


Please cite the Published Version

Ibrahim, Mohamad and Sohrabi Safa, Nader  (2023) Detecting message spoofing attacks on smart vehicles. *Computer Fraud & Security*, 2023 (12). ISSN 1361-3723

DOI: [https://doi.org/10.12968/s1361-3723\(23\)70054-7](https://doi.org/10.12968/s1361-3723(23)70054-7)

Publisher: Mark Allen Group

Version: Accepted Version

Downloaded from: <https://e-space.mmu.ac.uk/633784/>

Usage rights:  In Copyright

Additional Information: This is an author accepted manuscript of an article originally published in *Computer Fraud & Security*.

Enquiries:

If you have questions about this document, contact openresearch@mmu.ac.uk. Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from <https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines>)

Analyzing Machine Learning Models for Detecting Message Spoofing Attacks on Smart Vehicles

Abstract

In today's modern world, the rapid proliferation of smart vehicles, particularly connected vehicles, has given rise to an increase in cyber threats. Therefore, ensuring the security of associated equipment has become a pressing concern. Numerous studies have investigated various attack, anomaly, and intrusion detection techniques for smart automobiles. This paper presents an analysis of various machine learning models for detecting message spoofing attacks on smart vehicles. These types of attacks can pose a significant risk to the safety and security of smart vehicles such as accidents, hijacking incidents, and other severe consequences. The study utilizes datasets of message spoofing attacks to assess the efficacy of different machine learning models in detecting these types of attacks. The findings indicate the potential of machine learning models in detecting message spoofing attacks, with the "Reinforcement Learning" model achieving the highest accuracy, precision, and F1-score (FS). The results underscore the need for robust security measures to prevent message spoofing attacks on smart vehicles.

Table of Contents

Chapter 1: Introduction	1
Chapter 2: Literature Review	2
I. ADAS.....	2
II. Telematic System	3
III. CAN bus.....	4
IV. Message spoofing attacks.....	4
V. Message spoofing detection	7
VI. Limitations of existing studies.....	8
Chapter 3: Methodology.....	8
I. Study 1.....	9
II. Study 2.....	10
III. Result of the 2 Studies.....	11
Chapter 4: Conclusion	13
Appendix.....	14
References list.....	17

Table of Figures

Figure 1: ADAS features	2
Figure 2: ADAS systems	3
Figure 3: Telematic System	3
Figure 4: CAN bus	4
Figure 5: CAN bus Attack.	5
Figure 6: Message GPS spoofing attack	7
Figure 7: Spoofing attack IDS detection methods	7
Figure 8: RL message spoofing attack result	10
Figure 9: Result of the comparison between machine learning models.....	11
Figure 10: Machine learning results.....	12

List of Tables

Table 1: Attacks Categories on smart vehicles	4
Table 2: Message spoofing technique and components	6
Table 3: ML evaluation parameters	9
Table 4: RL message spoofing attack datasets.....	9
Table 5: RL message spoofing attack result	9
Table 6: Performance of Machine learning models against message spoofing attack.....	10
Table 7: Combining all models of the 2 studies in one table.....	12

Introduction

The automotive industry has been focused on enhancing safety, comfort, and convenience by integrating advanced computer systems, software, hardware, and communication networks into vehicles. One significant development is the Advanced Driver Assistance System (ADAS), which includes some components related to the Controller Area Network (CAN) bus and telematics system. However, as ADAS systems become more prevalent, concerns about their security against cyber-attacks have also grown. One of the most significant threats is message spoofing attacks through the CAN bus and Global Positioning System (GPS), where attackers send a fake message to the ADAS system, leading to false information, dangerous driving scenarios, and accidents.

To mitigate this issue, reinforcement learning (RL) based control has emerged as a promising solution to prevent message spoofing attacks. RL is a type of machine learning where an agent learns to make decisions based on trial and error, to maximize a cumulative reward. By using RL, the ADAS system can learn to detect and prevent GPS and CAN spoofing attacks by adapting its behaviour and adjusting its parameters.

This paper aims to propose a solution to prevent a message spoofing attack on ADAS systems. The paper will first outline the problem statement, define the key terms and concepts, explain the benefits of using RL for preventing GPS and CAN bus spoofing attacks and finally analyse the reason for choosing RL as a solution. Preventing message injection attacks through GPS and CAN bus spoofing in ADAS systems is a critical area of research that ensures the safety and security of drivers and passengers. This research can help in identifying and mitigating potential security vulnerabilities associated with such attacks and designing more secure and robust ADAS systems.

In conclusion, this paper provides a comprehensive analysis of a message spoofing attack on GPS and CAN bus. It aims to provide insights into the risks associated with these attacks and explore potential countermeasures, which is RL-based control, to ensure the safety and security of ADAS systems and their users.

Literature Review

I. ADAS

According to Sayar et al. (2022), ADAS are designed to enhance the safety, convenience, and security of driving a vehicle. This enhancement occurs due to the ADAS components which are becoming increasingly common in modern vehicles and are expected to play a crucial role in the future of transportation. For example, the employing of the sensors, cameras, radar, Lidar and other components of the ADAS system will lead to providing real-time information to drivers and assist them in controlling their vehicles more efficiently. As illustrated in Figure 1, this system offers numerous features.

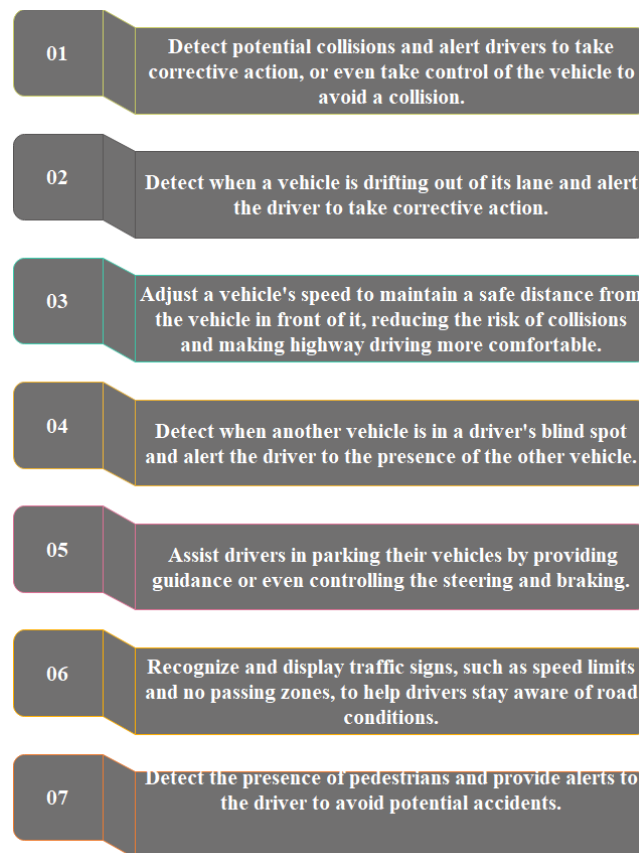


Figure 1: ADAS features

In their 2019 paper, Kurbanov et al. identified the Advanced Driver Assistance Systems (ADAS) that offer the functionalities listed in Figure 1. The ADAS system is subdivided into multiple subsystems, as depicted in Figure 2, each assigned specific responsibilities. ADAS use some components of the infotainment and telematic system to enhance the functionality of the system, such as GPS, sensors, cameras, and others.

