Towards Intrusion Detection Systems dedicated to Agriculture based on Federated Learning

Usman Rabiu Isah, Laurent Bobelin, Pascal Berthome

▶ **To cite this version:**

Usman Rabiu Isah, Laurent Bobelin, Pascal Berthome. Towards Intrusion Detection Systems dedicated to Agriculture based on Federated Learning. Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI2023), Mar 2023, Neuvy sur Barangeon, France. ⟨hal-04760766⟩

HAL Id: hal-04760766

https://hal.science/hal-04760766v1

Submitted on 31 Oct 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

HAL Authorization

Towards Intrusion Detection Systems Dedicated to Agriculture Based on Federated Learning

INSA Centre Val de Loire, Laboratoire d'Informatique Fondamentale d'Orléans, France
Usman Rabiu ISAH (Doctorant)
Laurent BOBELIN, and Pascal BERTHOME (Supervisors)

Context and Motivation

The rapid development of IoT devices in agriculture is revolutionizing traditional farming methods by providing fast and reliable information to feed decision analysis systems, but as the number of connected devices keeps increasing, IoT devices become a target for cybercriminals, which is why this research aims to develop a Deep Learning(DL)/Federated Learning (FL)-based Intrusion Detection Sytems (IDS) specific to IoT networks dedicated to agriculture.

Objectives

- Study the current state of the art in the use of FL in IDS.
- Set up simulation/emulation environment and develop algorithms to detect attacks on IoT devices.
- Deploy the solutions on real-life platforms to evaluate the performance in real-life conditions.

Smart Agriculture

Sensors are the most common IoT devices used in agriculture today. They can monitor various parameters such as rain, moisture, humidity, temperature, and wind to help farmers forecast necessary actions to maintain high production levels.

- IoT everywhere in fields: sensors, actuators
- Edge-computing used for AI-based precision agriculture
- Complex systems coupling IoT, UAV (drones), AIV (autonomous tractors), edge servers
- Growing threats on actors/production
- Low security

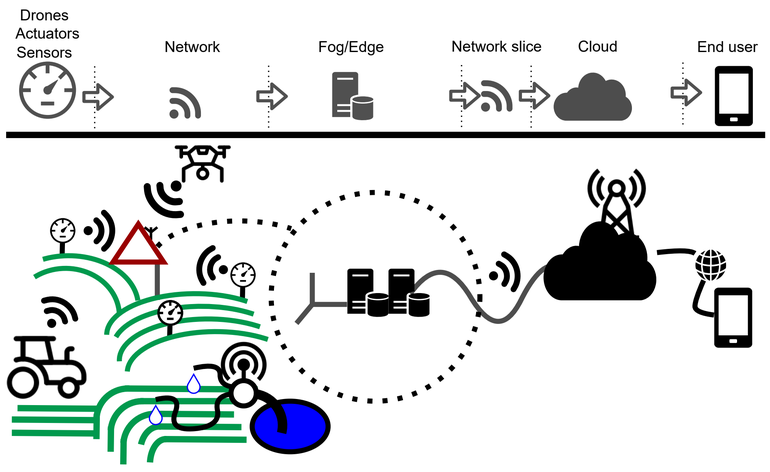

Figure 1: A Fully equipped agricultural exploration

Federated Learning

Federated Learning provides a framework for deep learning models to be trained in a collaborative manner without sharing data with a central data repository. FL provides a lot of benefits, such as improved privacy, and reduce communication costs. Some research works studied have proposed an FL approach to IDS. [1]

- AI distributed learning
- Local learners share their models
- Server aggregates models and send the result back to learners
- Local entities decide which model is the best.

