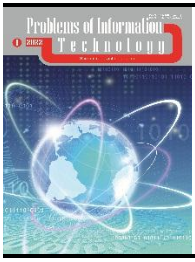


Available online at www.jpit.az

13(1)
2022

Development of a method for detecting GPS spoofing attacks on unmanned aerial vehicles

Fargana J. Abdullayeva[a], Orkhan V. Valikhanli[b]

[a,b]Institute of Information Technology, Azerbaijan National Academy of Sciences, B. Vahabzade str., 9A, AZ1141 Baku, Azerbaijan

[a] a_farqana@mail.ru; [b] orkhanvalikhanli@gmail.com

0000-0003-2288-6255[a]

0000-0001-6966-5084[b]

ARTICLE INFO

http://doi.org/10.25045/jpit.v13.i1.01

Article history:
Received 15 September 2021
Received in revised form 23 November 2021
Accepted 21 January 2022

Key words:
UAV
GPS spoofing
CNN
Intrusion detection system

ABSTRACT

As in other vehicles, unmanned aerial vehicles (UAV) mainly use GPS (Global Positioning System) for the provision of navigation. Non-execution of necessary measures on UAV, availability of the devices used in the process of attack may cause GPS spoofing attack on UAV. The quick detection of the attack plays an important role in obtaining safety precautions. The use of artificial neural networks in the detection of such attacks is very convenient. Therefore, in the article new approach based on convolutional neural network (CNN) method is proposed in order to detect GPS spoofing attack. The new approach has been developed for two different types of UAVs. As a result of conducted experiments, high-accuracy detection of GPS spoofing attack has been provided.

1. Introduction

Unmanned aerial vehicles (UAVs) have become an integral part of our lives. Recently, we observe their application in various areas. Especially, the implementation of artificial intelligence in UAVs has made it possible for them to operate in a fully autonomous mode. Thus, this not only reduces human labor but also increases the speed of the work process. According to statistics, the market value of UAVs is estimated to reach billions of dollars in the next 5-10 years. UAVs are already used not only on Earth, but also on other planets. An example of this, is the single-rotor UAV named "Ingenuity" sent to Mars by NASA (National Aeronautics and Space Administration).

The widespread use of UAVs in a short period causes some problems. The most important of these problems is their cybersecurity. Cybersecurity is not only a problem in commercial and consumer-type UAVs but also in military ones. Late detection of cyberattacks can lead to serious consequences. One such case occurred on 5 December 2011. Thus, the American UAV named “Lockheed Martin RQ-170 Sentinel” was captured by the armed forces of the Islamic Republic of Iran with a GPS spoofing attack (Yağdereli et al., 2015). Then, reverse engineering operations were carried out on the captured UAV and a similar one was made and put into operation.

Generally, there are various types of cyberattacks targeting UAVs. Cyberattacks include malware injection, jamming, Denial-of-service (DoS), Man-in-the-middle attack, and GPS spoofing. The most common of these cyberattacks is the GPS spoofing attack. Not only UAVs, but also any vehicle that uses a GPS receiver (such as ships, cars, etc.) may be target of GPS spoofing attacks. Considering these, in this work, a method for detection of GPS spoofing attacks is proposed.

Various methods based on machine and deep learning have been proposed to detect GPS spoofing attacks. Available methods mainly use CNN, RNN (recurrent neural network), MLP (multilayer perceptron), and LSTM (Long short-term memory). In addition, flight log files, various signal parameters and spectrograms are used in the training process. Comprehensive information on the analysis of available methods is provided in section 3.

The proposed method has higher detection accuracy compared to other methods. The proposed method also does not require any additional hardware component compared to other different approaches (e.g., method based on determining the direction of arrival of signal). Not implementing the additional hardware equipment, in turn, means saving the energy and weight of the UAV.

2. GPS spoofing attacks

During a GPS spoofing attack, the attacker transmits a counterfeit signal which is similar real one, however, with higher power (Borhani-Darian et al., 2020). GPS spoofing attack can alter the intended trajectory of UAV. As a result, the UAV may crash or be hijacked. Figure 1 illustrates the GPS spoofing attack process.

