



Machine Learning and Cyber Security: Robust Protection Against Digital Attacks



SINAPSE

Prof. Fun Hu

University of Bradford



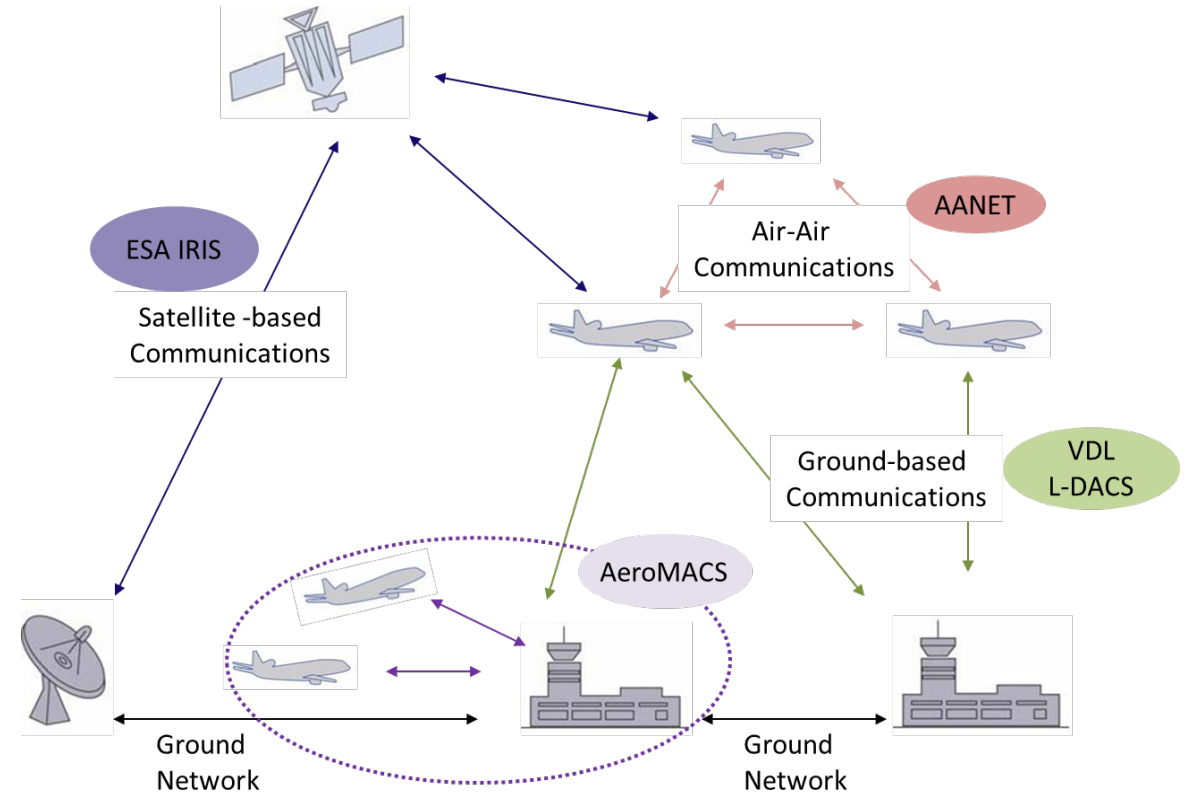
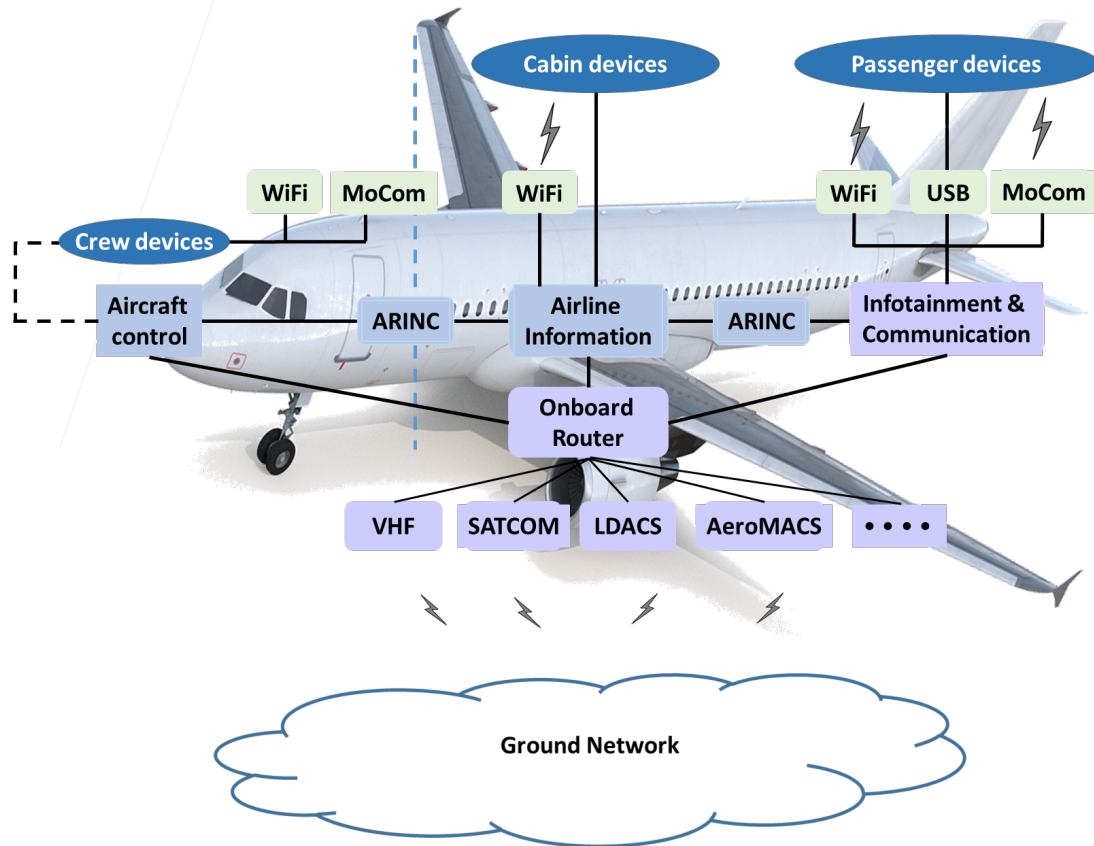
Co-funded by
the European Union

