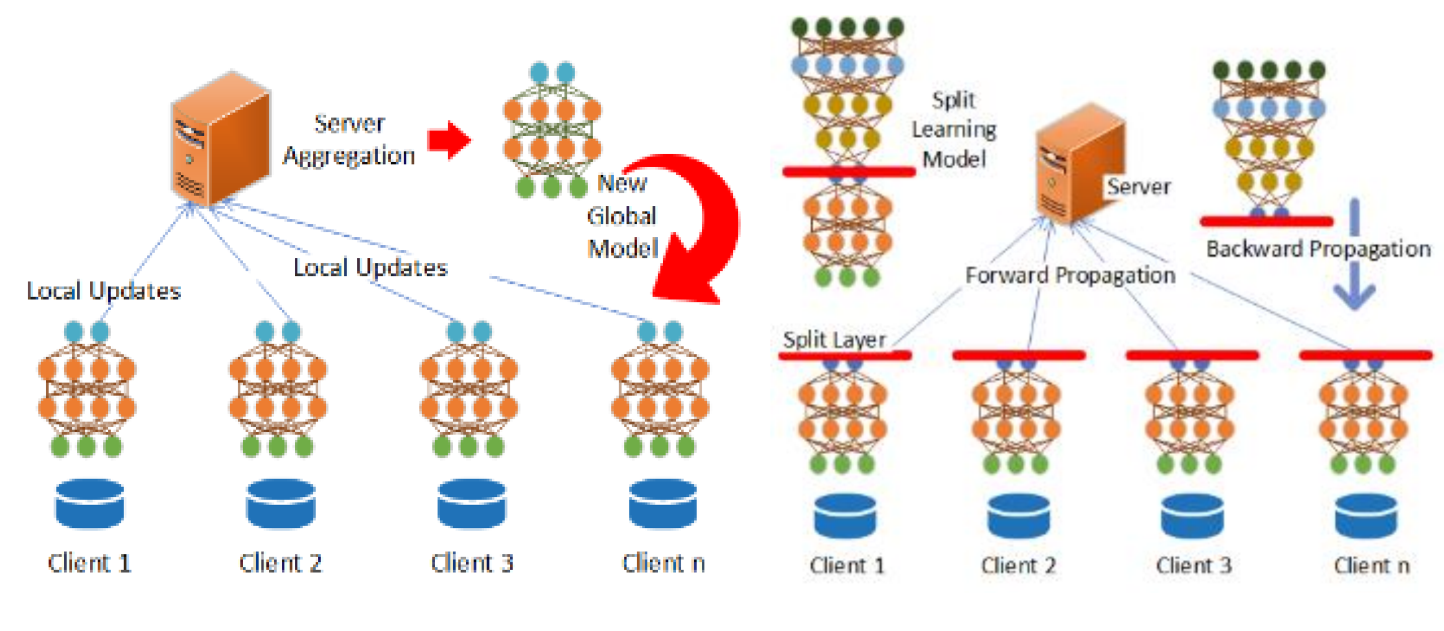
On Resource Consumption of Distributed Machine Learning in Network Security

Muzammal Hoque, **Ijaz Ahmad**
VTT Technical Research Center of Finland
muzammal.hoque@vtt.fi

- Machine Learning (ML) is expected to be at the core of 6G network security.
- The resource consumption of ML processes can be exhaustive, leading to compromises and security lapses.
- A comparative analysis of resource consumption for ML in network (6G) security is necessary.

Problem Statement

- ❖ Communication network transmission has limited resources like power, computation and bandwidth.
- ❖ Device specific resource constraints exist.
- ❖ Different security functions have different implementation methods and resource costs.
- ❖ Using ML for security functions consumes resources for both ML and security operations.
- ❖ Investigating resource consumption of ML techniques used for network security is necessary.
- ❖ This study examines resource consumption of Federated Learning (FL) vs. Split Learning (SL) for network DDoS detection in terms of:
  - CPU, Memory, Power, Delay and CO2 emission



(a) Federated Learning (b) Split Learning

Fig 1: A High-level Presentation of Two popular distributed learning.

Experimental Setup

- ❖ Experiment were conducted with 32 FL and SL clients:
  - 3 training setups: 10, 16 and 24 randomly picked clients contribute to training.
- ❖ Both SL and FL models use a similar neural network structure. The SL model is split into two parts:
  - Lower part of DNN model on the client device
  - Upper part the other on the server.
- ❖ The work utilized the DDoS evaluation dataset (CIC-DDoS2019) [1].

[1] I. Sharafaldin, A. H. Lashkari, S. Hakak and A. A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 2019, pp. 1-8, doi: 10.1109/CCST.2019.8888419.

Resource Consumption Analysis

Models	Avg. CPU (%)	Peak Memory (MB)	Power (Wh)	Time (Min)	CO2 (g)
Fed 10	8.10	1974.59	5.00	**19.29**	**0.71**
Split 10	8.52	5997.20	1.59	**5.73**	**0.23**
Fed 16	7.78	2000.15	7.56	**29.05**	**1.07**
Split 16	5.22	8286.37	2.19	**7.67**	**0.31**
Fed 24	8.38	1960.54	11.19	**43.31**	**1.59**
Split 24	8.81	11335.62	3.22	**11.14**	**0.46**

Table 1: Resource Consumption Comparison of different client batch size for training of FL and SL

