Analysis of Security Vulnerability Levels of In-Vehicle Network Topologies Applying Graph Representations

Zsombor Petho¹ · Intiyaz Khan¹ · Árpád Torok¹

Received: 23 April 2021 / Accepted: 26 October 2021 / Published online: 10 January 2022
© The Author(s) 2022

Abstract

This article investigates cybersecurity issues related to in-vehicle communication networks. In-vehicle communication network security is evaluated based on the protection characteristics of the network components and the topology of the network. The automotive communication network topologies are represented as undirected weighted graphs, and their vulnerability is estimated based on the specific characteristics of the generated graph. Thirteen different vehicle models have been investigated to compare the vulnerability levels of the in-vehicle network using the Dijkstra's shortest route algorithm. An important advantage of the proposed method is that it is in accordance with the most relevant security evaluation models. On the other hand, the newly introduced approach considers the Secure-by-Design concept principles.

Keywords In-vehicle network · Shortest path algorithm · Vulnerability · Security analysis

1 Introduction

Automotive security is a rapidly developing field, as the risk of securing automotive systems is increasing. New challenges emerge every day, which can lead to further security problems. Safety of vehicles from accidents and cyber-attacks will become the priority research orientation of the future development processes. In the in-vehicle network (IVN) protocol design process, automotive engineers have not addressed the cybersecurity issues adequately, instead, they focused on the safety aspects. Fault tolerance, robustness, reliability and an acceptable bandwidth were the key research objectives in this subdomain. Nevertheless, automotive trends have shown that transport and vehicles will be automated and communicate with each other to increase road safety, and the number of ECUs (Electronic Control Units) with ever-expanding ADAS (Advanced Driver Assistance Systems) functions will continue to grow. The growing number of ECUs implies that the required bandwidth is to widen, more subnets are present, and consequently more

error factors can be expected, which is already an embedded programming and electronic issue. If the problem is approached from a cyber-physical point of view, it can be seen that the protection of automotive communication networks is extremely important. The reason is that compromising the sensor or control data signals on the IVN can directly affect the physical operation of the vehicle, which has a direct impact on passenger safety. Based on these insights, it can be seen that security and safety co-engineering are required from the beginning of the design and development processes [21, 24].

Network protocols used currently in vehicles are LIN, CAN, FlexRay, MOST, and the automotive version of the well-known high-bandwidth Ethernet protocol. LIN (Local Interconnect Network) networks carry simple control signals (e.g., door and window operation); they are commonly used in subnets, and are not critical from a safety perspective. The CAN (Controller Area Network) is widely used in vehicular systems for its high reliability, robustness and low cost, for applications that do not necessarily need higher bandwidth than 1 Mbps. The cyber protection of the CAN bus is based on simple defense mechanisms, e.g. Cyclic Redundancy Checksum (CRC), Acknowledge (ACK), End of Frame (EOF) fields. However, several improvements have been made to the protocol since the first version appeared, e.g. time-triggered CAN, which further increased its security level [2, 6]. A newer generation

Responsible Editor: M. Tehranipoor

✉ Zsombor Petho
zsombor.petho@edu.bme.hu

¹ Department of Automotive Technologies, Budapest University of Technology and Economic, Budapest, Hungary

