National College of Ireland

Simulation of False Data Injection Attack & Threshold-Based Detection for FDIA

MSc Research Project
M.SC in Cybersecurity

Mane Sudhanshu
Student ID: 22114599

School of Computing
National College of Ireland

Supervisor: Khadija Hafeez

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Sudhanshu Sunil Mane
Student ID:	22114599
Programme:	M.SC in Cybersecurity **Year:** 2023-24
Module:	Research in Computing
Supervisor:	Khadija Hafeez
Submission Due Date:	14/12/2023
Project Title:	Simulation of False Data Injection Attack (FDIA) & Threshold-Based Detection Strategy for FDIA
Word Count:	6257 **Page Count:** 18 Pages

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Sudhanshu Sunil Mane

Date: 14/12/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Simulation of False Data Injection Attacks & Threshold-Based Detection of FDIA

Sudhanshu Mane
22114599

Abstract

The research projects cover's the understanding and implementation of simulation of False Data Injection Attack and Threshold-Based Detection to detect False Data Injection using MATLAB code. The need for this project is to achieve end goal of contributing to the world of cybersecurity and achieve safety in V2V communication, if not addressed in time, inter-vehicular errors in sensors can happen which might disrupt communication network, further it also can cause chaos on the roads if accidents happen due to failure of sensors or any in-vehicular network disruption. The code used in MATLAB is simulating communication between two vehicles where an attacker vehicle plans to inject False speed information inside the victim's vehicle. This provides simulation of False Data Injection Attacks (FDIA). For Threshold-Based Detection simulation we implemented MATLAB code for algorithm and detection functionality. An existing dataset provided the time taken to reach final velocity 100 and initial velocity 0. By using this data to calculate acceleration the threshold was set for two test cases. The motivation behind the project was to contribute to the world of cybersecurity. This project will help researchers analyse False Data Injection Attacks and Threshold-Based Detection strategy in a better way. This research can help to explore new pathways in the real world to implement Threshold-Based Detection strategy integrating it with physical entities that are present in V2V communication.

1 Introduction

Autonomous Vehicles represent significance to the Human modernization. People can travel within matter of minutes using vehicles [1]. These vehicles have been evolved in terms of technology as people have found various ways to evolve automotive industry and now, we have Intelligent Transportation System. Cyber-Physical-Systems are key enabler of vehicular communications as they interact with in-vehicular networks. Vehicles can now react according to environment and surroundings due to use of multiple sensors and a compatible network implemented in vehicle.

1.1 Research Problem Background

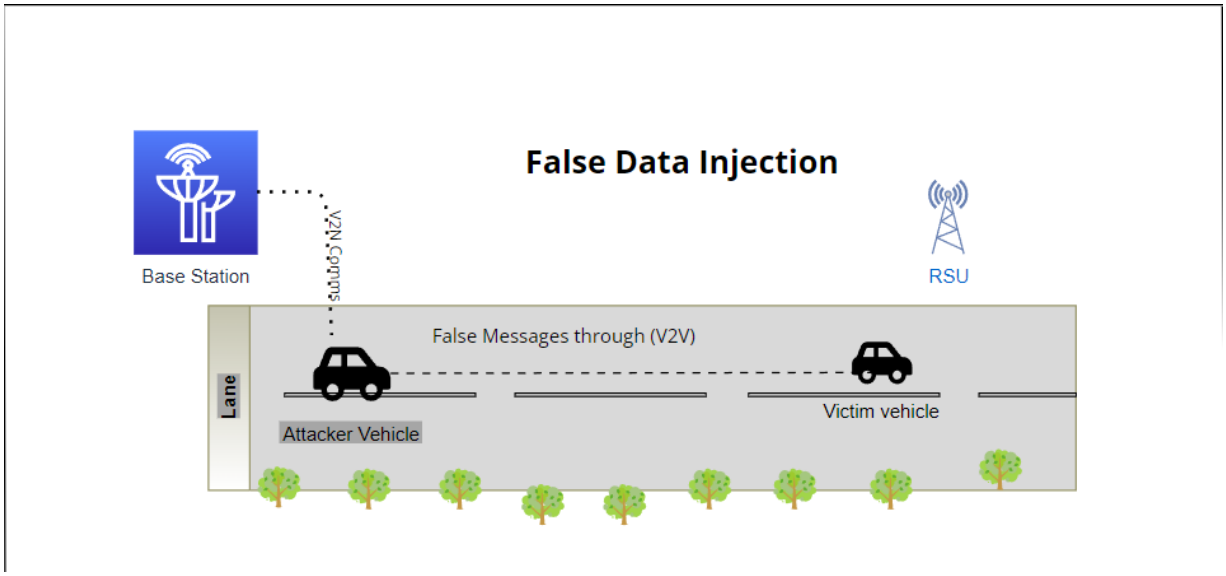


Fig 1] False Data Injection

Vehicular communication is enabled by various communication models present such as Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Everything (V2X), Vehicle-to-Pedestrian (V2P) and Cellular Vehicle-to-Everything (C-V2X) [2]. Vehicle Ad-Hoc Networks (VANETs) rely on timely exchange of data communication [3], hence, rises a need for safety in Vehicular Communication as it can be vulnerable to False Data injection attacks.

False Data Injection Attacks (FDIA) are cyber-attacks which are focused to compromise sensor readings or alter them [4]. In Vehicle-to-Vehicle communication False Data Injection attacks

can compromise vehicle sensor such as OBD-II port, DSRC communication, Global Positioning System (GPS) to alter the messages that provide information like speed messages, vehicle position info and many more [4].
If False Data Injection Attack (FDIA) can successfully be injected it can impact on vehicles sensors which play a role in vehicle safety. After the attack the sensors are disrupted, and this can affect vehicle communication and can trigger other safety sensors which might lead to unwanted collision or disruption in traffic.
However, there are no real-world attacks in V2V communications False Data Injection Attacks (FDIA) poses a threat and can be a threat. Many literatures have stated False Data Attack is manipulation or alteration of the data exchange held between vehicles. This data can be data relating vehicle position or manipulation of false messages relating speed. In these situations, communication models often need a safe space as the communications can be interrupted and may be vulnerable to False Data Injection Attacks.
False Data Injection Attacks can affect Integrity, as well as Availability of a vehicle. False Data Injection Attacks can affect in Smart Grids, IOT (Internet of Things), Vehicle Communication and various Cyber Physical Systems (CPS) .

