Dennemeyer
The IP Group

Report of May 2024

Cybersecurity in mobility

Recent developments

Curated and summarized - **Industry and Patent news**

Published by Dennemeyer India Private Limited

Parag Thakre (pthakre@dennemeyer.com)

Key Insights

❑ Cyber Attack Penetration testing labs are crucial for OEMs/Suppliers to ensure vehicle compliance with cybersecurity regulations, and to identify vulnerabilities in the software and hardware components of vehicles.

❑ A new open-source operating system (OS) certified for automotive safety standards is introduced, which paves the way for car companies to build secure ADAS functions and autonomous vehicles.

❑ To secure the Indian Space sector, SIA-India join forces with ISAC to create a common cybersecurity standards against cyberattacks targeting satellite operations and communication channels.

❑ Strict enforcement of Cybersecurity regulations (UN R155 & R156) by the EU compels some car manufacturers (VW, Porsche, Renault, Audi) to remove older models from their line-up due to the high cost of upgrading the components.

❑ New technologies are patented to detect and prevent attacks on In-Vehicle Network, Unmanned Aerial Vehicle (UAV).

❑ A new invention published as a patent application that describes the use of Digital Twin for security assessment of vehicles.

Collaboration

Vector enables the power of Infineon’s AURIX™ TC4x cyber security features

Infineon and Vector are collaborating to improve automotive cybersecurity. Infineon's new AURIX TC4x microcontrollers meet the latest cybersecurity and safety standards ISO/SAE 21434 and ISO 2626 and are designed to address the growing security risks associated with connected vehicles. Vector's firmware MICROSAR HSM Classic software supports the AURIX TC4x family and offers features like hardware-accelerated cryptography and secure communication protocols, making it easier for car manufacturers to build safe and reliable vehicles. This collaboration ensures compatibility and simplifies development for engineers working on next-generation software-defined cars.

Source
www.infineon.com

New Testing Lab

Argus Cyber Security Opens New Automotive Penetration Testing Lab in North America

Argus Cyber Security opened a new penetration testing lab in Detroit to cater the growing demand for local cybersecurity expertise in North America. This lab will help US car manufacturers (OEMs) and parts suppliers (Tier 1) to comply with cybersecurity regulations by identifying vulnerabilities in their vehicles' software and hardware components. Argus offers various penetration testing services including ECU (Electronic Control Unit) and full vehicle testing, along with code review and fuzz testing to find weaknesses. This local presence will speed up development and reduce costs for North American car companies.

Source
argus-sec.com

Open-source OS

Elektrobit open-source breakthrough accelerates transition to software-defined mobility

Elektrobit introduced EB corbos Linux for Safety Applications, the first open-source operating system (OS) certified for automotive safety standards. This accomplishment allows car companies to leverage open-source software for safety-critical functions in areas like advanced driver-assistance systems (ADAS) and autonomous vehicles. Benefits include faster development cycles, reduced costs, and longer security maintenance. This paves the way for more software-defined vehicles with over-the-air updates and is supported by industry leaders like Arm and Canonical.

Source
www.elektrobit.com

Dennemeyer
The IP Group

Industry news

Space Cybersecurity

SIA-India and ISAC forge alliance to strengthen space cybersecurity standards

To combat growing cyber threats in the rapidly expanding Indian space sector (valued at $8.4 billion, projected to reach $44 billion by 2033), SIA-India (Satcom Industry Association) and ISAC (Information Sharing and Analysis Centre) are joining forces. Their collaboration will establish common cybersecurity standards, specialized training programs, incident response capabilities for space professionals and emphasis in mitigating cyber threats that could disrupt satellite operations and communication channels. This initiative safeguards critical space infrastructure for ISRO, private companies, and startups, protecting billions in GDP and national security interests.

Source
www.financialexpress.com

Dennemeyer
The IP Group

Industry news

EU Mandates

New EU cybersecurity rules push carmakers to shun old models

The EU is enforcing stricter cybersecurity regulations (UN R155 & R156) to address software update vulnerabilities in modern cars, particularly electric vehicles. This compels some automakers (VW, Porsche, Renault, Audi) to remove older models from their European line-up due to the high cost of upgrading their electronics components. However, some manufacturers like Mercedes-Benz claim their current models will be compliant.

