Dennemeyer
The IP Group

Report of August 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.

Dennemeyer
The IP Group

Key Insights

- Cybersecurity agency CISA, has uncovered flaws in vehicle and train systems, ranging from insecure brake control protocols to exposed user data. Early detection of such flaws helps prevent major disruptions, highlighting the importance of proactive security testing, stronger cryptographic protocols and routine security patches.

- A recent attack on the Bluetooth stack left millions of vehicles including Mercedes-Benz, Volkswagen, and Skoda exposed to unauthorized remote access and data theft. Although patches were released promptly, supply-chain delays left many cars unprotected. This gap between patch availability and deployment exposes a systemic risk, as future attacks may exploit both technical flaws and operational bottlenecks.

- Strategic partnership between ETAS India & ARAI signal an industry-wide push to upskill India's mobility workforce through certified trainings and hands-on workshops. These initiatives aim to strengthen cybersecurity readiness, build domain expertise, and ensure compliance with evolving automotive standards and regulations.

- Bentley Motors, with MHP Consulting, has achieved UNECE WP.29 compliance for its GT range. This sets a higher bar for automotive cybersecurity, strengthens Bentley's compliance leadership, and boosts global customer trust.

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

  - Connected vehicles are adopting dynamic honeypot strategies, where decoys are intelligently placed across fleets and activated only during real attacks. Combined with automated attack analysis and Security Operation Center (SOC) integration, these systems divert attackers, generate real-time threat intelligence, and improve resilience.
  - Autonomous vehicles are adopting multi-sensor spoofing detection systems that fuse LiDAR, radar, GPS, and machine learning to verify obstacles and location data. These layered defenses improve accuracy against fake signals and can trigger adaptive responses like vehicle lockdown, rerouting, or alerts authorities.

Dennemeyer
The IP Group

Industry News

Train Braking Flaw

Major railroad-signaling vulnerability could lead to train disruptions

A serious flaw in train braking systems could allow hackers to remotely stop trains using cheap equipment, due to weak security in brake control signal protocols. If exploited, it could cause sudden stops or even derailments. The U.S. cybersecurity agency CISA warned that the flaw is easy to exploit and could disrupt train operations. Although a safer system is being developed, it won't be ready until at least 2027. Researchers who found the flaw said they warned authorities as early as 2012, but the rail industry ignored it, claiming the system was outdated even though it's still in use. CISA says the risk is limited because attackers would need special tools and access to rail lines, but the threat remains real. Similar attacks have already happened in Europe using cheap radio devices.

Source
https://www.cybersecuritydive.com/

Dennemeyer
The IP Group

Industry News

Bentley Cybersecurity Certification

Bentley and MHP ensure cyber security compliance with UNECE Vehicle Regulations

Bentley Motors, in collaboration with MHP Consulting UK, a subsidiary of Porsche that specializes in automotive process and IT consulting, has successfully achieved UNECE WP.29 certification for cybersecurity and software update management systems. This certification ensures that Bentley's GT car range meets the highest global standards for vehicle cybersecurity. The 24-month project involved aligning Bentley's existing systems with UNECE regulations R155 and R156. Phase 1 focused on developing compliant processes and tools, while Phase 2 operationalized them across Bentley's business. The initiative included thorough audit preparation, integration of ISO 21434 standards, and strong governance.

Source
https://www.mhp.com/

Dennemeyer
The IP Group

Industry News

EV Charger Security Threat

CISA alert: Liteon electric vehicle chargers

The Cybersecurity and Infrastructure Security Agency (CISA), a U.S. government agency responsible for protecting critical infrastructure from cyber and physical threats, has issued a warning about a cybersecurity flaw in Liteon electric vehicle (EV) chargers. The flaw involves the charger's firmware storing server access credentials in plain text within the logs. This vulnerability could allow hackers to access the charger and steal sensitive information, including the owner's password in plain text. Since these chargers are connected to the internet, they can be targeted like any other smart device. Liteon has released updated firmware to fix the issue.

