Dennemeyer
The IP Group

Special Edition – October 2025

Cybersecurity in Mobility

Recent developments

Curated and summarized - Industry and Patent news

Published by Dennemeyer India Private Limited
Parag Thakre (pthakre@dennemeyer.com)
Prachi Gupta (pgupta@dennemeyer.com)
Himanshu Varun (hvarun@dennemeyer.com)

Dennemeyer
The IP Group

Subscribe now

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

Dennemeyer
The IP Group

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 be exploring the recent cyberattack on Jaguar Land Rover (JLR), tracing its timeline, key threat actors, and organizational impact.

Dennemeyer
The IP Group

Special Edition

In this special edition of our monthly report, we take a deep dive into the recent cyberattack on Jaguar Land Rover (JLR), a major wake-up call for the automotive industry. The attack on JLR's IT and operational technology (OT) systems led to weeks of halted manufacturing, supply chain disruptions, and significant financial losses.

This month's report includes the following content:

**JLR is a wholly owned subsidiary of Tata Motors*

Dennemeyer
The IP Group

Key Insights this month

- Cyberattacks are no longer isolated incidents; they are part of an organized ecosystem where low-tier hackers steal and sell credentials that advanced groups later weaponize. As underground data markets evolve, this tiered ecosystem will expand, pushing automakers to tighten credential security, boost threat intelligence, and monitor the dark web.

- Data from minor leaks or malware infections can be used years later by hackers to exploit vulnerable targets and fuel delayed breaches, especially as advanced hacking tools become increasingly affordable and more common. Automakers must treat every alert as a potential indicator of a major attack and enforce continuous monitoring, credential rotation, forensic log reviews, and strong multi-factor authentication (MFA) as standard practice.

- As digital integration deepens across factories, OEM's, suppliers, and vehicle ecosystems, a single breach can trigger a full operational shutdown to contain lateral spread. This shutdown is typically company's final response when all other measures fail. Therefore, OEM's need to implement network segmentation, automated isolation frameworks, and rapid recovery strategies to prevent large-scale production halts and major financial losses.

- Accessing work tools outside secure networks on personal devices opens easy paths for attackers to bypass corporate defenses. As connected vehicle platforms grow, these gaps will be prime targets. To counter this, Zero Trust access, strict device compliance, and keeping sensitive apps in secure environments are essential.

- The absence of early threat detection allowed a minor breach to evolve into a multi-actor attack. Implementing an intrusion detection system (IDS) will enable timely identification and containment of threats, reducing the risk of such breaches in the future not only for JLR but for the whole automotive industry.

Dennemeyer
The IP Group

Key Insights this month

- A shift toward unified cybersecurity compliance services is reflected in the alliance between Fescaro and TUV Nord. As global regulations converge under UN R155 regulation, OEMs will increasingly favor suppliers offering turnkey solutions that reduce certification complexity and accelerate time-to-market.

- The MoU between C3iHub and ARAI signals a national-level push to position academic research at the core of next-generation automotive cybersecurity innovation. OEMs should engage in such collaborations to co-develop solutions and cultivate cybersecurity talent, positioning India as a future-ready mobility security hub.

- By aligning with the SAE J3101 standard and the SESIP method, Stellantis is driving secure SDV adoption, enabling component reuse across platforms and reducing certification costs. However, this standardization introduces systemic vulnerability risks that could impact multiple OEMs. To remain resilient at scale, automakers must pair standard adoption with rigorous supplier security checks.

- Many inventions that were published last month had major themes as below:

  - Connected vehicle systems are increasingly adopting federated learning, AI-driven, multi-layered threat detection. By combining edge device monitoring and advanced anomaly analysis, these solutions enable real-time identification and targeted mitigation of complex cyberattacks.

  - Automotive and charging ecosystems are adopting adaptive, context-aware protection that merges continuous signal monitoring with intelligent, situation-based responses. This enables gradual safety interventions and seamless communication with security centers, ensuring resilient and coordinated defense against evolving cyber threats.

Inside the JLR Cyberattack

Dennemeyer
The IP Group

JLR Cyberattack: Timeline and Threat Actors

Chronology of the JLR Cyber Attack

2021

Low-cost malware (Infostealer) stole random credentials, including one from a third party with JLR's JIRA access, which were later sold on the dark web.

Possible Cause:
Lack of two-factor authentication (2FA)

March 2025

Possible Cause:
Lack of regular password rotation

A Coordinated Hack by Hellcat and APTS

HELLCAT used stolen JIRA creds → leaked 700 docs (source code, employee data).

APTS worsened breach → exposed 350 GB sensitive data using old 2021 credentials.

August 2025

Hacker groups* leaked screenshots of internal documents & backend code, showing access to vehicle systems & cloud infra beyond JIRA. As a response, JLR shut down operations.

Possible Cause:
Delayed intrusion detection and follow-up actions after early breach warnings

A $10 hacking tool (Infostealer) evolved into a multi-actor attack causing billions in losses, proving that even low-sophistication threats can trigger widespread operational collapse.

