2026 IEEE 23rd Consumer Communications & Networking Conference (CCNC)

A Privacy Preserving Federated Learning-Based Authentication Scheme for Internet of Drones Systems

Image Bhattarai Cong Pu
Department of Computer Science, Oklahoma State University, Stillwater, OK, United States
Email: image.bhattarai@okstate.edu, cong.pu@ieee.org

Abstract—**As the drone technology rapidly progresses, the notion of Internet of Drones (IoD) has surfaced as a vital framework for facilitating connections between aerial drones and existing cyber infrastructures. With ubiquitous IoD applications deployed in the modern cities, we need to focus on resolving security and privacy matters before enjoying the welfare benefits brought by these advanced applications. A minority of machine learning-based authentication systems recently emerged in the Internet of Things (IoT) community, however, these intelligent techniques have the data privacy and scalability problems. To confront the current unresolved authentication challenges in the realm of IoD, we propose a novel federated learning (FL) based authentication scheme, also referred to as FLASH, for futuristic IoD systems. The FLASH's basic idea is that a deep neural network (DNN) architecture is deployed with the ground stations to train an authentication model with drones' radio characteristics (e.g., carrier frequency offset and I-Q imbalance) in a decentralized way. The newly trained local models at the ground stations are encrypted using homomorphic encryption and send back to the IoD federated server for the aggregation of a new global authentication model. We conduct an experimental study in MATLAB and evaluate the performance of FLASH and other four benchmark schemes; the simulation results demonstrate that the FLASH is more effective than its counterparts.**

Index Terms—**Security and privacy, Internet of Drones, deep neural network, federated learning, authentication.**

I. Introduction

Thanks to the fast-paced advancements in UAV/drone technology, the Internet of Drones (IoD) has become a burgeoning aerial communication architecture which can seamlessly assist the exchange of IoD resources. An IoD system refers to the collective network of aerial drones and ground-based telecommunication infrastructures as well as the technology that facilitates communication between drones and telecommunication infrastructures, and between drones themselves [1]. By reason of the introduction of low-cost computing chips and high-bandwidth telecommunications, the IoD architecture has brought forth radical transformations in various industries, offering extensive possibilities for automation, enhanced efficiency, and better decision-making. For example, the IoD smart farming system empowers farms to accurately monitor crop health through aerial images and automate farming tasks efficiently (e.g., pesticide spray) [2]. With the support of other technology like machine learning, it is foreseen that the IoD architecture and its next-generation systems will enhance lives and usher in a new age of innovation and efficiency.

In the IoD applications, the remote pilots operate drones to collect the information of the interested target and deliver it to the ground stations. Not only do the ground stations serve as the information receivers, but they also administer and monitor IoD drone operations by issuing instructions and commands through a wireless medium [3]. As the IoD applications often involve critical and sensitive information (e.g., law enforcement, security surveillance, etc.) [4], the shared wireless spectrum automatically becomes an attack surface that can be easily targeted for unauthorized information access. Moreover, the initial design of IoD paradigm does not place emphasis on security and privacy. The major entity of IoD systems, drones, are also resource constrained. Thus, specialized security solutions are necessitated to achieve the required level of trustworthiness and resource protection for various IoD applications. Last but not least, drones are moving freely through the air, so it is effortless for adversary to capture and launch memory dump attacks to access the critical information. Hence, minimizing the storage of cryptographic keys in the memory is a highly effective approach.

To address the abovementioned privacy and security issues, as a part of the first line of defense in information security, mutual authentication, has become a promising method for protecting IoD networks from cyber attacks within the cyber-threat ecosystem [5]. Recently, numerous mutual authentication protocols, e.g., public key- [6], certificate- [7], token-based [8], and other approaches, have been developed for IoD environments. For example, in the public key-based approaches, a pair of public/private keys is pre-issued to drones and will be utilized to establish secure channels between drones and ground stations. Even though the existing approaches can somehow protect IoD networks from certain cyber attacks, they either fail to fulfill all the necessary privacy and security standards or experience performance issues. First, a central server is usually considered as a part of the existing security frameworks, which is responsible for managing the involvement of drones in system operations by governing their cryptographic keys. However, the central server could become a single point of failure, which would compromise the entire system's reliability and availability. Second, as the scale of IoD applications is expanded, the number of drones could experience an exponential increase, which will impose a substantial authentication load on the central server. Last, providing physical protection to drones can be quite challenging because of widespread deployment and varied

This work was supported by the National Science Foundation (NSF) through SaTC under Award 2333777.

