Dang, Yongchao; Benzaid, Chafika; Taleb, Tarik; Yang, Bin; Shen, Yulong

Transfer Learning based GPS Spoofing Detection for Cellular-Connected UAVs

Published in:
2022 International Wireless Communications and Mobile Computing, IWCMC 2022

DOI:
10.1109/IWCMC55113.2022.9824124

Published: 19/07/2022

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Please cite the original version:
Dang, Y., Benzaid, C., Taleb, T., Yang, B., & Shen, Y. (2022). Transfer Learning based GPS Spoofing Detection for Cellular-Connected UAVs. In *2022 International Wireless Communications and Mobile Computing, IWCMC 2022* (pp. 629-634). (International Wireless Communications and Mobile Computing Conference). IEEE. https://doi.org/10.1109/IWCMC55113.2022.9824124

Transfer Learning based GPS Spoofing Detection for Cellular-Connected UAVs

Yongchao Dang*, Chafika Benzaïd†, Tarik Taleb†, Bin Yang‡, and Yulong Shen§
* Aalto University, Espoo, Finland, † University of Oulu, Oulu, Finland,
‡ Chuzhou University, Chuzhou, China and § Xidian University, Xi'an, China
* Email: yongchao.dang@aalto.fi, † Email: firstname.lastname@oulu.fi,
‡ yangbinchi@gmail.com and § ylshen@mail.xidian.edu.cn

***Abstract*—Unmanned Aerial Vehicles (UAVs) are set to become an integral part of 5G and beyond systems with the promise of assisting cellular communications and enabling advanced applications and services, such as public safety, caching, and virtual/mixed reality-based remote inspection. However, safe and secure navigation of UAVs is a key requisite for their integration in the airspace. The GPS spoofing is one of the major security threats to remotely and autonomously controlled UAVs. In this paper, we propose a machine learning-based, mobile network-assisted UAV monitoring and control system that allows live monitoring of UAVs' locations and intelligent detection of spoofed positions. We introduce the Convolutional Neural Network (CNN) in the edge UAV Flight Controller (UFC) to locate a UAV and detect any GPS spoofing by comparing differences between the theoretical path loss computed by UFC and the corresponding path loss reported by the connected base station (BS). To reduce the detection latency as well as to increase the detection accuracy, transfer learning is leveraged to transfer the CNN knowledge between edge servers when the UAV handovers from one BS to another. The performance evaluation shows that the proposed solution can successfully detect spoofed GPS positions with an accuracy rate above 88% using only one BS.**

***Index Terms*—Unmanned Aerial Vehicles (UAVs), GPS spoofing, Convolutional Neural Network (CNN), Transfer Learning, and Beyond 5G.**

I. Introduction

Unmanned Aerial Vehicles (UAVs), or drones, are considered a crucial part of upcoming Internet of Things (IoT) platforms, offering not only the potential of delivering IoT-based services but also the capability of providing wireless connections to IoT applications in dense and remote areas [1], [2]. According to the report in [3], the UAV market is valued at nearly 27.4B in 2021 and is expected to reach 58.4B dollars by 2026. Nevertheless, the safety and security of remotely and autonomously controllable UAVs are prime challenges that hamper the envisaged growth in UAV-based applications and services if they are not properly addressed.

In response, the Federal Aviation Administration develops Unmanned Aircraft Systems (UAS) Traffic Management (UTM) systems to manage air traffic [4]. The UTM provides drones' mission-related services, including drone authentication, flight plan authorization, real-time location tracking, and geofencing [4]. It is noteworthy that the UTM systems-derived services are highly dependent on location information. Specifically, the Global Navigation Satellite System (GNSS, e.g., GPS) is officially used by UTM because of its global coverage and accuracy. However, the civil GPS services are unencrypted which makes it vulnerable to spoofing attacks [5]. In practice, commercial software-defined radio tools can be used to generate fake GPS information and signals and deceive the GPS receiver to compute false positions [6]. Indeed, fake GPS positions can break through UTM regulations and lead UAVs up to no-fly zones and/or give rise to collision risks. Thus, appropriate measures must be incorporated into UTM systems to verify UAV location information to defend against GPS spoofing attacks.

