Using AI to face covert attacks in IoT and softwarized scenarios: challenges and opportunities

Angelica Liguori[1,2], Simone Mungari[1,2], Marco Zuppelli[4], Carmela Comito[1], Enrico Cambiaso[3], Matteo Repetto[4], Massimo Guarascio[1], Luca Caviglione[4], and Giuseppe Manco[1]

[1] Institute for High Performance Computing and Networking, Italy
[2] University of Calabria, Italy
[3] Institute of Electronics, Computer, and Telecommunication Engineering, Italy
[4] Institute for Applied Mathematics and Information Technologies, Italy

Ital-IA
ITALIA INTELLIGENZA ARTIFICIALE
Terzo Convegno Nazionale
Pisa 29-31 Maggio 2023
cini National Lab AIIS

Outline

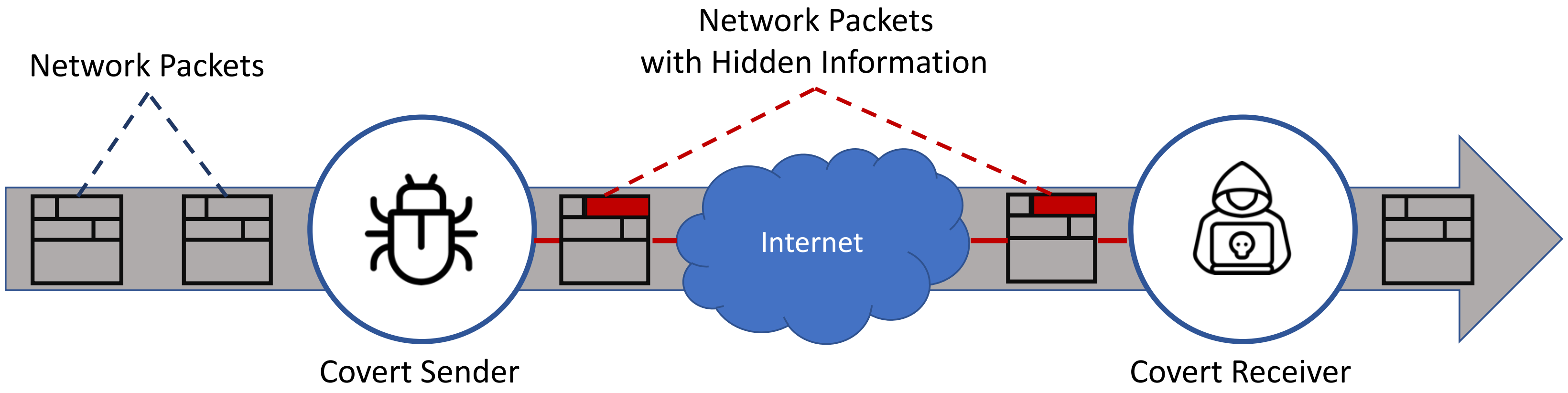
- Introduction
- Challenge 1
    - Covert Malware in IoT Scenarios
- Challenge 2
    - Container Security
- Challenge 3
    - Graph Generation
- Conclusion

Introduction

- **Problem**. An exponential increase of cyber attacks whose aim is to breach networked and softwarized environments
- **Goal**. Defining Artificial Intelligence (AI)-based solutions able to detect anomalous behaviors in such ecosystems
  - e.g., a malware endowed with information-hiding capabilities, or evolving cyber threats

Covert Malware in IoT Scenarios

- Network covert channels, i.e., hidden communication paths nested within legitimate traffic flows



