



Modelling the effects of certain cyber-attack methods on urban autonomous transport systems, case study of Budapest

Árpád Török¹ · Zsolt Szalay¹ · Gábor Uti² · Bence Verebélyi²

Received: 4 December 2018 / Accepted: 4 March 2019 / Published online: 12 March 2019
© The Author(s) 2019

Abstract

Based on the reviewed literature, the objective of the article is to investigate the most important cyberattack factors affecting the effectiveness of the connected and autonomous transport system. Accordingly, remotely implemented malicious interventions are in the focus of our study, especially considering cyberattacks on connected and autonomous vehicles. To introduce the expected impact of the analysed cyberattacks, certain cyberattack types are demonstrated in the paper. In the paper, malicious interventions are assumed to attack the transport network contrary to the individual road users, which assumption can strongly increase the risk of a given cyber-incident. To illustrate the effect of the evaluated cyberattacks, the transport system of Budapest is used. According to the results, some of the interventions might not be effective, while some of them can expectedly significantly increase travel time values of the network.

Highlights

1. A novel theoretical framework has been introduced to describe the effect of the analysed cyberattacks on urban transport system.
2. The new approach makes it possible to evaluate the risk and the impact of the represented cyberattacks targeting the connected and autonomous urban transport system.
3. The novel methodology allows the operator to indicate the weak points of the network from a vulnerability point of view, especially considering remotely controlled malicious interventions.

Keywords Security-and-privacy · Autonomous-driving-and-communication · Vehicle-to-vehicle/roadside/Internet-communication · Vehicular-security · Cyberattack

✉ Árpád Török
arpad.torok@auto.bme.hu
Zsolt Szalay
zsolt.szalay@auto.bme.hu
Gábor Uti
gabor.uti@relativegap.com
Bence Verebélyi
bence.verebelyi@relativegap.com

¹ Department of Automotive Technologies, Faculty of Transportation and Vehicle Engineering, Budapest University of Technology and Economics, Műegyetem rkp. 3, 1111 Budapest, Hungary

² RelativeGAP, Lingfield, Surrey, UK

1 Introduction

The spread of connected and autonomous vehicles (CAV) is one of the most awaited enhancements of the future (Szalay et al. 2018). Operators of urban transport systems approach similarly this question. However, they have numerous caveats about the appearance of autonomous vehicles in the urban environment. Most of the studies focusing on this field expect significant improvement in operation efficiency, estimate remarkable savings in external costs and basically emphasise the positive effects of the new forms of transportation. On the other hand, it would be important to have prognosis of the negative effects related to the new system to be able to form a balanced evaluation and to prepare for the expected difficulties (Zöldy 2018).

Based on the known global trends, it is expedient to give a brief overview about the recently applied assumptions and scientific evaluations related to future transport systems. This review can help the reader to have a clear impression about the most important challenges of the present and the possible development scenarios of the future. Accordingly, the expected minor permeation time of autonomous and connected vehicles makes it urgently necessary to estimate the transformation characteristics of the transportation system. Kröger, Kuhnimhof, and Trommer have concluded that the average number of autonomous vehicles is expected to be higher in Germany than in the USA, since the spread of up-to-date vehicle technology is traditionally faster in Germany. On the other hand, lower penetration level of autonomous vehicles can result in a growing travel demand level, since the public transport network is less dense in the USA (Kröger et al. 2018). Fox-Penner et al. (2018) have presented that the electric (and expectedly autonomous) vehicle fleet is going to have a large demand for electrical energy, but it seems to be possible to provide the necessary resources to supply these demands, so it is not going to limit the spread of autonomous vehicle technology. The model introduced by Farhan and Chen (2018) has derived that if 10% of total travel demand could be supplied by shared autonomous and electric vehicles, it could be financially feasible. Ye and Yamamoto have investigated the influence of connected and autonomous vehicles in an averagely parametrized road environment (two-lane, inhomogeneous traffic). The effect of road capacity broadening has been confirmed by their research (Ye and Yamamoto 2018). Iacobucci et al. have introduced a new modelling approach to investigate the feasibility of an autonomous transport system based on shared electric vehicles. The analysis has presented that all of the shared autonomous electric vehicles in the investigated area (Tokyo) could substitute 7–10 private cars (Iacobucci et al. 2018). Haboucha et al. have presented a comprehensive research focusing on the key factors of individual decisions related to autonomous car ownership and usage. They have concluded that an outstandingly advantageous property of the fully automated vehicle transportation is that it supports the formation of a new transportation mode combining the advantages of private and public transportation (Haboucha et al. 2017).

Important studies has evaluated the security effect of novel information technology solutions. Alsumayt et al. have analysed the impact of internet of things on security, especially focusing on mobile ad-hoc networks (MANET). Authors have found that because of the characteristic of MANET, like time variant topology and lack of registration point, many problems are embedded (e.g. Denial of Service—DoS attacks). Finally the article has introduced a newly developed model to recognize DoS like intrusion. (Alsumayt et al. 2017). Hamida and other researchers have

suggested different security solutions that are applicable to enhance the security of vehicular ad-hoc networks. Finally, a special modelling environment has been developed to verify the new framework and according to the results of the paper, the effectiveness improving effect of the novel model has proved to be significant. (Hamida et al. 2017). Other researchers (Darwish and Hassanien 2018) have analysed directly the expected security risk of special attacks targeting vehicular networks. Kong and colleagues have proposed a security risk assessment framework (Kong et al. 2018) to evaluate the related risks. The developed model has been used to investigate threats focusing on velocity and privacy.

On the basis of the evaluated researches the aim of the paper is to analyse the most emphatic cyberspace related risk factors influencing the efficiency of the connected autonomous systems. In case of our analysis, the cyberspace related effects are in the focus, especially considering malicious interventions on connected and autonomous transport systems. To illustrate the expected effects of the investigated cyber-incidents, examples related to certain cyberattack types are presented in the study. In case of our investigation, incidents are assumed to target the transport network, instead of the individual road users, which approach can multiply the risk of a given intervention. To demonstrate the results of the investigated cyberattacks, the transport network of Budapest has been used.

Our study is based on the Unified Traffic Model of Budapest (EFM¹) maintained by the Centre for Budapest Transport. During the analysis, a continuous growth has been assumed in the number of autonomous vehicles. Accordingly, the investigated scenarios are differentiated based on the proportion of autonomous vehicles in the urban vehicle fleet. Due to the development of connectivity and automated functions, in the urban vehicle fleet, following distance is also expected to be decreased significantly. However, the decrease of the average following distance is investigated depending on the penetration of autonomous vehicles in the vehicle fleet. The reason for this is presence of human factor in the urban transportation system, which cannot allow us to dispense with reaction time. On the other hand, the evaluation does not take into account the reduction of parking space occupancy expected due to the decreasing number of vehicles explained by the increasing vehicle occupancy data.

¹ EFM is the Hungarian abbreviation of “Egységes Forgalmi Modell”.

2 Methodology

The aim of this section is to introduce the theoretical and practical tools used during the investigation to describe the effect of the analysed cyberattacks. Firstly, the applied evaluation framework and the assumed conditions are presented, emphasizing the parameters of the baseline scenario. In the second step, the analysed attack scenarios are introduced briefly.

To describe the operation processes and the efficiency of an assumed autonomous urban transportation system—especially from a methodological point of view—it is a key issue to define the most significant vehicle related parameters, which directly influence the effect of autonomous vehicles on the operation efficiency of the urban transportation system.