communication protocol is FlexRay, a fault-tolerant, deterministic, high-speed protocol, which supports safety and time-critical applications such as X-by-wire. Additionally, it is suitable as a communication backbone, which connects heterogeneous subnets together. The protocol has two main modes: single or dual channel mode; and each channel has a maximum bandwidth of 10 Mbps. Therefore, a dual-channel configuration can operate 20 times faster than the CAN bus data rate specification [6]. From a security perspective, the FlexRay system has a huge advantage, if data transfer is jammed or fails during one channel transmission, data can be authenticated on the other channel [21]. Nowadays, cars have domain ECUs and central gateways, but in the near future, the emergence of zonal gateways and central computing platform is expected, which will revolutionize in-vehicle E/E (electrical / electronic) architectures, and the requirements will also be fulfilled for the automotive Ethernet protocol. Nevertheless, the current and oldest E/E architectures and domain controllers could offer a high level of security if the topology design is very precise, and there are additional sub gateways besides the central gateway, which connect safety-critical function controllers [7, 19]. According to [20], segmented topologies and additional gateways support more stable and robust communication for critical applications by taking into account only a few ECUs interconnected by a small segment. Lots of vehicle functions need segment transitions (e.g. from CAN to FlexRay), and this presupposes resource-intensive load for ECUs, which actually act as transit gateways. Experience shows that intervening in additional ECU-gateways influences the overall network topology efficiency [9, 20]. In vehicles where all four communication protocols mentioned above (except automotive Ethernet) are present, the following topology types are used: star, bus, ring, and a mixture of these called a hybrid topology. In star topology, all the ECUs are connected to the central hub with individual lines. If the central ECU or the main hub fails, then the entire communication breaks down. However, if only one ECU fails, then the rest of the network continues to function. This kind of topology could be suitable for security and safety applications. The most common topology is bus topology, in which all ECUs are connected to the mainline. If the mainline is interrupted, two segments are formed, which normally continue to function. Ring topology has two main types: single ring and double ring. In the single ring topology, the information is sent in one direction from one node to the next one until the messages reach the destination node. This kind of connection has a big disadvantage, because when a single node fails, it disables the whole communication system. In contrast, in the double ring topology, the information flow is bidirectional, which is more reliable.

In the next section, we discuss the related research, results, and threat and vulnerability assessment methods that can be used to explore the vulnerability of vehicles to cyber-attacks.

2 Related Works

In particular, the safety design principles must be followed throughout the life cycle of vehicle network design and production, in accordance with the Functional safety (ISO26262) and the Road Vehicles – Safety of the Intended Functionality (SOTIF) standard (ISO / PAS 21448). As state-of-the-art vehicle systems should be treated as cyber-physical systems, SAEJ3061 (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems) standard should be considered with the same emphasis from the initial design phase. By adhering to these, several vulnerabilities may have emerged in the design of E/E architectures that would have been hidden during a traditional product development procedure. On the other hand, developers can support the robustness of the vehicle's network architecture by using the Secure by Design development concept, which reduces risks or, where appropriate, makes it nearly impossible for a malicious attacker to achieve its goal. In system evaluation processes, including vulnerability assessment, the main activity is threat modeling. Using the top-down deductive approach, threat modeling and vulnerability assessment tools help the developers make architectural decisions, reduce potential vulnerabilities, and consider every hidden security breach. In threat modeling, every development stage has its objectives with different requirements regarding input factors. One of the most widely used threat modeling procedures is STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of privilege), a software-centric model that also forms the basis of other threat modeling methods. Initially used in business enterprise IT systems, however, it has been successfully adopted by the automotive industry, as it covers all essential cybersecurity principles. As part of the EVITA research project (E-Safety Vehicle Intrusion Protected Applications), the researchers identified the E/E use cases and the potential threats and risks associated with them [8]. The level of risk associated with threats was assessed as a function of severity and likelihood, similar to the HARA (Hazard Analysis and Risk Assessment) safety-oriented methodology [11]. Another systematic identification process is TVRA (Threat Vulnerability and Risk Analysis) [4], which was introduced by ETSI in order to support security-oriented standardization processes. A combination of the above-mentioned STRIDE and HARA methodology is the SAHARA (Safety aware hazard analysis and risk assessment) method [16],

which considers safety and security co-engineering principles to enhance the effectiveness of security-aware safety development of cyber-physical systems.

