# Safety, Stability and Environmental Impact of FDI Attacks on Vehicular Platoons

**Taylor, S. J., Ahmad, F., Nguyen, H. N., Shaikh, S. & Evend, D.**



**Original citation & hyperlink:**
Taylor, SJ, Ahmad, F, Nguyen, HN, Shaikh, S & Evend, D 2022, Safety, Stability and Environmental Impact of FDI Attacks on Vehicular Platoons. in P Varga, LZ Granville, A Galis, I Godor, N Limam, P Chemouil, J Francois & M-O Pahl (eds), Proceedings of the IEEE/IFIP Network Operations and Management Symposium 2022: Network and Service Management in the Era of Cloudification, Softwarization and Artificial Intelligence, NOMS 2022. Proceedings of the IEEE/IFIP Network Operations and Management Symposium 2022: Network and Service Management in the Era of Cloudification, Softwarization and Artificial Intelligence, NOMS 2022, IEEE, pp. 1-6, The 5th International Workshop on Intelligent Transportation and Autonomous Vehicles Technologies , Budapest, Hungary, 25/04/22.
https://dx.doi.org/10.1109/NOMS54207.2022.9789808

DOI 10.1109/NOMS54207.2022.9789808
ISBN 978-1-6654-0601-7

Publisher: IEEE

# Safety, Stability and Environmental Impact of FDI Attacks on Vehicular Platoons

Sean Joe Taylor*, Farhan Ahmad*, Hoang Nga Nguyen*, Siraj Ahmed Shaikh*, and David Evans†
*Systems Security Group, Centre for Future Transport and Cities (CFTC), Coventry University, Coventry, UK
†IDIADA Automotive Technology UK, Cambridge, UK
Email: taylo314@uni.coventry.ac.uk, {ad5899, ac1222, aa8135}@coventry.ac.uk, david.evans.g@gmail.com

***Abstract*—Vehicular platooning is a promising technology for improving road safety, increasing vehicle efficiency, and reducing traffic congestion by enabling high-speed vehicles to travel in close formation with minimum inter-vehicular distance. However, a False Data Injection (FDI) attack can destabilise and break up vehicular platoons in several different ways. First, an attacker can inject false leave or split messages leading to a breakup of the vehicular platoon. Another way is by sending fake beacons or tampering information (such as speed, acceleration, distance, location etc) in a beacon. Upon receiving this false data, the platoon will destabilise as the members receives tampered information from the attacker. In this paper, we studied the impact of FDI attacks on the vehicular platoon by modifying significant information in a beacon. We carried out a simulation-based study, where a FDI attacker is modelled in Plexe simulator to attack a platoon. We considered two scenarios for an FDI attack, i.e., the attacker can be present both inside and outside of the platoon. Further, two flavours of FDI attacks are implemented, i.e., (1) Constant FDI: where, the attacker is launching FDI attack constantly throughout it's journey, and (2) Intelligent On-Off FDI: where the attacker is performing FDI for short period of time and then hides his identity by performing legitimate communication with platoon members. We studied the impact of FDI attacks on vehicular platoons from three significant aspects: environmental ($CO_2$ emissions), safety (distance), and stability (speed). Our study showed that FDI attacks can have drastic impact on the vehicular platoons.**

***Index Terms*—Platoons, Cyber Attacks, False Data Injection, Smart Cities, Communication Security**

## I. Introduction

Vehicular platooning is a novel technology to improve transportation on an increasingly congested road network infrastructure, by enhancing road safety, reducing fuel consumption, traffic congestion, and $CO_2$ emissions [1], [2]. Unfortunately, attackers can quickly wipe such benefits away and create chaos for vehicular platoons by injecting false information into the wireless network that the technology relies on [3]. To prevent and counter such attacks, the effects of such attacks need to be explored and the impacts understood.

Vehicular platooning is realised when two or more vehicles are linked together and communicate using vehicle-to-vehicle (V2V) communications. The lead vehicle dictating the behaviour of all connected vehicles with little to no involvement by their own driver [1], [2]. This interaction is made possible using Vehicular Ad-hoc NETwork (VANET) [4] and Cooperative Adaptive Cruise Control (CACC) [2]. VANET enables vehicles to communicate with each other using Vehicle-to-Vehicle (V2V) communications [4], CACC is an advanced version of Adaptive Cruise Control. As well as using sensor information the platooning vehicle also uses V2V communications to maintain a safe inter-vehicle distance from other vehicles within the platoon as well as maintaining the formation [2]. The advantage of platooning is by using V2V communications platoon acts as a single entity as members act almost instantly upon actions taken by other platooning vehicles. Thus, platooning will improve road safety by removing human error and by reducing the workload on drivers [5] as well as significantly decreasing the reaction times of platooning vehicles by acting autonomously to actions taken by the leader and other members [1]. Furthermore, while being driven in this semi-autonomous state, member vehicles can handle most driving situations using instructions from the lead vehicle needing little input from their driver [6].

