Igor Fernandes Carneiro

A systematic review of security challenges in vehicular platooning

Universidade Federal de Pernambuco
graduacao@cin.ufpe.br
www.cin.ufpe.br/~graduacao

Recife
2023

Igor Fernandes Carneiro

A systematic review of security challenges in vehicular platooning

A B.Sc. Thesis presented to the Centro de Informática of the Universidade Federal de Pernambuco in partial fulfillment of the requirements for the degree of Bachelor in Information Systems.

Concentration Area: *Computer Networks and Distributed Systems*
Advisor: *Divanilson Rodrigo de Sousa Campelo*

Recife
2023

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Carneiro, Igor Fernandes.
A systematic review of security challenges in vehicular platooning / Igor Fernandes Carneiro. - Recife, 2023.
37 : il., tab.

Orientador(a): Divanilson Rodrigo de Sousa Campelo
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Informática, Sistemas de Informação - Bacharelado, 2023.

1. Security. 2. Vehicular Platooning. 3. Platoon stability. I. Campelo, Divanilson Rodrigo de Sousa. (Orientação). II. Título.

000 CDD (22.ed.)

IGOR FERNANDES CARNEIRO

A SYSTEMATIC REVIEW OF SECURITY CHALLENGES IN VEHICULAR PLATOONING

Dissertação apresentada ao Programa de Graduação em Sistemas de Informação da Universidade Federal de Pernambuco, Centro de Informática, como requisito para obtenção do grau de Bacharel em Sistemas de Informação. Área de concentração: Redes de Computadores e Sistemas Distribuídos.

Aprovado em: ___/___/_____.

BANCA EXAMINADORA

_____
Prof. Dr. Divanilson Rodrigo de Sousa Campelo (Orientador)
Universidade Federal de Pernambuco - UFPE

_____
Prof. Dr. Abel Guilhermino Da Silva Filho (Examinador Interno)
Universidade Federal de Pernambuco - UFPE

ABSTRACT

The industry and academia have been paying much attention to autonomous vehicles (AV) since this technology promises to increase mainly road safety and fuel efficiency. Vehicle platooning is a sub-field of AVs that aims to group vehicles on the road to achieve those benefits. Usually, the formation is a leader vehicle that guides the follower vehicles to the destination.

This work systematically reviews relevant articles from the literature about security in vehicle platooning. The goals are to point out the main security issues and current solutions, identify research tendencies and give future research directions for security in vehicle platooning.

The analysis showed that network and application-layer issues are the only topics in vehicle platooning articles. In contrast, the autonomous vehicles (AV) field also includes system issues. The issues in the platoon realm are related to string stability, and the solutions try to prevent them from getting broken. Moreover, although the general field (AV) and the sub-field (platoon) don't share many vulnerabilities, malware attacks were identified as potential threats to platoons.

Despite these findings, the chosen parameters for this systematic review limited the achievement of more accurate results about the research tendencies and gaps in the platoon field. Using the same methodology, future systematic reviews on this theme shall improve the search term and increase the number of reviewed articles.

Keywords: Security, Vehicular Platooning, Platoon stability

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

ACC	Adaptive Cruise Control
AV	Autonomous vehicle
CAPES	Coordination for the Improvement of Higher Education Personnel
C-V2X	Cellular Vehicle-to-Everything
CACC	Cooperative Adaptive Cruise Control
CAN	Controller Area Network
CPS	Cyber-Physical system
DoS	Denial of service
ECU	Electronic Control Unit
LiDAR	Light Detection and Ranging
OBU	On-Board unit
PUF	Physical Unclonable Function
RSU	Roadsite unit
SLR	Systematic Literature Review
VANET	Vehicular Ad-Hoc Network

CONTENTS

1

INTRODUCTION

In the last years, the number of road accidents has increased around the world [4]. Most road accidents have the root cause of humans as they can lose attention and get distracted [5]. Because of that, Autonomous vehicle (AV) have drawn much attention from the industry and research community since the technology promises to increase road safety, capacity, and fuel efficiency. s An autonomous vehicle is a Cyber-Physical system (CPS) that integrates cameras, LiDAR, and sensors in a physical system capable of mobility. From those components, the vehicle software can perceive the environment and make decisions about braking and steering. Due to these systems interacting with the physical world, cyber attacks can cause significant or even catastrophic damage [6]. The sensors are part of the attack surface in autonomous vehicle systems, and they may be vulnerable to false data injection attacks and adversarial-object attacks [7]. Nonetheless, the automotive industry wants to achieve a level-5 of automation where the vehicles can automatically park themselves and pick up the users [8]. Those capabilities can only be possible by connecting the car to the Internet. Vehicle networks, like sensors, have their set of vulnerabilities, including Denial of service (DoS), replay attacks, and packet falsification [9].

As a sub-field of AV, there is vehicle platooning. Platooning is a group of vehicles on the road in formation, and usually, there is a leader vehicle conducted by humans, serving as a guide for other vehicles (followers). From an industry perspective, the most notable advantage of this system is cost reduction (human resources for driving). However, that is not the only one. Since vehicles are controlled by software, they can efficiently travel along the road with a small distance between each other, increasing the lane capacity [10]. The close gaps also reduce air pollution and save fuel due to lower air resistance experienced by the following vehicles. Some experiment results showed the reduction could reach up to 8% in specific conditions [11]. Furthermore, the benefits of vehicle platooning extend beyond the industrial realm; individual vehicles can join a platooning to take most of the advantages discussed previously [12].

This work aims to systematically review the literature in order to identify the main security issues in platoon systems, along with the proposed solutions for such problems. As platooning involves a group of self-driving vehicles, it is subject to the same security concerns as autonomous vehicles. For this reason, this research has three specific goals: compare security issues between the autonomous driving realm and platoon field, identify research gaps, and

examine how the academic community has addressed security issues by analyzing the number of papers published in the last years.

The organization of this work is as follows. Chapter 2 presents some essential concepts to give the reader the foundational knowledge to comprehend the results and discussion. Chapter 3 outlines the selection criteria and steps taken for this systematic review. Chapter 4 presents all the findings regarding platooning-specific issues, solutions, and research tendencies. Chapter 5 gathers the results, gives them meaning, and the chosen methodology's advantages and disadvantages. Chapter 6 closes this work, summarizes the discussion, and suggests the next directions for this research.

2

BACKGROUND

Vehicle platooning has an exclusive set of concepts like control strategy, network topology, platoon stability, and vehicle heterogeneity. Furthermore, it shares some of its concepts with autonomous vehicles, such as vehicle networks and vehicular vulnerability classification. The following sections explain what those concepts are and what challenges and security threats they bring to this research field.

2.1 PLATOON CONTROL STRATEGY

The platooning control strategy is the algorithm that controls the speed of the platooning vehicles to maintain the desired gap between them. The distance between the string nodes is chosen based on fuel saving and risk analysis. By keeping the vehicles close to each other, the fuel is saved due to lower air resistance experienced by them. Hence the engine needs to apply less force to maintain the vehicle velocity. In addition, the road capacity is improved since more cars can fit on the road [12]. However, some threats come from reducing the gap inadvertently since it takes time for the vehicles to stop after braking the command, and the other vehicles may not have enough time to stop, potentially causing a collision [13].

Those threats are inherent to the system, and it's necessary to have risk management. But, there are some vulnerabilities that exploit the platooning control strategy in diverse ways. These cyber-attacks aim to break the platoon's stability, thus affecting the distance between the group's vehicles. Section 2.5 presents some of these vulnerabilities.

2.2 PLATOON NETWORK TOPOLOGIES

As a collection of vehicles targeting to reach the destination, the platoon vehicles need to be interconnected to synchronize braking and acceleration, enabling the system to realize the advantages discussed in the previous sections. Some network topologies were proposed by academia to guarantee that, and they can be organized into two practical groups: *Nearest Neighbor*, and *Leader-to-All* [1].

The nearest neighbor topologies are all arrangements for connecting vehicles to the

nearest nodes. For instance, in *predecessor following* topology, every vehicle connects to its immediate neighbor unidirectionally. Nonetheless, there is the bidirectional topology, where the vehicles are interconnected to their direct front and back vehicles [1].

In leader-to-all topologies, the leader vehicle is connected to all the nodes of the platoon. Such as nearest neighbor topologies; they also can be unidirectional and bidirectional. Compared to the previous topologies, all vehicles communicate directly with the leader. Thus, if a malicious vehicle is in the network, the other vehicles would not be affected unless the leader is compromised.

