

Report of February 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.

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.

Key Insights

- ❑ VicOne's partnerships with MediaTek and NXP Semiconductors have introduced xCarbon, an AI-powered system that efficiently detects and stops cyber threats while using very little CPU and memory, highlighting a trend towards lightweight, AI-driven cybersecurity for future automotive safety and connectivity.
- ❑ At the 2025 Pwn2Own Automotive Security event in Tokyo, researchers uncovered multiple security flaws in Tesla's EV chargers. They also found vulnerabilities in car operating systems and in-vehicle infotainment (IVI) systems from various other vendors. These findings highlight the urgent need for stronger cybersecurity measures in the automotive sector.
- ❑ To enhance automotive cybersecurity through certifications and regulations, NVIDIA's autonomous vehicle (AV) platform, DRIVE AGX™ Hyperion, has successfully passed TÜV SÜD and TÜV Rheinland assessments, two of the industry's leading authorities for automotive safety and cybersecurity. This ensures future readiness for the automotive OEMs.
- ❑ Patents published in the last month address in-vehicle communication vulnerabilities. One approach uses lightweight devices called telematics boxes (T-BOX) to monitor the network flow and compare it with pre-set rules. Another approach involves vehicle communication interfaces (VCI) that connect directly to the vehicle's communication port. This ensures that the electronic control units (ECUs) within the vehicle can interact securely without needing to be constantly connected to diagnostic tools.

Nvidia's Cybersecurity Milestone

NVIDIA DRIVE Hyperion Platform Achieves Critical Automotive Safety and Cybersecurity Milestones for AV Development

NVIDIA's autonomous vehicle (AV) platform, called NVIDIA DRIVE AGX™ Hyperion, has passed automotive cybersafety assessments by TÜV SÜD and TÜV Rheinland, two of the industry's leading authorities for automotive safety and cybersecurity. The platform, featuring NVIDIA DriveOS automotive operating system, a set of sensors, and a safety systems, is being adopted by OEMs like Mercedes-Benz, JLR, and Volvo Cars. DRIVE Hyperion's design is modular and upgradeable, ensuring it works with future systems. This achievement shows NVIDIA's dedication to improving AV safety and innovation, paving the way for the future of self-driving cars.

Source

<https://nvidianews.nvidia.com/>



Tesla's Charger Hacked

Tesla Gear Gets Hacked Multiple Times in Pwn2Own Contests

At this year's Pwn2Own automotive hacking contest in Tokyo, researchers successfully hacked Tesla's electric vehicle charger. The event, part of the Automotive World tradeshow, aims to uncover security weaknesses in car technology. PHP Hooligans, a team of cybersecurity researchers, exploited a software bug to take control of the charger, earning \$50,000 and a high score. Another team, Synacktiv, also hacked the charger through the charging connector, winning \$45,000. In total, the organizers paid out \$718,250 in rewards.

Source

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



IVECO Bus Cybersecurity

Digital Security: Iveco Bus At The Forefront Of Protecting Its Vehicles

IVECO BUS is ensuring that their buses and coaches are protected from cyber threats right from the design stage. Their team of technicians and engineers works hard to prevent cyber incidents and keep up with changing regulations. With over 10,000 connected buses, they offer services to optimize fleet management and protect data. They comply with the UN R155 regulation to protect vehicles from cyberattacks. By integrating cybersecurity into the design and employing systems to detect and respond to threats, they maintain secure and connected vehicles. Additionally, regular software updates address new risks, ensuring their buses meet the latest regulations and keep passengers safe.

Source

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



Collaborative Telematic Safety

VicOne and MediaTek demonstrate automotive cybersecurity at CES 2025

At CES 2025, VicOne and MediaTek presented their xCarbon cybersecurity solution for vehicles. This technology focuses on keeping telematics safe, which involves communication, road safety, sensors, and wireless tech. VicOne's xCarbon can detect and stop cyber threats while using very little CPU and memory. They demonstrated how it protects against different attacks, like harmful web access and unknown app execution. This partnership aims to ensure vehicles are secure and connected, addressing the increasing complexity and cyber threats in the car industry.