There are two kinds of methods for GPS spoofing detection, namely GPS navigation signal analysis methods (e.g., [7]–[10]) and GPS navigation message encryption methods (e.g. [11]–[15]). For instance, using multi-antenna techniques to measure the GPS signals direction of arrival, the work in [7], [8] presented methods that can filter out fake GPS signals and mitigate spoofing attacks. Similarly, the work in [9], [10] developed multiple GPS receivers-based spoofing detection methods through the cross-correlation property between the military and civil GPS signals. These methods need a secure receiver which serves as a ground-truth source in the cross-correlation process. Jansen *et al.* in [11] devised Crowd-GPS-Sec; an approach that uses the automatic dependent surveillance-broadcast messages and their time of arrival information to detect and localize the GPS spoofing attacks. The author in [12] proposed signature-based navigation messages authentication methods to prevent the GPS receiver from GPS spoofing attacks. Subsequently, Liu *et al.* in [14] leveraged a trusted hardware to generate cryptographic signatures for GPS messages to prevent their spoofing. The author in [14] developed SM cryptographic algorithms for BeiDou-II system in order to encrypt navigation messages.

Although the aforementioned methods are effective, they require more antennas and computing load on the receiver, which inhibits their adoption in UAV systems due to the limited battery capacity and weight load of UAVs. Furthermore, UAVs are considered as a victim in most existing work, while UAVs can be also an attacker and may report fake GPS locations to UTM in order to break through regulations. Fortunately, 3GPP has defined new standards that aim to enhance LTE support for Unmanned Aerial Systems (UAS) [16]–[18]. The new standards allow the UAS to access the Mobile Positioning System (MPS) services to locate and track the UAVs. Rather

than replacing the GPS positioning and navigation system on the UAV, the MPS service is used to assist in UTM for cross-checking the validity of the GPS information [19].

The authors in [20] introduced the Adaptive Trustable Residence Area (ATRA) to locate and track UAVs for GPS spoofing detection in UTM by leveraging the up-link Received Signal Strength Indication (RSSI) provided by the MPS service. Despite the advantages in GPS spoofing detection performance that ATRA offers, it requires at least three BSs, and its performance dramatically drops when the communication links between BSs and UAVs are less than three [20]. To overcome these weaknesses, the authors in [21] leveraged deep learning models, particularly Multi Layer Perceptron (MLP), to independently detect GPS spoofing at an edge server that is associated with three, two, or one BS, whereby the inputs of the deep learning model is the statistical difference between the theoretical path losses for the planned path and the real-time path losses obtained from each BS. Regardless of the performance brought by the deep learning model, its performance heavily depends on the volume of the training data; that is, the more the data are available, the more accurate the model will be [22]. Nevertheless, the transmission of a large amount of data takes too much time as well as consumes a lot of bandwidth, which may lead to network congestion and degradation in network performance. Furthermore, the statistical results are inadequate that may drop some of the original features from the inputs and bring a higher miss detection or false alarming. Therefore, this paper aims to leverage the efficient and economic Convolutional Neural Network (CNN) method to extract the deep trajectory features from the original data combing with the MLP models for GPS spoofing detection. The use of convolution layers in the CNN network allows the integration of the possessive features of the inputs and further enhances the detection accuracy.

In this paper, we introduce the CNN and transfer learning method into the edge servers for checking the authenticity of the GPS position reported to UTM by a UAV. The proposed method leverages the theoretical path losses difference computed by the edge servers to indicate the integrity and authenticity of the planned and real-time UAV's trajectory, enabling UTM to verify the UAV GPS information through the edge UAV Flight Controller (UFC). Compared with the aforementioned approaches, the proposed method migrates the GPS spoofing detection to the edge server, above all without any more requirements at the UAVs. In addition, using the transfer learning method, the edge servers can share the features knowledge of the UAV trajectory through CNN Convolution layers in order to increase detection accuracy as well as to shorten the detection latency. The major contributions of this paper are listed as follows:

- We investigate the 5G-assisted UAS system built on the Multi-access Edge Computing (MEC) architecture (see Fig. 1) that allows UTM to push UFC control and monitoring services to the network edges (e.g., base stations). It shall be noted that placing the UFC at the network edges can reduce the communication latency and enhance the communication reliability [23]. In addition to the reliable and low-latency communication, UTM can also track and verify the UAV GPS position through the MPS service at the edge server.
- To improve the GPS spoofing detection accuracy, we introduce CNN in UFC at the edge to monitor and verify UAV locations as well as to detect GPS spoofing. The CNN inputs are the differences between the theoretical path loss computed by the network edge BS and the corresponding path loss reported by the UAV, where the CNN Convolutional layers are used to extract the features of path losses and the dense layers are used to classify the test positions into spoofed and non-spoofed.
- With regard to reducing the detection latency as well as increasing the detection accuracy, we use the transfer learning technique to transfer the CNN knowledge between edge servers when the UAV handovers from one BS to another. It is worth mentioning that transfer learning allows sharing the neural network knowledge rather than the raw path losses data, which helps to reduce the amount of data transmission over network and mitigate network congestion.