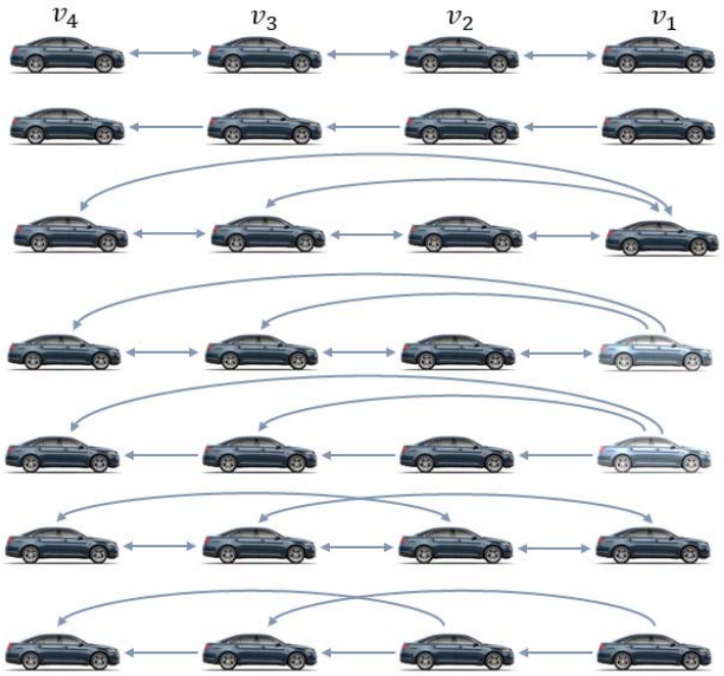

Figure 1: Nearest Neighbor and Leader-to-All topologies. Image from [1].

2.3 PLATOON HETEROGENEITY

Most of the platooning research has been focused on homogeneous platooning, where all vehicles in the platoon have the same characteristics, such as size, weight, and performance (same vehicle model). That scenario may be actual in the logistics industry where trucks are used. However, platooning is also applicable to regular vehicles like cars. On the road, cars of different models will be traveling, and if they are organized as a platoon with a control system, the road capacity and traffic flow can be increased [14].

The Cooperative Adaptive Cruise Control (CACC) is a car system that aims to control the vehicle's speed on the road by using wireless communication to share information with other close cars. It's the collaborative version of Adaptive Cruise Control (ACC), the system able to maintain the car under a velocity by braking and accelerating the vehicle when it's necessary. Theoretically, in a highway that can accommodate 8,200 vehicles/h, if all vehicles use CACC,

the road capacity could reach 10,500 vehicles/h [15].

2.4 VEHICULAR COMMUNICATION AND NETWORKS

There are some communication and network protocols with active research on autonomous vehicles. They can be categorized according to the type of devices that participate in the network.

2.4.1 Intra-vehicular network

Regarding the communication between the vehicle components and mobile-to-vehicle communication, they form the in-vehicle network [16]. The Controller Area Network (CAN) is a lightweight serial and asynchronous network protocol to connect the Electronic Control Units (ECUs). Such as some traditional serial communication protocols it has a bus to transfer data shared by all the components. Also, it aimed to be lightweight and less robust. Hence it lacks authentication of the connected components and data encryption during transfer. For example, if some of the components are compromised by malware, other parts can also be affected [2].

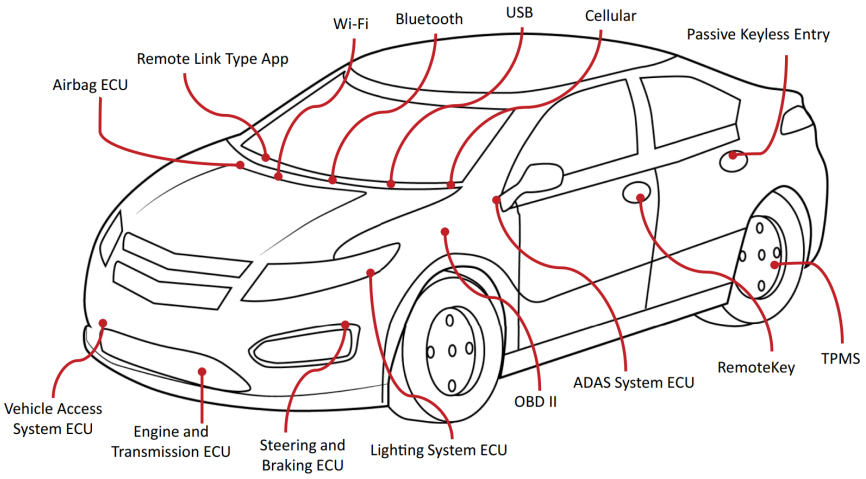

Figure 2: Vehicle's electronic control units. Image from [2].

2.4.2 Vehicule-to-everything communication (V2X)

In addition to the communication among internal electronic components of the vehicle, the vehicle can also communicate with the road infrastructure and other vehicles; they are called vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V), respectively. The vehicle-to-everything (V2X) is the generalization and communication to any component of an autonomous driving infrastructure [17].

The Cellular Vehicle-to-Everything (C-V2X) is a V2X communication technology built on cellular networks. The idea is to use cellular infrastructure to create a reliable channel for the vehicles on the road to communicate with each other. It has different names depending

on its cellular network type: LTE-V2X for 4G and 5G-V2X for 5G infrastructure. As this communication technology occurs over a cellular network infrastructure, it inherits any associated issues. Although cellular networks have been implemented and used for some years, security issues may still be encountered. For instance, an attack scenario that can cause a DoS on the vehicles communicating through this technology have been discovered in [18].

2.4.3 VANET

VANET is a vehicular ad-hoc network that enables V2V and V2I communication. To achieve this, it relies on Roadsite units (RSUs) as part of the infrastructure to provide authentication, security, and communication to the vehicles. In addition, vehicles must also have On-Board units (OBUs) installed to participate in VANET communication [3]. The network infrastructure facilitates sharing crucial information, such as traffic updates, road conditions, and collision warnings, to optimize route planning [19], for instance.

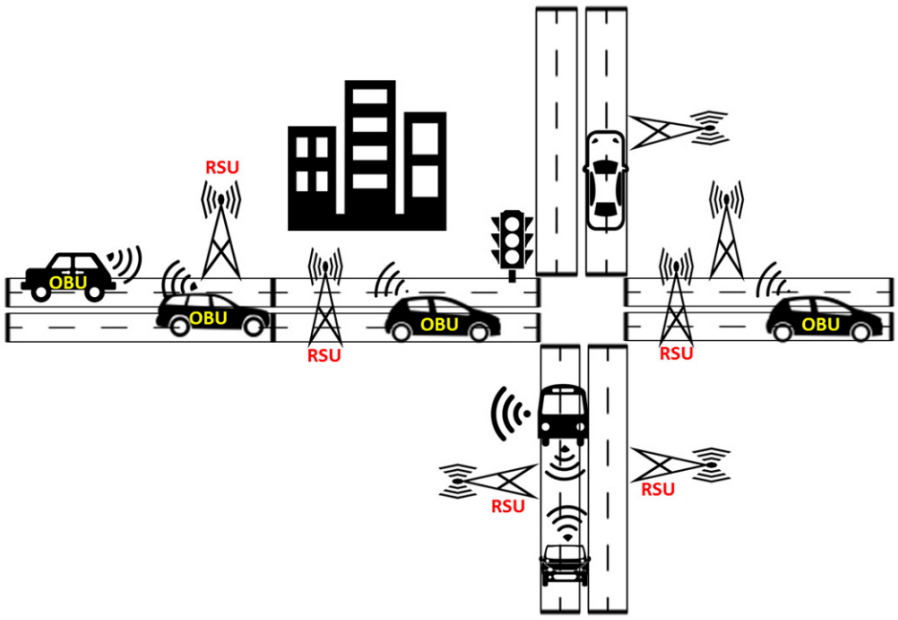

Figure 3: VANET network. Image from [3].

To ensure network scalability, the protocol projects multi-hop communication, which includes vehicles as intermediate nodes. The protocols utilized over the VANET network must consider the possibility of malicious vehicles. Otherwise, messages could arrive at the network nodes in a tampered state. For instance, Geocast protocols enable vehicles to know the geolocation of the neighbor cars. It does so by the vehicles periodically broadcasting *beoconing messages* periodically [20]. If the protocol lacks mechanisms to preserve message integrity as it passes through an intermediate node, features that rely on the Geocast protocol may be compromised.