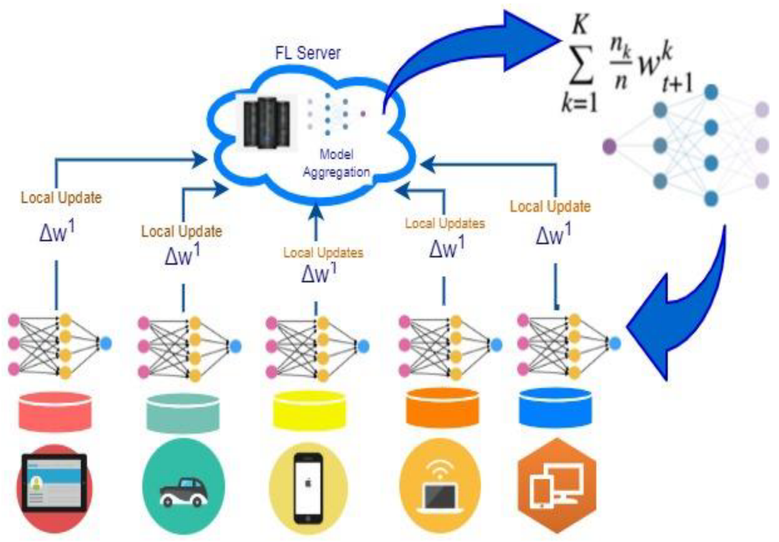

Figure 3: Federated Learning Framework

Network-based IDS

For decades, research is been conducted to improve the efficiency of IDS. The advances in artificial intelligence (AI) and machine learning (ML) have opened a new niche for research by incorporating ML into an IDS, for example. [3, 2, 4]

- IDS filter traffic
- Signature-based, Anomaly-based or AI-based
- FL + IDS in AI-based setup
- from preliminary experiments, federated learning shows promising advantage in learning from data not centrally located.
- Many open challenges: resources, efficient management of IoT, aggregation, personalization.
  This research will work with a software-defined (SDN) network architecture as shown in fig 2 to develop an IDS classifier for IoT in Agriculture.

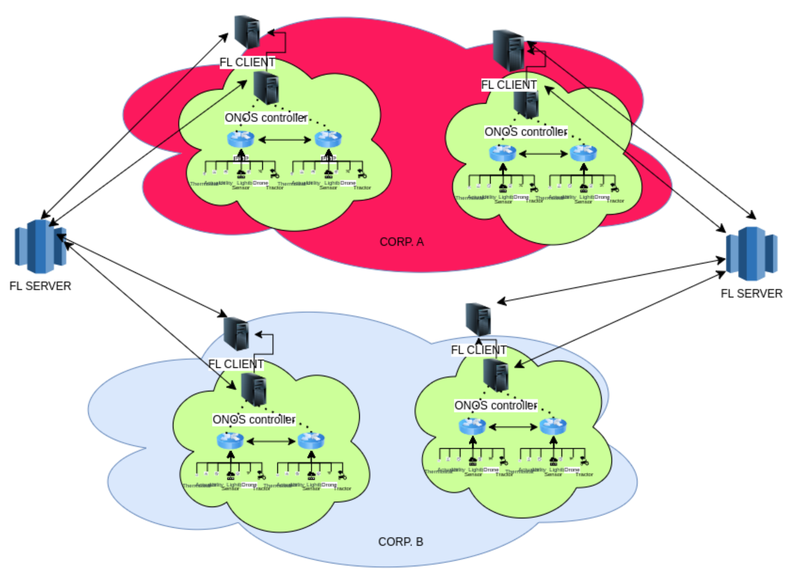

Figure 2: A schematic SDN-based architecture of IDS in network edge

Smart Agriculture, Intrusion Detection Systems, and Federated Learning (OUR ROAD-MAP)

Agricultural enviroments have so many challenges with regard to connected devices which may not be limited to:

- Low computing/energy devices
- Remote location, possibly disconnected
- Specific protocols

this research will consider all these and bring together IDS and FL to secure such devices.

Conclusion

- This research aims to develop solutions against threats to IoT devices in agricultural environments that can be deployed in real-life.
- We hope to show that it is possible to secure IoT devices in agriculture.

Acknowledgements

Ph.D. Work funded by PTDF Nigeria.

[1] Aouedi, Ons and Piamrat, Kandaraj and Muller, Guillaume and Singh, Kamal *Intrusion detection for Softwarized Networks with Semi-supervised Federated Learning*.ICC 2022 - IEEE International Conference on Communications, June 2022 Seoul, South Korea

[2] Swarna Sugi, S. Shinly and Ratna, S. Raja.*Investigation of Machine Learning Techniques in Intrusion Detection System for IoT Network* 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS).

[3] Jien, Ng Yee and Tahir, Mohammad and Dabbagh, Mohammad and Meng, Yap Kian and Farooq, Ali Smith. *erformance Evaluation of Machine Learning Algorithms for Intrusion Detection in IoT Applications.* 2022 IEEE (IICAIET) doi=10.1109/IICAIET55139.2022.9936863

[4] Dholu, Manishkumar and Ghodinde, K.A. Internet of Things (IoT) for Precision Agriculture Application 2018 2nd (ICOEI) doi=10.1109/ICOEI.2018.8553720