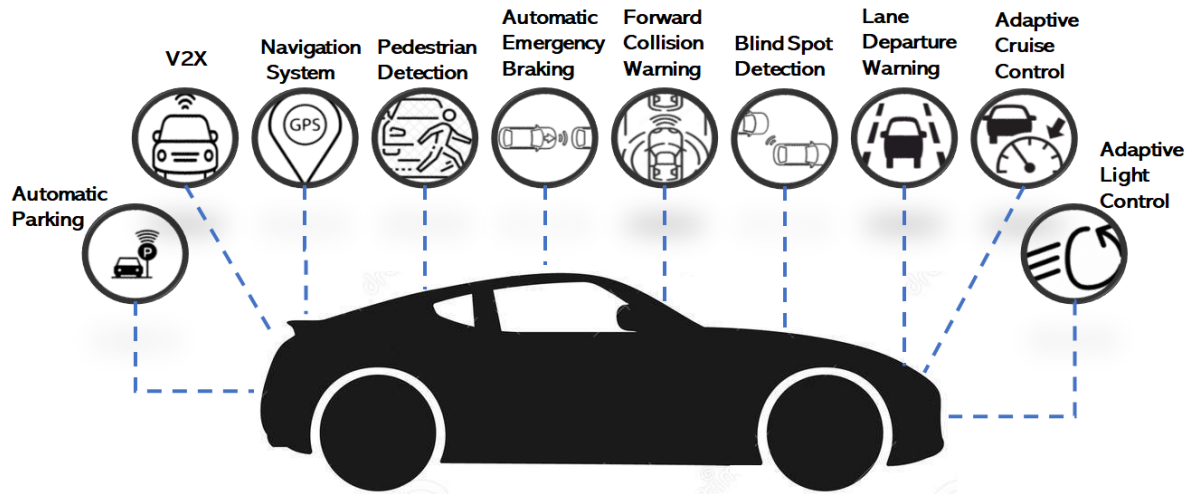


Figure 2: ADAS systems

II. Telematic System

A telematics system is a vehicle monitoring approach that integrates a Global Positioning System (GPS) with onboard diagnostic technology to record and map the precise location and velocity of a car and correlate this with its internal performance. As shown in Figure 3, the system includes a device for tracking vehicles that can receive, transmit, and store telemetry data, and it connects to a wireless network through a SIM card and an onboard modem, using the vehicle's onboard diagnostics (OBDII) or CAN bus port. Telematics systems gather a wide range of information, such as speed, idling, tire pressure, fuel consumption, and hazardous driving behaviours, which are collected from the vehicle and sent to GPS tracking software for examination. This data can be analyzed and utilized to improve fleet efficiency (Young et al., 2020).

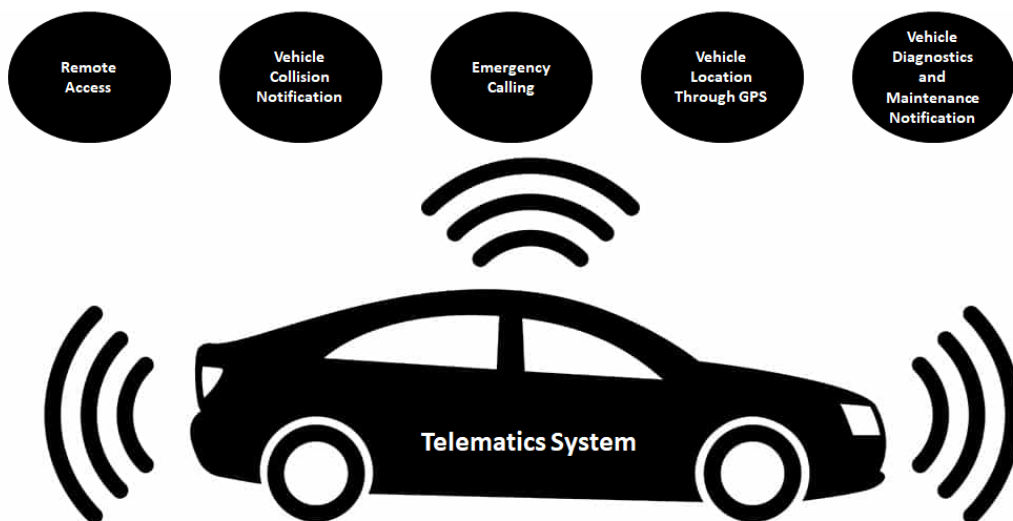


Figure 3: Telematic System

III. CAN bus

According to Md. Delwar Hossain et al. (2020), one of the most significant innovations in the automotive sector is the Controller Area Network (CAN) bus protocol. CAN bus is a type of vehicle bus standard for connecting electronic control units (ECUs) within a vehicle. The CAN bus is a serial bus, that uses only two wires to transmit data, which makes it a very efficient way to connect a large number of devices including ADAS systems.

As shown in Figure 4, the CAN bus in smart cars coordinates the functions of various systems and devices, such as the engine control unit (ECU), the anti-lock braking system (ABS), the electronic stability control (ESC), and the infotainment system, enabling data transmission between them. In conclusion, the CAN bus facilitates data sharing and communication among different devices.

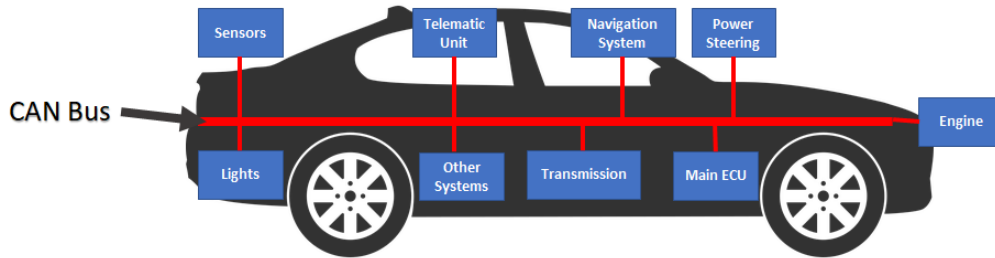


Figure 4: CAN bus

IV. Message spoofing attacks

According to Vitale et al. (2021), there are several categories of attacks on smart vehicles which are indicated in Table 1.

Table 1: Attacks Categories on smart vehicles

Category	Attack Types
Authenticity/identification attacks	Sybil attack
	Location Service Jamming and Spoofing
Availability attacks	Denial of Service (DoS) attack
	Timing attack
	Flooding and Jamming attack
Confidentiality/privacy attacks	Eavesdropping attack
	Traffic analysis attack
Data integrity	Replay attack
	Data alteration/Data injection attack

Table 1 indicates that message spoofing attacks fall under the category of Authenticity or Identification attacks and Data Integrity, with potentially critical impacts on the system.