2.1 Applied traffic modelling framework

The basics of our analysis has been implemented in PTV VISUM framework, however the general EFM model has been developed by the description of the expected effect of autonomous vehicles on saturation.

The traffic assignment procedure is performed by the equilibrium method. The equilibrium assignment is described as an optimization problem. Where the aim is to minimize the total resistance like property (e.g. travel time) related to all the elements of the network.

$$T = \sum_{k=1}^n \int_0^{f_k} I_k(x) dx \rightarrow \min! \tag{1}$$

$$f_{ijl} > 0, \quad \forall ij l \tag{2}$$

$$f_{ij} = \sum_{l=1}^m f_{ijl}, \quad \forall ij \tag{3}$$

$$f_k = \sum_{l=1}^m f_{ijl}, \quad \forall k \Leftrightarrow k \in R_{ijl} \tag{4}$$

$$\sum_{a=1}^n f_a - \sum_{b=1}^n f_b = \sum_{h=1}^n f_{hc} - \sum_{h=1}^n f_{ch} = A_c - D_c, \quad \forall c$$

$$\Leftrightarrow \forall a \in g_{qc}, \quad c \in N \wedge \forall q \in N \wedge g_{qc} \in E, \quad \forall b \in g_{cu}, \quad c \in N \wedge \forall u \in N \wedge g_{cu} \in E. \tag{5}$$

where T is the minimized objective function, E is the set of links contained by the graph, N is the set of nodes contained by the graph, $I_k(x)$ is the resistance like property of network element k loaded by x volume of traffic, f_{ijl} is traffic loaded

on route l from district i to district j , f_{ij} is the sum of traffic loaded on the network from district i to district j , f_k is the traffic loaded on network element k , R_{ijl} is the route k from district i to district j , A_c is the total traffic arriving to node c , and, D_c is the total traffic departing from node c .

The introduced representation describes the total traffic load of a given network element (f_k) based on the sum of traffic demand between the investigated model districts with regard to the relevant routes (R_{ijl}) between the districts. As a boundary condition it is assumed that the total traffic arriving to a given node is equal to the total traffic departing from the investigated node. According to the presented optimization framework, the objective of the constrained minimization problem is to minimize the sum of the introduced resistance like parameter ($I_k(x)$) depending on the loaded traffic on a system level.

The route choice related decision process is a multifactor based cost function, which is influenced on the one hand by the travel time depending on the saturation of the given network elements and on the other hand by the constant components, like travel distance and road toll. The variable resistance like property of the network components has been calculated based on volume delay functions. Depending on the type of network element, more types of volume delay function can be applied, although the most of the network elements use BPR like function form, published by Bureau of Public Roads. However the traditional equation is extended by the autonomous vehicles related passenger car unit parameter, which aims to influence the infrastructure capacity depending on the penetration of the automated vehicles. This approach makes it possible to represent the effect of automated vehicles on network capacity and travel time.

$$I_k = t_0 \cdot \left[1 + a \cdot \left(\frac{f_k \cdot AV_{PCU}}{c_k} \right)^b \right] + CF_k, \tag{6}$$

where t_0 is the free flow travel time on network element k per unit of time, c_k is the capacity of network element k per unit of time, AV_{PCU} is the passenger car unit parameter related to autonomous vehicles, a , b is the road type dependent estimation parameter, and CF_k is the other costs of network element k per unit of time (e.g. length, toll, etc.).

In case of the analysis related to local attacks the blocking back model has been applied which makes it possible to evaluate the effect of limited capacity resources. The so called blocking back model can be applied together with the originally applied assignment. In the model, firstly the excess congestion parameter (Eq. 7) is calculated related to the investigated network element. In the next step, based on the derived excess congestion parameters the wait times of the network are defined.

$$Fe_k = \frac{fa_k}{c_k \cdot S - fb_k}, \quad (7)$$

where Fe_k is the excess congestion factor, fa_k is the traffic of edge k resulted from the assignment, fb_k is the basic traffic of edge k , and S is the correction parameter.

2.2 Selecting relevant model parameters

To define the most relevant factors and their model values, it is necessary to consider the autonomous vehicle related generally accepted information set as premises. Beside this, the most important parameter values have to be derived from the universally applied technical formulas.

According to the conservative approach of the study—on a macro level, savings related to the effect of urban autonomous transportation system on operation efficiency improvement are mostly resulted by:

- Relative capacity increase caused by the reduction of following distance,
- Time savings of supplementary trip components related to individual vehicle transportation (walking, parking).

Accordingly it is necessary to estimate the expected change in the following distance values based on characteristics of automated vehicles.

In the next step of the parameter specification, the expected factor of following distance reduction has been defined according to the different levels of automation. First of all, the extreme values of the scale are expedient to be defined. During the identification of the model parameter values, the parameters applied in the literature have been considered. In most of the researches, following distance and traffic density are strongly related, since average following distance can be derived from traffic density and average flow speed. Based on this approach Iacobucci et al. (2018) have shown in their article that average improvement in capacity can be between 15 and 100% depending on the assumed traffic behaviour of autonomous vehicles (e.g. acceleration, deceleration, lane changing characteristic, etc.). Howard and Dai (2014) present in their study that even more than 350% capacity improvement can be realistic.

To remain by the previously accepted estimation principle, it is favourable to apply a conservative assumption to avoid overestimation of benefits, accordingly capacity improvement factor related to the introduction of autonomous vehicles is assumed to be 40%.

After the estimation of the capacity improvement factor, in the next step it becomes possible to define the following distances of the future systems.

The other important analysed factor is the time savings of supplementary trip components related to individual vehicle transportation (walking, parking). In this case an additive parameter is applied, of which values reduce constantly the time necessity of supplementary trip components in the model depending on the penetration of the automated vehicles. This effect is represented in the EFM model by the reduction of resistance like properties of zone connectors. Based on the reviewed literature, the average searching time for parking spots in the bigger cities of the world is between 4 and 14 min (Shoup 2006; Benenson et al. 2008). In the case of supplementary trip components related savings, it is still practical to use the previously mentioned conservative approach, so the maximum value of this parameter is assumed to be 2 min. This means that according to our assumption the maximum value of assumed time saving related to supplementary trip components is 2 min, which represents SAE5 level. In case of SAE1 there is no improvement prognosticated.

The constraint of the current study let us only evaluate a limited number of attack types. However the flexibility of the model environment makes it possible to extend the set of analysed attacks. Although, it is expedient to take into account that due to the macroscopic characteristic of the analysis, the novel modelling approach is reasonable to be used if the investigated processes and effects occur at system level. It is important to emphasize that the application of the current methodology makes it necessary to define the relationship between the investigated attack type and relevant parameters of the model. Accordingly, a new cyberattack can primarily be well described by the model if it is possible to estimate its effect on capacity, saturation, following distance, speed or traffic volume reliably.

2.3 Scenario analysis

The effect of different attack types is evaluated through three scenarios. In the first type of the investigated attacks, a hardly detectable intervention is analysed, which is expected to have reasonable impact on the system in case of a long term, permanently undetected operation period. This kind of incident is assumed to maliciously influence the freely or restrictedly available navigation systems or a part of them, modifying its capability to reliably support the transportation process of road users on the urban network. There are many ways to reduce the reliability, or the efficiency of the navigation processes. However there is only a limited set of interventions considered in the paper, which constitute the marginal reduction and increase in the resistance-like property of certain network elements. This would systematically influence route choices significantly reducing system efficiency. On the other hand, a more safety critical incident is also tested in the paper, where critical components of the

infrastructure network are assumed to be attacked by specific maliciously influenced vehicles in the given locations reducing or eliminating network capacity. Five important network components have been assumed to be independently attacked, the effects of the attacks are compared to the baseline scenario. The comparison has been performed based on the change in total travel time and total traffic performance of the whole system.

