DOCTOR OF PHILOSOPHY

The use of Multiple Criteria Decision Analysis to Identify False Beacons in a Platooning Network

Taylor, Sean Joe

Award date:
2024

Awarding institution:
Coventry University

The use of Multiple Criteria Decision Analysis to Identify False Beacons in a Platooning Network

Sean Joe Taylor

PhD

July 1, 2024

The use of Multiple Criteria Decision Analysis to Identify False Beacons in a Platooning Network

A thesis submitted in partial fulfilment of the University's requirements
for the degree of Doctor of Philosophy

July 1, 2024

Declaration

All sentences or passages quoted in this document from other people's work have been specifically acknowledged by clear cross-referencing to author, work and page(s). Any illustrations that are not the work of the author of this report have been used with the explicit permission of the originator and are specifically acknowledged. I understand that failure to do this amounts to plagiarism and will be considered grounds for failure.

Name: _____

Signature: _____

Date: _____

Acknowledgement

A PhD is said to be the work of a single person who has dedicated many years to their education. Well, I feel that this is wrong. In practice, a PhD is earned by a single individual; however, it takes a team of people to make a PhD a success.

First, I must thank Dr Siraj Shaikh for spotting my potential to achieve something as great as a PhD. When we first met, I had been struggling to land my first role out of university and was starting to feel I was not good enough; however, I must have impressed him with what I can only think of as my enthusiasm and my willingness to overcome challenges as I had no background in Cyber Security. Then there is Dr Hoang Nga Nguyen, who has immense patience, as, without his guidance in my first year, my future career would be so bright. So much of the experience from writing my first paper has shaped how I write and structure my work. Dr Farhan Ahmad, my longest-serving director of studies, thank you for all the help, support, and advice you gave me during my PhD journey. I know I have made you suffer much during this time with all the stuff I was doing and all the crazy ideas I was coming up with. Who would think they would work? Thank you for being there to support me. Then there is Dr Jeremy Bryans, who was thrown into being my director of studies in the last six months after having virtually no understanding of my project. Thank you for guiding me through this time of form filling and consolidating three and a half years of work into a single and comprehensive document. Finally, I must thank my industry sponsors IDIADA and their staff, who have been there to answer and ask the hard questions and provide me with valuable and interesting information that has enabled my work to better model and match real-world counterparts.

People say that family is everything; I know I would not be where I am today without my family. Firstly, I want to thank my mom (Mrs Rebecca Taylor), Who has always fought hard to convince others to see my potential, not just my disability. Thank you for all the fights with doctors, schools and other professionals. Then there is my grandmother (Mrs Pam Gardner), who never got to see me go off to university sadly, but without who and all of the fights at the dinner table over homework, I would never have been able to achieve my GCSE's, let alone a PhD. I thank my family and friends for all the help and support they have given me over the years. Finally, I thank my girlfriend Charlotte, who has had to put up with me through all my stress and worry over whether I am good enough to complete a PhD.

Abstract

Vehicle Platooning applications will impact driving by improving the safety, efficiency and fuel economy of platooning-enabled vehicles and road networks. A vehicle platoon is when two or more vehicles travel together with minimal inter-vehicle distance, and the actions of the leading vehicle are copied by all non-leader member vehicles using sensors and wireless communications. Non-leader member vehicles are semi-autonomous or entirely autonomously driven when platooning. The challenge with keeping platooning safe from many cyber attacks is securing the wireless communication channels used to enable platooning, such as Eavesdropping, Spoofing and False Data Injection (FDI) attacks, to name a few. Such attacks on communication, which is a primary method of control for platooning vehicles, can significantly damage the platoon's availability, stability and safety.

There is a range of proposed solutions to prevent attacks on platoons, with many proposed solutions being inspired by solutions to VANET (Vehicle Ad hoc Networks), such as using private and public key infrastructure and trust methods. While it shares many similarities with VANET, Platooning requires more secure communications due to the communications used to drive a platoon vehicle directly in situations where the margin of error is significantly low. During platooning, the momentary disruption of the communications between vehicles from attackers is more likely to cause more damage to platooning vehicles and other road users due to the need for constant communications to maintain safe platooning due to the use of semi and completely autonomous driving of the vehicles. Currently, VANET is used to increase situational awareness for drivers and not to control a vehicle directly; therefore, platoon security methods can take time to identify attackers and take action, leaving the platoon vulnerable to attacks that manipulate or fake beacons in the platoon communication network.

Therefore, this thesis presents a novel approach by proposing the development and utilization of Multiple Criteria Decision Analysis (MCDA) as an additional layer of defence. This innovative method empowers platoon members to swiftly assess a received beacon, thereby rejecting false or tampered beacons and replacing them with a reasonable alternative. This capability allows the attacked vehicle and, consequently, the platoon to continue platooning as usual, even under heavy assault by an attacker. To validate the effectiveness of MCDA in mitigating the effects of both internal and external False Data Injection (FDI) attacks on a platoon, the platooning simulation software Plexe is employed. The Plexe simulations can replicate platooning as well as the effects that external and internal attackers have on a platoon. This research demonstrates how the use of MCDA and trust together

can effectively mitigate the effects of these attacks on platoon members and the platoon as a whole.

Contents

List of Figures

List of Tables

List of Publications

S. J. Taylor, F. Ahmad, H. N. Nguyen, S. A. Shaikh, D. Evans and D. Price, *"Vehicular Platoon Communication: Cybersecurity Threats and Open Challenges,"* 2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Taipei, Taiwan, 2021, pp. 19-26, doi: 10.1109/DSN-W52860.2021.00015.

S. J. Taylor, F. Ahmad, H. N. Nguyen, S. A. Shaikh and D. Evans, *"Safety, Stability and Environmental Impact of FDI Attacks on Vehicular Platoons,"* NOMS 2022- 2022 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 2022, pp. 1-6, doi: 10.1109/NOMS54207.2022.9789808.

S. J. Taylor, F. Ahamad, H. N. Nguyen, S. A. Shaikh, D. Evans and C. E. Wartnaby, *"ARISTOTLE: AddRessIng falSe daTa injectiOn atTacks in vehicLE platoons,"* 6th Smart Cities Symposium (SCS 2022), Hybrid Conference, Bahrain, 2022, pp. 198-203, doi: 10.1049 /icp.2023.0403

S. J. Taylor, F. Ahmad, H. N. Nguyen, and S. A. Shaikh, *"Vehicular Platoon Communication: Architecture, Security Threats and Open Challenges,"* Sensors, vol. 23, no. 1, p. 134, Dec. 2022, doi: 10.3390/s23010134.

S. J. Taylor, F. Ahamad, H. N. Nguyen, S. A. Shaikh, J. Bryans and C. E. Wartnaby, *"A Comparative Analysis of Multi-Criteria Decision Methods for Secure Beacon Selection in Vehicular Platoons,"* Transactions on Emerging Telecommunications Technologies. Accepted and awaiting publication.

Acronyms

Table 1: *Acronyms*

Acronym	**Meaning**
ACC	Adaptive Cruse Control
ADAS	Advanced Driver Assistance System
AHS	Automated Highway System
AI	Artificial Intelligence
CACC	Co-operative Adaptive Cruse Control
CAN	Controller Area Network
CAV	Connected and Autonomous Vehicle
CCH	Control Channel
SCH	Service Channel
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DoS	Denial of service
DSRC	Dedicated Short-Range Communications
FDI	Fake Data Injection
GPS	Global Positioning System
HGV	Heavy Goods Vehicle
ID	Identification
IoT	Internet of Things
ITS	Intelligent Transportation Systems
LiDAR	Light Detection and Ranging
MAC	Media Access Control
MCDA	Multiple Criteria Decision Analysis
PKI	Public Key Infrastructure
RSU	Road Side Unit
SP-VLC	Secure Platoon Visible Light Communication
TA	Trusted Authority
TCP	Transmission Control Protocol
TOPSIS	Technique for Order of Preference by Similarity to Ideal Solution
UDP	User Datagram Protocol
V2I	Vehicle-to-Infrastructure communications

V2V	Vehicle-to-Vehicle communications
V2X	Vehicle-to-Everything communications
VANET	Vehicular Ad hoc NETwork
VPD-ADA	Vehicle Platooning Disruption attack detection algorithms
VPD	Vehicle Platoon Disruption
WAVE	Wireless Access in Vehicular Environment
WHO	World Heath Organisation
WLAN	Wireless Local Area Network
WSMP	WAVE Short Message Protocol
PHY	Physical Layer

Chapter 1

Introduction

There is a current trend toward vehicle automation with a race towards self-driving vehicles; vehicle platooning is a step towards vehicle automation and provides a test bed for developing future autonomous vehicles. Vehicular platooning technology promises to improve road safety, reduce fuel consumption, traffic congestion, and CO_2 emissions by making use of wireless communications and autonomous driving [36, 68, 64] and is now starting to see limited and controlled deployment [10]. A platoon is where two or more vehicles drive in a close convoy formation, and the lead vehicle sends driving commands using wireless communications to the other vehicles in the platoon, enabling a high degree of autonomous driving to these vehicles. Each vehicle in a platoon is bound to the others using wireless communications, which form invisible links between the vehicles, binding them together [36]. The Vehicle to Vehicle (V2V) communications between platooning vehicles play a mission-critical function because the vehicles rely on the communications to drive safely cite15. Therefore, the communications must be protected from attack.

Communications security for platoons can be broadly broken down into four topics: Encryption, Trust, Intruder Detection and Hybrid Communication. Public and private key methods are common for encryption, with research focusing on securely and secretly having platooning vehicles agree on the shared key [46]. Trust in platoons is used to discourage dishonest platoon members by sanctioning them [12, 14]. Hybrid communications are used to increase the robustness of the communications and provide a second channel by which information can be passed on. Intrusion detection methods look to identify anomalies in communications and identify attackers in the platoon network.

Multiple Criteria Decision Analysis (MCDA) is just one way to apply machine learning to vehicle cybersecurity. Its application is best used to compare information from one or more vehicles to build up a bigger picture of the situation and to identify patterns in the information; this leads it also to be able to identify abnormalities and, therefore, identify potential attackers. MCDA is not a miracle cure that can stop all attacks; however, it is an additional tool for building cybersecurity.

1.1 Introduction to platooning and related technologies

1.1.1 Platoons

All vehicles in a vehicular platoon use wireless communications to pass information between members. The information in a beacon includes the transmitting vehicle's speed, location, change in speed or acceleration and deceleration, the time the beacon was created and the maximum acceleration or deceleration of the transmitting vehicle and their unique platoon ID [98]. Using this information, all member vehicles in the platoon can use automated driving by copying the actions of the leader vehicle. Automated driving is when the vehicle can take on the role of the driver even in a limited capacity, reducing the workload for the driver. Diving automation is split into six levels defined in the SAE J3016™ Levels of Driving Automation™ [51]. Levels zero to two are considered to be driver support features where the driver is still required to drive the vehicle even if the vehicle needs constant supervision by the driver, as shown in figure 1.1.

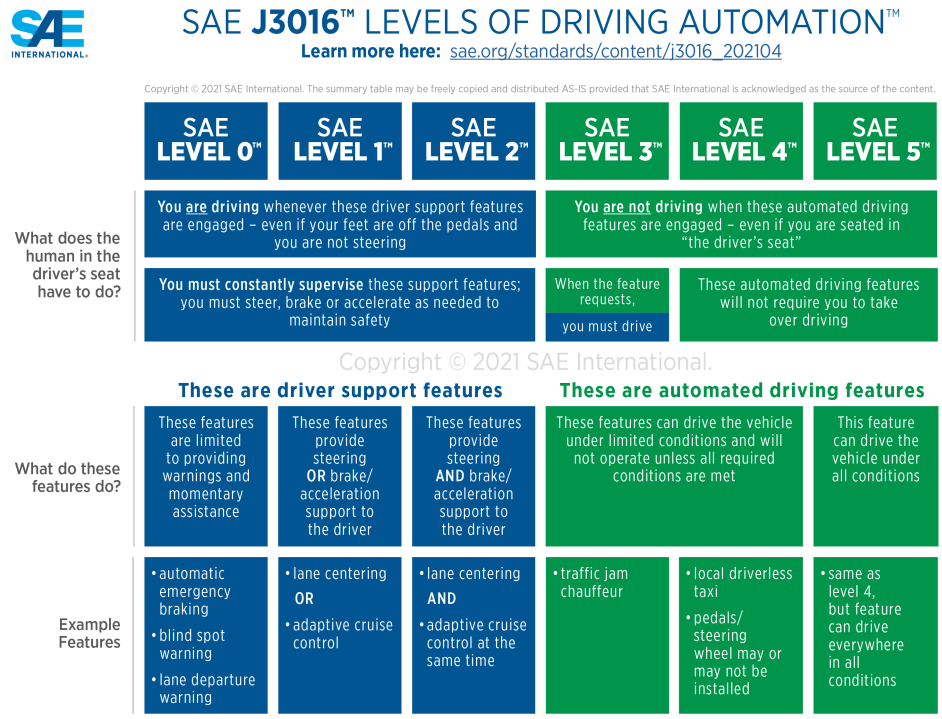


Figure 1.1: *SAE J3016 Levels of Driving Automation graphic [51].*

Levels three to five, however, are considered automated driving, where the driver is not considered to be driving when the automated driving features are engaged. Vehicle platooning can be classified as an SAE level three as the platoon controller can drive the vehicle when part of a platoon, and the driver is responsible for the control of the vehicle when the vehicle is not a member of a platoon, as shown in figure 1.1. Platooning also uses a

cooperative automation model as platooning vehicles for networks that cooperatively share information about their driving, which other members can use to improve their decision-making ability. As a result, using automated driving reduces the chances of an accident due to human error by reducing the workload on member vehicle drivers without increasing the workload of the leader vehicle driver [36]. In addition, automation enables vehicles to travel safely at high speed in compact formations [36].

A platoon comprises a leader vehicle and one or more members. There are also the temporary roles of joiner and leaver, where vehicles transition in or out of the platoon. While a vehicle is part of a platoon, all vehicles communicate using beacons of the same construction and type. Members differ from each other using their platoon IDs [85]. Each vehicle in a platoon will have a different ID. The platoon ID is issued based on the vehicle location and position in the platoon [85]. All vehicles are connected using V2V wireless communications, called beacons, and broadcast to all network members. A human driver always drives the leader's vehicle, whose actions and movements dictate the behaviour of all platoon members. The member vehicles will act upon the platoon leader's wireless messages while platooning. Joining members are, at the start, driven by human drivers who want to join a platoon. Once they are in a suitable and safe position, they switch to automated driving; this is when a joiner becomes a member [36, 84]. Likewise, the leaving vehicle will be under automated control until it is safe for the driver to take over. Some methods of platooning also use roadside units (RSUs) and other infrastructure to improve connectivity and availability [98]. By adding additional infrastructure like RSUs, the platoon uses V2I communication and trusted authorities such as the platoon, enabling companies to improve the user's experience.

Figure 1.2 provides a high-level realisation of platooning in a smart city context. The platoon leader continuously shares critical information with their platoon members in a beacon message. Depending on the communications structure for the platoon protocol, the member vehicles will also communicate with their neighbours using beacon messages, thus forming a platoon network within the VANET network. Further, it shows how new vehicles can join the existing platoon via V2X communication and how platoons can be integrated with other traffic using the VANET network.

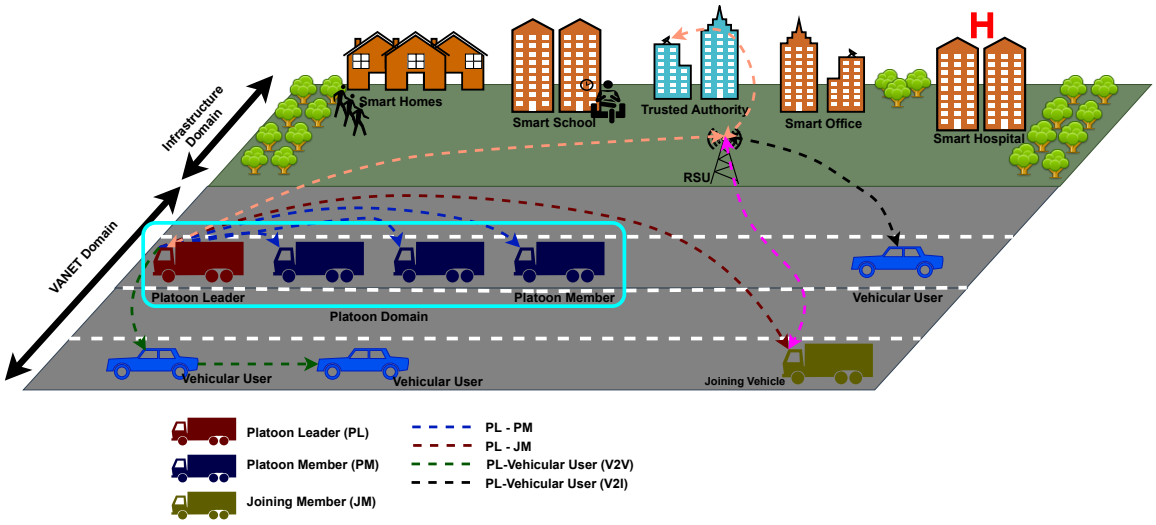


Figure 1.2: *Application of Platooning technology in the context of Smart City.*

1.1.2 VANET and the need to maintain security

VANET is the concept of establishing a network of vehicles for specific needs or situations [81]. This technology can improve road travel by making roads more efficient and safer [76]. VANET can make road travel more efficient by improving driver situational awareness of other road users through sensors that constantly monitor the environment and the vehicle [70]. This data can then be packaged and broadcast to all nearby nodes, such as other vehicles, roadside units (RSU), or pedestrians. These nodes will then respond by acknowledging the message or re-transmitting the message to improve the range.

Since critical information is shared among nodes within a VANET, security becomes critical and essential. Security in platoons includes the physical security of vehicles, cybersecurity and respecting the privacy of the vehicle [36]. If any one of these security elements is compromised, an attacker can seek personal or financial gain. For example, if the vehicle is left with the key unattended, then the physical security is compromised. Likewise, if the communication between two platooning vehicles is open and unencrypted, attackers can eavesdrop on the shared information, thus compromising cybersecurity. This is an extreme example, as communications are always encrypted in practice. In this thesis, only cybersecurity will be considered, with some overlap with privacy.

1.1.3 WAVE Standard

Wireless Access in Vehicular Environment (WAVE) is used for all wireless communications for connected vehicles [75, 57]. WAVE is built upon Dedicated Short-Range Communications (DSRC) based on the IEEE $802.x$ family [33] of standards. DSRC uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) that operates between 5.850 GHz to 5.925 GHz and as defined in IEEE 1609.4 [31, 57]. The stack is also shown in Figure 1.3. DSRC spectrum is formed using seven channels, one central Control Channel (CCH) and six Service Channels (SCHs). In addition, DSRC supports channel switching and simultaneous access of CCH and SCHs [75, 57], which is achieved as each channel is a $10MHz$ band allocated to each channel. A $5MHz$ guard band separates each channel [75, 57].

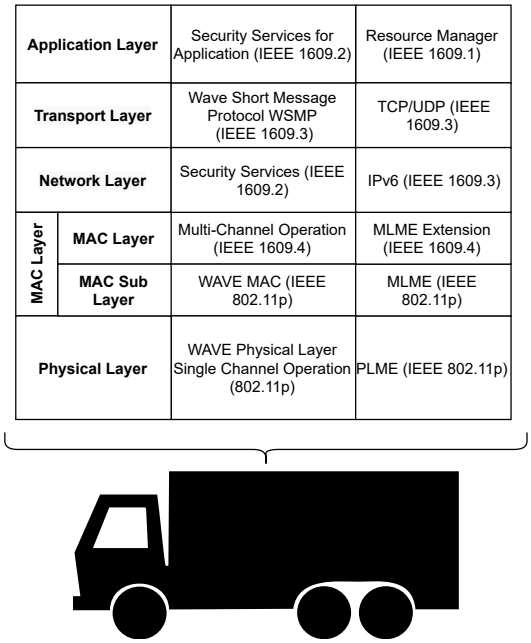


Figure 1.3: *WAVE network stack*

DSRC describes how the communication stack should be arranged and, thus, how tasks like adding and removing frame headers and security measures are to be carried out. WAVE uses the IEEE standard, i.e., IEEE 802.11p, created explicitly for vehicle networks [57]. IEEE 802.11p is only used in the communication stack's physical and data link layers; IEEE P1609 standard handles the rest of the stack [100]. WAVE can form networks with and without IP, using WAVE Short Message Protocol (WSMP) in non-IP applications inherited from DSRC.

IEEE standard 1609.4 is used to manage the time between the SCHs and the CCH to enable the multi-channel operation of WAVE. IEEE standard 1609.3 specifies WSMP with definitions that include User Datagram Protocol (UDP), Transmission Control Protocol (TCP),

and IPv6 within the system; these are taken from DSRC. Defining these management functions is necessary to provide network services. Further, the IEEE standards 1609.2 and 1609.1 are used. The 1609.2 standards describe the security service block for the protocol, and 1609.1 describes the resource manager.

WAVE is used in vehicular platooning [75, 57]. It defines the communication message steps between all vehicles in a platoon regardless of their role in the platoon. The WAVE network stack seen in Figure 1.3 handles all communications between platooning vehicles [99]. The WAVE stack is also used in other V2V applications such as VANET and, as such, also enables platooning vehicles the ability to communicate with other CAV [75, 57].

Platooning uses a range of technologies; however, the most important one in the cybersecurity of platoons is wireless communications. More specifically, the communications protocol used, 802.11p for platooning, is from the 802.11 family and is the key to platooning wireless communications. The standard IEEE 802.11 defines the physical layer (PHY) specifications, the media access control (MAC) when implementing a Wireless Local Area Network (WLAN) using 2.4, 3.6, 5 and 60 GHz frequency bands [9]. IEEE 802.11p is an extension of IEEE 802.11 explicitly created for in-vehicle networking and roadside infrastructure use. The frequency band it is assigned is 5.9GHz band (5.850-5.925)GHz, with the channel spacing of 20MHz, 10MHz and 5MHz [9]. IEEE 802.11p is stated to have a maximum range of 1km and a data rate between 3Mbps and 27Mbps, even at speeds well above legal road speeds [9]. However, it is most reliable under a range of 0.5km. The 802.11p protocol can also handle BPSK, QPSK, 16-QAM and 64-QAM modulation methods for its wireless transmissions [9].

1.1.4 History of Vehicle Platooning

While not platooning, it is worthy of mention due to its similarities with platooning, and an early example of a VANET is the Automated Highway System (AHS) [32]. This project started in 1994 and ended in 1998 to create a prototype AHS where vehicles can be entirely autonomously driven in a dedicated lane on US highways. The project was an RSU-controlled network with various sensors, enabling each vehicle to be driven without the driver's constant active engagement.

The SARTRE project introduced the world to platooning in 2009 [80]. The project was a European joint research project running between 2009 and 2012 and involved seven companies led by Ricardo UK [2]. Other participants in this project include the Spanish companies Fundacion Tecnalia Research & Innovation and IDIADA Automotive Technology SA, the German Rheinisch-Westfaelische Technische Hochschule Aachen and the Swedish companies Rise Research Institutes of Sweden AB, VOLVO Personvagnar AB and Volvo Technology AB. This project aimed to develop environmental road trains (platoons). To achieve this, a new method for how a lead, professionally driven vehicle that is followed by multiple

semi-autonomous vehicles was developed.

In 2016, the first European truck platooning challenge was hosted by the Netherlands [11]. Six companies participated in this challenge and successfully created platoons that travelled from several European cities to finish at the port of Rotterdam [11]. This challenge involved DAF Trucks, Daimler Trucks, Iveco, MAN Truck & Bus, Scania and Volvo Group, where each company had entered one platooning-enabled vehicle. The challenge was a success and a big step in bringing CAVs to European roads.

The next major step in platooning started in 2019 with the ENSEMBLE project [4]. The ENSEMBLE project has been set up much like the SARTRE project to bring safe and secure platooning to Europe. It brings together multiple different companies and academic institutes across Europe. Companies involved in the ENSEMBLE project are Applus IDIADA, Bosch, Brembo, CLEPA, Continental, DAF, Daimler, ERTICO, Fleet Board, IFSTTAR, IVECO, Kungl Tekniska Högskoln, MAN, NXP, Renault Trucks, SCANIA, TNO, VOLVO, Vrije Universiteit Brussel, WABCO and ZF. This project aims to create a foundation for standardising platooning technology, enabling vehicles from different manufacturers to platoon together and demonstrating platooning in real-world conditions and across borders. This project also aims to assess the impact of platooning on traffic safety, fuel economy and traffic flow. This ongoing project was scheduled to finish in May 2021 with a public demo; however, by January 2021, due to its success, the decision was taken to extend the project further, both in time and scope, with the project's final event held on 17th March 2023.

Table 1.1: *Platooning Projects*

Project	Years	Location	Aims the Project
Automated Highway System (AHS), [32]	1994-1998	USA	To convince various stakeholders that the highways of the future will be make heavy use of driver assistance systems and that high level of connectivity between vehicles will improve safety and make road transport better.
SARTRE project [2]	2009-2012	Europe	To encourage a change in personal transport usage by developing environmental road trains.
European Truck Platooning Challenge [11]	2016	Europe	To have multiple vehicles from different manufacturers successfully platoon across borders on public roads.
ENSEMBLE Project [4]	2019-2023	Europe	To enable the adoption of multi-brand truck platooning across Europe, improving fuel economy, safety and reducing congestion.

1.1.5 Platoon architecture

A platoon comprises multiple vehicles, a human-driven lead vehicle, and one or more autonomous member vehicles. Autonomous member vehicles use sensors, and information is transmitted wirelessly to them by the leader and the preceding vehicle to maintain safe and steady driving. This thesis assumes that a platoon's architecture and behaviour are considered to be the same as that defined in the ENSEMBLE project [37]. The ENSEMBLE project discusses how a platoon is to be set up and maintained the platoon in great detail.

There are four main behaviours to a platoon: (1) formation, (2) engagement, (3) platooning and (4) disengagement [37].

1. ***Formation*** is the first step in creating a platoon; this process organises the platoon, designating roles and if the vehicle is starting or creating their platoon.

2. ***Engagement*** is when a platoon forms, V2V communications between the vehicles enable all vehicles to move into position ready to start platooning. Engagement is short-lived and, when successful, is taken over by platooning.

3. ***Platooning*** is when two or more vehicles co-operatively drive using CACC, and the lead vehicle leads the platoon using V2V communications. There is little spacing between vehicles, and the Advanced Driver Assistance System (ADAS) is active to

prevent a collision. When in this state, the platoon can function at its optimum and, as such, is considered the normal state of the platoon.

4. ***Disengagement*** is when a platoon brakes up. Platoon break-up can be intentional or forced, but it must happen safely in both cases. A platoon may disengage when the vehicles need to go separate ways. However, they may also disengage for safety reasons, such as if an attacking vehicle has broken into the platoon.

A vehicular platoon is a group of vehicles that relies on wireless communications (IEEE 802.11p [21, 20, 97]) to maintain a tight, cohesive convoy formation where the lead vehicle dictates the behaviour of all other vehicles [36]. Vehicles within the platoon can take one of the following four positions: (1) *leader* – the first vehicle in the platoon, (2) *member* – any vehicle apart from the leader, (3) *joiners* – vehicles transitioning into the platoon, and finally (4) *leavers* – which transition out of the platoon [55]. The leader and member vehicles transmit *beacons* containing sensitive information such as *position, speed, acceleration, target speed and acceleration, vehicle ID, membership status, and travel direction*.

1.1.6 Cooperative Adaptive Cruise Control (CACC)

The Cooperative Adaptive Cruise Control (CACC) controller translates beacon information from other vehicles and sensor information into commands used to control the vehicle when it is platooning. The CACC model used in this thesis is Cooperative Adaptive Cruise Control (CACC), created by the California PATH project [86]. CACC extends Adaptive Cruise Control (ACC) by enabling the vehicles to exchange information between themselves using V2V communications, where ACC relies on sensor information to maintain inter-vehicle distance. Using sensors alone results in a large gap error when vehicles brake and accelerate. By reducing the gap error between vehicles, it is possible for vehicles to safely travel closer together without the risk of collision during heavy acceleration and deceleration. In CACC, each vehicle communicates with the vehicle directly behind it to minimise gap error when accelerating and decelerating and receives beacons from the leader vehicle to guide positioning and actions that are to be taken by all members. Using both leader and previous beacons to maintain the platoon means that the topology of the communications is predecessor-leader following as shown in Figure 1.4.

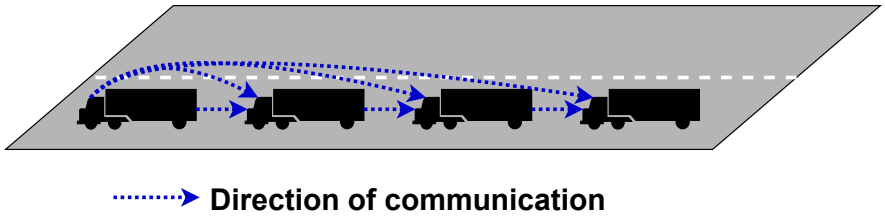


Figure 1.4: *Beacon flow within a platoon*

1.2 Cyber Security Risks to Vehicle Platoons

The cyber security risks of vehicular platoons share similarities with VANETs and Connected and Autonomous Vehicles (CAVs) [42]. However, they also present their own specific set of challenges. Many can trace themselves to trusting that what a beacon says is truthful and safe [21, 20]. Platoons, as has been stated, have short inter-vehicle distances. As such, any disruption to the V2V communications can endanger the safety of the platoon and those around them. Suppose this system is not properly secure and reliable. In that case, there is a high chance of platooning members failing to respond appropriately, leading to collisions [21, 20].

Due to the nature of wireless communication and broadcasting used in platooning, communication in platoons is vulnerable to a wide range of cyberattacks. Radio wireless signals such as the IEEE 802.11p standard are currently used as an open standard within the platoons that anyone with a receiver can eavesdrop on. As a result, there are many threats to platoons identified in the literature, such as False Data Injection attacks [97], Sybil attacks [82], and

Flooding attacks [42] to name a few.

The research recently investigates how to secure platoons from various attacks, such as [61, 77, 59, 48, 62, 25, 95]; however, most of the research discussed only a single attack within the platoons in terms of security. There is a survey paper on platoons called A Survey on Platoon-Based Vehicular Cyber-Physical Systems [56], while this paper discusses the cyberattacks on platoons, it covers many attacks that are also seen in various survey papers for connected and autonomous vehicles (CAVs) [67, 17, 74]..

When investigating the cyber security of vehicle platoons, attacks and defence solutions are grouped and classified in various ways. Some are grouped by the range from which an attacker can perform the attack [30], others group attacks together by security requirements or attributes that are broken or compromised by an attack [71, 17, 67]. The security attributes are Authenticity, Availability, Confidentiality, Integrity and Non-repudiation/Accountability [71, 17, 67]. Authenticity, Availability, Confidentiality and Integrity are all applied to platooning and discussed in Section 2.2.7.

1.3 Communication Topology

Many wireless communication topologies can be implemented in platooning [42, 84, 98]. Each topology comes with different advantages and disadvantages. Overall, the goal is to create a stable network that creates a stable platoon where information is quickly and reliably transmitted to all members. The result is the creation of three topologies: Centralized, Decentralized, and Hybrid, which are much visually shown in Figures 1.5–1.10, respectively.

1.3.1 Centralized Topology

Centralised topology is where the leader communicates with all vehicles in the platoon. On the other hand, member vehicles do not communicate with any vehicle in the platoon, leaving the leader in sole control. This approach is advantageous for quickly making all members aware of actions done by the leader. However, it leaves them without information about other platoon members, such as the vehicle in front of them. There is still communication with the leader, but only GPS and the vehicle's velocity are included in the beacons. The leader will decide what information each member will receive and transmit individual commands to each vehicle. The challenge with this method is the high number of packets transmitted within the platoon, which can produce a significant transmission delay. As a result, packets are usually received by the members very late and outside of tolerance limits. This topology is shown in Figure 1.5, highlighting that only a leader can communicate with their platoon members.

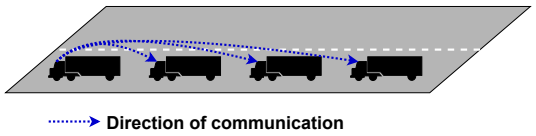


Figure 1.5: *Centralised topology of platooning communications.*

1.3.2 Decentralized Topology

In decentralised topology, each vehicle communicates with the vehicle directly behind them, and each vehicle has no awareness of other vehicles in the platoon. With this topology, the lead vehicle does significantly fewer computation tasks, as it only generates beacons for a single vehicle, the one behind it. Each member vehicle also creates a new beacon for the vehicle directly behind it. Beacons are not re-transmitted. In addition, packets are less likely to be significantly delayed as fewer packets are transmitted to maintain platoon stability. The challenge with this topology is that it can create instability within the platoon when vehicles are leaving and joining. When a vehicle leaves a platoon and is not the rear vehicle, it can create a connectivity hole that must be closed. When a vehicle joins or leaves, member vehicles must sense and adjust their velocity to maintain platoon stability quickly. This topology is presented in Figure 1.6.

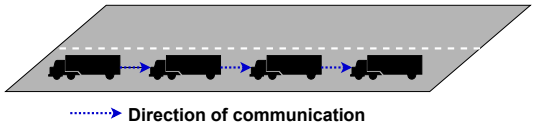


Figure 1.6: *Decentralised topology of platooning communications.*

1.3.3 Hybrid Topology

For hybrid topology, there are four main ways that centralised and decentralised topologies can be combined. Each method has advantages and disadvantages and seeks to overcome the problems of just using a single topology. These topologies are (a) Predecessor-leader following, (b) Bidirectional, (c) Bidirectional leader, and (d) Two-predecessors following.

Predecessor-leader following works by having the leader transmitting to all vehicles, and each vehicle communicates with the vehicle directly behind it, as shown in Figure 1.7. This topology, along with *Bidirectional* topology, was designed to take advantage of Cooperative Automated Cruise Control (CACC). Using CACC, far more information can be passed between members without significantly increasing the number of beacons transmitted per second. This is because the leader's beacon is now the same for all vehicles, without leading to the dropping of packets.

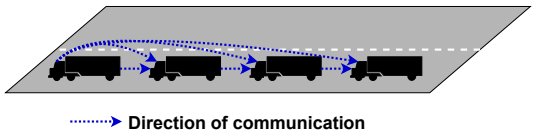


Figure 1.7: *Predecessor-leader following topology of platooning communications.*

Bidirectional topology is when each vehicle can send and receive messages from neighbouring vehicles as depicted in Figure 1.8. The advantage to this is that information from members can flow both ways, which is helpful as environmental sensor and vehicle information can be passed to all members. An example of when this would be useful is when a car overtakes the platoon. The vehicle at the rear can inform all member vehicles that the vehicle is approaching. The disadvantage of this method is that information from the leader, such as emergency braking, is slow as it has to be passed from one vehicle to the next.

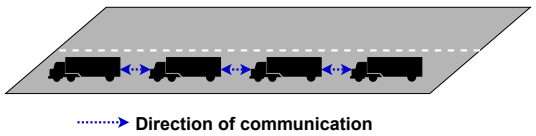


Figure 1.8: *Bidirectional following topology of platooning communications.*

Bidirectional-leader takes Bidirectional along with Centralised to create a topology that seeks to overcome the weaknesses of both methods. By having the leader control the platoon size and stability, the members can communicate directly, as shown in Figure 1.9 to maintain stability and positioning.

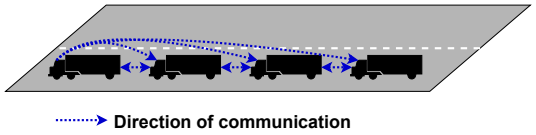


Figure 1.9: *Bidirectional-leader topology of platooning communications.*

Two-predecessors following is an advancement on predecessor-leader following to give vehicles better awareness of what other vehicles are doing without increasing the number of transmitted packets as shown in Figure 1.10. Situational awareness is improved; however, it will require far greater processing power to process and act on all this additional information quickly.

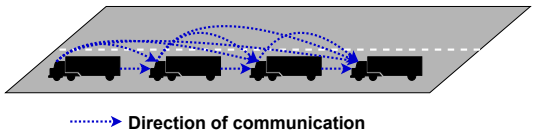


Figure 1.10: *Two-predecessors following the topology of platooning communications.*

1.4 Advantages of Platooning

Platooning technology has two main advantages: reduced inter-vehicle spacing and improved traffic safety. By reducing the inter-vehicle spacing, the fuel economy of the vehicles involved is also improved, in some cases dramatically. By improving the vehicle's fuel economy, the running costs are significantly reduced, as well as the vehicle's output of harmful greenhouse gasses [91, 87, 34] for the same trip. Reducing inter-vehicle distance also means platooning vehicles occupy a smaller space on the road lowering congestion.

1.4.1 Inter-vehicle Spacing

Wireless communications enable platoon members to drive significantly closer to each other safely compared to regular driving due to automated driving that uses information from the preceding vehicle to improve the reaction time. In platoon applications, an inter-vehicle distance of $15m$ is used for safety reasons. However, a possible theoretical gap as small as $7m$ at speeds up to $80km/h$ [36] is possible. In comparison, safe inter-vehicle spacing is recommended in the United Kingdom as the braking distance for a standard vehicle is $53m$ [3] at $80km/h$. This distance is, however, for Heavy Goods Vehicles (HGV) such as Lorry can be significantly more, up to 40% [73]. Therefore, reducing the safe inter-vehicle distance for each vehicle will significantly reduce road space used by platooning vehicles. An example of a simple, three-vehicle platoon compared to three non-platooning following vehicles considering the inter-vehicle of $53m$ is shown in Figure 1.11. Here, three non-platooning vehicles with a total minimum footprint of $L_1 + 53 + L_2 + 53 + L_3$ where L is the length of the vehicle. A three-vehicle platoon with an inter-vehicle distance of $15m$ will be instead $L_1 + 15 + L_2 + 15 + L_3$ again L is the length of each vehicle. The inter-vehicle distance between two consecutive vehicles is $53m$. In this scenario, the total inter-vehicle distance among the three vehicles is $106m$, with each vehicle maintaining a distance of $53m$ with the vehicle in front. In contrast, a three-vehicle platoon cuts this down to just $30m$, with an inter-vehicle distance of $15m$; this is a decrease of approximately 71.3% of wasted space between platooning vehicles.

