INTEC

Co-funded by the European Union

UNIVERSITETI POLIS

BOOK OF PROCEEDINGS

INTERNATIONAL CONFERENCE

SUSTAINABLE MOBILITY

5-6 MARCH

2026

The INTEC International Conference brings together academics, researchers, policymakers and industry experts to discuss innovative approaches and collaborative solutions for a sustainable future in engineering and mobility. The conference will be hosted by POLIS University in Tirana, Albania, and co-organized by partners from across the EU as part of the Erasmus+ CBHE Project 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2.

INTEC International Engineering Competence Centres to push sustainable mobility development in Albania and Montenegro
Project Reference: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Project Partners:

FH JOANNEUM University of Applied Sciences · Frankfurt University of Applied Sciences · UPT · UCG · UDG · AVL · GAMA-AUTO · ALFA Centar

ISBN 9789928347268

DOI: 10.37199/c41001000

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Co-funded by the Erasmus+ Programme of the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Co-funded by the Erasmus+ Programme of the European Union

Partner Universities

Project Coordinator: FH JOANNEUM Gesellschaft mbH (FHJ), Austria
Frankfurt University of Applied Sciences (FRA-UAS), Germany
University of Split (US), Croatia
POLIS University (POLIS), Albania
Polytechnic University of Tirana (PUT), Albania
University of Vlore "Ismail Qemali" (UV), Albania
University of Montenegro (UOM), Montenegro
Adriatic University Bar (FSKL), Montenegro
University of Donja Gorica (UDG), Montenegro
AVL List GmbH (AVL), Austria
Gama Auto d.o.o. (GA), Montenegro
NVO Alfa Centar (AC), Montenegro

Conference Chair

DI Daniela Wenzl
Dr. Elona Karafili
Dr. Flora Krasniqi

Conference Keynote Speaker

DI Horst Pflügl, AVL List GmbH (AVL), Austria
MSc. Mine Bushi, General Directorate of Road Transport Services in Albania

Scientific Committee

Prof. Emeritus Dr. Nataša Gospić, Adriatic University Bar (FSKL), Montenegro
Prof. Dr. Bhavin Kapadia, FH JOANNEUM Gesellschaft mbH (FHJ), Austria
Assoc. Prof. Dr. Ivan Tolj, University of Split (US), Croatia
Prof. Dr. Kristofor Lapa, University of Vlore "Ismail Qemali" (UV), Albania
Prof. Dr. Damir Sedlar, University of Split (US), Croatia
Prof. Dr. Boško Ilija Matović, University of Montenegro (UOM), Montenegro
MA Adrian Millward-Sadler, FH JOANNEUM Gesellschaft mbH (FHJ), Austria
Dr. Anis Sulejmani, Polytechnic University of Tirana (PUT), Albania
Dr. Enkelejd Mëhilli, University of Vlore "Ismail Qemali" (UV), Albania
Dr. Blenard Xhaferraj, Polytechnic University of Tirana (PUT), Albania
Dr. Elona Karafili, POLIS University (POLIS), Albania
Dr. Flora Krasniqi, POLIS University (POLIS), Albania
Dr. Ivana Ognjanović, University of Donja Gorica (UDG), Montenegro

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Co-funded by the Erasmus+ Programme of the European Union

Organizing Committee

DI Daniela Wenzl
Dr. Keti Hoxha
Dr. Flora Krasniqi
Dr. Elona Karafili
MSc. Sadmira Malaj
MSc. Sindi Doce
MSc. Glejdi Fejza

TABLE OF CONTENTS

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Co-funded by the Erasmus+ Programme of the European Union

42

THREAT LANDSCAPE AND MULTI-LAYERED PROTECTION MECHANISMS FOR AUTONOMOUS AND ELECTRIC VEHICLE SYSTEMS

DOI: 10.37199/c41001042

Marko ASANOVIC
Faculty for Traffic, Communication and Logistics, Montenegro
asanovicmarko@live.com

Oliver POPOVIĆ
Faculty for Traffic, Communication and Logistics, Montenegro

Zoran AVRAMOVIĆ
Faculty for Traffic, Communication and Logistics, Montenegro

Nataša GOSPIĆ
Faculty for Traffic, Communication and Logistics, Montenegro

Abstract

Autonomous and electric vehicles represent a key component of modern intelligent transportation systems. However, their increasing connectivity also exposes them to a wide range of cyber threats. This paper analyses the cybersecurity challenges faced by autonomous vehicles operating in VANET and 5G environments, with particular emphasis on attacks targeting vehicle-to-vehicle and vehicle-to-infrastructure communication. Common attack scenarios, such as Sybil attacks, bogus information dissemination, replay attacks, and unauthorised system access, are discussed in relation to real-world incidents. In addition, the paper highlights specific security risks associated with electric vehicles, including battery management systems, charging infrastructure, and software updates. Based on current standards, regulatory frameworks, and practical solutions, a set of recommended multi-layered protection mechanisms is presented.

Keywords: *autonomous vehicles, cybersecurity, regulatory framework*

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Co-funded by the Erasmus+ Programme of the European Union

I. INTRODUCTION

Gartner Information Technology Glossary defines autonomous vehicle (AV) as "one that can drive itself from a starting point to a predetermined destination in autopilot mode using various in-vehicle technologies and sensors, including adaptive cruise control, active steering (steer by wire), anti-lock braking systems (brake by wire), GPS navigation technology, lasers and radar." AV can sense its environment and navigate without a driver, or possibly even without passenger involvement. It can even be discussed if a human passenger is required to be in the vehicle at all.