Sources: Link1, Link2, Link3, Link4, Link5

*Hacker groups: Scattered Lapsus$, Scattered Spider, and ShinyHunters

Disclaimer: Based on publicly available information

Dennemeyer
The IP Group

Impacts of the JLR Cyberattack

Exceeds JLR's entire FY24-25 (Apr'24 to Mar'25) profit of £1.8B**

Source: Link1

Key Impact Area

- **Timing:** Cyberattack occurred days before *Tata Motor's demerger record date.
- **Layoffs:**
  - Genex UK, a JLR component supplier laid off 18 staff;
  - Alps Electric, an electronic component supplier for JLR temporary laid off 210+ staff after the production halt.
- **Production Halt:** Attack crippled IT and OT systems, stopping operations for >4 weeks and halting production of around 1,000 vehicles per day.
- **Revenue Dependency:** JLR contributes ~70% of Tata Motors' consolidated revenue; Q2 FY25-26 (July to September 2025) revenue projected to drop ~22%.
- **Sales Drop:** Wholesales in Q2 FY25-26 (July to September 2025) were down 24.2% vs. Q2 FY24-25 (July to September 2024) .
- **Stock Crash:** Tata Motors' stock fell by ~4% post cyberattack.
- **Cyber Insurance Gap:** Lack of cyber insurance leads to JLR bearing the full cost of an attack.
- **Data Theft & IP Exposure:** JLR confirmed sensitive internal data was stolen, including proprietary code and system logic, raising risks of IP theft.
- **Government Bailout:** €1.5B loan for stabilizing operations.

Sources: Link2, Link3, Link4, Link5, Link6, Link7, Link8

*JLR is a wholly owned subsidiary of Tata Motors

**JLR's fiscal year (FY) runs from 1 April to 31 March

Dennemeyer
The IP Group

‹Industry news

Dennemeyer
The IP Group

Industry News

Partnership

Fescaro, TUV Nord join forces on auto cybersecurity compliance

Fescaro, a provider of cybersecurity solutions for vehicles, has signed an agreement with TUV Nord to collaborate on automotive cybersecurity compliance. Together, they plan to offer a one-stop solution that helps automakers and suppliers meet strict security regulations through consulting, training, security solutions, and regulatory approval. As cars increasingly rely on software, governments worldwide are tightening cybersecurity laws. The EU, China, India, and South Korea have all aligned their regulations with the UN's vehicle cybersecurity standards.

Source
https://www.fescaro.com/

Dennemeyer
The IP Group

Industry News

Cyber Alliance

C3ihub, IIT kanpur, and automotive research association of india (ARAI) join hands to strengthen automotive security

C3iHub, a cybersecurity innovation hub at IIT Kanpur, has signed an MoU with the ARAI to strengthen research and innovation in automotive security. The collaboration aims to develop new technologies, conduct joint research, and tackle emerging threats in vehicle cybersecurity. With connected and autonomous vehicles becoming common, securing mobility systems is now a global priority. Through this partnership, the two institutions will focus on creating practical solutions to improve the safety of future transportation. Both organizations see this as a step toward ensuring safe and future-ready vehicles for India and the world.

Source
https://www.iitk.ac.in/

Dennemeyer
The IP Group

Industry News

Securing EV Ecosystem

Sasken Partners with VicOne to Deliver End-to-End Automotive Cybersecurity Solutions

Sasken Technologies, a provider of engineering R&D and digital transformation services for the automotive, semiconductor, and industrial sectors has partnered with VicOne to enhance cybersecurity in vehicles and EV charging systems for OEMs and Tier-1 suppliers. VicOne offers solutions such as xCarbon, an intrusion detection and prevention system; xNexus, a security operations center for fleets; and EV charging protection. These tools are specifically designed for vehicles and charging stations, providing companies with greater visibility into threats and enabling faster response times. By combining their expertise, this partnership aims to secure ECUs, operating systems, and cloud platforms across vehicles, while also strengthening the resilience of EV charging infrastructure.

Source
https://vicone.com/

Dennemeyer
The IP Group

Industry News

Digital Key Solutions

AUTOCRYPT and Valtech Mobility Showcase Digital Key solution at IAA Mobility 2025 in Munich

AUTOCRYPT and Valtech Mobility have teamed up to create a secure and flexible digital key system for carmakers and drivers worldwide. They announced the partnership at IAA Mobility 2025, where they showed how their solution lets drivers use a smartphone to lock, unlock, and start their cars using Ultra-Wideband technology. Valtech Mobility handles the car apps and backend systems, while AUTOCRYPT takes care of security, including authentication and key management. The system runs on the cloud, protects against cyber threats, and connects safely with carmaker servers. It follows global standards and can be scaled for different car brands and fleets.