1.2 Research Questions:

This research aims to study and simulate FDIA attacks in Vehicular Communication in way that the FDIA is easier to understand and study or propose effective mechanisms that prevent False Data Injection Attack in V2V communication. The key research questions we aim to study on are as follows:
1] What have existing literatures done for understanding of FDIA and detection strategies?
2] What is the most effective security mechanism that can be used to provide safety against FDIA attacks that alter or manipulate the speed informative messages in V2V communication?
Literature Review focuses key points implying reviews and source of the key aspects such as simulation and analysis of False Data Injection attacks and effective detection and mitigation strategies.

1.3 Motivation & Purpose

The understanding of False Data Injection Attacks depends on real-world attack history and scenarios, simulation, and research papers. However, there aren't many real-world attack histories making it difficult to attain solutions for the attack. Although there is limited amount of simulation run by researchers. Research papers provide effective ideas that can be analysed to detect or prevent False Data Injection Attacks. This research aims to provide simulation of False Data Injection Attacks (FDIA) that increases speed and provide effective simulation of Threshold-Based detection strategy to contribute providing simulation of the strategy to detect the attack. The research also aims to understand the False Data Injection Attacks in a simplified manner so that motivated researcher can gain more knowledge in an easier way. However, there are few limitations while running the simulation, the simulation satisfies need of understanding FDIA. The purpose of this research can generate new ideas to work around FDIA attack which in future can enhance road safety, provide a safe space for V2V

communications, the Threshold-based detection strategy can be grounds for exploring new pathways also understand the strategy in simplified manner and implemented simulation makes it easier to understand the logic to set the detection pattern.

1.4 Structure of Report

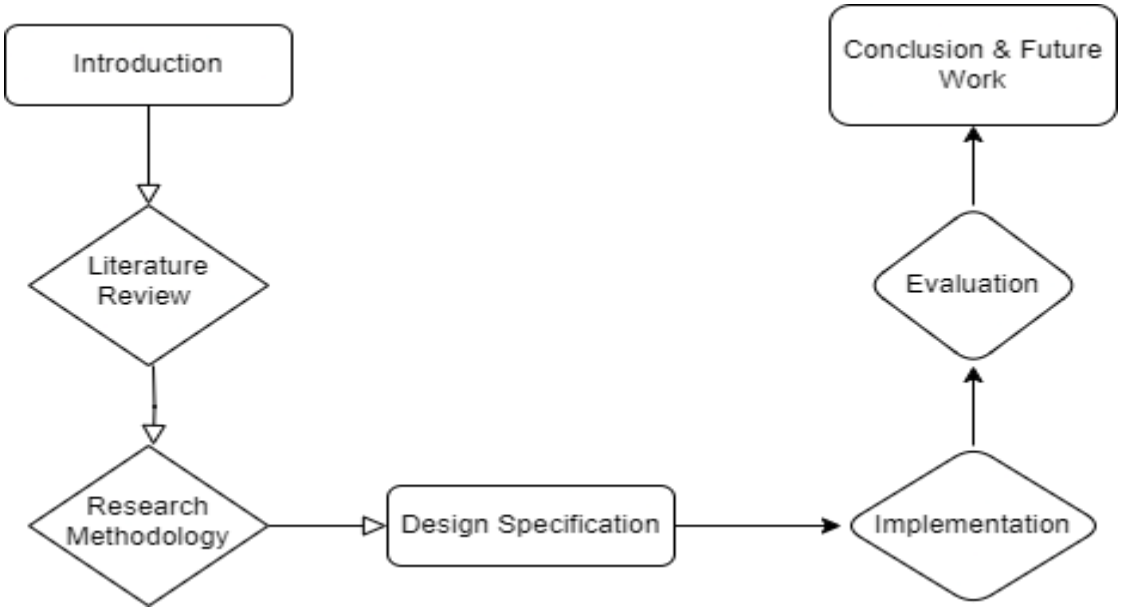


Figure 2: Structure of Report

2 Related Work

Thorough review of existing literature was done using research papers and web articles. This was done to understand the implementation and various related work articles to determine gap analysis. Understanding and knowledge of Vehicle-to-Vehicle (V2V) communications and security challenges faced in Vehicle-to-Vehicle (V2V) were studied. After understanding of Vehicle-to-Vehicle (V2V) the study of False Data Injection Attacks in Intelligent Transportation system helped analyze of False Data Injection Attacks. Existing Literature helped studying nature and execution of False Data Injection Attacks where few literatures provided simulation of FDIA using various techniques and provided a detection strategy which gained helpful insights on detection work.

The study conducted by [4] research explained the threat FDI (False Data Injection) in Vehicular platoons. Platoon network includes communication concepts of vehicles such as, Vehicle-to-Vehicle communication, Lead vehicle controls, the minor inter vehicle distances and many more. The researchers explained FDIA after attack scenarios such as Impact on safety and stability, the vehicles speed and carbon emissions. During constant FDIA attack scenario the following vehicles speed increased affecting platooning formation. On and Off FDIA attacks showed constant speed change high to low, low to high. This research was helpful in the context of FDIA attack scenarios. Solutions to mitigate these attacks are the following future work stated by the researchers. The author [5] proposed Support Vector