Source
www.dw.com

Dennemeyer
The IP Group

The editor‘s shortlist

Patents of the month

Dennemeyer
The IP Group

Patents of the month

Published in April 2024

Shortlisted and summarized by our analyst

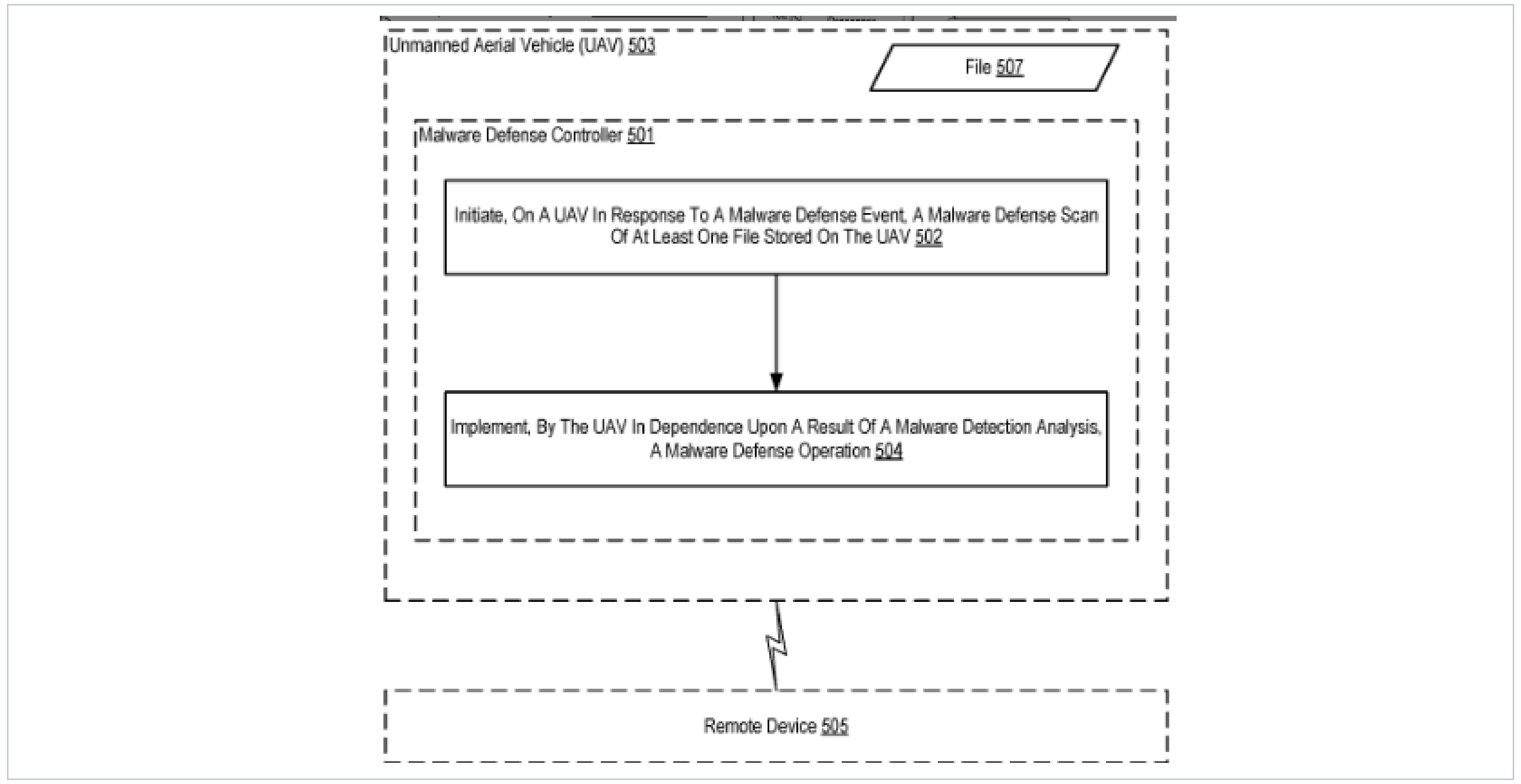
- US2024119152A1 - Providing malware protection on an unmanned aerial vehicle
  Assignee: Skygrid LLC
- US11966503B2 - Glitch attack mitigation for in-vehicle networks
  Assignee: Intel corp
- US11952013B2 - Trusted context self learning method for an in-vehicle network intrusion detection system developed to limit calibration proliferation and development costs
  Assignee: GM Global Tech Operations LLC
- US11973790B2 - Cyber digital twin simulator for automotive security assessment based on attack graphs
  Assignee: Accenture Global Solutions Ltd
- US2024137373A1 - Advanced intrusion prevention manager
  Assignee: Continental Teves AG & Co OHG
- IN202441023921A - System for detecting advanced persistent threats in unmanned aerial systems and method thereof
  Assignee: Manipal Academy Of Higher Education
- IN532899A1 - Method for protecting a vehicle from cyber attacks, and corresponding device
  Assignee: Marelli Europe SPA, Univ of Pisa
- CN117879915A - Vehicle intrusion detection and defense system based on AutoSAR CP
  Assignee: Wuhu Etec Automotive Electronic Co Ltd
- JP2024055384A - Vehicle control device
  Assignee: Subaru Corp
- EP4193567B1 - Method for securely equipping a vehicle with an individual certificate
  Assignee: Mercedes Benz Group AG

US2024119152A1

Providing malware protection on an unmanned aerial vehicle

Company name	Skygrid LLC
Inventors	Ali Syed Mohammad, Duke Lowell L, Akbar Zehra, Husain Syed Mohammad Amir, Schmidt Taylor R, Lopez Milton, Pinnamaneni Ravi Teja
Priority date	02 Mar 2022
Publication date	11 Apr 2024

Summarized by Dennemeyer


Unmanned Aerial Vehicle (UAV) 503
File 507
Malware Defense Controller 501
Initiate, On A UAV In Response To A Malware Defense Event, A Malware Defense Scan Of At Least One File Stored On The UAV 502
Implement, By The UAV In Dependence Upon A Result Of A Malware Detection Analysis, A Malware Defense Operation 504
Remote Device 505

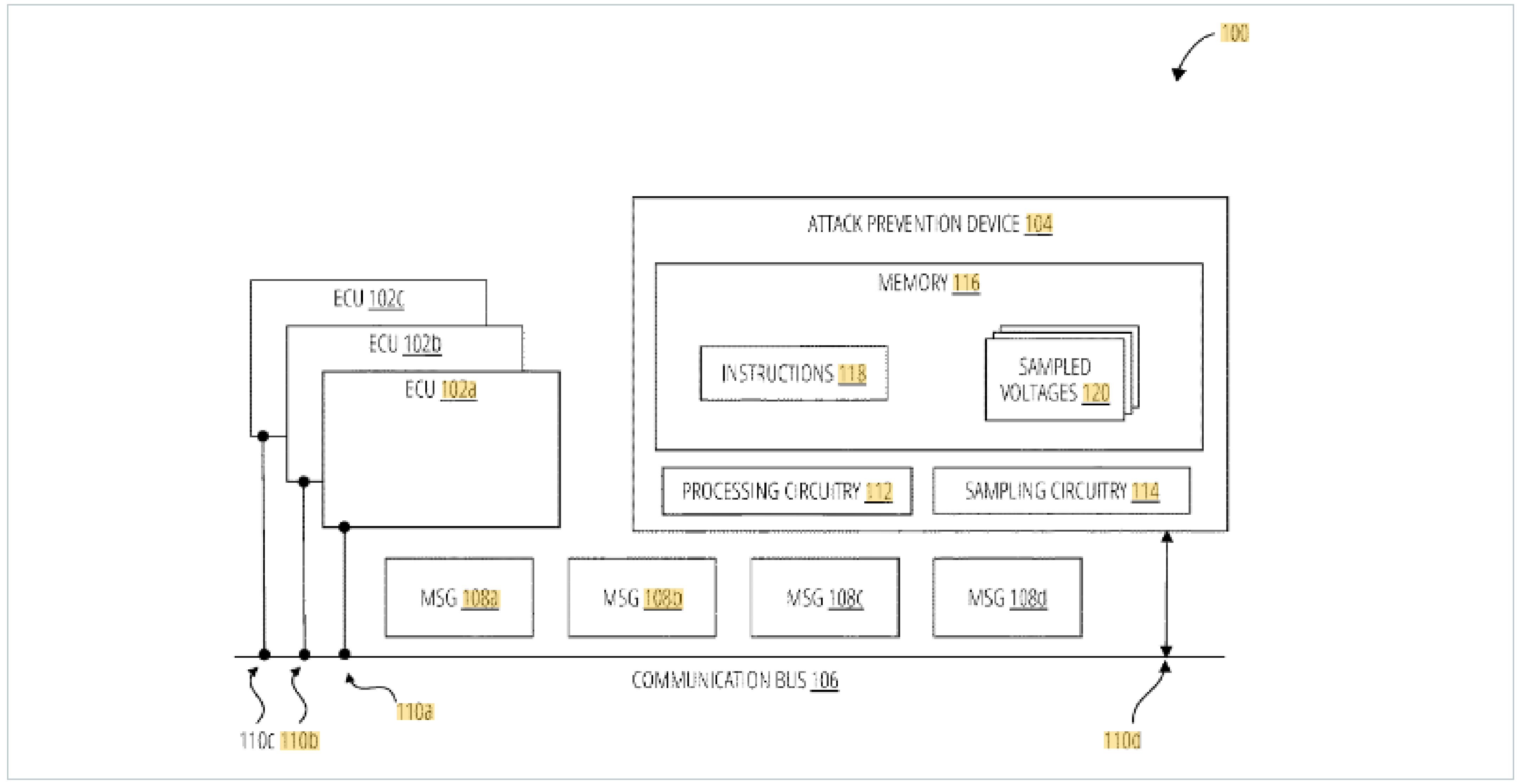
The patent proposes a system to shield Unmanned Aerial Vehicles (UAVs) from malware threats. As UAVs transition to higher-altitude roles and integrate more into airspace, their cybersecurity becomes paramount. The traditional air traffic management system is limited in scope. The invention addresses this gap by providing autonomous malware protection for UAVs. The system involves controllers that manage these defense operations. It also includes generating metadata for files, analyzing them for malware using trained models, and communicating with remote devices for further analysis. This is crucial because malware attacks can hijack UAVs, disrupt missions, or steal data.

