Mehran University Research Journal of Engineering and Technology

https://doi.org/10.22581/muet1982.2303.09

2023, 42(3) 79-88

Artificial intelligence (AI) empowered anomaly detection for autonomous vehicles in 6G-V2X

Irfan Ali Kandhro [a, *], Fayyaz Ali [b], Ali Orangzeb Panhwar [c], Raja Sohail Ahmed Larik [d], Kanwal Fatima [a]

[a] *Department of Computer Science, Sindh Madressatul Islam University, Karachi Sindh Pakistan*

[b] *Department of Software Engineering, Sir Syed University of Engineering and Technology, Karachi Sindh Pakistan*

[c] *Department of Computer Science, Shaheed Zulfikar Ali Bhutto Institute of Science and Technology Gharo Sindh Pakistan*

[d] *School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing, 210094, P.R. China.*

[*] Corresponding author: Irfan Ali Kandhro, Email: irfan@smiu.edu.pk

Received: 29 January 2023, Accepted: 26 June 2023, Published: 01 July 2023

K E Y W O R D S

Artificial Intelligence (AI)

6G-V2X

Vehicle-to-everything (V2X)

Intelligent reflective surfaces Autonomous Vehicles

Multi-Agent Reinforcement Learning

Maximum Entropy Inverse Reinforcement Learning

A B S T R A C T

The development of advanced Intelligent Transportation Systems has been made possible by the rapid expansion of autonomous vehicles (AVs) and networking technology (ITS). The in-vehicle users' increased data needs from AVs put the vehicle's trajectory data in danger and make it more susceptible to security threats. In this paper, Autonomous vehicles (AVs) transform the intelligent transportation system by exchanging real-time and seamless data with other AVs and the network (ITS). Transportation that is automated has many advantages for people. However, worries about safety, security, and privacy continue to grow. The AVs need to exchange sensory data with other AVs and with their own for navigation and trajectory planning. When an unreliable sensor-equipped AV or one that is malicious enters connectivity in such circumstances, the results could be disruptive. To effectively detect anomalies and mitigate cyberattacks in AVs, this study suggests the Efficient Anomaly Detection (EAD) method. The EAD technique finds and isolates rogue AVs using the Multi-Agent Reinforcement Learning (MARL) algorithm, which operates over the 6G network to thwart modern cyberattacks and provide a quick and accurate anomaly detection mechanism. The expected outcomes demonstrate the value of EAD and have an accuracy rate that is 8.01% greater than that of the current systems.

1. Introduction

Automotive technology is identified as a key feature of Intelligent Transportation Systems and is one of the most modern fields of study in the last ten years. A multitude of advantages for sustainability, accessibility and security is provided by autonomous vehicles (AVs), which have the potential to totally revolutionize the ITS industry [1]. To collaborate and communicate with one another as well as with the transportation infrastructure, AVs use wireless technology [2]. Moreover, Dedicated Short-Range Communications and different kinds of communications technology are used by Roadside Units (RSUs) and AVs so they can continuously connect and acquire information such as speed, distance, braking

condition, traffic light status, and so on [3]. The Cellular Vehicle, also known as (C-V2X) is necessary to ensure the flawless connection between Avs to synchronize the driving trajectories and exchange real-time data. However, to make 6G-V2X interaction extremely efficient and competent and to concurrently enable quick, incredibly dependable, and a latency limit massive communication, sixth generation (6G) technology is likely to be V2X compliant in the future [4]. In addition, more spectrum is supported by 6G, allowing for a great amount of fully connected autos, and meeting the framework's stricter requirements for dependability, latency, and efficiency for attack detection. A must-have for critical V2X services, including automated driving, safety, and effective security measures, is avoiding an abrupt session stoppage. Therefore, raising the quality of service is a vital problem to consider. Additionally, tactile connections with extremely fast and limited connectivity are needed by the AVs in the framework to enable dependable and real-time information transmission. The training devices have local storage for all the vehicular data, which must be fetched to process the important data. Finding abnormalities in the real-time data from the AVs is both a crucial and difficult task because these data are important for making significant choices. It's important to find the problem and eliminate the undesirable facts from the decision-making process [4]–[9]. The discovery technique proposes two mistakes: unfavourable effects and false advantages. It is simple to understand how a mistake could result in inaccurate data having an impact on traffic planning and perhaps having disastrous effects [10]. Even if it is less obvious, making a mistake can still have a big impact. The structure of visual information has suddenly changed because of the following hypothetical real occurrence on the network. an AV experiences a sudden shift, maybe due to a failure and causing data loss, the program may cease to timely and effectively respond to such sudden network changes, thus putting users in danger [11]. To prevent this kind of positive error, AV must use greater bandwidth information in its system of error detection. The Algorithms for detecting errors must distinguish between sensor and noise in the transmission channel, which increases the possibility of missing values and communication delays in the obtained data in addition to distinguishing between real network situations and malformations [12]. A group of scattered enterprises as agents—that make decisions on their own and interact in a common space are referred to as a multi-agent system. Each agent works toward a distinct goal that may need a variety of skills. Depending on the purpose, complex interactions between agents may develop, leading to inter-agent cooperation or rivalry. It can be difficult to define a posterior approach in complex systems. The Agents must therefore be capable of learning and adapting with time [4], [13], [14]. The branch of study known as "inverse reinforcement studies" looks at how an agent's aims, beliefs, or rewards are affected by how well it performs. [4], [15], [16]. Inverse reinforcement learning (IRL) is employed in the environment described above. To boost efficiency and precision in AV anomaly detection, we present a Hybrid Deep Anomaly Detection also known as (EAD) architecture on a 6G-V2X network that combines IRL hosting with multi-agent Learning. The framework does lessen a network's absolute catastrophic failure and stops many modern attacks including Distributed Denial of Service attacks. A variety of disruptive technologies, such as more reliable decision-making, effective air interfaces, computation, and resource allocation, will need to be integrated into 6G to accomplish the ambitious goals.