Machine-base Intrusion Detection System (IDS) was proposed in the following paper. According to [5] FDIA attacks challenge the networks integrity by manipulating the messages. These messages are sent within the network and can affect the behaviour of communication nodes. The concept of Host-based Intrusion Detection System (HIDS) was discussed for interpreting broader strategies. The above paper is like [6] **as** it embarks Cloud-Based Sandbox Detection techniques to detect False Data Injection Attacks highlighting V2V and V2I communication models. The aim of this is to detect FDIA in Controlled and Automated Vehicles. The paper highlights vulnerable components such as adaptive cruise control, advance assistance systems and signal controls. The study discussed [7] researchers have addressed issues underlying in Co-operative Adaptive Cruise Control systems. These systems are vulnerable to False Data Injection attack. Research was completed by using PDE based approach focusing on real-time identification of FDIA. The PDE based model is designed to make an observer-based algorithm which can locate FDIA attacks. In the research paper [8] research method studied and applied was to detect and isolate of False Data Injection Attack in Intelligent Transportation System using Robust State Observer method. The design is focused to adapt the scenarios in a quicker way to respond and isolate the malicious packets and hence, robust state observer banks to isolate FDI attacks were created. Road-Side Units were vulnerable components which are critical operations for Intelligent Transportation Systems. Anomaly-based detection and mitigation techniques using machine learning detectors were implemented in RSUs. In the paper written by [9]**,** analysis of FDIA in vehicle Platooning has been done. The aim of this paper was to identify this attack using longitudinal motion of these vehicles. The paper also addresses the critical issue on Cyber Physical Systems (CPS). It demonstrates the FDIA is affecting sensor data and the vehicles acceleration and delays of important message packets. [10] proposed multiple detection strategies. [10] focused this paper on three main aspects which were characteristic of Vehicular Ad-Hoc Networks (VANETs), its attack scenarios and their solutions, further they were compared to establish a security criterion. [10] left a useful impact on his research as multiple solutions were stated for false message injection attack in other research papers. [11] implemented and proposed use of a group-signature-based security framework to achieve authenticity and data integrity. A signature verification scheme was developed to detect tampered messages. Though the model is impactful, complex integration of the key managers can be an issue. In the paper written by [12], proposed a solution which to enhance privacy introducing Group Formation for Security Framework. This detection strategy is considers using optimized link state routing (OSLR) for communication which will help group formation for security. Although the privacy in produced by the solution but fails to enhance privacy for the group leader in the formation as the group leader is managing and authenticating group members. Also, this model fails to show impact and counter measures for rapid topology change in groups. [13] demonstrates a false information attack on a vehicle. In this scenario one vehicle is sending false information to other vehicle resulting the false information receiver changing direction. The author suggests using (Elliptic Curve Digital Signature Algorithm) as a solution the attack. In the paper written by [14] classifies security issues and vulnerabilities in Intelligent Transportation system. [14] has stated importance of Intelligent Transport Systems and why the security needs to be addressed. [14] has stated, false data injection types which include GPS manipulation, false broadcast messages into the network. The research provides impactful, understanding of False Data injection and has referenced solutions provided by other sources.

Table1: Related work

Ref	Detection Strategies	Limitation of Detection Strategies
[10]	Classification of Implementation Strategies	Did not implement detection strategies but mentions solutions proposed by other research papers.
[11]	Group-Signature based framework	Complex Integration of key managers. Not scalable in a large network.
[12]	Group Based Communication Network	Group formation can be challenging and can impact vehicular network performance and raising issue of rapid topology change.
[13]	Elliptical Curve Digital Signature Alogrithm	No limitations were found
[14]	Classification of Multiple Strategies	Did not implement detection strategies but mentions solutions proposed by other research papers.
[8]	Robust-State-Observer model by implementing Anomaly-Based Detection	There is lack in dependency of parameter estimation of the observer model used in the paper.
[6]	Used Cloud-Based Sandboxing	More computing power
[7]	Real-Time Detection using PDE based approach	Small FDIA attacks may blend into the noise as per [7]
[5]	SVM-Based Detection to detect FDIA	SVM require linear datasets. If the datasets are non-linear it might struggle in analysing large datasets.

3 Research Methodology

3.1 Research Model

Thorough understanding and various simulation models which explain about False Data Injection Attack and detection strategies were provided by existing literature. The research was led by understanding of V2V communication and gained knowledge about working of communication mechanisms used in V2V, various sensors that are used in vehicles for safety and that are used in V2V. The MATLAB code was understood and implemented to provide simulation and impact of False Data Injection Attacks (FDIA). An existing dataset provides 0-100 acceleration time. This helped us analyzed acceleration per second of two test cases that are two different vehicles leading to simulation of detection strategy. The graphs and plots were implemented to describe the impact and provide analysis of real mechanisms that

can be affected in V2V communication. The detection strategy was studied using different literatures making use of Threshold Based Detection Strategy to detect False Data Injection Attack in Smart Grids. However, we came to conclusion that this strategy can also be used to detect False Data Injection Attack in V2V, and we provided a simulation for it.

3.2 Simulation Methods (FDIA & Threshold-Based Detection)

Study of literature review provides insights of past simulation propagating a difficult structure to analyze and understand False Data Injection Attacks (FDIA). The simulation is a simplified simulation to understand False Data Injection Attacks. This is important to understand the methodology and techniques that are used to simulate the attack. This step took an experimental research approach to define the impact and methodology of False Data Injection Attack that alters speed data. The use of MATLAB indicates quantitative approach where the algorithms and model are developed to simulate FDIA and Threshold based detection.

3.3 Evaluation of Simulation Results

Model was created to understand the behavior and impact of False Data Injection Attack and utilizing the data we introduced a threshold-based detection strategy. Impact and behavior generated by the model is compared to real world message transmission in Vehicle-to-vehicle communication to determine the affecting factors, hence comparative analysis. The visualization provides graphs to pinpoint key findings.

4 Design Specification

The design specification outlines a framework which has been developed using MATLAB. The model is used to analyze the effects of False Data Injection Attack on V2V communications. A real-world scenario is generated to study effects when a malicious endpoint is altering speed information to send it to the victim to receive speed information. The time step model is designed to understand the attack which captures data transmission between two vehicles. However, we faced multiple challenges and limitations to provide deep research on False DataInjection Attacks and they are as follows.