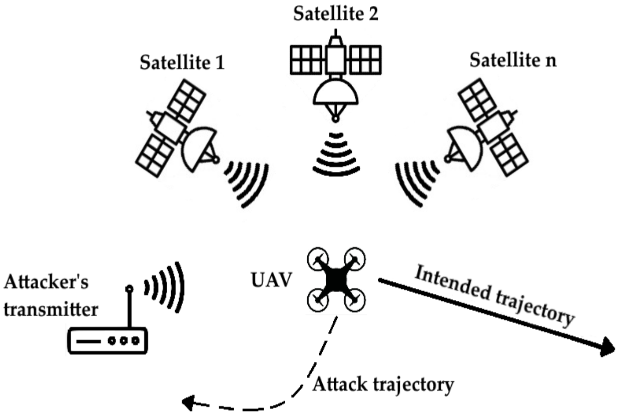


Figure 1. GPS spoofing attack process

To perform GPS spoofing attacks, special devices are used. Such devices are called software-defined radios (SDR). SDR is a radio communication system in which signal processing is done by software instead of hardware components. These types of devices include HackRF, BladeRF, USRP, etc. (Semanjski et al., 2020).

Detection of GPS spoofing attacks is not limited to machine and deep learning methods. Other detection methods are described below. These methods include those requiring both software and hardware.

- Machine and deep learning methods
- A method based on determining the direction of arrival (DoA) of the signal
- A method based on signal processing
- Hybrid methods

Various algorithms are implemented for the methods based on machine and deep learning. These algorithms are used for the detection of anomalies in the received GPS signal or other collected data (Riahi Manesh et al., 2019). Determining the DoA of a signal for the detection of GPS spoofing attacks is another preferred method. In this method, several antennas are attached to the UAV and special calculations are performed (Riahi Manesh et al., 2019; Psiaki et al., 2016). The goal here is to determine the arrival direction of the GPS signal because, during a GPS spoofing attack, counterfeit signals are often sent from the same source. On the other hand, normal signals are sent by GPS satellites and from different directions. Thus, this approach makes it possible to detect GPS spoofing attacks. This method requires additional hardware. The signal processing method is based on the analysis of signal quality during the attack (Psiaki et al., 2016). Thus, in a GPS spoofing attack, a counterfeit signal is tried to be aligned with the real one. During the alignment process, distortions occur in a short time period. Regular monitoring of signal quality makes it possible to detect such distortions and therefore attacks too. A hybrid-based method is an implementation of multiple methods together which is mentioned above (Riahi Manesh et al., 2019). Thus, when one method is ineffective, another may detect the attack.

3. Related work

(Borhani-Darian et al., 2020) uses deep learning methods to detect GPS spoofing attacks. MLP, simple-CNN, and complex-CNN are selected from these deep learning methods. The structure of a simple CNN is defined as 3 convolution layers and 3 fully connected layers.

The structure of a complex CNN is defined by 13 convolution layers and 3 fully connected layers. The ReLU activation function is used for all three methods. Stochastic Gradient Descent with Momentum (SGDM) and adaptive moment estimation (Adam) are used as optimizers in the implemented methods. 10,000 synthetically created samples are used during the training process. According to carried out experiments, the complex-CNN has shown better results. Also, the accuracy of the Adam Optimizer has been higher for each method. MLP has shown poor results compared to others. (Manesh et al., 2019) uses a neural network to detect GPS spoofing attacks. 5 five features are selected for the algorithm. Comparison operations are done between these features to get better accuracy and reduce the complexity of the algorithm. Thus, three of these features, signal-to-noise ratio, pseudo distance, and doppler effect are selected as the main features. 2000 samples are used in the training process. One and then two hidden layers are defined for the neural network. Neurons in the range of 1-25 are defined for each hidden layer. As a result, a neural network consisting of two hidden layers (with 3 neurons in each) demonstrated better performance. In (Shafiee et al., 2017), along with the MLP neural network, KNN (k-nearest neighbors) and Naive Bayes classification algorithms are also used. The structure of the MLP is defined as 3-2-1. 3 is the number of neurons in the input layer, 2 is the number of neurons in the hidden layer, and 1 is the number of neurons in the output layer. Signal level, delta, and early-late phase are selected as the main features for the methods. As a result, MLP performed better. In (Xiao et al., 2019), simple-RNN, LSTM-RNN, and GRU-RNN (gated recurrent unit-recurrent neural network) neural networks are used. Also, the DoA evaluation algorithm is used in the training process to provide better accuracy. Totally, 30,000 samples are chosen. 20,000 samples for training and 10,000 samples for testing are used. The number of layers is defined as 3-4, and the number of neurons as 16 and 32. According to carried out experiments, simple RNN and LSTM-RNN demonstrated better performance. In (Park et al., 2020), an autoencoder is used for the detection of GPS spoofing attacks. In the training process, only normal flight information is selected. The optimization function of the method is Adam, and the activation function is ReLU.

