Modern Detection Techniques of False Data Injection Attacks in V2X Communication: A Critical Analysis

Thejmeela Seetamonee(✉) and Girish Bekaroo

Middlesex University Mauritius, Flic-en-Flac, Mauritius
TS984@live.mdx.ac.uk

Abstract. During the previous decade, renowned companies such as Tesla, Ford and Volkswagen have actively been researching and investing in the production of connected and automated vehicles (CAVs). The vehicle-to-everything (V2X) technology, which is used to operate CAVs, has recently gained considerable attention due to its various benefits such as improved road safety, energy efficiency and enhanced traffic efficiency on roads. A significant growth is expected in CAVs and V2X which will, however, be positively linked to an increase in the risk of cyber-attacks, notably, False Data Injection (FDI) attacks, due to their high connectivity. The aim of FDI in CAVs is to alter data and/or make CAVs unresponsive to the driver. The impact of these attacks is alarming due to the possibility of death, injury and major infrastructural damages. The ability of FDI attacks to modify or suppress data, such as speed, distance, acceleration and position of CAVs makes it even more critical to study FDI detection techniques. As such, this paper critically compares and analyses key techniques used to detect FDI attacks within V2X communication. As part of this study, five modern FDI detection techniques, notably, State Residuals-based detection, Data Fusion Algorithm, MFC-DI, History Trajectory Scheme and Machine Learning Approach were investigated in terms of their detection accuracy, time, reliability, adaptability to varying V2X environments and ability to detect new attacks.

Keywords: False data injection (FDI) · Vehicle-to-Everything (V2X) · Connected and Autonomous Vehicles (CAVs) · cyber-security · modern detection techniques

1 Introduction

In this age of intelligent mobility and automated vehicles, Vehicle-to-Everything (V2X) communication is increasingly gaining attention. The notion of "connected car", which is still at its early release stage, is enabled through wireless communication and has been designed to provide drivers with a panoply of services [1]. V2X is a wireless communication which enables vehicles to communicate with each other and with multiple components, such as physical infrastructures, road traffic signals, pedestrians and cloud computing infrastructures [2]. By allowing vehicles and infrastructures to communicate, V2X limits the risks of accidents and increases road traffic efficiency [3].

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2024
Published by Springer Nature Switzerland AG 2024. All Rights Reserved
A. Seeam et al. (Eds.): InterSol 2023, LNICST 541, pp. 66–80, 2024.
https://doi.org/10.1007/978-3-031-51849-2_5

It is expected that the market for autonomous vehicle will be at a worldwide estimation of 400bn USD by 2025 and driver-free highways will be the norm in advanced countries by 2050 [4]. With the expected increase in intelligent mobility and automated vehicles, V2X communication will be used extensively as a wireless vehicular communication [5]. Consequently, V2X communication has resulted in expanded surface attacks and with its widespread use, novel security concerns arise. Attacks along the V2X communication channel are significantly more dangerous as it is challenging for the driver to circumvent the corrupted information or to fix a bug in the automated system [6]. Therefore, it is crucial to secure the line along the V2X communication to prevent injurious attacks that hinder road safety and put people at risks. There are multiple attacks to which the V2X channel can be subject to, such as denial-of-service (DOS) attacks or integrity attacks, replay attacks and false data injection (FDI) attacks [7].

Among these attacks, FDI is becoming increasingly significant, especially with the exponential increase in the use of internet and connected devices [8]. FDI is an attack that targets sensor communication network to alter and manipulate data packets, leading to a divergence in the expected result [9]. The aim of an FDI attack is to compromise the integrity of data. FDI attacks targeting the location and speed of the vehicle have drastic consequences for road safety [7]. Hence, the timely detection and prevention of security weaknesses which may lead to FDI attacks along the communication channel is a problem that should be researched upon [10]. Therefore, the purpose of this study is to critically compare and analyse the key techniques used to detect FDI attacks within V2X communication.

The research paper is structured as follows. The next section provides a background on the key topics investigated in this paper, notably, V2X communication and FDI. Then in Sect. 3, related research pertaining to detection of FDI are discussed. Section 4 then explores the methodology utilised in order to achieve the purpose of this research paper. Section 5 is the core of the research paper, whereby the modern techniques for FDI detection in V2X are elaborated and are then critically analysed in Sect. 6. Sect. 7 provides a final note on the research paper and explores possibilities for future research.

