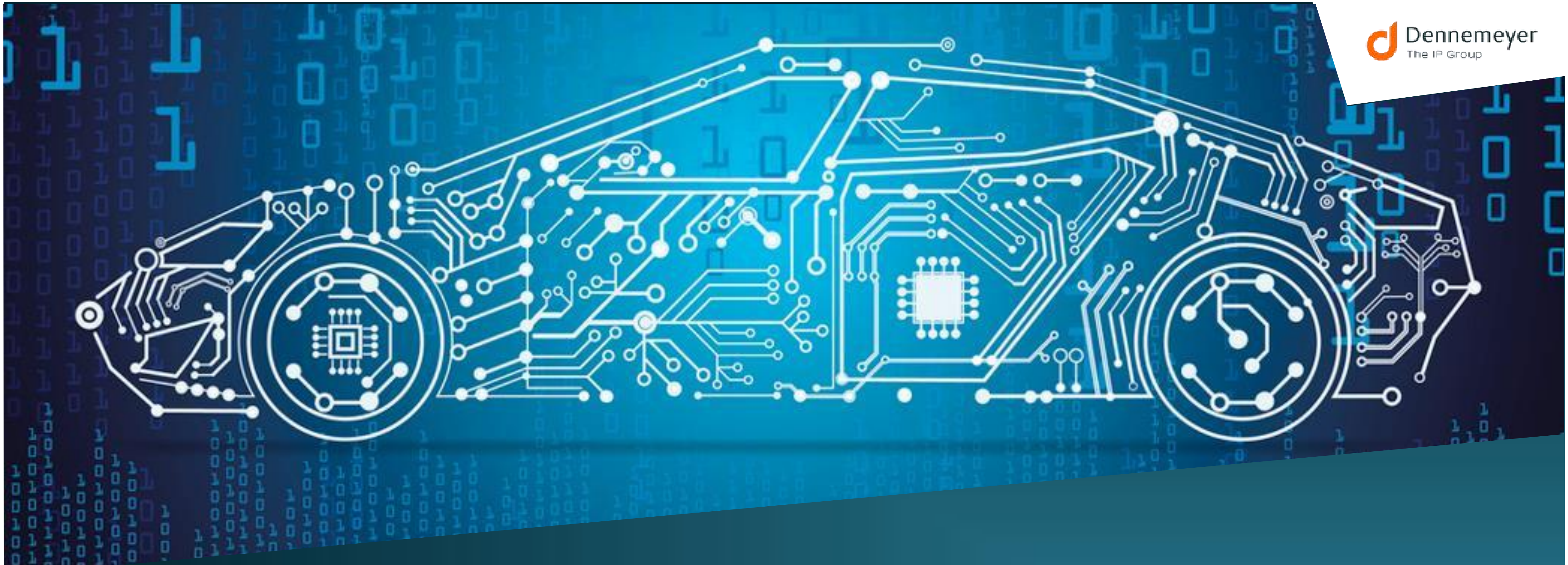


Cybersecurity in Mobility

February 2024 Report

Published by: Dennemeyer India Private Limited

Contact : Parag Thakre
pthakre@dennemeyer.com

scan me

CONTENT

- ❑ Latest News published in January 2024
  - curated and summarized, with reference link to the external source
- ❑ Latest Patents published in January 2024
  - relevant patents shortlisted and summarized, in simple language

LATEST NEWS

(Curated and summarized by analyst)

Telsa Hacked - Zero-Days Unveiled in Automotive Cybersecurity

At a cybersecurity hacking event Pwn2Own Automotive 2024 , a hacking company Synaktive, enabled malicious actors to remotely control a Tesla vehicle. They also hacked Ubiquiti Connect EV Station and the JuiceBox 40 Smart EV Charging Station. The findings of Pwn2Own Automotive event carry significant repercussions and escalate necessity for strong cybersecurity in the automotive sector. The event has set a crucial 90-day deadline for vendors to develop and release security patches for the discovered vulnerabilities.

