


Article

Aircraft Trajectory Prediction Enhanced through Resilient Generative Adversarial Networks Secured by Blockchain: Application to UAS-S4 Ehécatl

Seyed Mohammad Hashemi *, Seyed Ali Hashemi, Ruxandra Mihaela Botez  and Georges Ghazi

Laboratory of Applied Research in Active Controls, Avionics and AeroServoElasticity LARCASE, École de Technologie Supérieure (ÉTS), Université de Québec, Montréal, QC H3C 1K3, Canada; alihashemi15784@gmail.com (S.A.H.); ruxandra.botez@etsmtl.ca (R.M.B.); georges.ghazi@etsmtl.ca (G.G.)

* Correspondence: seyed-mohammad.hashemi.1@ens.etsmtl.ca

Abstract: This paper introduces a novel and robust data-driven algorithm designed for Aircraft Trajectory Prediction (ATP). The approach employs a Neural Network architecture to predict future aircraft trajectories, utilizing input variables such as latitude, longitude, altitude, heading, speed, and time. The model's foundation is rooted in the Generative Adversarial Network (GAN) framework, known for its inherent generative capabilities, rendering it remarkably resilient against Adversarial Attacks. To enhance its credibility, the Blockchain is employed as a Ledger Technology (LT) to securely store legitimate predicted values utilized in subsequent trajectory predictions. The Blockchain ensures that only authorized and non-adversarial samples are stored in the blocks, rejecting any adversarial predictions. In the validation process, trajectory data for training the GAN model were generated through the UAS-S4 Ehécatl simulation model. The performance evaluation relies on the model's resistance to adversarial attacks, measured by fooling rates. The results acquired affirm the excellent efficacy of the GAN model, Secured by Blockchain, approaching against adversarial attacks.

Keywords: robustness; aircraft trajectory prediction; generative adversarial networks; blockchain



Citation: Hashemi, S.M.; Hashemi, S.A.; Botez, R.M.; Ghazi, G. Aircraft Trajectory Prediction Enhanced through Resilient Generative Adversarial Networks Secured by Blockchain: Application to UAS-S4 Ehécatl. *Appl. Sci.* **2023**, *13*, 9503. <https://doi.org/10.3390/app13179503>

Academic Editor: Wei Huang

Received: 23 July 2023

Revised: 17 August 2023

Accepted: 18 August 2023

Published: 22 August 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Aerial transportation may be formulated as critical aviation problem with special requirements to ensure flight safety [1]. In fact, “safety” is the first and main concern related to the aerial transportation [2,3]. The design and development of a reliable transportation algorithm require awareness of aircraft trajectories [4]. Trajectory awareness can significantly increase aerial transportation performance [5]. The prediction of future trajectories contributes to the Aerial Transportation Algorithm [6] (ATA) in terms of path planning and collision avoidance [7].

Precise trajectory prediction can boost an ATA's efficiency in terms of safety, costs, and time [8]. Numerous research investigations have concentrated on precise trajectory prediction as a fundamental requirement for enhancing safe and efficient ATAs [9]. Eurocontrol's CASCADE Project [10], NASA's Air Traffic Management Research [11], and Single European Sky ATM Research (SESAR) [12] are the most well-known practical applications for accurate trajectory prediction in the real world. Eurocontrol implemented advanced trajectory prediction algorithms that analyze real-time data from aircraft, weather conditions, and air traffic control systems. By accurately predicting aircraft trajectories, controllers can proactively identify potential conflicts between flights and provide timely instructions to pilots to avoid collisions. NASA's AAC project incorporates advanced trajectory prediction algorithms to model aircraft movements and predict potential conflicts. By integrating data from various sources, including radar, ADS-B (Automatic Dependent Surveillance-Broadcast), and weather data, the system can anticipate trajectory deviations and suggest route adjustments to air traffic controllers. Within SESAR, trajectory prediction

is a fundamental component of the “trajectory-based operations” concept. This involves using accurate trajectory predictions to enable more precise planning and coordination of flights, from departure to arrival.

In this context, our research has been directed toward formulating and creating a reliable methodology for precise predictions of aircraft trajectories. In essence, there are two methods that can be employed for predicting flight paths: the “Deterministic” approach [13] and the “Probabilistic” approach [14]. Predictions of deterministic trajectories involve methods where forthcoming paths are determined based on their initial parameter values. Deterministic methodologies can be designed using statistical [15], artificial intelligence [16], and hybrid [17] models. Receding Horizon techniques that utilize kinematic and kinetic models have been the dominant type applied and have demonstrated their effectiveness [18,19].

Deterministic methods have the ability to forecast aircraft paths by solving intricate dynamic programming problems while considering various constraints [20]. While they are good in predicting short-term trajectories, their accuracy reduces over the long-term due to error propagation throughout the prediction horizon [21]. This error is due to variety of factors including complexity of dynamic environments, uncertainty in environmental conditions, limited data and observations, nonlinear behavior of dynamic environments, interaction and cooperation complexity, cumulative sensing and actuation errors, and computational loads [22]. Hence, probabilistic [23] approaches were created and advanced to enhance the accuracy of long-term trajectory prediction.

Regarding probabilistic techniques, evolutionary algorithms [24], such as Genetic Algorithms (GAs) [25], Particle Swarm Optimization (PSO) [26], and hybrid GA-PSO, have effectively been employed for probabilistic ATP [27]. GA simulates evolution by generating a population of potential solutions, evaluating their fitness, selecting the fittest individuals, combining their traits through crossover and mutation, and iterating over generations to improve solutions. This diversity-driven approach helps explore various possibilities and avoids getting stuck in local optima, making it suitable for probabilistic prediction where uncertainty is prevalent. PSO imitates the social behavior of particles in a swarm. Particles move through the solution space, adjusting their positions based on their own experiences and the swarm’s best results. This balance between local and global exploration allows PSO to effectively handle uncertainty and produce diverse solutions, making it fitting for probabilistic prediction tasks where multiple outcomes need to be considered. Both algorithms offer ways to navigate complex solution spaces and embrace uncertainty, making them well-suited for generating a range of potential outcomes in probabilistic prediction scenarios. However, these evolutionary algorithms focused solely on nearby local consistencies during their optimization process [28], resulting in generating single point locations without considering the entire trajectory.

The trajectory prediction problems have been revolutionized by Neural Networks (NN) employing deep structures that rely on data loggers that provide extensive and rich datasets [29]. By employing deterministic datasets and architectures, featuring probabilistic activation functions, NN models can be trained to achieve highly accurate predictions of long-term trajectories. A variety of data-driven models, including Logistic Regression (LR), Deep Neural Network (DNN), Support Vector Regression (SVR), Recurrent Neural Network (RNN), Convolutional Neural Network (CNN), and Long-Short Term Memory (LSTM) models, have been effectively utilized as benchmark techniques for ATPs [30]. Regarding the representative neural network for trajectory prediction, hybrid architectures combining transformers and recurrent layers are among the most novel approaches. Combinations of transformers and recurrent layers [31] to leverage the strengths of both architectures have emerged. Transformers excel at capturing global dependencies, while recurrent layers are efficient at modeling temporal patterns. These architectures could significantly improve trajectory prediction performances.

