Simulation Modelling Practice and Theory 136 (2024) 103005

Contents lists available at ScienceDirect

Simulation Modelling Practice and Theory

journal homepage: www.elsevier.com/locate/simpat

A simulation framework for automotive cybersecurity risk assessment

Don Nalin Dharshana Jayaratne [a,c,*], Suraj Harsha Kamtam [a,c], Siraj Ahmed Shaikh [b], Muhamad Azfar Ramli [c], Qian Lu [a], Rakhi Manohar Mepparambath [c], Hoang Nga Nguyen [b], Abdur Rakib [a]

[a] *Centre for Future Transport and Cities (CFTC), Coventry University, United Kingdom*
[b] *Systems Security Group (SSG), Department of Computer Science, Swansea University, United Kingdom*
[c] *Institute of High Performance Computing (IHPC), Agency for Science, Technology and Research (A*STAR), Singapore*

ARTICLE INFO

Keywords:
Connected vehicles
Automotive cybersecurity
Risk assessment
Simulation

ABSTRACT

Human-initiated disruptions such as cyberattacks on connected vehicles have the potential to cause cascading failures in transport systems, leading to systemic risks. ‘ISO/SAE 21434:2021 Road vehicles - Cybersecurity engineering’ is the current standard for risk management of road vehicles. However, the threat analysis and risk assessment framework given in the standard focuses on asset-level analysis and assessment. Hence, this study develops a novel simulation-based framework to perform threat analysis and risk assessment on connected vehicles from a transport network perspective. The proposed framework is developed based on the ISO/SAE 21434 threat analysis and risk assessment methodology. We demonstrate the applicability and usefulness of the framework through a remote attack via the cellular network on the in-vehicle communication bus system of a connected vehicle to show the potential impacts on the transport network. Based on the findings of our case studies, we exemplify how cyberattacks on individual system components of a connected vehicle have the potential to cause systemic failures.

1. Introduction

Traditionally, the ‘car’ was isolated in terms of connectivity from the outside world [1,2]. As a result, cybersecurity was not a significant concern for the automotive industry. However, as connected vehicles have become more prevalent, the automotive industry has become highly vulnerable to cyber attacks [3]. Automotive cybersecurity research has discovered vulnerabilities in numerous in-vehicle components such as key fobs, sensors, infotainment devices, and software that may lead to cyber-related threats. One such highly publicised cyberattack was Miller and Valasek’s Jeep hack of 2015 [4]. The attack involved remotely exploiting a vulnerability in the 2014 Jeep Cherokee’s onboard entertainment system, which was connected to the vehicle’s internal network and control systems, such as the brakes and transmission. By sending a series of adversarial messages over the Internet, the hackers could take control of the Jeep’s systems and perform a range of malicious actions, including disabling the brakes, killing the engine, and manipulating the car’s speed and steering. Such an attack exemplifies the potential risk that comes with the growing number of connected vehicles that give bad actors more attack surfaces to exploit.

[*] Corresponding author at: Centre for Future Transport and Cities (CFTC), Coventry University, United Kingdom.
E-mail addresses: jayaratned@uni.coventry.ac.uk (D.N.D. Jayaratne), kamtams@uni.coventry.ac.uk (S.H. Kamtam), s.a.shaikh@swansea.ac.uk (S.A. Shaikh), ramlimab@ihpc.a-star.edu.sg (M.A. Ramli), ad5271@coventry.ac.uk (Q. Lu), rakhimm@ihpc.a-star.edu.sg (R.M. Mepparambath), h.n.nguyen@swansea.ac.uk (H.N. Nguyen), ad9812@coventry.ac.uk (A. Rakib).

https://doi.org/10.1016/j.simpat.2024.103005
Received 16 February 2024; Received in revised form 1 July 2024; Accepted 28 July 2024
Available online 31 July 2024

Table 1
Glossary covering key terms used in this paper including references to standards.

Acronym	Description
ACC	Adaptive cruise control
CACC	Cooperative Adaptive Cruise Control
CAN	Controller Area Network
CIA	Confidentiality, Integrity, and Availability
CVSS	Common Vulnerability Scoring System
DSRC	Dedicated Short-Range Communication
ETSI	European Telecommunications Standards Institute
EVITA	E-safety vehicle intrusion protected applications
ISO/SAE 21434:2021	Standard for Road vehicles — Cybersecurity engineering risk management
LOS	Level of Service
LTE	Long Term Evolution
RSU	Road Side Unit
TARA	Threat Analysis and Risk Assessment
TRaCI	Traffic control interface
US-HCM	US Highway Capacity Manual
V2I	Vehicle-to-infrastructure
WAVE	Wireless Access in Vehicular Environments

The complexity of software stacks in modern vehicles is increasing due to the integration of systems from multiple vendors, introducing more potential ingress points for cyberattacks. This trend underscores the urgency for secure and resilient vehicular operations to avert serious safety, operational and financial consequences. The enhanced connectivity of vehicles brings heightened cybersecurity risks, with potential impacts ranging from data breaches to physical harm. To address these issues, the automotive industry is adopting Secure-by-Design principles, guided by standards such as ISO/SAE 21434 [5], which mandates Threat Analysis and Risk Assessment (TARA). However, while existing research on TARA has focused on the vehicle level, assessing threats and vulnerabilities of individual components [6–13], there is a scarcity of studies exploring the systemic effects of cyberattacks on transportation networks. Moreover, traditional TARA approaches are contingent upon the assessors' expertise, which, while adept at evaluating risks to vehicle components, may not suffice for systemic risk analysis across expansive transport networks.

The proposed work builds upon the automotive TARA approach defined in the ISO/SAE 21434 standard (cf. Section 2.2), extending it to encompass the risk of the wider transport network. In addition, it proposes employing simulation techniques to quantify the impact of cyber risk assessments, This overcomes the limitation of existing TARA methods, which rely heavily on human knowledge and are impractical for assessing systemic risks for wider transportation networks. The main contributions of the paper are summarised as follows:

1. A novel simulation-based framework for automotive cyber risk assessment, which can facilitate TARA as defined in ISO/SAE 21434. The framework incorporates a simulation platform integrating vehicle communications and microscopic traffic simulation to model and quantify cyber risks on connected vehicles;
2. Development and modelling of two case studies portraying a remote cyberattack on a connected vehicle using the proposed simulation-based framework. This is achieved using the Miller and Valasek Jeep Hack of 2015 as an example for assessing the traffic impact of a cyber threat-induced traffic incident in a quantitative manner; and
3. Operational impact analysis of resultant damage scenarios arising from the cyberattack incident.

The rest of the paper is organised as follows. Section 2 presents background information and related work necessary to understand why and how the described approach and experiment were conducted. Section 3 discusses the novel simulation-based risk assessment framework. Section 4 presents use cases of the developed framework evaluating the resulting operational impact. Finally, Section 5 concludes the paper by outlining our contributions and directions for further work. For clarity and ease of reference, a glossary of key terms used throughout this paper is provided in Table 1.

2. Background and related work

In this section, we provide a review of relevant literature on cyberattacks on connected vehicles, automotive cybersecurity risk assessment, simulation-based studies and frameworks.

2.1. Cyberattacks on connected vehicles

Connected vehicles, increasingly integrated with multiple devices, are susceptible to cyberattacks, which can be conducted remotely with minimal physical interaction, posing significant risks to vehicle security [4,14–17]. This is especially concerning as these attacks have the potential to compromise the security of multiple vehicles simultaneously.

To address these vulnerabilities, a three-layer framework for connected vehicles has been proposed by El-Rewini et al. in [10], consisting of control, communication, and sensing layers. This framework helps pinpoint critical components and their vulnerabilities, though the study primarily focuses on individual vehicle impacts rather than systemic network effects.

Table 2
Notable attacks on connected vehicles: Descriptions, attack vectors, and consequences.

Attack	Type of attack	Attack vector	Target	Result
Web-based vehicle immobilisation [14]	Spoofing	Web application vulnerability	Vehicle immobilisation system	Disabling multiple vehicles and activating secondary vehicular functions.
Miller and Valasek's remote exploitation [4]	Zero-day exploit	Open port in infotainment system	Infotainment system	Allowing remote control of steering, brakes, and transmission.
Mobile application exploitation [15]	Privilege escalation	Mobile app authentication vulnerability	Mobile application	Accessing and activating a vehicle's secondary functions (e.g., door locks, headlights, wipers, sunroof, and horn).
OBD-II device compromise [16]	Spoofing	Malicious messages via OBD-II device	Internet-enabled OBD-II devices	Breaching the vehicle's internal network and taking control of the braking system.
Car Wi-Fi network compromise [17]	Privilege escalation	Wi-Fi network vulnerability	Internal Wi-Fi network	Unauthorised access of vehicle allowing to manipulate the lights, door locks, and deactivate the car's alarm system.

The work by Malik & Sun in [18] demonstrates possible attacks on connected vehicles, including attacks on fleets, over-the-air updates, and zero-day exploits. Cyber threat analysis is done evaluating the attack feasibility, impact, and attack vectors of the cyberattacks on connected vehicles, and is simulated using the CARLA simulator. However, this research falls short in assessing the cascading effects of connected vehicle cyberattacks. Some notable connected vehicle attacks from the literature are presented in Table 2. These examples highlight various types of attacks, their vectors, targets, and consequences. Among these, the case studies presented in Section 4 are based on Miller and Valasek's remote exploitation attack.

2.2. Cybersecurity risk frameworks for automotive systems

The ISO/SAE 21434: Road vehicles — Cybersecurity engineering standard aligns with the security objectives of United Nations Regulation No. 155, which governs cybersecurity management within vehicular systems [19].