Using V2V communications, the platoon members are able to almost instantly react to any sudden changes. This enables them to safely drive significantly closer together, which significantly reduces road congestion [1]. In addition, the vehicles are less affected by air resistance, which reduces fuel consumption [7], [8] and, by extension, reducing $CO_2$ emissions [8].

Vehicular platoons rely on wireless communications to maintain their close and organised formations [6], these represent an opportunity for cyberattacks. The wireless communication can be used as an access point for cybercriminals due to the nature of wireless communications. Vehicular platoons are heavily reliant on V2V communications to maintain safety and formation. The wireless radio signals of the IEEE 802.11p standard is vulnerable to a range of attacks; including jamming attacks [9], Sybil attacks [10], ghost vehicles attacks [11], and False Data Injection (FDI) attacks [3], to name a few [12].

Attacks on platoons disrupt and destabilises their normal operations leading to the platoon becoming unsafe and or inefficient. In this paper, our contribution is a simulation-based study on the impact caused by false data injection attack on an eight-vehicle platoon, where the attacker propagates and share false information with the platoon members. Since critical information (speed, distance, location) is being shared between vehicles, FDI attacks can drastically impact the platooning ability of vehicles. Furthermore, the attacker aims to disrupt the network by propagating false information. In this paper, we equipped the FDI attacker with the ability to transmit false speed information. To this end, our study on the impact caused

by FDI attacks on safety, stability and $CO_2$ output, reveals that the inter-vehicle distance between members under such an attack can be affected by up to $25\%$, with the speed of platooning members affected by up to $4.058\%$ and the $CO_2$ output of platooning members varying by $0.024\%$. In addition to this, the experiment shows it takes at least $30s$ for the platoon to recover after an attack stops.

This paper is organised as follows Section II introduces platoons and explains the CACC platoon controller used to maintain the vehicle platoon in this experiment. Section III introduces FDI attacks in vehicular platoons. The following Section IV and Section V discusses the simulation environment and the results. Finally, Section VI concludes this paper.

## II. Vehicular Platoon

In this section, the concept of a vehicular platoons will be briefly explained. Vehicular platoons are made up of a leader vehicle and member vehicles; there are also vehicles referred to as join/leavers. Join/leavers are vehicles in transition between manual and automatic driving modes as they enter and leave the platoon [4]. To maintain the platoon, members pass information about their behaviours to others in the platoon using beacons. Beacons in platoons broadcast information related to the *position, speed, acceleration, target speed and/or acceleration, vehicle ID, membership status, and travel direction* of the vehicle to all other member vehicles via IEEE 802.11p [13]–[15].

To dictate the platoon structure and flow using the information from other platoon members, platoon controllers are used. Such controllers can be very basic where vehicles communicate one way to the vehicle behind them or more complicated, like two vehicles back and the leader. In this paper, the controller used is called Cooperative Adaptive Cruise Control (CACC) as created in the California PATH project [16].Here ACC is then adapted into CACC by including V2V communication between vehicles in the platoon. This enables the member vehicles to understand what the vehicle in front is doing to reduce the error in the inter-vehicle gap presented by ACC. This therefore means that vehicles can travel at high speed in very close formations safely. In addition to this there are also provisions for vehicles joining the platoon and the ideal way to have members join the platoon. The information flow in a CACC platoon is shown in Figure 1.

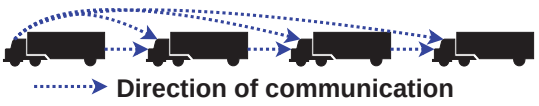



Fig. 1: Beacon information flow within a CACC platoon.