Since the aim of the attacks is to increase the aggregated travel time of the system undetectably, the most important evaluation parameter is the change in total travel time. On the other hand, the change in traffic performance can be also interesting, however it is only a secondary factor. The reason for this can be well explained by the case of an extremely overloaded direct and short connection. In this case all the traffic between the two connected zones would be assigned due to the cyberattack on a given route. This means that the vehicles would use the shortest available path, so the total traffic performance would be extremely good, however the travel time value would increase significantly. This specific incident could be defined as an efficient intervention.

3 Data

To define the expected following distance reduction factor, it is necessary to derive the recently typical following distance values. Therefore in the first step, the average following distance value has been defined based on the average traffic performance and speed parameters in case of the representative road network (where saturation is equal or larger than 80%), weighted by the traffic performance (Table 1).

Since the introduced value of the capacity improvement factor of autonomous vehicles has been estimated to 40%, it is now possible to verify our assumption by comparing the following distances of the recently applied and the future systems (Table 2).

Since the presented following time values in comparison with the values of the current systems are proved to be realistic and acceptable, the estimated maximum value of achievable capacity improvement factor can be assumed to

be 40%. Accordingly, the limit value of capacity improvement factor related to SAE5 level is 40% in our investigation. In case of 40% capacity improvement, the resulted average value of following distance is 66% of the original value. In case of the so called SAE1 project alternative, the capacity improvement factor is prognosticated to be 1%. The reason for this is the assumed 100% penetration of automated vehicles from the investigated SAE level. Since the assumed 100% penetration of SAE1 level vehicles would already mean an improvement related to the characteristics of current traffic flow.

As mentioned above, the maximum value of supplementary trip components related savings, is estimated to 2 min, representing SAE5 level automation. SAE1 level automation is assumed to have no effect on travel time related to supplementary trip components. In terms of the conservative approach in case of the other scale values instead of a linear, equidistant partition a more moderated polynomial estimation based scaling has been applied (Table 3).

During the analysis, the attack scenarios have been analysed in case of four penetration alternatives, where AV1 represents the present situation, AV50 represents an initial phase of autonomous vehicles' spread, AV95 represents the phase of system saturation related to CAV usage, whilst AV100 is applicable to describe the case of full CAV system penetration (Table 4).

The statistical significance of the applied data is provided by using the data of the official EFM framework. The Traffic Model of Budapest and its data framework is a widely used and permanently maintained decision supporting environment, which has been developed from European funds based on the contract nr. KÖZOP-5.5.0-11-2011-0025. In the framework of the project a representative household survey has been performed, of which methodology is strictly regulated by the guide of EFM framework. The household survey has to be performed in every 4 years, the sample has to contain the data of 10,000 households from the city, 4000 households from the agglomeration. Beside this it has to include a stated preference survey with a sample size of 1000 households. Furthermore traffic counts are organized in hundreds of counting locations in every 6 month to calibrate and update the database.

Table 1 Typical following distance values of EFM model—present state

Representative road categories	Sum of product of traffic performance and following distance (veh/day × m × m)	Sum of traffic performance (veh/day)	Average following distance (m)
BP built-in area—collector road 2 × 1	623,144.5	11,371.0	54.8
BP rural—collector road 2 × 1	3,425,981.8	62,503.5	54.8
BP rural—primary main road (cat I.) 2 × 1	2,034,677.3	48,420.4	42.0
BP built-in area—secondary main road (cat II.) 2 × 1	1,608,666.5	34,854.5	46.2
BP built in area—local residential street 2 × 1	91,800.0	1525.9	60.2
Aggregated	7,784,270.1	158,675.4	49.1

Table 2 Assumed following distance values of EFM model—autonomous vehicles

Representative road categories	Average following distance (m)	Average following time (s)
BP built-in area—collector road 2×1	38.5	2.9
BP rural—collector road 2×1	38.7	2.5
BP rural—primary main road (cat I.) 2×1	30.5	1.7
BP built-in area—secondary main road (cat II.) 2×1	33.1	2.1
BP built in area—local residential street 2×1	42.8	6.4
Aggregated	35.3	2.6

Table 3 Assumed capacity improvement and supplementary trip components time saving related to the spread of autonomous vehicles

SAE categories	Capacity increase (m)	Supplementary trip components time saving (min)
SAE0	0	0
SAE1	0.01	0.1
SAE2	0.04	0.2
SAE3	0.1	0.4
SAE4	0.2	0.9
SAE5	0.4	2

4 Results

Firstly, those attack types are investigated which aim to modify the route planning model. Accordingly, these incidents can influence not only the highly automated vehicles but the partly or fully connected cars as well. Contrarily these kind of malicious interventions are able to affect all components of the transport process, which is supported by any kind of navigation equipment or application. This attack is characterised by a long-term exposure, and a difficult detectability.

4.1 Route choice related attack scenarios

In the first scenario (K1) the route choices of the vehicles are assumed to be influenced by preferring certain routes or infrastructure elements inordinately in comparison with the other network elements. In case of this intervention

the navigation system considers the length of the targeted network elements to be marginal. If this intervention is implemented in moderate way, it will not be easily discoverable neither by the users, nor by the operator. While the small-scale individual losses are not perceptible, the system-scale effect can be significant, especially considering socio-economic disbenefits.

The attack of the second scenario (K2) is developed in the opposite way in comparison with the previously introduced incident type. In this case the length of the selected network elements are increased artificially assumed to be outstandingly long compared to the other infrastructure elements. The targeted route components are considered by the navigation system to be twice as long as in reality.

The targeted components are as follows:

- *Ring Nagyszőlős road—Petőfi Bridge—Nagykörút Boulevard—Margit Boulevard—Budaörsi road*; total length of the route: 15.6 km; total traffic performance of the route: 723,600 vehicle km/day; average traffic on the section 46,000 vehicle/day.
- *Embankment Route of the Pest-side Embankment from the Soroksári Road to the Dráva Street*. Total length of the route: 7.3 km; total traffic performance of the route: 261,900 vehicle km/day; average traffic on the section 35,900 vehicle/day.
- *Artery I The axle of Fehérvári Road—Nagytétényi Road*; total length of the route: 9.9 km; total traffic performance of the route 121,700 vehicle km/day; average traffic on the section 12,300 vehicle/day.

Table 4 CAV penetration in the investigated alternatives

	SAE0	SAE1	SAE2	SAE3	SAE4	SAE5
AV1	0.95	0.04	0.01	0	0	0
AV30	0.7	0.18	0.07	0.03	0.02	0
AV50	0.5	0.19	0.12	0.11	0.06	0.02
AV70	0.35	0.15	0.15	0.15	0.15	0.05
AV95	0.05	0.01	0.04	0.03	0.07	0.8
AV100	0	0	0	0	0	1

- *Artery 2* Route of Hegyalja Road—Kossuth Lajos Stree—Rákóczi Road, total length of the route: 4.7 km, total traffic performance of the route: 204,500 vehicle km/day; average section traffic: 43,300 vehicle/day.
- *Bridge* Petőfi Bridge, total length of the route: 0.6 km; total traffic performance of the route: 52,300 vehicle km/day, average traffic on the section 84,200 vehicle/day.