979-8-3315-9673-6/26/$31.00 ©2026 IEEE

environments. Thus, integrating the physical uniqueness of drones into an authentication approach can greatly improve the security of IoD systems [9].

Inspired by the preceding discussion, in this paper we propose a *F*ederated *L*earning-based *A*uthentication *S*c*H*eme (referred to as *FLASH*) for IoD systems. The basic idea of *FLASH* is that ground stations in the IoD networks collaboratively build a global authentication model by training and submitting local authentication models to the federated server. To be specific, ground stations take advantage of drones' quadrature amplitude modulation (QAM) modulated radio frequency signal such as carrier frequency offset (CFO), I-Q features, and coefficient of frequency offset to train local models which will be used to authenticate drones within a federated learning framework. After that, ground stations encrypt their local model updates using homomorphic encryption before sending them to the federated server. In summary, the contributions of this paper are listed below:

- We propose a federated learning based authentication framework (hereinafter referred to as *FLASH*) for IoD environment, where ground stations collaboratively build a global authentication model in a federated manner.
- We select the unique features of drones' quadrature amplitude modulation (QAM) modulated radio frequency signal such as carrier frequency offset (CFO), I-Q features, and coefficient of frequency offset to train local models for drone authentication.
- We build an experimental environment in MATLAB and conduct extensive simulation-based evaluation with the comparsion of four benchmark schemes liteA4 [10], SLAP-IoD [11], SAAF-IoD [12], and PUF-IPA [13]. The source codes are publicly available at https://github.com/congpu/FLASH.

II. Background

A. Quadrature Amplitude Modulation (QAM) Modulation

In Fig. 1, we present an information flow diagram for drones' QAM modulated radio frequency signal based on [14]. Specifically, the transmitter (Tx) employs a 16-QAM modulator which is composed of two paths, In-phase (I) and Quadrature (Q), along with a DAC, known as digital-to-analog converter. The basic operational flow is that the DAC converts the digital signal into an analog signal, which will be further mapped to constellation points. The constellation points are used to portray various combinations of phase shifts and amplitude. A local oscillator (LO) frequency and a root-raised-cosine (RRC) filter are added to convert digital signals from one frequency to another and reduce intersymbol interference, respectively. Finally, the power amplifier (PA) id equipped to increase the power of signal to reach the receiver (Rx).

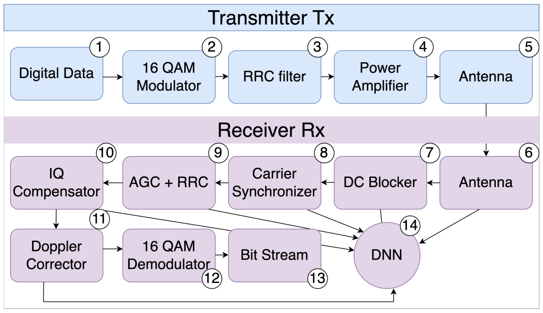

Fig. 1. Information flowchart for QAM modulated radio frequency signal.

On the receiving (Rx) side, the signal first passes through a direct current (DC) blocker, where the desired AC signals are processed, while any unwanted DC components are filtered out. After that, the signal reaches a carrier synchronizer, ensuring that the receiver's local oscillator is synchronized in frequency and phase with the incoming signal's carrier wave. The signal strength will then be adjusted by the automatic gain control (AGC) and RRC filter. In addition, an I-Q compensator is used to correct amplitude and phase imbalances between the in-phase (I) and quadrature (Q) components of a signal, while a Doppler corrector is employed to adjust for frequency shifts caused by relative motion between the transmitter and receiver. Finally, the signal is demodulated from the 16-QAM constellation to the bit stream. A Deep Neural Network (DNN) is also properly configured on the receiver (Rx) side to uniquely identify each component by analyzing distortions and transmission-induced features and assigning a unique identifier that facilitates multiclass classification.