Source

<https://vicone.com/>



Enhanced AI Security

VicOne Expands Collaboration With NXP Semiconductors to Enable Automakers With Innovative, AI-Powered Services

VicOne is teaming up with NXP Semiconductors, a trusted partner in the automotive market, to enhance vehicle cybersecurity using AI-powered services. Their goal is to improve vehicle protection as the industry shifts toward more AI and software-based services. VicOne's xCarbon intrusion detection or prevention system (IDS/IPS) will work with NXP's OrangeBox platform to monitor vehicle data and security events. This system organizes scattered data into attack paths based on real incidents, using fast AI processing to detect and stop threats.

Source

<https://vicone.com/>





PATENT

The editor's shortlist

Patents of the month

Patents of the month

Published in January 2025

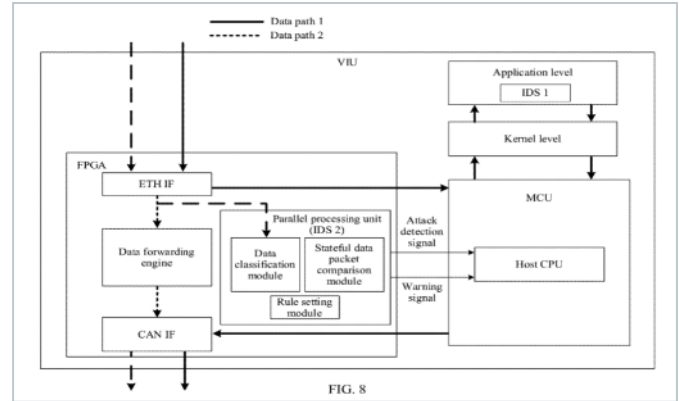


Shortlisted and summarized by our analyst

- [US2025023890A1](#) - Security Detection Method And Apparatus, And Vehicle
Assignee: Huawei Technology Co Ltd
- [US2025026309A1](#) - Systems And Methods For Detecting Vehicle Controller Spoofing
Assignee: GM Global Technology Operations LLC
- [US2025026311A1](#) - Securing Communication Requests From A Vehicle Communication Interface To A Vehicle
Assignee: Volvo Truck Corp
- [US2025039212A1](#) - Fraud Detection Method, Fraud Detection Device, And Recording Medium
Assignee: Panasonic IP Corp Of America Inc
- [IN202441100187A](#) - Enhanced Security and Authentication Framework for Mitigating Attacks in Vehicular Ad-Hoc Networks
Assignee: Koneru Lakshmaiah Education Foundation
- [EP3726796B1](#) - System And Method For Providing Secure In-vehicle Network
Assignee: Hyundai Motor Co, Kia Corp
- [WO2025011539A1](#) - Vehicle-end Dynamic Blockchain-based Information Transmission Method For Internet Of Vehicles
Assignee: Chongqing Univ Of Posts & Telecom
- [JP7612711B2](#) - Attack analysis device, attack analysis method, and program
Assignee: Panasonic IP Corp Of America Inc
- [CN119106712B](#) - Vehicle intrusion detection system and method based on Hybrid EfficientNet model
Assignee: Univ Changchun
- [CN119299226A](#) - Lightweight vehicle-mounted network security defense system
Assignee: Shaanxi Bianyun Collaborative Network Technology Co.,Ltd

◀ US2025023890A1

Security detection method and apparatus, and vehicle



This patent talks about making in-vehicle communication systems safer. Sometimes, harmful data packets can slip through without proper detection, causing vehicles to perform dangerous actions if incorrect data is processed. To tackle this, a multi-level security detection system has been introduced for vehicles. The system starts by getting a data packet and checking it with a security detection device to get a security result. If the result shows that the data packet is a security threat, another data packet is obtained and checked with a different security detection device. Based on the results, the second data packet is either sent through, or the system executes a security instruction to control the vehicle and keep it safe.