Source
https://www.cisa.gov/

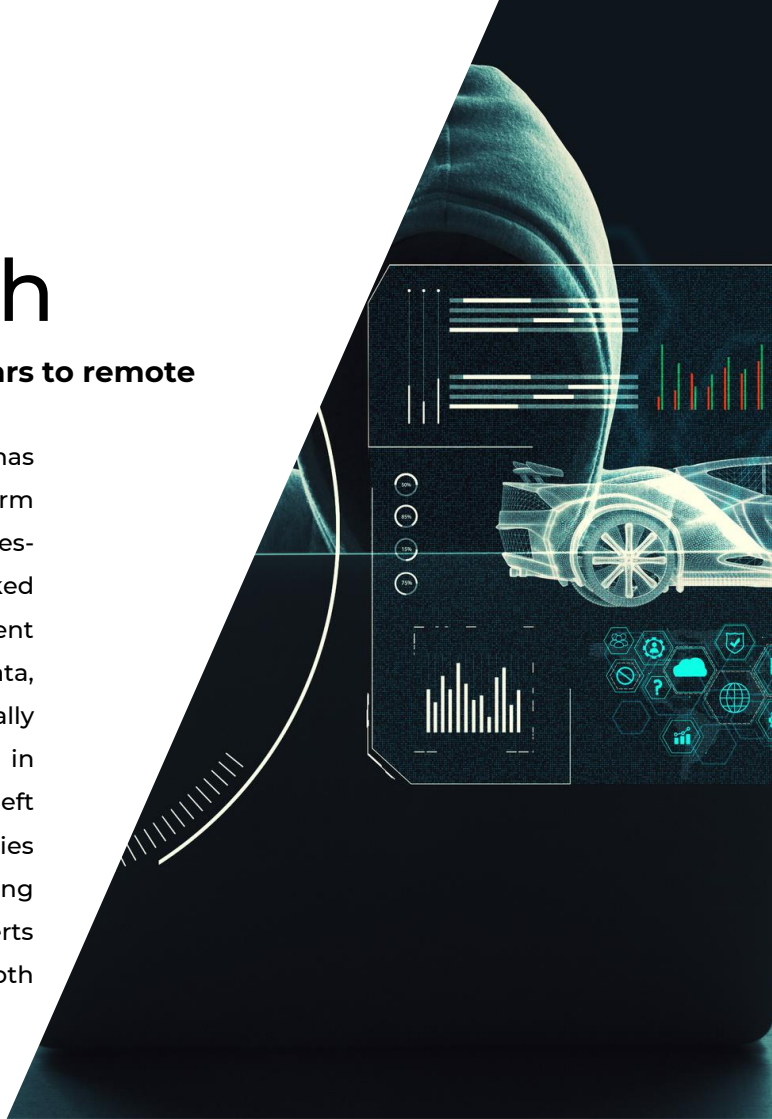
Dennemeyer
The IP Group

Industry News

Bluetooth Breach

New PerfektBlue attack exposes millions of cars to remote hacking

A major Bluetooth security threat called PerfektBlue has been discovered in OpenSynergy's Bluetooth platform (BlueSDK), affecting millions of vehicles including Mercedes-Benz, Volkswagen, and Skoda. This attack uses four linked vulnerabilities to remotely take control of infotainment systems with just one click. Hackers can access GPS data, record audio, steal personal information, and potentially control vehicle electronics. Despite fixes released in September 2024, delays in the automotive supply chain left many vehicles unpatched until June 2025. The vulnerabilities exploit weaknesses in Bluetooth protocols, allowing attackers to execute code by manipulating memory. Experts recommend updating firmware and disabling Bluetooth when not needed.



