


montimage

# Whitepaper: Cyber Secure Communications in Intelligent Transport Systems

November 27, 2024

Edgardo Montes de Oca
edgardo.montesdeoca@montimage.eu
Huu Nghia Nguyen
huunghia.nguyen@montimage.eu

Montimage
https://montimage.eu
39 rue Bobillot
75013 Paris

# Introduction

In Intelligent Transport Systems (ITS), network communication is the backbone that enables connected vehicles, infrastructure, and other systems to interact together in real time. A dependable network communication is critical for facilitating a range of critical functions, from traffic management and collision avoidance to autonomous driving and vehicle-to-everything (V2X) communication. The reliability of the system is based on two key components: secure communication, which ensures data integrity and confidentiality, and deterministic communication, which guarantees predictable and consistent message delivery.

Secure communication is essential in protecting the integrity, confidentiality, and availability of the exchanged data. It involves strong encryption, authentication mechanisms, and access control measures to prevent unauthorized access, data tampering, and cyber-attacks, such as remote vehicle attacks, eavesdropping, or data breaches. It ensures that all transmitted information remains protected from malicious actors and maintains the privacy of users.

Deterministic communication refers to the network's ability to deliver messages within a predictable and guaranteed time frame. This predictability is vital in the context of ITS where delays in communication of applications like autonomous driving or collision avoidance can lead to catastrophic consequences. It eliminates uncertainty and ensures that messages are consistently delivered with bounded jitter or variation in timing, supporting smooth and coordinated operations in a highly dynamic traffic environment.

Together, secure communication and deterministic communication create a reliable network where the data exchanged is both protected from cyber-threats and reliably delivered in real-time, ensuring that connected vehicles can safely navigate and interact within the ITS.

In this whitepaper, we present the cyber-security challenges and potential solutions to achieve dependable ITS network communication. The paper serves as an informative foundation and a starting point for further discussion and collaboration. The primary aim is to outline the current state of cyber-security, examining the key challenges and how emerging technologies, such as 5G, are addressing these issues, along with future expectations from 6G. Additionally, the paper highlights how companies like Montimage are contributing to securing ITS networks. This is not intended to be an exhaustive review but rather a focused overview to stimulate continued exploration and dialogue in this rapidly evolving field.

# Challenges

The challenges of ensuring dependable communication in ITS[1] arise from its three core characteristics: cyber-physical systems, heterogeneous system compositions, and wireless communications. As a cyber-physical system, ITS integrates physical and digital components, making it vulnerable to cyber-attacks with real-world impacts. Additionally, the diversity of devices and communication protocols, coupled with the risks of wireless connectivity, creates a complex environment that requires robust security solutions to protect critical data and operations.

## Cyber-Physical System

A Cyber-Physical System (CPS) refers to an interconnected system of physical components, such as vehicles, traffic lights, sensors, that are monitored and controlled by computational cyber-processes. In the context of ITS, the network topology is highly complex, with widely distributed vehicles and rapidly changing information flows. Advances in embedded systems and communication technologies have enabled faster, more reliable interactions between vehicles and other devices, facilitating dynamic route guidance and real-time decision-making. However, this deep integration also introduces significant security challenges, as any vulnerability in the communication or control systems can have direct, real-world consequences for traffic safety and system reliability, including:

- **Attack Surface Expansion:** The close integration of physical processes, like vehicle control, with networked software makes CPS particularly vulnerable. Any cyber-attack, for example a remote attacker that exploits software vulnerability, can directly affect physical operations, leading to catastrophic consequences. Furthermore, vehicles involve distributed, decentralized components, such as road infrastructure, traffic management systems, and cloud-based services. Attackers can target different entry points, such as sensors, control units, or communication links, compromising the entire CPS.
- **Latency Sensitivity Communication:** In CPS, the interaction between the physical and cyber-components must happen in real-time to avoid any lag in critical decision-making. If communications are delayed, it can disrupt vehicle coordination and cause

[1] A. Pundir, S. Singh, M. Kumar, A. Bafila and G. J. Saxena, "Cyber-Physical Systems Enabled Transport Networks in Smart Cities: Challenges and Enabling Technologies of the New Mobility Era," in *IEEE Access*, vol. 10, pp. 16350-16364, 2022, doi: 10.1109/ACCESS.2022.3147323.
Online: https://ieeexplore.ieee.org/document/9695482

accidents. Traditional network security measures like deep packet inspection may introduce latency, complicating the balance between security and system responsiveness.

- **Data Integrity and Availability:** CPS in vehicles depends on accurate and timely data, such as speed, location, and environmental conditions. Cyber-attacks that target the integrity of this data, for example GPS spoofing or sensor manipulation, can lead to wrong decisions, like sudden braking or lane changes, risking accidents. Similarly, denial of service (DoS) attacks can render critical services unavailable when they are most needed.