In-Depth analysis of network nodes and in-vehicular is not possible due to insufficient resources and funding. Insufficient data for analyzing FDIA attacks makes it challenging as the data can be convenient to study the behavior of in-vehicular networks and V2V communication whenfalse data injected through the network. Preventive measures can only be stated and be used as source of information that can beused to research in future due to lack of resources and in-real life practices. Mitigative measures can limit themselves to study of security implementation that can beused to prevent FDIA attacks. The aim of the simulations is to simplify the understanding of False Data Injection attacksfrom vehicle to vehicle. Although there is a lack of implementation of network models like V2V. The purpose of the simulation is to gain knowledge regarding FDIA attacks via visual simulation of graphs and output.

The model is simulated for research purposes and provides an understandable model on how False Data Injection Attack might impact the message transmission in V2V communication. The simulated model lacks in real V2V scenarios that can provide factors like networklatency and more sophisticated attack patterns. These patterns can be integrated with V2V communication model real world scenariosusing this FDIA simulation model in future.

4.1 Design Specification for False Data Injection Attack Simulation

4.1.1 Simulation Architecture

A time-stepped simulation model approach is created within MATLAB environment to model and simplify the understanding of behaviour in V2V communication. In the architecture two main entities are a vehicle who is transmitting speed messages, and the other vehicle is receiving the messages with associated speed parameters.
An event simulation framework is implemented where the predefined time and timestep to achieve real-time data transmission between the vehicles and attack scenario. An attack vector is created to simulate False Data Injection Attack. Following with the transmission of the data in intentionally altered to generate an attack window for a particular amount of time. The model and requirements have ability to track and store speed data to mark the circumstance of False Data Injection Attack (FDIA). The functions then store the data and visualize the results for analysis.

4.1.2 Algorithm Functionality

A simultaneous process is required to perform the simulation and iterate over each timestep with total simulation time therefore, to do so simulation operates in a loop. The data transmission is modelled to transmit value of speed directly from the transmitting vehicle to the receiver. The algorithm is designed to model the transmission of data by 1.5 to represent False Data Injection Attack (FDIA). To assess the impact of False Data Injection Attack (FDIA) the outputs generate speed data before and after the attack. The plot determines the factors required for visualization which highlights the attack period, constant speed of attack and the hike of speed after given time which indicates that speed has been altered and signs FDIA.

4.2 Design specification for Threshold-Based Detection Strategy

4.2.1 Simulation Architecture & Algorithm Functionality

The code which is implemented in MATLAB gives a model of V2V communication system, where attacker vehicle is transmitting speed information to victim vehicle. The time stepped simulation approach is taken to define speed information transmission in time interval of 1 second. The attacker vehicle is sending speed information where the vehicle is travelling at a constant rate of 60 kmph. The attack phase is artificially defined where the attacker vehicle is transmitting false data. The victim vehicle observes speed 90 kmph and the speed hike by 1.5 percent is observed. Thresholds are set according to the vehicles' max acceleration limit. Below are the following thresholds:

Table 2: Measuring Accelerations

Brand	Model	Time taken (Final Velocity)	Acceleration per Second
Tesla	Model 3 Long Range Dual Motor	4.6 seconds	21.74 km/h
BMW	iX3	6.8 seconds	14.71 km/h

The values are taken from existing dataset and acceleration per second defines the threshold. The 'Brand' in dataset defines vehicle owning companies. 'Model' defines model name of the vehicle and 'AccelSec' defines time taken to reach 0-100 velocity. To calculate the following average acceleration, we have used two test cases to simulate threshold-based detection simulation in MATLAB.

5 Implementation

5.1 Tools and Language

The simulation, algorithms and model were created using MATLAB. The reason for choosing MATLAB is it provides robust set of tools that can provide better mathematical computation. The data visualization makes it easier to understand what's going inside simulation. There are different tools to provide visualization but as it being outside my domain knowledge, to adapt to OMNET++ learning is time consuming and understanding and simulating the attack to make people understand can be difficult. MATLAB provides better scripting facilities and is efficient to show manipulation of data.

5.2 Implementation for FDIA Simulation

The implementation of False Data Injection Attack (FDIA) simulation explains the final stage of simulation. It describes the outputs produced as well as the questionnaires administered. Also, explanation of tools implemented and all the factors that were used to produce the output.

5.2.1 Final Stage Description

A model of an attack is created to simulate the FDIA attack. This model describes the behaviour of a vehicle under normal operation undergoing a False Data Injection Attack. The output is generated using data points which represents a malicious vehicle transmitting the speed to the victim vehicle within the period where FDIA occurred. The graphical representation is produced to analyse and visualise the attack phase. The visualization specifies the attack time window, the speed alteration during the time FDIA occurred, speed after and before the attack. The transmission of speed data shows impact of FDIA in between vehicle to vehicle.

5.1.2 Outputs

The final set of results provide speed values of before and after the False Data Injection Attack in between Vehicle-to-Vehicle. The output displays a continuous point of time of attack to visualize when has the FDIA occurred. Plots features visualization of before and after attack speeds, and when the FDIA has occurred in the simulation model. In conclusion, the implementation of simulation model provides insights and output of FDIA in vehicular communication where data driven analysis provides impact without needing of real-world testing.

5.3 Threshold-Based Detection Strategy Simulation

5.3.1 Final Stage Description

In the final stage we have implemented an algorithm functionality to detect the anomaly. The anomaly is speed hike more than maximum acceleration per second. The algorithm defines pattern to detect the anomaly based on threshold-based detection. The MATLAB code is implemented to detect the anomaly. Refer figure 2. The test cases taken from existing dataset determines acceleration per second using the formula.

```
% Threshold-Based Detection
if t > 1 && abs(vehicle1_speed_data(t) - vehicle1_speed_data(t-1)) > max_acceleration
    fprintf('False Data Injection Attack Detected at time %d sec\n', time_vector(t));
    anomaly_detected_vector(t) = 1;
end
```