Source: codelock.it

Industry leaders unite to pioneer next-generation Automotive and Mobility security solution

The automotive industry needs to comply with UNECE's WP.29 and ISO 21434 for the security lifecycle of automobiles. As part of its security strategy, the automotive industry needs to cover all three phases of a vehicle's lifecycle: design development, manufacturing, and operation. Argus Cyber Security, CyberArk, Device Authority, and Microsoft are joining forces to address the complex challenges of securing connected vehicles, ensuring data sovereignty, management, compliance, and safeguarding cloud and enterprise environments by leveraging the latest Azure OpenAI Security Co-pilot technologies from Microsoft.

Source: argus-sec.com

New Automotive Cybersecurity Documents in Development

SAE and ISO are jointly developing two new documents for automotive cybersecurity, specifically introducing a new concept and providing additional guidance relative to the ISO/SAE 21434 Road Vehicles - Cybersecurity Engineering standard. The Vehicle Cybersecurity Systems Engineering Committee is developing this work, which covers Cybersecurity Assurance Level (CAL) and Targeted Attack Feasibility (TAF) processes, as well as Verification and Validation (V&V).

Source: www.sae.org

ETAS and Rambus plan joint development of automotive cybersecurity solutions

ETAS and Rambus are co-developing a security offering for the automotive industry by combining Rambus RT-640 embedded hardware security module (eHSM) IP integrated with the ETAS SoC security software solution ESCRYPT CycurSoC. From chip to cloud, this solution helps improve the security of automotive SoCs, strengthen overall security, and provide a solid trust foundation for defense-in-depth strategies.

Source: etas.com

VicOne and Primax Partner to Improve Efficiencies in Protecting Intelligent Fleet Management and Applications Platform

VicOne (automotive cybersecurity solutions provider) will provide xZETA, security scanning and SBOM (software bill of materials) management tools, for enhancing the cybersecurity protection of Primax's QCS6490-based IoT gateway platform, used for fleet management. ViceOne's xZeta will provide continuous monitoring of Primax's IoT platform and reports if any anomaly is identified.

Source: vicone.com

Smart Eye and Green Hills Software Collaborate on Production-Focused, AI-Driven, Driver Monitoring System (DMS) Platform for Vital In-Cabin Vehicle Safety Systems

Smart Eye (Provider of Human Insight AI) and Green Hills Software (embedded safety and security) are developing integrated DMS platforms for rapid Tier 1 and OEM adoption and use. Automakers can rapidly create and deploy essential safety- and security-critical automotive in-cabin applications using the DMS platform. The DMS platform integrates Smart Eye's core DMS software with the ASIL-certified INTEGRITY® RTOS from Green Hills to detect driver behavior.

Source: ghs.com

LATEST PATENTS

(Shortlisted and summarized by analyst)

- US20240007859A1 - Detecting spoofed ethernet frames within an AUTOSAR
- US2024021028A1 - Method of preventing vehicle controller from being hacked and system thereof
- WO2024018683A1 - Intrusion detection device and intrusion detection method
- WO2024014159A1 - Onboard device, road-side equipment, vehicle-exterior device, security management method, and computer program
- WO2024014252A1 - Theft prevention device and theft prevention method
- IN202341083301A - System and method for blockchain-based integration of renewable energy sources and electric vehicles