The following table contains the aggregated parameters describing the effect of the certain attack scenarios and CAV penetration alternatives. It has to be emphasised that the table compares the scenarios to their own baseline scenario belonging to the given CAV penetration (Table 5).

The analysis results of the scenarios and alternatives can be classified basically in three groups. There are cases where the travel time values increase significantly. In this case, the value of traffic performance change is not significant, these attacks can be characterised by success. Those attacks, which moderately increase total travel time and also have negative impact on traffic performance can be described

by moderate efficiency. Those incident alternatives, which result decrease or non-significant increase in total travel time are considered to be inefficient. In case of the parameter values in certain rows it can be contradictory for the first look, that the total change of a given parameter value (total) is not equal to the sum of change on the network of the city centre (BP) and the agglomeration (BPAG). The reason for this can be explained by the journeys originating and terminating in the agglomeration. These flows are not included in the table, which also explains the occasionally differing signs of total change in a given parameter value and the sum of change on the network of the city centre and the agglomeration. On the basis of the results, it can be concluded that K2 attack type is less efficient compared to K1. Beside this, the system is less sensitive to attacks targeting the Bridge and Artery 1.

In case of the third attack-scenario, the sudden reduction of certain network elements' capacity are simulated, for example due to remotely disabled vehicles. The bottlenecks caused by the disabled vehicles are assumed to result in congestions and queues, which expand from the

Table 5 Results of the attacks targeting the navigation system

Project	Change in travel time (vehicle hour)			Change in traffic performance (vehicle kilometre)		
	Total	BPAG	BP	Total	BPAG	BP
AV1_K1_Ring	87	74	54	-547	773	520
AV50_K1_Ring	2021	1930	1092	-3351	681	3031
AV95_K1_Ring	2623	2528	1422	-9516	-8427	-1534
Av100_K1_Ring	2754	2657	1506	-11,940	-10,292	-3041
AV1_K1_Embankment	159	152	97	259	678	802
AV95_K1_Embankment	1176	1146	743	4509	5662	7138
AV1_K1_Artery1	32	34	51	508	559	577
AV95_K1_Artery1	587	600	664	-2997	-2820	-2041
AV1_K1_Artery2	133	121	66	-666	42	177
AV95_K1_Artery2	959	883	482	-284	-781	-1157
AV1_K1_Bridge	22	19	13	-775	-314	-192
AV95_K1_Bridge	76	77	41	-765	-632	386
AV1_K2_Ring	107	101	69	965	1585	806
AV50_K2_Ring	-84	-44	0	17,496	13,573	8585
AV95_K2_Ring	91	86	18	30,646	27,162	14,048
Av100_K2_Ring	1225	1177	733	32,357	30,020	13,660
AV1_K2_Embankment	89	85	55	432	451	36
AV95_K2_Embankment	583	560	345	656	-169	-3342
AV1_K2_Artery1	7	6	2	266	295	127
AV95_K2_Artery1	185	173	69	6945	6812	5417
AV1_K2_Artery2	120	114	81	-350	267	-212
AV95_K2_Artery2	-274	-249	-127	6713	5334	3061
AV1_K2_Bridge	-8	-10	-9	28	140	110
AV95_K2_Bridge	-53	-52	-36	991	668	-73
AV95-20_K1_Ring	1935	1876	1068	-9634	-8548	-1654
AV95-50_K1_Ring	1030	1013	583	-8002	-7208	-1697
AV95-80_K1_Ring	293	291	161	-4581	-4396	-1561

reduced capacity components to neighbouring links and nodes. To describe this effect adequately, the conventional volume-delay function based model has been transformed to a ‘blocking back model’ based approach, which makes it possible to model the effect of the bottlenecks on the traffic of the preceding network elements. This method makes it necessary to consider hourly traffic volumes, which have been derived from the morning peak between 7 and 8. If there are more lanes in one direction on the attacked road, the intervention is modelled through 50% reduction of the capacity value. If the influenced link has two lanes in total, then its capacity has been reduced uniformly to 200 pcu/h.

4.2 Capacity reducing attack scenario

K3 attacks are focused on the most important network components of the system. In case of the higher penetration scenarios, the significant capacity increase makes these infrastructure components more attractive. Therefore, it can be assumed that the effect of the third attack scenario is dominated by the higher penetration alternatives in case of the lowest penetration alternative (AV1). In light of this and in case of a conservative estimation, the low penetration alternative is adequate to be investigated. Accordingly, in general, the third attack scenario is tested considering a conventional transportation system, with 95% penetration of SAE0 only 5% penetration of SAE1 and SA2 vehicles. However, in case of Artery 1, three other alternatives (AV30, AV70, AV100) are evaluated to give a brief presentation about the expected effect of penetration growth.

The targeted components are as follows:

- *Artery 1* Budaörsi Road by the Dayka Gábor Street, in the direction of the city centre. The traffic in the morning peak hour is 6200 pcu/h, (capacity is reduced from 3780 to 1900 pcu/h).
- *Artery 2* Budaörsi Road—Hegyalja Road Overpass in the direction of the city centre. The traffic in the morning peak hour is 1450 pcu/h (capacity is reduced from 780 to 200 pcu/h).
- *Artery 3* Szilágyi Erzsébet Boulevard in the direction of the city centre at Gábor Áron Street. The traffic in the morning peak hour is 1553 pcu/h, (capacity is reduced from 840 to 200 pcu/h).
- *Artery 4* The first section of M3 highway, at Szerencs Street. The traffic in the morning peak hour is 3722 pcu/h, (capacity is reduced from 2520 to 1260 pcu/h).
- *Bridge 1* Kvassay Jenő Road in the direction of the city centre at Hajóállomás Street. The traffic in the morning peak hour is 2310 pcu/h (capacity is reduced from 1440 to 480 pcu/h).

- *Bridge 2* From Petőfi bridge in the direction of Boráros Square. The traffic in the morning peak hour is 1470 pcu/h, (capacity is reduced from 2340 to 200 pcu/h).
- *Bridge 3* From the Erzsébet Bridge to the Szabad sajtó Road. The traffic in the morning peak hour is 3490 pcu/h (capacity is reduced from 2340 to 1170 pcu/h).
- *Embankment* In the north direction along Id. Antal József Embankment in front of the Parliament. The traffic in the morning peak hour is 1327 pcu/h, (capacity is reduced from 1080 to 200 pcu/h).

Based on the results of the model, the efficiency damage caused on network operability does not seem to be critical for the first look. However, even in case of a single attack the average travel time of the affected vehicles can increase by 20–30 min which intervention can have crucial psychological influence on individual road users. On the other hand, even considering an only monthly repeated single attack and assuming conservatively the value of hourly travel time cost to be under 15 EUR, the yearly loss resulted by the incidents can easily exceed the level of 200,000 EUR. In case of simultaneous interventions the multiplicative effect of network level infections can result multiple losses.

It seems to be clear, that from a system operability point of view, considering the-change-in-travel-time indicator, the most vulnerable component of the network is Artery 1 due to the lack of alternative routes. However, it has to be emphasised that its effect is mainly confined to the agglomeration, so the centre can remain still operable, if this component is attacked. Beside this, the system is seriously sensitive on the operability of Artery 3 and Bridge 2 and in case of these components the effect distribution between the agglomeration and the centre is much more balanced. In case of Table 6, it can also be ambiguous, that the change of the output indicator values related to the total network (total) is not equal to the sum of change on the network of the city centre (BP) and the agglomeration (BPAG), however this contradiction can also be explained by the journeys realized within the agglomeration.