Source
https://autocrypt.io/

Dennemeyer
The IP Group

Industry News

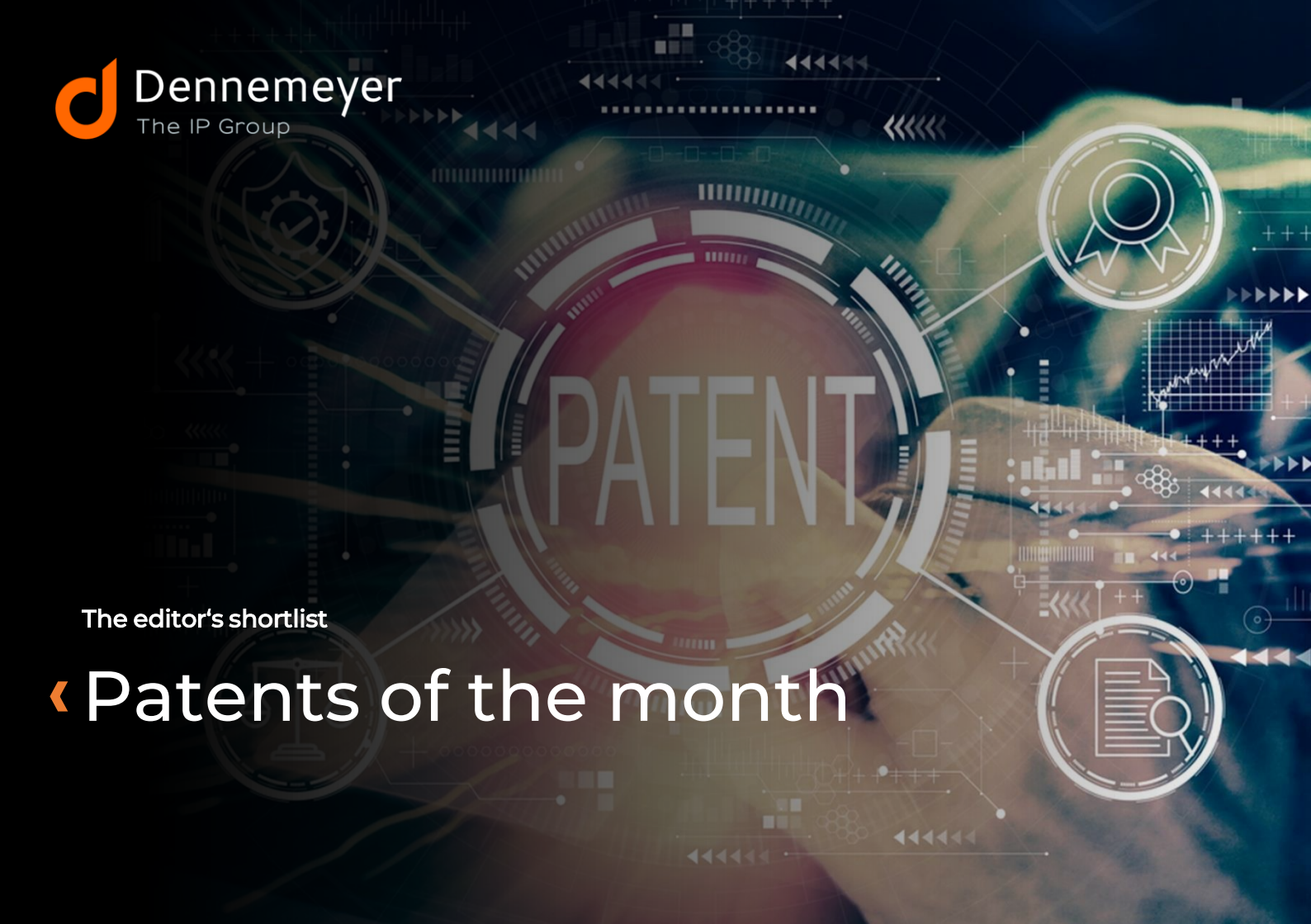
Task Force for Vehicle Cybersecurity

Stellantis Joins GlobalPlatform to Advance Global Automotive Cybersecurity Standards

Stellantis, the company behind Jeep, Fiat, and Alfa Romeo, has joined GlobalPlatform to help strengthen cybersecurity standards for modern vehicles. It will co-lead GlobalPlatform's Automotive Task Force group, which brings together carmakers, and security experts. The group recently aligned its work with the SAE J3101 standard, making it easier for suppliers to meet security requirements and giving automakers greater confidence in the components they use. Their new protection profile, based on the Security Evaluation Standard for IoT Platforms (SESIP) method, allows certified parts to be reused across different platforms, helping save time and reduce costs. This partnership reflects their commitment towards secure, standardized vehicle technology.