While NN ATP models demonstrated strong performance in terms of prediction accuracy, they exhibited vulnerability to adversarial attacks [32]. Adversarial attacks on

trajectory prediction models pose serious risks to various applications, including flight safety and operational efficiency. These attacks can exploit the vulnerabilities of neural network models, leading to incorrect predictions that could have far-reaching consequences. It may cause collisions due to airspace congestion, misleading control decisions, operational delays [33].

The ATA's major concern, i.e., safety, was affected by the Adapted Fast Gradient Sign Method (AFGSM) attacks. Furthermore, even with enhanced resilience through adversarial retraining, ATP models continued to be vulnerable to black-box adversarial attacks [34]. Therefore, we conducted a study aimed at devising a resilient algorithm founded on the principles of the Generative Adversarial Network (GAN) methodology [35] to be robust against both white- and black-box adversarial attacks.

Generative Adversarial Networks (GANs) offer a unique approach to trajectory prediction, utilizing two components—a generator and discriminator—to generate realistic trajectory predictions. The generator learns from historical data to create synthetic trajectories, while the discriminator evaluates their authenticity. GANs excel in capturing complex patterns and generating diverse, plausible trajectories. They are especially suitable for tasks that involve uncertain outcomes and multiple potential paths. However, challenges such as mode collapse, training instability, and ensuring realism need to be addressed for GANs to reach their full potential in producing accurate and safe trajectory predictions [36].

The Generative Adversarial Network (GAN) is structured around two networks: the “Generator” and the “Discriminator”. Utilizing the original dataset, the “Generator” learns to generate new datasets with similar statistics to the original data, while the “Discriminator” assesses these generated datasets [35]. This framework finds application in various contexts, particularly data reconstruction. The GAN can also generate adversarial samples, where the prediction model is trained using a provided dataset, while the Generator simultaneously produces adversarial samples that are being used in the training phase. This approach's strength lies in its capacity to defend against both white-box and black-box attacks.

GAN algorithms have been successfully utilized to solve unmanned moving vehicle trajectory prediction problems. A GAN model was designed for a UAS with the aim of predicting the landing trajectories [37]. Such a model could be used to manage landing paths around an airport. A GAN model was also used in another research study for an UAV's long-term trajectory prediction [38]. The GAN algorithms have been used for marine and ground transportation to accurately predict trajectories [39]. In terms of reliability, GAN algorithms remain susceptible to black-box attacks. It is, therefore, essential to label and store the original values of predicted trajectories to improve data security and the GAN's performance.

To improve the reliability of GAN algorithms (the first objective of our study), Blockchain was utilized as a Ledger Technology (LT) to record the predicted trajectory values [40] (the second objective of our study). Integrating Blockchain technology as a ledger for storing predicted trajectories offers robust advantages in data security, integrity, and resilience against adversarial attacks. The immutable nature of Blockchain ensures trajectories remain tamper-resistant, transparent, and traceable. Decentralization and cryptographic security further bolster trust in trajectory data. Consensus mechanisms prevent unauthorized alterations, maintaining data accuracy. This blockchain-based approach assures accountability, compliance, and data protection, making it a powerful solution for secure trajectory storage, particularly in scenarios where data integrity and resilience against adversarial threats are paramount [41].

This approach boosts the resilience of the GAN-ATP model against forthcoming adversarial attacks. Blockchain Ledger Technology (BLT) stores both the GAN-predicted trajectories, relying on previous block confirmations on the blockchain. The hash associated with the previous block and the predicted trajectories values are stored in the new block for forthcoming predictions. Note that the hash is a unique digital fingerprint that verifies the integrity and authenticity of data.

For development of smart contracts associated with the BLT, formal methods play a pivotal role by using mathematical techniques to rigorously verify correctness, security, and reliability. They ensure that smart contracts adhere to intended behaviors, preventing costly errors and security breaches. Formal methods involve creating models, defining specifications, and employing verification tools to prove mathematically that smart contracts meet desired properties [42]. The benefits include early issue detection, heightened security, enhanced trust, and long-term reliability, making formal methods an essential practice for building robust and trustworthy blockchain applications [43].

This research study offers four main contributions. The first constitutes the design of a customized GAN architecture for trajectory prediction application to our UAS-S4. Expressing the adversarial attack concept in time-series problems and imposing adversarial attacks on the GAN-based UAV trajectory prediction are the second and third contributions. The fourth major contribution is the design of a blockchain-based ledger technology that stores original predicted trajectories and has a high level of robustness in the face of adversarial attacks.

This article comprises five sections. Section 2 describes the aircraft trajectory prediction problem in detail. The trajectory prediction model is formulated through the utilization of a GAN, and then is secured using the Blockchain, as elaborated in Section 3. Section 4 presents results and assesses the performance of the proposed model when subjected to adversarial attacks. Finally, Section 5 gives conclusions regarding the GAN trajectory prediction model and evaluates the contribution of Blockchain to its robustness against adversarial attacks.

2. Problem Statement

It is assumed that an aircraft is flying in its corridor, as shown in Figure 1. The objective is to predict the future trajectory of this aircraft for the next i steps by using a set of data at $time = T_n$, composed of latitude, longitude, altitude, heading, speed, and time.

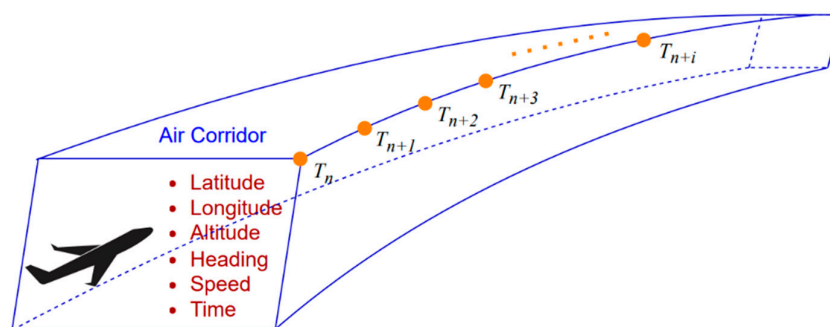


Figure 1. Air Corridor Containing an Aircraft Alongside its GPS Data.

With this aim, a deep neural network model must be trained in order to predict future trajectories in real time operations. Neural networks with deep architectures composed of multiple layers are capable of efficiently learning complex patterns. Such networks do not require complex activation functions, and they can learn from raw datasets. A prediction model using a deep neural network should be trained using a large and rich aircraft trajectories database. After training the prediction model and fine-tuning its hyper parameter, aircraft GPS datasets are applied to the trained model. The trained deep neural network is then able to predict future trajectories of the aircraft for T_{n+1} to T_{n+i} . Figure 2 shows the procedure for the off-line training and then real-time testing of the Aircraft Trajectory Prediction (ATP) model.

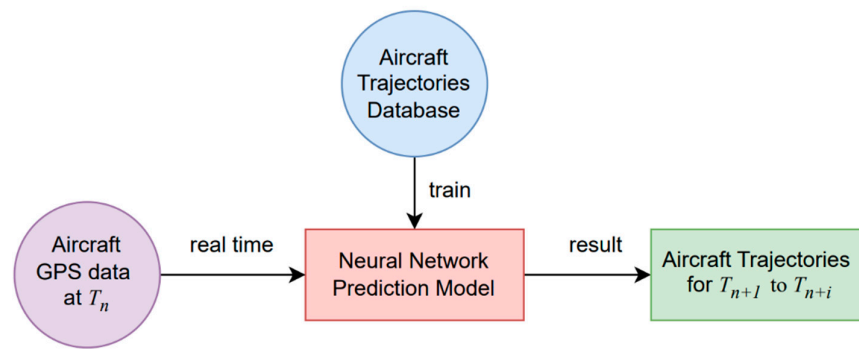


Figure 2. Off-line Training and Real-Time Testing of the Deep Neural Network Designed for the ATP.