AVs are rapidly changing transportation; they combine advanced sensors, artificial intelligence (AI), real-time data analysis, and communication with other vehicles and infrastructure. When real-time communication between vehicles and infrastructure occurs, it creates Vehicular Ad Hoc Networks or VANET. These networks coordinate vehicles, influence traffic flow and increase traffic safety. VANET relies on 5G mobile networks for their low latency and high data transfer speeds. However, VANET, like all Ad Hoc Networks, makes users, in this case vehicles, more vulnerable to cyberattacks. Constant data sharing via VANET and 5G mobile networks as data carriers provides hackers with opportunities to access AV communication systems and take control of the vehicle and its hardware, putting passengers and other traffic participants at risk. These safety issues are among the main concerns about using AVs as a regular part of traffic. As stated, VANET is an open Ad Hoc Network that is highly dynamic, with frequent changes in the set of vehicles participating in communication, and frequent messages between all participants, infrastructure nodes, and mobile nodes. This environment is susceptible to various attacks, including Sybil, bogus information dissemination (BID), replay, man-in-the-middle, denial-of-service, and unauthorised system access. Besides the attacks mentioned that take over the vehicle, risks for user privacy and confidentiality are also present.

The following incidents confirm the cybersecurity threats mentioned. Miller and Valasek conducted a Sybil cyberattack as an experiment, resulting in gaining full control over critical Jeep Cherokee functions, including steering, braking, and engine operation. Because of this incident, approximately 1,4 million vehicles were recalled. A ransomware attack in London in 2022 led to the theft of multiple luxury vehicles by exploiting vulnerabilities in keyless entry systems, allowing hackers to enter and gain full control of the vehicles. The attack resulted in the theft of 25 luxury cars. Authors also document other cyberattacks and disruptions that illustrate the consequences of inadequate cybersecurity protection. In addition, electric vehicles introduce additional security challenges related to battery management systems, charging infrastructure, and over-the-air (OTA) software updates.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Co-funded by the Erasmus+ Programme of the European Union

This paper analyses cybersecurity threats targeting autonomous and electric vehicles operating in VANET networks in a 5G environment. The paper proposes one possible approach to increase cybersecurity protection by using a Jump Server as a centralised communication and control point.

1. Architecture of Autonomous Vehicles

The architecture of autonomous vehicles is a four-layer system that includes three logical and one hardware layer, as shown in Figure 1. Logical layers are the perception and localisation layer, the planning and decision layer, the control and actuation layer, and the hardware layer, which is the actual vehicle, also referred to as the vehicle platform.

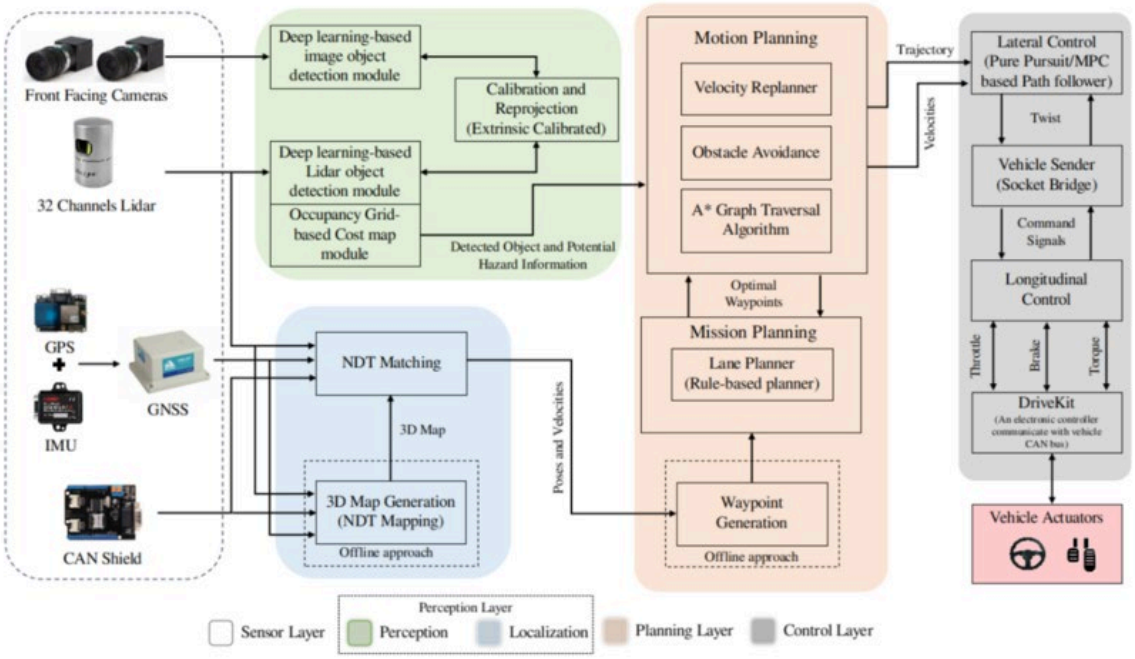

Figure 1. Autonomous vehicle architecture

The perception and localisation layer is responsible for collecting information about the environment, other participants, and vehicle positioning. This layer is the eyes of the vehicle. Various heterogeneous sensors, cameras, radar and LiDAR continuously collect raw data related to road geometry, other vehicles, pedestrians, traffic regulations and environmental conditions, while global navigation satellite systems (GNSS) are used for positioning of the vehicle on a map. From a cybersecurity standpoint, this layer is highly vulnerable to data manipulation attacks, mainly spoofing or false sensor data injection, that interfere with decision-making.

