Considering PKI safety impact on network performance during V2X-based AD/ADAS function development processes

Zsombor Pethő
Dept. of Automotive Technologies
Budapest University of
Technology and Economics
Budapest, Hungary
Email: zsombor.petho@edu.bme.hu

Tamás Márton Kazár
Dept. of Automotive Technologies
Budapest University of
Technology and Economics
Budapest, Hungary
Email: kazar.tamas@kjk.bme.hu

Roland Kraudy
Microsec Software Management
and Consulting ltd.
Budapest, Hungary
Email: roland.kraudy@microsec.com

Zsolt Szalay
Dept. of Automotive Technologies
Budapest University of
Technology and Economics
Budapest, Hungary
Email: szalay.zsolt@kjk.bme.hu

Árpád Török
Dept. of Automotive Technologies
Budapest University of
Technology and Economics
Budapest, Hungary
Email: torok.arpad@kjk.bme.hu

***Abstract*—In this research, we examine the impact of PKI on vehicle safety and thus make suggestions for further improvements to V2X-based safety application design processes. In the first step, we introduce the novel methodological background of characterizing the safety impact of the network performance metrics on the V2X-based automotive applications. Following this, we investigated two cases: with and without Public Key Infrastructure (PKI) authorization, to identify the potential safety effect if the V2X device is unprepared for the additional computational overhead caused by the authentication framework-related processes. Based on our results, we can identify the operational domain of a specific V2X-based application that can be used safely.**

Keywords*—automotive safety, public key infrastructure, safety risk, network performance, V2X

I. Introduction

This conference article is based on the results of a joint research between Microsec and BME. The aim of present research is to investigate the safety impact of PKI authentication process on network performance to improve the efficiency and safety of V2X-based (Vehicle-to-everything) AD (Automated Driving) / ADAS (Advanced Driver Assistance System) function's development processes [1] [2]. The future transportation systems will be much safer due to V2X communication technology [3] [4], because Intelligent Transportation System (ITS) users will be able to receive awareness messages, reasonably earlier than in the case of a classical perception processes (human perception).

Among others, CAMs (Cooperative Awareness Message) in ITS carry safety-related information [5]. In order to prevent compromised messages from being transmitted during V2X communication, we must ensure that only parties with a valid digital certificate can join the communication. However, this communication process, secured by the PKI security framework, requires additional computation (time or resource), which we need to consider when developing the ADAS function [6] [7], especially for safety-critical applications that require real-time intervention (such as Autonomous Emergency Braking System - AEBS). Suppose we do not allocate additional computational resources. In that case, the authorization process may affect the end-to-end latency (E2E) and the available time frame to react to the traffic situation. In normal traffic situations, the small amount of overhead added by the authentication process should not be a problem, as up-to-date, sophisticated, and fast algorithms (e.g., Elliptic Curve Cryptography - ECC) are available. However, we must mention that either an intentional intervention [8] or random failure can reduce the network performance significantly. The Hardware Security Module (HSM) that performs the cryptographic operations and stores the cryptographic keys also uses dedicated, high-performance cryptographic accelerators, which are way faster than general-purpose processors.

A regular X.509 Public Key Infrastructure (PKI) system uses digital signatures, hash functions, and timestamps, thereby providing authentication, non-repudiation, reliability, message freshness, and integrity. To ensure the data privacy of the users and the authenticity of exchanged cooperative messages, connected and highly automated transport systems use pseudonym identities (or certificates) provided by a specific PKI. This PKI uses a more compact format to reduce security overhead, not using any identifier at the end user certificates to maintain the anonymity of the driver, and the most important aspect of it is that it manages the rights and permission of the ITS participants (e.g., a police car should have different permissions than a regular vehicle). This is a mandatory part of the system, but the quality of communication can deteriorate

due to a number of factors, this should be considered when designing V2X-based safety applications, including the extra security overhead added by the PKI-based permission and access management, even with this tailormade solution.