2 Background

2.1 An Overview of V2X Communication

Since its first release as 1G-V2X (Level 1 automation level for Society of Automotive Engineers (SAE) J3016), V2X has continuously evolved over the years and its conception propelled the manufacturing of CAVs. With advancement in V2X, the need for design of new or improved messages, communication protocols, and their standardisation are becoming prerequisites [11]. Vehicle-to-everything (V2X), which refers to vehicular applications and communications technologies, is divided into four categories: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-network (V2N), and vehicle-to-pedestrian (V2P) [12]. All the components of V2X are supported by Dedicated Short Range Communications (DSRC) which is being further designed with the help of standardisation bodies, such as IEEE, the European Telecommunication Standards Institute (ETSI) and the SAE International [13].

Figure 1 shows the interaction between various components of a V2X communication, namely V2N, V2I, V2V and V2P. Vehicle-to-self (V2S) and Vehicle-to-Roadside Unit (V2R) are sub-components within V2X.

1. V2N: V2N, or wide area cellular communication, is a cellular infrastructure that allows communication between vehicles to facilitate vehicular traffic operations [14]. The primary objective of V2N is to enable constant network coverage on the streets [15].
2. V2I: The term "vehicle-to-infrastructure" (V2I) refers to communication between a vehicle and the infrastructure, known as the Roadside Unit (RSU). They can share and transmit some delay-insensitive information, such as gathered traffic data for extensive traffic monitoring [3].
3. V2V: V2V communication is used among vehicles to send brief messages, mostly geared toward enhancing road safety [16]. V2V uses mainly ad hoc networks technology to allow vehicles to communicate over a short distance [17].
4. V2P: Vehicle to pedestrian (V2P) technology is designed to help pedestrians who have physical or visual challenges by sending appropriate alerts to oncoming automobiles [18].

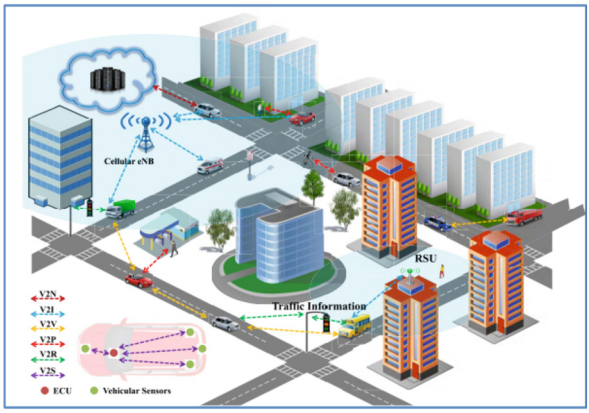

Fig. 1. An example of a V2X scenario [19]

A V2X communication system focuses on three key areas: energy efficiency, traffic efficiency, and road safety [19]. The inherent flexibility of V2X communication to adapt to any type of network, device, or data as well as to ensure the network's stability, resilience, and reliability are its most alluring advantages [20]. Additionally, V2X's role in enabling more effective vehicular transportation intervals from automated smart parking, to improved traffic flow through decreased vehicle-to-vehicle spacing on highways and coordinated intersections is crucial in today's overcrowded cities [21]. These are main reasons why V2X is becoming prevalent and is promoting autonomous driving.

However, with the extent of connectivity and autonomy provided by V2X, the need to address security and privacy concerns, including the potential identification and tracking

of specific vehicles, the fabrication and jamming of real message traffic, the threat of vehicular malware, and the potential use of vehicular botnets are crucial [22].

2.2 An Overview of FDI and Its Impact on V2X Communication

An estimate of 400 crashes of vehicles operating with partially automated driver assist systems have been recorded from July 2021 to May 2022 [23]. Most automated vehicles require symmetrical sensors that constantly transmit information, such as location, speed and the state of surrounding over a channel (V2X) to understand the immediate environment [24]. Therefore, it is imperative to secure the communication line of automated vehicles to limit unauthorised interferences, such as FDI attacks, that may lead to severe crashes and even the possibility of death.

FDI is an attack scenario whereby a rogue vehicle, which acts as an authorised one, communicates with other legitimate vehicles and sends false data about its placement, celerity and acceleration (see Fig. 2) [25].

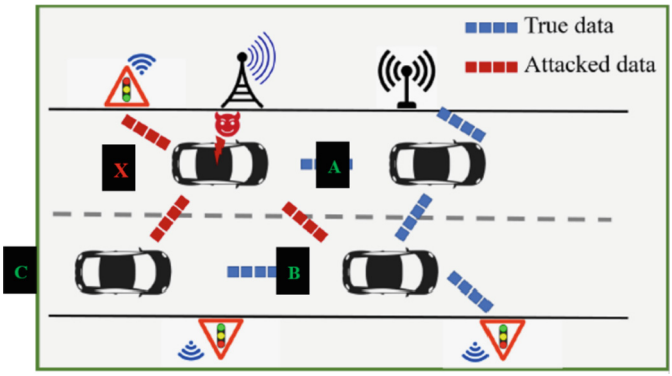

Fig. 2. FDI attacks launched by rogue vehicles [25]