## Heterogeneous System Composition

Connected vehicle networks involve heterogeneous systems with various devices, networks, platforms, and protocols that must interact seamlessly. This diversity increases the complexity of ensuring consistent and robust communication across the entire network, as vulnerabilities in one component can potentially compromise the entire system, making it essential to implement comprehensive security measures that account for this heterogeneity in the following areas:

- **Diverse Protocols and Standards:** For a long time, the only V2X solution was the Dedicated Short-Range Communication (DSRC) that is based on IEEE 802.11[2]. In 2017, 3GPP proposed the so-called cellular-enabled V2X (C-V2X[3]) that relies on the capabilities of 4G, 5G and future 6G cellular networks to provide significantly higher performance, thus enabling higher levels of safety to more road users. C-V2X Direct comprises short-range communication between vehicles (V2V), between vehicles and infrastructure (V2I), and vehicles and pedestrians (V2P). The recently emerged concept of Internet of Vehicles (IoV) extends the connectivity of vehicles to a broader

[2] Bai F, Stancil DD, Krishnan H. Toward understanding characteristics of dedicated short range communications (DSRC) from a perspective of vehicular network engineers. InProceedings of the sixteenth annual international conference on Mobile computing and networking 2010 Sep 20 (pp. 329-340).
Online: https://www.researchgate.net/profile/Daniel-Stancil/publication/220926534_Toward_understanding_characteristics_of_Dedicated_Short_Range_Communications_DSRC_from_a_perspective_of_vehicular_network_engineers

[3] Papathanassiou A, Khoryaev A. Cellular V2X as the essential enabler of superior global connected transportation services. IEEE 5G Tech Focus. 2017 Jun;1(2):1-2.
Online:
https://people.computing.clemson.edu/~jmarty/projects/lowLatencyNetworking/papers/3GPP/5GURLLC/Cellular%20V2X%20-%20IEEE%205G.pdf

network to allow integrating vehicles with the Internet. Ensuring compatibility between these protocols while maintaining security is difficult. Attackers could eventually exploit vulnerabilities in one protocol to compromise the entire system.

- **Inconsistent Security Levels:** Different manufacturers and developers may implement different security mechanisms for their products. While some might follow strict cyber-security standards, others may cut corners to save costs or meet deadlines. This inconsistency can lead to weak links in the network, where attackers focus their efforts. For instance, a poorly secured third-party sensor could be exploited to gain unauthorized access to the vehicle's communication system.
- **Legacy Systems and Upgradability Issues:** Vehicles are long-lasting assets, and older vehicles may lack the advanced security features available in newer models. These legacy systems are harder to update and secure, making them vulnerable to attacks. Connected vehicle networks must account for this heterogeneity and develop strategies for integrating older systems without exposing them to cyber-security risks.

## Wireless Communication

Wireless communication in ITS offers several advantages, such as increased mobility, flexibility, and reduced installation costs by eliminating the need for physical connections. However, it also presents considerable security challenges in ensuring reliable communication, which encompass the need to address:

- **Wireless Communication Vulnerabilities:** Unlike wired communication, wireless signals can be intercepted and manipulated over the air including signal jamming, eavesdropping, and Man-in-the-Middle (MitM) attacks. Attackers can intercept vehicle communication, alter it, or even block critical messages. For example, jamming a vehicle's communication link could cause it to miss crucial updates, while GPS spoofing could cause a vehicle to misinterpret its location, leading to dangerous driving behavior.
- **Deterministic Communication:** Achieving deterministic communication in wireless networks presents several challenges due to the inherently unpredictable nature of wireless environments, such as interference, signal fading, and varying channel conditions. Attackers can exploit this unpredictability to disrupt or degrade communications. Additionally, securing communications requires sophisticated techniques that strike a careful balance between robust security measures and operational efficiency to avoid compromising the deterministic performance, i.e.

introducing significant latency or variability that could disrupt the system's real-time requirements.

- **Over-the-Air (OTA) Updates:** OTA updates are crucial for maintaining and updating software in connected vehicles without requiring physical access. However, these updates are transmitted wirelessly, and attackers may try to intercept or manipulate them. Compromised OTA updates could allow attackers to install malicious firmware or disable important security patches, posing a major threat to the safety and security of the vehicle.

## Cyber-security Strategies

As the complexity of ITS systems increases with advancements in communication technologies like 5G and the future 6G mobile networks, cyber-security strategies must continuously adapt to keep up with the growing attack surface. Addressing the cyber-security[4] challenges identified necessitates a thorough, multi-faceted approach that encompasses:

- **Enhanced Encryption and Secure Communication Protocols:** Strong encryption methods must be applied across all communication layers to ensure that data exchanged over wireless networks remains confidential and tamper-proof. Public Key Infrastructure (PKI) and secure V2X communication standards like IEEE 1609.2[5] for wireless communication can protect data integrity and privacy.
- **Secure Device Identity and Authentication:** Vehicles and infrastructure must be able to authenticate each other securely before exchanging data. This can be achieved using multi-factor authentication, digital certificates, and blockchain-based decentralized identity management to ensure only trusted entities are communicating. The standard ISO/IEC 9797-1[6] specifies mechanisms for Message Authentication Codes (MACs) to ensure the integrity and authenticity of messages in cryptographic communication systems, providing protection against tampering and unauthorized data modification.
- **Intrusion Detection and Prevention Systems (IDPS):** IDPS systems can monitor network traffic in real-time, analyzing patterns for suspicious activity that could

[4] Mecheva T, Kakanakov N. Cybersecurity in intelligent transportation systems. Computers. 2020 Oct 13;9(4):83.
Online: https://www.mdpi.com/2073-431X/9/4/83/pdf
[5] https://standards.ieee.org/ieee/1609.2/10258/
[6] https://www.iso.org/standard/50375.html

indicate an ongoing attack. These systems are essential for detecting cyber-attacks in both the wired and wireless portions of the connected vehicle ecosystem.