EUROPEAN PARTNERSHIP

SINAPSE TEAM



Today's aeronautical communications



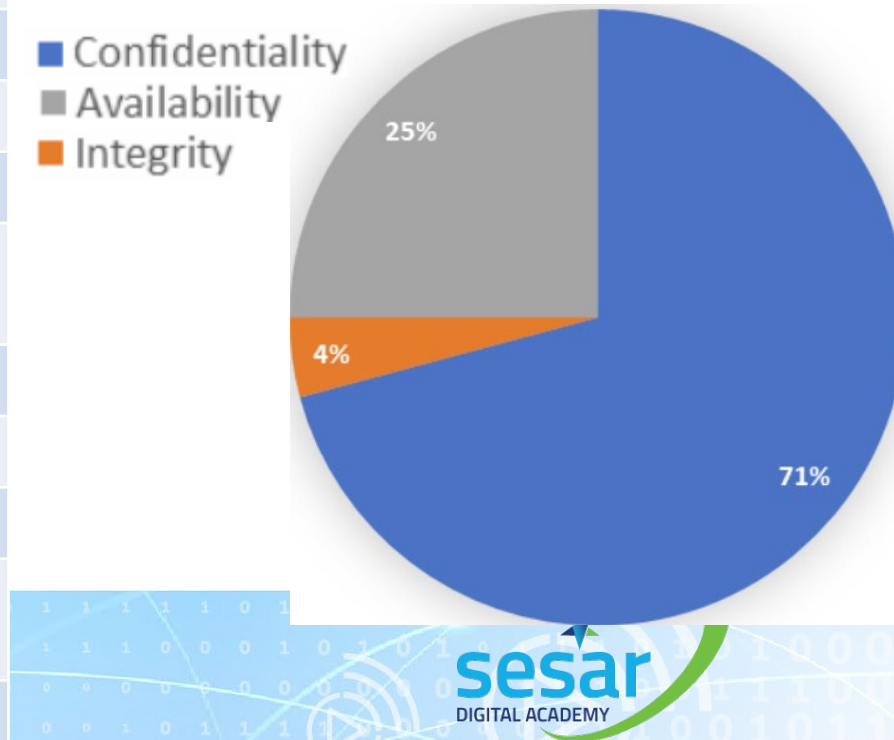
Recent ATM related Cyber Crimes

E. Ukwandu, M.A. Ben-Farah et al, "Cyber-Security challenges in Aviation Industry: A Review of Current and Future Trends", MDPI Information 2022, doi.org/10.3390/info13030146.

Attack Type	Year	Location	Incident
I	2021	Birmingham, United Kingdom	Software error resulted into 1606KG more than take-off limit
C	2020	San Antonio, USA	Ransomware attack
C	2020	Denver, USA	Ransomware attack
C	2019	New Zealand	Phishing attack
C	2019	Europe	Crypto mining Malware Infection
C	2019	Albany, USA	Ransomware attack
C	2019	Toulouse, France	Cyber incident
A	2019	Ben Gurion Airport, Israel	Bot attacks
A	2018	Sweden	Cyber-attack launched by Russian APT28 group
C	2018	Washington, DC, USA	Data breach
A	2018	Bristol Airport, UK	Ransomware attack
C	2018	United Kingdom	British Airways Data breach of about 380K customers' PID information
A	2018	Boryspil, Ukraine	Malware Cyber-attack

Some cyber attacks in aviation reported in OTR during last 5 years

High number of confidentiality attacks in aviation demands higher measures for data privacy and minimised data vulnerabilities