## III. FDI Attacks in Platoon

False Data Injection attacks (FDI) are when an attacker transmits false information or data into the platoon network [3]. The data injected into the vehicular platoon network can be simple changes to individual data points to whole fabricated messages. Any false message or information will negatively impact stability, safety and affect the platoon's environmental impact. To be successful the attacker must create its beacon in the same format as the network it is attacking. An attacker can obtain the format of the message by being part of the platoon network or copying the message format from a captured beacon. The attacked platoon is disrupted as members will act upon the faked information, causing the platoon stability and therefor safety to decrease.

FDI attacks on vehicular platoons are of extreme concern as they can suddenly change and alter the behaviour of a platoon to the benefit of the attacker. In addition to this, the nature of FDI means that precisely what the attack does varies depending on what false information is injected into the network. Vehicular platoons communicate between members using beacons as described in Section II. Therefore, an attacker can fake many different data points or even whole messages. In addition to this, FDI attacks could also be used to break up a platoon by injecting fake leave or split messages to members. In addition to this the attacker can inject false or altered beacons, enabling the attacker to change parameters such as speed, acceleration, target speed and/or acceleration and vehicle ID. In this experiment, the attacker will be creating fake speed data for the platoon beacon that is then transmitted into the network.

### A. Flavours of FDI Attack

This paper considers two FDI attack cases where the attacker fakes the speed in its beacon. The first attack type is a constant attack, and the second is an On-Off attack.

*1) Constant FDI Attack:* The constant attack represents an attacker attacking a platoon for the whole length of the journey that it undertakes. Every message that the attacker transmits contains false information. In this case, the faked information will be constant throughout; however, what the attacker fakes could change over time. This would still count as a constant attack so long as the attacker constantly attacked.

*2) On-Off FDI Attack:* The On-Off attacker represents an intelligent attacker that attempts to hide by going through periods of attacking and not attacking. This kind of attacker behaviour can be created in several different ways, such as; using a timer so the attack will run for a set time before stopping and then starting again after a predetermined amount of time. In this way, the attacker can hide its identity by pretending to be a legitimate member of the platoon. In addition, an attacker can achieve the same using a counter to count the number of messages the attacker transmits a set number of messages before hiding again. The final way is for the attacker to be triggered by specific messages received by the attacker. On-Off attacks can be more difficult to detect and counter as the attacker is not constantly attacking and therefore cant be as easily identified and removed.

## IV. Simulation

In this study, we used an open source software called Plexe [17], which is a cooperative driving framework that extends

Veins [18] and links with SUMO [19] to provide a realistic simulation environment for platoons within an OMNET++ network simulator. Plexe handles the platoon protocols and applications, Veins handles vehicle network communications and links to SUMO which is used for traffic modeling.

### A. Scenarios

When considering the effects of a constant FDI attack and an On-Off FDI attack, it is also essential to understand how the attacker's position affects the effectiveness of the attack. To consider this, the experiment will have two scenarios. (1) *Insider FDI*: where the attacker is a member of the platoon, and (2) *Outsider FDI*: when the attacker is a vehicle travelling alongside a platoon. All other variables and settings within the simulation are kept constant to compare the attacks and the scenarios fairly. The experiment is set up on a straight multi-lane roadway without any incline or decline for all experiments. The speed for all vehicles in the simulation is set to $80km/h$ or $22.2222m/s$. The platooning vehicles have an inter-vehicle distance of $15m$ as identified in the paper [1]. In the paper, they identify that for European trucks where the minimum distance for braking at $90km/h$ is $7.56m$, which is then doubled and applied to the slower speed of $80km/h$ to give suitable safe traveling distance. This inter-vehicle distance and speed will be used for the CACC platoon controller. The simulation length is $1000s$, enabling adequate time for multiple rounds of On-Off attacks to be simulated. In order to understand the impact of FDI attacks on platoons, there is only one attacker in simulations which will change its speed that is shared in the platoon network.

*1) Insider FDI:* In this scenario, the attacker is node one, and they are a member of the platoon when carrying out the attack. They are positioned directly behind the lead vehicle, setting up the attack to be able to course maximum impact on the platoon. When carrying out a constant FDI attack on the platoon, the attacker constantly reports that they are going $+0.5m/s$ faster in their beacons to the rest of the platoon.

