Quantifying Cyber Risks: The Impact of DoS Attacks on Vehicle Safety in V2X Networks

Zsombor Pethő, Tamás Márton Kazár, Zsolt Szalay, and Árpád Török

***Abstract*— This paper presents a novel framework for analyzing the interrelationships between vehicle dynamics, communication characteristics and cyberattacks on V2X-based functions, highlighting their impact on vehicle safety. The research implements a simulation-based approach and uses various regression models to describe the complex interactions between cyber-physical components, providing a nuanced understanding of the mathematical relationships. It provides a robust simulation framework for assessing DoS attack's impact on the traffic safety risk. From a societal perspective, it addresses fundamental road safety issues in the face of increasing reliance on connected technologies. From a technical perspective, it presents an innovative ASIL-compatible risk classification methodology for DoS attacks, contributing to standardised cyber threat assessments in line with automotive security standards. The research serves as a methodological basis for investigating DoS attacks on vehicle safety and introduces a quantifiable risk assessment approach that can be used in adaptive security solutions. The risk classification system facilitates scenario assessment, improve intrusion detection and ensure the resilience of connected and intelligent transport systems.**

***Index Terms*— V2V communication, safety risk, cybersecurity, denial-of-service (DoS), safety analysis, network performance.**

I. Introduction

IN LIGHT of the overarching societal goal to significantly reduce the number of accidents, the utilisation of V2X (Vehicle-to-Everything) technology is becoming increasingly important. Improving safety is a key objective of Cooperative Intelligent Transportation Systems (C-ITS), but as systems become more complex and interconnected, new types and causes of accidents will emerge. In addition, with the integration of advanced communication technologies into the transport system, various remote cyber-attacks against vehicle systems and transport infrastructure are becoming feasible [1].

Wireless communication is particularly important where the reliability of information from other environment perception sensors cannot be guaranteed. Typical cases are Non-line of sight (NLoS) situations, e.g. intersections in densely built-up urban environments where neither radar, LIDAR nor camera can detect objects behind buildings [2]. The detection of a dangerous situation and the appropriate decision can remain uncertain if the quality of the wireless communication is bad [3]. Accordingly, for safety applications, availability is the most critical cybersecurity aspect of the CIA (Confidentiality, Integrity, Availability) triad because if the information is unavailable in time, the Automated Driving System / Advanced Driver Assistance System (ADS / ADAS) functions (e.g., AEB - Automated Emergency Braking) cannot intervene in order to avoid the potential collision / accident [4], [5].

Given the importance of availability, for safety-critical applications, such as collision warning systems, AEB, and Adaptive Cruise Control (ACC), low end-to-end latency (E2E) and a high packet delivery ratio (PDR) are crucial. In these systems, data must arrive with predictable delay and jitter to enable timely control decisions for safe driving [6], [7], [8]. Attacks that compromise the availability of critical information are a particular threat to the safety of connected vehicles [9]. Therefore it is important to understand the relationship between communication, physical system functionality and risk associated with failures [10]. In this case, a method is needed that can estimate the change in risk as a function of the change in quality of service (QoS), so that the system can be kept in a safe state [11]. Accordingly, we can characterize one of the most important cybersecurity parameters, availability, by analyzing the effect of Network Performance Metrics (NPMs) such as PDR and E2E [12].

Due to a cyberattack [13] or any other unintentional wireless communication failure, PDR and E2E can be degraded by a certain level [3], [14]. So far, no modeling concept has been developed to quantify cyber-attack's impact on vehicle safety focusing on vehicle-to-vehicle communications, in line with the automotive safety principles (ISO26262 [15], [16]). Although Javed et al. [17] have shown that cybersecurity, QoS, and safety together have an impact on the operation of C-ITS, they have not explored the functional relationships between the factors and have not examined the impact of each intervention on the probability and severity of a potential incident. In line with this, the present research aims to develop a new modeling framework to explore and quantify the relationships between cybersecurity, vehicle safety, and wireless communication quality, considering V2X-based automated vehicle functions. Accordingly, the main contributions of this paper can be summarized as follows.

Manuscript received 18 January 2024; revised 30 April 2024 and 24 June 2024; accepted 11 July 2024. This work was supported in part by European Union within the Framework of the National Laboratory for Autonomous Systems under Grant RRF-2.3.1-21-2022-00002; and in part by the New National Excellence Program of the Ministry for Culture and Innovation from the Source of the National Research, Development and Innovation Fund under Grant ÚNKP-23-4-I-BME-158. The Associate Editor for this article was S. Kumari. *(Corresponding author: Zsombor Pethő.)*

The authors are with the Department of Automotive Technologies, Budapest University of Technology and Economics, 1111 Budapest, Hungary (e-mail: petho.zsombor@kjk.bme.hu; kazar.tamas@kjk.bme.hu; szalay.zsolt@kjk.bme.hu; torok.arpad@kjk.bme.hu).

Digital Object Identifier 10.1109/TITS.2024.3436840

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

- A notable aspect of this paper is the integration of hardware and software system components, which has enabled the creation of a unique framework for testing cyber-physical processes by combining vehicle simulation, network simulation and standard communication devices.
- In this research, we laid the methodological foundation for investigating the impact of Denial-of-Service (DoS) attacks on vehicle safety for connected vehicles, taking into account relevant vehicle dynamics factors.
- Another unique novelty achieved by this research is that we can quantify safety risk with our simulation framework, depending on the vehicle dynamics and cyberattack parameters. This is an essential research milestone to implement adaptive security solutions to handle network disruption and degraded performance in inter-vehicular wireless communication.
- A key achievement is that we have successfully built a risk classification system, allowing us to evaluate different cyberattack-related driving scenarios, considering the vehicle dynamics under investigation and the fundamental characteristics of cyber-attacks.