In Fig. 2, there are four connected vehicles, namely A, B, C and X. Vehicles A, B and C are genuine connected cars and are transmitting true data within the environment. However, vehicle X is a malicious connected car and is transmitting distorted data, which is represented by the red dotted line. The aim of emitting distorted data is to tamper with the original state of the environment, specifically connected cars C and B and the traffic light. Therefore, FDI attacks within V2X, is simply the action of emitting distorted data to alter the original state of connected components. In the original state of the environment as depicted in Fig. 2, X is 20 m ahead of car C. However, X emits a distorted data, stating that it is 100 m behind C and can be overtaken. C would attempt to overtake and would eventually collide with X.

As further purported in a previous study, there is the possibility of collision between two connected and automated vehicles which are targeted by stealthy FDI attacks performed over V2V communication [26]. Ghost vehicles are injected into the network of connected vehicles as part of a smart FDI attack. Ghost vehicles have the ability to

impair the system performance of authentic connected vehicles, resulting in fatal collisions and worsened traffic conditions [27]. Hence, FDI attacks have a high probability of causing considerable damage to road infrastructure and serious harm to pedestrians and drivers alike. Therefore, the purpose of this research paper, which is to critically analyse the techniques for the effective detection of FDI attacks over V2X network becomes pertinent.

3 Related Works

There have been various studies conducted on the security and challenges of V2X communication channel. The studies have focussed on either the detection and mitigation of cyber-attacks along V2X or the detection of FDI attacks over the whole Intelligent Transport System (ITS). However, limited studies have been done for the timely detection of FDI attacks along V2X. Among the related works, a previous study [2] discussed the security concerns related to V2X and classified as well as analysed the various security threats into active attacks, such as FDI attacks, and passive attacks. The study explored three key terminologies related to FDI attacks as explained in Table 1.

Table 1. Terminologies related to FDI attacks [2]

Terminology	Description
Cooperative Adaptive Cruise Control (CACC)	CACC enables cars to "cooperate" by talking with one another while in adaptive cruise control mode. For instance, with CACC, a car would keep a suitable distance by slowing down once it becomes too near of the car in front of it [28]. CACC is a key function in V2X and is oftentimes the target of FDI attacks
GPS Spoofing	It is a type of FDI attack during which an attacker would insert erroneous position data by targeting the GPS simulators of victim cars
Replay Attack	It is a type of FDI attack whereby the attacker would keep an event information and resend the same delayed information which is no longer valid. For instance, at 11pm, the speed of the car was 80 km/h, the attacker would send the same data at 12pm when the car is actually driving at 100 km/h

At the end of the same study, the authors emphasised on the need to investigate on innovative security techniques created for V2X for more safety-critical and cyber-physical domains. Another paper [29] developed and assessed the effectiveness of a new state residuals-based detection technique intended to address the issue of obsolete detection techniques. In addition to detecting FDI attacks, the proposed model also

reduced the time taken to isolate the attacks. Similarly, another research proposed an attack detection decision scheme which relies on the results of the proposed data fusion algorithm applied to detect and confine the FDI attack in CAVs [30]. The proposed decision scheme was effective in identifying the rogue vehicle with a high true positive detection rate at 100% CAV penetration rate. In addition, a past study proposed a deep learning technique called Multivariate Fuzzy Clustering-based Data Imputation (MFC-DI) to identify if nodes have been compromised through FDI [31]. Another previous study proposed a scheme to detect complex attacks, such as FDI attacks, through the application of behavioural information [32]. The scheme was able to detect attacks with a probability of 97.56 in 80% of the simulated attacks. Likewise, a past research paper applied a machine learning approach, more specifically a neural network-based fault detection technique combined with a fuzzy decision system, to identify and trace FDI attacks targeting CACC [33].

Based on the previous studies, there exists several detection techniques to identify FDI attacks along V2X communication, be it for CAV or ITS. Nevertheless, limited studies have been undertaken to critically analyse existing detection approaches. Therefore, this research paper addresses this research gap to critically analyse the various modern detection techniques, as described in the following sections.

4 Methodology

The main sources of information for this research paper were research databases, such as Google Scholar, ResearchGate and IEEE Xplore. As per the title of this research paper, jargons such as "V2X", "FDI", "DSRC" and "Detection techniques" were searched among others to enhance the searches in accordance with the purpose of this research study. The most relevant and research papers published in the year 2015 and above were chosen to critically analyse the effectiveness of the selected modern proposed techniques used to detect FDI attacks along V2X. 12 applicable research papers were read and assessed to further shortlist most relevant papers based on the detection techniques applied for FDI detection. The 5 most recent research papers were shortlisted, and their proposed FDI detection techniques were thoroughly examined to perform a critical comparison of the proposed techniques. The proposed detection techniques were eventually elaborated and critically analysed through an adapted version of the criteria proposed in a previous research paper, meant for comparing attack detection mechanisms [34].