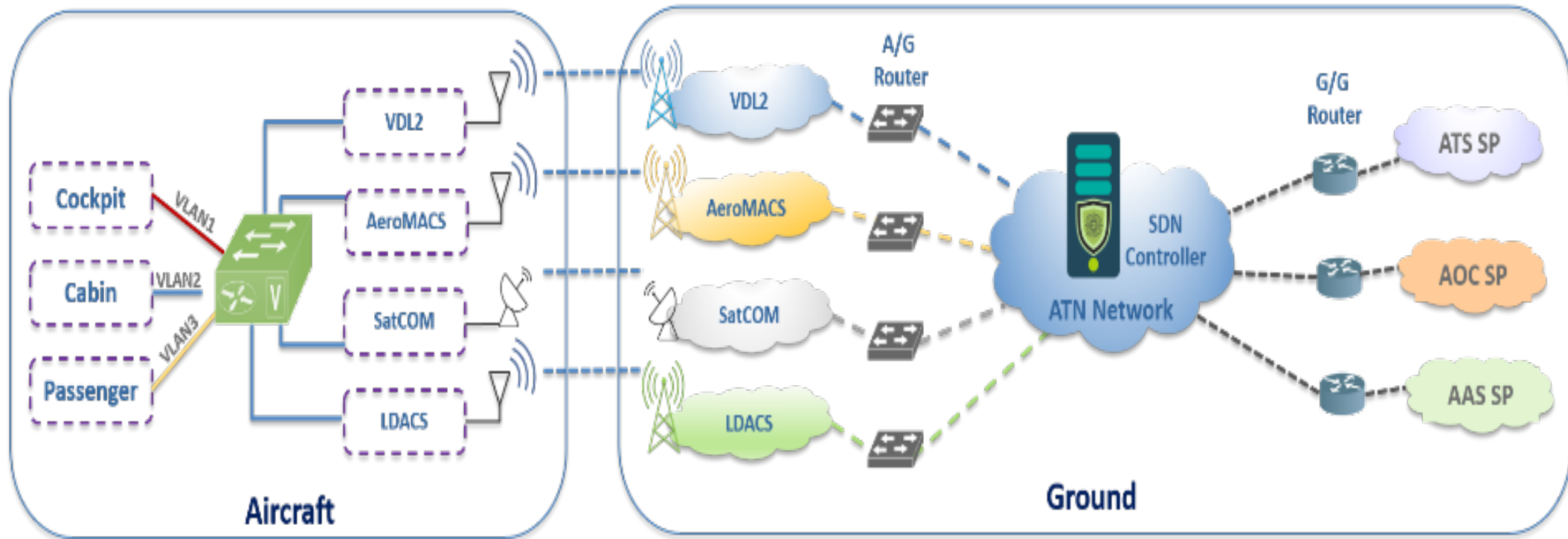


SINAPSE Project Objectives

Intelligent & secured Aeronautical Datalink Communications network based on Software Defined Networking (**SDN**) augmented with Artificial Intelligence (**AI**)

- Predict and prevent safety services outages (e.g. ATN CPDLC)
- Optimize networking (e.g., QoS prediction and path selection)
- Intelligent Cybersecurity functions

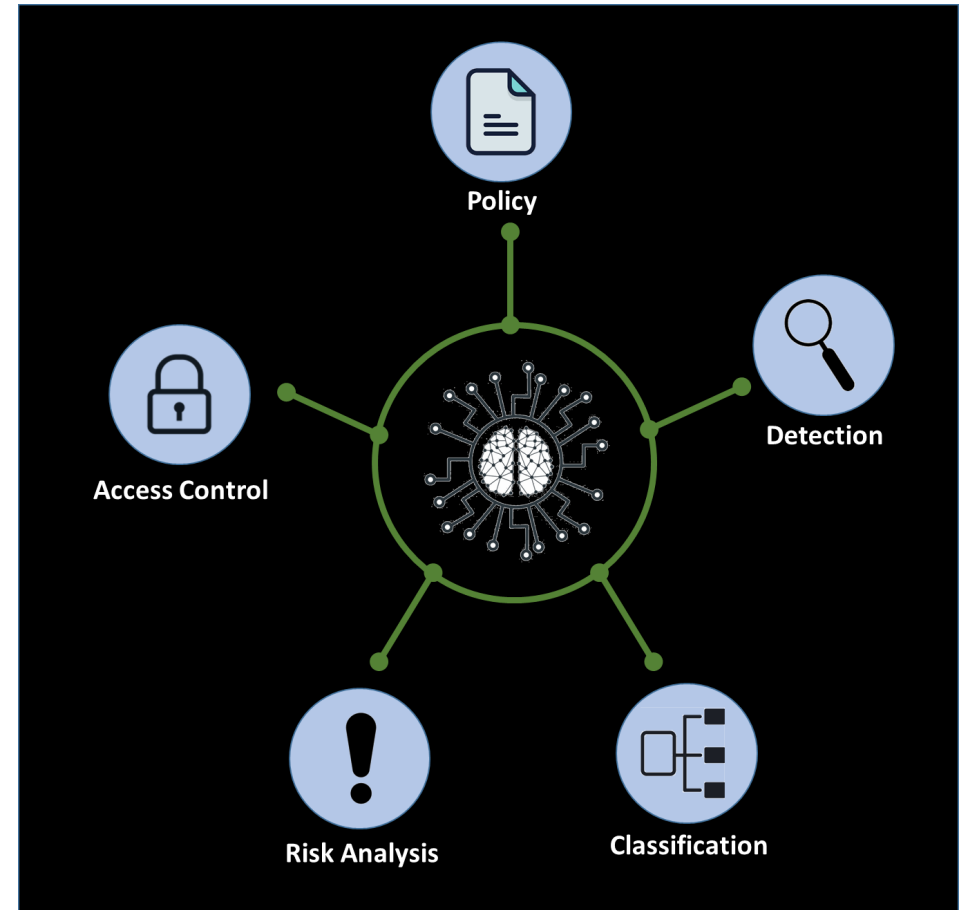
SINAPSE SDN-based Conceptual Digital Communication Infrastructure



SINAPSE Intelligent Security Platform

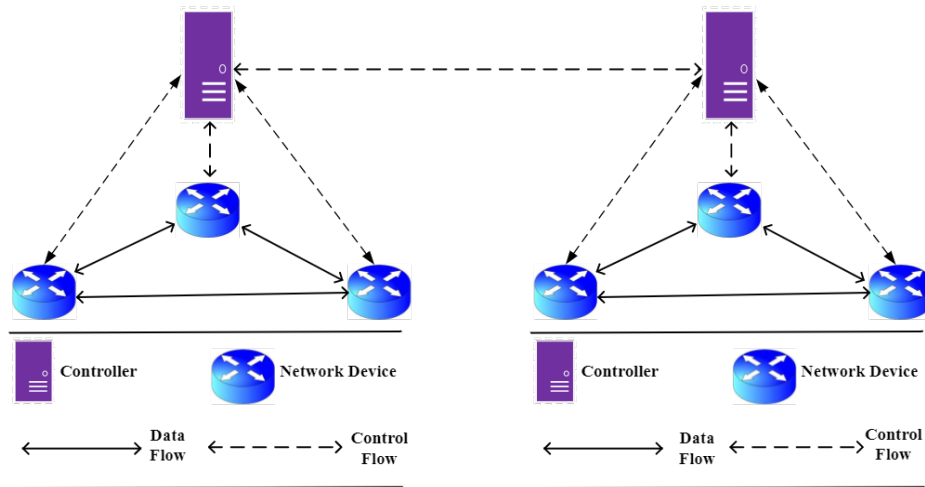
SINAPSE aims to develop a ML based network intrusion and detection system (NIDS) for binary intrusion classifications i.e. classification between normal and attack traffic.