II. Related Works

Recently, V2X communication technologies has significantly enhanced the capabilities of intelligent transport systems. These advances have led to an increased interest in understanding the cybersecurity challenges posed by the integration of vehicle networks and cyber-physical systems. A number of studies have examined the vulnerabilities of V2X communications, specifically the challenging aspects of DoS attacks [18]. Lyamin et al. [19], [20] proposed solutions for real-time jamming detection in 802.11p vehicular networks. Based on these studies, the results supported that communication link metrics (e.g., jitter) have a crucial effect on predictable and uniform message reception, and accordingly, on the whole system reliability. Kim and colleagues [21] investigate DoS attacks on Cellular Vehicle-to-Everything (C-V2X) networks from several perspectives. They applied system-based simulations and quantified the impact of a DoS attack on communication quality indicators such as reliability, coverage and timeliness. The simulation results show that DoS attacks can significantly affect the detection and decision-making processes of highly automated vehicles. Similarly, Twardokus and Rahbari [22] proposed mitigation techniques in order to maintain QoS in C-V2X networks. This article [23] focuses on the importance of secure transmission for intelligent V2X communications in the context of increasing connectivity. It highlights the limitations of existing cryptographic and physical layer security techniques, which often reduce throughput performance due to high vehicle mobility and low short-term channel quality statistics. The concept of statistical security is introduced, which uses time-sensitive information to increase throughput while maintaining security. The paper proposes an optimal power allocation scheme within a queueing system model that addresses different security QoS requirements and demonstrates significant performance improvements over existing baseline schemes through simulation results. However the above introduced research studies did not focus on the safety consequences of degraded wireless performance. These papers did not investigate the potential collision risk associated with different cyberattacks on the V2X network. Petit et al. [24] presented the Coordinated Mobility for X (CMX) framework, which is designed to ensure safety, privacy, efficiency, and cybersecurity (SPEC) in networks of highly automated vehicles. The CMX framework incorporates various cyber-physical components and relies on protocols and algorithms for reliable inter-vehicle communication and coordination. Although they considered safety and cybersecurity in an integrated way, the framework did not numerically represent the safety risk. This study [25] investigated the impact of driving assistance from a connected environment on driving behaviour and safety through an innovative driving simulator experiment. Communication delay and loss scenarios were included to realistically imitate connected environment conditions. The study also examined the impact of these communication impairments on specific driving events along the motorway, suggesting further research into their impact on other traffic interactions. However, this research focuses on the interaction between QoS and safety, without considering cyberattack characteristics, systematic analysis and V2X-specific safety indicators.

III. Methodology

Based on the introduction, it is imperative to define a methodological framework that captures the sequential effects resulting from cyber-attacks, compromising communication QoS, influencing vehicle dynamics and degrading vehicle safety. This requires the development of a structured approach that comprehensively accounts for the interrelated and cascading effects of these multiple domains. Accordingly, a significant contribution of this research is the integration of hardware and software elements, which allowed the establishment of a novel environment for testing and analysing cyber-physical processes by combining vehicle simulation, network simulation and standard communication devices. By using real devices in the communication process and integrating different simulation solutions to model the interacting mobility and data exchange processes, it is possible to study the traffic safety aspects of denial of service attacks.

Various statistical and machine learning (ML) methods, such as polynomial regression, neural networks, and also random forest algorithms can be used to estimate the correlations between accident probability and severity based on the cyber-physical parameters of a given test scenario. Building on our previously established testing concept [3], we adapted the theory of the introduced risk estimation approach to develop the methodological framework and the estimation procedure for simulating hazardous events and quantifying the associated risks due to a deliberate communication failure caused by a DoS attack. As part of our innovation efforts, we aim to introduce a complex simulation toolchain based on a consistent theoretical background that can quantify the expected risk of traffic accidents by simulating the impact of DoS attacks, taking into account attack rate (AR) and attack packet length (APL).

TABLE I
DRIVING TEST SCENARIOS WITH THE DEFINED SPEED LEVELS

Scenario	v_{RV} [km/h]	v_{HV} [km/h]
S1	20	40
S2	50	70
S3	20	70
S4	50	100
S5	20	100
S6	50	130

Our investigation aims to explore the relationships between cyber threats, communication QoS, and vehicle safety. Therefore we chose a test scenario:

- that is statistically characterised by an increased level of risk
- where the other environmental sensors cannot detect hazardous events in time, and only V2X communication can currently provide accurate detection from a sufficient distance.

The study focuses on Straight Crossing Path (SCP) intersection scenarios (see Table I), where a Host Vehicle (HV) and a Remote Vehicle (RV) approach a right-angled intersection at different speeds and cross each other's paths simultaneously in the conflict zone. The flowchart in Figure 1 represents the steps of the methodology of this research, the individual phases are detailed in the following subsections. To achieve the research objective, we define common driving test scenarios (Figure 1 - block 1) for both Hardware-in-the-loop (HIL) and network simulation. During HIL simulation phase (Figure 1 - blocks 2, 3, 4, 5) we quantify the vehicle safety impact based on NPMs. During the network simulation phase (block 6) we compute NPMs based on the attack parameters. We then process these results to obtain the generalized estimator function characterizing the Safety Risk posed by the attack - SRI_{ATT} (Figure 1 - block 7) and derive the risk classification matrix (Figure 1 - block 8) to identify critical cases (Figure 1 - block 9). As can be seen from the overall research methodology described, the following subsections detail the steps of the simulation and modelling processes. However, it is important to emphasize that a detailed description of the process and the sharing of data is necessary to ensure the replicability of the research.

A. Hardware-in-the-Loop Simulation

The simulations (see Figure 1 - `HIL simulation` block) provided the GNSS feed for the Cohda MK5 On Board Units (OBU), which communicated with each other on the 802.11p physical layer. The OBUs logged the communication data to Packet Capture (PCAP) files. The standardized logging procedure provides the transmitted and received Cooperative Awareness Messages (CAM). V2X data extracted from logged messages contain vehicle dynamics parameters (VDPs), including vehicle speed and acceleration, as well as GNSS position. This data generated from simulated driving scenarios was modified to comply with the predefined NPMs (e.g, PDR, E2E), as shown in Figure 1 - `Data processing` block.

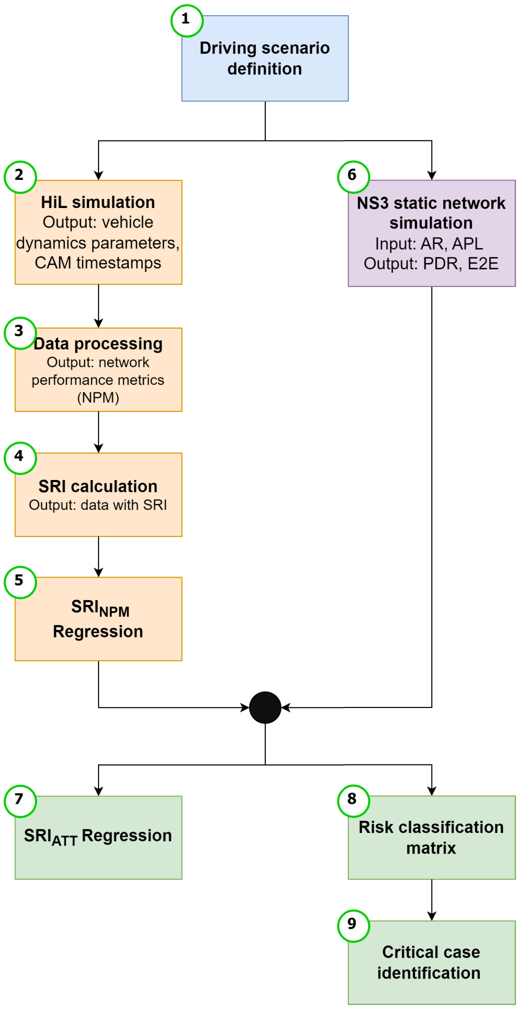

1
Driving scenario definition
2
HiL simulation
Output: vehicle dynamics parameters, CAM timestamps
3
Data processing
Output: network performance metrics (NPM)
4
SRI calculation
Output: data with SRI
5
SRI_NPM Regression
6
NS3 static network simulation
Input: AR, APL
Output: PDR, E2E
7
SRI_ATT Regression
8
Risk classification matrix
9
Critical case identification

Fig. 1. Process flow diagram.