5 Techniques for the Detection of FDI Attacks in V2X Communications

Using the methodology described in the previous section, the following detection techniques are reviewed and analysed:

5.1 State Residuals-Based Detection

According to a previous study [29], State Residuals-based detection was proposed as a modern security measure to identify and confine FDI attacks. The study proposed

an attack detection logic in the form of an equation designed from multiple logical equations. The equation is as follows:

$$\begin{cases} ||R(t)|| \leq Jth \text{ Normal} \\ ||R(t)|| > Jth \text{ Attack} \end{cases} \quad (1)$$

In the above equation, R (t) refers to the norm of state estimation error and the norm of disturbance error. If the estimation error is equal to or less than the adaptive detection threshold, then the data is deemed to be a proper estimate of the transmitted data. However, if the estimation error is higher than the adaptive detection threshold, then the transmitted data is detected as an attack. Figure 3 enumerates the steps to detect the FDI attack.

Algorithm 1: State residuals-based detection of FDI attacks in vehicle networking system.

1. Input: Establish the vehicle networking model in Equations (1)–(3);
2. Design the corresponding robust state observer in Equation (9);
3. Compute the adaptive threshold in Equation (24) and residual in Equation (25);
4. for All the intelligent vehicles
   if $\|R(t)\| \leq J_{th}$ then
      No FDI attacks;
   else
      There exists the injected FDI attacks;
   end if
5. end for
6. Output: The vehicle networking system is attacked.

Fig. 3. Steps for State Residuals-based detection [29]

According to the same study [29], once the FDI attack has been detected, it should be isolated within the shortest possible timeframe. Iteratively repeating the detection algorithm for each half of the subset results in the isolation of the attacked vehicle networking sensor nodes. Therefore, the isolation range is immediately cut in half if the attack is discovered in the first subset. The suggested isolation method can hasten the separation of attacked vehicle networking sensor nodes through continual dichotomous iteration.

5.2 Data Fusion Algorithm

In another previous study [30], a data fusion algorithm has been derived from the Monte Carlo Localisation (MCL) algorithm, which consists of a collection of weighted samples (particles), each representing the position, speed and yaw angle of the vehicle. Particles alienated from the most likely state gradually dissipate while particles closer to the state combine to form an average. This principle is known as the particle filter (PF). The data fusion applies the modified version of the PF principle as shown in Fig. 4. In the same figure, the neighbouring vehicles are the samples used to provide an estimate of particle states of the ego vehicle. The neighbouring vehicles' estimation of the states of the ego vehicle are treated as further measurements since regular particles are assigned to them using stratified sampling based on their weights calculated in the first stage. This increases the reliability of the state estimation generated by the neighbouring vehicle.

Therefore, it is easier to detect an FDI attack launched by a neighbouring vehicle based on if the estimated state exceeds the threshold. The threshold is determined through statistical hypothesis testing. Based on the estimation and results of the study, the proposed data fusion algorithm was deemed to be scalable and was able to detect attacks within an average of 0.2 s with an average false alarm rate of 0.0156 over multiple CAV penetration rates.

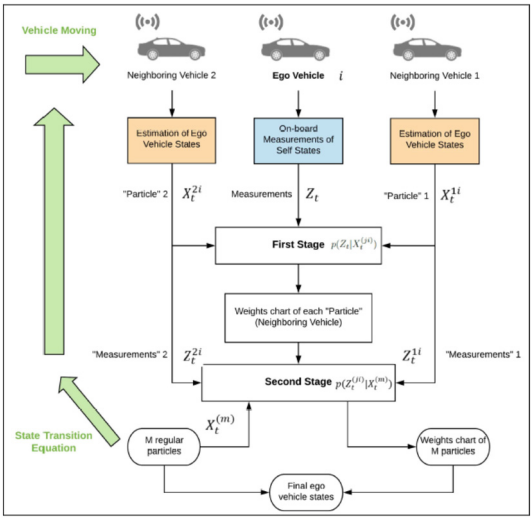

Fig. 4. Presentation of the data fusion algorithm in a two-stage architecture [30].