Deep neural network architectures can work efficiently if they are provided with a large and rich database. To obtain such a database, we used our UAS-S4 simulation model to generate a large number of aircraft trajectories. Figure 3 shows the Hydra Technologies UAS-S4 Ehecattl, and Table 1 gives its geometrical and flight data specifications [44].



Figure 3. Hydra Technologies UAS-S4 Ehecattl.

Table 1. The UAS-S4 Geometrical and Flight Data Specification.

Specification	Value
Wing area	2.3 m ²
Wingspan	4.2 m
Mean aerodynamic chord	0.57 m
Total length	2.5 m
Empty weight	50 kg
Maximum take-off weight	80 kg
Loitering airspeed	35 knots
Maximum speed	135 knots
Operational range	120 km
Service ceiling	15,000 ft

The aircraft trajectories' database was created using a simulator that was designed based on support vector regression flight dynamics model [45,46] and its robust adaptive fuzzy controller [47,48].

3. Methodology

The Generative Adversarial Network (GAN) can generate new aircraft trajectory data that are statistically the same as those of the given training dataset. The concept behind the GAN relies on training a prediction model indirectly through a discriminator [49]. In this process, another supportive neural network criticizes the predicted data and updates itself accordingly. The generator network is not supposed to minimize the loss corresponding

to a specific trajectory, but rather to mislead the discriminator. Therefore, the GAN can be trained while remaining robust, even when dealing with adversarial data [50].

For the mathematical representation of the GAN model concept, we consider a probability space (ω, μ_{ref}) , where ω is the sample space and μ is the event space. In addition, the “Generator” is considered an actor, while the “Discriminator” is considered a critic. Both contest each other. The generator network tactic, denoted by $P_G(\omega)$, is composed of measured probabilities μ_G over ω . In contrast, the discriminator’s tactic is based on Markov kernels such that $\mu_D : \omega \rightarrow P[0, 1]$. The GAN is supposed to solve a zero-sum game according to the following objective function [51].

$$\min_G \max_D V(D, G) = E_{x \sim P_{data}(x)} [\log D(x)] + E_{z \sim P_z(z)} [\log(1 - D(G(z)))] \tag{1}$$

D and G are Discriminator and Generator neural network functions, respectively. E is the logarithm probability of D and G predictions associated with the GPS data, whether is genuine or not.

By applying input noise P_z , the GAN prediction model learns the distribution of the Generator network P_G over trajectory data x . Therefore, mapping to the data space is achieved through $G(z; \theta_G)$ by relying on the generator’s weighing parameters θ_G .

The GAN is trained while updating the discriminator’s weighting parameters. The training process continues until when the discriminator cannot differentiate between the G and D distributions, and $D(x) = 1/2$. The following Algorithm 1 is employed for training the GAN model based on gradient descent [51].

Algorithm 1: GAN’s Gradient Descent Training.

for a number of training iterations **do**

for k steps **do**

- Pick a batch of h number of noise samples $\{z_1, \dots, z_h\}$ from the prior noise $P_G(z)$.
- Pick a batch of h number of samples $\{x_1, \dots, x_h\}$ from the data generating distribution $P_{data}(x)$.
- Update the discriminator’s weighting parameters by ascending gradient as:

$$\nabla_{\theta_D} \frac{1}{h} \sum_{l=1}^h = [\log D(x_{(l)}) + \log(1 - D(G(z_{(l)})))]$$

end for

- Pick a batch of h number of noise samples $\{z_1, \dots, z_h\}$ from the prior noise $P_G(z)$.
- Update the discriminator’s weighting parameters by ascending gradient as:

$$\nabla_{\theta_G} \frac{1}{h} \sum_{l=1}^h = [1 - \log(1 - D(G(z_{(l)})))]$$

end for

there is no restriction for utilizing the gradient descent algorithm.

We designed the trajectory prediction model based on GANs to address the issue of Adversarial Attacks targeting Neural Networks. Figure 4 illustrates the structure of the developed GAN designed for executing the ATP task.

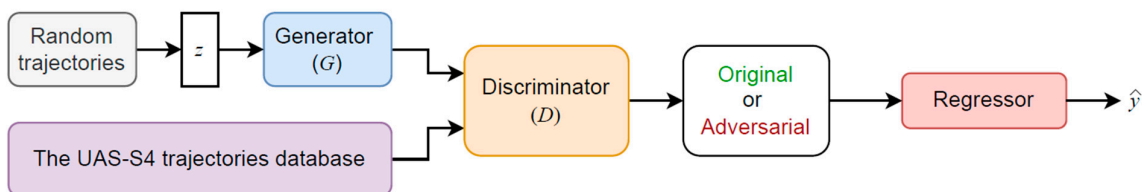


Figure 4. The structure of the developed GAN designed for executing the ATP task.

As depicted in Figure 4, the GAN architecture consists of two primary components: the Generator (G) and the Discriminator (D) [35]. Random feasible trajectories following

a Gaussian distribution are fed into the feature extractor (z). The G-network generates samples resembling those within the database, while the D-network differentiates between the data generated by the Generator and the data from the trajectory database. The D-network undergoes training based on its inputs, and the Regressor predicts forthcoming trajectories by considering both original and adversarial samples.

The detailed architecture of the proposed Generative Adversarial Networks aimed at Aircraft Trajectory Prediction (GAN-ATP) is shown in Figure 5, in which the trajectories' data generation is illustrated step by step [52].

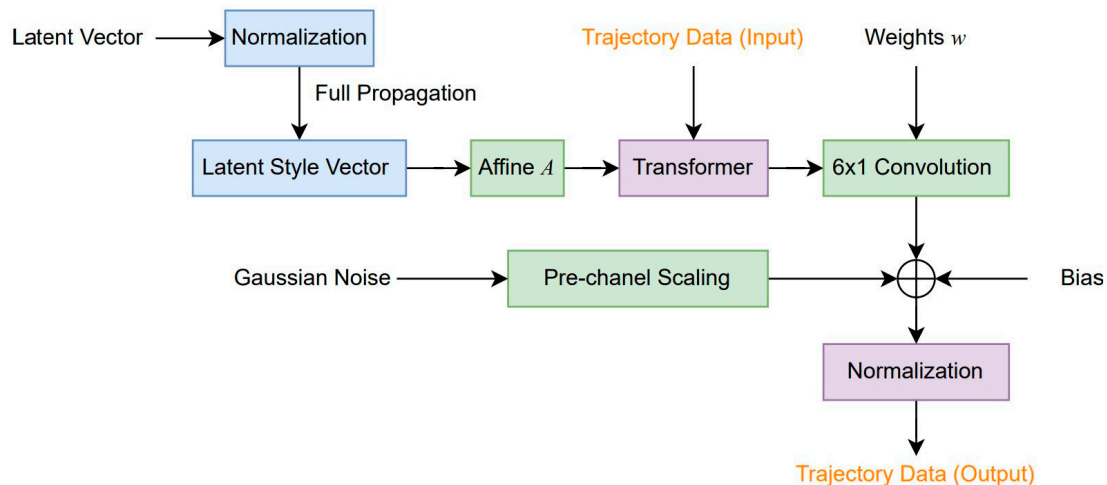


Figure 5. The designed GAN architecture for aircraft trajectory data generation.

