Applied Information Technology And Computer Science Vol. 2 No. 2 (2021) 141-154

AITCS

Homepage: http://publisher.uthm.edu.my/periodicals/index.php/aitcs
e-ISSN :2773-5141

A Comparative Study of Drone GPS Spoofing Detection Algorithm Between Naïve Bayes and Artificial Neural Network

Nurul Ain Wahida Azaha, Shamsul Kamal Ahmad Khalid*

Fakulti Sains Komputer and Teknologi Maklumat,
Universiti Tun Hussein Onn Malaysia, Parit Raja, 86400, MALAYSIA

DOI: https://doi.org/10.30880/aitcs.2021.02.02.010
Received 14 June 2021; Accepted 09 September 2021; Available online 30 November 2021

Abstract: Global Positioning System (GPS) spoofing attack overwhelms a target Unmanned Arial Vehicle (UAV) or drone by sending spoof data to interrupt the location of the drone. Researchers have done many works in overcoming the GPS spoofing attack yet the performance analysis of some of the common methods are not available. In this study, the Naïve Bayes and Artificial Neural Network (ANN) classification and detection of GPS spoofing are analyzed. The experiment was carried out and tested on UAV Attack dataset. The experiments cover several performance metrics like True Positive Rate, False Positive Rate, Error rate and accuracy in identifying the best performance classifiers. At the end of the study, the ANN classifiers are identified to be best classifiers with 91.68% of accuracy in average compared to Naïve Bayes classifiers with 87.26% of accuracy in average for the accuracy of GPS spoofing detection. The TPR of ANN is higher as compared to Naïve Bayes, while the FPR of ANN is lower as compared to Naïve Bayes.

Keywords: GPS Spoofing, Machine Learning, Deep Learning, Naïve Bayes, Artificial Neural Network

1. Introduction

Drone or unmanned aerial vehicles (UAVs) are aircraft in absence of a human pilot on board. Otherwise, an operator or system control the flight autonomously. There are two type of drone which is military and civilian [1]. Drone function properly because it has various of module. The modules also can give potential security vulnerabilities to the drone. Originally the drone is used by military to carry out high risk mission. Nowadays, drone has been used for many purposes by military and civil. The drone can be exposed to the threats such as jamming, Global Positioning System (GPS) spoofing and message injection. GPS spoofing is one of the top threats for the drone. The goal of this paper is to make comparative study of GPS spoofing detection algorithms between Naïve Bayes and Artificial Neural Network (ANN).

In several years drone has been for the multipurpose task such as surveillance, emergency rescue, aerial photography, disaster management, environmental protection is increasing at rapid growth rate

*Corresponding author: shamsulk@uthm.edu.my

[2], [3], [4]. For the drone, hijacked by GPS spoofing by an unauthorized person is the top threat besides jamming, message injection, and message modification [5], [6]. The covert and overt attacks are two kinds of GPS spoofing attacks. Cover attack occurred when attackers avoid activating spoofing detection techniques within the GPS receiver. At that point, the attacker can precisely monitor the drone and broadcast the spoofing signal with specific power and frequencies. The attacker may also be forced to restrict the changes it can force on a drone. Meanwhile, the overt attack is a contrast to the covert attack because the attacker has the risk of being detected and only can impose to any location [6].

Civil GPS signals is not secure because the signal is open to the public and unencrypted while military GPS signals is heavily encrypted but in 2011, a CIA stealth drone (RQ170) was hijacked in Iran by GPS spoofing. Iran military makes RQ170 land in Iran rather than Afghanistan [4]. The transmission GPS signal transmits from the satellites to the earth. Because of significant distance, the signal is very week when it is received on earth. When a spoofing attack occurred, the receiver believes that the spoofing signal is the true signal. This way, the receiver is controlled by the spoofing signal [7].

Figure 1 shows an example of GPS-spoofing-based hijacking of a drone. In the starting point, the drone plans to fly to the planned destination. At the middle of the plans, GPS spoofing starts. Then the counterfeit GPS signal report the wrong coordinate and the drone deviate from its planned route. Based on Figure 1, the drone flies in the opposite direction of the plan after a counterfeit GPS signal report the wrong coordinate [4].

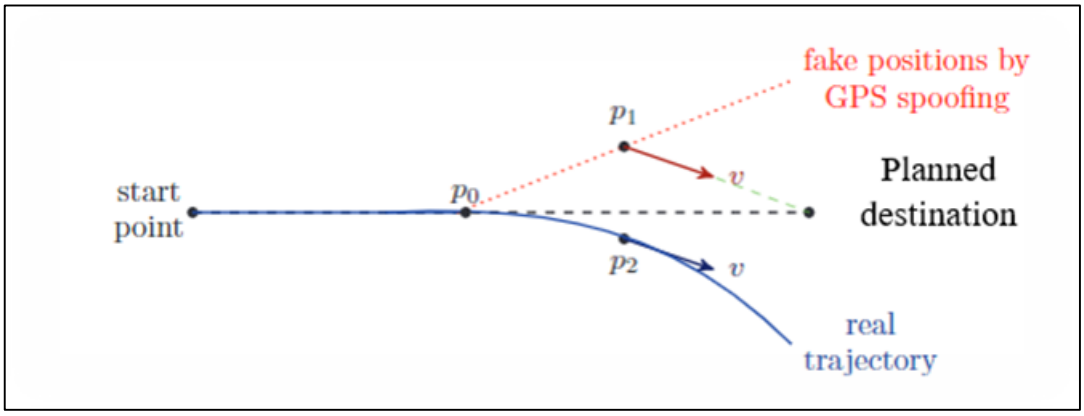


Figure 1: Example of drone hijacking by GPS spoofing [2]