B. Data Augmentation Based on NPMs

The subcases were created by modifying the data set offline using previously defined PDR and E2E parameter values (**PDR:** 10%, 50%, 100%, **E2E:** 100ms, 500ms, 1000ms). A certain percentage of the packets were dropped in order to match the desired PDR value. At PDR = 100% no packets were dropped from the dataset. For applying E2E values, we shifted the received CAMs in time to process the messages with a specific latency value. The investigated PDR and E2E network performance metrics were defined based on the following formulas:

$$PDR = \frac{\sum \text{nr. of packets successfully received}}{\sum \text{nr. of packets transmitted}} \tag{1}$$

$$E2E = N^{-1} \cdot \sum_{i=1}^{N} \tau_i \tag{2}$$

where τ_i is the aggregated delay of the following components,

- Transmission delay, τ_{trans} - the time it takes to push the packet's bits onto the link;
- Propagation delay, τ_{prop} - the time required for a signal to propagate through the transmission medium;

- Processing delay, τ_{proc} - the time it takes a router to process the packet header;
- Queuing delay, τ_{queue} - the time the packet spends in routing queues, and
- N - nr. of packets transmitted.

C. Safety Risk Calculation and Estimation

Following the data augmentation step, we calculated the Safety Risk Index (SRI) value (Eq. 3) for each sub-case (see Figure 1 - `SRI calculation` and SRI_{NPM} `regression` blocks). SRI is a Surrogate Measure of Safety (SMoS) indicator that has been previously introduced [3] and is specifically tailored to measure safety risk in V2X-based applications.

$$SRI = (t_{MSG} - t_{CENTER}) \cdot d_{SS} \tag{3}$$

To assess the risk of a hazardous event, we estimated parameter values that directly correlate with the probability and severity of a collision resulting from delayed or missed reception of V2X safety messages. The time difference between the reception of the V2X message (t_{MSG}) and the center of the safe interval (t_{CENTER}) determines the probability of delayed or missed reception. Severity is proportional to the kinetic energy of the collision [26], as per Equation 4. Therefore, we can represent severity by d_{SS}, which is approximately proportional to the square of the velocity.

$$d_{SS} = (v_{HV} \cdot t_{PR}) + \frac{v_{HV}^2}{2 \cdot \mu \cdot g} + d_{safe} \tag{4}$$

where,

- d_{SS} is the stopping sight distance in [m];
- v_{HV} is the speed of the HV in $[\frac{m}{s}]$;
- t_{PR} is the perception-reaction time [s];
- μ is the friction coefficient;
- g is gravitational acceleration in $[\frac{m}{s^2}]$;
- d_{safe} is the safe stopping distance in [m].

In [3] we previously presented the SRI indicator for the Forward Collision Warning (FCW) type safety application. In this article, we adapted the SRI to SCP scenarios. When applying the SRI approach to intersection scenarios, we examined the cases where the ego vehicle collides with the crossing vehicle from the side. In this case, we assumed that the velocity vector of the remote vehicle is perpendicular to the velocity vector of the host vehicle.

In the next step we estimate the relationship between the risk of crossing vehicle movements and the QoS parameters (Eq. 5) depending on PDR, E2E, v_{RV}, v_{HV}. The following ML models were applied to reveal the correlation between the studied factors: Ordinary Least Squares Polynomial Regression (OLS-PR), Support Vector Regression (SVR), Feedforward Neural Network (FFNN) and Random Forest (RF) [27]. The input features of the regression models are presented on the right side of the Eq. 5.

$$SRI_{NPM} = f(v_{HV}, v_{RV}, PDR, E2E) \tag{5}$$

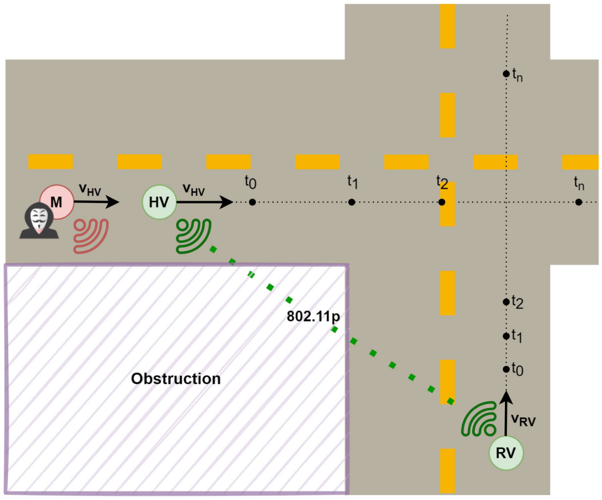


Fig. 2. Network simulation mobility scenario with two vehicles (HV, RV) and one malicious node (marked with M).

D. Network Simulation

We used the open-source discrete-event simulator `ns-3` to model wireless communication process (see Figure 1 - `NS3 static network simulation` block). Benin et al. [28] validated that these models can accurately model the physical propagation characteristics of 5.9 GHz radio waves under certain parameter settings.

In the simulated scenarios, HV and RV transmit periodic CAMs with a frequency of 10 Hz with an average packet size of 350 bytes [29].

In our research, we conducted a comprehensive exploration of propagation models to replicate a well-understood output characteristic – the relationship between PDR and inter-vehicular distance. After experimenting with multiple configurations, we opted for a hybrid approach, combining the `Nakagami-m` fading model with the `ThreeLogDistance` propagation model. The Nakagami-m model introduced statistical fading effects, allowing us to simulate NLoS conditions, where signal strength fluctuates due to obstructions or reflections. However, we encountered a challenge with limited communication range. To address this issue, we implemented an adaptive transmitter power strategy, varying the power level according to inter-vehicular distance (see power level values in Table II). This compensation effectively extended our communication range to match with analytical results [30] and real world measurements [31]. Notably, our scenario, despite lacking physical obstructions, matched NLoS characteristics due to virtual obstructions (See Fig. 2), which significantly impacted radio propagation.