It should be mentioned that the PKI system is not only used to authenticate the processes of intelligent transport systems, but also in many other areas, such as e.g. the energy sector [9], which is also considered a critical infrastructure from the point of view of cyber security [10].

Several previous studies have addressed the time required for the authentication process [11], the efficiency of the C-ITS Credential Management System (CCMS) architecture [12] [13] [14] [15], and the computational needs of related encryption algorithms [16]. Based on the performed literature review, we can conclude that the safety impact of PKI authentication processes on network performance is a quite under-researched area.

In order to determine the operational design domain during development, within the intervals of which highly automated vehicle functions can be operated safely, it is necessary to know the level of risk. Thereby we can operate the system below the acceptable risk level. In the case of a network performance drop (e.g., due to adversarial intervention or communication failure), the system can be controlled to a safe state [17] [18].

II. Methodology

Our study evaluates the risk of specific incidents and the probability of a possible communication failure potentially resulting in an accident related to V2X-based systems. Accordingly, we first present the methodology used in the risk assessment and then the methodology used to estimate the probability of occurrence [19].

A. Test method

We generated six scenarios (S1-S6) during our analysis to evaluate the Intersection Collision Risk Warning (ICRW) application [20]. Each scenario contains two vehicles with perpendicular intersecting trajectories. The velocities of vehicles are presented in the following table.

TABLE I: Test scenarios with the defined speed levels

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

The test scenarios were built up using Cohda vsim simulation framework with the following architecture (Fig 1).
The scenarios were performed in the ZalaZONE automotive proving ground digital environment in order to carry out

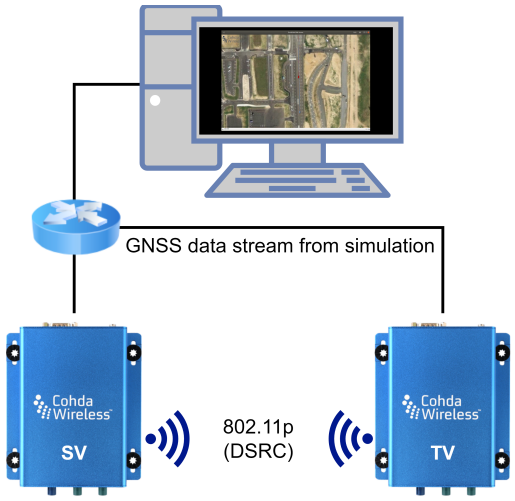

Fig. 1: VSIM simulation environment

similar real-word test to later validate the results [21]. The following figure (Fig 2) shows the implemented setup.

Fig. 2: Experimental setup

B. Safety Risk Index

The following subsection introduces the Safety Risk Index (SRI) identification method. Besides physical factors, the SRI takes into account on packet delivery ratio (PDR) and end-to-end latency of the wireless communication process. We investigated the stopping distance (indicated as d_{crit}) as a derived vehicle dynamics parameter for the Intersection Collision Risk Warning test case.
If CAMs are received within the stopping time interval (t_{crit}), the vehicle system will probably run out of time and cannot stop before the predicted collision point. Accordingly, we can define a warning time interval (t_{warn}) in which the vehicle should successfully receive the awareness message to avoid the accident. If the intersecting vehicle has a higher velocity, then the t_{warn} interval should be longer. During the design process of ADAS functions, we need to pay special attention to the ratio of t_{warn} and t_{crit}, since if this ratio is higher, the system will be safer but less efficient.
To calculate SRI, we use parameter values that can describe the probability and severity of an accident due to lately received CAMs.
The likelihood of the lately received CAMs are estimated by the time distance between CAMs (t_{TS_CAM}) and the middle of the warning interval (t_{TS_MID}).
We assume that, the severity can be represented by the energy of the potential collision. Accordingly the severity is estimated

by the square of the speed. Based on the previous considerations, SRI is described by Eq. 1.

$$SRI = (t_{TS\_CAM} - t_{TS\_MID}) \cdot d_{crit} \quad (1)$$

SRI is predicted with polynomial regression based on the Response Surface Methodology (RSM). The general form of the response surface function for two-level factors is expressed by the following equation:

$$\hat{y} = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_{12} x_1 x_2 + \beta_{13} x_1 x_3 + \cdots \quad (2)$$

C. Message Reception Probability

If an experiment can have two types of outcomes, then we should use a binomial model to describe its probability distribution.

