Federated Learning for Intrusion Detection and Mitigation

Hands-on Machine Learning for Security, CIDRE

Léo LAVAUR, IMT Atlantique, IRISA, Cyber CNI

2021-09-24

Advisors:

- Marc-Oliver Pahl, IMT Atlantique, IRISA, Cyber CNI
- Yann Busnel, IMT Atlantique, IRISA
- Fabien Autrel, IMT Atlantique, IRISA, Cyber CNI

chairecyber-cni.org/

Chaire Cyber CNI
5 industrial partners
8+ associated researchers
12 PhD students (2020/5)

References

[1] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions", Computers & Security, 2019.

[2] S. Rathore, B. Wook Kwon, and J. H. Park, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network", Journal of Network and Computer Applications, 2019.

[3] M. Aledhari, R. Razzak, R. M. Parizi, and F. Saeed, "Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications", IEEE Access, 2020.

[4] M.-O. Pahl, A. Kabil, E. Bourget, M. Gay, and P.-E. Brun, "A Mixed-Interaction Critical Infrastructure Honeypot," 2020.

[5] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A.-R. Sadeghi, "DÏoT: A Federated Self-learning Anomaly Detection System for IoT," in 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), 2019.

References

[6] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, “DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber-Physical Systems,” IEEE Transactions on Industrial Informatics, 2020.

[7] W. Schneble and G. Thamilarasu, “Attack detection using federated learning in medical cyber-physical systems,” Aug. 2019.

[8] Y. Chen, J. Zhang, and C. K. Yeo, “Network Anomaly Detection Using Federated Deep Autoencoding Gaussian Mixture Model,” in Machine Learning for Networking, 2020.

[9] M.-O. Pahl and F. X. Aubet, “All Eyes on You: Distributed Multi-Dimensional IoT Microservice Anomaly Detection,” 14th International Conference on Network and Service Management, CNSM 2018 and Workshops, 2018.

[10] W. Zhang, T. Zhou, Q. Lu, X. Wang, C. Zhu, H. Sun, Z. Wang, S. K. Lo, and F.-Y. Wang, “Dynamic Fusion based Federated Learning for COVID-19 Detection,” arXiv, 2020.

Contents

1. Context

Introduction to federated learning, and how can it be applied to

Thesis objective

Caveats of collaborative security*

*From ~200 reviewed papers, including 15 surveys

(a) **Lack of collective knowledge**
There is a lack of collective knowledge in cybersecurity, and more particularly in the OT. [1]

(b) **Lack of incentives**
Trust and privacy are major hurdle for stakeholders to share data. [1]

(c) **Architectural isolation**
The siloed architecture of detection systems is an obstacle to their effectiveness. [3]

(d) **Insuffisant resiliency**
Centralized systems represent a Single Point of Failure and can induce a communication overhead. [2]

R.Q: *How to federate knowledge and defense between non-trusting parties?*

- What to collect?
- What to share?
- How to share it?

Limitation of IDSs

- Signature–based IDSs are inefficients against APTs and unknown attacks.

Limitation of IDSs

- Signature–based IDSs are inefficients against APTs and unknown attacks.
- ML–based IDSs need a lot of data to be accurate.
- ML–based IDSs need heterogeneous data to avid bias.

Limitation of IDSs

- Signature–based IDSs are inefficients against APTs and unknown attacks.
- ML–based IDSs need a lot of data to be accurate.
- ML–based IDSs need heterogeneous data to avid bias.

Collaborative IDS

Limitations of collaborative IDSs

- Centralized systems may induce a single point of failure (SPoF).

Limitations of collaborative IDSs

- Centralized systems may induce a single point of failure (SPoF).
- Centralized CIDSs increase latency and bandwidth when compared to local detection.

Limitations of collaborative IDSs

- Centralized systems may induce a single point of failure (SPoF).
- Centralized CIDSs increase latency and bandwidth when compared to local detection.
- Centralized CIDSs can expose sensitive information and weaken security.

Limitations of collaborative IDSs

- Centralized systems may induce a single point of failure (SPoF).
- Centralized CIDSs increase latency and bandwidth when compared to local detection.
- Centralized CIDSs can expose sensitive information and weaken security.