Source
https://cybersecuritynews.com/

Dennemeyer
The IP Group

Industry News

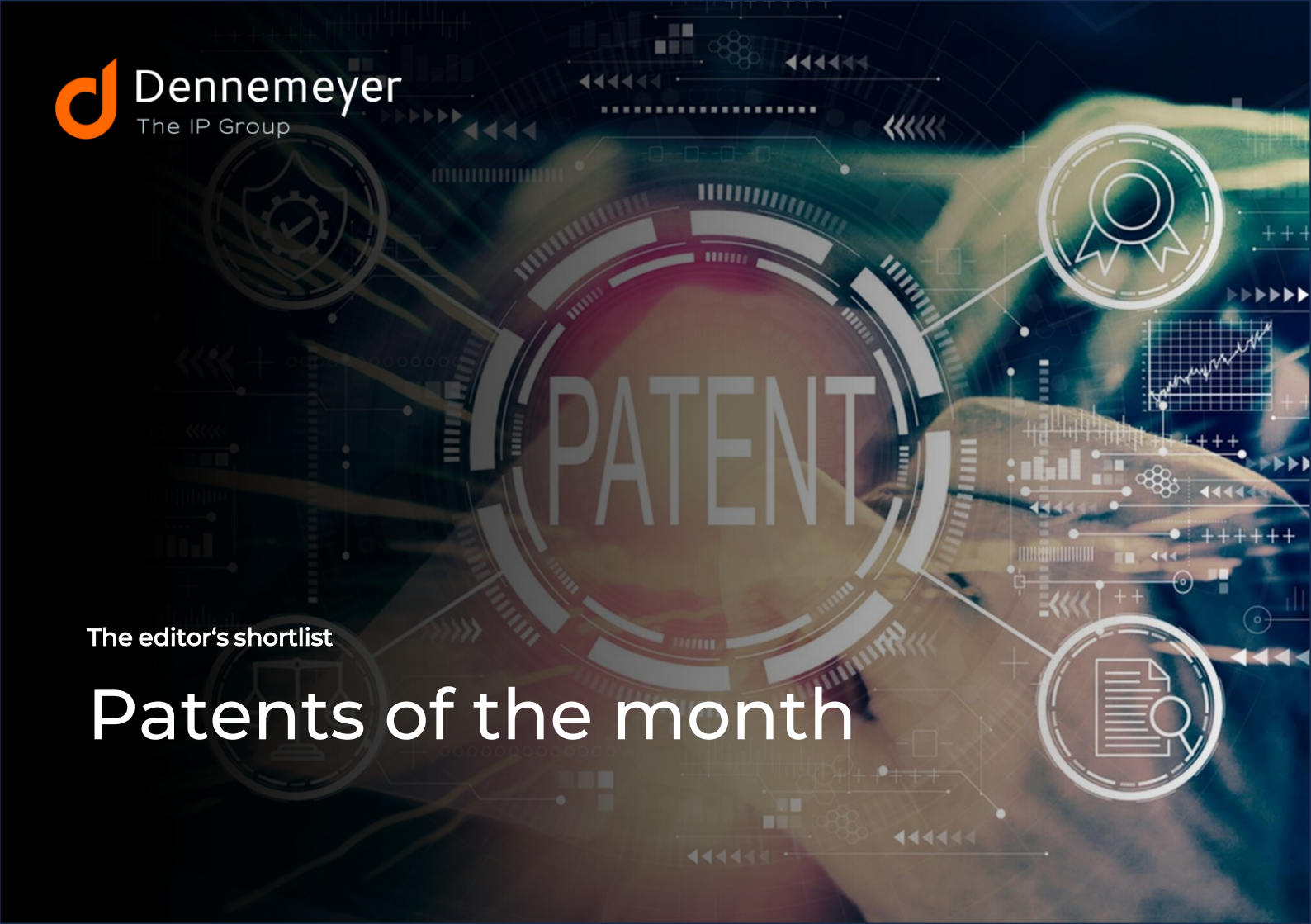
Cybersecurity Collaboration

MOU with ARAI to strengthen automotive cybersecurity readiness in India

ETAS India, a provider of tools, software, and services for developing and securing embedded systems in the automotive industry has signed an MoU with ARAI to boost cybersecurity readiness in India's growing automotive sector. As vehicles become more connected and software-driven, this partnership aims to equip OEMs, suppliers, startups, and professionals with the skills to handle emerging cyber threats and meet global regulations. ETAS India and ARAI will offer training programs, workshops, and certifications to raise awareness and build expertise. This initiative marks a key step toward a more secure and resilient automotive future in India.