During an On-Off attack, the attacker will attack for $30s$ where it reports its speed has been $+0.5m/s$. The attacker will then stop attacking for $30s$ and report accurately. The reason behind using a $30s$ attack period is that it takes $30s$ for the attacker to have the maximum impact on the attacked vehicles' inter-vehicle distance. If the attack were for a shorter time, then the effect on the inter-vehicle distance would not be as significant. A longer time would not cause any greater disruption to the inter-vehicle distance. The attacker will then start to attack again; however, this time, the attacker reports its speed as $-0.5m/s$ slower than it is for $30s$. Finally, the attacker will stop attacking for $30s$ and report accurately again—this cycle repeats every 120s for the whole $1000s$ of the simulation.

*2) Outsider FDI:* An Outsider attack is when a non-platooning vehicle injects false beacons into the platoon. In this case, the vehicle is traveling along side parallel to the platoon. As such, it must fake or capture the information needed to create a beacon. In addition, it must also impersonate a legitimate member of the platoon. Otherwise, the platoon will ignore the message. Therefore, the attacker creates a fake message and impersonates node 1 as it drives alongside the platoon. The way it attacks is the same as when they are a member, first with a constant and then using the On-Off approach's described for the insider attack.

## V. Simulation Results

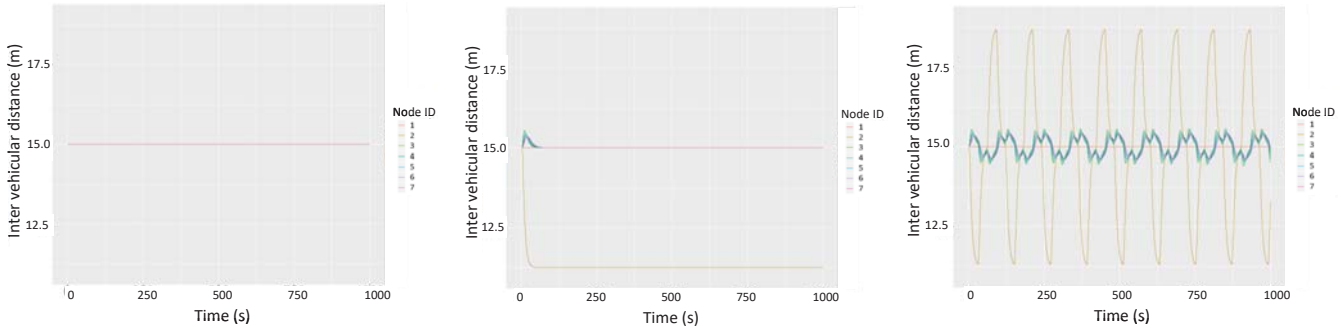
In this section, the results of the simulations are presented and discussed in detail.

### A. Results from Safety and Stability Aspects of Platoons

Due to the inter-vehicle distance between vehicles in a platoon, the platoon's safety is linked to the stability of the platoon and the platoons controllers ability to maintain a constant inter-vehicle with minimal gap errors. Therefore using the inter-vehicle distance and vehicle speed, the risk of collision can be understood.

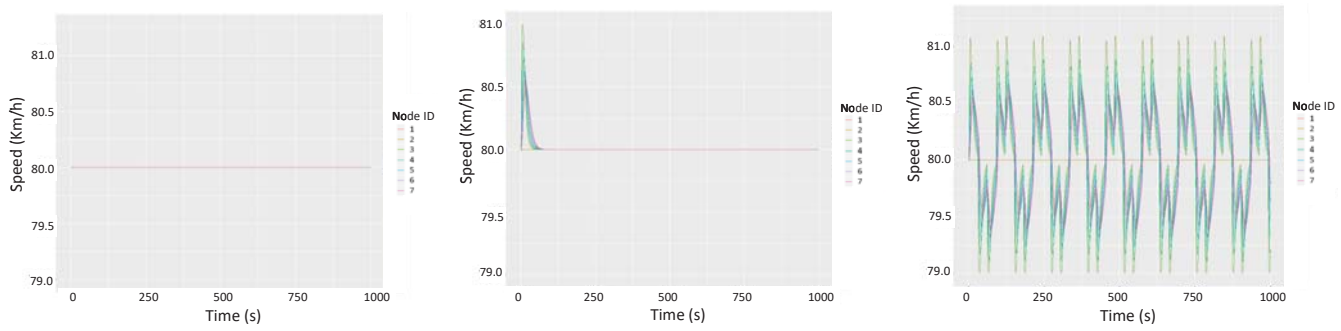
*1) Insider FDI Attack:* Figure 2 highlights the inter-vehicle distance in vehicular platoons when considering an internal FDI attack. Under ideal conditions with no attack as highlighted in Figure 2a, all vehicles have a constant inter-vehicle distance of $15m$, which does not change throughout the experiment. When node one, an insider attacker inserts a bogus speed value into its beacon, node two is most significantly affected as shown in Figure 2b and Figure 2c. The fake speed value will course node two to accelerate to match the new speed that node one reports. Therefore during a constant FDI attack, the inter-vehicle distance between node two and node one reduces to $11.25m$ which is nearly $25\%$ decrease in inter-vehicle distance compared to the ideal. This change takes place over the first $100s$ and remains until the end of the simulation. The inter-vehicle distance variation during the On-Off attack forms a sine wave. The formation of the sine waveform is because the attacker cycles through being active and then dormant. The effect is amplified as the attacker cycles through reporting high speeds and low speeds in the fake beacon. During an On-Off attack, the inter-vehicle distance for node two is slightly less affected than under constant attack at $3.682m$, which is a $24.547\%$ change in inter-vehicle distance compared to the ideal.