The research develops a benchmark by using the IoT with Consortium network environment as the baseline technique. In proposed approach, a number of factors led to the decision of the IoT with V2X as the baseline strategy. First off, the connection between autonomous vehicles within the 6G network environment is greatly facilitated by the IoT with V2X. It is a crucial part of a dependable and effective data sharing system. In addition, the IoT with V2X provides a variety of openly available resources, such as infrastructure, tools, and statistics. The implementation and assessment of the baseline plan are considerably aided by these easily accessible materials. This pragmatism makes it possible to create a reliable baseline and conduct fruitful comparison analysis.

Fig. 2 depicts a 6G-V2X system that supports a range of advanced use cases using several vehicular communication technologies. Low-earth orbit satellites and UAVs may substantially expand and seamlessly extend the scope of V2X systems, aiding in raising the quality of communication, especially in some possible blind spots that conventional terrestrial communication systems may experience. V2X communication devices will benefit from edge/fog computing, caching, and enhanced decision-making for longer battery life and faster computation. To attain cheap setup costs, extremely high data rates, improved security, and low power consumption, classical RF-based communications will coexist alongside visible light communication (VLC)-aided V2X communications.

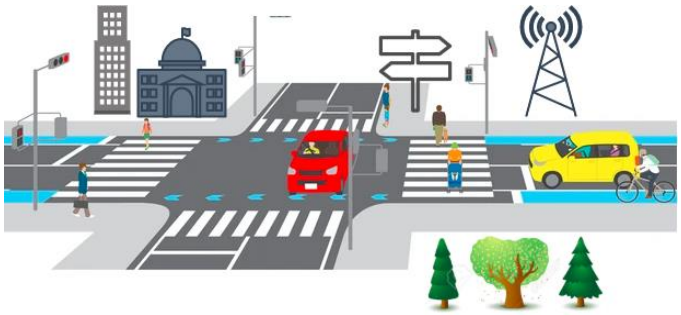

Fig. 1. V2X Communications Atmosphere

The main contributions and objectives of paper:

1. A decentralized 6G network is offered by Multi-Agent Reinforcement Learning (MARL) to prevent a catastrophic EAD failure. Anomaly detection is extremely precise thanks to the MARL algorithm, which allows several AVs to identify unusual behavior.
2. To identify the aberrant behavior and the AVs that relate to it, the Maximum Entropy IRL (MaxEntIRL) methodology is used to compare the sensory data from the present and the past. Using MARL, malicious AVs can be categorized according to the severity of their abnormal behavior. This guarantees that attack mitigation will happen quickly and effectively.

The following sections make up the remainder of this paper. The relevant current works are represented in Section 2. Section 3 presents the suggested working environment and discusses the Intrusion Detection System (IDS) implementation, as well as the vulnerabilities and attack scenario. In section V, the suggested hybrid learning EAD framework for sensor identification is shown. Section shows the simulation results and explains the efficiency obtained.

