POSTER: FL-Guard: A Federated Learning Based Ground-Air Secure Communication Model For Future Aviation Network

Suleman Khan, An Braeken, Pardeep Kumar, Andrei Gurtov

ABSTRACT

L-band Digital Aeronautical Communication System (LDACS) is a newly proposed modern state of the art system that will enable communication, navigation, and surveillance in the future aviation network. The current LDACS system does not prevent and detect intrusion within the LDACS domain. Therefore, it may suffer from various cyber-attacks, including spoofing, injection and many more attacks. To the best of our knowledge, this paper proposes the first federated learning-based attack detection model, called FL-Guard for LDACS. Our proposed model exploits a federated learning environment, and it uses a deep neural network (DNN) to detect possible attacks on LDACS based Air-Ground communication. FL-Guard is simulated on a network of four airplanes, and the preliminary results show that the proposed model can detect attacks with 89% accuracy.

ACM Reference Format:

Suleman Khan, An Braeken, Pardeep Kumar, Andrei Gurtov. 2022. POSTER: FL-Guard: A Federated Learning Based Ground-Air Secure Communication Model For Future Aviation Network. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Developing new modes of communication for future aviation network is one of the challenges in aviation industry. A recent report [1] shows that the world's aircraft fleet will be expected to grow from 26,000 to over 49,500 aircraft between 2019 and 2039. Consequently, the current Air Traffic Management (ATM) system will approach its current capacity limit, especially in Europe and the United States [5]. Therefore, their is an immense need of new aviation communication systems that can meet the future demands.

However, new advancements such as a digital-based architecture for aeronautical communications will likely replace the traditional analog systems, such as very high frequency. In this aspect, the European aviation network along with several research organizations have launched a Single European Sky ATM Research (SESAR) project. The main focus of SESAR is to enhance the digital transformation and decarbonization of aviation communication using Internet Protocols (IPs) and network softwarization. Therefore, IP-based global air-ground, ground-ground and air-air communication networks are being built and that will enhance new broadband air-ground data link services for future communication infrastructure.

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

L-band Digital Aeronautical Communications System (LDACS) is one of the initiatives for the Future Communication Infrastructure (FCI). LDACS is used for long-range terrestrial aeronautical communications systems [3], and it supports two communication links (i) Air-Ground (A/G) link for long-distance terrestrial communication, and (ii) Air-Air (A/A) link. The LDACS will enable IP-Based various services such as communication, navigation, and surveillance in an aviation network.

Indeed, LDACS supports various innovations, e.g., digital transformation and decarbonization of aviation communication using (open) Internet protocols (IPs). However, the current LDACS neither detect not protect intrusion and that will open an immense threat vector. Such intrusion may lead to several attacks on LDACS-based aviation. More precisely, a malicious attacker with low cost devices can trigger various irreversible cyber attacks to capture and manipulate messages, delete them, inject false messages between the air-ground communications. In addition, an attacker can also pose the privacy issues on air-ground communication, if a very important person or a celebrity is on-board. However, the current attack detection systems may not be directly deployed as they suffers from various adversarial and posing attacks. Therefore, a robust solution is needed, which can achieve data security and privacy in LDCAS based future aviation network.

To mitigate aforementioned issues, we developed FL-Guard, a novel specialized security model that will utilize federated learning not only to enhance the security of the LDCAS communication but it will also provide the privacy to the aircraft's messages, such as latitude, longitude, velocity, squawk, etc. It is worth to mention that the FL-Guard model can be deployed at the ground station (i.e., air traffic controller (ATC)) and/or at the aircraft. In air-to-ground link, whenever, an aircraft is communicating messages to the ATC, all the messages will be first filtered by the FL-Guard and then the filtered messages will be forwarded to the ATC. If the message is abnormal then the FL-Guard will raised an alarm and drop the communication. Otherwise, it will directly forward those messages to the ATC. Likewise, the FL-Guard will detect and protect the air-air communication in LDCAS network. We evaluated our FL-Guard security model on 4 aircrafts and we achieved promising 89% testing accuracy for attack class.