According to Figure 5, generated trajectory data are applied to the Transformer. Simultaneously, the Latent Vector is normalized and fully propagated through the latent style vector. The output of the Latent Style Vector block is then passed to the Transformer via the affine A ("adaptive instance normalization") block. The mixture is transmitted from the Transformer into 6×1 convolution layers supported by weights w . Gaussian noise is then added via Pre-channel Scaling, and Bias is added as well. New trajectory data are generated after normalization. One style of latent vector per generated trajectory is used during training, as it performs its stylization independently of other style blocks.

Initialization and batch normalization procedures were executed prior to the training phase, and both the Generator (G) and Discriminator (D) networks were established using a full-propagation architecture. The Mean Square Error (MSE) served as the metric for performance assessment, and the error rates were employed to gauge the effectiveness of the Regressor.

The GAN framework has the potential to enhance its ability against adversarial attacks through a more effective defense strategy when compared to the adversarial retraining technique. This advantage arises from the GAN's defense approach, which can effectively counter both white-box and black-box attacks, whereas adversarial retraining is limited to addressing white-box attacks exclusively.

Predictably, the GAN remains vulnerable to adversarial attacks, inevitably allowing some adversarial samples to pass the Discriminator when the GAN is fooled, resulting in erroneous predictions by the regressor for future trajectories \hat{y} . In such instances, the application of Blockchain, a form of Distributed Ledger Technology (DLT), becomes relevant. It can be utilized to retrieve data registered in the preceding block [40].

Drawing upon the reliable and authenticated trajectory data, if a predicted trajectory surpasses a particular threshold, the prediction is considered unsuccessful. Consequently, the Blockchain ensures that inaccurately predicted trajectories are prevented from being recorded in the subsequent block [53]. In fact, its consensus protocol hinders the incorporation of the new block into the chain. To this end, Figure 6 shows the configuration of

the Blockchain, trajectory storage (data within blocks), consensus determination, and the implementation of new blocks.

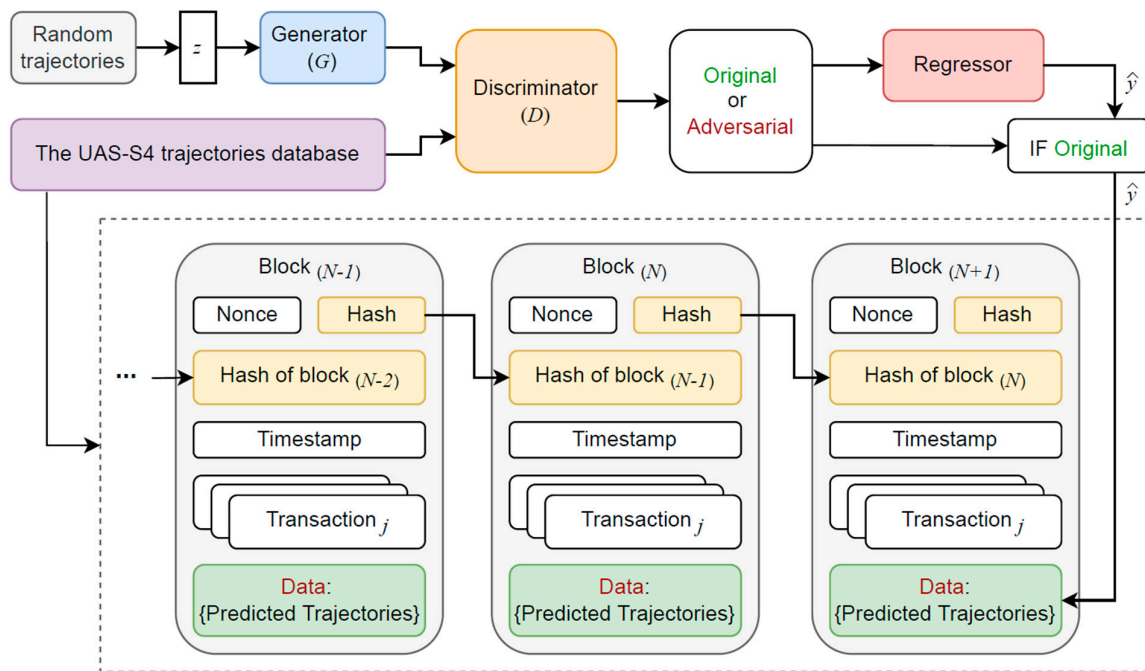


Figure 6. The structure governing Consensus Decision, Trajectory Storage, and the Execution of New Blocks.

As shown in Figure 6, the Generator G produces adversarial samples that are similar to those in the UAS-S4 trajectory database. Next, the Discriminator D discriminates between two inputs (those from Generator G and those from the UAS-S4 trajectory database) and trains the samples regardless of if they are original or adversarial. Then, the future trajectories are predicted by the regressor. Meanwhile, the original UAS-S4 trajectories are stored in the UAS-S4 database via the Blockchain. Within the blockchain, $\text{Block}_{(N+1)}$ can be processed for trajectory storage provided that the originally known predicted value \hat{y} and the Hash of $\text{Block}_{(N)}$ collectively verify that the predicted trajectory remains below a threshold defined by the trajectories stored in $\text{Block}_{(N+1)}$. A hash is a fixed-size digital fingerprint generated from input data, ensuring data integrity and security within the decentralized network.

Predicted trajectories are transformed into the encrypted data stored within the block. This on-chain procedure involves the utilization of the hash from the preceding block, the execution time (timestamp), a random number (nonce) added to the hash, and j number of trajectory predictions (transactions). The evaluation of the GAN model's performance against adversarial attacks, is elaborated upon in the subsequent section.

4. Results and Discussion

The database used in this study for testing and validation of the proposed methodology comprised a total of 1820 trajectories and was composed of 218,400 samples. In which, each sample is a vector representing the GPS data (i.e., $[\text{latitude}, \text{longitude}, \text{altitude}, \text{heading}, \text{speed}, \text{time}]_{6 \times 1}$) [54]. For enhancing the stability of the GAN model, Initialization of the weight vector and batch normalization were undertaken. "Z-score normalization" and "Batch normalization" are common methods used to normalize latent vectors. We utilized batch normalization methodology as it has faster convergence. For the proposed generative adversarial model, batch normalization aims to normalize the activations of neurons in a network layer by adjusting them based on the statistics of the current batch of data during

training. While batch normalization is commonly used in the layers of a neural network, it is not typically applied directly to latent vectors.

Furthermore, a regularization process was implemented to reduce the magnitude of the regressed values. L_2 regularization methodology was utilized, in which it added a penalty term $\lambda \|w\|_2^2$ to the loss function, and encouraged the weights to be small, and eventually to avoid overfitting. λ denotes regularization strength hyperparameter for parameter vector w .