The remainder of this paper is organized as follows. Section II presents the framework of 5G-assisted Unmanned Aerial Systems. Section III introduces the system model and formulates the target problem. Section IV presents the CNN-based GPS spoofing detector and the transfer learning approach for the improvement of multi-edge servers GPS spoofing detection efficiency. The performance evaluation of the CNN and transfer learning is discussed in Section V. Concluding remarks and some future work are presented in Section VI.

II. 5G-assisted Unmanned Aerial Systems

The envisioned 5G and beyond wireless communication system is connected with UTM to support the ultra-reliable and low-latency communication for beyond the visual line-of-sight control of UAVs [23], [24]. In this vein, UTM can access all services provided by the mobile network, such as Mobile Positioning System (MPS) services [18]. With the aid of MPS services, UTM can track the UAV through rough position locations as well as check the validity of the position information and telemetry data [16].

Fig. 1 shows the MEC-based 5G-assisted UAS high-level architecture, which consists of the remote operator, the cloud services, the core and transport networks, the edge servers, and the cellular networks [23]. The remote operator can monitor and interact with UAVs through the Operator Command and Control Service (OCCS) provided by the cloud interfaces. Other cloud services include the Supplementary Data Provider Service (SDPS) to provide the meteorological data and other information that are necessary for UAV flight planning, and the UAS Traffic Management services (UTMS) to govern all UAVs data and UAV related services including UAVs' registrations and identification, UAVs' flight plan and location, airspace restrictions and rules [4]. Note that all the data are

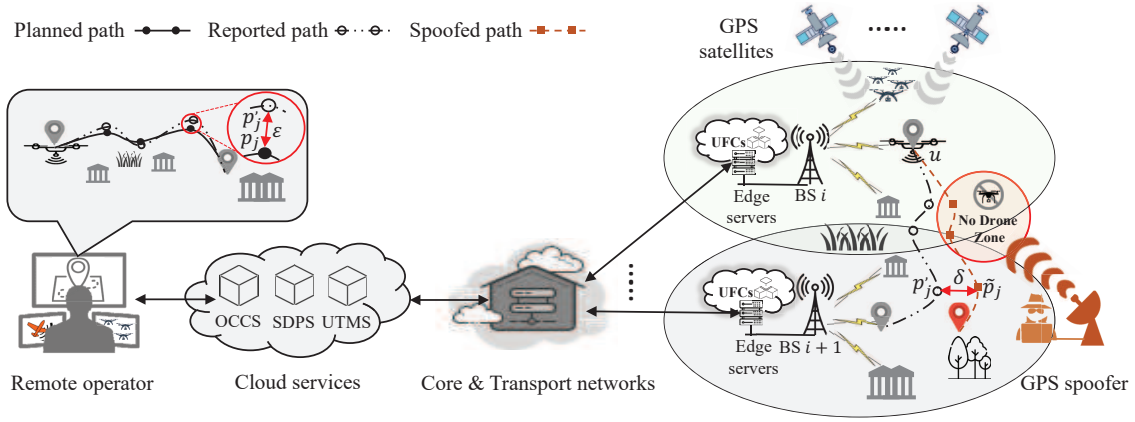


Fig. 1. A MEC-based 5G-assisted Unmanned Aerial System (UAS).

transmitted over the core and transport networks. In this work, the edge servers, collocated with the cellular network's BS, are used to host the UFC services that are in charge of executing the UAV mission, for examples monitoring and controlling the UAV flight. The MEC-based 5G-assisted UAS aims at leveraging 5G's promised features in terms of ultra reliability and low latency for the control and monitoring of UAV flights, but it lacks network security considerations. GPS is the main navigation and positioning system used in this system. Although UTM can use the 3GPP's MPS services to cross-check the validity of UAVs' GPS positions, it is not enough to protect the system from GPS spoofing attacks because of the low accuracy of the 3GPP MPS. Indeed, MPS provides location verification services that can make sure that the UAV is within the BS radius coverage area of about 30 meters to 80 meters [19]. As Fig. 1 shows, the MPS's low accuracy gives a chance to attackers that can design the spoofed trajectory in order to lead UAVs into no-fly areas or trap them into wrong destinations. It is worth noting that MPS can provide better positioning services with higher accuracy using either the trilateration methods requiring at least three BSs or the radar techniques demanding multi-antennas [25].