US11966503B2

Glitch attack mitigation for in-vehicle networks

Company name	Intel corp
Inventors	Juliato Marcio, Lesi Vuk, Gutierrez Christopher, Ahmed Shabbir, Wang Qian, Sastry Manoj
Priority date	24 Sep 2021
Publication date	23 Apr 2024

Summarized by Dennemeyer



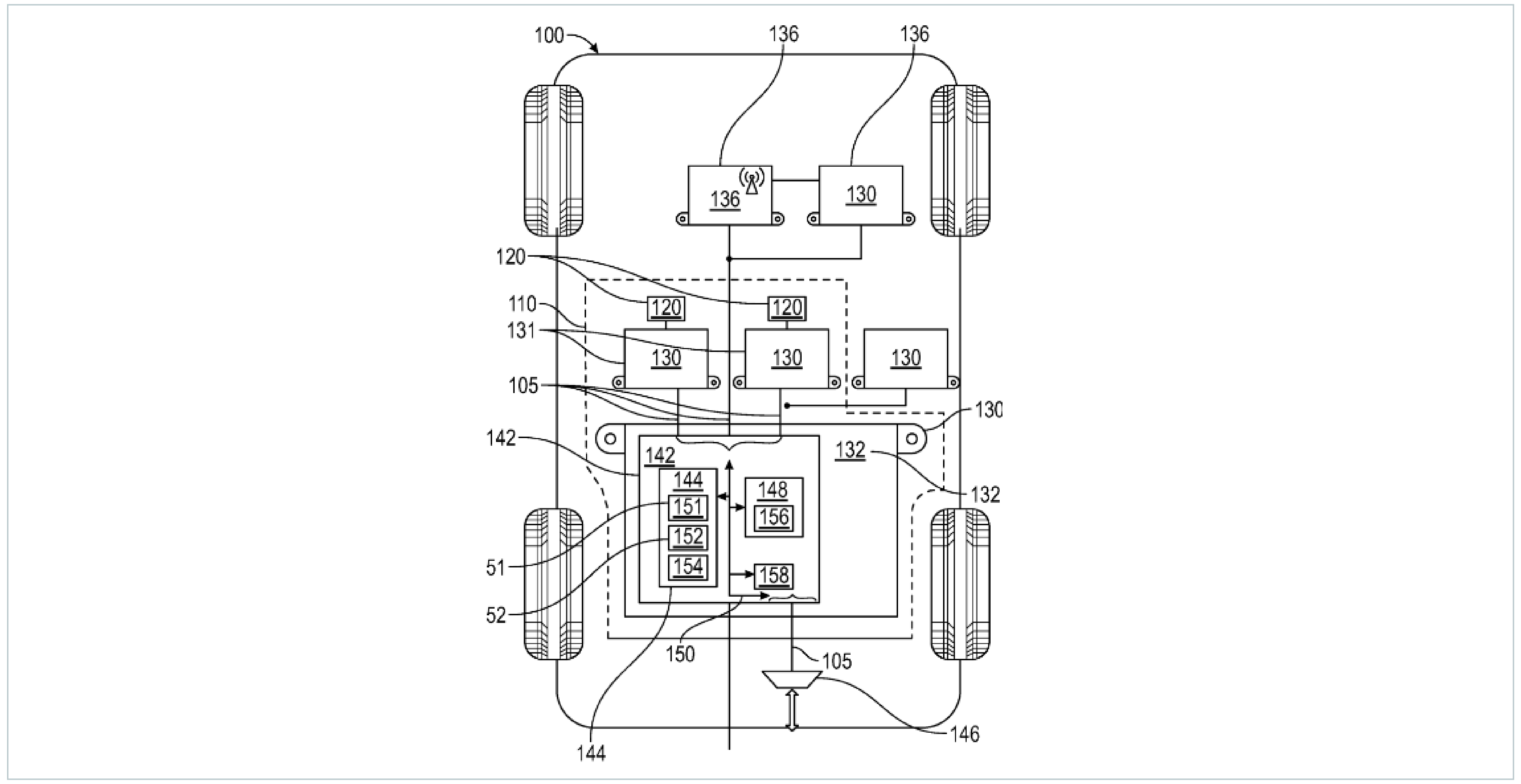
This invention addresses "glitch attacks" on communication networks where attackers trick devices by sending messages with fluctuating voltage. The result is different devices interpreting the same message differently. The solution involves enforcing constant signal levels throughout data transmission, ensuring all receivers get the same information, regardless of their sampling times. This can be done centrally or by individual network nodes. While described for car networks, it applies to any communication network vulnerable to these timing-based attacks.