B. Federated Learning

In 2017, Google scientists invented federated learning [15] with the goal of improving the effectiveness of machine learning models on electronic handheld devices while preserving user privacy. Since its inception, the concept of federated learning has broadened its applications to various domains such as supply chain, finance, healthcare, etc., where ensuring data privacy and security is crucial. The basic idea of federated learning is that a number of clients (or simply referred to as entities) collaboratively train a local model using their on-device data without sharing the actual data. After the local training session, each client shares the local model updates (e.g., biases and weights) with a central server, which further aggregates these decentralized updates to form a global model. Finally, the updated global model is then sent back to the clients, and the process repeats. In the cycles of federated learning, several aggregation techniques are available for the central server to aggregate local model updates. One of widely adopted approaches is Federated Averaging (in short FedAvg) which combines local model updates from clients by averaging them to create an improved global model.

III. Related Work

In [16], the authors introduced a swarm authentication mechanism that utilizes blockchain for the storage of drones' identity and cryptographic information. The approach was made feasible by using a clustering technique to dynamically form drone clusters based on their locations. Although the experimental study has demonstrated some improvements in network performance, the proposed approach still suffers from a scalability issue when the number of drones increases in the network, causing an increase in blockchain transactions. Consequently, the authentication bottleneck problem will occur as drones attempt to authenticate and update their cluster-related information. In [10], a novel authentication and key agreement approach is designed for aerial-ground communication environments, where drones and ground stations negotiate data type sensitive session keys with the assistance of cryptographic primitives such as hash function, bitwise XOR, and physical unclonable function (PUF). Unfortunately, as the aerial-ground communication systems expand to meet the diverse needs of various applications, the authentication scalability issue will require more effort to be addressed. [17] presents an authentication scheme that authenticates drones while maintaining a safe distance from the verifier. This is done by using machine learning to compare the sound recordings of drones against the sound recordings of the verifier. If the recordings are similar, the authentication succeeds. The problem with this approach is that the experiments were conducted in a controlled environment. It might not work or may introduce complexities when the environment changes (e.g. gusty winds).

Radio frequency (RF) fingerprinting is widely regarded as a technique to identify a radio transmitter (or wireless communication device) based on the unique characteristics of its signal transmission. The authors in [18] provide a tutorial of RF-based identification and authentication for Internet of Thing (IoT) devices, and then present a hybrid approach which takes advantage of deep learning's capability to extract the similarity of devices' fingerprints. The RF dataset of legitimate IoT devices is trained locally at the wireless receiver. However, the lack of physical protection for wireless receivers will make them vulnerable and a potential single point of failure. In [19], a fingerprinting framework is presented for Bluetooth devices. The proposed fingerprinting approach adopts convolutional neural network and gated recurrent unit to achieve high fingerprinting accuracy. However, the gated recurrent unit introduces additional complexity to the framework, which might require significant computational power.

IV. The Proposed Authentication Scheme

In this section, we describe the proposed federated learning (FL) based authentication scheme (later just FLASH) for IoD systems. The basic idea of the FLASH is to deploy a deep neural network (DNN) model at ground stataions to train an authentication model with drones' radio characteristics (e.g., carrier frequency offset and I-Q imbalance) in a decentralized way. The newly trained local models at the ground stations are encrypted using homomorphic encryption and sent back to the IoD federated server for the aggregation of a new global authentication model. The rationale behind using radio characteristics for drone authetnication is that the manufacturing process of each drone's radio transmitter has slight differences, which can be exploited to uniquely identify each drone.

A. System and Adversary Models & Security Requirements

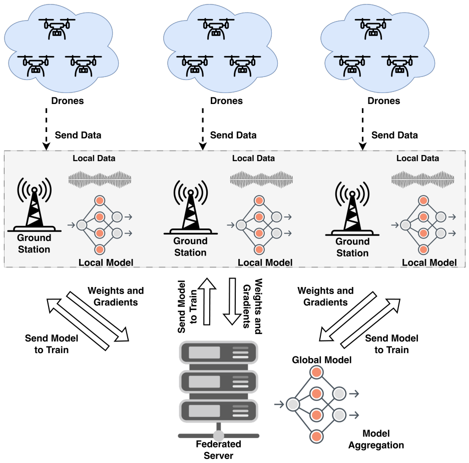

Fig. 2. The system architecture of FLASH.