The following are the objectives of this project:

- To study GPS spoofing detection using two well-known classifiers which is Naïve Bayes and Artificial Neural Network (ANN).
- To perform experiments using Naïve Bayes and Artificial Neural Network classifiers in the GPS spoofing detection problem.
- To evaluate the performance of the classifiers in terms of accuracy.

2. Literature Review

This chapter, will focus on drone system, GPS spoofing and the classifiers in drone GPS spoofing detection problem which is Naïve Bayes and Artificial Neural Network (ANN).

2.1 Drones

A drone, in technological terms is an unmanned aircraft vehicle (UAV). In few years, a number of events have occurred leading to enormous changes in the way of understanding the Drone Market. On

the one hand, a large number of companies providing drone products and services in general, and electric multicopters in particular, have arisen, reshaped and enriched the industry. Because of legislative difficulties, this scenario has turned the drone industry that initially small into a very complicated environment, with massive competition and a much-reduced market.

Satellites, UAVs, datalinks and ground terminals that relate to smart phones or remote controls constitute a full drone system. Satellites relay GPS signals to UAVs and need at least four satellites to locate an exact location. Wi-Fi or radio is the mainstream of modern UAV-ground terminal communication. There is a small contact distance from Wi-Fi, typically just a few hundred meters. Radio contact is longer and is capable of covering thousands of meters [8].

A UAV normally consists of a power system, a control system, various sensors and a module for communication. In particular, for rotors with one or more batteries, the power system provides power for the entire UAV and sufficient energy is a requirement for flight. By regulating the rotation of rotors according to instructions, the control system may adjust flight attitudes. Sensors sense information about the environment and send information to the control system.

In the drone system, it is possible for each part of the system to have different vulnerabilities. The possible threats that may occur for each security objective maybe differ. Table 1 shows the potential threats that may occur for each component of the drone system.

Table 1: Potential threats on drone system [9]

Security Objective	System Objective	Attack Method
Confidentiality	Ground Control System (GCS)	Virus
		Malware
		Keyloggers
		Trojans
	Drone	Spoofing
	Communication Link	Eavesdropping
		Man-in-the-middle
Integrity	Communication Link	Message injection
		Replay attack
		Man-in-the-middle
		Message deletion
Availability	Ground Control System (GCS)	Denial of service
	Drone	Fuzzing
		Jamming
	Communication Link	Flooding
		Buffer overflow

2.2 Classification method

Based on Bayes' Theorem, Bayesian classifier are statistical classifiers and known as conditional Theorem. Bayesian classifiers or known as Naïve Bayes (NB) is to predict the probability of the data.

In the data mining algorithms for classification, NB is the one of the most popular. It makes conclusion based on the probability based on the training data. This assumption is drive by the requirement to estimate the multivariate probabilities from the training data. In practice, classification

performance is affected by the attribute independent assumption. Consequently, direct estimation of each important multi-variate probability will not be reliable. NB circumvents this predicament by its conditional independence assumption. In spite of this strict independence assumption, NB is a really competent classifier in many real-world applications.

The main reason for choosing this method to use as a part of the research study is because it is easily programmable by the researchers into the particular tools for an example like Google Colaboratory, MATLAB, WEKA etc. Thus, the time consumption on working with the code of the program is not affected by the research. Besides that, this classifier also works really faster and it is easy to be trained in the data analysis.

Deep learning is a subset of Artificial Intelligence and machine learning. Deep learning is the type of machine learning inspired by the structure of the human brain. In terms of deep learning, this structure is called an artificial neural network. The example of the different between machine and deep learning are machine learning can classify based on the featured of each class while deep learning is picked out by the neural network without human intervention.