ISO/SAE 21434 sets the framework for the cybersecurity process within in-vehicle systems, provides guidance on risk mitigation and ensures consistent terminology across the domain [20]. TARA is outlined in Clause 8, dedicated to evaluating the cybersecurity risks in vehicles [5]. TARA assesses potential impacts of cyberattacks in terms of financial, safety, operational, and privacy aspects — details of which are further explored in Section 3.2. Given the widespread acceptance of ISO/SAE 21434, TARA is recognised as the standard risk assessment approach within the automotive industry.

For risk assessment, TARA presents a framework that evaluates both the feasibility of an attack and its potential impacts. This makes it adaptable for systemic risk management in the ever-evolving connected vehicle landscape. However, the scope of TARA within the standard focuses only on components inside the vehicle or components on the vehicle's perimeter. Although it acknowledges that external systems can be considered, they are not the primary focus of the standard. Moreover, the standard relies heavily on the assessors' expertise for threat and vulnerability assessment, which may not suffice for a comprehensive evaluation of systemic risks across expansive transport networks. Given these limitations, there is a pressing need for enhanced methods that can account for the broader network interactions and systemic impacts. This has motivated the development of a simulation-based framework designed to support systemic TARA and address the complex dynamics of connected vehicle environments.

Several other frameworks are commonly used for risk analysis in cyber–physical systems, emphasising the integration of safety and security concepts. The Goal Tree Success Tree-Master Logic Diagram (GTST-MLD) [21] uses a top-down approach to analyse component failures and cyber threats, particularly suitable for process industries that often lack historical data. S-CUBE [22] is a model-based risk analysis framework supporting risk assessment during design and operational phases, relying on a domain-specific language that governs occurrence and interaction rules. The Boolean Driven Markov Processes (BDMP) [23] serves as a formal graphical tool for structuring both qualitative and quantitative security analysis, offering an alternative to traditional attack tree and Petri-net methods. Conversely, CHASSIS [24] adopts a semi-formal approach geared towards requirements engineering through use cases and sequence diagrams.

While these frameworks integrate safety and security domains in more generic cyber–physical systems, our proposed framework is designed specifically for the automotive domain. Additionally, the goal of our work is not to integrate safety and security analysis but to utilise vehicular communication simulations as an additional tool for security analysts while performing TARA for connected vehicles. Further details of the systemic phenomena in the cybersecurity context are provided in Section 2.3.

2.3. Systemic risks and cascading failures

Systemic risks in interconnected networks arise from the interdependence between nodes, where effects can propagate unpredictably and are challenging to manage [25]. Quantifying such risks poses a significant challenge due to the interlinkages and complexities involved in the components of the systems.

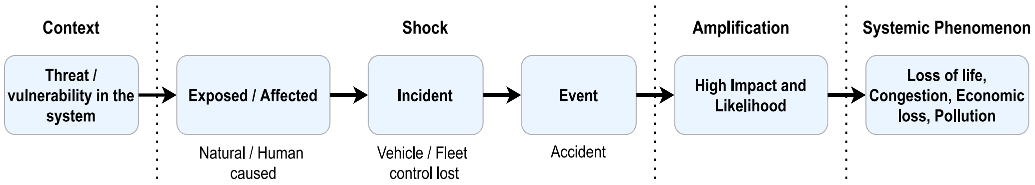
Context
Shock
Amplification
Systemic Phenomenon
Threat / vulnerability in the system
Exposed / Affected
Incident
Event
High Impact and Likelihood
Loss of life, Congestion, Economic loss, Pollution
Natural / Human caused
Vehicle / Fleet control lost
Accident

Fig. 1. Systemic risk is a combination of localised risks projected to the global system, where the global system is impacted due to cyber-attacks on individual components. Connected vehicle based systemic cyber risk model consists of four phases: Context, Shock, Amplification and Systemic Phenomenon [25,27].

The emergence of systemic risks requires three conditions to be met [26]: (i) the event must possess a reasonable attack feasibility and high impact; (ii) there must be interacting and dependent events or systems; and (iii) one failure must trigger another dependent event or system.

The systemic cyber risk model consists of four phases, namely, context, shock, amplification, and systemic event [27] (depicted in Fig. 1). The context phase in which systemic risk develops due to a cyberattack is what is referred to as the threat/vulnerability in the system. The second phase is the shock phase, which determines the impact and entails three sub-phases: exposed/affected (e.g. human-caused cyberattack), incident (e.g. vehicle attacked), and event (e.g. vehicle stopped in the middle of the motorway). Also, depending on the attacker's expertise, they might intensify the attack; this is the amplification phase which would finally trigger the last phase, a systemic phenomenon.

The failure mechanism of complex systems is unpredictable, with accidents having different chains of events leading to disasters [25]. The response of interconnected systems to external stress, safety, and security threats is often unknown, as they operate at the edge of stability, and even minor changes can cause significant disruptions. For instance, in a critical infrastructure outage, the cascading effects may decrease as they move away from the source or increase until the entire dependent network infrastructure is down. The robustness of a network can be compromised by cascading failures that have domino-like effects, such as blackouts, congestion, and bankruptcies [28].

2.4. Urban road network risk

Understanding the existing works related to urban road network risk is crucial for our study as they provide the relevant information for building a simulation-based systemic risk assessment framework for connected vehicles. Hence, this section discusses the literature on urban road network risk assessment. In a study done evaluating urban road network vulnerability and resilience to large-scale attacks Vivek & Conner [29], developed a framework for quantifying, detecting, and mitigating the cascading consequences of targeted attacks on road transportation networks, using a combination of theory, traffic modelling, network analysis, and GPS trip data. They applied this framework to the urban road network of Boston and showed that targeted removal of a small fraction of nodes leads to disproportionately larger disruptions of routes and subsequent city-scale traffic jams within a couple of hours. However, the authors also noted some limitations of their work, such as the need for more consideration of the impact of existing traffic jams prior to the attacks and the lack of consideration of recovery where emergency personnel would assist in removing road blockages caused by malicious actors. They have further emphasised the importance of considering various local disruptions caused by different types of cyber attacks on connected transport networks.

The previous study primarily discussed the impact of targeted attacks on the macroscopic scale of urban road transportation networks. However, it lacked consideration for the impact of attacks at the microscopic level and the potential consequences on network resilience. Additionally, the study modelled network disruptions and cascades, assuming that nodes and edges operate binarily without considering the layered structure of transportation networks. Furthermore, the study does not model cyberattacks specifically. In contrast, our research will complement the existing literature by addressing the gap in research in understanding the systemic cyber risks on transportation networks and their cascading effects on critical infrastructure by modelling attacks at both microscopic and macroscopic levels while considering the network's layered structure.

The study by Xu et al. [30] proposes a framework for assessing the vulnerability of freeway networks based on risk analysis by considering both the probability and consequences of vulnerability. The authors conducted network cascading failure analysis using an improved coupled map lattice model that incorporates tunnels' negative effects and optimises local traffic redistribution rules. In contrast to the reviewed literature, our research incorporates a framework for risk assessment of automotive cyber threats in connected vehicles that aligns with the ISO/SAE 21434 TARA framework, focusing on simulation-based threat attack feasibility and impact assessments.

2.5. Simulation-based platforms and studies for connected vehicles

Simulation tools are pivotal in the pre-deployment assessment of connected road transportation systems, particularly in analysing the mobility and network layers at a microscopic level. Traditional traffic simulators such as SUMO [31], VISSIM [32], and AIMSUN [33], originally designed for human-driven vehicles, now incorporate connected features. For vehicular communication network simulations, OMNeT++ [34] and NS-3 [35] are commonly used. NS-3 uses a Python scripting interface [36], whereas

OMNeT++ has a modular structure written in C++ and uses NED (NEtwork Description) language [37]. Both simulators include built-in IEEE 802.11 modules, with studies showing that NS-3 performs marginally better but has scalability issues [36–39].

The 'Veins' framework, building on OMNeT++ and SUMO, stands out with its comprehensive models for IEEE 802.11p and multi-channel DSRC/WAVE networks, extendable for various communication technologies [40]. Its real-time bidirectional coupling with SUMO through TraCI offers an ideal setup for modelling cyber threats within vehicular networks. Veins couples the network and the mobility simulator by creating a node in OMNeT++ with a network stack that includes an IEEE 802.11p wireless network interface, a beaconing protocol and one or more applications running on top of it for each vehicle travelling in SUMO.

Other commonly used co-simulators include Plexe' for platooning [41], Artery' for V2X communication based on ETSI ITS-G5 protocols [42], Open-CV2X' for LTE network simulations [43], VENTOS' for DSRC wireless communication and various driving modes [44], iTETRIS' which uses NS-3 for network simulation [45], MOSAIC' for intelligent and connected mobility [46], and 'AIMSUN' V2X SDK with VANET communication capabilities [47].

Literature on simulation-based cybersecurity for automotive systems is limited [48,49], but platforms like the 'SURE' framework for attacker-defender scenarios and integrated simulators combining SUMO, OMNeT++, and Webots for connected and automated driving dynamics have been showcased [48]. Veins' alignment with this research's needs – its open-source nature, support for relevant protocols, and large-scale simulation capability – renders it the platform of choice. Simulation for threat modelling has been explored using securiCAD [50] and CARLA [18], though these often omit the vehicular communication aspect crucial for connected vehicle threats. Other works have applied simulation for threat analysis and risk assessment (TARA), security testing, and security algorithm development [51–54], typically focusing on vehicle-level security rather than broader systemic impacts.

Addressing this gap, our research opts for Veins to capture a systemic view of cyber threats and their ramifications across transportation networks, advancing beyond the current state of mostly theoretical connected vehicle cybersecurity research.