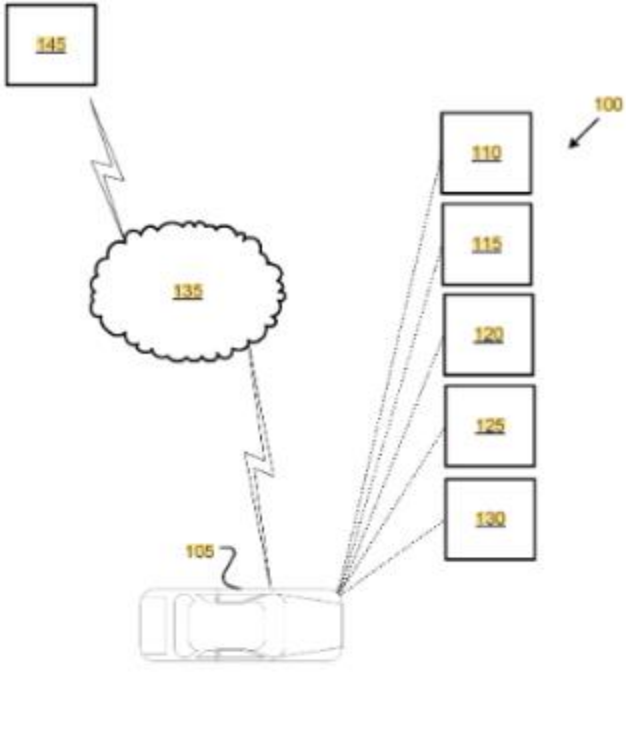
- ❑ IN202341089574A - An IoT based electric vehicle charging station intrusion detection system using machine learning
- ❑ EP4307609A1 - System and method for decentralized intrusion detection system
- ❑ EP3828502B1 - Computer-implemented method and apparatus for detecting spoofing attacks on automated driving systems
- ❑ CN117425153A - Risk detection method and device for Internet of vehicles terminal

US20240007859A1- Detecting spoofed ethernet frames within an AUTOSAR communication stack

Assignee	GM Global Technology Operations LLC
Inventors	Mohamed A. Layouni, Vinaya Rayapeta, Manohar Reddy Nanjundappa, Thomas M. Forest, Karl Bernard Leboeuf
Dates	Priority date: 29-Jun-2022 Publication date: 04-Jan-2024

Summary

The invention relates to determining whether one or more Ethernet frames within an Automotive Open System Architecture (AUTOSAR) communication stack have been spoofed. The ethernet interface is connected to the device drivers of the vehicle controller or Electronic control unit (ECU) to receive the Ethernet frames transmitted from the AUTOSAR communication stack. The device driver compares the source MAC address of the received ethernet frame to a list of authorized source MAC addresses stored in a database. If the extracted source MAC address is not contained in the list, the device driver identifies the Ethernet frame as spoofed and transmits a cancelation command.



Back

US2024021028A1 - Method of preventing vehicle controller from being hacked and system thereof

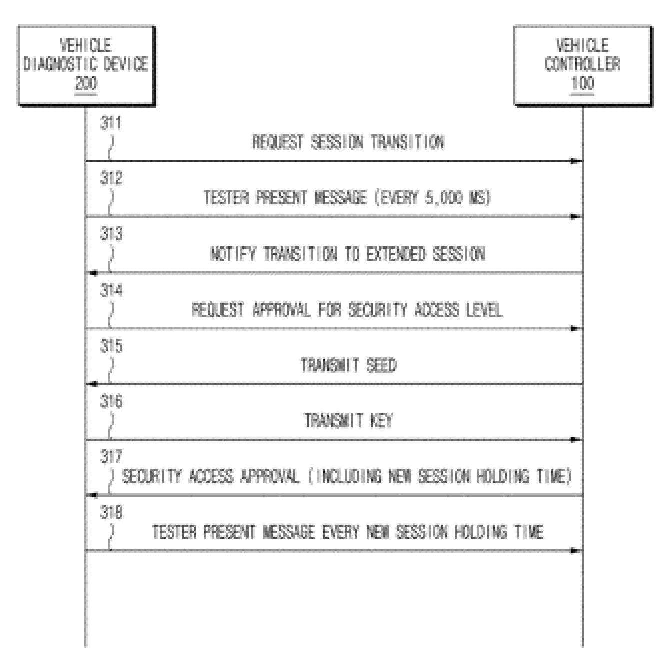
Assignee Hyundai Motor Company, Kia Corporation