When looking at other members of the platoon under constant attack, all nodes after node two see a slight increase in inter-vehicle spacing during the initial attack; this then returns to the ideal when node two becomes constant. On the other hand, during an On-Off attack, the nodes after node two also form a sinusoidal pattern opposite to node two. In addition to this, they form a double peak, as platoon members adjust between being attacked and repairing the damage caused by the attack on the platoon. During the attack, all nodes after node two have some small displacement from the ideal opposite to that of node two. This is because the gap distance changes as node two changes its speed to match the fake beacon and, therefore, is the opposite of node two's divergence from the ideal. The behaviour is then reversed when the platoon is recovering from the attack as all members




(a) (b) (c)

Fig. 2: Inter-vehicle distance of platooning vehicles (a) under ideal conditions, (b) internal constant FDI attack and (c) internal On-Off FDI attack.



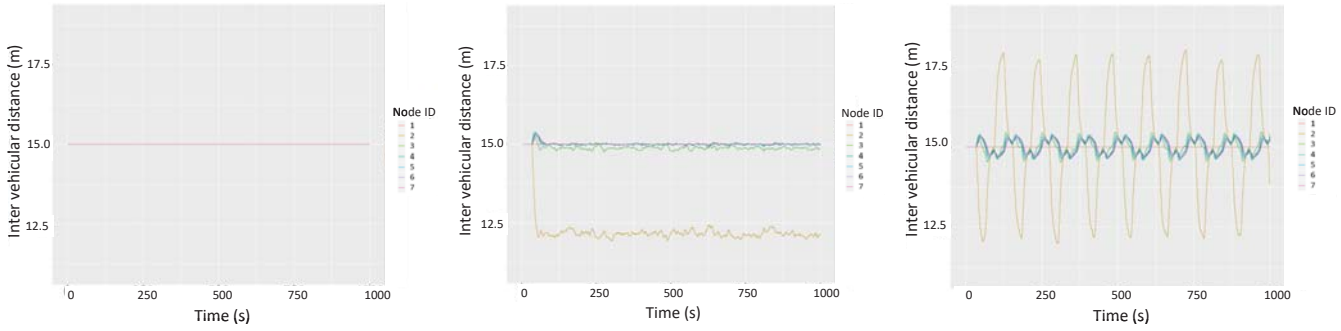

(a) (b) (c)

Fig. 3: Vehicle speed of platooning vehicles (a) under ideal conditions, (b) internal constant FDI attack and (c) internal On-Off FDI attack.

seek to reobtain the ideal inter-vehicle distance. However, this recovery is never completed as the attacker starts to attack again, and because the attacker alternates between a positive speed and negative speed, a second peak forms.