US11952013B2

Trusted context self learning method for an in-vehicle network intrusion detection system developed to limit calibration proliferation and development costs

Company name	GM Global Tech Operations LLC
Inventors	El Rifai Mayssaa, Kupfer Samuel B, Ploucha Joseph E, Carleton Ron C
Priority date	16 Sep 2022
Publication date	21 Mar 2024

Summarized by Dennemeyer



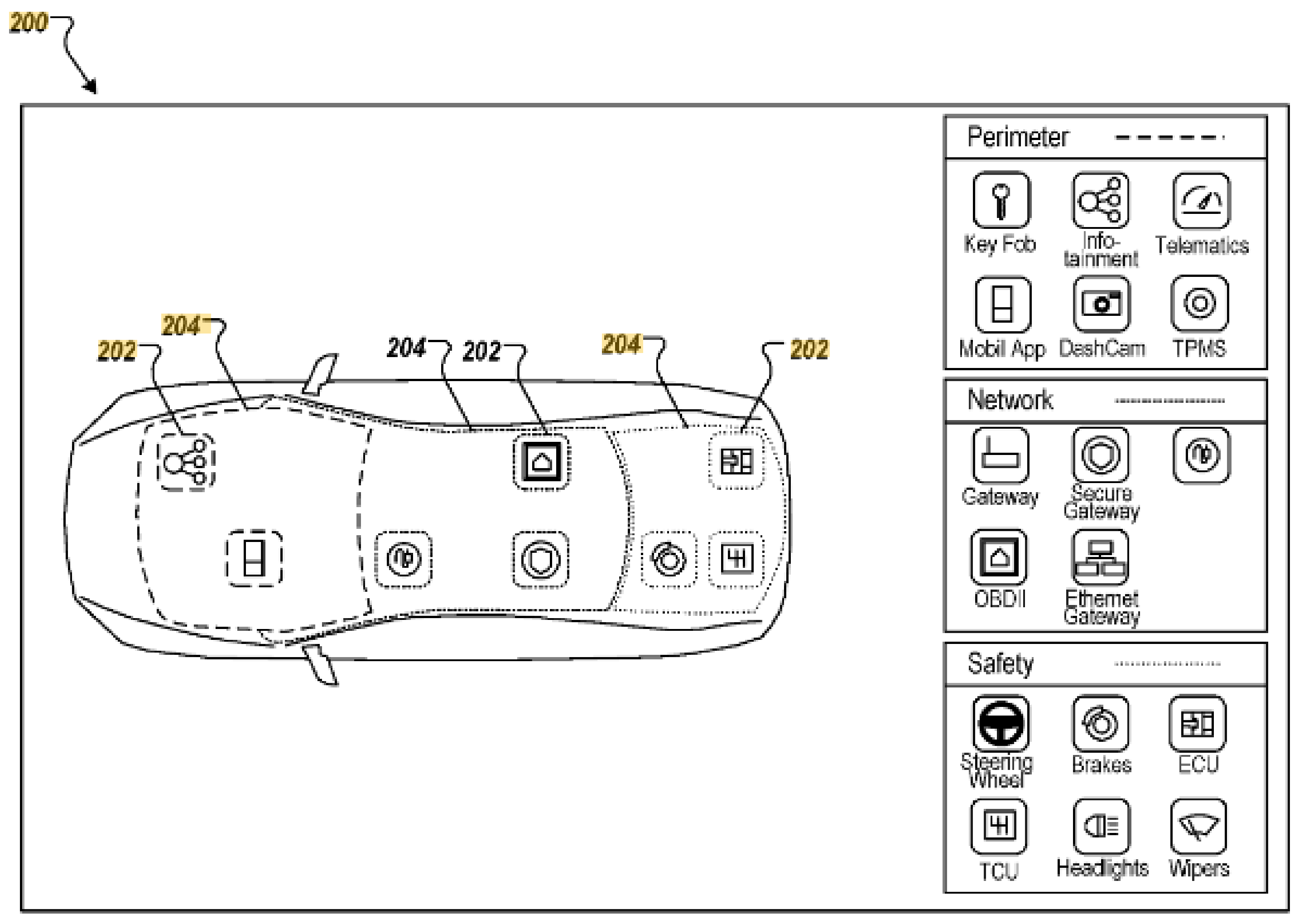
The invention proposes a method for self-learning secure network topology in vehicles. Current methods for Network Intrusion Detection Systems (NIDS) rely on pre-configured network maps, which can be expensive and time-consuming to create for every vehicle variation. This new system allows the NIDS to learn the network topology itself. It monitors various aspects of the vehicle (ECUs, state elements) to identify a safe window (trusted window) when learning can occur without risking unauthorized access. This allows the NIDS to build a vehicle-specific configuration containing a list of networks and allowed messages.

US11973790B2

Cyber digital twin simulator for automotive security assessment based on attack graphs

Company name	Accenture Global Solutions Ltd
Inventors	Klein Dan, Segev Elad
Priority date	09 Nov 2021
Publication date	30 Apr 2024