2. Related Work

Finding attacks in intra-vehicle networks is the focus of many research projects [17]. Real-world and academic studies have shown several AV threats [18], [19]. To improve AV security and protect passengers and drivers from dangers, numerous studies and solutions have been carried out for security systems [20], [21]. Numerous applications, including intrusion detection, surveillance, and diagnosis, make use of techniques for spotting anomalies. Appropriate configuration management procedures can be put in place to avoid or reduce potential responsibility if the cause of an anomaly is quickly identified [22], [23]. In recent years, numerous methods for spotting aberrant behavior and figuring out what caused it has been created. To detect anomalies, the One-Class Support Vector Machine is modified, and sensor inputs are collected using an Adaptive Extended Kalman Filter (AEKF), however, it primarily focuses on the delay of time [24]. Numerous circumstances can affect sensor readings, leading to the acquisition of false data [25]. For example, aging sensors and atmospheric instability may make failure more likely. Other reasons for inaccurate data reporting include tripping, a shaky cable connection, inadequate battery power, and unusually large variations in sensor readings or noise. Anomalies in sensor measurements can also be caused by malicious attacks [26]. Advanced threat surfaces that can be used by hostile actors to access and corrupt AVs come in many different forms. Two of the most dangerous potential AV attacks are the injection of false information and the poisoning of map databases. Even though insertion attacks can be recognized using message entropy, assaults that change the content of messages cannot be assessed using this method [27]. In multiple research investigations, the widely used classification technology Support Vector Machine (SVM) surpassed traditional learning techniques. The SVM has a high detection rate for unknown assaults and can recognize the data fields. bypassing the limitations of conventional machine-learning detection algorithms. However, only a small number of individual attacks have had the effectiveness of this method proven [28, 29]. The Long Short Term Memory technique is utilized for signal extraction and real-time classification [30]. To obtain a promising performance a multistage attention method is used for both types of anomalies [31]. However, a source rating blockchain-based approach is created to promote data integrity and fair evaluation requirements to improve the usage of crowdsourced data and data screening [32]. To facilitate the evaluation of protective measures, supervised methods are adopted that integrate plausibility checks with the data-centric misbehaviour detection model [33]. The Internet of Moving Things anomalies are found using the Moving Things Outlier Detection (MTOD) method. MTOD considers both the location and distance of moving objects [34]. The disparity between the data from various sensors is designed to be monitored by an auxiliary detector. It combines observations from numerous sensors using a combination of a Cumulative SUM (CUSUM) and

an Extended Kalman Filter (EKF) discriminator [35]. The real-time detection of the irregularities in this case is predicated on the vehicle's decision to accelerate. The data from the leader is used by a kinematic model in [36] to identify any unexpected deviations. The advantage is taken by a sensor fusion technique of the same physical variable as determined by the attacks of multiple sensors in a platoon [37]. As a result, performance deterioration is decreased [37]. To minimize the computational overhead, the sensors are placed in a ring shape [38]. Although mitigating sensor anomalies in AVs and detecting them can have serious consequences, there are no anomaly detection algorithms in the ITS literature [39]. Cyber-security in AVs or ITS in general has not been the subject of many investigations. Most previous works focus on a single element solely rather than considering a variety of impact parameters including time, attack duration, attack kind, etc. Major studies rely on a few simple machine learning techniques, which pay little attention to attack detection and what happens once an attack occurs. Additionally, the available studies solely focus on a select few impact factors and do not suggest any remedial actions. The EAD model, a hybrid deep learning framework, is used in this study to identify and categorize anomalies. The concerned AV is isolated from the system in the planned research to assure security, and after it is determined to be secure, it is added to the network.

Table 1

V2X communication and detection mechanisms

Reference	Approach/Decision	Main Idea/Objective	Types of Defence Attacks	Limitations
Grover et al. [39]	OBU-C (Data-centric)	Focuses on V2X neighbour-set with multiple vehicles.	The Sybil-attack	Feasible false and true errors with no prevention
Zhou et al. [40]	RSU(Entity-centric)	Hash function with Pseudonyms to common values	The Sybil-attack	Not covering the privacy preservation of central authority.
Kerrache et al. [41]	Entity (data-centric)	Vehicle misbehavior is eliminated via a trust-based data verification and routing method.	Packet flooding (Dos)	The Sneaky attackers bypass detection process
Hortelano et al. [42]	OBU-L, OBU	Predict behavior with the help of watchdog	DoS (malicious packet dropping/forwarding)	There is no mention of privacy, and it just looks for illicit packet forwarding.
Daeinabi et al. [43]	Data-Centric (OBU-C and RSU)	Expected behavior of the neighbors with watchdog	Malicious packets with forwarding and dropping	Only detects malicious attacks with forwarding.
Hamieh et al. [44],	Entity-centric (OBU-L)	The Detect patterns and information in radio interference legitimate cases.	Jamming with DoS	Only DOS, no attacker identification
Ruj et al. [45]	Data-centric (RSU and OBU-L)	To determine whether such occurrences occurred, keep an eye on the signals and compare them to a behavioral model that is expected.	Position cheating (Sybil attack)	Performance test with Unrealistic assumptions, no validation
Golle et al. [46]	Sybil-attack	Compare the resurrected data to the predicted model.	Data-centric (OBU-C)	Require an appropriate model to compare to; no validations or performance tests are run.

