One Bus is All it Takes: The Impact of Cyber Attacks in Customised Bus Services

Rongge Guo[1], Alexandros Nikitas[2], Simon Parkinson[1] and Mauro Vallati[1]

***Abstract*— Connected and Autonomous Vehicle (CAV) technologies have the potential to revolutionise public transport systems, making them more financially and environmentally sustainable, accessible, and user-centric. However, CAV-based bus services are vulnerable to cyber attacks manifesting in unwanted, deceitful behaviour. This includes behaviours such as suppression, overloading, and substitution, which could be used by malicious actors to disrupt service and cause significant damage to both the transport operator and passengers.**

This paper raises awareness about the potential impact of deceitful behaviour on transport systems by instantiating the ideas in a customised bus system example. More specifically, this work evaluates the impact of a deceitful vehicle in Customised Bus (CB) services, when considering (i) different customer demand profiles, (ii) at what point in planning and control the attack occurs, and (iii) whether the controller has detected the attack. Our empirical analysis shows how an attack aimed at compromising a single vehicle can lead to a surge in operating costs of up to 48%. Further, there is an increase in cost, distance travelled, and unserved passengers when the attack goes undetected. The results underscore the importance of preventing and detecting cyber attacks in the deployment of CAV-based solutions and emphasise the need for a proactive approach in managing the associated risks.

I. Introduction

The bus is the universally recognised backbone of every public transport system for all locality scales and urban contexts due to its low vehicular and infrastructure investment and operational costs [1]. It is arguably a flexible, easily implementable and space-efficient value-for-money mode. Traditional bus services have not been capable nevertheless to create a sufficient modal shift momentum moving commuters away from the automobile in the complex and dynamic urban landscapes of the 21st century, with very few exceptions [2]. However, Connected and Autonomous Vehicle (CAV) technologies offering demand-responsive, door-to-door travel could change that by making buses more modern, attractive, visible and user-centric [3] and capable of offering accessibility, traffic reduction, environmental, air quality and energy consumption benefits [4]. CAVs supported the design and implementation of Customised Bus (CB) systems, that do not rely on fixed routes but adapt the path to the demand and requirements of passengers [5]. At the same time though this transition to CAVs, and CAV-based buses in particular, may also create a new layer of unprecedented risks that revolve around cybersecurity issues [6], [7], since the powerful notion of connectivity opens the door to increased opportunities for an adversary to implement a successful attack [8], [9]. More specifically, CAVs manipulated by users, traffic controllers or third parties may exhibit deceitful behaviours for the 'selfish' or malicious purposes of the hacker including: suppression/camouflage, overloading, mistake, substitution, target conditioning, repackaging capability signatures, amplification and reinforcing impression [10]. Thus, attacks like starvation, denial-of-service, session hijacking, man-in-the-middle, poisoning, masquerading, flooding and spoofing may become a genuine threat to the resilience of a CAV-centric mobility eco-system [10] and a single bus could be the source of problems spanning for travel delays, street congestion and traffic bottlenecks to life-threatening cyber-terrorism events. There is a need thus, for identifying and developing pro-actively mitigation strategies to protect CAVs against these dangers especially when this technology is applied to vehicles open to the general public that are used to move many people at once like buses.

Previous work has demonstrated that successfully disabling 1 in 10 vehicles through a cyber attack would be enough to bring Manhattan to a standstill [11]. This work focused on understanding how the impact of vehicle movement through the city would be affected by a successful cyber attack. The work assumes the vehicles are individually compromised, which would represent a large-scale attack, something that is more difficult to happen. It is perhaps a lot more likely that cyber attacks will affect smaller numbers of vehicles to achieve specific outcomes. In this work, we refer to these specific outcomes as types of *deceitful behaviours*, and unlike the simulation on Manhattan, we are focused on understanding the quantifiable impacts on CB systems.