As shown in Fig. 2, the FLASH consists of three major entities, drones, ground stations, and a federated server. A number of uniquely-identified drones perform tasks in an area of interest and deliver them (i.e., data) to ground stations via unsecured wireless channels. When the drone flies into the communication scope of ground station, it broadcasts a beacon message which piggybacks its pseudonym. It is worth mentioning that the drone flies fast along a specified path or trajectory and the communication scope of ground station is constrained. The process of authenticating the drone not only needs to be communication-efficient, but also does not take up too much of the drone's sojourn time within the ground station's coverage area. The rationale is that when the drone flies out of the coverage area of ground station, the authentication as well as the task delivery process will fail. We assume that each drone is equipped with an integrated circuit consisting of a unique radio transmitter due to variations in manufacturing techniques and processes, however, the design of radio transmitter is out of the scope of this paper. Ground stations are considered as trusted entities, while drones are untrusted and resource-constrained.

According to the widely adopted Dolev–Yao adversary model in [20], entities using an insecure wireless channel for communication are deemed untrustworthy. Consequently, an adversary can eavesdrop on, copy, tamper with, modify, replay, or erase the messages transmitted over insecure wireless channels. The adversary's objective is to set up an authenticated communiation with ground stations without being noticed, and then establish an authentication with ground stations without being detected, and then inflict significant harm on individuals or organizations. The FLASH must achieve the following security requirements. (i) Authentication: The identity of drones needs to be verified, ensuing that the drone delivering tasks is who it claims to be. (ii) Integrity: The accuracy and consistency of local authentication models and global authentication model cannot be compromised. (iii) Pseudonym: The legitimate drone will use its fictitious name as an alternative to its real identifier in the beacon messages. (iv) Confidentiality: Legitimate devices' identity information and their radio frequency (RF) signals' characteristics shall not be included in local authentication models. and (v) Access Control: Unauthorized drones shall not be allowed to deliver tasks to ground stations.

B. Federated Learning-Based Authentication Scheme

In the following, we present the details of the proposed federated learning-based authentication scheme (FLASH), As

TABLE I
DNN MODEL PARAMETERS

DNN Parameters	Details
Input Size	10
Output Size	2
Hidden Layers Count	3
No. of Neurons in Layers*	150/80/50
Batch Size	32
Activation Function (Hidden)	ReLU
Activation Function (Output)	Softmax
Regularization	L2

*:150 neurons in the first layer, 80 neurons in the second layer, and 50 neurons in the third layer.

shown in Fig. 2, a deep neural network (DNN) architecture is deployed at ground stations to train an authentication model with drones' radio characteristics (e.g., carrier frequency offset and I-Q imbalance) in a non-centralized fashion. And then, the ground stations encrypt the newly trained local models using homomorphic encryption and send them back to the IoD federated server which will aggregate them into a new global authentication model.

First, the federated server initializes the global model utilizing a deep neural network. Here, the global model $GlobalModel$ and the threshold value thr_{auth} of authenticating drones are initialized with the radio characteristics of several legitimate drones. The $GlobalModel$ is a base template that will be iteratively updated based on the local models from the ground stations. After initialization, the federated server distributes $GlobalModel$ and thr_{auth} to all participating ground stations in the framework. As a result, all ground stations have a copy of $GlobalModel$, which enables them to begin the training of local models.