Figure 3: Detection Algorithm

Average acceleration determines the time taken for a vehicle to gain speed at a maximum acceleration also average acceleration is calculated in scenarios where vehicles hold data where 0-100 speed needs to be calculated and analyzed. Average acceleration can be calculated using the following formula $\overline{a} = \frac{\Delta v}{\Delta t} = \frac{v_f - v_0}{t}$ where Δv represents the velocity, Δt represents time taken to reach maximum velocity, v_f represents final velocity, v_0 represents initial velocity, t represents time taken to reach maximum velocity. The dataset contains acceleration time, where time taken for vehicles speed initiating at 0 kmph to and final speed is at 100 kmph. These are the following speeds at which a vehicle can accelerate in 1 second. For vehicle brand Tesla Model 3 Long Range Dual Motor can accelerate up to 21.74 km/h per second. For this vehicle we have artificially set the False Data Injection attack to occur by setting the multiplying the speed value by 1.5 after 60 seconds to determine the FDIA detection scenario Vehicle BMW iX3 can accelerate up to 14.71 km/h per second. For this vehicle we have artificially set that FDIA is not going to occur. Although we set additional speed message to determine speed increasing below threshold by multiplying the constant speed by 1.2, making it a legitimate scenario.

If any speed is hiking up by the preferred threshold, then we can say that False Data Injection has been detected. This strategy provides an efficient way to detect False Data Injection Attack.

5.3.2 Outputs

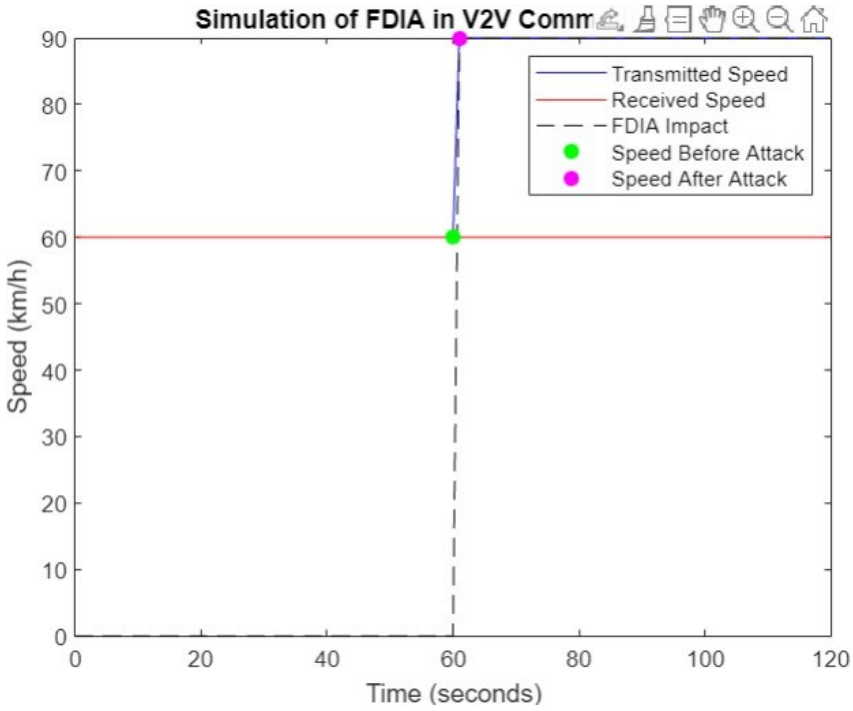
The outputs generated defines that anomaly is detected. We have added a functionality to determine whether the attack has occurred in the simulation or not. The plots and graph provide visualization and using this impact can be analysed. For this we implemented the plot generating code in MATLAB. In the output section we implemented an algorithm and when

the attack is generated, the detection code activates, and outputs are printed in the output section of MATLAB providing the time step of and time interval of attack detection.

6 Evaluation

6.1 Evaluation of FDIA simulation (Graph)

The simulation model was run to simulate False Data Injection Attacks which compromise or alter the speed of a vehicle. The results define that the False Data Injection Attack was successfully simulated resulting in the compromise of speed of transmitter (Vehicle 1). Below is a plotted graph stating the work of simulation.



]

Figure 4: Plots of FDIA attack

The plot explains that before FDIA attack started after 60 seconds. The hike is represented via dashed line (---). The time interval is presented by X axis and the rising Speed (km/h) is represented by Y axis. As the constant speed of transmitting vehicle is 60 KM/H, after 60 seconds the speed of transmitting vehicle is hiked up to 90 KM/H. The green circle represents speed before attack which is 60 Km//H and purple circle determines the speed after attack which is 90 Km/H. Hence, we can say that the False Data Injection Attack was successfully simulated artificially.

6.2 Why is it False Data Injection and not a system failure?

We analysed the impact of False Data Injection using MATLAB. We saw that two speed message transmission data are transmitting from one vehicle. This leads to two assumptions of the results. The first assumption is that the False Data Injection Attack has occurred and second, there might be a weak-vulnerable sensor. Vehicles have an Event Data Recorder

(EDR) present in vehicles to generate information from vehicle components in case of crash and they keep assessing the vehicle components such as sensors, Engine Control Unit (ECU) and other critical infrastructure. They have the capacity to generate safety notifications. OBD-II devices also have the ability to generate safety notifications. Using these mechanisms, in vehicles we can analyse if any weak sensor or component is vulnerable and damaged. In conclusion, it is safe to assume that False Data Injection Attack has occurred if any safety messages are not generated using vehicle mechanisms.

6.3 V2V Communication:

The simulation is a simplified way of understanding False Data Injection Attacks. This section provides understanding of real-world components which can be affected by FDIA. The communication channels play an important role when transmitting a message in V2V. As per [3] Dedicated Short Range Communication and few more IEEE standards are used in V2V communication. Sensors such as Global Positioning System (GPS) collect information about the position of the vehicle and are sent to On-Board Units (OBU). 75 MHz band wide from 5850 to 5925 GHz spectrum is allocated to DSRC which defines the range for communication. WAVE IEEE 1609 is a set of standards which include protocols, interfaces and services enable key communication factors.
Engine Control Units (ECU) understands the factors and controls services like braking and acceleration. According to [15] the information messages incoming through the OBD-II port which is operated by Controlled Area Network (CAN). In the book written by [16] mentions that reducing the message transmission which can contain failure and notification message is main goal of OBD-II port in vehicles.