In this work we show how the ideas from [10] can be instantiated to define a class of attacks in an applied bus-based example. We specifically focus on customised bus systems, and we show, through a simulation exercise, how an apparently limited attack - aiming at rerouting a single vehicle - can lead to significant disruptions for the transport operator and for the passengers. Despite the involvement of a single vehicle our experimental analysis, based on historical data, shows that a smart attacker can cause a surge in operating costs of up to 48% for the service provider.

The remainder of this paper is organised as follows. First, we provide the necessary background on CB systems. Then, we discuss in detail the considered attack and its dimensions.

[1]Rongge Guo, Simon Parkinson and Mauro Vallati are with the School of Computing and Engineering, University of Huddersfield, Huddersfield, United Kingdom. Rongge Guo and Mauro Vallati were supported by a UKRI Future Leaders Fellowship [grant number MR/T041196/1]. n.surname@hud.ac.uk

[2]Alexandros Nikitas is with the Huddersfield Business School, University of Huddersfield, Huddersfield, United Kingdom. a.nikitas@hud.ac.uk

In Section IV we provide the empirical assessment of the impact of a deceitful CAV on a fully-operational CB system, and in the next section we discuss the implications of the results. Finally, we give a conclusion and present potential areas for future work.

II. Background on Customised Bus Systems

The CB system is an innovative on-demand public transit (PT) service, that has the potential to alleviate traffic congestion and improve the mobility, accessibility and reliability of PT [12]. Unlike fixed-route PT systems, CB systems aim to provide "door-to-door" and demand-oriented services to passengers with similar travel requirements in terms of time and space, which has been identified as a promising alternative to conventional buses and private cars [13].

Existing CB systems enable passengers to reserve CB services in advance via an online platform. This allows the system to discover and explore passenger travel patterns before operation. The aggregated travel requests, that consider temporal and spatial restrictions of reserved demands, are then used for the CB network design (i.e., determining passenger-to-vehicle assignment, vehicle routes and scheduling plans) [14]. However, this approach is rigid in that the determined travel plans cannot be changed during operation.

To enable a highly flexible and efficient on-demand CB service, the advanced CB system incorporates real-time travel demands into the operation planning process, i.e., the on-demand CB service can address incoming passengers who submit travel requests during operation. Most previous studies have tackled this issue with dynamic routing and scheduling, such as one key work where multi-objective optimisation has been used for real-time CB routing [15]. However, traditional human-driven vehicles constrained by driver behaviours and crew schedules are not able to perform effective vehicle dispatching and re-allocation in real-time. The emerging CAV technologies offer the opportunity to handle the mentioned hindrance. CAVs provide the possibility for real-time communication between the central system, vehicles and incoming requests while improving the safety of driving and alleviating driver schedule constraints, which helps to enhance passengers' travel experience and system performance by automatically dispatching the nearby vehicles to respond [16], [17].

Figure 1 presents the example of the real-time CB operation with CAVs: when the real-time demands (from O_2 and D_2) appears at timestamp t, the running CAV planned at start time t_0 for reserved demands (from O_1 and D_1) is re-optimised for service. In the figure, we also emphasise the roles of the involved technologies, i.e. connectivity and autonomous driving.

III. Attack: Dimensions and Classification

The *deceitful* CAV has been defined in previous work as one that is deliberately trying to deceive the smart traffic network based on an ulterior motive [10]. The term deceitful covers a range of eight tactical behavioural types,