Source
https://www.etas.com/

Dennemeyer
The IP Group



The editor's shortlist

Patents of the month

Dennemeyer
The IP Group

Patents of the month

Published in July 2025

Shortlisted and summarized by our analyst

- US2025225241A1 - Identification and mitigation of spoofing attacks on autonomous vehicles
  Assignee: Kyndryl Inc
- US12348565B2 - Arrangement of cyber security and prognostics, coexisting on a single platform
  Assignee: Toyota Motor Co Ltd
- US2025247411A1 - Attack analysis device, attack analysis method, and storage medium thereof
  Assignee: Nippon Denso Co
- US2025220432A1 - Systems and methods to detect GPS spoofing attacks
  Assignee: Intelligent Fusion Tech Inc
- JP2025520248A - Fraud indication aggregator for identifying fraud situations in a vehicle-to-everything (V2X) communication system
  Assignee: Qualcomm Inc
- EP4586550A1 - Method for placing honeypots in a vehicle fleet network
  Assignee: Robert Bosch Gmbh
- KR102832064B1 - Method and apparatus for generating dataset for detecting cyber attack on internal network of unmanned ground vehicle
  Assignee: Agency for Defense Development Korea
- FR3158161A3 - Countermeasure method against man-in-the-middle attacks in the UWB protocol
  Assignee: Ingenico Belgium
- IN568351A1 - A system and a method for vehicle security and threat scanner
  Assignee: Pooja Upadhyay
- CN120344967A - Attack path prediction method, attack path prediction device, and program
  Assignee: Panasonic IP Management Co Ltd

Dennemeyer
The IP Group

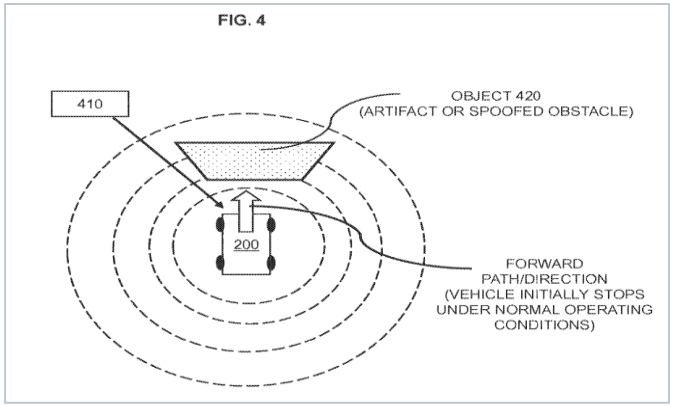
Latest patents

US2025225241A1

Identification and mitigation of spoofing attacks on autonomous vehicles

Company name	Kyndryl Inc
Inventors	Rodriguez Bravo Cesar Augusto
Priority date	09 Jan 2024
Publication date	10 Jul 2025

Summarized by Dennemeyer



This patent tackles the problem of spoofing attacks on self driving vehicles, where fake obstacles are created to trick the vehicle's sensors, potentially causing it to stop or behave dangerously. The invention uses the vehicle's sensors to detect objects in its path and then checks if those objects are real or fake. If it suspects a trick, the system takes safety actions like stopping the vehicle and verifying the object using other sensors. It improves detection by using multiple sensor types like LiDAR and radar and applies machine learning to better identify threats. It also includes security responses such as alerting users, locking doors, contacting authorities, or move car to safety. This makes self driving vehicles smarter and safer by helping them tell the difference between real and fake obstacles.