- **Network Segmentation and Isolation:** In a heterogeneous system, network segmentation can isolate critical vehicle systems, like breaking or navigation, from less critical ones. This isolation prevents an attack on one part of the system from cascading into others.
- **Regular Security Updates:** Ensuring that all components, from legacy vehicles to modern autonomous systems, are regularly updated with the latest security patches is critical. Secure OTA mechanisms should be implemented to deliver these updates in a trusted and authenticated manner.
- **AI-Powered Threat Detection and Mitigation:** Artificial intelligence (AI) and Machine Learning (ML) can be employed to identify anomalies and emerging threats in real-time. By analyzing large datasets of vehicle behavior, AI systems can predict and help prevent potential attacks before they cause harm.

## 5G infrastructure

The introduction of 5G technology is a game-changer for cyber-secure communications in ITS, offering significant improvements in speed, reliability, and security over previous wireless technologies[7]. As connected vehicles and autonomous systems become more integrated, 5G addresses critical challenges in securing their communication networks. The main ones are:

- **Ultra-Reliable Low-Latency Communication (URLLC):** One of the most important features of 5G is its ability to deliver ultra-reliable low-latency communication. In ITS, real-time data exchange is crucial for V2V and V2I communication. 5G's latency can be reduced to as low as 1 millisecond, enabling rapid decision-making and preventing potentially dangerous delays. This significantly reduces the risk of accidents due to communication lags or slow responses, making the system resilient against attacks aiming to exploit latency vulnerabilities.
- **Enhanced Security Protocols and Encryption:** 5G networks incorporate advanced security protocols, including stronger encryption, more robust mutual authentication, and end-to-end data protection. These enhanced measures provide a layer to protect V2X communications from eavesdropping, tampering, and Man-in-the-Middle

[7] Gohar A, Nencioni G. The role of 5G technologies in a smart city: The case for intelligent transportation system. Sustainability. 2021 May 6;13(9):5188.
Online: https://www.mdpi.com/2071-1050/13/9/5188/pdf

attacks, ensuring the confidentiality and integrity of the data exchanged between vehicles and infrastructure. This is especially important for ITS applications that handle location data, driving behavior, or other personal information.

- **Massive IoT Connectivity and Scalability:** As ITS ecosystems grow, the number of connected devices, such as sensors, cameras, and vehicles, will increase exponentially. 5G supports massive machine-type communication (mMTC), enabling reliable communication between millions of devices with minimal delay. This scalability ensures that the security of the system is maintained even as the number of connected devices rises.
- **Network Slicing:** Network slicing allows the creation of isolated virtual networks tailored to specific services. In ITS, critical communication channels, such as those used for vehicle control or safety functions, can be segregated from less critical data flows. This segmentation ensures that an attack on one part of the network doesn't compromise other more critical functions, enhancing overall system security. Each slice can be custom-tailored with its own security policies, providing dedicated security for high-priority, mission-critical communications in ITS.

## Looking to 6G

While 5G mobile networks have already been deployed to address many of the current challenges, 6G is expected to introduce groundbreaking advances in network security, particularly for connected vehicles[8]. These are for instance:

- **Deterministic communication:** Even though 5G is able to provide low latency, it still operates on a best-effort basis, meaning it cannot fully guarantee strict timing for every application. 6G will push latency even lower, introducing bounded, ultra-reliable latency to ensure precise, real-time communication for critical applications like autonomous driving and smart infrastructure.

- **Distributed AI and Blockchain for Security:** 6G is expected to integrate distributed AI and blockchain technology to further decentralize security, reducing the risks associated with single points of failure in centralized systems. Blockchain could provide secure, transparent, and immutable logs of all communications, ensuring data integrity.

[8] Liu R, Hua M, Guan K, Wang X, Zhang L, Mao T, Zhang D, Wu Q, Jamalipour A. 6G enabled advanced transportation systems. IEEE Transactions on Intelligent Transportation Systems. 2024 Feb 19. Online: https://arxiv.org/pdf/2305.15184

- **Advanced Quantum-Resistant Encryption:** As quantum computing develops, traditional encryption methods may become vulnerable. 6G networks will likely incorporate quantum-resistant encryption to protect vehicle communications from future quantum-based attacks. Quantum Communications and Quantum Key Distribution will also enhance the security and efficiency of data transmission in ITS.
- **Edge Computing and Security at the Network Edge:** 6G will push computing resources closer to the data source, enabling vehicles and infrastructure to process data locally rather than relying on centralized cloud services. This reduces latency and improves security and privacy by reducing the risk of data being intercepted during transmission.
- **Full-Spectrum Communications:** 6G will operate across an even wider spectrum, including terahertz frequencies. This will enable higher data rates and more robust security features, but also introduce new challenges in terms of securing these communications.

# Montimage Resources

Montimage offers a comprehensive suite of cyber-security solutions designed to address the challenges posed by ITS. Their approach focuses on attack generation, security-by-design, in-network security, and the use of explainable AI, ensuring robust protection for connected vehicles and V2X communications. Here's how Montimage's open-source solutions[9] work in these areas.

## Attack generation

Montimage provides attack generation and simulation tools[10] that help test and evaluate the cyber-security of connected vehicle systems and ITS infrastructures against cyber-attacks. This feature allows organizations to simulate a wide range of cyber-attacks, such as DoS, MitM, spoofing, and remote vehicle attacks, in controlled environments. These simulations enable ITS developers and operators to assess how their systems will perform under real-world cyber-threats and identify vulnerabilities before they can be exploited. By creating

[9] https://github.com/Montimage/

[10] Salazar Z, Nguyen HN, Mallouli W, Cavalli AR, Montes de Oca E. 5greplay: A 5g network traffic fuzzer-application to attack injection. InProceedings of the 16th International Conference on Availability, Reliability and Security 2021 Aug 17 (pp. 1-8).
Online : https://arxiv.org/pdf/2304.05719

various attack scenarios, Montimage can help organizations test the resilience of their systems and improve their defenses through rigorous stress testing and validation.