2.5 PLATOON VULNERABILITIES

As a collection of autonomous vehicles, the platoon has its own vulnerabilities, most targeting network and application layers. In contrast, system layer and perception vulnerabilities are more common when considering the vehicles individually.

2.5.1 Application layer and perception

The application layer is the upper layer of the system. In platooning, the application layer refers to the software (platoon control strategy) that manages the speed and distance between the vehicles. That means vulnerabilities in this layer trick the software into making undesired decisions. Some vulnerabilities in the application layer include *replay attacks*, *sybil attacks*, *spoofing attacks*, and *packet falsification*, for instance. These vulnerabilities can cause severe damage to the platoon system or even collisions with other vehicles. Replay attacks, for example, eavesdrop on the messages exchanged by the participants, save them, and eventually send them. Since the message's integrity was kept, the members may believe it came from a legitimate sender when actually it was sent by the attacker who captured the original messages. The received message may not reflect the vehicle's current state and can cause the system to make incorrect decisions. In sybil attacks, the attacker fabricates fake vehicles in the network to deceive other members and influence their decision-making. On the other hand, in spoofing attacks and packet falsification, the attacker fakes messages on the network. The messages containing speed may affect the string stability and potentially cause vehicle collisions. Unlike spoofing attacks, where attackers impersonate legitimate senders to inject false data into the platoon system, packet falsification involves modifying or deleting packets in transit. Some of those vulnerabilities are possible because a vehicle can act as a relay node [21].

The perception layer is part of the application layer, but they are emphasized individually for this work. The perception layer is the middle layer between decision-making (upper layer) and the sensors (lowest layer) [22]. It's where the vehicle reads the sensors' data and recognizes objects on the road. The most common vulnerability is the adversarial object attack, where the attacker jams the sensors injecting false data to give the vehicle a wrong perception of the environment [23]. That can cause the system to perceive the object with incorrect distances and make unsafe decisions. *Light Detection and Ranging (LiDAR) spoofing* is a type of adversarial object attack, in which the LiDAR sensor is tricked. The attacker can build an object using a 3D printer, which can cause a sudden stop (emergency braking) decision by the car. The consequences may be injuries to passengers or rear-end collisions [7]. There are countermeasures for adversarial object attacks, like using multi-sensor fusion, which can be more robust since different sources are used to recognize the environment. However, even the multi-sensor fusion strategy can not secure the system completely for some attack scenarios, as seen in [24].

2.5.2 Network layer

On the network layer, attacks do not target some functionality but communication. In other words, the vulnerabilities prevent the application that relies on the network from functioning correctly. Some vulnerabilities in the application layer include *Denial of service (DoS)* and *radio jamming*. The DoS attack occurs when the target receives several requests or messages beyond what it can process, causing service instability or even interruption. On the other hand, in a radio jamming attack, the attacker broadcasts a radio signal on the same frequency as the one used by the target network in order to send noise to the receiver and render legitimate messages incomprehensible [3]. Both vulnerabilities compromise communication and can cause serious accidents. Therefore, solutions for at least detecting attacks are necessary, so the vehicle under attack or the platoon can downgrade the CACC system to ACC, as proposed in [21].

2.5.3 System layer

The system layer is where the firmware of the autonomous vehicle is, but it also includes the sensor components. Attacks at this layer encompass forging sensors, modifying, or injecting malware into the system [21]. For instance, the attacker can tamper with the sensor or upgrade the vehicle software with a malicious version that can interfere with the sensor data, leading to a wrong perception of the environment and bad decisions. The academia has been researching Physical Unclonable Function (PUF), an additional physical layer to encrypt the communication in a CAN network, to address attacks at this layer. For example, in [25], the proposed framework authenticates each node in the network by using public-private key mechanisms enrolled in a trusted environment (factory). This solution would reject ECU in a tampered state to be part of CAN network.

3

METHODOLOGY

This work uses Systematic Literature Review (SLR) as methodology, which provides well-defined procedures for all phases of the literature review process, from article selection to analysis. Using SLR improves the research's reproducibility and facilitates comparisons between methodologies.

Thus, aiming to ensure a rigorous and comprehensive review, this work first defines the review protocol, which shares the same procedures in the guideline: *Systematic literature reviews in software engineering – A tertiary study* [26]. Therefore, the protocol followed by this work is: defining the research question, delimiting the source and amount of articles, outlining the search term, establishing inclusion and exclusion criteria, selecting the papers, and extracting and synthesizing data from the selected articles. All those phases are detailed in the following sections.

3.1 RESERCH QUESTION

The motivation for this work is understanding the challenges from a security perspective associated with the operation of vehicle platoons on public roads. By identifying the threats and solutions, this study can address future research areas by highlighting the gaps and unexplored topics. Thus, to guide this investigation, the research questions are:

- What are the autonomous vehicles and platoon vulnerabilities?
- What are the defense solutions for platoon and autonomous vehicles?

3.2 ARTICLE COLLECTION

As part of the article collection process, Google Scholar was chosen as the article indexer for the search in the literature. Google Scholar is an extensive search engine that finds articles from various journals, magazines, and newspapers.

To enable the research questions to be answered, a carefully crafted search term was required. Therefore, locating articles more likely to demonstrate vulnerabilities and solutions to

address security concerns become easier. As a result, the following search term was chosen:

> (“security” **OR** “secure” **OR** “insecure” **OR** “cyber attack”) **AND** ("vehicle platoon” **OR** “autonomous driving” **OR** “platooning” **OR** “connected vehicle” **OR** “vehicular communication”)

In addition to the search term, search limits were required, and therefore, it was defined that only articles from the first 10 pages of the search results would be included in this work. Additionally, to obtain a more reliable snapshot of the current moment, all result pages were accessed within a 3-hour interval.

A spreadsheet was created in Google Sheets to organize the article collection. In the first tab, all the articles from the search were listed with their title, authors, year, and source. Using a spreadsheet facilitates the filtering process in the next phase.

3.3 INCLUSION AND EXCLUSION CRITERIA

The next phase defined which articles would be selected from the articles pool. The inclusion criteria refer to all the characteristics that must be present in the article. Conversely, the exclusion criteria comprise the characteristics that are not acceptable.

Furthermore, to be able to analyze more articles and meet the deadline for this work, the chosen inclusion criteria aimed to filter by quality. Therefore, more excellent guarantees exist that the selected papers are backed by valid evidence. Among the criteria, this study uses the Qualis metric, a quality classification based on the source of the article’s publication. The metric was developed by Coordination for the Improvement of Higher Education Personnel (CAPES) in Brazil, and it classifies sources from A1 (most relevant) to C (least relevant), with B1-B4 also being used as intermediate labels [27]. As a result, the inclusion criteria are:

- English article
- Peer-reviewed article
- Source Qualis classification: A1-A3

Additionally, this SLR aims to identify only security threats related to the cyber layer of vehicle platoons and potential solutions for these threats. In order to achieve this goal, the following exclusion criteria were selected. The exclusion criteria were applied to the articles’ abstracts.

- Book. The reference cannot be a book since it usually does not point to recent vulnerabilities and focuses more on concepts.

- Articles that do not address security concerns related to autonomous vehicles and platoons. Specifically, articles that do not demonstrate vulnerabilities/threats or provide solutions or security improvements for AV systems.
- Articles that only measure the performance of a solution without addressing security concerns.
- Articles that aim to improve an existing solution only for performance reasons, without addressing security concerns.

During the first phase, all articles were gathered and organized in a spreadsheet. Each source was carefully examined and classified based on its Qualis rate and whether or not it has a peer-review process. To determine if the source has a peer-review process, the official page of each source was consulted. For the Qualis rating, all references were classified based on the Qualis rating list of the Post-Graduate Program in Computer Science at PUCRS, which compiles the ratings of academic journals [28]. If that information was not available, the source was declassified. The results of this process were recorded in a separate tab of the spreadsheet, which included columns for each source's Qualis rating, peer-reviewed status (Yes/No), whether or not it was a book (Yes/No), and the website's link that confirms the information.