The planning and decision layer is the brain of the AV; it makes decisions on global and situational levels. This layer maps the path from the starting to the end point, and makes real-time decisions

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

based on collected information (change lane, stop for a red light, nudge by a cyclist) using AI and machine learning. This layer represents the critical attack surface, and it is susceptible to unauthorised access, malicious code injection or decision-manipulating attacks.

The control and actuation layer is the vehicle's Nervous system, transferring decisions into specific commands and actions.

The hardware layer, or physical execution layer, transfers control commands into mechanical actions. It also consists of electronic control units (ECU) responsible for steering, braking, and similar actions. ECUs interact with actuators and other vehicle subsystems via in-vehicle communication networks (CAN, FlexRay, automotive Ethernet). ECUs in regular vehicles are isolated; modern/new autonomous vehicles started connecting these networks to an external communication interface to increase response times. This leaves vehicles vulnerable to infotainment unit attacks and control modules.

Apart from the autonomous vehicles' core layers, AVs rely on VANET networks, vehicle-to-vehicle communication and data exchange (V2V) and roadside infrastructure communication (V2I). Vehicles are also connected to other cloud and edge computing platforms for map updates, fleet management or OTA updates. These networks and interfaces enhance vehicle capabilities but also extend trust boundaries beyond the vehicle itself, making secure vehicle communication, authentication and access control a challenge. A successful attack on a single layer can spread across the system, which makes understanding of autonomous vehicle architecture a prerequisite for analysing potential attacks and designing effective multi-layer cybersecurity protection mechanisms.

2. Cyberattack Scenarios in VANET Networks

VANETs are ad hoc networks that support V2V and V2I communication, making VANETs a prerequisite for autonomous driving. In the beginning, VANET was implemented on the IEEE 802.11p amendment to 802.11 (Wi-Fi), which adds wireless access in vehicular environments (WAVE). Although the 802.11p standard provided low-latency local communication, it offered limited scalability, coverage and data speed. The introduction of fifth-generation (5G) mobile networks significantly expands the capabilities of VANETs. 5G mobile networks introduce ultra-reliable low-latency communication (uRLLC), with extremely low latency (less than 1ms) and high reliability up to 99.9999%, enhanced mobile broadband (eMBB), and massive machine-type communication (mMTC). This enables vehicles to interact with roadside units (RSU), edge computing nodes, and cloud platforms, allowing cooperative decision-making and centralised traffic management.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

However, this also introduces new and expands existing attack surface and adds trust challenges. Frequent topology and participant changes, V2V and V2I communication, complicate authentication, authorisation and trust management. Messages are often broadcast to multiple recipients, giving opportunity for spoofing, replay and injection attacks. Integration of VANETs and 5G networks also raises privacy issues, enabling tracking and profiling if adequate access control and authorisation mechanisms are not implemented. Autonomous vehicles depend on cooperative communication, making the confidentiality, integrity, and authenticity of transmitted data essential. VANET networks enhanced by 5G technology enable communication capabilities, cooperative and connected driving and decision-making functions for AVs that can't be achieved through sensor communication alone. However, this, in combination with the complexity and openness of 5G VANET environments, introduces new cybersecurity challenges. Possible attack scenarios in VANET environment differ from those in conventional wired or static wireless networks due to the open, decentralised and highly dynamic nature of these networks. These challenges need to be addressed through security-by-design multilayered mechanisms. One possible solution will be discussed after a review of cybersecurity threats.

Cyber attacks can be generally classified as Active or passive. Active attacks disrupt network availability or information integrity by overwhelming communication channels or infrastructure. In scenarios that involve AVs' loss of communication availability or even quality degradation, impact cooperative functions and forces vehicles to only rely on onboard sensors, reducing system performance. Active attacks include denial of service and distributed denial of service attacks on V2V and V2I communication. Passive attack, focus on data collection without directly altering communication; these attacks pose privacy risks and are usually a preparation for more advanced attacks.

Cyber attacks can also be classified based on their objectives. Attacks can target confidentiality, integrity, availability or authenticity. Attacks that target confidentiality aim to expose sensitive data, attacks that target integrity manipulate message content, attacks on availability disrupt communication services, and attacks on authenticity involve identity spoofing, where vehicles falsely present themselves as authorised entities.

Overall, the diversity and severity of cyberattack scenarios in VANET and 5G environments demonstrate that cybersecurity threats to autonomous vehicles are both realistic and multifaceted. Effective protection requires not only cryptographic mechanisms but also architectural solutions capable of monitoring, controlling, and isolating communication flows. These considerations motivate the need for a centralised and structured protection approach, which is introduced in the following section.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Co-funded by the Erasmus+ Programme of the European Union

3. Attacks on Vehicle-to-Vehicle Communication (V2V)

V2V supports the exchange of critical information, including autonomous vehicle position, speed and driving intention. This communication enables a Sybil attack in which malicious software generates fake identities and simulates the presence of an indefinite number of vehicles. Manipulating this information gives AVs false information about traffic density, vehicle location and distribution. In the end, AVs make bad routing decisions, trigger false congestion alerts and disrupt cooperative driving algorithms.