There are two further categories of entity-centric detection methods: (a) behavioural (for example, observing trends in the behavior of nodes at the protocol level), and (b) trust-based (e.g., evaluation of trust-score, often using a central authority to remove malicious nodes). Data-centric techniques compare the information received with the information previously known from previous history or behavior, like intrusion detection in traditional computing systems. These strategies can either be (a) model-based (verifying if the data communicated from a certain sender is consistent with the model) or (b) consistency-based (e.g., use the information of packets – generally from multiple participants – to determine the trustworthiness of new data). We draw attention to the fact that normally orthogonal detection techniques for entities and data, and that researchers frequently suggest combining the two. Detection methods either (a) local (i.e., performed close to where the vehicle is, say by its OBUs, and unaffected by detection methods in other cars; or (b) cooperative (detection depends on cooperation between vehicles/RSUs) depending on the scope. OBU-based techniques do not require specialized infrastructure, Comparatively to RSU-based mechanisms (e.g., vehicles performing situation evaluation by themselves without any infrastructure). Researchers have also suggested hybrid systems where misbehaviour detection is shared by RSU and OBUs (see Sections VI and VII). While consistency and trust-based schemes rely on collaboration among vehicles/RSUs to uncover inconsistencies, behavioural and plausibility methods often function locally. For more precise detection, numerous consistency-based methods can be applied locally, however, doing so exposes them to Sybil attacks. Table 01 summarized how to protect V2X communications from various types of attacks.

3. Experimental Procedures

The EAD framework, which offers inter-vehicle sensor systems on a 6G network with the highest level of security, is described in this section. Fig. 1 presents the MARL architecture. MaxEntIRL and multi-agent reinforcement learning are installed in the sensor network over the AV Network (AVN). A 6G network is used to host the AVN to minimize latency difficulties and guarantee speed and effectiveness. The sensor network operation will be split among the various AVN agents using multi-agent reinforcement learning. In an AVN context, numerous agents will communicate and share characteristics like lane topology and wheel speed. A total cascade failure will be prevented by this ability to keep shared data. The robustness and dependability of the framework will also be guaranteed by the usage of 6G. To detect malicious and anomalous activity quickly and accurately, EAD combines IRL with multi-agent reinforcement learning and maximum entropy. This component's goal is to train the AVs of a particular network to recognize malicious and trustworthy AVs by using the shared sensor network data. A decentralized approach like this prevents modern impersonation and stops hostile attackers from using brute force to break network encryption. Such modern cyberattacks are susceptible to current deep learning systems. Therefore, MaxEntIRL offers an effective defence against such attacks when other models fall short. Once a malicious AV has been correctly discovered using the hybrid technique, its reward function is tweaked using MaxEntIRL. This method carefully alters the incentive system of the malicious AV to progressively scale back its privileges. The reward feature will make the malicious AV effective again. It will start distributing healthy data over the network after the AV problems have been fixed. Other agents will perceive such a healthy transmission, which will set off the tweaking of the reward function and eventually restore the infected AV's capabilities. Thus, the EAD framework offers anomaly mitigation and detection that is dependable, secure, and safe while preserving the robustness of the system, successfully defending the system against assaults that the existing anomaly detection models are unable to handle. The hybrid architecture's process is shown in Fig. 2.

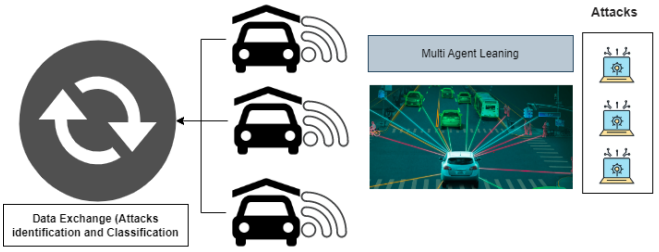

Fig. 2. Workflow of Reinforcement based Anomaly detection approach

The general architecture and AV attack scenarios are protected by the IDS. Internal attacks usually target the onboard diagnostics interface to take control of the CAN nodes, transmit accepting false CAN messages into the AVs, and perform illegal acts like abrupt braking. Cyberattacks are launched by external attackers via a variety of wireless interfaces, including cellular networks, Bluetooth, WiFi, etc. The proposed IDS can be installed in multiple places throughout AVNs to find, categorize, and deal with threats for a secure IoV platform. In this setup, The CAN bus has an IDS installed on top of it to detect malicious

communications. The IDS will also transmit messages if the signal level drops after increasing since messages are forwarded to every node. Further, the IDS examines the spot intrusions and packets. All nodes will emit alarms if any incursion is discovered. The recommended IDS will identify and categorize any attack attempted by delivering a significant amount of malicious traffic, against an AV system. The alarm is subsequently set off, and access for the attacker is forbidden. Moreover, the network is disconnected after the identification of malicious traffic. To assist with a variety of activities, modern AVs usually feature 100 Electronic Control Units (ECUs). A communication protocol for buses called CAN creates an international standard for reliable and seamless connectivity between ECUs within vehicles. AVs have numerous control modules added for security, efficiency, and performance.