Second, when a drone flies into the broadcasting range of the ground station, it sends a beacon message piggybacked with its fictitious identifier FID_{drone} to the ground station. If there is an entry in the database that stores all registered drones' FID_{drone} and other identification information, the ground station proceeds with the following steps. Otherwise, the ground station will discard the drone's beacon message. The usage of FID_{drone} in the beacon message will guarantee the privacy of drone identities. After receiving drones' beacon messages, the ground stations commence training the local autnetication models and authenticting the drones in the following steps. (i) The ground stations use the drones' radio frequency information to train the local authentication model iteratively using stochastic gradient descent (SGD). (ii) The ground stations adjust their local model parameters (weights and biases); (iii) The ground stations calculate the Euclidean distance between their local model updates and the global authentication model. If the Euclidean distance is less than thr_{auth}, the drones are authenticated. Otherwise, the beason messages are discared and the authentication requests of drones are declined. and (iv) The ground stations encrypt the local model updates using homomorphic encryption and send them to the federated server for aggregation.

Third, after receiving the local model updates from ground stations, the federated server aggregates them using Federated Averaging (FedAvg). Here, FedAvg enables the federated server to build a global authetnication model without requiring the transfer of drones' radio frequency information from the ground stations. After the aggregation process is completed, the federated server form a new global authentication model $GlobalModel$. And then, the federated server redistributes the updated $GlobalModel$ to all ground stations. Finally, the ground stations replace their local models with the newly received $GlobalModel$.

C. Deep Neural Network Architecture

The ''Datasets for RF fingerprinting'' [21] is used in the deep neural network (DNN) architecture. We first preprocess the raw continuous stream of IQ values into distinct frames and discard noisy frames. After that, we apply various signal processing techniques ncluding matched filtering, frequency compensation, and timing recovery to process each frame. These signal processing techniques help enhance the signal-to-noise ratio and are useful for correcting the frequency offset as well as timing errors observed during transmission and reception. The outcome of the dataset preprocessing process is robust data that is reliable for interpretation and analysis by the DNN architecture.

The proposed DNN model consists of three hidden layers, each followed by a Rectified Linear Unit (ReLU) activation function. The input layer directly depends on the number of features extracted for drone authentication. In this paper, 10 features including radio frequency and I-Q are adopted. The first hidden layer consists of 150 neurons, which work as an abstraction for the input data. The ReLU activation function is critical as it introduces non-linearity and enables the learning of complex patterns within the model. The second layer is composed of 80 neurons to support and capture the convoluted relationships in the feature set. The third layer contains 50 neurons and continues abstraction while learning the relationships and patterns from the preceding layers. Finally, the output layer uses a softmax activation function for multi-class classification. It converts the model output into probability scores that are ideal for drone authentication. Table I lists all parameters used in the proposed DNN model.

D. Drone's Radio Frequency (RF) Features

Radio frequency (RF) properties are widely regarded as a robust mechanism for electronic device identification and authentication. The rationale is that the unique fingerprints of radio frequencies derived from devices' communication signals are inherently tied to their transmitters. In the FLASH, we consider the RF features derived from the Quadrature Amplitude Modulation (QAM) [22]. QAM is a modulation technique that combines amplitude and phase modulation to transmit data efficiently over various types of media.

Frequency Features: In the drone's radio transmitter, the ocal oscillator (LO) causes the small deviations between the intended frequency and the actual frequency, which is widely known as frequency offset. The permissible frequency offset range varies based on the applicable standard. For example,

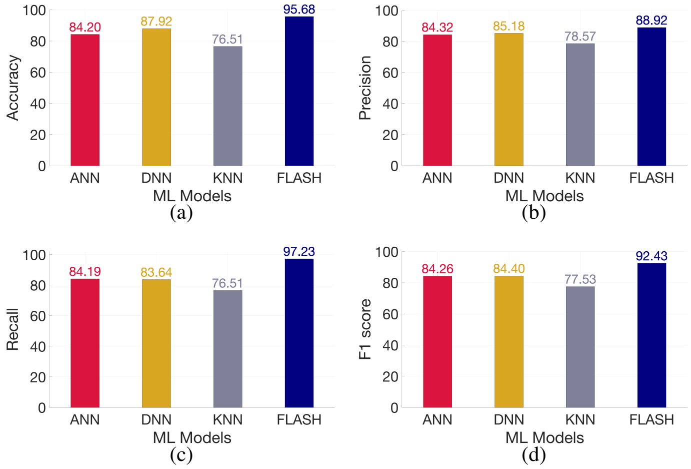

Fig. 3. The results of accuracy, precision, recall, and F1 score for the FLASH and other machine learning models.

according to the IEEE 802.11b standard, the deviations should be within 25 parts per million (ppm).