Another common threat with similar consequences is the **bogus information attack**, where false or manipulated data is intentionally transferred within the network. An example is giving a fake accident warning, an incorrect traffic congestion report, or incorrect road condition data.

AVs influenced by either of these two successful attacks alter driving behaviour, which can further influence other traffic participants due to the nature of V2V communication, meaning one successful attack influences other participants not directly under attack.

4. Attacks on Vehicle-to-Infrastructure communication (V2I)

V2I communication connects AVs with roadside units, traffic control systems, and smart city platforms. This communication is essential for cooperative traffic management, signal optimisation, and perception data. This communication introduces additional attack vectors.

The most common attacks in V2I communication are replay attacks, where previously received valid messages are retransmitted with a time delay to mislead vehicles or infrastructure components. An example is outdated traffic signal information that causes incorrect driving decisions.

Man-in-the-middle attacks are common attacks in 5G environments. An attack allows hackers to intercept, modify or block V2I communication. This attack needs special attention because it can affect multiple vehicles simultaneously, amplifying the attack's impact.

Cyber attacks in VANET and 5G environments differ in diversity and severity. Effective protection requires a multilayered approach that implements more than just cryptographic mechanisms. The need for an architectural solution capable of monitoring, controlling and isolating communication flows increases. In the following section authors introduce a centralised and structured protection approach.

Additionally, electric vehicles (EVs) have their own set of cybersecurity challenges that extend those found in autonomous driving systems, presented in the following paragraph.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Co-funded by the Erasmus+ Programme of the European Union

5. Security Challenges of Electric Vehicles

Electric vehicles introduce a set of cybersecurity challenges that complement and extend those found in autonomous driving systems. In addition to conventional in-vehicle networks and communication interfaces, electric vehicle relies on specialised components such as battery management systems (BMS), electric powertrain controllers, and charging interfaces, all of which are increasingly software-defined and network-connected. Compromise of these components may result not only in data breaches but also in physical damage, reduced battery lifetime, or safety-critical failures. BMS component represents a high-value target that requires strong isolation and access control. Charging infrastructure represents another significant attack surface. Public charging stations interact with vehicles and have access to backend management systems and payment platforms. Charging protocols have significant vulnerabilities that can be exploited to manipulate charging parameters, disrupt service availability or establish unauthorised communication with vehicles.

Over-the-air (OTA) updates are essential for maintaining EV functionality, deploying security patches and adding new features in EVs. However, OTA updates introduce inherent risks of authentication, integrity verification and rollback protection that also need to be addressed. Therefore, an effective protection platform must also consider EV components as an integral element of the overall AV security architecture, rather than as an isolated subsystem.

6. Proposed Protection Mechanism: Jump Server Architecture

To address previously defined cybersecurity threats in VANET and 5G environment, as well as the specific challenges associated with EV subsystems, the authors propose a centralised protection mechanism based on implementing a hardened intermediary device on a network to securely access and manage systems in an isolated, highly restricted security zone. This device is actually the definition of a Jump server architecture. Jump server creates a single-entry point that needs to be secured, monitored and managed for access, reducing attack surface. Jump server acts as a gateway between AVs, roadside infrastructure, EVs, charging systems, and external services such as cloud platforms and fleet management systems. Instead of allowing direct communication, all sensitive interaction is routed through the Jump server. Jump server adds a layer in AV and EV software architecture that concentrates all protection mechanisms at a single control point, limiting attack opportunities.

Introducing an additional layer, a Jump server allows authentication and authorisation policies to be enforced before messages are received or forwarded, significantly reducing the risk of spoofing, Sybil attacks, and bogus information attacks. This also mitigates replay and man-in-the-middle attacks by performing message integrity and reliability checks. Jump server can also implement rate

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

limiting and traffic inspection mechanisms to raise resilience against DDoS and DoS attacks. Jump server operates at the network and application layers, meaning it doesn't replace existing VANET security standards; it amplifies them.

Jump server also directly addresses the cybersecurity challenges of electric vehicles. Communication related to BMS, charging session, and all OTA updates can be treated as high-risk traffic and routed solely through the Jump server. For the charging infrastructure Jump server can validate the charging request, enforce a secure session and monitor abnormalities before they may indicate abuse. This approach reduces the possibility of indirect access to vehicle networks if the charging station used is compromised. For OTA updates Jump server is a verification and control point, allowing only authenticated and verified software packages to be delivered to vehicles. Centralised logging and update validation enable rapid detection of abnormalities and ensure rollback mechanisms in the event of compromised communication.

Jump server also increases incident response capabilities, focusing all communication through a single point, and ensures that all logs and security events are on a single system, enabling real-time monitoring and post incident analysis more easily. Jump server is in compliance with security-by-design principles and international standard ISO/SAE 21434 and UNECE R155 and R156.

Jump server architecture raises scalability and creates single point of failure risks, but these limitations can be mitigated through redundancy, load balancing and distributed deployment across nodes.