Several studies have shown that at the embedded system level, it is worthwhile to examine the system architecture and provide innovative solutions at the processor and memory management level. Zheng et al. [28, 29] shows how to prevent side-channel attacks (e.g., cache attack, timing attack) using the digital PUFs (Physical Unclonable Functions), applied in the authentication mechanism at the machine level as a digital fingerprint, thus protecting the embedded system from tampering. Research has also highlighted the importance of protecting the intellectual property (IP) and integrity of the hardware with more sophisticated countermeasures like IP watermarking [22]. Certain design phases may assume the inclusion of Hardware Trojans (HT) that can modify the operation and parameters of the hardware even by leaking private cryptographic keys, which can lead to severe consequences. In the review [10], the authors summarize the critical vulnerabilities of the IVN that a malicious attacker can exploit using a different types of attack scenarios. According to this study, one of the weakest points of IVN is that there is no authentication process, and it is sensitive to spoofing attacks when a rogue node sends authentic messages to the bus. Another weak point in the communication system is that the data is broadcasted on the bus and this is feasible to passive eavesdropping attacks. DoS attacks can take advantage of the arbitration mechanism of the CAN bus because messages with low IDs are prioritized, so flooding a similar message can disrupt the whole communication process. Replay attacks can take advantage of the design flaw that message frames do not contain timestamp information.

According to a basic research study [14], major hazards originate from the interconnection of different car bus systems via various gateway devices, and when a single node is compromised all the other nodes are endangered. Furthermore, gateways can also interpret and compose all the distinct physical interfaces and manage protocol conversion and error protection of message verification. As centralized architectures with Ethernet backbone are lacking, in our research, gateways have a central role. They are present in the IVN, they offer advanced security countermeasures and improve the functional safety of the whole vehicle. In order to improve security of the controllers and gateways, one of the most commonly used countermeasures to handle impersonation type attacks is authentication. Authentication confirms that only valid controllers can communicate within the automotive bus system. Controllers need to have a certificate to send messages to the gateway as a valid sender. The certificate consists of the controller ID, a public key and the authorization of the controller. Accordingly, gateways contain a public key of OEMs (Original Equipment Manufacturer) of vehicles. The controller certificates are verified

from the OEMs with secret keys. Gateways use the public key of the OEM to verify the validity of the controller certificate [26].

Corresponding to the above-mentioned properties in the vehicular bus communication system, the gateway can be operated as a functional firewall [27]. The firewall rules are based on the authorization certificate (AC) between the gateway and the other controllers. Accordingly, only certified controllers can send messages into the vehicle bus system. The rules of firewalls can be applied to support the approval process related to the subnets. The vehicle has a vast number of components inside the vehicle communication network, and every component has a unique protection parameter. The aim of this study is to determine the vulnerability of a given vehicle. For this analysis, each protection parameter is represented as a cost function. To identify the shortest path from one component to another component, consecutive path lengths are examined. Hence, the vulnerability of a given vehicle is determined based on the shortest path.

3 Methodology

The main research idea is to identify the vulnerable points and the communication sublinks of a certain in-vehicle network. In this study, the degree of exposure of vehicular network topologies to cyberattacks was tested for fifteen vehicles. The analyzed vehicle types were selected based on which topologies were available online and those found in other cybersecurity studies [17]. Accordingly, in the first step, the topologies of the investigated communication networks were represented, then the communication links between the different components were ranked based on the security level of the given link. There are also industry standard vulnerability indicators like CVSS (Common Vulnerability Scoring System) [2], which generally evaluate software vulnerabilities in IT systems on a scale of 1 to 10. As the vulnerability score was evaluated according to automotive topologies, a new scoring system was developed.