- Highly accurate
- Data locality protection
- Data privacy
- Scalability

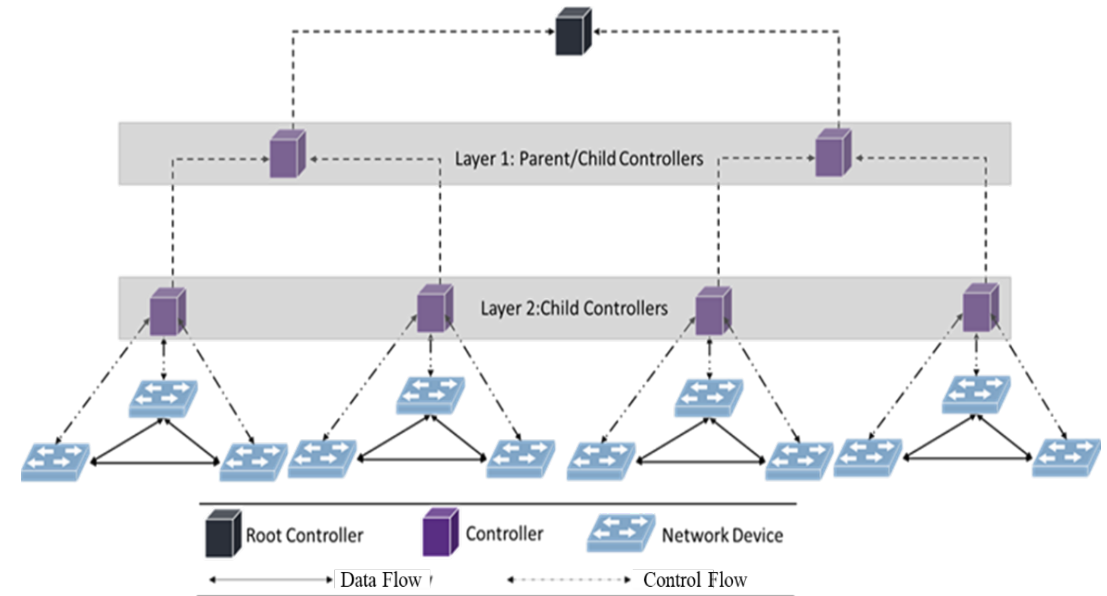


SDN Controller Architecture

- Flat Topology

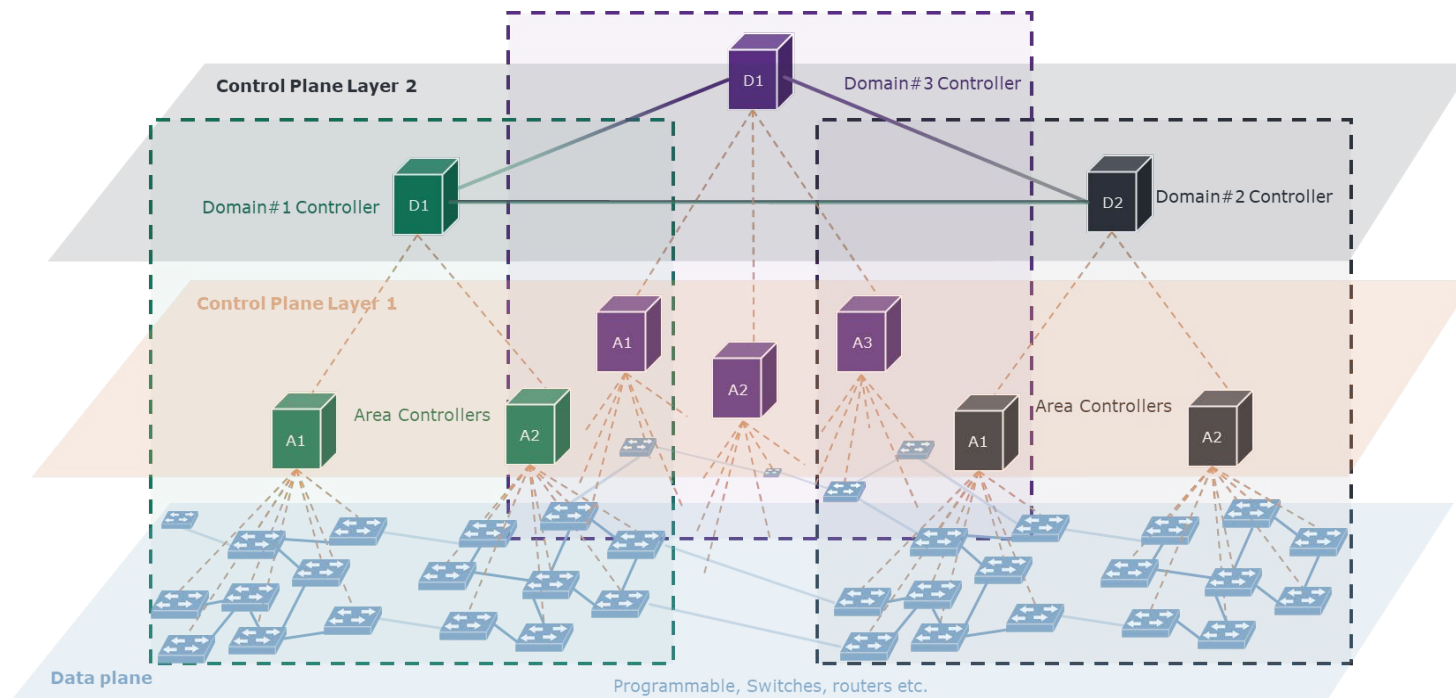


- Hierarchical Topology

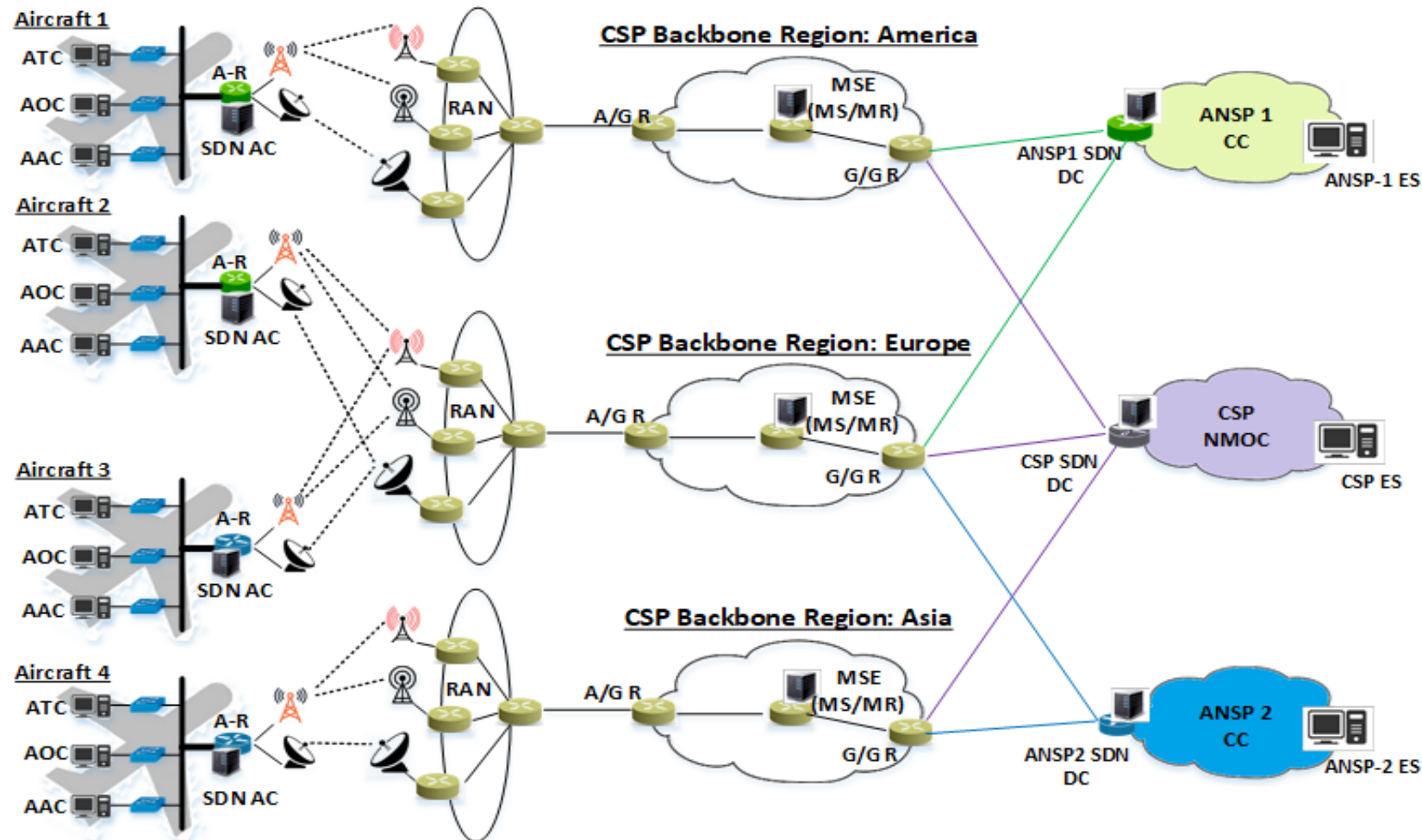


SINAPSE SDN Controller Architecture

- Hybrid Architecture



SINAPSE SDN Controller Architecture in FCI



Security risks



Data transfer within domains



Sharing of critically and commercially sensitive data among different service provider domains