These modules greatly enhance AV performance by combining better prediction with extra components as required. Through a CAN communication system, the AV system regulates internal communications and modulates signals from the control units. The Data is sent and received over a network of parallel ECUs through the CAN communication system, which functions as a multi-master system. The ECU nodes do not include the sender's and recipient's addresses in a CAN message. The other ECUs go into reception mode when one ECU transmits a message. The transmitted CAN message is recognized by the ECU if it receives it; otherwise, it is disregarded. CAN-Low and CAN-High are the two signals on the CAN-bus. The priority increases with decreasing CAN ID values. In the event of a crash during message delivery, low-value IDs are therefore permitted. Based on the bus cycle of CAN, low-priority messages are subsequently broadcast again. However, because of its lack of security features, broadcasting distribution method, and unprotected priority system, CAN is vulnerable to numerous cyber-attacks. The attacks using message injections are the primary focus of this investigation. The most frequent intra-vehicle attack is a message injection, with fuzzy, spoofing, and DoS attacks as its three main targets. Massive high-priority messages flood the CAN during a DoS attack, delaying or denying other valid communications. Fuzzy attacks cause randomly generated communications to contain arbitrary false identities or packets, which causes compromised vehicles to exhibit unexpected actions like abrupt braking. It is common knowledge that spoofing attacks inject messages with certain CAN IDs seem to be authorized and authenticated to take command of the vehicles.

The agent AVU in the HDAD approach follows a strategy that improves the value function by locating anomalies during data transfer. An explanation of multi-agent reinforcement learning is provided using the process of modified Markov decision. It is possible to write the mMDP simply (S; A; R; ϕ) for M agents, where state space is represented by the symbol S, action space is represented by the symbol A, rewards space is represented by the symbol R, and transition probability space is represented by the symbol ϕ. The agent AVU monitors the environment's current state st at each interval of time t before acting in accordance with the policy (A|s) at that moment. The agent is dispatched to the following state (st + 1) after receiving a reward of rt. Below is a list of the reward, action, and state space. The various services' utility features frequently differ. The state should therefore use the inclusion of the selection component, μm, to show how AVUs can be used in a heterogeneous binary manner. Any agent's power and channel limitations have an impact on its utility function. Each agent's ability to perform its utility function depends on the power and channel restrictions it has.

Additionally, the state space of the multi-agent can be described as S= {s1, s2,., sm}. The State includes dimensions of the vector ηm and the continuous discrete variables. Moreover, the spread of their input data and scalability can affect neural networks so normalization is essential. The min-max normalization is used prior to the learning algorithm receiving the state to improve the training process.

4. Result and Discussion

The experiment was carried out using an Intel Core i7 processor running at 3.5 GHz, 6 GB of RAM, and an NVIDIA GPU. Python is utilized to implement the model utilizing DL frameworks like Keras. The dataset used in this study includes several fields pertaining to vehicle dynamics, trajectory data, and GPS information. The Deep Deterministic Policy Gradient (DDPG) algorithm's performance is optimised by tuning hyperparameters to maximise total rewards and preserve a stable policy. A batch size of 50 is used during training for 4 episodes spread across 20 epochs. The actor network's input layer has 15 feature state vectors, while the critic network's input layer has an action vector. These components make up the neural network architecture used in the DDPG algorithm. In comparison to the critic network, which contains two fully connected layers with 600 neurons, the actor network has two fully

connected layers with 300 neurons. The dataset also contains trajectory data, which is a time-series dataset made up of arranged item positions. In this paper, Multi-Agent Reinforcement Learning (MARL) algorithms have been applied to issues including anomaly detection and categorization in a variety of disciplines. The DL-based Multi-Agent Reinforcement Learning (MARL) algorithm a model for identifying AV abnormalities is proposed in this paper. An instantaneous anomaly type is used to train the DL-MARL model, and the hyperparameters are tuned using a DL technique, both of which contribute to increased accuracy. An analysis of the suggested efficiency of the work on the test results was done using a confusion matrix. The columns of the confusion matrix contain information about the predicted class, whereas the rows reveal details about the true class. True Positive (TP), True Negative (TN), False Positive (FP), and False Negative are the four outputs of this matrix (FN). TP indicates that the outcome falls under the positive class category if it is positive. TN indicates that the outcome falls under the negative class category if it is negative. If the outcome is negative, according to FP, it belongs to the category of the positive class. If FN predicts a negative outcome, the class category for that result is negative. Each class has a different number of FNs and FPs because of differences in the classes and the volume of data sets. The suggested model's confusion matrix for Adam optimizer-based anomaly detection is shown in Fig. 3. The FP, FN, TN, and TP norms can be found using the confusion matrix for each position on the test dataset.