While the proposed Jump Server architecture introduces a degree of centralisation that may raise concerns regarding scalability and single-point-of-failure risks, these limitations can be mitigated through redundancy, load balancing, and distributed deployment across edge computing nodes. As such, the architecture provides a practical and scalable foundation for enhancing cybersecurity in autonomous and electric vehicle ecosystems operating in VANET and 5G environments.

7. Example of a Jump server implementation

Jump server is implemented as a secure, virtualised edge node positioned between AVs, EVs, roadside units, charging infrastructure, and cloud-based services. It is implemented as a hardened gateway deployed at the edge of the vehicular communication infrastructure. The server has zero trust security model, where no entity is trusted, regardless of its location.

This Jump server hosts several security functions; it acts as an authentication broker, validating vehicle and infrastructure identities using digital certificates in compliance with PKI (public key infrastructure) applied in V2x communication. This identity-based authentication mechanism

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

operates with minimal latency. Rather than performing full cryptographic handshakes for every message, authentication is applied in a staged manner.

At start-up motor unit establishes a secure session with the nearest Jump server or edge security node. This initial session consists of authentication by using pre-installed cryptographic certificates and is executed only once or at infrequent intervals. Once a session is established, short-lived session keys are generated and cached for communication. Pre-established session keys are used for regular V2V and V2I messages. In latency-sensitive cases, e.g. collision avoidance, local trust decision has priority, vehicles validate message signatures locally and act without delay, while the Jump server performs asynchronous verification and anomaly detection. If malicious behaviour is detected, affected identities are isolated from the network, and revocation information is disseminated.

For a charging session Jump server verifies the charging request, enforces parameter constraints defined by the BMS and monitors session behaviour. Latency has no impact on this process, allowing the Jump server easy communication and monitoring. Any deviation, unexpected power level, abnormal duration, or other triggers alert or cause session termination. For OTA update Jump server acts as a trusted proxy. Software packages are received by the Jump server, verified and then forwarded to vehicles. The Jump server monitors version control, integrity verification and rollback options.

Jump server deployed in this manner integrates traffic inspection and logging mechanisms for VANET and 5G environment. Future work should discuss the deployment of a distributed set of redundant nodes across multiple locations in order to avoid a single point of failure limitation while preserving the benefits of centralised security point enforcement.

Figure 2 presents a model where the Jump server acts as a trusted intermediary between all VANET participants.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Co-funded by the Erasmus+ Programme of the European Union

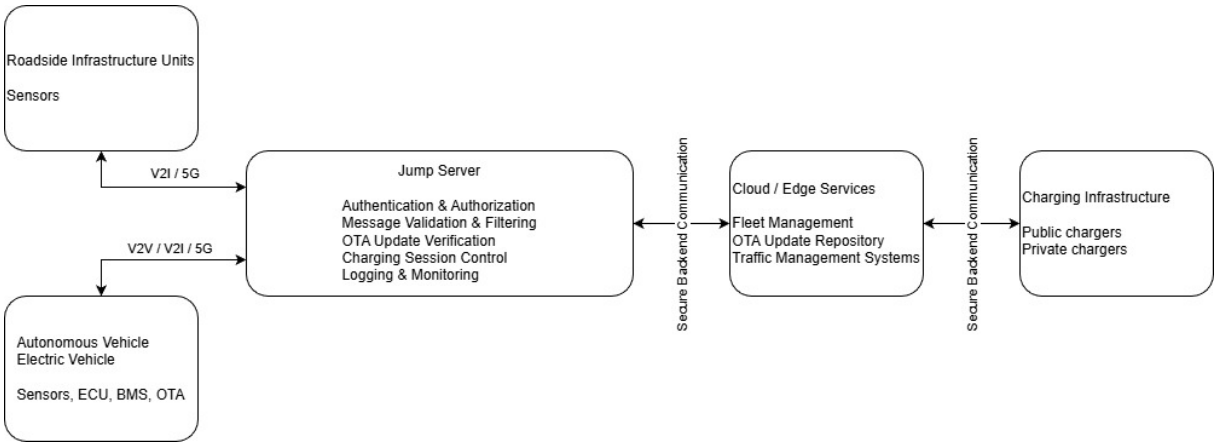

Figure 2. Jump Server architecture

The architecture illustrated in Figure 2 presents one of the possible implementations of the Jump server as an intermediary between VANET participants.

II. DISCUSSION AND CONCLUSION

Cybersecurity in all fields, not only VANET networks, is a major concern. Classification of attack threats and real-world incidents presented clearly shows that risks are not hypothetical. Vehicle-centric security mechanisms are insufficient in highly dynamic and distributed communication environments. Sybil, bogus information dissemination, replay, and DDoS attacks exploit the decentralised nature of VANET and can affect multiple vehicles simultaneously. Additional vulnerabilities are introduced with AVs being electric vehicles. These challenges require a security solution that extends beyond the individual vehicle and that addresses the system. This paper proposed a Jump server-based architecture as a centralised control. By routing sensitive communication through a secure intermediary, the proposed approach reduces the surface and enables consistent enforcement of authentication and authorisation. It is important to note that this architecture addresses both the VANET environment and the EV-specific risks, including charging and OTA update management.

While the introduction of a Jump Server introduces additional architectural complexity and potential scalability concerns, these limitations can be mitigated through distributed deployment, redundancy, and integration with edge computing infrastructure.