Summarized by Dennemeyer



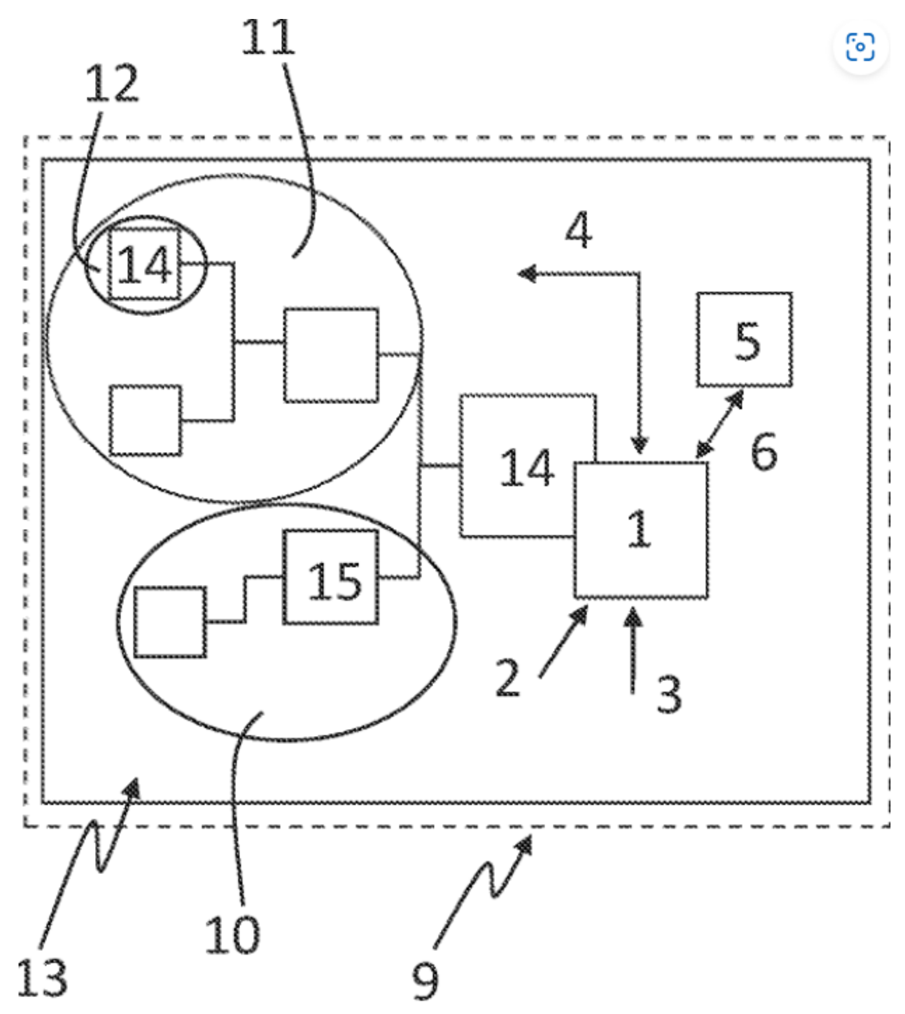
This invention proposes a connected vehicle cybersecurity platform that uses digital twin across multiple layers of the connected vehicle ecosystem to evaluate vulnerabilities and provide remedies. Digital twins are virtual representations of physical systems. These digital replicas of vehicles, infrastructure, and back-office systems allow generating attack graphs that simulate how attackers might move across the network. By analyzing these graphs, vulnerabilities can be identified and addressed more efficiently than traditional manual testing methods.

US2024137373A1

Advanced intrusion prevention manager

Company name	Continental Teves AG & Co OHG
Inventors	Klapper Patrick Thomas Michael, Roth Christopher
Priority date	20 Sep 2020
Publication date	25 Apr 2024

Summarized by Dennemeyer



The invention relates to prevention of intrusions on an in-vehicle network, such as Automotive Ethernet in-vehicle networks. The invention uses an Advanced Intrusion Prevention Manager (AIPM) to receive intrusion information from an in-vehicle network. The AIPM receives information about intrusions, the car's state (parked/driving), and the environment (raining, etc.), and then chooses a pre-defined security policy based on this information. This policy is then sent to the relevant car component to enforce.

Dennemeyer
The IP Group

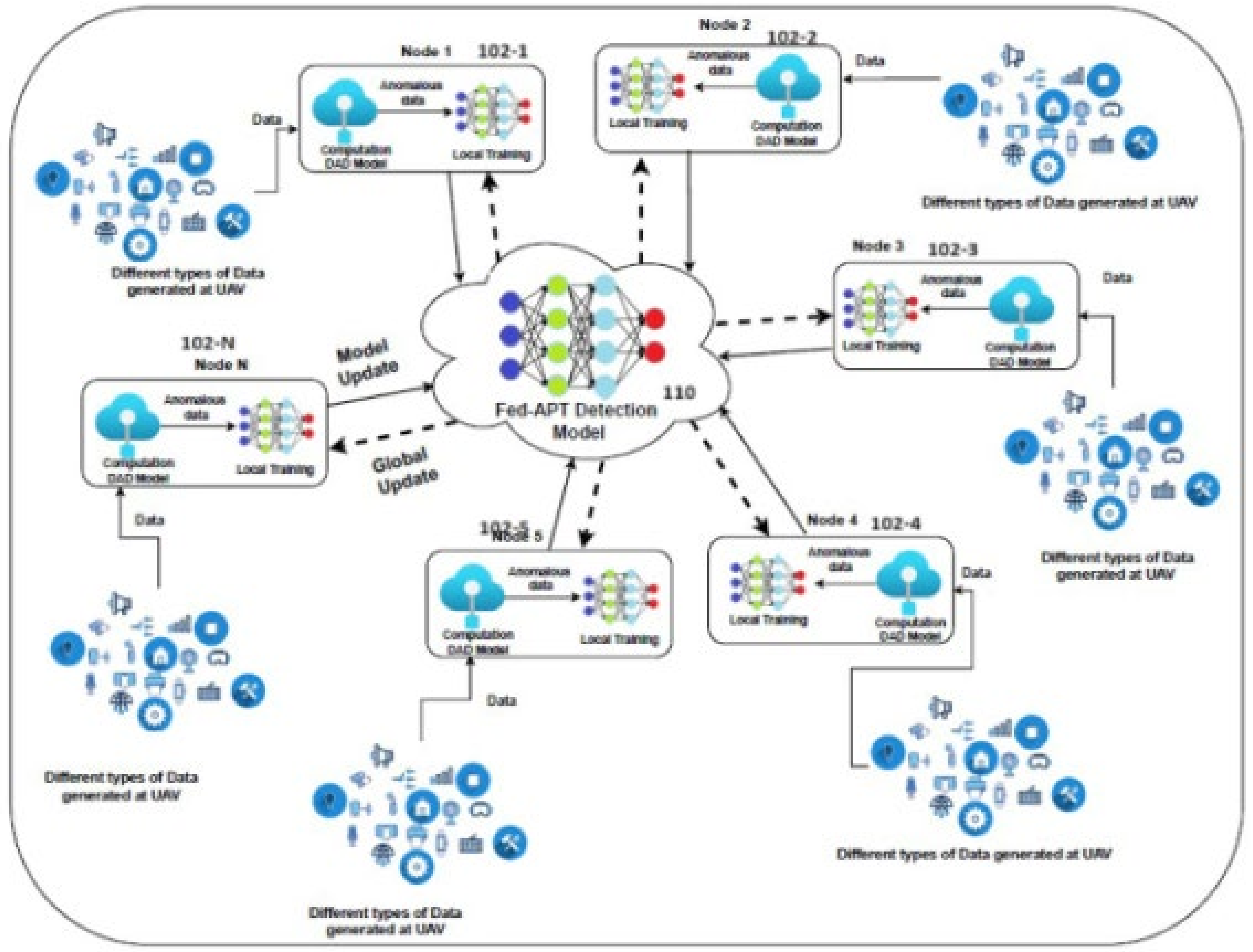
Latest patents

IN202441023921A

System for detecting Advanced Persistent Threats in unmanned aerial systems and method thereof