In order to detect a well-designed spoofing trajectory without additional hardware and with even one BS, we introduce the CNN and transfer learning methods to the edge UFC for GPS spoofing detection. In the next section, we describe our proposed methods.

III. System Model and Problem Formulation.

This section describes the network and communication models considered in this study. It also mathematically defines how the UFC detects GPS spoofing using the differences between the theoretical path losses and the BS measured path losses.

A. System Model

1) Network Model: As shown in Fig.1, we consider an edge network scenario consisting of two base stations, BS i and BS $i+1$, a victim UAV u, and a GPS spoofer. The GPS spoofer can send fake GPS signals to the victim UAV. Let (x_i, y_i, h_i) and $(x_{i+1}, y_{i+1}, h_{i+1})$ denote the location of the i^{th} and $(i+1)^{th}$ BS, respectively. Leaving out the GPS spoofing and GPS error, u should be at time t at the planned way point p_j. In the presence of a GPS error, the reported location at time t is at $p_j^{'}$, that is far away from p_j with an error ϵ. If the GPS is spoofed at time t, the UAV locates at $\tilde{p}_j$ that deviates from p_j with δ, where $\epsilon \leq dE < \delta$ and dE is the system's tolerable GPS margin error. However, the current MPS service may not notice this because the UAV is in the planned BSs radius.

2) Communication Model: In this paper, we consider that the channel model between UAV u and BS i or $(i+1)$ consists of both Line-of-Sight (LoS) links and Non-Line-of-Sight (NLoS) links. The theoretical path loss $\overline{L}_{iu}$ between BS i and UAV u is defined by 3GPP as in [17].

B. Problem Formulation

As Fig.1 shows, the GPS attacker can mislead the UAV to deviate from its planned path without being detected by the remote operator, and this is due to the wrong GSP positions received by the UAV GPS receiver. In this vein, it is necessary to use the properties of wireless communication links to cross-check whether the UAV GPS position is spoofed or not. According to [17], the UFC computes the theoretical path loss $\overline{L}_{iu}$ using the BS and UAV locations and obtains the corresponding path loss L_{iu} from the BS. Since the path loss is theoretically affected by the distance between the BS and UAV, the absolute difference ΔL_{iu}, $(\Delta L_{iu} = |\overline{L}_{iu} - L_{iu}|)$, can indicate the deviation between $p_j^{'}$ and $\tilde{p}_j$. Hence, the GPS spoofing detection problem is formulated as a hypothesis testing in Eq. (1).

$$\begin{cases} H_0: & \Delta L_{iu} > T, \\ H_1: & \Delta L_{iu} \leq T, \end{cases} \tag{1}$$

where H_0 represents that the GPS position is spoofed when ΔL_{iu} is above the threshold T, while H_1 means that there is no GPS spoofing. It is worth noting that the path loss L_{iu} is varying with the environment changes, such as temperature, humidity, cloud, and fog. Thus, the hypothesis testing in Eq. (1) may not represent the real distance deviation between the BS and the UAV. Besides, appropriate thresholds are important to the hypothesis testing performance; a smaller threshold may lead to a higher probability of false alarms, while a bigger

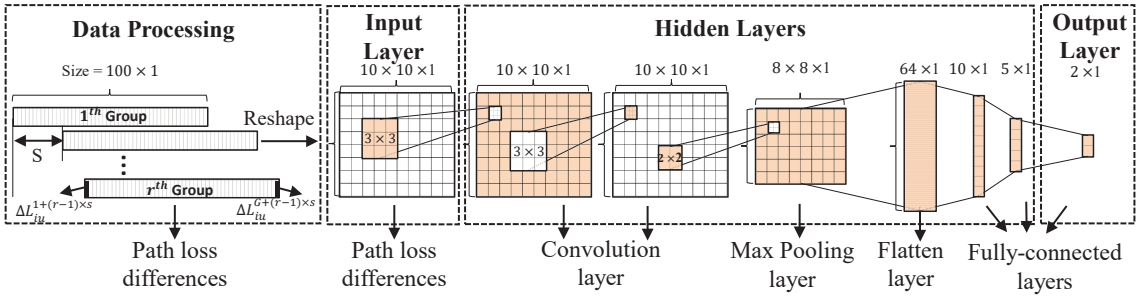


Fig. 2. Convolution neural network for GPS spoofing detection.

threshold may result in missed detection. To overcome these challenges, our previous work [21] uses statistical methods to mitigate the environmental variance on path losses computation and introduces deep neural network based model to find the apposite threshold for improving the detection accuracy. However, statistical analysis and neural network training can induced additional latency that may hinder the timely detection of GPS spoofing attack in an UAV environment.