Table 2

Confusion matrix for the DL- MARL

True C / Predict C	Anomaly	Not Anomaly
Anomaly	2701	7933
Not Anomaly	173	503

In Fig. 3, showed the performance of proposed model with respect to accuracy, precision, and recall, it showed that model depicts the true and false predication with (AV1-AV3). The accuracy of is quite well as compared to the precision and recall.

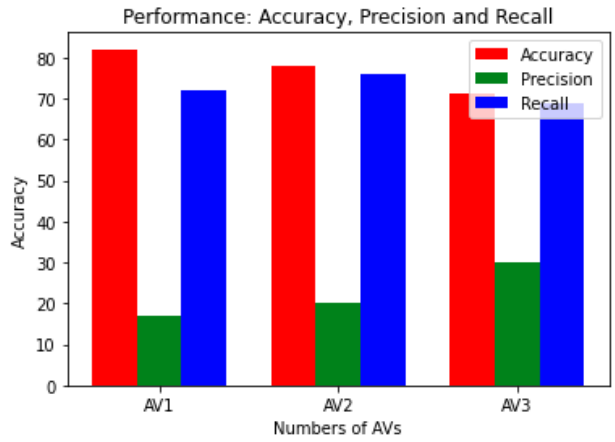

Fig. 3. Accuracy, Precision and Recall of model with AV1-AVs3

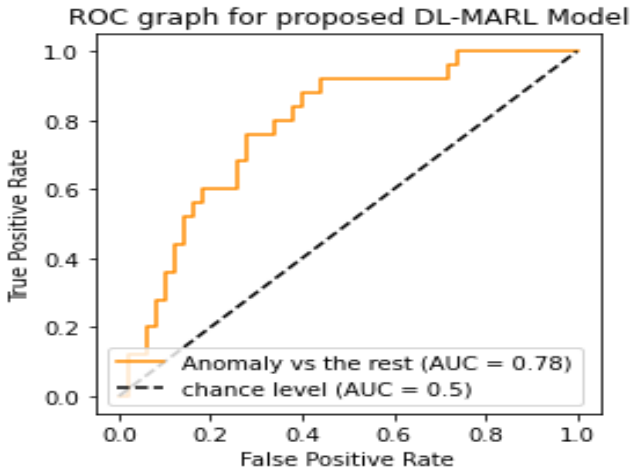

Fig. 3. Accuracy, Precision and Recall of model with AV1-AVs3

When compared to the previous work, the suggested work accurately detects the abnormality in AV, as shown by the ROC curve in Fig. 4 which is closer to the top left corner. To separate the signal from the noise, The True Positive Rate (TPR) is plotted versus the False Positive Rate (FPR) over several threshold levels using a probability curve ROC. To separate the signal from the noise, the True Positive Rate (TPR) vs the False Positive Rate (FPR) is plotted on a probability curve called (ROC).

Table 3. showed the performance of the model with random samples from the dataset for detection in AVs. The model uses 03 hyperparameters such as start time, acceleration values, and lateral GPS_time from AV. Since there is a sudden significant shift in the values of these three data points, the moment an anomaly in AV is found.

Table 3

Attacks detection of DL- MARL Model on Random Samples.

Start Time	GPS_Time	Speed	L_ Accuracy
12:01:31	48.803	1.2451E+12	1001
13:01:32	49.802	1.2455E+12	2001
08:01:32	47.113	1.2241E+12	1001
22:01:31	51.999	1.2441E+12	1001
14:01:32	48.803	1.2425E+12	2001

4. Conclusion

Vehicle-to-everything (V2X) communication platforms are made possible by contemporary vehicular wireless technology, which enables cars to communicate information at any time, from any location to any network. V2X applications have advantages, but they also have a lot of risks to privacy and security. By identifying sensor anomalies in the AVN, the EAD model we developed in this research can improve AV security. Multiple AVs can accurately identify the malicious AV by 12.13%. Additionally, MaxEntIRLs comparison methodology effectively identifies fraudulent AV. In general, the sensor anomaly detection is enhanced by 8.01% when using the EAD compared to the state-of-the-art, and the detection rate delay is decreased by 10.06%. The effectiveness of the DL-MARL model is further assessed using ROC, AUC, precision, and recall. The EAD paradigm thereby protects the AV against harmful sensory habits. Future studies will be important in detecting other AV attacks, even though the current approach helps to spot instant anomalies in AVs.

5. References

[1] H. S. M. Lim and A. Taeihagh, "Autonomous Vehicles for Smart and Sustainable Cities: An in-depth Exploration of Privacy and Cybersecurity Implications", Energies, vol. 11, no. 5, p. 1062, 2018.