Dennemeyer
The IP Group

Latest patents

US12348565B2

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

Company name	Toyota Motor Co Ltd
Inventors	Okada Kazuya
Priority date	07 Nov 2022
Publication date	01 Jul 2025

Summarized by Dennemeyer

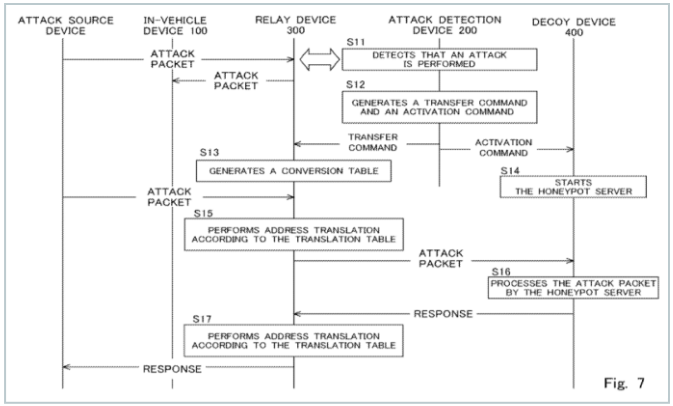


Fig. 7

This patent focuses on protecting connected vehicles from network attacks, where traditional blocking methods might alert attackers and allow them to adapt. This invention introduces a two-device system: the first device monitors vehicle communications and detects attacks, while the second device uses a honeypot server to handle malicious traffic. When an attack is detected, the honeypot is activated, which mimics the vehicle's system and redirects harmful data away from the real vehicle. It also uses specific vehicle data like location, direction, and speed to make the simulation more convincing. The system only activates these defenses during an actual attack, saving resources, and shuts them down once the threat is gone. This approach allows real-time monitoring, tricks attackers without revealing security strategies, and ensures the vehicle remains safe and functional.

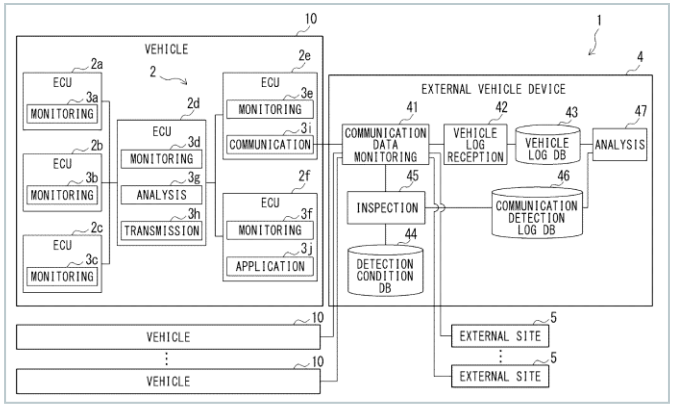
Dennemeyer
The IP Group

Latest patents

US2025247411A1

Attack analysis device, attack analysis method, and storage medium thereof

Company name	Nippon Denso Co
Inventors	Ikuse Tomonori, Egawa Masumi, Abe Taiji, Utsunomiya Hiroyuki, Nagara Keigo
Priority date	30 Sep 2022
Publication date	31 Jul 2025



This patent talks about the growing threat of cyberattacks targeting vehicles with advanced electronic control systems and communication features like vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). The invention introduces an attack analysis device that examines both system logs and communication logs to detect if any known type of attack has occurred. It checks whether any part of the vehicle's control system has been compromised by comparing the logs with predefined attack patterns. It then improves accuracy by combining different sources of data and helps classify how likely it is that a system has been violated. It also strengthens cybersecurity by offering a structured way to assess threats and respond effectively, making connected vehicles more secure against network-based attacks.