Network Packets

Network Packets
with Hidden Information

Internet

Covert Sender

Covert Receiver

➡ Legitimate Network Traffic

▬ Covert Channel

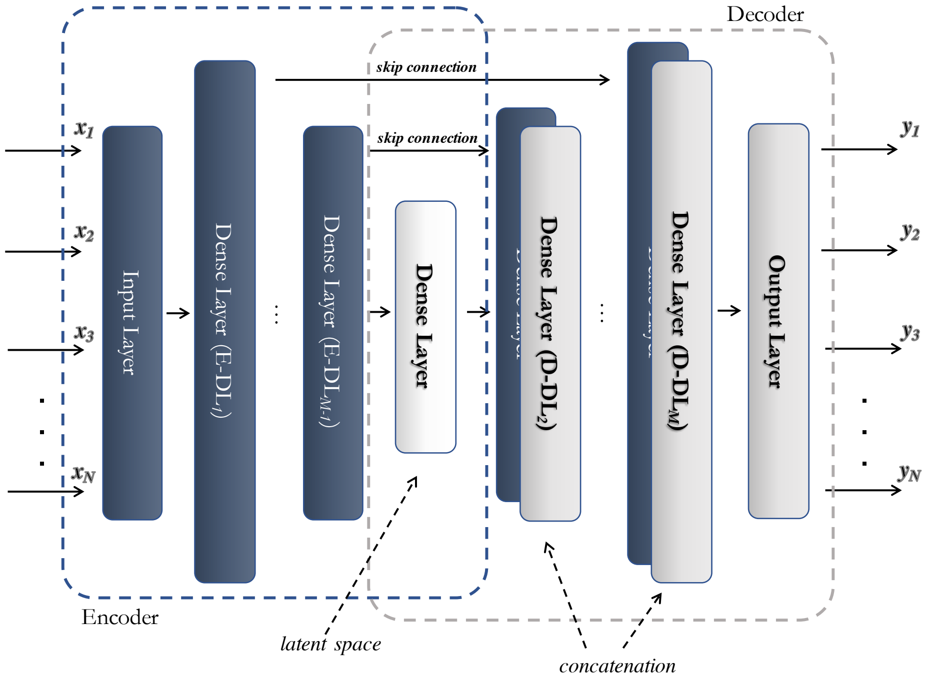
Covert Malware in IoT Scenarios

- **Goal**. Identifying the presence of network covert channels targeting the IPv4 protocol used in an IoT ecosystem

- **Idea**. Developing a covert channel detection method based on unsupervised deep learning models

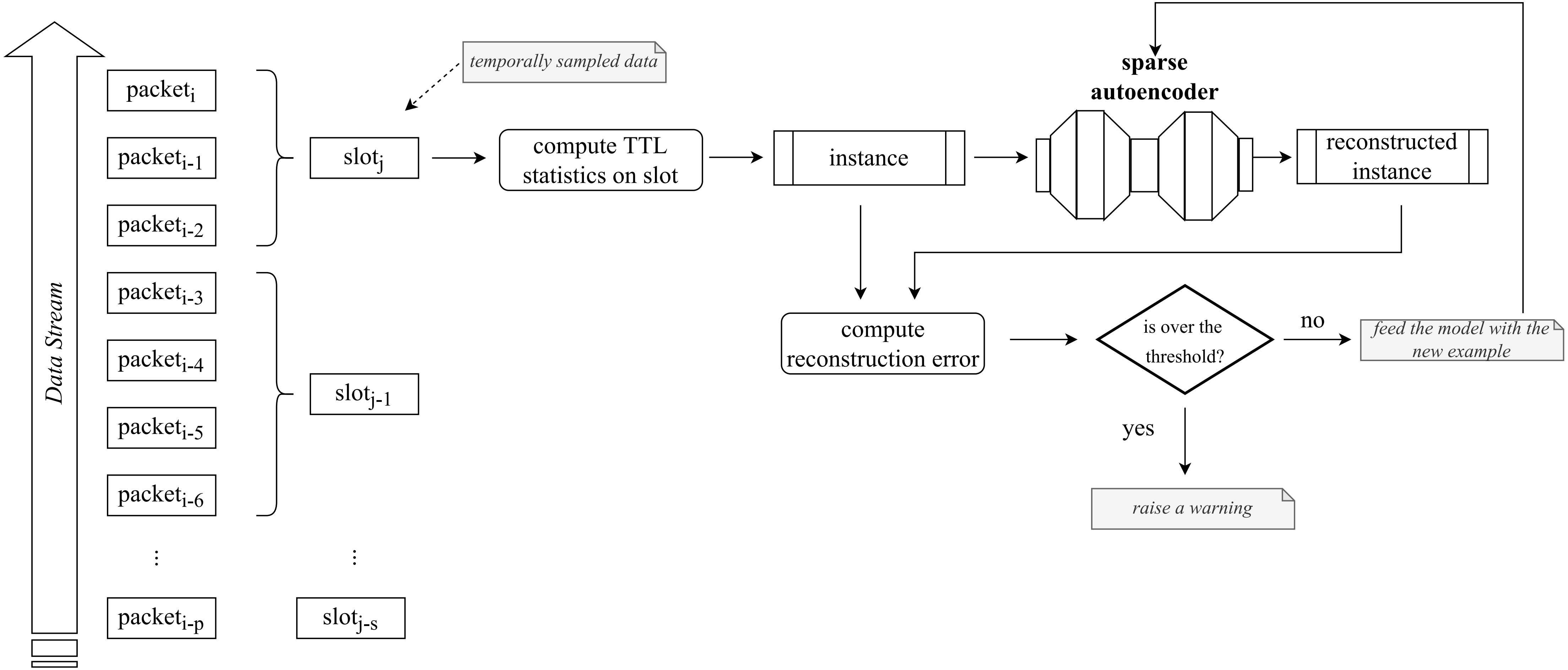
Covert Malware Detection via Autoencoders