Table 1: Sample of sources classification sheet

Source	Peer-reviewed	Qualis	Book	Reference
IEEE Transactions on Computers	Yes	A2	No	Link
Proceedings - 12th IEEE International...	Yes	A4	No	Link
IEEE Transactions on Industrial Informatics	Yes	A1	No	Link
Proceedings - 3rd IEEE International...	Yes	A4	No	Link

With all the necessary information about the sources, the articles were filtered according to the defined inclusion criteria. Then, the abstracts of the remaining papers were read to assess whether they fit the exclusion criteria. However, despite the relatively straightforward criteria, the classification still has subjectivity. Additionally, it is essential to note that only one researcher carried out the classification process.

3.4 DATA EXTRACTION AND SYNTHESIZATION

This work followed a thematic synthesis process adapted from [29] to identify the vulnerabilities and solutions from the selected papers. The process consists of extracting three types of data: publication details, the paper context, and results. The publication data is authors, title, year, and source. The paper's context includes the technologies and subjects of the article. And finally, the results have the objective achieved with the work.

The publication details do not need to be synthesized since they are already straightforward. Differently from publication details, which are usually straightforward, work context and results do not follow a standardized pattern and may be scattered across different sections of the articles. For instance, results are typically reported in a dedicated section or the conclusion. Still, sometimes there is no explicit results section, and the information is described elsewhere in the work [29]. Thus, to find them required to read articles in detail. Since the evidence is not the focus of this work, the evidence details were disregarded in the reading phase.

To collect the context and results, the researcher summarized text segments from the articles that appeared relevant. After reading all papers, it was possible to understand the potential types of contexts in the works. Therefore, based on the summarized information of context and results, labels were created for a subsequent generation of insights. The list of context and results were recorded in the same spreadsheet used in the filtering process. The tables below provide an example of the summarization and labeling process.

Table 2: Sample of article's context and results summarization

Title	**...**	**Contexts**	**Results**
...	...	- Defense solution - Vehicular communication - Proposes a Vehicular public-key infrastructure (VPKI) system - Privacy protection: against honest-but-curious entities, VPKI servers collude - Review literature: VPKI system solutions/projects/schemes - Review literature: security/privacy requirements on vehicle-VPKI interactions	- VPKI schemes comparison table - Experiments were done by deploying cloud servers - The servers can serve on-demand requests with very low delay
...	...	- Vulnerability demonstration - Multi-sensor (Camera and LiDAR) fusion attack - Adversarial 3D-printed object - Novel attack pipeline: non-differentiable target camera and LiDAR sensing systems - Suggests some defense strategies: add more one sensor (RADAR) and retrain DNN models	- The attack succeeds 90% of the time across different object types - Simulations were done with Apollo AV - Defense suggestion decreases the attack success rate to 66%
...	...	- Vulnerability demonstration - Focused on platoon - Platoon stability - Assumption: some following vehicles with malicious intentions - Insider version of replay attack	- Theoretically, the attacker can control the relative position and velocity of surrounding vehicles

Table 3: Sample of labeling summarized context

Context	**Labels**
Adversarial 3D-printed object	Vulnerability: Adversarial object
Adversarial Machine Learning to generate adversarial examples	Vulnerability: Adversarial object Strategy: Machine Learning Strategy: Neural Network
Develop a platooning control strategy	Solution: Platooning control strategy Layer: Application
Develop an algorithm to identify intermittent DoS attacks	Solution: Attack detection Vulnerability: DoS Layer: Network
Present security flaws of LTE-V2X	Vulnerability presentation: New Network: LTE-V2X Network: Cellular
Survey vulnerabilities and defenses strategies for Deep-Learning based autonomous driving	Vulnerability presentation: Review Survey: Yes Defense presentation: Review

The context segments labeled "Review literature" were excluded, as they do not represent the primary purpose of the articles. Additionally, each context or result segment could have multiple labels. Afterward, all papers were tagged according to their context and result labels.

3.4.1 Deviation from protocol

In the data extraction phase, text segments were collected from the articles. Then, in the data synthesis phase, it became apparent that certain text segments would generate valuable insights, but some papers lacked the necessary data for labeling. As a result, particular articles had to be revisited to ensure proper labeling. This deviation from the protocol was necessary due to three labeling criteria: platoon topology, platoon heterogeneity considerations, and attack/defense experimentation.

Unlike the exclusion by criteria phase, the data extraction phase required reading the articles fully, where only the abstract was analyzed. The researcher didn't expect to find articles meeting the exclusion criteria during the readings. However, such cases did occur. These articles were excluded from the analysis as soon as it was determined that they were outside the scope of this study.

4

RESULTS

As a result of the filtering process, from 100 papers initially gathered from Google Scholar, only 52 articles were included based on the inclusion criteria, and 15 papers were excluded based on the exclusion criteria. During the data extraction phase, 1 article was identified as out of the scope of this study. The total of selected articles was 36.

Table 4: Remaining articles along the phases

Phase	Remaining articles
Article collection	100
Inclusion criteria application	52
Exclusion criteria application	37
Exclusion in data extraction	36

Out of the 36 reviewed papers, 21 focused on autonomous driving, while the remaining 15 were centered on platooning. The charts below show how many papers were found focusing on particular vulnerabilities for the selected articles. The first chart displays how many articles were found about platooning against general works related to autonomous driving. The second and third charts focus on papers with a particular vulnerability as a theme.

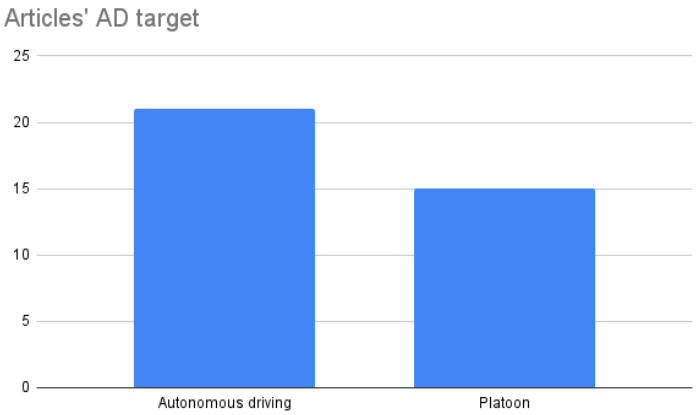

Figure 4: Articles' AD target

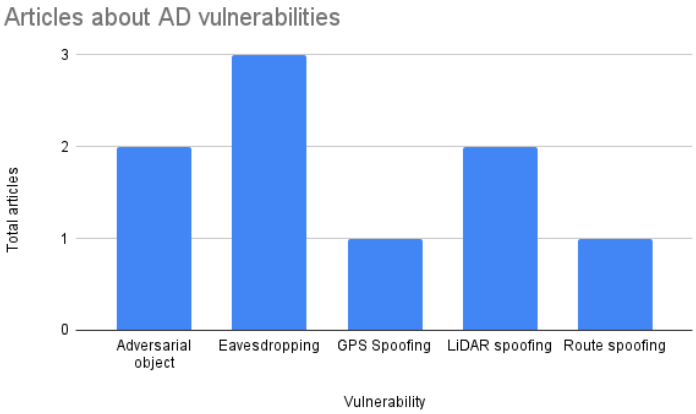

Figure 5: Articles about AD vulnerabilities

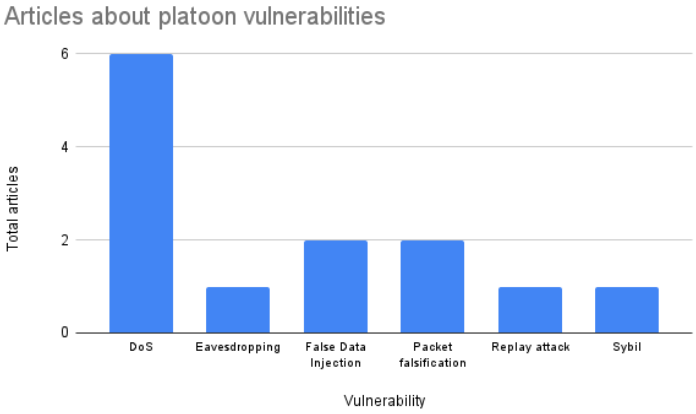

Figure 6: Articles about Platoon vulnerabilities

The following two charts illustrate the number of papers categorized by the target layer. The first focuses on general works related to autonomous driving, and the second on articles related to platoon systems.