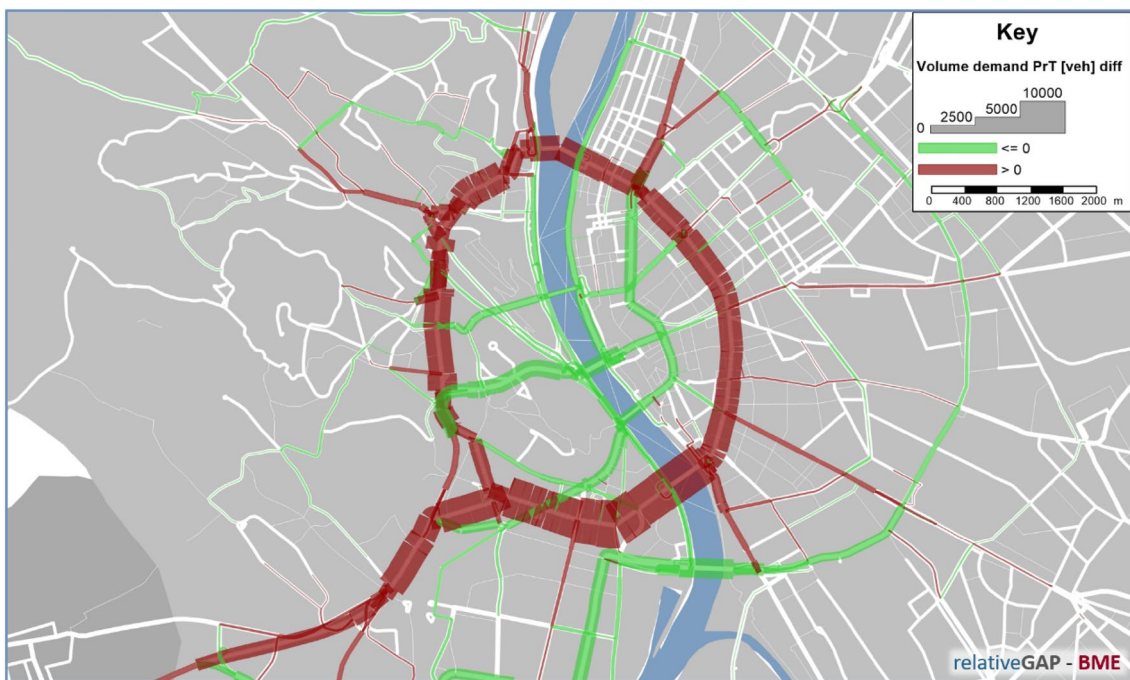
5 Discussion

To summarise the lessons learnt from the evaluation of the different attack types it can be concluded that some of the simulated attacks can rather have relevant effect in case of a long term, undercover operation period, whilst certain investigated attack types can have significant influence on the transport system even in case of a non-continuous attack. On the other hand certain attack types are not proved to have significant effect on total travel time of the investigated transport system.

In case of the attack type K1, the targeted route is overloaded due to the erroneous under estimation of its

Table 6 Results of the attacks targeting the critical network elements

Project	Change in travel time			Change in traffic performance		
	Total (vehicle hour)	BPAG (vehicle hour)	BP (vehicle hour)	Total (vehicle kilometre)	BPAG (vehicle kilometre)	BP (vehicle kilometre)
AV1_Artery1_K3	1137	1127	83	17	17	24
AV1_Artery1_AV30_K3	1243	1226	118	44	42	-15
AV1_Artery1_AV70_K3	1597	1561	91	-37	-44	0
AV1_Artery1_AVI00_K3	1639	1594	-6	17	11	-3
AV1_Artery2_K3	219	224	19	310	325	73
AV1_Artery3_K3	734	727	304	204	234	75
AV1_Artery4_K3	88	92	-130	51	-31	-51
AV1_Bridge1_K3	90	90	214	434	427	234
AV1_Bridge2_K3	980	980	513	149	151	22
AV1_Bridge3_K3	508	507	298	8	6	4
AV1_Embankment_K3	585	580	280	21	-1	-31

**Fig. 1** Change in traffic structure in case of AV95_K1_Ring

resistance-like characteristic parameter of the given network component, for example the length of that network component (Fig. 1).

It can be observed, that the targeted network components are more attractive for the road users, hence the traffic of some other network parts are reduced. Accordingly, the average speed of the ring reduces, whilst the flow of the relieved components is faster. This is presented in Fig. 2.

Based on the presented results, it can be concluded that in case of an adequate preparation process and well selected target objects, the attack type K1 can expectedly significantly increase travel time values of the network, besides a small-scale growth of traffic performance values can also be occurred. Summing up, attack type K1 can be a cunning intervention, since it does not focus on affecting safety critical processes. Therefore it can remain undiscovered for a longer period, causing significant losses for the society.



Fig. 2 Change in speed in case of AV95_K1_Ring

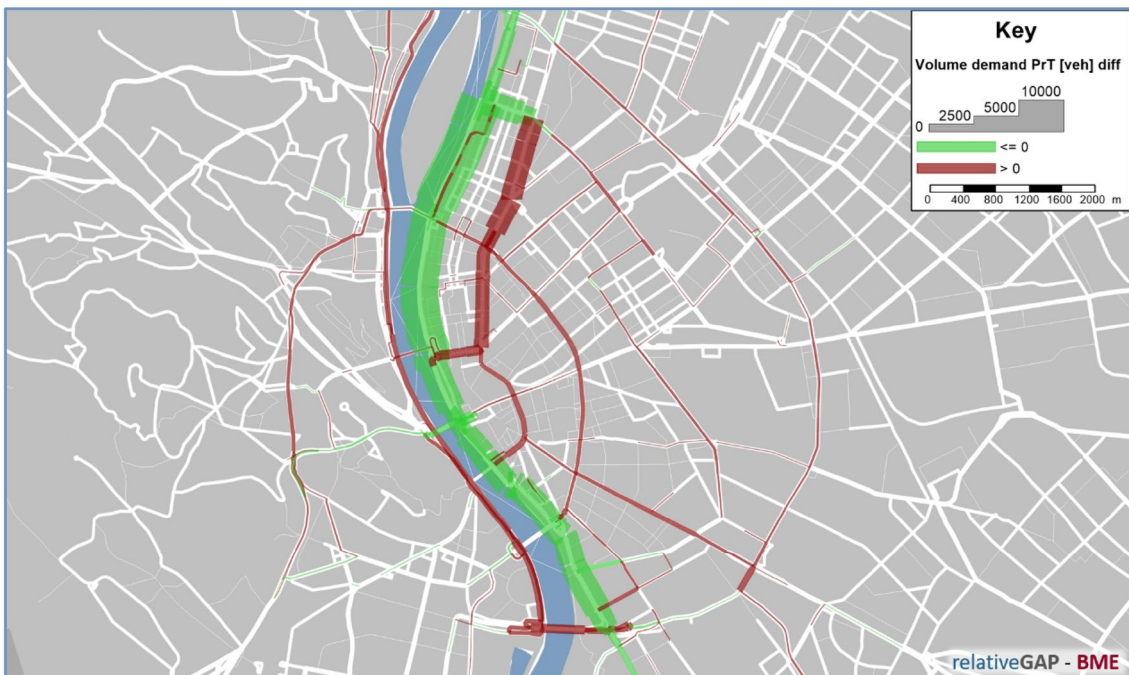


Fig. 3 Change in traffic structure in case of AV95_K2_Embankment

K2 type intervention makes the vehicles avoiding the object components of the attack, since the resistance-like characteristic parameter of the given network element, for example when the length of the route is erroneously over estimated. It can be seen, that the object components of the

attack targeted are less attractive for the road users, hence the traffic of some other network parts are enhanced. At the same time the flow of targeted components becomes relatively faster. This is presented in Fig. 3.