## Security-by-design

Montimage promotes security-by-design (e.g. in future 6G mobile networks[11]) that embeds cyber-security into every layer from communication protocols to software controls to mitigate the risks associated with wireless communication and the shift from wired systems. Design principles are essential for securing vertical applications such as ITS and connected vehicle systems. This proactive approach ensures that each component of the ITS architecture is inherently secure, reducing the attack surface and making it more difficult for cyber-criminals to exploit vulnerabilities. In heterogeneous systems, Montimage standardizes security protocols and ensures consistent implementation across various devices, manufacturers, and platforms, addressing the challenges posed by varying security levels and third-party vulnerabilities.

## In-network security

Montimage's MMT framework leverages *in-network* security[12], focusing on real-time monitoring and protection within the communication networks that link connected vehicles, infrastructure, and other elements of ITS. Montimage's MMT solution continuously monitors network traffic in real-time to detect anomalies, malicious behavior, or any deviations from normal traffic patterns. This proactive monitoring helps identify and neutralize threats before they affect vehicle operations, focusing on real-time monitoring and protection within the communication networks that link connected vehicles, infrastructure, and other elements of ITS.

## Explainable AI

Montimage leverages explainable AI (XAI)[13] to enhance threat detection and response within ITS environments. Their AI-powered algorithms analyze vast amounts of network traffic data

[11] Sharma, Gourav Prateek, et al. "Toward deterministic communications in 6G networks: state of the art, open challenges and the way forward." IEEE Access 11 (2023): 106898-106923.
Online:
https://www.researchgate.net/publication/374013627_Towards_Deterministic_Communications_in_6G_Networks_State_of_the_Art_Open_Challenges_and_the_Way_Forward
[12] https://github.com/Montimage/in-network-inference-using-p4
[13] https://github.com/Montimage/maip

to detect patterns indicative of cyber-attacks, such as abnormal traffic spikes or unauthorized access attempts. What sets Montimage apart is its use of explainable AI, which provides transparent and understandable insights into how decisions are made by the AI models. This ensures that human operators can understand why an alert is triggered, what actions need to be taken, and how the AI reached its conclusions.

## A more technical illustration of how to monitor and detect attacks in ITS messages

The following example is extracted from our published work[14], and was implemented and evaluated in the 5GopenRoad[15] project and, concerning XAI, the SPATIAL[16] project.

Monitoring serves as a vital, proactive strategy to bolster the resilience of crucial systems, including Critical Infrastructures and Cyber Physical Systems (CPS), by perpetually overseeing system events. This approach entails the methodical gathering of data, encompassing both inbound and outbound traffic along with internal system data. The data collected is analysed to pinpoint system behavior anomalies. The analysis outcomes are then conveyed through reports or alerts, which are subsequently interpreted and responded to by human operators or automated orchestrators.

Figure 1 illustrates an example of a monitoring mechanism of a 5G mobile network. The monitoring can be done in a non-disruptive way (e.g., using traffic mirroring) or in the communication path (e.g., acting as a firewall). The data, upon arrival, is directed to both the 5G core and the monitoring framework. For the monitoring, a probe receives the data for further analysis. Subsequently, the collected data undergoes comprehensive analysis, enabling the generation of detailed dashboards and reports presenting the key findings and observations. The monitoring framework used is Montimage's open-source solution MMT. MMT is equipped to validate both functional and security properties, providing a mixed distributed/centralized network monitoring solution. It consists of MMT-Probes to capture the required features and an MMT-Operator application to manage and visualise the results obtained from the analysis performed by the probes and the application (e.g., network traffic statistics, detected anomalies). It integrates AI techniques for analysing encrypted network

[14] A. R. Cavalli and E. Montes De Oca, "Cybersecurity, Monitoring, Explainability and Resilience," *2023 Fourteenth International Conference on Mobile Computing and Ubiquitous Network (ICMU)*, Kyoto, Japan, 2023, pp. 1-7, doi: 10.23919/ICMU58504.2023.10412157.
Online: https://drive.google.com/file/d/1usGFFSlzPPyDibIFUyhkUp310ltTmRwC/view
[15] http://5gopenroad.com/
[16] https://spatial-h2020.eu/

traffic, performing root cause analysis, interacting with an orchestrator to perform remediations actions, replaying modified network traffic for penetration testing, and more.