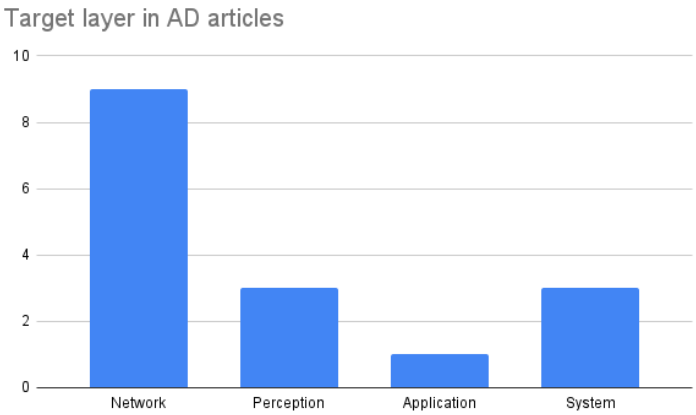

Figure 7: Target layer in AD articles

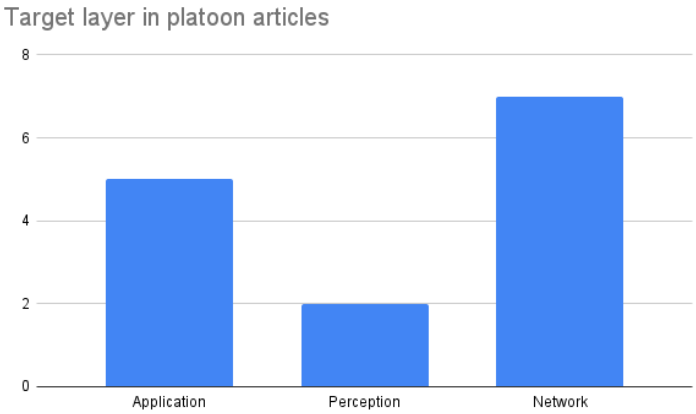

Figure 8: Target layer in Platoon articles

To distinguish between studies that focused on vulnerabilities and those that presented solutions in the context of platoon applications, the author categorized them into two groups: Attack and Defense. Articles that identified new vulnerabilities were classified as Attack, while those proposing solutions to known vulnerabilities were classified as Defense. Survey papers and those proposing new features were excluded from this classification. The chart below displays the number of articles in each category for both platoon and autonomous driving papers.

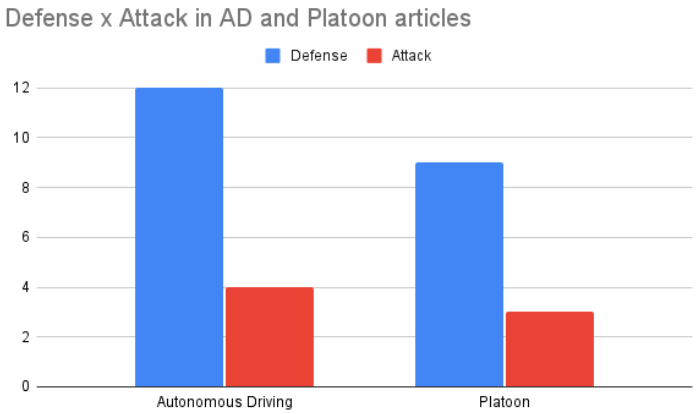

Figure 9: Defense and Attack articles (AD and Platoon)

This work also analyzed how academia has approached various platoon topologies and considered platoon heterogeneity. The following charts indicate the number of papers that consider a specific topology and their purpose: to propose a defense solution, a new functionality, or an attack scenario. Additionally, the charts demonstrate how the studies have addressed platoon heterogeneity. However, some papers did not clearly specify whether the considered composition was heterogeneous or homogeneous or for which topologies their attack scenario or solution is applicable. Such papers were classified as "Not specified". Moreover, surveys were classified as "Not Applicable".

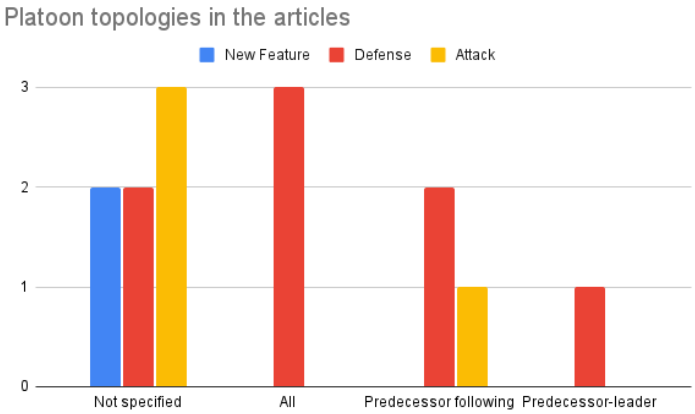

Figure 10: Platoon topologies in the articles

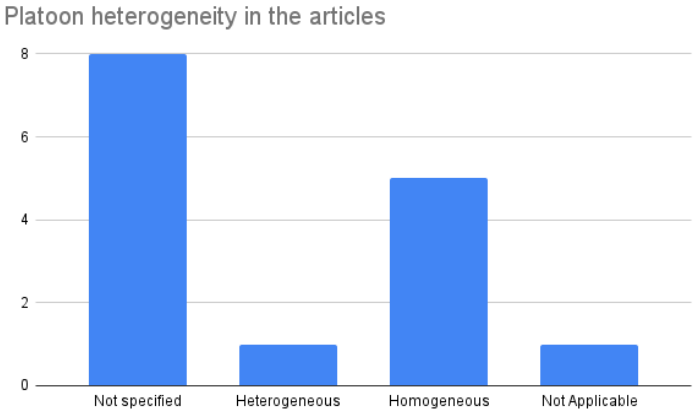

Figure 11: Platoon heterogeneity in the articles

Additionally, this study evaluated how the papers have been validating their work. The following chart displays that in the platoon and general autonomous driving works. The experimentation methods were classified as Not Applicable, No, Physical-world, and Simulation.

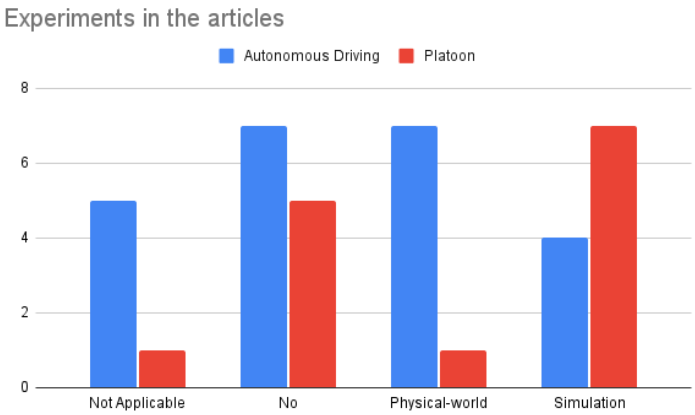

Figure 12: Experiments in the articles

To identify current research trends in platooning and autonomous driving, the chart below displays the number of articles published in both scopes, with survey articles highlighted. All 36 selected papers were taken into account.

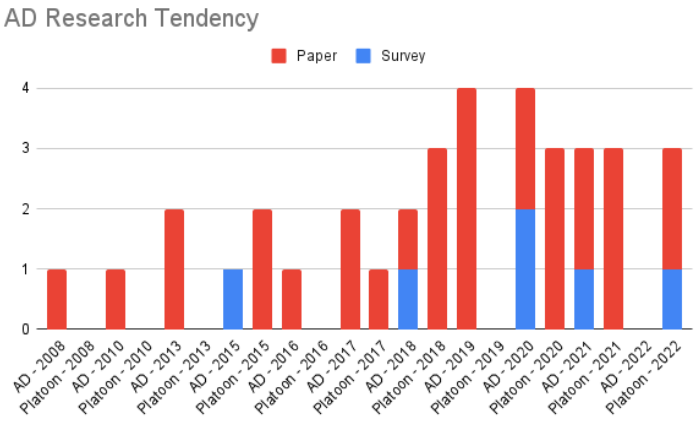

Figure 13: AD Research Tendency

5

DISCUSSION

5.1 VULNERABILITY DIFFERENCES

This work's theme is understanding the security challenges in vehicle platoons. Since a platoon is a collection of vehicles that shares the same steering profile to get to the destination, the first research question aimed to comprise the existence of differences between autonomous driving vulnerabilities and platoon. From this review's result, Figure 5 and Figure 6 display that those realms don't share many common vulnerabilities. Nevertheless, the target layers of those vulnerabilities are similar. Most of the papers are about threats in the network and application layer (including the perception layer), as displayed in Figures 7 and 8. According to the results, the system vulnerabilities are limited to the autonomous driving domain, although platoons can have their system compromised by malware or forged sensors. As pointed out in [30, 31] malware is a threat to platoon systems. The consequences may be different from an autonomous vehicle, given that the flaw might not keep the vehicle's speed according to the platoon's steering profile or even prevent the nodes of the platoon from communicating with each other when they are planning to break themselves. A compromised communication can cause severe damage in platooning scenarios, as the vehicles are typically positioned close together to take advantage of the lower air resistance and save fuel. However, if the platoon travels at high speed, not all nodes may receive critical information, such as the lead vehicle's intention to brake. Additionally, threats arise when platoon members utilize forged sensors.