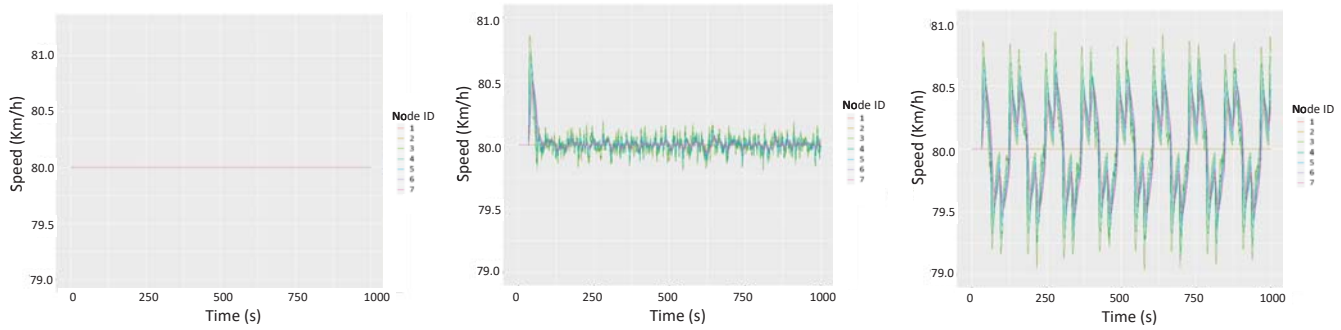
The speed of the platoon when not under attack and then under constant and On-Off FDI attack by an internal attacker are all shown in Figure 3. Under ideal conditions shown in Figure 3a, the speed of all vehicles starts and remains at $80km/h$. When under a constant FDI attack, the speed of all nodes after node one increases sharply as shown in Figure 3b, with node two peaking at $81km/h$. While this new maximum speed is not that much of a radical change, it does significantly impact the overall platoon formation as it courses the inter-vehicle spacing to reduce. In addition to this, the new speed is not held throughout the simulation length as the controller can use on-board sensors, which with such a small change, can prevent the speed from causing a collision. When looking at the On-Off attack again, all nodes after node one are affected by the attack. The peaks are slightly taller at just over $81km/h$. However, the interesting thing is that the speed for all attacked vehicles shows the same double peak pattern seen by the nodes after node two when looking at the inter-vehicle distance of the On-Off attack, because the attacker is attacking the speed component of the beacon, which then impacts the inter-vehicle distance. As the platoon controller reacts to the fake speed from the attacker. Overall, this movement makes the platoon more unstable when under an On-Off attack than a constant attack.

*2) External FDI Attack:* Figure 4 shows the inter-vehicle distance between platooning vehicles when under an FDI attack from a non-member attacker. Figure 4a is when there is no attacker present, Figure 4b is the platoon under constant attack and Figure 4c is of the On-Off attack by an external attacker. The overall effects are the same as the insider attack; however, there are small but significant differences. The first difference is that the platoon is more unstable during the external attack, which is clearly seen in Figure 4b where nodes two and three are very clearly unable to hold a steady inter-vehicle distance. This behaviour is also seen in the On-Off attack. This behaviour is due to the attacked vehicle receiving genuine and fake beacons. This improves the inter-vehicle distance between node one and two, which is now a minimum of $12.18m$, an $18.8\%$ reduction in distance compared to the ideal. Further, node three also reduces its inter-vehicle distance by $0.373m$, or $2.488\%$ less than the ideal distance. The On-Off attack sees a reduction in the maximum and minimum inter-vehicle peaks, with them around $+-2.742m$ or $18.277\%$ from the ideal inter-vehicle distance.




(a) (b) (c)

Fig. 4: Inter-vehicle distance of platooning vehicles (a) under ideal conditions, (b) external constant FDI attack and (c) external On-Off FDI attack.




(a) (b) (c)

Fig. 5: Vehicle speed of platooning vehicles (a) under ideal conditions, (b) external constant FDI attack and (c) external On-Off FDI attack.

As seen with the inter-vehicle distance, the overall patterns for the speed are the same as the internal attacker. However, as seen with the inter-vehicle distance, the peaks are smaller. For example, the speed of node two is less than $0.75km/h$ increase from the ideal during the constant attack and never rises as high as $81km/h$ for the On-Off attack. The improvement is because node two receives both genuine and fake beacons when under attack by the external attacker. However, when under attack from an external attacker, the stability is significantly affected. This can be seen most clearly in the constant attack where all nodes after node one cannot maintain a constant speed once the attack starts. This is because node two implements both genuine and fake beacons and passes these on to following members. As such, this mixing of beacons makes the platoon speed very unstable with the speed variable up to $0.25km/h$ during the constant attack after the initial spike in speed which is not seen when under constant insider attack.