Federated Learning for IDSs

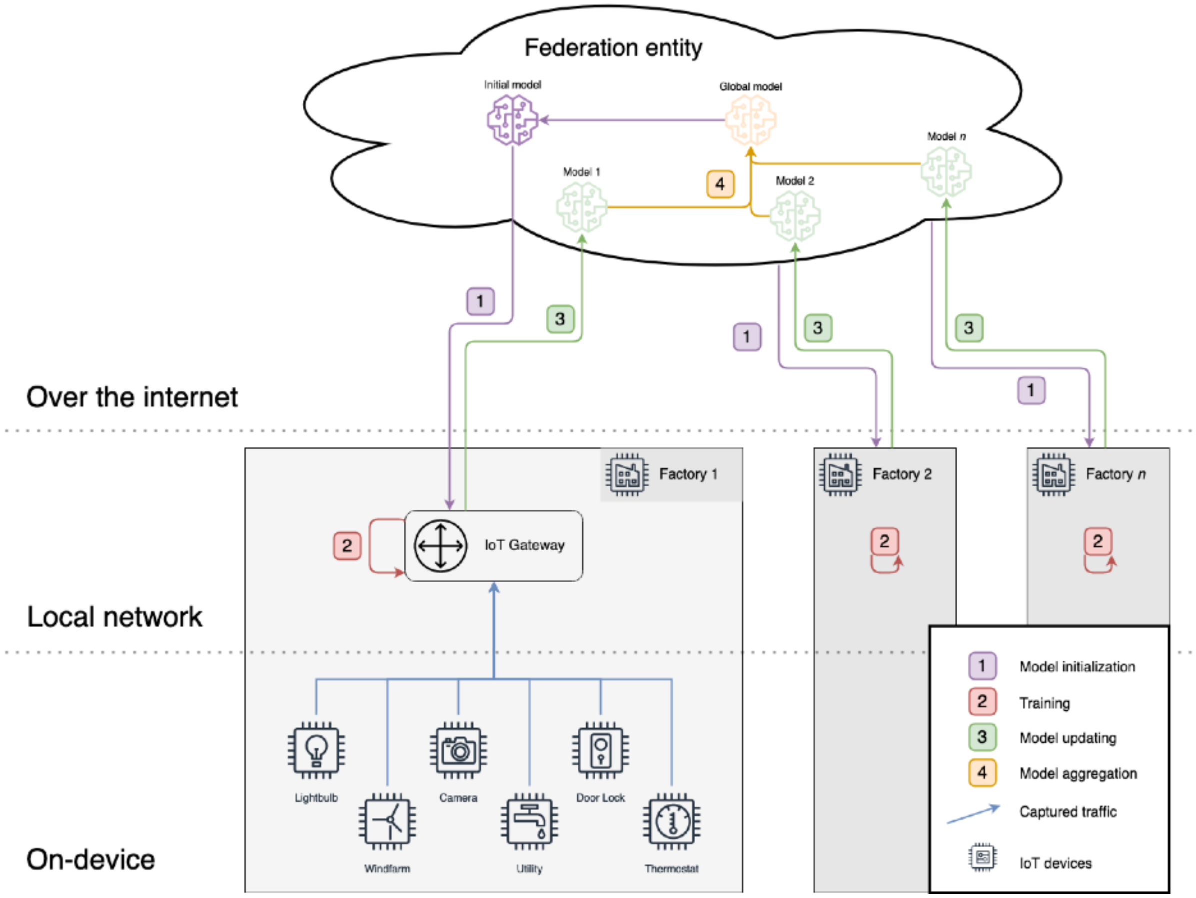


Fig. 1. FL–based detection in smart factory

- Horizontal FL: aggregation of homogeneous models
  - Local collection and analysis of data
  - Better privacy, reduced bandwidth
- Note: collection of additional data could be performed using a *Honeypot Factory*