4. Proposed method

In this paper, a CNN-based method for the detection of GPS spoofing attacks is proposed. The proposed method is based on the analysis of log files recorded by the UAV during the flight. Since the classes (normal and GPS spoofing) are known in the dataset, supervised machine learning is used for detection. The proposed method uses ReLU and Sigmoid as activation functions, Adam as an optimizer. Figure 2 illustrates the structure of the proposed method.

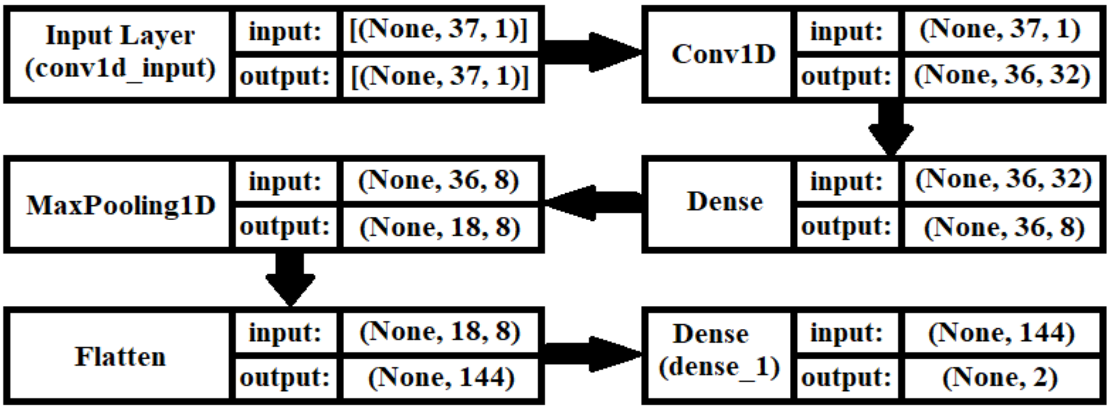


Figure 2. The structure of the proposed method

As shown in Figure 2, the method structure consists of 1 input, 4 hidden, and 1 output layer. Each layer has its input and output. The number of neurons is determined by the size of the shapes at the output layer. For instance, let's take a look at the one-dimensional convolutional hidden layer in figure 2. The shapes at the output layer are defined as 36*32. This means that the number of neurons in the layer is 1152. When neurons in the other layers are calculated and results are summed, then the total number reaches 1728. It should be noted that some sources include the number of neurons in the input and output layers, while others do not. In this work, the number of neurons in the layers is not taken into account.

Two possible ways are available for the implementation of the proposed method. The first is the subsequent analysis of log files recorded by the UAV. The second is using the method in the intrusion detection system (IDS) during the flight. In the case of a GPS spoofing attack, IDS will immediately warn the system.

5. Experiments

"UAV attack dataset" is used in this work (Whelan et al., 2020). The dataset consists of several types of UAVs and two of them are selected for this research. One of them contains the flight data of a quadcopter-type UAV and consists of 3247 samples. Another one contains the flight data of the tailsitter-type of UAV and consists of 1209 samples. Each selected dataset is divided into two classes. One class includes normal flight data and another one includes flight data with a GPS spoofing attack. A normal flight is labeled as "0" and a flight with a GPS spoofing attack is labeled as "1". The dataset has a total of 89 features including the label. Some of the features are constant or empty, that's why they are excluded. Thus, 37 valid features are selected. A standardization operation is also performed on the dataset to achieve higher accuracy.