Company name Huawei Technology Co Ltd

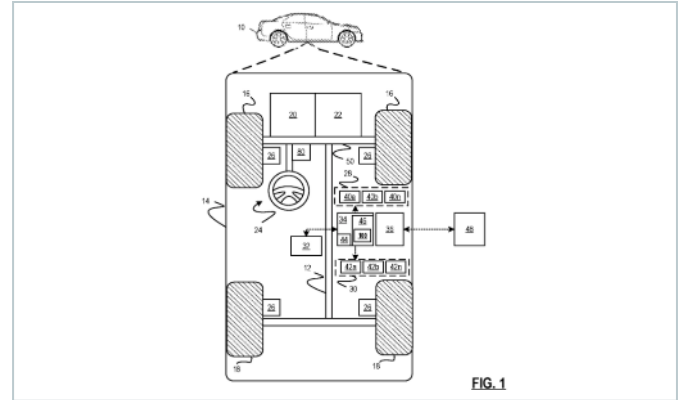
Inventors Wang Chenyu,
Wu Yongzheng,
Wei Zhuo

Priority date 31 Mar 2022

Publication date 16 Jan 2025

◀ US2025026309A1

Systems and methods for detecting vehicle controller spoofing



This patent focuses on preventing vehicle controller spoofing. Spoofing happens when a fake controller pretends to be a real one to get past security measures, leading to attacks on connected vehicles. The solution involves checking the source address of data coming into the vehicle's network against a known, valid address stored in memory. If the address doesn't match, it creates an alert showing that a fake controller is trying to act like a real one by using a different address.

Company name GM Global Technology Operations LLC

Inventors Sunny Ahmed,
Kupfer Samuel B

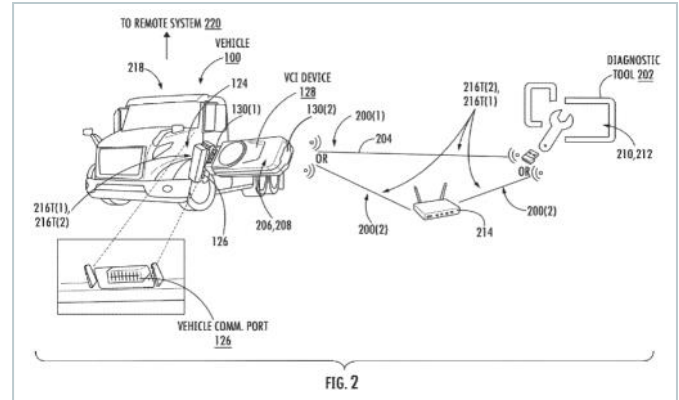
Priority date 19 Jul 2023

Publication date 23 Jan 2025



◀ US2025026311A1

Securing communication requests from a vehicle communication interface to a vehicle



The patent talks about the issue of unauthorized access to vehicle data caused due to unauthorized communication between the vehicle electronic control units (ECUs) and diagnostic tools. The solution is a vehicle communication interface (VCI) device that connects to a vehicle's communication port and supports secure communications with the ECU. The VCI device can receive security features from an authorized diagnostic tool, allowing it to communicate securely with the ECU even when it's not connected to the diagnostic tool. This works because the VCI can authenticate itself using security protocols from the diagnostic tools, allowing it to operate independently without needing a constant connection to the diagnostic tool.