In our simulation methodology, we established driving scenarios wherein the trajectory of each vehicular node was discretized into a series of fixed trajectory points. Network performance metrics were computed at each of these static positions. To facilitate this process, we employed the `ConstantPositionMobilityModel` to manipulate the relative air distances between vehicles. Consequently, for each specific driving scenario, we subdivided the trajectories of the two vehicles into equidistant points. Subsequently, the

TABLE II
NS3 PARAMETERS FOR THE VEHICULAR COMMUNICATION SIMULATIONS

Common parameters	**Values**
Mac Helper	`WifiMacHelper`
Mac Type	`AdhocWifiMac`
PHY standard	`WIFI_STANDARD_80211p`
PHY mode	`OfdmRate6Mbps` (Data rate = 6 Mbps)
Propagation Delay Model	`Constant Speed`
Propagation Loss Model	`Three Log Distance` d0: 1.0, d1: 250, d2: 400 e0: 1.9, e1: 6.0, e2: 4.65
Propagation Fading Model	`Nakagami-m` d1: 80, d2: 200 m0: 0.25, m1: 0.75, m2: 0.75
Error rate model	`YansErrorRateModel`
Channel bandwidth	10 MHz
Transmission power levels	[10 dB, 11 dB, 14 dB, 16 dB, 18 dB]
CAM transmit frequency	10 Hz
CAM packet length	350 bytes
Max. range (NLOS link)	400 m
Simulation time	10 s
Attack parameters	**Values**
Attack rate (AR)	[0 ... 6] Mbps (step = 0.5 Mbps)
Attack packet length (APL)	[100 ... 1000] bytes, (step = 100 bytes)

network metrics generated for each scenario were derived by calculating the mean values across all the individual points. This systematic approach allowed us to rigorously evaluate and analyze network performance under various conditions.

For measuring network performance metrics, `ns-3` provides several tools and methods for a simulated network. We used the `FlowMonitor` module, which is specifically designed to measure network performance metrics at the flow level. During the network simulation, this module collects real-time statistics for each data link in the network, including the number of packets exchanged, packet loss rate, delay, jitter and throughput.

Based on the six driving scenarios (Table I) and the attack parameters (attack packet length, attack rate), 780 scenarios were simulated for a total of 15,600 unique test points. The dataset created with the above settings during the tests was made available in the Zenodo open repository [32].

E. Risk Estimation Based on Attack Parameters

As discussed earlier, availability can be significantly affected by DoS-type attacks [22], therefore network performance parameters can degrade. DoS-type attacks can be implemented in such a way that the routing services are disrupted, thus, the given node will be forced into isolation and no longer transmit V2X messages. Cyberattack can force the network nodes to drop data packets or even flood the V2X communication channel with meaningless messages and unnecessary route request messages (RREQ) [33], [34]. Most DoS-type attacks affect the network and transport layers (according to OSI model) of network nodes (OBUs). Additionally, physical layer attacks, such as jamming (disrupting radio signals with overpowered signals), influence the arrival of already packets.

Based on our assumptions, the intruder node has already infiltrated the vehicular communication system and possesses a valid authentication certificate. As a result, the malicious node can transmit corrupted V2X messages to other vehicles, thereby causing the recipient node to perceive them as authentic messages. We put the focus on high risk and hard-to-detect scenarios, therefore, we modelled the attack using standard communication protocols. To make it more difficult to detect, we considered unicast communication to make the attack more efficient, as unicast transmissions require acknowledgements from the receiver, which adds overhead in terms of signalling and processing time. If the network is congested due to a DoS attack, these acknowledgments may be delayed or lost, resulting in increased latency as the sender needs to retransmit packets.

We investigated a possible attack scenario (see Fig. 2), that describes when the attacker floods the V2X communication channel, which can be described as follows:

- The attacker positions itself close to the target vehicle.
- The attacker generates a large number of messages to flood the V2X communication channel.
- Intense messaging causes the V2X communication channel to become congested, potentially making it difficult for the target vehicle to receive legitimate messages from other nearby vehicles.
- As a result, the legitimate nodes may experience delays or be unable to receive critical safety-related messages, such as warnings about potential collisions or hazardous road conditions.
- If the attack is successful, the quality of communication between the target vehicle and other vehicles can deteriorate, leading to potentially dangerous situations on the roads.

To study the impact of the attack, we needed to differentiate the strength of the attack based on the primary communication parameters. Thus we considered two communication parameters: the attacker's data transmission rate (AR) and the attack packet's length (APL). We divided the AR and APL values into three categories each, as follows:

- **No attack** - is the case when there is no attack, but we still evaluated the SRI based on the PDR and E2E. This can be the base of comparison.
- **AR1** - this category includes lower data rates [0.5 - 3 Mbps];
- **AR2** - this category includes higher data rates [3.5 - 6 Mbps];
- **APL1** - this category includes the 100 - 300 byte long packets;
- **APL2** - this category includes the 400 - 600 byte long packets;
- **APL3** - this category includes the 700 - 1000 byte long packets.

Dos-type attacks typically have a cascading effect on different layers of the ITS stack [33], mostly affecting bandwidth, so we need to investigate how channel saturation affects network performance metrics.

Accordingly, in the next step, the PDR and E2E values were calculated from the simulation data in each static measurement point. The network performance metrics of the static measurement points were then averaged per scenario. Using this data, the characteristic SRI values of the scenarios were calculated (see Figure 1 - SRI_{NPM} `regression` block) using the adapted SRI ML models. This enabled the identification of the optimal ML model that best describes the relationship between the scenario-specific AR and APL values and the SRI indicator (see Figure 1 - SRI_{ATT} `regression` block). The general form of the function (Eq. 6) relating the attack parameters, the vehicle speeds under consideration (as input features) and the safety risk (as the output variable) is given below.

$$SRI_{ATT} = f(v_{HV}, v_{RV}, AR, APL) \tag{6}$$

To select the appropriate regression model, several ML methods were compared. In a first step, OLS-PR analysis was performed assuming a nonlinear relationship. The polynomial reduction was performed using the backward elimination method, and components with less influence on the efficiency of the estimation were removed from the regression function. The elimination criterion was to ensure that the change in R-squared (R^2) remained below 10%. Besides OLS-PR, we investigated RF regression which is a flexible ML method for estimating the nonlinear relationship between different variables. It aggregates the predictions of various decision trees to minimise overfitting and enhance accuracy. Another model examined was SVR, which is used to identify a function that best predicts the continuous output variables for a given regression problem by capturing complex patterns. Finally, we implmented a FFNN, which can learn hierarchical representations of the input features through the hidden layers. Each hidden layer learns to extract and transform features from the previous layer, enabling the network to discover relevant representations of the data for regression tasks.

Utilizing the formulated estimation models, it becomes feasible to establish a framework for the risk factors (see Figure 1 - `Risk classification matrix` block) that is compatible with the Automotive Safety Integrity Level (ASIL) related standard [15]. We can then identify the critical cases (see Figure 1 - `Critical case identification` block) and carry out a more in-depth analysis.

IV. Results and Discussion

In this section, we derive the impact of attack characteristics on communication parameters and safety risk based on a systematic analysis of the given attack mechanism. Firstly, the relationship between the relevant attack parameters (AR, APL) and the network performance metrics (PDR, E2E) is described. Using the developed risk estimation methods, we investigate the relationship between VDPs, NPMs and safety risk.

Finally, a detailed analysis of the relationship and interactions among the attack, communication quality, and safety risk in selected critical scenarios was performed.