In this paper, we only considered alteration and spoofing attacks. The data of these attacks were generated using the ADSB simulator, while normal aircraft messages were collected from the Arlanda Airport, Sweden. While to protect the system from adversary and poisoning attacks, we used the federated learning technique. Federated learning will serve us in two ways by providing security and privacy for the LDACS base aircraft.

2 THREAT MODEL FOR FCI

It is worth to note that the current FCI communication system broadcast plain text (e.g un-encrypted messages). However these

plain text messages can be manipulated or intercepted by an attacker using inexpensive off-the-shelf hardware and software [2]. Moreover, an attacker can perform other attacks such as poisoning and adversarial attacks. As shown in Figure 1, we assume that an attacker will be able to capture the plain text messages on the ground communication from the LDACS communication and can then poison them. Data poisoning may include the alteration of features like for example ICAO number, speed, position information, latitude or longitude, etc.

In the adversarial attack, we assume that an attacker can get somehow into the training system and he or she can change the training parameters of the system to mislead the training system. Again in that case the training model will not be the ideal one, which can lead to many issues on the LDACS based Air-Ground communication system. In addition an attacker can also launch traditional attacks as Alteration attack, replay attack, spoofing attack etc. Such attacks may lead to wrong decisions, eventually being life threatening in Air-Ground communication.

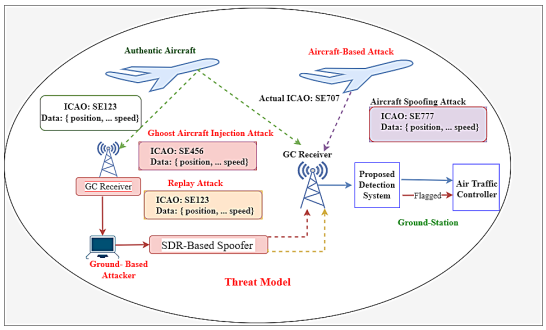

Figure 1: Threat Model for FCI [4]

3 PROPOSED SOLUTION

Our proposed FL-Guard security model exploits federated learning along deep neural network (DNN) to achieve security and privacy during the training phase.

We selected 4000 data samples for four aircrafts. These data samples consist of normal messages and anomaly messages. After data collection we performed data standardisation to scale the numeric values. After that, the categorical features are converted into numeric features before passing these features to our proposed model. We split the data-set into 90:10 ratio for training and testing respectively.

3.1 Federated Averaging on MLP model: Training on edge.

We propose a novel attack detection framework to train the LDACS data model on the edge without compromising on aircraft data privacy and reducing the bandwidth cost in data transfer between air traffic controllers and aircraft pilots. The framework is an implementation of a DNN model consisting of two hidden layers that are used as a classification model to detect and identify attacks in the LDACS message protocol. To illustrate, we send the training data to four virtual aircrafts and send our local Multi-layer Perceptron (MLP) model to train on each of these aircrafts. Once the training on every aircraft is complete, we fetch the trained parameters and aggregate them onto a federated server. Next time, we update and send an improved version of the model. The training and update are thus making the model more robust to new changes in the aircraft message data and enable quickly learning and adapting to it. Algorithm 1 (i.e., 1-9 steps) shows the FL-based FL-Guard.

Algorithm 1: Federated Averaging on MLP model

1. **Input**: X ← LDACS Message Sequence Data
2. **Output**: O ← LDACS attack detection
3. Data Pre-processing: Initial Feature set F:, {f1,f2,....,f9}
3.1 Label Encoding, X[C] ← L(C) where C is set of categorical features from F
3.2. $X' = \frac{X-\mu}{\sigma}$ Data Standardization
4. Load the training data X ← Tensor(X') as pytorch tensors
5. X1 ← X[:1000].to(A1), X2 ← X[1000:2000].to(A2), X3 ← X[2000:3000].to(A3), X4 ← X[3000:4000].to(A2) : Data-set Split
7. **for** `epoch in range(1, 25)` **do**
   for `batch(X) in Data Locate:{X1, X2, X3, X4}` **do**
      `L1 <- ReLU(Linear(batchX))`
      `L2 <- ReLU(Linear(L1, 100))`
      `L3 <- ReLU(Linear(L2, 50))`
      `Output <- Softmax(L3)`
      `L <- cross-entropy-loss(Output, Label)`
      $\frac{\partial L}{\partial W}$, `Gradient local optimization`
      `model <- Get(modelX)`
      `Final Model,` $W_{t+1} \leftarrow \sum_{i=1}^{K} \frac{n_i}{N} W_{t+1}^{i}$ `Aggregate(model: X1, X2, X3, X4)`
   end
end
8. $\sum_{i=1}^{K} W_{t+1}^{i} \leftarrow W_{t+1}$, Model updates on local servers
9. Test the model accuracy % on **Federated Server**, return.