Company name Volvo Truck Corp

Inventors Pastorello Darus,
Maitre Julien

Priority date 20 Jul 2023

Publication date 23 Jan 2025



◀ US2025039212A1

Fraud detection method, fraud detection device, and recording medium

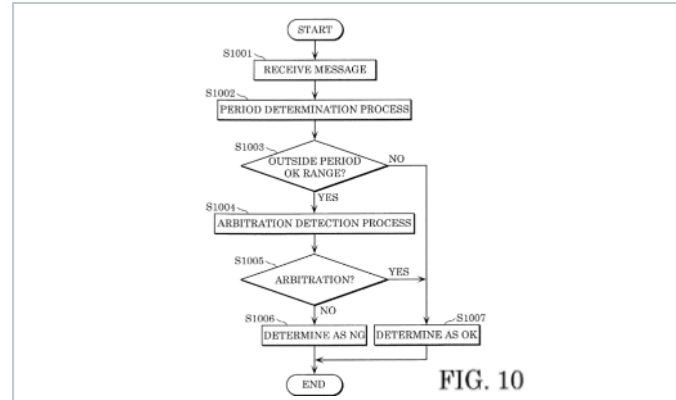


FIG. 10

The patent addresses the challenge of detecting unusual messages in a vehicle's network, especially when normal message timing gets disrupted by disturbances like arbitration. Arbitration decides which message gets priority when multiple messages are sent at the same time. Existing methods may struggle to accurately determine whether a message is real or fake under these conditions. The solution involves checking if a message arrives at the expected time based on the timing of a previous similar message. It also checks if arbitration occurred during this time. The system then assesses whether the start time of arbitration falls within or outside the upper limit of the expected range. By comparing these details, the system decides if the message is normal or abnormal.

Company name Panasonic IP Corp Of America Inc

Inventors Maeda Manabu,
Kishikawa Takeshi,
Kunimune Daisuke

Priority date 29 Mar 2018

Publication date 30 Jan 2025

◀ IN202441100187A

Enhanced security and authentication framework for mitigating attacks in vehicular ad-hoc networks

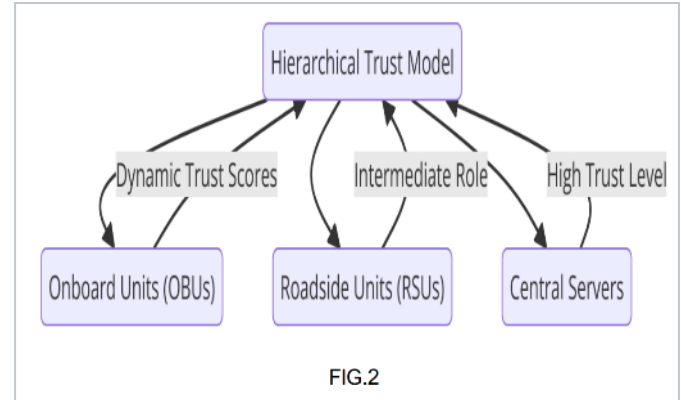


FIG.2

This invention is designed to make connected vehicles safer by addressing security threats in networks that allow vehicles to communicate with each other (known as Vehicular Ad-Hoc Networks or VANETs). These networks can be vulnerable to attacks because they use unsecured channels. To fix this, a new system is needed to ensure secure and efficient communication while detecting and mitigating threats in real time. The solution is a security system that includes a model that assigns trust scores to vehicles, uses lightweight encryption for secure key sharing and digital signatures, detects unusual traffic using machine learning, and employs blockchain for secure logging. It also utilizes multiple authentication methods and ensures low-latency communication for real-time operations.

Company name Koneru Lakshmaiah Education Foundation

Inventors Arun Singh Kaurav,
Dr K Srinivas

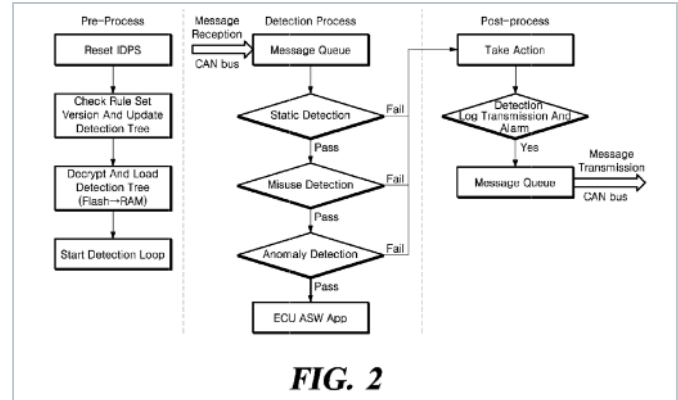
Priority date 17 Dec 2024

Publication date 03 Jan 2025



◀ **EP3726796B1**

System and method for providing secure in-vehicle network



This patent discusses improving security for in-vehicle networks, which are becoming more vulnerable to attacks as more electronic control units (ECUs) are connected via wireless networks. The system works by first collecting a new message from the vehicle's internal network. Then, it decides the best order in which to apply various detection methods to this new message, based on how successful these methods have been at identifying threats in previous messages. The system then uses these detection techniques in the determined order to figure out if the new message poses a security threat.