5.3 MFC-DI

The Multivariate Fuzzy Clustering-based Data Imputation (MFC-DI) technique was proposed by a previous study [31]. In this technique, the collected data from the ITS goes through the processes of normalisation, standardisation and imputation. First, the data is collected from neighbouring vehicles within the environment which is later used for estimation of missing values during imputation. Then data normalisation is applied based on the Min-Max formula in Eq. 2 below.

$$\overline{X} = \frac{X - Xmin}{Xmax - Xmin} \tag{2}$$

In Eq. 2, if X = Xmin, then the value is 0 while if X = Xmax, the value is 1. This allows for scaling between 0 and 1 only, whereby each attribute, such as speed, acceleration and distance are treated fairly. The data obtained during the initial stages are approximated by the MFC-DI to estimate missing data. The latter is the result of an FDI attack. This technique of imputation is used to address the possibility of missing data injection among connected vehicles. The results of the previous research work proved more effective than a mere Pearson-based missing data imputation.

5.4 History Trajectory Scheme

A previous study [32] proposed a scheme known as History Trajectory. The scheme adopts a two-step procedural security technique to identify FDI attacks. The first step is to detect normal and abnormal behavioural information. Through this first step, collisions are prevented as the autonomous vehicle is stopped when abnormal behaviour has been detected. In the second step, the attacked network communication is identified for further analysis. Current detection systems like Secure and Efficient Ad hoc Distance Vector (SEAD) and Cumulative Sum Control Chart (CUSUM) are used to identify a single assault. However, high performance computation is required as this approach calls for a thorough investigation (Fig. 5).

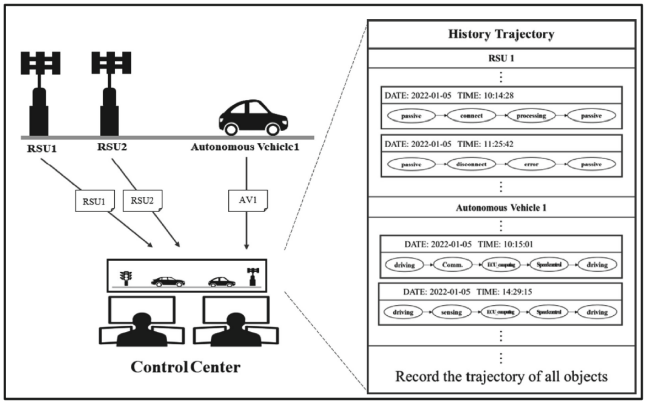

Fig. 5. Structure of the second step of the History Trajectory Scheme [32]

5.5 Machine Learning Approach (NN-Based)

According to a previous study, a neural network-based (NN-based) fault detection technique combined with a fuzzy decision system is proposed to identify and trace FDI attacks targeting CACC [33]. The proposed technique includes a bi-objective controller, a decision-making unit and a discrete controller. The bi-objective controller is in charge of adjusting vehicle speed and separation. Speed and distance errors are the controller's inputs, and its output is the braking or acceleration actuation. For the decision-making unit, a NN-based algorithm has been constructed to identify and estimate FDI attacks. The attack is identified in real time and the decision-making unit calculates a recommended safe distance (Fig. 6).

The speed of the following vehicle and the speed error—the difference between the leading vehicle's real and anticipated speed—are inputs to the proposed fuzzy system. The result is a recommended safe distance that is added to the present gap to prevent mishaps while alerts are delivered to the advisory system and the system waits for the user to take the proper action. The experiment resulted in accurate detection of the FDI attack and correction of the estimated false data transmitted.

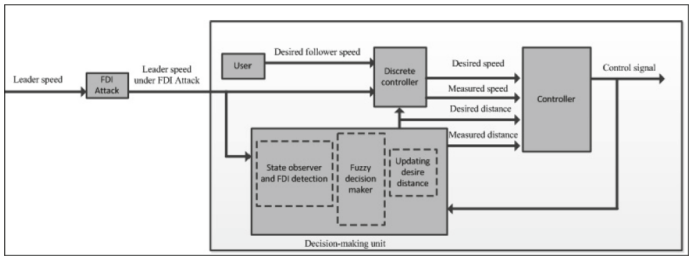

Fig. 6. Structure of the Machine Learning Approach [33]

6 Critical Analysis

The five selected modern detection techniques, explained in the previous section, are critically analysed and compared based on an adapted version of the comparison criteria used in a previous research paper [34]. This method of comparison was chosen due to its relevance in comparing attack detection techniques. As such, the following five criteria were selected to critically analyse the five modern FDI attack detection techniques, namely (Table 2):

Table 2. Criteria for Comparative Analysis

No.	Criteria	Description
C1	Detection Accuracy	The ability for the detection technique to correctly and precisely detect FDI attacks
C2	Detection Time	The time frame through which FDI attacks are detected
C3	Detection Reliability	The ability for the detection technique to detect a broad range of FDI attacks with varying parameters
C4	Adaptability to varying V2X environments	The ability of the detection technique to adapt to different V2X environments (e.g., small, and larger scales)
C5	Ability to Detect new attacks	The ability for the detection method to be adapted in order to detect new and more sophisticated types of FDI attacks targeting V2X

The selected criteria were applied to the five FDI attack detection mechanisms using the Low-Medium-High scale following review and critical analysis of published literature that refer each attack detection technique. Findings are summarised in Table 3.