Shah Alam Khan, Mohsin and Iqbal (2021) mentioned in their research the two communications protocols in smart vehicles for exchanging information among different components, namely the CAN bus and GPS which makes them vulnerable to message spoofing attacks. Therefore, there are 2 types of message spoofing attacks, CAN bus spoofing and GPS spoofing. CAN bus spoofing involves sending fake messages on the CAN bus to gain unauthorized access to the vehicle's components or to take control of the vehicle by injecting spoofing messages (Baldini, 2022).

Earlier studies show that the Jeep Cherokee was the target of the most attacks on automobiles, with the WiFi and CAN bus security of the vehicles being compromised. This attack disables the brakes, stops the engine, and controls the steering by delivering false messages to on-board subsystems over the CAN bus (Samira Tahajomi Banafshehvaragh and Amir Masoud Rahmani, 2022).

The attack reported by Yang, Duan and Tehranipour (2020) is characterized by an increased rate of CAN bus frames to disguise the attack message as legitimate. An IDS was developed to detect attacks based on the periods between messages. However, newer attacks like the bus-off attack could still bypass this IDS.

Despite the weaknesses of cryptographic authentication on the CAN bus, it remains a viable solution. The limited data rate of the bus makes it difficult to use strong encryption or one-way functions that can resist attacks with high computing power. Additionally, the CAN bus serves as a diagnostic tool for mechanics, which means that authentication keys for accessing it need to be shared with many users, making it difficult to keep them secure (Yang, Duan and Tehranipour, 2020).

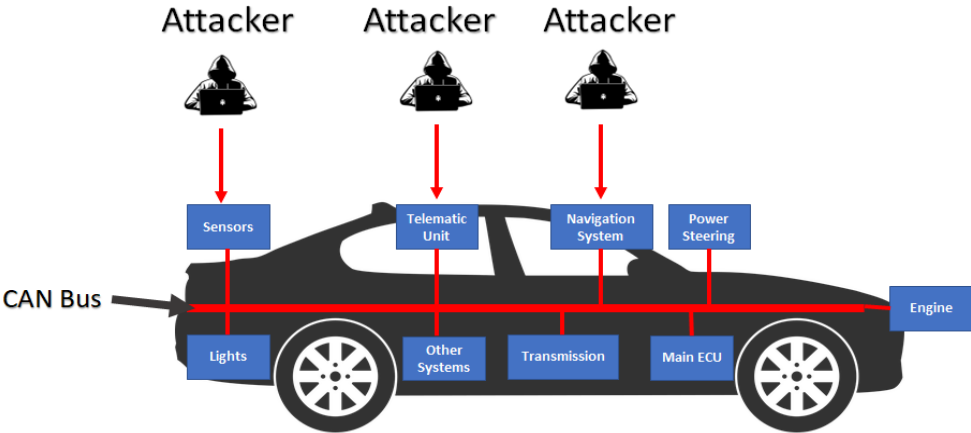


Figure 5: CAN bus Attack.

There are various techniques and common devices that can be employed for message spoofing attacks, as presented in Table 2.

Table 2: Message spoofing technique and components

Techniques	Description
Signal injection	The attacker sends false GPS signals to the target vehicle. These false signals can be generated using a variety of methods, including using a portable GPS spoofing device or broadcasting false GPS signals from a nearby location.
Signal jamming	The attacker uses a device to jam the target vehicle's GPS signal. This can be done using a variety of methods, including using a high-powered radio transmitter or using a physical object to block the GPS signal.
Signal modification	An attacker modifies the target vehicle's GPS signal. This can be done by using a device to add or subtract information from the signal.
Components	
Portable GPS spoofing devices	These devices are small, handheld devices that can be used to send false GPS signals to a target vehicle. They are relatively inexpensive and easy to use, making them a popular choice for attackers.
GPS spoofing software	Many software programs can be used to generate false GPS signals. These programs are typically more expensive than portable GPS spoofing devices, but they offer a wider range of features.
GPS spoofing hardware	Several hardware devices can be used to generate false GPS signals. These devices are typically more expensive than software programs, but they offer the highest level of performance.

Message spoofing attacks can be executed through the injection, jamming, or modification of a signal, utilizing one of the components, GPS satellite, or antenna, as detailed in Table 2. Such attacks can confuse smart cars between their true position and the false position presented by the attacker, potentially leading to accidents and posing a serious threat to both drivers and pedestrians as shown in Figure 6.

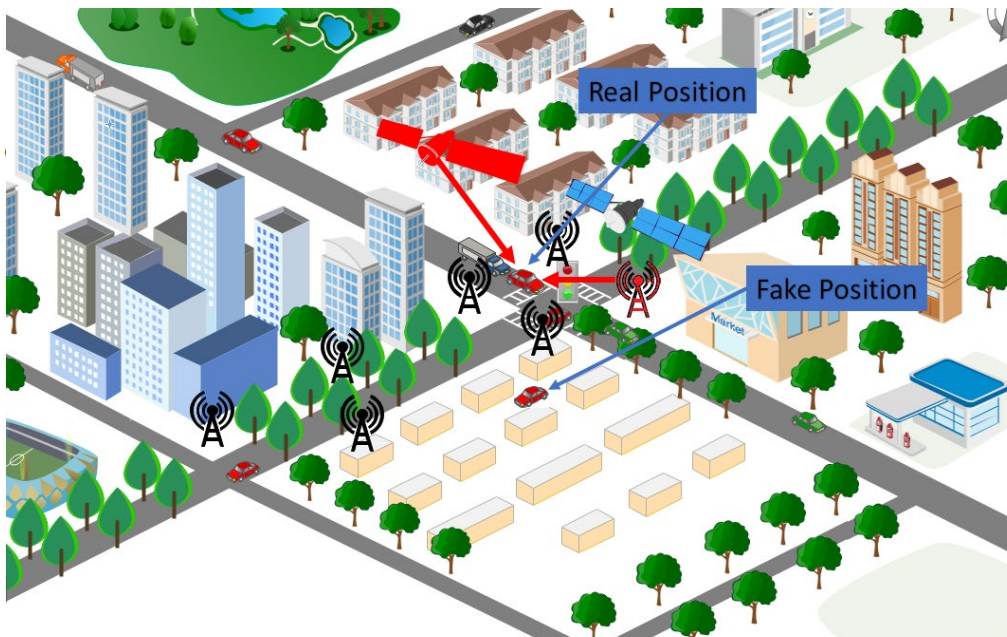


Figure 6: Message GPS spoofing attack

V. Message spoofing detection

The study by Tahajomi et al. (2022) explores various machine learning-based intrusion detection systems (IDSs) to detect message spoof attacks. The IDSs use supervised and unsupervised learning, ensemble learning, optimization algorithms, neural networks and deep learning, and hybrid algorithms. Supervised algorithms categorise data based on specific outputs for certain inputs, while unsupervised algorithms classify data patterns without generating outputs. Combining various algorithms is how ensemble learning techniques improve detection performance, and optimisation algorithms are used to boost other machine learning techniques. Neural networks and deep learning algorithms, and other algorithms as shown in Figure 7 are also used. Hybrid algorithms incorporate various machine learning methods to improve detection performance.