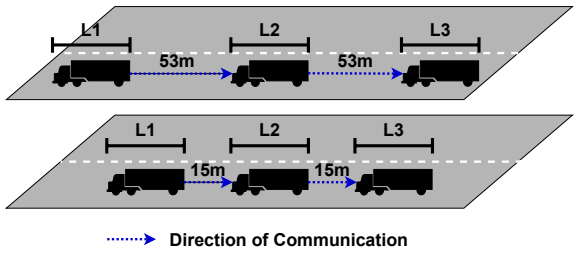


Figure 1.11: *Platoon inter-vehicle space compared to non-platooning vehicles.*

1.4.2 Fuel Economy

The air drag experienced by a vehicle can constitute 23% of the total force acting against a $40t$ HGV when operating under normal driving conditions [64]. The reduction in inter-vehicle space means that the drag forces from air resistance are significantly reduced [27]. Vehicle engines will work less and consume less fuel for a journey than the same journey without platooning. The reduction in fuel consumption can be up to 9.7% for a member vehicle and up to 5.3% for the leader in a platoon of two vehicles, thus resulting in the overall fuel savings being between 3.7% and 6.4% [60]. These values can vary depending on how the vehicle is driven. When a vehicle is idling or accelerating often, the efficiency will reduce overall. Platooning vehicles can maintain the formation without regular braking and acceleration, naturally improving fuel economy. Member vehicles with an inter-vehicle gap of $1s$ can save up to 7.7% fuel when driving at $70km/h$ on a highway; it has also been indicated that this can reach up to 20% [64]. In the SAE International article 'Research on Control Target of Truck Platoon Based on Maximising Fuel Saving Rate', that an average fuel saving of 10% is realistically achievable using a vehicle spacing of $10m$ on German highways over $1000km$ [47]. The vehicle can travel much further by reducing the fuel used, increasing the length of time vehicles can travel without stopping for more fuel. Refuelling less often, truck operators will save money that would have otherwise been spent on fuel [53].

1.4.3 Environmental Impact

Besides saving fuel, the vehicle will produce less CO_2 and other greenhouse gas emissions by reducing fuel consumption. Reducing fuel consumption and, therefore, reducing CO_2 is vital as businesses, consumers, and governments collectively push to reduce greenhouse gas emissions. Currently, in the UK, it is assumed that, on average, with an average size load, a Heavy Goods Vehicle (HGV) will output $0.85049kg/km$ of CO_2[5]. This value is highly volatile as the amount of CO_2 produced will change depending on the manner of driving, the specific route the vehicle uses, and the traffic conditions. A drop of around 5% over a single journey will have a small but meaningful impact on the surrounding environment [60] as we strive for net zero emissions. The slight reduction can quickly snowball into a far more considerable reduction over an entire fleet of vehicles [53] as the benefits quickly multiply.

1.4.4 Traffic Safety

Worldwide, there is a drive to improve road safety, as an estimated 90% of road accidents are attributed to or caused by human error [53]. With around 1.19 million fatalities on roads worldwide each year [8]. A further 20-50 million people suffer non-fatal injuries, with many becoming disabled in road accidents each year [8]. Not only does this impact human loss, but road accidents also have a financial impact. The WHO estimates that for many countries, as much as three per cent of their gross domestic product could be lost through road traffic incidents [8]. Platooning helps to remove human error from driving as all braking and acceleration are controlled by the lead vehicle driver, and there is almost no delay between braking and reaction between platooning members [4]. By adopting technologies such as platooning, self-driving vehicles and other VANET technologies that will decrease driver error and increase driver situational awareness, it is hoped that the EU and UK will continue their downward trend in road injuries and deaths [6, 7].

1.5 Motivation

The communications between vehicles in a platoon are crucial in the safe operations of platoons [4]. Therefore, missing or abnormal information in the beacons will lead to the platoon's breakdown as vehicles cannot coordinate and safely operate [4]. A range of ideas and concepts are being researched to secure platoons, such as encryption [62], Trust [107]. Intrusion detection methods [77]. These methods aim to prevent attackers from being able to be part of the network. To do this, they first identify and remove attackers.

Current wireless communications in a platoon network propose using public and private keys to encrypt all communications [92, 61, 17, 63, 62, 46, 104]. It is commonly used in existing communication standards, including the IEEE 802.11 family [67]. The concept behind public and private keys is to make it so that only the intended target of a message can read it. A range of ways is proposed to establish keys between members of a platoon secretly [59, 63, 61, 62]. The weakness of keys in platooning is the ad hoc networking between vehicles, thus meaning that each time a new vehicle enters the platoon, a new key needs to be shared with them [59, 63, 61, 62]. During key establishment, great care needs to be taken to prevent an adversary from being able to copy the key [104].

In addition, there is the risk of a legitimate member of the platoon network turning rogue, as in any network; this has led to the use of Trust in platoons [48, 107]. In VANET, Trust between members can build over time; however, this method can lead to problems in platooning, expressly with ad-hoc platooning, due to the need for members to trust each other as soon as they start communicating [48]. Therefore, Trust between platooning vehicles needs to act differently from that of VANETs; the information is directly used for platoons to drive member vehicles [4]. Therefore, an attacker will have a window of opportunity to attack a platoon before the trust method can isolate the attacker [48]. In a VANET, this will lead to the driver being given bad information for a short time and less likely to cause a collision

[13]. In comparison, it can lead to a collision in platooning because beacons are used to operate vehicles directly [48, 107]. In a platoon, the beacons are used to maintain vehicle speed and position; as shown in this thesis, a small change for a few seconds will lead to coalitions or near misses by member vehicles.

In platoons, vehicles need accurate beacons from the vehicle in front of them regularly to maintain their position in the platoon [4]. As such, any deviation will destabilise the platoon and can lead to collisions or other unwanted behaviour by the platoon. An attacker can exploit a window of opportunity during key agreement [59, 63, 61, 62]. Trust algorithms by identifying and rejecting the false beacons or members [48]. Therefore, creating a method to close this window of opportunity for an attacker is vital. In this thesis, it is proposed that there should be a way for platooning vehicles to identify potentially harmful messages, reject them and replace them with a safe alternative. To this end, it is proposed that Multiple Criteria Decision Analysis (MCDA) be used to compare current, past, and leader beacons to identify anomalies. Once identified, the vehicle must also have a safe alternative beacon to maintain its position in the platoon. MCDA can also provide sensible alternative beacons to maintain safe platooning even under attack. Thus, by giving a trust algorithm time to identify the attacker, the trust algorithm can also give feedback to the MCDA to improve the resilience to attacks.

1.6 Aim and Objectives

This thesis aims to design, propose and implement a novel solution to address a high-risk cybersecurity attack in vehicle platoons.

To achieve this aim, the following objectives will need to be achieved:

- To perform a literature survey and identify cyber security threats in a vehicle platoon domain from internal and external threats.
- To implement a False Data Injection (FDI) attack on a vehicle platoon, considering an internal and an external attack. The platoon will be studied under constant and on-off FDI attacks from internal and external attackers. This will show that FDI attacks have a high impact on vehicle platoons.
- To design and implement a solution to address external FDI attacks. For this purpose, the Multiple Criteria Decision Analysis technique will prevent false beacons from being disseminated by a platooning vehicle.
- To address the internal FDI attack on vehicle platoons, a trust-based method to complement Multiple Criteria Decision Analysis will be developed and implemented.

Chapter 2

Literature Review

The following chapter examines the vast amount of current literature on platoon cybersecurity. First, there is a brief section on the other methods of implementing platoon controllers. Next, it discusses how Vehicle to Everything (V2X) communications can be attacked in platooning before discussing current methods to prevent and mitigate attacks. The discussions will focus on Public and private keys, Intrusion Detection Methods and Trust Management in platoons. Discussing public and private keys is understanding and explaining current concerns with securely decrementing keys in a highly mobile ad hoc network. Intrusion detection methods are discussed as MCDA will function to identify potential intruders within the network and prevent them from impacting the performance of the platoon. Finally, trust management in platoons is discussed, as platoon members need to fully trust that others are fully cooperating with them and have no ill intentions for them. Using MCDA and trust, untruthful vehicles can be safely identified during platooning and ignored.

2.1 Other Vehicle Platoon Controllers

FLATBED is a CACC method created by Rima Al Ali et al. [19]. This controller model uses a unidirectional spring-damper model, which relies more on sensor information than CACC. The critical factor the controller seeks to keep constant is the inter-vehicle spacing. FLATBED can be imagined as each vehicle sits on the back of a virtual flatbed truck, hence its name. Therefore, by using the sensors more, the platoon is less susceptible to erroneous beacon information; however, it is slower to react to actions from the leader and requires more sensors and processing power than in CACC. The advantage of using FLATBED is that this controller can maintain a safe state even if there is a total loss of V2V, thus making it naturally resistant to some attacks.

As created by Jeroen Ploeg et al. [78], Ploeg uses a string-stable approach to maintain minimal gap error between two platooning vehicles. Here, the platoon controller uses V2V communications; however, the Ploeg method also uses onboard sensors, enabling it to main-

tain formation without communicating with other platoon members. Ploeg, therefore, has the same advantages and disadvantages as the FLATBED CACC method.

Consensus platoon controller, created by Santini et al. [83], uses a complex algorithm to enable platoon members to maintain platoon stability by following a consensus or average of other vehicles' actions. Unfortunately, the consensus method relies heavily on wireless communications, making it vulnerable to attacks targeting V2V communications. However, this method gets around this by calculating a consensus of what should be done. The weakness of this method is that it can have a significant gap error, mainly if there is any oscillation in the platoon driving.

2.2 Vehicle Platoon Wireless Communication threats

Vehicular platooning security threats are wide-ranging and diverse. In this thesis, only wireless communications threats are investigated, and physical threats to the vehicle are not considered. Even within this now smaller list of threats, there is a great range of attacks that seek to break one or more of the seven cryptography concepts: Authentication, Availability, Confidentiality, Data Verification, Integrity, Privacy, and Non-Repudiation.

Authentication

Authentication is a cyber security concept that is a method or mechanism that provides credibility that the node communicating with is truly that node. Authentication is achieved in various ways, such as with security certificates or using distinctive markers. These markers validate who the sender is and that they have permission to communicate.

Availability

Availability in platooning networks is the ability for platooning vehicles to connect, form, and maintain a network. Therefore, platooning vehicles must maintain access to information and data from each other, as well as RSUs and prospective members. Therefore, availability needs to be maintained at all times during platooning. However, there are times when availability may degrade naturally, such as adverse weather and physical barriers such as tunnels. In addition, an attacker can compromise the availability of a platoon network with jamming attacks or by Denial-of-Service (DoS) attack [108].

Confidentiality

Confidentiality in platoon communications means that only the appropriate platoon network node receives and, therefore, can use a beacon or other command. To achieve confidentiality in wireless communications, additional steps are needed to prevent any node that is a member of the network from reading the beacon.

Data Verification

Data verification involves constantly checking data using multiple messages and sensors. It is helpful to check that the messages propagating through the platoon domain are correct and, therefore, ensure the platoon's high integrity. In addition, data verification can also prevent errors from causing unintended consequences.

Integrity

Integrity is where the reliability of the information is assured, there has been no tampering with the message, and the message content is accurate. When an attacker compromises the integrity, there can be no way to guarantee the reliability or accuracy of the received communication without additional information [54].

2.2.1 Privacy

Privacy is essential in any network, and platoons are no different. For platoon networks, users and their vehicles should only expose or give away necessary information to enable platooning. All parties involved must also treat this information with care. All information should be destroyed after it is used and only kept for as long as needed. In addition, all information should be shared anonymously, thus enabling privacy to be maintained.

2.2.2 Non-Repudiation

Non-repudiation ensures that once a message is received, the sender cannot deny it and must take responsibility [41]. It can be achieved using a secure black box recorder-type device to resolve incidents and disputes.

There are various cybersecurity threats that vehicular platoon communications are facing [93]. Some of these are direct, aiming to disrupt or damage a platoon's integrity to make it less efficient and cause discomfort to passengers. Some attackers will seek to break up or prevent platoons' formations. Other attacks could be more subtle and seek to steal information about the users, vehicle, and load. Attacks on vehicular platoons can be classified in a range of different ways. One common approach is cryptography-related classification [71, 67]. Another approach for sorting attacks is by the layer they target in the communication stack, like in [42].

The security requirements for platoons are described below, with the attacks grouped into each attack's goal. Table 2.1 presents each attack identified in the literature, the attack's goal and the broken security requirement.

Attack Name	Short Summary of the Attack	Goal of the Attack	Effected Domain
Black Hole [65]	Compromises the Availability by not passing on messages to other members.	Platoon Disruption	Platoon
Collision attacks [42]	Compromises the Availability as the attacker deliberately causes message collisions and controls what packets are transmitted.	Access Management	Platoon
Denial Of Service [108]	Compromises the Availability of the network by preventing users from joining or creating a platoon.	Prevent Platooning	Platoon
Eavesdropping [62]	Compromises the Confidentiality of the network because an attacker can understand the information transmitted within the platoon. This can lead to data theft and privacy violation.	Data Collection	Platoon
Fake Manoeuvere attack [102, 84]	Compromises the Integrity of the network by creating fake manoeuvre requests for members in the platoon. This will destabilise and prevent users from using the platoon by breaking it into smaller platoons or creating entrance gaps for non-existent vehicles. Members can also be removed.	Platoon Disruption	Platoon
False Data Injection [101]	Compromises the traceability, data verification and integrity of the platoon as the attacker can inject fake messages to manipulate the platoon behaviour to there advantage.	Platoon Disruption	Platoon
Fake position attacks [42]	Compromises the Integrity of the platoon as the attacker reports to be in a different position in the platoon.	Platoon Disruption	Platoon

Flooding [106]	Compromises the Availability and Data Verification as the attacker overwhelms the network with more messages or data than is can handle.	Availability attack	Platoon
Illusion [42]	Compromise the Data Verification and Integrity of the platoon network as the attacker creates one or more ghost vehicles.	Platoon Disruption	Platoon
Impersonation [48]	Compromises the Integrity of the network by an attacker posing as a different individual in the network. This leads to false representation and reputation damage.	Access Management	Platoon
Information Theft [74]	Compromises the platoons Privacy as the attacker is able to capture data from platoon members.	Data Collection	Platoon
Jamming [95]	Compromise the Availability of the network as an attacker seeks to prevent all communications on platoon frequencies in the local area. As platoon members can no longer communicate, it will disband.	Availability attack	Platoon
Jamming and Spoofing Sensors [90, 74]	Compromises Authenticity and Availability of sensors. This is done using malware or directly attacking the sensor, which will lead to false sensing.	Platoon Disruption	Platoon

Table 2.1: *Threats to platoons and a summary of how the attack will compromise the platoon.*

2.2.3 Access Management

An Access Management attack occurs when attackers seek to manipulate access to the vehicular platoon or platooning service. Such attacks can control who can access and use platooning services and are closely related to Preventing platooning attacks. Access Management attacks can be achieved in many ways, including Impersonation, Sybil, and Manoeuvre attacks.

Collision Attacks

In Collision attacks, the attacker seeks to force packet collisions, which will result in the dropping of packets [42]. Therefore, collision attacks will result in members not receiving

packets, resulting in an integrity violation of the information transmitted, as discussed in the previous section [42]. As a result, such an attack can prevent some or all traffic on the network by a platoon.

Impersonation

An Impersonation attack is where a malicious node pretends to be another node in the network. To do this, an attacker must obtain another vehicle's ID. As such, an Impersonation attack compromises the integrity of messages in the platoon system. Whatever the malicious node does, others will think the user with its ID copied has done it [48]. Using a stolen ID can enable users or vehicles not paying for platooning service or for banned or poorly rated drivers to access the platooning service [48]. The impersonated user will see increased account use when the malicious node is impersonating them. There is also the potential for sudden dropouts from the platoon service provider needing clarification on two identical IDs being used simultaneously. The attacker can also commit other attacks without fear of reprisal when using a cloned ID [48]. All reprisals for the attackers' actions are taken by the cloned vehicle [48].

Manoeuvre Attacks

Platoon Manoeuvre attacks are fake entrance, fake leave, and fake split requests [102]. Fake entrance attacks can lead to gaps in platoons as members may open up to let new vehicles in without permission from the leader or leave space for non-existent vehicles [84]. In addition, this can reduce the number of member vehicles able to join the platoon as the leader thinks more vehicles are part of the platoon than there actually are [84].

Fake leave and split requests can cause platoons to break up, which will decrease the efficiency of the platoons even more [84]. In this case, the attacker can use this to become the leader to target and deny specific vehicles access to the platoon [84]. This can then lead to a denial of service attack on vehicles. Overall, Fake Manoeuvre attacks damage the Integrity and Availability of security characteristics.

Repudiation Attack

With Repudiation attacks, the attacker attempts to confuse the network by denying that they have received messages when there is any dispute over messages [22]. In platoons, it is believed that this can cause the system to assign the same identity to multiple vehicles [42]. However, this attack makes it almost impossible for network members to distinguish between members [42] or fully identify other vehicles. Furthermore, it enables the attacker to pretend to be other vehicles and manipulate the platoon [42].

Sybil Attacks

Sybil attacks [44, 43] are committed by malicious nodes that create one or more manufactured vehicles upon entering the platoon network and try to have these ghost vehicles accepted into the platoon [82, 48]. When the ghost vehicles are part of the platoon, they can destabilise it by creating gaps. The leader will also think there are more vehicles than there are, stopping new vehicles from joining. The attacker can take it further and try to take control of the platoon off the leader using the ghost vehicles [82, 48]. Overall, Sybil attacks break authentication as nodes cannot differentiate ghost vehicles from real ones.

2.2.4 Data Collection

In Data Collection attacks, the attacker will target the message transmitted between nodes to extract useful information about the vehicular platoon or vehicles in the platoon. The information can then be used or passed on to others. Therefore, Data Collection attacks naturally target the privacy of all platooning vehicles and nodes.

Eavesdropping Attacks

An Eavesdropper listens to and logs the communications of a network [62]. In platooning, the attacker can see the beacon that members use to maintain the formation. If the network uses encryption, the attackers must decrypt the message to understand the communicated data. The primary goal of this attack is to gain information about the platoon and the member vehicles [62]. Finally, an eavesdropping attack on the platoon compromises the privacy of the platoon network.

The attacker can use the information acquired to carry out another attack, such as Replay or Sybil, by knowing how the platoon needs beacon information and how to make the fake messages look authentic to the platoon [62]. In addition, it may show various aspects of the platoons' plans, such as rest stops and where vehicles plan to split up [62].

Information Theft

As a rule of thumb, information is precious. However, all collected information for platoons contains sensitive information about the platoon, platooning vehicles and drivers. The information can be gathered and used both legally and illegally [74]. When a vehicle is in a platoon network, it will be transmitting a multitude of information. The members will transmit information by beacons to other members, including status updates and routes to vehicle-enabling platforms via RSU and GPS pings. This information can be used in various ways, both to improve the platoon service or to target individual vehicles by criminals [74]. Platooning-enabling companies may sell some information to third parties to enable them to better target drivers with advertising. A current issue is who owns all this information: the driver, the fleet manager, the platooning enabling company, or another entity [74]? Not understanding who is legally responsible can lead to data leaks and misusing personal and

confidential information. This type of attack breaks the privacy of the attacked vehicle and driver.

Location Tracking

Location tracking attacks are where the attacker can track the position of a vehicle. Location tracking is achieved in one of two ways. The first way is by intercepting the GPS location information of a vehicle, and the second is by extracting it from the beacon. When intercepting the information from the GPS, an attacker is merely eavesdropping on the communications between the vehicle and the GPS satellites overhead. This type of attack breaks the privacy of the attacked vehicle. When the location information is extracted from the beacon, this breaks down confidentiality between platoon members. All members must remain anonymous in platoons [62]. Only the intended target of a beacon should be able to use the location information within the beacon.

2.2.5 Financial Gain

In a financial gain attack, the attacker will seek to directly steal or obtain financial information from the attacked platoon, vehicle, or service provider. Additionally, during an attack for financial gain, the attacker will compromise the confidentiality of the network or vehicle.

Malware Attack

Malware attacks on platoons can have catastrophic consequences for platooning capable vehicles, as they can shut down the whole network. In addition, malware attacks have the potential to prevent users from platooning and even potentially using affected vehicles. It's crucial to understand that malware attacks on platoons can present a diverse range of forms and goals, such as data collection and platoon destabilisation. This diversity and complexity of the threat further underlines the need for a comprehensive cybersecurity strategy. In such attacks, while any security requirement can be broken by a malware attack, in most cases, Availability, Confidentiality, and Privacy are broken.

The malware first needs to infect a vehicle's Onboard Computer; this can be done by connecting an infected device to a vehicle. CAV have many interfaces that an attacker can use to get the malware onto the vehicle [74]. These interfaces are the Onboard Diagnostic (OBD) port, CD drive, USB interface, Bluetooth, and the wireless communication network link [74].

CDs and USB interfaces can be exploited using an infected multimedia file. Mechanics and Engineers use the OBD port to pull the sensor. The CAN bus information off the vehicle and updates the vehicle's onboard computer. This information is beneficial for understanding the health and shape of the vehicle in great detail. It is also used to tune the vehicle and can provide firmware updates. As such, malware can be installed using this port. Finally,

an attacker can infect a vehicle by sending the malware using Bluetooth or other wireless communication links [74].

Ransomware Attack

One potential malware attack on platoons is a Ransomware attack. In this type of attack, an attacker can choose to hit individual vehicles, fleet management, or the platooning service itself. In such an attack, the attacker can lock out the platooning service and vehicles. If done on a big enough scale, such an attack has the potential to cause mass disruption. Therefore, this type of attack is a genuine threat to platoons and CAVs in general, as such attacks are becoming more high profile with such attacks on infrastructure and hospitals making worldwide news [24, 1, 58]. In such attacks, the attacker promises to release held computer systems, files and functions if a fee has been paid to the ransomer. Such an attack on platooning vehicles would result in vehicles being unable to use a platooning provider or, worse still, whole fleets of platooning-capable vehicles.

2.2.6 Availability attacks

When an attacker targets a platoon, they can do so with the intent to stop platooning altogether or at specific times. Additionally, such attacks can target specific vehicles or groups of vehicles. In such attacks, the attacker compromises the Availability of the platooning system, as nodes cannot join or form platoons.

Denial-of-Service (DoS) Attacks

DoS attacks can affect a platoon in one of two ways; the first is that the platoon service provider can be attacked, making vehicles unable to connect to them. The second is to target specific platoons. When targeting the platoon service provider, the attacker can prevent most, if not all, formed platoons from accepting new members, and no new platoons can be formed. An attacker can achieve this by swamping the provider with more join requests than it can handle. The downside of this method is that it requires a large amount of equipment and good technical knowledge to carry out.

The second method of targeting individual platoons and vehicles is very realistic. Platoons will likely have a maximum number of members that can join. This reduces the complexity of the attack as the attacker only needs to fabricate up to that many vehicles to prevent new members from joining [108]. This is because the leader will think that there are more vehicles in the platoon than there are [108]. Such attacks can be made using copied or fake vehicle IDs to connect multiple ghost vehicles to the platoon.

Flooding Attack

Flooding attacks on platoons are where an attacker exhausts the network resources, thus preventing communications from taking place [106]. There are two types of flooding attacks:

data flooding and routing control packet flooding. In data flooding, the attacker creates and transmits too many packets for the network to handle [42]. For routing control packet flooding, the attacker will send routing requests to all nearby connected vehicles regardless of whether they are part of the platoon [106]. The result is that platoon members cannot communicate with each other, thus breaking up the platoon. The attacker compromises the network's data verification and availability by performing such an attack.

Jamming Attacks

Jamming attacks can be complex and straightforward, with the attacker preventing a platoon from maintaining communication [95]. Jamming attacks target the Physical Layer by flooding the channels with random noise, preventing platooning communications [95]. As a result, platoon members cannot communicate with each other reliably, leading the platoon to break up or take other measures to prevent an accident [95]. When the platoon is jammed, there is a chance that a collision can occur between members. The attacker can act smartly and target individual messages or block specific channels and jam communications until the platoon breaks up and stops until the platoon reforms. In addition, the platoon will lose any benefits it had for platooning each time it breaks up or adjusts for safety.

Worm Hole Attack

Wormhole attacks are where two vehicles form a private communication link and pass messages to each other. The two vehicles in question are far from each other, so by doing this, they exclude one or more vehicles [71]. Such attacks could be very problematic for very large platoons. Wormhole attacks will cut out the vehicles between the two attackers and manifest as a DoS attack [71] for the missed vehicles. Having two non-neighbours exchange communications as if they were neighbours will lead to the exclusion of the cut-out vehicles, which will cause them to become ejected from the platoon or cause a collision. A Wormhole attack will damage the availability of the platoon.

2.2.7 Platooning Disruption

Platooning disruption attacks target platoons to disrupt and make them inefficient. Platoon disruption attacks can lead to a wide range of outcomes to prevent platoon members from gaining the benefits of platooning and making the experience unpleasant for passengers.

Black Hole Attacks

A Black Hole attack is when a malicious node receives packets from the network and will not re-transmit the information to others in a routing network [41]. By doing so, the malicious node prevents other members from receiving information in a timely manner [65, 15]. As the members communicate closely together, vehicular platoon members can talk directly with

other members. This attack could still severely affect decentralised and bidirectional communication topology methods of platooning. Using decentralised and bidirectional topology, the attacker could prevent messages from going further down the platoon, leading to platoon destabilisation. By doing this, the attacker is affecting the availability of messages in the network.

Fake Data Injection (FDI) Attacks

A fake data injection attack (FDI) is when a malicious node creates a fake message and transmits it into the network [101, 93]. To do so, the attacker needs to create a packet in the same format as the network it is attacking transmits. This can be done by being a network member or copying a message format from a captured packet. Such attacks can disrupt platoons as members act upon fake information, which will degrade the platoon's stability. Additionally, this will affect a platoon's traceability, data verification, and integrity.

Fake Position Attacks

Fake position attacks can disrupt the stability of a platoon as the attacker transmits fake position coordinates into the platoon network [42]. This misleading information will change the perceived order and position of vehicles in the platoon, leading to vehicles getting messages late due to altered message routing [42], damaging the integrity of the platoon network. In addition to routing changes and delays, this can lead to inaccurate information being used by members or even enabling the attacker to receive the information they would typically not be able to access, thus compromising privacy and integrity.

GPS and Sensor Spoofing

Platoons like CAVs have many sensors that supply information about road conditions, vehicle conditions, and other traffic to the onboard computer. Additionally, GPS provides accurate vehicle positioning. Unfortunately, every sensor on a vehicle can be compromised. For example, high-powered torches and lasers can partially or entirely blind cameras [74]. Natural and accidental threats, such as strong sunlight, dirt, and dust, can also affect cameras, creating sensor blind spots. This can prevent the vehicle from reacting in time to hazards, leading to incidents.

GPS is vulnerable to jamming and spoofing attacks, also known as tunnelling attacks [42]. The attacker copies the GPS transmission before replaying it, slowly moving the position away from the vehicle's location. During this time, the strength of the fake signal must be stronger than the original one as GPSs are often set up to take the strongest signal as the true original message [90]. Jamming a vehicle's GPS can be done like jamming other wireless communications. Such attacks can lead to vehicles being unable to platoon effectively, as platooning relies heavily on accurate location data to maintain coherence. Thus, the attack can damage the data verification and integrity of the platoon.

Illusion Attack

An Illusion attack is where the malicious node transmits false or misleading information into the network. For example, the malicious node will create fake messages about traffic conditions, driving conditions, and members [66]. An Illusion attack can also affect the MAC layer and disrupt the cooperation of MAC protocols. The attack can result in traffic jams, accidents, a decrease in the performance of a platoon, and degrading the integrity and data verification within the platoon network.

Message Altering Attack

Alteration attacks target the information within a message when relayed between members [38]. The effectiveness of this attack depends on the topology of the platoon. As with Black Hole attacks, this attack works best against decentralised and bidirectional topology as messages are routed through the attacker. The attacker could also delay the re-transmission or change the order of messages instead of changing the actual message content itself [38]. The effect of this is that member vehicles will get out-of-date or inaccurate messages, which will compromise the integrity of the network. This will lead to a reduction in the stability of the platoon as members will be reacting to old or altered messages.

Replay Attacks

Replay attacks are where the attacker replays old messages back into a platoon [25, 95]. As discussed before, replay attacks will cause the platoon to become unstable as members react to the replayed message. The instability of the platoon can cause several problems, such as significant gaps or oscillation of the platoon, resulting in decreased efficiency. In addition, replay attacks will affect the privacy and integrity of the platoon network.

2.3 Methods to prevent Attacks to Platoons

This section explains the range and use of security mechanisms and countermeasures proposed in the literature to the attacks identified in Section 2.2.2 concerning platoons. In addition to presenting the countermeasures, the section will discuss the advantages and disadvantages of using each security method. Table 2.2 introduces each countermeasure and briefly summarises what it counters, how it works, and the open challenge it faces.

2.3.1 Private and Public Keys

Platooning networks can use encryption keys to prevent non-member nodes from understanding messages between members and ensure that only authorised nodes in the network can read other messages. Encryption keys are classified as (1) *Public key:* known by many nodes in a network or all of them. (2) *Private keys* are known only by a few nodes that regularly communicate. Using encryption like this forms the public key infrastructure (PKI) [92].

Table 2.2: *Vehicular Platoon defence methods identified from the literature.*

Security Mechanism	Security Attribute Secured	Open Challenge
Secret and Public Keys	Authentication, Confidentiality, Integrity and Privacy	Large scale testing of current methods of key creation and distribution to compare effectiveness against the cost.
Roadside Units (RSU)	Availability and Data Verification	More research into RSU network deployment and identification of rouge RSUs.
Control Algorithms	Authentication, Data Verification, Integrity and Non-repudiation	Where in the network is the most efficient to deploy and use the algorithms.
Hybrid Communications	Availability, Data Verification and Integrity	The use of VLC and wireless radio communications between V2I is lacking.
Trust-Based methods	Authentication, Confidentiality and Integrity	Requires connection to a trusted authority for management and distribution of trust values.
Blockchain	Authentication, Data Verification, Non-repudiation and Integrity	Reducing computational power required for large networks and maintaining privacy.

For PKI to work, member nodes must agree on a shared or group of standard keys to use [92].

Both public and private keys work by encoding a message with predetermined algorithms; the algorithm used is the key. The keys may also add information to the message, such as security certificates, credentials, and time stamps [71, 92, 67, 61, 17, 63, 62]. The additional information can be used to prevent replay attacks and give the receiver assurances on the message's validity [61, 67]. Public keys help to prevent a range of attacks on platoons, such as eavesdropping, False Data Injection Information Theft, and False Data Message Altering [61, 71, 92, 49, 67, 59].

The challenge with keys, specifically private keys, is how to share keys between nodes to prevent an attacker from obtaining the keys. One proposed method uses the Received Signal Strength (RSS) as a method to use inherently random spatial and temporal variations of the reciprocal wireless channel to extract a secret key from that [61, 63, 62] to quickly and securely distribute private keys amongst members, even in the presence of an attacker. The method works as multipath fading can be quantised, and this new digital signal can be interpreted as a key [61, 63, 62]. Using this method, no key is ever transmitted; therefore, an attacker cannot capture the key. Furthermore, the attacker cannot obtain the key by eavesdropping on other communications as the fading is different for each receiver in the network and changes regularly due to variations in relative vehicle positioning. The challenge with this method is that it requires additional antenna and computing abilities on all network nodes, thus increasing costs and complexity.

Another proposed method is Convoy Protocol [46]. Here, two nodes that want to share a private key will use accelerometer data and a fingerprint extraction function to create the private key [46]. However, the method still relies on transmitting the key to check and form an agreement on the key. Then, the fingerprint is applied to add an element of randomness

to the key and prevent an attacker from guessing the key [46]. In other cases, the sensor information creates private keys between vehicles, as seen in [104]. Gyroscope and accelerometer information is extracted from a shared private key using a fingerprint extraction function [104]. Using two sensors makes it more challenging to replicate by the attacker than if only one sensor is used. However, it relies on the sensors being calibrated properly and correctly. Using sensors to generate and maintain keys relies on the sensors being well-maintained and calibrated correctly to ensure accuracy, as any variation will lead to keys needing to be generated correctly.

2.3.2 Roadside Units

Another way to coordinate platoons and distribute private and public keys is to use roadside infrastructure as part of the network, RSU. RSUs can provide a link point between platooning vehicles, road users, and companies providing platoon services [59, 45] as part of a wider internet of things and smart city construction. The advantage of using RSUs is two-fold. First, they can serve as middle-man to communicate up-to-date information to vehicles and the Trusted Authority (TA), enabling improved connectivity. Secondly, they can monitor the driver's behaviour within the platoon network, ultimately detecting various attacks, including Sybil attacks [39].

RSUs can, therefore, act as 'middle-men' to distribute private and public keys to vehicles wishing to form, join and maintain platoons [59, 82, 42]. However, the RSU has limited authority. Its primary role is to improve situational awareness of vehicles and platoons and be an access point to the platooning network and other services [59]. In some cases, the RSU creates the secret keys; in others, it is just public keys. Using RSUs to distribute and coordinate keys and platoons enables the trusted authority much better control over who has access to the keys and, therefore, platooning services so that anomalous users can be screened out. For this approach to work, the nodes wanting to connect must be within range of an RSU and, ideally, the same RSU. The issue with this method is that if there is no RSU in the range of the vehicles, the keys cannot be updated or issued to vehicles. Finally, the keys are vulnerable to eavesdropping attacks from the attacker when the keys are being transmitted.

RSUs are still susceptible to damage, failure, and attack. The open challenge with them is identifying and removing faulty RSUs quickly and reliably without damaging the network. Another open challenge is handling areas of the network with a low density of RSUs where platoons can not rely on them to update them from a TA.

2.3.3 Control Algorithms

In vehicle platooning, it is vital to detect abnormal behaviour of platooning vehicles. By detecting abnormal behaviour, the vehicle can alert the driver or take corrective steps to prevent damage to the platoon's integrity. The software enabling the vehicle to detect abnormal

behaviour is often called a control algorithm. These algorithms can reduce the impact of Sybil, replay and manoeuvre attacks, and many others that disrupt the expected behaviour of platooning members. In addition, the algorithms detect damaging behaviours and communications caused by these attacks [77, 48]. Control algorithms check sensor and communication information using them to adjust and correct any abnormal behaviour.

Platoon control algorithms can work together collectively where each vehicle exchanges sensor information and positional information between members [77]. This information can then be filtered and statistically processed to identify and prevent potentially damaging behaviours [77]. Methods of platoon control algorithms, such as FLATBED, are also implemented in specific platoon controllers. Control algorithms give the platoon controller natural resistance to such attacks. An Adaptive Sliding Mode Observer method has been proposed to counter attacks involving the data communicated between members [52]. It is assumed that vehicles can sense the vehicle in front position and velocity using frontal sensors and the intended acceleration of the vehicle using V2V communications. The approach uses past behaviours to predict what the vehicle will do. That is then used to identify attacks and reduce the magnitude of the impact of the attack [52]. An Adaptive Sliding Mode Observer relies on access to a range of forwards-facing sensors that can be used to observe the preceding vehicle, which themselves can be attacked.

Packet Delivery Ratio (PDR) can indicate whether a platoon is attacked [23, 72]. PDR can be used to detect jamming attacks as there will be a rapid change to the PDR in the MAC layer in any given period [72]. A vehicle can be considered jammed when the PDR rate exceeds or exceeds the decrease rate threshold. If the PDR value is equal to or below the PDR threshold, and if the PDR decrease is positive, the value is not equal to zero. If these conditions are met, the node will warn others that it is jammed [42] before taking action to maintain its safety and the safety of others. To maintain safety, the jammed vehicle or platoon will stop using CACC in favour of ACC. The disadvantage of this method is that while the platoon maintains safety when jammed, the platoon is disbanded still.

2.3.4 Trust Based Security Management

Trust is an essential part of communications [12, 14], which becomes even more essential when used in platooning as platooning vehicles must work together cooperatively [4]. Trust in platoons is a numeric value representing the reliability of the past behaviour of a platooning-enabled vehicle. In many trust-based systems, vehicles will provide feedback on their experience communicating with other vehicles. In this way, trust can be used as a security measure to identify and remove potential attackers from the platoon network.

Platooning trust-based systems depend more on having high trust values between nodes than other CAVs [48]. Therefore, a high trust value overall will be a highly desirable trait to a platooning node [48]. In vehicle platooning, the trust value is almost always issued by

TA [107]. Using TA to calculate and issue the trust values requires RSUs to collect feedback information from platooning vehicles about the vehicles they were platooning with. In VANET, however, vehicles can build their trust values for vehicles close to them and manage them [13, 16]. The creation of trust in using these methods would be impractical for platoons as the extended set-up time establishing trust between members will reduce the efficiency and safety of the platoon.

More trust models must be proposed for platoons to achieve security within vehicle platoons. For instance, the REPLACE trust model presented by Hu et al. [48] relies heavily on a TA, which handles requests and access to the server. The server stores and calculates the trust scores stored in feedback data tables. The RSUs act as an intermediary between platooning vehicles and the trusted authority. In this role, they constantly update the servers with up-to-date trust values for the trust tables. Finally, the vehicles themselves are divided into three categories: platoon leader vehicles, which are platoon leaders, and potential platoon leaders. Potential users can become platoon members but cannot be considered platoon leaders. Finally, there are User vehicles, which are platoon members.