Some of the vulnerabilities observed only in the autonomous driving domain were *route spoofing* and *GPS spoofing*. These vulnerabilities are classified as application-layer vulnerabilities since they alter the system's behavior through the application's protocols, rather than through injected malware. Route spoofing is a vulnerability that seeks to modify the route selected by the software of the target vehicle. One way to accomplish this is by leveraging the same principles and techniques used in a Sybil attack, by fabricating dummy vehicles in the network and broadcasting their location to simulate a traffic jam, then making the software take another route [32]. The GPS spoofing, on the other hand, is not a problem exclusive to the scope of this study since the vulnerability lies within the GPS communication protocol. Thus, other applications such as smartphone operating systems also suffer from the same issue.

For the GPS sensor to work, it listens to signals sent by four or more satellites to determine its geographical location [33]. However, the signals are not encrypted and neither there is an authentication mechanism to verify the legitimacy of the source who sent the message. Therefore, an attacker can fabricate GPS signals within a range aiming to trick the vehicles' GPS receivers. As demonstrated in [34], GPS spoofing is capable of causing vehicles to be diverted off-road or taken the wrong way. Although, as also pointed out in the same study, AD systems use other sensors to locate the vehicle in space. For example, the LiDAR sensor helps the vehicle perceive its position relative to surrounding objects and buildings, thus contributing to making GPS spoofing attacks not entirely effective, although still possible.

The vulnerabilities at the network layer in the autonomous driving domain are associated with the papers investigating the threats in VANETs. Although VANETs can be utilized to manage platoons [21], the identified articles aimed to propose and demonstrate network solutions in general rather than specific to platooning. Typically, VANET packets hold information that helps vehicles in the network visualize the other cars' location on the road and also trace routes. Since vehicles can serve as intermediate nodes in communication, the network may be vulnerable to malicious nodes who falsify packets. Such packet falsification may cause the cars to make incorrect decisions, such as leaving the road [34].

While the potential presence of malicious vehicles in VANETs is a concern, other platoon papers have also highlighted an additional issue. Communication with platoon vehicles is protected with cryptographic keys, regardless of topology, which mitigates the risk of packet falsification for scenarios where the attacker is not part of the platoon [21]. However, the leakage of cryptographic keys creates a new attack surface, enabling attackers to exploit the communication protocol to manipulate the group's behavior on the road. The consequences of such attacks are comparable to the malware injection into the system. Vulnerabilities originating from the presence of a malicious vehicle in the platoon are referred to as *insider attacks* [35]. In contrast, insider attacks were not observed in autonomous driving articles because there is only one internal agent in this context: the vehicle itself.

In addition to these threats to the application layer in VANET networks, the other application threats that autonomous vehicles may face during their operations must also be considered. The reviewed articles showed that techniques such as *LiDAR spoofing* and *adversarial object attacks* alter the vehicle's environment perception, leading to incorrect decision-making. Some papers, for instance, exploit vulnerabilities in deep learning-based object system detection aiming to find inputs that can cause misinterpretation or make the object invisible [7]. In these attack scenarios, a possible consequence is a collision or improper lane deviation. Although these kinds of attacks can compromise the stability of the platoon formation, and it was not observed in the literature during the review, solving these issues from the research in the autonomous driving field will benefit the platoon field.

Based on the articles reviewed, vulnerability studies in the platooning domain primarily focus on disrupting the stability of the formation, thus, shared vulnerabilities between these

domains are unlikely. On the other hand, since system-related problems, such as sensor tampering, are inherent to individual vehicles, they are studied within autonomous driving. As a result, the targeted layers are common, except for the system layer, for which no platooning-related studies have been observed.

5.2 SOLUTION PROPOSALS

The author chose the second research to identify what solution the academia is proposing to mitigate the vulnerability of autonomous driving and platoons found in the first research question. The results of this investigation demonstrate that there are more studies seeking solutions rather than presenting new attack scenarios (Figure 9). This trend is evident in both fields of study. It was impossible to identify similar solutions among them, which is reasonable considering that the challenges faced in each context are unique.

In the platoon realm, the most basic solution for a group under attack is to downgrade the platoon to ACC [21]. In other words, the vehicles cease to behave as a group and begin taking individual actions, prioritizing collision avoidance over maintaining the steering profile defined by the platoon. However, the vehicle must first recognize that it is under attack to initiate a downgrade. As a result, many of the reviewed works focus on developing solutions that identify these threats during platoon operations. Among the reviewed papers, more optimized solutions go beyond the basic principle. An example is the ability to recognize tampered communication or communication from a malicious source, intending only to assimilate relevant and truthful information [36]. The detection can also occur through the perception of the behavior of the front or rear vehicle [37].

In the field of autonomous driving in general, the proposed solution works target the network, application, perception, and system layers. Some observed topics were about intra-vehicle security for secure communication between ECUs on CAN networks and solutions to create a system capable of managing credentials and allowing anonymity of vehicles in VANETs [25, 38, 39]. However, most articles proposed ways to prevent eavesdropping in vehicle-to-vehicle networks such as VANET. Techniques such as communicating through directional transmission with noise added in other directions were observed to ensure that only the intended recipient receives the message [40, 41]. Those solutions are also applicable in platoons since the formation is usually static, unlike communication between individual cars on the highway where vehicles may be in different lanes, and lane-changing or passing is a common movement. Despite this, no papers in the platoon domain applying this strategy were observed.

This study conducted a further observation from the reviews. Few studies in platoons proposed security enhancements in topologies beyond predecessor-following (Figure 10). Together with leader-to-all topologies, they are the simplest topologies and, therefore, good candidates for testing solutions. However, they are not the best when the goal is a robust and distributed system. Topologies such as k-nearest neighbors show great results in keeping the platoon's

formation stable when a malicious vehicle is in the group [1]. Nonetheless, this consideration was not observed in the reviewed works. Thus, the question remains about how generalizable the proposed solutions for platoons that choose to validate their studies based on a specific topology are, given that different topologies entail different implementation complexities.

Similarly, the heterogeneity of the platoon is also a little-explored aspect in the literature (Figure 11). A good portion of the reviewed articles considered the system homogeneous for evaluative purposes, which can compromise the solution's applicability to heterogeneous systems. Although some papers have been categorized as "Not specified", it is not unlikely that their assumptions are similar to the ones that are considered homogeneous. During the reviews, no variables or formulas were observed that considered the possibility that each vehicle could have a different length or even the time that each vehicle model takes to decelerate, which would affect the distance calculations between vehicles. However, to avoid errors due to a lack of more profound technical knowledge on the subject, the author decided to keep them as "Not specified". Nevertheless, solutions for heterogeneous platoons are valuable. On the road, ordinary cars from different manufacturers could join to compose a platoon and enjoy the advantages of reducing fuel consumption and increasing road capacity. To make that solution feasible, there are already studies exploring the possibility of creating protocols for dynamic platoon formation, where vehicles can enter and leave the group when on a highway [12].

In addition, this research observed how the autonomous driving and platoon papers validate their solutions (Figure 12). Since accidents in these domains can be catastrophic, the results of solution evaluations must be highly reliable, therefore, experiments must be as close to reality as possible. Most of the reviewed articles validate by doing some kind of experiment in the real world or by simulation. However, a significant portion of the works was limited to theory only, around 38% (excluding works not applicable for experimentation). This ratio is the same for both fields of study (platoon and autonomous driving), but in the platoon domain, there are more papers that conduct experiments through simulations rather than real-world applications. It's noteworthy that financial and spatial barriers hinder the validation of the concepts addressed in the research. The lack of resources such as space and vehicles, as well as the need for machines capable of performing complex simulations, make it impractical to proceed with the research development in some cases. Given this, solutions such as cloud simulations, already discussed in [23], may offer a viable alternative for researchers who wish to conduct experiments in a more accessible and cost-effective manner.