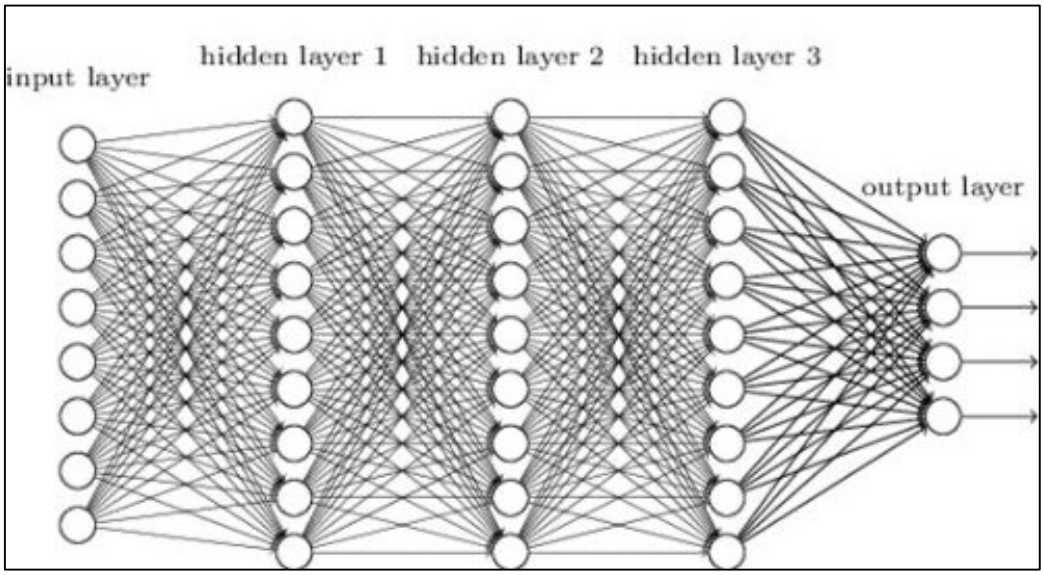


Figure 2: Deep learning neural network [10]

Neuron is the basic building block of ANN. The neuron gets input layer and has output layer as shown in Figure 2. Input layer contain input value which is independent variable. In the experiment, the value will be normalized to get the same values. It is to make easier for ANN to process the values. The output value that contains output value can be continues, binary or categorical variable.

In this study, Google Colaboratory is used to run the experiments in detecting GPS Spoofing for selected classifiers. Colaboratory is a product from Google Research. It is a web-based Python editor that allows anybody to create and run arbitrary Python code. It's particularly useful for machine learning, data analysis, and teaching.

2.3 Comparison between previous research works

Table 2 shows the comparison of method in spoofing detection.

Table 2: Comparison of method in spoofing detection

Research	Title of the research	Method used	Description

Selected	Detection of Spoofing Attack using Machine Learning base on Multi-Layer Neural Network in Single-Frequency GPS Receivers [11].	K-Nearest Neighbourhood Classifier, Naive Bayesian Classifier, and Design, Training and Validation of NN for Spoof Detection.	The research focused on Multi-Layer Neural Network in Single Frequency GPS Receivers. The proposed method is to detect the GPS spoofing based on multi-layer Neural Network.
	Detection of GPS Spoofing Attacks on Unmanned Aerial Systems [12].	Neural network.	The research proposed a supervised machine learning method based on the artificial neural network to detect GPS spoofing signal. The classification of GPS signal used different features such as pseudo range, Doppler shift and signal-to-noise ratio (SNR).
	A Vision-Based GPS-Spoofing Detection Method for Small UAVs [13].	Vision-based.	The research is done to detect GPS spoofing based on the vision sensor. Monocular camera and inertia measure unit (IMU) are used to get drone velocity and position.
Proposed	A Comparative Study of Drone GPS Spoofing Detection between Naïve Bayes and Artificial Neural Network (ANN)	Naïve Bayes classifier and Artificial Neural Network classifier.	The proposed research study focused on the anomaly detection of GPS spoofing attack on drone though the proposed algorithm.

3. Methodology

In order to detect GPS spoofing, there are several methods available. In this thesis, two methods were studied, namely Naïve Bayes classifiers and Artificial Neural Network classifiers. In this chapter, the methodology used to investigate the methods will be described. Both methods will be configured and tested on Google Colaboratory platform.

3.1 Dataset Description

In this research, the UAV Attack Dataset [14] will be used. This dataset is the data of simulation of multiple drone platform experiences GPS spoofing attack. The standard Gazebo/PX4 was used for the simulation environment. Normal GPS signal are stopped when the attack starts and the Gazebo environment create and injected signal to the autopilots GPS sensor for 30 seconds. The flight survey is conducted for average 20 minutes flight time [14].

In this dataset, there are six drone platforms are used which are 3DR IRIS+ (Quadcopter, SITL), Holybro S500 (Quadcopter, HITL), Yuneec H480 (Hexacopter, SITL), DeltaQuad VTOL (VTOL, SITL), PX4 Standard Tailsitter (Tailsitter, SITL), PX4 Standard Plane (Plane, SITL) [14]. For each of

drone platform there are two data which is normal data and GPS Spoofing data. Normal data is when GPS Spoofing is not performed while GPS Spoofing data is the data that Gazebo inject the false signal for 30 seconds.

3.2 Classifier Algorithms

The following sections will be described about the Naive Bayes classifier and Artificial Neural Network classifier.

Naïve Bayes algorithm provides a simple probabilistic learning approach. The algorithm works by assuming attributes to find its belonging classes of data. According to this algorithm the attack and normal types of data is easily classified because the algorithm works by setting an event condition towards the data.