The REPLACE method aims to create a reliable platoon recommendation service, prevent malicious user use and abuse, and make accurate judgments and evaluations of platoon leaders. To calculate trustworthiness, a Dirichlet-based model accounts for historical data about the trustworthiness of the vehicle, enabling a quick recovery from a small one-off change in feedback but a far, much longer recovery from continuous low feedback scores. Overall, the REPLACE method works well in creating a database of trust values for all users. Low-trusted users could have their positions within a platoon restricted or unable to connect to a platoon. On the other side, members with high trust values are grouped, enabling members to trust each other. The disadvantage of such a method is impersonation attacks where an attacker can disguise themself as another vehicle and then reduce the trust score of the cloned vehicle.

The Trust-based and Privacy-Preserving Platoon Recommendation (TPPR) scheme proposes a way to use a trust-based system while preserving the privacy of vehicles in the network [107]. The format of TPPR is very much the same as that of REPLACE. A TA is in charge of maintaining the trust values and predicting future values based on historical data. The service provider enables the connection of the RSU to a more extensive network and enables user feedback and trust values. In TPPR, a truth discovery-based evaluation algorithm is used to calculate the reputation scores of header vehicles. RSUs again act as intermediaries, identifying users in the network and relaying information between the nodes and the service provider. This time, there are only two vehicles: header vehicles or platoon leaders, and the second is user vehicles, which are member vehicles.

The main difference between TPPR and REPLACE is that TPPR uses pseudonyms and the Paillier cryptosystem to improve the privacy of member vehicles. In addition, TPPR uses its method to evaluate the trust score of leader vehicles. However, this method's primary

focus is to preserve the privacy of member vehicles, which REPLACE does not do.

Vehicle platoons that use trust-based algorithms for regulating and selecting vehicles to platoon together are shown to be resistant to attacks where false or misleading information is injected into the data stream, such as FDI attacks [48, 107]. Trust systems provide additional authenticity and integrity, with the trusted authority telling members whom to trust.

2.4 FDI Attack Solutions

FDI attacks on vehicle platoons can be categorized into the following types: (1) Internal FDI, where the attack is from another member of the same platoon; (2) External FDI – where the attacker is not part of a platoon. Garlichs et al. [40] propose TriP as a trusted method in platoon networks to detect misbehaving platoon nodes in the presence of insider FDI attacks. This method compares what nodes are saying and what they do. Based on this comparison, the trust value is calculated. If trust drops below a threshold, the vehicle will stop acting on the information an untrustworthy vehicle gives. The challenge presented by TriP is keeping vehicle information secure and anonymous within a network.

In addition to trust, vehicle platooning disruption attack detection algorithms can detect FDI attacks from internal platoon attackers. One such solution is proposed by Bermad et al. [25], where a reputation-based model is utilized to identify attackers damaging the integrity of the platoon. First, attackers are identified by verifying vehicle locations within the platoon, keeping them within a known tolerance. Further, the location of each vehicle is tracked throughout the journey. Suppose anomalies are detected in the vehicle location information. In that case, the system classifies it as an attacker. Finally, a reputation-based, reliable mitigation algorithm is used to discard fake or untrustworthy beacons. The drawback is that there needs to be an evaluation of the approach's effectiveness at dealing with attacks on the platoon, such as comparing it to other existing methods or just comparing it against if there was no defence.

Although creating a secure defence against FDI attacks is vital, it is also essential to understand how vehicular platoon controllers react when subjected to FDI attacks. Heijden et al. [97] investigated the impact of an FDI attack on different platoon controllers at varying inter-vehicle distances and speeds. The experiment investigated how the platoon is affected due to false speed, acceleration, and position values. This thesis shows that the consensus controller is the most resistant to FDI attacks. This was because CACC and Ploeg relied on information from the lead and preceding vehicles. In contrast, the consensus controller receives information from many vehicles and is less susceptible to a rogue vehicle; however, a comprehensive look into how FDI attacks can disrupt a vehicle platoon is presented, although there is no solution to FDI attacks.

Dutta et al. [35] investigated FDI attacks on vehicle platoons due to compromised sensor data. They propose to use a Resilient Distributed State Estimator (RDSE) to defend against FDI attacks in a scenario where multiple sensors are compromised. However, the performance of resilient distributed state estimators usually decreases when the number of corrupted sensors in the system increases. Therefore, Yu et al. [105] proposed a fast and resilient distributed state estimator. In this technique, bounded state estimation errors are still produced, no matter the magnitude of the attack or how many sensors are compromised. The main advantage of this mechanism is that it is computationally faster than other existing methods.

Some studies also addressed outsider FDI attacks in vehicle platoons. For instance, Biroon et al. [28] proposed a new approach by enabling the partial differential equation model to include traffic density. The proposed solution measures the change in the traffic density to detect FDI attacks and the position of the attack within the platoon. To identify the position of attack, the leader observes all members in the platoon, thus enabling it to determine the location of an attack. This approach effectively identifies an FDI attack on a platoon when considering ideal road conditions.

Another proposed solution by Zhao et al. [109] is a cloud-based sandboxing framework to detect FDI attacks in platoons and CAV networks. While the approach itself is not novel, its application to vehicle cyber security is, as it is traditionally used in computer security. The sandbox framework isolates and evaluates data exchanged in the network that affects the vehicle control systems. From this, abnormalities in data are identified as an FDI attack. The solution is tested in the VISSIM traffic simulator and shown to be able to successfully detect and identify an FDI attacker in real-time and under $0.2s$. However, only the ideal communication channel is considered, which is the main drawback of this study.

Xuan et al. [103] proposed a robust method for detecting FDI attacks at both the network and component levels. There are two complementary systems; the first is applied to individual nodes in a network and checks for corrupted sensor readings and actuator signals. At the network level, the second target nodes are corrupted by a potential FDI attack. This is achieved using a model-based detection and identification algorithm using a class of discrete Linear Time-Invariant systems and using delays from an observer called Generalized Luenberger Observer (GLO). The observer creates a tight residue binding. As a result, the residue no longer satisfies the binding during an attack and can detect the false beacon. However, the method does not revoke FDI attacks.

Table 2.3: *Related papers discussing FDI attacks in Platoons.*

Paper	Year	Theme of the Paper	Attacker Model
Heijden et al. [97]	2017	Investigating the effects of FDI attacks on platoons	Internal attacker
Bermad et al. [25]	2019	Vehicle platooning disruption attacks detection algorithms	Internal attacker
Dutta et al. [35]	2020	Resilient Distributed State Estimator (RDSE)	Internal attacker
Yu et al. [105]	2020	Propose the use of a fast, resilient distributed state estimator	External attacker
Wang et al	2020	Reducing computational power required for large networks and maintaining privacy.	External attacker
Biroon et al. [28]	2021	Traffic Density in addition to existing partial differential model	Internal attacker
Cabelin et al. [29]	2021	Machine learning using Support Vector Machines (SVM)	Internal attacker
Zhao et al. [109]	2021	Cloud-based sandboxing	Internal attacker
Xuan et al. [103]	2021	Model-based detection and identification algorithm	Internal attacker

In a nutshell, various studies are conducted to tackle FDI attacks in vehicular platoons. However, in this literature review, most current methods have various challenges in revoking the FDI attacks in platoons. Furthermore, very few studies have been conducted to study external FDI attackers. In this paper, we proposed a novel method to select the best beacon based on two Multi-Criteria Decision Analysis (MCDA) techniques, which can detect and reduce the impact of FDI attacks efficiently. Table 2.3 compares our study with the related works.

Chapter 3

Research Methodology

The research method applied here is Quantitative, as the research will be carried out predominantly through experimentation and statistical analysis of results. As discussed above, the aim is to identify high-risk attacks (such as FDI) on vehicle platoons. Therefore, the first step will comprise an extensive literature review that will explore current attacks on the wireless communications of vehicle platoons and the existing methods to prevent attacks on the wireless communications of vehicle platoons. With this understanding of the vulnerabilities of wireless communications in vehicular platoons and the currently proposed defence mechanisms, the next step will be to evaluate the risk of each attack. The risk an attack poses is worked out by conducting a comprehensive risk assessment, completed using the SAE/ISO 21434 standard. The justification for carrying out the risk assessment is to understand what attacks are high-risk and, therefore, of significant concern. The next step is implementing one or more high-risk attacks identified from the risk assessment in a platoon simulation. Finally, the attack's implementation will identify the risks to the platoon, such as the attack's safety, stability, and environmental impact. With the attack implemented in the simulator, it is then possible to create and test the proposed solution methods in the simulator and compare them to those of already existing solutions.

3.1 Simulation Environment

The main simulation software used is called Plexe. Plexe is an open-source simulator explicitly designed to model, implement and evaluate the performance of vehicular platoons [85]. Platoons are realized on a map of $650km \times 250km$ where the roadway is a four-lane highway-type road that is perfectly straight. The used dimensions mean the platoon will have sufficient roadway during the simulation. If this was smaller than for longer tests, the platoon could run out of the road. A mobility trace is created using SUMO [89] for an eight-vehicle platoon with one leader and seven members. When external attackers or vehicles are required, one or more human-driven vehicles can also be added, as well as additional platoons. OMNET++ is a network simulation software, and Plexe uses this program to handle the wireless communications between vehicles and any RSUs.

3.1.1 Plexe

Plexe is an extension of the Veins vehicle network simulator created to simulate realistic simulations of platoons. Veins is an open-source CAV network simulator that has been around since 2006 [85] and is under constant development even though the initial project to create it has finished. Veins are used in academic research, research and development in industry and governmental bodies [88]. Plexe has libraries for simulating the handling of IEEE 802.11p protocol for wireless communications in VANET and has an example code for a user to use to get familiar with the environment. The software also links smoothly with others, enabling various ways to assess and analyse the simulations.

Veins, an open-source framework, is designed to run vehicular network simulations. It is built upon OMNeT++ and SUMO, two other open-source tools known for their adaptability. OMNeT++ is a well-established open-source, extensible, modular, C++-based simulation library and framework designed to simulate networks. It contains the libraries and component architecture to create network simulations and is widely used to do so in the vast user community that includes industry and academia. SUMO, or Simulation of Urban MObility, is an open-source simulation software used to simulate road vehicle interactions on actual and proposed road networks. SUMO supports route finding, visualisation, network import and emissions calculation. The architecture of Veins, shown in figure 3.1, demonstrates the flexibility of these tools, how they interact with one another, and what each program contributes.

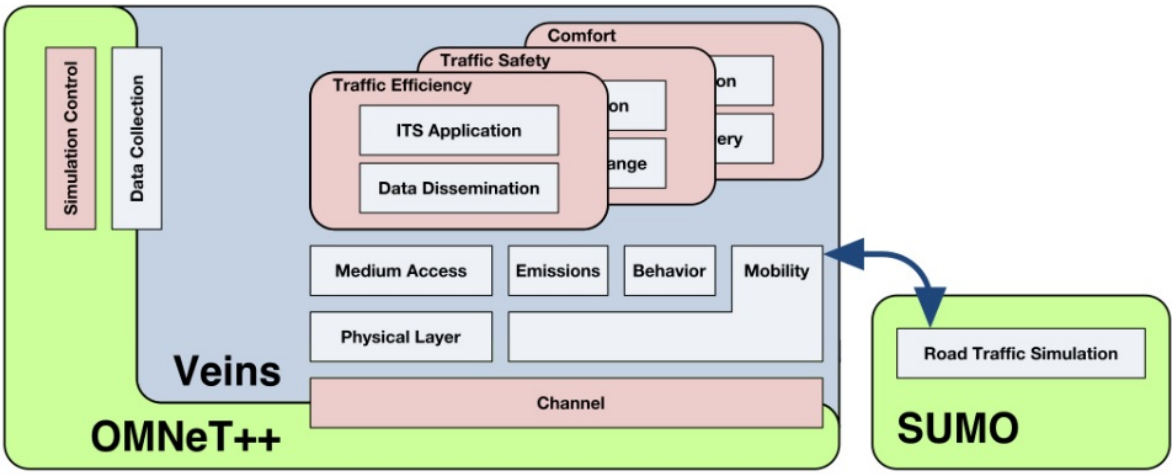


Figure 3.1: *The architecture of Veins and its interactions between SUMO and OMNeT++ [88].*

Plexe provides platooning files and libraries, extending the capabilities and enabling the support of platooning within Veins [85]. Plexe is only responsible for handling the platooning systems of the simulation, such as platoon controllers and behaviours, as well as beacon construction, use and structure [85]. Several different platoon scenarios can be easily simulated, such as simple platooning scenarios, eavesdropper attacks and FDI attacks. Plexe is advantageous over other simulators, such as NS3, as it is specifically created to simulate

vehicle platoon communications and behaviours, whereas NS3 is a potent network simulator tool.

3.1.2 Platoon Behaviour Model

The platoon has certain behaviours and assumptions that it will use to make the simulations easy to understand. First, the platoon is already formed when the attacker starts their attack, and no vehicles join or leave the platoon during the simulation. This is to test the effects of attacks and defences under the most common platoon operating condition, steady state platooning. The platoon controller used is CACC, as described in the California path project [86]. The Leader vehicle can maintain a secure connection to all platoon members during the experiment and only transmits accurate information in its beacons. The leader also remains the same. It is also assumed that all sensors onboard and all platooning vehicles are fully functional, working, and calibrated the same.

As such, each member vehicle can pass on accurate and truthful information in its beacons. There is also only one platoon, and all member vehicles are the same type of vehicle, in this case, an Articulated Lorry. The target platooning speed of the platoon is $80kmph$ with an inter-vehicle distance of $15m$ [36]. The MAC and Network protocol are standard unmodified IEEE 802.11p and WAVE, respectively. A platoon beacon will use all standard security credentials in the Security Services (IEEE 1609.2) for the application and network layer. The beacon will contain the vehicle's *speed, Controller Acceleration, Acceleration x and y coordinates and time the beacon was created*. The radio propagation model is a Two-Ray Interference with a packet size of $200bits$. The message bit rate used is $6Mbps$, and the packet loss rate is 0.2. This information is also available in Table 3.1 along with additional information about the general simulations. It is also assumed that when using any defence method, every member vehicle can use the defence method, and it is permanently active.

3.1.3 Attacker Behavior Model

An attacker will be needed to simulate the attack on the platoon. The attacker must conform to rules and assumptions called the attacker model. The attacker's model will change depending on the attack scenario, although some conditions will be constant throughout the experiment. As shown in Chapter 2 for vehicle platoons, there is a significant amount of work surrounding the secure sharing and agreement of security keys. This is needed to prevent attackers from obtaining the keys and, therefore, breaking the authentication and privacy of the wireless communication network in the platoon [61, 63, 62, 46, 104]. This thesis acknowledges that platoons would employ one or more methods to maintain authentication and privacy on the network in the real world. This thesis aims not to test the resilience of such methods but to explore supporting methods of quickly detecting and rejecting fake or harmful beacons from a potential attacker as an intruder detection method. Therefore, the external attacker is assumed to be able to create beacons that interact with a vehicle in the platoon. For internal attackers, it is assumed that a legitimate vehicle turns rogue or has

Table 3.1: *Simulation Parameters*

Parameters	Value
Simulation Time (secs)	$1000s$
Simulation Area (km $\times$ km)	650km $\times$ 250km
Total Number of Vehicles in Platoons	8
Human-driven Vehicle (Attacker)	1
MAC Protocol	IEEE 802.11p
Network Protocol	WAVE
Radio Propagation Model	Two-Ray Interference
Packet Size	$200bits$
Ideal Inter-vehicle Distance	$15m$ [36]
Platooning Vehicle Speed	$80kmph$
Message bit rate	$6Mbps$
Packet Loss Rate	0.2

some malfunction, leading it to create beacons with misleading information. The attacker is within range of the platoon to be able to secure a connection to the platoon network at all times when attacking.

As both external and internal attacks are considered, it is essential to highlight the difference between the two types of attackers. An external attacker is modelled as a non-platoon member vehicle driving at the same speed as the platoon in the next lane to the platoon or in the same lane as the platoon in front or behind the platoon. On the other hand, the internal attacker is restricted to attacking the vehicle directly behind them as the platoon uses CACC platooning, which uses a Predecessor-leader following communication topology.

External Attacker

The external attacker has three attack scenarios and two attack modes. The two attack modes are ((1) *Constant FDI* and (2) *On-Off FDI*).

Mode 1 – Constant FDI Attack
In addition to the abovementioned behaviours, the attacker continuously transmits fake beacons into the platoon network throughout the simulation. The attacker also increases the speed of the beacon by $0.5m/s$. Therefore, every beacon that the attacker transmits will contain the fake speed value. Finally, to ensure that the attacker's beacon is used, the attacker will spoof the ID of node 1, the first member vehicle in the platoon.

Mode 2 – On-Off FDI Attack
The attacker will attack the platoon for about $30s$ before stopping for around $30s$ to remain undetected. The attacker will then start to attack again, cycling through periods of attacking

and not attacking. In addition, the attacker will add $0.5m/s$ to its speed component during its cycle. This adds a layer of instability to the attack. Finally, again, the attacker will spoof the ID of node 1, the first member vehicle in the platoon.

The three attack scenarios are (1) *Single Attacker Multiple Victims*, (2) *Multiple attackers Single Victim* and (3) *Multiple Attackers Multiple Victims*.

Scenario 1 – Single Attacker Multiple targets
A single attacker attacks two or more member vehicles in the platoon. The attacker's time is spent attacking each vehicle equally, achieved by changing the spoofed ID used for each false beacon created. The spoofed ID cycles through each victim in order of the closest to the leader, e.g. ID2, then ID3.

Scenario 2 – Multiple Attackers Single target
In this scenario, multiple attackers cooperate to attack a single-member vehicle in the platoon by spoofing the same member ID. The attackers seek to flood the platoon network with false beacons targeting a single vehicle, reducing the effect of any true beacons received by the victim vehicle.

Scenario 3 – Multiple Attackers Multiple targets
In this attack scenario, multiple attackers again cooperatively attack the platoon, but instead of attacking a single vehicle, they each target a different member vehicle. As such, each attacker is spoofing the ID of a different member vehicle; this type of attack means that the leader has diminished control of the platoon as the attackers double the member vehicle messages to the attacked vehicles, creating conflicting driving behaviours.

Internal Attacker

The internal attacker is different to the external attacker and, as such, uses similar but different attack scenarios. The three attack scenarios used for the internal attacker are (1) *Constant FDI* and (2) *On-Off FDI* and (3) *Random Attacker Random Attack Period.*

Scenario 1 – Constant FDI
One member vehicle will attack the platoon throughout the simulation time. The test is designed to be a deliberate act by the attacker, not as a damaged sensor or other problem that could alter the beacon information. The attacker will increase the speed of the beacon by up to $0.5m/s$. Having such a significant change means that the attacker can quickly cause disruption and cause a collision in the platoon.

Scenario 2 – On-Off FDI
One member vehicle will attack the platoon intermittently in a two-minute repeating cycle like the external On-Off attacker. The test is designed to represent a damaged sensor or other problem that could alter the beacon information, as the attacker's impact on the platoon will

be most significant at the beginning of the platoon. Hence, the previous rules about the positioning of the attacker are still the same.

Scenario 3 – Random Attacker Random Attack Period

In this final scenario, a known number of attackers in random positions will attack at random intervals for up to two minutes at a time. This means that any member vehicle can become an attacker and that the attacks are of random time lengths; this represents an intermittent fault or error on any member vehicle or an advanced On-Off attacker attempting to hide in the platoon.

3.2 Multiple Criteria Decision Analysis

Multiple Criteria Decision Analysis (MCDA) or Multiple-Criteria Decision-Making (MCDM) is a mathematical method used in decision-making. When using MCDA, each choice is compared against the other using a standard set of shared attributes. MCDA has a wide range of applications from business planning to infrastructure development and construction; examples of it are also used in cyber security [26, 18].

Beacon selection is crucial as the receiving vehicles must act upon the information transmitted by the beacon. In this study, we utilized Multiple-Criteria Decision Analysis (MCDA) [94] to select the beacon. These techniques are helpful as they enable the system to detect the fake beacons immediately before the attacker can cause damage to the integrity of the platoon. The system can then suppress the attack by revoking the fake beacons and determining the probabilistic best beacon for a platooning vehicle to act on to maintain its platoon position even when under an FDI attack.

MCDA can be applied to platooning to identify and exclude beacons that appear anomalous compared to other beacons a member vehicle receives. Beacons contain many attributes that can be used in MCDA comparison that a malicious actor may want to alter; these attributes are the beacon information itself. Five beacon components are used for MCDA: Speed, Acceleration, Controller Acceleration, Location and Time. By comparing the values using MCDA in the beacons from the Leader beacon, the Current beacon and the Previous beacon, any abnormalities can be identified within the Current beacon by producing a numerical value for the optimal choice.

In this thesis, MCDA is proposed to enable member beacons to quickly identify, reject and replace beacons that do not conform to expected attribute patterns by identifying anomalies and inconsistencies within the beacon attributes data to identify fake or misleading beacons. MCDA will produce a score for each beacon between one and zero. One means that this beacon is mathematically ideal to be used by the vehicle and the best that it can be, while zero means that the beacon is mathematically the worst choice available. The beacon that scores closer to one is the most similar to the others, while a beacon that scores zero will be very different from the other choices. The score for each beacon is then augmented by the

trust method based on the trustworthiness of the source of the beacon. Finally, the beacon with the most significant score is deemed the best for the vehicle. That beacon is the one that is passed to the platoon controller within the vehicle. This is all detailed in figure 3.2.

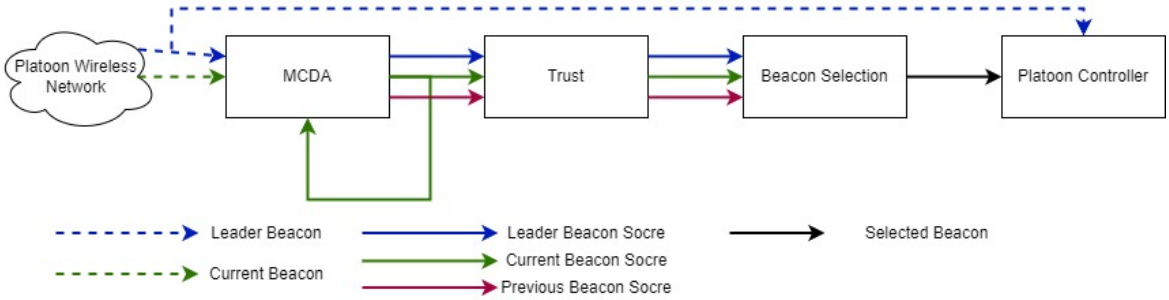


Figure 3.2: *Block diagram showing the way that beacons are assessed by the member vehicles.*

Table 3.2: *Beacon Characteristics*

Platoon Beacon Characteristics	Details	Accronym
Beacon Choices	Leader Beacon	LB
	Current Beacon	CB
	Previous Beacon	PreB
Beacon Attributes	Speed	s
	Acceleration	a
	Controller Acceleration	ca
	Location	Pos
	Time	t

3.2.1 Technique for Order of Preference by Similarity to Ideal Solution

The MCDA method used is the Technique for Order of Preference by Similarity to the Ideal Solution (TOPSIS). Ching-Lai Hwang and Kwangsun Yoon originally developed TOPSIS in 1981 [50]. The concept of TOPSIS is that the chosen alternative should have the shortest geometric distance to the positive ideal solution and be furthest from the negative ideal solution. To achieve this, an ideal best and an ideal worst are selected for each attribute for each choice. As such, each choice compares attributes, with the best becoming the ideal best and the worst becoming the ideal worst.

Normalisation

The starting step of TOPSIS is to create Table 3.3 with the choices in the first column and the beacon attributes on the top row. The corresponding values are then entered, with Table

Table 3.3: *Beacon attributes table*

Beacon	s	a	ca	Pos	t
Leader Beacon	22.22	0.001	0.002	100	1.45
Current Beacon	22.22	8.80E-05	0.002	74	1.48
Previous Beacon	22.22	8.80E-05	0.002	74	1.47

3.3 showing an example. The next step is to normalise each attribute (X) using Eq. 3.1. The normalisation step is critical as MCDA can only be used to compare standardised values, e.g. apples compared to apples. Next, each attribute value for each choice is added and divided by the number of choices before dividing this value by the original attribute choice value to give the normalised value.

$$x_{ij} = \frac{X}{\sqrt{\sum_{j=1}^{n} X^2}} \tag{3.1}$$

This equation is then translated into the following sudo code 1 that was then implemented in the plexe simulation for each of the checked attributes.

Algorithm 1 How the normalisation is carried out for the beacon components.

1: sum = $\sqrt{leaderX^2 + currentX^2 + previousX^2}$
2: $x_{ij} = leaderX \div sum$ ▷ Leader normalised value.
3: $x_{ij} = currentX \div sum$ ▷ Current normalised value.
4: $x_{ij} = previousX \div sum$ ▷ Previous normalised value.

Once each attribute value is normalised for each choice, the next step is multiplying the normalised attribute value by the attribute relative weighting (w_j).

Defining w_j

The relative weight of each attribute is a numerical bias for the favourability of each beacon component and, therefore, its importance. An attribute with a significant weighting will be able to exert more influence on the overall outcome of the MCDA. In contrast, a smaller weight will mean a minor impact on the MCDA. The relative weight is calculated using the Best Worst Method (BWM), created by Jafar Rezaei [79] and is a pairwise comparison. The first step in BWM is to determine the decision criteria. These criteria are the beacon components for beacons and are shown in Table 3.2.

The next step is identifying the *Best* and the *Worst* criteria. The best criteria is the attribute that will impact the MCDA the most and, therefore, needs to be a highly influential attribute for the platoon controller. The worst attribute will influence the MCDA the least and, therefore, should be an attribute that is not very influential on platooning behaviour. So, to select the best and the worst, two beacon attributes must be selected. The first needs to be

Table 3.4: *Beacon components related against best.*

Best To Others	Controller Acceleration	Acceleration	Speed	Position	Time
Time	4	3	1	9	2

the attribute that has the most impact on the behaviour of a vehicle using CACC. The second should be the attribute that has the least impact on the CACC. K, Garlichs et al. [40] state that acceleration and speed were the most influential beacon attributes when determining platoon member behaviour as these two values control the longitudinal position of a platooning vehicle. The controller acceleration is not involved directly with vehicle positioning. It is used to tell the CACC the target acceleration of the preceding vehicle. It is, therefore, the least influential attribute [40]. Therefore, using acceleration or speed would be best to use as the *Best* attribute, and controller acceleration would be the *worst*.

During testing, however, it was found that by using acceleration or speed as the best attribute, an attacker can brute force the MCDA by using a huge value. To overcome this, time is used as the best attribute, strengthening the most up-to-date beacon, and speed is the second most weighted attribute. Additionally, using time is better as vehicles can compare the time stamps of beacons to their own clock time to prevent brute force attacks like that. Finally, the worst attribute was found to be the vehicle's position. The position attribute is the least important as it is rarely used when using the CACC method of platooning.

Therefore, the best attribute is time, and the worst attribute is position. After selecting the best and worst, the next step is to determine the preference of the best overall other criteria using a number between one and nine. Where one is time, and nine is position, creating a best-to-others vector shown in equation 3.2 with A_{Bj} being best-to-other criteria and B is the best attribute and j is its perceived value compared to B. Table 3.4 shows the perceived value of the best attribute compared to all others.

$$A_{Bj} = (t_{Bj}, Pos_{Bj}, a_{Bj}, ca_{Bj}, s_{Bj}) \tag{3.2}$$

Once the best is identified, the next step is to rank all the beacon components by the worst. This is done the same way as the best, but this time, it creates an others-to-worst vector shown in equation 3.3. Where A_{Wj} is worst-to-other criteria, W is the worst attribute, and j this time is the perceived value to W. An easy way to understand this is with table 3.5, which shows each beacon component and its corresponding rating between one and nine, the same as table 3.4.

$$A_{Wj} = (t_{Wj}, Pos_{Wj}, a_{Wj}, ca_{Wj}, s_{Wj}) \tag{3.3}$$

The last step is calculating the optimal weights w_j using the best-to-others and worst-to-others vectors. To do this, $w_B/w_j = a_{Bj}$ and $w_j/w_W = a_{jW}$ where w_B is the weighted best, and w_W is the weighted worst. So the find j the solution should be solved where the absolute

Table 3.5: *Beacon components related against worst.*

Worst To Others	Controller Acceleration	Acceleration	Speed	Position	Time
Position	6	7	9	1	8

maximum differences are shown in equation 3.4 and when j is minimized, shown in equation 3.5. Considering the weights as non-negatives and the sum condition for the weights, then the equation 3.6 is formed.

$$\frac{W_B}{W_j} - a_{Bj} \tag{3.4}$$

$$\frac{w_j}{W_W} - a_{jW} \tag{3.5}$$

$$\begin{aligned} min \max_j \left\{ \frac{W_B}{W_j} - a_{Bj} \ , \ \frac{W_j}{W_W} - a_{jW} \right\} \\ s.t. \\ \sum_j^{W_j} = 1 \\ W_j \geq 0, \ for\ all\ j \end{aligned} \tag{3.6}$$

Finally, to solve equation 3.6, equation 3.7 is used, and a consistency index (ξ) is created [79].

$$\begin{aligned} min\ \xi \\ s.t. \\ \frac{W_B}{W_j} - a_{Bj} \ \leq \xi, \ for\ all\ j \\ \frac{W_j}{W_W} - a_{jW} \ \leq \xi, \ for\ all\ j \\ \sum_j W_j = 1 \\ W_j \geq 0, \ for\ all\ j \end{aligned} \tag{3.7}$$

For ease of use, the Best-Worst calculations are calculated using the BWM-Solver-4 (version 1) [79]. Table 3.6 shows the W_j (weighting) used for the MCDA.

Table 3.6: *The weighting of each component.*

Weights	Controller Acceleration	Acceleration	Speed	X Position	Y Position	Time
	0.06741573	0.11797753	0.03370787	0.39325843	0.23595506	0.38764045

Selection of Best and Worst

Once the beacon components have been multiplied by w_j, the next step is to identify the ideal best and the ideal worst attribute for each beacon component. The ideal best is the most advantageous attribute, for the example in Table 3.7 for a, the ideal best value is 0.058 (LB_a). The ideal worst is the least advantageous. For example, in Table 3.7 for a, the ideal worst value is 0.004 (CB_a and $PreB_a$). The beacon components and the ideal best and the ideal worst attributes are calculated using the following sudo code 2.

Algorithm 2 How the attribute weighting and selection of best and worst are implemented in the code.

Weighted Normalised Leader$x_{ij} = Leaderx_{ij} \times w_j$ ▷ Leader attribute weighted value.
Weighted Normalised Current$x_{ij} = Currentx_{ij} \times w_j$ ▷ Current attribute weighted value.
Weighted Normalised Previous$x_{ij} = Preveousx_{ij} \times w_j$ ▷ Previous attribute weighted value.
if Weighted Normalised Leaderx_{ij}¿=Weighted Normalised Currentx_{ij} **then** ▷ Check for the largest x_{ij}
    if Weighted Normalised Leaderx_{ij}¿=Weighted Normalised Previousx_{ij} **then**
        Ideal Bestx_{ij}=Weighted Normalised Leaderx_{ij}
    end if
else
    if Weighted Normalised Currentx_{ij}¿=Weighted Normalised Leaderx_{ij} **then**
        if Weighted Normalised Currentx_{ij}¿=Weighted Normalised Previousx_{ij} **then**
            Ideal Bestx_{ij}=Weighted Normalised Currentx_{ij}
        end if
    else
        Ideal Bestx_{ij}=Weighted Normalised Previousx_{ij}
    end if
end if
if Weighted Normalised Leaderx_{ij} <=Weighted Normalised Currentx_{ij} **then** ▷ Check for the Smallest x_{ij}
    if Weighted Normalised Leaderx_{ij} <=Weighted Normalised Previousx_{ij} **then**
        Ideal Worstx_{ij}=Weighted Normalised Leaderx_{ij}
    end if
else
    if Weighted Normalised Currentx_{ij} <=Weighted Normalised Leaderx_{ij} **then**
        if Weighted Normalised Currentx_{ij} <=Weighted Normalised Previousx_{ij} **then**
            Ideal Worstx_{ij}=Weighted Normalised Currentx_{ij}
        end if
    else
        Ideal Worstx_{ij}=Weighted Normalised Previousx_{ij}
    end if
end if

Table 3.7: *TOPSIS complete table*

Beacon	s	a	ca	XPos	YPos	t	S_i^+	S_i^-	Performance Score
	$x_{ij} * w_j$	$x_{ij} * w_j$	$x_{ij} * w_j$	$x_{ij} * w_j$	$x_{ij} * w_j$	$x_{ij} * w_j$			P_i
LB	0.114	0.058	0.013	0.097	0.068	0.201	0.004	0.069	0.941
CB	0.114	0.004	0.014	0.072	0.068	0.206	0.059	0.036	0.380
PastB	0.114	0.014	0.014	0.072	0.068	0.204	0.051	0.036	0.415
Best	0.114	0.058	0.014	0.097	0.068	0.206			
Worst	0.114	0.04	0.013	0.068	0.068	0.201			

The ideal best and worst are used to calculate the ideal best Euclidean distance (S_i^+) and the ideal worst Euclidean distance (S_i^-). Eq. 3.8 shows the ideal best Euclidean distance equation where V_{ij} is the weighted normalised value, and V_j^+ is the ideal best attribute.

$$S_i^+ = \left[\sum_{j=i}^{m}(V_{ij} - V_j^+)^2\right]^{0.5} \tag{3.8}$$

Eq. 3.9 shows the ideal worst Euclidean distance equation where V_{ij} is the weighted normalised value, and V_j^- is the ideal worst attribute.

$$S_i^- = \left[\sum_{j=i}^{m}(V_{ij} - V_j^-)^2\right]^{0.5} \tag{3.9}$$

With the Euclidian distances calculated using eq. 3.8 and 3.9 for each beacon, the final step is to calculate the performance score (P_i). Where the ideal worst Euclidean distance is divided by the ideal best Euclidean distance added to the ideal worst Euclidean distance, shown in eq 3.10, the most significant performance score is the best beacon to be used by the CACC controller. In this example, it would be the leader beacon (LB).

$$P_i = \frac{S_i^-}{S_j^+ + S_j^-} \tag{3.10}$$

3.3 Trust method

With the P_i values for each beacon calculated, the platoon controller uses the beacon with the highest score. However, it will not reliably prevent FDI attacks from an internal attacker. For this, a simple trust method enables platooning vehicles to prevent FDI attacks from other platoon members and replace the fake beacons with safe beacons. For this to work, each vehicle needs to establish and maintain trust with the preceding vehicle, referred to as local evaluation [69]. Local evaluation is where each vehicle maintains a trust score for the preceding vehicle. Each vehicle does not need to keep a trust score for platoon members from whom they are not receiving beacons. For example, member vehicle three would not need to keep a trust score for member vehicle six as they do not use any beacons from that vehicle when platooning. The local trust score is a percentage score between zero and one hundred, where one hundred is fully trusted, and zero is no trust at all. The trust score is calculated by evaluating the beacons received and using its sensors and the results of the MCDA to verify the beacons. The trust is taken from two areas: *Sensor Readings*,

Chapter 4

Simulation Results

In the previous chapter, the simulation environment and methods were detailed. This chapter aims to present and explain the interactions of an FDI attacker on a platoon, both from an internal attacker and an external attacker. The effects of the attacks will be explained when no solution method is applied and when the MCDA methods described above and the trust method are used to identify and prevent the false message from being used by the platoon controller.

This chapter is organised in the following way. First, methods of assessing the impact of an FDI attack on a platoon and then how to measure how successful MCDA is at preventing an attack; this includes discussion on how statistics can be used to prove effectiveness. Following this is a demonstration of the damage an FDI attack can cause to a platoon, depending on whether it is an internal or external attacker. Then, MCDA is applied to the platoon, and its effects are discussed. Finally, MCDA and trust are used together.

4.1 Measurable Characteristics

4.1.1 Inter-vehicle Distance

The Inter-vehicle distance is the first physical attribute to be discussed. Safety is the most critical attribute to be discussed here. Evaluating and discussing inter-vehicle distance is vital as it directly corresponds to the safety of platoon members, the platoon as a whole, and all other traffic and road users. As such, the Inter-vehicle distance will be used to understand and demonstrate the platoon's safety and will be primarily measured and discussed by looking at the deviation from the platoon's ideal inter-vehicle distance, which is $15m$. The only way the inter-vehicle distance can change between vehicles in the experiments is if the attacker alters the inter-vehicle distance of one or more vehicles. Shorter inter-vehicle distances mean less time for the vehicle to brake, thus increasing the chance of vehicles colliding during braking or speed changes. In addition, it should be understood that the attacker can force vehicles to collide just with the false beacons. More significant gaps are also dangerous as other non-

platooning traffic may enter the platoon, resulting in the platoon no longer functioning safely without colliding with non-platooning vehicles.

4.1.2 Vehicle Speed

The vehicle speed is vital as the goal behind a platoon is to have all members driving together and acting in unison [4]. In the experiments, all vehicles should maintain a constant speed of $80kmph$ or $22.22mps$. As such, it becomes easy to identify any changes to the stability of the platoon as attacked vehicles can see a change in their travelling speed. Due to there being no need for vehicles to deviate from the ideal speed set by the leader. Regular deviation from the ideal speed or any repeating pattern can make the platoon unstable [4] and can indicate that one or more vehicles are receiving beacons that are not ideal. It will impact safety as instability creates and can lead to collisions between members and non-member vehicles if their drivers are not paying attention or there is a sudden change in driving behaviour due to the short inter-vehicle distance between platooning vehicles [36]. Thus impacting the safety of the platoon and other vehicles.