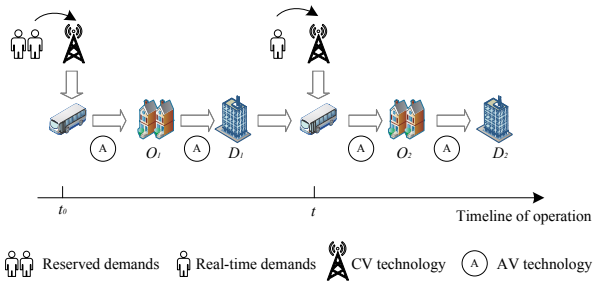

Fig. 1. Example of real-time CB operation applied CAVs

that have been defined based on an understanding of deceitful behaviours in military environments. These range from *overloading* where the controller is overwhelmed with communication to corrupt and confuse to *reinforcing the impression* where the controller is made to believe that one or more vehicles are taking one course of action, when in fact a different one is taken. The interested reader is referred to [10] for additional details. Vehicle behaviour can be thought of as an effect of a successful attack. How this attack is launched is not the focus of this paper; however, the full extent of the possibilities can be seen in survey publications [8].

In this work, we are particularly interested in the deceitful behaviour of *Reinforcing the impression*, and we ground this type of behaviour in the CB eco-system, where the CB operator is misled to believe vehicles are taking a planned route when in fact they are not. We assume the attacker is targeting a single vehicle, to minimise the possibility of early discovery and to reduce the cost of the attack itself.

Following the discussion presented in [10], the impact of deceitful behaviour can be examined in terms of the following five dimensions:

- **Time Frame**: This is the duration of the attack and is used to differentiate attacks to understand whether they occur in a short duration or over a longer period of time. This can help plan appropriate detection and response mechanisms. For the attack considered in this work, the time frame is short-term. This would typically be quantifiable in tens of minutes and would at maximum last for the duration of the bus service.
- **Engagement**: Instigating deceptive activity requires active engagement from an adversary or a group in collaboration. This scale of engagement is intrinsically linked to the sophistication of the attack. In this work, an adversary is required to actively attack a specific vehicle to prevent it from following the instructions provided by the CB system. Furthermore, in the more advanced case in which the vehicle is camouflaging its behaviour, the agent must continuously act to deceive the control system.
- **Infrastructure**: This dimension is used to measure and report the extent of how much of the control

infrastructure is attacked to successfully achieve the desired deception. In this work, the attacks involve the autonomous vehicle that is targeted and the communication channel that is used by the CB operator to send instructions to the vehicles and to receive information on their position and conditions.

- **Scale**: This dimension reports the size of the area being attacked, which could range from a small-scale impact on a single vehicle or infrastructure component to those with a wide-ranging scale such as affecting a metropolitan area. The attack presented in this work is targeting a single vehicle; however, the scale is the whole CB system that is operated by the automated controller.
- **Impact**: This dimension is used to capture the overall impact of deceitful behaviour. The overall impact is quantified, in monetary terms, in our experimental analysis. From a general perspective, the implications can be significant and include a reduction in the ability of the CB system in serving passengers, potentially leading to the disaffection of users and loss of trust in the service.

Having characterised the attack that we aim at assessing in this work, we can now turn our attention to the experimental analysis, where the attack is simulated.

IV. Deceitful CAVs in CB Systems: Empirical Evaluation

This section aims at demonstrating the detrimental impact of the *Reinforcing the impression* deceitful CAVs behaviour on an operating CB System. To do so, we apply the methodology proposed in [5] to perform large-scale experiments through two operation scenarios based on historical data.

A. Experiment design

This study applies the methodology proposed in [5], and eliminates the influences of electric technology. To be specific, we consider CAVs in CB systems with two vehicle states, namely idle and en-route. The idle state corresponds to the vehicle positioned at the depot for allocation, while the en-route state represents the CAV on the road for picking up or dropping off passengers. To deal with heterogeneous passengers, we employ the two-phase optimisation model introduced in [5] for the CB service design: the first (static) phase optimises the vehicle routes, schedules, and passenger-to-vehicle assignment based on reserved demands; the second (dynamic) phase re-optimises existing services according to real-time requests. The overall goal of the proposed approach is to minimise the operation costs while serving all the passengers.