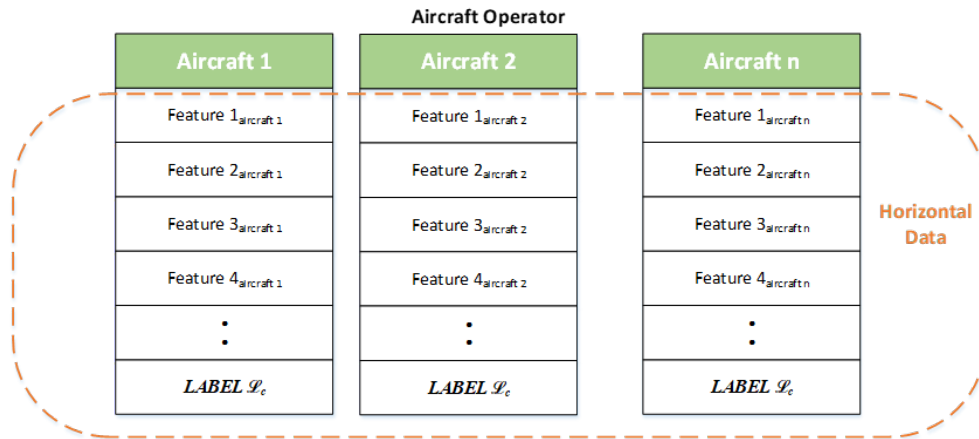


→ Federated Learning to improve data security and privacy

Federated Learning

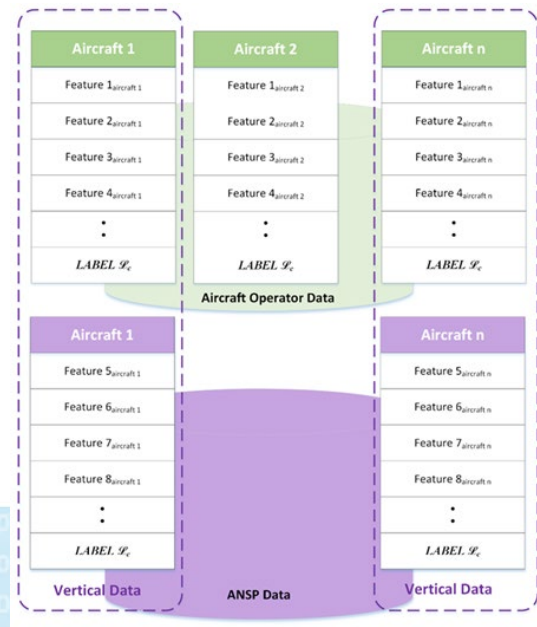
- A collaborative machine learning technique
- Training across multiple nodes holding local data samples but without exchanging them
- Preserve data privacy, data security, data access rights
- Horizontal and Vertical Federated Learning

Horizontal and Vertical FL



Horizontal federated learning

Datasets of any participating clients share the same feature space but different sample space

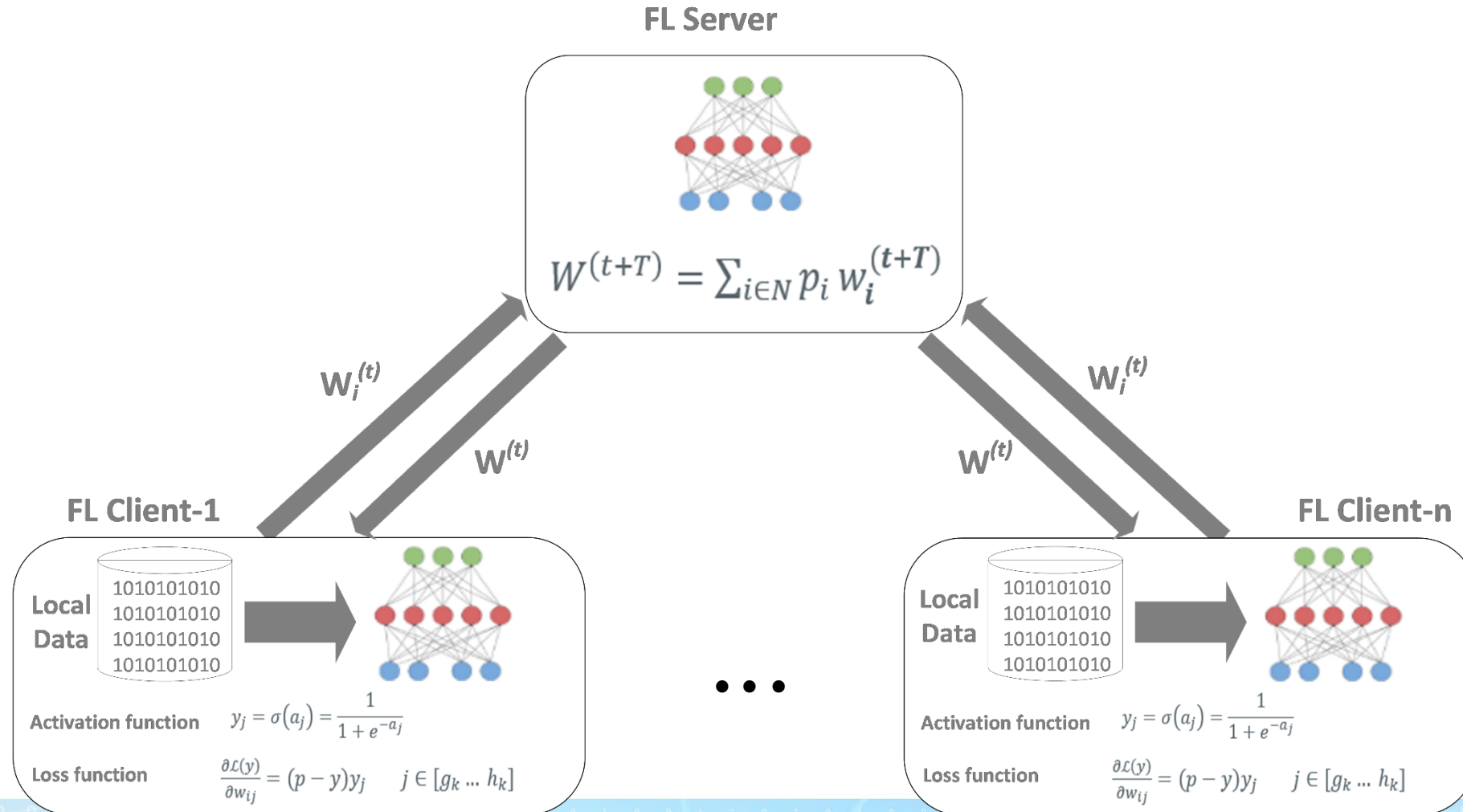


Vertical federated learning

Data sets of participating clients share the same sample space but differ in the feature space and the label space