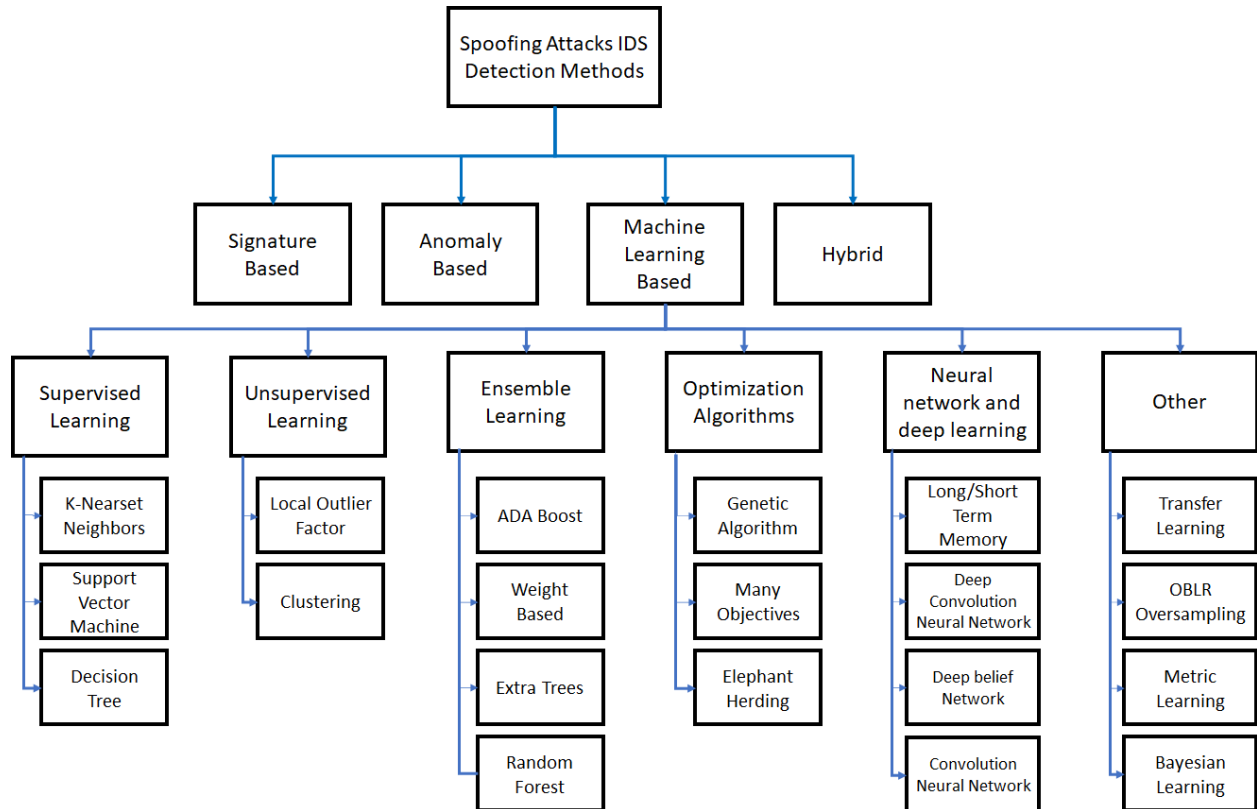


Figure 7: Spoofing attack IDS detection methods

SVM and bagged decision trees (BDT) are mostly used to protect CAN bus due to the ability to implement them in real vehicles and detect masquerade, and bus-off attacks with low error rates and covering all types of CAN data frames.

While k-nearest neighbour and random forest assist in the detection of GPS spoofing attacks, which can increase the detection accuracy by using relative speed for position verification.

Jiang, Wu, and Xin (2021) conducted a study that compared the performance of various machine learning classifiers for GPS spoofing detection and classification, such as Random Forest, K-Nearest Neighbors, Support Vector Machines, Logistic Regression, Decision Trees, and Gaussian Naive Bayes. The results showed that each classifier had its strengths and weaknesses, and the most accurate algorithm depends on the dataset and application. They concluded that the decision tree was the best for location-dependent datasets, while logistic regression was the best for location-independent datasets.

In another study, Dasgupta, Ghosh, and Rahman (2022) created an RL-based turn-by-turn spoofing attack detection model that utilized low-cost in-vehicle sensor data. They developed and evaluated the model using ten attack and non-attack datasets from the Honda Dataset. The results showed that the model had high accuracy and recall, but its precision and F1 score varied. Overall, the model was successful in identifying turn-by-turn attacks, but there were a few cases of false detection. The researchers plan to investigate the model's effectiveness in detecting other types of sophisticated spoofing attacks in future studies.

VI. Limitations of existing studies

The literature on the implementation of machine learning in detecting GPS and CAN spoofing attacks in smart vehicles is limited. Previous research studies have primarily focused on GPS spoofing attacks in the aviation industry, and there is a dearth of research that specifically addresses GPS and CAN spoofing attacks in smart vehicles. The studies that have focused on detecting GPS and CAN spoofing attacks using machine learning face certain limitations in terms of the datasets available. As a result, the evaluation of the efficacy of machine learning in detecting spoofing attacks may not be entirely accurate and requires further clarification in future studies.

Moreover, some studies have evaluated a limited number of machine learning techniques and concluded that one technique is superior in detecting GPS and CAN spoofing attacks. However, these studies fail to consider the fact that various additional machine-learning methods may be more efficient. Therefore, determining the best strategy for identifying GPS and CAN spoofing attacks in smart vehicles requires comparing and contrasting a variety of machine-learning techniques.

Chapter 3: Methodology

This section outlines the methodology employed to collect a dataset from various studies that utilized Intrusion Detection Systems (IDS) in conjunction with machine learning to detect and prevent message spoofing attacks. The accuracy, precision, recall, and F1-score (FS) were some of the criteria used to assess the classifiers' performance.

Table 3: ML evaluation parameters

Parameters	Description
Accuracy	The metric of accuracy refers to the percentage of correctly predicted samples in a given dataset.
Precision	It is a metric that evaluates the ability of a classifier to classify samples correctly. It is calculated by dividing the number of samples that were accurately predicted by the total number of positive samples anticipated.
Recall	A measure of the classifier's ability to correctly predict all samples. It is determined by dividing the total number of positive samples by the proportion of positively predicted positive samples.
F1-score (FS)	The harmonic mean of the precision and recall. It is a measure of the classifier's overall performance.