In order to mimic the behaviour of an attacker aiming at disrupting the service, and in line with the dimensions discussed in the previous section, we consider that vehicles en route can be targeted and forced to follow fake operation instructions (ignoring the planned routes and travel to a distant station with no passengers). The goal of the attacker is to identify a single vehicle to target so that the operation cost increase is maximum for the CB service operator. We are also assuming that the attacker focuses on vehicles without in-vehicle passengers, to avoid more serious charges; however, the attack may cause a penalty for CB systems, as the passengers who have been assigned to attacked vehicles are not served.

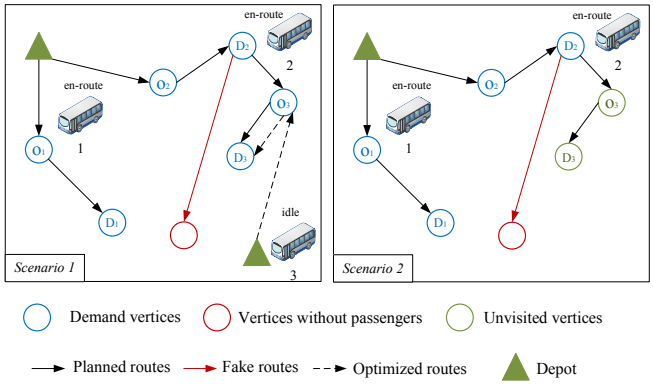

Fig. 2. Example of Scenario 1 and Scenario 2.

The experimental analysis is conducted on an urban road network in Beijing, where the historical smartcard data from 24th to 28th April 2017 are collected to aggregate the spatial-temporal travel demands into different groups. Specifically, the morning commuting trips, consisting of 36 demand vertices, are extracted to generate three instances (R, C and RC), representing random, cluster and mixed passenger distributions. Each instance is associated with 300 passengers, including 20 groups of reserved demands and six groups of real-time requests. A detailed description can be found in [5]. We assume a homogeneous fleet of 40-people CAV buses, each of which departs from and drives to depots after service. Additional parameters are: the departure cost per vehicle is ¥500, the travel cost is 15¥/km and the penalty per unserved passenger is ¥100.

To better contextualise the impact of deceptive behaviours, we consider two different scenarios, as given in Figure 2. In the first scenario, we consider the case where the CB service provider can detect the incorrect behaviour of en-route vehicle 2 and can try to counteract it. For this scenario, we extend the approach proposed in [5] to dispatch an additional idle vehicle 3, if available, to deal with the passengers ($O_3 \rightarrow D_3$) left unserved by the attack. In the second scenario, we instead consider the case where the CB service provider is fully deceived and cannot identify the misbehaviour of one of the dispatched vehicles, that is vehicle 2, and then cause the unserved passengers ($O_3 \rightarrow D_3$). Four important performance indicators are considered under each scenario: operating costs, vehicle distance traveled, number of vehicles in operation, and number of unserved passengers.

B. Scenario 1: Rerouting and re-dispatching

This scenario assumes that the central system can detect the fact that one vehicle is not behaving as expected, and can assign another CAV to take over the delivery task. To be specific, when a CAV deviates from its planned route, the

TABLE I

IMPACT OF DECEITFUL CAVS ON R, C, AND RC INSTANCES UNDER SCENARIO 1.

	Cost/¥		Distance/km		Vehicle/veh		Unserved	
		Diff.		Diff.		Diff.		Diff.
R	10281.2		385.4		9		0	
R1-P1	13621.8	32.5%	441.5	14.5%	10	1	20	20
R1-P2	12841.5	24.9%	456.1	18.3%	10	1	10	10
	Cost/¥		Distance/km		Vehicle/veh		Unserved	
		Diff.		Diff.		Diff.		Diff.
C	10048.1		369.9		9		0	
C1-P1	12929.3	28.7%	442.0	19.5%	10	1	13	13
C1-P2	12016.8	19.6%	394.5	6.6%	10	1	11	11
	Cost/¥		Distance/km		Vehicle/veh		Unserved	
		Diff.		Diff.		Diff.		Diff.
RC	10279.2		385.3		9		0	
RC1-P1	13737.2	33.6%	442.5	14.8%	10	1	21	21
RC1-P2	13020.5	26.7%	434.7	12.8%	10	1	15	15

Cost indicates the operation cost; Distance is the total travelled distance; Vehicle is the number of running AVs; Unserved is the number of unserved passengers.