As per Table 3, each detection technique was found to have its own strengths and limitations. Firstly, the State Residuals-based detection was able to effectively detect different simulated FDI attacks and showed high accuracy and reliability in detecting

Table 3. Analysis of modern FDI detection techniques

Technique	C1	C2	C3	C4	C5
State Residuals-based Detection [29]	High	Low	High	Med	Med
Data Fusion Algorithm [30]	High	High	Med	Med	Low
MFC-DI [31]	High	N/A	High	Low	Med
History Trajectory Scheme [32]	Med	Med	Low	High	High
Machine Learning Approach [33]	High	High	High	Low	High

such attacks. In addition to detecting the attack, the model was able to determine the impact of the attack on the vehicle's state. The model further developed the algorithm to also remediate attacks through isolation. Hence, algorithm 1 was applied to successfully detect the attack and algorithm 2 was applied to isolate the attack. However, the technique is not scalable and is incredibly difficult to implement in large-scale urban traffic networks, thus depicting low adaptability to varying V2X environments. The model is unreliable due to the high dispersion and hysteresis linked to a heavy-traffic network. The detection time of the model has been estimated at 58.7 s, which is higher than the other detection techniques. Finally, the detection technique also demonstrated a high ability to detect new and more sophisticated types of FDI attacks targeting V2X [29].

The Data Fusion Algorithm was tested under varying scale of attack. Results revealed that the algorithm was highly accurate based on the true positive rate and false alarm rate collected during the attack simulation. The Data Fusion Algorithm had a relatively low detection time of 0.2 s and a detection rate of 1.00 at 100% CAV penetration rate. The combination of the detection algorithm and decision-making scheme allowed the proposed technique to isolate the attacker. However, the proposed technique considered only position and velocity data as targets in the attack which were applied in the simulation of the FDI attack. The compromise of data such as relative distance and acceleration which may be compromised in some forms of FDI attacks were not considered during the simulation. Hence, its ability to detect new attacks was deemed as being low [30].

The MFC-DI involves the calculation of the missing values in addition to the values of the same attribute, unlike existing imputation methods that only consider the values of the same attributes. As a result, the MFC-DI guesses the missing values using both data from the associated attributes and data from the same attribute. This makes the MFC-DI reliable as it relies on varying parameters to detect FDI attacks. The simulation exercises for the MFC-DI did not consider the time taken to detect the attack and was thus deemed not applicable as illustrated in Table 3. While the MFC-DI can handle a V2X environment with a significant amount of adjacent missing data and surpassed results achieved using traditional Pearson correlation, the computational overhead of the multivariate approach is a potential drawback, particularly for online models that adjust to topological and environmental changes within the vehicular environment. Hence, its adaptability to varying V2X environments was deemed low [31].

During the simulation for the History Trajectory Scheme, a compound attack could be identified with an accuracy probability of 83.10% which is quite low compared to

the other four detection methods. As all the history trajectories are stored in the control centre, historical behaviour can be examined to identify sophisticated attacks. Additionally, the first procedure of the method was found to be efficient in detecting and responding to the simulated FDI attack. The proposed approach, however, struggles to handle a significant amount of security knowledge; whereby, as security knowledge grows, the detection time increases since multiple situations must be identified. Furthermore, high-performance computer is necessary since this detection approach necessitates considerable analysis [32].

The Machine Learning approach and neural networks (NN) are effective for defect detection within the data collected, which facilitates function categorisation and approximation, as well as handling non-linearity and uncertainty. The NN-based method, hence, aids in not only the precise detection of FDI attack but also its high reliability. Additionally, under the ML approach, the attack is detected in real-time; hence the NN-based algorithm is able to detect the FDI attack as soon as it is occurring. The proposed method also changes based on the car's speed in accordance with the degree of errors in the distance estimations and the braking of the leading vehicle. In the NN-based algorithm, the ML can detect various types of FDI attacks which the targeted vehicle is subjected to as it relies on the nonlinear system. However, the attack was simulated within only a platoon of vehicles which normally has a leading vehicle and follower vehicle(s). The proposed method has yet to be tested within an environment where the CAVs do not operate in a platoon system [33].