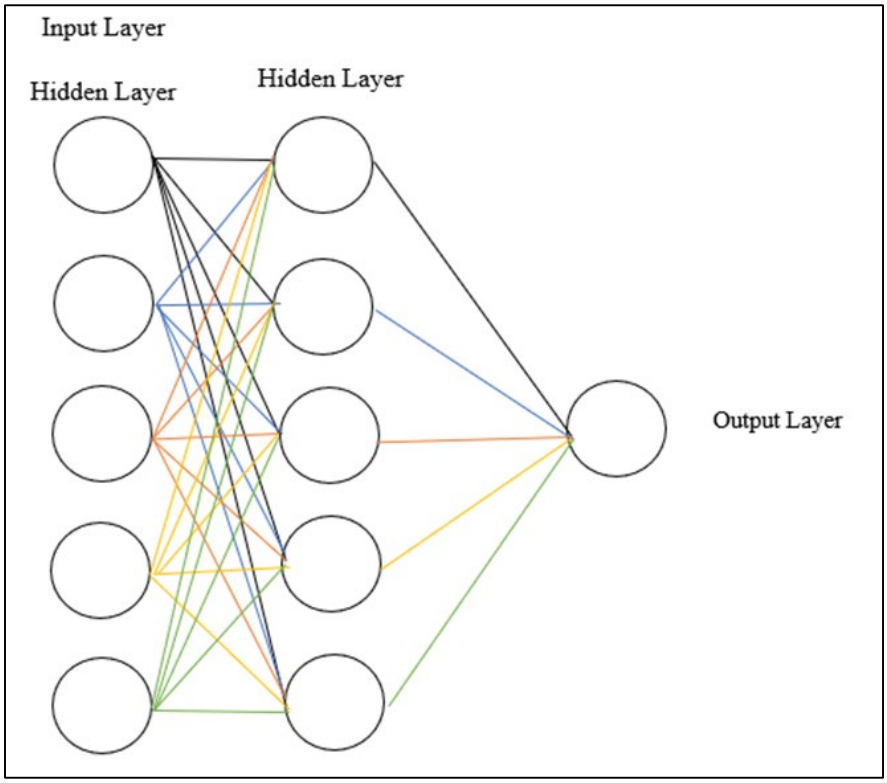
$$P(A|B) = \frac{P(B|A)}{P(A)P(B)} \qquad Eq.1$$

The presented Eq. 1 above is the base formula in Bayes theorem for analyzing the data. The equation works by calculating the probability of event A that is conditioned towards the data B. Thus, it works by first calculating the probability of data B conditioned to the event A and then the probability A and B is multiplied and normalized as in the equation shown. So, the same concept is used in this study. The classes of data are set with a probability of occurrence value and the data are classified according to the probability value following the applied equation above.

Artificial Neural Network (ANN) are a type of machine learning algorithm inspired by biological neurons in the brain and central nervous system. The artificial neurons in one or more hidden layers are fed the inputs to the ANN, where they are weighted and processed to determine the output to the next layer. Back-propagation of errors based on gradient descent is frequently used in ANN, allowing the set of weights and biases for the hidden layer and output layer neurons to be adaptively modified. Because of its self-adaptive nature, ANN may capture very complicated and non-linear interactions between dependent and independent variables without the need for prior information. ANN have been used to solve a wide range of classification problems in a number of applications [15].

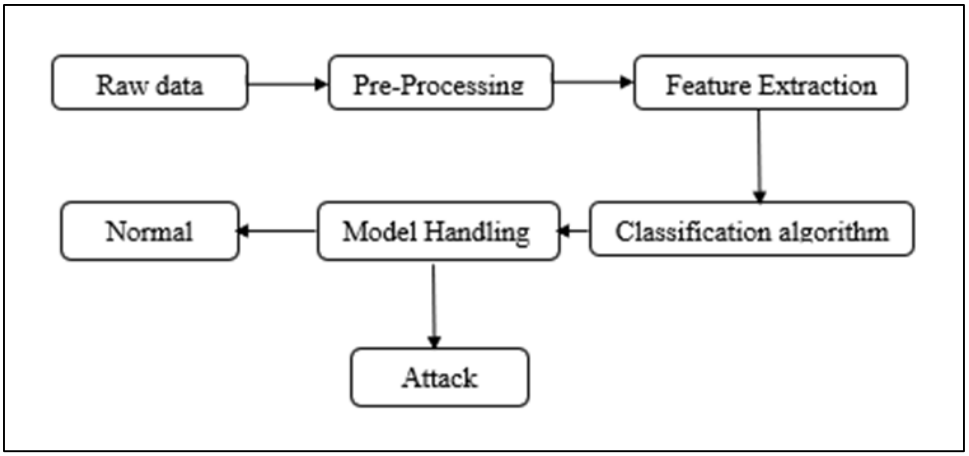
ANN consist from tree layers, input layer, hidden layer and output layer. In order to consider compelling to (0-1) range, the input and output layers must be numeric values. As a result, the data is normalized within the range before being passed to the input layer. In the hidden layer, the Weight is a set of performance parameters for the feed-forward neural network. Starting with random weights, bestowing the data, instance by instance, modifying the weights imparting the error for each instance, and continuing until the error is very small, the training method of the ANN is exaggerated. The weights are adjusted by the backpropagation algorithm for each instance based on the variance of the actual output and function output [16].