Inventors Ho Jin Jung

Dates Priority date: 18-July-2022
Publication date: 18-Jan-2024

Summary

The invention relates to preventing a session interruption between a vehicle diagnostic device and a vehicle controller (e.g., an Electronic control unit (ECU)). The vehicle diagnostic device is connected to an On-board diagnostic (OBD) Connector in the vehicle, to access the security of the Electronic control units (ECUs). When the vehicle diagnostic unit is connected to the OBD port, the ECUs transition from the lock state to the unlock state for a predetermined session timing. Hackers use this active session to hijack ECUs by connecting a hacking tool to the OBD connector and to stop session hijacking, dynamic session timing is used. Since hackers don't know what the dynamic session timing is, they can't hack the ECUs if they don't get the request within the session timing.


VEHICLE DIAGNOSTIC DEVICE 200
VEHICLE CONTROLLER 100
311
REQUEST SESSION TRANSITION
312
TESTER PRESENT MESSAGE (EVERY 5,000 MS)
313
NOTIFY TRANSITION TO EXTENDED SESSION
314
REQUEST APPROVAL FOR SECURITY ACCESS LEVEL
315
TRANSMIT SEED
316
TRANSMIT KEY
317
SECURITY ACCESS APPROVAL (INCLUDING NEW SESSION HOLDING TIME)
318
TESTER PRESENT MESSAGE EVERY NEW SESSION HOLDING TIME

← Back

WO2024018683A1 - Intrusion detection device and intrusion detection method

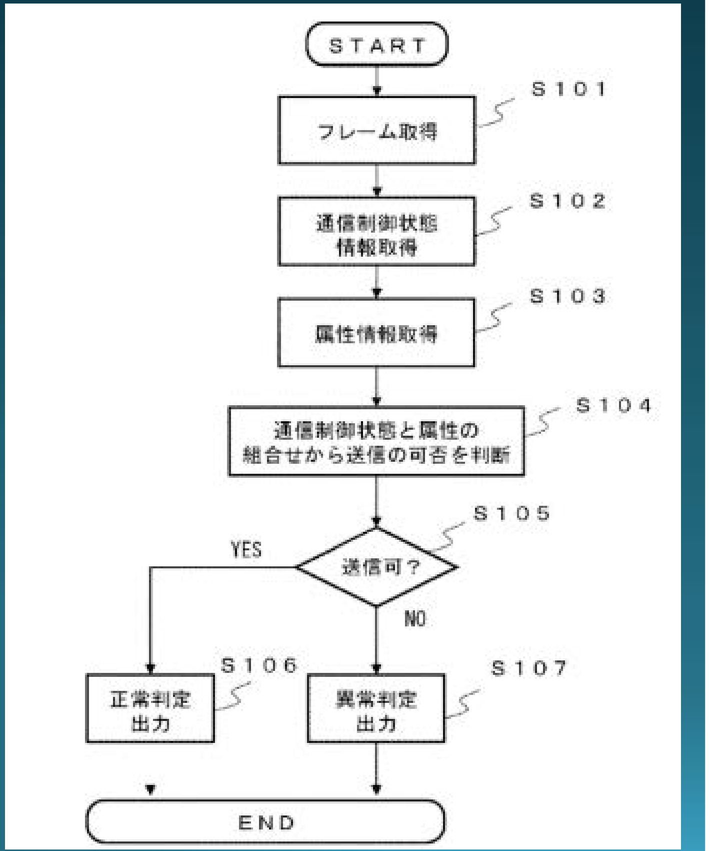
Assignee HITACHI ASTEMO LTD

Inventors NOMURA Teruaki, MORITA Nobuyoshi, KANEKO Shuhei, FUJII Yasuhiro, KATAOKA Mikio

Dates Priority date: 20-July-2022
Publication date: 25-Jan-2024

Summary

The invention is about detecting unauthorized communication in a vehicle using an intrusion detection device (IDS) and an abnormality detection device. The IDS receives and sends frames to and from an in-vehicle electronic device and determines the attributes of the frame and the current state of the electronic unit. The abnormality detection device then identifies abnormalities in an electronic unit based on the data provided by the IDS. Even if the number of frames transmitted per unit of time is within a predetermined range, it can detect unauthorized communication.