- In [1] we developed an autoencoder-based approach to detect covert channels
  - Only legitimate traffic information has been given to the model to perform the training
- Results considering a channel within the TTL of IPv4 showcased the effectiveness of the proposed approach, i.e., we obtained ~91% and ~94% for the accuracy and the precision, respectively



[1] M. Guarascio, M. Zuppelli, N. Cassavia, G. Manco, L. Caviglione, Detection of Network Covert Channels in IoT Ecosystems Using Machine Learning, in: Proc. of The Italian Conference on CyberSecurity, Volume 3260 of CEUR Workshop Proceedings, 2022, pp. 102–113

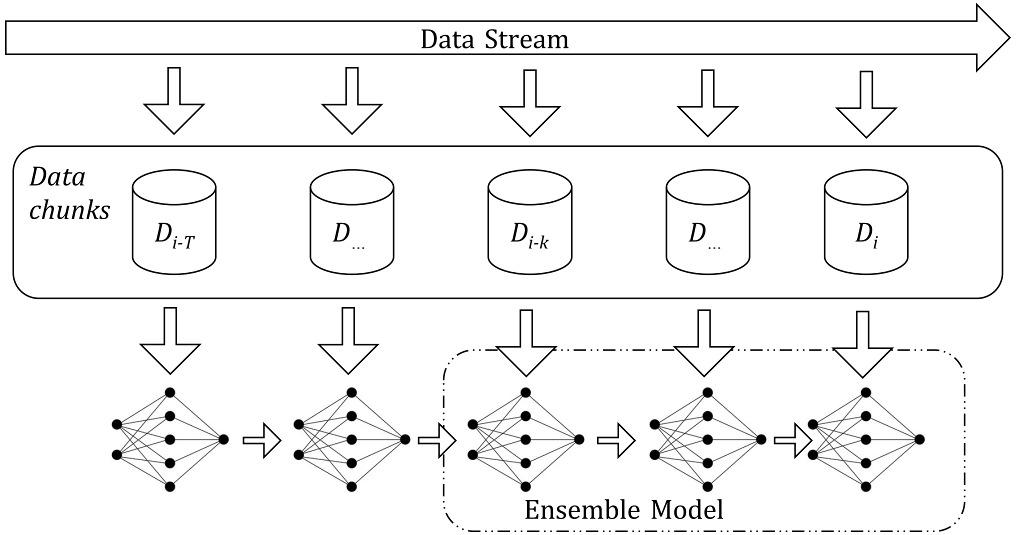
Detection Mechanism



[1] M. Guarascio, M. Zuppelli, N. Cassavia, G. Manco, L. Caviglione, Detection of Network Covert Channels in IoT Ecosystems Using Machine Learning, in: Proc. of The Italian Conference on CyberSecurity, Volume 3260 of CEUR Workshop Proceedings, 2022, pp. 102–113