Summarized by Dennemeyer

Dennemeyer
The IP Group

Latest patents

US2025220432A1

Systems and methods to detect GPS spoofing attacks

Company name	Intelligent Fusion Tech Inc
Inventors	Tian Xin, Fan Zhengyang, Pham Khanh, Blasch Erik, Wei Sixiao, Shen Dan, Chen Genshe
Priority date	27 Dec 2023
Publication date	03 Jul 2025

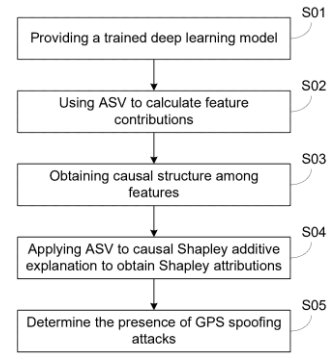


FIG. 7

This patent tackles the problem of GPS spoofing attacks, where fake GPS signals are used to mislead systems like drones or autonomous vehicles that rely on accurate location data. The solution uses a deep learning model trained to detect such attacks by analyzing GPS signal features. It calculates how much each feature contributes to the signal and uses these insights to identify spoofed signals. The invention also explains why a signal is classified as spoofed, making the detection process more transparent. By combining this analysis with machine learning, the system improves accuracy and interpretability, helping protect critical navigation systems from being tricked.

Dennemeyer
The IP Group

Latest patents

JP2025520248A

Fraud indication aggregator for identifying fraud situations in a vehicle-to-everything (V2X) communication system

Company name	Qualcomm Inc
Inventors	Ansari Mohammad Raashid, Petit Jonathan, Monteuuis Jean-philippe, Chen Kong
Priority date	25 Apr 2022
Publication date	03 Jul 2025

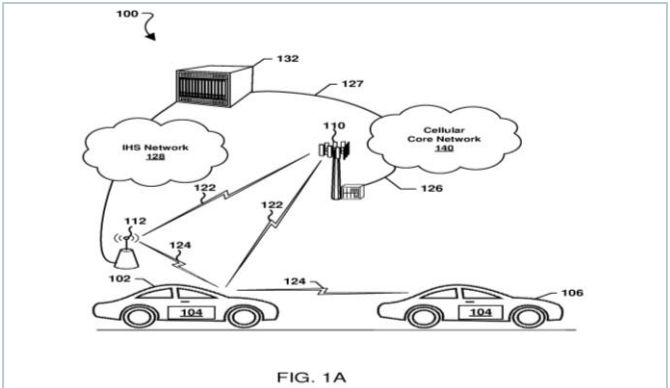


FIG. 1A

This patent addresses the problem of vehicles sending incorrect or fake information in V2X communication systems, which can flood the Misbehavior detector with too many reports and waste network resources. The invention suggests detecting signs of misbehavior using multiple detection tools, then combines these signs to decide if the issue is serious enough to report or act on. This helps avoid sending duplicate or unnecessary reports. The system uses smart thresholds and majority decisions to judge whether a misbehavior is real, and adjusts its sensitivity based on live data. This makes the process more efficient, reduces network load, and improves how misbehavior is handled in connected vehicle systems.

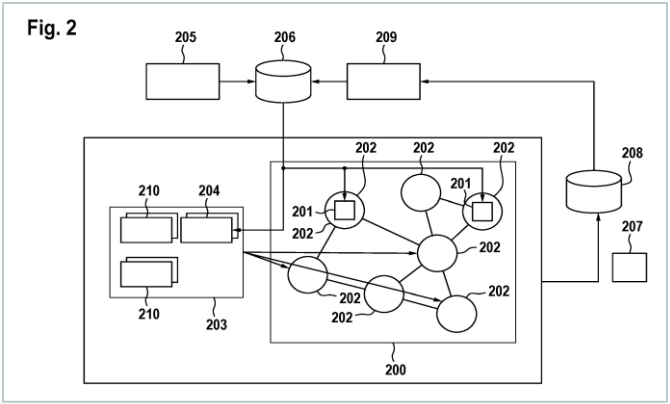
Summarized by Dennemeyer

Dennemeyer
The IP Group

Latest patents

EP4586550A1

Method for placing honeypots in a vehicle fleet network



Company name	Robert Bosch Gmbh
Inventors	Ilg Niclas, Huth Christopher, Sisejkovic Dominik
Priority date	12 Jan 2024
Publication date	16 Jul 2025

This patent solves the problem of intelligently placing honeypots, which are decoy systems meant to attract cyber attackers, within a network of vehicles. As these networks expand and threats evolve, optimal placement becomes increasingly complex. The solution determines where to deploy honeypots across a fleet by analyzing attack data, calculating the likelihood of detection, and adjusting their positions over time to improve effectiveness. It involves selecting locations, running honeypots, collecting data, and evaluating detection performance. By continuously learning from real-time attack feedback and fleet operations, the system ensures that honeypots remain both attractive to attackers and effective for defense.