4.1.3 Vehicle CO_2 Output

Finally, there is the CO_2 output of the platooning vehicles. The CO_2 is measured here as it indicates how much work each vehicle engine is doing, as platooning is a technology that promises to reduce Fuel consumption by improving the efficiency of how each platoon member travels. In an ideal platoon, each member vehicle will output about the same amount of CO_2 with the leader outputting slightly more; however, all vehicles will output significantly less than any non-platooning vehicle [4]. If the CO_2 output of a vehicle is altered from the ideal, then that vehicle may be the subject of an attack. This is because the beacons are directly responsible for controlling the driving of the vehicles; this includes acceleration and braking. A vehicle not driving at a steady constant rate will see changes to the CO_2 output [60]. Vehicles in a platoon rely on the beacon wireless communications between each other to be able safely to drive as a level 3 autonomous vehicle [51] loss, disruption and alteration of beacons will change the driving behaviour of a platooning vehicle [4]. Therefore, an attacker can manipulate the amount of fuel consumed.

Additionally, it is possible to reduce platooning's efficiency but cause platooning vehicles to output more CO_2 than what would be produced if they were working individually. This will reduce the vehicles' fuel efficiency and, therefore, cause them to lose the benefits of platooning and the increased risks associated with the attacks. Finally, the increase in CO_2 means the platoon's environmental impact will increase.

4.2 FDI Attacks without any Protection

It is vital to understand the damage that an attack can cause on an unprotected platoon to better understand the benefits of using MCDA to prevent FDI attacks on vehicle platoons. Then, the effects of the FDI attacks described in the methods section are explained and discussed in detail to give a control that can be compared to when MCDA is applied. First, the external attacker will be explored using constant and on-off attacks before explaining the results of the internal attacker on the platoon.

4.2.1 Inter-vehicle distance

Constant attack

There are two types of attackers: internal attackers and external attackers. The internal Attacker is a member of the platoon that is transmitting altered beacons. These altered beacons are created by adding $0.5mps$ to the speed component of the beacon when it is created by the attacking vehicle just before broadcasting it on the platoon network. Algorithm 3 is an example showing the sudo code from the BaseProtocal file sendPlatooningMessage function. In this function, the transmitting vehicle creates the beacon. It contains a lot of information from the transmitting vehicle, such as the attributes: Speed (line 12), Acceleration (line 11), Controller Acceleration (line 10), Time (line 17) and X and Y position (line 15 and 16). There is also additional data such as length, which is the length of the beacon, SpeedX and SpeedY, and the vehicle's speed along the X and Y axes. RelayerId, the ID of the transmitting vehicle; Kind, what type of message it is; ByteLength, which is the packet size; and the SequenceNumber, which allows for keeping track of the order in which beacons are created. The simulator needs the additional information and is used by the receiving vehicle to carry out some operations. The influence of the platoon controller was found to be negligible compared to the attributes used for the MCDA. There is also the Attacker, which is used to identify the beacon from the Attacker and to track the beacon and the actions the MCDA takes with the beacon. The Attacker is ignored by the MCDA, trust method and platoon controller.

Fig. 4.1 shows the inter-vehicular distance for an attacked platoon when under constant internal attack. In this attack, the attacker increases the speed component within the beacon by $0.5m/s$. It can be observed that the directly attacked vehicle (Node 2) reduces its inter-vehicular distance by 2.75 meters. The attack tells the directly attacked vehicle to travel faster to maintain the required distance with the vehicle in front. The attacking vehicle, however (Node 1), has not increased its speed, so Node 2 is no longer maintaining a safe inter-vehicle distance [36]. Node 2 does not continue to close the distance and crash into Node 1 as the platoon controller on the vehicle can use sensor information to prevent a coalition; however, the CACC controller is more reliant on communications to maintain its position than the sensors [86]. As Node 2 speeds up, it has a knock-on effect on all other platoon members following it as the inter-vehicle distance between it and Node 3 will increase. This is shown

Algorithm 3 When generating beacons, constant attacker example.

```
1: Plexe::VEHICLE_DATA data
2: traciVehicle→getVehicleData(&data)  ▷ get information about the vehicle via traci
3: UnicastMessage* unicast = new UnicastMessage("", BEACON_TYPE)  ▷ create and send beacon
4: unicast→setDestination(-1)
5: unicast→setPriority(priority)
6: unicast→setChannel(Channels::CCH)
7: PlatooningBeacon* pkt = new PlatooningBeacon()
8: myId = positionHelper→getId()
9: if Attacker then
10:     pkt→setControllerAcceleration(data.u)
11:     pkt→setAcceleration(data.acceleration)
12:     pkt→setSpeed(data.speed)+0.5
13:     pkt→setVehicleId(myId)
14:     pkt→setAttacker(1)
15:     pkt→setPositionX(data.positionX)
16:     pkt→setPositionY(data.positionY)
17:     pkt→setTime(data.time)
18:     pkt→setLength(length)
19:     pkt→setSpeedX(data.speedX)
20:     pkt→setSpeedY(data.speedY)
21:     pkt→setAngle(data.angle)
22:     pkt→setRelayerId(myId)
23:     pkt→setKind(BEACON_TYPE)
24:     pkt→setByteLength(packetSize)
25:     pkt→setSequenceNumber(seq_n++)
26: else if Member then
27:     pkt→setControllerAcceleration(data.u)
28:     pkt→setAcceleration(data.acceleration)
29:     pkt→setSpeed(data.speed)
30:     pkt→setVehicleId(myId)
31:     pkt→setPositionX(data.positionX)
32:     pkt→setPositionY(data.positionY)
33:     pkt→setTime(data.time)
34:     pkt→setLength(length)
35:     pkt→setSpeedX(data.speedX)
36:     pkt→setSpeedY(data.speedY)
37:     pkt→setAngle(data.angle)
38:     pkt→setRelayerId(myId)
39:     pkt→setKind(BEACON_TYPE)
40:     pkt→setByteLength(packetSize)
41:     pkt→setSequenceNumber(seq_n++)
42: end if
43: unicast→encapsulate(pkt)
44: sendDown(unicast)
```

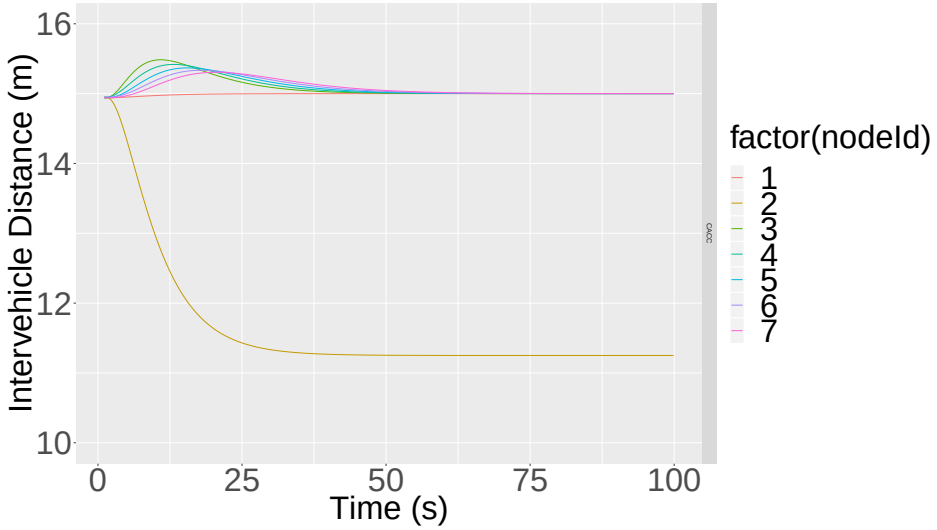


Figure 4.1: *Inter-vehicle distance under constant internal FDI attack without MCDA applied.*

by the increase in inter-vehicle distance seen by Node 3, which starts just after Node 2 starts to decrease its inter-vehicle distance. Node 3 inter-vehicle distance then peaks at about 10s. Using its sensors, the platoon controller on Node 3 realises that the inter-vehicle distance is wrong and self-adjusts back to $15m$ over the next $25s$. All other platoon members observed the same behaviour after the attack on the vehicle. Node 2, Node 1 is unaffected not because it is the attacker but because it is positioned in front of the attacked vehicle.

When looking at the effects of a consent attack from an external attacker attacking Node 2, the inter-vehicle distance between Node 1 and Node 2 decreases as shown in figure 4.2; however, the change is significantly less at less than $0.9m$. The effect on the inter-vehicle distance between members is also muted. Generally, it reflects the pattern in figure 4.1. The difference is that around half of the beacons received in this case are true, and the other half are fake. This leads to the instability shown by the platoon due to the platoon controller of Node 2 receiving conflicting messages. The instability of Node 2 is reflected onto the other nodes that follow it, the same as in the internal attacker example. The external attacker vehicle is created using the HumanInterfearingProtocal. In this file, the vehicle is set up in the same way as a member of the platoon and is, however, it contains the function sendInterferingMessage, which only contains the attacker if statement from 3.

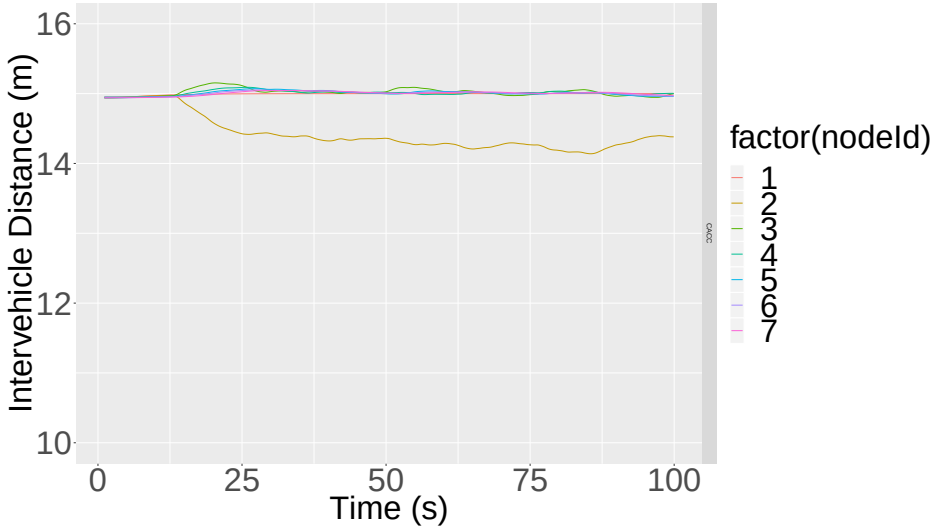


Figure 4.2: *Inter-vehicle distance under constant external FDI attack without MCDA applied.*

On-Off attack

When conducting an on-off attack, the same method is the same as a constant attack using the same scenario. The difference here is that a counter determines the attack time on and off; this is shown in 4. Each vehicle transmits ten beacons every second, so creating a 600 counter cycle divided into two parts will give a $30s$ attack period.

Algorithm 4 When generating beacons, on-off attacker example.

```
1:  if Attacker then
2:      counter++
3:      if counter<=300 then
4:          Create attacking beacon
5:      end if
6:      if counter> 300 && counter<=600 then
7:          Create normal member beacon
8:      end if
9:      if counter>=600 then
10:         counter=0
11:     end if
12: else if Member then
13:     create member beacon
14: end if
```

The platoon's inter-vehicle distance will oscillate when the attacker carries out an on-off attack on a vehicle platoon. This is caused by the attacker going through periods of attack and dormant periods. During the dormant periods, the platoon will recover from

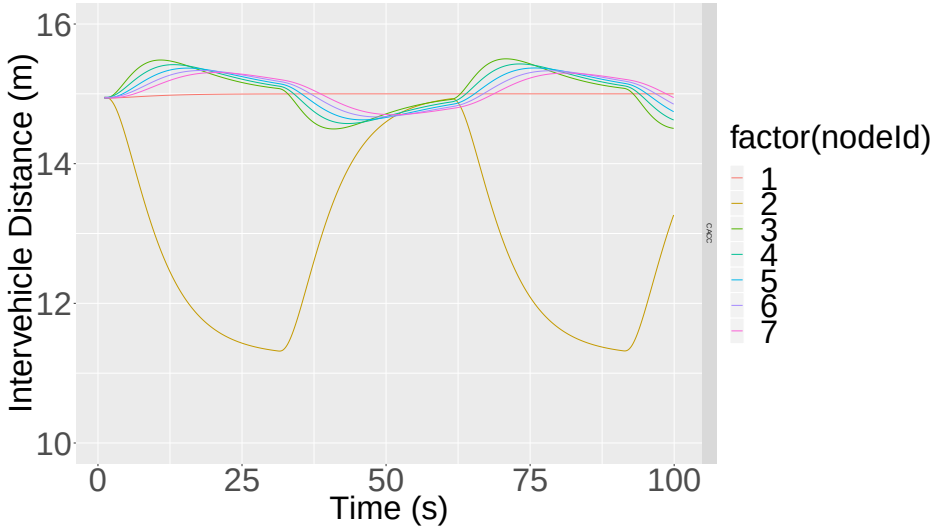


Figure 4.3: *Inter-vehicle distance under on-off internal FDI attack without MCDA applied.*

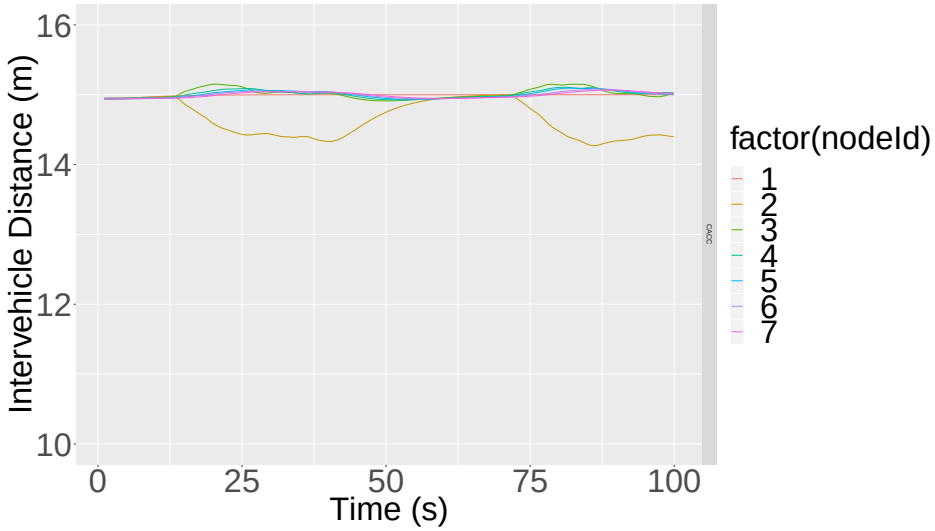


Figure 4.4: *Inter-vehicle distance under on-off external FDI attack without MCDA applied.*

the attack. The oscillation is clearly defined in Fig. 4.3 as the attacker alternates between increasing and reducing the speed. As a result, the minimum inter-vehicle cost is $11.25m$ for the directly attacked vehicle. The attacker causes the inter-vehicle distance to close while it is attacking. However, during the off period here, starting at $30s$ and finishing at $60s$, the attacked vehicle quickly starts to recover to the ideal inter-vehicle distance. In addition, other vehicles following the directly attacked vehicle are also affected, thus leaving the overall platoon in a destabilised state. Here, the other nodes start to deviate in the same way as with the constant attack. The difference is that as the attacked vehicle recovers, this causes the vehicles not to overshoot the ideal inter-vehicle distance, and this is what causes the Nodes 3 to 7 to oscillate around the ideal inter-vehicle distance. The external On-Off attacker is shown in figure 4.4. The attacked node, Node 2, deviates from the ideal like in the constant attack; however, once the attack stops (at $30s$ the vehicle recovers back to the ideal. Then, at $60s$, the attack starts again, and the node deviates from the ideal. The nodes following Node 2, the attacked node, also deviate from the ideal, but this is by no more than $0.2m$.

4.2.2 Vehicle Speed

Constant attack

When the attacker attacks a platoon by increasing the speed component of the beacon, the speed of the attacked vehicle will increase. However, the speed increase only happens for a very short time within the first $10s$. It only increases the speed of the attacked vehicle by just over $1km/h$ as seen in Fig. 4.5. The attacked vehicle does not collide with the preceding vehicle because the vehicle's sensors detect that the inter-vehicle distance is becoming too small. The vehicle platoon controller can deal with the slight change in speed without a collision; however, an alteration of $4m/s$ will result in a collision as the attacked vehicle platoon controller cannot react to the change in speed in time. Node 3 to Node 7 also see an increase in their speeds. The increased driving speed is to close the inter-vehicle game created when Node 2 is attacked, causing it to move forward. This shows that these vehicles are platooning normally. Overall, the smooth and steady flow suggests that although the platoon is attacked, it is still relatively stable.

When looking at the speed for the platoon when attacked externally, as shown in figure 4.6, the speed is unstable for the attacked vehicle and all others that follow it. However, the instability is less than $0.25k/h$ deviation from the ideal. The instability is due to the attacked vehicle receiving both true and false beacons, which it will use, resulting in instability as the platoon controller shifts between $22.22m/s$ and $22.27m/s$. Adding more attackers does not impact the speed of the vehicles in the platoon, with the only effect being how quickly each vehicle is affected. When there are multiple victims, the speed change is seen on all members more quickly.

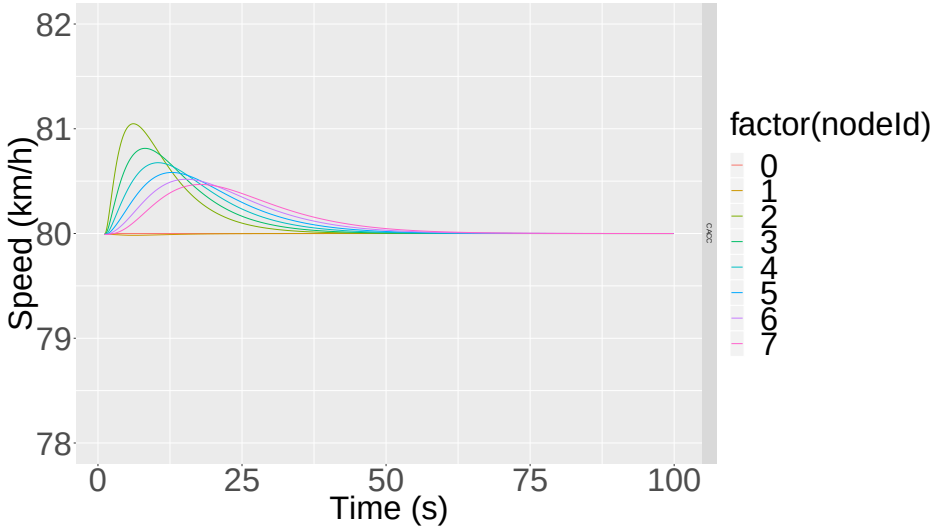


Figure 4.5: *Vehicle speed under constant internal FDI attack without MCDA applied.*

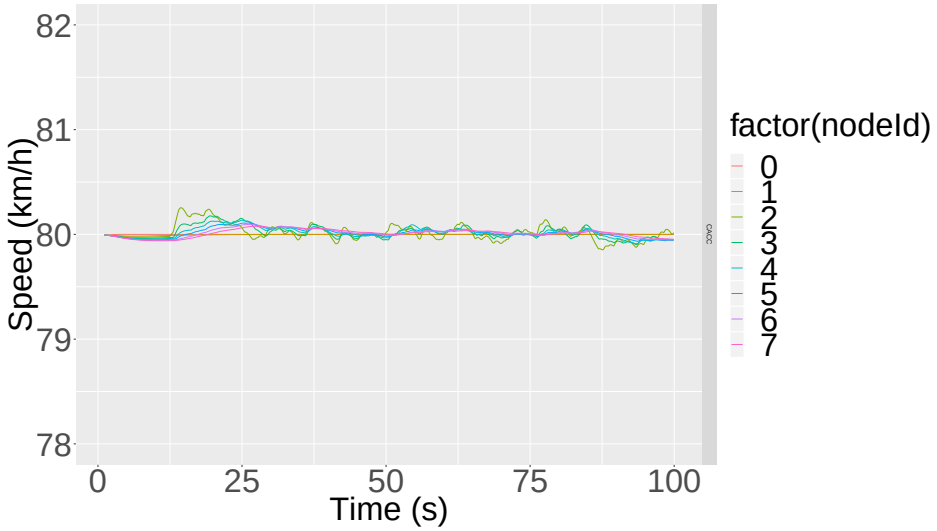


Figure 4.6: *Vehicle speed under constant FDI external attack without MCDA applied.*

On-Off attack

Under the FDI On-Off attack, a double peak waveform is formed, as shown in Fig. 4.7. This behaviour is produced by the platoon being attacked and the members recovering. In Fig. 4.7, the attacker makes the attacked vehicle accelerate before halting the attack. The positive peaks show that the attacked vehicle Node 2 increases to just over $1k/h$, and like when under constant attack, the vehicles that follow the attacked vehicle are also affected; infarct, the pattern is the same as the constant attack. The difference is at the $30s$ where the attacker stops attacking. At this point, there is an abrupt change in the behaviour of all vehicles; this is when the attacker stops attacking the platoon. The effect is that now all the vehicles slow down as the attacked vehicle returns to its correct position within the platoon. This leads to an oscillation effect as vehicles cycle through acceleration and deceleration cycles. For the external attacker, it is also possible to see the time the attacker is active and when the attacker is not active, as shown in figure 4.8. When the attacker is active $10s - 40s$, the effects of the attack on the platoon cause the vehicles not to hold a constant speed. The directly attacked vehicle Node 2 is the worst affected but never sees more than a $0.25k/h$ change in speed. This is due to the attacked vehicle receiving both true and false beacons. All vehicles following the attacked vehicle are also disrupted. The external attacker does not form the smooth waveform of the internal attacker; instead, it is more chaotic, making the platoon unstable as members are always adjusting their speed to maintain safe platooning. Between $40s$ and $70s$, the attacker goes dormant, and the platoon recovers from the attack.

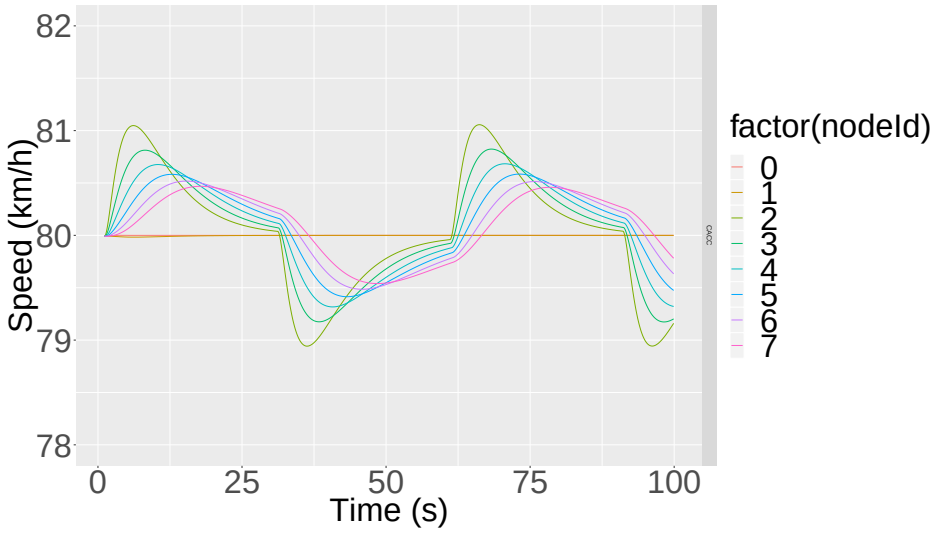


Figure 4.7: *Vehicle speed under internal on-off FDI attack without MCDA applied.*

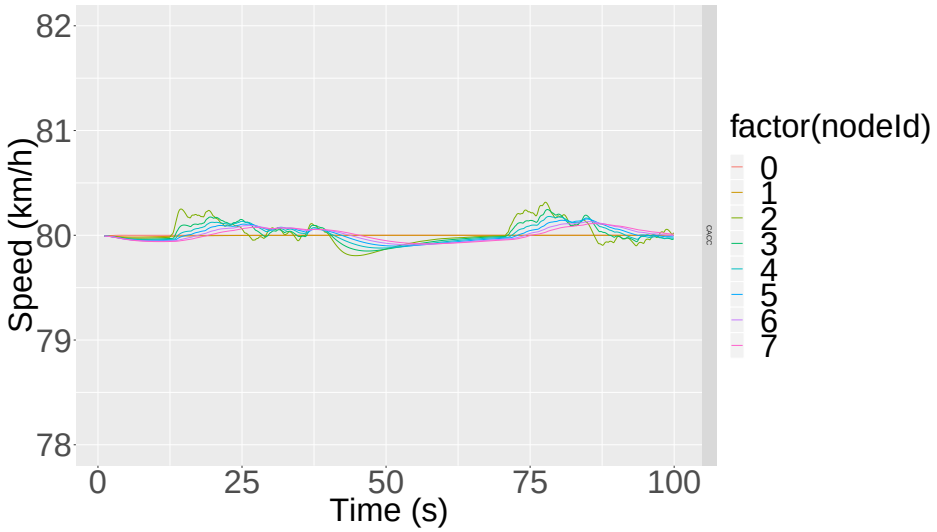


Figure 4.8: *Vehicle speed under external on-off FDI attack without MCDA applied.*

4.2.3 Carbon Dioxide Output

Finally, the attack has an environmental impact where the platoon produces more CO_2 than usual regardless of the attack. By producing more CO_2, it can be inferred that more fuel is used up, reducing the platoon's range[96]. In Fig. 4.9, vehicles one and two are unaffected by the attack and, therefore, have an ideal output of CO_2. Vehicles three to eight, however, output more CO_2 in most cases. During attacks from an external attacker, the change in CO_2 output by vehicles three to eight is negligible, with just over $0.1g$ of additional CO_2 output over $1000s$. When an internal attacker attacks constantly, there is an increase in CO_2 output of up to $0.7g$ over $1000s$. The small increase will impact overall efficiency expressly as this slight increase will add up over a more extended period. As for an internal on-off attacker, interestingly, vehicles three to six produce less CO_2, whereas vehicle eight produces more CO_2.

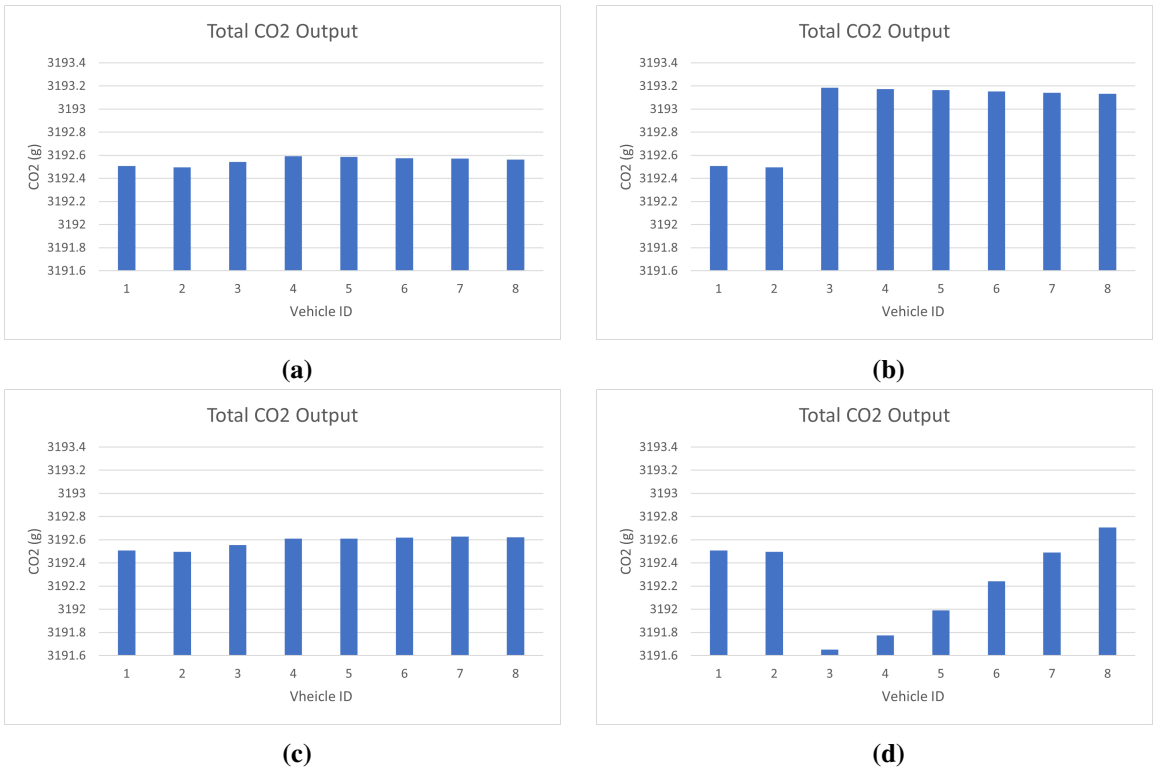


Figure 4.9: *Vehicle CO_2 output when under FDI attack with no solution (a) external constant, (b) internal constant, (c) external on-off and (d) internal on-off*

4.2.4 Measuring Accuracy

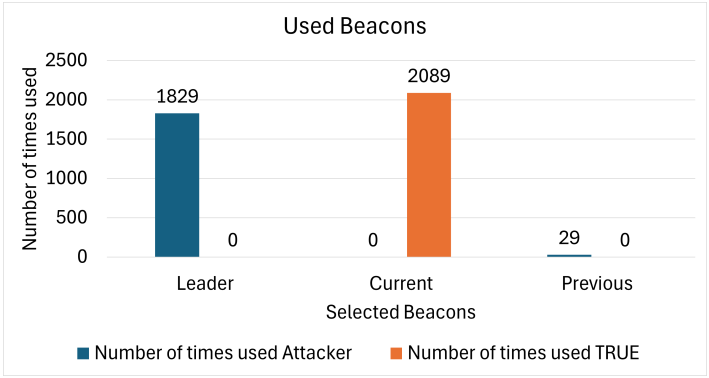
The solution's effectiveness on a platoon under an FDI attack can be examined in terms of its true/false positives and true/false negatives. Using the statistical analysis alongside the measurable physical characteristics proves that the test works as intended. First, it is important to see the attack vehicle's beacon using MCDA TOPSIS. Fig. 4.10 shows the beacon usage by the platoon under constant and on-off attacks using TOPSIS.

Vehicle One will only select and use the Current beacon every time, as shown in Fig. 4.10. With vehicle one only selecting the current beacon means that MCDA TOPSIS is not preventing any true beacons from the leader from being used by the first member vehicle. It should be noted that even if vehicle one did use the leader's beacon, there would be a negligible difference in performance as this beacon is the same as the current. All the other vehicles use a range of different beacons. To make sense of this, a statistical analysis of the beacons used needs to be carried out, first by identifying the True Positives, False Positives, False Negatives and True Negatives, which are then used to calculate the Sensitivity and Specificity. Finally, the F1 Score can be calculated using Sensitivity and Specificity.

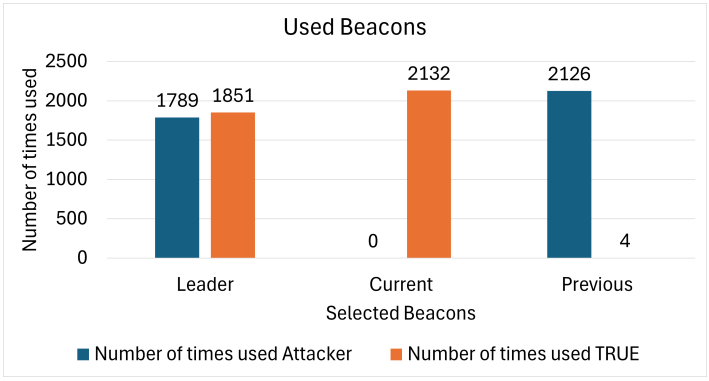
Positives and Negatives

Defining a positive or negative result is crucial to understanding the F1 Score, Sensitivity and Specificity. This section seeks to explain and identify not just what a positive and negative result is but also what a true positive, false positive, true negative and false negative result is. Starting with the positive results, two types can be obtained. The first is a true positive when the test gives an accurate positive result. When testing the MCDA methods, the true positive results are that all the beacons from the leader and all the current beacons not from the attacker are selected. A false positive, on the other hand, is when the test gives a positive result, but what is tested for is not there. In this use case, a false positive is when the platoon controller selects and uses the attacker's beacon. When looking at the negative results again, there are true negatives and false negatives. A true negative is when the test successfully does not identify the positive condition. In this application, a true negative is when the attacker is attacking, and the MCDA method does not select the attacker's beacon; in other words, the test shows that there is an attacker, but the attacker's message is ignored and safely replaced. Finally, there are false negatives when the test fails; in this case, the true, current beacon is dropped and replaced by another one that is not the current beacon.

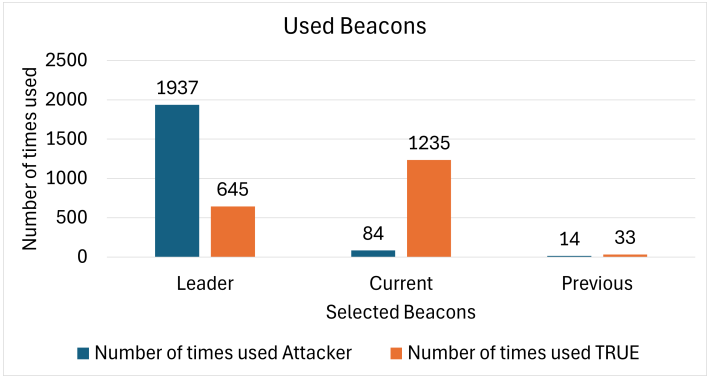
In table 4.1, a true positive is considered to be when the false beacon from the attacker is not loaded to the platoon controller. What beacon is loaded does not matter, as the attacked vehicle is not exclusively getting its information from the attacker. On the other hand, a True Negative is considered each time the current beacon from another member vehicle is loaded into the platoon controller. A False Negative is when a fake beacon from the attacker is loaded into the platoon controller. Finally, a False Positive is when a beacon from another member is not loaded into the platoon controller.



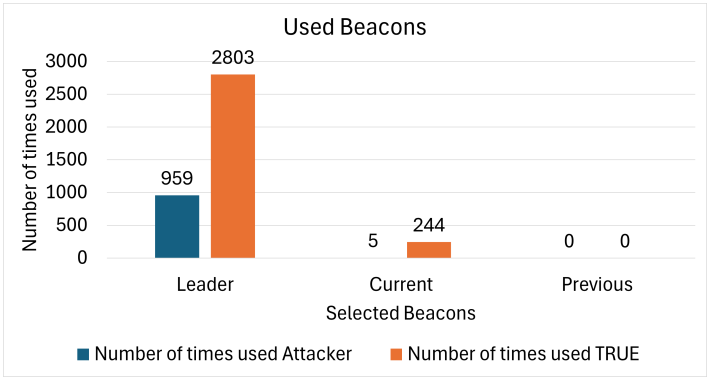
(a)



(b)



(c)



(d)

Figure 4.10: *The beacons used by the attacked vehicle (a) Constant internal attack, (b) Constant external attack, (c) On-Off internal attack and (d) On-Off external attack.*

Table 4.1: *Simplify and state what a True Positive, True Negative, False Positive, False Negative are considered to be.*

	Beacon from Member	**Beacon from Attacker**
Current Beacon Loaded into Platoon Controller	True Negative	False Negative
Current Beacon not Loaded into Platoon Controller	False Positive	True Positive

Sensitivity and Specificity

The Sensitivity (true positive rate) is the statistical probability that the test will successfully identify positive cases. A true positive is when the attacker's beacon is not loaded into the platoon controller in this application. To see what beacons are loaded by any vehicle and whether they are from the attacker, a period of $1000s$ Fig 4.10 is created. Fig 4.10 itself does not show anything more than what beacons are used and when; however, using this table, statistics such as the Sensitivity, false positive rate and others can be calculated. These can be worked out using Fig 4.10 and are shown in table 4.2. To help explain the Sensitivity and specificity of the MCDA, the table 4.1 below helps to explain what is considered to be a true positive, true negative, false positive, or false negative.

To calculate the Sensitivity (true positive rate (TPR)), eq: 4.1 is used where the true positives represented by TP are divided by the true positives plus the false negatives represented by FN. The result is a decimal value where one is the best possible result and the worst is zero. If a value is outside this range, then there is a problem.

$$TPR = \frac{TP}{TP + FN} \tag{4.1}$$

Eq: 4.2 calculates the false positive rate (FPR). In this equation, the false positives represented by FP are divided by the false positives plus the true negatives represented by TN. The false negative rate (FNR) and specificity (true negative rates (TNR)) are calculated using eq: 4.3 and 4.4. The resulting values are decimal values where one is the absolute best possible value and the worst is zero. Therefore, any values outside this range would be considered a problem and suggest a mathematical error.

$$FPR = \frac{FP}{FP + TN} \tag{4.2}$$

$$FNR = \frac{FN}{TP + FN} \tag{4.3}$$

$$TNR = \frac{TN}{FP + TN} \tag{4.4}$$

Table 4.2: *Example showing the true positive, true negative, false positive and false negative rates*

	Constant internal attack	Constant external attack	On-off internal attack	On-off external attack
True Positive	100%	76.8%	88.6%	60.3%
True Negative	47.1%	100%	95.9%	99.5%
False Positive	52.9%	0%	4.13%	0.519%
False Negative	0%	23.2%	11.4%	39.7%

Table 4.2 clearly shows that both methods are very effective at removing the false beacons injected into the platoon network by the attacker. Shown by the sensitivity for TOPSIS is 1 or 100%, and WSM scores 0.984 to three significant figures or 98.4%. The true negative or specificity of the system is relatively low as $0.166 - 0.167$ or $16.6\% - 16.7\%$ for TOPSIS and $0.375 - 0.378$ or $37.5\% - 37.8\%$ for WSM. The specificity of both MCDA methods is disappointing. However, it is down to how aggressively they target false beacons, making it almost impossible for the fake messages to impact the platoon. True messages are also adversely affected. In addition to this, the stats here do not present the whole picture. The vehicle will also use the predicted or the leader's beacon instead of the current one from the vehicle in front when it is under attack. Choosing these other beacons is not bad; it still enables the member to maintain a safe platoon position; however, it is not optimal. When looking at the attacking beacon loading, these other beacons are considered the goal instead.