5.3 TENDENCIES AND STUDY LIMITATIONS

This systematic review was conducted using a search term and parameters that resulted in the inclusion of articles published from 2008 to 2022. The result analysis suggests that there has been an increasing tendency over the years, although the tendency curve cannot be determined precisely due to the defined limit of articles and the filtering based on the inclusion and exclusion

criteria. Out of the defined limit of 10 pages on Google Scholar, which corresponds to 100 papers, only 36 remained (Table 4). Notably, research on platooning began in 2015 and has maintained a constant quantity in the last three years, as shown in Figure 13. However, these results may not fully reflect the real trend, as among the reviewed works, a survey indicates that there are many more articles on platooning than shown [42]. That paper presented other surveys dating back to 2011, which suggests that there have been more studies in this field in previous years.

In addition, the methodology adopted may have caused bias in the results obtained since the search term used ended up highlighting vulnerabilities in autonomous vehicles more prominently than vulnerabilities in platooning. Although the goal was to understand the differences between these two domains, the wrong choice of the search term may have impacted the results. To address this issue, a possible solution would be to perform two separate searches: one to exclusively evaluate vulnerabilities in platooning and another to assess vulnerabilities in autonomous vehicles. This approach would allow for a more comprehensive and accurate analysis of the differences between these two domains. Moreover, the chosen inclusion and exclusion criteria may have hindered the detection of novel vulnerabilities, potentially missing key areas for future research. However, due to the deadline constraints, the author prioritized criteria ensuring the quality of the included articles without evaluating the evidence of the studies.

6

CONCLUSION

After conducting this systematic literature review, the results suggest that while platooning involves a group of vehicles intending to arrive at a destination, inheriting the same issues as an autonomous vehicle, the two fields of study do not investigate similar vulnerabilities. The main goal of the papers on the platoon's security domain is to maintain the platoon formation stable when facing cyber attacks in communication between the vehicles. Most defensive studies propose solutions to detect these threats and mechanisms to deal with them during operation, ultimately downgrading the attacked vehicle to ACC and turning it into an autonomous vehicle outside the group.

An analysis of threats in the autonomous driving field has revealed a potential area for future research in platooning: malware attacks. None of the reviewed articles addressed this topic. Malware attacks can potentially compromise the proper functioning of autonomous vehicle systems and create instability in the formation of a platoon. If one vehicle is infected, the other vehicles may stop receiving control messages or fail to ensure the combined steering profile.

Composition heterogeneity is an aspect of platooning that has been underexplored. To extend the advantages of fuel consumption reduction and increased highway capacity beyond the industry branch, where it is more feasible for trucks to be of the same model, researchers must account for varying vehicle lengths and engine reaction times across different brands. Such consideration is necessary for dynamic platooning on highways to be feasible and exploit these benefits.

Despite the findings, the accuracy of this research was limited by the parameters used in the applied methodology. The search term selected and the limit of articles narrowed the number of papers found related to platooning, which is the main focus of this study. Consequently, it was impossible to determine the trend in research on the platoon domain and whether there are sufficient papers addressing malware in platoon systems. For future research using the same methodology, it's recommended to increase the number of articles to be reviewed and perform two separate searches in the indexer: one focused exclusively on terms related to platooning and another focused solely on terms related to autonomous driving.

REFERENCES

[1] Mohammad Pirani, Simone Baldi, and Karl Henrik Johansson. Impact of network topology on the resilience of vehicle platoons. *IEEE Transactions on Intelligent Transportation Systems*, 23:15166–15177, 9 2022.

[2] Clinton Young, Joseph Zambreno, Habeeb Olufowobi, and Gedare Bloom. Survey of automotive controller area network intrusion detection systems. *IEEE Design and Test*, 36:48–55, 12 2019.

[3] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti. Vanet security challenges and solutions: A survey. *Vehicular Communications*, 7:7–20, 1 2017.

[4] World Health Organization. Global status report on road safety, 2018.

[5] Jin Cui, Lin Shen Liew, Giedre Sabaliauskaite, and Fengjun Zhou. A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. *Ad Hoc Networks*, 90, 7 2019.

[6] Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo. Cyber-physical systems security - a survey. *IEEE Internet of Things Journal*, 4:1802–1831, 12 2017.

[7] Yulong Cao, Yimeng Zhou, Qi Alfred Chen, Chaowei Xiao, Won Park, Kevin Fu, Benjamin Cyr, Sara Rampazzi, and Z. Morley Mao. Adversarial sensor attack on lidar-based perception in autonomous driving. *Proceedings of the ACM Conference on Computer and Communications Security*, pages 2267–2281, 11 2019.

[8] Holger Banzhaf, Dennis Nienhuser, Steffen Knoop, and J. Marius Zollner. The future of parking: A survey on automated valet parking with an outlook on high density parking. *IEEE Intelligent Vehicles Symposium, Proceedings*, pages 1827–1834, 7 2017.

[9] Eman Mousavinejad, Fuwen Yang, Qing Long Han, Xiaohua Ge, and Ljubo Vlacic. Distributed cyber attacks detection and recovery mechanism for vehicle platooning. *IEEE Transactions on Intelligent Transportation Systems*, 21:3821–3834, 9 2020.

[10] Duo Lu, Zhichao Li, and Dijiang Huang. Platooning as a service of autonomous vehicles. *18th IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks, WoWMoM 2017 - Conference*, 7 2017.

[11] Fred Browand, John McArthur, and Charles Radovich. Fuel saving achieved in the field test of two tandem trucks. 6 2004.

[12] 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, 9 2017.

[13] S. Sivanandham and M. S. Gajanand. Platooning for sustainable freight transportation: an adoptable practice in the near future? *https://doi.org/10.1080/01441647.2020.1747568*, 40:581–606, 9 2020.

[14] Cong Wang and Henk Nijmeijer. String stable heterogeneous vehicle platoon using cooperative adaptive cruise control. *IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC*, 2015-October:1977–1982, 10 2015.

[15] Joel Vander Werf, Steven E Shladover, Mark A Miller, and Natalia Kourjanskaia. Effects of adaptive cruise control systems on highway traffic flow capacity. *Transportation Research Record*, 1800(1):78–84, 2002.

[16] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Snachám, and Stefan Savage. Experimental security analysis of a modern automobile. *Proceedings - IEEE Symposium on Security and Privacy*, pages 447–462, 2010.

[17] Shanzhi Chen, Jinling Hu, Yan Shi, Li Zhao, and Wen Li. A vision of c-v2x: Technologies, field testing, and challenges with chinese development. *IEEE Internet of Things Journal*, 7:3872–3881, 5 2020.

[18] Pengfei Zhu, Konglin Zhu, and Lin Zhang. Security analysis of lte-v2x and a platooning case study. *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2020*, pages 532–537, 7 2020.

[19] Monika Jain and Rahul Saxena. Overview of vanet: Requirements and its routing protocols. *Proceedings of the 2017 IEEE International Conference on Communication and Signal Processing, ICCSP 2017*, 2018-January:1957–1961, 2 2018.

[20] Andreas Festag, Panagiotis Papadimitratos, and Tessa Tielert. Design and performance of secure geocast for vehicular communication. *IEEE Transactions on Vehicular Technology*, 59:2456–2471, 6 2010.

[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*, 53:126–132, 6 2015.

[22] Yao Deng, Tiehua Zhang, Guannan Lou, Xi Zheng, Jiong Jin, and Qing Long Han. Deep learning-based autonomous driving systems: A survey of attacks and defenses. *IEEE Transactions on Industrial Informatics*, 2021.

[23] Junjie Shen, Ningfei Wang, Ziwen Wan, Yunpeng Luo, Takami Sato, Zhisheng Hu, Xinyang Zhang, Shengjian Guo, Zhenyu Zhong, Kang Li, Ziming Zhao, Chunming Qiao, and Qi Alfred Chen. SoK: On the Semantic AI Security in Autonomous Driving. *arXiv preprint arXiv:2203.05314*, 2022.

[24] Yulong Cao, Ningfei Wang, Chaowei Xiao, Dawei Yang, Jin Fang, Ruigang Yang, Qi Alfred Chen, Mingyan Liu, and Bo Li. Invisible for both camera and lidar: Security of multi-sensor fusion based perception in autonomous driving under physical-world attacks. *Proceedings - IEEE Symposium on Security and Privacy*, 2021-May:176–194, 5 2021.