4 EXPERIMENT SETUP AND RESULT

Google Colab, Google's online Graphical Processing Unit (GPU), is used for the experiment. We used Python 3.7 as our programming language and a personal computer with a higher-capacity operating system (Windows 10), 8GB RAM, and a Core i7 system with a 1.8GHz processor for this study.

Our proposed model testing accuracy is 87%, and we believe that it will increase as we collect more data and train and test our proposed model in more aircrafts, which is the subject for our future work.

5 CONCLUSION AND FURURE WORK

In this paper, we proposed an attack detection model FL-Guard for the LDACS aviation network. We used Federated Learning to achieve model privacy and detect cyber attacks on the LDACS system. Currently, our initial results show that our proposed system is 89% accurate. In the future, we will extend this work to collect more LDACS datasets in order to perform more attacks and test our model on a generalized dataset.

REFERENCES

[1] 2017. Asia's Civilian Aircraft Fleet to be Biggest by Far in 2035. https://www.statista.com/chart/9874/size-of-civilian-aircraft-fleets-by-world-region
[2] Manesh et.al. 2017. Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system. *International Journal of Critical Infrastructure Protection* 19 (2017), 16–31.
[3] Schnell et.al. 2014. LDACS: Future aeronautical communications for air-traffic management. *IEEE Communications Magazine* 52, 5 (2014), 104–110.
[4] Ying et.al. 2019. Detecting ADS-B spoofing attacks using deep neural networks. In *2019 IEEE conference on communications and network security (CNS)*. IEEE, 187–195.
[5] EUROCONTROL. 2020. Challenges of Growth 2013 Task 4: European Air Traffic in 2035. http://www.eurocontrol.int/articles/challengesgrowt

Poster: FL-Guard: A Federated Learning Based Ground-Air Secure Communication Model For Future Aviation Network

Suleman Khan, An Braeken, Andrei Gurtov, Pardeep Kumar

Introduction

- Developing new modes of communication for future aeronautical communications is one of civil aviation's significant challenges in the coming years.
- A digital-based architecture for aeronautical communications will likely replace the traditional analog systems.
- L-band Digital Aeronautical Communications System (LDACS) is one of the initiative for the Future Communication Infrastructure (FCI).
- LDACS (L-band Digital Aeronautical Communications System) is a candidate for long-range terrestrial aeronautical communications systems.
- The LDACS will enable IP-Based various services such as communication, navigation, and surveillance in an aviation network.
- However, it opens an immense threat vector that may lead to several attacks on LDACS base air-ground communication system.

Key Challenges	
LDACS	A malicious attacker with low-cost devices mat performs injection, replay, spoofing alteration attacks, etc.
	It is easy to break the FCI's security using commercial hardware and software
	Traditional machine learning attack detection system suffers from adversary and poisoning attacks
FL	Privacy-preserving in learning and aggregation
	Robust to adversarial attacks
	Complex incentive mechanism