Federated Learning Training Process

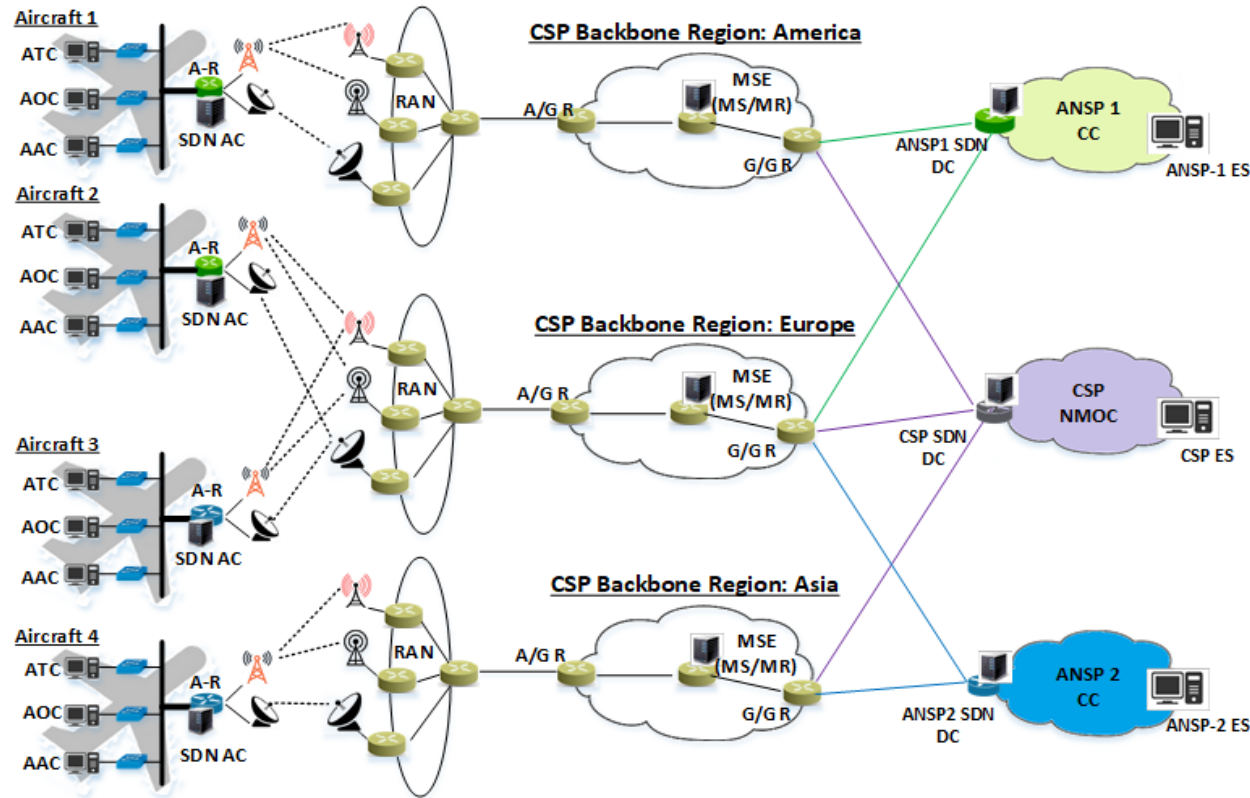
- $\mathcal{T}$ the set of time instances at which a global update occurs i.e.



Federated Learning Hyper-parameters

- the total number of hidden layers
- the number of neurons in hidden layer i
- the weights of the global model in training round t
- the local weights of client i in local training round t_e
- the learning rate

Federated Learning



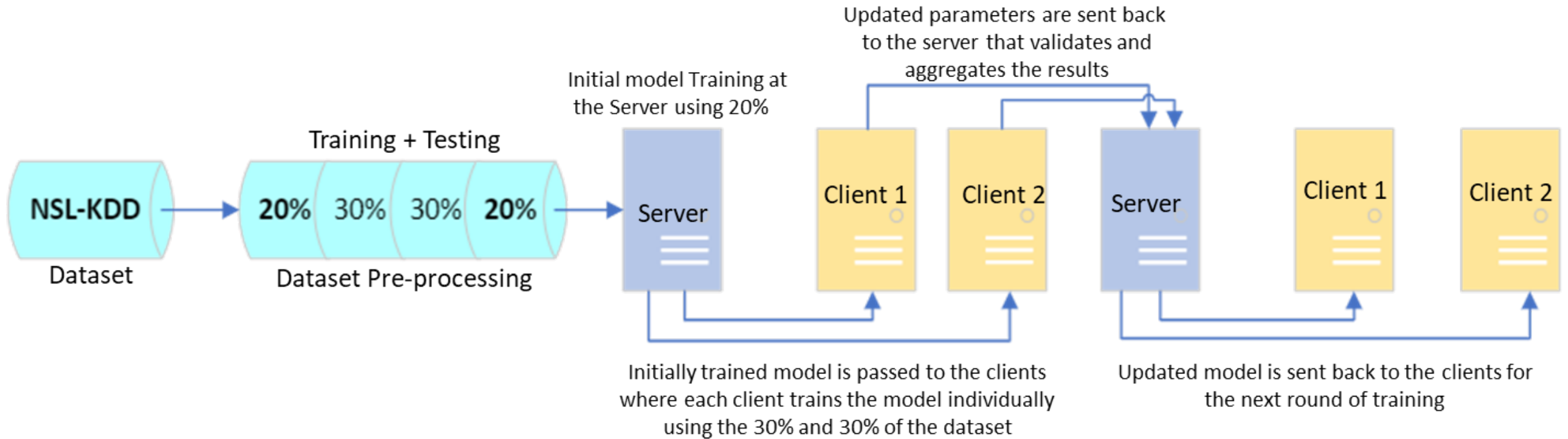
- **ANSP Domain**

- FL Server: ANSP CC/ANSP SDN DC
- FL Clients: A-R

- **CSP Domain**

- FL Server: CSP NMOC/CSP SDN DC
- FL Clients: MSE (MS/MR)