The likelihood (P) that the variable of successful outcomes s_i, is equal to k_i is defined with the regression functions independent variables (X). In light of this, we are able to define s_i depending on our experimental factors [22].

$$MRP = P(s_i = k_i | X = x_{i,1}, \ldots x_{i,j}, \ldots x_{i,m}) = \binom{n_i}{k_i} p_i^{k_i} \cdot (1 - p_i)^{n_i - k_i}, \forall j = 1..m \quad (3)$$

III. Results and Discussion

In this chapter, we would like to present and discuss the experimental evaluations of the performed simulation tests for all investigated scenarios. Accordingly we evaluate the safety risk of the V2V scenarios based on the introduced indicators (SRI and MRP) in the Section II. Each figure shows two response surfaces next to each other, of which the left side surface is based on the data recorded with the PKI authentication turned off, and the right side represents the safety effect of the enabled PKI authentication framework.

A. Scenario S1

The first scenario has the lowest speed for both vehicles and a speed difference of 20 km/h, which predicts that the safety risk, in this case, will not be significant. The slope of $SRI_{PKI,OFF}$ surface is less steep than the $SRI_{PKI,ON}$, and in extreme cases (PDR=10%, E2E=1000 ms), the maximum point is around 0.25.

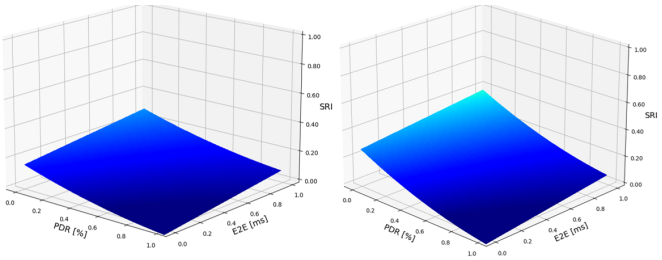

Fig. 3: SRI response surface for S1 scenario

The MRP surface generated from the binomial regression illustrates that the reception probability of CAMs in this low-velocity case is similar in the two PKI setup.

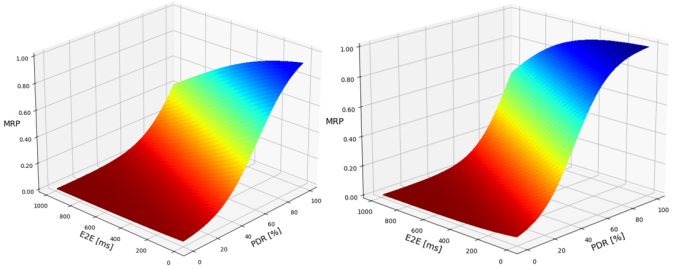

Fig. 4: MRP response surface for S1 scenario

B. Scenario S2

The second scenario is similar to S1 in that the speed difference is the same at 20 km/h, but both vehicles have higher speeds. It can be observed that at this speed level, the effect of PKI authentication on safety is not significant.