I-Q Features: In-phase (I) and quadrature (Q) components enable a QAM modulator to encode information by varying both the amplitude and phase of a signal. Due to variations in the manufacturing process of transmitters, the in-phase and quadrature components may not have the same amplitude, which may result in an amplitude mismatch. Likewise, the phase can be deviated and the quadrature phase may not be exactly 90 degrees out of phase with the in-phase component.

Coefficient of Frequency Offset: The coefficient of frequency offset is defined as the ratio of standard deviation to the mean of carrier frequency offset.

In summary, a total of ten features are derived for the training of DNN model. Carrier frequency and coefficient of frequency offsets represent two features. The remaining eight features are extracted from the I-Q values with one feature from each of the four quadrants.

V. Performance Evaluation

A. Experimental Environment and Dataset

We set up a MATLAB-based simulation environment on a Windows 11 desktop with 16GB of RAM and a 12th generation Intel processor (2.10 GHz) for experimental study. The FLASH is simulated using the Neural Network Toolbox in MATLAB, adhering to a 16-QAM modulation scheme. The preprocessing steps, such as matched filtering, frequency compensation, etc., are achieved using MATLAB‘s Signal Processing Toolbox. Not only do we implement the FLASH, but we also choose to implement four other benchmark schemes such as liteA4 [10], SLAP-IoD [11], SAAF-IoD [12], and PUF-IPA [13] for performance comparison and analysis. The simulation results of running time, CPU time, and memory overhead are measured and obtained by changing the number of algorithm executions.

The dataset that we used to train the authentication model is ‘‘Datasets for RF Fingerprinting’’ [21]. The dataset contains raw IQ samples from 16 USRP X310 software-defined radios (SDRs) which were taken at varying distances between 2 feet and 62 feet. As 16 USRP X310 SDRs were utilized in the dataset and each SDR generates 1000 frames, the input size for the FLASH is 16,000. For a total of 10 features, the size of feature set become $1.6{\times}10^5$. In addition, the emissions of USRP X310 SDRs are IEEE 802.11a standard-compliant and can be generated by MATLAB WLAN System toolbox. After preprocessing, the entire dataset is distributed into multiple subsets: 70% for training, 15% for validation, and 15% for testing, respectively.

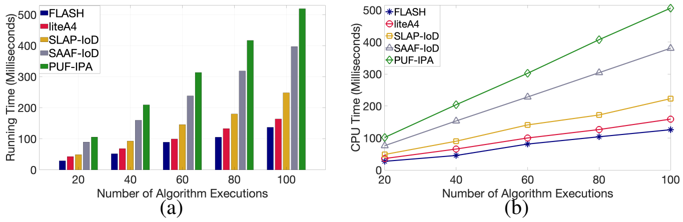

Fig. 4. Comparison of running time and CPU time against the number of algorithm executions.

B. Comparison with Machine Learning Models

First, we compare the FLASH with other machine learning models including Artificial Neural Network (ANN), Deep Neural Network (DNN), and K-Nearest Neighbors (KNN) in terms of accuracy, precision, recall, and F1 score. Accuracy measures the overall correctness of a given machine learning model’s predictions, and it is calculated as the ratio of the number of correct predictions to the total number of predictions made. As shown in Subfig. 3(a), our approach FLASH obtains the highest accuracy in comparison to other three machine learning models. The rationale behind that is the nature of collaborative learning in the FLASH, which enables ground stations to learn from various drones’ RF signals without utilizing the centralized data. Precision measures the accuracy of positive predictions. In Subfig. 3(b), the FLASH achieves the highest precision among all tested machine learning models. Here, achieving a higher precision value indicates that the FLASH does not consider adversarial drones’ RF signals as legitimate ones. Recall is the measurement of the machine learning model’s ability to correctly identify all instances from all positive samples in the dataset. As shown in Subfig. 3(c), the FLASH shows the highest recall value, while KNN delivers the lowest recall score. These results prove that our approach FLASH is able to effectively identity legitimate drones in highly dynamic environments. F1 score represents the harmonic mean of precision and recall of a machine learning model. For the machine learning based authentication model, providing high security (high precision) while maintaining availability for legitimate drones (high recall) is both important. It is clear that our approach FLASH outperforms other three machine learning models in Subfig. 3(d). It effectively conveys that the FLASH has a balanced performance, as indicated by the highest F1 score, making it an ideal authentication protocol for real-world applications.