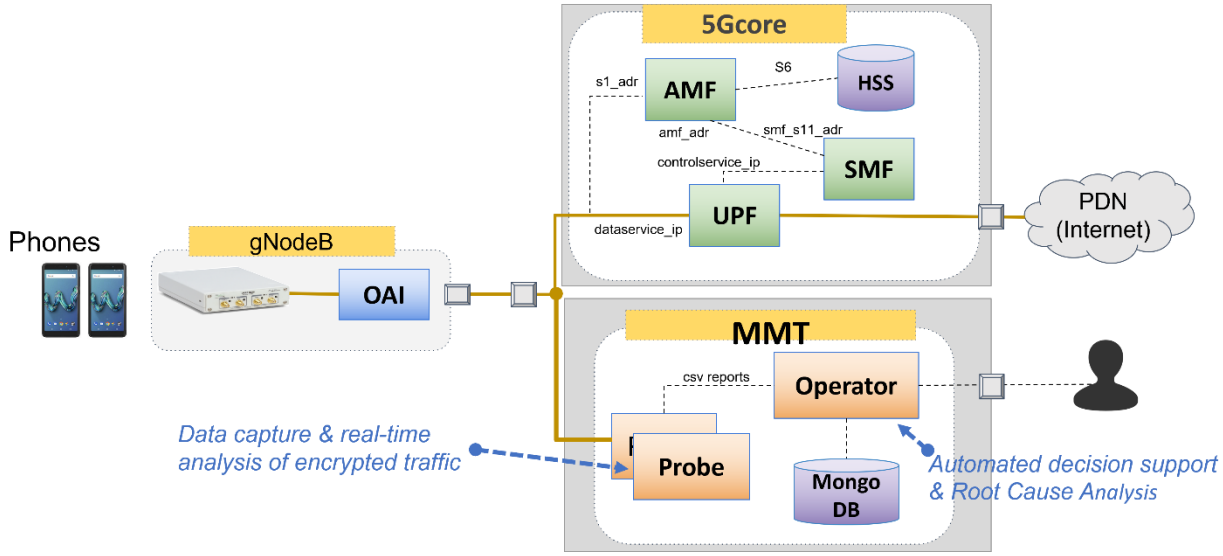


*Figure 1: Monitoring of a 5G network}*

The communication in an ITS is based on two main types of messages (illustrated by Figure 2). A CAM message (Cooperative Awareness Messages) that provides data about the state of a vehicle, such as: position, speed and direction. A CPM (Collective Perception Messages) that provides information about the detected objects, such as: pedestrians, obstacles, and other vehicles, and allows receiving data beyond the cars' sensor range.

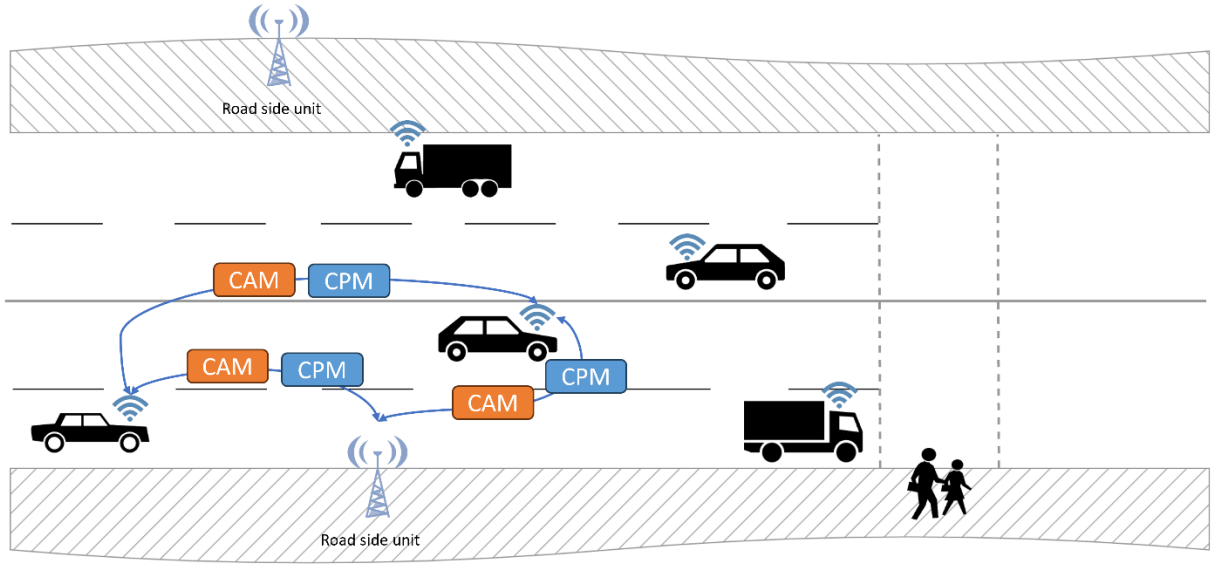


*Figure 2: Intelligent Transport System*

The safety of an ITS system depends totally on the information exchanged between vehicles. And like any information network, communication needs to be monitored and protected from attacks.

The MMT monitoring solution provides the possibility to monitor the communications, decode and extract attributes of CAM/CPM packets, detect attacks based on CAM/CPM protocols and visualize the network state as well as security information via its web interface, and identify potential attacks leveraging CAM/CPM protocols.

In the 5GOpenRoad project a 5G network and ITS system for managing autonomous vehicles has been deployed in the Paris-Saclay region. This allowed testing and demonstrating how the monitoring solution can analyse CAM/CPM packets within the network traffic and detect a security attack. As an example, here we present a simple attack scenario where an attacker suddenly changes his/her vehicle type to be something else caused either by malicious intent or compromised software in the vehicle. This is a typical poisoning attack where faulty information will lead to incorrect calculations and decisions that compromise the safety of the ITS.

In this attack scenario, the attacker's vehicle is pretending to be a train (shown in Figure 3), which creates confusion for other vehicles and generates chaos in the ITS system. The monitoring was able to detect and generate an alert so the attack can be mitigated. To detect this poisoning attack, the monitoring system follows the vehicle type value (i.e., *camParameters/basicContainer/stationType*), if this value changes or is in contradiction with observations sent by other vehicles then this implies an attack. Figure 4 shows the dashboard presenting the protocol statistics and Figure 5 shows the dashboard presenting the alerts.