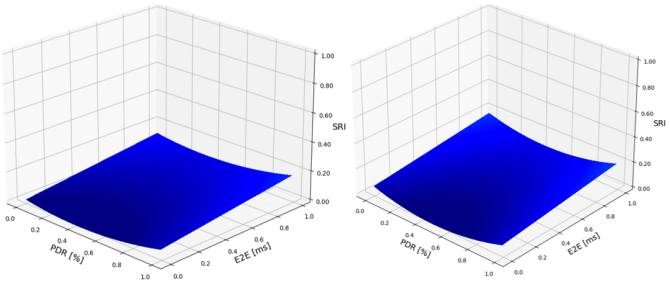

Fig. 5: SRI response surfaces for S2 scenario

At the MRP surface, it can be observed that with low network performance ($PDR < 20\%, E2E > 600ms$), the minimal overhead generated by the PKI means that fewer successfully received CAMs can be expected.

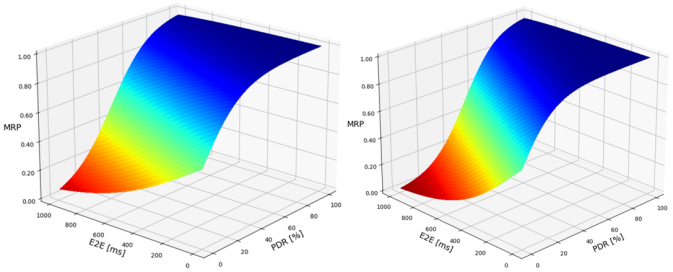

Fig. 6: MRP response surface for S2 scenario

C. Scenario S3

In this scenario, the speed difference is 50 km/h, so a higher increase in safety risk can be observed in the case of lower network performance. However, the two network performance metrics do not affect risk equally. The decrease in PDR shows a more intense increase in the response surface, while SRI is less affected by latency. Analyzing the maximum safety risk values, a difference of 0.1 can be observed between the $SRI_{PKI,OFF}$ and $SRI_{PKI,ON}$ cases.

Analyzing the MRP surface, it can be noticed that the difference between the $MRP_{PKI,OFF}$ and $MRP_{PKI,ON}$ cases is

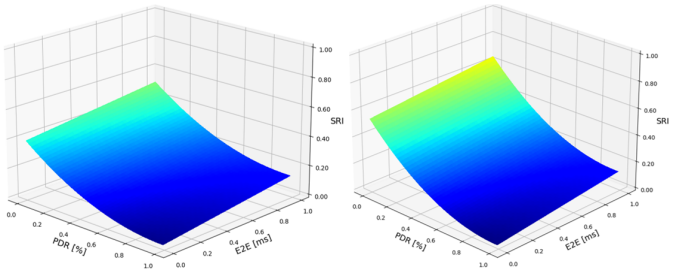

Fig. 7: SRI response surfaces for S3 scenario

that the shapes of the surfaces are slightly different but show remarkable similarity to the response surface presented in the S1 scenario.

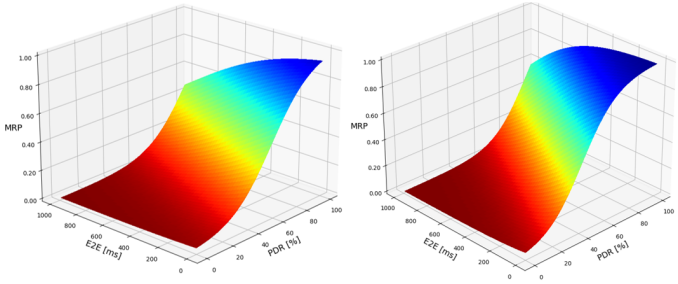

Fig. 8: MRP response surface for S3 scenario

D. Scenario S4

In the scenario S4, there is no real difference in the response surfaces. The speed difference is 50 km/h, making the surface very similar to the previous S3 surface.