3.1 Newly Developed Security Level Assessment Methodology

The results of our previous research pointed out that relatively few security levels can be adequate for efficiently characterizing the in-vehicle network's protection level. Based on the performed regression and cluster analyses, three levels are sufficient to rank the vulnerability of the vehicular communication networks [5]. In accordance with this, the typical IVN architecture frequently consists of three or four hierarchy levels: network domains separated by gateways (first level), subdomains handled by domain controllers (second level), and the bottom of the hierarchy tree is mainly

Table 1 Description of the protection levels applied in the graph-based analysis

Security level	Description
1	There is no protection between the connected nodes
2	In the evaluated link, the examined nodes are on a separate subnetwork
3	The link is protected with additional security measures (e.g., authentication, IDS)

built up from subnetworks (third level) [1]. Our scoring system distinguishes the protection status / vulnerability of a given communication link on 3 levels, which is briefly described below and presented in Table 1. If a link or section is not protected by any special security measures, including data encryption, authentication, gateway, HSM (Hardware Secure Module), or IDS (Intrusion Detection System), its security level is ranked 1. If the communication link is connected directly to a gateway, but no other security measures are applied (encryption, authentication), its security level is ranked 2. The third case is when a link is protected by a gateway acting as a firewall and has a strong authentication process: this corresponds to security level 3.

The figure below (Fig 1) illustrates how an arbitrary vehicle network topology was transformed into an undirected weighted graph and what weights were assigned to each edge. In practice, this means that the security level of the link between two ECUs is 1, as no extra protection can be found, such as an interleaved gateway, because they communicate with each other on the same bus. (An authentication process can actually be present between controllers, this is just an example for illustration). If an intruder wants to reach the convenience ECU (node no. 10) through the central gateway

(Main GW, node no. 0), this attack results in a cost of 4, as the cost of the edges is added upon the shortest route.

Thus, the examined networks were represented by graphs, and considering the protection level of the edges as resistance-like parameters, we estimated the overall protection level of each communication network. According to our concept, if a network is built-up from relatively less protected components, then the sum of the shortest path between the network nodes will be lower. Following this, in our study, the shortest path was identified from one vehicle component to the other in a vehicle communication network using the generalized Dijkstra's algorithm by assuming the protection level of components [3]. Then a comprehensive database was constructed to characterize vehicle security-related parameters. The Dijkstra's algorithm checks the shortest path from the starting node to the destination point. The generalized Dijkstra's algorithm assumes the initial node has zero weight, and it compares the next minimum weight functions (summing the edges' costs of the given route towards the destination node) from the origin point. At every node, it seeks the minimum weight to the next node, and then later, it forms the shortest path according to the lowest weight. We described the applied model by the following pseudo-code. The command $i \leftarrow \text{nodes in } N \text{ with min distance}[i]$, finds the node i in the node set N that has the least distance $[i]$ value. $\text{Length}(i, j)$ represents the length of the newly added link among the points i and j . The parameter former describes the length of the route between the starting point and the point j (in the case of entering i). If the current shortest route is shorter than the newly defined route assigned to j , then the actual route is replaced with this diff path. The former array includes the pointer to the "following-target" point of the investigated network to identify the shortest path to the starting point.

Fig. 1 Simplified in-vehicle network topology (left) transformed into a weighted undirected graph (right)

Algorithm 1 Shortest path algorithm

```

1: function SHORTESTPATH( $N, starting\_point$ )
2:   initialize  $N$  set of nodes
3:   for  $i = 1$  to  $N$  do
4:      $distance[i] \leftarrow \infty$ 
5:      $former[i] \leftarrow$  not identified
6:     assign  $i$  to  $N$ 
7:   end for
8:    $distance[starting\_point] \leftarrow 0$ 
9:   while  $N$  is not empty do
10:     $i \leftarrow$  node in  $N$  with min  $distance[i]$ 
11:    remove  $i$  from  $N$ 
12:  end while
13:  for every neighbor  $j$  of  $i$  do //if  $N$  contains  $j$ 
14:     $diff \leftarrow distance[i] + length[i, j]$ 
15:    if  $distance[j] > diff$  then
16:       $distance[j] \leftarrow diff$ 
17:       $former[j] \leftarrow i$ 
18:    end if
19:  end for
20:  return  $distance[ ]$ ,  $former[ ]$ 
21: end function