In conclusion, effective cybersecurity for autonomous and electric vehicles requires a holistic and architectural approach rather than isolated protective measures. The Jump Server–based architecture presented in this paper provides a practical and scalable foundation for enhancing security in VANET and 5G-enabled vehicle ecosystems. Future work should focus on experimental

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

validation of the proposed architecture in real or simulated vehicular environments, performance evaluation under heavy traffic loads, and integration with AI-based intrusion detection mechanisms to further improve system resilience. Future work should also analyse the implementation of a firewall on the endpoint nodes as one of the possible solutions.

REFERENCES

Azam, S. & Munir, F. & Sheri, A. & Kim, J., & Jeon, M (2020). *System, Design and Experimental Validation of an Autonomous Vehicle in an Unconstrained Environment.* Sensors. 20. 5999. 10.3390/s20215999.

Buchholz, M., Strohbeck, J., Adaktylos, A.-M., Vogl, F., Allmer, G., Barros, S. C., Lassoued, Y., Wimmer, M., Hätty, B., Massot, G., Ponchel, C., Bretin, M., Sourlas, V., & Amditis, A. (2020). *Enabling automated driving by ICT infrastructure: A reference architecture*. arXiv:2003.05229. https://arxiv.org/abs/2003.05229

California Department of Motor Vehicles. (2022). *Autonomous vehicle collision and disengagement reports: Cruise LLC.* https://www.dmv.ca.gov

Etukudoh, E. A., & Sonko, O. (2024). A comprehensive review of embedded systems in autonomous vehicles: Trends, challenges, and future directions. *World Journal of Advanced Research and Reviews*, *21*(1), 1640–1655. https://doi.org/10.30574/wjarr.2024.21.1.0268

Europol. (2022). *Spotlight on vehicle crime: Keyless theft and cyber-enabled vehicle crime.* Publications Office of the European Union. https://www.europol.europa.eu

Garikapati, D., & Shetiya, S.S. (2024). *Autonomous Vehicles: Evolution of Artificial Intelligence and the Current Industry Landscape.* Big Data and Cognitive Computing, 8(4), 42-67.

International Organisation for Standardisation & SAE International. (2021). *Road vehicles — Cybersecurity engineering* (ISO/SAE 21434:2021). https://www.iso.org/standard/70918.html

Llorca, D.F., Hamon, R., Junklewitz, H., Grosse, K., Kunze, L., Seiniger, P., Swaim, R., Reed, N., Alahi, A., Gómez, E., Sánchez, I., & Kriston, A. (2025). *Testing Autonomous Vehicles and AI: Perspectives and Challenges from Cybersecurity, Transparency, Robustness and Fairness.* European Transport Research Review, 17(38), https://doi.org/10.1186/s12544-025-00732-x

Llorca, D. F., Parra, I., Sotelo, M. A., & Sánchez, S. (2025). *Testing autonomous vehicles and artificial intelligence: Challenges and future directions.* European Transport Research Review, 17(4), 1–18. https://doi.org/10.1186/s12544-025-00612-3

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Miller, C., & Valasek, C. (2015). *Remote exploitation of an unaltered passenger vehicle.* In Proceedings of Black Hat USA 2015. Black Hat. https://www.blackhat.com/us-15/briefings.html

National Institute of Standards and Technology. (2020). *Zero trust architecture* (NIST Special Publication 800-207). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207

Raya, M., & Hubaux, J.-P. (2007). Securing vehicular ad hoc networks. *Journal of Computer Security*, *15*(1), 39-68. https://doi.org/10.3233/jcs-2007-15103

Sonko, Sedat & Etukudoh, Emmanuel & Ibekwe, Kenneth & Ilojianya, Valentine & Daudu, Cosmas. (2024). *A comprehensive review of embedded systems in autonomous vehicles: Trends, challenges, and future directions.* World Journal of Advanced Research and Reviews. 21. 2009-2020. 10.30574/wjarr.2024.21.1.0258.

United Nations Economic Commission for Europe. (2021). *UN Regulation No. 155 - Uniform provisions concerning the approval of vehicles with regard to cybersecurity and cybersecurity management system* (E/ECE/TRANS/505/Rev.3/Add.154).

United Nations Economic Commission for Europe. (2021). *UN Regulation No. 156 - Uniform provisions concerning the approval of vehicles with regard to software update and software update management system* (E/ECE/TRANS/505/Rev.3/Add.155)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Co-funded by the Erasmus+ Programme of the European Union

INTEC

Co-funded by the European Union

International conference on sustainable mobility

Agenda

Project title: International Engineering Competence Centres to push Sustainable Mobility Development in Albania and Montenegro
Acronym: INTEC

Work package	
WP11	**International conference**
TASK	
11.4	Coummunity Building Events

Dates	05.03.-06.03.2026
City	Tirana
Meeting venue	POLIS University Entrance Hall
Address	Rr. Bylis 12, Kodi Postar 1051, Kutia Postare 2995, Tirana, Albania