Source
https://www.mobis.com/

Dennemeyer
The IP Group



The editor's shortlist

Patents of the month

Dennemeyer
The IP Group

Patents of the month

Published in September 2025

Shortlisted and summarized by our analyst

- US2025301328A1 - Distributed anomaly detection and localization for cyber-physical systems
  Assignee: General Electric Co
- US2025301014A1 - Systems, methods, and apparatus for cyberattack mitigation and protection for extreme fast charging infrastructure
  Assignee: Battelle Energy Alliance LLC
- US2025296712A1 - Apparatus and method for detecting attack on gyro sensor of unmanned vehicle
  Assignee: Electronics & Telecommunications Research Institute (ETRI)
- EP4621443A1 - Trusted PNT solution by CRPA assisted GNSS spoofing protection
  Assignee: Rockwell Collins Deutschland GMBH
- JP2025132262A - Vehicle control device and vehicle control method
  Assignee: Panasonic Automotive System Co Ltd
- DE112023004773T5 - Attack analysis device
  Assignee: Astemo Ltd
- DE102025110497A1 - Systems and methods for managing data relay attacks
  Assignee: Ford Global Technology LLC
- FR3160496A1 - Communication method, in the event of detection of an attack on a motor vehicle, associated device and vehicle.
  Assignee: FCA US LLC, Stellantis Auto SAS
- CN120710769A - Attack detection method, device, equipment and storage medium
  Assignee: Guangzhou Tongda Auto Electric Co Ltd
- CN119135418B - Lightweight VANET black hole attack and gray hole attack detection method
  Assignee: Univ Hainan

Dennemeyer
The IP Group

Latest patents

US2025301328A1

Distributed anomaly detection and localization for cyber-physical systems

Company name	General Electric Co
Inventors	Abbaszadeh Masoud, Nielsen Matthew, Bush Stephen F
Priority date	23-May-2022
Publication date	25-Sep-2025

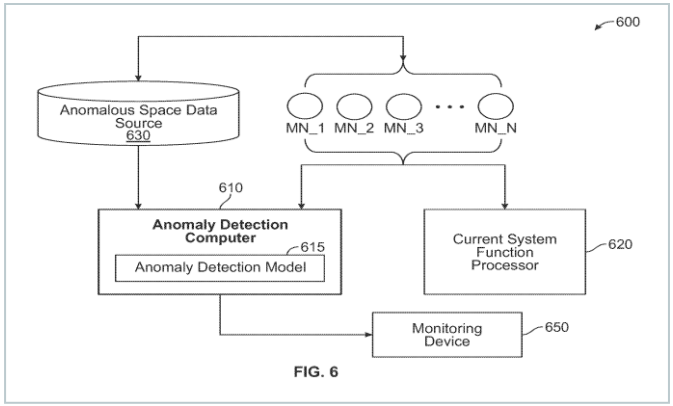


FIG. 6

This patent tackles the problem of cyberattacks on industrial control systems that are now more exposed due to widespread networking through 5G and IoT. It improves on traditional, centralized cybersecurity methods that are slow and ineffective against complex, large-scale threats. The solution involves multiple edge devices, each equipped with a virtual agent that use machine learning to spot abnormal behavior based on past normal data and simulated attacks. These agents work together and update their models through federated learning, which means they learn together without sharing sensitive raw data. The system uses secure communication and time-series analysis to detect cyber threats quickly and locally while still supporting global coordination.

Dennemeyer
The IP Group

Latest patents

US2025301014A1

Systems, methods, and apparatus for cyberattack mitigation and protection for extreme fast charging infrastructure

Company name	Battelle Energy Alliance LLC
Inventors	Rohde Kenneth W, Carlson Richard W, Salinas Sean C, Crepeau Matthew J
Priority date	10-May-2022
Publication date	25-Sep-2025

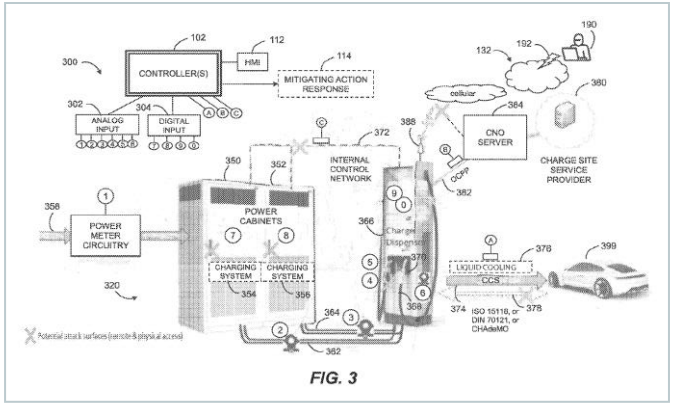


FIG. 3

This patent addresses cybersecurity risks at extreme fast charging (XFC) stations, which are vulnerable to attacks that can bypass safety systems and endanger users, equipment, and the power grid. The solution is a system for EV chargers that includes controllers, sensors, and communication monitors. It continuously checks factors such as power levels, temperatures, and component positions, along with communication signals within the system and from external sources like EVs. If abnormal behavior is detected, the system takes intelligent actions, including safely reducing power, blocking harmful messages, tricking sensors to trigger built-in protections, or remotely restarting the charger to prevent harm. This enables gradual, adaptive safety responses instead of complete shutdowns, thereby enhancing charger security.