```

We created a MATLAB code to construct the network topologies: the edges of a network were defined by their starting points s and their terminating points t . The estimated security level of the edges is described by w . The graph of the topology is built up by the graph command, and the shortest path command defines the shortest routes between the nodes of the graph. Finally, the total security parameter of the topology is stored in A . The symbolic representation of A can be given as follows:

$$A = \sum_{i=1}^n \sum_{j=1}^n SR_{ij} \quad (1)$$

Where,

- A is the security parameter characterizing the protection level of the network;
- SR_{ij} is the shortest route between i and j nodes;
- n is the number of nodes in the graph.

The code below describes the algorithm responsible for generating the A parameter.

Figure 2 represents the generated simplified topology diagram of an Audi A6 as an example. The diagram is a simplified topology that provides an overall view of the communication architecture of the vehicle and the control unit protocol that performs the key functions. As the figure below shows, all communication buses are connected to the central gateway, which already presupposes a higher level of security. Most of the safety-critical control units are connected to the FlexRay bus. Some of these ECUs also have other bus connections, e.g. the Power Steering Control Module is also connected to the Powertrain CAN. The gateway can be accessed via an OBD-II connection on the diagnostic CAN. The multimedia-related ECUs are connected to the MOST bus in a ring topology. The heating, ventilation, and air conditioning (HVAC) module, illumination control module, and other sensors are connected to the LIN subnetworks. The control units with comfort functions (e.g. seat control) are connected to the Convenience CAN, which usually operates at 100 kbps, in contrast to the Powertrain CAN, which supports data transfer at a speed of 500 kbps.

Algorithm 2 Vulnerability evaluation algorithm

```

1: function VULNERABILITYEVALUATION( $G, S, t$ )
2:    $s = [i_1 \dots i_k \dots i_n]$ 
3:    $t = [j_1 \dots j_k \dots j_n]$ 
4:    $weights = [sec_1 \dots sec_k \dots sec_n]$ 
5:   for  $s = 1$  to  $n$  do
6:     for  $t = 1$  to  $n$  do
7:        $[P, d] \leftarrow ShortestPath(G, s, t)$ 
8:        $A[s, t] \leftarrow d$ 
9:     end for
10:  end for
11: end function

```

Fig. 2 Simplified topology representation diagram of Audi A6 SSP

3.2 Comparative Methods

We briefly present a security analysis and evaluation procedure developed during a previous research process using an alternative method to compare previous results with the current results. In the first step of the method, the relevant characteristics of the IVN topologies (the number of safety-critical ECUs protected, etc.) were determined [5]. Homogeneous vehicle groups were identified by cluster analysis of the relevant characteristics. Subsequently, the security level of each vehicle was determined using a regression estimation procedure. Ordinal logistic regression was performed in order to estimate the protection cluster of the investigated vehicle. The applied method uses a cumulative probability model. The sum of the cluster probabilities is 1. C represents the number of categories, while c represents each specific category. The likelihood of classifying an object into the c -th category is π_c . In accordance with this, in the case of the cumulative log link function, (η_c) the log odd ratio provides the relationship between likelihood of being contained by cluster c (π_c) and its complementary likelihood ($1 - \pi_c$). The log odd ratio is expressed below:

$$\eta_c = \frac{\pi_c}{1 - \pi_c} \quad (2)$$

4 Results

In the previous section, we described the applied evaluation methodology to analyze the vulnerability of the different communication network topologies. The shortest routes in the communication network were identified by Dijkstra's algorithm. Considering the generated indicator, it became possible to improve the topology structure until the network characteristic reaches the acceptable security level. It is possible to enhance the security level of the in-vehicle communication network by applying advanced encryption techniques, authentication methods or intrusion detection systems.