Company name Hyundai Motor Co, Kia Corp

Inventors Park Seung Wook,
Kim Seil,
Cho Aram

Priority date 19 Dec 2018

Publication date 22 Jan 2025

◀ WO2025011539A1

Vehicle-end dynamic blockchain-based information transmission method for internet of vehicles

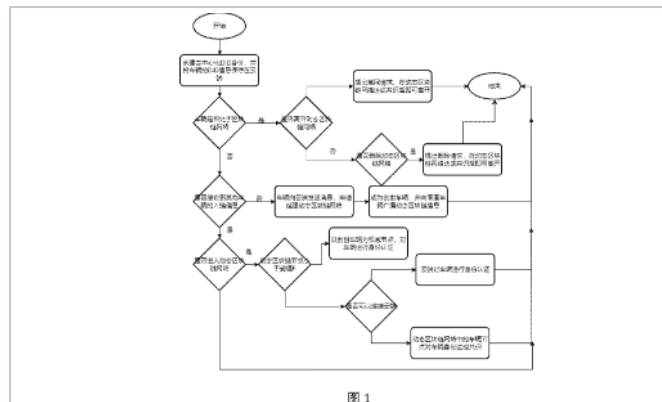


图 1

This patent talks about improving vehicle blockchain systems, which currently face challenges like relying on fixed trusted devices, lacking computing power, and high maintenance costs. The solution allows vehicles to create a flexible blockchain network where each vehicle acts as a node. This means they can participate in secure transactions and manage the blockchain, making the system more secure and resistant to attacks. The network enables vehicles to store, share, and collaborate on data based on agreed rules, which helps with driving and traffic information sharing. The solution also cuts costs because vehicles can use basic software and equipment, eliminating the need for expensive hardware and maintenance. Additionally, with dynamic blockchain and identity checks, vehicles gain more autonomous control over their operations.

Company name Chongqing Univ Of Posts & Telecom

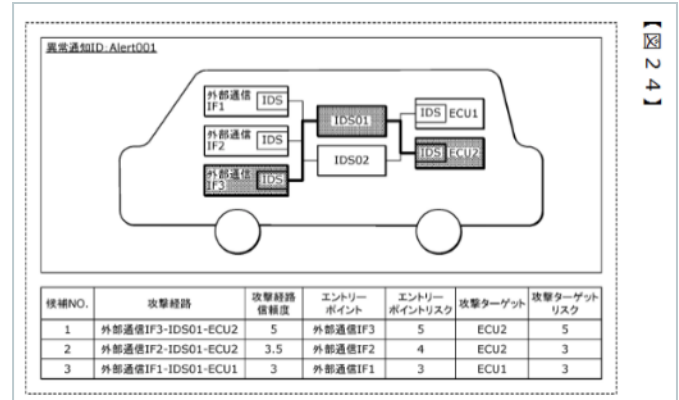
Inventors Chen Qiaosong,
Hu Jie,
Piao Changhao,
Geng Ziyuan,
Yin Zhongyu,
Zhang Xingyu

Priority date 12 Jul 2023

Publication date 16 Jan 2025

◀ JP7612711B2

Attack analysis device, attack analysis method, and program



The patent focuses on analyzing cyber attacks on in-vehicle networks by accurately estimating the attack path. It identifies where the attack starts and what it's targeting. The solution involves a device that collects information about the vehicle network, including details about its configuration, external communication points, and control units (ECUs). It also gathers data on any detected unusual activities in the network. Using this information, the device predicts the cyber attack's route, identifying the entry point as an external communication interface and the attack target as the specific ECU being targeted. This helps in understanding and mitigating potential security threats to the vehicle's network.