Various metrics are used to evaluate the effectiveness of the proposed method. These metrics are precision, recall, F-measure, and accuracy. Metrics are calculated as follows:

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (1)$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (2)$$

$$\text{F} - \text{measure} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \quad (3)$$

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \quad (4)$$

Where True Positive (TP) is correctly predicted positive samples, true negative (TN) is correctly predicted negative samples, false positive (FP) is incorrectly predicted positive samples, and false negative (FN) is incorrectly predicted negative samples.

The achieved experimental results for the proposed method are shown in table 1. The accuracy for both types of UAVs is 0.99. This is a good result for the detection of GPS spoofing attacks.

Table 1. Results of the proposed method

Datasets (UAV type)	Classes	Accuracy	Precision	Recall	F1-score
Quadcopter-type UAV	Normal (0)	0.99	0.99	0.97	0.98
	GPS spoofing (1)		0.97	0.99	0.98
Tailsitter-type UAV	Normal (0)	0.99	0.97	1	0.99
	GPS spoofing (1)		1	0.98	0.99

Also, a confusion matrix is used to illustrate the results graphically. The confusion matrix is a summary of the performance of the classification algorithm (Brownlee, 2016). Figure 3 illustrates the confusion matrix for both datasets.

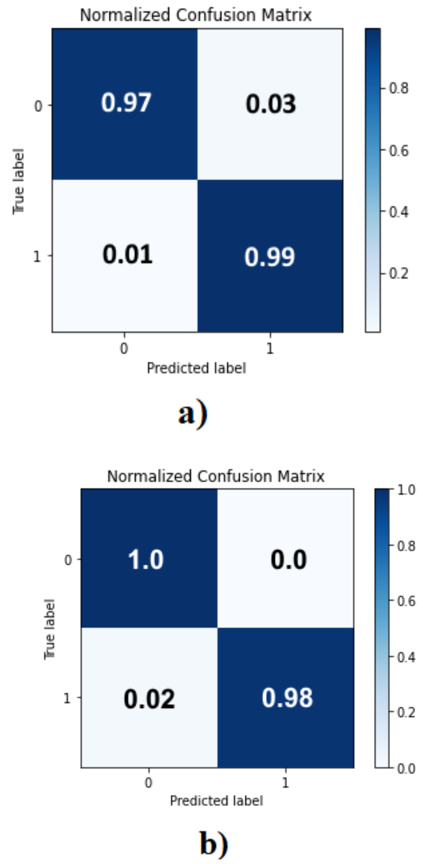
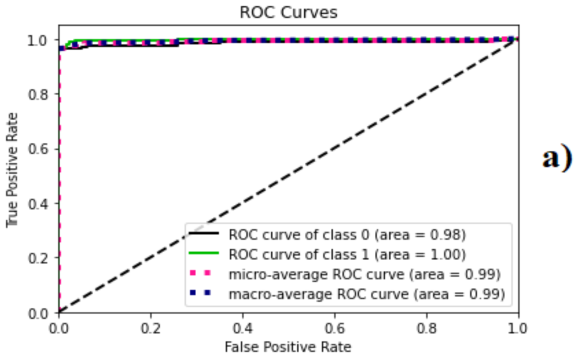


Figure 3. Confusion Matrix (a- quadcopter UAV, b- tailsitter UAV)

The Receiver Operating Characteristic (ROC) curve is another evaluation metric. ROC is a method for visualizing, organizing, and selecting classifiers based on their efficiency (Fawcett, 2006). Figure 4 illustrates the ROC graph for both datasets.