3. Simulation-based risk assessment framework

Risk is defined as the uncertainty in a situation involving danger, loss, or harm that can impact the life, health, or environment of an individual, project, or organisation [55,56]. Thus, a risk framework should be able to analyse a use case or scenario to identify its cause, frequency, and consequences. ISO/SAE 21434 defines risk (Eq. (1)) as the uncertainty of vehicle cybersecurity expressed in terms of attack feasibility and impact [57]. Attack feasibility, also termed as threat likelihood, is the ease of successfully carrying out a set of actions that would result in a cyberattack. Impact can be defined as the 'estimate of the magnitude of damage or physical harm from a damage scenario' where a damage scenario is an 'adverse consequence involving a vehicle or vehicle function and affecting a road user'.

$$Risk = f(attack\ feasibility, threat\ impact) \tag{1}$$

Transportation systems are often designed to operate close to capacity conditions with minimal redundancies to minimise costs. However, such designs make these systems vulnerable to natural and artificial disruptions. Furthermore, the additional interdependencies introduced to the transport networks through connectivity raise further vulnerabilities that could lead to severe cascading failures throughout the transportation system.

Our proposed framework employs a simulation-based approach to assess systemic risks in connected transport networks resulting from cyberattacks on connected vehicles, as shown in Fig. 2. The framework utilises a vehicular communications-based simulation platform to model and quantify cyber risks, with a focus on remote network threats illustrated in Table 1. Our approach includes in-depth threat analysis to identify attack scenarios, which are then modelled in the simulation framework primarily for impact analysis. The attack feasibility analysis provides an assessment of the probability of a particular threat being successfully implemented, while the impact analysis assesses the consequences of the threat to the transport network. Our research emphasises the evaluation of systemic risks while also aligning with the ISO/SAE 21434 standard to ensure proper integration. Further details on the approaches and parameters of the attack feasibility and impact can be found in Sections 3.1 and 3.2.

3.1. Attack feasibility

Threat analysis and modelling of a vehicle's assets are critical components of the risk assessment process performed by OEMs and suppliers, ideally performed prior to the release of the car to the market. Therefore, performing threat analysis and modelling for each asset is essential to determine the attack feasibility of that asset being compromised. The overall attack feasibility for a car combines all possible attacks on the car's assets, and two methods, top-down and bottom-up, are used to identify and analyse the attack paths. Threat analysis consists of multiple steps including:

1. Asset identification and prioritisation;
2. Defining asset functionalities;
3. Determining information flow and connectivity through system architecture diagrams;
4. Identifying vulnerabilities to determine threats; and
5. Evaluating possible attack scenarios compromising the security-based CIA triad.

For determining the attack feasibility, the ISO/SAE 21434 standard defines three approaches: the attack potential-based approach, the Common Vulnerability Scoring System (CVSS)-based approach, and the attack vector-based approach, with usage depending on the chosen life cycle phase and information available to the assessor. The attack feasibility value can be High, Medium, Low, or Very low, which determines the probability of a threat occurring in a given scenario.

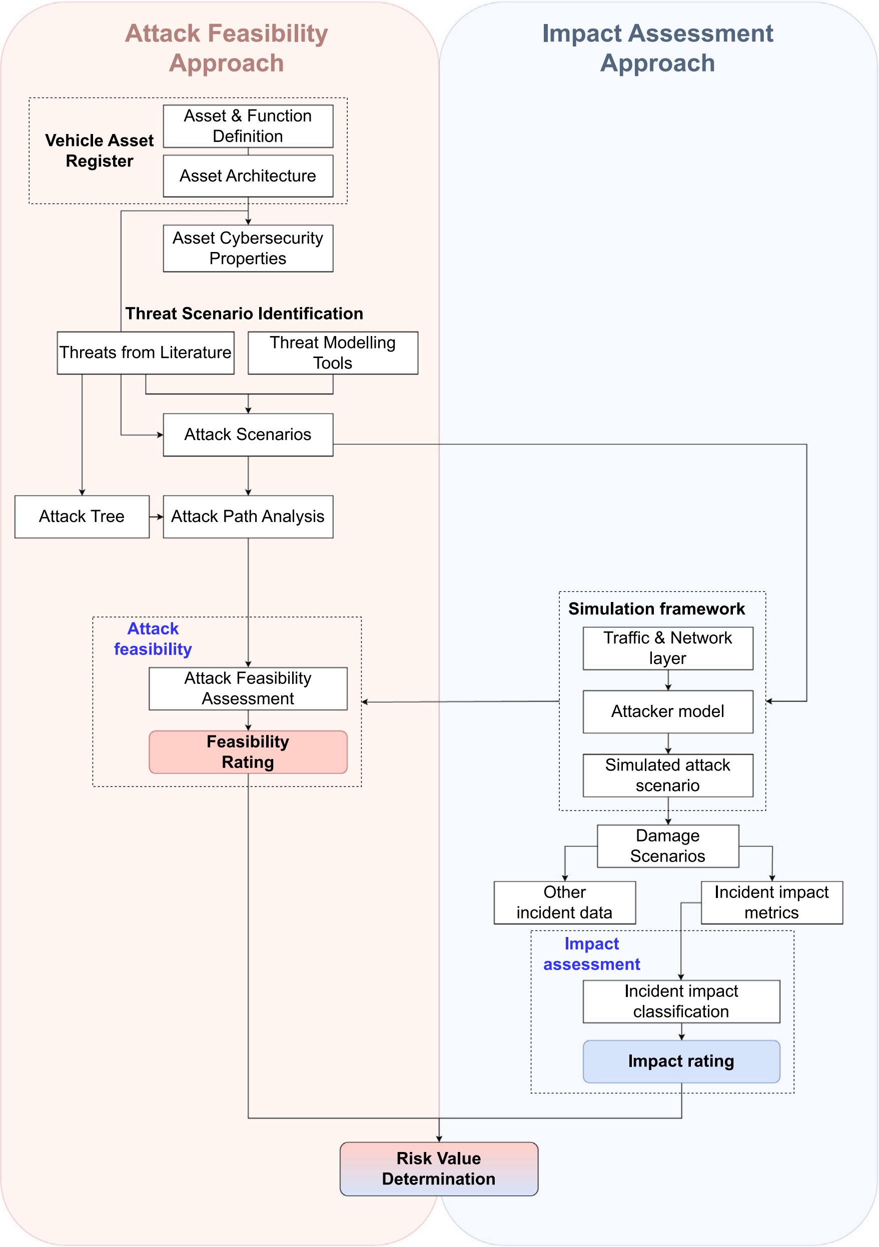

Fig. 2. Simulation-based risk assessment framework: Attack feasibility analysis approach on the left (red) and impact assessment approach on the right (blue).

3.2. Impact

The scope of analysis of the ISO/SAE 21434 standard is limited to the vehicle and the road user (passenger, pedestrian, motorist). The standard identifies four categories of impact at this level of analysis. Namely, safety, financial, operational and privacy, with an impact rating that can vary between severe, major, moderate and negligible for each category. Safety impact relates to the severity of injuries to the affected road user, financial impact relates to the financial damage to the affected road user, operational impact relates to the loss of functionality of the affected vehicle, and privacy impact relates to the severity of the sensitive information compromised due to the damage scenario. Whilst the ISO/SAE 21434 standard does not guide how the damage scenario's scalability will affect the impact rating, it points to an EVITA report that provides a more detailed classification scheme [58].

This study focuses on evaluating transport network risks, with a focus on the tangible impact categories of safety and operational. Operational impact metrics include variations in temporal and geographical link travel time, intersection delay, and congestion,

Table 3
Mean run-time per iteration for the simulated scenarios.

Input flow (veh/h/l)	Motorway scenario run-time (s)	Intersection scenario run-time (s)
500	81	148
600	91	150
700	103	151
800	117	153
900	134	154
1000	154	159

while safety impact metrics are quantified through collisions. As shown in Fig. 2, the impact assessment approach involves several steps:

1. Attack scenario identification;
2. Modelling of the incident environment on simulation platform — mobility network and infrastructure, communications network and traffic flows;
3. Modelling of attack scenario;
4. Simulation of the developed model for analysis of resultant damage scenario;
5. Extraction of operational and safety metrics from damage scenario;
6. Assessment of operational and safety impact based on performance metrics; and
7. Development of impact rating for risk value determination.

4. Case studies

This section explores the application of our simulation-based framework in assessing the impact of a cyberattack across two different traffic network configurations: a motorway and a four-way intersection, illustrating the varying impacts due to road network characteristics.

4.1. Attack scenario

The cyberattack considered in the hypothetical scenarios involves the remote exploitation of a connected vehicle's engine control. This is based on the cyberattack carried out by Miller and Valasek in 2015, where they disabled the engine of a fast-moving vehicle on a motorway by accessing the vehicle's internal CAN bus through a vulnerability in its on-board infotainment system [4]. The CVSS rating for the attack feasibility of this attack (*CVE-2015-5611*) is 8.3 (High) [59,60]. In the modelled scenarios, we assume that a single human-driven vehicle with cellular internet connectivity is attacked, disabling the engine and causing the vehicle to come to a standstill.

4.2. Simulation setup

For the case studies, we utilised the Veins 5.2 co-simulation framework, integrating SUMO 1.8.0 for road traffic and network geometry simulation and OMNeT++ 5.6.2 for communication network modelling. This allows for automated communication between the two tools. The cyberattack scenario involved disabling the target vehicle's engine, causing it to decelerate and come to a complete standstill, as emulated in the SUMO simulation. For simplicity, the traffic stream was populated only with passenger cars. The default car-following model, Krauss [61], and the lane-changing model, LC2013, were used to control vehicle longitudinal and lateral dynamics. The vehicles were modelled to have a speed distribution where approximately 95% have a maximum speed varying from 80% to 120% of the speed limit. The simulation step length was set at 0.1 s. Unless otherwise mentioned, all simulation parameters were left at their default settings in SUMO.