I. Study 1

Dasgupta, Ghosh, and Rahman (2022) evaluated the performance of a RL model for message spoofing attack detection using the Honda Dataset. The results of their study are shown in Table 4.

Table 4: RL message spoofing attack datasets

Attack Scenario	Recall	Precision (%)	Accuracy (%)	f1-score
1	100	98.57	99.99	99.28
2	100	98.29	99.99	99.14
3	100	100	100	100
4	100	98.57	99.99	99.28
5	100	93.44	99.99	96.61
6	100	100	100	100
7	100	97.72	99.99	98.85
8	100	97.43	99.99	98.70
9	100	94.44	99.99	97.14

Table 5: RL message spoofing attack result

Attack Scenario	Precision (%)	Accuracy (%)	f1-score
count	9.0	9.000000	9.000000
mean	100.0	99.99	99.14
std	0.0	2.269692	0.004410
min	93.440000	99.990000	96.610000
25%	97.430000	99.990000	98.700000
50%	98.290000	99.990000	99.140000
75%	98.570000	99.990000	99.280000
max	100.000000	100.000000	100.000000

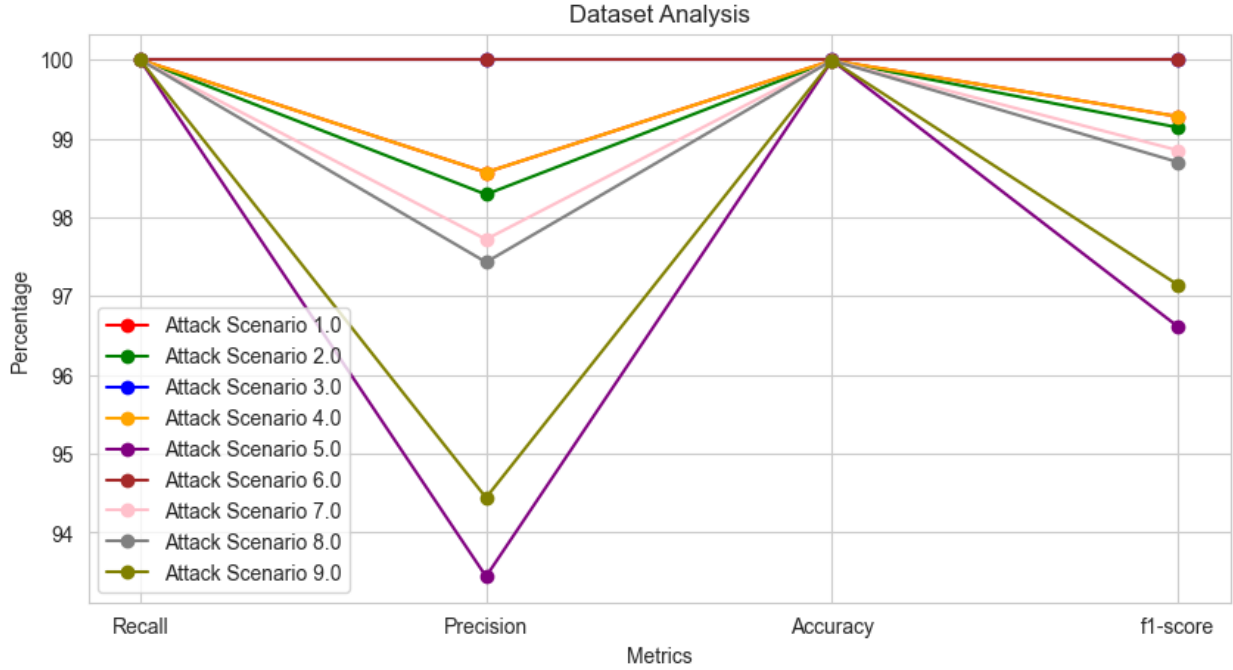


Figure 8: RL message spoofing attack result

Based on Figure 8 and Table 5 it could be concluded the following

- The precision and recall values are very high, indicating that the RL model was very effective at detecting message spoofing attacks.
- The accuracy values are also very high, indicating that the RL model was very effective at classifying the attack and non-attack datasets.
- The F1-scores are intermediate between the precision and recall values, indicating that the RL model was effective at both detecting and classifying the attack and non-attack datasets.

Overall, the results of the study suggest that the RL model is a promising approach for message spoofing attack detection as shown in Figure 8.

II. Study 2

In another study, Nayfeh et al. (2023) evaluated the performance of several machine learning models for message spoofing attack detection based on accuracy, precision, and F1 score.

The results of their study are shown in the following table 6:

Table 6: Performance of Machine learning models against message spoofing attack

Model	Accuracy (%)	Precision (%)	f1-score
Random Forest (RF)	90.89	90.04	0.90

Nearest Neighbors (KNN)	87.99	90.53	0.86
Multilayer Perceptron (MLP)	89.64	90.24	0.89
Logistic Regression (LR)	90.53	91.13	0.90
Decision Tree (DT)	92.36	93.95	0.92
Support Vector Machines (SVM)	89.84	90.66	0.89
Naive Bayes (NB)	91.17	91.10	0.91

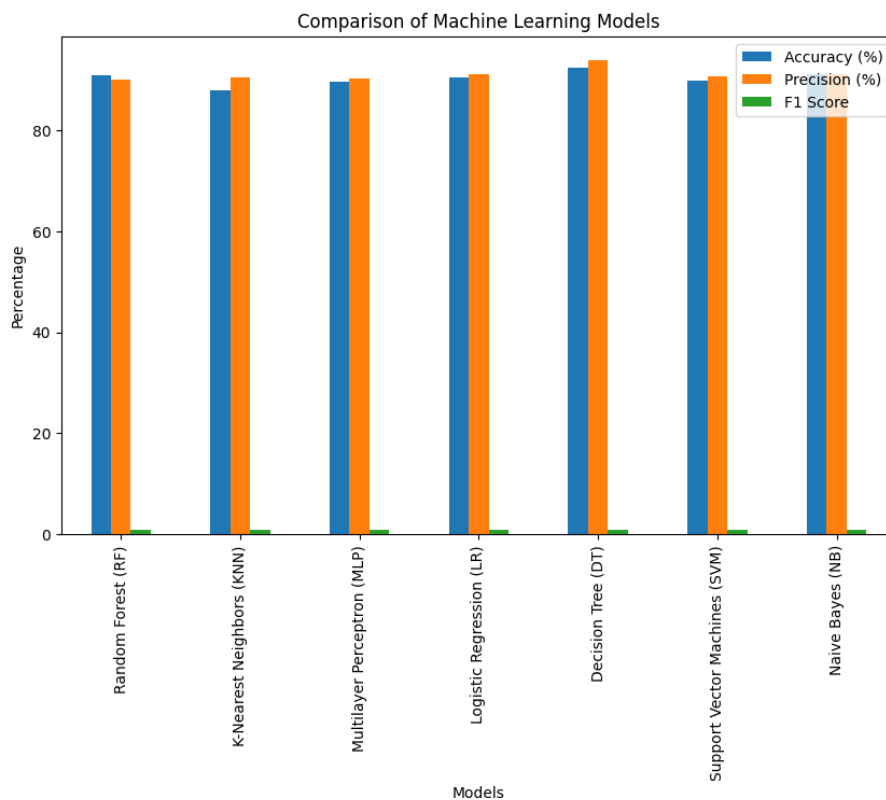


Figure 9: Result of the comparison between machine learning models

Table 6 and Figure 9 indicate that the performance of each model varies across the different parameters. The "Decision Tree" model achieved the highest accuracy (92.36%), while the "Naive Bayes" model achieved the highest precision (91.10%). The RL model achieved the highest accuracy (99.99%), precision (100%), and F1 score (0.99).