4.1 Main Findings of the Evaluation

The result of the performed vulnerability analysis is presented below. Towards the bottom of the table, the security of the network increases and accordingly, the estimated vulnerability of the topologies decreases. Based on the presented investigation, we can conclude that the 2014 Chrysler has the lowest security level, it seems to be the most vulnerable model out of the examined fifteen vehicles. On the other hand, the 2018 Toyota Avensis has the highest protection score, accordingly, it appears to be the least vulnerable one. Compared to other research studies [5, 17, 18] that have in some way ranked vulnerability levels of vehicles on the basis of in-vehicle network

Table 2 Results of the vulnerability analysis and comparison with previous research results

Vehicle models	Protection level (curr. method)	Vulnerability level [5]
2012 Chrysler 300C	36	2.00
2014 Jeep Cherokee	84	3.00
2010 Range Rover Sport	100	1.40
2014 Honda Accord Lx-sedan	136	2.17
2013 Ford Fusion	138	2.00
2015 Cadillac Escalade	168	2.67
2014 BMW X3	190	1.00
2014 Range Rover Evoque	196	0.79
2014 BMW 3 series F30	224	0.65
2014 Infinite Q50	236	0.00
2014 Audi A8	404	0.38
2014 BMW i12	450	0.75
2015 Toyota Prius	584	0.25
2017 Audi Q7	592	0.20
2018 Toyota Avensis	596	0.00

topology/architecture, it can be seen that similar results were obtained. A well-known remote exploitation experiment [18] has proven how vulnerable the Jeep Cherokee is, and our analytical calculation gave the same result. Higher-ranking cars, like BMW, Audi, tend to be in the middle and upper field, but the brand is no guarantee that the vehicle will be protected from a cybersecurity standpoint. As considered by the applied methodology, the vehicle components with lower security value are more vulnerable. On the other hand, a vehicle with a higher security score has more protection among the elements of the communication network (see Table 2).

Based on the defined Spearman rank correlation coefficient ($r_s = -0.8712$), the association between the results of the two compared methods is statistically significant on an $\alpha = 0.05$ significance level ($p = 0.00002$).

4.2 Effectiveness of the Proposed Method Related to the Relevant Attack Scenarios

The essential objective of protecting the in-vehicle network is to ensure the reliability of the communication process, especially considering integrity, availability, confidentiality. Assuming a malicious intervention, a breach of integrity can be accomplished by sending compromised messages (e.g., replay attack, injection attack). On the other hand, the availability of the communication network can be reduced by overloading the system with an excessive amount of messages (e.g., Denial-of-Service type attack). Confidentiality can be mainly harmed by applying passive attacks such as eavesdropping when a malicious attacker gathers sensitive data from the network.

Our evaluation strategy gives higher scores for

- Rationally segmented E/E architectures,
- Application of better-protected entry points,
- Application of additional security measures.

Well-segmented topologies can reduce the effectiveness of most attack scenarios. Gateways and domain controllers can make it difficult for an attacker to access subnets with different communication protocols, maintaining integrity, availability, and confidentiality. Application of additional security solutions like IDS (Intrusion Detection System), IPS (Intrusion Prevention System), firewall, honeypots, and other active measures can hinder the execution of the attack scenario. In accordance with this, the developed graph-based methodology can significantly contribute to the establishment of a highly-secured vehicular system.

5 Conclusion

In our study, the vulnerability of different in-vehicle networks was investigated based on Dijkstra's shortest path algorithm. In the first step, from the database of the investigated communication networks, the topologies were generated. Then the communication links between the different components were ranked (1, 2, 3) based on the security level of the given link. Following this, the analyzed networks were represented by undirected weighted graphs, and considering the protection level of the edges as resistance-like parameters, the overall protection level of each communication network was estimated. According to this concept, if a network is built-up from relatively less protected components, then the sum of the shortest path between the network nodes will be lower. Results shown that the 2018 Toyota Avensis had the highest vulnerability score from analyzed vehicles. One of the limitations of our method is that it works when the E/E architecture of the investigated car consists of domain controllers and has a central gateway. If the IVN has redundant computing platforms and automotive Ethernet as a backbone communication protocol, then this graph-based algorithm has to be reconsidered and upgraded. After adapting the requirements of different state-of-the-art communication protocols, the proposed methodological approach can be widely used in the automotive security evaluation domain. An important advantage of the proposed method that it is in accordance with the most relevant security evaluation models (TARA, C-SIL, EVITA, Heaven [12, 13, 15, 23, 25]). On the other hand, the newly introduced approach considers the Secure-by-design concept principles (e.g., network segmentation, making compromise and disruption difficult).