Summarized by Dennemeyer

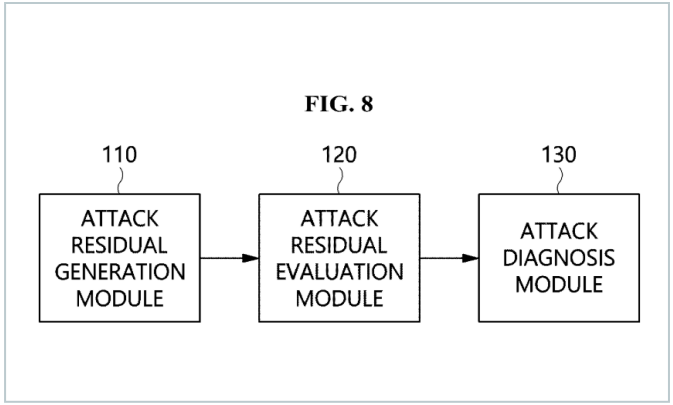
Dennemeyer
The IP Group

Latest patents

US2025296712A1

Apparatus and method for detecting attack on gyro sensor of unmanned vehicle

Company name	Electronics & Telecommunications Research Institute (ETRI)
Inventors	Hong Sung Kyung, Park Il Hwan, Lee Sang Wook, Lee Seok Tae, Jeong Han Sol
Priority date	19-Mar-2024
Publication date	25-Sep-2025



The patent focuses on protecting unmanned vehicles like drones from attacks that disrupt gyro sensors, which are essential for stable flight. Such attacks exploit the sensors' frequencies, causing false readings and risking crashes. The invention introduces a software-based detection that uses a mathematical model to monitor the drone's rolling, pitching, and yawing motions. By fusing sensor data, it generates residuals that highlight unusual behavior possibly caused by an attack. These residuals are analyzed using a filtering and evaluation process that compares them to set thresholds to confirm if an attack has occurred. Unlike costly hardware solutions, this approach works effectively in real-world flight conditions, reducing false alarms while accurately detecting ongoing acoustic attacks on gyro sensors.

Dennemeyer
The IP Group

Latest patents

EP4621443A1

Trusted PNT solution by CRPA assisted GNSS spoofing protection

Company name	Rockwell Collins Deutschland GMBH
Inventors	Ehinger Markus
Priority date	22-Mar-2024
Publication date	24-Sep-2025

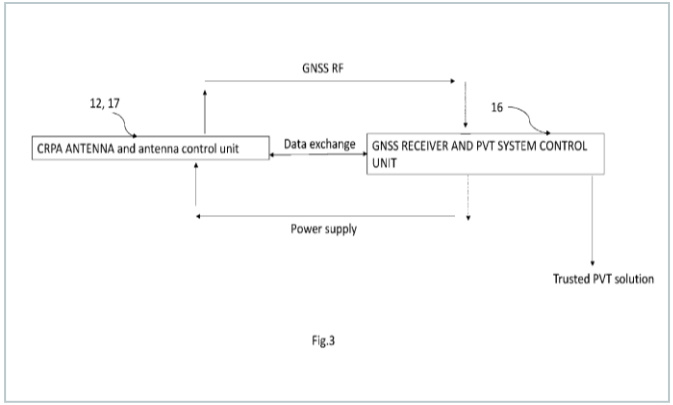


Fig.3

The patent talks about spoofing of signals sent to GPS receivers, particularly in vehicles that use advanced antennas called CRPAs. These antennas are typically designed to block jamming but not spoofing. The invention proposes that the antenna perform two separate scans of the same satellites and compare the signal strengths from both scans to detect anomalous differences that could indicate spoofing. It also uses data from motion sensors and satellite positions to figure out the vehicle's direction and aim the antenna at the satellites more accurately. By checking the timing of the signals from both scans, it can catch small delays used in replay attacks. The system also looks for missing or changed satellite signals to confirm if spoofing is happening.

Dennemeyer
The IP Group

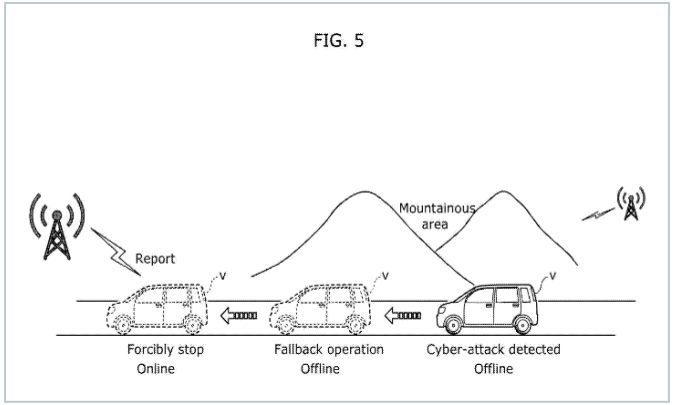
Latest patents

JP2025132262A

Vehicle control device and vehicle control method

Company name	Panasonic Automotive System Co Ltd
Inventors	Fukumoto Satoshi
Priority date	29-Feb-2024
Publication date	10-Sep-2025