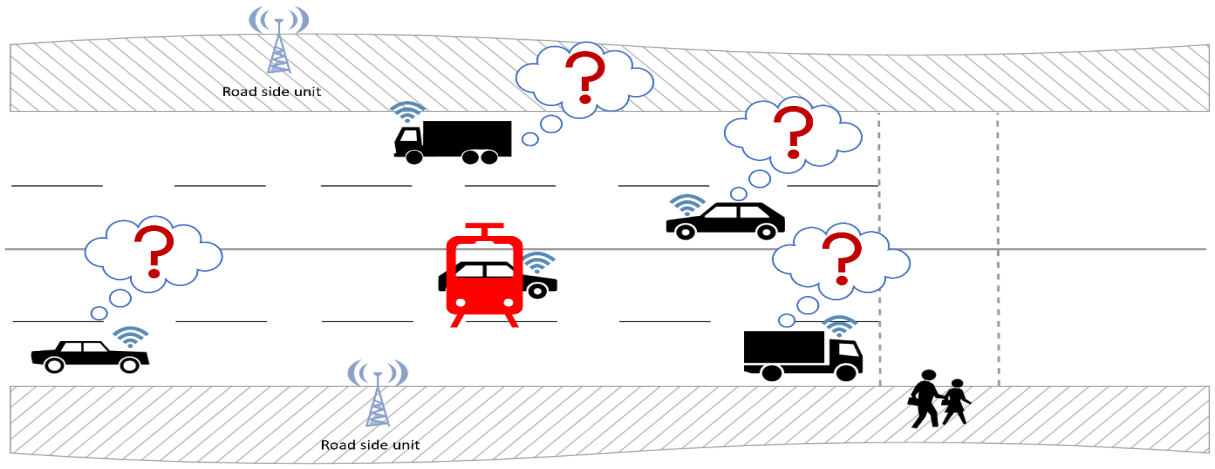


*Figure 3: Poisoning attack*

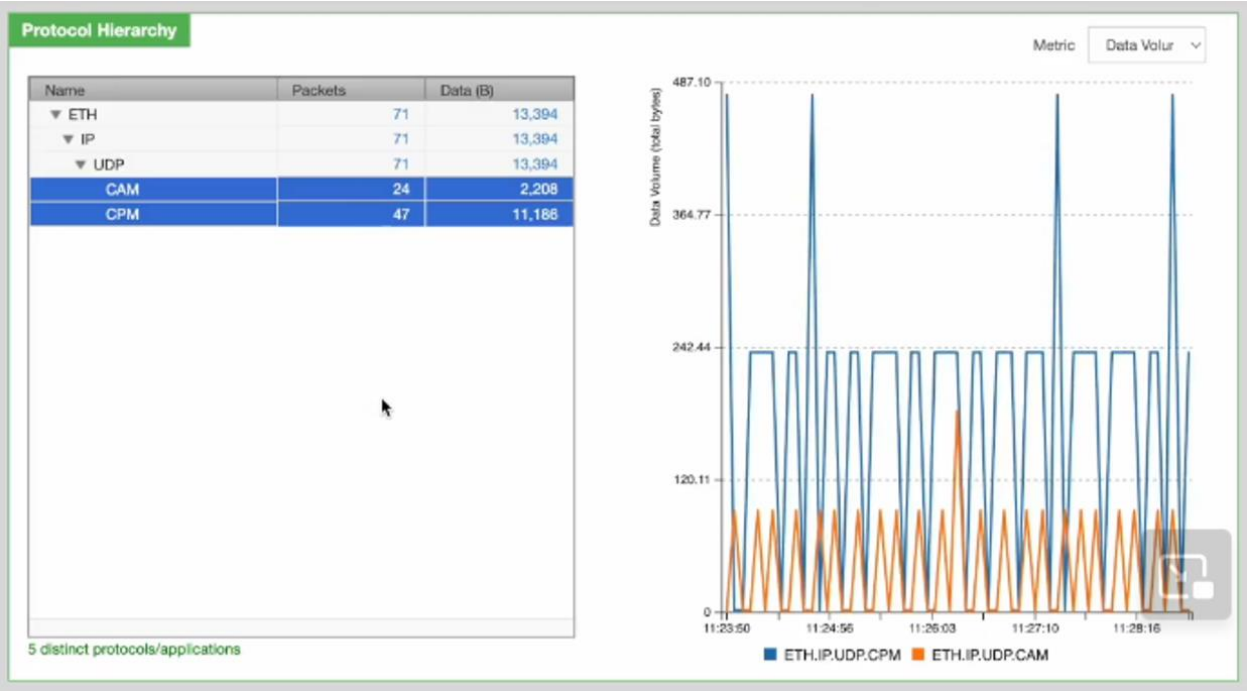


*Figure 4: Inspection of CAM and CPM messages*

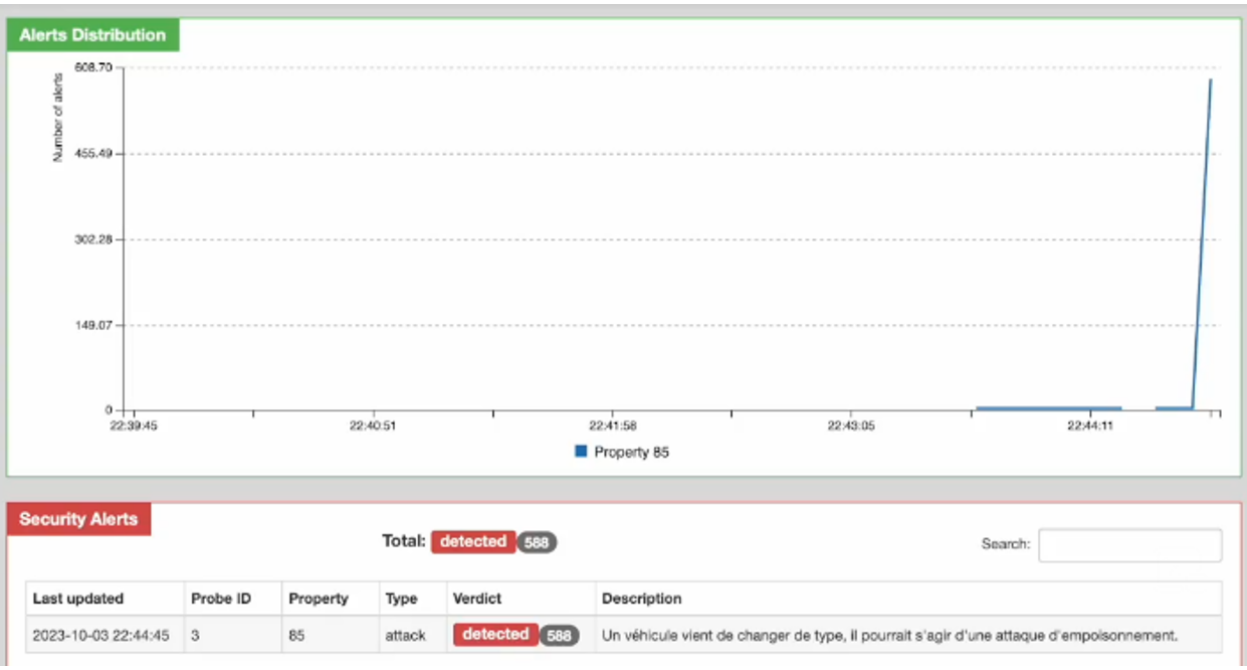


*Figure 5: Detection of poisoning attack*

While AI demonstrates remarkable performance in detecting and mitigating cyber-attacks, the lack of interpretability and explainability inherent in many AI models poses significant challenges. There is a growing need for explainability and striking a balance between trust and efficacy when safeguarding digital assets.

Model-agnostic techniques like Local Interpretable Model-agnostic Explanations (LIME) and Shapley Additive Explanations (SHAP) offer post hoc explanations for predictions made by complex AI models[17]. Unlike model-specific interpretability methods that work only for a particular type of model, these techniques can be applied to any machine learning model, including but not limited to neural networks, random forests, and support vector machines.

LIME works by perturbing the input data and observing the changes in predictions. For each instance to be explained, it generates a new dataset consisting of perturbed samples, computes the predictions for these new samples using the complex model, and then fits a simpler, interpretable model like a linear regression to this perturbed dataset. The coefficients of the simpler model serve as an explanation for how the original model makes its predictions, but only in a local region around the instance in question.

On the other hand, SHAP values are rooted in cooperative game theory and offer a unified measure of feature importance. The SHAP value for a feature essentially represents the average contribution of that feature to all possible combinations of features. It does so by calculating the marginal contribution of each feature to the prediction for every possible subset of features, then averaging these marginal contributions. Both LIME and SHAP provide a way to understand how individual features impact a specific prediction, making them invaluable tools for deciphering the behavior of otherwise "black box" models, particularly in domains like cybersecurity where interpretability is crucial.