### *B. Results from Environment Aspects*

In Plexe, $CO_2$ is modelled according to [20]. When under ideal conditions the $CO_2$ output for each vehicle will be $3192.508g$ over the course of this simulation. Vehicles one and two platoon normally as they are not affected by the fake beacon, only from vehicle 3 onward are effected. This is reflected by having the same $CO_2$ output in all runs regardless of the attack. Whereas from vehicle three onward, the $CO_2$ production of the vehicles varies a lot, with some vehicles producing less $CO_2$ and other produce more when under attack. The largest increase in $CO_2$ is seen by vehicle three under a constant FDI from another member of the platoon, which sees an increase of $0.699g$. An increase in $CO_2$ means that the vehicles engine is having to work harder and therefore use more fuel. The largest saving of $CO_2$ is also vehicle three when under an On-Off attack from another member of the platoon, which sees a reduction of $0.759g$.

It is the On-Off attacks where things get very interesting. Here the controller suffers the most deviation from the ideal. Instead of vehicles outputting more $CO_2$ than vehicles one and two, as seen for the constant attacks. Many vehicles output less as seen in Figure 6. When the attacker is a member of the platoon, vehicles three, four, five and six see a reduction in $CO_2$ with only vehicles seven and eight increasing $CO_2$ output. Vehicle three sees a saving of $0.024\%$, whereas vehicle eight sees an increase of $0.010\%$. The same pattern is also seen when the attacker is not a platoon member; however, the maximum reduction in $CO_2$ is $0.016\%$ for the controller. Seeing the $CO_2$ production of vehicles three, four, five and six decrease was surprising as the vehicles are having to accelerate regularly and cannot hold a steady speed. In addition, vehicles

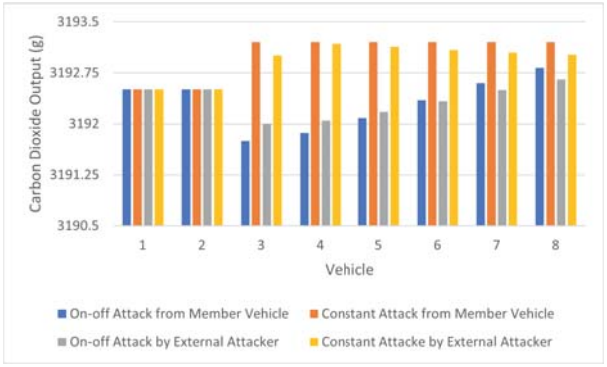



Fig. 6: Total $CO_2$ output of all vehicles under each scenario.

cannot hold the ideal safe inter-vehicle distance, thus losing out on the additional fuel efficiency benefits of platooning. The possible reason for this behaviour is that the vehicles can use the slipstream of the vehicle in front which reduces the fuel used to accelerate significantly. In this experiment, the $CO_2$ changes are tiny, less than $0.024\%$, which looks insignificant; however, this will lead to much more substantial effects when applied to the real world. For example, the current simulation is for $1000s$ or $0.278$ hours, whereas vehicles such as trucks would be platooning for significantly longer. In addition, the effects are for a single vehicle, not the platoon as a whole. While the $CO_2$ impact of the FDI attack is still going to be relatively small, its impact becomes amlified when more realistic platooning times are used. In addition to this platooning is aimed to reduce $CO_2$ output and any degradation of this will have an overall negative impact on its use.

## VI. Conclusion and Future Work

Vehicle platooning is a significant transportation technology with the potential to improve safety and reduce congestion on our roadways. However, the challenge with the technology is its use and reliance on wireless V2V communications which provides ample opportunity for attackers to disrupt, hijack and attack the platoons. This paper shows how an FDI attack can disrupt a platoon making it unsafe, unstable and altering the environmental impact of the platoon. The disruption caused by the attacker is very significant from both the internal and external attacker. In future, we will extend this work further by proposing a light-weight and efficient solution to mitigate false data injection attacks within the vehicular platoons to improve the stability and safety even under FDI attacks.

## References


[1] S. Ellwanger and E. Wohlfarth, "Truck platooning application," in *IEEE Intelligent Vehicles Symposium (IV)*, 2017, pp. 966–971.

[2] F. Ma, Y. Yang, J. Wang, X. Li, G. Wu, Y. Zhao, L. Wu, B. Aksun-Guvenc, and L. Guvenc, "Eco-driving-based cooperative adaptive cruise control of connected vehicles platoon at signalized intersections," *Transportation Research Part D: Transport and Environment*, vol. 92, p. 102746, 2021, DOI:https://doi.org/10.1016/j.trd.2021.102746. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S136192092100050X

[3] M. Wolf, A. Willecke, J.-C. Müller, K. Garlichs, T. Griebel, L. Wolf, M. Buchholz, K. Dietmayer, R. W. van der Heijden, and F. Kargl, "Securing cacc: Strategies for mitigating data injection attacks," in *2020 IEEE Vehicular Networking Conference (VNC)*, 2020, pp. 1–7.