As seen in Figure 3, the experiment for ANN that will discuss in next section have five inputs for the first and hidden layer, five inputs for second hidden layer and 1 input for output layer. In this study, ANN was used to analyzed the performance of this classifiers in GPS spoofing detecting in term of accuracy.



3.3 Research Framework

The framework for this research study explains about the process detection and classification of GPS spoofing attack using the UAV Attack Dataset. Through this development of GPS spoofing detection framework, the objective of the research study will be accomplished successfully. The Figure 4 below shows the step to conduct the study. The framework simplifies the process flow of this research classification into an understandable form.



Raw data is known as the data which is not undergoing any filtering and normalization process. Thus, for this experiment the raw data is obtained from UAV Attack dataset. The dataset consists of six types of drones and renamed as shown in Table 3. Then, the data are loaded and save as .CSV (Coma

delimited) file. Then, the data file is processed by removing the redundant data in it and divided it to 60:40 ratios for training and testing process.

Table 3: Dataset in UAV Attack Dataset

Dataset	Name of dataset in UAV Attack Dataset
A	PX4-PLANE-SITL
B	PX4-PLANE-SITL
C	PX4-QUAD-HITL
D	PX4-QUAD-SITL
E	PX4-TAIL-SITL
F	PX4-VTOL-SITL

Pre-processing of the data from the acquired UAV Attack dataset is an important process before it is used to publish into the learning machine. Through the preprocessing process the relevant data is identified for the study. In the UAV Attack dataset, it contains all together 88 features. From 88 features, there are 44 features categorized into numeric group while another 44 features are nominal group. The dataset is already divided in to classes that denotes normal and GPS spoofing. Table 4 describes the main two classes from the acquired dataset.

Table 4: Description of main classes in the dataset

Number	Classes	Descriptions
1	Normal	In this class, the data have normal GPS latitude and longitude.
2	GPS Spoofing	In this class, the data have same GPS latitude and longitude during flying

Table 5: Subclasses of attacks from main class

Number	Main class of attack	Sub classes
1	GPS spoofing attack	gps.lon, gps.lat, flightdistance, distanceToNextWP, distanceToHome, estimatorStatus.vorizPosRatio, estimatorStatus.vertPostRatio, estimatorStatus.horizPosAcccury, estimatorStatus.vertPosAccuracy.

Table 5 describe the derivative subclasses of GPS spoofing from the main classes presented in Table 4.

The 88 features from the acquired dataset were analyzed thoroughly by carrying out a pre-processing process in identifying GPS spoofing. In this UAV Attack dataset, the GPS spoofing can be identified by the features in Table 6.

Table 6: Features for GPS spoofing

Feature	Descriptions	Types
gps.lon	The longitude of drone during flying.	Discrete

gps.lat	The latitude of drone during flying.	Discrete
flightDistance	The distance of the drone fly.	Discrete

Table 6: (cont.)

Feature	Descriptions	Types
headingtoNextWP	Heading to the next Waypoint	Discrete
estimatorStatus.horizPosRatio	The horizontal position ratio estimator status.	Continuous
estimatorStatus.horizPosAcccur	The horizontal Position Accuracy estimator status	Continuous
estimatorStatus.vertPosRatio	The vertical position ratio estimator status	Continuous
estimatorStatus.vertPosAccuracy	The vertical position Accuracy estimator status	Continuous

In algorithm classification phase, the study comprises of two machine learning approaches namely Naïve Bayes algorithms and Artificial Neural Network (ANN) algorithm to test the dataset. The two methods are implemented in the chosen software Google Colaboratory and it is classified based on its performance and accuracy in detecting the GPS spoofing classified features from the dataset. Thus, the training and testing dataset are loaded into the classifiers to obtain the output.

Model building is the phase designed for GPS spoofing detection study at where, the dataset will undergo testing process for both implemented algorithms. The data stored in the dataset will be test based on its accuracy. Through the testing and training of the dataset, the difference between the two chosen approaches is classified and compared.

The last phase of the framework is results. The data packets from the dataset are classified in the form of graphs. The graphs are developed based on the classification process that conducted in the model building phase. The graphs are also presented based on the tasks that comprises of Error Rate, accuracy True Positive Rate (TPR) and False Positive Rate (FPR)the dataset. Thus, in overall this result phase is utilized to analyze and categorized the data packets.

3.4 Performance Metrics

The following sections will discuss performance metrics that will be used in the experiments namely accuracy, error rate, TPR and FPR.

Accuracy is a measurement that calculates on the percentage of correctness in predicting the infected data packets. This measurement helps in determining whether all the decisions that is predicted and taken is correct or wrong. The Eq. 2 designed below shows the way on calculating the accuracy of the testing models [17].

$$n = \frac{Nc}{Nt} \qquad Eq.2$$

n- Accuracy measurement.

Nc- Testing that classified as the correct numbers.