In the following part, we introduce a novel solution based on Convolutional Neural Networks (CNN) and Transfer Learning to enable an effective UAV position monitoring and GPS spoofing detection on UFC. The CNN uses the convolution layer to extract the deep features of the path losses and remove environment impacts, and its fully-connected layers are used to deal with the thresholds issues. Meanwhile, the transfer learning method is leveraged to reduce the training time.

IV. Transfer Learning based GPS Spoofing Detection Approach.

A. Convolutional Neural Network

CNN has attracted a lot of attention in the past ten years, especially in pattern recognition such as image classification and voice recognition [26]. Fig.2 shows the structure of CNN designed for GPS spoofing detection. It consists of four kinds of layers, including convolution layer, max pooling layer, flatten layer, and fully-connected layers. The convolution layer is the core layer of CNN and contains a set of kernels and learnable parameters for the training process. Note that the size of kernels should be smaller than that of the input data. The pooling layer is used to down sample the number of parameters and reduce computation in the network, hence controlling overfitting. The pooling layer is used together with 2×2 filters that curtail its inputs by 2 on each width and height. The flatten layer is used to flatten the max pooling layer and bridge to fully-connected layers. The fully-connected layers carry out the final GPS spoofing decision based on the difference between the theoretical path loss computed by UFC and the corresponding path loss reported by the connected BS.

In Fig.2, the data processing is responsible for the grouping of the path losses data and the reshaping of each group into a grid pattern as required by the CNN model. Let $\mathcal{L}_{iu}^{1}$ denote the first grouped path losses differences computed by BS i; it is given by

$$\mathcal{L}_{iu}^{1} = \left\{\Delta L_{iu}^{1}, ..., \Delta L_{iu}^{g}, ..., \Delta L_{iu}^{G}\right\}, \quad (2)$$

where G is the length of each group, $G > 0$ and $\sqrt{G} \in \{1, 2, 3, ...\}$. It is noteworthy that the problems solved by CNN should have spatially independent features [26]. In other terms, CNN can only give the spoofing decision on each group regardless of the spoofed positions in the group. In this vein, we use a step s when choosing a new group, as shown in Fig.2. Thus, the r^{th} $(r > 1)$ group starts at $\Delta L_{iu}^{1+(r-1)\times s}$ and ends at $\Delta L_{iu}^{G+(r-1)\times s}$. Furthermore, the size of group is reshaped from $(1 \times G)$ to $(\sqrt{G} \times \sqrt{G})$ before inputs to the CNN.

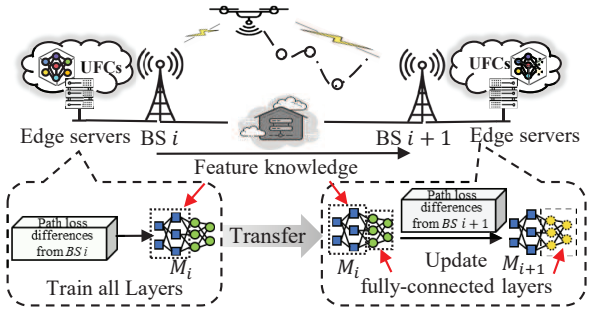
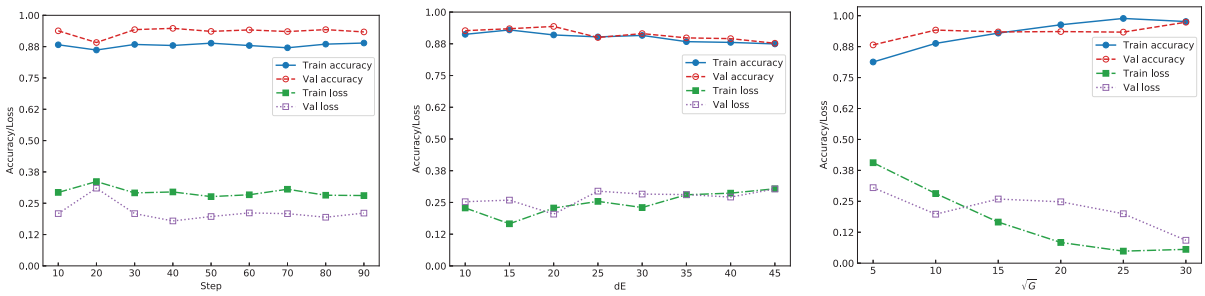


Fig. 3. Transfer learning based GPS spoofing detection.