F-Score, Precision and Sensitivity

The F-score is a measure of the overall accuracy of a test. As such, the F-score positively reflects how successfully the proposed method can remove fake beacons. This is done by dividing the number of true positives by the number of positive results. When working out the F-Score, a perfect score is considered 1 or 100%, which means there is perfect Sensitivity and Precision. The lowest possible score is zero, meaning there is no Sensitivity and or Precision in the test. The equation for F-score calculation is below in eq: 4.5.

$$F - score = 2 * \frac{Precision * Sensitivity}{Precision + Sensitivity} \tag{4.5}$$

In eq:4.5, precision is the number of true positive results divided by the number of true positives plus the number of false positives. It is shown mathematically in equation4.6. Sensitivity is the number of true positive results divided by the number of true positive and false positive results. It is shown in eq:4.7.

$$Precision = \frac{TruePositive}{TruePositive + FalsePositive} \tag{4.6}$$

$$Sensitivity = \frac{TruePositive}{TruePositive + FalseNegative} \tag{4.7}$$

Table 4.3 concludes the example by demonstrating the F1 Score, Precision and Sensitivity using the values from in Fig. 4.10. Using the F-score and the precision, it is possible to

Table 4.3: *F-score, Precision and Sensitivity example.*

Attack Type	F-Score	Precision	Sensitivity
Constant internal attack	79.4%	65.8%	100%
Constant external attack	86.9%	100%	76.8%
On-off internal attack	93.2%	98.4%	88.6%
On-off external attack	75.2%	99.9%	60.3%

describe and explain the true negative and false positive scores and how they impact the solution's ability to maintain safe platooning even under attack. Precision here is the percentage of true positives concerning all positive results. Ideally, the precision should be 100% as this means there are no false positives; however, this is not always the case in practice. Likewise, sensitivity is the percentage of false beacons that are currently identified. To be a reliable test, the sensitivity should be high. In practice, it is a balancing act between precision and sensitivity, as often improving one will decrease the effectiveness of the other. In this thesis, as safety is a major factor, sensitivity will be favoured over precision, which is why the precision in the example is low. Therefore, there will be many dropped true beacons; however, there will be no false beacons from an attacker.

The F-score is the harmonic mean between the precision and the sensitivity and is used to test the accuracy of the test itself. A harmonic mean is a numerical average that is calculated by dividing the number of values by the reciprocal of each number in the series. As such, it will provide a clear idea about the effectiveness of MCDA as a beacon selection method to identify and remove fake beacons from an attacked platoon. Table 4.2 shows that MCDA can remove the false beacons extremely well, providing a sense of reassurance about the solution. However, very high false positive rates, up to 83.418%, are not ideal. The MCDA method also removes large numbers of true beacons. The F-score can be used to determine the accuracy of MCDA.

4.3 Single Attacker, Single target

When simulating with MCDA, the results are visible when running the simulation; there is a reduced deviation from the ideal formation under internal and external attacks—looking at the inter-vehicle distance when under external attack shown in Figures 4.11 MCDA is capable of not just dampening the impact of the attack but completely nullifies the attack this is the case for both constant and on-off attacks. At the start, there is a $0.125m$ deviation from the ideal for all members, and this is caused by the simulation not starting the platooning vehicle at exactly $15m$ intervals. For the external attacker, MCDA, on its own, is highly effective at preventing visible signs of attack on the inter-vehicle distance of platooning vehicles.

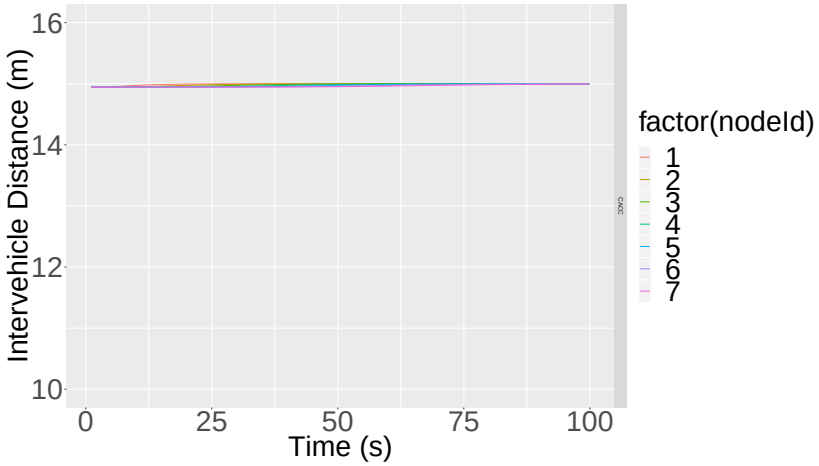


Figure 4.11: *Inter-vehicle distance under Constant external attack.*

When looking at the internal attacker shown in Figures 4.12, MCDA can sometimes suppress the attacker; however, the attacker can still disrupt the platoon formation. In constant and on-off attacks, MCDA can suppress the attacker for just over $120s$ on average before the attacker can attack the platoon. The constant internal attacker clearly shows that MCDA will then suppress the attacker again shortly after the first break; however, it cannot sustain the suppression of the attack. After this, the attacker is suppressed sporadically. The attacker can have some impact on the platoon. However, the attacker cannot coarse the inter-vehicle distance to reduce as much as they were able to when MCDA is not applied, with the minimum inter-vehicle distance only being $12m$. When under Constant internal attack, the inter-vehicle is less stable when using MCDA because the inter-vehicle distance does not settle into a constant rate. For the on-off attack, the behaviour is the same as that of the constant attacker, with the attack being suppressed for around half the time.

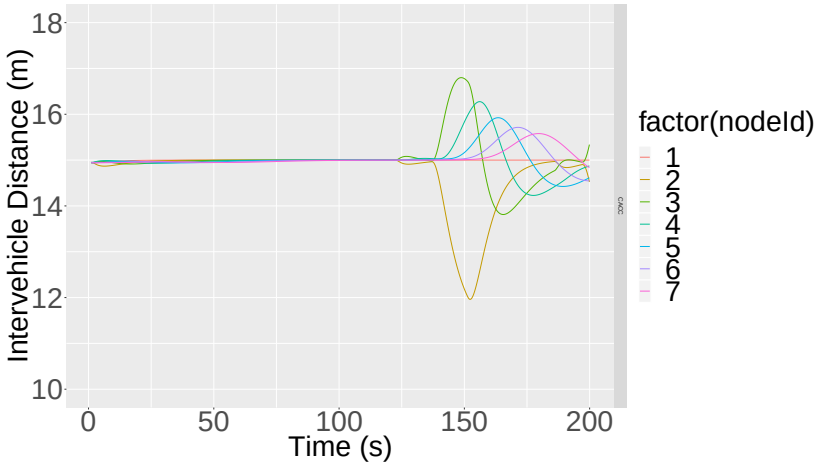


Figure 4.12

Figure 4.13: *Inter-vehicle distance under Constant internal attack.*

The speed and speed changes of platoon members can be used to understand the overall stability of the platoon and its members. Because under ideal platooning, all vehicles should travel at the same speed, and these speeds should be the same. In the simulation, the ideal platooning speed is $80kmph$. Figure 4.14 shows the speed of each platooning vehicle under external constant and on-off attacks, as they are the same; only one is shown here. As was seen in the inter-vehicle distance, the platoon maintains ideal platoon speed throughout the simulation with a negligible adjustment at the start. The behaviour shown is expected as there were no changes to the inter-vehicle distance. MCDA, therefore, again shows that it can prevent an external attacker from having any physical effect on the platoon formation, which is very impressive.

When looking at the speed of the platooning vehicles under internal FDI attack, there are small but meaningful changes in vehicle speed for both constant and on-off attacks. The constant attack shown in figure 4.15 is quite interesting as it shows multiple positive and negative peaks in speed when under attack. The positive peaks occur when the inter-vehicle distance reduces, and the negative peaks occur when the vehicles return to the ideal, extending to the on-off attacker. The changing of the vehicle speeds of up to $\pm 1kmph$, while small, can have a massive impact on the platoon and its overall stability and safety. As the speed changes regularly, the platoon is unstable, which can reduce platoon members' ability to respond promptly to commands from the lead vehicle. For the constant internal attack, MCDA reduces the stability as MCDA struggles to suppress the attacker, resulting in peaks in speed. When there is an on-off internal attacker, MCDA does improve the resilience of the destabilisation effects of the attacker. However, the attacker can still significantly damage the platoon's stability.

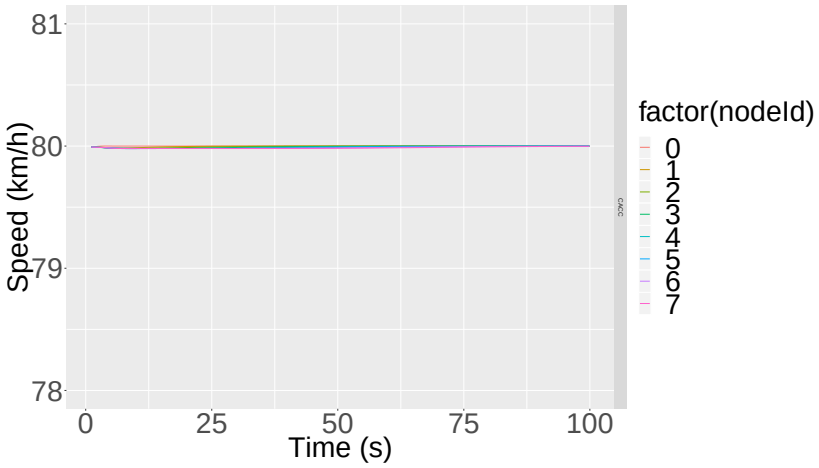


Figure 4.14: *Vehicle speed under Constant external attack.*

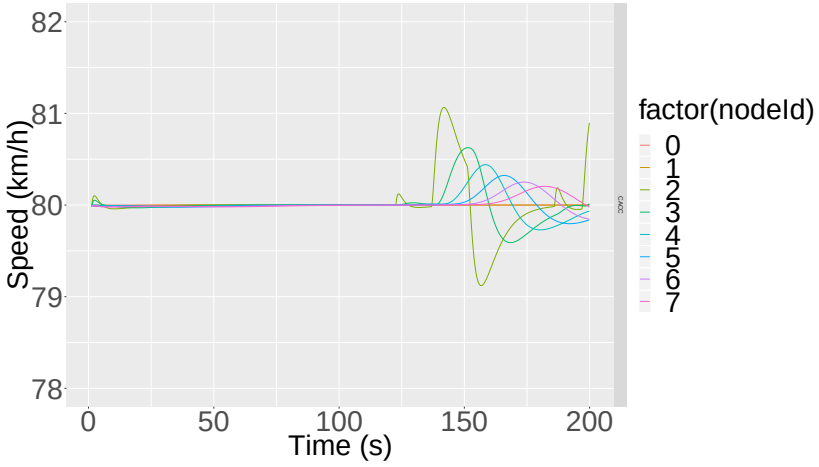


Figure 4.15: *Vehicle speed under Constant internal attack.*

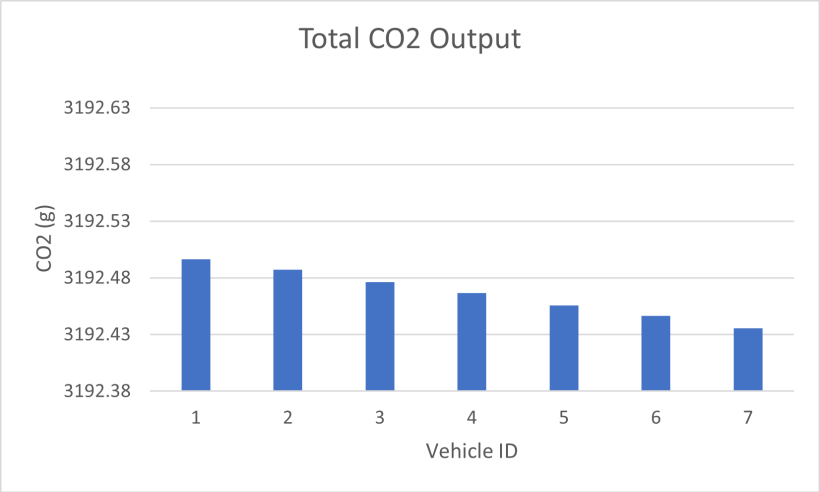


Figure 4.16: *Vehicle CO_2 output under external attack.*

The CO_2 output of each member is taken and presented below in Figure **??**. Vehicle 1 is the leader, so it sees little efficiency saving. Vehicle eight sees the most savings, so the CO_2 output of each vehicle decreases. For external attacks, the CO_2 output is ideal and clearly shows how platooning position can affect the efficiency saving of each vehicle as the attack is countered. For the internal attacker, the situation is more complex. When looking at how MCDA interacts with the FDI attacks, the CO_2 output aligns more with the ideal; however, vehicles are not getting the full benefits of platooning, with a noticeable drop in output when under constant internal attack and vehicle three, the directly attacked vehicle outputting near to expected amounts of CO_2. Vehicle four sees its CO_2 output drop to below-expected levels. Finally, vehicles five to eight see increased levels of CO_2 output. Vehicle three outputs more CO_2 than expected for the on-off attacker, whereas vehicle four outputs an expected amount of CO_2. Overall, using MCDA improves the CO_2 output of platooning members, and under external attackers, MCDA is enough; however, against internal attackers, it can improve but not prevent damage from an attack.

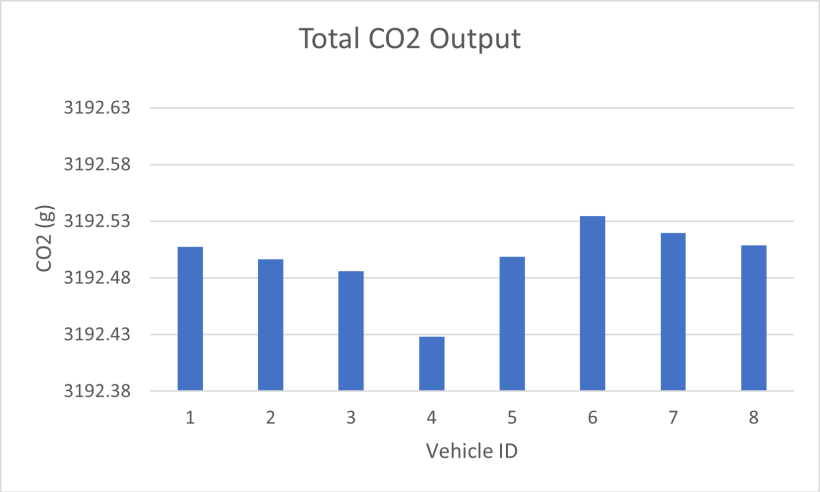


Figure 4.17: *Vehicle CO_2 output under internal attack.*

The F1 score of each vehicle in the platoon is quite interesting. Although the external attacker could not impact the platoon physically, the F1 score is not high overall, with only vehicle ID one for the constant attack and vehicle IDs one to three effectively 100%. All other vehicles have an F1 score of 90% or less. When under external attack, vehicle ID seven has the lowest F1 score of just over 70%, which is a low score. It is even more surprising that the attacker had no visible effect on the platoon in both external attacker simulations. What this means is that the precision was high; however, the sensitivity was low. In other words, while the attacker's beacons were removed successfully, many true beacons from the preceding vehicle were wrongly rejected. For the internal attacker, it shows that only a small number of false beacons from the attacker need to get through to enable the attacker to be successful. The F1 score for the internal attackers is relatively high at $80\%+$. For external attacks, it is not that true beacons are identified as false but that false beacons are identified as true, which reduces the F1 score, meaning that the platoon attacked by an internal attacker sees a low precision but a high sensitivity. One reason for seeing this is that the external attacker can misidentify a beacon. In contrast, there is less chance for this to happen when the attacker is internal.

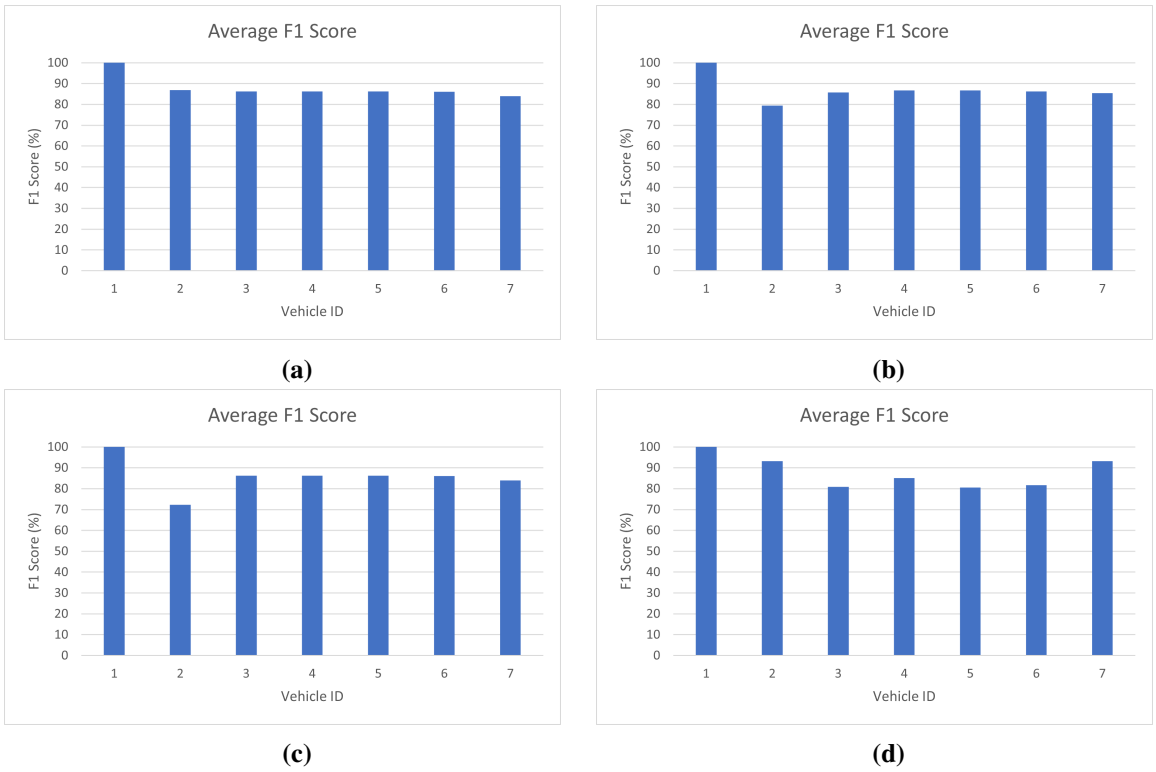


Figure 4.18: *Vehicle F1 score under (a) Constant external attack, (b) Constant internal attack, (c) On-off external attack and (d) On-off internal attack.*

4.4 Multiple Attackers, Single target

When multiple attackers attack a single target, the number of false beacons injected into the platoon will increase. If there are two attackers, then the number of false beacons will be double that of a single attacker. If there are three attackers, the number of false beacons will be three times as many, leading to a greater chance that a false message will be picked up and used by the victim's vehicle. The idea behind this is to stress test MCDA to assess how MCDA reacts to an increase in the number of fake beacons that a vehicle receives. While the road conditions used are idealised, this thesis aims to establish if MCDA can effectively identify false beacons in a platoon network. The focus at this point is to see if the vehicles can successfully and safely process and implement MCDA on a live data stream during platooning. Due to the communication topology, multiple attackers attacking a single target is only achievable by external attackers. Therefore, there are no internal attackers for this attack. Figure 4.19 shows eight attackers attacking Node ID 2. For both constant and on-off attacks, the victim vehicle shows no deviation from the ideal, and overall, the performance of the platoon to maintain $15m$ inter-vehicle distance between member vehicles is unaffected. This is irrespective of the number of attackers present when testing between two and eight. This is because by screening the received beacons before they are used by the platoon controller on the attacked vehicle, MCDA can successfully prevent fake beacons from being used by the platoon controller. This means the attack has no visible effect on the inter-vehicle distance between platooning vehicles. Therefore, it shows that MCDA can maintain safety despite several external attackers. MCDA is strong at defending against multiple external attackers as there are still those true beacons available to itself, which it can successfully identify and use while screening out the fake beacons from multiple attackers.

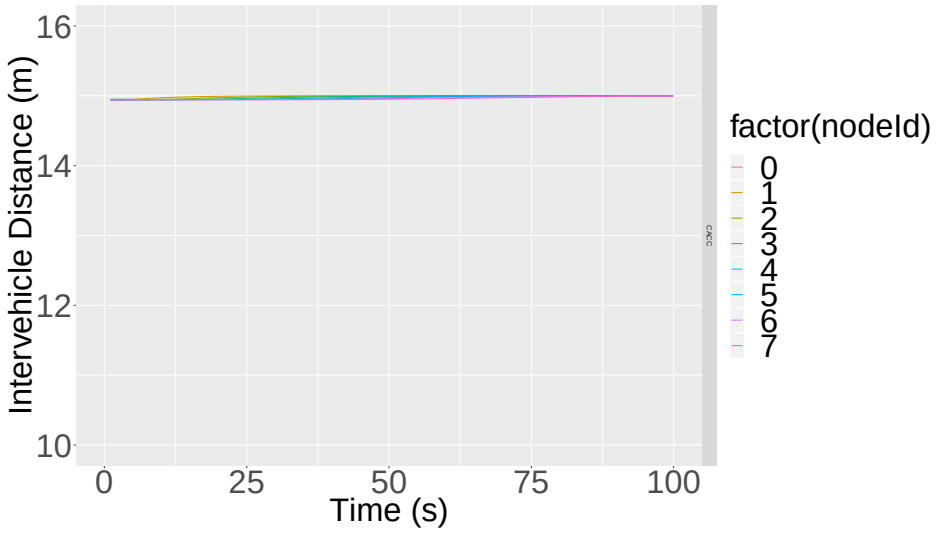


Figure 4.19: *Vehicle speed under Constant external attack by eight attackers.*

When looking at the speed shown in Figure 4.19, it is clear that even with up to eight

external attackers, the stability of the platoon using MCDA remains ideal as there is no difference between the platooning vehicles' speed when the number of external attackers increases. Once again, there is only a fractional difference in starting vehicle speed from the simulation. The stability of the speed at a constant $80kph$ shows that the attacker's beacons are going unused by the attacked vehicle platoon controller. The use of MCDA to screen the incoming beacons can, in this set-up, completely nullify the effects of the attackers on the vehicle speed. While under the bombardment of fake beacons, the attacked vehicle can still successfully identify the true beacons using MCDA. This shows that increasing the number of attackers attacking a vehicle in the platoon will not affect the stability of platoon members or the platoon overall.

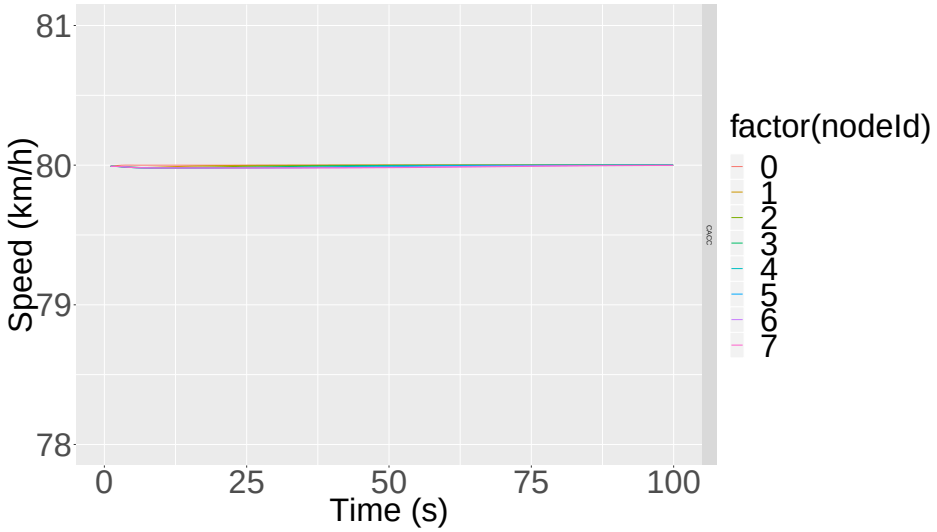
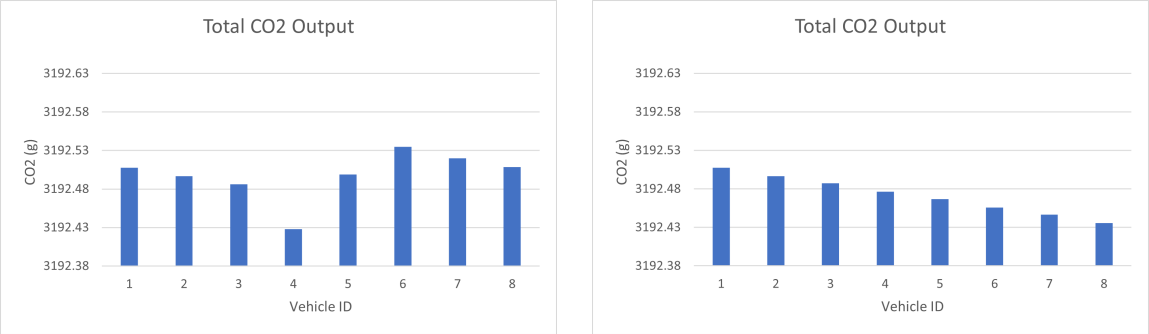


Figure 4.20: *Vehicle speed under Constant external attack by eight attackers.*

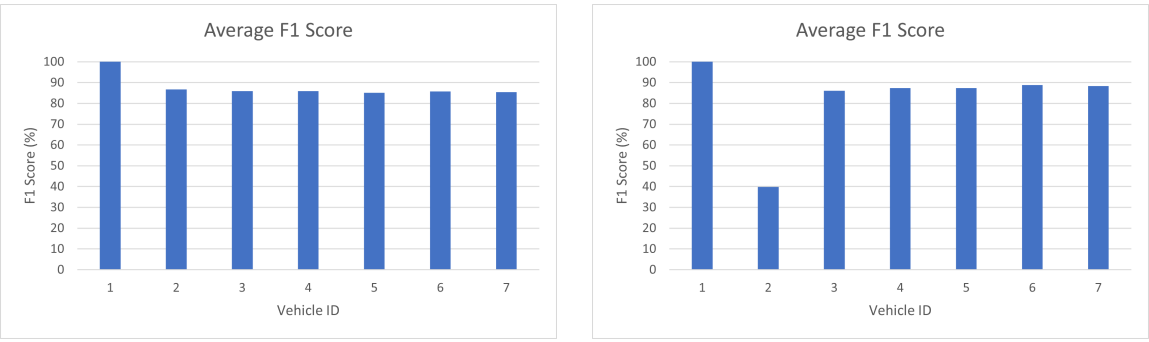
In addition to understanding the physical impact that the MCDA has on the extent the attack can disrupt the platoon, also looking at the effect the MCDA solution has on the vehicle has on the CO_2 output of each vehicle along with seeing the environmental impact of the attack and solution but also gauge how the attack affects the fuel economy of the vehicle. When looking at a constant attack from six attackers and one victim, vehicle four outputs less CO_2 compared to if there is a single attacker; however, vehicles five to eight output more CO_2 than if it was a single attacker. The change in CO_2 output is quite surprising considering that the vehicles have no noticeable change in their inter-vehicle distance or speed, suggesting that the platoon is acting as expected. The only explanation for such a difference is that the increased number of attackers affects the platoon, but there are no visible signs. Interestingly, there is no difference between the one and six attackers for the on-off attack.

Something interesting happens when looking at the solution, the F1-Score, for when multiple attackers attack a single vehicle. Firstly, the constant attack sees the F1 score of member vehicles two to seven all sit at the same place of around 86%; for vehicle two, this



(a) **(b)**

Figure 4.21: *Vehicle CO_2 output under (a) Constant external attack and (b) On-off external attack.*



(a) **(b)**

Figure 4.22: *Vehicle F1 score under (a) Constant external attack and (b) On-off external attack.*

is an increase in the F1 score. The increase in F1 score is due to six times the number of false beacons it can detect. Therefore, the test's sensitivity is increased without degrading the precision, leading to a better F1 score. For the on-off attack, there is a significant decrease in the F1 score of vehicle ID two down to just 40% from its previous 99%. In addition, vehicles three and four also have a decrease in F1 score; however, vehicles five to seven see an increase in F1 score. Vehicle two's decrease in F1 score is most likely due to the MCDA's inability to maintain a high sensitivity when multiple attackers attack a single vehicle using an on-off approach, leading to an extremely high number of true beacons being ignored and replaced. The result of this is that the platooning vehicles appear outwardly to be unaffected by the attack; however, what is happening is that while the attacker is unsuccessful at getting their beacons used by the victim vehicle, they can prevent the victim vehicle from being able to use the true beacons from the preceding vehicle forcing them to rely on beacons from the leader.

4.5 Multiple attackers, Multiple victims

This time, the attackers each attack a different member vehicle. If there are five attackers, the platoon has five victim vehicles. For external attackers, using MCDA alone can prevent any noticeable change to the inter-vehicle distance. This is true for both constant and on-off attacks, as shown previously. Therefore, figure 4.23 shows only the constant attacker example. For the internal attack, this is where things get interesting. Node 6 in Figure. 4.24 and 4.25 is the last vehicle in the platoon that is attacked and behaves like Node 2 does when there is a single attacker. In addition, in both of these, the use of MCDA does prevent the attackers from disrupting the platoon formation for the first $200s$, the same as when there is just a single attacker. After this point, MCDA can again not reliably prevent the attacker's attack on the platoon, and it fails. However, it is not a complete failure. There are sporadic instances when the MCDA can suppress the attackers again, as seen at $475s$ in figure 4.24 and at the very end of figure 4.25. This is the same behaviour seen when there is a single internal attacker. This suggests that increasing the number of internal attackers does not affect the MCDA's ability to suppress internal attacks.

Thus, this suggests that the MCDA can suppress the attacker's beacons and prevent them from damaging the platoon for these vehicles. However, MCDA cannot prevent the attack on the final attacked vehicle. When looking at different numbers of attackers, the last vehicle is always the one that deviates from the ideal. The exact cause of this behaviour is fully understood once looking at the F1 scores and selected beacons. Finally, node ID 7 also deviates from the ideal inter-vehicle distance due to adjusting to the preceding vehicle being attacked.

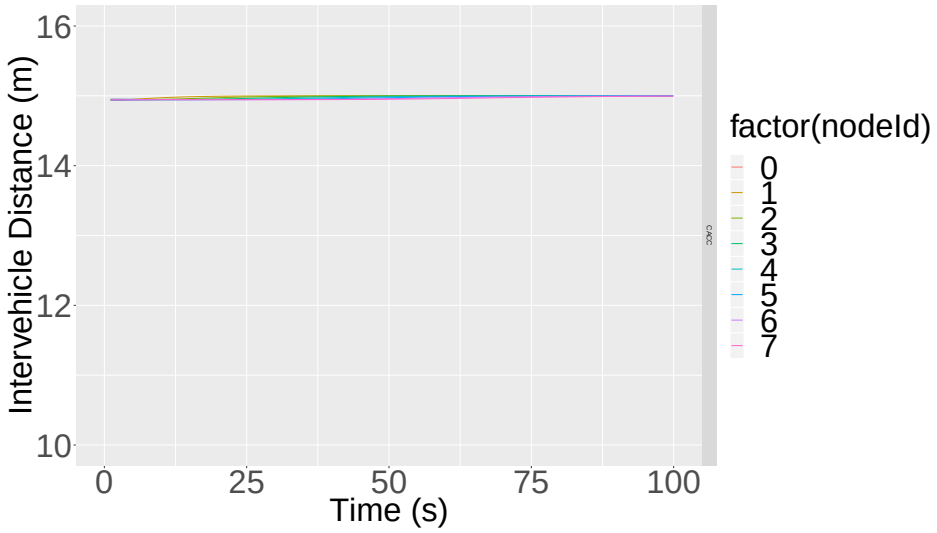


Figure 4.23: *Inter-vehicle distance under attack from five external constant attackers each attacking a different vehicle.*

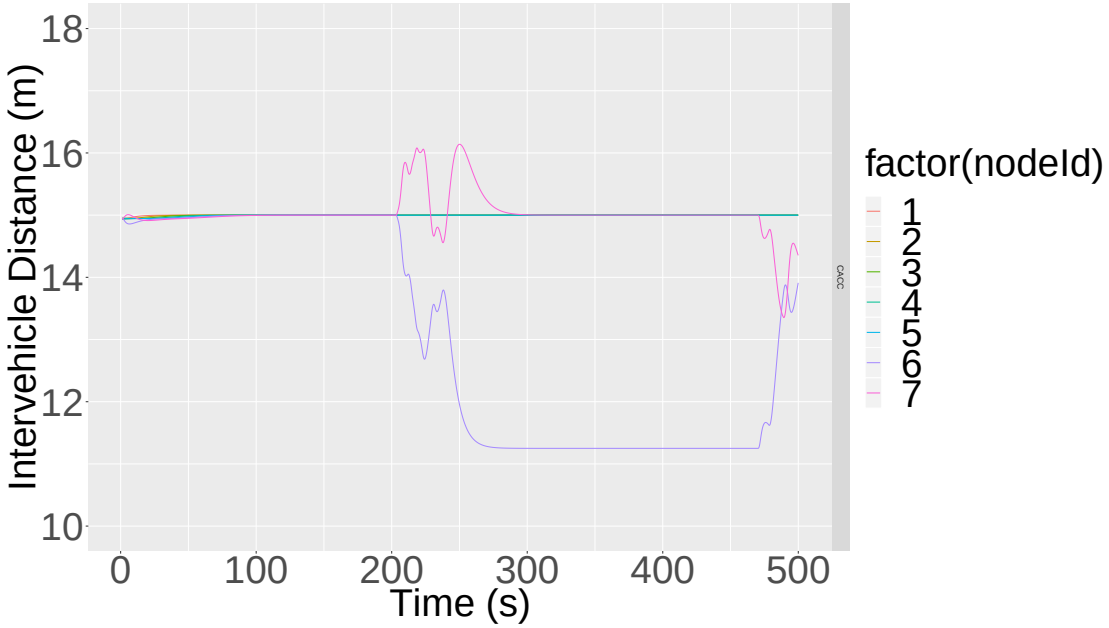


Figure 4.24: *Inter-vehicle distance under five internal constant attackers each attacking a different vehicle.*

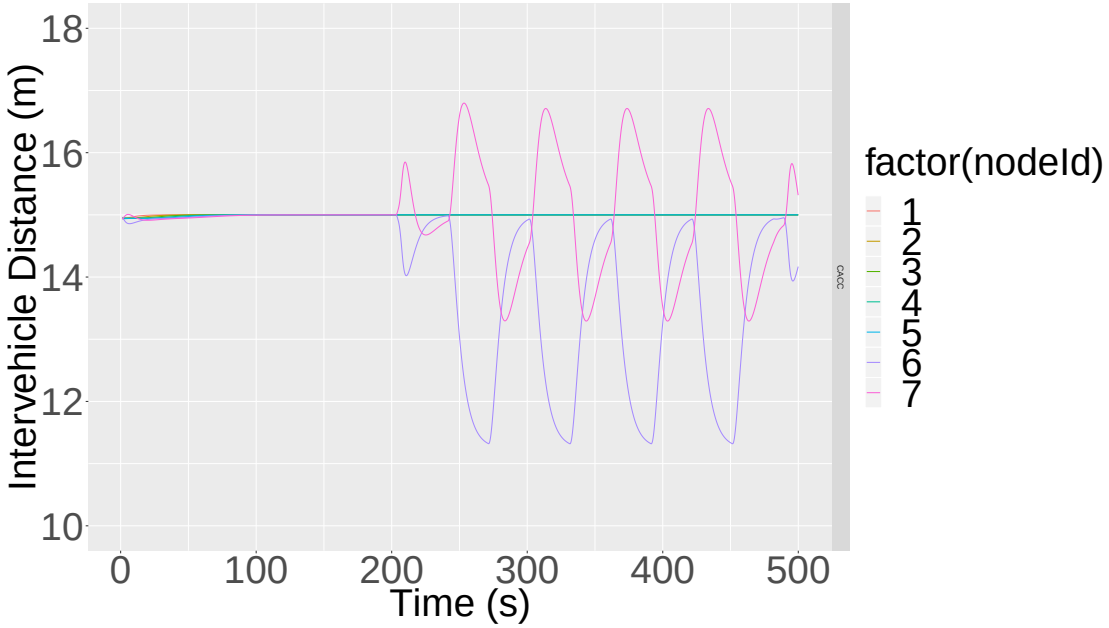


Figure 4.25: *Inter-vehicle distance under attack from five internal on-off attackers each attacking a different vehicle.*

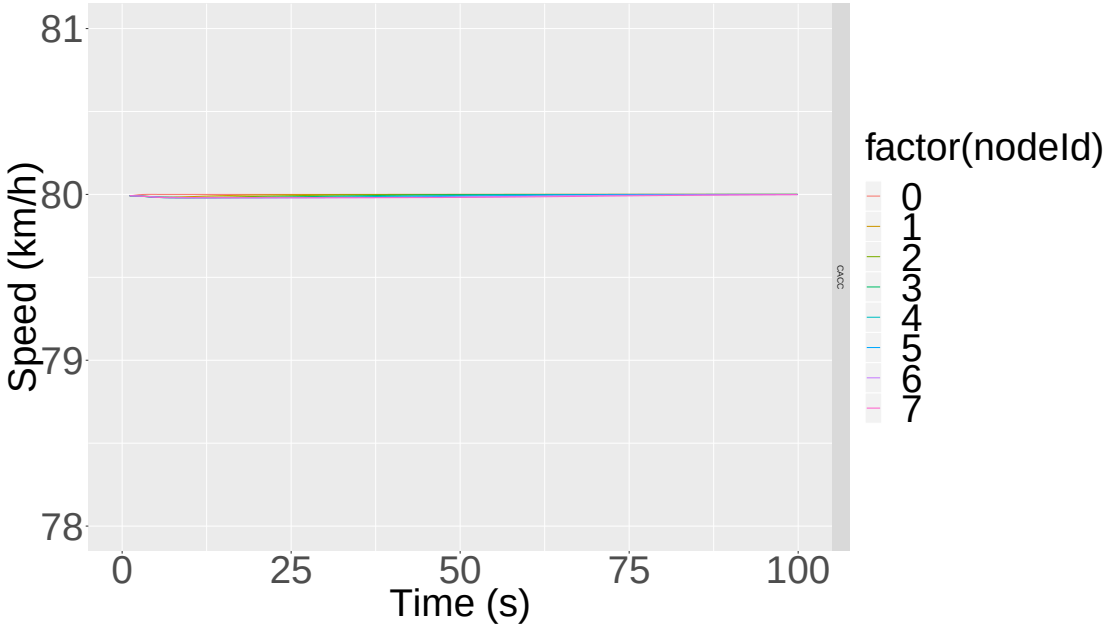


Figure 4.26: *Inter-vehicle Speed under attack from five external constant attackers each attacking a different vehicle.*

The speed of vehicles in the platoon reflects the inter-vehicle distance. The external attackers cannot make the platooning vehicles deviate from the ideal. The internal attackers only make the final attacked vehicle. The vehicle immediately behind the attacked vehicle deviates from the ideal, and the deviation matches that of a single attacker. The only real change is that the stability is slightly worse for node ID six under internal attacks shown in Figures 4.24 and 4.25 than just a single attacker. The vehicle speed shows very clearly when the MCDA fails; at $200s$, there is a period of instability for both constant and on-off attacks. Whether it is when the MCDA fails or when the MCDA suppresses the attack. In figure 4.28, the peaks correspond to when the attacker is attacking and has been dormant, just like when there is a single attacker.