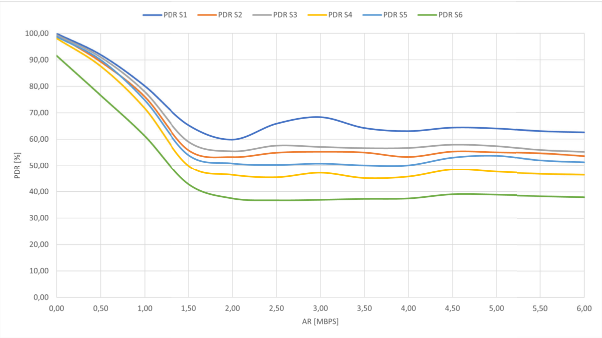


Fig. 3. PDR mean values for each scenario (S1-S6) for different attack rates (AR).

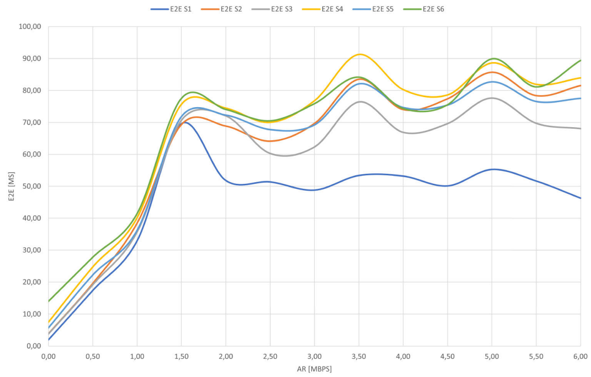


Fig. 4. E2E mean values for each scenario for different attack rates (AR).

A. Simulation Results

Considering the relevant attack parameters and the network performance metrics, the effect of different attack rates on PDR was analyzed.

It can be observed in Fig 3 that there is a breakpoint (over 1.5 Mbps) beyond which the increasing DoS attack rate (AR) does not further degrade the PDR significantly. The main reason for this is that the communication protocol defines standard methods (such as Carrier Sense Multiple Access/Collision Avoidance - CSMA/CA) that have a significant impact on the temporal distribution of packets. This includes variables such as the interval between successive transmissions and the effective utilisation of the channel, as indicated by Inter-Frame Space (IFS) values and the Contention Window (CW) value adjusted in accordance with the backoff algorithm. In line with the above, we also tested, on a purely experimental basis, what would happen if we deviated from the standard protocol and minimised the different inter-packet intervals. In fact, we did see a significant reduction in the PDR.

Figure 3 indicates that the speed of the two vehicles involved in the driving scenario significantly impacts the sensitivity of the communication quality (particularly the PDR) to the attack (the speeds corresponding to S1-S6 scenarios in Table I). Accordingly, S6 is the most sensitive to the specified DoS attack, in which both involved vehicles have the highest speed among the examined scenarios. In line with this, S1 is the least sensitive to the given attack type.

Figure 4 shows that latency growth slows significantly after the AR threshold of 1.5 Mbps. This phenomenon is essentially due to the unicast nature of the communication, as increased channel contention and potential packet loss results in a significant delay in transmission. Consistent with the literature [35], our tests in broadcast communication environments generally showed latencies of less than 1-2 ms, with a monotonically increasing characteristic. For APL, the simulation shows that the PDR and E2E degrade up to about 200 bytes, but beyond this threshold the effect of the change in APL on the NPMs is not significant. As a result of the network simulation, the AR, APL, PDR and E2E values are available for the scenarios tested (see Figure 1 - block 6, AR and APL values in Table II). Based on this, the SRI values of the scenarios were determined using the developed ML models. The estimation models linking VDPs, AR, APL and SRI_{ATT} were then identified.

B. Comparison of Different Regression Models

In a first step, the relationships between the data provided by the V2X HiL simulation and the calculated SRI_{NPM} were investigated using the different methods. In the case of the polynomial function, the second-degree forms of the factors and their combined multiplications ($R^2 = 0.95$) were used. The reason for this is that increasing the number of degrees in a polynomial may increase the achievable correlation, but it also significantly raises the probability of overfitting. A shallow FFNN model (with one hidden layer; [64,32,1]) was applied with ReLU (rectified linear unit) activation functions in the hidden layer and a linear function in the output layer. For the training process, the 'Adam' optimizer algorithm was applied using the Mean Square Error (MSE) and R^2 as performance indicators. The number of neurons significantly affects the efficiency of the FFNN model; an inadequate number of neurons will deteriorate the generalisation ability of the model as it cannot represent different nonlinear functions, while too many neurons will significantly prolong the training time and even lead to overtraining. A number of experiments were carried out to train the FFNN with different numbers of neurons in order to define the best performing network ($R^2 = 0.92$). In order to identify the appropriate SVR model, it is necessary to set the hyperparameters C and ϵ in a reasonable way, and to select proper kernel type as inappropriate parameterisation will degrade the performance of the model. In this case, the optimal values of the parameters were $C = 8, \epsilon = 0.01$ and the applied kernel was radial basis function ($R^2 = 0.9$). Using the RF algorithm, we set the number of estimators and the chosen criterion function to calibrate the regression method. In this case, we used 100 trees and the Poisson criterion to measure the quality of the split ($R^2 = 0.93$). The ML methods presented were then used to investigate the relationships between the data obtained from the attack simulation and the estimated SRI_{ATT}. For the polynomial function, the third-degree forms of the factors and their combined multiplications ($R^2 = 0.98$) were used. The shallow FFNN model was applied with the same inner architecture as previously ($R^2 = 0.98$). The SVR method was applied with the following optimized parameters $C = 1, \epsilon = 0.01$ with radial basis function ($R^2 = 0.97$). In this case of RF method, we used the same parametrization as in the case of SRI_{NPM} estimation ($R^2 = 0.99$).

TABLE III
COMPARISON OF IMPLEMENTED ML REGRESSION MODELS BASED ON R^2

	OLS-PR	FFNN	SVR	RF
SRI_{NPM}	0.95	0.92	0.9	0.93
SRI_{ATT}	0.98	0.98	0.97	0.99

Table III summarises the R^2 values of the compared ML models.

Based on the R^2 correlation indicator, it can be concluded that OLS-PR gave the best results for SRI_{NPM}, while RF proved to be the most accurate regression estimator for SRI_{ATT}.

The developed estimator methods can be integrated into a cybersecurity framework so that once an attack is detected, the system can estimate the expected impact of the attack on vehicle safety risk.

Applying a network monitoring module, the regression estimator can effectively detect anomalies or suspicious patterns in V2X communication by incorporating features such as PDR and E2E. This is critical for early threat detection in next-generation intrusion detection systems (IDSs), enabling timely response to potential security incidents. The estimator's ability to account for factors such as VDPs further enhance its adaptability to dynamic conditions, making it well suited for improved IDSs that need to respond to evolving threats in real-time. Adaptive security solutions can modify 802.11p PHY layer parameters (e.g. modulation coding scheme, channel switching, transmit power) or tune the VDPs to achieve a tolerable risk level in response to changing network conditions.

C. Risk Classification Framework

With the input and output factors of the network simulation (AR, APL, PDR, E2E), risk estimation was performed using SRI_{NPM} and risk classes were defined based on the resulting dataset.