Company name	Manipal Academy Of Higher Education
Inventors	Udhina Kumar G K, Krishna Prakasha K, Balachandra Muniyal
Priority date	26 Mar 2024
Publication date	05 Apr 2024

Summarized by Dennemeyer



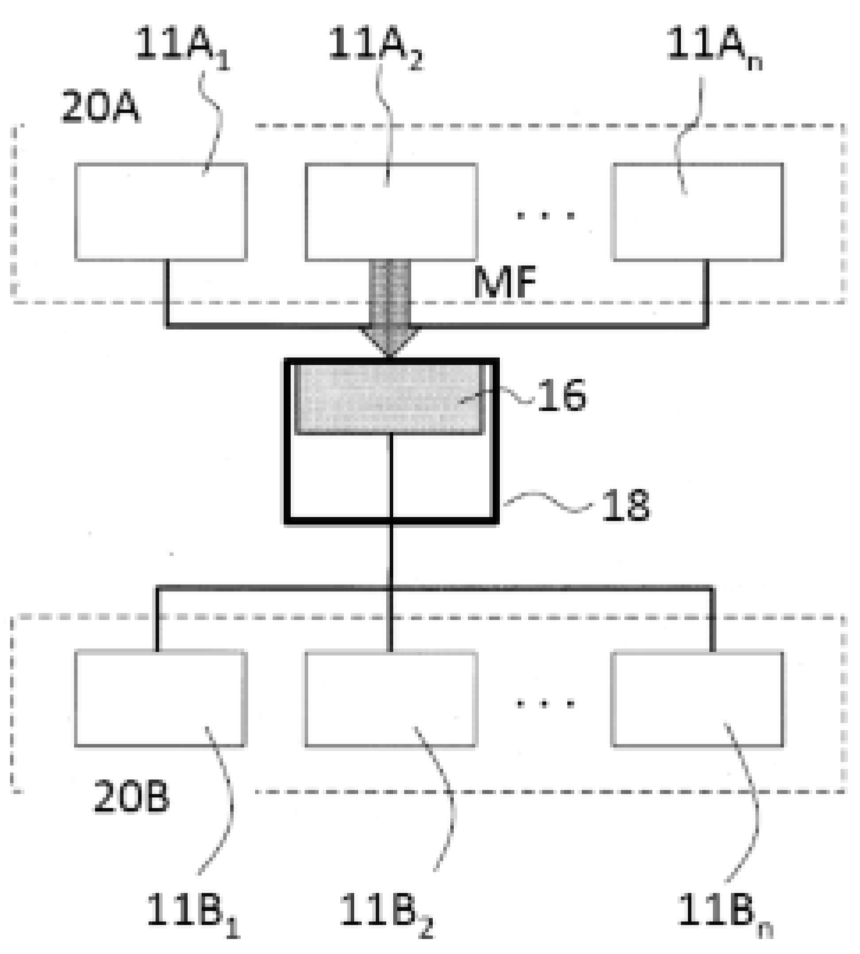
The invention relates to detecting advanced persistent threats (APT) in unmanned aerial systems. Traditional methods rely on centralized data collection, which raises privacy concerns. To overcome these challenges the system leverages a federated learning approach to train threat detection models on data collected directly by the drones, ensuring data privacy by only sharing model weights with a central server. It also utilizes distributed anomaly detection and machine learning techniques to efficiently identify and respond to both known and emerging APT threats.

IN532899A1

Method for protecting a vehicle from cyber attacks, and corresponding device

Company name	Marelli Europe SPA, Univ of Pisa
Inventors	Rosadini Christian, Nesci Walter, Baldanzi Luca, Crocetti Luca, Fanucci Luca
Priority date	31 Dec 2018
Publication date	15 Apr 2024