TABLE II

IMPACT OF DECEITFUL CAVS ON R, C, AND RC INSTANCES UNDER SCENARIO 2.

	Cost/¥		Distance/km		Vehicle/veh		Unserved	
		Diff.		Diff.		Diff.		Diff.
R	10281.2		385.4		9		0	
R2-P1	15294.0	48.8%	452.9	17.5%	9	0	40	40
R2-P2	14054.3	36.7%	437.0	13.4%	9	0	30	30
	Cost/¥		Distance/km		Vehicle/veh		Unserved	
		Diff.		Diff.		Diff.		Diff.
C	10048.1		369.9		9		0	
C2-P1	14599.1	45.3%	426.6	15.3%	9	0	37	37
C2-P2	13653.9	35.9%	376.9	1.9%	9	0	35	35
	Cost/¥		Distance/km		Vehicle/veh		Unserved	
		Diff.		Diff.		Diff.		Diff.
RC	10279.2		385.3		9		0	
RC2-P1	14774.3	43.7%	425.0	10.3%	9	0	39	39
RC2-P2	14257.6	38.7%	417.2	8.3%	9	0	35	35

Cost indicates the operation cost; Distance is the total travelled distance; Vehicle is the number of running AVs; Unserved is the number of unserved passengers.

central system is triggered to counteract the attack by dispatching an idle CAV from the nearest depot to minimize the impact of unserved passengers. Based on these assumptions, we consider two cases for each instance: that is, the attack appears involving vehicles whose route has been optimised in the first phase (i.e., instances R1-P1, C1-P1 and RC1-P1), or in the second phase (i.e., instances R1-P2, C1-P2 and RC1-P2).

Table I shows an overview of the plans and the relative differences with regard to the operation of non-attack scenarios (i.e., instances R, C and RC). It is worth noting that even an attack on a single bus can have a significant impact on operating costs. The average rise in costs is 28.7%, 24.2% and 30.2% over the three instances. Regarding the travelled distance of CAVs, this rises by 14.4% on average due to the rerouted and newly dispatched vehicles. In terms of the unserved passengers, attacking scenarios in the first phase generate higher values than that in the second phase over three instances. The reason is as follows: the first operational phase involves static planning that relies on known demands, that tend to be large, whereas the second phase is characterised by reactive planning for dynamic demands, which is generally limited. The limited number of passengers to be served in the second phase means that it is easier to address the unserved ones, enabling services to fulfil spatial and temporal travel requests.

C. Scenario 2: Rerouting and Camouflaging

This section focuses on the performance of the CB system when the attacked vehicle can not be identified during the operations, but only after the end of the service when passengers submit complaints for the lack of service. In other words, the attacked vehicle can camouflage its behaviour so that it is not recognisable, leading to the impossibility of reacting for the CB service provider.

Table II reports the operational indicators and the differences compared to non-attack instances for this scenario. We observe that the attack of a single CAV that cannot be recognised dramatically reduces operational efficiency for the CB service. Regarding operating costs, the average increases are approximately 42.8%, 40.6% and 41.2% for R, C and RC, respectively. Despite the absence of the newly dispatched vehicles to counter the attack, as in scenario 1, there is an average increase of 15.5%, 8.6%, and 9.3% in the travelled distance – due to the movement of the attacked vehicle to a remote station for no reason. The attack also significantly increases the number of unserved passengers, which reaches 40 in the case of R2-P1. The findings indicate that the camouflage poses a serious threat to CB service providers, as the dramatic increase in operating costs and a large number of unserved passengers can lead to financial losses for the provider. Despite the fact that a single vehicle is attacked, it is worth noting that in the long term, a number of these attacks can result in passengers opting for a different service or a different provider, with disastrous consequences for the provider.