III. Result of the 2 Studies

By aggregating all models and performing comparative analysis, the results presented in Table 7 indicate that the average accuracy, precision, and F1 score across all models are 91.54%, 92.21%, and 0.91, respectively.

Table 7: Combining all models of the 2 studies in one table.

Models	Accuracy (%)	Precision (%)	f1-score
Random Forest (RF)	90.89	90.04	0.90
Nearest Neighbors (KNN)	87.99	90.53	0.86
Multilayer Perceptron (MLP)	89.64	90.24	0.89
Logistic Regression (LR)	90.53	91.13	0.90
Decision Tree (DT)	92.36	93.95	0.92
Support Vector Machines (SVM)	89.84	90.66	0.89
Naive Bayes (NB)	91.17	91.10	0.91
Reinforcement Learning (RL)	99.99	100.0	99.14

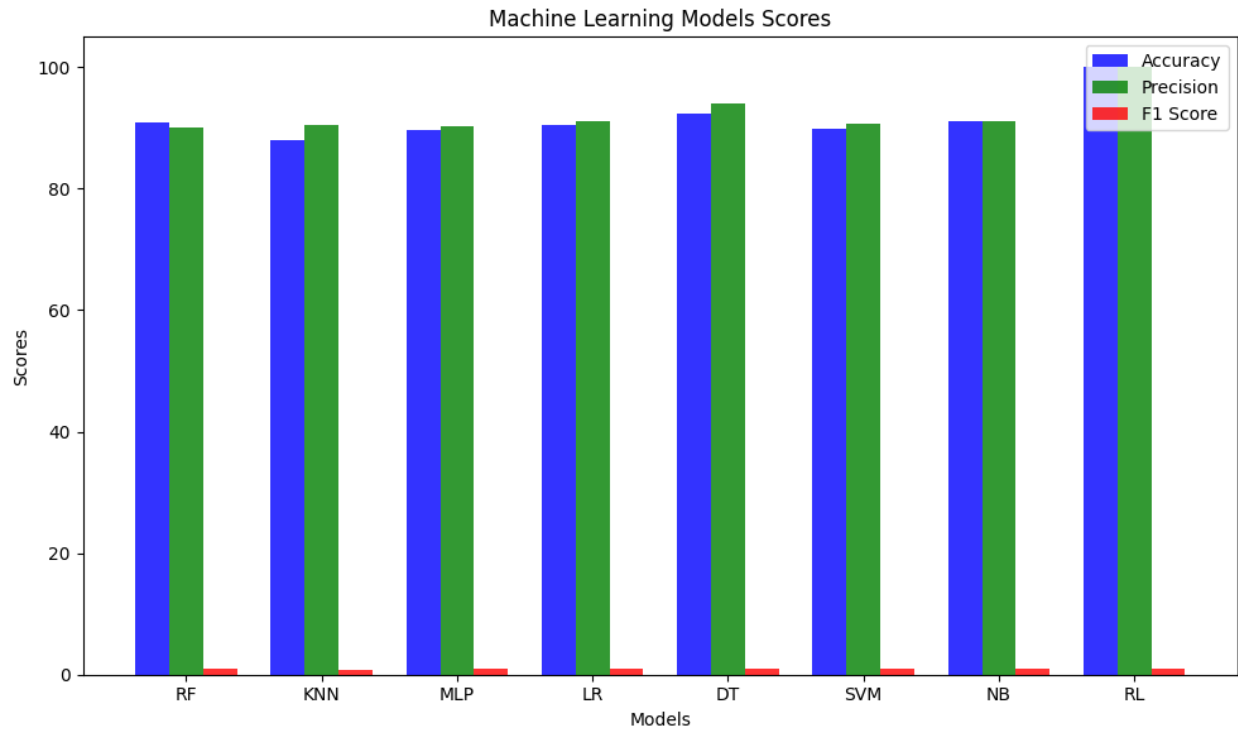


Figure 10: Machine learning results

- Mean Accuracy: 91.54%
- Mean Precision: 92.21%
- Mean F1 Score: 0.91
- Max Accuracy: 99.90%
- Max Precision: 100.00%
- Max F1 Score: 0.99
- Model with the highest accuracy: RL

Based on the results presented in Table 7 and Figure 10, the RL model achieved the highest accuracy, precision, and F1 score values of 99.99%, 100%, and 0.99, respectively. These results

suggest that the RL model has the potential to effectively identify message-spoofing attacks on smart vehicles. However, it is necessary to emphasise that the effectiveness of any model depends mainly on the number of datasets and tasks being addressed.

Chapter 4: Conclusion

In conclusion, message spoofing attacks targeting GPS and CAN bus cause significant threats to the security and safety of smart vehicles, with potentially catastrophic impacts ranging from accidents to hijacking events. Therefore, it is crucial to create an efficient technique for identifying and preventing message spoofing attacks on smart vehicles.

This paper has proposed a reinforcement learning-based control solution to prevent message spoofing attacks on ADAS systems. The analysis of various machine learning models for detecting message spoofing attacks on smart vehicles has shown that the RL model achieved the highest mean accuracy, precision, and F1 score, making it a promising technique for detecting these types of attacks.

Although further research is required to determine the effectiveness of these machine learning models against specific attacks, the combination of machine learning models with other physical and hardware countermeasures can enhance the prevention of message spoofing attacks through GPS or CAN bus.

Overall, utilising machine learning models to identify message spoofing attacks on smart vehicles is a promising strategy that can improve the security and safety of critical systems. Moreover, it is essential to continue developing and enhancing these models in order to address the changing nature of security threats which can be beneficial for the automotive industry.