Ensembling Sparse Autoencoders for Network Covert Channel Detection

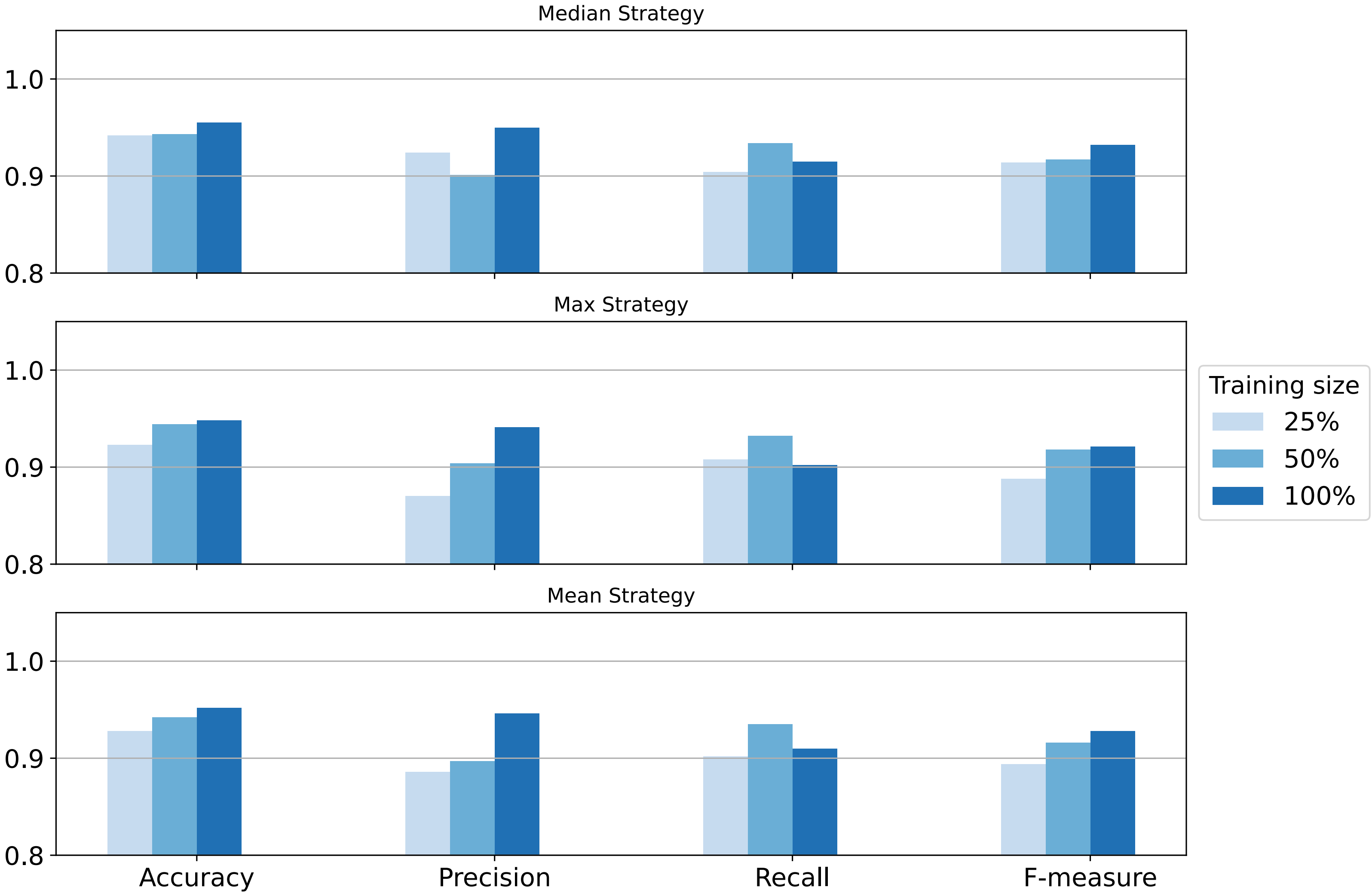
- [1] was extended to evaluate an incremental learning scheme based on an ensemble of autoencoders trained on disjointed data chunks [2]



- The adoption of the ensemble strategy improves the performances compared to using a single autoencoder
  - We obtained ~95% both for the accuracy and the precision

[2] N. Cassavia, L. Caviglione, M. Guarascio, A. Liguori, M. Zuppelli, Ensembling Sparse Autoencoders for Network Covert Channel Detection in IoT Ecosystems, in: Foundations of Intelligent Systems: 26th International Symposium, Springer, 2022, pp. 209–218

Ensembling Sparse Autoencoders for Network Covert Channel Detection



Ital-IA
ITALIA INTELLIGENZA ARTIFICIALE
Terzo Convegno Nazionale
Pisa 29-31 Maggio 2023
cini National Lab AIIS