A Veins-based application layer was configured for each vehicle in OMNeT++. The simulation incorporates an attack mechanism designed to replicate the consequences of a cyber intrusion. This is implemented through a script within the vehicle's application layer in OMNeT++, programmed to halt the targeted vehicle. This approach simulates the remote exploitation impact by forcibly stopping the vehicle, mimicking the direct effect of the cyber threat. To evaluate the traffic demand's sensitivity to the cyberattack incident, six different vehicle input flows were investigated, with flow rates varying in increments of 100 veh/h/l, ranging from 500 to 1000 veh/h/l. Each flow scenario was simulated for 30 iterations with distinct random seeds to ensure robustness and statistical accuracy. This approach helps mitigate the effects of stochastic variability, providing a more reliable and representative analysis of the cyberattack's impact across different traffic conditions. To ensure a comprehensive analysis, both the motorway and the intersection scenarios were simulated over a period of 60 min each, allowing us to observe the long-term effects of the cyberattack and the resulting traffic behaviour post-incident.

The simulations were run on a dedicated workstation with the following hardware specifications: Intel(R) Xeon(R) W-2125 4.00 GHz CPU, 32 GB RAM, running Ubuntu 22.04. The mean simulation run-time per iteration for the scenarios under each traffic flow level is provided in Table 3.

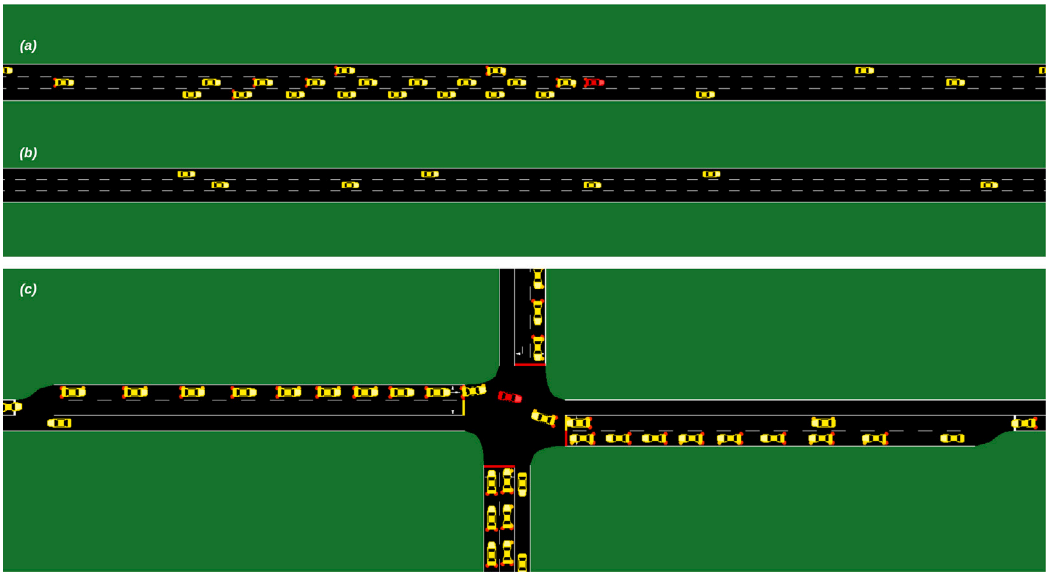

Fig. 3. (a) Attack scenario showing the attacked vehicle in red and subsequent queue build-up at t = 150 s from the time of attack in flow scenario: 1000 veh/h/l on the motorway; (b) baseline scenario with no attack under similar conditions; (c) depicts the traffic condition t = 30 s post-breakdown at the signalised intersection.

4.3. Scenario setup

The two network configurations explored in the case studies are illustrated in Fig. 3. The first scenario (Fig. 3(a), (b)), evaluates a cyberattack on a passenger car on a motorway. The simulation models a six-lane highway section, divided into three lanes for each direction of travel, with no intersections, ensuring uninterrupted flow in normal traffic conditions. A speed limit of 70 mph (113 km/h) is enforced over a 1000 m stretch, supplemented by 500 m feeder and exit sections, and the lanes are each 3.5 m wide. Fig. 3(a) and (b) contrasts the traffic stream conditions 150 s after the cyberattack with those of the baseline scenario.

In the second scenario (Fig. 3(c)), the same cyberattack is applied to a four-way signalised intersection. In this scenario, the attack is executed as the targeted vehicle traverses the intersection under all possible movements; left turn, through movement, and right turn, each with separate implications on the traffic flow. The intersection is modelled with a static 90 s signal cycle, featuring a 6 s dedicated right-turn green phase and 33 s left and through movement green phase. Right turns are permitted when the left and through movements are green on the same approach and the opposing approach if appropriate gaps in opposing traffic are detected. All four approaches to the intersection consist of two-lane, two-way roads, each supplemented by a 100 m right-turn-only bay at the intersection. Traffic flow scenarios ranging from 500 to 1000 veh/h/l are simulated, with each approach having equal flow rates and turning ratio distributions of 60:20:20 for through, left, and right movements, respectively.

Parameters for the simulation are consistent with those from the motorway scenario, suitably adapted for the intersection's control features and geometry. This approach simulates the cyberattack's disruptive effect across the intersection, revealing the intersection's vulnerability to blockages as a result of the attack. Multiple simulation iterations accommodate the inherent variability and dynamics of intersections, ensuring a comprehensive reflection of potential outcomes in the simulation outputs.

4.4. Impact quantification metrics

Distinct operational impact metrics are selected to evaluate the effects of traffic incidents across two case studies, as summarised in Table 4. These metrics highlight the unique operational challenges and responses in each setting.

For the motorway scenario, flow rate, space mean speed, spot mean speed, lane density and Level of Service (LOS) are primarily used to capture the dynamic nature of high-speed, high-volume roadways. Space mean speed and spot mean speed provide insights into the speed patterns over a distance and at specific points, respectively, helping to analyse the fluidity and sudden changes in speed post-incident. Lane density offers a measure of vehicle spacing, which is crucial for assessing congestion levels and the potential for bottleneck formation. LOS defined by the US Highway Capacity Manual (US-HCM) [62], uses a qualitative scale from 'A' (best) to 'F' (worst) to describe operational efficiency. This metric is particularly useful in the motorway context as it gives a holistic view of traffic flow quality.

Conversely, in the intersection scenario, where interactions and conflicts between different traffic flows are more pronounced, queue build-up rate and time-to-gridlock are employed as indicators. The queue build-up rate is vital for understanding the efficiency of traffic dispersal at intersections following an incident, reflecting the immediate operational impact. The time-to-gridlock metric,

Table 4
Operational impact metrics used for each case study.

Operational impact metric	Motorway scenario	Intersection scenario
Flow	Flow rate	Flow rate
Speed	Space mean speed Spot mean speed	NA
Density	Lane density	NA
Level of service	Motorway level of service	NA
Queue	Maximum queue length Mean queue length	Queue build-up rate
Time-to-gridlock	NA	Time taken for intersection gridlock since incident

Table 5
Incident impact metrics of motorway scenario.

Impact category	Performance metrics						
	Input flow	Scenario	Mean speed	Lane density	Queue build-up (m)		LOS
	(veh/h/l)		(km/h)	(veh/km/l)	mean	max	
Operational	Scenario I: 500	Baseline	112	5	0	0	A
		Attack	103	5	05	27	A
	Scenario II: 600	Baseline	111	5	0	0	A
		Attack	100	7	09	44	A
	Scenario III: 700	Baseline	111	6	0	0	A
		Attack	97	8	14	67	B
	Scenario IV: 800	Baseline	110	7	0	0	B
		Attack	93	10	24	109	B
	Scenario V: 900	Baseline	109	8	0	0	B
		Attack	89	12	38	155	C
	Scenario VI: 1000	Baseline	108	9	0	0	B
		Attack	85	14	57	274	C

indicating the duration before an intersection reaches a standstill, provides a direct measure of the resilience of an intersection under stress.

The selection of these metrics is guided by their relevance to the operational characteristics of each scenario. For instance, speed metrics are not employed in the intersection scenario due to the typically lower speeds and higher levels of interaction that make such measures less informative. Further details of each performance metric are discussed in Appendix A.

4.5. Results

This section presents the findings from the two distinct case studies.

Motorway scenario

The motorway case study employs several key metrics, such as mean speed, lane density, and LOS, to quantify the operational impact of incidents at different traffic volumes. Given that safety impact is evaluated based on collision occurrences, no safety impact was observed in any of the scenarios. As summarised in Table 5, the operational impact on motorways is assessed over a range of traffic flows from 500 to 1000 veh/h/l. At lower flows, the infrastructure demonstrates resilience, maintaining an LOS of ‘A’ even under attack conditions. However, as flow increases, the operational impact becomes more pronounced, with noticeable degradation in LOS, speed, and lane density, indicating reduced traffic efficiency and increased congestion. Figs. 4, 5, 6, and 7 provide a detailed visualisation of these trends.

The operational metrics deteriorate consistently as the input flow increases, highlighting the influence of existing traffic conditions on the severity of a cyber threat-induced incident’s impact. To illustrate these dynamics, Fig. 4 presents the mean spot-speeds across the traffic flows, recorded at 50 m intervals from the incident site. The solid blue lines represent baseline scenarios whereas the dashed orange lines represent the corresponding attack scenarios, with the shaded areas encompassing the intermediate flows. This visualisation delineates how increased flow intensifies the traffic disruption, with speeds stabilising farther upstream as flow increases, indicating a wider impact of incidents at higher densities.