Summarized by Dennemeyer



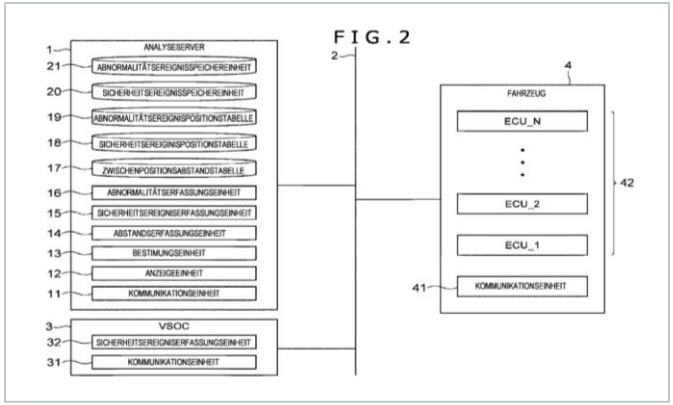
The patent tackles the challenge of protecting vehicles from cyberattacks when communication with external systems like a security center is unavailable. Traditional systems often stop the vehicle abruptly or follow preset instructions, which can be unsafe. This invention introduces a vehicle control device that first detects a cyber-attack and then checks whether the vehicle is online or offline. If online, it can safely stop the vehicle and connect with external servers for real-time security updates. If offline, it switches to a fallback mode that allows the vehicle to continue moving safely at reduced speed until the connection is restored. The system can also alert nearby people or vehicles about the attack using lights or wireless signals. Overall, it enables smarter, situation-based vehicle responses to cyber-attacks, improving safety and coordination.

Dennemeyer
The IP Group

Latest patents

DE112023004773T5

Attack analysis device



Company name	Astemo Ltd
Inventors	Ideguchi Kota, Sasa Shinya, Yamaguchi Takashi
Priority date	22-Mar-2023
Publication date	18-Sep-2025

Summarized by Dennemeyer

The patent solves the problem of telling whether something that is going wrong in a vehicle is caused by a cyberattack or just a regular malfunction. This is something current systems often can't do well. It introduces a special analysis tool that checks where unusual activity and security-related events happen in the vehicle and measures how close they are, either physically or in the software system. It uses a weighted graph to show how secure different parts of the system are, helping it judge more accurately whether the issue is likely an attack. This method helps detect real threats faster and reduces false alarms. If the unusual behavior and security event are closely linked, the system launches a deeper check, such as analyzing communication protocols. This makes threat detection more accurate and efficient.

Dennemeyer
The IP Group

Latest patents

DE102025110497A1

Systems and methods for managing data relay attacks

Company name	Ford Global Technology LLC
Inventors	Bandi Krishna, Datta Gupta Somak, Linkowski Gregory P, Menon Meghna, Santillo Mario Anthony
Priority date	21-Mar-2024
Publication date	25-Sep-2025

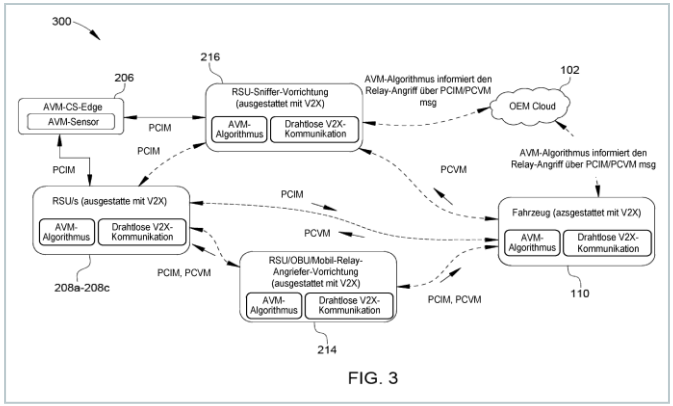


FIG. 3

This patent addresses the issue of replay attacks in vehicle networks, where attackers intercept and resend valid messages between vehicles and roadside units (RSU), leading to unauthorized actions or delays. The solution involves an infrastructure controller that has one RSU send messages and checks whether another nearby unit receives matching ones within a set time. If not, it flags potential attacks. The system also uses vehicle-side algorithms, reviews message histories, and assesses network traffic patterns to detect suspicious behavior. Signal strength and randomized data rates across RSUs help pinpoint attackers more accurately. Once an attack is detected, the system can trigger responses such as stopping vehicles in certain zones and sending alerts to central systems.