SINAPSE Federated Learning Implementation

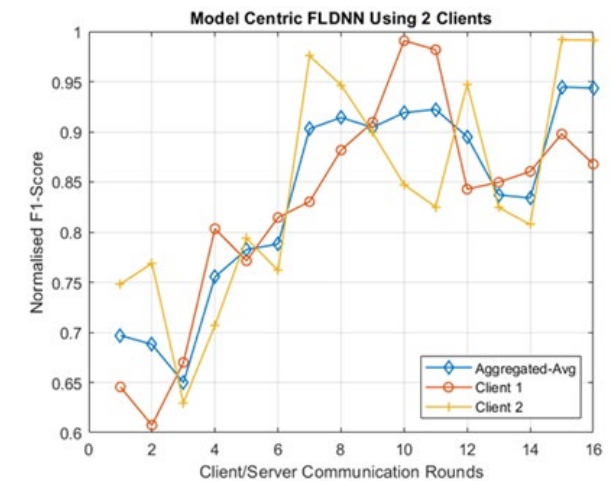
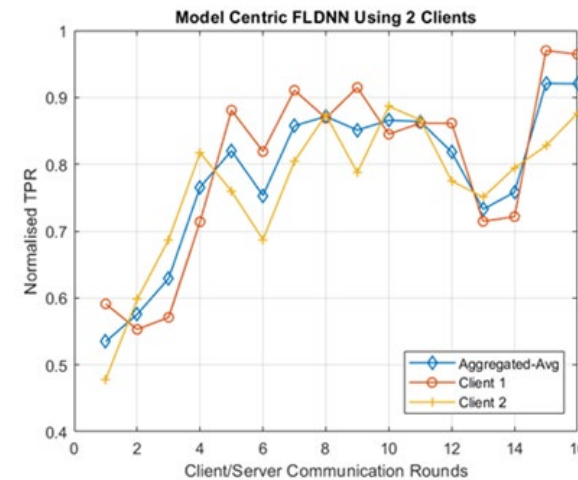
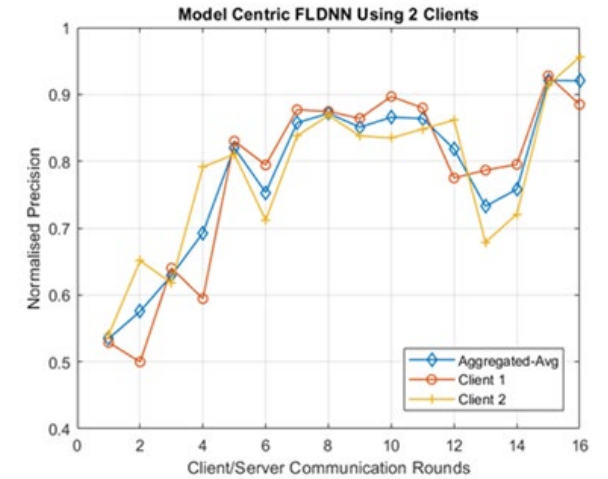
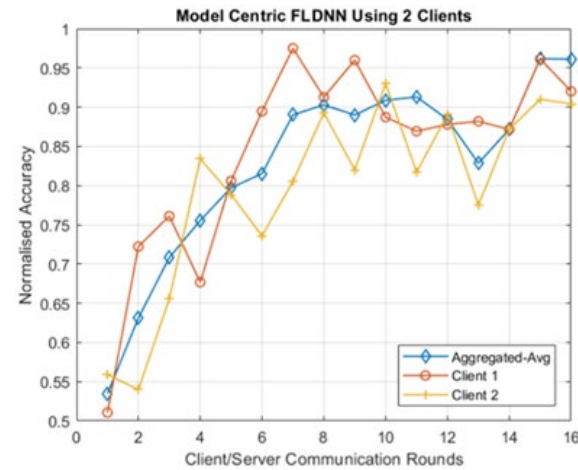


- **NSL-KDD dataset**

- DoS attack
- 29K sample
- 38 out of 41 features used
- Data segmented between FL Server, FL Clients and for validation purpose

Performance Metrics

- Results
 - Accuracy
 - Precision
 - Recall
 - F1- Score



Conclusion & Future Work

- **Conclusion**

- Two major solutions are presented : hybrid SDN and Federated learning.
- Hybrid SDN combining hierarchical and flat SDN controller topologies for the inter- and intra-domain communications, removing the risk of central point of failure.
- Federated Learning simulation performed using NSL-KDD dataset with one FL server and two FL clients
- Safety-critical aeronautical services can make use of FL to detect attack traffic

- **Challenges & Future Work**

- NSL-KDD dataset does not represent real air traffic data → publicly available air traffic data is required
- FL needs to be tested on non-iid (independent and identically distributed) data in real life situation → publicly available air traffic data
- Encryption to protect model parameters during global training rounds
- Optimum client selection/data selection is required
- Optimisation of communication exchanges between Server and Clients

A large, faint blue play button icon with concentric circles, positioned on the left side of the slide.

Thank you for your attention!

Any Question?



This project has received funding from the SESAR Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 892002



Co-funded by
the European Union

EUROPEAN PARTNERSHIP