6.4 Message Transmission Analysis (REAL WORLD)

Let us create a scenario where Vehicle A is sending speed information to Vehicle B using following key components:
DSRC: To transfer the message between to vehicles using Radio Channels.
In-Vehicular Networks: In Vehicle A, speedometer collects speed data, Engine Control Unit generates message and using DSRC sends it to Vehicle B. The Vehicle B Receives speed data of Vehicle A. As vehicle B receives message the On-Board Units asses the information and formats into structured and standardized format which is suitable for transmission [17].

6.5 Analysis by comparing simulation to real world Message Transmission Analysis

Vehicle A is travelling 60 KM/H at a constant speed. The Vehicle A is transmitting message and Vehicle B is receiving a message. The time interval is set to 60 seconds to simulate attack in the model. When the time hits 60 seconds the speed data transmitted from Vehicle A and received to Vehicle B showed speed hike and is increased to 90 KM/H. Using this logic, it is enough to assume that the data came through Vehicle A is false, and false data injection attack has been used to disrupt V2V communication and creating a false circumstance.

6.6 Simulation of Threshold-Based Detection Strategy

We took a scenario where existing dataset has provided time taken to accelerate from 0-100. We are going to calculate the acceleration per second to determine the threshold value for speed that can be gained in one second. Any speed data incoming through the attacker vehicle is analyzed by V2V communications and if speed per second data coming through the next

following second has a hike more threshold coming through, it can be said that attack has been detected. This simulation is implemented and is run by MATLAB.

6.6.1 Threshold-Based Detection Visualization

1] Test Case 1:

Below are the results of Threshold-Based Detection simulation run for Brand Tesla, Model 3 Long Range Dual Motor which has acceleration per second of 21.74 kmph.

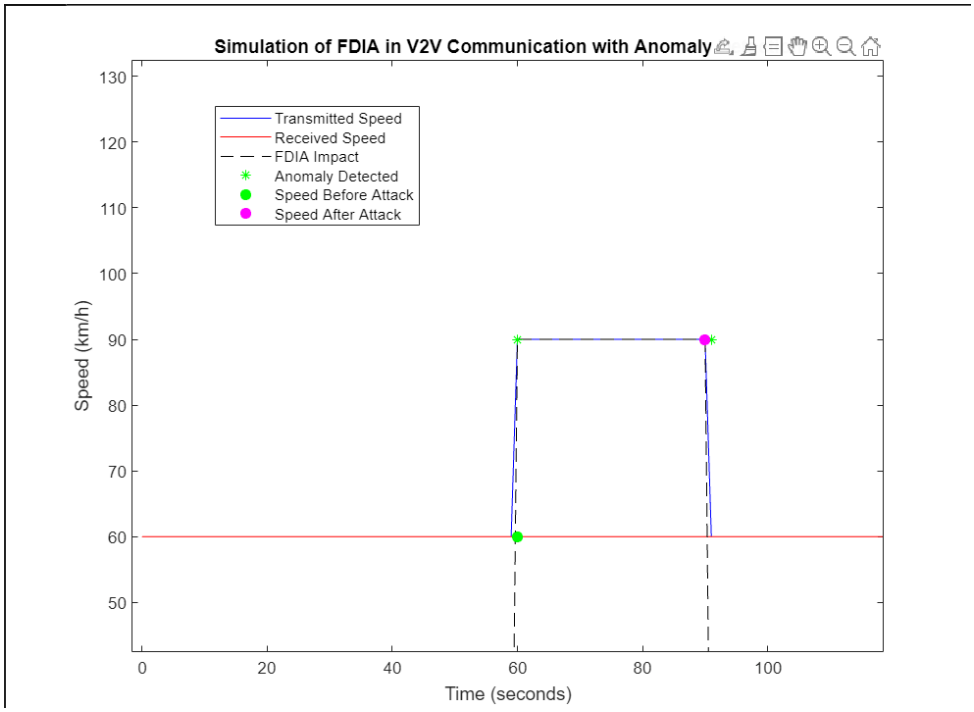


Figure 5: Anomaly Detected (Test Case 1)

In the visualized graph we can see that False Data Injection Attack has occurred. We see that after 60 seconds there is hike of extra 30 km/h in speed in one second. But according to the acceleration per second threshold of Brand Tesla, Model 3 Long Range Dual Motor is 21.74 and there is additional 8.26 kmph speed hike which is impossible under normal conditions. Hence it is safe to state that False Data Injection Attack has been detected. In figure [] there is output of speed message shared between two vehicles and the attack detected message when unrealistic speed message was captured by the victim vehicle.

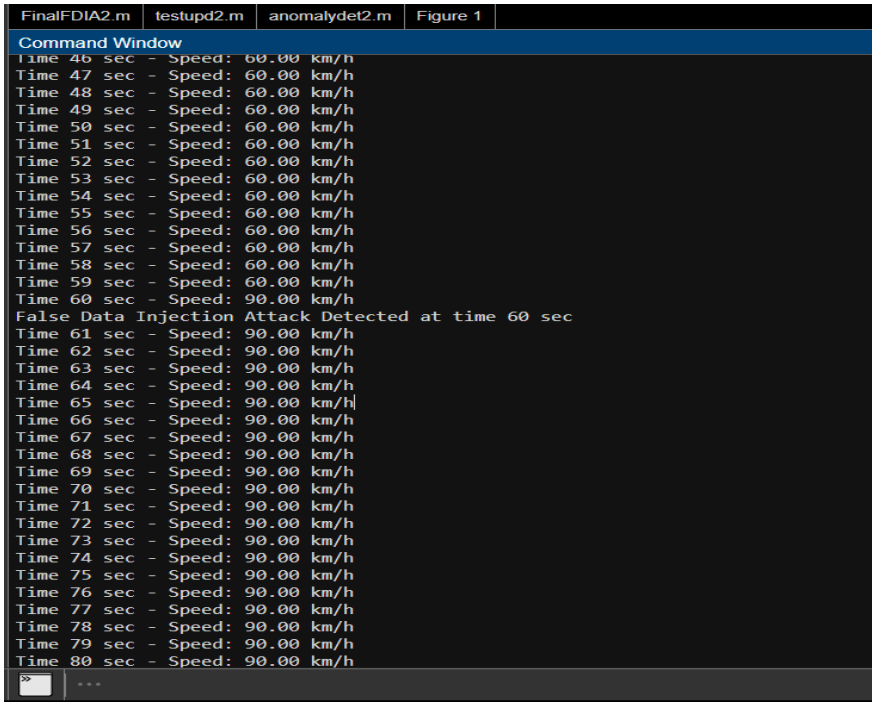


Figure 6: Output (Test Case 1)

2] Now for the 2nd test case we took Brand BMW, Model iX3 which has acceleration per second of 14.71 kmph.