C. Comparison with Traditional Authentication Schemes

Second, we compare the FLASH with four traditional authentication schemes such as liteA4, SLAP-IoD, SAAF-IoD,

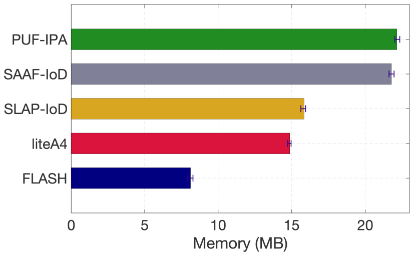

Fig. 5. Storage overhead.

and PUF-IPA. Here, the training portion of the FLASH is not considered in the comparison.

In Subfig .4(a), we measure and present the running time of FLASH, liteA4, SLAP-IoD, SAAF-IoD, and PUF-IPA. It is clearly shown that the FLASH has the least running time because it simply measures the distance between model updates and compares drones' RF signals with the authentication threshold. In contrast, liteA4, SLAP-IoD, SAAF-IoD, and PUF-IPA not only need to frequently retrieve the stored cryptographic information, but also to encrypt/decrypt it. Moreover, the CPU time with a varying number of algorithm executions is presented in Subfig .4(b). Apparently, the FLASH achieves the least CPU time since it executes the smallest number of operations to authenticate drones. Finally, we demonstrate the storage overhead of FLASH, liteA4, SLAP-IoD, SAAF-IoD, and PUF-IPA in Fig. 5. The median value of memory (RAM) is plotted, with error bars showing the maximum and minimum values. The traditional authentication approach, i.e., liteA4, SLAP-IoD, SAAF-IoD, and PUF-IPA, utilize a significant amount of memory to perform cryptographic operations such as hashing, pairing, etc. However, our approach FLASH requires less memory to authenticate drones as it only needs to compute the distance between model updates and compare it with the authentication threshold.

VI. Conclusion

In this paper, a novel federated learning based authentication approach was proposed for IoD systems, wherein multiple ground stations train drones' RF signals locally and submit the updated weights and gradients to the IoD federated server. Our approach utilizes the inherent variations present in radio transmitters (Tx) to extract features and build a deep neural network (DNN), resulting in a robust machine learning model that can authenticate drones based on their radio RF signals. We implemented our approach and benchmark schemes in MATLAB, and compared them in terms of accuracy, precision, recall, and F1 score, running time, CPU time, and storage overhead. The experimental study showed that our approach is more effective than its counterparts. For future work, we plan to use other modulation schemes such as orthogonal frequency-division multiplexing (OFDM) to extract features and explore other neural networks such as Recurrent Neural Networks (RNN) or Convolutional Neural Networks (CNN).

References

[1] C. Pu, A. Bilal, N. Park, J. Seol, and K. Choo, "A Redactable Blockchain-Assisted Application-Aware Authentication System for Internet of Drones," *IEEE internet of things journal*, vol. 12, no. 14, pp. 27 206–27 221, 2025.

[2] M. Elumalai, T. Fernandez, and M. Ragab, "Machine Learning (ML) Algorithms on IoT and Drone Data for Smart Farming," *Intelligent Robots and Drones for Precision Agriculture*, pp. 179–206, 2024.

[3] C. Pu, C. Warner, K. Choo, S. Lim, and I. Ahmed, "liteGAP: Lightweight Group Authentication Protocol for Internet of Drones Systems," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 4, pp. 5849–5860, 2024.

[4] A. Shahidinejad and J. Abawajy, "Anonymous Blockchain-Assisted Authentication Protocols for Secure Cross-Domain IoD Communications," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 3, pp. 2661–2674, 2024.