Nt- Number of testing's.

Error rate is defined as the classification of incorrect decisions during the analysis of data packets. The Eq. 3 below is used to calculate the error rates from the classification.

$$\sum = \frac{Nt-Nc}{Nt} \quad Eq.3$$

∑- Error rate measurement.

Nc- Testing that classified as the correct numbers.

Nt- Number of testing's.

True Positive Rate (TPR) is the criteria discussed when the system identifies the uninfected data packets as the infected data packets and blocks the entry of the data into the system [17]. The Eq. 4 below is used in calculating the TPR.

$$TPR = \frac{TP}{TP+FN} \quad Eq.4$$

FP- Number of True positive.

FN- Number of False negative.

False Positive Rate (FPR) is the criteria discussed where the infected data packets are accepted by the system as the uninfected packets and allow its entry to the system without any denial [17]. The Eq. 5 below indicates the calculation for FPR.

$$FPR = \frac{FP}{FB+TN} \quad Eq.5$$

FP- Number of False positive.

TN- Number of True negative.

4. Result and Analysis

4.1 Experiment with the classifiers

In this experiments phase, the classifiers performance evaluation is conducted based on the proposed algorithm which are Naïve Bayes and Artificial Neural Network (ANN). In these experiments the error rate, True Positive rate (TPR), False Positive rate (FPR) and F- Measure of the classifiers in analyzing the dataset is tabulated with its percentage level. There are six datasets that used to test and train using the proposed algorithm are split with the ratio 60:40 randomly in the experiments. The training dataset contains 60% of the data and the testing dataset contains 40% of the data. The classifier is trained well with many data in the training phase in order it to function normally.

4.2 Performance Metrics

The performance metrics used in these two experiments to study the dataset with the classifiers are Accuracy, Mean Absolute Error (MAE), True Positive Rate (TPR) and False Positive Rate (FPR). The formulas used in calculating the results are presented in the previously section.

Through result obtained, Naïve Bayes classifiers is able to identify the A, B, C, D, E, and F dataset with the accuracy 95.00%, 74.58%, 94.00%, 97.00%, 79.00%, and 84.00% while Artificial Neural Network (ANN) able to classify the A, B, C, D, E, and F dataset accurately by 98.00%, 89.585 %, 94.50%, 97.00%, 82.00%, and 89.00% as shown in Table 7 and Figure 5. The average of accuracy for

each classifier is calculated as in Eq. 6 and the average accuracy for Naïve Bayes is 87.26% while ANN is 91.68%.

$$Average = \frac{Sum\ of\ accuracy\ for\ each\ dataset}{Number\ of\ dataset} \quad Eq.6$$

Table 7: Accuracy of selected classifiers

Dataset	Percentage of accuracy for Naïve Bayes (NB) (%)	Percentage of accuracy for Artificial Neural Network (ANN) (%)
A	95.00	98.00
B	74.58	89.58
C	94.00	94.50
D	97.00	97.00
E	79.00	82.00
F	84.00	89.00

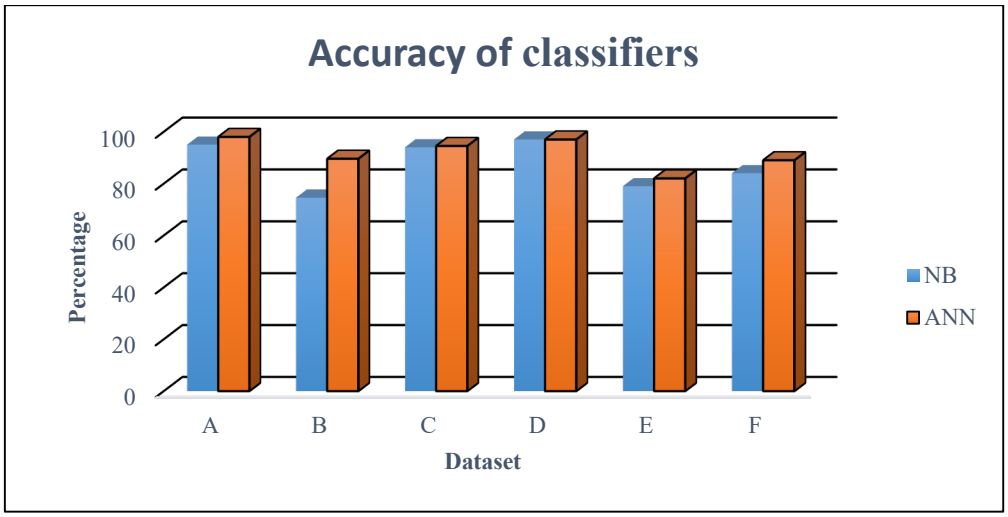


Figure 5: The graph of accuracy

Figure 6 show the mean absolute error for the two classifier's experiment. Based on Figure 5, the test dataset of A, B, C, D, E, and F for Artificial Neural Network (ANN) algorithm has lower error rate with the value 0.020, 0.104, 0.060, 0.025, 0.180, and 0.110 while for Naïve Bayes algorithm has higher error rate with value 0.050, 0.254, 0.060, 0.030, 0.210, and 0.160 as shown in Table 8.