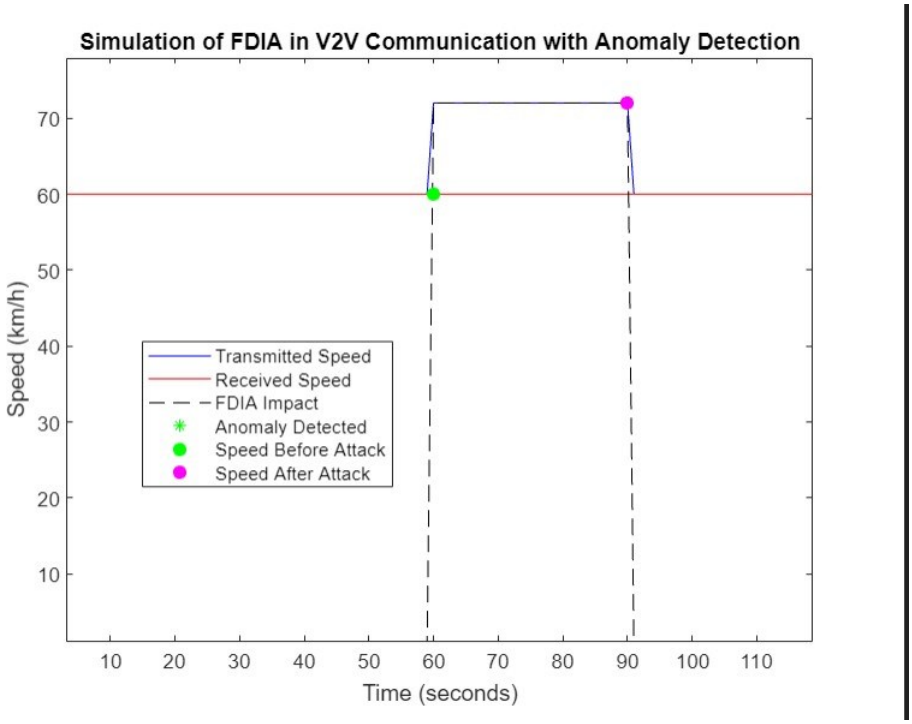


Figure 7: Normal Communication (Test Case 2)

Here you can see there is no anomaly detected for this case as maximum acceleration per second for Brand BMW, Model iX3 is 14.71. The vehicle after 60 seconds only accelerated an additional 12 kmph. Hence, the speed information received to the vehicle is legitimate as 12 kmph can be legitimate and acceptable threshold for the vehicle to accelerate. Hence no

False Data Injections Attack occurred in V2V communication. Below is output tab for speed message received for each 1 second time interval (No Attack Detected).

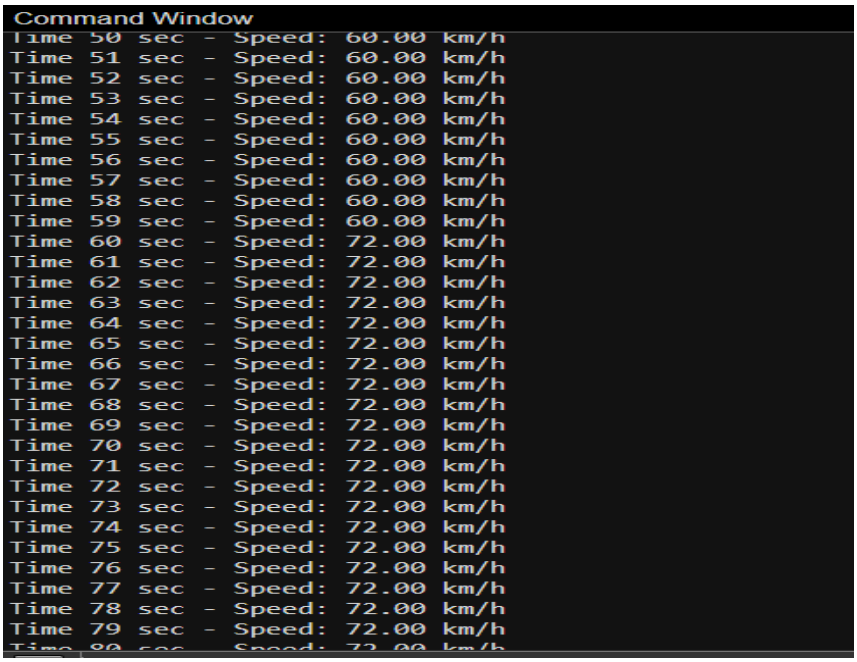


Figure 8: Output (Test Case 2)

6.6 Discussion

The simulation of False Data Injection Attack that alter messages that provide information on speed and simulation of detection strategies were implemented in this research project and analysing security aspects present in V2V communication and to analyse impact of False Data Injection Attacks and provide visualisation. The FDIA simulation explains how the attack works in Vehicle-to-Vehicle communication by implementing MATLAB code. This simulation provides understanding of False Data Injection Attacks that alter speed message. The model doesn't implement the exact network communication nodes that are present V2V but just a basic simulation which provides better understanding of False Data Injection Attack than other existing literatures. The simulation model can later be updated and modified by using core network connections of V2V using MATLAB's priced version as well as physical entities. Theoretical analysis and comparative analysis are provided to understand False Data Injection Attack impact in real world also comparing it with simulation entities.
The Threshold-Based Detection strategy was proposed by [18] in Smart Grids where values of sensors are altered. In this research project we implemented a simulation of threshold-based detection strategy. The model includes a threshold-based algorithm to detect which false speed messages transmitting from attacker vehicle. The existing dataset provides time taken to reach final velocity 100. Using that time provided to reach 100 we utilized the model to calculate the acceleration per second of the vehicle. Using this we were able to use effective threshold-based algorithms in MATLAB. The simulation model gives effective understanding of detection strategies that can be implemented in real life. The threshold-based algorithm implemented in MATLAB is effective strategy implemented, however the model is based on two test cases and not each vehicle using V2V communication. The model needs to be perfected and effective security mechanisms should be applied in physical entities to analyze this strategy. However,

the two test cases applied to study detection strategy suggests that it can be one of the best security mechanisms that can be used to study.