All the studied FDI attack detection mechanisms were found to have respective limitations as illustrated in Table 3 and as discussed above. For instance, although the State Residuals-based Detection method was found to have medium-high scores in most criteria studied, it was rated low for "Detection Time" as the latter was higher than what was recorded for the other four detection techniques. Similarly, the Data Fusion Algorithm was deemed low for the ability to detect new attacks as not all data related to the vehicle, such as relative distance and acceleration, were considered as main points of FDI attacks. Overall, the ML approach has a higher combined results as compared to the other four detection techniques. However, this approach has not yet been applied within other large-scale V2X environments. It has yet to be fully relied upon for implementation within a real-world scenario. To overcome this limitation, the ML approach could be further developed and tested within several V2X environments, although more data will be required to further train and enhance existing detection models built within.

Even though the analysis revealed insightful findings as discussed above, this study is still undermined by a few limitations. Firstly, the comparative analysis was performed using literature analysis where simulation of the different detection techniques could yield varying results. Moreover, other aspects such as performance, efficiency, and data quality attributes, among other parameters could have been investigated in order to broaden the analysis and gather more critical insights.

7 Conclusion

V2X communication is increasingly gaining attention in this era of intelligent mobility and automated vehicles. Although V2X communication has significantly improved since its conception, there are still further research works being done on how to make V2X

more scalable and stable, especially with the expected rise in CAV in the coming years. As any advancements in the IT industry, V2X and CAV are not without vulnerabilities and are often exploited by attackers. CAV are specifically vulnerable to FDI attacks. FDI attacks have a high likelihood of seriously harming both drivers and pedestrians while also causing significant damage to road infrastructure and the surrounding environment. Due to the alarming consequences of FDI attacks in V2X communication, this research study critically analysed the modern techniques used to detect FDI attacks, notably, State Residuals-based Detection, Data Fusion Algorithm, MFC-DI, History Trajectory Scheme and Machine Learning Approach. These detection mechanisms were analysed in terms of their detection accuracy, time, reliability, adaptability to varying V2X environments and ability to detect new attacks. It was found that all detection mechanisms have their own limitations pertaining to the criteria studied as none of them were able to achieve the highest scores in all the criteria. Among the approaches studied, machine learning scored the highest, although it showed low adaptability to varying V2X environments. Since this study did not perform a practical quantitative comparison of the five modern detection techniques, this limitation could be further explored in future research works.

References

1. Seo, H., Lee, K.D., Yasukawa, S., Peng, Y., Sartori, P.: LTE evolution for vehicle-to-everything services. IEEE Commun. Mag. **54**, 22–28 (2016)
2. Hasan, M., Mohan, S., Shimizu, T., Lu, H.: Securing vehicle-to-everything (V2X) communication platforms. IEEE Trans. Intell. Veh. **5**(4), 693–713 (2020)
3. Saulaiman, M.N.E., Kozlovszky, M., Csilling, A.: A survey on vulnerabilities and classification of cyber-attacks on 5G-V2X. In: IEEE 21st International Symposium on Computational Intelligence and Informatics, Budapest (2021)
4. Statista. Projected autonomous vehicle market size worldwide between 2021 and 2025. Statista (2020). https://www.statista.com/statistics/1224515/av-market-size-worldwide-forecast/. Accessed 07 Nov 2022
5. Lozano Domínguez, J.M., Mateo Sanguino, T.D.J.: Review on V2X, I2X, and P2X communications and their applications: a comprehensive analysis over time. Sensors **19**(12), 2756 (2019)
6. Petit, J., Shladover, S.E.: Potential cyberattacks on automated vehicles. IEEE Trans. Intell. Transp. Syst. **16**(2), 546–556 (2015)
7. Chattopadhyay, A., Mitra, U., Ström, E.G.: Secure estimation in V2X networks with injection and packet drop attacks. In: 2018 15th International Symposium on Wireless Communication Systems (ISWCS), pp. 1–6 (2018)
8. Ahmed, M., Pathan, A.-S.K.: False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure. Complex Adapt. Syst. Model. **8**(4), 2–14 (2020)
9. Mode, G.R., Calyam, P., Hoque, K.A.: False data injection attacks in internet of things and deep learning enabled predictive analytics. In: 32nd IEEE/IFIP Network Operations and Management Symposium (NOMS 2020), Hugary (2019)
10. Ullah, H., Nair, N.G., Moore, A., Nugent, C., Muschamp, P., Cuevas, M.: 5G communication: an overview of vehicle-to-everything, drones, and healthcare use-cases. IEEE Access **7**, 37251–37268 (2019)
11. Hobert, L., Festag, A., Llatser, I., Altomare, L., Visintainer, F., Kovacs, A.: Enhancements of V2X communication in support of cooperative autonomous driving. IEEE Commun. Mag. (ComMag) **53**(12), 64–70 (2015)