2. State of the Art

Existing works applying federated learning to intrusion detection

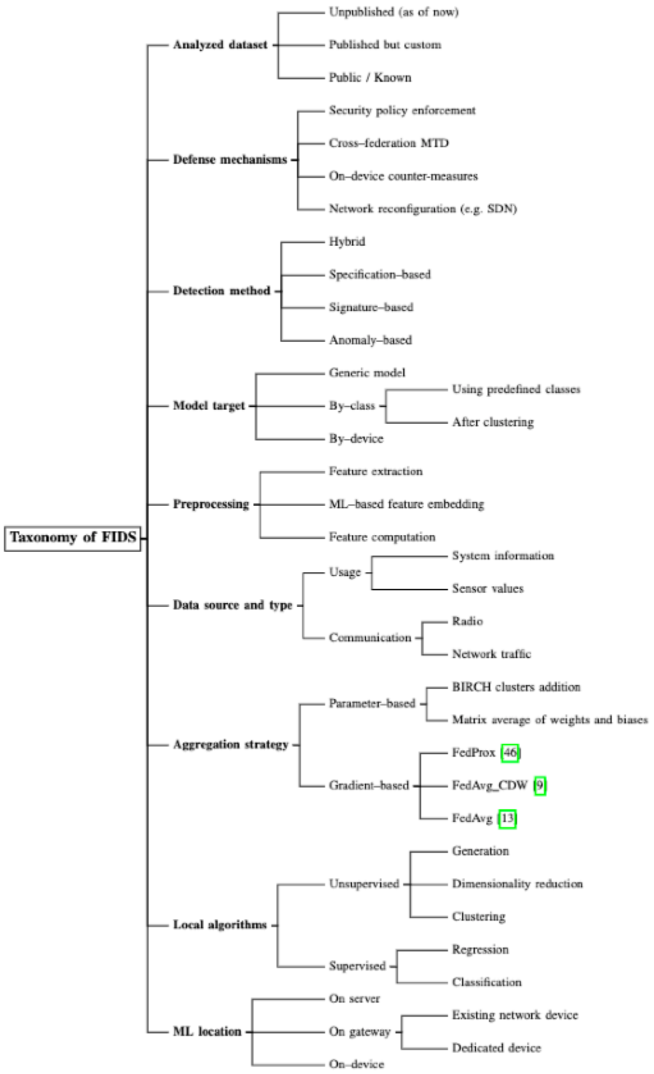


Fig. 2. Taxonomy of FIDS (provisional)