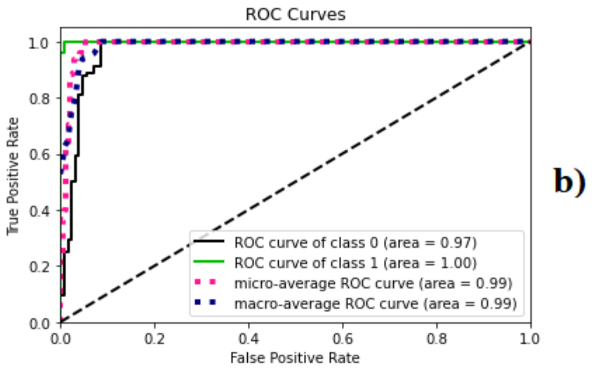


Figure 4. ROC curve graphs (a- quadcopter UAV, b- tailsitter UAV)

6. Conclusion

The paper proposed a method for the detection of GPS spoofing based on the analysis of UAV flight log files. Though the proposed method achieved high accuracy, sometimes this may be insufficient for detection. This is due to the constant emergence of new types of GPS spoofing attacks. To provide a better detection system, it's better to implement other methods along with the machine and deep learning. Therefore, if one method fails, others will provide the detection.

References

Borhani-Darian, P., Li, H., Wu, P., & Closas, P. (2020). Deep Neural Network Approach to Detect GNSS Spoofing Attacks. Proceedings Of The 33Rd International Technical Meeting Of The Satellite Division Of The Institute Of Navigation (ION GNSS+ 2020), Manassas, Virginia, USA, September 2020, (pp. 3241-3252). https://doi.org/10.33012/2020.17537

Brownlee, J. (2016). What is a confusion matrix in machine learning. Machine Learning Mastery. https://machinelearningmastery.com/confusion-matrix-machine-learning

Fawcett, T. (2006). An introduction to ROC analysis. Pattern Recognition Letters, 27(8), 861-874. https://doi.org/10.1016/j.patrec.2005.10.010

Manesh, M., Kenney, J., Hu, W., Devabhaktuni, V., & Kaabouch, N. (2019). Detection of GPS Spoofing Attacks on Unmanned Aerial Systems. 16Th IEEE Annual Consumer Communications & Networking Conference (CCNC), Piscataway, New Jersey, USA, January 2019 (pp. 1-6). https://doi.org/10.1109/ccnc.2019.8651804

Park, K., Park, E., & Kim, H. (2020). Unsupervised Intrusion Detection System for Unmanned Aerial Vehicle with Less Labeling Effort. Information Security Applications, 45-58. https://doi.org/10.1007/978-3-030-65299-9_4

Psiaki, M., & Humphreys, T. (2016). GNSS Spoofing and Detection. Proceedings Of The IEEE, 104(6), 1258-1270. https://doi.org/10.1109/jproc.2016.2526658

Riahi Manesh, M., & Kaabouch, N. (2019). Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. Computers & Security, 85, 386-401. https://doi.org/10.1016/j.cose.2019.05.003

Semanjski, S., Semanjski, I., De Wilde, W., & Muls, A. (2020). Use of Supervised Machine Learning for GNSS Signal Spoofing Detection with Validation on Real-World Meaconing and Spoofing Data—Part I. Sensors, 20(4), 1171. https://doi.org/10.3390/s20041171

Shafiee, E., Mosavi, M., & Moazedi, M. (2017). Detection of Spoofing Attack using Machine Learning based on Multi-Layer Neural Network in Single-Frequency GPS Receivers. Journal Of Navigation, 71(1), 169-188. https://doi.org/10.1017/s0373463317000558

Whelan, J., Sangarapillai, T., Minawi, O., Almehmadi, A., & El-Khatib, K. (2020). UAV Attack Dataset. IEEE Dataport. https://dx.doi.org/10.21227/00dg-0d12

Xiao, K., Zhao, J., He, Y., Li, C., & Cheng, W. (2019). Abnormal Behavior Detection Scheme of UAV Using Recurrent Neural Networks. IEEE Access, 7, 110293-110305. https://doi.org/10.1109/access.2019.2934188

Yağdereli, E., Gemci, C., & Aktaş, A. (2015). A study on cyber-security of autonomous and unmanned vehicles. The Journal Of Defense Modeling And Simulation: Applications, Methodology, Technology, 12(4), 369-381. https://doi.org/10.1177/1548512915575803