B. Transfer learning

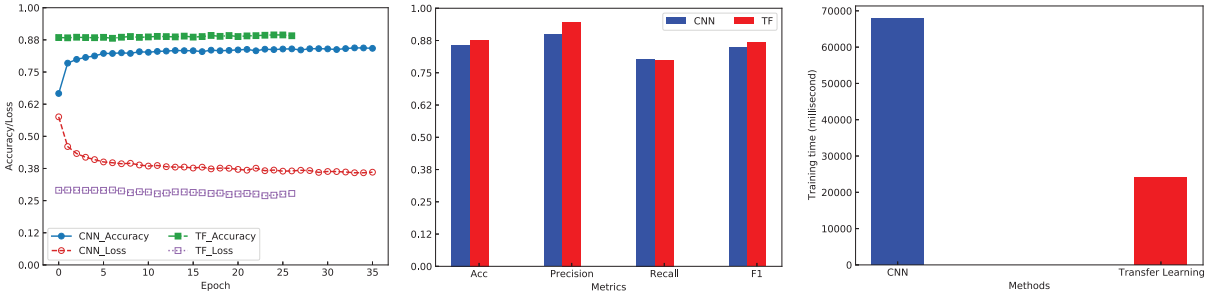
The CNN is built on deep neural networks and requires a lot of data to train the model parameters. To overcome this limitation, transfer learning comes into play [27]. Transfer learning is a representative and valid machine learning approach that allows training the new model with fewer data by using the pre-trained model. Moreover, transfer learning can help reducing the training time, thanks to the use of the pre-trained model.

Fig.3 presents the transfer learning based GPS spoofing detection for edge servers. BS i uses the path losses differences data to train the model M_i on its edge server and then share the knowledge of the model with the next edge server instead of transmitting the raw data over the network. On one hand, transfer learning can avoid network congestion by sharing the knowledge of the data between the deep learning models. On the other hand, the time required by BS $i+1$ for training the new model M_{i+1} can be greatly reduced because of the use of the same convolution layers as M_i for feature extraction. It is worth mentioning that the transfer learning procedure is triggered at the same time as the UFC service migration [28], [29].



(a) Step size (S), $dE = 15$, $\sqrt{G} = 10$ (b) GPS error(dE), $S = 50$, $\sqrt{G} = 15$ (c) Group size($\sqrt{G}$),$S = 50$, $dE = 15$

Fig. 4. The accuracy and loss of the CNN with different settings



(a) Training history (b) Performance metrics (c) Training time

Fig. 5. Training history and performance recording

V. Performance Evaluation

A. Simulation Setup

The performance evaluation is conducted using a simulator built with python 3.7 and Tensorflow 2.7. Python constructs the simulation platform while Tensorflow builds the CNN and transfer learning models. We consider two BSs located at the 3D points $(150, 0, 35)$ and $(150, 300, 35)$ (all in meters), respectively. A UAV starts at $(150, 150, 150)$ and moves towards a destination 100 meters away from the start point. We consider a spoofing attacker who can lead the UAV to the spoofed destination with 100 meters away from the start point. A total of 16 potential destinations are evenly distributed over a 3D space, including one real destination and 15 spoofed destinations [21]. The communication models between the BSs and the UAV are defined in [17] and the channel frequency is set to 2.0 GHz.

The structure of the used CNN model is given in Fig.2, including the input layer, hidden layers, and output layer. The inputs fed into the CNN is a tensor with size $\sqrt{G} \times \sqrt{G} \times 1$, where G is the number of elements in each group and $\sqrt{G}$ is between 5 and 30. The hidden layers comprise two identical convolution layers for feature extraction having a 3×3 kernel, one pooling layer for dimensionality reduction using a 2×2 kernel, followed by a flatten layer and 3 fully-connected layers for GPS spoofing detection. To prevent overfitting, the dropout layers with a dropout rate set to 0.1 are inserted after each layer and early stopping with a patience of 20 is used. Moreover, all layers use the optimizer $RMSprop$ and the activation function $ReLU$ except the output layer which uses the $softmax$ as its activation function. We consider that the UAV's GPS is spoofed when δ is bigger than the tolerated GPS margin error dE.

B. Performance Results

To assess the performance of the proposed CNN and transfer learning models for GPS spoofing detection, we use accuracy and the sparse categorical crossentropy as performance metrics. The evaluation of CNN-based GPS spoofing detector is performed by varying the data processing $step$ from 0.1 to 0.9 in G, the tolerated GPS margin error d_E from 10 meters to 45 meters and the reshaped group size $\sqrt{G}$ from 5 to 30. The performance measures illustrated in Fig. 4 and Fig. 5 are obtained using 1.5 million data points with a validation split of 0.3.