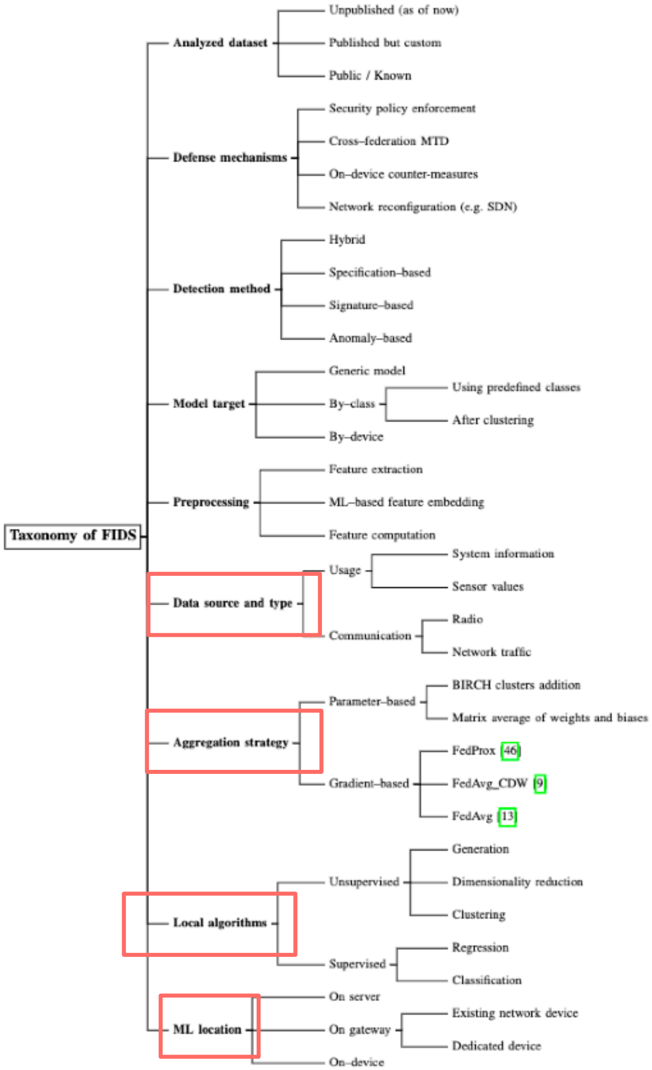
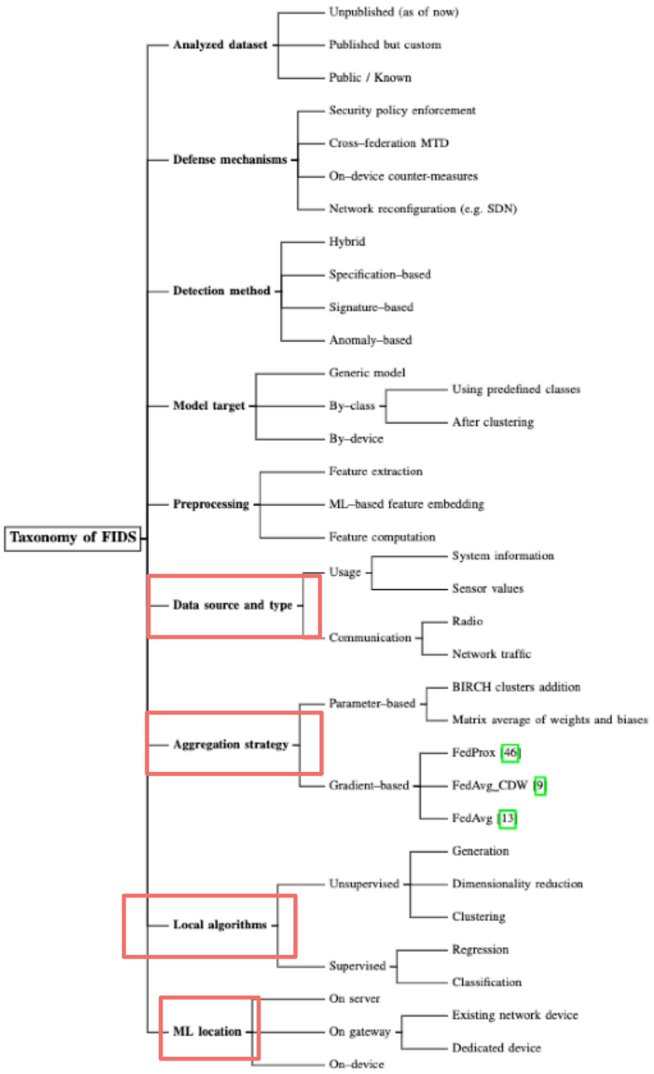


Fig. 2. Taxonomy of FIDS (provisional)



- Local algorithm is selected in accordance to the type of data
- The aggregation depends on the local strategy
- Architecture reflects the use case and its constraints

Fig. 2. Taxonomy of FIDS (provisional)