D. Scenario 1 vs. Scenario 2

This section further compares the detrimental impact of the attacks for the two considered scenarios. Figure 3 and Figure 4 present the operating costs of instances when the attack occurs during two different phases, respectively.

As a first remark, it is easy to notice that the first phase, where operations are optimised for serving reserved demands, is the one more susceptible to attacks. This phase tends to be highly optimised and deals with the largest number of passengers, hence disruptions can have a significant overall impact in terms of operating costs. The second phase is less costly, but can still lead to pronounced increases.

Summarising, even under the best circumstances, i.e. when the attack can be identified and mitigation strategies can be put in place, a *Reinforcing the impression* attack made on a

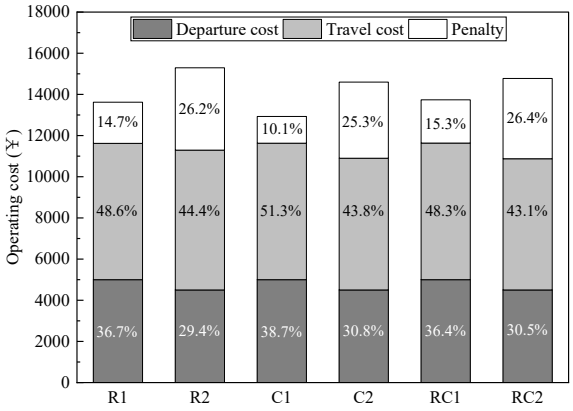

Fig. 3. Comparison of Scenario 1 and Scenario 2 when the attack occurs in the first phase P1

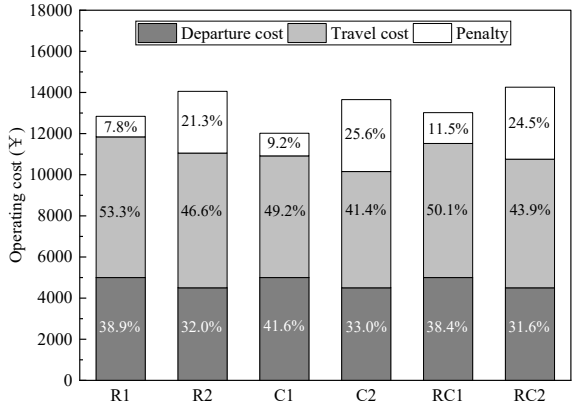

Fig. 4. Comparison of Scenario 1 and Scenario 2 when the attack occurs in the second phase P2

smartly selected CAV can have a remarkably high impact on the operations of a CB service.

V. Discussion

Given the potential impact of a single deceitful vehicle on the whole CB system, and that the impacts are greater when the attack goes undetected, it is imperative to design and invest in strategies to mitigate or eliminate disruption. Prevention and early detection of these congestion-inducing incidents, described herein, can on the one hand have significant socio-economic benefits for built environments and cities and on the other hand make smoother the transition to a genuinely bus-centric transport eco-system that would dethrone the still very resilient, even during Covid, automobile. For instance, traffic on London's roads alone, cost to the United Kingdom's capital city economy approximately £5.1 Billion a year, or £1,211 per driver[1]. These are phenomenal loses that could have been significantly marginalised by a system that revolves efficiently around difficult-to-deceive CAV-based CB systems. These savings could have increased investments designed to enhance the wellbeing of our societies in general and out transport systems in particular. Furthermore, with strong cybersecurity-enhancing schemes in place to protect and defend CBs, these services and PT in general, would be more effectively branded by operators and accepted by people as a safe, secure and resilient form of transport.