Fully connected Deep Neural Networks (DNN) architecture, with 12 hidden layers and 12 neurons in each one activated by *ReLU* (Rectified Linear Unit) functions, were utilized for both Generator and Discriminator. In order to make a trade-off between the conservatism and sensitivity of the GAN model, the prediction threshold was set to 0.8.

As the GAN model was further designed and developed for trajectory prediction, its learning curves must be evaluated. The GAN should be trained such that the prediction model avoids both overfitting and underfitting. For this purpose, training curves were plotted to show the variation of the Mean Square Error (MSE) loss versus the number of training epoch. Figure 7 shows GAN's training and validation performance in terms of MSE loss variation with the number of training epoch.

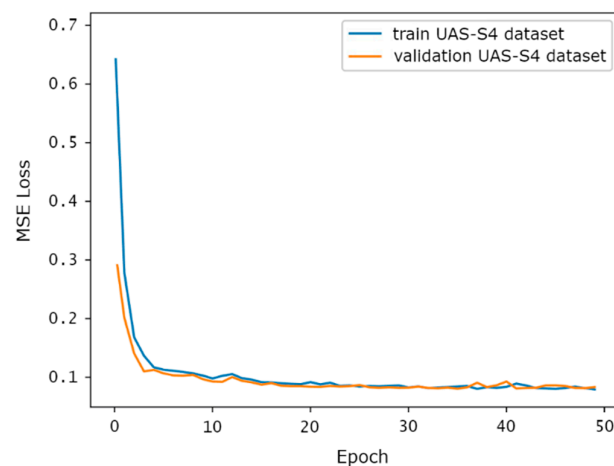


Figure 7. GAN's training and validation performance.

As shown in Figure 7, the GAN model was well-trained, as the MSE loss decreased over the epochs without abrupt fluctuations. After four epochs, MSE loss curves related to the training and validation performance stabilized and converged to the point of stability with a very small difference. Given the small difference between the learning curves, it can be inferred that the GAN model provided a very good generalization for future trajectory prediction.

The other important metric related to the trained GAN model's efficiency is its Discriminator output behaviour during divergence minimization. Figure 8 illustrates the Discriminator's output for the UAS-S4's real and fake trajectory data.

As shown in Figure 8, the GAN-generated trajectory data has the aim of converging the Discriminator's output at 0.5. It could consistently minimize the UAS-S4 trajectory divergences corresponding to the real and fake data, showing that the discriminator assigned the same probability of a fake or a real trajectory existence.

The Receiver Operating Characteristic (ROC) curve was also considered for the performance analysis. The ROC curve indicates the prediction model parameters, namely, the true and false-positive predicted trajectory rates. A ROC curve serves as a performance index when various thresholds are considered. The area under the ROC curve helps to assess a trained prediction model's efficiency. Figure 9 shows the ROC performance curves related to each of the three methodologies.

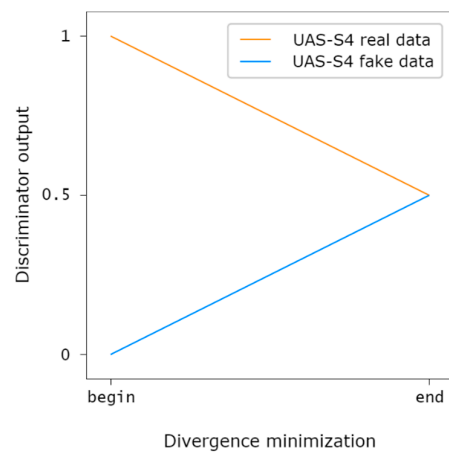


Figure 8. GAN Discriminator's output.

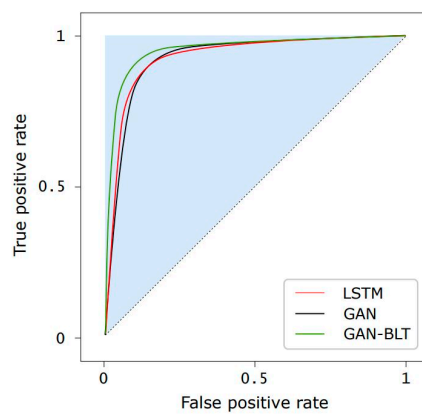


Figure 9. Receiver operating characteristic (ROC) performance for the LSTM, GAN, and GAN-BLT.

An ROC is a probability curve, so that the area under it measures the trajectory separation. It reveals to what extent the trajectory prediction model can distinguish between inbound and outbound trajectories.

Figure 9 indicates that there is not a high difference between the GAN and LSTM ROC performance. However, our proposed GAN-BLT shows a higher value for the area under the ROC, which confirms the superiority of this method in the correct recognition of inbound and outbound trajectories. The well-trained GAN and its optimized Discriminator allowed the model to accurately predict the forthcoming trajectories of the UAV-S4. Table 2 gives the GAN model accuracy-based performances describing the details of the ROC curves.

Table 2. Performance of the LSTM, GAN, and GAN-BLT at trajectory prediction.

Method	Training Accuracy (%)	Testing Accuracy (%)	Precision (%)	Sensitivity (%)	F1 Score (%)
LSTM	94.9	90.6	97.2	93.6	93.7
GAN	96.5	92.1	95.6	91.2	94.1
GAN-BLT	95.7	91.6	94.1	94.3	96.4

In accordance with the results in Table 2, among the three models analyzed, the GAN model obtained the best trajectory prediction accuracy for both training (96.5%) and testing (92.1%) phases. The Long Short-Term Memory (LSTM) gave a 97.2% precision, and it outperformed GAN-based methodologies in terms of precision. Using the Blockchain Ledger Technology, the GAN sensitivity was improved, up to 94.3%; this was higher than that of the LSTM. The F1 score performance index confirmed the superiority of the GAN-BLT over the two other trajectory prediction methodologies.

Blockchain Ledger Technology (BLT) was designed to safely store trajectory data in an untrusted environment, even when new agents were approached. Therefore, a sufficient delay was needed for confirmation in order to generate a new on-chain block for trajectory data storage. Figure 10 shows the agents' (UAVs) agreement confirmation probability.

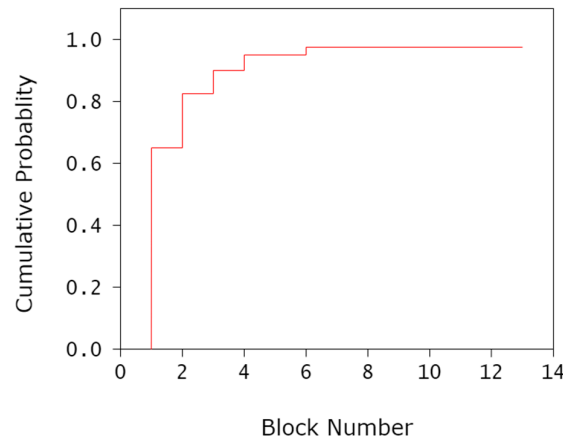


Figure 10. Agents (UAV's) trajectory prediction confirmation probability.

Figure 10 shows the cumulative probability versus the block number. Hence, a percentile analysis can estimate the percentile of executed confirmations up to the generation of a particular block. This metric is used by ground satiation to evaluate the risk from confirmation failures. According to Figure 10, the cumulative probability of a successful confirmation is 64.7% after the first block generation. After generating four blocks, this value settles on 97.2%, and exceeds 99.1% when the sixth block is generated. Consequently, the generation of six blocks was considered essential for the storage of future trajectory data.