In this real-case example implemented in the SPATIAL project, we consider the vulnerabilities of IoT/5G devices to different kinds of cyberattacks, such as botnet, ransomware. The detection model combines 2 Deep Learning techniques: Stack Autoencoders and Convolutional neural networks. Each of the autoencoders is trained separately with normal and malicious samples. The output of each of the autoencoders is concatenated to one vector and passed as input to the one-dimensional CNN. We use 59 flow-based features independently of whether the traffic is encrypted or not. For the current evaluation, we use the public dataset (CSE-CIC-IDS2018[18]) of 7 different cyber-attack scenarios and private datasets (i.e., captured by our own honeypots).

---

[17] Nguyen, MD., La, VH., Mallouli, W., Cavalli, A.R., Oca, E.M.d. (2024). Toward Anomaly Detection Using Explainable AI. In: Sadovykh, A., Truscan, D., Mallouli, W., Cavalli, A.R., Seceleanu, C., Bagnato, A. (eds) CyberSecurity in a DevOps Environment . Springer, Cham. https://doi.org/10.1007/978-3-031-42212-6_10
Online: https://zenodo.org/records/13693509

[18] https://www.unb.ca/cic/datasets/index.html

SHAP uses cooperative game theory and offers a unified measure of feature importance, where: 1) Values represent the average contribution of a feature; 2) The marginal contribution of each feature is calculated; and 3) The marginal contributions are averaged.

We apply SHAP feature importance to estimate how much each feature contributes to the model's prediction. In Figure 6 we have 3 summary plots showing top 10 most important features extracted by SHAP analysis of 50 random samples. We find that the most important feature in all 3 cases is flow duration. Flow duration is one of the most applied characteristics used in ML for botnet detection. Some botnets establish brief connections, other botnets are known to be chatty yielding long duration. A simple strategy to prevent detection of a botnet is by randomly reconnecting as an established connection. Thus, features related to number of TCP packets with some flags like Reset (RST) or Finished (FIN) for closing a connection are important. The results show that our model's predictions have parity with the domain knowledge and match with our assumption in detecting those attacks.

