messages and responds to them. Key improvements include keeping vehicle communication working during attacks, effectively spotting DoS attacks based on message timing and importance, and managing signals efficiently using specific types of electronic components.

Company name Korea Automobile Research Institute

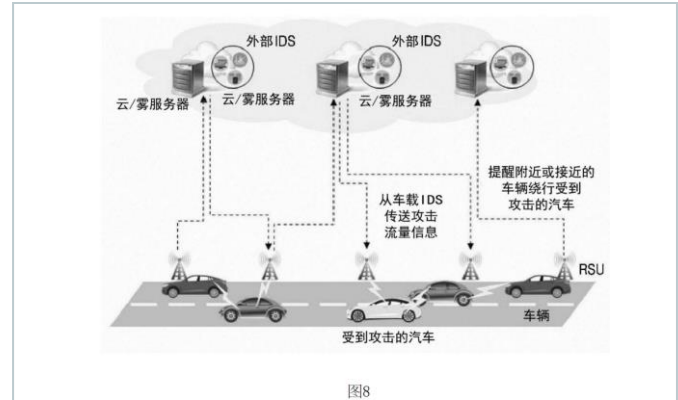
Inventors Kim Yong-eun,
Park Seong-min,
Son Young-wook,
Lee Ho-seong

Priority date 24-May-2023

Publication date 04-Dec-2024

◀ **CN114208116B**

Intrusion handling system and method



The patent addresses the problem of in-vehicle networks being vulnerable to attacks, with the increase in communication between connected cars. Current systems for detecting intrusions struggle due to the limited computing power in vehicles. The proposed solution is to make an intrusion prevention system using a technology called software-defined networking (SDN), which allows network management through software rather than hardware. This solution involves an SDN-enabled switch in the vehicle network and a remote SDN controller. The controller gathers data from the switch, sends it to a detection system for analysis, and updates the network based on detected threats. This method allows for high-performance detection using techniques like AI without being limited by the vehicle's resources.

Company name Hyundai Motor Co

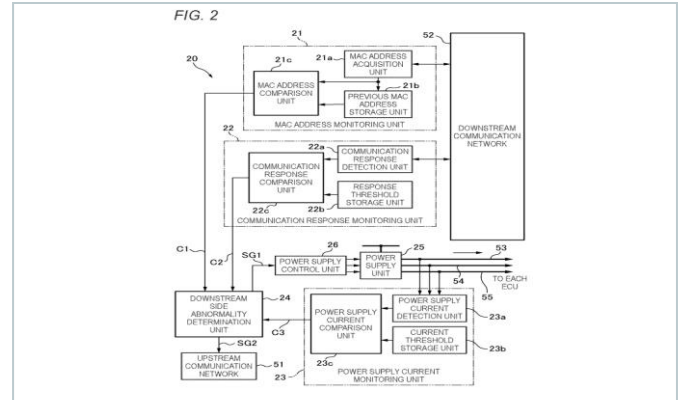
Inventors Jin Huigang,
Zheng Chengxun,
Pu Shengyu,
Lin Heping

Priority date 31-Jul-2019

Publication date 03-Dec-2024

◀ **CN118870367B**

Intrusion detection method and device for vehicle-mounted CAN (controller area network), vehicle and storage medium



The patent addresses the security vulnerabilities in vehicle-mounted Controller Area Network (CAN) systems that pose risks to vehicle safety and passenger privacy. The solution is to detect intrusions in CAN systems. It involves collecting data frames from the CAN bus, extracting key details like timestamps, CAN IDs, and data field features, and compiling them into a complete data image. Additionally, it creates various such data images using a technique and feeds them into a trained model that can detect intrusions in real-time.

Company name Hefei University Of Technology

Inventors Wang Chuansu,
Shi Qin,
Cheng Teng,
Liu Junyu

Priority date 24-Sep-2024

Publication date 24-Dec-2024

We are now in India

Your global full-service IP partner

With **60+ years of experience** and **23 offices worldwide**, **Denemeyer 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
- Recordals
- DIAMS IP Management Software



Visit us

at www.dennemeyer.com to find out more about us.

 Denne Meyer India Private Limited
Bengaluru
info-india@dennemeyer.com

 North & East India
+91 79831 15166

South & West India
91 88266 88838

DISCLAIMER: This report, including external links, is generated using databases and information sources believed to be reliable. While effort has been made to employ optimal resources for research and analysis, Denne Meyer expressly disclaims all warranties regarding the accuracy, completeness, or adequacy of the information provided. We do not control or endorse the content of external sites and are not responsible for their accuracy or legality. The information provided in this report should not be construed as legal advice, and users are strongly advised to consult with qualified legal professionals for specific legal guidance.