The blockchain used in this study was also evaluated in terms of reliability [55], and its error rates were considered as the performance index. Error rates arising from failures in block execution were measured while various consensus mechanisms were experiencing adversarial attacks. Concretely, Leader-based, Leader-free, and Deterministic consensus methodologies were utilized.

Table 3 shows that the leader-free consensus methodologies caused 0.63% block execution error rates, while deterministic and leader-based approaches caused 2.03% and 1.86% block execution error rates, respectively. In accordance with the error rate values, it can be inferred the leader-free blockchain is more reliable than deterministic and leader-based consensus protocols in terms of adversarial attacks resiliency.

Table 3. Blockchain Reliability relying on different Consensus Methodology Approaches.

	Consensus Methodology Approaches		
	Deterministic	Leader-Based	Leader-Free
Error Rate %	2.03	1.86	0.63

For a comparative analysis, a Long Short-Term Memory model (LSTM) [30] was employed. Adversarial attacks based on Adapted Fast Gradient Sign Method (AFGSM) were imposed in order to attack resiliency evaluation. Excluding adversarial attacks, the prediction accuracy stood at 99.51% for LSTM and 99.1% for GAN. These findings imply that both methods can effectively predict future trajectories as they are not facing adversarial samples.

To further scrutinize the efficacy of the LSTM and GAN models, another analysis was carried out when adversarial attacks were considered. The model's effectiveness was assessed while adversarial samples (generated via AFGSM) were being imposed. Table 4 presents the Fooling Rate (%) for both the GAN and LSTM models under adversarial attacks.

Table 4. LSTM and GAN Model Performance under White-Box Attacks Generated by the AFGSM.

Iterations		1	2	3	4	5
Fooling Rate [%]	LSTM methodology	29.4	41.7	48.2	54.1	59.9
	GAN methodology	31.5	43.2	49.5	56.7	61.3

In accordance with Table 4, there is a direct correlation between the increase in the number of iterations and the rise in the fooling rate. Both the LSTM and GAN models are sensitive to adversarial samples generated through AFGSM. After five iterations, the LSTM slightly outperforms the GAN in terms of fooling rate (59.9% vs. 61.3%). In both cases, the trajectory prediction models could be deemed unsuccessful against adversarial attacks. Consequently, defense strategies were devised, including Adversarial Retraining (AR) for white-box attacks and Generative Adversarial Networks (GANs) secured by Blockchain Ledger Technology (BLT) for black-box attacks.

Table 5 illustrates the effectiveness of the defense mechanisms in relation to their fooling rates when confronted with black-box attacks.

Table 5. Performance of the Defense Mechanisms Adversarial Retraining, GAN, and Blockchain Undergoing Black-Box Attacks.

Iterations		1	2	3	4	5
Fooling Rate [%]	AR-LSTM	25.4	14.7	11.1	10.3	9.8
	GAN	27.3	12.5	8.4	5.5	4.8
	GAN-BLT	13.7	7.6	4.8	2.9	2.8

Table 5 outlines the outcomes confirming that the AR defense implemented on the LSTM (AR-LSTM) exhibited the lowest resilience (9.8% fooling rate after five iterations) when confronted with black-box adversarial samples. In contrast, the GAN defense method recorded nearly double the efficacy (4.8% fooling rate after five iterations) in comparison to Adversarial Retraining. The GAN defense methodology enhanced by Blockchain Ledger Technology (GAN-BLT) demonstrated the highest performance, causing a 2.8% fooling rate after five iterations. The incorporation of BLT notably amplified the efficiency of the GAN defense methodology. Nevertheless, BLT could yield even greater effectiveness if the occurrence of transaction execution failures during data registration in new blocks was reduced.

5. Conclusions

A method resilient to adversarial attacks was developed for predicting aircraft trajectories. A trajectory prediction model was designed based on a Generative Adversarial Network (GAN). Demonstrating its capability, the GAN effectively predicted forthcoming trajectories using the provided UAS-S4 trajectory database, encompassing vectors containing latitude, longitude, altitude, heading, speed, and time.

The adversarial attack concept was explained, showcasing the GAN's ability for producing adversarial samples during its training process. The designed GAN was subjected to a comparison with the Long-Short Term Memory trajectory prediction model, evaluating their respective robustness against attacks. Both the LSTM and GAN models were evaluated, during which they were exposed to adversarial attacks founded on the Adapted Fast Gradient Sign Method (AFGSM). The resulting fooling rates validated that both models were vulnerable to adversarial samples generated through a white-box approach.

In order to formulate effective defense strategies, algorithms such as Adversarial Retraining (AR), Generative Adversarial Networks, and Blockchain Ledger Technology (BLT) were developed. The GAN-BLT algorithm that was ultimately designed showed the highest performance compared to the three defense algorithms, in which it recorded a

fooling rate of 2.8%. The GAN-BLT model exhibits the ability to excel beyond both GAN and AR-LSTM defense strategies when confronted with either white- or black-box attacks.

Author Contributions: Conceptualization, S.M.H.; Methodology, S.M.H. and S.A.H.; Software, S.M.H. and S.A.H.; Validation, S.M.H., R.M.B. and G.G.; Formal analysis, S.M.H., S.A.H. and G.G.; Investigation, S.M.H. and S.A.H.; Resources, R.M.B. and G.G.; Data curation, S.M.H., S.A.H. and G.G.; Writing—original draft, S.M.H.; Writing—review & editing, R.M.B. and G.G.; Supervision, R.M.B. and G.G.; Project administration, R.M.B.; Funding acquisition, R.M.B. and G.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by NSERC within the Canada Research Chairs program, which made possible the realization of this research and the publication of this paper. Ruxandra Botez is the Canada Research Chair Tier 1 Holder in Aircraft Modeling and Simulation New Technologies.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Special thanks are due to the Natural Sciences and Engineering Research Council of Canada (NSERC) for the Canada Research Chair Tier 1 in Aircraft Modeling and Simulation Technologies funds. We would also like to thank Odette Lacasse and Oscar Carranza for their support at ETS, as well as Hydra Technologies' team members Carlos Ruiz, Eduardo Yakin, and Alvaro Gutierrez Prado in Mexico. Finally, we wish to express our appreciation to the Canada Foundation for Innovation CFI, the Ministère de l'Économie et de l'Innovation and Hydra Technologies for their support of the acquisition of the UAS-S4 at the LARCASE.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Nomenclature

D	=	Discriminator network
G	=	Generator network
h	=	number of noise samples
i	=	Number of steps for future trajectory prediction
j	=	Number of executed transactions
N	=	Number associated with a block in the chain
T_n	=	Time during which the aircraft is as step n
\hat{y}	=	Predicted Trajectory
z	=	Filter for feature extraction
ω	=	Sample space
(ω, μ_{ref})	=	Probability space
$P_G(\omega)$	=	Generator strategy
θ_G	=	Generator's weighing parameters