According to Table IV, as AR and APL increase, so does the risk of the adverse impact of an unexpected event caused by an attack. It can also be observed that higher vehicle speeds result in increased safety risk. In order to get a more comprehensive picture of the consequences of the risk values presented, a detailed interpretation of the risk level of a possible scenario is presented below. For example, considering scenario S6, with attack factor pair `[APL = 300 bytes, AR = 4 Mbps]`, it is possible to estimate the packet delivery ratio and the latency.

This approach is well suitable for performing Threat Analysis and Risk Assessment (TARA) since we can determine the scenario parameters by identifying VDPs and can model the impact of different DoS attack scenarios by tuning attack parameters. For Connected and Automated Vehicles (CAVs), it will be possible to integrate the associated risk function into the control concept at the design stage of the ADAS/ADS functions and to minimise the high-risk domains associated with the Operational Design Domain (ODD).

TABLE IV

SRI_{ATT} VALUES ACCORDING TO ATTACK MATRIX (SEE AR$_{CAT}$ AND APL$_{CAT}$ DESCRIPTIONS IN SUBSECTION III-E)

	AR$_{CAT}$	No	AR1			AR2		
	APL$_{CAT}$	Attack	APL1	APL2	APL3	APL1	APL2	APL3
v$_{HV}$	**v$_{RV}$**							
40	20	0.000	0.003	0.002	0.003	0.002	0.003	0.004
70	50	0.056	0.022	0.024	0.022	0.016	0.012	0.009
	20	0.012	0.039	0.044	0.046	0.054	0.060	0.069
100	50	0.028	0.025	0.025	0.026	0.031	0.031	0.040
	20	0.087	0.081	0.090	0.088	0.089	0.097	0.109
130	50	0.178	0.194	0.188	0.191	0.193	0.192	0.237

In terms of severity, in the investigated test cases, the largest possible instantaneous theoretical kinetic energy change can occur during the deceleration from 130 km/h to 0 km/h, which can conceivably occur in connection with the S6 scenario. In the case of perpendicular transverse vehicle motions, if the mass of the host vehicle is orders of magnitude less than the mass of the remote vehicle (e.g., the remote vehicle is an oversized heavy truck), and if the crossing remote vehicle's perpendicular velocity component - which is parallel to the host vehicle's velocity - is zero, then the collision energy likely approaches the theoretical upper limit. Consequently, we can also expect that the biomechanical load on the human body approaches the introduced theoretical upper limit in this scenario.

In the case of an 80 kg person, during sudden deceleration from 130 km/h to 0 km/h, the theoretical upper limit of the change in the kinetic energy of the human body is $\Delta K_{e,130} = \frac{1}{2} \cdot 80 \cdot (\frac{130}{3.6})^2 = 52160.5\ J$. However, similarly to the probability of occurrence (P_{exp}) we would like the value of severity indicator to fall between 0 and 1. Thus, we use the normalized values of the expected change in kinetic energy. In accordance with this, if we consider a 70 km/h scenario, the theoretical upper limit of the change in the kinetic energy of the human body is $\Delta K_{e,70} = \frac{1}{2} \cdot 80 \cdot (\frac{70}{3.6})^2 = 15123.5J$, in which case the normalized severity value can be calculated as the ratio of scale interval's upper boundary and the investigated indicator value $S = \frac{K_{e,70}}{K_{e,130}} = 0.29$. In addition to quantifying the severity, the presented method can also be used to support estimation procedures for expected injuries; since by specifying the examined scenario and the modeled collision speed, it is already possible to estimate risk related to Abbreviated Injury Scale (AIS) levels, using previous research results of the field [36]. For example, in the case of a side collision, in which the investigated vehicles travel at 70 km/h, the expected probability that the investigated accident will have a severe or fatal outcome (MAIS3+F) is more than 50% [36].

Therefore, the risk values above 0.2 in the presented risk classification matrix can be interpreted as the product of a high occurrence probability value (e.g., 0.237) and a high severity indicator value (e.g., 1). As we can see, the introduced classification method can estimate the risk level of typical scenarios and compare the impact of different attacks on vehicle safety.

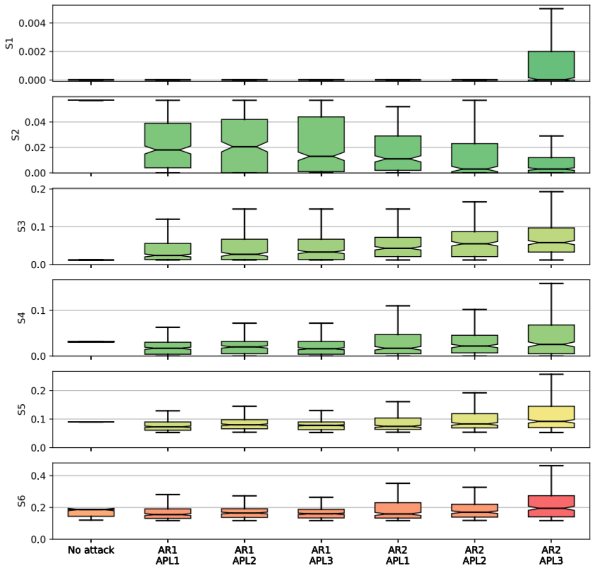


Fig. 5. Box plot diagrams for SRI_{ATT} values.

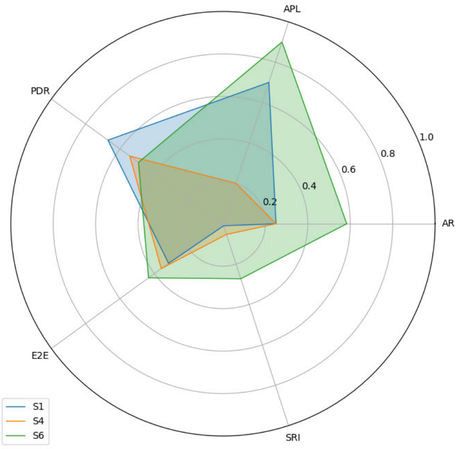


Fig. 6. Representation of certain safety-critical cases on a radar chart.

Displaying the results in a boxplot diagram (see Figure 5) can provide further valuable insight into the relationship between attack and risk, as it includes information on the variance, range, minimum and maximum values of the patterns, in addition to the scenario averages.

The boxplot indicates that as the values of the (AR, APL) pair increase, the expected risk of an accident resulting from a DoS attack exhibits greater variability across most scenarios. As the (AR, APL) value pairs increase, providing a precise estimate of the anticipated risk of a DoS attack-related accident becomes increasingly challenging. It is worth mentioning that in S2, except for the no-attack scenarios, the anticipated risk values for the attack have a considerable degree of variation. However, it is important to note that the highest estimated risk value for S2 is reasonably low.