Summarized by Dennemeyer



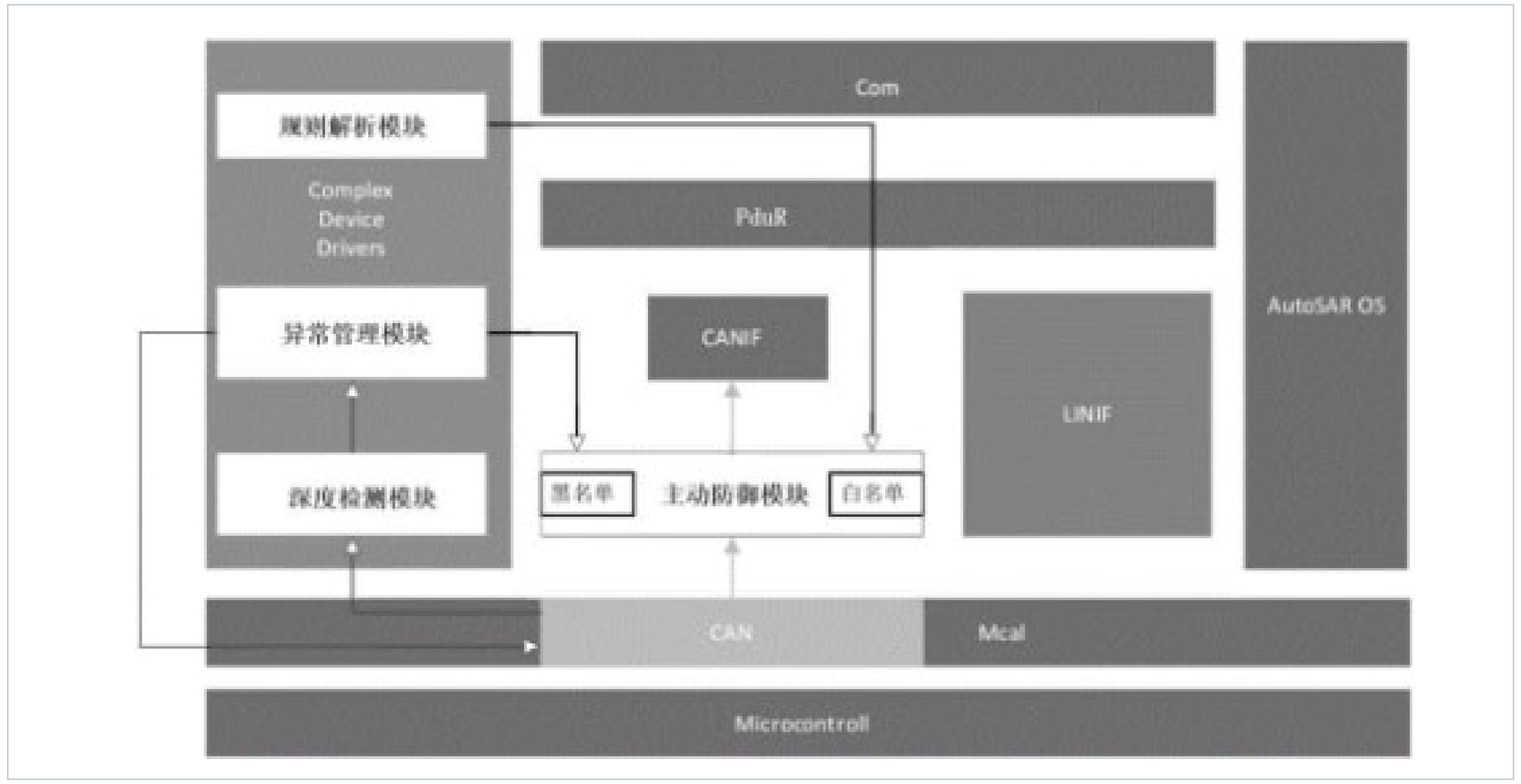
The invention describes a method to protect vehicles from cyber attacks on the Controller Area Network (CAN bus).The invention equips a protection device between the CAN controller and transceiver in a vehicle node (e.g., engine control unit). The device monitors messages traveling on the CAN bus and can block malicious messages. When a malicious message is detected, the device corrupts it with a specific bit sequence to render it invalid for the CAN controller. This way, the malicious message is not processed or propagated further.

CN117879915A

Vehicle intrusion detection and defense system based on AutoSAR CP

Company name	Wuhu Etec Automotive Electronic Co Ltd
Inventors	Chen Zejian, Chen Yong, Liu Hui
Priority date	28 Dec 2023
Publication date	12 Apr 2024

Summarized by Dennemeyer



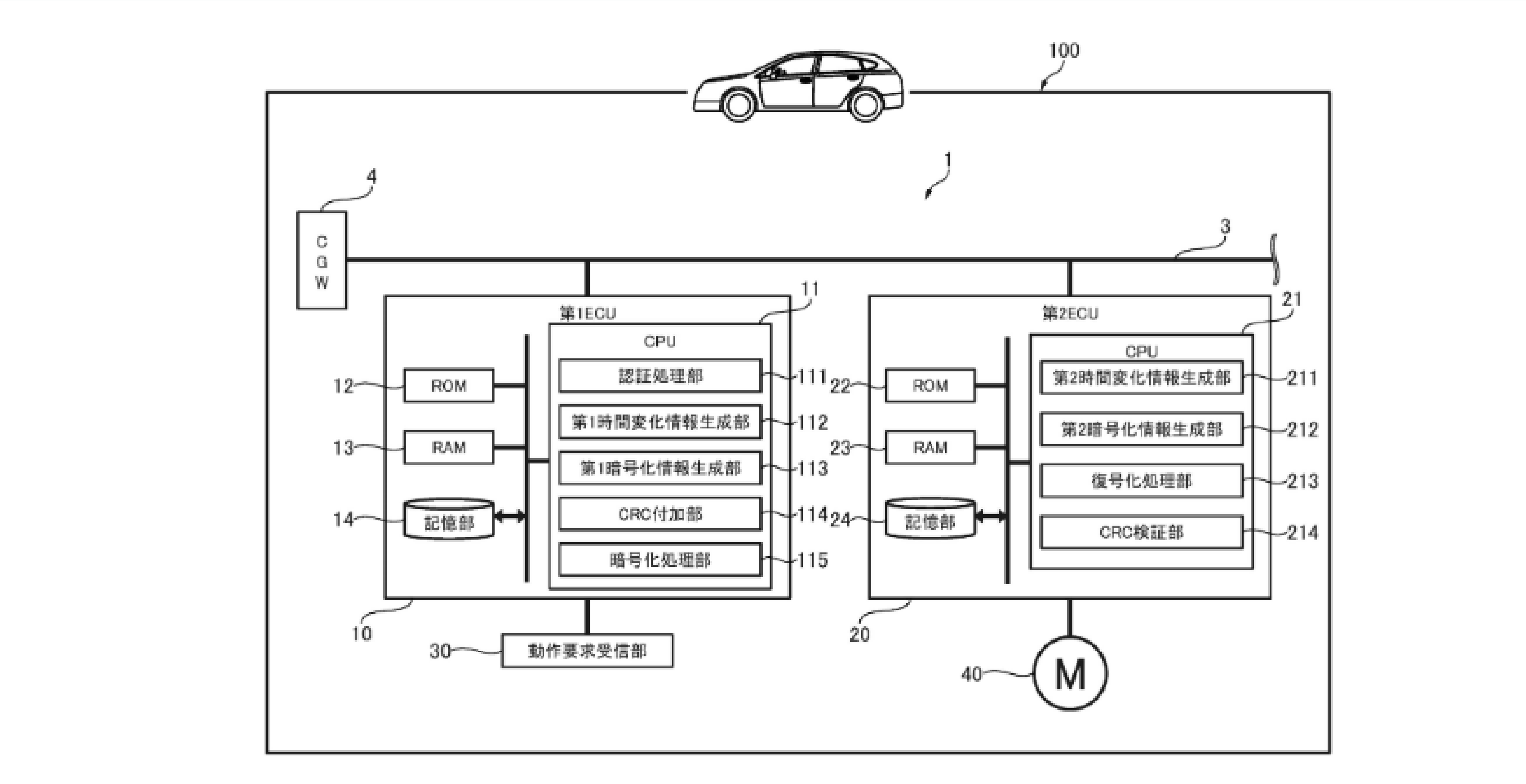
The invention provides an automotive intrusion detection and prevention system based on an AutoSAR CP. To address car hacking, the system incorporates multiple modules. These modules analyze message flow and content to identify safe communication and anomalies. The system prioritizes low-impact background tasks for anomaly detection to minimize interference with critical car functions. It can also upload suspicious messages for further analysis and implement hardware filtering in extreme situations. Overall, this system improves car security on the AutoSAR CP platform by proactively detecting and preventing intrusion attempts.