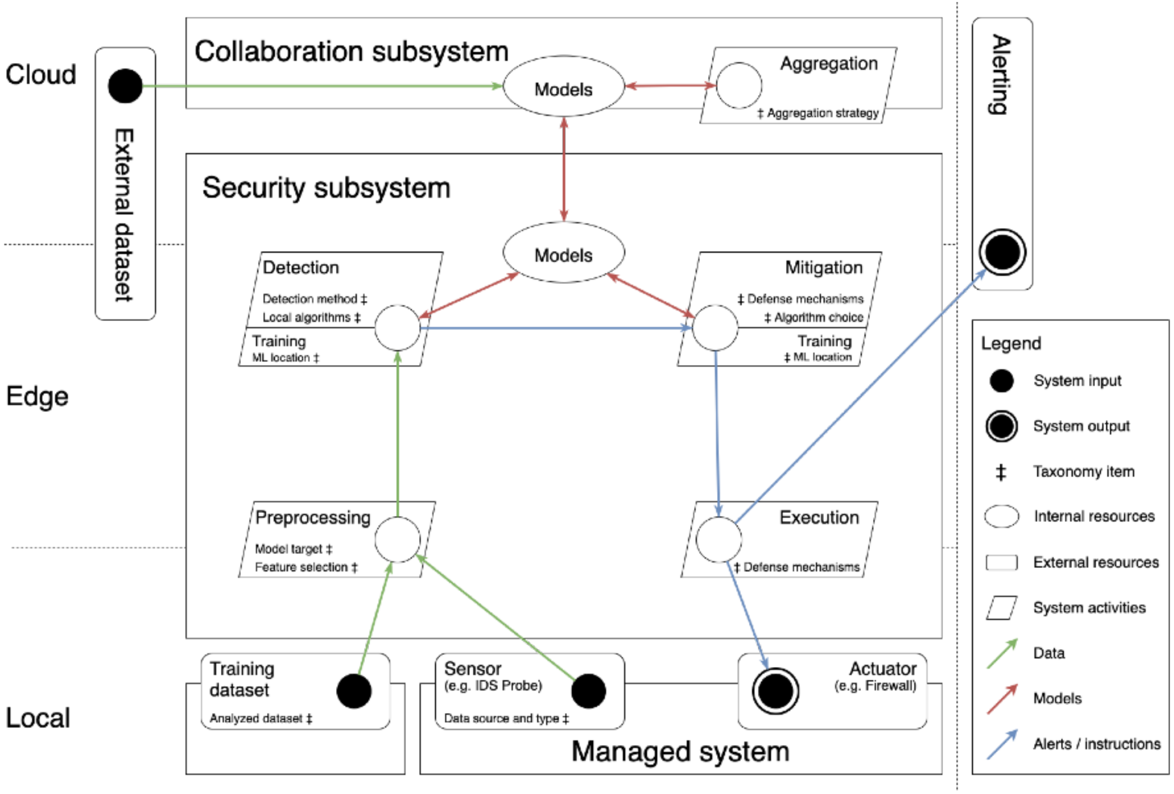


Fig. 3. Reference architecture

- Generic architecture for federated or centralized learning
- Relation with autonomous systems (MAPE-K)

State-of-the-Art

	ML location	Data type	Local algorithm	Aggregation strategy
Pahl and Aubet 2018 [9]	On-device	Network (middleware)	BIRCH / K-Means	Cluster addition
Nguyen et al. 2019 [5]	On-gateway	Network	NN (RNN)	Gradient-based
Rathore et al. 2019 [2]	On-gateway (fog)	Network	NN	Matrix parameter avg
Schneble et al. 2019 [7]	On-gateway	Sensors	NN (MLP)	Matrix parameter avg
Li et al. 2020 [6]	On-gateway	Network	NN (RNN)	Matrix parameter avg
Chen et al. 2020 [8]	On-gateway	Network	NN	Matrix parameter avg
Zhang et al. 2020 [10]	On-gateway	Sensors	NN	Gradient-based

Hypotheses

I. *Periodicity-mining and other time–based techniques are only effective on constrained devices with predictable traffic.*

II. *Performance decreases the closer the model is from the monitored device.*

   a. *Classification can be used to reduce the number of generated models.*

   b. *Ponderation can cope with heterogeneous data.*

III. *The model cannot target features that are specific to the local network.*

3. Future work

System comparison and use cases

Reproducibility

Implement

Reimplement the related works with one codebase, and one ML network.

Define dataset

Run the experiments on the same datasets to get meaningful results.

Compare results

Compare the announced results with the obtained ones, and draw conclusions.

TensorFlow + Keras

Real-world use cases

IT networks

Detecting threats in typical IT networks with high traffic volume.

AIRBUS

Smart factory

Detecting attacks in constrained and heterogeneous context.

eDF

Smart building

Detecting anomalies in sensor–focused environments.

eDF

BNP PARIBAS
La banque d'un monde qui change

Conclusion

Federated architectures for knowledge & defense between non-trusting parties

- **Ongoing survey:**
  - Compare the related works, extract significative features and future research leads
- **Next steps:**
  - reproduce and compare the state-of-the-art
  - build the testbeds to host the experiments

leo.lavaur@imt-atlantique.fr