Specific cases have been selected for further analysis to illustrate (see Fig. 6) the interaction of cyber-physical factors concerning DoS attacks. The axes show the normalized values of the cyber-physical factors under investigation. After removing the outliers, the maximum values considered are, in consecutive order, AR = 6 Mbps, APL = 1000 bytes, PDR = 100%, E2E = 410 ms, and SRI = 1.

In the first investigated case (S1 - marked in blue in Fig. 6), the attack occurs in low-speed conditions (20 and 40 km/h). The APL is 700 bytes, and the AR is 1.5 Mbps. The estimated PDR resulting from the DoS attack is 67%, and the associated delay E2E = 130 ms. The network performance parameter values indicate that the attack's impact is significant, but the vehicle safety risk level is not high (SRI = 0.01). This is mainly due to the low-speed conditions.

In the second investigated case (S4 - marked in orange in Fig. 6), the attack occurs in medium-speed conditions (50 and 100 km/h). The APL is 200 bytes, and the AR is 1.5 Mbps. The anticipated PDR due to the DoS attack is 54.3%, and the corresponding E2E delay is 147 ms. Although the network performance parameter values suggest a notable impact of the attack, the risk to vehicle safety remains low (SRI = 0.053). Detecting this attack can be difficult, as the AR and APL are relatively low, and the APL is similar in size to an average CAM message. Nevertheless, it is an effective attack, as it achieves a significant impact in terms of PDR and E2E.

In the third case (S6 - marked in green in Fig. 6), the attack occurs in relatively high-speed conditions (50 and 130 km/h). The APL is 900 bytes, and the AR is 3.5 Mbps. The expected PDR resulting from the DoS attack is 49.2%, and the associated E2E delay is 177.7 ms. These network performance parameter values indicate a considerable impact of the attack, and the safety risk level is also markedly high in this case (SRI = 0.272). The high SRI value is mainly due to the fact that the speed difference between the two vehicles is 80 km/h, which is considered high, and also because of the PDR, every second message is received with a relatively high latency.

V. Conclusion

This paper focuses on examining the impact of specific cyber attacks (DoS) on vehicle safety by varying communication parameters such as packet length and attacker data rate in a simulation of six different scenarios. As a main result, our methodology enables a comprehensive, systematic and standardised assessment of cyber threat risks and help develop effective risk mitigation strategies in the context of automotive safety standards and requirements.

Following the generated boxplot diagrams, we also recognized that as the applied attack factors increase, the standard deviation of the expected risk also becomes larger, which significantly complicates the estimation of risk values during an intensive attack process. For analyzing additional scenarios, the method presented should be used to estimate a new SRI function. The propagation loss models used in ns-3 are specific to the scenarios studied and, therefore, cannot be generalized in their present form. The radio propagation models and their parameters have to be adapted for different scenarios and environments. In the present research, the type of attack that has a significant impact on the availability of information was investigated, for other types of attacks the methodology needs to be adapted.

To summarize the purpose and applicability of the developed methodology, we can say that the presented approach allows to test V2X-based vehicle functions from a cyber security point of view and to explore the correlations between cyber-physical parameters, with particular attention to the characteristics of the cyber attacks under investigation. Given the dynamic nature of ad hoc networks, real-time threat detection and response mechanisms becoming crucial. Our research shows that the network performance may vary rapidly, necessitating adaptive security solutions capable of responding swiftly to emerging threats or disruptions [37]. Following this, the presented methodology is capable of quantifying risk associated with DoS-like attacks and supports development and testing of defensive strategies. By using attack rate and attack packet length parameters, our method increases the realism of the simulations, helping to identify and proactively detect cyber threats, thereby enhancing intrusion detection capabilities. As real-time risk assessment plays an important role in adaptive security solutions, our methodology contributes to an immediate response to detected malicious intrusions. Consequently, by incorporating an ASIL-like framework, our approach facilitates the development of inherently secure systems that can dynamically respond to changing threat levels, thereby ensuring the resilience and security of C-ITS.

References

[1] Z. Su, Y. Hui, and Q. Yang, "The next generation vehicular networks: A content-centric framework," *IEEE Wireless Commun.*, vol. 24, no. 1, pp. 60–66, Feb. 2017.

[2] W. W. Wen and L.-T. Hsu, "3D LiDAR aided GNSS NLOS mitigation in urban canyons," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 18224–18236, Oct. 2022.

[3] Z. Pethő, Z. Szalay, and Á. Török, "Safety risk focused analysis of V2V communication especially considering cyberattack sensitive network performance and vehicle dynamics factors," *Veh. Commun.*, vol. 37, Oct. 2022, Art. no. 100514.

[4] G. De La Torre, P. Rad, and K.-K.-R. Choo, "Driverless vehicle security: Challenges and future research opportunities," *Future Gener. Comput. Syst.*, vol. 108, pp. 1092–1111, Jul. 2020.

[5] Q. Yang, S. Fu, H. Wang, and H. Fang, "Machine-learning-enabled cooperative perception for connected autonomous vehicles: Challenges and opportunities," *IEEE Netw.*, vol. 35, no. 3, pp. 96–101, May 2021.

[6] F. A. Teixeira, V. F. E. Silva, J. L. Leoni, D. F. Macedo, and J. M. S. Nogueira, "Vehicular networks using the IEEE 802.11p standard: An experimental analysis," *Veh. Commun.*, vol. 1, no. 2, pp. 91–96, Apr. 2014.

[7] Z. Abdollahi Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, Dec. 2018.

[8] J. Thunberg, D. Bischoff, F. A. Schiegg, T. Meuser, and A. Vinel, "Unreliable V2X communication in cooperative driving: Safety times for emergency braking," *IEEE Access*, vol. 9, pp. 148024–148036, 2021.

[9] Z.-Q. Liu, X. Ge, Q.-L. Han, Y.-L. Wang, and X.-M. Zhang, "Secure cooperative path following of autonomous surface vehicles under cyber and physical attacks," *IEEE Trans. Intell. Vehicles*, vol. 8, no. 6, pp. 3680–3691, Jun. 2023.

[10] X. Zhao, S. Jing, F. Hui, R. Liu, and A. J. Khattak, "DSRC-based rear-end collision warning system—An error-component safety distance model and field test," *Transp. Res. C, Emerg. Technol.*, vol. 107, pp. 92–104, Oct. 2019.

[11] E. Moradi-Pari, D. Tian, M. Bahramgiri, S. Rajab, and S. Bai, "DSRC versus LTE-V2X: Empirical performance analysis of direct vehicular communication technologies," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 5, pp. 4889–4903, May 2023.

[12] X. Sun, F. R. Yu, and P. Zhang, "A survey on cyber-security of connected and autonomous vehicles (CAVs)," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6240–6259, Jul. 2022.

[13] A. Alnasser, H. Sun, and J. Jiang, “Cyber security challenges and solutions for V2X communications: A survey,” *Comput. Netw.*, vol. 151, pp. 52–67, Mar. 2019.

[14] F. Santoso and A. Finn, “A data-driven cyber–physical system using deep-learning convolutional neural networks: Study on false-data injection attacks in an unmanned ground vehicle under fault-tolerant conditions,” *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 53, no. 1, pp. 346–356, Jan. 2023.