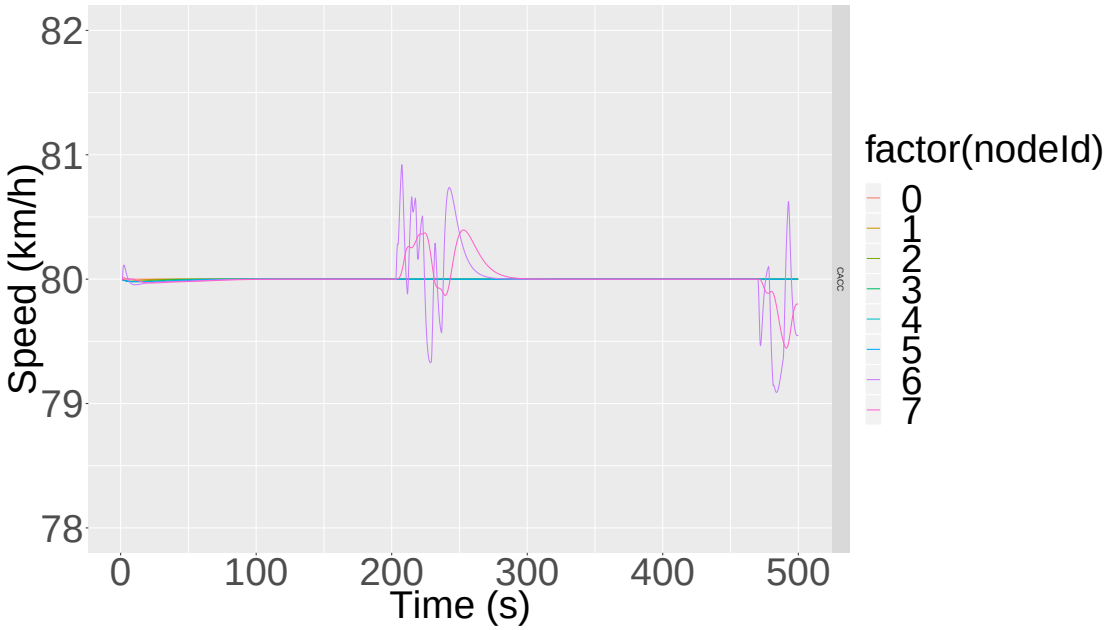


Figure 4.27: *Inter-vehicle speed under attack from five internal constant attackers each attacking a different vehicle.*

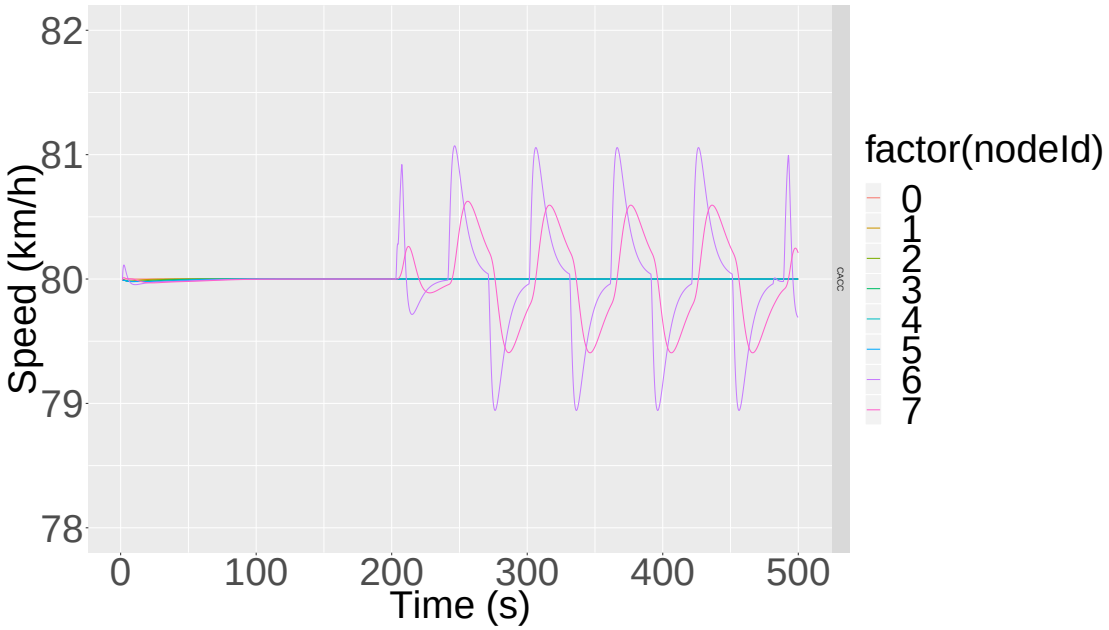


Figure 4.28: *Inter-vehicle speed under attack from five internal on-off attackers each attacking a different vehicle.*

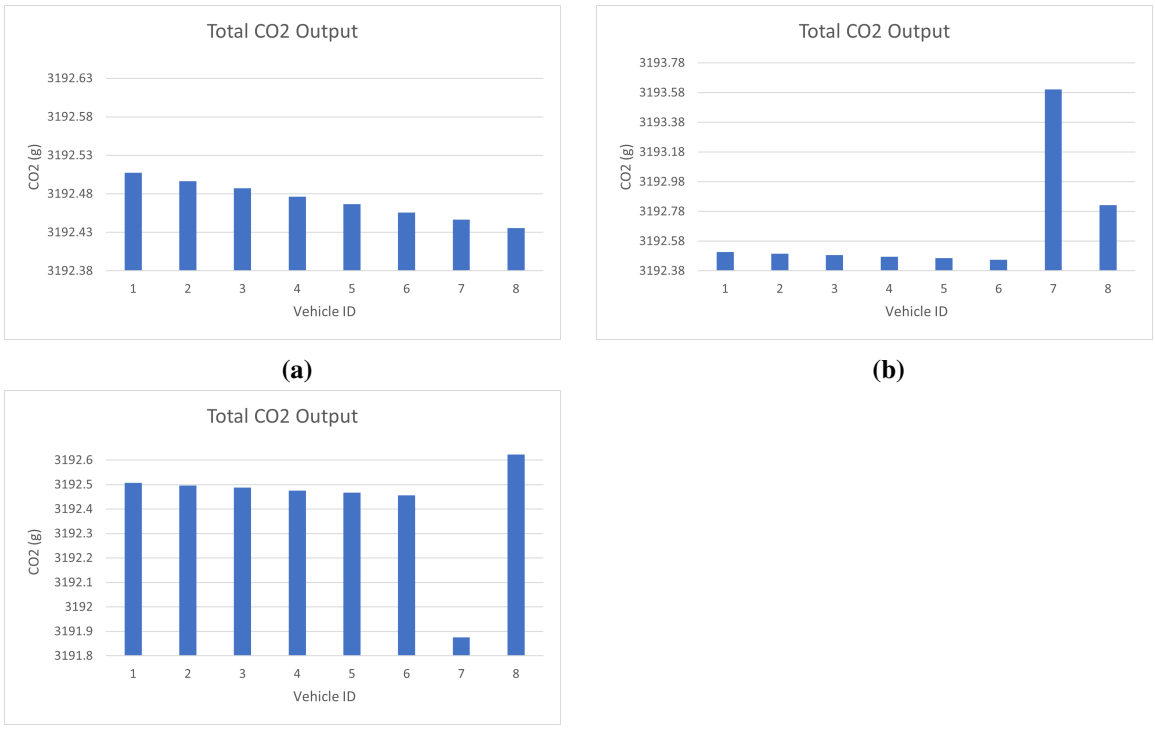


Figure 4.29: *Vehicle CO_2 output under (a) Constant external attack from five attackers, (b) Constant internal attack from five attackers and (c) On-off internal attack from five attackers.*

When considering the CO_2 usage of the platoon when externally attacked like this, two attackers are identical to if there is just a single attacker. Only for three attackers, vehicles four, five and six will output less CO_2 than before. In contrast, vehicles seven and eight produce slightly more. This means that individual vehicles are not seeing significant disturbance from the attack. Even when vehicles produce more or less CO_2, the amount is minimal at less than $0.005g$ over the test time. When looking at the internal attacker, 4.29a, the CO_2 output of the platooning vehicles is virtually ideal. The reason for this is that the use of MCDA can prevent the attacker from altering the driving behaviour of the platooning vehicles.

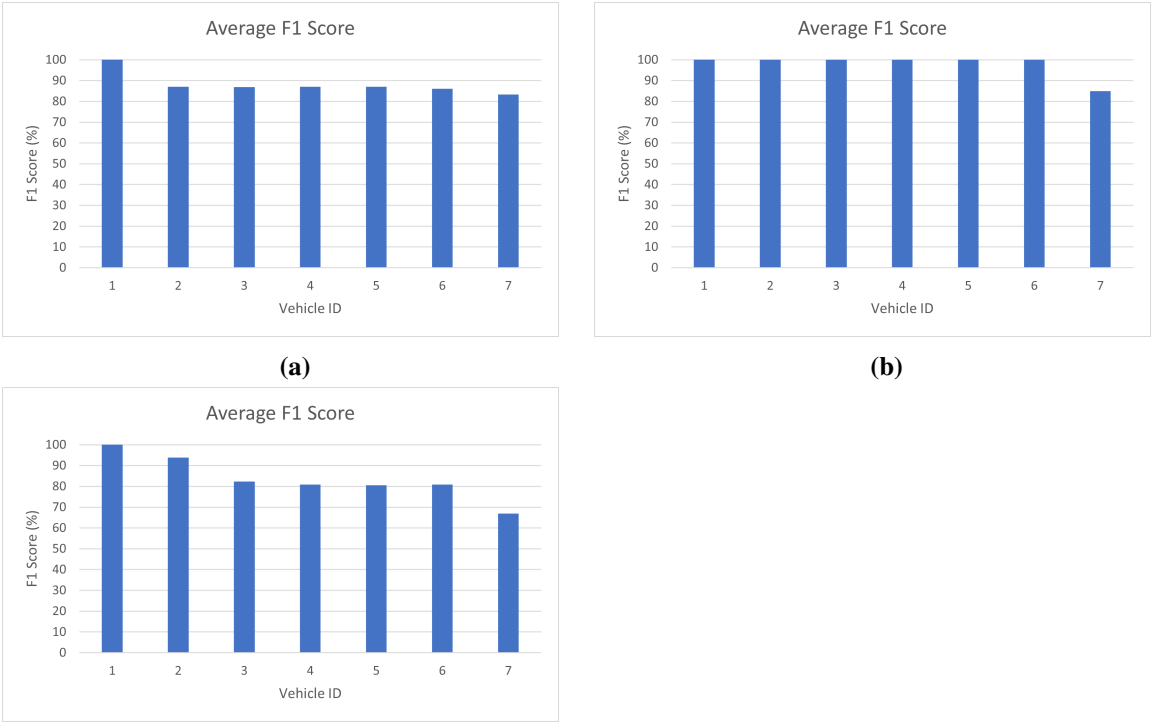


Figure 4.30: *Vehicle F1 score under (a) Constant external attack from five attackers, (b) Constant internal attack from five attackers and (c) On-off internal attack from five attackers.*

When looking at the F1 score of platoon members only using MCDA to prevent FDI attacks from multiple attackers on multiple victims, there are some interesting comparisons to be drawn from. First, the Constant attacks from internal and external attackers are similar. All attacked vehicles (two to six) have similar and high F1 scores in their respective scenarios. Vehicle seven drops its F1 score to about 85% for both attacks. Looking at the constant internal attacks, the F1 score is very high at $97 + \%$ for vehicles one to six. Such a high F1 score means that the MCDA accurately identified true and false beacons. What is strange is that vehicle ID 6 here is the final attacked vehicle and, therefore, is successfully attacked by the attackers when looking at the inter-vehicle distance and vehicle speed. What is happening here is showing the limitations of using only MCDA. It only takes a small number of false beacons to disrupt a platoon member. It prevents them from being able to platoon successfully. The on-off attacks, both internal and external, see a decline in the F1 score of platoon members, with the internal on-off attack seeing the most significant change with an 8% drop in F1 score for vehicle seven and a 5% to 10% drop in F1 score for all other members. While the external attacker also sees a drop in the F1 score for attacked vehicles of about the same as the internal vehicle, seven sees an increase in the F1 score of about 5%. The increase suggests that the F1 score of unattacked vehicles is linked to the number of false beacons the attacked vehicle receives. As these decrease, the F1 score increases.

4.6 MCDA and Trust Solution for External FDI attacks

MCDA, on its own, has shown that it cannot prevent internal FDI attacks; a simple trust method was developed to enable MCDA to counter this kind of threat. When MCDA and trust are used together, even the simple trust method described in the methods section, the attacker's ability to negatively impact the platoon's safety is reduced. The following section assesses how using MCDA and trust affects an external attacker's ability to attack the platoon. In all attacker models and with various numbers of attackers and attacked vehicles, the platoon can maintain ideal platooning inter-vehicle, as shown in Fig. 4.32 and 4.33 being examples of the worst performing situations. It is the only time when external attackers can have any effect on the platoon. Overall, however, all other cases tested include single attackers with multiple victims, multiple attackers with single victims and multiple attackers with multiple victims. This is all in line with previous tests with only using MCDA. Overall, all the use of MCDA and trust together to prevent external attackers slightly negatively affects the inter-vehicle distance of platoons. When attacked by six attackers and six victim vehicles, constant and on-off attacks were not seen before; however, these deviations are minimal at smaller than $+/-0.04m$. The performance of the platoon when under FDI attack is as expected due to the impressive performance of MCDA on its own, as the trust method is created to not interfere with the MCDA when dealing with an external attacker. Using MCDA and Trust together means the platoon can maintain safe platoon formation even under a range of external attackers trying to manipulate one or more member vehicles' behaviour.

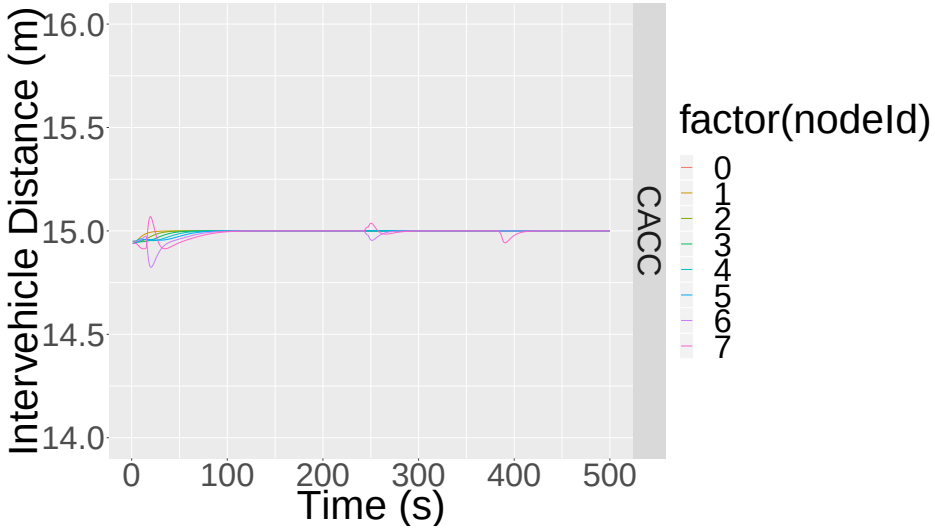


Figure 4.31

Figure 4.32: *Inter-vehicle distance under constant external attack six attackers and six victims.*

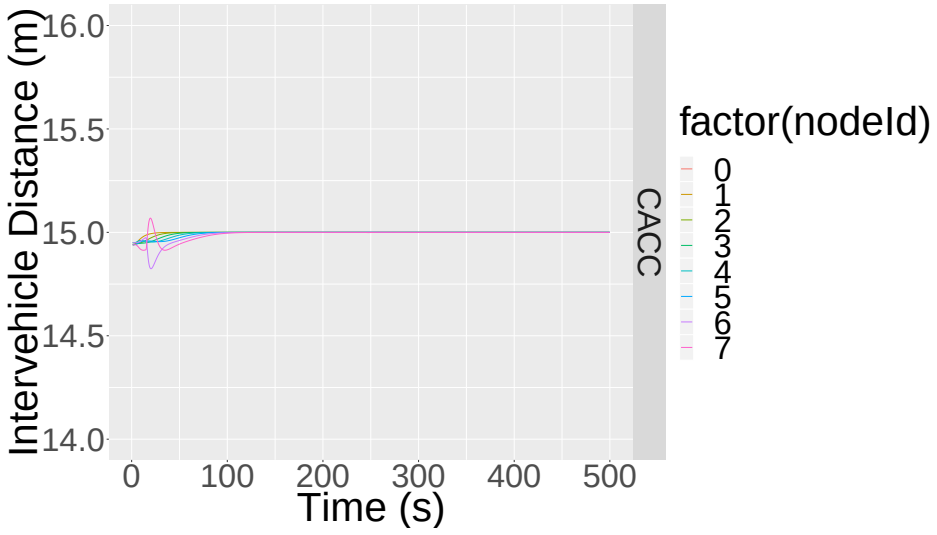


Figure 4.33: *Inter-vehicle distance under on-off external attack six attackers and six victims.*

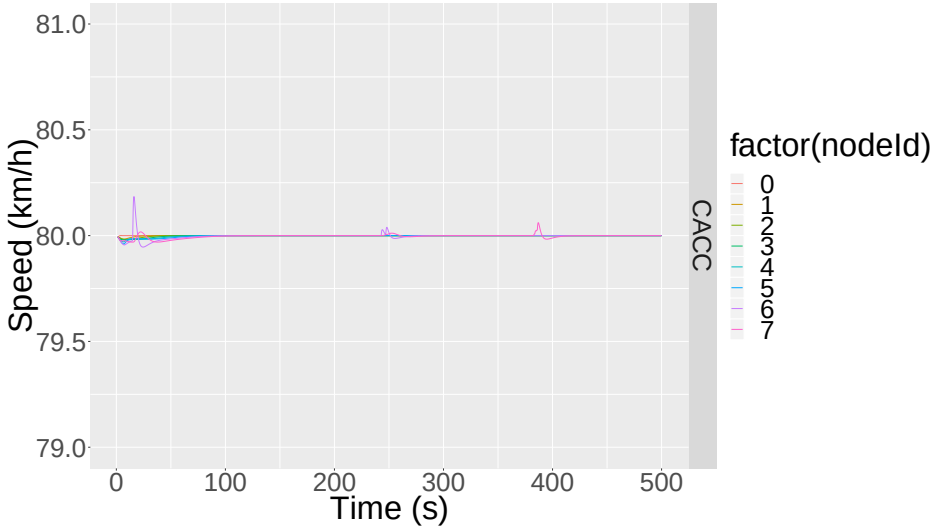


Figure 4.34: *Vehicle Speed under constant external attack six attackers and six victims.*

When looking at the stability of the platoon, the results are the same as before when there was no trust method complementing the MCDA solution. The platoon member vehicles can maintain an ideal speed of $80kmph$ or $22.22mps$, shown in Fig. 4.34 and 4.35. When looking at these graphs, it is important to understand that when all member vehicles, node ID one to seven, maintain the same speed as the leader vehicle, node ID zero, the platoon is considered stable as all member vehicles are platooning and travelling constantly without oscillating or other destabilising behaviours. The improvement in stability is evident when comparing the vehicle speeds for external on-off attacks without any solution in Fig. 4.7 and now using MCDA and trust in Fig. 4.35 and 4.34. Without any solution, the platoon starts oscillating from the position of the attacked vehicle as the vehicle switches between attacked and not attacked. The oscillation behaviour is completely removed when MCDA and trust are used together for external on-off attacks, regardless of the number of attackers and victims. When there are six attackers and six victims within the platoon, the attackers can disrupt the platoon slightly. This is predominately at the start with the $0.2kph$ increase in speed by Node 6, the second to last vehicle in the platoon. What triggers this is that the trust algorithm enables the attacker to bypass the MCDA briefly and successfully at this point before it is quickly corrected. Then, when under constant attack, there are two points where it would appear that the trust enables the attacker to bypass the MCDA for Nodes 6 and 7. This is not ideal; however, it is only when an attacker attacks all members of the platoon at the same time.

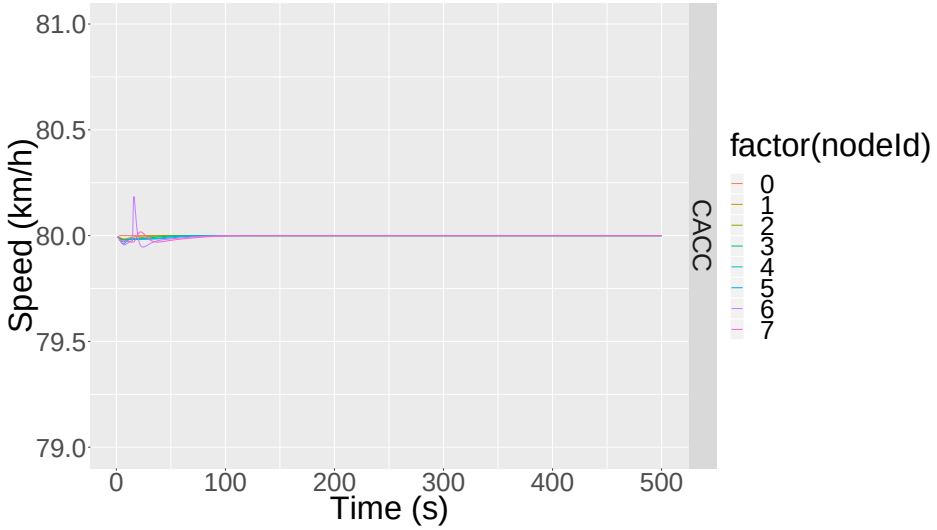


Figure 4.35: *Vehicle Speed under on-off external attack six attackers and six victims*

When using MCDA and trust together to prevent FDI attacks from an external attacker, the CO_2 output of the platoon is the same as if there was no attacker. This is also true of the two cases above, where the attacker has negatively impacted the platoon. This is because the platoon members can receive all the environmental benefits of platooning even under a range of FDI attacks due to MCDA and trust removing beacons, the false beacon and replacing them with safe alternatives, thus enabling the platoon to maintain ideal formation. Like when MCDA only is used, the attacks that see the most improvement are those of the on-off attacker who, on an unprotected platoon, can cause a significant increase in CO_2 output due to the engine's increased work to maintain formation. Figure 4.36 and 4.37 show the average output of each vehicle under each of the attacks. The vehicle CO_2 is identical to when just MCDA is used. The two being the same is because the vehicles travel the same way over the same distance; therefore, the ideal vehicle CO_2 output of both scenarios is the same.

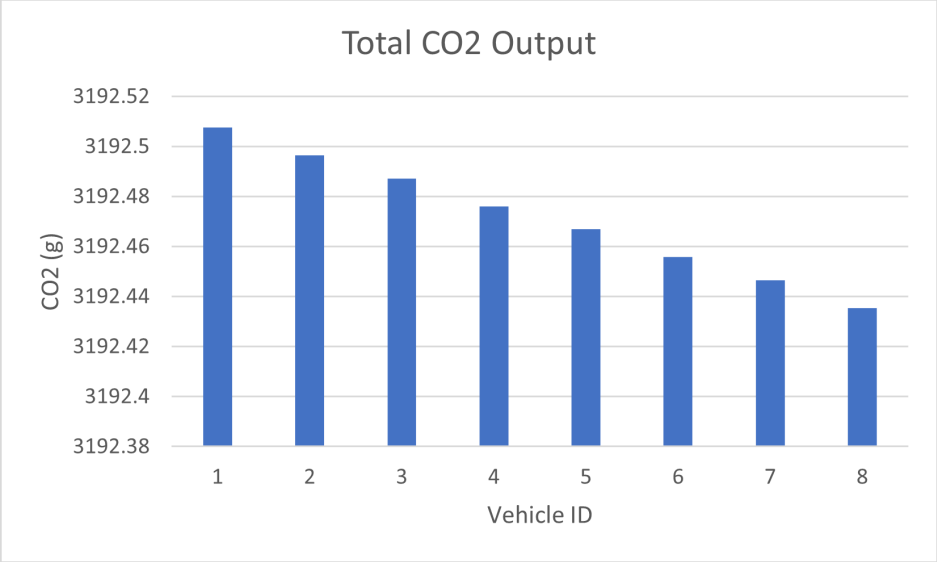


Figure 4.36: *Vehicle CO_2 output under external constant attack six attackers and six victims.*

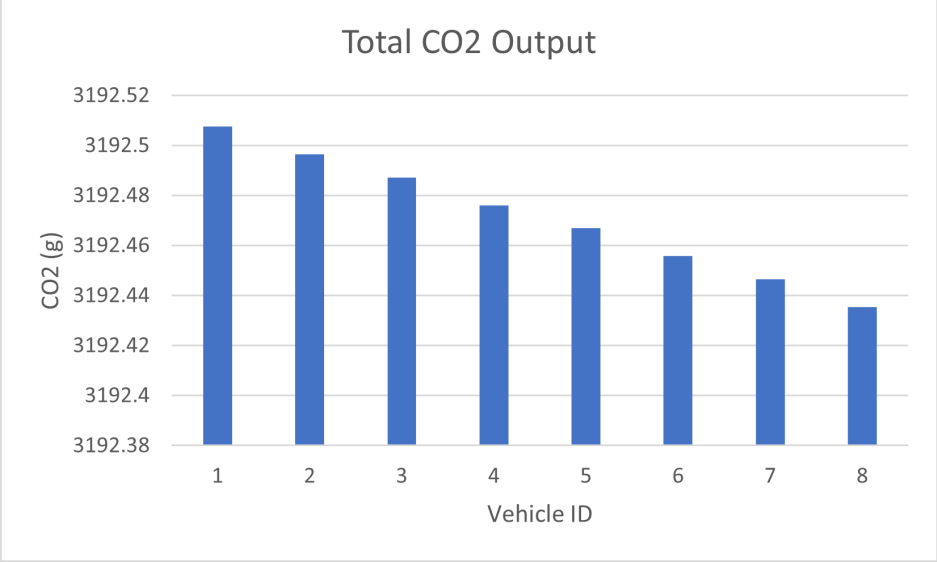


Figure 4.37: *Vehicle CO_2 output under On-off constant attack six attackers and six victims.*

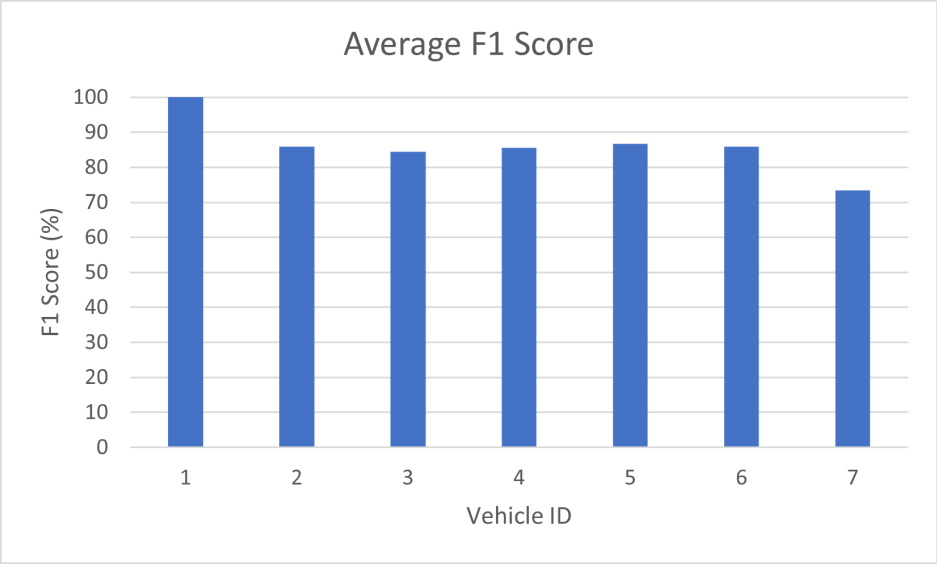


Figure 4.38: *Vehicle F1 score under constant attack six attackers and six victims deveated from that is expected.*

When using MCDA and trust together, the F1 score of vehicles in the platoon when dealing with the external attacker remains largely the same, as the vehicle's physical performance is the same as with MCDA alone. MCDA, on its own, is very good at identifying and removing false beacons. This leads to the F1 score of the vehicles under external attacks being remarkably similar with little changes. Firstly, when there are six attackers and six victims, as seen in the inter-vehicle distance and speed for a constant attack on the platoon, there is a drop in the F1 score for vehicle seven to just below 75%. This reflects that there are times when the use of MCDA and trust together fails to protect the platoon from attack. The rest of the differences surround the on-off attacks, with the most meaning full been about 8% improvement for vehicle ID 2 when six attackers are attacking six victims in the platoon. This means that for the external attacker, the MCDA is the primary method for screening out the false beacons injected into the platoon by that attacker and not the trust method. The fact that the MCDA and not the trust method is the driving force behind the selection of beacons is an advantage because the attacker cannot cause innocent vehicles in the platoon to be unfairly sanctioned for actions they have not committed. Suppose trust was the driving force behind the beacon selections. In that case, the vehicle the attacker is pretending to be would see the trust between itself and others decrease even though it is being truthful and not attacking. As such, using trust and MCDA together significantly improves each other's performance without compromising the other under external FDI attacks.

When looking at the F1 score for platoon members under an on-off attack by an external attacker, there is an even more significant drop in the average F1 score. With the attacker now attacking in an on-off way, the trust method and the MCDA method conflict with each other more as the trust becomes degraded from the attacker's presence and, as such, leads to more

Figure 4.39: *Vehicle F1 score under on-off attack (a) two attackers and two victims, (b) six attackers and six victims, (c) one attacker and two victims, (d) one attacker and six attackers, (e) two attackers one victim and (f) six attackers one victim.*

false positives, which reduce the F1 score of member vehicles. The average F1 score for member vehicles under each attack is 85.6%, 83.6% and 85.6% when under multiple attackers, multiple victims, multiple attackers, single victim and single attacker multiple victims, respectively, which are slightly better overall compared to the constant attack, that is except for multiple attackers single victim who sees a 0.9% reduction in F1 score compared to the constant attack. As seen in the constant attack, the member vehicle ID one is not attacked and therefore scores 100%. When looking at the F1 score of only attacked vehicles, the average F1 score drops to 83.2%, 80.8% and 83.2% when under multiple attackers multiple victims, multiple attackers single victim and single attacker multiple victims respectfully. The drop in F1 score is between 2.8 and 4.2% compared to the constant attack. When multiple attackers target a single vehicle, the attacked vehicle, vehicle ID two, the F1 score drops to an average of 58.9%. The F1 score so low is problematic as this means that the vehicle can only successfully identify the false beacons just under two-thirds of the time. This is caused by the trust method degrading the trust between the vehicle and the vehicle in front of it. When the MCDA and trust interact together because the trust is so low, the high MCDA score cannot overcome the low trust value. However, it is essential to point out that the true beacons are lost and instead replaced by beacons from the leader, enabling the vehicle to maintain safe platooning even with all the fake beacons the vehicle received.

4.7 MCDA and Trust Solution for Internal FDI attacks

For the platoon's safety, a simple trust method is implemented when, under an internal FDI attack, an attack from another member vehicle, MCDA, on its own, struggles to identify and counter such attacks. Overall, the performance of the inter-vehicle distance is significantly improved when using MCDA and trust to prevent internal FDI attacks, reducing the attack from $\pm 3m$ from the ideal to less than $\pm 0.3m$. The improvement in the inter-vehicle distance is an improvement of 90%. Such an improvement is outstanding as such deviation is not ideal; it broadly enables the platoon to stay safe. Examples of the deviation are shown in Fig. 4.40. Unlike in Fig. 4.33, the inter-vehicle distance maintains close to the ideal inter-vehicle distance in all scenarios, particularly when the attacker attacks in an on-off method. The method quickly corrects and prevents significant deviation from the ideal inter-vehicle distance overall. Looking at the on-off methods, it is clear that when the attacker has been truthful, the trust between the vehicles increases. When they are attacking, the trust falls very quickly, as in Fig. 4.40c and 4.40d, the deviation from the ideal inter-vehicle distance follows a repeating pattern. While using MCDA and trust together does not prevent an attack on the platoon, it significantly dampens the attack's impact, reducing it to a more managerial level that may have little impact on the overall safety of the platoon.

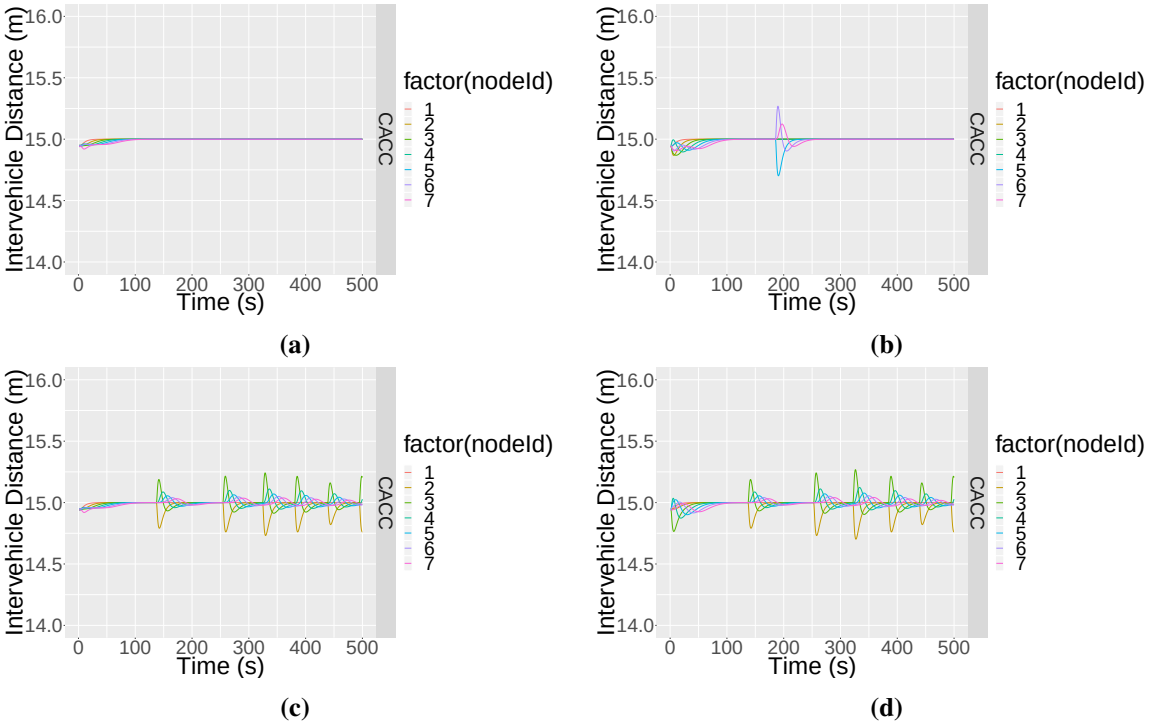


Figure 4.40: *Inter-vehicle distance under internal attack (a) constant one attacker, (b) constant six attackers, (c) on-off one attacker and (d) on-off six attackers.*

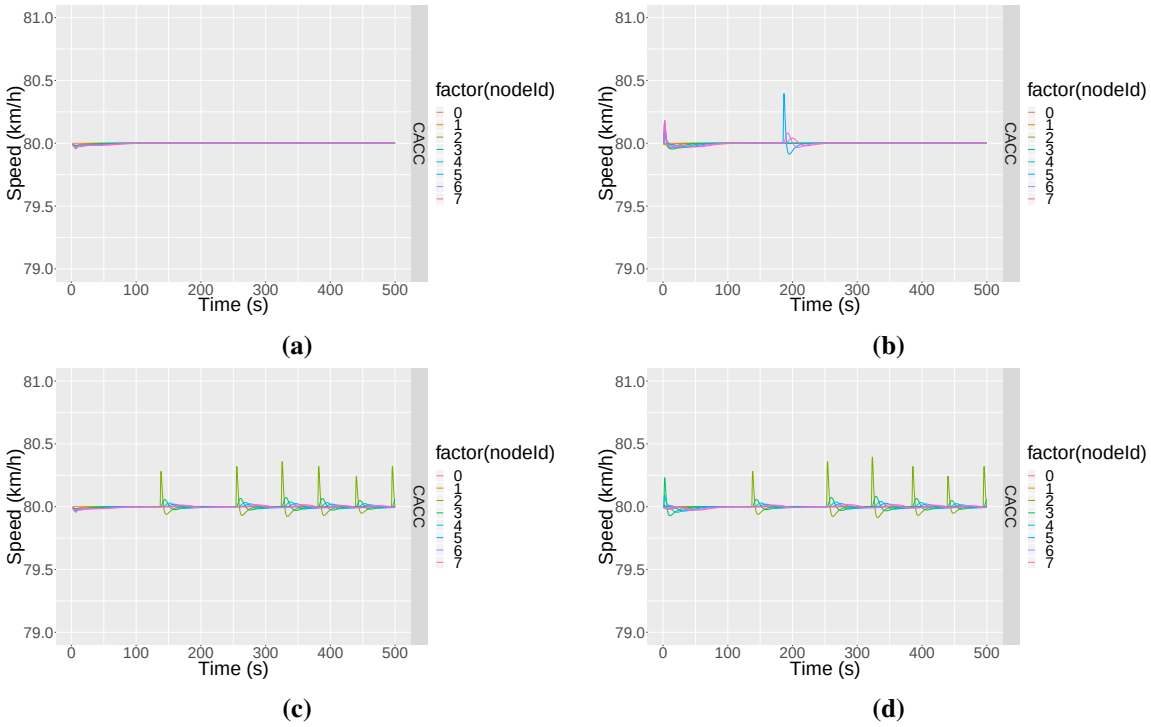


Figure 4.41: *Vehicle speed under internal attack (a) constant one attacker, (b) constant six attackers, (c) on-off one attacker and (d) on-off six attackers.*

This leads to the platoon's stability, which is clearly shown by the speed of each vehicle in Fig.4.41. This figure clearly shows that the attacker can destabilise the platoon, as shown by the spikes in speed. The spikes in speed are worse and create more instability for the on-off attacker as the attacker can repair its trust when not attacking. The constant attackers also see an abnormal spike in speed at around the $180s$ mark when three or more attackers are in the platoon attacking the vehicle directly behind them—a more significant initial spike in speed, as seen before. The more significant initial spike in speed is from where the attacker starts their attack and is established as untrustworthy. Then, as the number of attackers increases to four or more, the stability of the platoon under constant attack breaks down more. A second spike in speed may occur for four attackers and will happen for five more attackers. The spike in speed happens between $160s$ and $230s$. The vehicle with an increased speed is not always the same; however, when there are six attackers, the affected vehicle is vehicle five and happens at the same time $180s$. For four and five attackers, the timing and the affected vehicle changed. Vehicles ID five and six also spike when under five constant internal attacks on multiple vehicles. However, when the vehicles increase their speed under constant attack, it is always a minimal amount, less than $0.5kmph$. While this is not ideal, the small amount of speed increases and the change is within acceptable levels for such a short period.