As seen in Fig. 5, the interquartile range (IQR) of speeds during attack scenarios significantly widens compared to baseline conditions, reflecting increased speed variability and operational instability. This variability suggests that drivers are reacting unpredictably to the incident, potentially increasing the risk of accidents or further traffic disruptions. Fig. 6 depicts the kernel density estimate (KDE) plots showing the distributions of the individual vehicle space-mean speeds over the analysis section during baseline and attack conditions of the 500 veh/h/l and 1000 veh/h/l flow scenarios. Whilst the curves remain approximately the

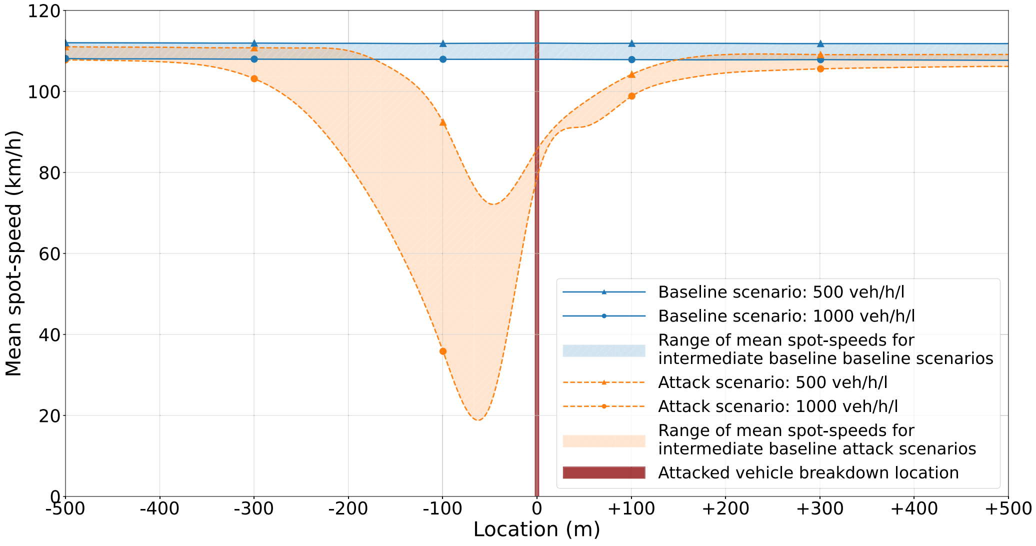

Fig. 4. Mean spot-speed versus location plots for baseline and attack scenarios with traffic flows of 500 veh/h/l and 1000 veh/h/l, including intermediate flow scenarios (600, 700, 800, and 900 veh/h/l) represented by shaded regions along a 1000 m motorway section. The location of the ego vehicle breakdown is indicated in red.

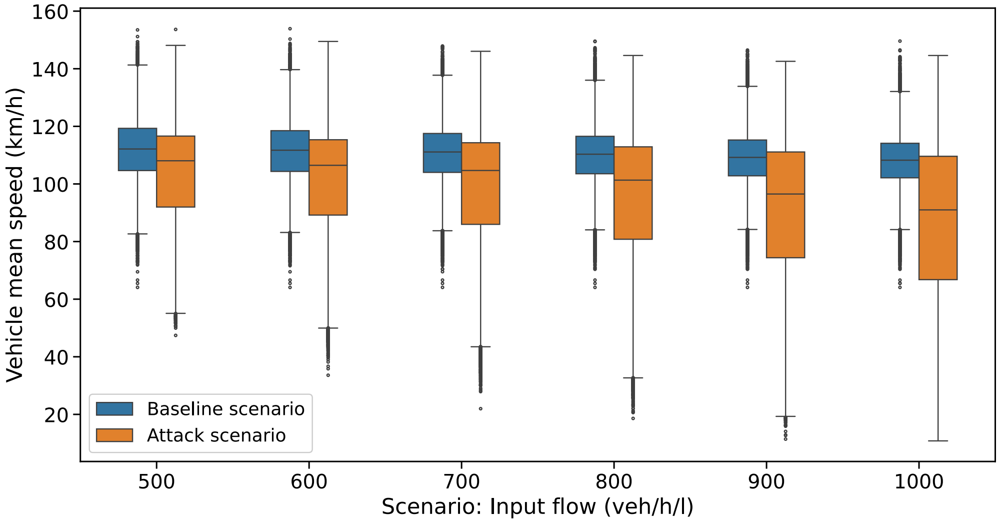

Fig. 5. Box-plots comparing the variation in vehicle mean speeds between the baseline and attack scenarios.

same for the baseline conditions through 500 veh/h/l to 1000 veh/h/l, significant depletion of space mean speeds are observed when moving from 500 veh/h/l to 1000 veh/h/l in the attack conditions.

To quantify the observed variations in vehicle speeds and substantiate the visual evidence, a Wilcoxon signed-rank test was conducted for each flow scenario. The statistical analysis confirms that the differences between baseline and attack scenarios are significant across all levels of traffic flow, with p-values less than 0.001. This strong statistical evidence, summarised in Table B.7 in the Appendix B, reinforces the conclusion that cyber threat-induced incidents consistently and significantly reduce vehicle speeds, thus influencing traffic flow dynamics.

Fig. 7 provides further insight into the compounding effects of the cyberattack on motorway operation. Fig. 7(a) illustrates the correlation between traffic flow and mean lane density for both baseline and attack scenarios, with dashed lines highlighting the trend of increasing density as flow escalates. The shifts in lane density, juxtaposed with the corresponding LOS, emphasise how traffic efficiency and quality degrade from LOS A to C under escalating flow conditions, especially when under attack. Fig. 7(b) captures the progressive queue build-up behind the attacked vehicle, a direct reflection of the operational strain imposed by increasing traffic volume.

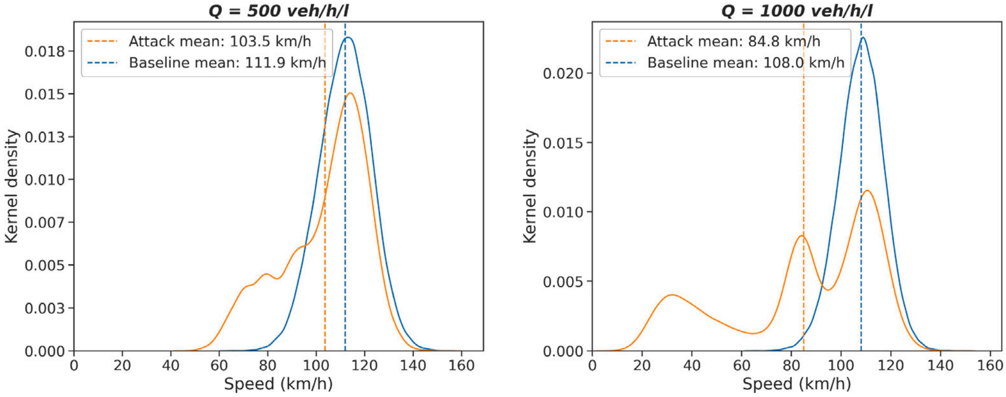

Fig. 6. Kernel density estimate plots of baseline and attack scenario vehicle mean speeds for input flows 500 veh/h/l (left) and 1000 veh/h/l (right).

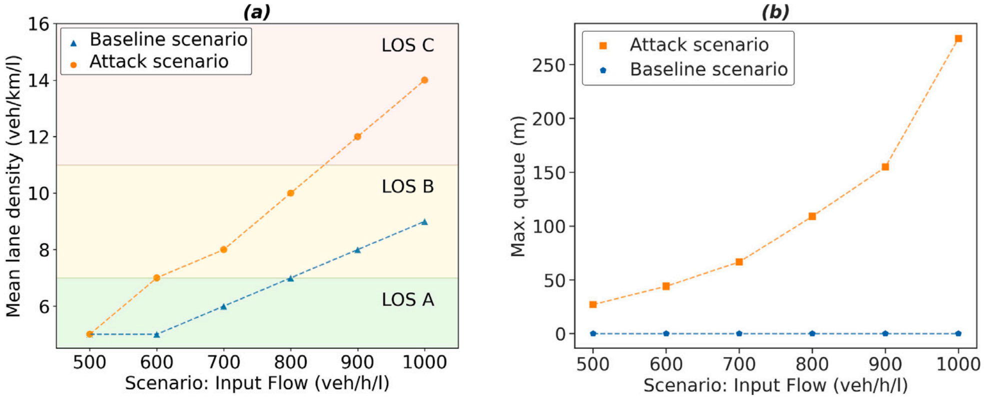

Fig. 7. Scatter-plots of (a) mean lane density and LOS variation of baseline and attack scenarios, with dashed lines connecting the scatter plot points to illustrate trends, and (b) maximum observed queue build-up of attack scenarios.