Back

WO2024014159A1 - Onboard device, road-side equipment, vehicle-exterior device, security management method, and computer program

Assignee | Sumitomo Electric Industries, Autonetworks Technologies Ltd, Sumitomo Wiring Systems

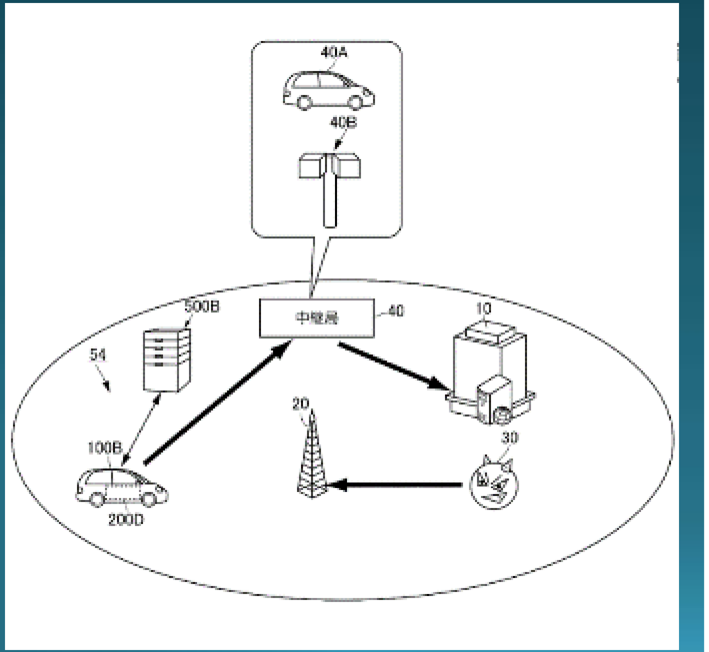
Inventors | Ogawa Akihiro, Kakito Kazuhiro

Dates | Priority date: 15-July-2022
Publication date: 18-Jan-2024

Summary

The invention relates to detecting a cyberattack on a vehicle using a device mounted on the vehicle. The in-vehicle device can communicate with the outside of the vehicle by using multiple wireless interfaces. When the attack detection unit detects a cyberattack on one of its wireless interfaces, it switches the destination route through the relay station to provide a more secure communication path. In turn, cutting off the attack path of the cyberattack.

.