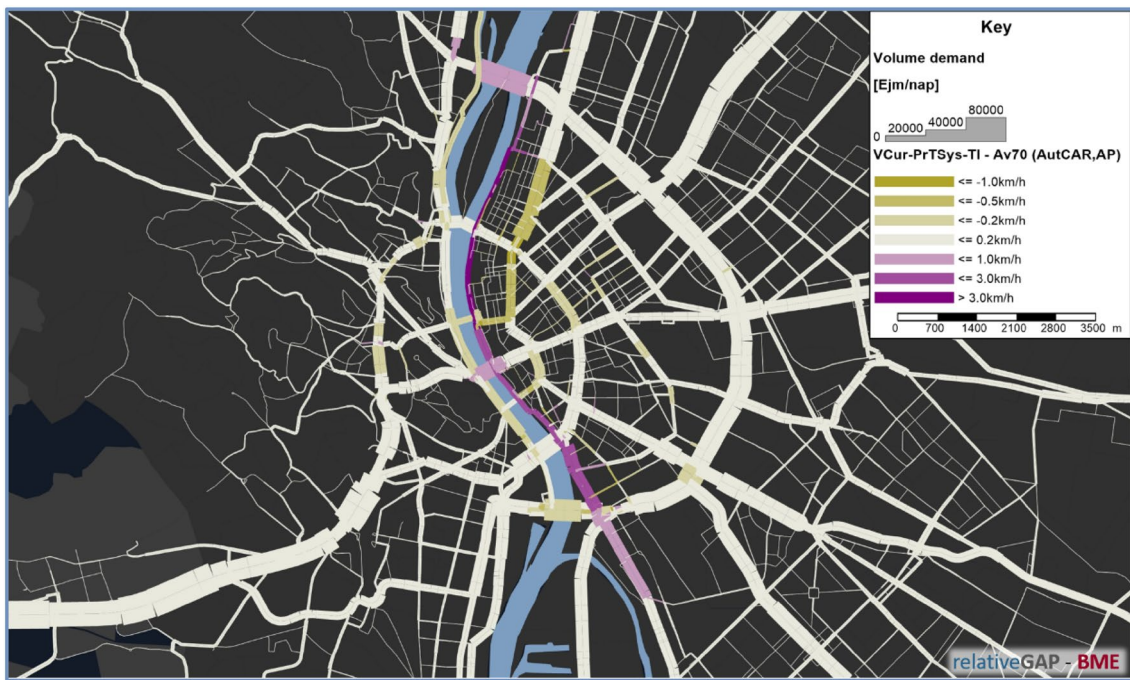


Fig. 4 Change in speed in case of AV95_K2_Embankment

In light of the presented processes and considering the system level evaluation of the network, the positive effect of K2 attack type, namely the speed increase on the targeted core network element is much more significant than the travel time increasing effect of the re-routed traffic (Fig. 4).

Purely from the travel time point of view, the attack type K2 might not be an effective intervention, however it should also be mentioned that in some cases, K2 attacks can strongly influence the total traffic performance (e.g. in case of the alternative targeting Ring component).

In the next part of the paper K3 attack is introduced in details related to the Artery 1 alternative. According to the analysed attack scenario, the capacity of the targeted component is significantly reduced by remotely disabling a car in the given section. In this case, the targeted network component is a main link connecting the city centre and the agglomeration. The investigated network element is already a bottleneck without the assumed intervention, which operates reasonably close to its capacity constraint (Fig. 5).

As it can be observed, a strong congestion is occurred on the Budaörsi Road, where the attack is going to be implemented and on the Balatoni Road and on the related network parts. The malicious intervention is implemented in the indicated location, at the connection of Dayka Gábor Street, where the capacity of the route to the city centre is halved. The restructured traffic flows are presented by the next figure (Fig. 6).

It is clear that the drivers choose alternative routes instead of the infected axle, however the effect of the rerouting

is marginal, the value of the change is between 30 and 50 pcu/h. If the mode of action is analysed in details related to the given intervention, it is possible to get a clearer picture about its impact (Fig. 7).

Congestions on the yellow coloured edges exist also in case of the normal operation scenario, while on the blue coloured links congestions are occurred only in case of the attacked scenario. It can be concluded that the intervention causes kilometre long congestions on the related network parts, especially considering the common section of M1 and M7 highway, the Budaörsi Road and the Rétköz Street. On the other hand congestion disappears from sections located beyond the attacked component. The following figure also contains the changes in traffic flow speed values, which are not significant in case of the previously already congested sections, however in case of the newly congested network components the speed reduction can reach the 80 kmph (Fig. 8).

The travel time of the red coloured route would be close to 4 min in case of an empty network. In the morning peak it takes about 8 min based on the assignment results of the model, while in case of the attack scenario the travel time on the red coloured route increases with an additional 38 min.

From a system operability point of view the effect of K3 attack on travel time is not critical. On the other hand the significant individual losses can reasonably influence social morale, which can be an efficient tool to make the inhabitants of the attacked region disappointed and disconcerted