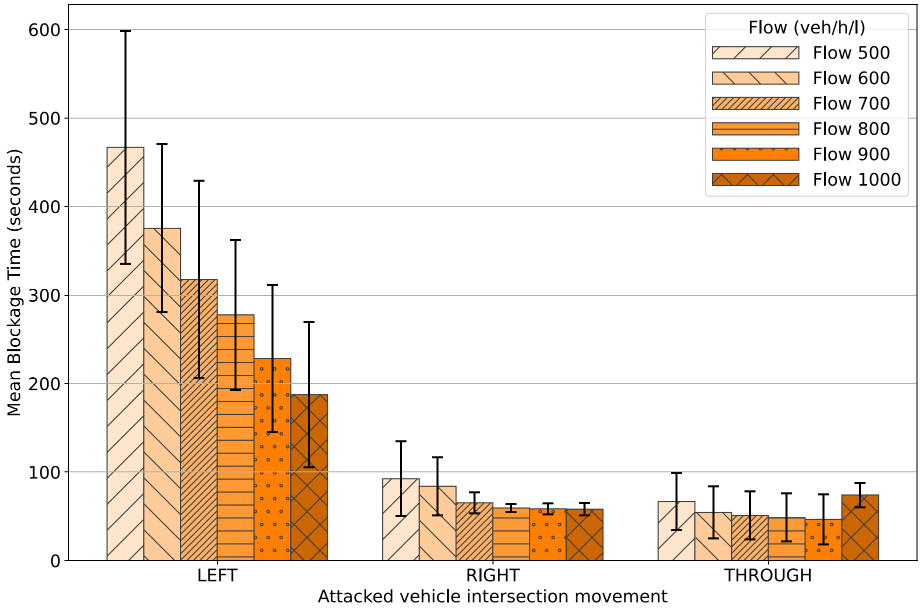

Fig. 8. Mean time to gridlock for the intersection for left, right and through movements for each flow scenario since cyberattack induced vehicular breakdown.

Table 6
Incident impact metrics of intersection scenario.

Impact category	Input flow (veh/h/l)	Mean time-to-gridlock (s)			Mean queue buildup rate
		Left	Right	Through	(m/min)
Operational	Scenario I: 500	467	92	67	70
	Scenario II: 600	375	84	54	88
	Scenario III: 700	317	65	51	104
	Scenario IV: 800	278	59	49	122
	Scenario V: 900	228	58	47	132
	Scenario VI: 1000	188	58	74	171

Intersection scenario

The analysis of intersection dynamics under cyberattack centred on two pivotal metrics: mean intersection flow breakdown times and the queue build-up rate. These metrics are particularly telling at intersections, where they capture the efficacy of traffic movement and the intersection's capacity against interruptions. Table 6 presents a detailed breakdown of the times to gridlock alongside the mean queue buildup rates, measured as the average queue length increase per minute, for each traffic flow scenario.

The mean time-to-gridlock at the intersection, differentiated by the type of vehicle movement when under attack, is illustrated in Fig. 8, with corresponding standard deviations shown. It is notable that the breakdown times for left and right turns decrease as traffic volumes increase. However, these turning movements display an inherent resilience to flow increases due to their path of travel. In the case of the left turn, when the attacked vehicle initiates the manoeuvre, it obstructs fewer conflicting flows, allowing other movements such as through and right turns to proceed with minimal initial interference. Similarly, the existence of a dedicated right turn lane allows a degree of flow continuity for left and through movements, even when the attack occurs during this turning phase. Contrastingly, the through movement demonstrates a different pattern. When the attacked vehicle is moving straight through the intersection, the blockage created impacts a larger array of conflicting movements. Hence, despite the direct nature of the through movement, it exhibits a smaller change in breakdown times across varying flows. This suggests that the through movement's capacity to induce gridlock is less about the volume of traffic and more about the strategic impact it has when obstructed.

4.6. *Comparative analysis of case studies*

The examination of operational impact across motorway and intersection scenarios reveals distinct responses to cyberattack-induced incidents. While both environments are subject to increased strain as traffic volume rises, the nature and immediacy of their operational impacts diverge.

In the motorway scenario, the increase in traffic flow from 500 to 1000 veh/h/l corresponds with a gradual degradation of operational metrics. Space mean speed, spot mean speed, and lane density all deteriorate, contributing to a steady decline in the LOS from 'A' to 'C'. This degradation, illustrated in Figs. 4 and 7, showcases the motorway's initially robust infrastructure which gradually succumbs to congestion as vehicle volume increases.

Conversely, the intersection scenario, outlined in Table 6 and depicted in Fig. 8, presents a different picture. Here, the queue build-up rates and the mean time-to-gridlock significantly vary across the turning movements. While left and right turns benefit from separate lanes and less cross-traffic interference, the through movement, obstructed during an attack, swiftly impacts other movements, highlighting a vulnerability unique to the intersection's design. This pattern demonstrates that intersections may face sudden operational collapse with little warning, as opposed to the motorway's more gradual approach to capacity limits.

Fig. 9 demonstrates the divergent behaviours of traffic queues in motorway and intersection scenarios, revealing the intrinsic capacity of each network element to handle incidents. The motorway demonstrates an inherent ability to absorb disruptions, indicated by the erratic but ultimately manageable patterns of queue lengths. Despite fluctuations, the motorway's queues do not consistently reach a state of gridlock within the observed intervals, suggesting a certain resilience and adaptability in the face of incidents. The broad expanse of the motorway, coupled with multiple lanes and the opportunity for vehicles to change lanes, disperses the impact, preventing immediate systemic failure.

On the other hand, intersections operate as critical nodes in the traffic network where multiple flows converge, making them natural bottlenecks. The intersection queues, as seen in Fig. 9, escalate in a more uniform and rapid manner once the traffic flow is obstructed. This reflects the limited capacity of intersections to accommodate disruptions. Once an intersection reaches gridlock, the impact is not just localised but propagates swiftly upstream, leading to significant queue lengths in a short period. This domino effect can instigate cascading failures, as the blocked intersection halts the traffic flow across all directions, causing widespread congestion that can cripple the network.

5. Conclusions and future work

As the landscape of vehicular transportation continues to evolve, integrating robust cybersecurity measures within connected vehicle systems has become paramount. Our literature review has highlighted a significant gap: a lack of robust methodologies for assessing systemic risks associated with cyber threats in connected networks. In response, we have developed a novel simulation-based framework designed to evaluate both the feasibility of cyberattacks and their potential impacts on transport systems. The key outputs of our study include,

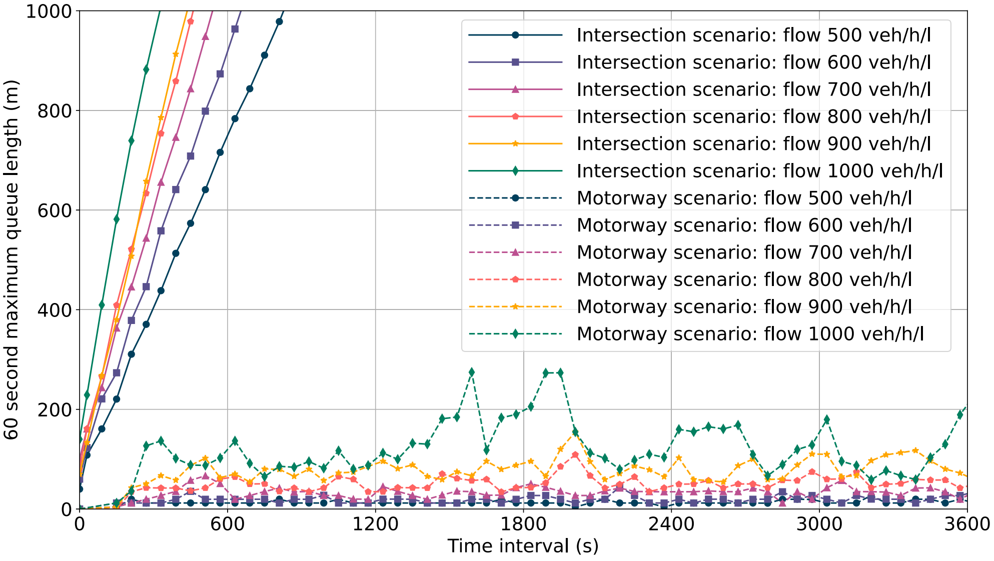

Fig. 9. Comparison of 1-min interval max queues with time between the motorway and intersection case studies.

1. Novel framework: We introduced a simulation-based approach for systemic risk assessment for connected vehicles. This framework enhances the ISO/SAE 21434 TARA process, infusing traditional risk assessment methods with robust, quantitative data.
2. Case studies: We presented two case studies based on the real-world event of the 2015 Miller-Valasek Jeep hack. These studies modelled remote cyberattacks on a connected vehicle infotainment system and evaluated their operational impact using the proposed simulation-based approach.
3. Operational impact metrics: We identified a variety of operational metrics based on scenario-specific requirements to quantify the damage scenarios for each case study.

The case studies illustrated that traffic demand and network configuration are two primary factors contributing to increased systemic risks associated with cyberattacks in connected vehicles. This highlights the critical need to identify and address cyber vulnerabilities of connected vehicles, especially in areas with dense traffic and intricate network layouts. The simulation methodology used in our framework can model cyberattacks that manipulate vehicular communications and impact the drivetrain of individual vehicles at a microscopic level. This ensures that a wide range of cyberattacks such as false data injection, message replay attacks, and denial of service attacks can be evaluated for risk assessment.

Moving forward, this research will be expanded to encompass a broader array of cyber–physical threats affecting connected vehicles and their infrastructure. We plan to conduct simulations of cyberattacks across various network types, incorporating heterogeneous traffic flows and diverse rates of connected vehicle penetration to assess risk factors and potential cascading failures. Further, we will enhance our impact assessments by integrating financial and safety metrics alongside the current operational impact metrics. Attack potential-based metrics will also be developed and included for the evaluation of attack feasibility. These metrics will lead to the provision of a risk value for a given cyberattack.

The complexity of road transport systems and the unpredictable nature of traffic flows present significant challenges for conducting empirical studies on the impacts of cyber threats on connected infrastructure. Simulation offers a controlled environment that enables the modelling of various scenarios and the assessment of their potential impacts effectively. As connected vehicles become increasingly integrated into our transportation infrastructure, the need for sophisticated cybersecurity measures becomes more critical. Our work represents a significant advancement in understanding and mitigating the risks associated with cyber threats, providing valuable insights that benefit both researchers and practitioners in the field of automotive cybersecurity.