Ensembling Sparse Autoencoders for Network Covert Channel Detection

Benefits

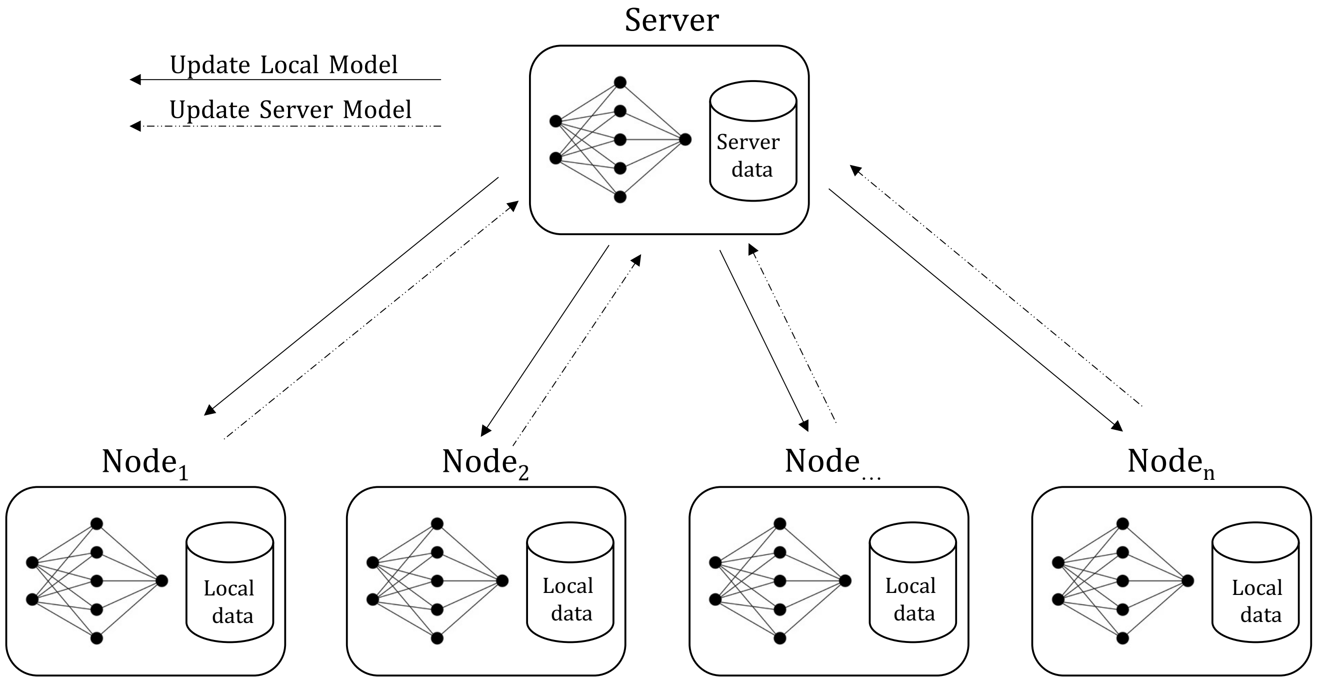
- Incremental learning allows to deploy the ensemble-based model on devices with limited computational storage resources
    - e.g., in home gateways or edge nodes

Limits

- An ensemble-based model requires to set the ensemble size
- Training only against the data available on a single edge
    - Data owners could be not inclined to share them

Revealing Information Hiding through Federated Learning

- Federated Learning (FL) could be useful when information is stored in several data centers, and cannot be moved to learn a detection model in a centralized fashion



Revealing Malicious Contents through Federated Learning

- In [3], we evaluated the benefits of FL-based approaches to detect malicious payloads hidden within high-resolution icons of mobile apps

- Results showcased the effectiveness of the approach
    - Our FL solution achieves performances similar to a centralized approach without the necessity of moving data in a single node

[3] N. Cassavia, L. Caviglione, M. Guarascio, A. Liguori, G. Surace, M. Zuppelli, Federated learning for the efficient detection of steganographic threats hidden in image icons, in: Pervasive Knowledge and Colletive Intelligence on Web and Social Media, Springer Nature Switzerland, Cham, 2023, pp. 83–9