Acknowledgements The research presented in this paper have been supported by the NRDI Office, Ministry of Innovation and Technology, Hungary, within the framework of the Autonomous Systems National Laboratory Programme, and the NRDI Fund based on the charter of bolster issued by the NRDI Office. 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. Moreover, the authors are grateful for the support of New National Excellence Programme Bolyai+ scholarship. Supported by the ÚNKP-20-5 New National Excellence Program Of The Ministry For Innovation And Technology from the source of the National Research, Development And Innovation Fund.

Funding Open access funding provided by Budapest University of Technology and Economics.

Data Availability Statement The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- (2021) Vag self study program. http://www.volkspage.net/technik/ssp/index4_eng.php
- Bajpai P, Enbody R (2020) Towards effective identification and rating of automotive vulnerabilities. In: Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security, pp. 37–44
- Deng Y, Chen Y, Zhang Y, Mahadevan S (2012) Fuzzy Dijkstra algorithm for shortest path problem under uncertain environment. *Appl Soft Comput* 12(3):1231–1237
- ETSI T (2017) 102 165-1 v5. 2.3 (2017-10) cyber; methods and protocols; part 1: Method and proforma for threat, vulnerability. Risk Analysis (TVRA) Standard, European Telecommunications Standards Institute (ETSI)
- Ghadi M, Sali Á, Szalay Z, Török Á (2020) A new methodology for analyzing vehicle network topologies for critical hacking. *J Amb Int Humanized Comp* pp. 1–12
- Groza B, Murvay S (2013) Efficient protocols for secure broadcast in controller area networks. *IEEE Trans Industr Inf* 9(4):2034–2042
- Hegde R, Kumar S, Gurumurthy K (2013) The impact of network topologies on the performance of the in-vehicle network. *Int J Comput Theory Eng* 5(3):405
- Henniger O, Ruddle A, Seudié H, Weyl B, Wolf M, Wollinger T (2009) Securing vehicular on-board it systems: The evita project. In: VDI/VW Automotive Security Conference, p. 41
- Huang T, Zhou J, Wang Y, Cheng A (2017) On the security of in-vehicle hybrid network: Status and challenges. In: Proc. International Conference on Information Security Practice and Experience, pp. 621–637. Springer
- Hu Q, Luo F (2018) Review of secure communication approaches for in-vehicle network. *Int J Automot Technol* 19(5):879–894
- Khastgir S, Birrell S, Dhadyalla G, Sivencrona H, Jennings P (2017) Towards increased reliability by objectification of hazard analysis and risk assessment (hara) of automated automotive systems. *Saf Sci* 99:166–177
- Kocsis B, Vida G, Szalay Z, Ágoston G (2021) Novel approaches to evaluate the ability of vehicles for secured transportation. *Period Polytech Transp Eng* 49(1):80–88
- Kong HK, Hong MK, Kim TS (2018) Security risk assessment framework for smart car using the attack tree analysis. *J Ambient Intell Humaniz Comput* 9(3):531–551
- Lukasiewicz M, Glaß M, Haubelt C, Teich J, Regler R, Lang B (2008) Concurrent topology and routing optimization in automotive network integration. In: Proceedings of the 45th Annual Design Automation Conference, pp. 626–629
- Macher G, Armengaud E, Brenner E, Kreiner C (2016) A review of threat analysis and risk assessment methods in the automotive context. In: International Conference on Computer Safety, Reliability, and Security, pp. 130–141. Springer
- Macher G, Sporer H, Berlach R, Armengaud E, Kreiner C (2015) Sahara: a security-aware hazard and risk analysis method. In: Proc. Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 621–624
