Federated Learning for IoT Security

Han Wang, PhD student in RISE Cybersecurity Unit
Supervisor: Shahid Raza, Director of Cybersecurity Unit

han.wang@ri.se
Han Wang
PhD student in RISE Cybersecurity Unit and Uppsala University

Research interests:
Machine Learning for IoT security, Decentralized Learning, Adversarial attack.

Background:
Degree of Master of Science, Uppsala University (dual degree)
Degree of Master of Engineering, National Taiwan Normal University, Taiwan.
Outline

• Background and motivation
• How federated learning works?
• Possibilities and uses cases for federated learning
• Challenges
• Security and Privacy issues
• Applications
Security attack in IoT network

Where machine learning can help?

- Intrusion detection/ Anomaly detection
  - IDS at the edge
  - Forecasting
  - Unsupervised Learning, Outlier detector

- Malware detection
  - Signature matching

- Authentication
  - Fingerprinting, Device Identification
Security Motivation

- Low Power Supply
- Limited storage space
- Limited memory
- A data Integrator in IoT
- Most in sleep mode

Constrained-resource

Industrial IoT
- E-Health
- Smart Home
- Telecom

Vulnerability Database

IoT Device

Powerful Server

Cloud

ML Detection Engine

Information Leak Network Overhead Privacy Problem

Enforcement from GDPR

GDPR

TensorFlowLite

arm MBED

IoT

IoT
Motivation

- Privacy and data ownership, such as GDPR, Privacy-by-design and privacy-by-default.
- High Latency.
- Model personalization and customization.
- Improve cost efficiency on IoT edge device.
Federated Learning

• A distributed ML approach that enabling IoT edge devices to collaboratively train models in a decentralized way and keep the private data staying on the devices at the same time.

• First introduced by McMahan in 2017.

• Google Keyboard

Brendan McMahan and Daniel Ramage, Google AI Blog, April 6, 2017
Federated Learning

Steps:

1. Deploy a global model to every client.
2. Training on the device with local dataset.
3. Aggregate to the cloud and update.
Federated Learning

• Algorithm for aggregation: FedAvg

\[
F^k(w) = \frac{1}{|D_k|} \sum_{j_{k}=1}^{|D_k|} f^k_j \left( w; x^j_k, y^j_k \right)
\]

\[
\min_w \sum_{k=1}^{n} p^k F^k(w),
\]

Algorithm 1: FederatedAveraging

initialze \( w_0 \)

for each round \( t = 1, 2, \ldots \) do

\( S_t \leftarrow \) (random set \( S \) of devices)

for each client \( k \in S_t \) do

\( \omega^k_{t+1} \leftarrow \text{ModelUpdate}(k, \omega_t) \)

\( \omega_{t+1} \leftarrow \sum_{k=1}^{K} \frac{n_k}{n} \omega^k_{t+1} \)

Security Use cases for Federated Learning

- Banking system – Fraud detection
- Health care – Anomaly detection in medical system
- Telecommunication [H2020 CONCORDIA]
  - Preventing flooding attack in 5G network
    (New EU Horizon2020 project on IoT security starts in May)
  - Federated MISP Threat Intelligence Platform
- Connected vehicles – Intrusion detection [H2020 CONCORDIA]
Challenges

• Expensive Communication
  • Model size
  • Communication delay [1]

• System Heterogeneity [2]
  • Variability in hardware, network connectivity, communication bandwidth

• Statistical Heterogeneity
  • Non-independent and identically distributed (Non-IID) data
    - Shared global dataset [3], multi-task, meta-learning
    - Imbalanced data

Security and Privacy Issues

- Adversarial ML: Data poisoning attack
- Dirty-label attack, label-flipping
- Adversarial ML: Model poisoning attack

How to defend?

- Differential Privacy [1]
  - Adding some noise to mask the influence of client on the model
- Secure Multi-Party Computation
  - It aims creating methods for parties to jointly compute a function over their inputs while keeping those inputs private.
  - Adding additional communication round to mask
- Homomorphic Encryption
  - A form of encryption that allows computation on encrypted data
- Hybrid protocols

Applications of Federated Learning in IoT Security
FL4IoT: IoT Device Fingerprinting and Identification using Federated Learning

In collaboration with David Eklund, Shahid Raza, Alina Oprea (Northeastern University, U.S.)
Motivation and Goal

- Unauthorized IoT devices with weak security can become a source of attack to the global Internet. It is therefore necessary to fingerprint and identify connected devices and remove undisclosed or unauthorized devices from the networks.