Covert and Hidden Threats Detection

Open Challenges

- Lack of publicly-available datasets
- Class imbalance
- Real data are usually affected by noise
- Errors in classifying infrequent legit behaviors
- Threat-dependent models
- Definition of the boundary between normal and abnormal behaviors

Container Security

- Containerization facilitates the creation, the distribution and the deployment of applications in a lightweight, portable, and scalable manner

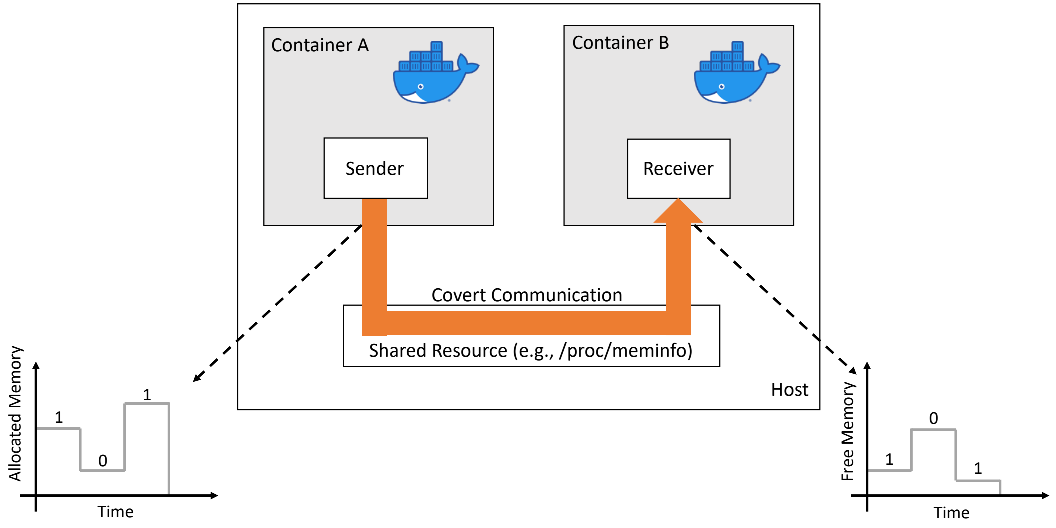
- Despite the various advantages, container security is not fully understood
  - e.g., Docker images may contain vulnerable software or be susceptible to kernel-level vulnerabilities

- Threat actors are exploiting the “imperfect” isolation of containers to leak information or orchestrate attacks via covert channels, e.g., via the /proc filesystem

Container Security

- Container A and Container B can covertly communicate to exfiltrate information or orchestrate attacks (e.g., co-residency attacks)

- To do this, they manipulate a shared resource of the host leveraging its “imperfect” isolation, e.g., the CPU load has a global visibility



Container Security: Example

- For example:
    - A sender process of a container can increase the used memory to alter the overall (host-level) free memory
    - A receiver process of a receiving container can infer the secret message by inspecting the behavior of the overall memory

- A promising detection approach relies on AI. For example:
    - it can search for anomalous “wake-sleep” patterns of processes
    - it can be used to define the “normal” behavior of the containers
    - it can be used to analyze network communications among containers to spot anomalous traffic

Graph Generation

- Cyber attacks can be represented as dynamic graphs
    - e.g., network traffic for intrusion detection, flow of API calls for malware detection
- We plan to devise a deep learning-based approach aiming at predicting graph evolution
- Modeling and predicting the evolution of such graphs could be useful to identify polymorphic cyber attacks
    - e.g., polymorphic malware

Graph Generation

Open Challenges

- Modeling graph evolution is a complex task due to the dynamic nature of the underlying process
    - Continuous changes in the graph structure need flexible architecture

- State-of-the-art systems lack flexibility
    - It is crucial devising architectures that guarantee invariance w.r.t. the input size -- as the changes are not only on topology, but also on dimension

Conclusion

- We discussed the opportunities of using AI to detect emerging threat endowed with covert attacks, especially when targeting realistic scenarios based on IoT or container technologies
- We investigated the main challenges in employing AI-based framework
- We described some preliminary results obtained by adopting Deep Learning architectures

Ital-IA
ITALIA INTELLIGENZA ARTIFICIALE
Terzo Convegno Nazionale
Pisa 29-31 Maggio 2023
cini National Lab AIIS

Thank you for your attention!