12. Sun, S.H., Hu, J.L., Peng, Y., Pan, X.M., Zhao, L., Fang, J.Y.: Support for vehicle-to-everything services based on LTE. IEEE Wirel. Commun. **23**(3), 4–8 (2016)
13. Chen, S., Hu, J., Shi, Y., Peng, Y., Fang, J., Zhao, R., Zhao, L.: Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G. IEEE Commun. Stand. Mag. **1**, 70–76 (2017)
14. Tahir, M., Leviäkangas, P., Katz, M.: Connected vehicles: V2V and V2I road weather and traffic communication using cellular technologies. Sens. (Basel) **22**(3), 1142 (2022)
15. Saeed, U., Hämäläinen, J., Mutafungwa, E., Wichman, R., González, D., Garcia-Lozano, M.: Route-based radio coverage analysis of cellular network deployments for V2N communication. In: International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona (2019)
16. Sanguesa, J., et al.: Sensing traffic density combining V2V and V2I wireless communications. Sens. (Basel) **15**(12), 31794–31810 (2015)
17. Santa, J., Gómez-Skarmeta, A.F., Sánchez-Artigas, M.: Architecture and evaluation of a unified V2V and V2I communication system based on cellular networks. Comput. Commun. **31**(12), 2850–2861 (2008)
18. Gupta, M., Benson, J., Patwa, F., Sandhu, R.: Secure V2V and V2I communication in intelligent transportation using cloudlets. IEEE Trans. Serv. Comput. **15**, 1912–1925 (2020)
19. Tong, W., Hussain, A., Bo, W.X., Maharjan, S.: Artificial intelligence for vehicle-to-everything: a survey. IEEE Access **7**, 10823–10843 (2019)
20. Khan, M.A., et al.: Robust, resilient and reliable architecture for V2X communication. IEEE Trans. Intell. Transp. Syst. **22**(7), 1–18 (2021)
21. Boban, M., Kousaridas, A., Manolakis, K., Eichinger, J., Xu, W.: Use cases, requirements, and design considerations for 5G V2X. arXiv preprint arXiv (2017)
22. MacHardy, Z., Khan, A., Obana, K., Iwashina, S.: V2X access technologies: regulation, research, and remaining challenges. IEEE Commun. Surv. Tutor. **20**(3), 1858–1877 (2018)
23. The Associated Press. Nearly 400 car crashes in 11 months involved automated tech, companies tell regulators. NPR (2022). https://www.npr.org/2022/06/15/1105252793/nearly-400-car-crashes-in-11-months-involved-automated-tech-companies-tell-regul. Accessed 28 Nov 2022
24. Alsulami, A., Abu Al-Haija, Q., Alqahtani, A., Alsini, R.: Symmetrical simulation scheme for anomaly detection in autonomous vehicles based on LSTM model. Symmetry **14**(7), 1450 (2022)
25. Koley, I., Adhikary, S., Rohit, R., Dey, S.: A CAD framework for simulation of network level attack on platoons. arXiv (2022)
26. Yang, T., Murguia, C., Lv, C.: Risk assessment for connected vehicles under stealthy attacks on vehicle-to-vehicle networks. J. Latex Class Files **14**(8), 1–12 (2020)
27. Biroon, R.A., Biron, Z.A., Pisu, P.: False data injection attack in a platoon of CACC: real-time detection and isolation with a PDE approach. IEEE Trans. Intell. Transp. Syst. **23**(7), 8692–8703 (2022)
28. UC Berkeley. Cooperative Adaptive Cruise Control. UC Berkeley | Institute of Transportation Studies (2022). https://path.berkeley.edu/research/connected-and-automated-vehicles/cooperative-adaptive-cruise-control. Accessed 25 Dec 2022
29. Huang, X., Wang, X.: Detection and isolation of false data injection attack in intelligent transportation system via robust state observer. Processes **10**, 1–13 (2022)
30. Zhao, C., Gill, J.S., Pisu, P., Comert, G.: Detection of false data injection attack in connected and automated vehicles via cloud-based sandboxing. IEEE Trans. Intell. Transp. Syst. **23**(7), 9078–9088 (2022)
31. Almalki, S.A., Sheldon, F.T.: Deep learning to improve false data injection attack detection in cooperative intelligent transportation systems. In: 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver (2021)

32. Chung, W., Cho, T.: Complex attack detection scheme using history trajectory in internet of vehicles. Egypt. Inform. J. **23**, 499–510 (2022)
33. Sargolzaei, A., Crane, C., Abbaspour, A., Noei, S.: A machine learning approach for fault detection in vehicular cyber-physical systems. In: 15th IEEE International Conference on Machine Learning and Applications, Anaheim (2016)
34. Shurman, M.M., Khrais, R.M., Yateem, A.A.: IoT denial-of-service attack detection and prevention using hybrid IDS. In: 2019 International Arab Conference on Information Technology (ACIT), Al Ain (2019)