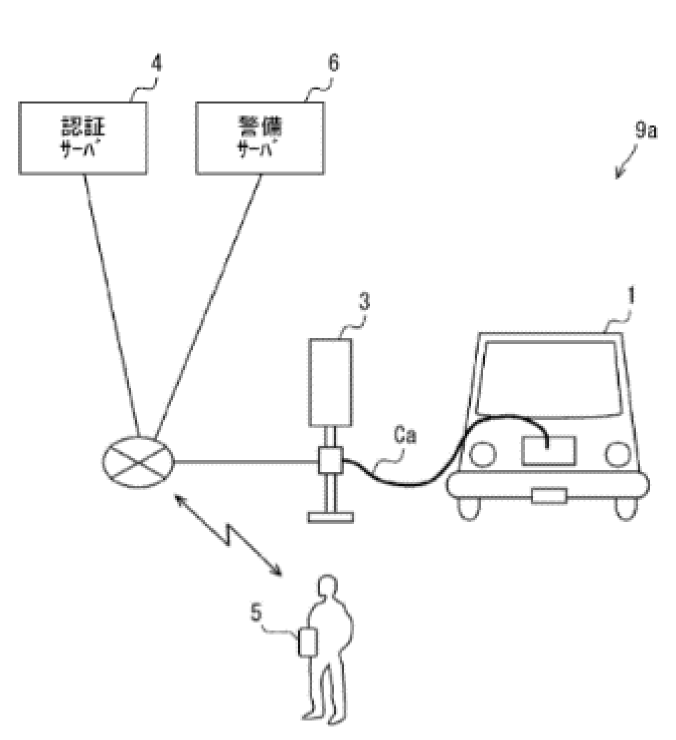
← Back

WO2024014252A1 - Theft prevention device and theft prevention method

Assignee	DENSO CORP
Inventors	Kanda Takayuki; Kubo Shunichi; Shamoto Michio; Takatsu Masahiro; Takehara Kota
Dates	Priority date: 15-July-2022 Publication date: 18-Jan-2024

Summary

The invention relates to providing theft countermeasures that make it easier to recover a stolen electric vehicle. Electric vehicle charging stations are connected to an authentication server, which has the identification information of the authorized users as well as the registered identification information of a stolen vehicle. The authentication server performs the authorization on the vehicle's identification number before it allows it to charge at a charging station. If the identification number is registered as stolen, driving operations/functions of the vehicles are disabled.



Back

IN202341083301A - System and method for blockchain-based integration of renewable energy sources and electric vehicles

Assignee GITAM School of Technology

Inventors K Sravan Kumar;
P H J Venkatesh

Dates Priority date: 06-Dec-2023
Publication date: 05-Jan-2024

Summary

The invention talks about blockchain-based peer-to-peer energy transfers between renewable energy sources and owners of electric vehicles through a decentralized energy nexus (DEN) platform. By using blockchain and smart contracts, DEN makes energy transfers transparent and automated. Blockchain networks record and verify energy transactions, making them secure, transparent, and tamper-proof. Additionally, DEN offers an energy tokenization system that incentivizes participation in the renewable energy ecosystem by trading surplus energy tokens on a marketplace.

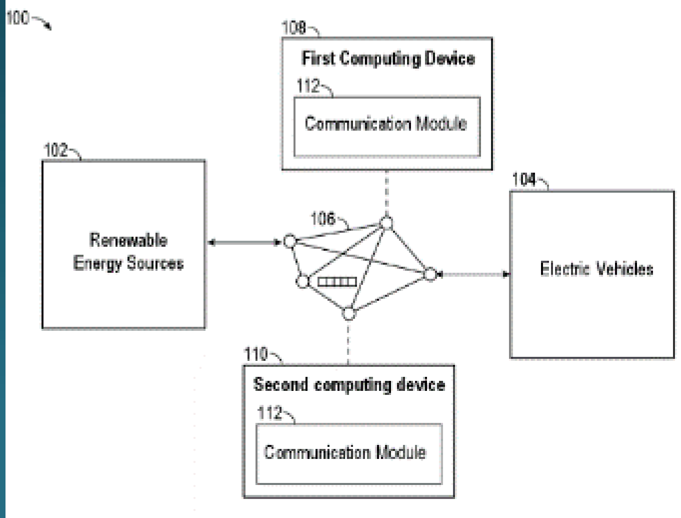


FIG. 1

Back

IN202341089574A - An IoT based electric vehicle charging station intrusion detection system using machine learning

Dennemeyer
The IP Group

Assignee CVR College Of Engineering

Inventors Mr D Shyam Prasad; Ms Y Divya; Dr Venkata Krishna Odugu;
Dr B Janardhana Rao; Dr Gade Harish Babu; Mr B Satish

Dates Priority date: 28-Dec-2023
Publication date: 12-Jan-2024

Summary

The invention relates to a system for detecting intrusions in Electric Vehicle Charging stations (EVCS) based on the Internet of Things (IoT). The intrusion detection system (IDS) uses machine learning based on classifier technique, to identify fraudulent traffic in an IoT setting. The goal of the ML algorithm is to increase classification accuracy by studying the patterns of behavior in both benign and malicious network traffic.