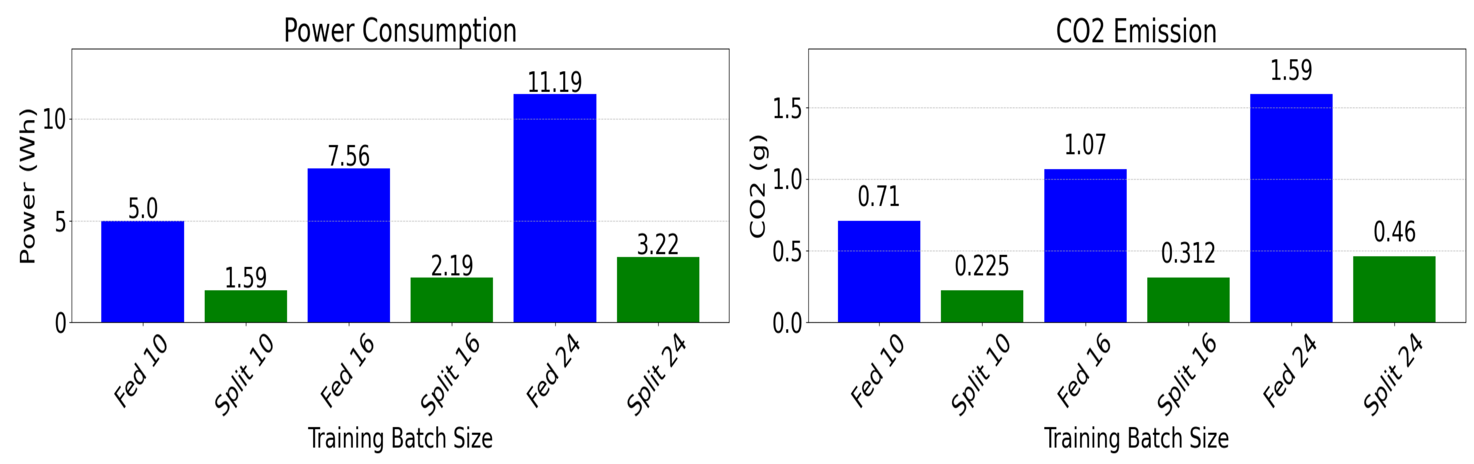


Fig 2: Power Consumption and CO2 emission of different client batch size for training FL and SL

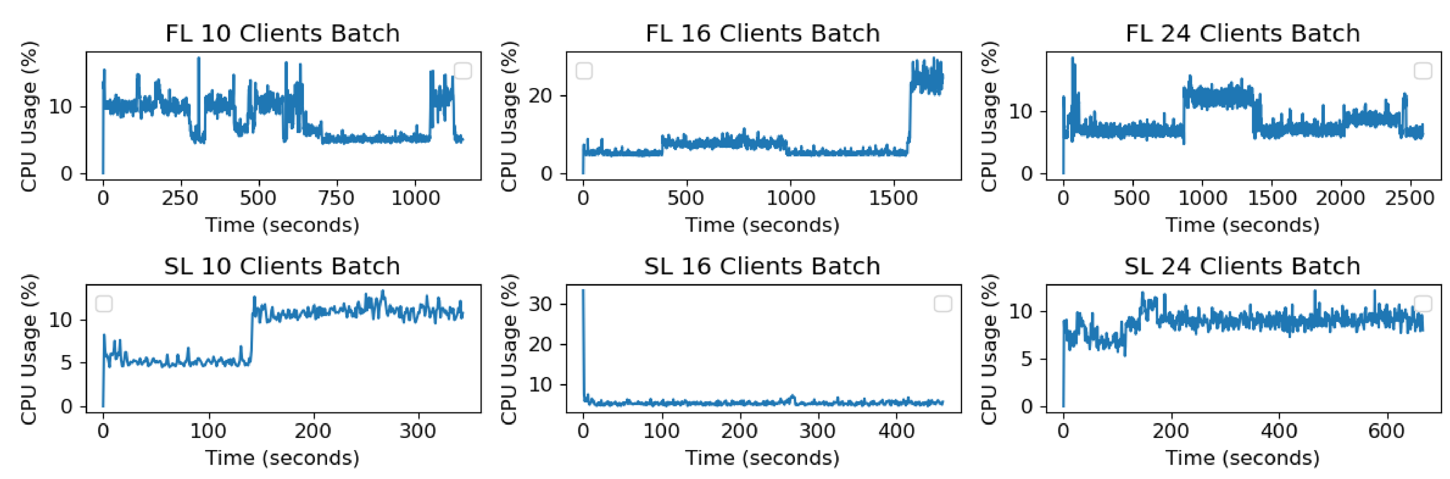


Fig 3: CPU usage of different client batch size for training of FL and SL

Takeaways

- **Both FL and SL perform well with 99.6% accuracy for all DDoS detection scenarios.**
- **Resource consumption:**
  - **CPU usage:** SL had higher CPU usage, while FL had higher peaks and variability.
  - **Memory usage:** FL used 3-5.8x less memory than SL.
  - **Power consumption:** SL used 3.1-3.46x less power than FL.
  - **Delay:** SL was 3.4-3.9x faster than FL.
  - **CO2 emission:** SL emitted 3.2-3.5 times less CO2.
- **There should be adaptive security and ML selection procedures to fit ML-based security according to available resources.**

www.vttresearch.com

Contact: Muzammal Hoque, Research Assistant,
Tel. +358 505995038, muzammal.hoque@vtt.fi

beyond the obvious

Acknowledgements: Marchal Samuel is thanked for technical assistance, and SUNSET-6G and VTT for funding the work.