CRediT authorship contribution statement

Don Nalin Dharshana Jayaratne: Conceptualization, Methodology, Software, Formal analysis, Investigation, Writing – original draft, Visualisation. **Suraj Harsha Kamtam:** Conceptualization, Methodology, Investigation, Writing – original draft, Visualisation. **Siraj Ahmed Shaikh:** Conceptualization, Methodology, Writing – review & editing, Supervision, Project administration. **Muhamad Azfar Ramli:** Conceptualization, Formal analysis, Writing – review & editing, Supervision. **Qian Lu:** Methodology, Writing – review & editing, Supervision, Project administration. **Rakhi Manohar Mepparambath:** Conceptualization, Formal analysis, Writing – review & editing, Supervision. **Hoang Nga Nguyen:** Conceptualization, Methodology, Supervision. **Abdur Rakib:** Methodology, Writing – review & editing, Supervision.

Data availability

No data was used for the research described in the article.

Acknowledgements

This work was supported by Coventry University and the A*STAR Research Attachment Programme (ARAP).

Appendix A. Operational impact metrics

A.1. Space-mean speed

The space-mean speed of a traffic stream v_{mean} during a given analysis period is calculated as shown in Eq. (A.1)

$$v_{mean} = \frac{\sum_{i=1}^{N} \left(\frac{\sum_{i=1}^{r} d_i}{rS} \right)}{N} \tag{A.1}$$

where N is the total number of vehicles, d_i is the distance travelled by vehicle i during the simulation step of length S, and r is the total number of simulation steps.

A.2. Lane density

The lane density ρ_l is the mean number of vehicles on a lane during a given analysis period as shown in Eq. (A.2)

$$\rho_l = \frac{\sum_{i=1}^{r} n_i}{r \times KD} \tag{A.2}$$

where n_i is the number of vehicles on the analysis section D during simulation time-step i, K is the number of lanes, and r is the total number of simulation steps.

A.3. Queue length

The queue length L_q is the length of vehicles with speed below the threshold value of $0.1\,\mathrm{ms}^{-1}$ as shown by Eq. (A.3)

$$L_q = \sum_{i=1}^{n} \left(l_i + g_i \right) \tag{A.3}$$

where l_i is the length of the ith vehicle in the queue and g_i is the distance between the ith vehicle and $(i-1)\mathrm{th}$ vehicle in the queue.

A.4. Queue build-up rate

Queue build-up rate (L_{q-rate}) calculates the rate at which the length of the queue increases per unit time, as shown in Eq. (A.4)

$$L_{q-rate} = \frac{\Delta L_q}{\Delta t} \tag{A.4}$$

where ΔL_q is the change in queue length over the time interval and Δt is the time interval during which the queue length change is observed after the attack

A.5. Flow rate

The flow rate of vehicles Q, is the number of vehicles passing a given point of analysis per unit time and per lane, as given in Eq. (A.5)

$$Q = \frac{3600 \times n_t}{tK} \tag{A.5}$$

where n_t is the number of vehicles passing a given point during time t measured in seconds.

A.6. Time to gridlock

Time to gridlock ($T_{gridlock}$) metric measures the duration from the start of the cyberattack to the point when no vehicles can pass resulting in gridlock, as given in Eq. (A.6)

$$T_{gridlock} = t_{gridlock} - t_{attack} \tag{A.6}$$

where $t_{gridlock}$ is the time at which the traffic flow ceases completely, leading to gridlock and t_{attack} is the time at which the cyberattack was initiated.

Table B.7
Wilcoxon's signed-rank test for mean speeds — Motorway scenario.

Flow (veh/h/l)	Test statistic	P-value	Significance
500	300 773	<0.001	Yes
600	425 331	<0.001	Yes
700	501 040	<0.001	Yes
800	567 178	<0.001	Yes
900	605 215	<0.001	Yes
1000	657 284	<0.001	Yes

A.7. Level of service

The LOS of motorway facilities is categorised based on the lane density as follows: LOS is A if lane density less than or equal to 7 pc/km/l, B if lane density is between 7–11 pc/km/l, C if lane density is between 11–16 pc/km/l, D if lane density is between 16–22 pc/km/l, E if lane density is between 22–28 pc/km/l and F when flow exceeds the lane capacity or lane density is greater than 28 pc/km/l, where pc denotes passenger car unit.

Appendix B. Wilcoxon's signed-rank test

See Table B.7.

References

[1] J. Deichmann, B. Klein, G. Scherf, R. Stuetzle, The race for cybersecurity: Protecting the connected car in the era of new regulation, 2019, URL https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/the-race-for-cybersecurity-protecting-the-connected-car-in-the-era-of-new-regulation.

[2] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaâniche, Y. Laarouchi, Survey on security threats and protection mechanisms in embedded automotive networks, in: 2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop, DSN-W, IEEE, 2013, pp. 1–12, http://dx.doi.org/10.1109/DSNW.2013.6615528.

[3] Cybersecurity challenges in the uptake of artificial intelligence in autonomous driving, 2021, URL https://www.enisa.europa.eu/news/enisa-news/cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving.

[4] C. Miller, C. Valasek, Remote exploitation of an unaltered passenger vehicle, Black Hat USA 2015 (S 91) (2015).

[5] ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering, 2021, URL https://www.iso.org/standard/70918.html.

[6] B. Sheehan, F. Murphy, M. Mullins, C. Ryan, Connected and autonomous vehicles: A cyber-risk classification framework, Transp. Res. A: Policy Pract. 124 (2019) 523–536, http://dx.doi.org/10.1016/j.tra.2018.06.033.

[7] C. Maple, M. Bradbury, A.T. Le, K. Ghirardello, A connected and autonomous vehicle reference architecture for attack surface analysis, Appl. Sci. 9 (23) (2019) 5101, http://dx.doi.org/10.3390/app9235101.

[8] M. Pham, K. Xiong, A survey on security attacks and defense techniques for connected and autonomous vehicles, Comput. Secur. 109 (2021) 102269, http://dx.doi.org/10.1016/j.cose.2021.102269.

[9] X. Sun, F.R. Yu, P. Zhang, A survey on cyber-security of connected and autonomous vehicles (CAVs), IEEE Trans. Intell. Transp. Syst. (2021) http://dx.doi.org/10.1109/TITS.2021.3085297.

[10] Z. El-Rewini, K. Sadatsharan, D.F. Selvaraj, S.J. Plathottam, P. Ranganathan, Cybersecurity challenges in vehicular communications, Veh. Commun. 23 (2020) 100214, http://dx.doi.org/10.1016/j.vehcom.2019.100214.

[11] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, R. Das, Attacks on self-driving cars and their countermeasures: A survey, IEEE Access 8 (2020) 207308–207342, http://dx.doi.org/10.1109/ACCESS.2020.3037705.

[12] S. Parkinson, P. Ward, K. Wilson, J. Miller, Cyber threats facing autonomous and connected vehicles: Future challenges, IEEE Trans. Intell. Transp. Syst. 18 (11) (2017) 2898–2915, http://dx.doi.org/10.1109/TITS.2017.2665968.

[13] S.K. Khan, N. Shiwakoti, P. Stasinopoulos, Y. Chen, Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions, Accid. Anal. Prev. 148 (2020) 105837, http://dx.doi.org/10.1016/j.aap.2020.105837.

[14] P. Kevin, Hacker disables more than 100 cars remotely, 2010, https://www.wired.com/2010/03/hacker-bricks-cars/, [(Accessed 13 October 2023)].

[15] A. Himanshu, Chinese security firm hacks tesla model s to gain control of door locks, wipers, sunroof, and more, 2014, https://www.techspot.com/news/57455-chinese-security-firm-hacks-tesla-model-s-to-gain-control-of-door-locks-wipers-sunroof-and-more.html, [(Accessed 13 October 2023)].

[16] G. Andy, Hackers cut a corvette's brakes via a common car gadget, 2015, https://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/, [(Accessed 13 October 2023)].

[17] M.G. Jonathan, Hackers break the connected mitsubishi outlander hybrid wide open, 2016, https://arstechnica.com/cars/2016/06/mitsubishi-outlander-hybrid-is-the-latest-connected-car-to-prove-vulnerable-to-hacking/, [(Accessed 13 October 2023)].

[18] S. Malik, W. Sun, Analysis and simulation of cyber attacks against connected and autonomous vehicles, in: 2020 International Conference on Connected and Autonomous Driving, MetroCAD, 2020, pp. 62–70, http://dx.doi.org/10.1109/MetroCAD48866.2020.00018.

[19] M. Sandler, UN regulation no 155 & how to comply? What you need to know, 2022, https://www.cyres-consulting.com/un-regulation-no-155-requirements-what-you-need-to-know/, (Accessed 02 February 2023).

[20] C. Schmittner, G. Macher, Automotive cybersecurity standards-relation and overview, in: International Conference on Computer Safety, Reliability, and Security, Springer, 2019, pp. 153–165, http://dx.doi.org/10.1007/978-3-030-26250-1_12.

[21] F. Di Maio, R. Mascherona, E. Zio, Risk analysis of cyber-physical systems by GTST-MLD, IEEE Syst. J. 14 (1) (2019) 1333–1340.

[22] S. Kriaa, M. Bouissou, Y. Laarouchi, SCADA safety and security joint modeling (S-cube): case study of a dam, in: Proceedings of the 22th Computer & Electronics Security Applications Rendez-vous, C&ESAR'2015, 2015, pp. 55–69.

[23] L. Piètre-Cambacédès, M. Bouissou, Beyond attack trees: dynamic security modeling with boolean logic driven Markov processes, in: 2010 European Dependable Computing Conference, BDMP, IEEE, 2010, pp. 199–208.