- Miller C, Valasek C (2014) A survey of remote automotive attack surfaces. *Black hat USA 2014*, 94
- Miller C, Valasek C (2015) Remote exploitation of an unaltered passenger vehicle. *Black Hat USA 2015(S 91)*
- Moritz R, Ulrich T, Thiele L (2012) Evolutionary exploration of e/e-architectures in automotive design. In: Operations Research Proceedings 2011, pp. 361–366. Springer
- Neumann A, Mytych MJ, Wesemann D, Wisniewski L, Jasperneite J (2017) Approaches for in-vehicle communication—an analysis and outlook. In: Proc. International Conference on Computer Networks, pp. 395–411. Springer
- Püllen D, Anagnostopoulos NA, Arul T, Katzenbeisser S (2019) Security and safety co-engineering of the flexray bus in vehicular networks. In: Proceedings of the International Conference on Omni-Layer Intelligent Systems, pp. 31–37
- Shayan M, Basu K, Karri R (2019) Hardware trojans inspired ip watermarks. *IEEE Des Test* 36(6):72–79
- Tandon R, Gupta P (2021) Sv2vcs: a secure vehicle-to-vehicle communication scheme based on lightweight authentication and concurrent data collection trees. *J Amb Int Humanized Comp* pp. 1–17
- Török Á, Pethő Z (2020) Introducing safety and security co-engineering related research orientations in the field of automotive security. *Period Polytech Transp Eng* 48(4):349–356
- Török Á, Szalay Z, Sági B (2020) New aspects of integrity levels in automotive industry-cybersecurity of automated vehicles. *IEEE Trans Intell Trans Syst* 23(1):383–391
- Ueda H, Kurachi R, Takada H, Mizutani T, Inoue M, Horihata S (2015) Security authentication system for in-vehicle network. *SEI Tech Rev* 81:5–9
- Wolf M, Weimerskirch A, Paar C (2004) Security in automotive bus systems. In: Workshop on Embedded Security in Cars, pp. 1–13. Citeseer
- Zheng JX, Li D, Potkonjak M (2014) A secure and unclonable embedded system using instruction-level PUF authentication. In: Proc. 24th International Conference on Field Programmable Logic and Applications (FPL), pp. 1–4. IEEE
- Zheng JX, Potkonjak M (2014) A digital PUF-based ip protection architecture for network embedded systems. In: Proc. ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS), pp. 255–256

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Zsombor Pethő is currently a Ph.D. student in the Department of Automotive Technologies, Budapest University of Technology and Economics. He received his BSc degree from Technical University in Cluj Napoca, in Electrical Engineering. In 2019 received the MSc degree in Control Engineering in Budapest. His research focus include CCAM mobility, V2X communication, in-vehicle network, Cyber-Physical Systems, and safety-security co-engineering.

Intiyaz Khan finished his BSc in 2017 at Abdul Kalam Azad Technical University Lucknow, India as Mechanical Engineering. He graduated as a Vehicle Automation Engineer in 2020 at Budapest University

of Technology and Economics. His major focus domains are Computer Aided Processing, Vehicle Automation, and Research and development in Vehicle Industry.

Árpád Török graduated in 2006 at TU Budapest as a Transportation Engineer, and in 2009 at TU Budapest as a Transport Economist. He completed his PhD at TU Budapest in 2010. He has been working at the Department of Automotive Technologies since 2018, and is now the head of Safety and Security Research Team. His research team focuses on automotive safety and security analysis, especially considering the aspects of integrated methods. Árpád Török is a member of the Association for Transport Sciences since 2006 and a member of the Hungarian Scientific Academy since 2010.