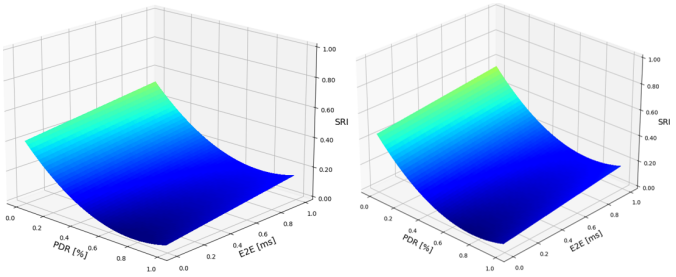

Fig. 9: SRI response surfaces for S4 scenario

For the MRP surface, it can be seen that in this scenario, the overhead effect of PKI can cause fewer received CAM messages only when the PDR drops below 30% and the latency is above 600 ms.

E. Scenario S5

The S5 scenario is unique because the large speed difference (80 km/h) increases the safety risk in both cases compared to the previous cases. The effect of PKI is more significant here. For MRP, the difference between $MRP_{PKI,OFF}$ and $MRP_{PKI,ON}$ is marginal in this scenario.

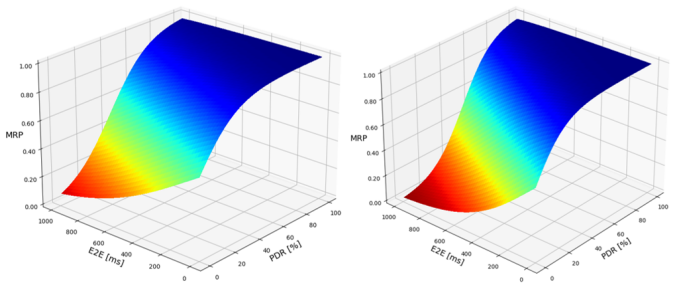

Fig. 10: MRP response surface for S4 scenario

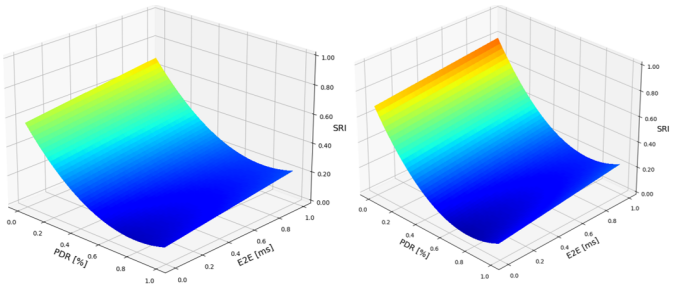

Fig. 11: SRI response surfaces for S5 scenario

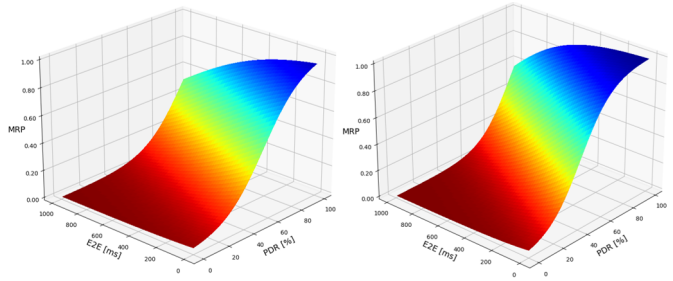

Fig. 12: MRP response surface for S5 scenario

F. Scenario S6

The highest speed and the highest speed difference scenario show a significant difference compared to the other scenarios, as the safety risk increases here at the fastest rate as a function of PDR.

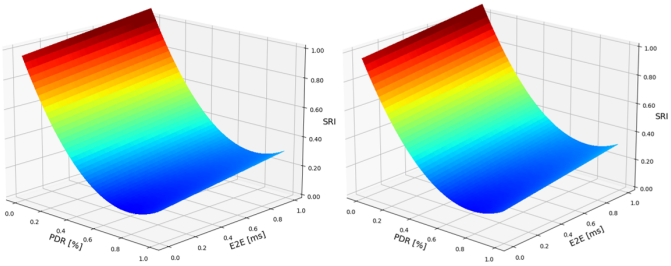

Fig. 13: SRI response surfaces for S6 scenario

As the figure shows, the size of the E2E and PDR intervals is more extensive for $MRP_{PKI,ON}$, where the MRP is less than 20%.