[24] C. Schmittner, Z. Ma, E. Schoitsch, T. Gruber, A case study of fmvea and chassis as safety and security co-analysis method for automotive cyber-physical systems, in: Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, 2015, pp. 69–80.

[25] R.G. Little, Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures, J. Urban Technol. 9 (1) (2002) 109–123, http://dx.doi.org/10.1080/106307302317379855.

[26] Citi GPS Cambridge Centre for Risk Studies, Systemic risk: systemic solutions for an increasingly interconnected world, 2021, URL https://www.jbs.cam.ac.uk/wp-content/uploads/2021/04/crs-citigps-systemic-risks-report.pdf.

[27] Systemic cyber risk - European systemic risk board, 2020, URL https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

[28] L. Daqing, J. Yinan, K. Rui, S. Havlin, Spatial correlation analysis of cascading failures: Congestions and blackouts, Sci. Rep. 4 (2014) 1–6, http://dx.doi.org/10.1038/srep05381.

[29] S. Vivek, H. Conner, Urban road network vulnerability and resilience to large-scale attacks, Saf. Sci. 147 (November 2021) (2022) 105575, http://dx.doi.org/10.1016/j.ssci.2021.105575.

[30] J. Xu, H. Huang, Y. Cheng, K. Chen, Vulnerability assessment of freeway network considering the probabilities and consequences from a perspective based on network cascade failure, PLoS One 17 (3) (2022) 1–28, http://dx.doi.org/10.1371/journal.pone.0265260.

[31] P.A. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner, E. Wießner, Microscopic traffic simulation using SUMO, in: The 21st IEEE International Conference on Intelligent Transportation Systems, IEEE, 2018, pp. 2575–2582, http://dx.doi.org/10.1109/ITSC.2018.8569938.

[32] M. Fellendorf, P. Vortisch, Microscopic traffic flow simulator VISSIM, in: J. Barceló (Ed.), Fundamentals of Traffic Simulation, Springer New York, New York, NY, 2010, pp. 63–93, http://dx.doi.org/10.1007/978-1-4419-6142-6_2.

[33] J. Barceló, J. Casas, Dynamic network simulation with AIMSUN, in: R. Kitamura, M. Kuwahara (Eds.), Simulation Approaches in Transportation Analysis: Recent Advances and Challenges, Springer US, Boston, MA, 2005, pp. 57–98, http://dx.doi.org/10.1007/0-387-24109-4_3.

[34] OMNeT++ Discrete Event Simulator. URL https://omnetpp.org/.

[35] ns-3 | a discrete-event network simulator for internet systems. URL https://www.nsnam.org/.

[36] S. Manzoor, Y. Yin, Y. Gao, X. Hei, W. Cheng, A systematic study of IEEE 802.11 DCF network optimization from theory to testbed, IEEE Access 8 (2020) 154114–154132, http://dx.doi.org/10.1109/ACCESS.2020.3018088.

[37] N. Kuse, B. Jaeger, Network simulation with ns-3, in: Network Architectures and Services, 2020, pp. 67–71, http://dx.doi.org/10.2313/NET-2020-11-1, no. November.

[38] A.R. Khan, S.M. Bilal, M. Othman, A performance comparison of open source network simulators for wireless networks, in: 2012 IEEE International Conference on Control System, Computing and Engineering, 2012, pp. 34–38, http://dx.doi.org/10.1109/ICCSCE.2012.6487111.

[39] R. Fernandes, M. Ferreira, Scalable VANET simulations with NS-3, in: IEEE Vehicular Technology Conference, 2012, http://dx.doi.org/10.1109/VETECS.2012.6240251.

[40] C. Sommer, R. German, F. Dressler, Bidirectionally coupled network and road simulation for improved IVC analysis, IEEE Trans. Mob. Comput. 10 (1) (2011) 3–15, http://dx.doi.org/10.1109/TMC.2010.133.

[41] M. Segata, S. Joerer, B. Bloessl, C. Sommer, F. Dressler, R.L. Cigno, Plexe: A platooning extension for Veins, in: IEEE Vehicular Networking Conference, VNC, 2014, pp. 53–60, http://dx.doi.org/10.1109/VNC.2014.7013309, (January).

[42] R. Riebl, C. Obermaier, H.-J. Gunther, Artery: Large scale simulation environment for ITS applications, in: A. Virdis, M. Kirsche (Eds.), Recent Advances in Network Simulation: The OMNeT++ Environment and Its Ecosystem, Springer International Publishing, Cham, 2019, pp. 365–406, http://dx.doi.org/10.1007/978-3-030-12842-5_12.

[43] B. McCarthy, A. Burbano-Abril, V.R. Licea, A. O'Driscoll, OpenCV2X: Modelling of the V2X cellular sidelink and performance evaluation for aperiodic traffic, 2021, http://dx.doi.org/10.48550/arXiv.2103.13212.

[44] M. Amoozadeh, A. Raghuramu, C.N. Chuah, D. Ghosal, H. Michael Zhang, J. Rowe, K. Levitt, Security vulnerabilities of connected vehicle streams and their impact on cooperative driving, IEEE Commun. Mag. 53 (6) (2015) 126–132, http://dx.doi.org/10.1109/MCOM.2015.7120028.

[45] D. Krajzewicz, L. Bieker, J. Härri, R. Blokpoel, Simulation of V2X applications with the iTETRIS system, Procedia - Soc. Behav. Sci. 48 (2012) 1482–1492, http://dx.doi.org/10.1016/j.sbspro.2012.06.1124.

[46] K. Massow, F.M. Thiele, K. Schrab, B.S. Bunk, I. Tschinibaew, I. Radusch, Scenario definition for prototyping cooperative advanced driver assistance systems, in: 2020 IEEE 23rd International Conference on Intelligent Transportation Systems, ITSC 2020, 2020, http://dx.doi.org/10.1109/ITSC45102.2020.9294238.

[47] F. Vrbanić, D. Čakija, K. Kušić, E. Ivanjko, Traffic Flow Simulators with Connected and Autonomous Vehicles: A Short Review, in: M. Petrović, L. Novačko (Eds.), Transformation of Transportation, Springer International Publishing, Cham, 2021, pp. 15–30, http://dx.doi.org/10.1007/978-3-030-66464-0_2.

[48] X. Koutsoukos, G. Karsai, A. Laszka, H. Neema, B. Potteiger, P. Volgyesi, Y. Vorobeychik, J. Sztipanovits, SURE: A modeling and simulation integration platform for evaluation of secure and resilient cyber–physical systems, Proc. IEEE 106 (1) (2018) 93–112, http://dx.doi.org/10.1109/JPROC.2017.2731741.

[49] D. Jia, J. Sun, A. Sharma, Z. Zheng, B. Liu, Integrated simulation platform for conventional, connected and automated driving: A design from cyber–physical systems perspective, Transp. Res. C 124 (2021) 102984, http://dx.doi.org/10.1016/j.trc.2021.102984.

[50] W. Xiong, F. Krantz, R. Lagerström, Threat modeling and attack simulations of connected vehicles: A research outlook, in: ICISSP, 2019, pp. 479–486.

[51] D.-H. Lee, C.-M. Kim, H.-S. Song, Y.-H. Lee, W.-S. Chung, Simulation-based cybersecurity testing and evaluation method for connected car V2X application using virtual machine, Sensors 23 (3) (2023) 1421.

[52] M. Zhou, S.-D. Lang, A frequency-based approach to intrusion detection, in: Proc. of the Workshop on Network Security Threats and Countermeasures, 2003.

[53] D.L. Hancock, G.B. Lamont, Multi agent system for network attack classification using flow-based intrusion detection, in: 2011 IEEE Congress of Evolutionary Computation, CEC, IEEE, 2011, pp. 1535–1542.

[54] R. Puzis, M. Tubi, Y. Elovici, C. Glezer, S. Dolev, A decision support system for placement of intrusion detection and prevention devices in large-scale networks, ACM Trans. Model. Comput. Simul. (TOMACS) 22 (1) (2011) 1–26.

[55] K. Berdica, An introduction to road vulnerability: what has been done, is done and should be done, Transp. Policy 9 (2) (2002) 117–127, http://dx.doi.org/10.1016/S0967-070X(02)00011-2.

[56] Risk definition meaning. URL https://www.merriam-webster.com/dictionary/risk.

[57] BSI Standards Publication, BSI ISO/SAE 21434:2021 Road vehicles - Cybersecurity engineering, 2021.

[58] A. Ruddle, B. Weyl, S. Idrees, Y. Roudier, M. Friedewald, T. Leimbach, A. Fuchs, S. Gürgens, O. Henninger, R. Rieke, et al., Security Requirements for Automotive On-Board Networks Based on Dark-Side Scenarios, European Commission, 2009, URL https://publica.fraunhofer.de/handle/publica/294396.

[59] M. NIST, NVD - CVE-2015-5611 — nvd.nist.gov, 2015, https://nvd.nist.gov/vuln/detail/CVE-2015-5611#vulnCurrentDescriptionTitle, [(Accessed 31 January 2023)].

[60] NIST, NVD - CVSS v2 calculator — nvd.nist.gov, 2015, https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?name=CVE-2015-5611&vector=(AV:A/AC:L/Au:N/C:C/I:C/A:C)&version=2.0&source=NIST, [(Accessed 31 January 2023)].

[61] S. Krauß, Microscopic Modeling of Traffic Flow: Investigation of Collision Free Vehicle Dynamics (Ph.D. thesis), Universität zu Köln, 1998, p. 116.

[62] Highway Capacity Manual: A Guide for Multimodal Mobility Analysis, 2016, Transportation Research Board.