[2] S. B. Prathiba, G. Raja, S. Anbalagan, K. Dev, S. Gurumoorthy, and A. P. Sankaran, "Federated Learning Empowered Computation Offloading and Resource Management in 6G-V2X", IEEE Transactions on Network Science and Engineering, 2021

[3] F. van Wyk, Y. Wang, A. Khojandi, and N. Masoud, "Real-time sensor anomaly detection and identification in automated vehicles", IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 3, pp. 1264–1276, 2020.

[4] S. Prathiba, G. Raja, and N. Kumar, "Intelligent cooperative collision avoidance at overtaking and lane changing maneuver in 6G-V2X communications", IEEE Transactions on Vehicular Technology, 2021, doi: 10.1109/TVT.2021.3127219.

[5] F. van Wyk, Y. Wang, A. Khojandi, and N. Masoud, "Real-time sensor anomaly detection and identification in automated vehicles", IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 3, pp. 1264–1276, 2020.

[6] C. Patel and N. Doshi, "Security challenges in IoT cyber world", Security in Smart Cities: Models, Applications, and Challenges. Springer, pp. 171–191, 2019.

[7] E. Lampiri, "Sensor anomaly detection and recovery in a nonlinear autonomous ground vehicle model", 11th Asian Control Conference, pp. 430–435, 2017.

[8] C. Ryan, F. Murphy, and M. Mullins, "End-to-end autonomous driving risk analysis: a behavioural anomaly detection approach", IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 3, pp. 1650–1662, 2021.

[9] R. Jin, B. Wei, Y. Luo, T. Ren, and R. Wu, "Blockchain-based data collection with efficient anomaly detection for estimating battery stateof-health", IEEE Sensors Journal, vol. 21, no. 12, pp. 13 455–13 465, 2021.

[10] Y. Liu, P. Ning, and M. K. Reiter, "False Data Injection Attacks against State Estimation in Electric Power Grids", ACM Transactions on Information and System Security, vol. 14, no. 1, pp. 1–33, 2011.

[11] S. B. Prathiba, G. Raja, A. K. Bashir, A. A. Alzubi, and B. Gupta, "SDNassisted Safety Message Dissemination Framework for Vehicular Critical Energy Infrastructure", IEEE Transactions on Industrial Informatics, 2021.

[12] Z. Khan, M. Chowdhury, M. Islam, C.-Y. Huang, and M. Rahman, "Long short-term memory neural network-based attack detection model for invehicle network security", IEEE Sensors Letters, vol. 4, no. 6, pp. 1–4, 2020.

[13] J. Fu, A. Tacchetti, J. Perolat, and Y. Bachrach, "Evaluating Strategic Structures in Multi-Agent

Inverse Reinforcement Learning", Journal of Artificial Intelligence Research, vol. 71, pp. 925–951, 2021

[14] Z.-J. Jin, H. Qian, and M.-L. Zhu, "Gaussian Processes in Inverse Reinforcement Learning", in 2010 International Conference on Machine Learning and Cybernetics, vol. 1, 2010, pp. 225–230.

[15] S. Zhifei and E. M. Joo, "A survey of inverse reinforcement learning techniques", International Journal of Intelligent Computing and Cybernetics, 2012.

[16] K.-S. Hwang, H.-y. Chiang, and W.-C. Jiang, "Adaboost-like method for inverse reinforcement learning", IEEE International Conference on Fuzzy Systems, pp. 1922–1925, 2016.

[17] M. Aloqaily, S. Otoum, I. Al Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities", Ad Hoc Networks, vol. 90, p. 101842, 2019

[18] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles", IEEE Transactions on Intelligent transportation systems, vol. 16, no. 2, pp. 546–556, 2014.

[19] S. B. Prathiba, G. Raja, S. Anbalagan, R. Narayanan, and K. B. Venkata Karthik, "SOSChain: self optimizing streamchain for LastMile 6G UAV-Truck networks", ser. 6G-ABS '21. New York, USA: Association for Computing Machinery, 2021, p. 19–24, doi: 10.1145/3477084.3484952

[20] A. Alshammari, M. A. Zohdy, D. Debnath, and G. Corser, "Classification approach for intrusion detection in vehicle systems", Wireless Engineering and Technology, vol. 9, no. 4, pp. 79–94, 2018.

[21] S. Prathiba, G. Raja, K. Dev, N. Kumar, and M. Guizani, "A hybrid deep reinforcement learning for autonomous vehicles smart platooning", IEEE Transactions on Vehicular Technology, 2021, doi: 10.1109/TVT.2021.3122257.

[22] J. J. Davis and A. J. Clark, "Data preprocessing for anomaly based network intrusion detection: a review", computers and security, vol. 30, no. 6-7, pp. 353–375, 2011.

[23] G. Raja, S. Anbalagan, G. Vijayaraghavan, S. Theerthagiri, S. V. Suryanarayan, and X.-W. Wu, "SP-CIDS: secure and private collaborative IDS for VANETs", IEEE Transactions on Intelligent Transportation Systems, 2020.