[5] I. Bhattarai, C. Pu, and K. Choo, "A Lightweight Aggregate Authentication Protocol for Internet of Drones," in *Proc. IEEE CCNC*, 2024, pp. 143–151.

[6] Z. Zhang, C. Hsu, M. Au, L. Harn, J. Cui, Z. Xia, and Z. Zhao, "PRLAP-IoD: A PUF-based robust and lightweight authentication protocol for Internet of Drones," *Computer Networks*, vol. 238, p. 110118, 2024.

[7] M. Khan, I. Ullah, N. Kumar, F. Afghah, G. Barb, F. Noor, and S. Alqahtany, "A Certificate-Based Ring Signcryption Scheme for Securing UAV-Enabled Private Edge Computing Systems," *IEEE Access*, vol. 12, pp. 83 466–83 479, 2024.

[8] C. Pu, A. Wall, and K. Choo, "Bilinear Pairing and PUF Based Lightweight Authentication Protocol for IoD Environment," in *Proc. IEEE MASS*, 2022, pp. 115–121.

[9] C. Pu, K. Choo, and I. Bhattarai, "Chebyshev Polynomial and Private Blockchain Based Cross-Domain Authentication Protocol for IoD Networks," in *Proc. IEEE CCNC*, 2024, pp. 931–936.

[10] I. Bhattarai, C. Pu, K. Choo, and D. Korać, "A Lightweight and Anonymous Application-Aware Authentication and Key Agreement Protocol for the Internet of Drones," *IEEE Internet of Things Journal*, vol. 11, no. 11, pp. 19 790–19 803, 2024.

[11] S. Yu, A. Das, Y. Park, and P. Lorenz, "SLAP-IoD: Secure and Lightweight Authentication Protocol Using Physical Unclonable Functions for Internet of Drones in Smart City Environments," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 10, pp. 10 374–10 388, 2022.

[12] M. Tanveer, H. Alasmary, N. Kumar, and A. Nayak, "SAAF-IoD: Secure and Anonymous Authentication Framework for the Internet of Drones," *IEEE Transactions on Vehicular Technology*, pp. 1–13, 2023.

[13] M. Qureshi and A. Munir, "PUF-IPA: A PUF-based Identity Preserving Protocol for Internet of Things Authentication," in *Proc. IEEE CCNC*, 2020, pp. 1–7.

[14] B. Chatterjee, D. Das, S. Maity, and S. Sen, "A Lightweight and Anonymous Application-Aware Authentication and Key Agreement Protocol for the Internet of Drones," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 388–398, 2018.

[15] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," in *Proc. AISTATS*, 2017, pp. 1273–1282.

[16] R. Karmakar, G. Kaddoum, and O. Akhrif, "A blockchain-based distributed and intelligent clustering-enabled authentication protocol for UAV swarms," *IEEE Transactions on Mobile Computing*, 2023.

[17] C. Wu and Q. Zeng, "Turning Noises to Fingerprint-Free "Credentials": Secure and Usable Drone Authentication," *IEEE Transactions on Mobile Computing*, vol. 23, no. 10, pp. 10 161 – 10 174, 2024.

[18] J. Zhang, G. Shen, W. Saad, and K. Chowdhury, "Radio Frequency Fingerprint Identification for Device Authentication in the Internet of Things," *IEEE Communications Magazine*, vol. 61, no. 10, pp. 110–115, 2023.

[19] A. Jagannath and J. Jagannath, "Embedding-Assisted Attentional Deep Learning for Real-World RF Fingerprinting of Bluetooth," *IEEE Transactions on Cognitive Communications and Networking*, vol. 9, no. 4, pp. 940–949, 2023.

[20] C. Pu, "A Featherweight Authentication and Key Agreement Scheme for Internet of Drones Applications," in *Proc. IEEE PIMRC*, 2023, pp. 1–6.

[21] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, and K. Chowdhury, "ORACLE: Optimized radio classification through convolutional neural networks," in *Proc. IEEE INFOCOM*, 2019, pp. 370–378.

[22] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning," *IEEE internet of things journal*, vol. 6, no. 1, pp. 388–398, 2019.