Looking at the on-off attacks, the attacker can destabilise the platoon significantly more

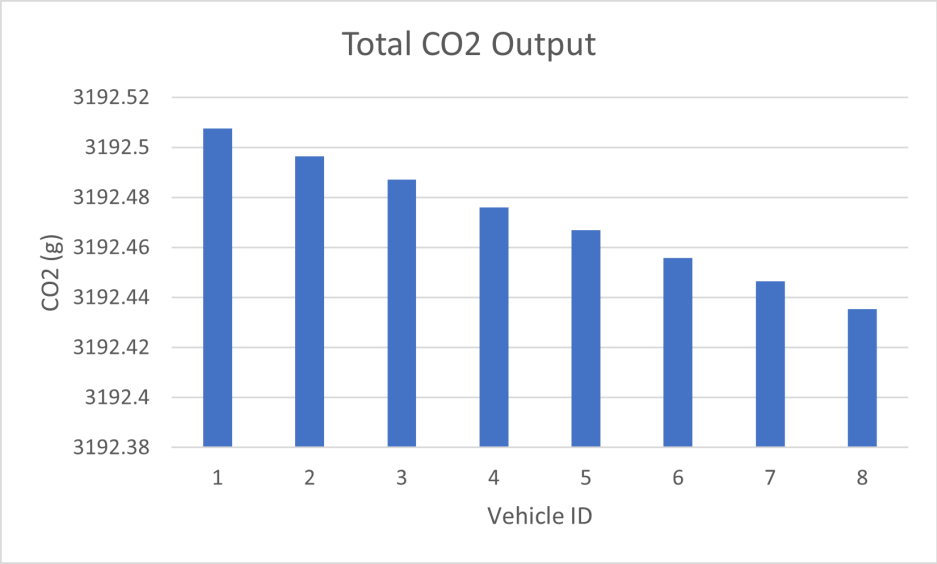


Figure 4.42: *Vehicle CO_2 output under constant internal attack attacker.*

than the constant attacker; however, the overall impact is reduced. When the attacker attacks, their position in the platoon plays a vital role in how unstable the platoon becomes; this is not seen in the constant attacker. In addition, increasing the number of attackers also does not necessarily mean the attacker can create more destabilisation. There is no increase in the severity of the attack by increasing the number of attackers. The main impact on the severity and regularity of the attack on the platoon is that shorter cycles of on-off attacks are more effective than longer cycles. The increase in speed is still less than $0.5kmph$, which has a minor impact on stability and safety; however, the overall platoon is not dangerously affected by the attacks.

The environmental impact on a platoon from one or more internal attackers when using MCDA and trust is relatively small; however, unlike with the external attacker, the internal attacker does cause there to be an increased level of CO_2 outputted by the platoon; this is particularly clear in the example shown in figure 4.42. The reason for this is due to the peaks caused during the attack. As such, the constant attacker only deviates from the control when there are four or more attackers; otherwise, the results are relatively identical to the ideal and the external attacker. When there is a single peak in the speed, there is a minimal increase in the CO_2 output for the vehicle that increased its speed. Therefore, there is a slight loss in the efficiency of the platoon, which, while not ideal, is insignificant; however, it becomes significant over a more extended period.

On the other hand, the on-off attacker has a more noticeable impact on the CO_2 output of the platoon. Here 4.43, there is an increased CO_2 output, which increases when there are more peaks in the vehicle speed. Although the platoon members output more CO_2, the amount is less than what is seen in the control, where there is a noticeable increase in the

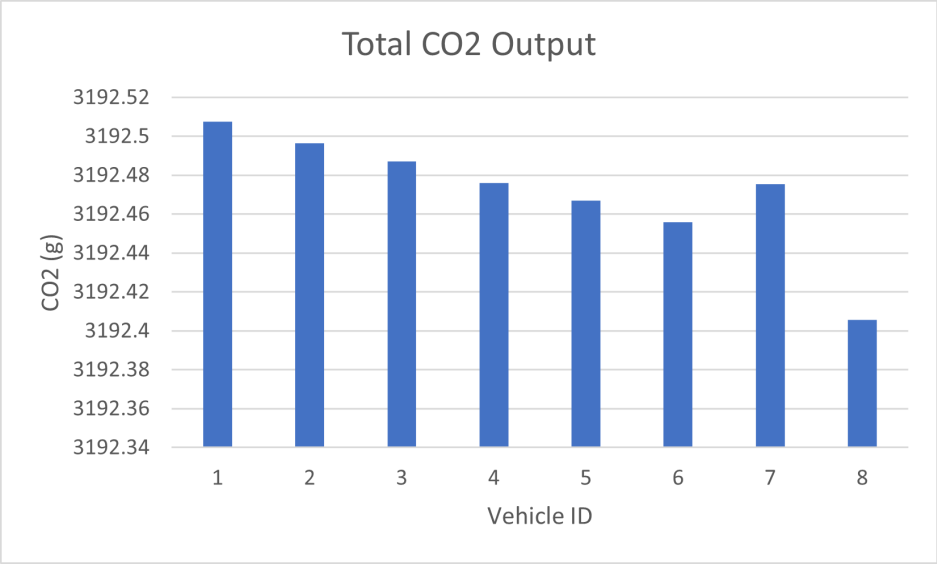


Figure 4.43: *Vehicle CO_2 output under internal attack six on-off attackers.*

CO_2 output of each platoon member.

The F1 score of the platooning members under an FDI attack from an internal attacker is excellent, with scores as high as 98.4% when dealing with up to six internal attackers, shown in figure 4.44. There is a significant improvement in the overall F1 score when MCDA and trust are used together to combat internal attacks. This is reflected in the physical improvements in inter-vehicle distance and vehicle speed. There is a significant improvement to the F1 score over what was previously seen with MCDA alone, and it has improved the physical attributes of the platoon, such as inter-vehicle distance and speed. It does need to be pointed out that while trust and MCDA together do improve the F1 score, the effect is not as good for on-off attacks, especially as the number of attackers increases as shown in 4.45 where the F1 score for the platooning vehicles is significantly less. The improvement in the F1 score is because of the way that the trust and MCDA are integrated; unless a vehicle has both a high trust and MCDA score, then the beacon will be rejected. Therefore, even though the attacker's beacons would produce a high F1 score because the attacker quickly becomes untrustworthy, their beacons are ignored until the trust has been repaired. The fact that the trust can and will be repaired over time is why the on-off attack can have some effect on the platoon, even if the attack is dampened and suppressed. While it is not a perfect system, it shows that using MCDA and trust together can prevent internal attackers from significantly impacting the platoon.

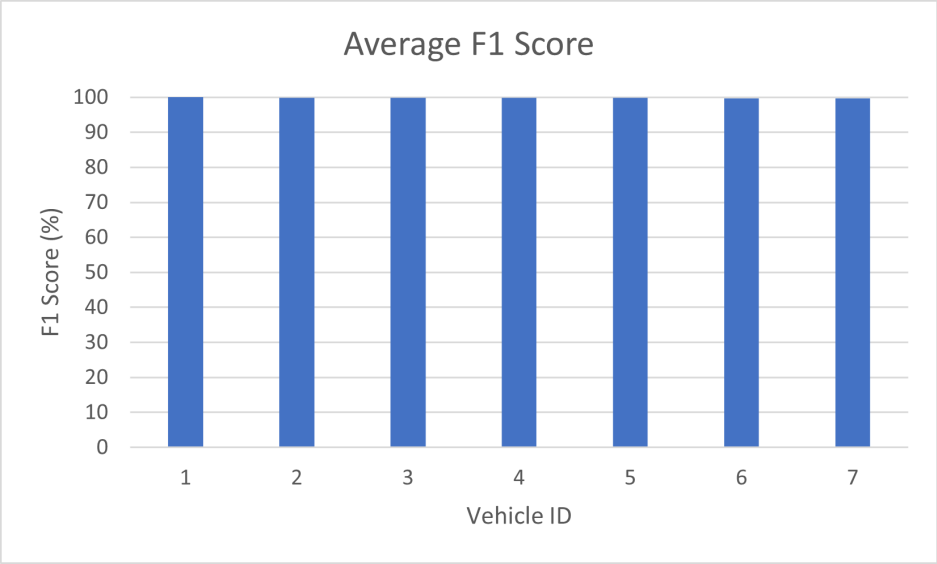


Figure 4.44: *Vehicle F1 score under internal attack constant six attacker*

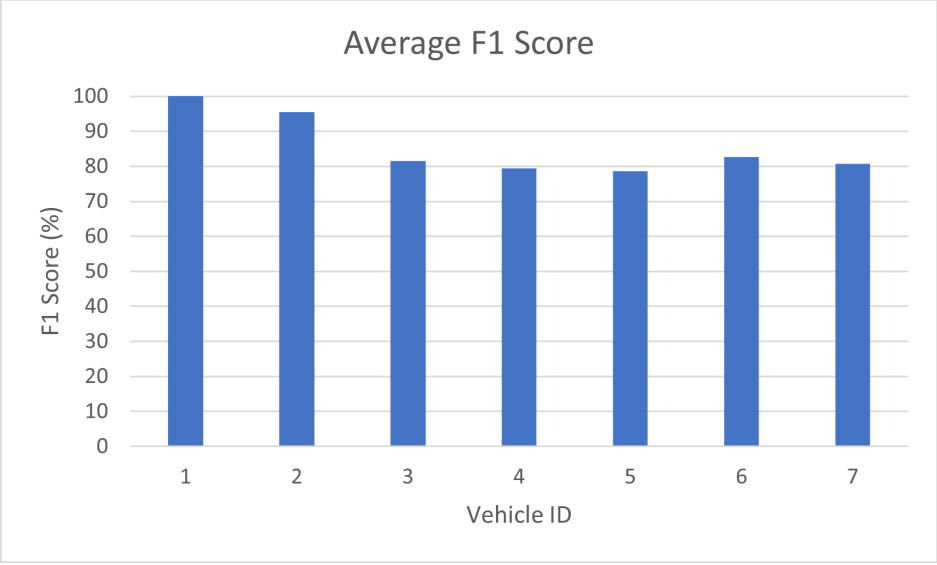


Figure 4.45: *Vehicle F1 score under internal attack on-off six attacker*

4.7.1 MCDA, Trust and Sanctions

The attacker can be suppressed using MCDA, but the attacker is not identified using MCDA alone. Attackers can be identified using trust. By implementing a trusted method in addition to MCDA, it is possible to suppress an attacker and identify the ID of vehicles that are poorly trusted that are members of the platoon, enabling further sanctions to be placed upon them, such as rejecting them from the platoon or preventing them from being able to join future platoons. It should be recognised at this point that using trust to identify and sanction vehicles is not without its risks of exploitation. When combating internal attackers, due to how CACC platooning works, regularly untruthful vehicles will only be read beacons transmitted by the preceding vehicle. As such, they can report to the leader when a vehicle is lacking trust. However, when dealing with external attackers, they are not part of the platoon, so the sanctioned vehicle will not be the attacker. While not ideal, this is how the current implementation works. Further development of the trust and sanction method is outside this thesis's scope. As discussed above, MCDA cannot adequately protect against internal FDI attacks. However, as shown in this section, trust significantly improves the platoon's ability to prevent FDI attacks. If the attacker constantly attacks the platoon, then the attacker is identified almost modestly. Within just $4s$, the attacker's trust value drops to the point where the beacons are ignored and replaced by the leader's beacon. At this point, the MCDA and trust countered the attacker and the platoon formation slowly returned to its ideal state. Finally, the vehicle is identified as an attacker if the trust does not improve over the following $11s$.

Figure 4.46 shows the constant FDI attack. Only the results of the constant attack are shown as the on-off FDI attack, which will produce the same results as the active and inactive time is $30s$, meaning the attacker will be identified and sanctioned in the first attack cycle and then sanctioned. With the constant attack, the time the simulation runs before the attacker is identified is just $16s$. In the previous examples, no sanctions were in place; therefore, the on-off attacker could impact the platoon differently. For instance, the platoon may experience periods of relative stability during the inactive times, followed by disruptions during the active times when the attacker is identified and sanctioned.

Having a lag between the attacker compromising the platoon and the trust showing the attacker to be untrustworthy is not ideal as it does present a chance for damage to the platoon. The platoon is protected from the most damaging behaviours an attacker can inflict due to the MCDA, which can suppress the worst of the effects caused by the attacker. In this section, the attacker tries to force vehicles to collide and use a significantly higher speed value in their attack. While the attacker can severely compromise the platoon's safety, it is only for a short time, and the trust method can start correcting the attack within $4s$. In this example, an extreme speed increase of $+10mps$ or $36kmph$ is added to the attacker's speed.

There are two ways in which the attacker vehicle is sanctioned; the first is by ending the platoon simulation and naming the attacker. Ending the simulation and naming the attacker

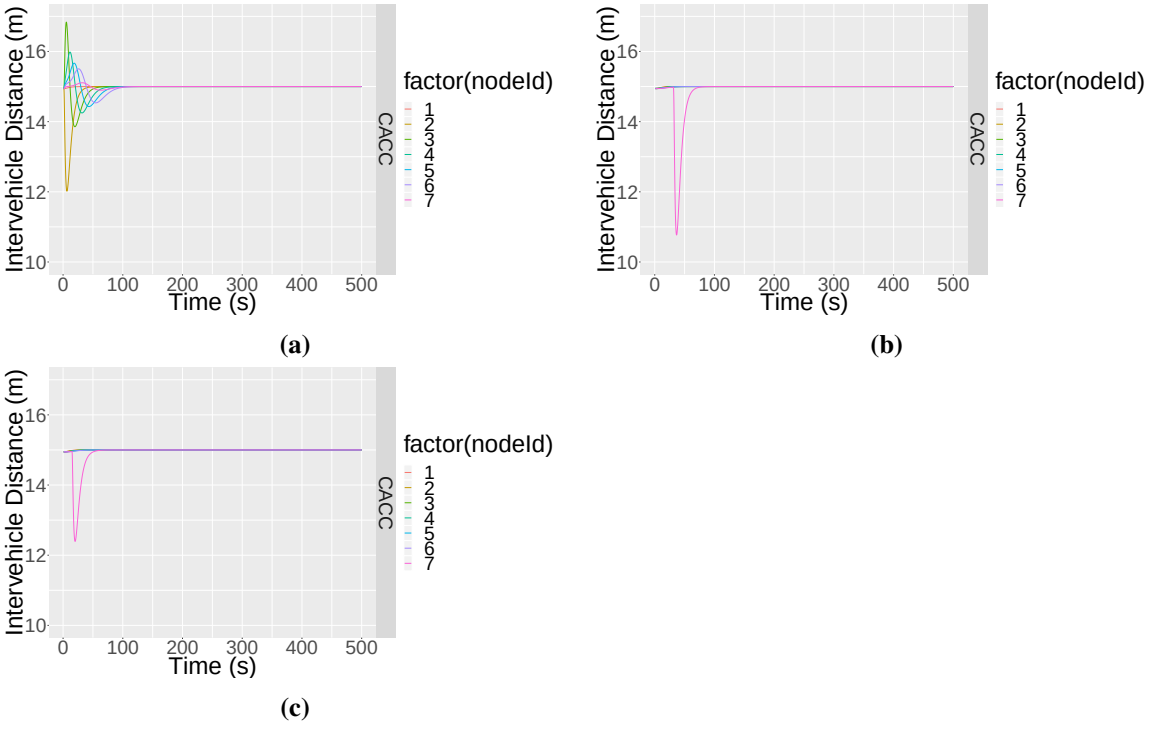


Figure 4.46: *Inter-vehicle distance under internal attack where low trust is ignored (a) Constant attacker, (b) Fixed vehicle on-off attacker and (c) Random vehicle on-off attacker.*

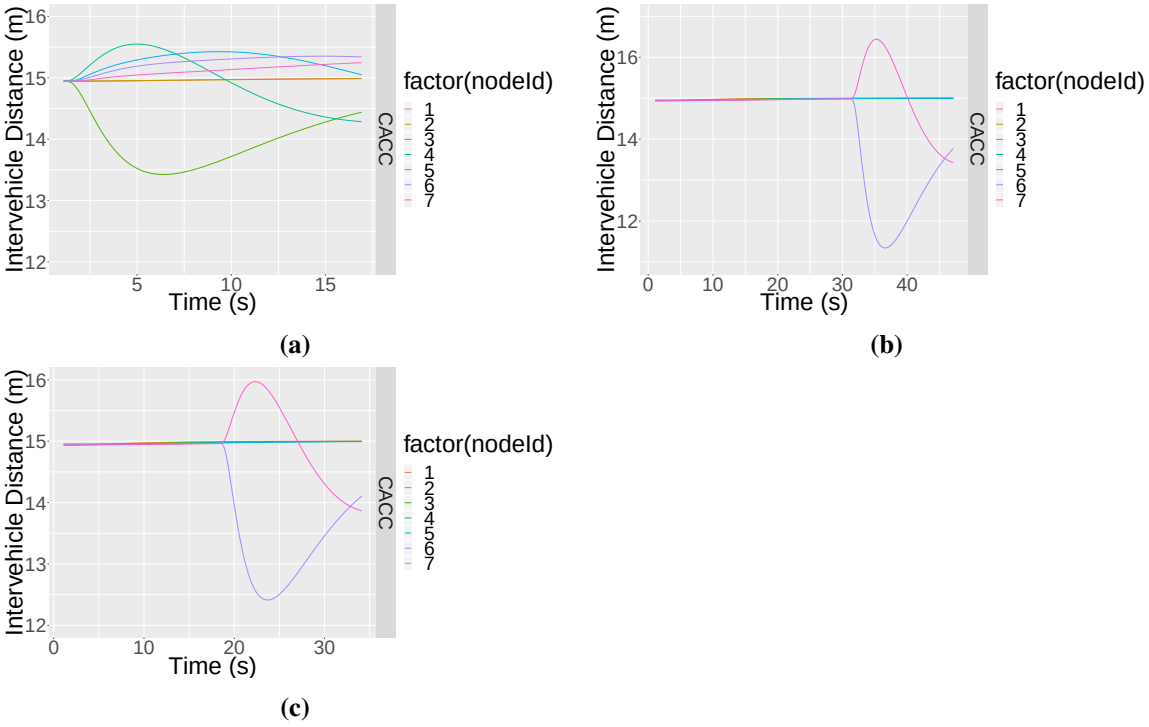


Figure 4.47: *Inter-vehicle distance under internal attack where low trust ends the simulation (a) Constant attacker, (b) Fixed vehicle on-off attacker and (c) Random vehicle on-off attacker.*

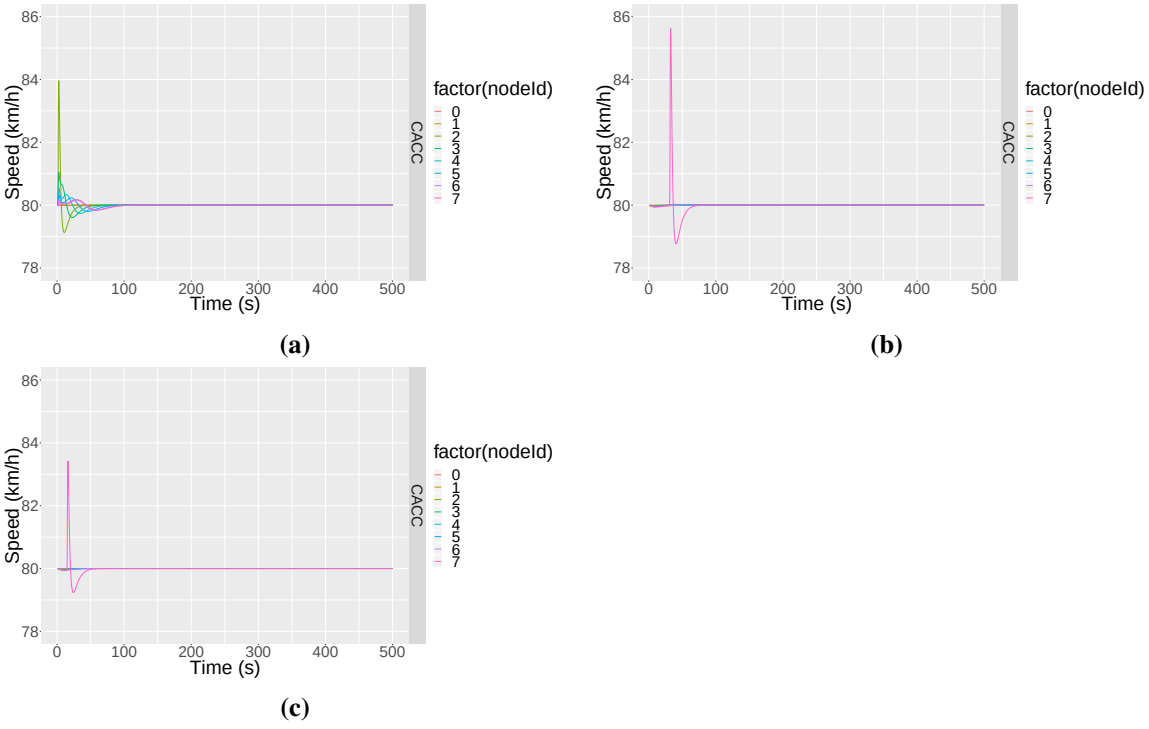


Figure 4.48: *Vehicle speed under internal attack where low trust is ignored (a) Constant attacker, (b) Fixed vehicle on-off attacker and (c) Random vehicle on-off attacker.*

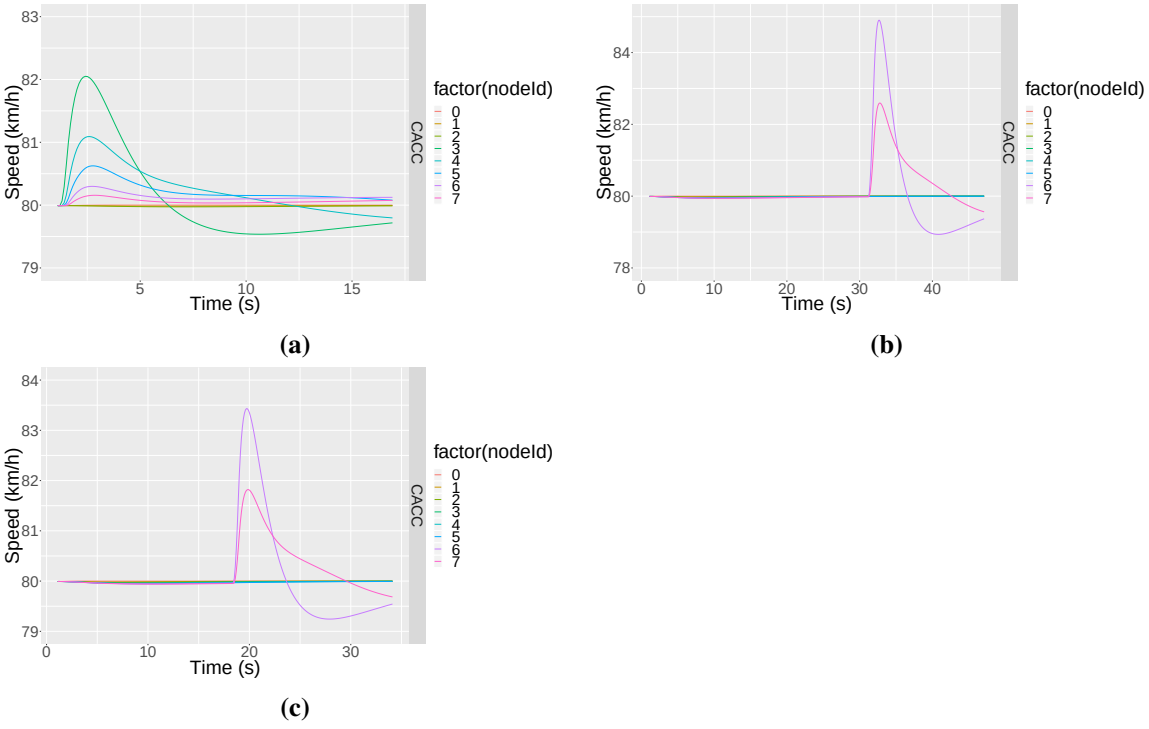


Figure 4.49: *Vehicle speed under internal attack where low trust ends the simulation (a) Constant attacker, (b) Fixed vehicle on-off attacker and (c) Random vehicle on-off attacker.*

simulates the scenario that the platoon has disbanded. The attacker's information can then be sent to back office infrastructure, where additional steps can be taken. The second method is that the attacked vehicle will always ignore the attacker's beacon from that point on. By ignoring the attacker's beacon, the attacker cannot disrupt the platooning formation by injecting false beacons. The attacker, however, is still a platoon member and receives all the benefits of being a platoon member. Both cases have advantages and disadvantages. The first method means that the platoon will disband, meaning all members will lose the benefits of platooning. However, the attacker is no longer getting the benefits of platooning. The second method means the platoon remains intact, but the attacker still benefits from platooning. Figure 4.46 and 4.47 show how the two methods of dealing with the attacker differ. When there is a constant attacking attacker, the attacker is detected very quickly, as shown in figure 4.47a as the simulation length is less than $17s$ long for the constant attacker. The attack starts just after $1s$, and by $6s$, it is at its maximum effect on the platoon. This is shown by Node 3 reducing its inter-vehicle distance.

At this time, the attacker is active and able to attack the platoon, and Node 3 trust in Node 2 will decrease. After $6s$, the attacker's effect on the platoon starts to decrease, with the attacked vehicle returning to its ideal platooning position. At this point, The MCDA and trust prevent the attacker from negatively affecting the platoon, and it is returning to ideal. Just after the $16s$ mark, the simulation ends as the attacker has been identified, and the platoon is to disband, thus ending the simulation. The attacker here is Node 2, as Node 3 only uses beacons created by Node 2 due to how CACC handles beacon usage. For the on-off example, the attacker is detected much later as their attack starts later. However, the attacker is still swiftly identified and counted in both cases. In these cases, the attacked vehicle is both Node 6 as it reduces its inter-vehicle distance. This means that Node 5 is the attacker and is identified through the fact that the trust score for Node 5 will be 0.

Figure 4.46 shows the same pattern initially, with the attacker's influence on the platoon reaching its peak at $5s$ before recovering to the ideal. As the platoon is not disbanding, the simulation continues, with the directly attacked vehicle ignoring the attacker's beacons and replacing them with beacons from the leader vehicle. This enables the platoon to maintain safe platooning even when under FDI attack.

When the attacker is attacking using an on-off method ether attacking for a fixed or random period, then the MCDA and trust method can prevent the attacker from damaging the platoon formation as shown in figure 4.46b, 4.46c, 4.47b and 4.47c. Here, the platoon can safely operate under ideal platooning before the attacker disrupts the platoon. The attacker is unnoticed for longer when attacking for random periods compared to the attacker that attacks for a fixed and repeated length of time. When the attacker can negatively impact the platoon, they can only do so for a short period, with the most deviation from the ideal being $4s$ after the attacker starts to deviate away from the platoon ideal with the vehicles, then gradually returning to the ideal as seen with the constant attackers. From here, there is little difference between it and the constant attacker.

Chapter 5

Discussion

This section will discuss in detail the benefits of using MCDA to prevent FDI attacks on vehicle platoons and its potential limitations.

5.1 Benefits of MCDA

In cyber security, there is much discussion about always creating a layered defence or defence in depth, which means there should be multiple methods to protect a system. If an attacker breaks one method, another layer is still protected against the attacker. When securing platoon communications, currently, there are many ideas, as discussed in the literature review, about securing the public and private keys and managing encryption, as well as research looking into the use of trust methods for platoons. Finally, stability algorithms seek to maintain stability in a platoon. These are the three methods proposed to prevent an attacker from altering the behaviour of platoon members through altering or injecting beacons into the platoon network. If all three methods are used to prevent attacks on platoon communications, it gives three layers of protection against attack. When looking at the literature, there has yet to be a consensus on what will be implemented in practice. The method of using MCDA to screen beacons before use by the vehicle will act as an additional layer of protection. Situated after public and private key infrastructure but before trust, as shown in the section 4, MCDA can prevent attacks from external attackers and buy time for a trusted method to degrade for an internal attacker. All without causing any additional problems for platoon members.

5.2 Performance

The performance using MCDA is a method to prevent external FDI attacks on vehicle platoons by enabling member vehicles to identify abnormal beacons and then safely replace the beacon with either the previous or the leader beacon. Using TOPSIS, a platoon member can prevent any negative impact from the attacker, even when the attacker tries to flood the victim's vehicle with false information. The effectiveness with average platoon F1 scores

of 97.1% is extremely high F1 score. Having such a high F1 score implies that the overall effect of the attack on the platoon will be negligible. Again, this is backed up when looking at parameters such as the inter-vehicle distance, vehicle speed or CO_2 output, which are all virtually ideal when using MCDA TOPSIS and WSM to prevent external FDI attacks.

What does this mean regarding the effectiveness of MCDA as a method of detecting and replacing fake beacons in a platoon network in real-time? For external attackers, there is a 100% decrease in the effectiveness of their attacks as shown in chapter 4 where the use of the MCDA method TOPSIS prevents the attacker from altering the inter-vehicle distance and the speed of any member of the platoon. The results show that the external attacker can reduce the inter-vehicle distance by 6.661%. Such a decrease in the inter-vehicle may not seem like a problem; however, platooning vehicles are already operating as close to each other as physically possible [36] and well within the recommended two-second gap that a human driver should observe. The attacker reducing the inter-vehicle distance between two platooning vehicles increases the risk to the platoon. When looking at the speed of the vehicles, which can indicate the platoon's stability, again, the external attacker sees a 100% decrease in the deviation from the ideal speed when under attack. Both the constant and on-off attacks saw a deviation from the ideal speed, which was at most 0.744% from the ideal. A 0.744% is almost a negligible change in speed; however, what matters here is how smooth and constant the speeds of each platooning vehicle are. When under external attacks, the trace of each platooning vehicle is erratic and has many peaks as shown in 4.6 and 4.8. The constant changing and adjustment of the platoon members' speed, even on a single individual, causes the following vehicles to alter and change their speed to maintain ideal inter-vehicle distance. The constant adjustments in speed lead to increased fuel consumption, thus negating the fuel-saving benefits of platooning [47]. The fuel consumption of platooning vehicles under external attack sees the vehicle that is attacked, and the vehicles following it have increased CO_2 output with the amount of extra CO_2 produced increasing the further from the attacked vehicle. The increase in CO_2 over the time of the experiment may be less than $0.2g$ over $1000s$; however, over a longer time, the impact will continue to compound and lessening benefit of platooning, which is an increment in fuel economy[47].

The benefits could be more impressive when looking at MCDA TOPSIS as a way to prevent internal FDI attacks. MCDA can suppress the attacker at times, and for the first $200s$, it is able to do so with a 100% improvement to the inter-vehicle distance and each platoon member's speed regardless of the number of attackers there are. After this, the MCDA's ability to suppress the attacker drops dramatically as the attacker can overwhelm the attacker. However, the attacker is still slightly suppressed as the MCDA can sufficiently suppress the attacker so that the inter-vehicle distance and speed begin to return to ideal. The use of MCDA alone cannot maintain ideal conditions. However, The attacker cannot have as much of an impact on the platoon as the inter-vehicle distance when MCDA is used is reduced by 12.766%. Thus, even though the attacker is still coursing the inter-vehicle distance to deviate from the ideal, it is less impactful than with MCDA. When looking at the vehicle speed and, therefore, stability of the platoon, the use of MCDA, the performance of the constant internal

attacker is worse than if MCDA was not used, and that is because the attacked vehicle will go through periods of activity where the speed of the vehicle wildly changes by up to $1kmph$ as shown in figure 4.27 and 4.28. The use of MCDA on its own can improve the stability of the internal attacker. This is highlighted even more when looking at the CO_2 output of the attacked vehicles, with the attacked vehicle outputting over $1g$ more CO_2 over $1000s$ compared to not under attack, which is a clear sign that the attacked vehicle is using more fuel along with the instability seen from the vehicle speed. Interestingly, the on-off attack increased the fuel economy of the attacked vehicle by about $0.5g$ over $1000s$ at the cost of insatiability, and the vehicle following it had a slight increase in CO_2 output.

When looking at the performance of MCDA and trust together for internal FDI attacks, the results are not as impressive as seen for the external attacker; however, the use of both shows how using a defence in depth approach can support and improve the security of platoon beacons. An attack that would have resulted in a collision previously now results in a minor change to the attacked members' position before reverting to normal. While it is not perfect, it does prevent catastrophic failure of the platoon and then return all vehicles to an ideal platooning state. Again, like with the external attacker, the F1 score of the attacked vehicle is awe-inspiring, with only a few of the attacker's beacons being used before the beacon selection method can identify and remove the beacons by the attacker, thus starting the repair of the platoon back to ideal platooning formation.

The use of MCDA and trust together is interesting for internal attacks as it impacts the attacker's ability to attack the platoon. The interesting thing is that the performance of the attack is strongly linked to the number of attackers present. More attackers mean a greater chance of one attacker being successful. In the results section, when there is a single constant internal attacker, the impact of the attack on the platoon is reduced by 100%, and the attack is completely suppressed. When the number of attackers is increased to six, it takes the platoon longer to achieve initial stability, and then just before $200s$, there is a small blip where Node 5 suddenly decreases its inter-vehicle distance; however, it is quickly corrected. When looking at the on-off attacks, the attack is suppressed; however, it is not entirely prevented. The attacker can still cause a $0.5m$ deviation from the idea inter-vehicle distance; however, it is a 87.5% reduction compared to when MCDA and trust are not used. In addition to this, there are also three fewer peaks of over $500s$ compared to when no MCDA and trust were used. When looking at the speed of the platoon during attacks, the story is very much the same as the inter-vehicle distance. However, this time, there is a 60% reduction in the size of the peaks seen and three fewer peaks for the on-off attack over $500s$. While this is not perfect, there is a significant improvement in the behaviour of the platoon vs internal FDI attacks when using MCDA and trusting each other.

When looking at the results of where the attacker is sanctioned, there is an initial period of instability when the attacker is actively engaged in an attack; however, they can be quickly identified, and after that, the attacker cannot have any further impact on the platoon. The attacker's impact is more severe than if no sanctions were used; however, the attack is always

stopped within the first $50s$ of the attack starting. Suppose the sanction is that the attacker is to be ignored. In that case, the platoon returns to ideal platooning with a 100% improvement in the inter-vehicle distance and speed. If the platoon is to be disbanded, the attacker is identified, and the platoon disbanded between $17s$ and $50s$ depending on the number of attackers and whether the attack is on-off or constant. Constant attacks can be identified and countered far faster than on-off attacks.

5.3 Limitations

The test cases show that using MCDA to identify and replace false or misleading beacons is quite effective. The peer-to-peer trust method that is also implemented is simple and effective. However, the testing and the methods used may have some potential limitations.