[24] Y. Wang, N. Masoud, and A. Khojandi, "Real-time Sensor Anomaly Detection and Recovery in Connected Automated Vehicle Sensors," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 3, pp. 1411–1421, 2020

[25] K. Ni, N. Ramanathan, M. N. H. Chehade, L. Balzano, S. Nair, S. Zahedi, E. Kohler, G. Pottie, M. Hansen, and M. Srivastava, "Sensor Network Data Fault Types," ACM Transactions on Sensor Networks (TOSN), vol. 5, no. 3, pp. 1–29, 2009

[26] P.-Y. Chen, S. Yang, and J. A. McCann, "Distributed Real-time Anomaly Detection in Networked Industrial Sensing Systems," IEEE Transactions on Industrial Electronics, vol. 62, no. 6, pp. 3832–3842, 2014.

[27] H. Qin, M. Yan, and H. Ji, "Application of controller area network (can) bus anomaly detection based on time series prediction," Vehicular Communications, vol. 27, p. 100291, 2021.

[28] V. Justin, N. Marathe, and N. Dongre, in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC).

[29] D. S. Kim, H.-N. Nguyen, and J. S. Park, "Genetic algorithm to improve SVM based network intrusion detection system", 19th International Conference on Advanced Information Networking and Applications, vol. 2. IEEE, pp. 155–158, 2005.

[30] R. Oucheikh, M. Fri, F. Fedouaki, and M. Hain, "Deep real-time anomaly detection for connected autonomous vehicles", Procedia Computer Science, vol. 177, pp. 456–461, 2020.

[31] A. R. Javed, M. Usman, S. U. Rehman, M. U. Khan, and M. S. Haghighi, "Anomaly detection in automated vehicles using multistage attentionbased convolutional neural network", IEEE Transactions on Intelligent Transportation Systems, 2020.

[32] R. Jin, B. Wei, Y. Luo, T. Ren, and R. Wu, "Blockchain-based data collection with efficient anomaly detection for estimating battery state-of-health", IEEE Sensors Journal,

2021.

[33] P. Sharma and H. Liu, “A machine-learning-based data-centric misbehavior detection model for internet of vehicles”, IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4991–4999, 2020.

[34] J. Tian, W. Ding, C. Wu, and K. W. Nam, “A generalized approach for anomaly detection from the internet of moving things”, IEEE Access, vol. 7, pp. 144 972–144 982, 2019.

[35] Y. Wang, Q. Liu, E. Mihankhah, C. Lv, and D. Wang, “Detection and isolation of sensor attacks for autonomous vehicles: framework, algorithms, and validation”, IEEE Transactions on Intelligent Transportation Systems, 2021.

[36] F. Alotibi and M. Abdelhakim, “Anomaly Detection for cooperative adaptive cruise control in autonomous vehicles using statistical learning and kinematic model”, IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 6, pp. 3468–3478, 2020.

[37] Z. Ju, H. Zhang, and Y. Tan, “deception attack detection and estimation for a local vehicle in vehicle platooning based on a modified ufir estimator”, IEEE Internet of Things Journal, vol. 7, no. 5, pp. 3693– 3705, 2020.

[38] F. Guo, Z. Wang, S. Du, H. Li, H. Zhu, Q. Pei, Z. Cao, and J. Zhao, “Detecting vehicle anomaly in the edge via sensor consistency and frequency characteristic”, IEEE Transactions on Vehicular Technology, vol. 68, no. 6, pp. 5618–5628, 2019.

[39] J. Grover, M. S. Gaur, V. Laxmi, and N. K. Prajapati, “A Sybil attack detection approach using neighboring vehicles in VANET”, ACM S, pp. 151–158, 2011.

[40] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, “P2DAP—Sybil attacks detection in vehicular ad hoc networks”, IEEE JSAC, vol. 29, no. 3, pp. 582–594, 2011.

[41] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, “TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs”, Veh. Comm., vol. 9, pp. 254–267, 2017.

[42] J. Hortelano, J. C. Ruiz, and P. Manzoni, “Evaluating the usefulness of watchdogs for intrusion detection in VANETs”, IEEE ICC, pp. 1–5, 2010.

[43] A. Daeinabi and A. G. Rahbar, “Detection of malicious vehicles through monitoring in vehicular ad-hoc networks”, Mult. tools and app., vol. 66, no. 2, pp. 325–338, 2013.

[44] A. Hamieh, J. Ben-Othman, and L. Mokdad, “Detection of radio interference attacks in VANET”, IEEE GLOBECOM, 2009, pp. 1–5.

[45] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, “On data-centric misbehavior detection in VANETs”, IEEE VTC (Fall), 2011, pp. 1–5.

[46] P. Golle, D. Greene, and J. Staddon, “Detecting and correcting malicious data in VANETs”, ACM VANET, 2004, pp. 29–37