7 Conclusion and Future Work

The research aimed to study False Data Injection Attack that alters and transmits false speed messages and propose an effective detection strategy. We studied, simulated, and analysed the False Data Injection Attack (FDIA) and proposed, implemented Threshold-Based Detection Strategy to detect False Data Injection Attack. The simulation models are implemented using MATLAB code. Although simulation is lacking in real world V2V networking scenarios due to insufficient time, domain knowledge and lack of open-source simulation resources. Existing dataset provided time taken for a vehicle to go 0-100 which helped us determine maximum acceleration. The algorithm model used for simulation can be used to integrate with real-world network scenarios. The key findings of this research project pinpoint the use of Threshold-Based Detection strategy can be used to detect the FDIA attack that alters false speed messages. This strategy needs to be studied in future to integrate it with Intelligent Transportation Systems. Threshold-Based Detection strategy is willingly the best effective security measured that can achieve integrity or availability in future.
In future, we plan to implement and analyse Threshold-Based Detection strategy usingdifferent scenarios and test if the algorithm model can be worked with real-world network simulations.

References

[1] F. Eckermann, M. Kahlert, and C. Wietfeld, “Performance Analysis of C-V2X Mode 4 Communication Introducing an Open-Source C-V2X Simulator.” arXiv, Jul. 23, 2019. doi: 10.48550/arXiv.1907.09977.

[2] S. Zhang, J. Chen, F. Lyu, N. Cheng, W. Shi, and X. Shen, “Vehicular Communication Networks in the Automated Driving Era,” *IEEE Communications Magazine*, vol. 56, no. 9, pp. 26–32, Sep. 2018, doi: 10.1109/MCOM.2018.1701171.

[3] Z. Lu, G. Qu, and Z. Liu, “A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760–776, Feb. 2019, doi: 10.1109/TITS.2018.2818888.

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

[5] “SVM-based Detection of False Data Injection in Intelligent Transportation System | IEEE Conference Publication | IEEE Xplore.” Accessed: Dec. 14, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9333942

[6] “Detection of False Data Injection Attack in Connected and Automated Vehicles via Cloud-Based Sandboxing | IEEE Journals & Magazine | IEEE Xplore.” Accessed: Dec. 14, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/9463871

[7] R. A. Biroon, Z. A. Biron, and P. Pisu, “False Data Injection Attack in a Platoon of CACC: Real-Time Detection and Isolation With a PDE Approach,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 8692–8703, Jul. 2022, doi: 10.1109/TITS.2021.3085196.

[8] X. Huang and X. Wang, “Detection and Isolation of False Data Injection Attack in Intelligent Transportation System via Robust State Observer,” *Processes*, vol. 10, no. 7, Art. no. 7, Jul. 2022, doi: 10.3390/pr10071299.
[9] B. Biswas, “Analysis of False Data Injection in Vehicle Platooning,” *All Graduate Theses and Dissertations, Spring 1920 to Summer 2023*, May 2014, doi: https://doi.org/10.26076/e378-1a4e.
[10] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, “VANet security challenges and solutions: A survey,” *Vehicular Communications*, vol. 7, pp. 7–20, Jan. 2017, doi: 10.1016/j.vehcom.2017.01.002.
[11] J. Guo, J. P. Baugh, and S. Wang, “A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework,” in *2007 Mobile Networking for Vehicular Environments*, May 2007, pp. 103–108. doi: 10.1109/MOVE.2007.4300813.
[12] B. Mokhtar and M. Azab, “Survey on Security Issues in Vehicular Ad Hoc Networks,” *Alexandria Engineering Journal*, vol. 54, no. 4, pp. 1115–1126, Dec. 2015, doi: 10.1016/j.aej.2015.07.011.
[13] V. Hoa La and A. Cavalli, “Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey,” *IJANS*, vol. 4, no. 2, pp. 1–20, Apr. 2014, doi: 10.5121/ijans.2014.4201.
[14] D. Hahn, A. Munir, and V. Behzadan, “Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges,” *IEEE Intelligent Transportation Systems Magazine*, vol. PP, pp. 1–1, Apr. 2019, doi: 10.1109/MITS.2019.2898973.
[15] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, “Intelligent Transportation System Security: Impact-Oriented Risk Assessment of In-Vehicle Networks,” *IEEE Intelligent Transportation Systems Magazine*, vol. PP, pp. 1–1, Jan. 2019, doi: 10.1109/MITS.2018.2889714.
[16] K. McCord, *Automotive Diagnostic Systems: Understanding OBD I and OBD II*. CarTech Inc, 2011.
[17] Y. Wu, P. Wang, and C. Sun, “Design and implementation of OBU terminal for Vehicle Ad-hoc Network,” *J. Phys.: Conf. Ser.*, vol. 1920, no. 1, p. 012016, May 2021, doi: 10.1088/1742-6596/1920/1/012016.
[18] P. Hu, W. Gao, Y. Li, M. Wu, F. Hua, and L. Qiao, “Detection of False Data Injection Attacks in Smart Grids Based on Expectation Maximization,” *Sensors*, vol. 23, no. 3, Art. no. 3, Jan. 2023, doi: 10.3390/s23031683.