Company name Panasonic IP Corp Of America Inc

Inventors Takamitsu Sasaki,
Takashi Ushio,
Hajime Tazaki

Priority date 20 Nov 2020

Publication date 14 Jan 2025

◀ **CN119106712B**

Vehicle intrusion detection system and method based on Hybrid EfficientNet model

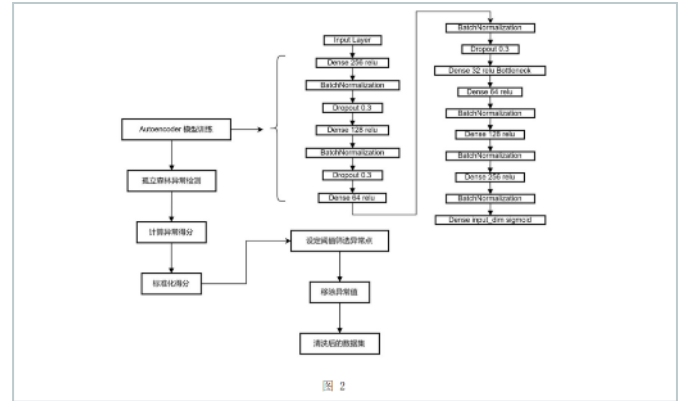


图 2

This patent talks about solving the problems of current vehicle intrusion detection systems, which are often too complicated for vehicles with limited resources. These systems struggle to detect new types of attacks and require a lot of maintenance because they rely on fixed rules. The solution is a new system based on Hybrid EfficientNet models, which use advanced neural networks. These networks combine multiple modules to process data efficiently while still accurately spotting unusual network activities. Key improvements include reducing the system's complexity, balancing efficiency and performance by using different convolutional modules, and enhancing attention mechanisms to better focus on important features during processing.

Company name Univ Changchun

Inventors Wang Shaoqiang, Wang Yizhe, Cheng Jiahui, Su Yu, Dai Yinfei, Sui Yuping, Liu Yubao, Wang Yanbai, Liu Zhiyuan

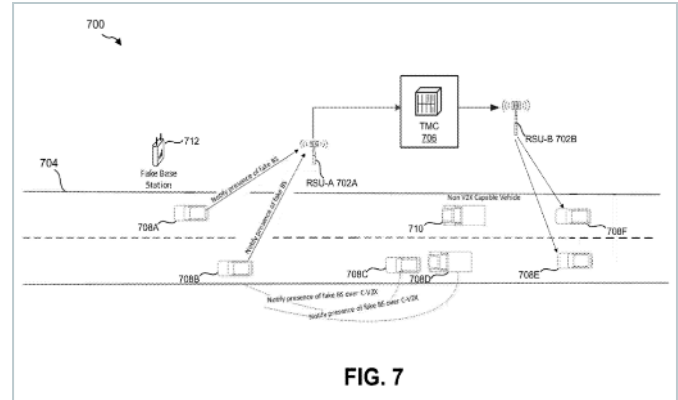
Priority date 01 Nov 2024

Publication date 03 Jan 2025



◀ CN119299226A

Lightweight vehicle-mounted network security defense system



This patent aims to improve safety in connected vehicles by addressing current security issues that can lead to accidents. The solution is a lightweight security system for detecting threats in vehicle data. The system consists of components like a T-BOX (TELEMATICS BOX, remote communication BOX) flow probe, traffic analysis engine, rule base, rule initialization engine, and flow detection engine. The T-BOX flow probe captures network flow from the T-BOX equipment of the automobile. The traffic analysis engine examines the captured network traffic and collects relevant data. The rule base and rule initialization engine store and set up the rules for conducting safety checks. Finally, the flow detection engine carries out these safety checks based on the set rules.

Company name	Shaanxi Bianyun Collaborative Network Technology Co.,Ltd
Inventors	Zhao Xu
Priority date	10-Dec-2024
Publication date	10-Jan-2025

We are now in India

Your global full-service IP partner

With 60 years of experience and 23 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 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
Vargarda, SE
Warsaw, PL
Woking, UK
Zagreb, HR

Talk to us now


Find out how we can support you
in these services and more.

- Patent Renewals
- Trademark Renewals
- Trademark Filing
- Recordals
- PCT Nationalization
- European Patent Validation
- DIAMS IP Management Software
- IP Analytics



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 9818599822

South & West India
+91 88266 88838