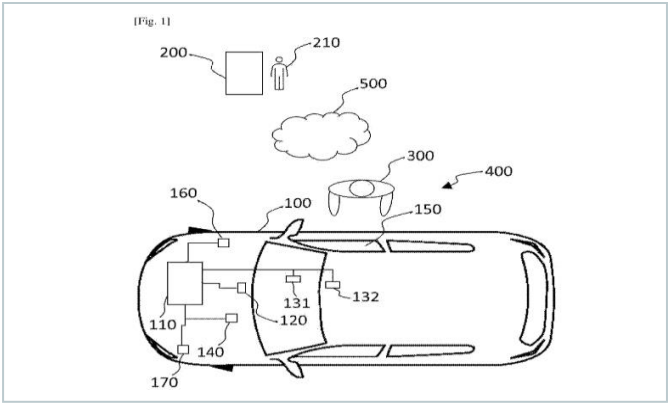
Dennemeyer
The IP Group

Latest patents

FR3160496A1

Communication method, in the event of detection of an attack on a motor vehicle, associated device and vehicle.

Company name	FCA US LLC, Stellantis Auto SAS
Inventors	Royer Guillaume, Boudan Julien, Peron Rodolphe
Priority date	20-Mar-2024
Publication date	26-Sep-2025



The patent focuses on improving how a vehicle detects and responds to cyber or physical attacks by ensuring quick and accurate communication with a security center. The solution is to use one sensor to detect an attack, and another one to gathers detailed security-related data. Once an attack is detected, the vehicle automatically starts a voice call with a human operator at the security center. During the call, the system can understand the operator's spoken questions and reply with relevant information using voice responses based on previously collected data. This removes the need for manual input during emergencies.

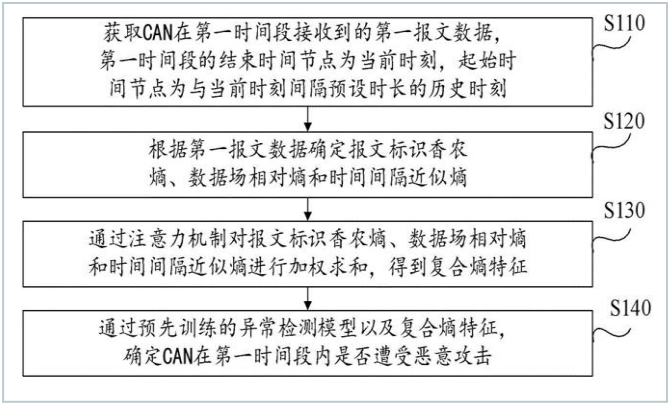
Summarized by Dennemeyer

Dennemeyer
The IP Group

Latest patents

CN120710769A

Attack detection method, device, equipment and storage medium



Company name	Guangzhou Tongda Auto Electric Co Ltd
Inventors	Zhang Jian, Shi Xiudong, Zhuang Guifen, Gao Zhigang, Lao Zhongjian, Hu Shaolin, Chen Jie, Lin Jiesong
Priority date	16-Jul-2025
Publication date	26-Sep-2025

The patent is about detecting cyberattacks on a vehicle's CAN bus system. This invention introduces an advanced way of analyzing CAN messages by performing three types of calculations: one for message ID randomness, one for how the data bytes differ from normal patterns, and one for timing irregularities. These are then combined using a system that decides which one matters most at any moment. A lightweight model, trained on both normal and attack data, then watches for signs of danger over time. The system also adjusts how much data it looks at based on how busy the network is, uses AI to simulate rare attacks, and compresses the model so it can run on car hardware. This helps it catch many types of attacks in real time without using too many resources.

Dennemeyer
The IP Group

Latest patents

CN119135418B

Lightweight VANET black hole attack and gray hole attack detection method

Company name	Univ Hainan
Inventors	Guo Zhen, Liu Dezhi, Ye Lvzhou
Priority date	20-Sep-2024
Publication date	26-Sep-2025