[15] *Road Vehicles—Functional Safety*, Standard ISO 26262, Int. Org. Standardization, 2018. [Online]. Available: https://www.iso.org/standard/68383.html

[16] Á. Török, Z. Szalay, and B. Sághi, “New aspects of integrity levels in automotive industry-cybersecurity of automated vehicles,” *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 1, pp. 383–391, Jan. 2022.

[17] M. A. Javed and E. B. Hamida, “On the interrelation of security, QoS, and safety in cooperative ITS,” *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 7, pp. 1943–1957, Jul. 2017.

[18] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and Y. Chen, “Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions,” *Accident Anal. Prevention*, vol. 148, Dec. 2020, Art. no. 105837.

[19] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, “Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks,” *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 110–113, Jan. 2014.

[20] N. Lyamin, D. Kleyko, Q. Delooz, and A. Vinel, “Real-time jamming DoS detection in safety-critical V2V C-ITS using data mining,” *IEEE Commun. Lett.*, vol. 23, no. 3, pp. 442–445, Mar. 2019.

[21] K. Kim, D. Kwon, W.-C. Jin, S. Choi, J. Kim, and J.-W. Choi, “Fatal C-V2X denial-of-service attack degrading quality of service in a highway scenario,” *J. Commun. Netw.*, vol. 26, no. 2, pp. 182–192, Apr. 2024.

[22] G. Twardokus and H. Rahbari, “Towards protecting 5G sidelink scheduling in C-V2X against intelligent DoS attacks,” *IEEE Trans. Wireless Commun.*, vol. 22, no. 11, pp. 7273–7286, Nov. 2023.

[23] Y. Xiao, Q. Du, Y. Zhang, and C. Lu, “Secure vehicular communications with varying QoS and environments: A unified cross-layer policy-adaptation approach,” *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 11, pp. 13462–13471, Nov. 2023.

[24] J. Petit and G. Le Lann, “Next generation vehicles, safety, and cybersecurity—The CMX framework,” *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 2, pp. 1333–1345, Feb. 2024.

[25] Y. Ali, A. Sharma, M. M. Haque, Z. Zheng, and M. Saifuzzaman, “The impact of the connected environment on driving behavior and safety: A driving simulator study,” *Accident Anal. Prevention*, vol. 144, Sep. 2020, Art. no. 105643.

[26] A. Sobhani, W. Young, D. Logan, and S. Bahrololoom, “A kinetic energy model of two-vehicle crash injury severity,” *Accident Anal. Prevention*, vol. 43, no. 3, pp. 741–754, May 2011.

[27] H. You et al., “Comparison of ANN (MLP), ANFIS, SVM, and RF models for the online classification of heating value of burning municipal solid waste in circulating fluidized bed incinerators,” *Waste Manage.*, vol. 68, pp. 186–197, Oct. 2017.

[28] J. Benin, M. Nowatkowski, and H. Owen, “Vehicular network simulation propagation loss model parameter standardization in ns-3 and beyond,” in *Proc. IEEE Southeastcon*, Mar. 2012, pp. 1–5.

[29] *Survey on Its-G5 CAM Statistics*, document TR2052, CAR 2 CAR Commun. Consortium, Dec. 2018.

[30] M. Sepulcre, M. Gonzalez-Martín, J. Gozalvez, R. Molina-Masegosa, and B. Coll-Perales, “Analytical models of the performance of IEEE 802.11p vehicle to vehicle communications,” *IEEE Trans. Veh. Technol.*, vol. 71, no. 1, pp. 713–724, Jan. 2022.

[31] Z. Liu, Z. Liu, Z. Meng, X. Yang, L. Pu, and L. Zhang, “Implementation and performance measurement of a V2X communication system for vehicle and pedestrian safety,” *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 9, Sep. 2016, Art. no. 155014771667126.

[32] Z. Pethő, T. M. Kazár, and Á. Török, “Safety impact of DoS attacks on V2X-based collision warning (version v1) [data set],” Tech. Rep., 2024, doi: 10.5281/zenodo.12155930.

[33] W. Ahmed and M. Elhadef, “DoS attacks and countermeasures in VANETs,” in *Advanced Multimedia and Ubiquitous Engineering*. Berlin, Germany: Springer, 2018, pp. 333–341.

[34] A. Kumar et al., “Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm,” *Microprocessors Microsystems*, vol. 80, Feb. 2021, Art. no. 103352.

[35] X. Ma, X. Chen, and H. H. Refai, “Performance and reliability of DSRC vehicular safety communication: A formal analysis,” *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, pp. 1–13, Dec. 2009.

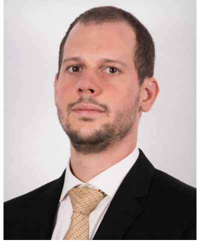
[36] S. D. Doecke, J. K. Dutschke, M. R. J. Baldock, and C. N. Kloeden, “Travel speed and the risk of serious injury in vehicle crashes,” *Accident Anal. Prevention*, vol. 161, Oct. 2021, Art. no. 106359.

[37] Z. Pethő, T. Kazár, R. Nagy, H. Dulaimi, and Á. Török, “New challenges in testing connected and cooperative transport systems,” in *Proc. FISITA World Automotive Congr.*, 2023.

Zsombor Pethő received the B.Sc. degree in electrical engineering from the Technical University of Cluj-Napoca and the M.Sc. degree in control engineering from Budapest University of Technology and Economics in 2019. He is currently pursuing the Ph.D. degree with the Department of Automotive Technologies, Budapest University of Technology and Economics. His research interests include CCAM mobility, V2X communication, in-vehicle networks, cyber-physical systems, and safety-security co-engineering.

Tamás Márton Kazár received the B.Sc. degree in mechanical engineering from Miskolc University and the M.Sc. degree in vehicle engineering in Budapest in 2022. He is currently a Researcher with the Department of Automotive Technologies, Budapest University of Technology and Economics. His research focuses on safety aspects of V2X communication, ADAS, and ADS function testing and validation. He has experience in simulation frameworks.

Zsolt Szalay received the M.Sc. degree in electrical engineering from Budapest University of Technology and Economics (BME) in 1995, the M.Sc. degree in business administration from Corvinus University in 1997, and the Ph.D. degree in mechanical engineering from BME in 2002. He is currently an Associate Professor and the Head of the Department of Automotive Technologies, Budapest University of Technology and Economics. His research focuses on advanced automotive technologies for testing and validating highly automated and autonomous mobility.



Árpád Török received the Graduate degree in transportation engineering and the Ph.D. degree from TU Budapest in 2006 and 2010, respectively. He has been with the Department of Automotive Technologies since 2018. He is currently the Head of the Safety and Security Research Team. His research team focuses on automotive safety and security analysis, especially considering the aspects of integrated methods. He has been a member of the Association for Transport Sciences since 2006 and a member of the Public Board of Hungarian Scientific Academy since 2010.