More specifically, mitigating the impact of deceitful CAVs in CB systems requires a multi-faceted, cross-disciplinary and inter-organisational approach that introduces a balanced portfolio of technical and non-technical measures. Technical measures primarily refer to engineering, infrastructure and computer science solutions, while non-technical measures are those with an educational, information-provision, policy, legislation and enforcement nature.

A first techno-centric approach can leverage techniques to detect patterns of deceitful behaviour in real-time. As simulated in the second scenario, it can be possible to closely monitor the movements of each vehicle to ensure that the instructions provided by the service operator are correctly followed by the vehicles. It could also be possible to identify unusual manoeuvres of a vehicle or unexpected communication patterns, that can flag the possibility that the CAV is under attack. Early identification makes it possible to react to an attack and minimise its overall impact.

Another mitigation strategy can focus on building redundancy and diversity into both CAVs and the CB system, for instance following the security by design paradigm [18]. This may involve using multiple communication channels, control centres, or redundant modules in the CAV itself. This strategy aims at making it more complicated for an attacker to compromise a vehicle or a component of the infrastructure. Also, multiple vehicles can be in an idle state and available to substitute compromised vehicles to minimise the negative impact on passengers. Cybersecurity technology advancements including machine learning and AI-based prevention mechanisms, anti-spoofing technologies, message encryption and novel heuristic decision and/or voting algorithms are all critical and dynamically developing tools in the toolbox of future transport operators.

Non-technical measures are human-centred mechanisms that enable people to protect their systems against these deceitful behaviours. Some of these measures can focus on educating and training system operators and passengers on how to recognise and report suspicious activities. Well-educated passengers and users, aware of cybersecurity threats and their likely detrimental aftermath that have the know-how to flag these up quickly and effectively, can play a crucial role in supporting operators and authorities in monitoring (or even in some cases preventing altogether) the possibly abnormal or deceitful behaviour of CAVs. Inter-institutional collaboration and information sharing between the different players of this future driverless mobility eco-system can help address the problem of deceitful CAVs. Sharing information, especially in real-time, about threats and vulnerabilities and working together to develop solutions tailored to the customised bus system can help mitigate the impact of

[1]https://www.london.gov.uk/press-releases/mayoral/cost-of-congestion-in-capital-revealed

deceitful CAVs. Finally, strict regulatory frameworks and anti-deception laws that penalise such attacks harshly with huge fines, full operator and passenger reimbursements and even imprisonment could reduce the appetite of hackers to damage PT systems.

VI. Conclusion

This paper raises awareness about the potential impact of deceitful CAV behaviours on transport systems by testing a likely single vehicle attack in a CB system. The experimental analysis, uses historical data from Beijing to consider different passenger distributions and scenarios, simulating the cases where the CB service provider can or cannot detect the attack performed by compromising one CAV bus.

The findings show that the deceptive behaviour of a single CAV can lead to a significant increase in operating costs and unserved passengers, posing a serious threat to CB service providers. In the long term, repeated attacks can result in passengers choosing different services or providers, leading to disastrous consequences for the CB system's economic performance and viability. These results are particularly concerning if the whole public transport system is considered: the negative impact of deceitful attacks on PT can extend beyond a single affected provider. As more systems are affected, passengers may start to lose trust in PT systems as a whole, leading to a decrease in ridership and an increase in car usage, which can worsen traffic congestion and air pollution in urban areas. Furthermore, such successful cyber-attacks compromising transport eco-systems and therefore jeopardising the very backbone of our urban fabric could potentially highlight the likely vulnerability of CAV technologies as a whole and create reluctance in their acceptance and full-scale adoption even for non-transport applications.

This paper is a call for action to the research community: it is crucial that future research explores solutions to mitigate the impact of deceitful CAV behaviours to avoid potentially devastating effects on urban mobility and, to a large extent, to air quality, greenhouse gas emission production and environmental degradation.