Table 8: Error Rate of selected classifiers

Dataset	Error Rate for Naïve Bayes (NB)	Error Rate for Artificial Neural Network (ANN)
A	0.050	0.020
B	0.254	0.104
C	0.060	0.060
D	0.030	0.025
E	0.210	0.180
F	0.160	0.110

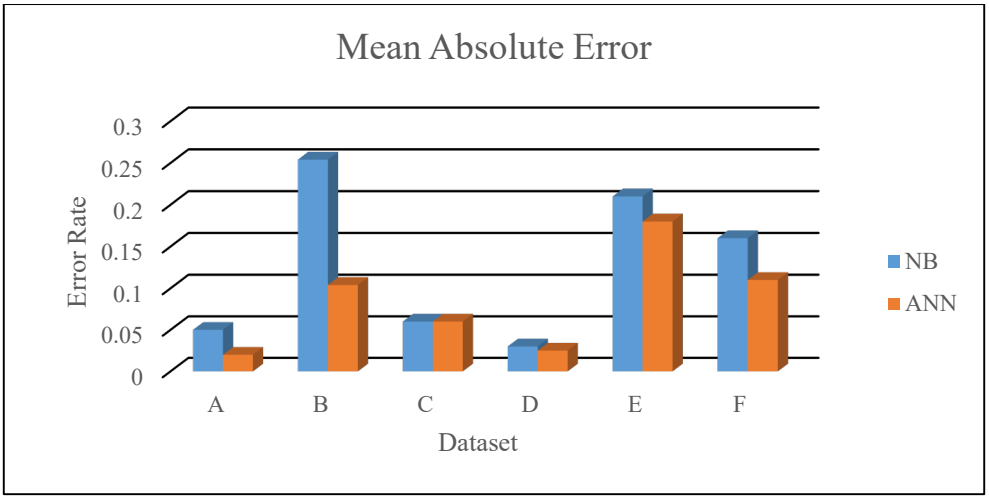


Figure 6: The graph of Mean Absolute Error

In the Table 9, the value for TPR and FPR obtained for testing dataset using Naïve Bayes and Artificial Neural Network classifiers are tabulated. The results are evaluated based on the number that TPR and FPR hold in the classification process. In theoretical, the highest TPR and lowest FPR is known to produce a best result. TPR values shows that the dataset is has positive Correctly classified features when compared to negative incorrectly classified features.

From the Table 9, the Artificial Neural Network (ANN) classifiers has TPR rate with the value 0.980, 0.896, 0.940, 0.975,0.820, for the A, B, C, D, E, and F test dataset. While in Naïve Bayes classifier the TPR value rate are 0.950, 0.746, 0.940, 0.970, 0.790, and 0.840for the A, B, C, D, E, and F test dataset. The highest TPR value obtains by A test dataset for ANN classifiers with value 0.980 while the highest TPR value obtains by A test dataset for Naïve Bayes classifier with value 0.970. The FPR value obtains by A, B, C, D, E, and F test dataset for ANN classifiers with value 0.020, 0.104, 0.060, 0.025, 0.180, and 0.110 while Naïve Bayes classifier with value 0.050, 0.254, 0.060, 0.030, 0.210, and 0.160. The lowest FPR value obtains by A test dataset for ANN classifiers with value 0.020 while the lowest FPR value obtains by B test dataset for Naïve Bayes classifier with value 0.030.

Table 9: True Positive Rate (TPR) and False Positive Rate (FPR)

Dataset	Classifier	TPR	FPR
A	NB	0.950	0.050
	ANN	0.980	0.020
B	NB	0.746	0.254
	ANN	0.896	0.104
C	NB	0.940	0.060
	ANN	0.940	0.060
D	NB	0.970	0.030
	ANN	0.975	0.025
E	NB	0.790	0.210
	ANN	0.820	0.180
F	NB	0.840	0.160
	ANN	0.890	0.110

5. Conclusion

Artificial Neural Network (ANN) algorithm and Naïve Bayes algorithm managed to classify the GPS spoofing based on the features of selected dataset. Other researcher has used many this algorithm to detect GPS spoofing and other threats. In this experiment, we selected nine features from the PX4-PLANE-SITL of UAV Attack dataset which can be obtain from as the training and testing dataset. We constructed the experiment using Google Colaboratory to get the accuracy and effectiveness of the result. This experiment evaluate dataset using the random spit size for testing and training which is 60:40 respectively. The higher prediction of the test result produced higher accuracy result and better performance. In this study, ANN have higher performance in term of accuracy than Naïve Bayes. The ANN achieve the 91.68% in average while Naïve Bayes only get 87.26 % in average for the accuracy of GPS spoofing detection. The TPR of ANN is higher as compared to Naïve Bayes, while the FPR of ANN is lower as compared to Naïve Bayes. The highest TPR value obtains by A test dataset for ANN classifiers with value 0.980 while the higher TPR value obtains by A test dataset for Naïve Bayes classifier with value 0.970. The lowest FPR value obtains by A test dataset for ANN classifiers with value 0.020 while the lowest FPR value obtains by A test dataset for Naïve Bayes classifier with value 0.030. This shows ANN is a more superior algorithm than Naïve Bayes.