Fig. 4 shows the performance of the CNN for GPS spoofing detection. The obtained results in Fig. 4(a) show that the proposed CNN performs well with different steps for both training and validation data, which demonstrates that the step size has no impact on the detection accuracy. It is worth noting that the higher accuracy and lower loss on the validation set compared to the training set is due to the fact that dropout layers are activated during the training but deactivated when evaluating on the validation set [30]. It is observed from Fig. 4(b) that the detection error increases as the tolerated GPS margin error increases, because a bigger dE makes it difficult to distinguish the trajectory deviation δ caused by the GPS spoofing attack from the GPS error ϵ. Fig. 4(c) shows that the more elements are in the group, the higher accuracy and the lower loss are achieved. In fact, increasing the size of the group allows providing more path losses data to the CNN model, which helps in better extracting the deep features. The training history and performance recording in Fig. 5 show that transfer learning can effectively leverage the knowledge of the pre-trained model to improve the detection accuracy while greatly reducing the time spent on training the new model

by almost 60%. Indeed, the results depicted in Fig. 5(a) and Fig. 5(b) show that the use of transfer learning has increased the detection accuracy of the CNN model to above 88%, achieving a gain of 5% compared to CNN. It is also observed from Fig. 5(b) that transfer learning delivers better precision and F1 score with a slight decrease in recall metric. Thus, considering the cost-performance trade-off, transfer learning has the upper hand compared to CNN, making it a promising solution to effectively detect GPS spoofing at the edge.

VI. Conclusion and Future Work

This paper introduced the CNN and transfer learning methods for the detection of GPS spoofing on unmanned aerial systems. The CNN model deployed on the edge server allows verifying UAV locations by using the difference between the base station theoretical and real-time path losses, where the convolutional layers can extract the deep features from path loss differences that are then used by fully-connected multi-layers to detect GPS spoofing. In addition, the transfer learning method is used to further decrease the CNN training time as well as to increase the CNN detection accuracy. The simulation results show the high effectiveness of our proposed method in detecting spoofed GPS positions with a rate of above 88% using transfer learning. In the future, we are planning to evaluate the effectiveness of the proposed solution in a real-world experimentation testbed comprising a UAV and several 5G BSs.

VII. Acknowledgement

The research work presented in this paper was partially supported by the European Union's Horizon 2020 Research and Innovation Program through the INSPIRE-5Gplus project under Grant No. 871808. It was also partially supported by the national key R&D program of China under Grant No.2018YFB2100400 and the national science foundation of China under Grant No.61972308.

References

[1] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV-based IoT Platform: A Crowd Surveillance Use Case," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 128–134, 2017.

[2] H. Hellaloui, A. Chelli, M. Bagaa, and T. Taleb, "Towards Mitigating the Impact of UAVs on Cellular Communications," in *Proc. of the IEEE Global Communications Conf. (GLOBECOM)*, 2018, pp. 1 – 7.

[3] U. Market, "Unmanned Aerial Vehicle (UAV) Market share Forecast to 2026, MarketsandMarkets," https://www.marketsandmarkets.com/Market-Reports/unmanned-aerial-vehicles-uav-market-662.html., January 2022.

[4] FAA, "Unmanned Aircraft System Traffic Management, Federal Aviation Administration (FAA)," https://www.marketsandmarkets.com/Market-Reports/unmanned-aerial-vehicles-uav-market-662.html., January 2021.

[5] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned Aircraft Capture and Control via GPS Spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[6] K. Pärlin, M. M. Alam, and Y. L. Moullec, "Jamming of UAV Remote Control Systems using Software Defined Radio," in *Proc. of the International Conf. on Military Communications and Information Systems (ICMCIS)*, May 2018, pp. 1 – 6.

[7] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A Low-Complexity GPS Anti-Spoofing Method using a Multi-Antenna Array," in *Proc. of the 25th ION GNSS*, Sept. 2012, pp. 1233 – 1243.

[8] J. Magiera and R. Katulski, "Detection and Mitigation of GPS Spoofing based on Antenna Array Processing," *Journal of Applied Research and Technology*, vol. 13, no. 1, pp. 45–57, 2015.

[9] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "GPS Spoofing Detection via Dual-receiver Correlation of Military Signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 4, pp. 2250–2267, 2013.

[10] B. W. O'Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Real-Time GPS Spoofing Detection via Correlation of Encrypted Signals," *Navigation*, vol. 60, no. 4, pp. 267–278, 2013.