References

1. Ghommam, J.; Saad, M.; Mnif, F.; Zhu, Q.M. Guaranteed performance design for formation tracking and collision avoidance of multiple USVs with disturbances and unmodeled dynamics. *IEEE Syst. J.* **2020**, *15*, 4346–4357. [[CrossRef](#)]
2. Zhou, X.; Yu, X.; Guo, K.; Zhou, S.; Guo, L.; Zhang, Y.; Peng, X. Safety flight control design of a quadrotor UAV with capability analysis. *IEEE Trans. Cybern.* **2021**, *53*, 1735–1751. [[CrossRef](#)] [[PubMed](#)]
3. Cestino, D.; Crosasso, P.; Rapellino, M.; Cestino, E.; Frulla, G. Safety assessment of pharmaceutical distribution in a hospital environment. *J. Healthc. Technol. Manag.* **2013**, *1*, 10–21. [[CrossRef](#)]
4. Zhou, X.; Yu, X.; Zhang, Y.; Luo, Y.; Peng, X. Trajectory planning and tracking strategy applied to an unmanned ground vehicle in the presence of obstacles. *IEEE Trans. Autom. Sci. Eng.* **2020**, *18*, 1575–1589. [[CrossRef](#)]
5. Papachristos, C.; Khattak, S.; Alexis, K. Uncertainty-aware receding horizon exploration and mapping using aerial robots. In Proceedings of the 2017 IEEE International Conference on Robotics and Automation (ICRA), Singapore, 29 May–3 June 2017; pp. 4568–4575.

6. Ghommam, J.; Saad, M.; Wright, S.; Zhu, Q.M. Relay manoeuvre based fixed-time synchronized tracking control for UAV transport system. *Aerosp. Sci. Technol.* **2020**, *103*, 105887. [[CrossRef](#)]
7. Qiu, D.; Qiu, D.; Wu, B.; Gu, M.; Zhu, M. Hierarchical control of trajectory planning and trajectory tracking for autonomous parallel parking. *IEEE Access* **2021**, *9*, 94845–94861. [[CrossRef](#)]
8. Ayhan, S.; Samet, H. Aircraft trajectory prediction made easy with predictive analytics. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, New York, NY, USA, 13–17 August 2016; pp. 21–30.
9. Lee, H.; Kim, H.; Kim, H.J. Planning and control for collision-free cooperative aerial transportation. *IEEE Trans. Autom. Sci. Eng.* **2016**, *15*, 189–201. [[CrossRef](#)]
10. Rekkas, C.; Rees, M. Towards ADS-B implementation in Europe. In Proceedings of the Tyrrhenian International Workshop on Digital Communications-Enhanced Surveillance of Aircraft and Vehicles, Capri, Italy, 3–5 September 2008; pp. 1–4.
11. Chan, W.N.; Barmore, B.E.; Kibler, J.L.; Lee, P.U.; O'Connor, C.J.; Palopo, K.; Thippavong, D.P.; Zelinski, S.J. Overview of NASA's air traffic management-exploration (ATM-X) project. In Proceedings of the AIAA Aviation Forum 2018, Atlanta, GA, USA, 25–29 June 2018.
12. Bolić, T.; Ravenhill, P. SESAR: The past, present, and future of European air traffic management research. *Engineering* **2021**, *7*, 448–451. [[CrossRef](#)]
13. Murrieta-Mendoza, A.; Botez, R. Aircraft vertical route optimization deterministic algorithm for a flight management system. In Proceedings of the SAE 2015 AeroTech Congress & Exhibition, Seattle, WA, USA, 22–24 September 2015.
14. Vaddi, S.; Kwan, J.; Fong, A.; Cheng, V. Deterministic and probabilistic conflict detection algorithms for nextgen airport surface operations. In Proceedings of the AIAA Guidance, Navigation, and Control Conference, Minneapolis, MN, USA, 13–16 August 2012; p. 4974.
15. Zhao, Y.; Schultz, R.; Zhao, Y.; Schultz, R. Deterministic resolution of two aircraft conflict in free flight. In Proceedings of the Guidance, Navigation, and Control Conference, New Orleans, LA, USA, 11–13 August 1997; p. 3547.
16. Bacchini, A.; Cestino, E. Key aspects of electric vertical take-off and landing conceptual design. *Proc. Inst. Mech. Eng. Part G J. Aerosp. Eng.* **2020**, *234*, 774–787. [[CrossRef](#)]
17. Huang, X.; Rosman, G.; Gilitschenski, I.; Jasour, A.; McGill, S.G.; Leonard, J.J.; Williams, B.C. HYPER: Learned hybrid trajectory prediction via factored inference and adaptive sampling. In Proceedings of the International Conference on Robotics and Automation (ICRA), Philadelphia, PA, USA, 23–27 May 2022; pp. 2906–2912.
18. Dunbar, W.B. *Distributed Receding Horizon Control of Multiagent Systems*; California Institute of Technology: Pasadena, PA, USA, 2004.
19. Izadi, H.; Gordon, B.; Zhang, Y. Safe path planning in the presence of large communication delays using tube model predictive control. In Proceedings of the AIAA Guidance, Navigation, and Control Conference, Toronto, ON, Canada, 2–5 August 2010; p. 8425.
20. Gonzalo, J.; Domínguez, D.; López, D. On the analytic and numeric optimisation of airplane trajectories under real atmospheric conditions. In Proceedings of the AIP Conference Proceedings, Bucharest, Romania, 16–20 June 2014; pp. 348–357.
21. Franco, A.; Rivas, D.; Valenzuela, A. Probabilistic aircraft trajectory prediction in cruise flight considering ensemble wind forecasts. *Aerosp. Sci. Technol.* **2018**, *82*, 350–362. [[CrossRef](#)]
22. Douglas, B.C.; Crowell, M. Long-term shoreline position prediction and error propagation. *J. Coast. Res.* **2000**, *16*, 145–152.
23. Wiest, J.; Höffken, M.; Kreßel, U.; Dietmayer, K. Probabilistic trajectory prediction with Gaussian mixture models. In Proceedings of the IEEE Intelligent Vehicles Symposium, Madrid, Spain, 3–7 June 2012; pp. 141–146.
24. Afzal, Z.R.; Prabhakar, P.; Prabhakar, P. Optimal tool path planning for 3D printing with spatio-temporal and thermal constraints. In Proceedings of the 6th Indian Control Conference (ICC), Hyderabad, India, 18–20 December 2019; pp. 176–181.
25. Baklacioglu, T.; Cavcar, M. Aero-propulsive modelling for climb and descent trajectory prediction of transport aircraft using genetic algorithms. *Aeronaut. J.* **2014**, *118*, 65–79. [[CrossRef](#)]
26. Wang, X.; Yang, R.; Zuo, J.; Xu, X.; Yue, L. Trajectory prediction of target aircraft based on HPSO-TPFENN neural network. *Xibei Gongye Daxue Xuebao/J. Northwestern Polytech. Univ.* **2019**, *37*, 612–620. [[CrossRef](#)]
27. Ma, S.; Liu, S.; Meng, X. Optimized BP neural network algorithm for predicting ship trajectory. In Proceedings of the IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 12–14 June 2020; pp. 525–532.
28. Mehrjerdi, H.; Saad, M.; Ghommam, J.; Zerigui, A. Optimized neuro-fuzzy coordination for multiple four wheeled mobile robots. *Inf. Technol. J.* **2010**, *9*, 1557–1570. [[CrossRef](#)]
29. Pang, Y.; Zhao, X.; Yan, H.; Liu, Y. Data-driven trajectory prediction with weather uncertainties: A Bayesian deep learning approach. *Transp. Res. Part C Emerg. Technol.* **2021**, *130*, 103326. [[CrossRef](#)]
30. Hashemi, S.M.; Botez, R.M.; Grigorie, T.L. New reliability studies of data-driven aircraft trajectory prediction. *Aerospace* **2020**, *7*, 145. [[CrossRef](#)]
31. Hutchins, D.; Schlag, I.; Wu, Y.; Dyer, E.; Neyshabur, B. Block-recurrent transformers. *Adv. Neural Inf. Process. Syst.* **2022**, *35*, 33248–33261.
32. Van Iersel, Q.G.; Murrieta-Mendoza, A.; Felix Patron, R.S.; Hashemi, S.M.; Botez, R.M. Attack and Defense on Aircraft Trajectory Prediction Algorithms. In Proceedings of the AIAA AVIATION 2022 Forum, Chicago, IL, USA, 27 June–1 July 2022; p. 4027.