Acknowledgement

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia for its support and encouragement throughout the process of conducting this study.

References

[1] D. He, S. Chan, and M. Guizani, “Communication Security of Unmanned Aerial Vehicles,” IEEE Wireless Communication, vol. 24, no. 4, pp. 134–139, Dec. 2016, doi: 10.1109/MWC.2016.1600073WC.

[2] Z. Renyu, S. C. Kiat, W. Kai, and Z. Heng, “Spoofing attack of drone,” in 2018 IEEE 4th International Conference on Computer and Communications, ICCC 2018, Dec. 2018, pp. 1239–1246, doi: 10.1109/CompComm.2018.8780865.

[3] N. Shijith, P. Poornachandran, V. G. Sujadevi, and M. M. Dharmana, “Spoofing technique to counterfeit the GPS receiver on a drone,” in Proceedings of 2017 IEEE International Conference on Technological Advancements in Power and Energy: Exploring Energy Solutions for an Intelligent Power Grid, TAP Energy 2017, Jun. 2018, pp. 1–3, doi: 10.1109/TAPENERGY.2017.8397268.

[4] Z. Feng et al., “Efficient drone hijacking detection using onboard motion sensors,” in Proceedings of the 2017 Design, Automation and Test in Europe, DATE 2017, May 2017, pp. 1414–1419, doi: 10.23919/DATE.2017.7927214.

[5] M. R. Manesh and N. Kaabouch, “Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions,” Computers and Security, vol. 85. Elsevier Ltd, pp. 386–401, Aug. 2019, doi: 10.1016/j.cose.2019.05.003.

[6] A. R. Eldosouky, A. Ferdowsi, and W. Saad, “Drones in Distress: A Game-Theoretic Countermeasure for Protecting UAVs Against GPS Spoofing,” IEEE Internet Things J., vol. 7, no. 4, pp. 2840–2854, Apr. 2020, doi: 10.1109/JIOT.2019.2963337.

[7] C. Jiang, S. Chen, Y. Chen, Y. Bo, Q. Xia, and B. Zhang, “Analysis of the baseline data based GPS spoofing detection algorithm,” in 2018 IEEE/ION Position, Location and Navigation Symposium, PLANS 2018 - Proceedings, Jun. 2018, pp. 397–403, doi: 10.1109/PLANS.2018.8373406.

[8] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and Privacy Issues of UAV: A Survey," Mobile Networks and Application, vol. 25, no. 1, pp. 95–101, Feb. 2020, doi: 10.1007/s11036-018-1193-x.

[9] Y. M. Kwon, J. Yu, B. M. Cho, Y. Eun, and K. J. Park, "Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles," IEEE Access, vol. 6, pp. 43203–43212, Aug. 2018, doi: 10.1109/ACCESS.2018.2863237.

[10] M. Awad and R. Khanna, "Deep Neural Networks," in Efficient Learning Machines, 2015, pp. 127–147.

[11] E. Shafiee, M. R. Mosavi, and M. Moazedi, "Detection of Spoofing Attack using Machine Learning based on Multi-Layer Neural Network in Single-Frequency GPS Receivers," Journal of Navigation, vol. 71, no. 1, pp. 169–188, Jan. 2018, doi: 10.1017/S0373463317000558.

[12] M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni, and N. Kaabouch, "Detection of GPS Spoofing Attacks on Unmanned Aerial Systems," Feb. 2019, doi: 10.1109/CCNC.2019.8651804.

[13] Y. Qiao, Y. Zhang, and X. Du, "A Vision-Based GPS-Spoofing Detection Method for Small UAVs," in Proceedings - 13th International Conference on Computational Intelligence and Security, CIS 2017, Feb. 2018, vol. 2018-January, pp. 312–316, doi: 10.1109/CIS.2017.00074.

[14] "UAV Attack Dataset | IEEE DataPort." https://ieee-dataport.org/open-access/uav-attack-dataset (accessed Jun. 12, 2021).

[15] A. Shenfield, D. Day, and A. Ayesh, "Intelligent intrusion detection systems using artificial neural networks," ICT Express, vol. 4, no. 2, pp. 95–99, Jun. 2018, doi: 10.1016/J.ICTE.2018.04.003.

[16] H. H. Heriz, H. M. Salah, S. Bashir, A. Abdu, M. M. El Sbihi, and S. S. Abu-Naser, "English Alphabet Prediction Using Artificial Neural Networks," 2018. Accessed: Jun. 09, 2021. [Online]. Available: www.ijeais.org/ijapr.

[17] H. Almarabeh, "Analysis of Students' Performance by Using Different Data Mining Classifiers," International Journal of Modern Education Computer Science., vol. 9, no. 8, pp. 9–15, 2017, doi: 10.5815/ijmecs.2017.08.02.