References

[1] A. Nikitas and M. Karlsson, "A worldwide state-of-the-art analysis for bus rapid transit: Looking for the success formula," *Journal of Public Transportation*, vol. 18, no. 1, pp. 1–33, 2015.

[2] C. Karolemeas, S. Tsigdinos, E. Bakogiannis, and A. Nikitas, "Evaluating the suitability of urban road networks to facilitate autonomous buses," *Transportation Research Procedia*, vol. 62, pp. 599–606, 2022.

[3] S. Tsigdinos, C. Karolemeas, E. Bakogiannis, and A. Nikitas, "Introducing autonomous buses into street functional classification systems: An exploratory spatial approach," *Case Studies on Transport Policy*, vol. 9, no. 2, pp. 813–822, 2021.

[4] A. Nikitas, A.-E. Vitel, and C. Cotet, "Autonomous vehicles and employment: An urban futures revolution or catastrophe?" *Cities*, vol. 114, p. 103203, 2021.

[5] R. Guo, W. Guan, S. Bhatnagar, and M. Vallati, "A two-phase optimization model for autonomous electric customized bus service design," in *2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC)*. IEEE, 2022, pp. 383–388.

[6] M. Pham and K. Xiong, "A survey on security attacks and defense techniques for connected and autonomous vehicles," *Computers & Security*, vol. 109, p. 102269, 2021.

[7] N. Liu, A. Nikitas, and S. Parkinson, "Exploring expert perceptions about the cyber security and privacy of connected and autonomous vehicles: A thematic analysis approach," *Transportation research part F: traffic psychology and behaviour*, vol. 75, pp. 66–86, 2020.

[8] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE transactions on intelligent transportation systems*, vol. 18, no. 11, pp. 2898–2915, 2017.

[9] A. Sui and G. Muehl, "Security for autonomous vehicle networks," in *2020 IEEE 3rd International Conference on Electronic Information and Communication Technology (ICEICT)*, 2020, pp. 67–69.

[10] A. Nikitas, S. Parkinson, and M. Vallati, "The deceitful connected and autonomous vehicle: Defining the concept, contextualising its dimensions and proposing mitigation policies," *Transport Policy*, vol. 122, pp. 1–10, 2022.

[11] S. Vivek, D. Yanni, P. J. Yunker, and J. L. Silverberg, "Cyberphysical risks of hacked internet-connected vehicles," *Physical Review E*, vol. 100, no. 1, p. 012316, 2019.

[12] T. Liu and A. A. Ceder, "Analysis of a new public-transport-service concept: Customized bus in china," *Transport Policy*, vol. 39, pp. 63–76, 2015.

[13] D. Huang, Y. Gu, S. Wang, Z. Liu, and W. Zhang, "A two-phase optimization model for the demand-responsive customized bus network design," *Transportation Research Part C: Emerging Technologies*, vol. 111, pp. 1–21, 2020.

[14] W. Shu and Y. Li, "A novel demand-responsive customized bus based on improved ant colony optimization and clustering algorithms," *IEEE Transactions on Intelligent Transportation Systems*, 2022.

[15] C. Wang, C. Ma, and X. D. Xu, "Multi-objective optimization of real-time customized bus routes based on two-stage method," *Physica A: Statistical Mechanics and its Applications*, vol. 537, p. 122774, 2020.

[16] H. Miao, H. Jia, J. Li, and T. Z. Qiu, "Autonomous connected electric vehicle (acev)-based car-sharing system modeling and optimal planning: A unified two-stage multi-objective optimization methodology," *Energy*, vol. 169, pp. 797–818, 2019.

[17] C. Tang, J. Liu, A. Ceder, and Y. Jiang, "Optimisation of a new hybrid transit service with modular autonomous vehicles," *Transportmetrica A: Transport Science*, pp. 1–23, 2023.

[18] A. Chattopadhyay, K.-Y. Lam, and Y. Tavva, "Autonomous vehicle: Security by design," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 11, pp. 7015–7029, 2021.