Dennemeyer
The IP Group

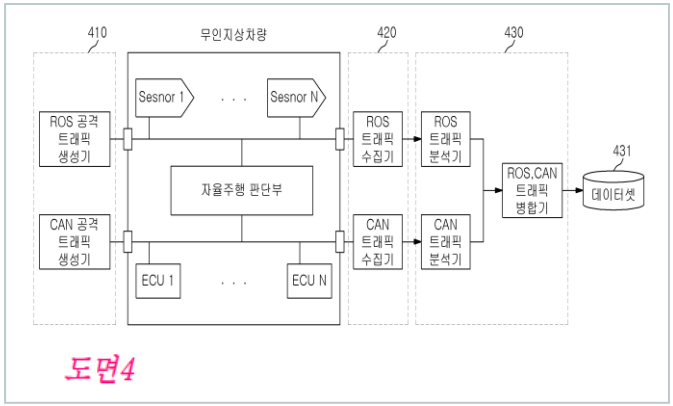
Latest patents

KR102832064B1

Method and apparatus for generating dataset for detecting cyber attack on internal network of unmanned ground vehicle

Company name	Agency for Defense Development Korea
Inventors	Yoo Changon, Lee Hwaseong, Lee Hyunwoo, Heo Seondong, Park Mooseong
Priority date	24 Jan 2024
Publication date	08 Jul 2025

Summarized by Dennemeyer



This patent addresses the rising cybersecurity risks in unmanned ground vehicles (UGVs) as autonomous driving technologies advance, pointing out the lack of proper datasets for detecting internal network attacks. The invention creates such datasets by injecting attack traffic into different parts of the UGV's internal network, recording all traffic during operation, and marking which parts correspond to the attacks. It then analyzes this data to label traffic as normal or abnormal based on its source and behavior. It helps build accurate datasets that support intrusion detection system (IDS) development, improves detection accuracy by using parameters like timestamps and message IDs, and enables combining data from different in-vehicle networks for a more complete security analysis.

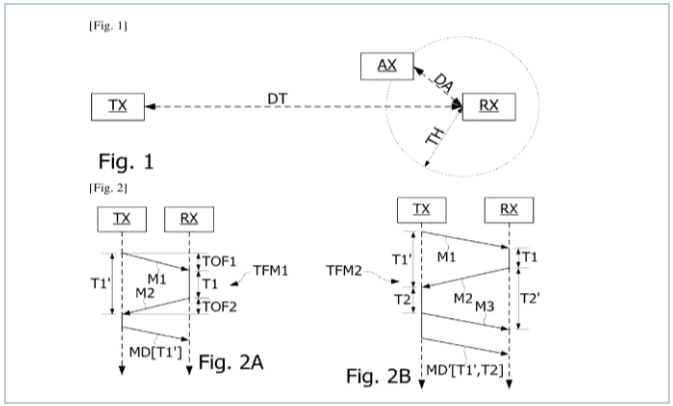
Dennemeyer
The IP Group

Latest patents

FR3158161A3

Countermeasure method against man-in-the-middle attacks in the UWB protocol

Company name	Ingenico Belgium
Inventors	Vanophalvens Mark
Priority date	15 Dec 2023
Publication date	11 Jul 2025



This patent focuses on the problem of man-in-the-middle attacks that interfere with distance measurements between devices using Ultra Wide Band (UWB) signals, which can affect systems like hands-free vehicle access. The invention performs two separate distance checks, one using UWB and another using a different communication method like Bluetooth. By comparing the results of both, it can detect if an attack has occurred based on whether the difference exceeds a certain threshold. If the measurements are close enough, the system may proceed with operations like unlocking the vehicle; otherwise, it blocks the action. This dual-check approach improves security without needing major hardware changes, using existing communication interfaces to detect and prevent interference.