Appendix

Python Code Table Find the Means and Max

```
import pandas as pd
# Create a dataframe to hold the dataset
data = {'Model': ['Random Forest (RF)', 'K-Nearest
Neighbors (KNN)', 'Multilayer Perceptron (MLP)',
'Logistic Regression (LR)', 'Decision Tree (DT)',
'Support Vector Machines (SVM)', 'Naive Bayes
(NB)'],
'Accuracy (%)': [90.89, 87.99, 89.64, 90.53,
92.36, 89.84, 91.17],
'Precision (%)': [90.04, 90.53, 90.24, 91.13,
93.95, 90.66, 91.1],
'F1 Score': [0.9, 0.86, 0.89, 0.9, 0.92, 0.89,
0.91]}
df = pd.DataFrame(data)
# Print the dataframe
print(df)
# Calculate the mean values for each metric
mean_accuracy = df['Accuracy (%)'].mean()
mean_precision = df['Precision (%)'].mean()
mean_f1_score = df['F1 Score'].mean()
# Print the mean values
print('Mean Accuracy:
{:.2f}%'.format(mean_accuracy))
print('Mean Precision:
{:.2f}%'.format(mean_precision))
print('Mean F1 Score: {:.2f}'.format(mean_f1_score))
# Calculate the maximum value for each metric
max_accuracy = df['Accuracy (%)'].max()
max_precision = df['Precision (%)'].max()
max_f1_score = df['F1 Score'].max()
# Print the maximum values
print('Max Accuracy:
{:.2f}%'.format(max_accuracy))
print('Max Precision:
{:.2f}%'.format(max_precision))
print('Max F1 Score: {:.2f}'.format(max_f1_score))
# Find the model with the highest accuracy
highest_accuracy_model = df.loc[df['Accuracy
(%)'].idxmax(), 'Model']
# Print the model with the highest accuracy
print('Model with the highest accuracy:
{}'.format(highest_accuracy_model))
```

Python Code for Figure 9

```
import pandas as pd
import matplotlib.pyplot as plt
# Create a dataframe to hold the dataset
data = {'Model': ['Random Forest (RF)', 'K-Nearest
Neighbors (KNN)', 'Multilayer Perceptron (MLP)',
'Logistic Regression (LR)', 'Decision Tree (DT)',
'Support Vector Machines (SVM)', 'Naive Bayes
(NB)'],
'Accuracy (%)': [90.89, 87.99, 89.64, 90.53,
92.36, 89.84, 91.17],
'Precision (%)': [90.04, 90.53, 90.24, 91.13,
93.95, 90.66, 91.1],
'F1 Score': [0.9, 0.86, 0.89, 0.9, 0.92, 0.89,
0.91]}
df = pd.DataFrame(data)
# Set the Model column as the index
df.set_index('Model', inplace=True)
# Plot a bar graph for each metric
fig, ax = plt.subplots(figsize=(10, 6))
df.plot(kind='bar', ax=ax)
ax.set_xlabel('Models')
ax.set_ylabel('Percentage')
ax.set_title('Comparison of Machine Learning
Models')
plt.show()
plt.plot(df)
plt.xlabel('Model')
```

Python Code for Figure 10

```
import matplotlib.pyplot as plt
import numpy as np
# Define the data
models = ['RF', 'KNN', 'MLP', 'LR', 'DT', 'SVM', 'NB', 'RL']
accuracy = [90.89, 87.99, 89.64, 90.53, 92.36, 89.84, 91.17, 99.99]
precision = [90.04, 90.53, 90.24, 91.13, 93.95, 90.66, 91.10, 100.0]
f1_score = [0.90, 0.86, 0.89, 0.90, 0.92, 0.89, 0.91, 0.99]
# Plot the bar chart
fig, ax = plt.subplots(figsize=(10,6))
index = np.arange(len(models))
bar_width = 0.25
opacity = 0.8
rects1 = ax.bar(index, accuracy, bar_width, alpha=opacity, color='b', label='Accuracy')
rects2 = ax.bar(index + bar_width, precision, bar_width, alpha=opacity, color='g', label='Precision')
rects3 = ax.bar(index + 2*bar_width, f1_score, bar_width, alpha=opacity, color='r', label='F1 Score')
# Add labels, titles and legends
ax.set_xlabel('Models')
ax.set_ylabel('Scores')
ax.set_title('Machine Learning Models Scores')
ax.set_xticks(index + bar_width)
ax.set_xticklabels(models)
ax.legend()
plt.tight_layout()
plt.show()
```

References list

- Aissou, G., Slimane, H.O., Benouadah, S. and Kaabouch, N. (2021). Tree-based Supervised Machine Learning Models For Detecting GPS Spoofing Attacks on UAS. *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. [online] doi:<https://doi.org/10.1109/uemcon53757.2021.9666744>.
- Baldini, G. (2022). Voltage Based Electronic Control Unit (ECU) Identification with Convolutional Neural Networks and Walsh–Hadamard Transform. *Electronics*, [online] 12(1), pp.199–199. doi:<https://doi.org/10.3390/electronics12010199>.
- Cheng, R., Orosz, G., Murray, R.M. and Burdick, J.W. (2019). *End-to-End Safe Reinforcement Learning through Barrier Functions for Safety-Critical Continuous Control Tasks*. [online] arXiv.org. Available at: <https://arxiv.org/abs/1903.08792> [Accessed 26 Apr. 2023].
- Dasgupta, S., Ghosh, T. and Md. Mizanur Rahman (2022a). A Reinforcement Learning Approach for Global Navigation Satellite System Spoofing Attack Detection in Autonomous Vehicles. *Transportation Research Record*, [online] 2676(12), pp.318–330. doi:<https://doi.org/10.1177/03611981221095509>.
- Dasgupta, S., Ghosh, T. and Md. Mizanur Rahman (2022b). A Reinforcement Learning Approach for Global Navigation Satellite System Spoofing Attack Detection in Autonomous Vehicles. *Transportation Research Record*, [online] 2676(12), pp.318–330. doi:<https://doi.org/10.1177/03611981221095509>.
- Irdin Pekaric, Sauerwein, C., Haselwanter, S. and Felderer, M. (2021). A taxonomy of attack mechanisms in the automotive domain. *Computer Standards & Interfaces*, [online] 78, pp.103539–103539. doi:<https://doi.org/10.1016/j.csi.2021.103539>.
- Jiang, P., Wu, H. and Xin, C. (2021). DeepPOSE: Detecting GPS spoofing attack via deep recurrent neural network. *Digital Communications and Networks*, [online] 8(5), pp.791–803. doi:<https://doi.org/10.1016/j.dcan.2021.09.006>.
- Kurbanov, A., Sergey Grebennikov, Salimzhan Gafurov and Alexandr Klimchik (2019). Vulnerabilities in the vehicle’s electronic network equipped with ADAS system. *2019 3rd School on Dynamics of Complex Networks and their Application in Intellectual Robotics (DCNAIR)*. [online] doi:<https://doi.org/10.1109/dcnair.2019.8875529>.
- Kuwahara, T., Baba, Y., Kashima, H. and Matsushima, H. (2018). *Supervised and Unsupervised Intrusion Detection Based on CAN Message Frequencies for In-vehicle Network*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/323762051_Supervised_and_Unsupervised_Intrusion_Detection_Based_on_CAN_Message_Frequencies_for_In-vehicle_Network [Accessed 25 Apr. 2023].