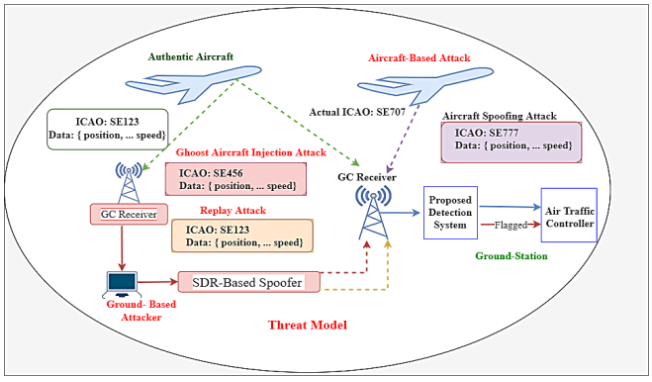

Fig 1: LDACS Threat Model [1]

	Main Objectives
1.	We developed FL-Guard, a novel specialized security model that will utilize federated learning to enhance the security and privacy of the training model for future aviation networks.
2.	Our proposed FL-Guard model will be deployed at both sides, e.g., Air and Ground.
3.	FL-Guard can detect the data sequence as normal or attack with high accuracy through experimentation at the earliest time.

FL-Guard Training

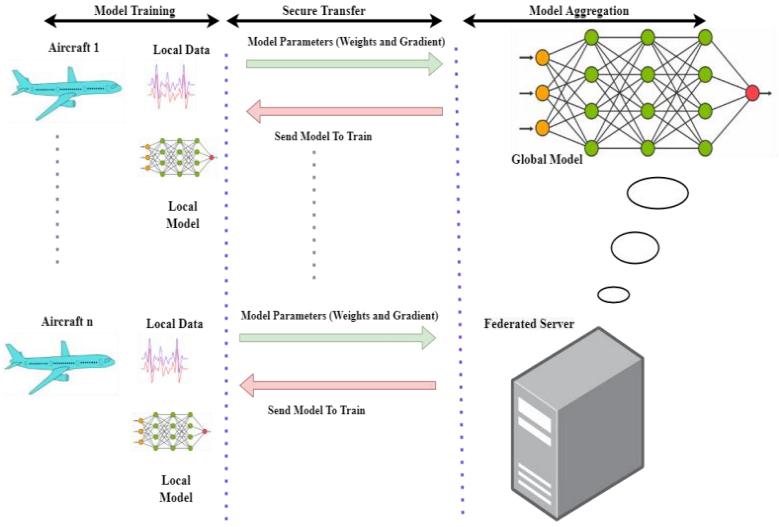

Fig 2: FL-Guard Training Architecture

Federated Averaging on MLP model: Training on the edge
➢ We propose a novel attack detection framework called FL-Guard to train and test LDACS data model on edge without compromising aircraft data security, privacy and reducing the bandwidth cost in data transfer between air traffic controller and aircraft pilot.
➢ The framework implements a Deep Neural Network model consisting of 2 hidden layers used as a classification model to detect and identify attacks in message protocol.
➢ To illustrate, we send the training data to 4 virtual aircraft and send our local (DNN) model to train on each of these aircraft.
➢ Once training on every aircraft is complete, we fetch the trained parameters only and aggregate them onto a federated server.
➢ Next time, update and send an improved version of the model.
➢ The training and update are continuous and thus making the model robust to new changes in aircraft message data and quickly learning and adapting to it.

Configuration of Experimental Nodes	
CPU	1.8 GHz Intel Core TM (7 cores)
Memory	16 GB
Storage	500 G HHD
OS	Windows 10

Initial Results

Our proposed FL-Guard model testing accuracy is 89%, and we believe that it will increase as we collect more data and train and test our proposed model in more aircraft, which is our future work.

Conclusions and Future Work

In this paper, we proposed a novel attack detection system called FL-Guard. The proposed solution will work on both side e.g., Air and ground to detect attacks on LDACS system. In the future, we will extend this work to collect LDACS dataset and perform more attacks and test our model on a generalized dataset.

Counter Measure Against Attacks
➢ To protect the LDACS system against cyberattacks, we will embed our proposed solution on the ground side (ATC) as well as inside cockpit.

References

[1] Ying, Xuhang, et al. "Detecting ADS-B spoofing attacks using deep neural networks." *2019 IEEE conference on communications and network security (CNS)*. IEEE, 2019

LINKÖPING UNIVERSITY

LINKÖPING UNIVERSITY
DEPARTMENT OR CENTRE