Summarized by Dennemeyer

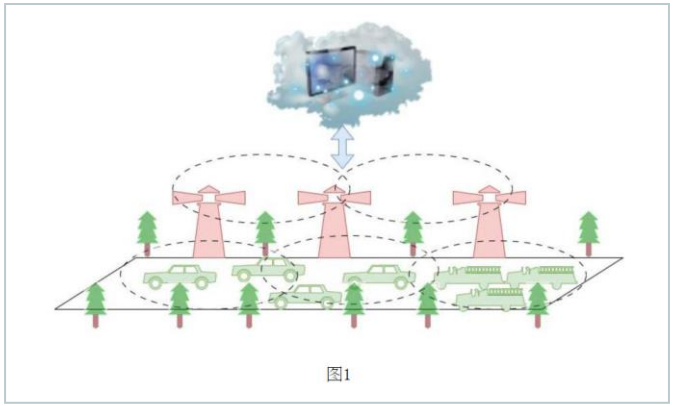
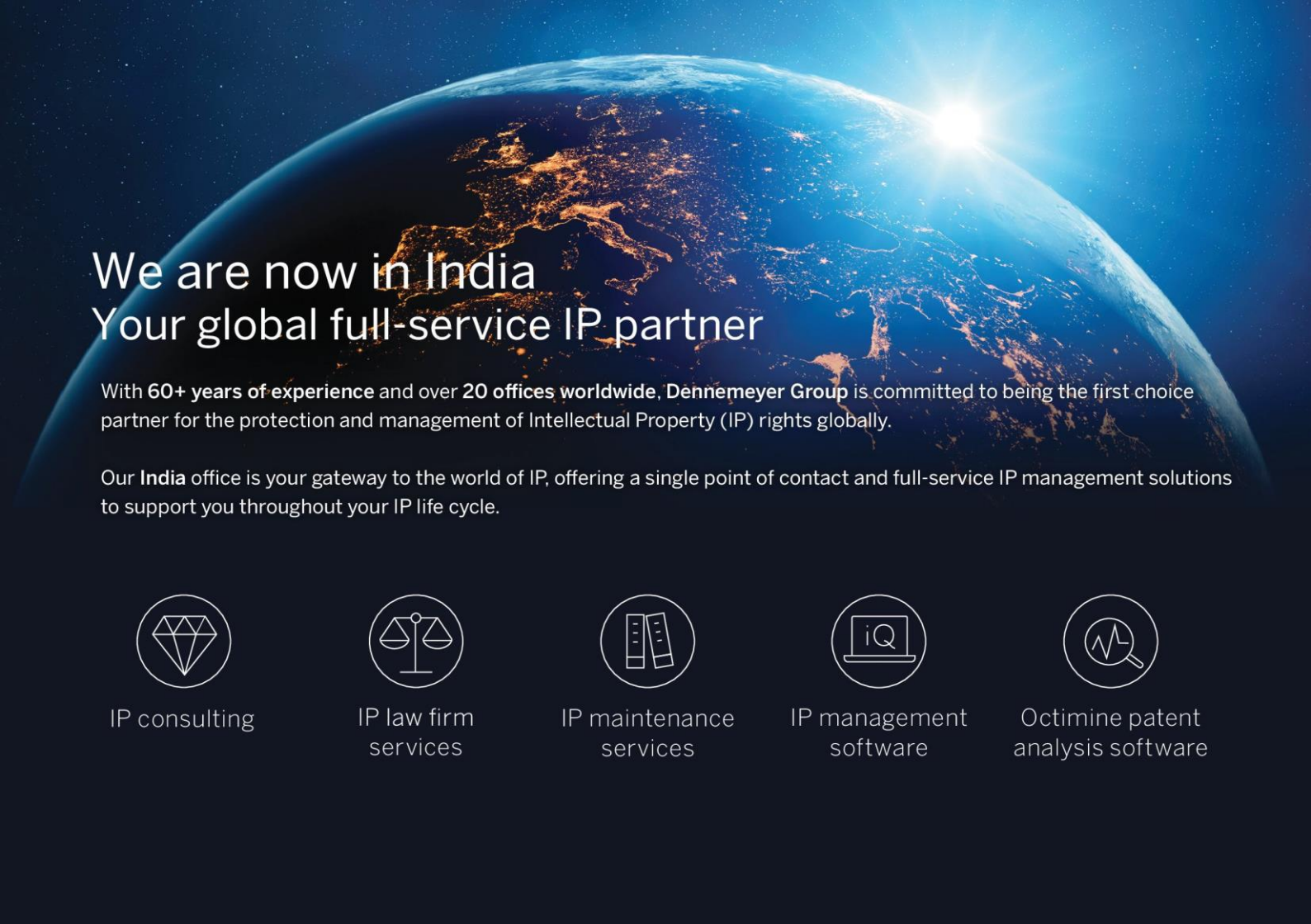


图1

This patent describes a smart way to detect cyberattacks called black hole and gray hole attacks in car networks, where some cars drop data on purpose to disrupt communication. The solution uses roadside units (RSUs) instead of cars to monitor the network. These RSUs look at certain message patterns and check if a car is acting suspiciously by comparing its behavior to a safe limit. If a car seems suspicious, it gets flagged, and others are warned to block it. For complex attacks, where cars behave normally at first but then drop messages, the system sends data through several paths and quickly switches if one path fails. It also keeps track of when data fails to send and uses this information to detect attacks. By using AI and shared monitoring, this method helps keep the network safe while remaining efficient.



We are now in India
Your global full-service IP partner

With **60+ years of experience** and over **20 offices worldwide**, **Dennemeyer 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
- Patent Search & Analysis

Dennemeyer
The IP Group

Visit us

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

Dennemeyer India Private Limited
Bengaluru
info-india@dennemeyer.com

North & East India
+91 9818599822

South & West India
+91 88266 88838