Summarized by Dennemeyer

Dennemeyer
The IP Group

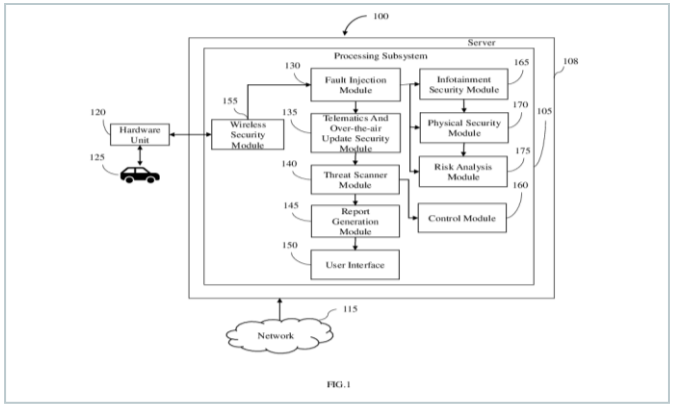
Latest patents

IN568351A1

A system and a method for vehicle security and threat scanner

Company name	Individual Inventor
Inventors	Pooja Upadhyay
Priority date	27 Jun 2024
Publication date	03 Jul 2025

Summarized by Dennemeyer



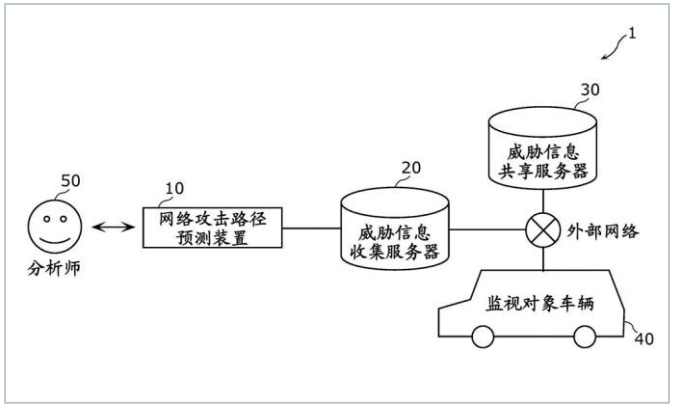
This patent tackles the rising cybersecurity risks in modern self-driving and electric vehicles, which depend heavily on software and wireless communication. As vehicles get more connected, they face dangers like hacking, data tampering, and unauthorized access. The invention provides a complete security system with two main parts: a hardware unit that connects to the vehicle's network and a server that does the processing. It uses a fault injection tool to simulate attacks such as spoofing, jamming, firmware changes, and code injection to find weak spots. It also checks the safety of telematics and over-the-air (OTA) updates, scans for threats, and generates detailed reports with clear guidelines. This helps identify vulnerabilities so manufacturers and operators can make vehicles safer.

Dennemeyer
The IP Group

Latest patents

CN120344967A

Attack path prediction method, attack path prediction device, and program



Company name	Panasonic IP Management Co Ltd
Inventors	Liu Guliang, Hoshi Tomoyuki, Ujiie Yoshihiro, An Entong Yang; Hiraishi Rikiya
Priority date	13 Dec 2022
Publication date	18 Jul 2025

This invention tackles the challenges Security Operation Centers (SOCs) face in predicting how cyber attacks on vehicles might progress. Traditional methods require expert knowledge, are expensive, and often lead to inconsistent results between analysts. This invention automates the process by collecting incident data from vehicle monitors, comparing it with past attack records, and using that information to predict possible future attack paths. If the initial search doesn't return enough data, the system adjusts the search conditions to find more relevant threats. This helps even less-experienced analysts perform advanced threat assessments more easily and accurately. By analyzing attack trends and automating queries, the system improves prediction accuracy, reduces costs, and makes SOC operations more consistent.

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