33. Shang, F.; Wang, B.; Li, T.; Tian, J.; Cao, K.; Guo, R. Adversarial examples on deep-learning-based ADS-B spoofing detection. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 1734–1737. [[CrossRef](#)]
34. Huang, S.; Papernot, N.; Goodfellow, I.; Duan, Y.; Abbeel, P. Adversarial attacks on neural network policies. *arXiv* **2017**, arXiv:1702.02284.
35. Goodfellow, I.; Pouget-Abadie, J.; Mirza, M.; Xu, B.; Warde-Farley, D.; Ozair, S.; Courville, A.; Bengio, Y. Generative adversarial nets. In Proceedings of the Advances in Neural Information Processing Systems, Montreal, QC, Canada, 8–13 December 2014; Volume 27.
36. Pang, Y.; Liu, Y. Conditional generative adversarial networks (CGAN) for aircraft trajectory prediction considering weather effects. In Proceedings of the AIAA Scitech 2020 Forum, Orlando, FL, USA, 6–10 January 2020; p. 1853.
37. Xiang, J.; Xie, J.; Chen, J. Landing Trajectory Prediction for UAS Based on Generative Adversarial Network. In Proceedings of the AIAA SCITECH 2023 Forum, National Harbor, MD, USA, 23–27 January 2023; p. 0127.
38. Wu, X.; Yang, H.; Chen, H.; Hu, Q.; Hu, H. Long-term 4D trajectory prediction using generative adversarial networks. *Transp. Res. Part C Emerg. Technol.* **2022**, *136*, 103554. [[CrossRef](#)]
39. Liu, R.W.; Liang, M.; Nie, J.; Deng, X.; Xiong, Z.; Kang, J.; Yang, H.; Zhang, Y. Intelligent data-driven vessel trajectory prediction in marine transportation cyber-physical system. In Proceedings of the IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), Melbourne, Australia, 6–8 December 2021; pp. 314–321.
40. Kakavand, H.; Kost De Sevres, N.; Chilton, B. *The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies*; SSRN: New York, NY, USA, 2017.
41. Bhutta, M.N.M.; Khwaja, A.A.; Nadeem, A.; Ahmad, H.F.; Khan, M.K.; Hanif, M.A.; Song, H.; Alshamari, M.; Cao, Y. A survey on blockchain technology: Evolution, architecture and security. *IEEE Access* **2021**, *9*, 61048–61073. [[CrossRef](#)]
42. Abdellatif, T.; Brousmiche, K.-L. Formal verification of smart contracts based on users and blockchain behaviors models. In Proceedings of the 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–5.
43. Krichen, M.; Lahami, M.; Al-Hajja, Q.A. Formal methods for the verification of smart contracts: A review. In Proceedings of the 15th International Conference on Security of Information and Networks (SIN), Sousse, Tunisia, 11–13 November 2022; pp. 1–8.
44. Hashemi, S.M. Novel Trajectory Prediction and Flight Dynamics Modelling and Control Based on Robust Artificial Intelligence Algorithms for the UAS-S4. Ph.D. Thesis, École de Technologie Supérieure, Montréal, QC, Canada, 2022.
45. Hashemi, S.M.; Botez, R.M. Support Vector Regression Application for the Flight Dynamics New Modelling of the UAS-S4. In Proceedings of the AIAA SCITECH 2022 Forum, San Diego, CA, USA, 3–7 January 2022; p. 2576.
46. Hashemi, S.M.; Botez, R.M. A Novel Flight Dynamics Modeling Using Robust Support Vector Regression against Adversarial Attacks. *SAE Int. J. Aerosp.* **2023**, *16*. [[CrossRef](#)]
47. Hashemi, S.; Botez, R. Lyapunov-based robust adaptive configuration of the UAS-S4 flight dynamics fuzzy controller. *Aeronaut. J.* **2022**, *126*, 1187–1209. [[CrossRef](#)]
48. Kuitche, M.; Yañez-Badillo, H.; Botez, R.; Hashemi, S. Stabilisation, tracking and disturbance rejection control design for the UAS-S45 Balaam. *Aeronaut. J.* **2022**, *126*, 1474–1496. [[CrossRef](#)]
49. Creswell, A.; White, T.; Dumoulin, V.; Arulkumaran, K.; Sengupta, B.; Bharath, A.A. Generative adversarial networks: An overview. *IEEE Signal Process. Mag.* **2018**, *35*, 53–65. [[CrossRef](#)]
50. Douzas, G.; Bacao, F. Effective data generation for imbalanced learning using conditional generative adversarial networks. *Expert Syst. Appl.* **2018**, *91*, 464–471. [[CrossRef](#)]
51. Goodfellow, I.; Pouget-Abadie, J.; Mirza, M.; Xu, B.; Warde-Farley, D.; Ozair, S.; Courville, A.; Bengio, Y. Generative adversarial networks. *Commun. ACM* **2020**, *63*, 139–144. [[CrossRef](#)]
52. Gui, J.; Sun, Z.; Wen, Y.; Tao, D.; Ye, J. A review on generative adversarial networks: Algorithms, theory, and applications. *IEEE Trans. Knowl. Data Eng.* **2021**, *35*, 3313–3332. [[CrossRef](#)]
53. Hashemi, S.; Hashemi, S.A.; Botez, R.M.; Ghazi, G. A Novel Air Traffic Management and Control Methodology using Fault-Tolerant Autoencoder and P2P Blockchain Application on the UAS-S4 Ehécatl. In Proceedings of the AIAA SCITECH 2023 Forum, National Harbor, MD, USA, 23–27 January 2023; p. 2190.
54. Hashemi, S.; Hashemi, S.A.; Botez, R.M.; Ghazi, G. Attack-tolerant Trajectory Prediction using Generative Adversarial Network Secured by Blockchain Application to the UAS-S4 Ehécatl. In Proceedings of the AIAA SCITECH 2023 Forum, National Harbor, MD, USA, 23–27 January 2023; p. 2192.
55. Hashemi, S.M.; Hashemi, S.A.; Botez, R.M.; Ghazi, G. A Novel Fault-Tolerant Air Traffic Management Methodology Using Autoencoder and P2P Blockchain Consensus Protocol. *Aerospace* **2023**, *10*, 357. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.