- We propose a FL approach to generate lightweight fingerprints for devices from unlabeled network traffic, and the fingerprints can help identify a newly observed traffic. The proposed approach is also able to detect spoofed devices.
Dataset: N-BaIoT

Number of instances (one record of packet traffic): 7,062,606
Number of devices: 9

Classes:
- Benign
- Attack:
  - Bashlite:
    - Scan: Scanning the network for vulnerable devices
    - Junk: Sending spam data
    - UDP: UDP flooding
    - TCP: TCP flooding
    - Combo: Sending spam data and opening a connection to a specified IP address and port
  - Mirai:
    - Scan: Automatic scanning for vulnerable devices
    - Ack: Ack flooding
    - Syn: Syn flooding
    - UDP: UDP flooding
    - UDP plain: UDP flooding with fewer options, optimized for higher packet per second (PPS)

Total: 10 classes + 1 class

Results – Device Identification

- Five devices from N-BaloT:
  - PT1: PT_838_Security Camera
  - PT2: PT737E_Security Camera
  - XC1: XCS7_1002_WHT_Security_Camera
  - XC2: XCS7_1003_WHT_Security_Camera
  - DB: Danmini Doorbell
- Overall Accuracy: 96.28% among 22,107 data
Results – Detecting spoofed devices

- Four devices from N-BaIoT:
  - PT1: PT_838_Security Camera
  - XC1: XCS7_1002_WHT_Security_Camera
  - DB: Danmini Doorbell
  - XC_A: Spoofed XC1

- Overall Accuracy: 99.43% among 19,247 traffic data
Non-IID Data Re-balancing at IoT Edge with Peer-to-peer Federated Learning for Anomaly Detection

In collaboration with David Eklund, Shahid Raza, Luis Muñoz-González (Imperial College London, U.K.)
Motivation and Goal

• A “rush-to-market” phenomenon has occurred among the IoT device manufacturers. Released products are usually poorly designed and there is a lack of security considerations. These kinds of devices are easy to be compromised.

• Data are non-IID and extremely imbalanced, which causes degradations of model performance.

• We propose a peer-to-peer FL approach to re-balance the local dataset for anomaly detection.
STOFA Re-balancing techniques

- Random Down-sampling
- Random Over-sampling
- Synthetic Minority Over-sampling Technique (SMOTE)
  - First, find k-nearest neighbors for every sample in minority class.
  - Second, select random one nearest neighbor of the sample.
  - Finally, generate a synthetic points by:
    \[ x = x + \text{rand}(0, 1) \times |x - x_k| \]
Results: On IID imbalanced data

<table>
<thead>
<tr>
<th>N-BaIoT - PT 838 Security Camera</th>
<th>Client A</th>
<th>Client B</th>
<th>Client C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training_benign</td>
<td>11821</td>
<td>11821</td>
<td>15762</td>
</tr>
<tr>
<td>Training_anomaly</td>
<td>23</td>
<td>34</td>
<td>58</td>
</tr>
<tr>
<td>Local_Val_benign</td>
<td>17732</td>
<td>17732</td>
<td>23643</td>
</tr>
<tr>
<td>Local_Val_anomaly</td>
<td>208</td>
<td>312</td>
<td>521</td>
</tr>
</tbody>
</table>
Results: On non-IID imbalanced Data

<table>
<thead>
<tr>
<th>N-BaIoT</th>
<th>Client A</th>
<th>Client B</th>
<th>Client C</th>
</tr>
</thead>
<tbody>
<tr>
<td>PT 838 Security Camera</td>
<td>11821</td>
<td>5590</td>
<td>7927</td>
</tr>
<tr>
<td>XCS7 1002 WHT Security Camera</td>
<td>23</td>
<td>66</td>
<td>102</td>
</tr>
<tr>
<td>Danmini Doorbell</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Train_benign</td>
<td>11821</td>
<td>5590</td>
<td>7927</td>
</tr>
<tr>
<td>Train_anomaly</td>
<td>23</td>
<td>66</td>
<td>102</td>
</tr>
<tr>
<td>Global_benign</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global_anomaly</td>
<td>5067</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What is next?

• Defending FL from Adversarial attack
• Trust communication between clients In FL
• Federated MISP for IoT network
Thank you very much!

han.wang@ri.se

shahid.raza@ri.se