[4] D. Jia, K. Lu, and J. Wang, "A disturbance-adaptive design for vanet-enabled vehicle platoon," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 2, pp. 527–539, 2014, DOI:10.1109/TVT.2013.2280721.

[5] S. C. Calvert, G. Mecacci, D. D. Heikoop, and F. S. de Sio, "Full platoon control in truck platooning: A meaningful human control perspective," in *21st International Conference on Intelligent Transportation Systems (ITSC)*, 2018, pp. 3320–3326.

[6] Vissers J., et al., "V1 platooning use-cases, scenario definition and platooning levels d2.2 of h2020 project ensemble," 2018. [Online]. Available: platooningensemble.eu

[7] Y. Bichiou and H. Rakha, "Vehicle platooning: An energy consumption perspective," in *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, 2020, pp. 1–6.

[8] M. P. Lammert, A. Duran, J. Diez, K. Burton, and A. Nicholson, "Effect of platooning on fuel consumption of class 8 vehicles over a range of speeds, following distances, and mass," vol. 7, no. 2, 10 2014, DOI:10.4271/2014-01-2438. [Online]. Available: https://www.osti.gov/biblio/1160183

[9] S. Ucar, S. C. Ergen, and O. Ozkasap, "Ieee 802.11p and visible light hybrid communication based secure autonomous platoon," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8667–8681, 2018, DOI:10.1109/TVT.2018.2840846.

[10] J. Santhosh and S. Sankaran, "Defending against sybil attacks in vehicular platoons," in *2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2019, pp. 1–6.

[11] J. Han, M. Harishankar, X. Wang, A. J. Chung, and P. Tague, "Convoy: Physical context verification for vehicle platoon admission," in *Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications*, ser. HotMobile '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 73–78. [Online]. Available: https://doi.org/10.1145/3032970.3032987

[12] S. J. Taylor, F. Ahmad, H. N. Nguyen, S. A. Shaikh, D. Evans, and D. Price, "Vehicular platoon communication: Cybersecurity threats and open challenges," in *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, 2021, pp. 19–26.

[13] M. Amoozadeh, A. Raghuramu, C.-n. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 126–132, 2015, DOI:10.1109/MCOM.2015.7120028.

[14] M. Amoozadeh, H. Deng, C.-N. Chuah, H. M. Zhang, and D. Ghosal, "Platoon management with cooperative adaptive cruise control enabled by vanet," *Vehicular Communications*, vol. 2, no. 2, pp. 110–123, 2015, DOI:https://doi.org/10.1016/j.vehcom.2015.03.004. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214209615000145

[15] R. van der Heijden, T. Lukaseder, and F. Kargl, "Analyzing attacks on cooperative adaptive cruise control (cacc)," in *IEEE Vehicular Networking Conference (VNC)*, 2017, pp. 45–52.

[16] S. Shladover, X.-Y. Lu, S. Yang, H. Ramezani, J. Spring, C. Nowakowski, and D. Nelson, "Cooperative adaptive cruise control (cacc) for partially automated truck platooning:final report," *Escholarship.org*, 2018. [Online]. Available: https://escholarship.org/uc/item/260060w4main

[17] M. Segata, S. Joerer, B. Bloessl, C. Sommer, F. Dressler, and R. L. Cigno, "Plexe: A platooning extension for veins," in *2014 IEEE Vehicular Networking Conference (VNC)*, 2014, pp. 53–60.

[18] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Transactions on Mobile Computing (TMC)*, vol. 10, no. 1, pp. 3–15, January 2011, DOI:10.1109/TMC.2010.133.

[19] P. A. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner, and E. Wießner, "Microscopic traffic simulation using sumo," in *The 21st IEEE International Conference on Intelligent Transportation Systems*. IEEE, November 2018, pp. 2575–2582. [Online]. Available: https://elib.dlr.de/127994/

[20] A. Cappiello, I. Chabini, E. Nam, A. Lue, and M. Abou Zeid, "A statistical model of vehicle emissions and fuel consumption," in *The IEEE 5th International Conference on Intelligent Transportation Systems*, 2002, pp. 801–809.