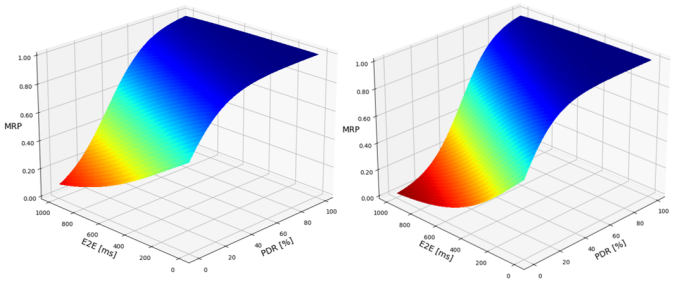

Fig. 14: MRP response surface for S6 scenario

G. Numerical results

We would like to support the conclusions drawn by comparing the numerical values summarized in Table II. To quantify the results, the points highlighted in S5 scenario are analyzed. At the PDR = 10% level, the SRI value ranges from 182 to 236. Comparing $SRI_{PKI,OFF}$ and $SRI_{PKI,ON}$ cases, it can be observed that the value of the SRI index for $SRI_{PKI,ON}$ is 20-30 higher.

As the PDR increases, it can be observed that the difference between $SRI_{PKI,OFF}$ and $SRI_{PKI,ON}$ decreases until, in the case of lossless communication, there is almost no difference between the two cases.

TABLE II: S5 scenario data

PDR	$E2E$	$SRI_{PKI_{OFF}}$	$SRI_{PKI_{ON}}$
10 %	0 ms	182	208
	500 ms	196	222
	1000 ms	211	236
50 %	0 ms	56	62
	500 ms	75	92
	1000 ms	118	135
100 %	0 ms	35	35
	500 ms	62	62
	1000 ms	80	87

IV. Conclusion

This study describes the safety effect of PKI security authentication processes' additional time demands, especially considering common network performance metrics (PDR, E2E). According to our research findings, we can conclude that the risk-increasing effect of the PKI framework is marginal. The additional computational demand of PKI, only in some exceptional, less likely cases, can lead to high-risk scenarios when the network performance drops below a critical level. PKI authentication is required in a V2X environment; however, when designing V2X-based AD/ADAS safety applications, we need to consider additional computational demands. For risk mitigation purposes, we can either apply the adaptive security principles or limit the operational design domain of the specific AD/ADAS application to maintain a tolerable risk level. Based on this approach, V2X-based AD/ADAS systems should be validated whether the system remains below an acceptable risk level throughout the operational design domain.

Acknowledgment

The research reported in this paper was supported by the ÚNKP-22-3-II and ÚNKP-21-5 new national excellence program of the Ministry for Innovation and Technology from the source of the National Research, Development and Innovation Fund.

The presented work was carried out within the MASPOV Project (KTI_KVIG_4-1_2021), which has been implemented with support provided by the Government of Hungary in the context of the Innovative Mobility Program of KTI.

References

[1] M. Zöldy, "Legal barriers of utilization of autonomous vehicles as part of green mobility," in *International Congress of Automotive and Transport Engineering*. Springer, 2018, pp. 243–248.

[2] H. Tschürtz and A. Gerstinger, "The safety dilemmas of autonomous driving," in *2021 Zooming Innovation in Consumer Technologies Conference (ZINC)*. IEEE, 2021, pp. 54–58.

[3] Z. Szalay, D. Ficzere, V. Tihanyi, F. Magyar, G. Soós, and P. Varga, "5g-enabled autonomous driving demonstration with a v2x scenario-in-the-loop approach," *Sensors*, vol. 20, no. 24, p. 7344, 2020.