[25] Ali Shuja Siddiqui, Chia Che Lee, Wenjie Che, Jim Plusquellic, and Fareena Saqib. Secure intra-vehicular communication over canfd. *Proceedings of the 2017 Asian Hardware Oriented Security and Trust Symposium, AsianHOST 2017*, 2018-May:97–102, 5 2018.

[26] Barbara Kitchenham, Rialette Pretorius, David Budgen, O. Pearl Brereton, Mark Turner, Mahmood Niazi, and Stephen Linkman. Systematic literature reviews in software engineering – a tertiary study. *Information and Software Technology*, 52:792–805, 8 2010.

[27] Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). Documento técnico do qualis periódicos. Technical report, 1 2023.

[28] Programa de Pós-graduação em Ciência da Computação da PUCRS. Qualis ciência da computação.

[29] Daniela S. Cruzes and Tore Dybå. Recommended steps for thematic synthesis in software engineering. *International Symposium on Empirical Software Engineering and Measurement*, pages 275–284, 2011.

[30] Sean Joe Taylor, Farhan Ahmad, Hoang Nga Nguyen, Siraj Ahmed Shaikh, David Evans, and David Price. Vehicular platoon communication: Cybersecurity threats and open challenges. *Proceedings - 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, DSN-W 2021*, pages 19–26, 6 2021.

[31] Leopoldo Angrisani, Nikos Fotiou, Ismail Butun, Sean Joe Taylor, Farhan Ahmad, Hoang Nga Nguyen, and Siraj Ahmed Shaikh. Vehicular platoon communication: Architecture, security threats and open challenges. *Sensors 2023, Vol. 23, Page 134*, 23:134, 12 2022.

[32] Qian Luo, Yurui Cao, Jiajia Liu, and Abderrahim Benslimane. Localization and navigation in autonomous driving: Threats and countermeasures. *IEEE Wireless Communications*, 26:38–45, 8 2019.

[33] Mohsen Riahi Manesh, Jonathan Kenney, Wen Chen Hu, Vijaya Kumar Devabhaktuni, and Naima Kaabouch. Detection of gps spoofing attacks on unmanned aerial systems. *2019 16th IEEE Annual Consumer Communications and Networking Conference, CCNC 2019*, 2 2019.

[34] Junjie Shen, Yeon Won, Zeyuan Chen, Qi Alfred Chen, and Jun Yeon Won. *Drift with Devil: Security of Multi-Sensor Fusion based Localization in High-Level Autonomous Driving under GPS Spoofing*, pages 931–948. 2020.

[35] Shunyuan Xiao, Xiaohua Ge, Qing Long Han, and Yijun Zhang. Secure distributed adaptive platooning control of automated vehicles over vehicular ad-hoc networks under denial-of-service attacks. *IEEE Transactions on Cybernetics*, 52:12003–12015, 11 2022.

[36] Mohammad Hossein Basiri, Nasser L. Azad, and Sebastian Fischmeister. Attack resilient heterogeneous vehicle platooning using secure distributed nonlinear model predictive control. *2020 28th Mediterranean Conference on Control and Automation, MED 2020*, pages 307–312, 9 2020.

[37] 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*, 23:AR, 4 2022.

[38] Mohammad Khodaei, Hongyu Jin, and Panagiotis Papadimitratos. Secmace: Scalable and robust identity and credential management infrastructure in vehicular communication systems. *IEEE Transactions on Intelligent Transportation Systems*, 19:1430–1444, 5 2018.

[39] Michael Feiri, Jonathan Petit, and Frank Kargl. Efficient and secure storage of private keys for pseudonymous vehicular communication. *Proceedings of the ACM Conference on Computer and Communications Security*, pages 9–18, 2013.

[40] Mohammed E. Eltayeb, Junil Choi, Tareq Y. Al-Naffouri, and Robert W. Heath. On the security of millimeter wave vehicular communication systems using random antenna subsets. *IEEE Vehicular Technology Conference*, 0, 7 2016.

[41] Mohammed E. Eltayeb, Junil Choi, Tareq Y. Al-Naffouri, and Robert W. Heath. Enhancing secrecy with multiantenna transmission in millimeter wave vehicular communication systems. *IEEE Transactions on Vehicular Technology*, 66:8139–8151, 9 2017.

[42] Ali Balador, Alessandro Bazzi, Unai Hernandez-Jayo, Idoia de la Iglesia, and Hossein Ahmadvand. A survey on vehicular communication for cooperative truck platooning application. *Vehicular Communications*, 35:100460, 6 2022.

[43] Panagiotis Papadimitratos, Levente Buttyan, Tamás Holczer, Elmer Schoch, Julien Freudiger, Maxim Raya, Zhendong Ma, Frank Kargl, Antonio Kung, and Jean Pierre Hubaux. Secure vehicular communication systems: Design and architecture. *IEEE Communications Magazine*, 46:100–109, 2008.

[44] 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, 6 2018.

[45] Hengyi Liang, Matthew Jagielski, Bowen Zheng, Chung Wei Lin, Eunsuk Kang, Shinichi Shiraishi, Cristina Nita-Rotaru, and Qi Zhu. Network and system level security in connected vehicle applications. *IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers, ICCAD*, 11 2018.

[46] Muhammad Atif Javed, Faiz Ul Muram, Sasikumar Punnekkat, and Hans Hansson. Safe and secure platooning of automated guided vehicles in industry 4.0. *Journal of Systems Architecture*, 121:102309, 12 2021.

[47] P. S.V. SathyaNarayanan. A sensor enabled secure vehicular communication for emergency message dissemination using cloud services. *Digital Signal Processing*, 85:10–16, 2 2019.

[48] Zoleikha Abdollahi Biron, Satadru Dey, and Pierluigi Pisu. Real-time detection and estimation of denial of service attack in connected vehicle systems. *IEEE Transactions on Intelligent Transportation Systems*, 19:3893–3902, 12 2018.

[49] Mohammad Khodaei and Panos Papadimitratos. The key to intelligent transportation: Identity and credential management in vehicular communication systems. *IEEE Vehicular Technology Magazine*, 10:63–69, 12 2015.

[50] Kyusuk Han, Swapna Divya Potluri, and Kang G. Shin. On authentication in a connected vehicle: Secure integration of mobile devices with vehicular networks. *Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems, ICCPS 2013*, pages 160–169, 2013.

[51] Xuewen Luo, Yiliang Liu, Hsiao Hwa Chen, and Qing Guo. Physical layer security in intelligently connected vehicle networks. *IEEE Network*, 34:232–239, 9 2020.

[52] Yiliang Liu, Wei Wang, Hsiao Hwa Chen, Feng Lyu, Liangmin Wang, Weixiao Meng, and Xuemin Shen. Physical layer security assisted computation offloading in intelligently connected vehicle networks. *IEEE Transactions on Wireless Communications*, 20:3555–3570, 6 2021.

[53] M. Mongelli. Design of countermeasure to packet falsification in vehicle platooning by explainable artificial intelligence. *Computer Communications*, 179:166–174, 11 2021.

[54] Soodeh Dadras, Ryan M. Gerdes, and Rajnikant Sharma. Vehicular platooning in an adversarial environment. *ASIACCS 2015 - Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, pages 167–178, 4 2015.

[55] Jianbing Ni, Xiaodong Lin, and Xuemin Shen. Toward privacy-preserving valet parking in autonomous driving era. *IEEE Transactions on Vehicular Technology*, 68:2893–2905, 3 2019.

[56] Yijie Xun, Jiajia Liu, and Yanning Zhang. Side-channel analysis for intelligent and connected vehicle security: A new perspective. *IEEE Network*, 34:150–157, 3 2020.

[57] Joshua E. Siegel, Dylan C. Erb, and Sanjay E. Sarma. A survey of the connected vehicle landscape - architectures, enabling technologies, applications, and development areas. *IEEE Transactions on Intelligent Transportation Systems*, 19:2391–2406, 8 2018.

[58] Alexios Lekidis and Faouzi Bouali. C-v2x network slicing framework for 5g-enabled vehicle platooning applications. *IEEE Vehicular Technology Conference*, 2021-April, 4 2021.

[59] Ibrar Yaqoob, Latif U. Khan, S. M.Ahsan Kazmi, Muhammad Imran, Nadra Guizani, and Choong Seon Hong. Autonomous driving cars in smart cities: Recent advances, requirements, and challenges. *IEEE Network*, 34:174–181, 1 2020.