[11] K. Jansen, M. Schäfer, D. Moser, V. Lenders, C. Pöpper, and J. Schmitt, "Crowd-GPS-Sec: Leveraging Crowdsourcing to Detect and Localize GPS Spoofing Attacks," pp. 1018–1031, May 2018.

[12] K. D. Wesson, M. Rothlisberger, and T. Humphreys, "Practical Cryptographic Civil GPS Signal Authentication," *NAVIGATION: Journal of the Institute of Navigation*, vol. 59, no. 3, pp. 177–193, 2012.

[13] Z. Wu, Y. Zhang, and R. Liu, "BD-II NMA&SSI: An Scheme of Anti-Spoofing and Open BeiDou II D2 Navigation Message Authentication," *IEEE Access*, vol. 8, pp. 23 759–23 775, 2020.

[14] T. Liu, A. Hojjati, A. Bates, and K. Nahrstedt, "Alidrone: Enabling Trustworthy Proof-of-Alibi for Commercial Drone Compliance," in *Proc. of the IEEE 38th International Conf. on Distributed Computing Systems (ICDCS)*, Jul. 2018, pp. 841–852.

[15] H. Zhu, M. L. Cummings, M. Elfar, Z. Wang, and P. Pajic, "Operator Strategy Model Development in UAV Hacking Detection," *IEEE Transactions on Human-Machine Systems*, vol. 49, no. 6, pp. 540–549, 2019.

[16] 3GPP TS 23.754, "Study on Supporting Unmanned Aerial Systems (UAS) Connectivity, Identification and Tracking," Dec. 2018.

[17] 3GPP TR 36.777, "Enhanced LTE Support for Aerial Vehicles," Dec. 2017.

[18] 3GPP TS 22.825, "Study on Remote Identification of Unmanned Aerial Systems (UAS)," Sept. 2018.

[19] A. Takacs, H. Mahkonen, and X. Lin, "Managing drone air traffic with network services," https://www.ericsson.com/en/blog/2017/11/managing-drone-air-traffic-with-network-services., Nov 2017.

[20] Y. Dang, C. Benzaïd, Y. Shen, and T. Taleb, "GPS Spoofing Detector with Adaptive Trustable Residence Area for Cellular based-UAVs," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*. IEEE, 2020, pp. 1–6.

[21] Y. Dang, C. Benzaïd, B. Yang, and T. Taleb, "Deep Learning for GPS Spoofing Detection in Cellular-Enabled UAV Systems," in *2021 International Conference on Networking and Network Applications (NaNA)*. IEEE, 2021, pp. 501–506.

[22] M. M. Najafabadi, F. Villanustre, T. M. Khoshgoftaar, N. Seliya, R. Wald, and E. Muharemagic, "Deep Learning Applications and Challenges in Big Data Analytics," *Journal of big data*, vol. 2, no. 1, pp. 1–21, 2015.

[23] O. Bekkouche, T. Taleb, and M. Bagaa, "UAVs Traffic Control based on Multi-Access Edge Computing," in *Proc. of the IEEE Global Communications Conf. (GLOBECOM)*, 2018, pp. 1 – 6.

[24] M. Maiouak and T. Taleb, "Dynamic maps for automated driving and UAVs geofencing," *IEEE Wireless Commun. Magazine*, vol. 26, no. 4, p. 54 – 59, 2019.

[25] N. Akbar, S. Yan, N. Yang, and J. Yuan, "Location-Aware Pilot Allocation in Multicell Multiuser Massive MIMO Networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7774–7778, 2018.

[26] S. Albawi, T. A. Mohammed, and S. Al-Zawi, "Understanding of A Convolutional Neural Network," in *2017 International Conference on Engineering and Technology (ICET)*. Ieee, 2017, pp. 1–6.

[27] S. J. Pan and Q. Yang, "A survey on transfer learning," *IEEE Transactions on knowledge and data engineering*, vol. 22, no. 10, pp. 1345–1359, 2009.

[28] O. Bekkouche, F. Z. Yousaf, X. Li, and T. Taleb, "Management and orchestration of mobile network services over federated mobile infrastructures," *IEEE Network*, vol. 35, no. 6, pp. 178–185, 2021.

[29] T. Taleb, A. Ksentini, H. Hellaoui, and O. Bekkouche, "On Supporting UAV Based Services in 5G and Beyond Mobile Systems," *IEEE Network*, vol. 35, no. 4, pp. 220–227, 2021.

[30] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, "Dropout: A Simple Way to Prevent Neural Networks from Overfitting," *The journal of machine learning research*, vol. 15, no. 1, pp. 1929–1958, 2014.