5.3.1 Simulation Environment

The simulation environment used for testing is straightforward. The road is flat and straight, and multiple lanes have no additional traffic. As such, the performance of using MCDA and the trust method interactions with bends in the road, changing of lanes or navigating with other traffic. For the MCDA, the most challenging part is changing lanes and turning, as one of the criteria that are compared is the vehicle's position. Currently, the y-axis is constant and fixed; therefore, any changes will give a large numerical difference in the MCDA score. In reality, the x and y-axis values will constantly change. To overcome problems with the location, both x and y coordinates are consolidated together and considered as a single value. Therefore, the weighting for the location component must be adjusted and fine-tuned with precision to improve performance when the x-axis is not constant.

The challenge of changing lanes and directions will also affect the trust method as it makes use of sensor information to gauge how far it is from the preceding vehicle. When vehicles change lanes or turn, this can lead to a momentary change or drop in the inter-vehicle distance. The change in vehicle position or total loss of the preceding vehicle will result in a drop in the trust between the vehicles until their positions normalise again. The decrease in member trust could be better, as this will lead to members being falsely accused of being untrustworthy for no reason. The effect on the platoon and how this will affect the platoon must be investigated and understood.

5.3.2 Trust Method

The implemented trust method is simplistic and highly effective in the environment it is created for. As discussed above, the trust method has limitations when it comes to its implementation, with the trust method being tailored for use on straight-road use. Going forward, it would be important to make use of a more advanced trust method such as REPLACE [48] or implement a trust management method from VANET for non-platooning vehicles such as MARINE [13]. Furthering this is that the trust method would, with sanctions, enable

falsely sanctioning an inherent vehicle due to the ripple effect of the attacker on the platoon resulting from their attack. The problem is only evident when the attacker vehicle is ignored and members replace the member's beacon with the leader's. Suppose the platoon breaks up when the attacker is detected. In that case, the behaviour is masked as the platoon breaks up before insistent vehicles are affected.

On the other hand, if the length of time before the attacker is sanctioned is increased, then the insistent vehicles can recover their trust value and not be falsely sanctioned. Equally, by not implementing any specific sanctions and relying on the flow of the trust values on the beacons, the attacker can be filtered out without permanently banning the attacker and, therefore, protecting insistent vehicles. For all of the limitations of the trust method used, it proves that MCDA can assist trust management methods by suppressing an attack, enabling the trust method more time to assess the trustworthiness of a platoon member even during active platooning.

Chapter 6

Conclusion and Future Work

This final chapter of this thesis has two sections: the first discusses the conclusions of this thesis and its major contributions, and the second discusses the future works resulting from this research.

6.1 Contributions

Vehicle platooning is a promising technology that is rapidly being taken from test tracks to our roadways, as platooning promises impressive efficiency savings for logistic companies, improving road safety and reducing road congestion overall. Platooning as a commercial service relies on its ability to maintain a mission-critical communication network. Attacks on this communication network will lead to undesirable actions by platoon members, resulting in platooning vehicles, at best, losing the benefits of platooning and, at worst, colliding with other platooning vehicles, non-platooning road users, or roadside infrastructure. To prevent such problems, robust and reliable cybersecurity will need to be employed, enabling the communications network to be highly robust, involving multiple layers of defences. Existing methods of maintaining secure platoon communications revolve around using public and private keys to prevent external attackers from attacking a platoon and trust to prevent internal attackers. In this thesis, a third method is proposed that can be implemented to assist in preventing both internal and external attackers. The proposed method involves using MCDA to enable platooning vehicles to detect beacons that may contain damaging behaviour for the vehicle and replace it with a safer alternative beacon, thus nullifying the effects of the attack.

The first step in achieving the aims and objectives of this thesis was to undertake a comprehensive literature review encompassing both attacks on platoons and existing defence methods. In chapter 2 of this thesis, the many different methods of attacking a platoon through the wireless communications network are discussed and detailed before exploring the defences for platoons. The attacks against the platoon were sorted into the intended outcome or reason to attack the platoon. The reason for doing this instead of more conventional methods is to bring a new and fresh perspective to attacks on platoons and to assist in creat-

ing the risk assessment. When looking at defences to attacks against platoons, they fell into one of five main methods: private and public key infrastructure, hybrid communications, trust methods, control algorithms and blockchain methods. Most existing methods focus on preventing external attackers from being able to communicate successfully in the platoon network through encryption or using multiple channels of communication. For internal attackers, there are control algorithms and trust methods; however, while attackers could be identified, there was often little that could be done to penalise attackers. The gap in the literature that was identified was the damage an external attacker could cause if they penetrate the description of the platoon network and how this can be used to prevent or lessen the impact of an internal attacker. In addition to this, there is no publicly available cybersecurity risk assessment for cyber attacks on platooning vehicle communications.

After identifying FDI as a high-risk attack, the next stage is to create a methodology and suitable platform to test both the effects of FDI attacks on platoons. Chapter 3 details the simulation environment Plexe, which is a platooning extension of the automotive open-source vehicular network simulation framework veins. Chapter 3 discusses the simulation environment, the vehicles used and the platooning protocol in great detail. Here, while there are multiple types of platooning protocols for use, the one to use is CACC, which is the one that is most prominently featured in the literature.

Chapter 3 is where the concepts of MCDA and Trust are introduced. For MCDA, a brief description is given, followed by a detailed discussion of each MCDA method. The methods discussed are TOPSIS, WSM and PROMETHEE II, where the mathematical proof of each method is presented alongside a worked example. The end of the chapter explains the trust method used for peer-to-peer trust. The MCDA and Trust are then used in Chapter 4 to protect a platoon of eight vehicles from various FDI attacks, both external and internal. The effectiveness of the method is analysed using both physical and statistical factors. This concludes that TOPSIS is the most effective MCDA method to prevent internal and external FDI attacks on a platoon.

Finally, Chapter 5 discusses the results of Chapter 4 and the benefits and limitations of the current work. The main takeaways are that the use of MCDA and peer-to-peer trust to prevent FDI attacks on platoons from having a significant negative impact is impressive both physically and statistically; further work is needed to tune the methods used and presented into a usable method that will be able to handle the many variables of driving.

6.2 Conclusions

This thesis was created to show how MCDA can be used to identify and replace false beacons within a platoon network quickly and reliably. To do this, a literature survey was carried out looking at what attacks are possible against platoons and how such attacks can impact a platoon. In addition to understanding attacks on platoons, methods to defend against them are

also investigated. It is identified that security in platooning relies on using public and private keys, which can be highly effective. The problem is that platoons ideally want to connect in an ad-hoc fashion, and the use of keys needs a secure way to exchange or agree on keys without a third party obtaining them. Another popular method is the use of trust. Trust in vehicles works by having two vehicles that communicate regularly together rank information from each other as being more reliable if there is a correct history of information. From this literature review, FDI attacks were identified as suitable to try to counter due to the variation in the possibilities of the impact that they can have on a platoon.

With FDI attacks identified, the next step was implementing an FDI attack in a suitable simulation environment. Plexe simulation environment was identified as suitable for simulating the platoon and the FDI attacks as it is a platooning extension to the prevalent VANET simulator Veins. In the plexe simulation, external and internal FDI attackers on an eight-vehicle platoon were simulated, and it was found that using a relatable small speed change can lead to platooning vehicles closing their inter-vehicle gap to dangerous levels and even cause coalitions between members if there is a suitably significant enough change in the speed that the attacker transmits.

The next step was implementing a method to prevent attackers from disrupting platoons. During the literature review, many others looked to secure a platoon from external attacks using public and private keys; however, the problem is that such methods require a way to agree or exchange the keys securely. During the exchange or agreement of keys, the challenge is keeping them private. MCDA, however, can be implemented on all vehicles and can be used to identify abnormalities in the beacon information and replace suspicious beacons with known trusted beacons. This means that even if an external attacker could carry out an FDI attack on the platoon, the member vehicles could quickly identify and ignore the fake beacon. This thesis has shown that MCDA TOPSIS is extremely effective at countering external FDI attacks on a platoon. MCDA TOPSIS, however, was not as effective when used to prevent internal FDI attacks.

To improve the effectiveness of MCDA TOPSIS against internal FDI attacks, a simple local trust method was implemented that would look at the beacon content and use the vehicle sensors to generate a trust value for the previous member vehicle in the platoon. The trust score is then modified to the MCDA score for each beacon, meaning that trusted beacons are more likely to be selected even if the MCDA score is low. By using the simple trust method described in this thesis, the impact of the internal attacker was significantly reduced, with the attacker becoming significantly suppressed and degrading the ability of the attacker to harm the platoon. This thesis aims to show that MCDA and trust can be used together to suppress an FDI attack on a platoon, ideally to the point where it does not impact the platoon at all. This thesis shows that the attacker has a significantly lower impact on the platoon when using MCDA and trust to screen beacons received by a platoon member in real-time to filter out fake beacons.

6.3 Future Work

In this thesis, MCDA or MCDM is proposed as a method that can be used by platooning member vehicles to prevent FDI attacks on them during standard platooning practices. MCDA enables platoons to compare the new beacon received from another member vehicle to the one received from the leader vehicle and the previous one from that member. If the new beacon is too different, it is discarded, and either the leader or previous beacon is selected to replace it. A peer-to-peer trust method is also proposed to bolster performance against internal FDI attackers further. Working in tandem with MCDA, this method enhances the platoons' ability to identify and discard false beacons, thereby improving overall performance. The methodology is then tested against various FDI attacks, both internal and external, to evaluate its performance. Under the ideal conditions scenarios, the method demonstrates outstanding results, preventing all impacts of external attackers, thwarting internal attackers from causing coalitions, and identifying potential attackers for sanctioning.

The next step is to use MCDA and peer-to-peer trust to be tested in a broader range of platooning scenarios that better represent real-world roadways. The change to realistic roads will increase the challenge for MCDA to identify true and false beacons successfully; as such, additional tuning will be needed for the method. Currently, only the platooning vehicles and any attackers are present, and there are no other traffic or V2V communications during testing. In future tests, it will be essential to ensure that the proposed methods in this thesis can remain safe within physical and wireless traffic. As for the communications here, the beacons are transmitted using 802.11p protocols. While currently, this is still the accepted communication protocol for V2V communications, it is likely to be replaced soon by 5G or similar technology, and as such, the proposed methods need to be compatible with the new communications protocol, even if the likelihood of there being a problem is small due to the methods only interested in the physical content of the beacon without the need to add additional aspects to the beacon.

As such, this thesis and work can be expanded upon in several different directions, such as:

- Implementation of a broader range of platoon manoeuvres described in the literature to provide further variety in sanctions that can be applied to potential attacking vehicles.
- Testing MCDA and peer-to-peer trust methodology described here in a more complex road network that features non-platooning, non-networked traffic to understand any potential challenges integrating platoons using these methods with current traffic.
- Testing MCDA and peer-to-peer trust methodology described within a larger VANET to ensure compatibility with future road networks and infrastructure.
- The development of a more robust peer-to-peer trust method that platoon members can use during platooning.
- To look at other attacks on platoons to see if the proposed use of MCDA and Trust can also be used against those attacks.
- Look to expand the capabilities of this method to incorporate additional platoon manoeuvres and beacons from the leader using artificial intelligence to enhance the capabilities of the existing method.

Bibliography

[1] Cyber-crime: Irish health system targeted twice by hackers. https://www.bbc.co.uk/news/world-europe-57134916. Accessed: 24/06/2021.

[2] Safe road trains for the environment; developing strategies and technologies to allow vehicle platoons to operate on normal public highways with significant environmental, safety and comfort benefits, May 2017. URL https://cordis.europa.eu/project/id/233683.

[3] Closer than you think: Know your stopping distances, 2021. URL https://www.theaa.com/breakdown-cover/advice/stopping-distances.

[4] Ensemble, 2021. URL https://platooningensemble.eu/.

[5] Research and analysis greenhouse gas reporting: conversion factors 2021, 2021. URL https://www.gov.uk/government/publications/greenhouse-gas-reporting-conversion-factors-2021.

[6] Road safety statistics 2022 in more detail, 2022. URL https://transport.ec.europa.eu/background/road-safety-statistics-2022-more-detail_en.

[7] National statistics reported road casualties in great britain, provisional estimates: year ending june 2022, 2023. URL https://www.gov.uk/government/statistics/reported-road-casualties-in-great-britain-provisional-estimates-year-ending-june-2022/reported-road-casualties-in-great-britain-provisional-estimates-year-ending-june-2022.

[8] Road traffic injuries, 2023. URL https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries.

[9] Abdeldime MS Abdelgader and Wu Lenan. The physical layer of the ieee 802.11 p wave communication standard: the specifications and challenges. In *Proceedings of the world congress on engineering and computer science*, volume 2, pages 22–24, 2014.

[10] ACEA. What is the european truck platooning challenge?, 2016. URL https://www.acea.auto/fact/what-is-the-european-truck-platooning-challenge/. Accessed: 28/06/2021.

[11] ACEA. First cross-border truck platooning trial successfully completed, 2016. URL https://www.acea.be/press-releases/article/first-cross-border-truck-platooning-trial-successfully-completed.

[12] F. Ahmad, J. Hall, A. Adnane, and V. N. L. Franqueira. Faith in vehicles: A set of evaluation criteria for trust management in vehicular ad-hoc network. In *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 44–52, 2017.

[13] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain. Marine: Man-in-the-middle attack resistant trust model in connected vehicles. *IEEE Internet of Things Journal*, 7(4):3310–3322, 2020. doi:10.1109/JIOT.2020.2967568.

[14] F. Ahmad, F. Kurugollu, C. A. Kerrache, S. Sezer, and L. Liu. Notrino: a novel hybrid trust management scheme for internet-of-vehicles. *IEEE Transactions on Vehicular Technology*, pages 1–1, 2021. (Early Access), doi:10.1109/TVT.2021.3049189.

[15] Farhan Ahmad, Asma Adnane, Virginia NL Franqueira, Fatih Kurugollu, and Lu Liu. Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies. *Sensors*, 18(11):4040, 2018.

[16] Farhan Ahmad, Asma Adnane, Chaker A. Kerrache, Fatih Kurugollu, and Iain Phillips. On the design, development and implementation of trust evaluation mechanism in vehicular networks. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, pages 1–7, 2019. doi: 10.1109/AICCSA47632.2019.9035312.

[17] Mohammed Saeed Al-Kahtani. Survey on security attacks in vehicular ad hoc networks (vanets). In *2012 6th International Conference on Signal Processing and Communication Systems*, pages 1–9. IEEE, 2012. doi: 10.1109/ICSPCS.2012.6507953.

[18] Mamdouh Alenezi, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. Evaluating performance of web application security through a fuzzy based hybrid multi-criteria decision-making approach: Design tactics perspective. *IEEE Access*, 8: 25543–25556, 2020. doi: 10.1109/ACCESS.2020.2970784.

[19] Alan Ali, Gaetan Garcia, and Philippe Martinet. The flatbed platoon towing model for safe and dense platooning on highways. *IEEE Intelligent Transportation Systems Magazine*, 7(1):58–68, 2015. DOI:10.1109/MITS.2014.2328670.

[20] Mani Amoozadeh, Hui Deng, Chen-Nee Chuah, H Michael Zhang, and Dipak Ghosal. Platoon management with cooperative adaptive cruise control enabled by vanet. *Vehicular communications*, 2(2):110–123, 2015.

[21] Mani Amoozadeh, Arun Raghuramu, Chen-Nee Chuah, Dipak Ghosal, H Michael Zhang, Jeff Rowe, and Karl Levitt. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine*, 53(6):126–132, 2015.

[22] Farooque Azam, Sunil Kumar, KP Yadav, Neeraj Priyadarshi, and Sanjeevikumar Padmanaban. An outline of the security challenges in vanet. In *2020 IEEE 7th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, pages 1–6. IEEE, 2020.

[23] Pooja Bansal, Shabnam Sharma, and Aditya Prakash. A novel approach for detection of distributed denial of service attack in vanet. *International Journal of Computer Applications*, 120(5), 2015.

[24] BBC. Ransomware attack takes us maritime base offline, 2020. URL `https://www.bbc.co.uk/news/technology-50972890`.

[25] N. Bermad, S. Zemmoudj, and M. Omar. Securing vehicular platooning against vehicle platooning disruption (vpd) attacks. In *8th International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)*, pages 1–6, 2019.

[26] Seema Gupta Bhol, J. R. Mohanty, and Prasant Kumar Pattnaik. Cyber security metrics evaluation using multi-criteria decision-making approach. In Suresh Chandra Satapathy, Vikrant Bhateja, J. R. Mohanty, and Siba K. Udgata, editors, *Smart Intelligent Computing and Applications*, pages 665–675, Singapore, 2020. Springer Singapore. ISBN 978-981-32-9690-9.

[27] Youssef Bichiou and Hesham Rakha. Vehicle platooning: An energy consumption perspective. In *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, pages 1–6. IEEE, 2020.

[28] Roghieh A. Biroon, Zoleikha Abdollahi Biron, and Pierluigi Pisu. False data injection attack in a platoon of cacc: Real-time detection and isolation with a pde approach. pages 1–12, 2021. DOI:10.1109/TITS.2021.3085196.

[29] Joe Diether Cabelin, Paul Vincent Alpano, and Jhoanna Rhodette Pedrasa. Svm-based detection of false data injection in intelligent transportation system. In *International Conference on Information Networking (ICOIN)*, pages 279–284, 2021. doi: 10.1109/ICOIN50884.2021.9333942.

[30] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, et al. Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium*, volume 4, pages 447–462. San Francisco, 2011.

[31] Qi Chen, Daniel Jiang, and Luca Delgrossi. Ieee 1609.4 dsrc multi-channel operations and its implications on vehicle safety communications. In *2009 IEEE vehicular networking conference (VNC)*, pages 1–8. IEEE, 2009.

[32] National Automated Highway System Consortium. System objectives and characteristics, 1995. URL `https://path.berkeley.edu/sites/default/files/ahs_system_objectives_characteristics1.pdf`.

[33] Brian P Crow, Indra Widjaja, Jeong Geun Kim, and Prescott T Sakai. Ieee 802.11 wireless local area networks. *IEEE Communications magazine*, 35(9):116–126, 1997.

[34] Arturo Davila, Eduardo del Pozo, Enric Aramburu, and Alex Freixas. Environmental benefits of vehicle platooning. Technical report, SAE Technical Paper, 2013.

[35] Raj Gautam Dutta, Yaodan Hu, Feng Yu, Teng Zhang, and Yier Jin. Design and analysis of secure distributed estimator for vehicular platooning in adversarial environment. *IEEE Transactions on Intelligent Transportation Systems*, pages 1–12, 2020. DOI:10.1109/TITS.2020.3036376.

[36] S. Ellwanger and E. Wohlfarth. Truck platooning application. In *2017 IEEE Intelligent Vehicles Symposium (IV)*, pages 966–971. IEEE, 2017.

[37] John Vissers et al. V1 platooning use-cases, scenario definition and platooning levels. *D2.2 of H2020 project ENSEMBLE*, 2018. URL `platooningensemble.eu`.

[38] Mushtak Y Gadkari and Nitin B Sambre. Vanet: routing protocols, security issues and simulation tools. *IOSR Journal of Computer Engineering*, 3(3):28–38, 2012.

[39] Dhavy Gantsou. On the use of security analytics for attack detection in vehicular ad hoc networks. In *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pages 1–6. IEEE, 2015.

[40] Keno Garlichs, Alexander Willecke, Martin Wegner, and Lars C. Wolf. TriP: Misbehavior detection for dynamic platoons using trust. In *IEEE Intelligent Transportation Systems Conference (ITSC)*, pages 455–460, 2019. doi: 10.1109/ITSC.2019.8917188.

[41] Amrita Ghosal and Mauro Conti. Security issues and challenges in v2x: A survey. *Computer Networks*, 169:107093, 2020.

[42] Amrita Ghosal, Sang Uk Sagong, Subir Halder, Kalana Sahabandu, Mauro Conti, Radha Poovendran, and Linda Bushnell. Truck platoon security: State-of-the-art and road ahead. *Computer Networks*, 185:107658, 2021.

[43] Jyoti Grover, Manoj Singh Gaur, and Vijay Laxmi. A novel defense mechanism against sybil attacks in vanet. In *Proceedings of the 3rd international conference on Security of information and networks*, pages 249–255, 2010.

[44] Jyoti Grover, Manoj Singh Gaur, Vijay Laxmi, and Nitesh Kumar Prajapati. A sybil attack detection approach using neighboring vehicles in vanet. In *Proceedings of the 4th international conference on Security of information and networks*, pages 151–158, 2011.

[45] Abderrahim Guerna, Salim Bitam, and Carlos T Calafate. Roadside unit deployment in internet of vehicles systems: a survey. *Sensors*, 22(9):3190, 2022.

[46] Jun Han, Madhumitha Harishankar, Xiao Wang, Albert Jin Chung, and Patrick Tague. Convoy: Physical context verification for vehicle platoon admission. In *Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications*, HotMobile '17, page 73–78, New York, NY, USA, 2017. Association for Computing Machinery. ISBN 9781450349079. URL `https://doi.org/10.1145/3032970.3032987`.

[47] Kaiqiang Pan Wanjia Meng Rui L Hongyu Zheng, Jianjun Wu. Research on control target of truck platoon based on maximizing fuel saving rate. *SAE Int. J. Veh. Dyn., Stab., and NVH*, 4(2):135–150, 2020. doi: https://doi.org/10.4271/10-04-02-0010.

[48] Hao Hu, Rongxing Lu, Zonghua Zhang, and Jun Shao. Replace: A reliable trust-based platoon service recommendation scheme in vanet. *IEEE Transactions on Vehicular Technology*, 66(2):1786–1797, 2016.

[49] Jiaqi Huang, Dongfeng Fang, Yi Qian, and Rose Qingyang Hu. Recent advances and challenges in security and privacy for v2x communications. *IEEE Open Journal of Vehicular Technology*, 1:244–266, 2020.

[50] Ching-Lai Hwang and Kwangsun Yoon. *Methods for Multiple Attribute Decision Making*, pages 58–191. Springer Berlin Heidelberg, Berlin, Heidelberg, 1981. doi: 10.1007/978-3-642-48318-9_3.

[51] SAE International. Sae j3016 202104: Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. *SAE International*, 2021.

[52] Niloofar Jahanshahi and Riccardo MG Ferrari. Attack detection and estimation in cooperative vehicles platoons: A sliding mode observer approach. *IFAC-PapersOnLine*, 51(23): 212–217, 2018.

[53] Robbert Janssen, Han Zwijnenberg, Iris Blankers, and Janiek de Kruijff. Truck platooning. *Driving the*, 2015.

[54] Muhammad Awais Javed, Mohammad Zubair Khan, Usman Zafar, Muhammad Faisal Siddiqui, Rabiah Badar, Byung Moo Lee, and Farhan Ahmad. ODPV: An efficient protocol to mitigate data integrity attacks in intelligent transport systems. *IEEE Access*, 8:114733–114740, 2020. doi:10.1109/ACCESS.2020.3004444.

[55] Dongyao Jia, Kejie Lu, and Jianping Wang. A disturbance-adaptive design for vanet-enabled vehicle platoon. *IEEE Transactions on Vehicular Technology*, 63(2):527–539, 2014.

[56] Dongyao Jia, Kejie Lu, Jianping Wang, Xiang Zhang, and Xuemin Shen. A survey on platoon-based vehicular cyber-physical systems. *IEEE communications surveys & tutorials*, 18(1):263–284, 2015.

[57] Daniel Jiang and Luca Delgrossi. Ieee 802.11 p: Towards an international standard for wireless access in vehicular environments. In *VTC Spring 2008-IEEE Vehicular Technology Conference*, pages 2036–2040. IEEE, 2008.

[58] Joe Tidy. Colonial hack: How did cyber-attackers shut off pipeline?, 2021. URL `https://www.bbc.co.uk/news/technology-57063636`.

[59] Chengzhe Lai, Rongxing Lu, and Dong Zheng. Spgs: a secure and privacy-preserving group setup framework for platoon-based vehicular cyber-physical systems. *Security and Communication Networks*, 9(16):3854–3867, 2016. URL `https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1523`. DOI:https://doi.org/10.1002/sec.1523.

[60] Michael P Lammert, Adam Duran, Jeremy Diez, Kevin Burton, and Alex Nicholson. Effect of platooning on fuel consumption of class 8 vehicles over a range of speeds, following distances, and mass. *SAE International Journal of Commercial Vehicles*, 7(2014-01-2438): 626–639, 2014.

[61] Kai Li, Lingyun Lu, Wei Ni, Eduardo Tovar, and Mohsen Guizani. Secret key agreement for data dissemination in vehicular platoons. *IEEE Transactions on Vehicular Technology*, 68 (9):9060–9073, 2019. DOI:10.1109/TVT.2019.2926313.

[62] Kai Li, Lingyun Lu, Wei Ni, Eduardo Tovar, and Mohsen Guizani. Cooperative secret key generation for platoon-based vehicular communications. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2019.

[63] Kai Li, Wei Ni, Yousef Emami, Yiran Shen, Ricardo Severino, David Pereira, and Eduardo Tovar. Design and implementation of secret key agreement for platoon-based vehicular cyber-physical systems. *ACM Trans. Cyber-Phys. Syst.*, 4(2), nov 2019. ISSN 2378-962X. URL `https://doi.org/10.1145/3365996`. DOI:10.1145/3365996.

[64] Kuo-Yun Liang, Jonas Mårtensson, and Karl Henrik Johansson. When is it fuel efficient for a heavy duty vehicle to catch up with a platoon? *IFAC Proceedings Volumes*, 46(21):738–743, 2013. ISSN 1474-6670. doi: https://doi.org/10.3182/20130904-4-JP-2042.00071. URL https://www.sciencedirect.com/science/article/pii/S1474667016384622. 7th IFAC Symposium on Advances in Automotive Control.

[65] Jiajia Liu, Shubin Zhang, Wen Sun, and Yongpeng Shi. In-vehicle network attacks and countermeasures: Challenges and future directions. *IEEE Network*, 31(5):50–58, 2017.

[66] Lei Liu, Chen Chen, Qingqi Pei, Sabita Maharjan, and Yan Zhang. Vehicular edge computing and networking: A survey. *Mobile Networks and Applications*, pages 1–24, 2020.

[67] Zhaojun Lu, Gang Qu, and Zhenglin Liu. A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Transactions on Intelligent Transportation Systems*, 20(2): 760–776, 2018.

[68] Fangwu Ma, Yu Yang, Jiawei Wang, Xinchen Li, Guanpu Wu, Yang Zhao, Liang Wu, Bilin Aksun-Guvenc, and Levent Guvenc. Eco-driving-based cooperative adaptive cruise control of connected vehicles platoon at signalized intersections. *Transportation Research Part D: Transport and Environment*, 92:102746, 2021.

[69] Raquel G. Machado and Krishna Venkatasubramanian. Short paper: Establishing trust in a vehicular network. In *2013 IEEE Vehicular Networking Conference*, pages 194–197, 2013. doi: 10.1109/VNC.2013.6737611.

[70] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani. Internet-of-Things-Based Smart Cities: Recent Advances and Challenges. *IEEE Communications Magazine*, 55(9):16–24, Sep. 2017. ISSN 0163-6804. doi:10.1109/MCOM.2017.1600514.

[71] Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. Survey on vanet security challenges and possible cryptographic solutions. *Vehicular Communications*, 1(2):53–66, 2014.

[72] Lynda Mokdad, Jalel Ben-Othman, and Anh Tuan Nguyen. Djavan: Detecting jamming attacks in vehicle ad hoc networks. *Performance Evaluation*, 87:47–59, 2015.

[73] Graeme Morrison and David Cebon. Extremum-seeking algorithms for the emergency braking of heavy goods vehicles. *Proceedings of the Institution of Mechanical Engineers, Part D: Journal of automobile engineering*, 231(14):1961–1977, 2017.

[74] Simon Parkinson, Paul Ward, Kyle Wilson, and Jonathan Miller. Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Transactions on Intelligent Transportation Systems*, 18(11):2898–2915, 2017. DOI:10.1109/TITS.2017.2665968.

[75] Mohammad Pasha. A review of ieee 802.11 p (wave) multi-channel mac schemes. *Journal of Wireless Sensor Network*, 4, 2016.

[76] H. Peng, Le Liang, X. Shen, and G. Y. Li. Vehicular communications: A network layer perspective. *IEEE Transactions on Vehicular Technology*, 68(2):1064–1078, 2019. doi: 10.1109/TVT.2018.2833427.

[77] Alberto Petrillo, Antonio Pescapé, and Stefania Santini. A collaborative approach for improving the security of vehicular scenarios: The case of platooning. *Computer Communications*, 122:59–75, 2018. ISSN 0140-3664. DOI:https://doi.org/10.1016/j.comcom.2018.03.014.

[78] Jeroen Ploeg, Bart T. M. Scheepers, Ellen van Nunen, Nathan van de Wouw, and Henk Nijmeijer. Design and experimental evaluation of cooperative adaptive cruise control. In *2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, pages 260–265, 2011. doi: 10.1109/ITSC.2011.6082981.

[79] Jafar Rezaei. Best-worst multi-criteria decision-making method. *Omega*, 53:49–57, 2015. ISSN 0305-0483. doi: https://doi.org/10.1016/j.omega.2014.11.009. URL `https://www.sciencedirect.com/science/article/pii/S0305048314001480`.

[80] Tom Robinson, Eric Chan, and Erik Coelingh. Operating platoons on public motorways: An introduction to the sartre platooning programme. In *17th world congress on intelligent transport systems*, volume 1, page 12, 2010.

[81] Tanveer A. Zia Li h o ng Zhe ng Sabih ur Re hman, M. Arif Khan. Vehicular ad-hoc networks (vanets) - an overview and challenges. *Journal of Wireless Networking and Communications*, 3(3):29–38, 2013.

[82] Jesty Santhosh and Sriram Sankaran. Defending against sybil attacks in vehicular platoons. In *IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pages 1–6. IEEE, 2019.

[83] Stefania Santini, Alessandro Salvi, Antonio Saverio Valente, Antonio Pescapé, Michele Segata, and Renato Lo Cigno. A consensus-based approach for platooning with intervehicular communications and its validation in realistic scenarios. *IEEE Transactions on Vehicular Technology*, 66(3):1985–1999, 2017. doi: 10.1109/TVT.2016.2585018.

[84] Ankur Sarker, Chenxi Qiu, and Haiying Shen. Quick and autonomous platoon maintenance in vehicle dynamics for distributed vehicle platoon networks. In *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, pages 203–208, 2017.

[85] Michele Segata, Stefan Joerer, Bastian Bloessl, Christoph Sommer, Falko Dressler, and Renato Lo Cigno. PLEXE: A Platooning Extension for Veins. In *6th IEEE Vehicular Networking Conference (VNC 2014)*, pages 53–60, Paderborn, Germany, 12 2014. IEEE. ISBN 978-1-4799-7660-7. doi: 10.1109/VNC.2014.7013309.

[86] Steven Shladover, Xiao-Yun Lu, Shiyan Yang, Hani Ramezani, John Spring, Christopher Nowakowski, and David Nelson. Cooperative adaptive cruise control (cacc) for partially automated truck platooning:final report. *Escholarship.org*, 2018. URL https://escholarship.org/uc/item/260060w4main.

[87] S. Sivanandham and M. S. Gajanand. Platooning for sustainable freight transportation: an adoptable practice in the near future? *Transport Reviews*, 40(5): 581–606, 2020. URL https://doi.org/10.1080/01441647.2020.1747568. DOI:10.1080/01441647.2020.1747568.

[88] Christoph Sommer, Reinhard German, and Falko Dressler. Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis. *IEEE Transactions on Mobile Computing (TMC)*, 10(1):3–15, January 2011. doi: 10.1109/TMC.2010.133.

[89] SUMO. Simulation of Urban MObility. Available online: https://www.eclipse.org/sumo/ (Accessed: November 11, 2021).

[90] Mingshun Sun, Ali Al-Hashimi, Ming Li, and Ryan Gerdes. Impacts of constrained sensing and communication based attacks on vehicular platoons. *IEEE Transactions on Vehicular Technology*, 69(5):4773–4787, 2020.

[91] Xiaotong Sun and Yafeng Yin. Behaviorally stable vehicle platooning for energy savings. *Transportation Research Part C: Emerging Technologies*, 99:37–52, 2019.

[92] Edgar Talavera, Alberto Díaz Álvarez, and José E Naranjo. A review of security aspects in vehicular ad-hoc networks. *IEEE Access*, 7:41981–41988, 2019.

[93] Sean Joe Taylor, Farhan Ahmad, Hoang Nga Nguyen, Siraj Ahmed Shaikh, David Evans, and David 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)*, pages 19–26, 2021. doi: 10.1109/DSN-W52860.2021.00015.

[94] Gwo-Hshiung Tzeng and Jih-Jeng Huang. *Multiple attribute decision making: methods and applications*. CRC press, 2011.

[95] 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*, 67(9):8667–8681, 2018. doi: 10.1109/TVT.2018.2840846.

[96] Alvydas Pikūnas Valentinas Mickūnaitis and Igor Mackoit. Reducing fuel consumption and co2 emission in motor cars. *Transport*, 22 (3):160–163, 2007. doi: 10.1080/16484142.2007.9638119. URL https://www.tandfonline.com/doi/abs/10.1080/16484142.2007.9638119.

[97] Rens van der Heijden, Thomas Lukaseder, and Frank Kargl. Analyzing attacks on cooperative adaptive cruise control (cacc). In *2017 IEEE Vehicular Networking Conference (VNC)*, pages 45–52. IEEE, 2017.

[98] J. Vissers et al. *V1 Platooning use-cases, scenario definition and Platooning Levels D2.2*. of H2020 project ENSEMBLE (platooningensemble.eu), (2018).

[99] Vladimir Vukadinovic, Krzysztof Bakowski, Patrick Marsch, Ian Dexter Garcia, Hua Xu, Michal Sybis, Pawel Sroka, Krzysztof Wesolowski, David Lister, and Ilaria Thibault. 3gpp c-v2x and ieee 802.11 p for vehicle-to-vehicle communications in highway platooning scenarios. *Ad Hoc Networks*, 74:17–29, 2018.

[100] SY Wang, CL Chou, KC Liu, TW Ho, WJ Hung, Cheng-Fu Huang, MS Hsu, HY Chen, and CC Lin. Improving the channel utilization of ieee 802.11 p/1609 networks. In *2009 IEEE Wireless Communications and Networking Conference*, pages 1–6. IEEE, 2009.

[101] Michael Wolf, Alexander Willecke, Johannes-Christian Müller, Keno Garlichs, Thomas Griebel, Lars Wolf, Michael Buchholz, Klaus Dietmayer, Rens W van der Heijden, and Frank Kargl. Securing cacc: Strategies for mitigating data injection attacks. In *2020 IEEE Vehicular Networking Conference (VNC)*, pages 1–7. IEEE, 2020.

[102] Chang Xu, Rongxing Lu, Huaxiong Wang, Liehuang Zhu, and Cheng Huang. Tjet: ternary join-exit-tree based dynamic key management for vehicle platooning. *IEEE Access*, 5: 26973–26989, 2017.

[103] Yu Xuan and Mohammad Naghnaeian. Detection and identification of cps attacks with application in vehicle platooning: a generalized luenberger approach. In *2021 American Control Conference (ACC)*, pages 4013–4020, 2021. DOI:10.23919/ACC50511.2021.9483074.

[104] Lin Yang, Zhihong Liu, Yong Zeng, Shijia Mei, and Jianfeng Ma. Security mechanisms to provide convoy member co-presence authentication in vehicle platooning. In *2019 International Conference on Networking and Network Applications (NaNA)*, pages 58–63. IEEE, 2019.

[105] Feng Yu, Raj Gautam Dutta, Teng Zhang, Yaodan Hu, and Yier Jin. Fast attack-resilient distributed state estimator for cyber-physical systems. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 39(11):3555–3565, 2020. DOI:10.1109/TCAD.2020.3013072.

[106] Weiying Zeng, Mohammed AS Khalid, and Sazzadur Chowdhury. In-vehicle networks outlook: Achievements and challenges. *IEEE Communications Surveys & Tutorials*, 18(3): 1552–1571, 2016.

[107] Chuan Zhang, Liehuang Zhu, Chang Xu, Kashif Sharif, Kai Ding, Ximeng Liu, Xiaojiang Du, and Mohsen Guizani. Tppr: A trust-based and privacy-preserving platoon recommendation scheme in vanet. *IEEE Transactions on Services Computing*, 2019.

[108] Dan Zhang, Ye-Ping Shen, Si-Quan Zhou, Xi-Wang Dong, and Li Yu. Distributed secure platoon control of connected vehicles subject to dos attack: theory and application. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2020.

[109] Chunheng Zhao, Jasprit Singh Gill, Pierluigi Pisu, and Gurcan Comert. Detection of false data injection attack in connected and automated vehicles via cloud-based sandboxing. *IEEE Transactions on Intelligent Transportation Systems*, pages 1–11, 2021. DOI:10.1109/TITS.2021.3090361.

Appendices

Appendix A

Ethics Certificate

Certificate of Ethical Approval

Applicant:	Sean Taylor
Project Title:	Cybersecurity in platooning of Vehicles Thesis write up

This is to certify that the above named applicant has completed the Coventry University Ethical Approval process and their project has been confirmed and approved as Low Risk

Date of approval:	18 Jul 2023
Project Reference Number:	P162031

Figure A.1: *Ethics approval*

Appendix B

Vehicular Platoon Communication: Cybersecurity Threats and Open Challenges

Appendix C

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

Appendix D

ARISTOTLE: AddRessIng falSe daTa injectiOn atTacks in vehicLE platoons

Appendix E

Vehicular Platoon Communication: Architecture, Security Threats and Open Challenges

Appendix F

A Comparative Analysis of Multi-Criteria Decision Methods for Secure Beacon Selection in Vehicular Platoons