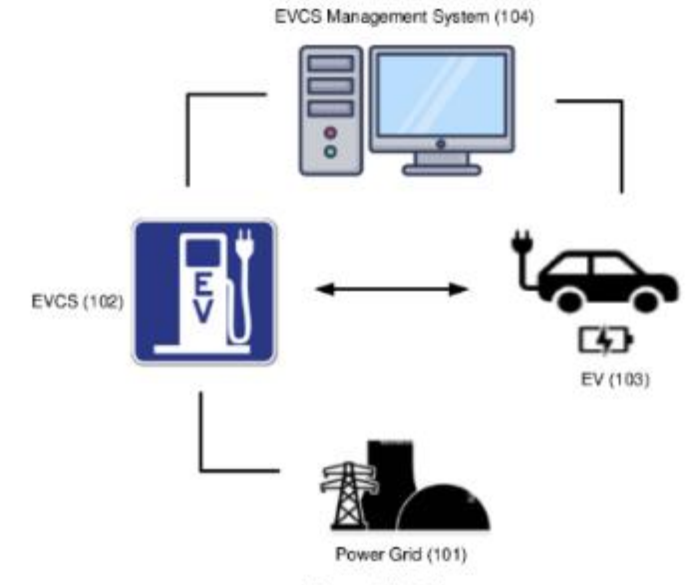


Figure 1 (100)

← Back

EP4307609A1 - System and method for decentralized intrusion detection system

Dennemeyer
The IP Group

Assignee	Argus Cyber Security Ltd
Inventors	Zlatokrilov, Haim
Dates	Priority date: 14-July-2022 Publication date: 17-Jan-2024

Summary

The invention relates to detecting an intrusion into an in-vehicle network by using a decentralized intrusion detection system (IDS). The electronic control units (ECUs) and sensors of a vehicle have an agent (i.e., an executable code), which sends relevant data to IDS for further processing and detecting if an intrusion has happened. For example, IDS can identify that several ECUs are receiving login requests from the same source (based on the data shared by the agents), which may cause the IDS to know that a hacker is attempting to login to the ECUs.