Mahdi Dibaei, Zheng, X., Jiang, K., Abbas, R., Liu, S., Zhang, Y., Xiang, Y. and Yu, S. (2020). Attacks and defences on intelligent connected vehicles: a survey. *Digital Communications and Networks*, [online] 6(4), pp.399–421. doi:<https://doi.org/10.1016/j.dcan.2020.04.007>.

Manesh, M. and Naima Kaabouch (2019). Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. *Computers & Security*, [online] 85, pp.386–401. doi:<https://doi.org/10.1016/j.cose.2019.05.003>.

Md. Delwar Hossain, Inoue, H., Ochiai, H. and Youki Kadobayashi (2020). *LSTM-Based Intrusion Detection System for In-Vehicle Can Bus Communications*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/347268419_LSTM-Based_Intrusion_Detection_System_for_In-Vehicle_Can_Bus_Communications [Accessed 25 Apr. 2023].

Muzaffar Khurram, Kumar, H., Adi Chandak, Varun Sarwade, Arora, N. and Quach, T. (2016). *Enhancing connected car adoption: Security and over the air update framework*. [online] 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). Available at: <https://www.semanticscholar.org/paper/Enhancing-connected-car-adoption%3A-Security-and-over-Khurram-Kumar/3b8edb8c904d6cbf22514a29cd019a1b41eac604> [Accessed 26 Apr. 2023].

Nayfeh, M., Li, Y., Khair Al Shamaileh, Vijay Devabhaktuni and Naima Kaabouch (2023). Machine Learning Modeling of GPS Features with Applications to UAV Location Spoofing Detection and Classification. *Computers & Security*, [online] 126, pp.103085–103085. doi:<https://doi.org/10.1016/j.cose.2022.103085>.

Pham, M. and Xiong, K. (n.d.). *A Survey on Security Attacks and Defense Techniques for Connected and Autonomous Vehicles*. [online] Available at: <https://arxiv.org/pdf/2007.08041.pdf>.

Rajkumar Singh Rathore, Chaminda T. E. R. Hewage, Omprakash Kaiwartya and Lloret, J. (2022a). In-Vehicle Communication Cyber Security: Challenges and Solutions. *Sensors*, [online] 22(17), pp.6679–6679. doi:<https://doi.org/10.3390/s22176679>.

Rathore, R.S., Hewage, C., Kaiwartya, O. and Lloret, J. (2022b). In-Vehicle Communication Cyber Security: Challenges and Solutions. *Sensors*, 22(17), p.6679. doi:<https://doi.org/10.3390/s22176679>.

Salvador, J., Oliveira, J. and Breternitz, M. (2020). *REINFORCEMENT LEARNING: A LITERATURE REVIEW (September 2020)*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/344930010_REINFORCEMENT_LEARNING_A_LITERATURE_REVIEW_September_2020 [Accessed 26 Apr. 2023].

Samira Tahajomi Banafshehvaragh and Amir Masoud Rahmani (2022). Intrusion, anomaly, and attack detection in smart vehicles. *Microprocessors and Microsystems*, [online] 96, pp.104726–104726. doi:<https://doi.org/10.1016/j.micpro.2022.104726>.

Shah Alam Khan, Mohsin, M. and Iqbal, W. (2021). On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. *PeerJ*, [online] 7, pp.e507–e507. doi:<https://doi.org/10.7717/peerj-cs.507>.

Sharma, A. and Jaekel, A. (2021). Machine Learning Approach for Detecting Location Spoofing in VANET. *International Conference on Computer Communications and Networks*. [online] doi:<https://doi.org/10.1109/icccn52240.2021.9522170>.

Siti-Farhana Lokman, Abu Talib Othman and Muhamad-Husaini Abu-Bakar (2019). Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review. *Eurasip Journal on Wireless Communications and Networking*, [online] 2019(1). doi:<https://doi.org/10.1186/s13638-019-1484-3>.

Sun, Q., Miao, X., Guan, Z., Wang, J. and Gao, D. (2021). Spoofing Attack Detection Using Machine Learning in Cross-Technology Communication. *Security and Communication Networks*, [online] 2021, pp.1–12. doi:<https://doi.org/10.1155/2021/3314595>.

Talaei Khoei, T., Ismail, S., Shamaileh, K.A., Devabhaktuni, V.K. and Kaabouch, N. (2023). Impact of Dataset and Model Parameters on Machine Learning Performance for the Detection of GPS Spoofing Attacks on Unmanned Aerial Vehicles. *Applied Sciences*, [online] 13(1), p.383. doi:<https://doi.org/10.3390/app13010383>.

Theyazn H. H. Aldhyani and Hasan Alkahtani (2022). Attacks to Automotous Vehicles: A Deep Learning Algorithm for Cybersecurity. *Sensors*, [online] 22(1), pp.360–360. doi:<https://doi.org/10.3390/s22010360>.

Vitale, C., Nikos Piperigkos, Christos Laoudias, Georgios Ellinas, Jordi Casademont, Josep Escrig, Kloukiniotis, A., Lalos, A.S., Moustakas, K., Rodriguez, R., Baños, D., Gemma Roqueta Crusats, P. Kapsalas, Hofmann, K. and Pouria Sayyad Khodashenas (2021a). CARAMEL: results on a secure architecture for connected and autonomous vehicles detecting GPS spoofing attacks. *Eurasip Journal on Wireless Communications and Networking*, [online] 2021(1). doi:<https://doi.org/10.1186/s13638-021-01971-x>.

Vitale, C., Nikos Piperigkos, Christos Laoudias, Georgios Ellinas, Jordi Casademont, Josep Escrig, Kloukiniotis, A., Lalos, A.S., Moustakas, K., Rodriguez, R., Baños, D., Gemma Roqueta Crusats, P. Kapsalas, Hofmann, K. and Pouria Sayyad Khodashenas (2021b). CARAMEL: results on a secure architecture for connected and autonomous vehicles detecting GPS spoofing attacks. *Eurasip Journal on Wireless Communications and Networking*, [online] 2021(1). doi:<https://doi.org/10.1186/s13638-021-01971-x>.

Wei, X., Wang, Y. and Sun, C. (2022). PerDet: Machine-Learning-Based UAV GPS Spoofing Detection Using Perception Data. *Remote Sensing*, [online] 14(19), pp.4925–4925. doi:<https://doi.org/10.3390/rs14194925>.

Yang, Y., Duan, Z. and Tehranipoor, M. (2020). *Identify a Spoofing Attack on an In-Vehicle CAN Bus Based on the Deep Features of an ECU Fingerprint Signal*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/338710382_Identify_a_Spoofing_Attack_on_an_In-

Vehicle_CAN_Bus_Based_on_the_Deep_Features_of_an_ECU_Fingerprint_Signal [Accessed 25 Apr. 2023].

Young, R.A., Fallon, S., Paul Mazhuvanchary Jacob and O'Dwyer, D. (2020). Vehicle Telematics and Its Role as a Key Enabler in the Development of Smart Cities. *IEEE Sensors Journal*, [online] 20(19), pp.11713–11724. doi:<https://doi.org/10.1109/jsen.2020.2997129>.