05.03.2026	
Entrance Hall, POLIS University	
8:30 – 9:00	**Registration**
9:00 – 9:30	**Opening Performance**
Welcome session – Auditorium A5 (Ground floor)	
9:30 – 10:00	**Opening Remarks** **Dr. Elona Karafili** (Vice Rector, POLIS University) **Dr. Flora Krasniqi** (Head of Office of Projects and Internationalization, POLIS University) **DI Daniela Wenzl** (INTEC Project Coordinator)
Auditorium A5 (Ground floor)	
10:00 –11:00	**Keynote speakers** **DI Horst Pflügl AVL** Collaborative Research for sustainable Mobility **DPSHTRR Representative** – (General Directorate of Road Transport Services in Albania)
11:15 – 11:30	**Coffee break (Moving into parallel sessions)**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

INTEC
Co-funded by the Erasmus+ Programme of the European Union
INTEC
Co-funded by the European Union

11:30	SESSION 1: POLITICAL AND REGULATORY FRAMEWORK AULA B1	SESSION 2: TECHNOLOGICAL INNOVATION AULA B4
11:30 – 11:45	**Opening Session:** Prof. Emeritus dr Nataša Gospić (FSKL)	**Opening Session:** Associate Prof. Ivan Tolj (US)
11:45 – 12:00	**Integrating Event Data Recorder (EDR) Technology into Sustainable Road Safety Frameworks within the European Green Deal** Eriselda Alimeti, Parid Milo, Mentor Çejku, Anis Sulejmani, Odhisea Koça	**Empirical Comparative Study of Structural CFRP Sandwich Structure Inserts for Out-of-Plane loads** Imre Kovács
12:00 – 12:15	**Infrastructure Readiness for Sustainable Mobility: EU Frameworks and the Case of Albania** Ervin Kalemaj, Parid Milo, Mentor Çejku, Anis Sulejmani, Odhisea Koça	**The Role of Intermodal Transportation for the Sustainable Mobility** Márton Kovács
12:15 – 12:30	**Review of the Evolution of International Ship Energy Efficiency Regulations and the Albanian context** Dr. Blenard Xhaferaj, Doklejda Hodaj	**Impact of Heat Pump Systems on Winter Energy Use and Driving Range in Battery Electric Vehicles** Luis Henrique Pereira Martins
12:30 – 12:45	**Renewable Energy Procurement (CPPA) and Transport Electrification: European Perspectives and Albanian Challenge** Antonio Ndoci, Anis Sulejmani, Odhisea Koça, Mentor Çejku, Parid Milo	**Liquid Cooling Systems for Electric Vehicle Batteries: Improving Safety, Performance and Sustainability** João Miguel de Almeida Ribeiro Silva
12:45 – 13:00	**The Current Status of Autonomous Vehicle**	**Analysis of Battery Charging and Discharging Behavior for Electric Vehicle Applications** Leona Markic, Luka Filipović

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

INTEC
Co-funded by the Erasmus+ Programme of the European Union
INTEC
Co-funded by the European Union

	Technology Adoption in the Balkan Region Darjana Lopičić, Oliver Popović, Miloš Ilić, Bojan Kocić	
13:00 – 14:00	**Lunch**	
14:00 – 14:15	**Reviewing the European Green Deal in Energy, Mobility and Industry** Veselinka Calasan, Ivana Ognjanovic	**Automotive Cooling Systems Sustainability: A Focus on the Expansion Tank** Ana Inês Barbeiro Casimiro
14:15 – 14:30	**The European Green Deal and its National Implementation: From Strategy to Practice** Blerina Bektashi, Andi Bektashi	**Design and Development of a Constant-Volume Combustion Chamber for Optical Investigation of Hydrogen and Water Injection Under Engine-like Conditions** Julius Hollerith, Prof. Dr. Bhavin Kapadia
14:30 – 14:45	**From Prediction to Regulation: Evidence Production Approaches in Autonomous Mobility Research and Their Policy Implications** Sadmira Malaj	**Emission Reduction of Marine Propulsion Systems in SECA Zones Through the Integration of Hydrogen Technologies** Motalleb Miri, Ivan Radaš, Marija Mandić, Ivan Tolj
14:45 – 15:00	**Questions and Discussion**	**A Comprehensive Analysis of Ventilation System for Enhanced Energy Efficiency in Marine Propulsion Applications** Sara Blašković, Gojmir Radica, Jakov Šimunović

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

INTEC
Co-funded by the Erasmus+ Programme of the European Union
INTEC
Co-funded by the European Union

15:00 – 15:15		**Design and Topology Optimization of a Lightweight Chain Sprocket for Electric Motorcycle Applications** Teo Čolović, Ivo Marinić-Kragić
15:15 – 15:30	**SESSION 3: ECONOMIC AND BUSINESS PRESPECTIVES + CASE STUDIES AND GOOD PRACTICES** Aula B1	**Questions and Discussion**
	Opening Session: Dr. Anis Sulejmani (PUT)	
15:30 – 15:45	**Managing Renewable Energy Resources as a Foundation for Sustainable Mobility Transitions** Deivi Sinanaliaj, Martin Bektashi	
15:45 – 16:00	**Feasibility of Electric Bus deployment in Montenegro: A Case Study of Budva (Erasmus+ INTEC / IECC Context)** Anastasija Mrkajic, Vinko Nikic.	
16:00 -16:15	**Children Paths as an Urban Regeneration Strategy: Naim Frasheri Study Case** Dejvi Dauti	
16:15 – 16:45	**Questions and Discussion**	