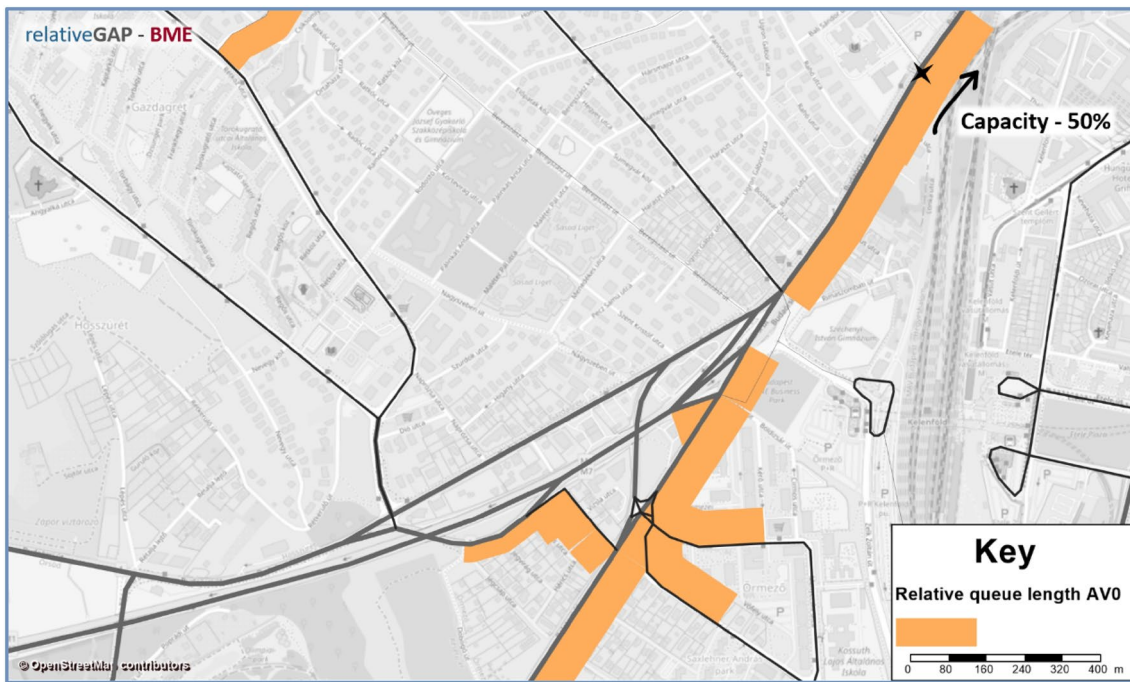


Fig. 5 Congestions on Artery 1

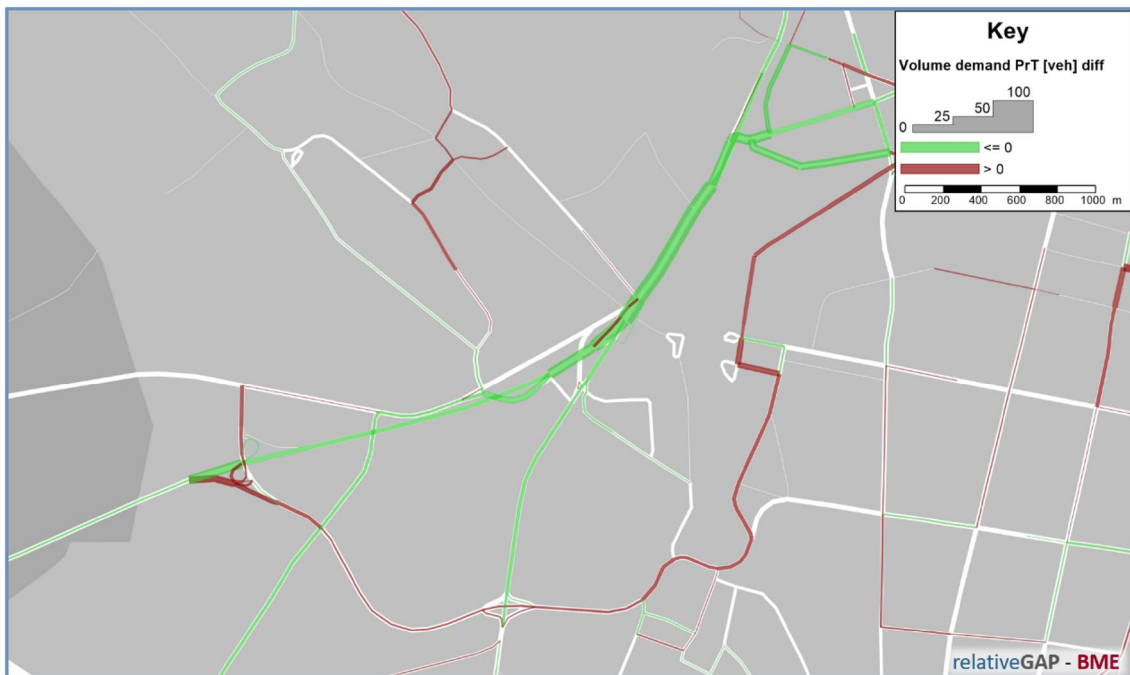


Fig. 6 Congestions on Artery 1

especially considering regularly and repeatedly implemented interventions.

It is an important question of the investigation, whether the results can be extrapolated to other cities or not. To answer this question it seems to be a reasonable way to

analyse if settlement patterns and properties is applicable to explain and classify the different urban traffic structures on a macroscopic level. If so, it can be assumed that in case of cities which can be characterized with similar settlement