[4] D. Grimm, M. Stang, and E. Sax, "Context-aware security for vehicles and fleets: A survey," *IEEE Access*, 2021.

[5] T. Sipos, A. Afework Mekonnen, and Z. Szabó, "Spatial econometric analysis of road traffic crashes," *Sustainability*, vol. 13, no. 5, p. 2492, 2021.

[6] T. Bécsi, Á. Szabó, B. Kővári, S. Aradi, and P. Gáspár, "Reinforcement learning based control design for a floating piston pneumatic gearbox actuator," *IEEE Access*, vol. 8, pp. 147 295–147 312, 2020.

[7] C. Csiszár and D. Földes, "System model for autonomous road freight transportation," *Promet-Traffic&Transportation*, vol. 30, no. 1, pp. 93–103, 2018.

[8] B. Nagy, P. Orosz, T. Tóthfalusi, L. Kovács, and P. Varga, "Detecting ddos attacks within milliseconds by using fpga-based hardware acceleration," in *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2018, pp. 1–4.

[9] J. Csatár and A. Dán, "Novel load flow method for networks with multipoint-grounded-neutral and phase-to-neutral connected equipment," *International Journal of Electrical Power & Energy Systems*, vol. 107, pp. 726–734, 2019.

[10] C. Krasznay and G. Gyebnár, "Possibilities and limitations of cyber threat intelligence in energy systems," in *2021 13th International Conference on Cyber Conflict (CyCon)*. IEEE, 2021, pp. 171–188.

[11] B. Fernandes, J. Rufino, M. Alam, and J. Ferreira, "Implementation and analysis of ieee and etsi security standards for vehicular communications," *Mobile Networks and Applications*, vol. 23, no. 3, pp. 469–478, 2018.

[12] B. Brecht and T. Hehn, "A security credential management system for v2x communications," in *Connected Vehicles*. Springer, 2019, pp. 83–115.

[13] H. Qiu, M. Qiu, and R. Lu, "Secure v2x communication network based on intelligent pki and edge computing," *IEEE Network*, vol. 34, no. 2, pp. 172–178, 2019.

[14] I. Agudo, M. Montenegro-Gómez, and J. Lopez, "A blockchain approach for decentralized v2x (d-v2x)," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4001–4010, 2020.

[15] M. Rumez, D. Grimm, R. Kriesten, and E. Sax, "An overview of automotive service-oriented architectures and implications for security countermeasures," *IEEE access*, vol. 8, pp. 221 852–221 870, 2020.

[16] A. Fazzat, R. Khatoun, H. Labiod, and R. Dubois, "A comparative performance study of cryptographic algorithms for connected vehicles," in *2020 4th Cyber Security in Networking Conference (CSNet)*. IEEE, 2020, pp. 1–8.

[17] G. Pauer and Á. Török, "Introducing a novel safety assessment method through the example of a reduced complexity binary integer autonomous transport model," *Reliability Engineering & System Safety*, vol. 217, p. 108062, 2022.

[18] Á. Török, "A novel methodological framework for testing automated vehicle functions," *European Transport Research Review*, vol. 12, no. 1, pp. 1–9, 2020.

[19] Z. Pethő, Z. Szalay, and Á. Török, "Safety risk focused analysis of v2v communication especially considering cyberattack sensitive network performance and vehicle dynamics factors," *Vehicular Communications*, p. 100514, 2022.

[20] T. Ormándi, B. Varga, and T. Tettamanti, "Distributed intersection control based on cooperative awareness messages," in *2021 5th International Conference on Control and Fault-Tolerant Systems (SysTol)*. IEEE, 2021, pp. 323–328.

[21] Z. Szalay, "Next generation x-in-the-loop validation methodology for automated vehicle systems," *IEEE Access*, vol. 9, pp. 35 616–35 632, 2021.

[22] S. Weisberg, *Applied linear regression*. John Wiley & Sons, 2005, vol. 528.