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

Co-funded by the Erasmus+ Programme of the European Union

INTEC

Co-funded by the European Union

International conference on sustainable mobility

Agenda

Project title: International Engineering Competence Centres to push Sustainable Mobility Development in Albania and Montenegro
Acronym: INTEC

Work package	
WP11	International conference
TASK	
11.4	Coummunity Building Events

Dates	05.03.-06.03.2026
City	Tirana
Meeting venue	POLIS University Entrance Hall
Address	Rr. Bylis 12, Kodi Postar 1051, Kutia Postare 2995, Tirana, Albania

06.03.2026		
First Floor Hall, POLIS University		
8:30 – 9:00	Registration	
9:00– 9:15	**SESSION 4: SOCIAL AND ENVIRONMENTAL IMPACT** AULA B1	**SESSION 5: FUTURE SCENARIOS** AULA B4
9:00 – 9:15	**Opening Session:** Prof. Dr. Bhavin Kapadia (FHF)	**Opening Session:** MA Adrian Millward-Sadler (FHJ)
9:15 – 9:30	**Comparison of Lifecycle Emissions of a SUV with Fuel Cell and Battery Electric Powertrains** - Bhavin Kapadia, Alper Sayin, Sandra Eisenträger	**GENAI Literacy as a Transversal Skill for Emerging Professionals: Implications for Sustainability-Critical Knowledge Work** – Adrian Millward-Sadler
9:30 – 9:45	**Smart Mobility Technologies and their Impact on Urban Sustainability: Insights from**	**Effects of Technical Traffic Calming Measures** – Filip Perović

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

INTEC
Co-funded by the Erasmus+ Programme of the European Union
INTEC
Co-funded by the European Union

	European and Western Balkan Cities – Alma Gjonaj, Vjola Ziu	
9:45 – 10:00	**The Disappearing Squares: Social and Environmental Impacts of Urban Mobility Planning in Durres –** Arjola Sava	**Cybersecurity Vulnerabilities in Electric Vehicle Operating Systems: A Global Awareness Analysis -** Aleksa Radević
10:00 – 10:15	**The City that Demands Continuous Movement: The Disappearance of the Right not to Move within the Framework of Sustainable Mobility –** Avrili Meshi	**Development of a risk assessment model for the transport of hazardous materials using ALOHA and GIS software tools –** Marko Radetić
10:15 – 10:30	**Between Rhetoric and Reality: Discursive Framings, Greenwashing and Outcomes in Sustainable Mobility –** Kejsi Veselagu	**Mapping Distance and Time Leveraging Isochrone Intelligence in Emerging Cities** - Andia Vllamasi, Erjon Cobani
10:30 – 10:45	**Reimagining the City Through Green Mobility Strategies: The Case of Tirana** - Vjola Ziu, Alma Gjonaj	**Can AI develop its Own "Taste" Automotive Design?** - Gregor Andoni, Kristjana Meço
	Coffee Break	
11:00 – 11:15	**Linking Morphology, Perceived Safety, and Sustainable Mobility in Post-Socialist Urban Contexts-** Sindi Doce	**Optimizing Public Transport Corridors Using AI-Based Scenario Modelling: A case Study on Tirana's Ring Road** - Erjon Çobani, Julian Beqiri, Merita Guri
11:15 – 11:30	**Towards Sustainable Transport: A Comparative Analysis of Electric Vehicle Adoption in Montenegro and Albania -** Radmila Milić	**Threat Landscape and Multi-Layered Protection Mechanisms for Autonomous and Electric Vehicle Systems** - Marko Asanovic, Oliver Popović, Zoran Avramović, Nataša Gospić

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2

INTEC
Co-funded by the Erasmus+ Programme of the European Union
INTEC
Co-funded by the European Union

11:30 – 11:45	Questions and Discussion	**Cybersecurity Challenges in Modern Vehicular Communication Networks** - Aleksandar Grgurević, Nataša Gospić, Oliver Popović
11:45 – 12:00		**Green Transition in Albania: Challenges and Future Actions** - Erik Kushta, Andi Hyka, Enea Nasto
12:00 – 12:15	**SESSION 6: CONTROVERSIES AND CHALLENGES** Aula B1 **Opening Session:** Prof. Kristofor Lapa (UV)	**Use of AI in the Process of Green Transformation and Impact on Public Health** - Esmeralda Hamiti, Federika Alliaj, Kristi Metushi
12:15-12:30	**The Adoption of Electric Vehicles in Albania: A Comparative Study with Other Western Balkan Countries** - Doklejda Hodaj, Andrea Lapa	**Development of an Automatic Traffic Sign Detection System Using YOLOv8** - Valentina Vojinović, Luka Filipović
12:30-12:45	**Application of Quality Tools in the Analysis of Factors Influencing the Development of Electromobility in Montenegro** - Jelena Šaković Jovanović, Draško Jovanović, Mirjana Grdinić Rakonjac, Marko Lučić, Miloš Perović, Aleksandar Vujović, Gordana Radulović	**The Historical Development of Artificial Intelligence and Its Influence on the job market in Automotive Engineering** - David Josef Pilgram
12:45 – 13:45	**Questions and Discussion**	**Questions and Discussion**
13:45	**Lunch**	

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them. Project ref.: 101081873-ERASMUS-EDU-2022-CBHE-STRAND-2