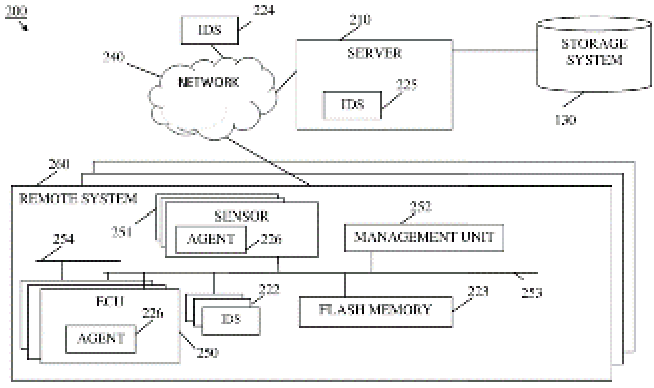


Fig. 2

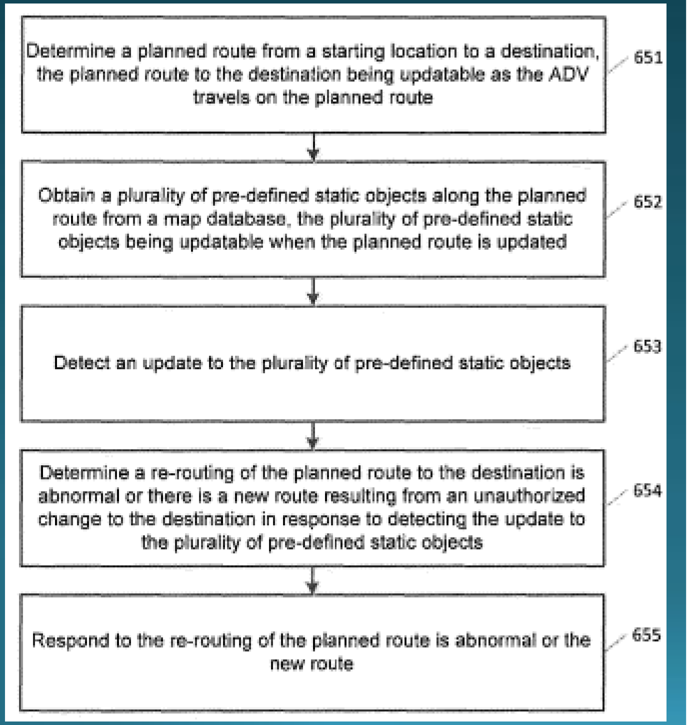
Back

EP3828502B1 - Computer-implemented method and apparatus for detecting spoofing attacks on automated driving systems

Assignee	Baidu USA LLC
Inventors	Liu Xiaodong, Qu Ning
Dates	Priority date: 15-Sep-2019 Publication date: 31-Jan-2024

Summary

The invention relates to detecting and mitigating cyber-attacks and spoofing attacks on autonomous driving vehicles (ADVs). ADVs use pre-defined static objects along their planned routes of travel to detect and counter attacks that change their destinations/routes. When the ADV goes through the route, it scans the static objects along the route and determines if they match the static objects available on the planned route. If not, then it checks if the objects are updated before the trip ends. When the static objects are updated, passengers will be notified that the route/destination has changed. If the passenger does not confirm the destination change or there is no passenger in the vehicle, it may report the suspicious destination change to a service provider.



Determine a planned route from a starting location to a destination, the planned route to the destination being updatable as the ADV travels on the planned route

Obtain a plurality of pre-defined static objects along the planned route from a map database, the plurality of pre-defined static objects being updatable when the planned route is updated

Detect an update to the plurality of pre-defined static objects

Determine a re-routing of the planned route to the destination is abnormal or there is a new route resulting from an unauthorized change to the destination in response to detecting the update to the plurality of pre-defined static objects

Respond to the re-routing of the planned route is abnormal or the new route

Back

CN117425153A - Risk detection method and device for Internet of vehicles terminal

Assignee
Xinhua San Network Information
Security Software Co ltd

Inventors
LI Mingchun; Liang Liwen

Dates
Priority date: 18-Dec-2022
Publication date: 19-Jan-2024

Summary

The invention relates to a risk detection method for a vehicle networking terminal, where risk detection and protection are cooperatively performed by the connected vehicle terminal and a server. The connected vehicle terminal needs to collect data and report it to the server. The server has excellent computing capabilities to detect whether the vehicle networking terminal has a security risk event or not based on a deep learning algorithm. Once a security risk event is detected, the server remotely calls the vehicle networking terminal to execute a protection strategy.

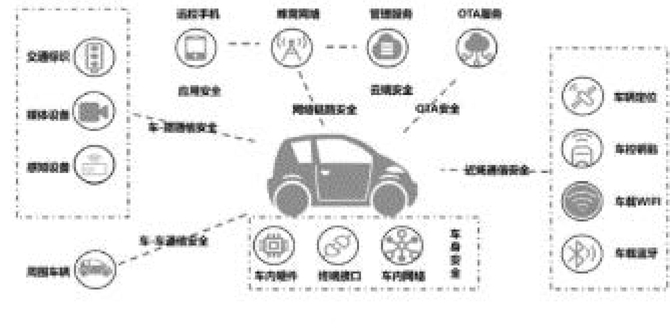
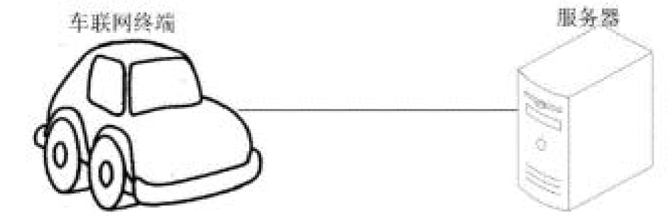


图1



Back

Dennemeyer
The IP Group

Thank You

To know more about us please visit

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.