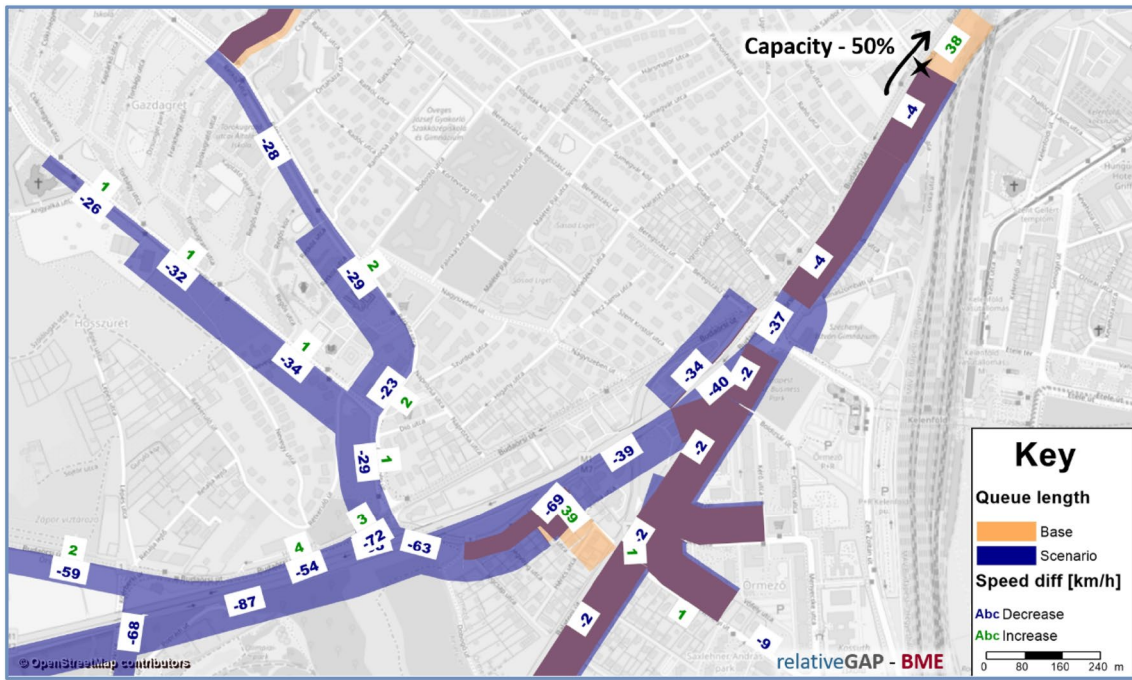


Fig. 7 Mode of action related to the occurrence of the congestions on Artery 1

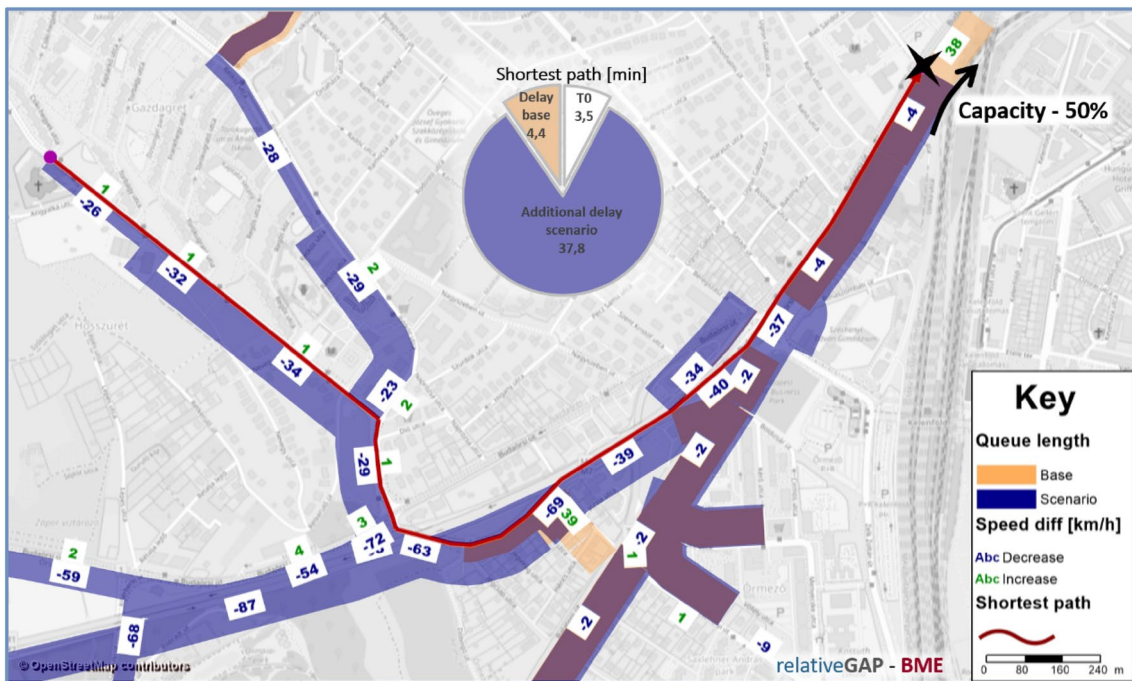


Fig. 8 Change in speed due to the attack targeting Artery 1

properties, malicious interventions implemented by the same method can have similarly serious impacts.

Theodore Tsekeris and Nikolas Geroliminis have introduced a new method to analyse the relationship among city size and network structure by considering traffic congestion

dynamics in large urban areas (Tsekeris and Geroliminis 2013). Their new approach suggest the application of Macroscopic Fundamental Diagram to analyse the relationship between land use and traffic congestion. One of the most important results of the paper has been to support the

deployment of simple control concepts in case of certain city sizes, for a specific network structures and traffic density characteristics. These results have been also supported by other important researches (Saeedmanesh and Geroliminis 2016). Therefore the findings of these papers strongly supports the assumption that cities with similar network structure settlement patterns can be characterized by similar traffic processes.

Alonso et al. (2015) have performed a thorough comparison of transport systems in European cities especially considering sustainability related aspects. During the investigation the classification of the cities has been performed. The outcomes of the paper confirms that the classification of urban transport system leads to groups characterized by different cultural, structural and size patterns. Similar findings have been performed by other researchers as well (Klinger et al. 2013), which strongly support the basic approach of the recent paper. These results are completely in accordance with our assumptions that cities with similar settlement patterns can be characterized by similar transport processes.

Based on the above exposed correspondences, it seems to be reasonable to expect that cyberattacks based on the same methodology, targeting the transportation systems of different, but similar urban regions can have similarly serious impacts.

6 Summary

Innovations related to connected and autonomous transportation are expectedly among the most remarkable and promising development orientations of the future. However it is required to have clear estimations also on the negative effects of the new systems.

Accordingly, the aim of the paper is to investigate the cyberspace related vulnerabilities, threats and their costs in case of the connected and autonomous transport systems. To describe the effects of the analysed attack scenarios, the macroscopic traffic model of Budapest is applied. In case of our evaluation, interventions target the transport network, instead of the individual road users, which assumption can multiply the risk of a given incident.

Since the study prioritises the conservative estimation approaches, only relative capacity increase and the time savings of supplementary trip components are considered as travel time saving factors. In the evaluation section three attack types are investigated. In case of K1 scenario the targeted routes are assumed to be preferred inordinately in comparison with the other network elements. K2 attack makes road users to avoid the targeted route by faking the length of the targeted section in an increasing manner. Attack type K3 assumes a sudden decrease of targeted

network elements capacity, for instance due to remotely disabled vehicles.

In case of an adequate preparation process and well selected target objects, the attack type K1 can expectedly significantly increase travel time values of the network. From the point of view of the travel time, the attack type K2 might not be an effective intervention. Due to the significant individual time losses, K3 attack can reasonably influence social confidence with a moderate risk related to threatening the integrity of safety.

Acknowledgements Open access funding provided by Budapest University of Technology and Economics (BME). The research reported in this paper was supported by the Higher Education Excellence Program of the Ministry of Human Capacities in the frame of Artificial Intelligence research area of Budapest University of Technology and Economics (BME FIKP-MI/FM).

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

- Alonso A, Monzón A, Cascajo R (2015) Comparative analysis of passenger transport sustainability in European cities. *Ecol Ind* 48:578–592
- Alsumayt A, Haggerty J, Lotfi A (2017) Using trust to detect denial of service attacks in the internet of things over MANETs. *Int J Space Based Situated Comput* 7(1):43–56
- Benenson I, Martens K, Birfir S (2008) PARKAGENT: an agent-based model of parking in the city. *Comput Environ Urban Syst* 32(6):431–439
- Darwish A, Hassanién AE (2018) Cyber physical systems design, methodology, and integration: the current status and future outlook. *J Ambient Intell Humaniz Comput* 9(5):1541–1556
- Farhan J, Chen TD (2018) Impact of ridesharing on operational efficiency of shared autonomous electric vehicle fleet. *Transp Res Part C Emerg Technol* 93:310–321
- Fox-Penner P, Gorman W, Hatch J (2018) Long-term transportation electricity use considering the effect of autonomous-vehicles: estimates and policy observations. *Energy Policy* 122:203–213
- Haboucha CJ, Ishaq R, Shiftan Y (2017) User preferences regarding autonomous vehicles. *Transp Res Part C Emerg Technol* 78:37–49
- Hamida EB, Javed M, Znaidi W (2017) Adaptive security provisioning for vehicular safety applications. *Int J Space Based Situated Comput* 7:16
- Howard D, Dai D (2014) Public perceptions of self-driving cars: the case of Berkeley, California. In: *Transportation Research Board 93rd annual meeting*, vol 14, no 4502
- Iacobucci R, McLellan B, Tezuka T (2018) Modeling shared autonomous electric vehicles: potential for transport and power grid integration. *Energy* 158:148–163
- Klinger T, Kenworthy JR, Lanzendorf M (2013) Dimensions of urban mobility cultures—a comparison of German cities. *J Transp Geogr* 31:18–29

- 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
- Kröger L, Kuhnimhof T, Trommer S (2018) Does context matter? A comparative study modelling autonomous vehicle impact on travel behaviour for Germany and the USA. *Transp Res Part A Policy Pract.* <https://doi.org/10.1016/j.tra.2018.03.033>
- Saeedmanesh M, Geroliminis N (2016) Clustering of heterogeneous networks with directional flows based on “Snake” similarities. *Transp Res Part B Methodol* 91:250–269
- Shoup DC (2006) Cruising for parking. *Transp Policy* 13(6):479–486
- Szalay Z, Tettamanti T, Esztergár-Kiss D, Varga I, Bartolini C (2018) Development of a test track for driverless cars: vehicle design, track configuration, and liability considerations. *Period Polytech Transp Eng* 46(1):29–35
- Tsekeris T, Geroliminis N (2013) City size, network structure and traffic congestion. *J Urban Econ* 76:1–14
- Ye L, Yamamoto T (2018) Modeling connected and autonomous vehicles in heterogeneous traffic flow. *Phys A* 490:269–277
- Zöldy M (2018) Investigation of autonomous vehicles fit into traditional type approval process. In: *Proceedings of ICTTE 2018 Belgrade*, pp 428–432

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