JP2024055384A

Vehicle control device

Company name	Subaru Corp
Inventors	Kyutaro Iiba
Priority date	07 Oct 2022
Publication date	18 Apr 2024

Summarized by Dennemeyer



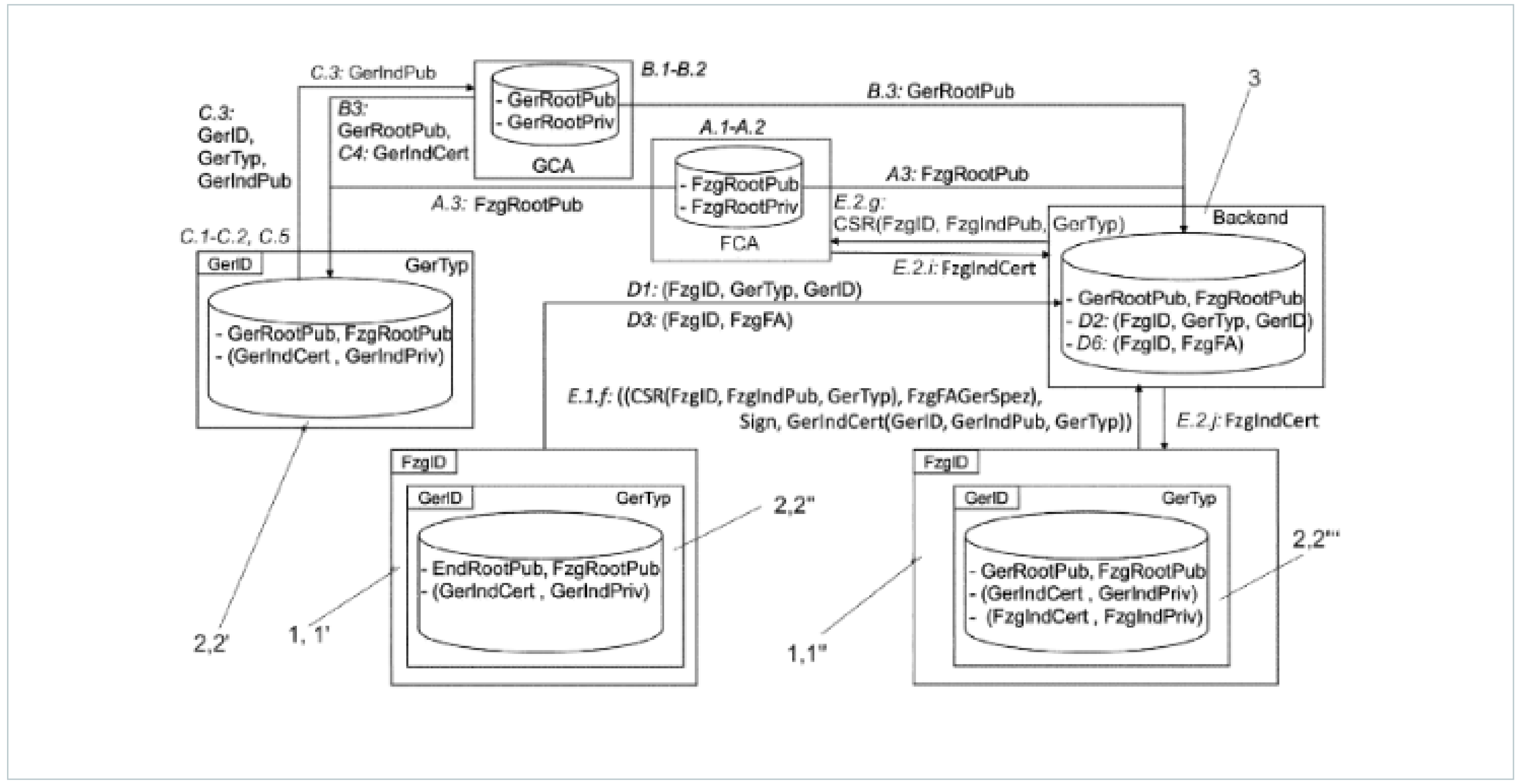
The invention addresses the unauthorized unlocking of car doors through hacking in-vehicle networks (CAN). The invention offers a solution to prevent such attacks by verifying data transmitted within the car. Existing methods using message authentication or encryption are slow or have limitations. The invention proposes a two-step process with a shared encryption key between car control units. It briefly interrupts communication between control units to generate encryption information, then resumes communication and transmits encrypted requests. This allows verification of data and prevents spoofing while maintaining responsiveness for door unlocking and other car controls.

EP4193567B1

Method for securely equipping a vehicle with an individual certificate

Company name	Mercedes Benz Group AG
Inventors	Held Albert, Friesen Viktor, Meidlinger Daniel, Dettling Matthias
Priority date	07 Aug 2023
Publication date	03 Apr 2024

Summarized by Dennemeyer



This invention describes a new method for securely equipping a vehicle with a unique certificate for communication within a vehicle ecosystem. Traditionally, a central authority issues certificates for car parts, but this had limitations. Here, two separate authorities are set up, one for car parts and one for vehicles. Car parts get pre-certificates during manufacturing, and when installed in a vehicle, a secure record links the part to the specific car. The car part then generates a unique key for the car and requests a final certificate from the vehicle authority, ensuring the private key never leaves the car part.

Dennemeyer
The IP Group

Thank you.

You want to know more? Visit us on www.dennemeyer.com

Contact us at

Dennemeyer India Private Limited

☎ 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, Dennemeyer 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.