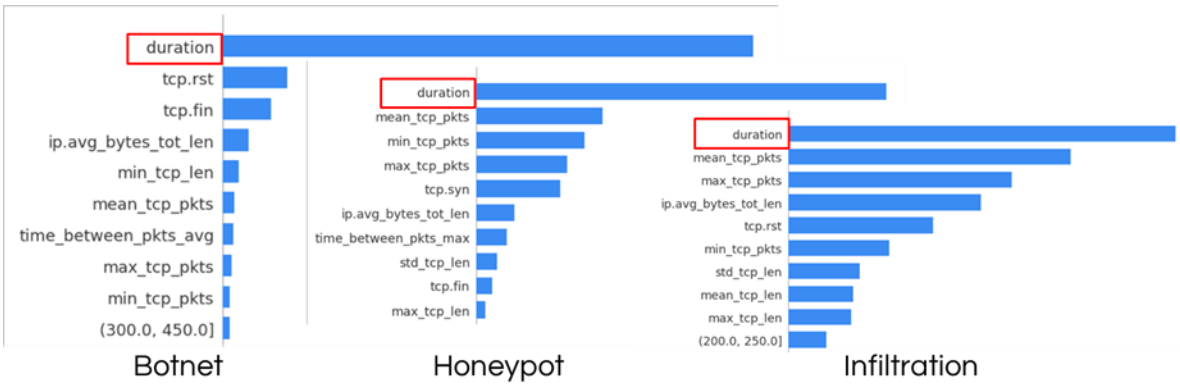


*Figure 6:SHAP feature importance for 3 types of attacks*

In Figure 7 we show the SHAP summary plots obtained for botnet detection (to the left) and for botnet detection under the target label flipping attack (type of data poisoning in which the labels of the training data are flipped or modified, causing the model's classification performance to degrade) with poisoning rate of 50%. By comparing the SHAP signatures with and without an attack, we clearly see the differences between the list of important features produced by SHAP. For instance, the feature *duration* is no longer the most important feature for botnet detection under the target label flipping attack. Furthermore, none of those features related to the number of TCP packets with specific flags appear in the top 20 feature list under the target label flipping attack. As a result, SHAP signatures can be useful to detect the existence of adversarial attacks by identifying the features whose SHAP values have been significantly altered due to the attack. Thus, this type of technique can be used to determine the resiliency of the AI methods used and improve the detection accuracy.

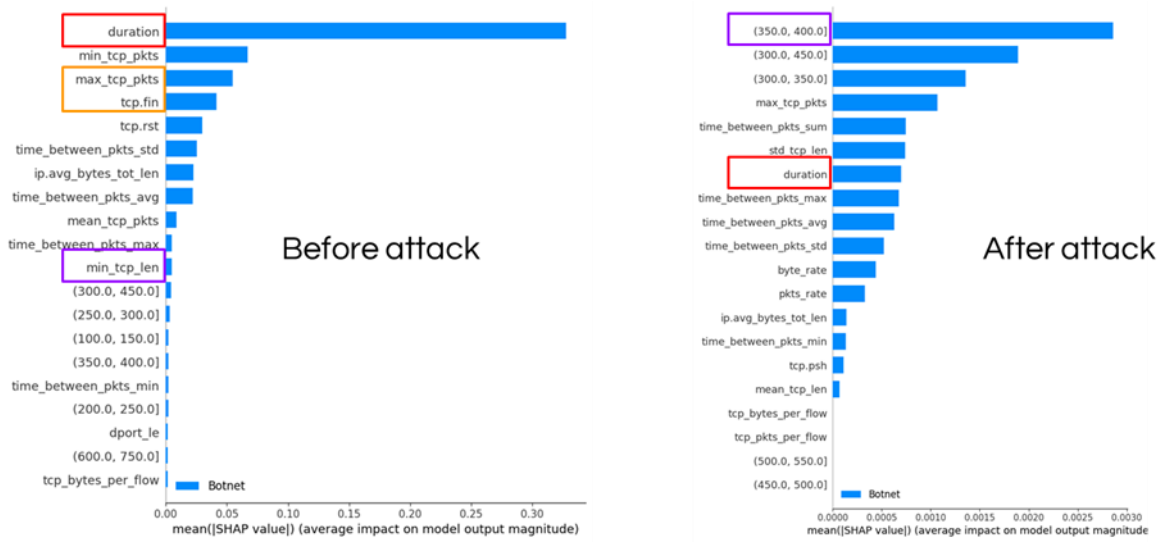


*Figure 7:SHAP feature importance without and with an attack*

## Conclusion

In ITS communication, safeguarding the transferred data is just as crucial as ensuring low latency. Protecting data means maintaining its confidentiality, integrity, and authenticity, preventing unauthorized access, tampering, or malicious attacks that could compromise vehicle and infrastructure operations. However, latency - the time it takes for data to be transmitted and received - is just as essential, because real-time ITS decisions such as collision avoidance or traffic management depend on the immediate and timely exchange of information.

The challenges of secure and deterministic communication in ITS arise from the complexities of cyber-physical systems, heterogeneous system compositions, and wireless communications, which increase vulnerability to cyber-threats, latency issues, and data integrity concerns. Cyber-security strategies for ITS focus on creating a resilient and secure communication environment through security-by-design, embedding protection into every layer of the communication system. Key approaches include real-time traffic monitoring to detect and neutralize threats before they impact vehicle operations, and the use of encryption and authentication to safeguard data integrity and confidentiality. These strategies work together to balance security with the need for low-latency, dependable communication in ITS.